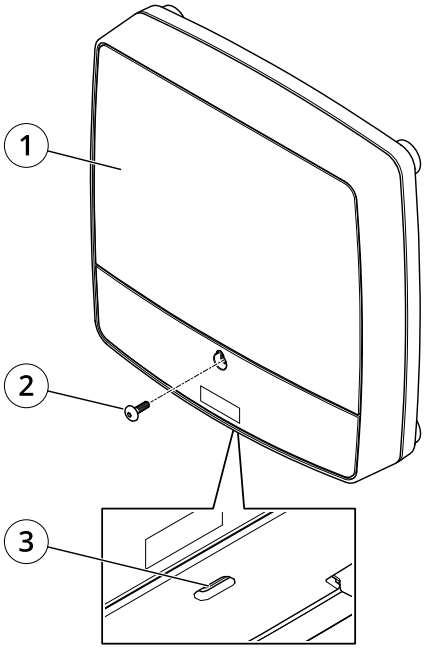
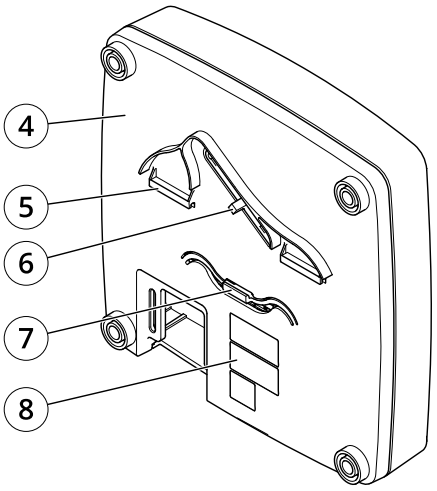
AXIS A1001 & AXIS Entry Manager

Manual del usuario

Índice

Información general del producto

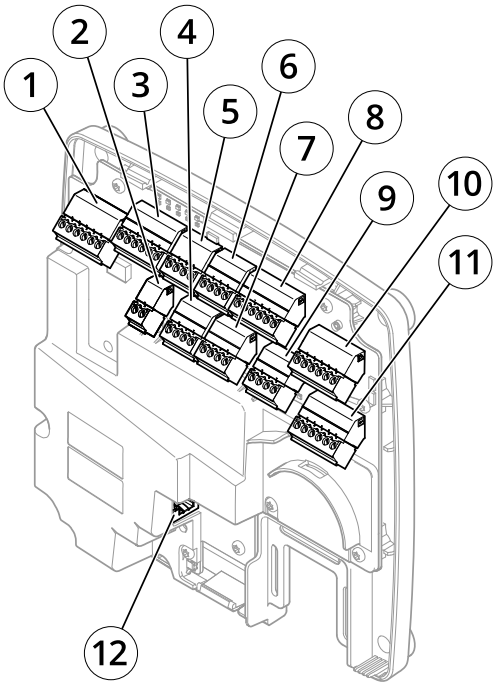




Parte delantera y trasera:

1 *Cubierta*
2 *Tornillo de la cubierta*
3 *Ranura de desmontaje de la cubierta*
4 *Base*
5 *Clip DIN (superior)*
6 *Interruptor de alarma antimanipulación (posterior)*
7 *Clip DIN (inferior)*
8 *Número de pieza (N/P) y número de serie (N/S)*

Información general del producto



Interfaz de E/S:

1 Conector de datos del lector (READER DATA 1)
10 Conector de datos del lector (READER DATA 2)
3 Conector de E/S del lector (READER I/O 1)
8 Conector de E/S del lector (READER I/O 2)
4 Conector de puerta (DOOR IN 1)
7 Conector de puerta (DOOR IN 2)
6 Conector auxiliar (AUX)
5 Conector de audio (AUDIO) (no se usa)

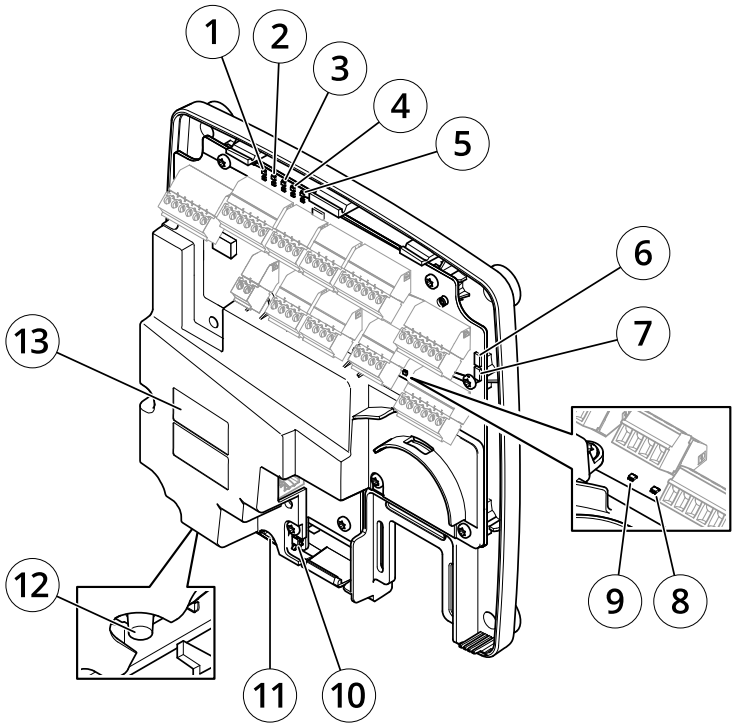
Entradas de alimentación externa:

2 Conector de alimentación (DC IN)
12 Conector de red (PoE)

Salidas de alimentación:

9 Conector de alimentación cerradura (LOCK)
11 Conector de alimentación y relé (PWR, RELAY)

Información general del producto



Indicadores LED, botones y otro hardware:

1 *Indicador LED de corriente*
2 *Indicador LED de estado*
3 *Indicador LED de red*
4 *Indicador LED 2 del lector (no se usa)*
5 *Indicador LED 1 del lector (no se usa)*
6 *Cabezal con pines de la alarma antimanipulación (delantero) (TF)*
7 *Cabezal con pines de la alarma antimanipulación (trasero) (TB)*
8 *Indicador LED de cerradura*
9 *Indicador LED de cerradura*
10 *Sensor de la alarma antimanipulación (delantero)*
11 *Ranura para tarjetas SD (microSDHC) (no se usa)*
12 *Botón de control*
13 *Número de pieza (N/P) y número de serie (N/S)*

Indicadores LED

LED	Color	Indicación
Red	Verde	Fijo para indicar una conexión a una red de 100 MBits/s. Parpadea cuando hay actividad de red.
	Ámbar	Fijo para indicar una conexión a una red de 10 MBits/s. Parpadea cuando hay actividad de red.
	Apagado	No hay conexión a la red.
Estado	Verde	Fijo en verde para indicar un funcionamiento normal.
	Ámbar	Fijo durante el inicio y al restaurar valores de configuración.
	Rojo	Parpadea despacio si se ha producido un error en una actualización.

Alimentación	Verde	Funcionamiento normal.
	Ámbar	Parpadea en verde/ámbar durante la actualización del firmware.
Cerradura	Verde	Luz fija cuando no hay alimentación.
	Rojo	Luz fija cuando hay alimentación.
	Apagado	Suelta.

Nota

- Se puede configurar el LED de estado para que parpadee mientras haya un evento activo.
- Se puede configurar el LED de estado para que parpadee e identifique la unidad. Acceda a **Setup > Additional Controller Configuration > System Options > Maintenance (Configuración > Configuración del controlador adicional > Opciones del sistema > Mantenimiento)**.

Conectores y botones

Interfaz de E/S

Conectores de datos del lector
Dos bloques de terminales de 6 pines compatibles con los protocolos RS485 y Wiegand para la comunicación con el lector. Para conocer las especificaciones, consulte *página 70*.

Conectores de E/S del lector
Dos bloques de terminales de 6 pines para entrada y salida del lector. Además del punto de referencia de 0 V CC y la alimentación (salida de CC), el conector de E/S del lector ofrece la interfaz para:

- Entrada digital: para conectar, por ejemplo, alarmas antimanipulación del lector.
- Salida digital: para conectar, por ejemplo, avisadores y LED del lector.

Para conocer las especificaciones, consulte *página 70*.

Conectores de puerta
Dos bloques terminales de 4 pines para conectar dispositivos de monitor de puerta y solicitud para dispositivos de salida (REX). Para conocer las especificaciones, consulte *página 71*.

Conector auxiliar
Bloque de terminales de E/S configurable de 4 pines. Se utiliza con dispositivos externos combinados, por ejemplo, con alarmas antimanipulación, activación de eventos y notificaciones de alarma. Además del punto de referencia de 0 V CC y la alimentación (salida de CC), el conector auxiliar ofrece la interfaz para:

- Entrada digital: una entrada de alarma para conectar dispositivos que puedan alternar entre circuitos cerrados y abiertos, por ejemplo, sensores PIR o detectores de cristales rotos.
- Salida digital: para conectar dispositivos externos como luces, sirenas o alarmas antirrobo. Los dispositivos conectados se pueden activar mediante la interfaz de programación de aplicaciones VAPIX® o mediante una regla de acción.

Para conocer las especificaciones, consulte *página 72*.

Entradas de alimentación externa

AVISO

El producto se conectará mediante un cable de red blindado (STP). Todos los cables que conecten el producto a la red deberán estar blindados para su uso específico. Asegúrese de que los dispositivos de red estén instalados de conformidad con las instrucciones del fabricante. Para obtener información sobre los requisitos normativos, consulte .

Conector de alimentación
Bloque de terminales de 2 pines para la entrada de alimentación de CC. Use una fuente de alimentación limitada (LPS) que cumpla los

requisitos de tensión muy baja de seguridad (SELV) con una potencia nominal de salida limitada a ≤100 W o una corriente nominal de salida limitada a ≤5 A. Para conocer las especificaciones, consulte *página 72*.

Conector de red
Conector Ethernet RJ45. Admite alimentación a través de Ethernet (PoE). Para conocer las especificaciones, consulte *página 73*.

Salidas de alimentación

Conector de alimentación de cerradura

Bloque de terminales de 4 pines para conectar una o dos cerraduras. Este conector de cerradura también podría usarse para proporcionar alimentación a dispositivos externos. Para conocer las especificaciones, consulte *página 73*.

Conector de alimentación y relé

Bloque de terminales de 6 pines para conectar el relé del controlador de puerta y de alimentación a dispositivos externos como cerraduras y sensores. Para conocer las especificaciones, consulte *página 73*.

Botones y otro hardware

Cabezal con pines de la alarma antimanipulación
Dos cabezales de dos pines para desconectar las alarmas antimanipulación delantera y trasera. Para conocer las especificaciones, consulte *página 74*.

Botón de control
El botón de control se utiliza para lo siguiente:

- Restablecer el producto a los ajustes predeterminados de fábrica. Consulte *página 65*.
- Conexión a un servicio AVHS de vídeo alojado (AXIS Video Hosting System). Consulte *página 59*. Para conectarse, mantenga pulsado el botón durante 1 segundo hasta que el indicador de estado parpadee en color verde.
- Conectarse al Servicio de DNS dinámico de Internet de AXIS. Consulte *página 59*. Para conectarse, mantenga pulsado el botón durante 3 segundos.

Instalación

Instalación

Para ver este vídeo, vaya a la versión web de este documento.

help.axis.com/?&piaId=19467&section=product-overview

Vídeo de instalación del producto.

Cómo acceder al producto

Cómo acceder al producto

Para instalar el producto de Axis, consulte la Guía de instalación proporcionada con él.

Acceder al dispositivo

1. Abra un navegador y escriba la dirección IP o el nombre de host del dispositivo Axis.

   Si no conoce la dirección IP, use AXIS IP Utility o AXIS Device Manager para localizar el dispositivo en la red.

2. Introduzca el nombre de usuario y la contraseña. Si accede al dispositivo por primera vez, debe establecer la contraseña root. Consulte .

3. Se abre AXIS Entry Manager en el navegador. Si utiliza un ordenador, alcanzará la página de Vista general. Si utiliza un dispositivo móvil, alcanzará la página de inicio para dispositivos móviles.

Acerca de la página de inicio para dispositivos móviles

La página de inicio para dispositivos móviles muestra el estado de las puertas y las cerraduras conectadas al controlador de puerta. Puede probar bloquearlas y desbloquearlas. Actualice la página para ver el resultado.

Un vínculo le lleva a Axis Entry Manager.

Nota

- Axis Entry Manager no es compatible con dispositivos móviles.
- Si continúa a Axis Entry Manager, no habrá ningún enlace para volver a la página de inicio para dispositivos móviles.

Cómo acceder al producto desde Internet

Un router de red permite a los productos de una red privada (LAN) compartir una única conexión a Internet. Para ello, se transfiere el tráfico de red de la red privada a Internet.

La mayoría de los routers está preconfigurada para detener los intentos de acceso a la red privada (LAN) desde la red pública (Internet).

Si el producto de Axis se encuentra en una intranet (LAN) y quiere que esté disponible desde fuera (WAN) con un router NAT (Traducción de direcciones de red), active la **NAT transversal**. Con la NAT transversal configurada correctamente, se envía al producto todo el tráfico HTTP a un puerto externo HTTP en el router NAT.

Cómo activar la función de NAT transversal

- Vaya a **Setup > Additional Controller Configuration > System Options > Network > TCP/IP > Advanced (Configuración > Configuración del controlador adicional > Opciones del sistema > Red > TCP/IP > Avanzada)**.
- Haga clic en **Enable (Activar)**.
- Configure manualmente su router NAT para permitir el acceso desde Internet.

Consulte también la información sobre el servicio de DNS dinámico de Internet de AXIS en *www.axiscam.net*

Nota

- En este contexto, un "router" hace referencia a cualquier dispositivo de enrutamiento de red, como un router NAT, un router de red, una puerta de enlace de Internet, un router de banda ancha, un dispositivo de uso compartido de banda ancha o un software, como un cortafuegos.
- Para que funcione la NAT transversal, debe ser compatible con el router. El router debe ser compatible también con UPnP®.

Cómo acceder al producto

Cómo establecer la contraseña root

Para acceder al producto de Axis, debe definir la contraseña para el administrador **root** predeterminado. Esta acción se lleva a cabo en el cuadro de diálogo **Configure Root Password (Configurar contraseña de root)**, que se abre cuando se accede al producto por primera vez.

Para evitar escuchas ilegales en la red, la contraseña de root se puede definir mediante una conexión HTTPS cifrada, que requiere un certificado HTTPS. HTTPS (protocolo de transferencia de hipertexto sobre SSL) es un protocolo que se usa para cifrar el tráfico entre los navegadores web y los servidores. El certificado HTTPS garantiza un intercambio cifrado de información. Consulte *HTTPS en la página 55*.

El nombre de usuario del administrador predeterminado **root** es permanente y no se puede eliminar. Si pierde la contraseña de root, habrá que restablecer el producto a su configuración predeterminada de fábrica. Consulte *Restablecimiento a la configuración predeterminada de fábrica en la página 65*.

Para definir la contraseña, escríbala directamente en el cuadro de diálogo.

La página de vista general

La página de vista general en AXIS Entry Manager muestra información sobre el nombre, la dirección MAC, la dirección IP y la versión de firmware del controlador de puerta. También permite identificar el controlador de puerta en la red o en el sistema.

La primera vez que acceda al producto de Axis, la página de vista general le pedirá que configure el hardware, establezca la fecha y hora, configure los ajustes de red y configure los controladores de puerta como parte de un sistema o como unidades independientes. Para obtener más información acerca de cómo configurar el sistema, consulte *Configuración: paso a paso en la página 11*.

Para regresar a la página de vista general desde otras páginas web del producto, haga clic en **Overview (Vista general)** en la barra de menú.

Configuración del sistema

Para abrir las páginas de configuración del producto, haga clic en **Setup (Configuración)** en la esquina superior derecha de la página de vista general.

El producto de Axis puede ser configurado por administradores. Para obtener más información acerca de los usuarios y administradores, consulte *página 31*, *página 40*, y *página 55*.

