AXIS Camera Station Pro Secure Entry

Manual del usuario

Acerca de

Secure Entry es un componente de AXIS Camera Station Pro. Úselo para añadir dispositivos y gestionar programas. Para obtener más información, consulte el *AXIS Camera Station Pro User Manual (manual de usuario)*.

Configure el control de acceso

Si agrega una controladora de accesos en red al sistema, puede configurar el hardware de control de acceso en AXIS Camera Station versión 6.x o posterior.

Para obtener un flujo de trabajo adecuado que permita configurar una controladora de accesos en red de Axis en AXIS Camera Station Pro Secure Entry, consulte *Configurar una controladora de accesos en red de Axis*.

Nota

Antes de empezar, haga lo siguiente:

- Actualice la versión del AXIS OS del controlador en **Configuration (Configuración) > Devices (Dispositivos) > Management (Gestión)**.
- Fije la fecha y la hora para el controlador en **Configuration > Devices > Management (Configuración > Dispositivos > Administrar)**.
- Active HTTPS en el controlador en **Configuration > Devices > Management (Configuración > Dispositivos > Administrar)**.

Workflow to configure access control (Flujo de trabajo para configurar el control de acceso)

1. Para editar los perfiles de identificación predefinidos o crear un nuevo perfil de identificación, consulte *Perfiles de identificación, on page 22*.
2. Para utilizar una configuración personalizada para los formatos de tarjeta y la longitud del PIN, consulte *Formatos de tarjeta y PIN, on page 24*.
3. Agregue una puerta y aplique un perfil de identificación a la puerta. Vea *Agregar una puerta, on page 7*.
4. Configure la puerta.
   - *Agregar un monitor de puerta, on page 14*
   - *Agregar entrada de emergencia, on page 16*
   - *Agregar un lector, on page 17*
   - *Agregar un dispositivo REX, on page 19*
5. Agregue una zona y agregue puertas a la zona. Vea *Agregar una zona, on page 20*.

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 que se enumeran a continuación solo se aplican cuando se actualiza desde su versión original recomendada de AXIS Camera Station Pro 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 AXIS Camera Station Pro.
- **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. Supongamos que está utilizando la versión 6.5 de AXIS Camera Station Pro y actualiza todos los dispositivos a la versión 12.0.86.2 de AXIS OS recomendada. Entonces, la versión 12.0.86.2 de AXIS OS se convierte en la versión mínima compatible para su sistema en adelante.
- **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 AXIS Camera Station Pro. 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 AXIS Camera Station Pro.
- **Futuras recomendaciones de AXIS OS:** Siga siempre la versión de AXIS OS recomendada para la versión correspondiente de AXIS Camera Station Pro con el fin de garantizar la estabilidad del sistema y una compatibilidad total.
- **Control de cambios:** Cambiar las versiones del firmware entre 10.12.xx y 11.0.xx o superior requiere un restablecimiento a valores de fábrica.

La siguiente tabla indica la versión mínima y recomendada del AXIS OS para cada versión de AXIS Camera Station Pro:

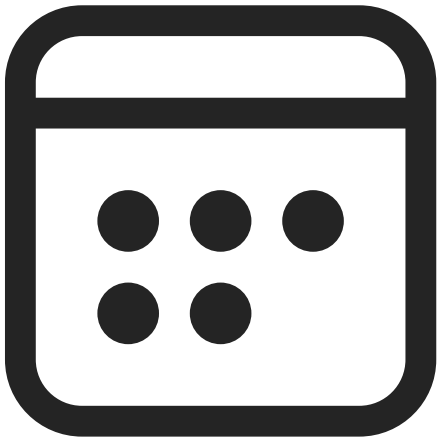
Versión de AXIS Camera Station	Versión mínima de AXIS OS	Versión recomendada de AXIS OS
Pro 6.15	12.5.68.1	12.8.55.1
Pro 6.14	12.5.68.1	12.8.55.1
Pro 6.13	12.5.68.1	12.6.102.1

La siguiente tabla indica la versión mínima y recomendada del AXIS OS para cada versión de AXIS Camera Station 5:

Versión de AXIS Camera Station	Versión recomendada de AXIS OS
5.59	12.4.68.1
5.58	12.4.68.1
5.57	11.8.20.2

Puertas y zonas

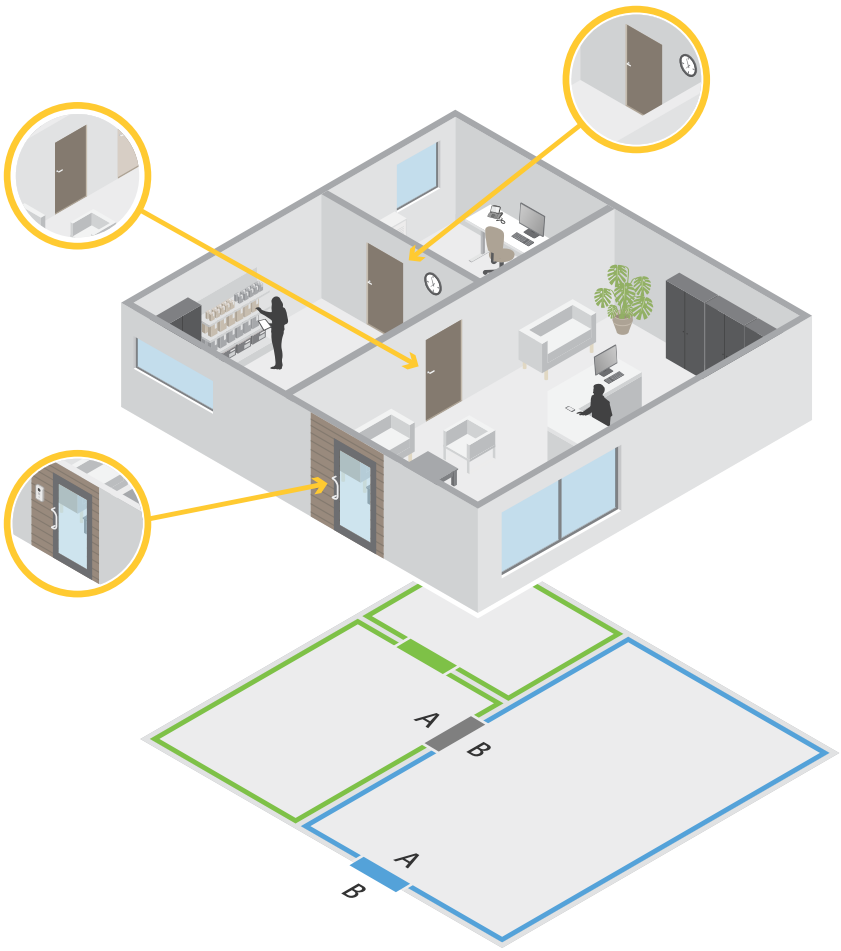
Vaya a **Configuration > Access control > Doors and zones (Configuración > Control de acceso > Puertas y zonas)** para obtener una visión general y configurar puertas y zonas.

 **Acciones manuales**	Establecer manualmente el estado de una puerta. Seleccione una de las siguientes opciones: **Reset (Restablecer)** (seguir las reglas del sistema), **Grant access (Conceder acceso)** (desbloquear la puerta durante 7 segundos), **Unlock (Desbloquear)** (mantener la puerta desbloqueada), **Lock (Bloquear)** (mantener la puerta bloqueada) o **Lockdown (Bloqueo total)** (nadie puede entrar ni salir).
 **Desbloquear programadores**	Configure una programación para desbloquear automáticamente las puertas a horas específicas. Las puertas permanecen cerradas con llave el resto del tiempo. Para que la primera persona deba abrir la puerta manualmente antes de que se active la programación, active **First person in (Primera persona)**.
Perfil de identificación	Cambie el perfil de identificación en las puertas.
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)**.
Canal seguro	Active o desactive OSDP Secure Channel para un lector específico.

Puertas	
Nombre	El nombre de la puerta.
Tipo	El tipo de configuración de la puerta.
Dispositivo	El dispositivo conectado a la puerta.