Configuración: paso a paso

Antes de empezar a utilizar el sistema de control de acceso, se deben completar los siguientes pasos de configuración:

1. Si el inglés no es su primera lengua, puede que prefiera que AXIS Entry Manager se muestre en un idioma diferente. Consulte *Seleccionar un idioma en la página 11*.
2. Configure la fecha y hora. Consulte *página 11*.
3. Configure los ajustes de red. Consulte *página 13*.
4. Configure el controlador de puerta y los dispositivos conectados, como lectores, cerraduras y dispositivos de solicitud de salida (REX). Consulte *Configuración del hardware en la página 13*.
5. Verifique las conexiones de hardware. Consulte *página 20*.
6. Configure tarjetas y formatos. Consulte *página 21*.
7. Configure el sistema de controlador de puerta. Consulte *Administrar controladores de puerta en red en la página 26*.

Para obtener información sobre cómo configurar y gestionar las puertas, programaciones, usuarios y grupos del sistema, consulte *Gestión de acceso en la página 31*.

Para obtener información sobre recomendaciones de mantenimiento, consulte *Instrucciones de mantenimiento en la página 29*.

Nota

Para añadir o eliminar controladores de puertas, para añadir, eliminar o editar usuarios, o para configurar el hardware, más de la mitad de los controladores de puerta en el sistema deben estar **en línea**. Para comprobar el estado del controlador de puerta, vaya a **Setup > Manage Network Door Controllers in System (Configuración > Administrar controladores de puerta de red en el sistema)**.

Seleccionar un idioma

El idioma predeterminado de AXIS Entry Manager es inglés, pero se puede cambiar a cualquiera de los idiomas incluidos en el firmware del producto. Para obtener información sobre el firmware más reciente disponible, consulte *www.axis.com*

Se puede cambiar el idioma en cualquiera de las páginas web del producto.

Para cambiar de idioma, haga clic en la lista desplegable de idioma y seleccione un idioma. Todas las páginas web y páginas de ayuda del producto se muestran en el idioma seleccionado.

Nota

- Cuando se cambia el idioma, también cambia el formato de fecha en un formato utilizado habitualmente en el idioma seleccionado. El formato correcto se muestra en los campos de datos.
- Si se restablecen los ajustes predeterminados de fábrica, AXIS Entry Manager se vuelve a mostrar en inglés.
- Si se restaura el producto, AXIS Entry Manager seguirá empleando el idioma seleccionado.
- Si se reinicia el producto, AXIS Entry Manager seguirá empleando el idioma seleccionado.
- Si se actualiza el firmware, AXIS Entry Manager seguirá empleando el idioma seleccionado.

Configurar fecha y hora

Si el controlador de puerta forma parte de un sistema, los ajustes de fecha y hora se distribuirán a todos los controladores de puerta. Esto significa que la configuración se envía al resto de controladores en el sistema, independientemente de si fecha y hora se sincronizan con un servidor NTP, se configuran manualmente o se obtienen de la fecha y hora del ordenador. Si no puede ver los cambios, pruebe a actualizar la página en el navegador. Para obtener más información sobre la gestión de un sistema de controladores de puerta, consulte *Administrar controladores de puerta en red en la página 26*.

Para configurar la fecha y hora del producto Axis, vaya a **Setup > Date & Time (Configuración > Fecha y hora)**.

Puede definir la fecha y hora de las formas siguientes:

- Obtener la fecha y hora desde un servidor Network Time Protocol (NTP). Consulte *página 12*.
- Establecer la fecha y hora manualmente. Consulte *página 12*.
- Obtener la fecha y hora desde el ordenador. Consulte *página 12*.

Current controller time (Hora actual del controlador) muestra la fecha y hora actual del controlador de puerta (reloj de 24 horas).

Las mismas opciones de fecha y hora también están disponibles en las páginas de opciones del sistema. Vaya a **Setup > Additional Controller Configuration > System Options > Date & Time (Configuración > Configuración de controlador adicional > Opciones del sistema > Fecha y hora**.

Obtener la fecha y hora desde un servidor Network Time Protocol (NTP).

1. Vaya a **Setup > Date & Time (Configuración > Fecha y hora)**.
2. Seleccione su **Timezone (Zona horaria)** en la lista desplegable.
3. Si se utiliza horario de verano en su región, seleccione **Adjust for daylight saving (Ajustar para horario de verano)**.
4. Seleccione **Synchronize with NTP (Sincronizar con NTP)**.
5. Seleccione la dirección DHCP predeterminada o introduzca la dirección de un servidor NTP.
6. Haga clic en **Save (Guardar)**.

Al sincronizar con un servidor NTP, la fecha y la hora se actualizan continuamente porque los datos se insertan desde el servidor NTP. Para obtener información acerca de los ajustes de NTP, consulte *Configuración NTP en la página 60*.

Si se utiliza un nombre de host para el servidor NTP, se debe configurar un servidor DNS. Consulte *Configuración DNS en la página 60*.

Establecer la fecha y hora manualmente

1. Vaya a **Setup > Date & Time (Configuración > Fecha y hora)**.
2. Si se utiliza horario de verano en su región, seleccione **Adjust for daylight saving (Ajustar para horario de verano)**.
3. Seleccione **Set date & time manually (Establecer fecha y hora manualmente)**.
4. Introduzca manualmente la fecha y la hora deseadas.
5. Haga clic en **Save (Guardar)**.

Al definir la fecha y la hora manualmente, estas se establecen una única vez sin posteriores actualizaciones automáticas. Esto significa que, si se deben actualizar la fecha o la hora, los cambios se deben realizar manualmente porque no hay conexión con un servidor NTP externo.

Obtener la fecha y hora desde el ordenador

1. Vaya a **Setup > Date & Time (Configuración > Fecha y hora)**.
2. Si se utiliza horario de verano en su región, seleccione **Adjust for daylight saving (Ajustar para horario de verano)**.

3. Seleccione **Set date & time manually (Establecer fecha y hora manualmente)**.
4. Haga clic en **Sync now and save (Sincronizar ahora y guardar)**.

Cuando se utiliza la hora del ordenador, la fecha y hora se sincronizan con la fecha y hora del ordenador una única vez, sin actualizaciones automáticas posteriores. Esto significa que si se cambia la fecha y hora en el equipo que utilice para gestionar el sistema, debe sincronizar nuevo.

Configurar los ajustes de red

Para configurar los ajustes básicos de red, vaya a **Setup > Network Settings (Configuración > Ajustes de red)** o a **Setup > Additional Controller Configuration > System Options > Network > TCP/IP > Basic (Configuración > Configuración de controlador adicional > Opciones del sistema > Red > TCP/IP > Básica)**.

Para obtener más información sobre la configuración de red, consulte *Red en la página 57*.

Configuración del hardware

Para poder gestionar las puertas y las plantas, el hardware se debe configurar mediante las páginas Configuración del hardware.

Puede conectar lectores, cerraduras y otros dispositivos al producto de Axis antes de finalizar la configuración del hardware. Sin embargo, la conexión de dispositivos será más fácil si completa la configuración de hardware primero. Esto se debe a que un gráfico de pines del hardware estará disponible cuando la configuración esté completa. El gráfico de pines del hardware es una guía sobre cómo conectar los dispositivos a los pines. Se puede usar como hoja de referencia para tareas de mantenimiento. Para conocer las instrucciones de mantenimiento, consulte *página 29*.

Para configurar el hardware por primera vez, seleccione uno de los siguientes métodos:

- Importación de un archivo de configuración de hardware. Consulte *página 13*.
- Creación de una nueva configuración de hardware. Consulte *página 14*.

Nota

Si el hardware del producto no se ha configurado antes o se ha eliminado, **Hardware Configuration (Configuración de hardware)** estará disponible en el panel de notificación de la página Overview (Descripción general).

Cómo importar un archivo de configuración de hardware

La configuración del hardware del producto de Axis se puede completar más rápidamente mediante la importación de un archivo de configuración de hardware.

Al exportar el archivo desde un producto e importarlo en otros, se pueden hacer numerosas copias de la misma configuración de hardware sin tener que repetir los mismos pasos una y otra vez. También se pueden almacenar los archivos exportados como copias de seguridad y usarlos para restaurar configuraciones de hardware previas. Para obtener más información, consulte *Cómo exportar un archivo de configuración de hardware en la página 14*.

Para importar un archivo de configuración de hardware:

1. Vaya a **Setup > Hardware Configuration (Configuración > Configuración de hardware)**.
2. Haga clic en **Import hardware configuration (Importar configuración de hardware)**. Si ya existe una configuración de hardware, haga clic en **Reset and import hardware configuration (Restablecer e importar una configuración de hardware)**.
3. En el cuadro de diálogo del navegador de archivos que aparece, localice y seleccione el archivo de configuración de hardware (*.json) en su equipo.
4. Haga clic en **OK (Aceptar)**.

Cómo exportar un archivo de configuración de hardware

La configuración de hardware del producto de Axis se puede exportar para realizar múltiples copias de la misma configuración de hardware. También se pueden almacenar los archivos exportados como copias de seguridad y usarlos para restaurar configuraciones de hardware previas.

Nota

No es posible exportar la configuración de hardware de plantas.

La configuración de las cerraduras inalámbricas no se incluye en la exportación de la configuración de hardware.

Para exportar un archivo de configuración de hardware:

1. Vaya a **Setup > Hardware Configuration (Configuración > Configuración de hardware)**.
2. Haga clic en **Export hardware configuration (Exportar configuración de hardware)**.
3. En función del navegador, es posible que se muestre un cuadro de diálogo para completar la exportación.

   A menos que se especifique lo contrario, el archivo exportado (*.json) se guarda en la carpeta de descargas predeterminada. Se puede seleccionar una carpeta de descargas en la configuración de usuario del navegador web.

Crear una nueva configuración de hardware

Siga las instrucciones de acuerdo con sus necesidades:

- *Cómo crear una nueva configuración de hardware sin periféricos en la página 14*
- *Cómo crear una nueva configuración de hardware para cierres inalámbricos en la página 18*
- *Cómo crear una nueva configuración de hardware con control de ascensor (AXIS A9188) en la página 19*

Cómo crear una nueva configuración de hardware sin periféricos

1. Vaya a **Setup > Hardware Configuration (Configuración > Configuración de hardware)** y haga clic en **Start new hardware configuration (Iniciar nueva configuración de hardware)**.
2. Introduzca el nombre del producto Axis.
3. Seleccione el número de puertas conectadas y haga clic en **Next (Siguiente)**.
4. Configure los monitores de puerta (sensores de posición de puerta) y las cerraduras según sus necesidades y haga clic en **Next (Siguiente)**. Para obtener más información sobre las opciones disponibles, consulte *Cómo configurar monitores y cerraduras de puerta en la página 14*.
5. Configure los lectores y dispositivos REX que se utilizarán y haga clic en **Finish (Finalizar)**. Para obtener más información sobre las opciones disponibles, consulte *Cómo configurar lectores y dispositivos REX en la página 17*.
6. Haga clic en **Close (Cerrar)** o en el enlace para ver el gráfico de pines del hardware.

Cómo configurar monitores y cerraduras de puerta

Si se selecciona una opción de puerta en la nueva configuración de hardware, puede configurar los monitores de puerta y cerraduras.

1. Si se utilizará un monitor de puerta, seleccione **Door Monitor (Monitor de puerta)** y, a continuación, seleccione la opción que coincida con el modo en que se conectarán los circuitos del monitor de puerta.
2. Si la cerradura de puerta debe bloquearse inmediatamente después de abrirse la puerta, seleccione **Cancel access time once door is opened (Cancelar tiempo de acceso una vez abierta la puerta)**.

   Si desea retrasar el bloqueo, defina el tiempo de retraso en milisegundos en **Relock time (Tiempo para bloqueo)**.

3. Especifique las opciones de tiempo del monitor de puerta o, si no se utilizará ningún monitor de puerta, las opciones de tiempo de bloqueo.
4. Seleccione las opciones que se ajusten al modo en que se conectarán los circuitos de la cerradura.
5. Si se utilizará un monitor de cerradura, seleccione **Lock Monitor (Monitor de cerradura)** y, a continuación, seleccione las opciones que coincidan con el modo en que se conectarán los circuitos del monitor de cerradura.
6. Si se deben supervisar las conexiones de entrada procedentes de lectores, dispositivos REX y monitores de puerta, seleccione **Enable supervised inputs (Habilitar entradas supervisadas)**.

   Para obtener más información, consulte *Cómo usar entradas supervisadas en la página 17*.

Nota

- La mayoría de las opciones de cerradura, monitor de puerta y lector se pueden modificar sin restablecer e iniciar una nueva configuración de hardware. Vaya a **Setup > Hardware Reconfiguration (Configuración > Reconfiguración de hardware)**.
- Puede conectar un único monitor de cerradura por controlador de puerta. De este modo, si lo que si utiliza puertas de cerradura doble, solo una de las cerraduras puede tener un monitor de cerradura. Si hay dos puertas conectadas al mismo controlador de puerta, no se pueden utilizar monitores de cerradura.
- Las cerraduras motorizadas se deben configurar como secundarias.

Acerca de las opciones de monitor de puerta y hora

Las siguientes opciones de monitor de puerta están disponibles:

- **Door monitor (Monitor de puerta)**: seleccionado por defecto. Cada puerta tiene su propio monitor de puerta que, por ejemplo, señalará si la puerta es forzada o permanece abierta durante un tiempo demasiado largo. Anule la selección si no se utilizará ningún monitor de puerta.
  - **Open circuit = Closed door (Circuito abierto = Puerta cerrada)**: seleccione esta opción si el circuito del monitor de puerta está normalmente abierto. El monitor de puerta proporciona la señal de puerta abierta cuando el circuito está cerrado. El monitor de puerta proporciona la señal de puerta cerrada cuando el circuito está abierto.
  - **Open circuit = Open door (Circuito abierto = Puerta abierta)**: seleccione esta opción si el circuito del monitor de puerta está normalmente cerrado. El monitor de puerta proporciona la señal de puerta abierta cuando el circuito está abierto. El monitor de puerta proporciona la señal de puerta cerrada cuando el circuito está cerrado.
- **Cancel access time once door is opened (Cancelar tiempo de acceso una vez que se abre la puerta)**: seleccione esta opción para prevenir infiltraciones. La cerradura se bloqueará tan pronto como el monitor de puerta señale que la puerta se ha abierto.

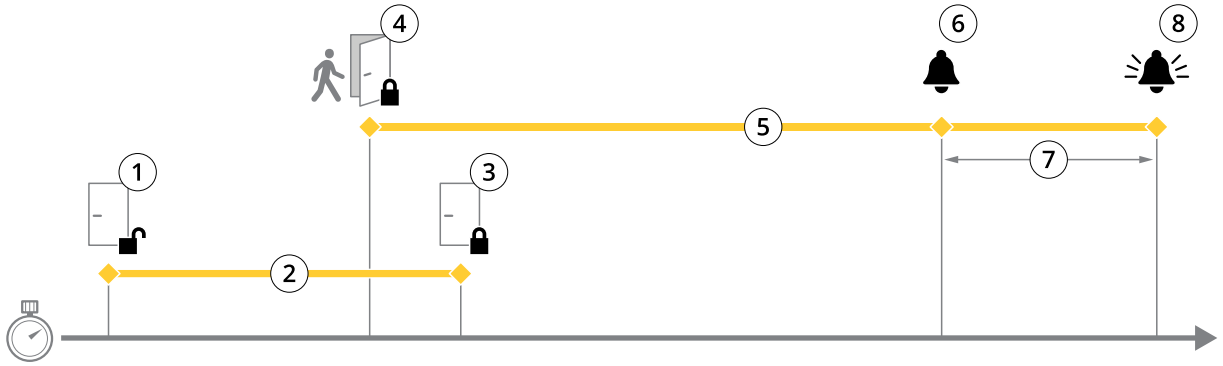
La siguientes opciones de tiempo de puerta están siempre disponibles:

- **Access time (Tiempo de acceso)**: establece el número de segundos que la puerta permanecerá desbloqueada una vez se ha concedido permiso de acceso. La puerta permanecerá desbloqueada hasta que se abra o hasta que haya transcurrido el intervalo de tiempo establecido. La puerta se bloqueará una vez cerrada, independientemente de que el tiempo de acceso no haya expirado.
- **Long access time (Tiempo de acceso largo)**: establece el número de segundos que la puerta permanecerá desbloqueada una vez que se ha concedido permiso de acceso. El tiempo de acceso largo reemplaza el tiempo de acceso establecido y se activará para los usuarios en los que se haya seleccionado el tiempo de acceso largo; consulte *Credenciales de usuario en la página 41*

Seleccione **Door monitor (Monitor de puerta)** para disponer de las siguientes opciones de tiempo de puerta:

- **Open too long time (Tiempo de apertura demasiado largo)**: establece el número de segundos que se permite que la puerta esté abierta. Si la puerta sigue abierta una vez transcurrido el período de tiempo determinado, se activa la alarma de puerta abierta durante demasiado tiempo. Configure una regla de acción para determinar qué acción debe activar el evento de puerta abierta durante demasiado tiempo.
- **Pre-alarm time (Tiempo de alarma previa)**: una alarma previa es una señal de advertencia que se activa antes de que se haya alcanzado el tiempo de apertura durante demasiado tiempo. Informa al administrador y advierte, en función de la

configuración de la regla de acción, a la persona que entra por la puerta que esta debe cerrarse a fin de evitar que se active la alarma de puerta abierta durante demasiado tiempo. Defina el número de segundos durante el cual se dará la señal de advertencia previa a la alarma antes de que el sistema active la alarma de puerta abierta durante demasiado tiempo. Para deshabilitar la advertencia previa a la alarma, defina el tiempo previo a la alarma al valor 0.



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 *Se desactiva el tiempo previo a la alarma*
7 *Tiempo previo a la alarma*
8 *La alarma de tiempo de apertura demasiado largo se desactiva*

Para obtener información sobre cómo configurar una regla de acción, consulte *Cómo configurar reglas de acción en la página 47*.

Acerca de las opciones de cerradura

Las siguientes opciones de circuito de cerradura están disponibles:

- 12 V
  - **Fail-secure (Protección en fallo)**: seleccione esta opción para que las cerraduras permanezcan bloqueadas durante un fallo de corriente. La cerradura se desbloquea al restablecerse la corriente eléctrica.
  - **Fail-safe (Seguridad en fallo)**: seleccione esta opción para que las cerraduras se desbloqueen durante un fallo de corriente. La cerradura se bloquea al restablecerse la corriente eléctrica.
- **Relay (Relé)**: solo se puede utilizar en una única cerradura por controlador de puerta. Si hay dos puertas conectadas al controlador de puerta, solamente se puede utilizar un relé en la cerradura de la segunda puerta.
  - **Relay open = Locked (Relé abierto = bloqueado)**: seleccione esta opción para que las cerraduras permanezcan bloqueadas cuando el relé está abierto (protección en fallo). Cuando se cierra el relé, la cerradura se desbloquea.
  - **Relay open = Unlocked (Relé abierto = desbloqueado)**: seleccione esta opción para que las cerraduras se desbloqueen durante un fallo de corriente (seguridad en fallo). Cuando se cierra el relé, la cerradura se bloquea.
- **None (Ninguna)**: disponible únicamente para la Cerradura 2. Seleccione esta opción si únicamente se utilizará una cerradura.

Las siguientes opciones de monitor de cerradura están disponibles para configuraciones de puerta única:

- **Lock monitor (Monitor de cerradura)**: seleccione esta opción para hacer disponibles los controles del monitor de cerradura. A continuación, seleccione la cerradura que se debe monitorizar. Solo se puede utilizar un monitor de cerradura en puertas de doble cerradura, pero no se puede utilizar si dos puertas están conectadas al controlador de puerta.

- **Open circuit = Locked (Circuito abierto = bloqueado)**: seleccione esta opción si el circuito de monitor de cerradura está normalmente cerrado. El monitor de cerradura proporciona la señal de desbloqueo de puerta cuando el circuito está cerrado. El monitor de cerradura proporciona a la puerta la señal de bloqueo cuando el circuito está abierto.
- **Open circuit = Unlocked (Circuito abierto = bloqueado)**: seleccione esta opción si el circuito de monitor de cerradura está normalmente abierto. El monitor de cerradura proporciona la señal de desbloqueo de puerta cuando el circuito está abierto. El monitor de cerradura proporciona a la puerta la señal de bloqueo cuando el circuito está cerrado.

Cómo configurar lectores y dispositivos REX

Una vez configurados los monitores de puerta y las cerraduras en la nueva configuración de hardware, puede configurar los lectores y dispositivos de solicitud de salida (REX).

1. Si se utilizará un lector, seleccione la casilla de verificación y, a continuación, seleccione las opciones que coincidan con el protocolo de comunicación del lector.
2. Si se utiliza un dispositivo REX, como un botón, un sensor o una barra de empuje, seleccione la casilla de verificación y, a continuación, seleccione la opción que coincida con el modo en que se conectarán los circuitos del dispositivo REX.

   Si la señal de REX no influye en la apertura de la puerta (por ejemplo, para puertas con manillas mecánicas o barras de empuje), seleccione **REX no desbloquea la puerta**.
3. Si se conecta más de un lector o un dispositivo REX al controlador de puerta, repita los dos pasos anteriores hasta que cada lector o dispositivo REX tenga la configuración correcta.

Acerca de las opciones de lector y dispositivo REX

Están disponibles las siguientes opciones de lector:

- **Wiegand**: seleccione esta opción para lectores que utilizan protocolos Wiegand. A continuación, seleccione el control de LED compatible con el lector. Por lo general, los lectores de un único control de LED alternan entre rojo y verde. Los lectores con control de led dual utilizan diferentes cables para los LED rojo y verde. Esto significa que los LED se controlan de manera independiente. Cuando se activan los dos LED, la luz se muestra ámbar. Consulte la información del fabricante en relación con el control de LED que admite el lector.
- **OSDP, half-duplex RS485**: seleccione esta opción para lectores RS485 que admiten half-duplex. Consulte la información del fabricante en relación con el protocolo que admite el lector.

Las siguientes opciones de dispositivo REX están disponibles:

- **Active low (Activar bajo)**: seleccione esta opción si el circuito se cierra al activarse el dispositivo REX.
- **Active high (Activar alto)**: seleccione esta opción si el dispositivo REX abre el circuito.
- **REX does not unlock door (REX no desbloquea la puerta)**: seleccione esta opción si la señal de REX no influye en la apertura de la puerta (por ejemplo, para puertas con manillas mecánicas o barras de empuje). La alarma de apertura forzada de puerta no se activará si el usuario abre la puerta dentro del tiempo de acceso. Anule la selección si la puerta se debe desbloquear automáticamente cuando el usuario activa el dispositivo REX.

Nota

La mayoría de las opciones de cerradura, monitor de puerta y lector se pueden modificar sin restablecer e iniciar una nueva configuración de hardware. Vaya a **Setup > Hardware Reconfiguration (Configuración > Reconfiguración de hardware)**.

Cómo usar entradas supervisadas

Las entradas supervisadas informan acerca del estado de la conexión entre el controlador de puerta y los lectores, dispositivos REX y monitores de puerta. Si se interrumpe la conexión, se activa un evento.

Para utilizar entradas supervisadas:

1. Instale resistencias de final de línea en todas las entradas supervisadas. Consulte el diagrama de conexión en *página 75*.
2. Vaya a **Setup > Hardware Reconfiguration (Configuración > Reconfiguración de hardware)** y seleccione **Enable supervised inputs (Habilitar entradas supervisadas)**. También puede habilitar las entradas supervisadas durante la configuración de hardware.

Acerca de la compatibilidad con la entrada supervisada

Los siguientes conectores admiten entradas supervisadas:

- Conector de lector de E/S: señal de manipulación. Consulte *página 70*.
- Conector de puerta. Consulte *página 71*.

Entre los lectores y switches que pueden utilizarse con entradas supervisadas se incluyen:

- Lectores y switches con 1 kΩ de pull-up interno a 5 V.
- Lectores y switches sin pull-up interno.

Cómo crear una nueva configuración de hardware para cierres inalámbricos

1. Vaya a **Setup > Hardware Configuration (Configuración > Configuración de hardware)** y haga clic en **Start new hardware configuration (Iniciar nueva configuración de hardware)**.
2. Introduzca el nombre del producto Axis.
3. En la lista de periféricos, seleccione un fabricante para la puerta de enlace inalámbrica.
4. Si quiere conectar una puerta con cable, seleccione la casilla **1 Door (1 puerta)** y haga clic en **Next (Siguiente)**. Si no se incluye ninguna puerta, haga clic en **Finish (Finalizar)**.
5. En función de su fabricante de cerraduras, continúe según uno de los puntos:
   - **ASSA Aperio**: Haga clic en el enlace para ver el gráfico de pines del hardware o haga clic en **Close (Cerrar)** y vaya a **Setup > Hardware Reconfiguration (Configuración > Reconfiguración de Hardware)** para completar la configuración. Consulte *Añadir puertas y dispositivos Assa Aperio™ en la página 18*.
   - **SmartIntego**: Haga clic en el enlace para ver el gráfico de pines del hardware o haga clic en **Click here to select wireless gateway and configure doors (Haga clic aquí para seleccionar la puerta de enlace inalámbrica y configurar las puertas)** para completar la configuración. Consulte *Cómo configurar SmartIntego en la página 26*.

Añadir puertas y dispositivos Assa Aperio™

Antes de añadir una puerta inalámbrica al sistema, es necesario emparejarla con el concentrador de comunicaciones Assa Aperio conectado mediante la herramienta de aplicación de programación Aperio PAP.

Para añadir una puerta inalámbrica:

1. Acceda a **Setup (Configuración)** > **Hardware Reconfiguration (Reconfiguración de hardware)**.
2. Debajo de Wireless Doors and Devices (Puertas y dispositivos inalámbricos), haga clic en **Add door (Añadir puerta)**.
3. En el campo **Door name (Nombre de puerta)**: introduzca un nombre descriptivo.
4. En el campo **ID (Identificación)**, debajo de **Lock (Cerradura)**: introduzca la dirección de seis caracteres del dispositivo que desee añadir. La dirección del dispositivo aparece impresa en la etiqueta del producto.
5. Si lo desea, en **Door position sensor (Sensor de posición de puerta externo)**: Seleccione **Built in door position sensor (Sensor de posición de puerta integrado)** o **External door position sensor (Sensor de posición de puerta externo)**.

Nota

Si utiliza un sensor de posición de puerta externo, asegúrese de que el dispositivo de bloqueo Aperio es compatible con la detección de estado del mango de la puerta antes de configurarlo.

6. Si lo desea, en el campo **ID** en **Door position sensor (Sensor de posición de puerta)**: introduzca la dirección de seis caracteres del dispositivo que desee añadir. La dirección del dispositivo aparece impresa en la etiqueta del producto.
7. Haga clic en **Add (Añadir)**.

Cómo crear una nueva configuración de hardware con control de ascensor (AXIS A9188)

Importante

Antes de crear una configuración de hardware, tiene que agregar un usuario a AXIS A9188 Network I/O Relay Module. Vaya a la interfaz web A9188> **Preferences > Additional device configuration > Basic setup > Users > Add > User setup (Preferencias > Configuración del dispositivo adicional> Configuración básica> Usuarios> Agregar> Configuración de usuario)**.

Nota

Se puede configurar un máximo de 2 AXIS 9188 Network I/O Relay Module con cada Axis Network Door Controller

1. En A1001, vaya a **Setup > Hardware Configuration (Configuración > Configuración de hardware)** y haga clic en **Start new hardware configuration (Iniciar nueva configuración de hardware)**.
2. Introduzca el nombre del producto Axis.
3. En la lista de periféricos, seleccione **Elevator control (Control de ascensor)** para incluir AXIS A9188 Network I/O Relay Module y haga clic en **Next (Siguiente)**.
4. Introduzca el nombre del lector conectado.
5. Seleccione los protocolos de lectores que se utilizarán y haga clic en **Finish (Finalizar)**.
6. Haga clic en **Network Peripherals (Periféricos de red)** para completar la configuración. Consulte *Cómo añadir y configurar periféricos de red en la página 19* o haga clic en el enlace para acceder al gráfico de pines del hardware.

Cómo añadir y configurar periféricos de red

Importante

- Antes de configurar los periféricos de red, se debe añadir un usuario en AXIS A9188 Network I/O Relay Module. Vaya a la interfaz web AXIS A9188 > **Preferences > Additional device configuration > Basic setup > Users > Add > User setup (Preferencias > Configuración del dispositivo adicional> Configuración básica> Usuarios> Agregar> Configuración de usuario)**.
- No añada otro AXIS A1001 Network Door Controller como periférico de red.

1. Vaya a **Setup > Network Periphals (Configuración > Periféricos de red)** para añadir un dispositivo
2. Identifique sus dispositivos en **Discovered devices (Dispositivos detectados)**.
3. Haga clic en **Add this device (Añadir este dispositivo)**.
4. Introduzca un nombre para el dispositivo
5. Introduzca el nombre de usuario y la contraseña para AXIS A9188.
6. Haga clic en **Add (Añadir)**.

Nota

Puede añadir periféricos de red manualmente introduciendo la dirección MAC o la dirección IP en el cuadro de diálogo **Manually add device (Añadir dispositivo manualmente)**.

Importante

Si quiere eliminar una programación, asegúrese primero de que el módulo de relé de E/S de red no la utiliza.

Cómo configurar E/S y relés de periféricos en red

Importante

Antes de configurar los periféricos de red, se debe añadir un usuario en AXIS A9188 Network I/O Relay Module. Vaya a la interfaz web AXIS A9188 > **Preferences > Additional device configuration > Basic setup > Users > Add > User setup (Preferencias > Configuración del dispositivo adicional> Configuración básica> Usuarios> Agregar> Configuración de usuario)**.

1. Vaya a **Setup > Network Periphals (Configuración > Periféricos de red)** y haga clic en la fila **Added devices (Dispositivos añadidos)**.
2. Seleccione los E/s y relés que se establecerán como planta.
3. Haga clic en **Set as floor (Establecer como planta)** e introduzca un nombre.
4. Haga clic en **Add (Añadir)**.

La planta es ahora visible en la pestaña **Floor (Planta)**, en **Access Management (Administración de accesos)**.

Nota

Puede añadir un máximo de 16 plantas a AXIS Entry Manager.

Verificar las conexiones de hardware

Una vez completada la instalación y la configuración de hardware, y en cualquier momento durante la vida útil del controlador de puerta, se puede verificar el funcionamiento de los monitores de puerta conectados, los módulos de relé de E/S de red, las cerraduras y los lectores.

Para verificar la configuración y el acceso a los controles de verificación, vaya a **Setup > Hardware Connection Verification (Configuración > Verificación de conexión de hardware)**.

Verificación de controles de puertas

- **Estado de puerta**: verificar el estado actual del monitor de puerta, alarmas de puerta y cerraduras. Haga clic en **Get current state (Obtener estado actual)**.
- **Cerradura**: activa manualmente la cerradura. Las cerraduras principales y secundarias, en su caso, se verán afectadas. Haga clic en **Lock (Bloquear)** o **Unlock (Desbloquear)**.
- **Lock (Cerradura)**: activa manualmente la cerradura para permitir el acceso. Solo se verán afectadas las cerraduras principales. Haga clic en **Access (Acceso)**.
- **Lector: Información**: verifica la información del lector, como sonidos y señales LED, para distintos comandos. Seleccione el comando y haga clic en **Test (Prueba)**. Los tipos de información disponibles dependen del lector. Para obtener más información, consulte *Información del lector en la página 52*. Consulte también las instrucciones del fabricante.
- **Lector: Manipulación**: proporciona información sobre el último intento de manipulación. El primer intento de manipulación se registrará al instalar el lector. Haga clic en **Get last tampering (Obtener última manipulación)**.
- **Lector: Deslizamiento de tarjeta**: proporciona información sobre la última tarjeta pasada u otros tipos de comprobante aceptados por el lector. Haga clic en **Get last credential (Obtener últimas credenciales)**.
- **REX**: proporciona información sobre la última vez que se pulsó el dispositivo de solicitud de salida (REX). Haga clic en **Get last REX (Obtener última REX)**.