Dirección IP	La dirección IP del 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.
Batería	El estado de la batería del controlador de la puerta.
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. • **Firmware antiguo:** El dispositivo posee una versión de firmware obsoleta. Actualice el firmware para garantizar un rendimiento y seguridad óptimos.
Zonas	
Nombre	Nombre de la zona.
Número de puertas	El número de puertas incluidas en la zona.
Nivel de seguridad	El nivel de seguridad aplicado a 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. Los controladores múltiples admiten configuraciones de bloqueo adicionales.
- Si un controlador de puerta no tiene puertas y está utilizando una nueva versión de AXIS Camera Station Pro Secure Entry con un firmware 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 firmware anterior si ya hay una puerta existente.

Cree una nueva configuración de puerta para agregar una puerta:

1. Vaya a **Configuration (Configuración) > Access control (Control de acceso) > Doors and zones (Puertas y zonas)**.

2. Haga clic en + **Add door (Añadir una puerta)** y seleccione un tipo de puerta en la lista desplegable.

Tipos de puerta	
Puerta	Puerta estándar con monitor que admite bloqueos y lectores. Requiere un controlador de puerta.
Puerta inalámbrica	Puerta configurable con bloqueos inalámbricos y hubs de comunicación ASSA ABLOY Aperio®. Para obtener más información, consulte *Agregar un bloqueo inalámbrico, on page 12*.
Puerta de supervisión	Puerta que puede notificar si está abierta o cerrada. Para obtener más información, consulte *Agregar una puerta de supervisión, on page 15*.
Puerta aprovisionada	Puerta que se puede añadir como marcador de posición en el sistema sin necesidad de seleccionar el hardware.
Planta	Un tipo de puerta para el control de ascensores que autentifica el acceso a las plantas mediante lectores de tarjetas. Para obtener más información, consulte *Añadir una planta para el control de ascensores BETA, on page 15*.

3. Introduzca un nombre para la puerta y seleccione un controlador de puerta en el menú desplegable **Device (Dispositivo)** para asociarlo a esta. El controlador aparece en gris cuando no se puede agregar otra puerta, cuando está sin conexión o si HTTPS no está activo.
4. Haga clic en **Next (Siguiente)** para ir a la página de configuración de la puerta.
5. En el menú desplegable **Primary lock (Cerradura principal)**, seleccione un puerto de relé.
6. Para configurar dos cerraduras en la puerta, seleccione un puerto de relé del menú desplegable **Secondary lock (Cerradura secundaria)**.
7. Seleccione un perfil de identificación. Vea *Perfiles de identificación, on page 22*.
8. Configure los ajustes de puerta. Consulte *Ajustes de puerta, on page 9*.
9. *Agregar un monitor de puerta, on page 14*
10. *Agregar entrada de emergencia, on page 16*
11. *Agregar un lector, on page 17*
12. *Agregar un dispositivo REX, on page 19*
13. Configure el nivel de seguridad. Vea *Nivel de seguridad de puerta, on page 10*.
14. Haga clic en **Save (Guardar)**.

Copiar configuración de una puerta:

1. Vaya a **Configuration (Configuración) > Access control (Control de acceso) > Doors and zones (Puertas y zonas)**.
2. Haga clic en + **Add door (Agregar puerta)**.
3. Introduzca un nombre para la puerta y seleccione un controlador de puerta en el menú desplegable **Device (Dispositivo)** para asociarlo a esta.
4. Haga clic en **Next (Siguiente)**.

5. 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.
6. Cambie los ajustes si lo desea.
7. Haga clic en **Save (Guardar)**.

Para eliminar una puerta:

1. vaya a **Configuration > Access control > Doors and zones > Doors (Configuración > Control de acceso > Puertas y zonas > Puertas)**.
2. Seleccione una puerta en la lista.
3. Haga clic en **Remove (Eliminar)** y confirme.

Agregar y configurar puertas y zonas

Ajustes de puerta

Para editar una puerta:

1. Vaya a **Configuration > Access control > Door and Zones (Configuración > Control de acceso > Puerta y zonas)**.
2. Seleccione la puerta que desea editar.
3. Haga clic en **Edit (Modificar)**.
4. Cambie los ajustes y haga clic en **Save (Guardar)**.

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.
Puerta forzada	Seleccione si desea que el sistema active una alarma cuando se fuerce una puerta. Requiere un sensor de posición de puerta (DPS).
Puerta abierta durante demasiado tiempo	Seleccione si desea que el sistema active una alarma cuando una puerta permanezca abierta demasiado tiempo.

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.

Cerradura – 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 **Configuration (Configuración)** > **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.

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 **Configuration (Configuración)** > **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**.

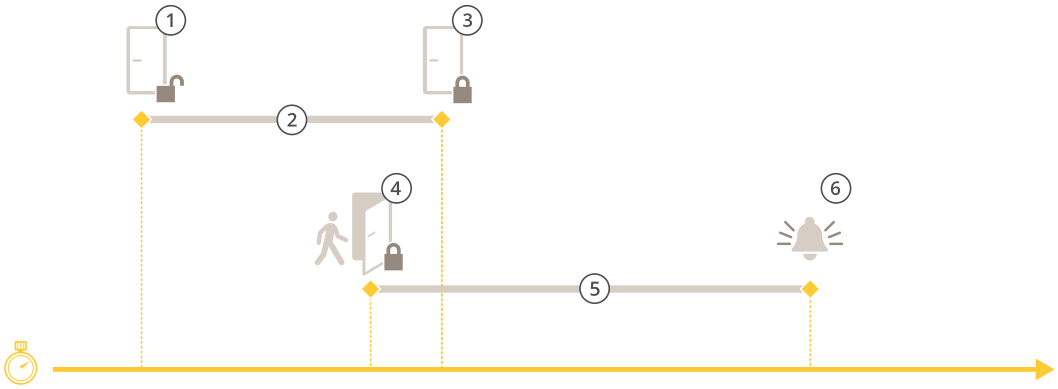
Regla de dos personas	
Lateral A y **Lateral B**	Seleccione los lados de la puerta en los que utilizar la regla.
Horarios	Seleccione cuándo está activa la regla.
Tiempo de espera (segundos)	El tiempo de espera es el tiempo máximo permitido entre los barridos de tarjeta u otro tipo de credencial válida.

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

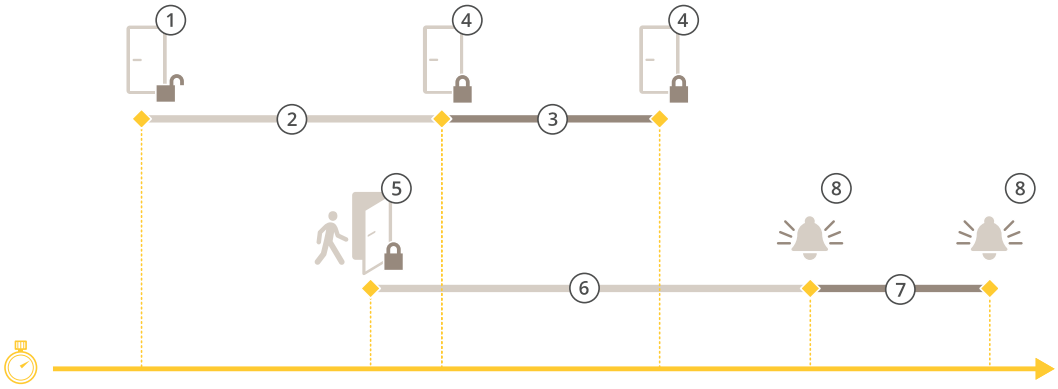
1. Vaya a **Configuration (Configuración)** > **Access control (Control de acceso)** > **Doors and zones (Puertas y zonas)**.
2. Seleccione la puerta para la que desea configurar un nivel de seguridad.
3. Haga clic en **Edit (Modificar)**.
4. Haga clic en **Security level (Nivel de seguridad)**.
5. Active el **barrido doble**.
6. Haga clic en **Aplicar**.
7. Aplique un **barrido doble** al titular de la tarjeta.
   7.1. Abra una pestaña **Gestión de accesos**.
   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 bloqueo inalámbrico

AXIS Camera Station Pro Secure Entry admite los bloqueos inalámbricos de ASSA ABLOY Aperio® y los concentradores de comunicaciones. El bloqueo inalámbrico se conecta al sistema a través de un concentrador de comunicaciones Aperio conectado al conector RS485 del controlador de puerta. Puede conectar 16 bloqueos inalámbricos a un controlador de puerta.

Nota

- La configuración requiere que el controlador de puerta de Axis tenga AXIS OS versión 11.6.16.1 o posterior.
- La configuración requiere una licencia de extensión de controlador de puerta AXIS válida.
- La hora en el controlador de puerta Axis y el servidor de AXIS Camera Station Pro Secure Entry debe estar sincronizada.
- Antes de comenzar, use la aplicación de Aperio compatible con ASSA ABLOY para emparejar los bloqueos Aperio con el concentrador de Aperio.
- Solo se puede conectar un concentrador de comunicaciones Aperio por cada conector RS485. No se admite la función de multiconexión.
- Los bloqueos inalámbricos no seguirán los horarios de desbloqueo cuando esté sin conexión.

1. Acceda al controlador de puerta.
   1.1. Vaya a **Configuración > Dispositivos > Otros dispositivos**.
   1.2. Abra la interface web del controlador de puerta conectado al concentrador de comunicaciones Aperio.
2. Active AXIS Door Controller Extension (Extensión de controlador de puerta AXIS).
   2.1. En la interface web del controlador de puerta, vaya a **Apps (Aplicaciones)**.
   2.2. Abra el menú contextual de AXIS Door Controller Extension .
   2.3. Haga clic en **Activate license with a key (Activar licencia con una clave)** y seleccione su licencia.
   2.4. Active **AXIS Door Controller Extension (Extensión de controlador de puerta AXIS)**.
3. Conecte el bloqueo inalámbrico al controlador de puerta a través del concentrador de comunicaciones.
   3.1. En la interfaz web del controlador de puerta, vaya a **Access control > Wireless locks (Control de acceso > Bloqueos inalámbricos)**.
   3.2. Haga clic en **Connect communication hub (Conectar concentrador de comunicaciones)**.
   3.3. Introduzca un nombre para el concentrador y haga clic en **Connect (Conectar)**.
   3.4. Haga clic en **Connect wireless lock (Conectar bloqueo inalámbrico)**.
   3.5. Seleccione la dirección de bloqueo y las capacidades del bloqueo que desea agregar y haga clic en **Save (Guardar)**.
4. Agregue y configure la puerta con el bloqueo inalámbrico.
   4.1. En AXIS Camera Station Pro Secure Entry, vaya a **Configuration > Access control > Doors and zones (Configuración > Control de acceso > Puertas y zonas)**.
   4.2. Haga clic en **Add door (Agregar puerta)**.
   4.3. Seleccione el controlador de puerta conectado al concentrador de comunicaciones Aperio, seleccione **Wireless door (Puerta inalámbrica)** como **Door type (Tipo de puerta)**.
   4.4. Haga clic en **Next (Siguiente)**.
   4.5. Seleccione su **Wireless lock (Bloqueo inalámbrico)**.

4.6. Defina los lados de puerta A y B y agregue sensores. Para obtener más información, vea *Puertas y zonas, on page 4*.

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

Una vez que haya conectado el bloqueo inalámbrico, podrá ver el nivel de batería y el estado en la descripción general de las puertas.

Nivel de batería	Acción
Bien	Ninguno
Bajo	El bloqueo funciona según lo esperado, pero debe sustituir la batería antes de que el nivel de batería sea crítico.
Crítico	Cambie la batería. Es posible que el bloqueo no funcione según lo esperado.

Estado de bloqueo	Acción
En línea	Ninguno
Atasco de bloqueo	Solucione cualquier problema mecánico con el bloqueo.

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. Vea *Agregar una puerta, on page 7*.
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)**. Vea *Entradas con supervisión, on page 22*.

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 firmware 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 AXIS Camera Station Pro, vaya a **Configuration (Configuración)** > **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**.

Añadir una planta para el control de ascensores BETA

Una planta es un tipo de puerta utilizada para controlar el acceso a las plantas del ascensor. Al añadir una planta, se crea un recurso de ascensor que agrupa todas las plantas de ese ascensor. Cada planta utiliza un lector de tarjetas dentro de la cabina del ascensor para autentificar a los usuarios antes de permitir el acceso a dicha planta.

Antes de empezar, necesita:

- Añadir un controlador de puerta de red compatible a su sistema, como *A1610*, *A1710-B* o *A1810-B*.
- Un *A9910 I/O Relay Expansion Module (Módulo de expansión de relés de E/S A9910)* para relés adicionales. Para obtener instrucciones sobre cómo añadir su módulo a un controlador, consulte .

Nota

Esta función está en fase beta y actualmente solo admite hasta 16 plantas y lectores de tarjetas.

Para configurar una planta:

1. Vaya a **Configuration (Configuración) > Access control (Control de acceso) > Doors and zones (Puertas y zonas)**.
2. Haga clic en **Add (Añadir)** y seleccione **Floor (Planta)** BETA.
3. Introduzca un nombre para la planta.
4. Seleccione su controlador.

5. En **Elevator (Ascensor)**, seleccione un ascensor existente o haga clic en **Create new elevator (Crear nuevo ascensor)** para añadir uno nuevo y, a continuación, introduzca un nombre.
6. En **Side A (Lado A)**, seleccione **Card reader (Lector de tarjetas)** y configure su lector. El **Side B (Lado B)** no se puede configurar por motivos de seguridad.
7. Haga clic en **Save and add new (Guardar y añadir nueva)** para añadir más plantas al mismo ascensor. La configuración del ascensor y del lector se mantiene para la siguiente planta. Tenga en cuenta que esta opción solo estará disponible si su controlador tiene relés disponibles.
8. Haga clic en **Save (Guardar)** una vez que añadida la planta. Las plantas aparecen conforme a la convención "Nombre del ascensor - Nombre de la planta". Por ejemplo: "Lado oeste - Planta 1".

Nota

- Los lectores empleados en varias plantas solo se pueden editar en la primera planta en la que se añadieron.
- Los ascensores se eliminan automáticamente al eliminar todas las plantas relacionadas.

Agregar entrada de emergencia

Puede agregar y configurar una entrada de emergencia para iniciar una acción que bloquee o desbloquee la puerta. También puede configurar cómo conectar el circuito.

1. Vaya a la página de configuración de la puerta. Vea *Agregar una puerta, on page 7*.
2. En **Sensors (Sensores)**, haga clic en **Add (Agregar)**.
3. Seleccione **Emergency input (Entrada de emergencia)**.
4. En **Emergency state (Estado de emergencia**, seleccione la conexión del circuito.
5. Para ignorar los cambios de estado antes de entrar en un nuevo estado estable, establezca un **Debounce time (ms) [Tiempo antirrebote (ms)]**.
6. Seleccione la **Emergency action (Acción de emergencia)** que se activa cuando la puerta recibe señal de estado de emergencia.

Estado de emergencia	
Circuito abierto	El circuito de entrada de emergencia está normalmente cerrado. La entrada de emergencia envía una señal de estado de emergencia cuando el circuito está abierto.
Circuito cerrado	El circuito de entrada de emergencia está normalmente abierto. La entrada de emergencia envía una señal de estado de emergencia cuando el circuito está cerrado.

Acción de emergencia	
Abrir puerta	La puerta se desbloquea cuando recibe la señal de estado de emergencia.
Cerrar puerta	La puerta se bloquea cuando recibe la señal de estado de emergencia.

Añadir un lector IP

Puede utilizar un intercomunicador de red Axis u otro dispositivo con capacidad IP como lector. Antes de poder asignarlo a una puerta, debe añadir el dispositivo a AXIS Camera Station Pro.

Nota

Antes de comenzar, asegúrese de que el lector IP esté encendido y conectado a la misma red que AXIS Camera Station Pro.

1. Vaya a **Configuration (Configuración) > Devices (Dispositivos) > Add devices (Añadir dispositivos)**.
2. Seleccione su lector IP de la lista de dispositivos detectados y haga clic en **Add (Añadir)**.
3. Introduzca las credenciales del dispositivo cuando se le solicite.

Una vez añadido el dispositivo, podrá asignarlo a una puerta. Consulte *Agregar un lector, on page 17*.