Verificación de controles de plantas

- **Floor state (Estado de planta)**: verifica el estado actual de acceso a la planta. Haga clic en **Get current state (Obtener estado actual)**.
- **Floor lock & unlock (Bloquear y desbloquear planta)**: activa manualmente el acceso a la planta. Las cerraduras principales y secundarias, en su caso, se verán afectadas. Haga clic en **Lock (Bloquear)** o **Unlock (Desbloquear)**.
- **Floor access (Acceso a planta)**: concede manualmente acceso temporal a la planta. Solo se verán afectadas las cerraduras principales. Haga clic en **Access (Acceso)**.
- **Lector de ascensor: Información**: verifica la información del lector, como sonidos y señales LED, para distintos comandos. Seleccione el comando y haga clic en **Test (Prueba)**. Los tipos de información disponibles dependen del lector. Para obtener más información, consulte *Información del lector en la página 52*. Consulte también las instrucciones del fabricante.
- **Lector de ascensor: Manipulación**: proporciona información sobre el último intento de manipulación. El primer intento de manipulación se registrará al instalar el lector. Haga clic en **Get last tampering (Obtener última manipulación)**.
- **Lector de ascensor: Deslizamiento de tarjeta**: proporciona información sobre la última tarjeta pasada u otros tipos de comprobante aceptados por el lector. Haga clic en **Get last credential (Obtener últimas credenciales)**.
- **REX**: proporciona información sobre la última vez que se pulsó el dispositivo de solicitud de salida (REX). Haga clic en **Get last REX (Obtener última REX)**.

Configurar tarjetas y formatos

El controlador de puerta incorpora algunos formatos de tarjeta predefinidos habitualmente utilizados que se pueden utilizar o modificar en función de las necesidades. También se pueden crear formatos de tarjeta personalizados. Cada formato de tarjeta incluye un conjunto de reglas y mapas de campo diferentes para la forma de organizar la información almacenada en la tarjeta. Al definir un formato de tarjeta, se indica al sistema cómo se debe interpretar la información que el controlador recibe del lector. Para obtener información acerca de los tipos de formato de tarjeta compatibles con el lector, consulte las instrucciones del fabricante.

Para habilitar formatos de tarjeta:

1. Vaya a **Setup > Configure cards and formats (Configuración > Configurar tarjetas y formatos)**.
2. Seleccione uno o varios formatos de tarjeta que coincidan con el formato de tarjeta utilizado por los lectores conectados.

Para crear nuevos formatos de tarjeta:

1. Vaya a **Setup > Configure cards and formats (Configuración > Configurar tarjetas y formatos)**.
2. Haga clic en **Add card format (Añadir formato de tarjeta)**.
3. En el cuadro de diálogo **Add card format (Añadir formato de tarjeta)**, introduzca el nombre, la descripción y la longitud de bits del formato de tarjeta. Consulte *Descripciones de formato de tarjeta en la página 22*.
4. Haga clic en **Add field map (Añadir mapa de campo)** e introduzca la información requerida en los campos. Consulte *Mapas de campo en la página 22*.
5. Para añadir varios mapas de campo, repita el paso anterior.

Para expandir un elemento en la lista **Card formats (Formatos de tarjeta)** y ver las descripciones de formato de tarjeta y mapas de campo, haga clic en  .

Para editar un formato de tarjeta, haga clic en  y modifique las descripciones de formato de tarjeta y mapas de campo de acuerdo con sus necesidades. A continuación, haga clic en **Save (Guardar)**.

Para eliminar un mapa de campo en los cuadros de diálogo **Edit card format (Editar formato de tarjeta)** o **Add card format (Añadir formato de tarjeta)**, haga clic en 

Para eliminar un formato de tarjeta, haga clic en  .

Importante

- Todos los cambios realizados en los formatos de tarjeta se aplican a todo el sistema de controladores de puerta.
- Solo se pueden activar y desactivar formatos de tarjeta si al menos un controlador de puerta en el sistema se ha configurado con al menos un lector. Consulte *Configuración del hardware en la página 13* y *Cómo configurar lectores y dispositivos REX en la página 17*.
- No pueden estar activos simultáneamente dos formatos de tarjeta con la misma longitud de bits. Por ejemplo, si se han definido dos formatos de tarjeta de 32 bits, "Formato A" y "Formato B", y se ha habilitado el "Formato A", no se puede habilitar el "Formato B" sin deshabilitar primero el "Formato B".
- Si no hay formatos de tarjeta habilitados, se pueden utilizar los tipos de identificación **Card raw only (Solo tarjeta sin formato)** y **Card raw and PIN (Tarjeta sin formato y PIN)** para identificar una tarjeta y permitir el acceso a los usuarios. Sin embargo, no se recomienda, dado que diferentes fabricantes o diferentes configuraciones de lectores pueden generar distintos datos de tarjeta sin formato.

Descripciones de formato de tarjeta

- **Name (Nombre)** (obligatorio): introduzca un nombre descriptivo.
- **Description (Descripción)**: introduzca la información adicional que desee. Esta información solo es visible en los cuadros de diálogo **Edit card format (Editar formato de tarjeta)** y **Add card format (Añadir formato de tarjeta)**.
- **Bit length (Longitud de bits)** (obligatorio): escriba la longitud de bits del formato de tarjeta. Debe ser un número entre 1 y 1000000000.

Mapas de campo

- **Name (Nombre)** (requerido): introduzca el nombre del mapa de campo sin espacios; por ejemplo, `OddParity` (paridad impar).

  Ejemplos de mapas de campo comunes:

  - `Parity` (paridad): la paridad bits se utiliza para la detección de errores. Los bits de paridad habitualmente se añaden al principio o al final de una cadena de código binario e indican si el número de bits es par o impar.
  - `EvenParity` (paridad par): los bits de paridad impar aseguran que la cadena contenga un número de bits par. Se cuentan los bits que tienen valor 1. Si el recuento ya es par, el valor de bits de paridad se establece en 0. Si el recuento es impar, se establece el valor de bits de paridad par en 1, de manera que el recuento total es un número par.
  - `OddParity` (paridad impar): los bits de paridad impar aseguran que la cadena contenga un número de bits impar. Se cuentan los bits que tienen valor 1. Si el recuento ya es impar, el valor de bits de paridad impar se establece en 0. Si el recuento es par, se establece el valor de bits de paridad par en 1, de manera que el recuento total es un número impar.
  - `FacilityCode` (código de instalación): los códigos de instalaciones se utilizan en ocasiones para comprobar que el token coincide con el lote de credenciales de usuario final ordenado. En sistemas heredados de control de acceso, se utilizaba el código de instalación para una validación reducida, permitiendo el acceso a todos los empleados incluido en el lote de credenciales que se había codificado con un código de instalación coincidente. Este nombre de mapa de campo, sensible a mayúsculas y minúsculas, es requerido para que el producto valide un código de instalación.
  - `CardNr` (número de tarjeta): el número de tarjeta o ID de usuario es lo que habitualmente se valida en sistemas de control de acceso. Este nombre de mapa de campo, sensible a mayúsculas y minúsculas, es requerido para que el producto valide un número de tarjeta.
  - `CardNrHex` (número hexadecimal de tarjeta): los datos binarios del número de tarjeta se codifican en el producto como números hexadecimales en minúsculas. Se utiliza principalmente para solucionar problemas cuando no se obtiene el número de tarjeta esperado del lector.

- **Range (rango)** (requerido): introduzca el rango de bits del mapa de campo; por ejemplo, 1, 2-17, 18-33 y 34.
- **Encoding (Codificación)** (requerido): seleccione el tipo de codificación de cada mapa de campo.

- **BinLE2Int**: los datos binarios se codifican como números enteros en orden de bits little-endian. Integer (entero) significa que debe ser un número entero (sin decimales). Orden de bits little-endian significa que el primer bit es el más pequeño (menos significativo).
- **BinBE2Int**: los datos binarios se codifican como números enteros en orden de bits big-endian. Integer (entero) significa que debe ser un número entero (sin decimales). Orden de bits big-endian significa que el primer bit es el más grande (más significativo).
- **BinLE2Hex**: los datos binarios se codifican como números hexadecimales en orden de bits little-endian. El sistema hexadecimal, también conocido como sistema numérico de base 16, consta de 16 símbolos únicos: los números 0-9 y las letras a-f. Orden de bits little-endian significa que el primer bit es el más pequeño (menos significativo).
- **BinBE2Hex**: los datos binarios se codifican como números hexadecimales en orden de bits big-endian. El sistema hexadecimal, también conocido como sistema numérico de base 16, consta de 16 símbolos únicos: los números 0-9 y las letras a-f. Orden de bits big-endian significa que el primer bit es el más grande (más significativo).
- **BinLEIBO2Int**: los datos binarios se codifican del mismo modo que en BinLE2Int, pero los datos de tarjeta sin formato se leen en un orden de bytes invertido en una secuencia multibyte antes de obtener los mapas de campo para la codificación.
- **BinBEIBO2Int**: los datos binarios se codifican del mismo modo que en BinBE2Int, pero los datos de tarjeta sin formato se leen en un orden de bytes invertido en una secuencia multibyte antes de obtener los mapas de campo para la codificación.

Para obtener información acerca de los mapa de campo que utiliza su formato de tarjeta, consulte las instrucciones del fabricante.

Código de instalación predefinido

Los códigos de instalación a veces se utilizan para comprobar que el token coincide con el sistema de control de acceso de la instalación. Con frecuencia todos los tokens emitidos para una misma instalación presentan el mismo código de instalación. Introduzca un código de instalación predefinido para facilitar el registro manual de un lote de tarjetas. El código de instalación predefinido se rellena automáticamente al añadir usuarios; consulte *Credenciales de usuario en la página 41*

Para establecer un código de instalación predefinido:

1. Vaya a **Setup > Configure cards and formats (Configuración > Configurar tarjetas y formatos)**.
2. En **Preset facility code (Código de instalación predefinido)**: Introduzca un código de instalación.
3. Haga clic en **Set facility code (Definir código de instalación)**.

Configurar servicios

La función de configurar servicios, en la página de configuración, se utiliza para acceder a la configuración de los servicios externos que se pueden utilizar con el controlador de puerta.

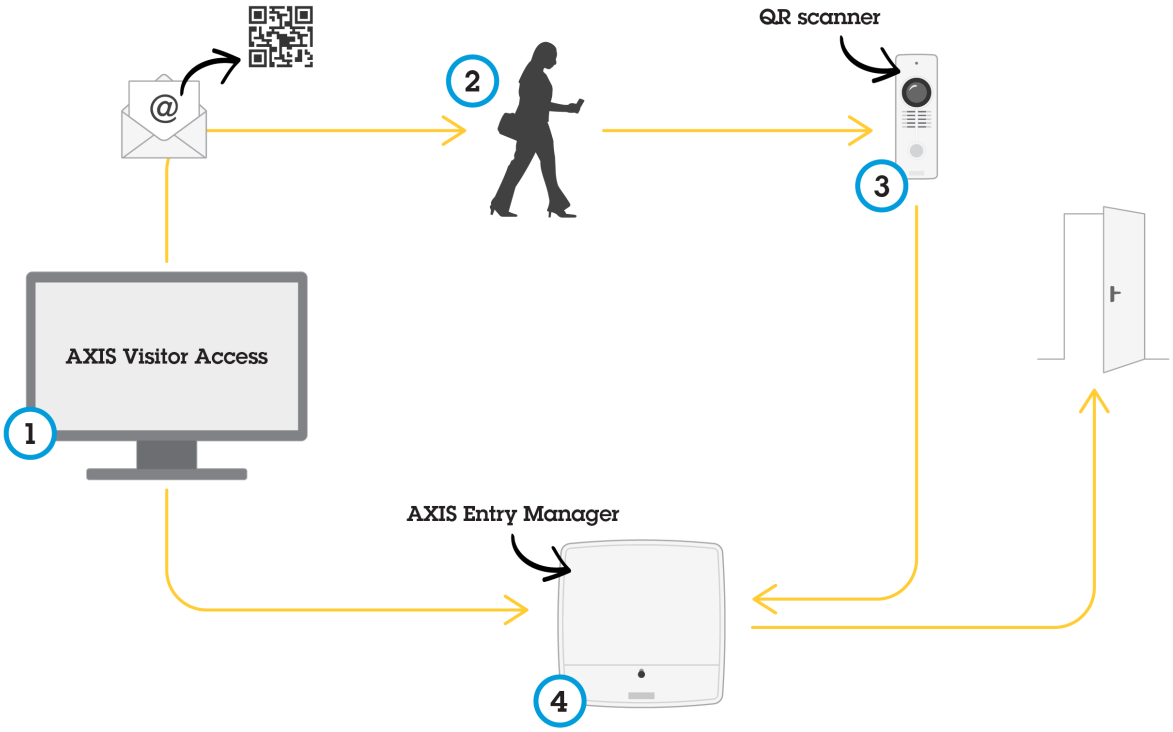
AXIS Visitor Access

Con AXIS Visitor Access, se pueden crear credenciales temporales en forma de código QR. Una cámara de red Axis o un videoportero conectado al sistema de control de acceso analiza el código QR.

El servicio se compone de:

- un controlador de puerta Axis con AXIS Entry Manager y versión de firmware 1.65.2 o superior
- una cámara de red o videoportero Axis, con la aplicación QR scanner instalada
- ordenador con Windows® con la aplicación AXIS Visitor Access instalada

Configuración del sistema



Uso del servicio AXIS Visitor Access

El usuario crea una invitación en AXIS Visitor Access (1) y envía la invitación a la dirección de correo electrónico del visitante. Simultáneamente, se crean las credenciales para desbloquear la puerta y se almacenan en el controlador de puerta de Axis conectado (4). El visitante muestra el código QR incluido en la invitación a la cámara de red o videoportero (3), que solicita al controlador de puerta (4) que desbloquee la puerta a los visitantes.

Código QR es una marca registrada de onda Denso, Inc..

Requisitos previos de AXIS Visitor Access

Para poder utilizar el servicio AXIS Visitor Access, es necesario:

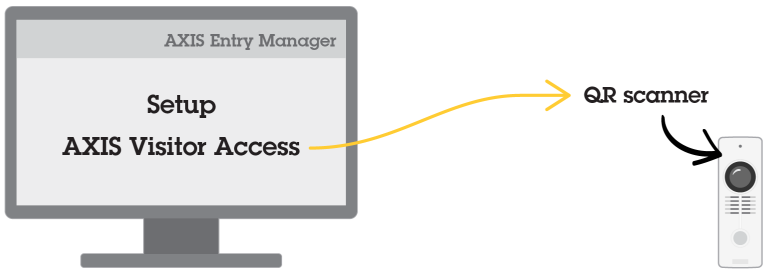
- para configurar el hardware del controlador de puerta
- un videoportero o una cámara de red Axis conectados a la misma red que el controlador de puerta y accesible a los visitantes en la puerta
- el paquete de instalación de AXIS Visitor Access. Puede encontrarlo en *axis.com*
- dos cuentas de usuario adicionales en el controlador de puerta, que utilizará exclusivamente el servicio AXIS Visitor Access. Necesita uno para la aplicación AXIS Visitor Access y otro para la aplicación QR scanner. Para obtener información sobre cómo crear cuentas de usuario, consulte *Usuarios en la página 55*.

Configuración del sistema

Importante

- Sólo se puede conectar el servicio AXIS Visitor Access a un solo controlador de puerta en todo el sistema.
- Con el servicio AXIS Visitor Access, solo se puede acceder a puertas controladas por el controlador de puerta conectado. No se puede acceder a otras puertas del sistema.
- Use la aplicación AXIS Visitor Access para modificar y eliminar visitantes. No utilice AXIS Entry Manager.
- Si cambia la contraseña de la cuenta de usuario utilizada para AXIS Visitor Access, tendrá que actualizarla también en AXIS Visitor Access.
- Si cambia la contraseña de la cuenta de usuario utilizada en la aplicación QR scanner, tendrá que volver a configurar el lector de códigos QR.

Configurar AXIS Visitor Access



La aplicación QR scanner se instala en la cámara de red o videoportero Axis al configurar el servicio AXIS Visitor Access. No es necesario realizar ninguna instalación independiente.

1. En la página web del controlador de puerta, vaya a **Setup > Configure Services > Settings (Configuración > Configurar servicios > Ajustes)**.
2. Haga clic en **Start a new setup (Iniciar una nueva configuración)**.
3. Siga las instrucciones para finalizar la configuración.

Importante

Si quiere aplicar HTTPS, asegúrese de que el controlador de puerta se comunica a través de HTTPS. De lo contrario, la aplicación no podrá comunicarse con el controlador de puerta.

4. Instale y configure la aplicación AXIS Visitor Access en el equipo que se utilizará para crear credenciales temporales.

SmartIntego

SmartIntego es una solución inalámbrica que aumenta el número de puertas que puede gestionar un controlador de puerta.

Requisitos previos de SmartIntego

Hay que reunir los requisitos previos siguientes antes de continuar con la configuración de SmartIntego:

- Hay que crear un archivo csv. El archivo csv contiene información sobre el GatewayNode y las puertas que se utilizan en la solución SmartIntego. El archivo se crea en un software autónomo proporcionado por un socio de SimonsVoss.
- Se ha completado la configuración de hardware de SmartIntego. Consulte *Cómo crear una nueva configuración de hardware para cierres inalámbricos en la página 18*.

Nota

- La configuración de SmartIntego debe ser la versión 2.1.6452.23485, compilación 2.1.6452.23485 (31/8/2017 1:02:50 h) o posterior.
- El estándar de cifrado avanzado (AES) no es compatible con SmartIntego y, por lo tanto, debe estar desactivado en la configuración de SmartIntego.

Cómo configurar SmartIntego

Nota

- Asegúrese de que se reúnen los requisitos previos enumerados.
- Para una mayor visibilidad del estado de la batería, vaya a **Setup (Configuración)** > **Configure event and alarms logs (Configurar registros de eventos y alarmas)** y añada **Door — Battery alarm (Puerta — Alarma de batería)** o **IdPoint — Battery alarm (IdPoint — Alarma de batería)** como alarma.
- Los ajustes de monitor de puerta provienen del archivo CSV importado. No debería tener que cambiar este ajuste en una instalación normal.

1. Haga clic en **Browse... (Examinar...)**, seleccione el archivo csv y haga clic en **Upload file (Cargar archivo)**.
2. Seleccione un GatewayNode y haga clic en **Next (Siguiente)**.
3. Se muestra una vista previa de la nueva configuración. En caso necesario, desactive los monitores de puerta.
4. Haga clic en **Configure (Configuración)**.
5. Se muestra una vista completa de las puertas incluidas en la configuración. Haga clic en **Settings (Configuración)** para configurar cada puerta individualmente.

Cómo configurar de nuevo SmartIntego

1. Haga clic en **Setup (Configuración)** en el menú superior.
2. Haga clic en **Configure Services (Configurar servicios)** > **Settings (Ajustes)**.
3. Haga clic en **Re-configure (Configurar de nuevo)**.
4. Haga clic en **Browse... (Examinar...)**, seleccione el archivo csv y haga clic en **Upload file (Cargar archivo)**.
5. Seleccione un GatewayNode y haga clic en **Next (Siguiente)**.
6. Se muestra una vista previa de la nueva configuración. En caso necesario, desactive los monitores de puerta.

Nota

Los ajustes de monitor de puerta provienen del archivo CSV importado. No debería tener que cambiar este ajuste en una instalación normal.

7. Haga clic en **Configure (Configuración)**.
8. Se muestra una vista completa de las puertas incluidas en la configuración. Haga clic en **Settings (Configuración)** para configurar cada puerta individualmente.

Administrar controladores de puerta en red

La página de administración de controladores de puerta en red en el sistema muestra información sobre el controlador de puerta, su estado de sistema y el resto de controladores de puerta que forman parte del sistema. También permite al administrador modificar la configuración del sistema, añadiendo y eliminando controladores de puertas.

Configuración del sistema

Importante

Todos los controladores de puerta de un sistema deben estar conectados a la misma red y estar configurados para su uso en un solo sitio.

Para administrar los controladores de puertas, vaya a **Setup > Manage Network Door Controllers in System (Configuración > Administrar controladores de puerta en red en el sistema)**.

La página de administración de controladores de puerta en red en el sistema incluye los paneles siguientes:

- **System status of this controller (Estado de sistema de este controlador)**: muestra el estado de sistema del controlador de puerta y permite alternar entre los modos de sistema e independiente. Para obtener más información, consulte *Estado de sistema del controlador de puerta en la página 27*.
- **Network door controllers in system (Controladores de puerta en red en el sistema)**: muestra información sobre los controladores de puerta en el sistema e incluye controles para añadir y eliminar un controlador del sistema. Para obtener más información, consulte *Controladores de puerta conectados en el sistema en la página 27*.

Estado de sistema del controlador de puerta

En función de su estado de sistema, el controlador de puerta puede formar parte de un sistema de controladores de puerta. El estado de sistema del controlador de puerta se muestra en el panel **System status for this controller (Estado de sistema de este controlador)**.

Si el controlador de puerta no está en modo independiente y desea evitar que el controlador de puerta se pueda añadir a un sistema, haga clic en **Activate standalone mode (Activar modo independiente)** para pasarlo a modo independiente.

Si el controlador de puerta está en modo independiente, pero desea añadir el controlador de puerta a un sistema, haga clic en **Deactivate standalone mode (Desactivar modo independiente)** para salir del modo independiente.

Modos de sistema

- **This controller is not part of a system and not in standalone mode (Este controlador no forma parte de un sistema y no está en modo independiente)**: el controlador de puerta no se ha configurado como parte de un sistema y no está en modo independiente. Esto significa que el controlador de puerta está abierto y se puede ser añadido a un sistema por parte de cualquier otro controlador en la misma red. A fin de evitar que el controlador de puerta se añada a un sistema, active el modo independiente.
- **This controller is set to standalone mode (Este controlador está establecido en modo independiente)**: el controlador de puerta no forma parte de un sistema. No puede ser añadido a un sistema por parte de otros controladores de puerta en la red ni se pueden añadir al mismo otros controladores de puerta. El modo independiente se utiliza normalmente en configuraciones pequeñas con un solo controlador de puerta y una o dos puertas. Para permitir que el controlador de puerta sea añadido a un sistema, desactive el modo independiente.
- **This controller is part of a system (Este controlador forma parte de un sistema)**: el controlador de puerta forma parte de un sistema distribuido. En el sistema distribuido, los usuarios, grupos, puertas y programaciones se comparten entre los controladores conectados.

Controladores de puerta conectados en el sistema

El panel **Network door controllers in system (Controladores de puerta en red en el sistema)** proporciona controles para los siguientes cambios en el sistema:

- Añadir un controlador de puerta a un sistema; consulte *Añadir controladores de puerta al sistema en la página 28*.
- Eliminar un controlador de puerta de un sistema; consulte *Eliminar controladores de puerta del sistema en la página 29*.

Lista de controladores de puerta conectados

El panel **Network door controllers in system (Controladores de puerta en red en el sistema)** también incluye una lista que muestra la siguiente información de identificación y estado en relación con los controladores de puerta conectados en el sistema:

- **Name (Nombre)** : el nombre del controlador de puerta definido por el usuario. Si el administrador no estableció un nombre durante la configuración del hardware, se mostrará el nombre predeterminado.
- **IP address (Dirección IP)**
- **MAC address (Dirección MAC)**
- **Status (Estado)**: el controlador de puerta desde el que se accede al sistema mostrará el estado **This controller (Este controlador)**. El resto de controladores de puerta en el sistema mostrarán el estado **Online (En línea)**.
- **Firmware version (Versión de firmware)**

Para abrir las páginas web de otro controlador de puerta, haga clic en la dirección IP del controlador.

Para actualizar la lista, haga clic en **Refresh the list of controllers (Actualizar la lista de controladores)**.

Nota

Todos los controladores de un sistema deben tener siempre la misma versión de firmware. Utilice Axis Device Manager para realizar una actualización paralela del firmware en todos los controladores en la totalidad del sistema.

Añadir controladores de puerta al sistema

Importante

Al emparejar controladores de puerta, todos los ajustes de gestión de acceso del controlador añadido se borran y son sustituidos por los ajustes de gestión de acceso del sistema.

Para añadir al sistema un controlador de puerta de la lista de controladores de puerta:

1. Vaya a **Setup > Manage Network Door Controllers in System (Configuración > Administrar controladores de puerta en red en el sistema)**.
2. Haga clic en **Add controllers to system from list (Añadir controladores al sistema desde lista)**.
3. Seleccione el controlador de puerta que desea añadir.
4. Haga clic en **Add (Añadir)**.
5. Para añadir más controladores de puerta, repita los pasos anteriores.

Para añadir un controlador de puerta al sistema por su dirección IP o dirección MAC conocida:

1. Vaya a **Manage Devices (Administración de dispositivos)**.
2. Haga clic en **Add controller to system by IP or MAC address (Añadir controlador al sistema por dirección IP o MAC)**.
3. Introduzca la dirección IP o MAC.
4. Haga clic en **Add (Añadir)**.
5. Para añadir más controladores de puerta, repita los pasos anteriores.

Una vez completado el emparejamiento, todos los usuarios, puertas, programaciones y grupos son compartidos por todos los controladores en el sistema.

Para actualizar la lista, haga clic en **Refresh list of controllers (Actualizar lista de controladores)**.

Eliminar controladores de puerta del sistema

Importante

- Antes de eliminar un controlador de puerta del sistema, restablezca su configuración del hardware. Si omite este paso, todas las puertas vinculadas al controlador de puerta eliminado permanecerán en el sistema y no se podrán eliminar.
- Al eliminar un controlador de puerta de un sistema de dos controladores, ambos controladores de puerta pasan automáticamente al modo independiente.

Para eliminar un controlador de puerta del sistema:

1. Acceda al sistema desde el controlador de puerta que desee eliminar y vaya a **Setup > Hardware Configuration (Configuración > Configuración de Hardware)**.
2. Haga clic en **Reset hardware configuration (Restablecer la configuración de hardware)**.
3. Una vez que se ha restablecido la configuración de hardware, vaya a **Setup > Manage Network Door Controllers in System (Configuración > Administrar controladores de puerta en red en el sistema)**.
4. En la lista **Network door controllers in system (Controladores de puerta en red en el sistema)**, identifique el controlador de puerta que desee eliminar y haga clic en **Remove from system (Eliminar del sistema)**.
5. Se abrirá un cuadro de diálogo que le instará a restablecer la configuración de hardware del controlador de puerta. Haga clic en **Remove controller (Eliminar controlador)** para confirmar.
6. Se abrirá un cuadro de diálogo para confirmar que desea eliminar el controlador de puerta. Haga clic en **OK (Aceptar)** para confirmar. El controlador de puerta eliminado se mostrará en modo independiente.

Nota

- Cuando se elimina un controlador de puerta del sistema, se eliminan todos sus ajustes de gestión de acceso.
- Solo se pueden eliminar controladores de puerta que estén en línea.

Modo de configuración

La primera vez que se accede al dispositivo, el modo de configuración es el modo estándar. Mientras el modo de configuración está deshabilitado, la mayoría de características de configuración del dispositivo están ocultas.

Importante

Para deshabilitar el modo de configuración no se debe tener en cuenta una característica de seguridad. Está diseñado para detener los errores de configuración, no para impedir que usuarios malicioso cambien ajustes vitales.

Cómo desactivar el modo de configuración

1. Vaya a **Setup (Configuración)** > **Disable Configuration Mode (Desactivar el modo de configuración)**.
2. Introduzca un PIN y seleccione **OK (Aceptar)**.

Nota

El PIN no es obligatorio.

Cómo habilitar el modo de configuración

1. Vaya a **Setup (Configuración)** > **Enable Configuration Mode (Activar el modo de configuración)**.
2. Introduzca el PIN y seleccione **OK (Aceptar)**.

Nota

Si no recuerda su PIN, puede activar el modo de configuración introduciendo `http://[IP-address]/webapp/pacs/index.shtml#resetConfigurationMode`.

Instrucciones de mantenimiento

Para mantener el sistema de control de acceso funcionando correctamente, Axis recomienda efectuarle un mantenimiento periódico, incluidos los controladores de puerta y los dispositivos conectados.

Efectúe tareas de mantenimiento al menos una vez al año. El procedimiento de mantenimiento sugerido incluye, aunque sin limitarse a ellos, los siguientes pasos:

- Compruebe que todas las conexiones entre el controlador de puerta y los dispositivos externos sean seguras.
- Verifique todas las conexiones de hardware. Consulte *Verificación de controles de puertas en la página 20*.
- Compruebe que el sistema funcione correctamente, incluidos los dispositivos externos conectados.
  - Pase una tarjeta y pruebe los lectores, las puertas y las cerraduras.
  - Si el sistema incluye dispositivos REX, sensores u otros dispositivos, pruébelos también.
  - Si están activadas, pruebe también las alarmas antimanipulación.

Si los resultados de cualquiera de los pasos anteriores indican que hay fallos o comportamientos inesperados:

  - Pruebe las señales de los cables usando los equipos adecuados y compruebe si los cables están dañados en algún sentido.
  - Sustituya todos los cables defectuosos.
  - Una vez que se hayan sustituido los cables, compruebe de nuevo las conexiones de hardware. Consulte *Verificación de controles de puertas en la página 20*.
- Asegúrese de que estén actualizados todos usuarios y los grupos, así como las puertas y las programaciones de acceso.
- Si el controlador de puerta no actúa del modo previsto, consulte *Solución de problemas en la página 67* y *Mantenimiento en la página 63* para obtener más información.

Gestión de acceso

Acerca de los usuarios

En AXIS Entry Manager, los usuarios son personas que se han registrado como propietarios de uno o varios tokens (tipos de identificación). Cada persona debe tener un perfil de usuario único para tener acceso a las puertas en el sistema de control de acceso. El perfil de usuario se compone de credenciales que indican al sistema la identidad del usuario y cuándo y cómo se le concede acceso a puertas. Para obtener más información, consulte *Crear y editar usuarios en la página 40*.

En este contexto no deben confundirse los usuarios con los administradores. Los administradores tienen acceso sin restricciones a todos los ajustes. Y en el contexto de la gestión del sistema de control de acceso, las páginas web del producto (AXIS Entry Manager), en ocasiones también se denomina usuarios a los administradores. Para obtener más información, consulte *Usuarios en la página 55*.

Página de gestión de accesos

La página de gestión de accesos permite configurar y gestionar los usuarios, grupos, puertas y programaciones del sistema. Para abrir la página de gestión de acceso, haga clic en **Access Management (Gestión de accesos)**.

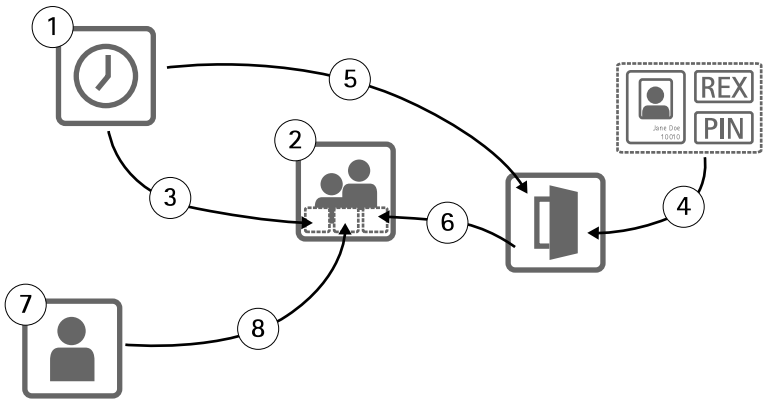
Para añadir usuarios a grupos y aplicar programaciones de acceso y puertas, arrastre los elementos a sus correspondientes destinos en las listas **Groups (Grupos)** y **Doors (Puertas)**.

Nota

Los mensajes que requieren una acción se muestran en texto rojo.