Agregar un lector

Puede configurar un controlador de puerta para que admita varios lectores cableados. Puede optar por añadir un lector a uno o a ambos lados de la 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)**. Vea *Puertas y zonas, on page 4*.

Nota

- También puede añadir hasta 16 lectores Bluetooth a un controlador de puerta. Para obtener más información, consulte *Añadir un lector Bluetooth, on page 18*.
- Si utiliza un intercomunicador de red Axis como lector de IP, el sistema utiliza la configuración de PIN establecida en la página web del dispositivo.

1. Vaya a la página de configuración de la puerta. Vea *Agregar una puerta, on page 7*.
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.

Para obtener información sobre cómo instalar un lector de códigos de barras AXIS, consulte *Instalar AXIS Barcode Reader, on page 28*.

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.
Lector de IP	En el caso de lectores de IP, seleccione **IP reader (Lector de IP)** y seleccione un dispositivo del menú desplegable. Es posible utilizar los intercomunicadores de red Axis como lectores IP.

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. Vea *Entradas con supervisión, on page 22*.

Añadir un lector Bluetooth

Puede utilizar el AXIS A4612 Network Bluetooth Reader para ampliar los límites de puertas cableadas de los controladores de puertas Axis, que permiten asignar hasta 16 de estos lectores a su propia puerta. Cada lector puede gestionar la cerradura de la puerta, la solicitud de salida (REX) y el interruptor de posición de la puerta (DPS).

Añadir y utilizar estos lectores no requiere ninguna licencia adicional.

Para añadir un AXIS A4612 Network Bluetooth Reader a una puerta:

1. Asegúrese de haber emparejado el AXIS A4612 con el controlador de puerta. Consulte *Utilice la aplicación AXIS Mobile Credential como credencial Bluetooth, on page 19*.
2. Vaya a la página de configuración de la puerta. Consulte *Agregar una puerta, on page 7*.
3. En uno de los lados de la puerta, haga clic en **Add (Añadir)** y, a continuación, en **Card reader (Lector de tarjetas)**.
4. Seleccione **IP reader (Lector IP)** y elija el AXIS A4612 emparejado en el menú desplegable. Si desea utilizar este lector para emparejar credenciales, márquelo para emparejamiento. Haga clic en **Añadir**.
5. En la pestaña **Overview (Descripción general)**, modifique el perfil de identificación. Puede utilizar los perfiles **Tap in app (Tocar la aplicación)** o **Touch reader (Tocar el lector)** si solo tiene el AXIS A4612 conectado a un lado de la puerta y utiliza un REX en el otro.

Utilice la aplicación AXIS Mobile Credential como credencial Bluetooth

En este ejemplo se muestra cómo agregar un AXIS A4612 Bluetooth Reader a nuestro sistema para permitir que los titulares de tarjetas desbloqueen las puertas mediante la aplicación móvil de AXIS Mobile Credential.

1. Instale el lector de Bluetooth y conéctelo a una controlador de puerta.
2. Agregue el lector Bluetooth al controlador de puerta de la interfaz web.
   2.1. Acceda al controlador de puerta y vaya a **Peripherals (Periféricos)** > **Readers (Lectores)**.
   2.2. Haga clic en **Add reader (Agregar lector)**.
   2.3. Introduzca la información necesaria en el cuadro de diálogo **Add Bluetooth reader (Agregar lector de Bluetooth)**.
   2.4. Haga clic en **Añadir**.
3. Agregue el lector de Bluetooth a una puerta en AXIS Camera Station Pro.
   3.1. Vaya a **Configuration (Configuración)** > **Access control (Control de acceso)** > **Doors and zones (Puertas y zonas)**.
   3.2. Seleccionar la puerta que desea agregar al lector de Bluetooth y haga clic en **Edit (Editar)**.
   3.3. Haga clic en **+ Add (+ Agregar)** en el lado de la puerta donde está ubicado el lector de Bluetooth.
   3.4. Seleccione **Card reader (Lector de tarjetas)**.
   3.5. En **Add IP reader (Agregar lector de IP)**, seleccione **IP reader (Lector de IP)**.
   3.6. En **Select IP reader (Seleccionar lector de IP)**, seleccione el lector de Bluetooth.
   3.7. Haga clic en **Añadir**.
4. Seleccione un lector de Bluetooth para el emparejamiento. Debe hacerlo para al menos un lector de Bluetooth en el sistema.
   4.1. Seleccione el lector de Bluetooth que acaba de agregar.
   4.2. Haga clic en **Edit (Modificar)**.
   4.3. En **Edit bluetooth reader (Editar lector de Bluetooth)**, seleccione **Use this reader for pairing (Usar este lector para emparejamiento)**.
   4.4. Haga clic en **Aplicar**.
5. Elija el perfil de identificación **Tap in app (Tocar la aplicación)** o **Touch reader (Tocar el lector)**. Consulte *Perfiles de identificación, on page 22* para obtener más información.
6. Agregue la credencial móvil al titular de la tarjeta. Vea *Agregar credenciales, on page 35*.
7. Empareje la credencial móvil con el lector de emparejamiento.
   7.1. Lleve el teléfono móvil del titular de la tarjeta al lector de Bluetooth habilitado emparejado.
   7.2. Siga las instrucciones proporcionadas en el correo electrónico enviado al titular de la tarjeta.

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. Vea *Agregar una puerta, on page 7*.
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)**. Vea *Entradas con supervisión, on page 22*.

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. Consulte *Ejemplo de puertas y zonas, on page 7* para acceder a una descripción general.

1. vaya a **Configuration > Access control > Doors and zones > Zones (Configuración > Control de acceso > Puertas y zonas > 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 **Configuration > Access control > Doors and zones > Zones (Configuración > Control de acceso > Puertas y zonas > 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 **Configuration > Access control > Doors and zones > Zones (Configuración > Control de acceso > Puertas y zonas > 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 **Configuration (Configuración)** > **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. Vea *Agregar un monitor de puerta, on page 14*.
- Conexión entre el controlador de puerta y el lector que utiliza protocolos Wiegand. Vea *Agregar un lector, on page 17*.
- Conexión entre el controlador de puerta y el dispositivo REX. Vea *Agregar un dispositivo REX, on page 19*.

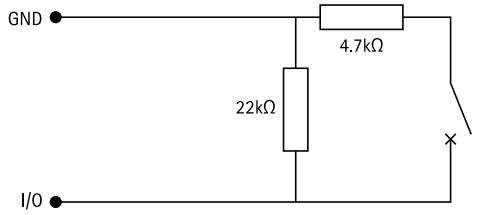
Para utilizar entradas supervisadas:

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 KΩ parallel resistor and a 4.7 KΩ serial resistor (Primera conexión en paralelo con una resistencia de 22 KΩ en paralelo y una resistencia de 4,7 KΩ 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

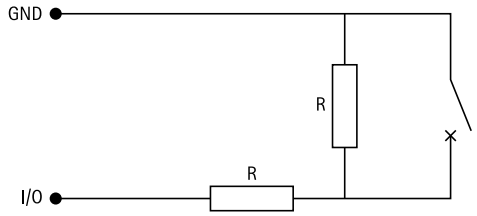
Parallel first connection (Primera conexión en paralelo)

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



Primera conexión en serie

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



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.

Nota

Debe utilizar el QR dinámico y el PIN juntos.

Vaya a **Configuration > Access control > Identification profiles (Configuración > Control de acceso > Perfiles de identificación)** para crear, editar o eliminar perfiles de identificación.

Perfiles de identificación disponibles:

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.

QR – Los titulares de tarjeta deben mostrar el código QR® a la cámara para acceder a la puerta. Puede usar el perfil de identificación QR para el QR estático y para el QR dinámico.

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

Tocar la aplicación – Los titulares de tarjeta deben tocar la credencial en la aplicación móvil de AXIS Camera Station mientras se encuentra en el rango del lector de Bluetooth.

Tocar el lector – Los titulares de tarjeta deben tocar la lector Bluetooth mientras llevan un teléfono móvil con una credencial móvil.

*QR Code es una marca comercial registrada de DensoWave Incorporated en Japón y otros países.