Seleccionar un flujo de trabajo

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



1. Crear programaciones de acceso. Consulte *página 32*.
2. Crear grupos. Consulte *página 34*.
3. Aplicar programaciones de acceso a grupos.
4. Añadir tipos de identificación a las puertas o plantas. Consulte *página 35* y *página 36*.
5. Aplicar programaciones de acceso a cada tipo de identificación.
6. Aplicar puertas o plantas a grupos.
7. Crear usuarios. Consulte *página 40*.

8. Añadir usuarios a los grupos.

Para consultar ejemplos aplicados de este flujo de trabajo, consulte *Ejemplo de combinaciones de programación de acceso en la página 42*.

Crear y editar programaciones de acceso

Las programaciones de acceso se utilizan para definir reglas generales sobre cuándo se puede acceder a las puertas. También se utilizan para definir reglas sobre cuándo pueden los grupos acceder a las puertas del sistema. Para obtener más información, consulte *Tipos de programaciones de acceso en la página 32*.

Para crear una nueva programación de acceso:

1. Vaya a **Access Management (Gestión de acceso)**.
2. En la pestaña **Access Schedules (Programaciones de acceso)**, haga clic en **Add new schedule (Añadir nueva programación)**.
3. En el cuadro de diálogo **Add access schedule (Añadir programación de acceso)**, introduzca el nombre de la programación.
4. Para crear una programación de acceso normal, seleccione **Addition Schedule (Programación de adición)**.

   O bien, para crear una programación de sustracción, seleccione **Subtraction Schedule (Programación de sustracción)**.

   Para obtener más información, consulte *Tipos de programaciones de acceso en la página 32*.
5. Haga clic en **Save (Guardar)**.

Para expandir un elemento en la lista **Access Schedules (Programaciones de acceso)**, haga clic en . Las programaciones de adición se muestran en texto verde, mientras que las programaciones de sustracción se muestran en texto rojo oscuro.

Para ver el calendario de una programación de acceso, haga clic en .

Para editar el nombre de una programación acceso o un elemento de una programación, haga clic en y realice los cambios. A continuación, haga clic en **Save (Guardar)**.

Para eliminar una programación de acceso, haga clic en .

Nota

El controlador de puerta dispone de algunas programaciones de acceso predefinidas de uso habitual que se pueden utilizar como ejemplo o modificar según las necesidades. En todo caso, la programación de acceso predefinida **Always (Siempre)** no se puede modificar o eliminar.

Tipos de programaciones de acceso

Existen dos tipos de programaciones de acceso:

- **Addition schedule (Programación de adición)**: programaciones de acceso normal que definen cuándo se puede acceder a las puertas. Las programaciones de adición más habituales son horario de oficina, horario laboral, fuera de horario u horario nocturno.
- **Subtraction schedule (Programación de sustracción)**: introducen excepciones a las programaciones de acceso normal. Se utilizan habitualmente para restringir el acceso durante un intervalo de tiempo específico contenido en el intervalo de tiempo de una programación normal (programación de adición): Por ejemplo, las programaciones de sustracción pueden utilizarse para denegar el acceso a los edificios por parte de los usuarios durante los días festivos que coincidan con días de la semana.

Los dos tipos de programaciones de acceso se pueden utilizar en dos niveles:

- **Identification type schedules (Programaciones de tipo de identificación)**: definen cuándo y cómo permiten los lectores el acceso a una puerta. Cada tipo de identificación debe estar conectado a una programación de acceso que indica al

sistema cuándo se concede acceso a los usuarios con ese tipo concreto de identificación. Se pueden añadir múltiples programaciones de adición y de sustracción a cada tipo de identificación. Para obtener información sobre los tipos de identificación, consulte *página 36*.

- **Group schedules (Programaciones de grupo)**: Definen cuándo (pero no cómo) pueden acceder a una puerta los miembros de un grupo. Cada grupo debe estar conectado a una o varias programaciones de acceso que indican al sistema cuando se concede acceso a sus miembros. Se pueden añadir múltiples programaciones de adición y de sustracción a cada grupo. Para obtener información acerca de los grupos, consulte *página 34*.

Las programaciones de grupo pueden restringir los derechos de acceso, pero no pueden extender los derechos de entrada o salida más allá de lo permitido por las programaciones de tipo de identificación. En otras palabras, si una programación de tipo de identificación restringe el acceso de entrada o salida en un momento determinado, una programación de grupo no puede invalidar dicha programación de tipo de identificación. Sin embargo, si una programación de grupo es más restrictiva en relación con el acceso que la programación de tipo de identificación, la programación de grupo prevalece sobre la programación de tipo de identificación.

Las programaciones de tipo de identificación y las programaciones de grupo pueden combinarse de distintas maneras para lograr diferentes resultados. Para obtener ejemplos de combinaciones de programaciones de acceso, consulte *página 42*.

Añadir elementos de programación

Las programaciones de adición y las programaciones de sustracción pueden ser eventos únicos o repetidos.

Para añadir un elemento de programación a una programación de acceso:

1. Expanda la programación de acceso en la lista **Access Schedules (Programaciones de acceso)**.
2. Haga clic en **Add schedule item (Añadir elemento de programación)**.
3. Introduzca el nombre del elemento de programación.
4. Seleccione **One time (Una vez)** o **Recurrence (Repetición)**.
5. Ajuste la duración en los campos de tiempo. Consulte *Opciones de hora en la página 33*.
6. Para programar eventos periódicos, seleccione los parámetros **Recurrence pattern (Patrón de repetición)** y **Range of recurrence (Rango de repetición)**. Consulte *Opciones de patrón de repetición en la página 33* y *Opciones de rango de repetición en la página 34*.
7. Haga clic en **Save (Guardar)**.

Opciones de hora

Están disponibles las siguientes opciones de hora:

- **All day (Todo el día)**: seleccione esta opción para eventos que duran las 24 horas del día. A continuación, introduzca la fecha de **Start (Inicio)** deseada.
- **Start (Inicio)**: haga clic en el campo de hora y seleccione la hora deseada. En caso necesario, haga clic en el campo de fecha y seleccione el mes, día y año deseado. También puede escribir directamente la fecha en el campo.
- **End (Finalización)**: haga clic en el campo de hora y seleccione la hora deseada. En caso necesario, haga clic en el campo de fecha y seleccione el mes, día y año deseado. También puede escribir directamente la fecha en el campo.

Opciones de patrón de repetición

Están disponibles las siguientes opciones de patrón de repetición:

- **Yearly (Anual)**: seleccione esta opción para que se repita cada año.
- **Weekly (Semanal)**: seleccione esta opción para que se repita cada semana.
- Se repite todas las semanas el **Monday (Lunes)**, **Tuesday (Martes)**, **Wednesday (Miércoles)**, **Thursday (Jueves)**, **Friday (Viernes)**, **Saturday (Sábado)** y **Sunday (Domingo)**: seleccione los días en los que se repetirá.

Opciones de rango de repetición

Están disponibles las siguientes opciones de rango de repetición:

- **First occurrence (Primera ocurrencia)**: haga clic en el campo de fecha y seleccione el mes, día y año deseado. También puede escribir directamente la fecha en el campo.
- **No end date (Sin fecha de finalización)**: seleccione esta opción para que la recurrencia se repita indefinidamente.
- **End by (Terminar en)**: haga clic en el campo de fecha y seleccione el mes, día y año deseado. También puede escribir directamente la fecha en el campo.

Crear y editar grupos

Los grupos le permiten gestionar de forma colectiva y eficiente los usuarios y sus derechos de acceso. Un grupo se compone de credenciales que indican al sistema qué usuarios componen el grupo y cuándo y cómo se concede acceso a las puertas para los miembros del grupo.

Cada usuario debe pertenecer a uno o varios grupos. Para añadir un usuario a un grupo, arrastre y suelte al usuario en el grupo deseado en la lista **Groups (Grupos)**. Para obtener más información, consulte *Crear y editar usuarios en la página 40*.

Para crear un nuevo grupo:

1. Vaya a **Access Management (Gestión de acceso)**.
2. En la pestaña **Groups (Grupos)**, haga clic en **Add new group (Añadir nuevo grupo)**.
3. En el cuadro de diálogo **Add Group (Añadir grupo)**, introduzca las credenciales del grupo. Consulte *Credenciales de grupo en la página 34*.
4. Haga clic en **Save (Guardar)**.

Para expandir un elemento en la lista **Groups (Grupos)** y ver su miembros, derechos de acceso a puerta y programaciones, haga clic en  .

Para editar el nombre de un grupo o la fecha de validez, haga clic en  y realice los cambios. A continuación, haga clic en **Save (Guardar)**.

Para comprobar cuándo y cómo puede un grupo acceder a determinadas puertas, haga clic en  .

Para eliminar un grupo o miembros del grupo, puertas o programaciones de un grupo, haga clic en  .

Credenciales de grupo

Las siguientes credenciales están disponibles para grupos:

- **Name (Nombre)** (requerido)
- **Valid from (Válido desde)** y **Valid to (Válido hasta)**: introduzca el intervalo de fechas durante el cual las credenciales del grupo serán válidas. Haga clic en el campo de fecha y seleccione el mes, día y año deseado. También puede escribir directamente la fecha en el campo.
- **Whitelist (Lista blanca)**: los usuarios en un grupo de lista blanca pueden acceder siempre a las puertas del grupo, incluso en caso de fallo en la red o la alimentación. Dado que los usuarios del grupo siempre tienen acceso a las puertas, las programaciones o las restricciones "válido hasta" y "válido desde" no son aplicables. El tiempo de acceso excesivo no se aplica a un usuario que abre una puerta en un grupo de lista blanca. Solo se pueden añadir al grupo puertas con cerraduras inalámbricas que admiten la funcionalidad de lista blanca.

Nota

- Para guardar el grupo, debe introducir el **Name (Nombre)** del grupo.
- "Válido hasta" y "Válido desde" dejan de aplicarse a un usuario al ser incorporado a un grupo de lista blanca.
- Sincronizar las credenciales en lista blanca con una cerradura inalámbrica lleva algo de tiempo e interfiere con los procedimientos normales de apertura de puerta. Evite añadir o eliminar grandes cantidades de credenciales en un sistema durante las horas punta. Una vez realizada la sincronización de credenciales actualizadas en la cerradura, el registro de eventos mostrará el aviso `SyncOngoing: false` para la cerradura.

Gestionar puertas

Las reglas generales para cada puerta se gestionan en la pestaña **Doors (Puertas)**. Las reglas incluyen añadir tipos de identificación que determinen cómo podrán los usuarios acceder a la puerta y las programaciones de acceso que determinan cuándo es válido cada tipo de identificación. Para obtener más información, consulte *Tipos de identificación en la página 36* y *Crear y editar programaciones de acceso en la página 32*.

Para gestionar una puerta, debe añadirla al sistema de control de acceso completando la configuración de hardware; consulte *Configuración del hardware en la página 13*.

Para gestionar una puerta:

1. Vaya a **Access Management (Gestión de acceso)** y seleccione la pestaña **Doors (Puertas)**.
2. En la lista **Doors (Puertas)**, haga clic en  junto a la puerta que desea editar.
3. Arrastre la puerta al menos a un grupo. Si la lista **Groups (Grupos)** está vacía, cree un nuevo grupo. Consulte *Crear y editar grupos en la página 34*.
4. Haga clic en **Add identification type (Añadir tipo de identificación)** y seleccione las credenciales que los usuarios necesitan para obtener acceso a la puerta. Consulte *Tipos de identificación en la página 36*.

   Añada al menos un tipo de identificación para cada puerta.
5. Para añadir varios tipos de identificación, repita el paso anterior.

   Si se añaden los dos tipos de identificación **Card number only (Solo número de tarjeta)** y **PIN only (Solo PIN)**, los usuarios pueden elegir pasar su tarjeta o introducir su PIN para acceder a la puerta. Si, en lugar de ello, solo se añade el tipo de identificación **Card number and PIN (Número de tarjeta y PIN)**, los usuarios deberán pasar su tarjeta e introducir el PIN para acceder a la puerta.
6. Para definir cuándo son válidas las credenciales, arrastre una programación a cada tipo de identificación.

Para desbloquear puertas, bloquear puertas o conceder acceso temporal manualmente, haga clic en una de las acciones manuales de puerta en función de las necesidades. Consulte *Usar acciones de puerta manuales en la página 37*.

Nota

Los controles para desbloquear puertas, bloquear puertas o conceder acceso temporal manualmente no están disponibles para dispositivos/puertas inalámbricos.

Para expandir un elemento en la lista **Doors (Puertas)**, haga clic en  .

Para editar un nombre de puerta o lector, haga clic en  y realice los cambios. A continuación, haga clic en **Save (Guardar)**.

Para comprobar el lector, el tipo de identificación y las combinaciones de programaciones de acceso, haga clic  .

Para comprobar la función de las cerraduras conectadas a las puertas, haga clic en los controles de verificación. Consulte *Verificación de controles de puertas en la página 20*.

Para eliminar tipos de identificación o programaciones de acceso, haga clic en  .

Tipos de identificación

Los tipos de identificación son dispositivos portátiles de almacenamiento de credenciales, fragmentos de información memorizada o distintas combinaciones de ambos que determinan el modo en que los usuarios pueden acceder a la puerta. Entre los tipos de identificación habituales se incluyen elementos como tarjetas o mandos a distancia, números de identificación personal (PIN) y dispositivos de solicitud de salida (REX).

Para obtener más información sobre credenciales, consulte *Credenciales de usuario en la página 41*.

Están disponibles los siguientes tipos de credenciales:

- **Solo código de instalación**: el usuario puede acceder a la puerta a través de una tarjeta u otro token con el código de instalación aceptado por el lector.
- **Solo número de tarjeta**: el usuario puede acceder a la puerta usando solo una tarjeta u otro token aceptado por el lector. El número de tarjeta es un número único que normalmente está impreso en la tarjeta. Consulte la información del fabricante de la tarjeta para identificar la ubicación del número de tarjeta. También se puede recuperar el número de tarjeta a través del sistema. Pase la tarjeta por un lector conectado, seleccione el lector en la lista y haga clic en **Retrieve (Recuperar)**.
- **Solo tarjeta sin formato**: el usuario puede acceder a la puerta usando solo una tarjeta u otro token aceptado por el lector. La información se almacena en la tarjeta en forma de datos en bruto. El sistema puede recuperar los datos sin formato de la tarjeta. Pase la tarjeta por un lector conectado, seleccione el lector en la lista y haga clic en **Retrieve (Recuperar)**. Utilice este tipo de identificación si no se puede localizar el número de tarjeta.
- **Solo PIN**: el usuario puede acceder a la puerta a través de un número de identificación personal de cuatro dígitos (PIN).
- **Código de instalación y PIN**: el usuario necesita la tarjeta u otro token con el código de instalación aceptado el lector y un PIN a fin de acceder a la puerta. El usuario debe presentar las credenciales en el orden especificado (tarjeta en primer lugar y a continuación el PIN).
- **Número de tarjeta y PIN**: el usuario necesita la tarjeta u otro token aceptado por el lector y un PIN a fin de acceder a la puerta. El usuario debe presentar las credenciales en el orden especificado (tarjeta en primer lugar y a continuación el PIN).
- **Tarjeta sin formato y PIN**: el usuario necesita la tarjeta u otro token aceptado por el lector y un PIN a fin de acceder a la puerta. Utilice este tipo de identificación si no se puede localizar el número de tarjeta. El usuario debe presentar las credenciales en el orden especificado (tarjeta en primer lugar y a continuación el PIN).
- **REX**: el usuario puede acceder a la puerta mediante la activación de un dispositivo de solicitud de salida (REX), como un botón, un sensor o una barra de empuje.
- **Solo matrícula**: el usuario solo puede acceder a la puerta mediante el número de matrícula de un vehículo.

Añadir estados de desbloqueo programados

Para mantener una puerta automáticamente desbloqueada durante un tiempo específico, puede añadir un estado de **Scheduled unlock (Desbloqueo programado)** para la puerta y aplicar una programación de acceso a la misma.

Por ejemplo, para mantener una puerta desbloqueada durante el horario de oficina:

1. Vaya a **Access Management (Gestión de acceso)** y seleccione la pestaña **Doors (Puertas)**.
2. Haga clic en  junto al elemento de la lista **Doors (Puertas)** que desea editar.
3. Haga clic en **Add scheduled unlock (Añadir desbloqueo programado)**.
4. Seleccione el **Unlock state (Estado de desbloqueo)** (**desbloqueado** o **desbloquear las dos cerraduras** en función de si la puerta tiene una o dos cerraduras).
5. Haga clic en **OK (Aceptar)**.
6. Aplique la programación de acceso predefinida **Office hours (Horario de oficina)** al estado **Scheduled unlock (Desbloqueo programado)**.

Para comprobar si se desbloquea la puerta, haga clic en .

Para eliminar un estado de desbloqueo programado o una programación de acceso, haga clic en .

Usar acciones de puerta manuales

Las puertas se pueden bloquear o desbloquear y se puede otorgar acceso temporal en la pestaña **Doors (Puertas)**, mediante la característica **Manual door actions (Acciones de puerta manuales)**. Las acciones de puerta manuales disponibles para una puerta específica dependen de cómo ha sido configurada la puerta.

Para utilizar las acciones de puerta manuales:

1. Vaya a **Access Management (Gestión de acceso)** y seleccione la pestaña **Doors (Puertas)**.
2. En la lista **Doors (Puertas)**, haga clic en junto a la puerta que desea controlar.
3. Haga clic en la acción de puerta que se requiera. Consulte *Acciones de puerta manuales en la página 37*.

Nota

Para utilizar las acciones de puerta manuales, se debe abrir la página de gestión de acceso mediante el controlador de puerta al que está conectada la puerta en cuestión. Si se abre la página de gestión de acceso a través de un controlador de puerta diferente, en lugar de las acciones de puerta manuales se mostrará un enlace a la página de vista general del controlador de puerta al que está conectada la puerta en cuestión. Haga clic en el enlace, vaya a **Access Management (Gestión de acceso)** y seleccione la pestaña **Doors (Puertas)**.

Acciones de puerta manuales

Las siguientes acciones de puerta manuales están disponibles:

- **Get door status (Obtener estado de puerta)**: verifica el estado actual del monitor de puerta, alarmas de puerta y cerraduras.
- **Access (Acceso)**: proporciona al usuario acceso a la puerta. Se aplica el tiempo de acceso determinado. Consulte *Cómo configurar monitores y cerraduras de puerta en la página 14*.
- **Unlock** (Desbloquear, para una cerradura) o **Unlock both locks** (Desbloquear las dos cerraduras, para dos cerraduras): desbloquea la puerta. La puerta permanecerá desbloqueada hasta que pulse **Lock (Bloquear)** o **Lock both locks (Bloquear las dos cerraduras)**, se active un estado de puerta programado o se reinicie el controlador de puerta.
- **Lock** (Bloquear, para una cerradura) o **Lock both locks** (Bloquear las dos cerraduras, para dos cerraduras): bloquea la puerta.
- **Unlock second lock and lock primary (Desbloquear cerradura secundaria y principal)**: Esta opción solo está disponible si se ha configurado la puerta con una cerradura secundaria. Desbloquear la puerta. La cerradura secundaria permanecerá desbloqueada hasta que pulse **Double lock (Cerradura doble)** o se active un estado de puerta programado.

Gestionar plantas

Si se ha instalado un módulos de relé y E/S de red AXIS 9188 en su sistema, las plantas se pueden administrar de forma similar a la administración de puertas.

Nota

Si se utiliza un A1001 en modo clúster con eventos globales activados, asegúrese de utilizar nombres descriptivos exclusivos para cada planta. Por ejemplo, *"Ascensor A, planta 1"*.

Nota

Se puede configurar un máximo de 2 módulos de relé y E/S de red AXIS 9188 con cada controlador de accesos en red A1001.

Las reglas generales para cada planta se gestionan en la pestaña **Floors (Plantas)**. Las reglas incluyen añadir tipos de identificación que determinen cómo podrán los usuarios acceder a la planta y las programaciones de acceso que determinan cuándo es válido

cada tipo de identificación. Para obtener más información, consulte *Tipos de identificación de planta en la página 38* y *Crear y editar programaciones de acceso en la página 32*.

Para gestionar una planta, debe añadirla al sistema de control de acceso completando la configuración de hardware; consulte *Configuración del hardware en la página 13*.

Para gestionar una planta:

1. Vaya a **Access Management (Gestión de acceso)** y seleccione la pestaña **Floors (Plantas)**.
2. En la lista **Floors (Plantas)**, haga clic en junto a la planta que desea editar.
3. Arrastre la planta al menos a un grupo. Si la lista **Groups (Grupos)** está vacía, cree un nuevo grupo. Consulte *Crear y editar grupos en la página 34*.
4. Haga clic en **Add identification type (Añadir tipo de identificación)** y seleccione las credenciales que los usuarios necesitan para obtener acceso a la planta. Consulte *Tipos de identificación de planta en la página 38*.

   Añada al menos un tipo de identificación para cada planta.
5. Para añadir varios tipos de identificación, repita el paso anterior.

   Si se añaden los dos tipos de identificación **Card number only (Solo número de tarjeta)** y **PIN only (Solo PIN)**, los usuarios pueden elegir pasar su tarjeta o introducir su PIN para acceder a la puerta. Si, en lugar de ello, solo se añade el tipo de identificación **Card number and PIN (Número de tarjeta y PIN)**, los usuarios deberán pasar su tarjeta e introducir el PIN para acceder a la puerta.
6. Para definir cuándo son válidas las credenciales, arrastre una programación a cada tipo de identificación.

Para desbloquear plantas, bloquear plantas o conceder acceso temporal manualmente, haga clic en una de las acciones manuales de puerta en función de las necesidades. Consulte *Utilizar acciones manuales de planta en la página 39*.

Nota

Los controles para desbloquear plantas, bloquear plantas o conceder acceso temporal manualmente no están disponibles para dispositivos/puertas inalámbricos.

Para expandir un elemento en la lista **Floors (Plantas)**, haga clic en .

Para editar un nombre de planta o lector, haga clic en y realice los cambios. A continuación, haga clic en **Save (Guardar)**.

Para comprobar el lector, el tipo de identificación y las combinaciones de programaciones de acceso, haga clic .

Para comprobar la función de las cerraduras conectadas a las plantas, haga clic en los controles de verificación. Consulte *Verificación de controles de plantas en la página 21*.

Para eliminar tipos de identificación o programaciones de acceso, haga clic en .

Tipos de identificación de planta

Los tipos de identificación son dispositivos portátiles de almacenamiento de credenciales, fragmentos de información memorizada o distintas combinaciones de ambos que determinan el modo en que los usuarios pueden acceder a la planta. Entre los tipos de identificación habituales se incluyen elementos como tarjetas o mandos a distancia, números de identificación personal (PIN) y dispositivos de solicitud de salida (REX).

Para obtener más información sobre credenciales, consulte *Credenciales de usuario en la página 41*.

Están disponibles los siguientes tipos de credenciales:

- **Solo código de instalación**: el usuario puede acceder a la planta a través de una tarjeta u otro token con el código de instalación aceptado por el lector.

- **Solo número de tarjeta**: el usuario puede acceder a la planta usando solo una tarjeta u otro token aceptado por el lector. El número de tarjeta es un número único que normalmente está impreso en la tarjeta. Consulte la información del fabricante de la tarjeta para identificar la ubicación del número de tarjeta. También se puede recuperar el número de tarjeta a través del sistema. Pase la tarjeta por un lector conectado, seleccione el lector en la lista y haga clic en **Retrieve (Recuperar)**.
- **Solo tarjeta sin formato**: el usuario puede acceder a la planta usando solo una tarjeta u otro token aceptado por el lector. La información se almacena en la tarjeta en forma de datos en bruto. El sistema puede recuperar los datos sin formato de la tarjeta. Pase la tarjeta por un lector conectado, seleccione el lector en la lista y haga clic en **Retrieve (Recuperar)**. Utilice este tipo de identificación si no se puede localizar el número de tarjeta.
- **Solo PIN**: el usuario puede acceder a la planta a través de un número de identificación personal de cuatro dígitos (PIN).
- **Código de instalación y PIN**: el usuario necesita la tarjeta u otro token con el código de instalación aceptado el lector y un PIN a fin de acceder a la planta. El usuario debe presentar las credenciales en el orden especificado (tarjeta en primer lugar y a continuación el PIN).
- **Número de tarjeta y PIN**: el usuario necesita la tarjeta u otro token aceptado por el lector y un PIN a fin de acceder a la planta. El usuario debe presentar las credenciales en el orden especificado (tarjeta en primer lugar y a continuación el PIN).
- **Tarjeta sin formato y PIN**: el usuario necesita la tarjeta u otro token aceptado por el lector y un PIN a fin de acceder a la planta. Utilice este tipo de identificación si no se puede localizar el número de tarjeta. El usuario debe presentar las credenciales en el orden especificado (tarjeta en primer lugar y a continuación el PIN).
- **REX**: el usuario puede acceder a la planta mediante la activación de un dispositivo de solicitud de salida (REX), como un botón, un sensor o una barra de empuje.

Añadir estados de desbloqueo programados

Para mantener automáticamente accesible una planta para todo el mundo durante un tiempo específico, se puede añadir un estado de **Scheduled unlock (Desbloqueo programado)** en una planta y aplicarle una programación de acceso.

Por ejemplo, para mantener una planta accesible para toda persona durante las horas de oficina:

1. Vaya a **Access Management (Gestión de acceso)** y seleccione la pestaña **Floors (Plantas)**.
2. Haga clic en  junto al elemento de la lista **Floors (Plantas)** que desea editar.
3. Haga clic en **Add scheduled unlock (Añadir desbloqueo programado)**.
4. Seleccione el **Unlock state (Estado de desbloqueo)** (**desbloqueado** o **desbloquear las dos cerraduras** en función de si la planta tiene una o dos cerraduras).
5. Haga clic en **OK (Aceptar)**.
6. Aplique la programación de acceso predefinida **Office hours (Horario de oficina)** al estado **Scheduled unlock (Desbloqueo programado)**.

Para comprobar cuándo es accesible la planta, haga clic en  .

Para eliminar un estado de desbloqueo programado o una programación de acceso, haga clic en  .

Utilizar acciones manuales de planta

Las plantas pueden tener diferentes tipos de acceso, restringidos o accesibles para todo el mundo. Se puede conceder acceso temporal en la pestaña **Floors (Plantas)** mediante **Manual floor actions (Acciones manuales de planta)**. Las acciones de planta manuales disponibles para una planta específica dependen de cómo ha sido configurada la planta.

Para utilizar las acciones de planta manuales:

1. Vaya a **Access Management (Gestión de acceso)** y seleccione la pestaña **Floors (Plantas)**.
2. En la lista **Floors (Plantas)**, haga clic en  junto a la planta que desea controlar.

3. Haga clic en la acción de planta que se requiera. Consulte *Acciones de planta manuales en la página 40*.

Nota

Para utilizar las acciones de planta manuales, se debe abrir la página de gestión de acceso mediante el controlador de planta al que está conectada la puerta en cuestión. Si se abre la página de gestión de acceso a través de un controlador de planta diferente, en lugar de las acciones de planta manuales se mostrará un enlace a la página de vista general del controlador de planta al que está conectada la planta en cuestión. Haga clic en el enlace, vaya a **Access Management (Gestión de acceso)** y seleccione la pestaña **Floors (Plantas)**.

Acciones de planta manuales

Las siguientes acciones de planta manuales están disponibles:

- **Get floor status (Obtener estado de planta)**: comprueba el estado actual del relé conectado a una planta.
- **Acess (Acceso)**: proporciona al usuario acceso a la planta. Se aplica el tiempo de acceso determinado. Consulte *Cómo configurar monitores y cerraduras de puerta en la página 14*.
- **Unlock (Desbloquear)**: la planta está totalmente accesible para todo el mundo hasta que se pulse **Lock (Bloquear)**, se active un estado de planta programado o se reinicie el controlador de puerta.
- **Lock (Bloquear)**: la planta está totalmente inaccesible para todo el mundo hasta que se pulse **Unlock (Desbloquear)**, se active un estado de planta programado o se reinicie el controlador de puerta.

Crear y editar usuarios

Cada persona debe tener un perfil de usuario único para tener acceso a las puertas en el sistema de control de acceso. El perfil de usuario se compone de credenciales que indican al sistema la identidad del usuario y cuándo y cómo se le concede acceso a las puertas.

Para poder gestionar de forma eficaz los derechos de acceso de usuario, cada usuario debe pertenecer a uno o a varios grupos. Para obtener más información, consulte *Crear y editar grupos*.

Para crear un nuevo perfil de usuario:

1. Vaya a **Access Management (Gestión de acceso)**.
2. Seleccione la pestaña **Users (Usuarios)** y haga clic en **Add new user (Añadir nuevo usuario)**.
3. En el cuadro de diálogo **Add User (Añadir usuario)**, introduzca las credenciales del usuario. Consulte *Credenciales de usuario en la página 41*.
4. Haga clic en **Save (Guardar)**.
5. Arrastre el usuario a uno o varios grupos en la lista **Groups (Grupos)**. Si la lista **Groups (Grupos)** está vacía, cree un nuevo grupo. Consulte *Crear y editar grupos en la página 34*.

Para expandir un elemento en la lista **Users (Usuarios)** y ver las credenciales del usuario, haga clic en  .

Para buscar un usuario específico, introduzca un filtro en el campo de filtro de usuarios. Para obligar a obtener resultados exactos, entrecomille el texto del filtro, por ejemplo, "Juan" o "garcía, virginia".

Para editar las credenciales del usuario, haga clic en  y cambie las credenciales de acuerdo con las necesidades. A continuación, haga clic en **Save (Guardar)**.

Para eliminar un usuario, haga clic en  .

Importante

Si se ha creado un usuario a través de AXIS Visitor Manager, no lo modifique ni lo elimine en AXIS Entry Manager. Para obtener más información sobre AXIS Visitor Manager y el servicio de lector de código QR, consulte *AXIS Visitor Access en la página 23*.

Gestión de acceso

Credenciales de usuario

Las siguientes credenciales están disponibles para los usuarios:

- **First name (Nombre)** (obligatorio)
- **Last name (Apellidos)**
- **Valid from (Válido desde)** y **Valid until (Válido hasta)**: introduzca el intervalo de fechas durante el cual las credenciales del usuario serán válidas. Haga clic en el campo de fecha y seleccione el mes, día y año deseado. También puede escribir directamente la fecha en el campo.
- **Suspend credential (Suspender credenciales)**: seleccione esta opción para suspender las credenciales. Mientras están suspendidas, el usuario no tiene acceso a las puertas en el sistema mediante las credenciales. Anule la selección para volver a permitir el acceso al usuario. La suspensión está diseñada para ser temporal. Si se debe denegar permanentemente el acceso al usuario, es preferible eliminar el perfil de usuario.
- **PIN** (obligatorio si no se emplea número de tarjeta o tarjeta sin formato): introduzca el número de identificación personal de cuatro dígitos (PIN) seleccionado por el usuario o asignado al mismo.
- **Facility code (Código de instalación)**: introduzca un código para verificar el sistema de control de acceso a instalaciones. Si se introduce un código de instalación predefinido, este campo se completa automáticamente; consulte *Código de instalación predefinido en la página 23*
- **Card number (Número de tarjeta)** (obligatorio si no se emplea PIN o tarjeta sin formato): Introduzca el número de tarjeta. Consulte la información del fabricante de la tarjeta para identificar la ubicación del número de tarjeta. También se puede recuperar el número de tarjeta a través del sistema. Pase la tarjeta por un lector conectado, seleccione el lector en la lista y haga clic en **Retrieve (Recuperar)**.
- **Card raw (Tarjeta sin formato)** (obligatorio si no se emplea PIN o número de tarjeta): Introduzca los datos de la tarjeta sin formato. El sistema puede recuperar los datos. Pase la tarjeta por un lector conectado, seleccione el lector en la lista y haga clic en **Retrieve (Recuperar)**. Utilice este tipo de identificación si no se puede localizar el número de tarjeta.
- **Long access time (Tiempo de acceso prolongado)**: seleccione esta opción para sustituir el tiempo de acceso existente y permitir que la puerta se abra durante el tiempo de acceso prolongado. Consulte *Acerca de las opciones de monitor de puerta y hora en la página 15*
- **License plate (Matrícula)** (esta credencial no está disponible en la instalación de un controlador de puerta de manera predeterminada): si esta credencial ha sido activada mediante software de terceros, introduzca el número de matrícula del vehículo del usuario.
  Esta credencial solo se puede utilizar junto con software de socios de Axis y una cámara con software de reconocimiento de matrículas. Para obtener más información, póngase en contacto con su socio de Axis o con su representante de ventas de Axis.