Crear un perfil de identificación

1. Vaya a **Configuration > Access control > Identification profiles (Configuración > Control de acceso > Perfiles de identificación)**.
2. Haga clic en **Create identification profile (Crear perfil de identificación)**.
3. Introduzca un nombre para el 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. Para el Lado A, haga clic en **+ Add (Añadir)**, seleccione un tipo de identificación y una programación.
   - Para exigir a los titulares de tarjetas que utilicen más de un tipo de identificación, seleccione varios tipos en la misma fila.
   - Para permitir que los titulares de tarjetas utilicen cualquiera de los dos tipos, vuelva a hacer clic en **+ Add (Añadir)** y añada otra fila.
6. Para el Lado B, haga clic en **+ Add (Añadir)**, seleccione un tipo de identificación y una programación.
7. Haga clic en **OK**.

Establecer perfiles de identificación

Editar un perfil de identificación

1. Vaya a **Configuration > Access control > Identification profiles (Configuración > Control de acceso > 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**.

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.

Eliminar un perfil de identificación

1. Vaya a **Configuration > Access control > Identification profiles (Configuración > Control de acceso > 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**.

Restablecer un formato de tarjeta predefinido

1. Vaya a **Configuration > Access Control > Card formats and PIN (Configuración > Control de acceso > Formatos de tarjeta y PIN)**.
2. Haga clic en para restablecer un formato de tarjeta al mapa de campos predeterminado.

Formatos de tarjeta y PIN

El formato de una tarjeta define cómo un lector de tarjetas interpreta los datos de la misma. Existen formatos de tarjeta predefinidos que puede usar o editar; además, puede crear formatos de tarjeta personalizados

Vaya a **Configuration > Access Control > Card formats and PIN (Configuración > Control de acceso > 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.

Configuración de PIN

1. Vaya a **Configuration > Access Control > Card formats and PIN (Configuración > Control de acceso > 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**.

Crear un formato de tarjeta

1. Vaya a **Configuration > Access Control > Card formats and PIN (Configuración > Control de acceso > 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.
- Los formatos de tarjeta predefinidos se pueden editar, pero no eliminar. Para deshacer cualquier cambio realizado en un formato predefinido, haga clic en el icono de reinicio para restablecer su configuración predeterminada. Podrá eliminar los formatos de tarjeta que haya creado.

ⓘ	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).

Configurar formatos de tarjeta

Editar un formato de tarjeta

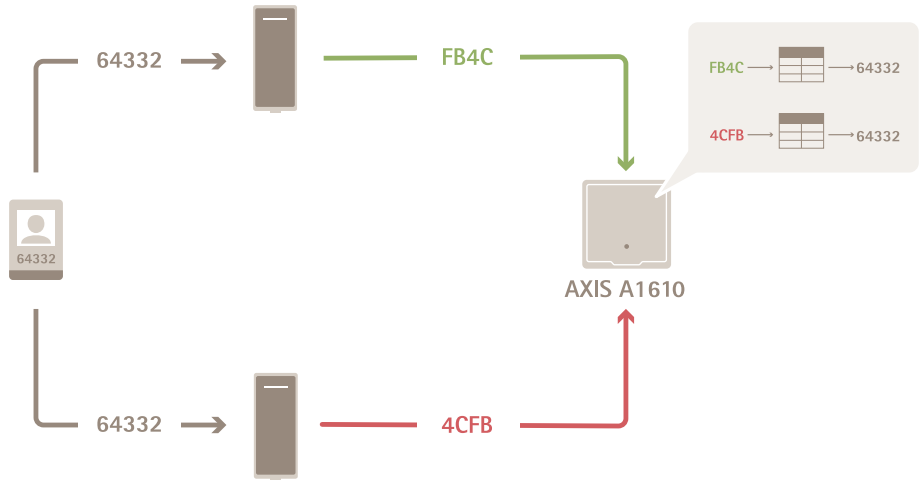
1. Vaya a **Configuration > Access Control > Card formats and PIN (Configuración > Control de acceso > Formatos de tarjeta y PIN)**.
2. Seleccione un formato de tarjeta y haga clic en .
3. Si edita un formato de tarjeta predefinido, solo puede editar **Invert bit order (Invertir orden de bits)** e **Invert 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 **Configuration > Access Control > Card formats and PIN (Configuración > Control de acceso > Formatos de tarjeta y PIN)**.
2. Seleccione un formato de tarjeta personalizado, haga clic en y en **Yes (Sí)**.

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.

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.

Formato de tarjeta Wiegand estándar de 26 bits

1 *Paridad líder*
2 *Código de instalación*
3 *Número de tarjeta*

4 *Paridad de cola*

Comunicación cifrada

Canal seguro OSDP

AXIS Camera Station 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 **Configuration > Access control > Encrypted communication (Configuración > Control de acceso > 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)*.

Nota

Si la unidad de control de acceso, el host o el panel admiten el canal seguro OSDP, recomendamos habilitarlo en el dispositivo lector para aumentar la seguridad de la comunicación. Para habilitar el canal seguro, active el interruptor DIP n.° 6 en el dispositivo lector.

La clave de cifrado se transmite en texto sin formato durante la configuración inicial, por lo que todo el cableado y los dispositivos RS485 deben estar bajo supervisión durante ese proceso.

AXIS Barcode Reader

AXIS Barcode Reader es una aplicación que se puede instalar en cámaras Axis. La controladora de acceso Axis utiliza la clave de autentificación de periféricos externos para otorgar acceso y autentificar el AXIS Barcode Reader y el AXIS License Plate Verifier. Para obtener un flujo de trabajo adecuado que permita configurar AXIS License Plate Verifier en AXIS Camera Station Pro, consulte .

Instalar AXIS Barcode Reader

1. Descargue el archivo de instalación de la aplicación de *axis.com*.
2. Vaya a la página web de su intercomunicador o cámara Axis.
3. Instale la aplicación.
4. Active la licencia.
5. Inicie la aplicación.
6. Recomendamos cambiar el siguiente ajuste de la cámara para obtener una precisión QR mejor.
   6.1. Vaya a los ajustes de la cámara.
   6.2. En **Image > Exposure (Imagen > Exposición)**, mueva el control **Blur-noise trade-off (Compensación de desenfoque-ruido)** hacia el centro.

Configurar AXIS Barcode Reader

1. Para cambiar el perfil de identificación QR, vaya a **Configuration (Configuración) > Access control (Control de acceso) > Identification profiles (Perfiles de identificación)** y haga clic en . Consulte *Perfiles de identificación*.
2. Agregar una puerta. Consulte *Agregar una puerta*.
3. Seleccione **QR** como perfil de identificación de esta puerta. Consulte *Ajustes de puerta*.
4. Agregue un lector de códigos de barras. Consulte *Agregar un lector*.
   4.1. Bajo un lado de la puerta, haga clic en **Add reader (Agregar lector)**.
   4.2. Seleccione **AXIS Barcode Reader (Lector de códigos de barras de AXIS)** en la lista desplegable **Reader type (Tipo de lector)**. Introduzca un nombre y haga clic en **OK (Aceptar)**.

1. Para cambiar el perfil de identificación QR, vaya a **Configuration (Configuración) > Access control (Control de acceso) > Identification profiles (Perfiles de identificación)** y haga clic en . Consulte *Perfiles de identificación*.
2. Agregar una puerta. Consulte *Agregar una puerta*.
3. Seleccione **QR** como perfil de identificación de esta puerta. Consulte *Ajustes de puerta*.
4. Agregue un lector de códigos de barras. Consulte *Agregar un lector*.
   4.1. Bajo un lado de la puerta, haga clic en **Add reader (Agregar lector)**.
   4.2. Seleccione **AXIS Barcode Reader (Lector de códigos de barras de AXIS)** en la lista desplegable **Reader type (Tipo de lector)**. Introduzca un nombre y haga clic en **OK (Aceptar)**.

1. Para cambiar el perfil de identificación QR, vaya a **Configuration (Configuración) > Access control (Control de acceso) > Identification profiles (Perfiles de identificación)** y haga clic en . Consulte *Perfiles de identificación*.
2. Agregar una puerta. Consulte *Agregar una puerta*.
3. Seleccione **QR** como perfil de identificación de esta puerta. Consulte *Ajustes de puerta*.
4. Agregue un lector de códigos de barras. Consulte *Agregar un lector*.
   4.1. Bajo un lado de la puerta, haga clic en **Add reader (Agregar lector)**.
   4.2. Seleccione **AXIS Barcode Reader (Lector de códigos de barras de AXIS)** en la lista desplegable **Reader type (Tipo de lector)**. Introduzca un nombre y haga clic en **OK (Aceptar)**.

Crear una conexión con un controlador de puerta

1. En AXIS Camera Station Pro Secure Entry:
   1.1. Vaya a **Configuration > Access control > Encrypted communication (Configuración > Control de acceso > Comunicación cifrada)**.
   1.2. 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)**.
2. En la interfaz web del dispositivo en la que se ejecuta AXIS Barcode Reader:
   2.1. Abra la aplicación AXIS Barcode Reader.
   2.2. Si el certificado del servidor no se configuró en AXIS Camera Station Pro Secure Entry, encienda **Ignore server certificate validation (Ignorar la validación del certificado del servidor)**. Consulte *Certificados* para obtener más información.
   2.3. Si el certificado del servidor no se configuró en AXIS Camera Station Pro Secure Entry, encienda **Ignore server certificate validation (Ignorar la validación del certificado del servidor)**. Consulte *Certificados* para obtener más información.

2.4. Si el certificado del servidor no se configuró en AXIS Camera Station Pro Secure Entry, encienda **Ignore server certificate validation (Ignorar la validación del certificado del servidor)**. Consulte *Certificados* para obtener más información.

2.5. Active **AXIS Camera Station Secure Entry**.

2.6. Haga clic en **Add (Agregar)**, introduzca la dirección IP del controlador de puerta y pegue la clave de autenticación.

2.7. Seleccione el lector que lee códigos de barras del menú desplegable de la puerta.

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 AXIS Camera Station 5.47 o posterior.
- 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 55767. Para obtener información sobre la configuración de puertos personalizada, consulte .
- Al conectar un servidor secundario a otro principal, se sustituye su clave de lector, lo que invalida cualquier credencial Bluetooth existente. Para evitarlo, establezca credenciales de Bluetooth en el servidor principal en lugar de en el secundario.

Flujo de trabajo

1. Configure un servidor como un servidor secundario y genere el archivo de configuración. Vea *Generar el archivo de configuración desde el servidor secundario, on page 30*.
2. Configure un servidor como servidor principal e importe el archivo de configuración de los servidores secundarios. Vea *Importar el archivo de configuración al servidor principal, on page 30*.
3. Configure los grupos de titulares de tarjeta y de titulares globales en el servidor principal. Vea *Agregar un titular de tarjeta, on page 33* y *Agregar un grupo, on page 37*.
4. Consulte y supervise los titulares de tarjeta y los grupos de titulares de tarjeta globales desde el servidor secundario. Vea *Gestión de acceso, on page 33*.

Generar el archivo de configuración desde el servidor secundario

1. Desde el servidor secundario, vaya a **Configuration > Access control > Multi server (Configuración > control de acceso > multi servidor)**.
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 **Configuration > Access control > Multi server (Configuración > control de acceso > multi servidor)**.
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 **Configuration > Access control > Multi server (Configuración > control de acceso > multi servidor)**.
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 > Dashboard (Gestión de acceso > Panel)**.
   1.2. Cambie los titulares de tarjeta y los grupos globales por los titulares de tarjeta y los grupos locales.
   1.3. Vaya a **Configuration > Access control > Multi server (Configuración > Control de acceso > 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 **Configuration > Access control > Multi server (Configuración > Control de acceso > Multiservidor)**.
   – Haga clic en **Sub server (Servidor secundario)** y **Revoke server (Revocar servidor)**.

Ajustes BETA de Active Directory

Nota

Las cuentas de usuario y los grupos de Microsoft Windows y Active Directory pueden acceder a AXIS Camera Station Pro Secure Entry. La forma de añadir usuarios en Windows varía en función de su versión. Para obtener más información, vaya a *support.microsoft.com*. Consulte el administrador de red si usa una red de dominio de Active Directory.

La primera vez que abra la página de configuración de Active Directory, podrá importar usuarios de Microsoft Active Directory a titulares de tarjetas en AXIS Camera Station Pro Secure Entry. Vea *Importar usuarios de Active Directory, on page 31*.

Después de la configuración inicial, se mostrarán las siguientes opciones en la página de ajustes de Active Directory.

- Cree y administre grupos de titulares de tarjetas basados en grupos en Active Directory.
- Configure la sincronización programada entre Active Directory y el sistema de gestión de acceso.
- Sincronice manualmente para actualizar todos los titulares de tarjetas importados desde Active Directory.
- Administre la asignación de datos entre los datos del usuario de Active Directory y las propiedades del titular de la tarjeta.

Importar usuarios de Active Directory

Para importar usuarios de Active Directory a titulares de tarjetas en AXIS Camera Station Pro Secure Entry:

1. Vaya a **Configuration (Configuración)** > **Access control (Control de acceso)** > **Active directory settings (Ajustes de Active Directory)**BETA.
2. Haga clic en **Set up import (Configurar importación)**.
3. Siga las instrucciones que aparecen en pantalla para completar estos tres pasos principales:
   3.1. Seleccione un usuario de Active Directory para usarlo como plantilla para la asignación de datos.
   3.2. Asigne datos de usuario desde la base de datos de Active Directory a las propiedades del titular de la tarjeta.
   3.3. Cree un nuevo grupo de titulares de tarjetas en el sistema de gestión de acceso y seleccione qué grupos de Active Directory importar.

No puede cambiar ninguno de los datos de usuario importados, pero puede añadir credenciales a un titular de tarjeta importado (consulte *Agregar credenciales, on page 35*).

Importante

Si desactiva un usuario en Active Directory, AXIS Camera Station Pro eliminará permanentemente al titular de la tarjeta y todos los datos relacionados, incluido su historial. Esta acción no se puede deshacer. Para bloquear el acceso de un titular de tarjeta sin perder sus datos, suspéndalo en AXIS Camera Station Pro en lugar de desactivarlo en Active Directory.

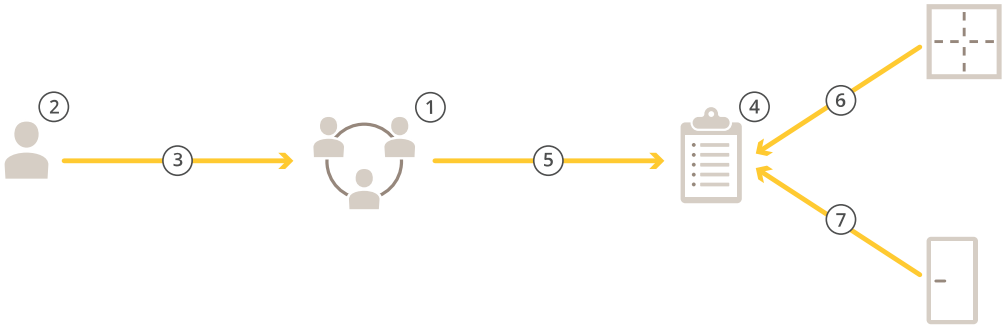
Gestión de acceso

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

Para obtener un flujo de trabajo adecuado que permita configurar una controladora de accesos en red de Axis en AXIS Camera Station Pro Secure Entry, consulte *Configurar una controladora de accesos en red de Axis*.

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 un grupo, on page 37*.
2. *Agregar un titular de tarjeta, on page 33*.
3. Agregar titulares de tarjeta a grupos.
4. *Agregar una regla de acceso, on page 38*.
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.

También puede elegir asignar usuarios de una base de datos de Active Directory como titulares de tarjeta, consulte *Ajustes BETA de Active Directory, on page 31*.

1. Abra una pestaña de Access management (Gestión de acceso).
2. Vaya a **Cardholder management (Gestión de titulares de tarjeta)** > **Cardholders (Titulares de tarjeta)** y haga clic en **+ Add (Agregar)**.
3. Introduzca el nombre y apellidos del titular. Si lo desea, añada más datos sobre el titular de la tarjeta:
   - En **Email (Correo electrónico)**, introduzca la dirección de correo electrónico del titular de la tarjeta.
   - En **Groups (Grupos)**, seleccione los grupos a los que desea añadir al titular de la tarjeta.
   - En **Access rules (Reglas de acceso)**, seleccione las reglas que desea aplicar al titular de la tarjeta.
4. Para añadir una foto, haga clic en **Cardholder picture (Foto del titular de la tarjeta)** y seleccione:
   - **Upload (Subir)** para añadir una imagen desde su dispositivo.

- **Capture (Captura)** para tomar una foto directamente usando su cámara.

Nota

La imagen debe ser un archivo JPG, PNG o GIF. Las imágenes se redimensionan automáticamente a un máximo de 700x700 píxeles y se convierten a formato JPG.

5. Haga clic en **Advanced (Avanzado)** para configurar opciones adicionales.
6. Agregar una credencial al titular de tarjeta. Vea *Agregar credenciales, on page 35*.
7. Haga clic en **Save (Guardar)**.
8. Para imprimir credenciales para uno o varios titulares de tarjetas, seleccione el/los titular/es y haga clic en **Print Badge (Imprimir credencial)**BETA. Para obtener más información, consulte *Print badge (Imprimir insignia) BETA, on page 44*.

Utilice el campo de búsqueda para encontrar al titular de la tarjeta por nombre o apellido. Para filtrar por origen, haga clic en **Filter (Filtro)** y seleccione **Local**, **Global**, **AD** o **Center (Centro)**.

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. Esto eliminará temporalmente todo acceso al 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 *BETA de varios servidores, on page 30*.

Agregar titulares de tarjeta y grupos

Agregar credenciales

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

- *Credencial con código QR, on page 35*
- *Credencial de PIN, on page 35*
- *Credencial móvil, on page 36*
- *Credencial de tarjeta, on page 36*
- *Credenciales de matrícula, on page 36*

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.

Credencial con código QR

Nota

El uso de códigos QR como credenciales requiere que la hora del controlador del sistema y de la cámara con AXIS Barcode Reader esté sincronizada. Recomendamos utilizar la misma fuente de hora para ambos dispositivos para una sincronización perfecta de hora.

Para agregar una credencial con código QR a un titular de tarjeta:

1. En **Credentials (Credenciales)**, haga clic en **+ Add (Agregar)** y seleccione **QR-code (Código QR)**.
2. Introduzca un nombre para la credencial.
3. **Dynamic QR (QR dinámico)** está activado de forma predeterminada. Debe utilizar el QR dinámico con credencial de PIN.
4. Establezca la fecha de inicio y fin para la credencial.
5. Para enviar el código QR por correo electrónico automáticamente después de guardar el titular de la tarjeta, seleccione **Send QR-code to cardholder when credential is saved (Enviar código QR al titular de tarjeta cuando se guarde la credencial)**.
6. Haga clic en **Añadir**.

Credencial de PIN

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. De forma opcional, para activar una alarma silenciosa con un PIN independiente, active **Duress PIN (PIN de coacción)** e introduzca un PIN de coacción.
4. Determine las fechas **Valid from (Válido desde)** y **Valid to (Válido hasta)** de la credencial.
5. Haga clic en **Añadir**.

Credencial móvil

Nota

El titular de la tarjeta debe tener una dirección de correo electrónico para recibir la credencial móvil.

Para agregar una credencial móvil a un titular de tarjeta:

1. En **Credentials (Credenciales)**, haga clic en **+ Add (Agregar)** y seleccione **Mobile credential (Credencial móvil)**.
2. Introduzca un nombre para la credencial.
3. Establezca la fecha de inicio y fin para la credencial.
4. Seleccione **Send the mobile credential to the cardholder after saving (Enviar la credencial móvil al titular de tarjeta después de guardar)**. El titular de la tarjeta recibe un correo electrónico con las instrucciones de emparejamiento.
5. Haga clic en **Añadir**.

Consulte el ejemplo en *Utilice la aplicación AXIS Mobile Credential como credencial Bluetooth, on page 19*.

Credencial de tarjeta

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)**.

Nota

Puede utilizar el lector de tarjetas USB 2N para obtener los datos de la tarjeta. Para obtener más información, consulte *Configurar el lector de tarjetas USB 2N*.

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**.

Credenciales de matrícula

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**.

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 Camera Station Pro Secure Entry. Vea .
2. Actualice el firmware de los dispositivos nuevos a la versión más reciente disponible. Vea .
3. Agregue una puerta nueva conectada al controlador de puerta. Vea *Agregar una puerta, on page 7*.
   3.1. Agregue un lector en el **Lado A**. Consulte *Agregar un lector, on page 17*.
   3.2. En **Door settings (Ajustes de puerta)**, seleccione **AXIS License Plate Verifier** como **Reader type (Tipo de lector)** e introduzca un nombre para el lector.
   3.3. Si lo desea, puede agregar un lector o dispositivo de solicitud de salida (REX) al **Lado B**.
   3.4. Haga clic en **Ok (Aceptar)**.
4. Instale y active AXIS License Plate Verifier en la cámara. Consulte el manual del usuario de *AXIS License Plate Verifier*.
5. Iniciar AXIS License Plate Verifier.
6. Configurar AXIS License Plate Verifier.
   6.1. Vaya a **Configuration > Access control > Encrypted communication (Configuración > Control de acceso > Comunicación cifrada)**.
   6.2. 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)**.
   6.3. Abra AXIS License Plate Verifier desde la interfaz web de la cámara.
   6.4. No realice la configuración.
   6.5. Vaya a **Settings (Ajustes)**.
   6.6. En **Access control (Control de acceso)**, seleccione **Secure Entry (Entrada segura)** como **Type (Tipo)**.
   6.7. En **IP address (Dirección IP)**, introduzca la dirección IP para el controlador de puerta.
   6.8. En **Authentication key (Clave de autenticación)**, pegue la clave de autenticación que copió anteriormente.
   6.9. Haga clic en **Connect (Conectar)**.
   6.10. En **Door controller name (Nombre del controlador de puerta)**, seleccione el controlador de puerta.
   6.11. En **Reader name (Nombre del lector)**, seleccione el lector que agregó anteriormente.
   6.12. Active la integración.
7. Agregue el titular de tarjeta al que desee acceder. Vea *Agregar un titular de tarjeta, on page 33*
8. Agregue las credenciales de la matrícula al nuevo titular de la tarjeta. Vea *Agregar credenciales, on page 35*
9. Agregar una regla de acceso. Vea *Agregar una regla de acceso, on page 38*.
   9.1. Agregue una programación.
   9.2. Agregue el titular de la tarjeta al que desee conceder acceso a la matrícula.
   9.3. 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. Abra una pestaña de Access management (Gestión de acceso).
2. Vaya a **Cardholder management (Gestión de titulares de tarjeta)** > **Groups (Grupos)** y haga clic en **+ Add (Agregar)**.
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. Vea *BETA de varios servidores, on page 30*.
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)**.
6. Haga clic en **Save (Guardar)**.
7. Para imprimir credenciales para todos los titulares de tarjetas de un grupo, seleccione el grupo y haga clic en **Print Badge (Imprimir credencial)**BETA. Para obtener más información, consulte *Print badge (Imprimir insignia) BETA, on page 44*.

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.

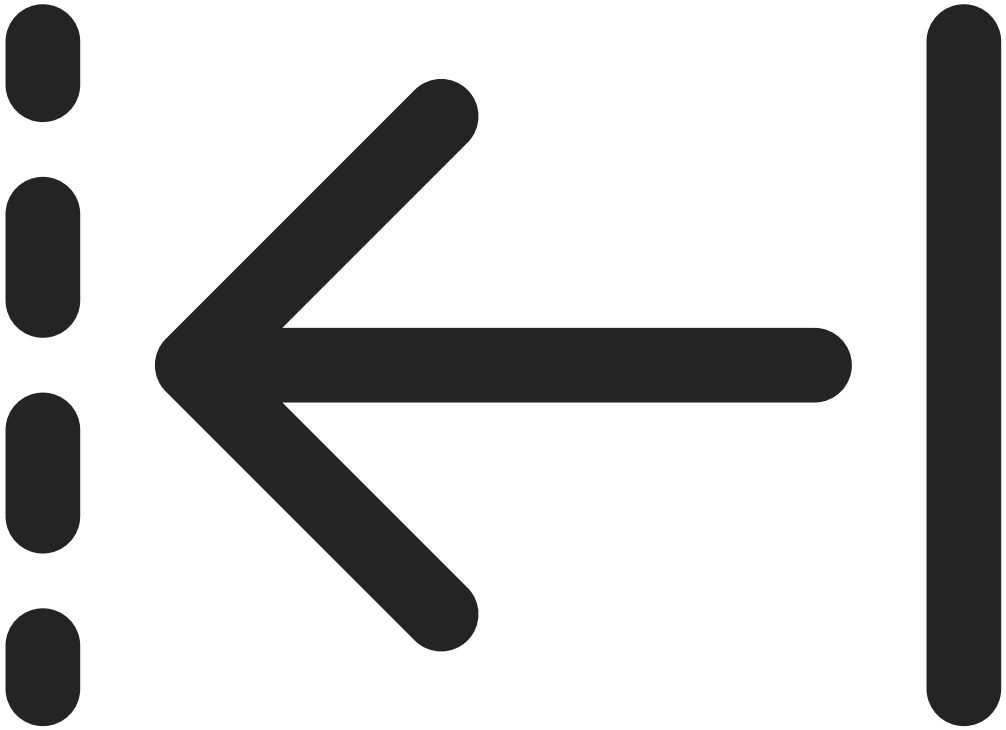
Puertas y zonas – dónde se aplica el acceso.

Horarios – cuándo conceder acceso.

Para agregar una regla de acceso:

1. Abra una pestaña de Access management (Gestión de acceso).
2. Vaya a **Cardholder management (Gestión de titulares de tarjeta)**.

3. En **Access rules (Reglas de acceso)**



, haga clic en **+ Add (Añadir)**.

4. Introduzca un nombre para la regla de acceso y haga clic en **Next (Siguiente)**.
5. Configure los titulares de tarjeta y los grupos:
   5.1. En **Cardholders (Titulares de tarjeta)** o **Groups (Grupos)**, haga clic en **+ Add (Agregar)**.
   5.2. Seleccione los titulares de tarjeta o grupos y haga clic en **Add (Agregar)**.
   5.3. También puede arrastrar y soltar un titular de tarjeta o un grupo directamente sobre una regla de acceso para aplicarla. Al arrastrar, se resaltan las reglas de acceso sobre las que puede soltar el elemento. Si arrastra varios titulares de tarjetas o grupos a la vez, un contador mostrará cuántos está moviendo.
6. Configure las puertas y zonas:
   6.1. En **Doors (Puertas)** o **Zones (Zonas)**, haga clic en **+ Add (Agregar)**.
   6.2. Seleccione las puertas o zonas y haga clic en **Add (Agregar)**.
7. Configure las programaciones:
   7.1. En **Schedules (Programaciones)**, haga clic en **+ Add (Agregar)**.
   7.2. Seleccione una o más programaciones y haga clic en **Add (Agregar)**.
8. 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)**.

Exportar informes de configuración del sistema

Puede exportar informes que contengan diferentes tipos de información acerca del sistema. AXIS Camera Station Pro Secure Entry 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:

1. Abra una pestaña de Access management (Gestión de acceso).
2. Vaya a **Reports (Informes)** > **System configuration (Configuración del sistema)**.
3. Seleccione los informes que desea exportar y haga clic en **Download (Descargar)**.

Informe de detalles de titulares de tarjeta	Incluye información sobre los titulares de tarjetas, credenciales, validación de tarjetas y última operación.
Informe de acceso de 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.
Informe de 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.
Informe de 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.
Informe de acceso de 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.
Informe de 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. Abra una pestaña de Access management (Gestión de acceso).
2. Vaya a **Reports (Informes)** > **Cardholder activity (Actividad de los titulares de tarjeta)**.
3. Haga clic en **+ Add (Agregar)** y seleccione **Roll call / Mustering (Pase de lista / Agrupamiento)**.
4. Introduzca un nombre para el informe.
5. Seleccione las zonas que desee incluir en el informe.
6. Seleccione los grupos que desee incluir en el informe.
7. Si desea obtener un informe de agrupamiento, seleccione **Mustering point (Punto de agrupamiento)** y un lector para el punto de agrupamiento.
8. Seleccione un marco temporal para el informe.
9. Haga clic en **Save (Guardar)**.
10. 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.

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.

También puede elegir asignar usuarios de una base de datos de Active Directory como titulares de tarjeta, consulte *Ajustes BETA de Active Directory, on page 31*.

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 Camera Station Pro Secure Entry 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)**.

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 *Perfiles de identificación, on page 22*.

Para editar una plantilla de correo electrónico con el fin de enviar una credencial QR o móvil:

1. En la pestaña **Access management (Gestión de acceso)**, haga clic en **Settings (Ajustes)** > **Email templates (Plantillas de correo electrónico)**.
2. Edite su plantilla y haga clic en **Update (Actualizar)**.

Plantillas de insignias BETA

Puede personalizar las plantillas de insignias con información del titular, fotos, logotipos y marca personalizada. Para crear una nueva plantilla:

1. Vaya a **Access management (Gestión de acceso) > Settings (Ajustes) > Badge templates (Plantillas de insignias)** BETA.
2. Haga clic en **Create new template (Crear nueva plantilla)**.
3. Introduzca un nombre en el campo **Template name (Nombre de la plantilla)**.
4. Seleccione **Use as default template for printing (Usar como plantilla predeterminada para imprimir)** si desea que esta sea la plantilla empleada por defecto.
5. Personalice el diseño de la insignia:
   - Seleccione hasta cinco campos de texto para mostrar en la parte frontal, incluyendo cualquier campo personalizado que haya creado. Al imprimir, solo aparecen los campos completados en la insignia.
   - Seleccione la fuente y el color del texto.
   - Añada un color o una imagen de fondo.
   - Suba el logotipo de su organización.
   - Para el envés, añada un color o una imagen de fondo.

6. Haz clic en **Save (Guardar)** para guardar los cambios o en **Save as (Guardar como)** para guardarla como una nueva plantilla.

Nota

Una vez creada una plantilla, ya no se podrá editar, solo cambiarle el nombre.

Print badge (Imprimir insignia) BETA

Puede imprimir insignias de identificación para titulares de tarjetas con las plantillas de insignias configuradas. Recuerde que actualmente no se admite la codificación de tarjetas. Antes de empezar:

- Asegúrese de que el titular de la tarjeta posee al menos una credencial de tarjeta. No puede imprimir insignias para titulares de tarjetas sin credenciales.
- Necesita una impresora compatible con tarjetas de tamaño CR80 y un material de impresión adecuado, como cartulina gruesa.
- Configure los ajustes de impresión de su navegador:
  1. Determine el tamaño de página en CR80 o un tamaño personalizado que se ajuste a las dimensiones de su tarjeta.
  2. Establezca la orientación en vertical.
  3. Desactive los márgenes o configúrelos al mínimo.

Importante

Secure Entry funciona con impresoras con controladores de Windows. Se ha verificado el correcto funcionamiento de la serie de impresoras HID Fargo. Si necesita un controlador para su impresora, contacte con el proveedor de la misma.

Para imprimir insignias:

1. Vaya a **Access management (Gestión de acceso) > Cardholder management (Gestión de titulares de tarjetas) > Cardholders (Titulares de tarjetas)**.
2. Seleccione un o más titulares de tarjetas.
3. Haga clic en **Print badge (Imprimir insignia)** BETA.
4. Haga clic en **Select template (Seleccionar plantilla)** y, en el menú desplegable **Template (Plantilla)**, seleccione la opción que desea utilizar.
5. Si el titular de la tarjeta tiene varias credenciales, seleccione una en el menú desplegable **Card (Tarjeta)**.
6. Haga clic en **Print (Imprimir)**.

Nota

Si su impresora no admite la impresión doble, imprima primero todas las páginas frontales, luego dé la vuelta a la pila de tarjetas y vuelva a colocarlas en la bandeja para imprimir el envés.

T10231644_es

2026-04 (M7.2)