Nota

El botón **Retrieve (Recuperar)** solo está disponible si se ha completado la configuración de hardware y uno o varios lectores están conectados al controlador.

Importar usuarios

Se pueden añadir usuarios al sistema mediante la importación de un archivo de texto en formato de valores separados por comas (CSV). Se recomienda importar usuarios cuando se necesite añadir numerosos usuarios al mismo tiempo.

Para poder importar los usuarios, debe crear y guardar un archivo (*.csv o *.txt) en el formato CSV correcto. Separe los valores mediante comas y sin espacios; separe cada usuario con un salto de línea.

Ejemplo

```
juana,gómez,1234,12345678,abc123
juan,gómez,5435,87654321,cde321
```

Para importar usuarios:

1. Vaya a **Setup > Import Users (Configuración > Importar usuarios)**.

2. Localice y seleccione el archivo *.csv o *.txt que contiene la lista de usuarios.
3. Seleccione la opción correcta de credenciales correctas para cada columna.
4. Para importar los usuarios al sistema, haga clic en **Import users (Importar usuarios)**.
5. Compruebe que cada columna contiene el tipo de credencial correcto.
6. Si las columnas son correctas, haga clic en **Start importing users (Iniciar la importación de usuarios)**. Si las columnas son incorrectas, haga clic en **Cancel (Cancelar)** y empiece de nuevo.
7. Una vez completada la importación, haga clic en **OK (Aceptar)**.

Están disponibles las opciones de credenciales siguientes:

- **First name (Nombre)**
- **Last name (Apellidos)**
- **PIN code (Código PIN)**
- **Card number (Número de tarjeta)**
- **License plate (Matrícula)**
- **Unassigned (No asignados)**: valores que no se importarán. Seleccione esta opción para omitir una columna en concreto.

Para obtener más información sobre credenciales, consulte *Crear y editar usuarios*.

Exportar usuarios

La página de exportación muestra una lista de valores separados por comas (CSV) de todos los usuarios del sistema. La lista se puede utilizar para importar los usuarios a otro sistema.

Para exportar la lista de usuarios:

1. Abra un editor de texto sin formato y cree un nuevo documento.
2. Vaya a **Setup > Export Users (Configuración > Exportar usuarios)**
3. Copie y seleccione todos los valores de la página.
4. Pegue los valores en el documento de texto.
5. Guarde el documento como archivo de valores separados por comas (*.csv) o como archivo de texto (*.txt).

Ejemplo de combinaciones de programación de acceso

Las programaciones de tipo de identificación y las programaciones de grupo pueden combinarse de distintas maneras para lograr diferentes resultados. Los siguientes ejemplos siguen el flujo de trabajo que se describe en *página 31*.

Ejemplo

Para crear una combinación de programaciones que

- permita el acceso a una puerta a los vigilantes en todo momento,
  - con su tarjeta durante el horario del turno de día (lunes-viernes, de 06:00 h a 16:00 h) y
  - utilizando su tarjeta y PIN antes y después del horario del turno de día, y que
- permita acceso a la misma puerta al personal del turno de día,
  - con su tarjeta solo durante el horario del turno de día:

1. Cree una **Addition schedule (Programación de adición)** denominada **Horario de turno de día**. Consulte *página 32*.
2. Cree un **Schedule item (Elemento de programación)** horario de turno de día que se repita de lunes a viernes, de 06:00 a 16:00 h.
3. Cree dos grupos, un **Group (Grupo)** denominado **Vigilantes** y otro **Group (Grupo)** denominado **Personal de turno de día**. Consulte *página 34*.
4. Arrastre la programación de acceso predefinida **Always (Siempre)** al grupo **Vigilantes**.
5. Arrastre la programación de acceso **Horario de turno de día** al grupo **Personal de turno de día**.
6. Añada los tipos de identificación **Card number and PIN (Número de tarjeta y PIN)** y **Card number only (Solo número de tarjeta)** al lector de la puerta.
7. Arrastre la programación de acceso predefinida **Always (Siempre)** al tipo de identificación **Card number and PIN (Número de tarjeta y PIN)**.
8. Arrastre la programación de acceso **Horario de turno de día** al tipo de identificación **Card number only (Solo número de tarjeta)**.
9. Arrastre la puerta a los dos grupos. A continuación, añada los usuarios correspondientes a los grupos. Consulte *página 40*.

Ejemplo

Para crear una combinación de programaciones que

- permita el acceso a una puerta a los vigilantes en todo momento,
  - con su tarjeta durante el horario del turno de día (lunes-viernes, de 06:00 h a 16:00 h) y
  - con su tarjeta y PIN antes y después del horario del turno de día, y que
- permita el acceso a la misma puerta al personal del turno de día entre las 06:00 h y las 16:00 h.,
  - con su tarjeta durante el horario de turno de día y
  - con su tarjeta y PIN durante las noches y fines de semana:

1. Cree una **Addition schedule (Programación de adición)** denominada **Horario de turno de día**. Consulte *página 32*.
2. Cree un **Schedule item (Elemento de programación)** horario de turno de día que se repita de lunes a viernes, de 06:00 a 16:00 h.
3. Cree una **Subtraction schedule (Programación de sustracción)** denominada **Noches y fines de semana**.
4. Cree un **Schedule item (Elemento de programación)** para noches y fines de semana que se repita de domingo a sábado, de 16:00 a 06:00 h.
5. Arrastre la programación predefinida **Always (Siempre)** y la programación de acceso **Noches y fines de semana** al **Personal de turno de día**.
6. Cree dos grupos, un **Group (Grupo)** denominado **Vigilantes** y otro **Group (Grupo)** denominado **Personal de turno de día**. Consulte *página 34*.
7. Arrastre la programación de acceso predefinida **Always (Siempre)** al grupo **Vigilantes** y al grupo **Personal de turno de día**.
8. Arrastre la programación de acceso **Noches y fines de semana** al grupo **Personal de turno de día**.
9. Añada los tipos de identificación **Card number and PIN (Número de tarjeta y PIN)** y **Card number only (Solo número de tarjeta)** al lector de la puerta.
10. Arrastre la programación de acceso predefinida **Always (Siempre)** al tipo de identificación **Card number and PIN (Número de tarjeta y PIN)**.

11. Arrastre la programación de acceso **Horario de turno de día** al tipo de identificación **Card number only (Solo número de tarjeta)**.
12. Arrastre la puerta a los dos grupos. A continuación, añada los usuarios correspondientes a los grupos. Consulte *página 40*.

Configuración de eventos y alarmas

Los eventos que se producen en el sistema, por ejemplo cuando un usuario pasa una tarjeta o se activa un dispositivo REX, se registran en el registro de eventos. Los eventos registrados se pueden configurar para activar alarmas, las cuales se registran a su vez en el registro de alarmas.

- Ver el registro de eventos. Consulte *página 45*.
- Exportar el registro de eventos. Consulte *página 45*.
- Ver el registro de alarmas. Consulte *página 46*.
- Configurar los registros de eventos y de alarmas. Consulte *página 46*.

También se pueden configurar las alarmas para que activen acciones como el envío de notificaciones por correo electrónico. Para obtener más información, consulte *Cómo configurar reglas de acción en la página 47*.

Ver el registro de eventos

Para ver los eventos registrados, vaya a **Event Log (Registro de eventos)**.

Si los eventos globales están activados, puede abrir el registro de eventos desde cualquier controlador de puerta en el sistema. Para obtener más información sobre los eventos globales, consulte *Configurar los registros de eventos y de alarmas en la página 46*.

Para expandir un elemento en el registro de eventos y ver los detalles del evento, haga clic en  .

Aplicar filtros al registro de eventos facilita encontrar eventos específicos. Para filtrar la lista, seleccione uno o varios filtros del registro de eventos y haga clic en **Apply filters (Aplicar filtros)**. Para obtener más información, consulte *Filtros de registro de eventos en la página 45*.

Como administrador, puede tener más interés en determinados eventos que en otros. De este modo, puede elegir los eventos que se deben registrar y para qué controladores. Para obtener más información, consulte *Opciones del registro de eventos en la página 46*.

Filtros de registro de eventos

Puede restringir el alcance del registro de eventos seleccionando uno o varios de los siguientes filtros:

- Usuario: filtrar por eventos relacionados con un usuario seleccionado.
- Puerta y planta: filtrar por eventos relacionados con una puerta o planta específicas.
- Asunto: filtrar por tipo de evento.
- Fuente: filtrar por eventos de un controlador seleccionado. Disponible solo en un clúster de controlador y cuando se activan los eventos globales.
- Fecha y hora: filtrar el registro de eventos por una fecha e intervalo horario.

Exportar el registro de eventos

Para exportar los eventos registrados, vaya a **Event Log (Registro de eventos)**:

1. Haga clic en  .
2. Seleccione el formato de exportación en el menú emergente para iniciar la exportación.

Nota

El formato CSV es compatible con todos los navegadores, el formato XLSX es compatible con Chrome™ e Internet Explorer®.

Nota

Tras una exportación completada, el botón de exportación cambia de  a  . Para iniciar otra exportación, actualice la página web. El botón de exportación cambiará a  .

Ver el registro de alarmas

Para ver las alarmas activadas, vaya a **Alarm Log (Registro de alarmas)**. Si los eventos globales están activados, puede abrir el registro de alarmas desde cualquier controlador de puerta en el sistema. Para obtener más información sobre los eventos globales, consulte *Configurar los registros de eventos y de alarmas en la página 46*.

Para expandir un elemento del registro de alarmas y ver los detalles de la alarma, como identidad de puerta y estado, haga clic en  .

Para eliminar una alarma de la lista después de comprobar la causa de la alarma, haga clic en **Acknowledge (Aceptar)**. Para eliminar todas las alarmas, haga clic en **Acknowledge all alarms (Aceptar todas las alarmas)**.

Como administrador, puede necesitar que algunos eventos activen alarmas. De este modo, puede elegir los eventos que activarán alarmas y para qué controladores lo harán. Para obtener más información, consulte *Opciones del registro de alarmas en la página 47*.

Configurar los registros de eventos y de alarmas

La página de configuración de registros de eventos y de alarmas permite definir qué eventos se deben registrar y activan alarmas.

Para compartir eventos y alarmas entre todos los controladores conectados, seleccione **Global events (Eventos globales)**. Si eventos globales está activado, basta con abrir una página del registro de eventos y una página del registro de alarmas para administrar al mismo tiempo los eventos y alarmas de todos los controladores de puerta en el sistema. Eventos globales está activado de forma predeterminada.

Si desactiva los eventos globales, tendrá que abrir una página del registro de eventos y una página del registro de alarmas para cada uno de los controladores de puerta y gestionar los eventos y alarmas por separado.

Importante

El registro de eventos se vacía cada vez que se activan o desactivan los eventos globales. Esto significa que se eliminan todos los eventos anteriores a ese momento y que el registro de eventos se vuelve a iniciar.

También se pueden configurar las alarmas para que activen acciones como el envío de notificaciones por correo electrónico. Para obtener más información, consulte *Cómo configurar reglas de acción en la página 47*.

Opciones del registro de eventos

Para definir los eventos que se incluirán en el registro de eventos, vaya a **Setup > Configure Event and Alarm Logs (Configuración > Configurar registros de eventos y alarmas)**.

Las siguientes opciones para el registro de eventos están disponibles:

- **No logging (Ningún registro)**: deshabilita el registro de eventos. El evento no se registrará ni se incluirá en el registro de eventos.
- **Log for all sources (Registro para todas las fuentes)**: habilita el registro de eventos en todos los controladores de puerta. El evento se registrará para todos los controladores y se incluirá en el registro de eventos.
- **Log for selected sources (Registro para las fuentes seleccionadas)**: habilita el registro de eventos en los controladores de puerta seleccionados. El evento se registrará para todos los controladores seleccionados y se incluirá en el registro de eventos. Seleccione esta opción para eventos que se combinarán con la opción del registro de alarmas **No alarms (Ninguna alarma)** o **Log alarm for selected controllers (Registro de alarmas para los controladores seleccionados)**.

  En la lista **Configure event logging (Configurar registro de eventos)**, haga clic en **Select controllers (Seleccionar controladores)** en el elemento de archivo de eventos que se desea habilitar. Se abrirá el cuadro de diálogo **Device Specific**

Event Logging (Registro de eventos específicos del dispositivo). En **Log event (Registrar evento)**, seleccione los controladores que tendrán habilitado el registro de alarmas y haga clic en **Save (Guardar)**.

Opciones del registro de alarmas

Para definir qué eventos deben activar una alarma, vaya a **Setup > Configure Event and Alarm Logs (Configuración > Configurar registros de eventos y alarmas)**.

Están disponibles las siguientes opciones de activación y registro de alarmas:

- **No alarms (Ninguna alarma)**: desactiva el registro de alarmas. El evento no activará ninguna alarma o no se incluirá en el registro de alarmas.
- **Log alarm for all sources (Registrar alarmas para todas las fuentes)**: activa el registro de alarmas en todos los controladores de puerta. El evento activará una alarma y se incluirá en el registro de alarmas.
- **Log alarm for selected sources (Registrar alarma para las fuentes seleccionadas)**: activa el registro de alarma en los controladores de puerta seleccionados. El evento activará una alarma y se incluirá en el registro de alarmas.

  En la lista **Configure alarm logging (Configurar registro de alarmas)**, haga clic en **Select sources (Seleccionar fuentes)** en el elemento del registro de alarmas que se desea activar. Se abrirá el cuadro de diálogo **Device Specific Alarm Triggering (Activación de alarma específica del dispositivo)**. En **Trigger alarm (Activar alarma)**, seleccione los controladores de puerta que tendrán habilitado el registro de alarmas y haga clic en **Save (Guardar)**.

Cómo configurar reglas de acción

Las páginas de eventos permiten configurar el producto de Axis para realizar acciones al producirse distintos eventos. Por ejemplo, el producto puede enviar una notificación por correo electrónico o activar un puerto de salida cuando se activa una alarma. El conjunto de condiciones que define cómo y cuándo se activa la acción se denomina regla de acción. Si se definen varias condiciones, todas ellas deberán cumplirse para que se active la acción.

Para obtener más información acerca de los activadores y acciones disponibles, consulte *Activadores en la página 48* y *Acciones en la página 50*.

En este ejemplo se describe cómo configurar una regla de acción para enviar una notificación por correo electrónico cuando se activa una alarma.

1. Configure las alarmas. Consulte *Configurar los registros de eventos y de alarmas en la página 46*.
2. Vaya a **Setup > Additional Controller Configuration > Events > Action Rules (Configuración > Configuración de controlador adicional > Eventos > Reglas de acción)** y haga clic en **Añadir**.
3. Seleccione **Habilitar regla** e introduzca un nombre descriptivo para la regla.
4. Seleccione **Registro de eventos** en la lista desplegable **Activador**.
5. Si lo desea, seleccione una **Programación** y **Condiciones adicionales**. Consulte a continuación.
6. En **Acciones**, seleccione **Enviar notificación** en la lista desplegable **Tipo**.
7. Seleccione un destinatario de correo electrónico en la lista desplegable. Consulte *Cómo añadir destinatarios en la página 51*.

En este ejemplo se describe cómo configurar una regla de acción para activar un puerto de salida cuando la puerta ha sido forzada.

1. Vaya a **Setup > Additional Controller Configuration > System Options > Ports & Devices > I/O Ports (Configuración > Configuración de controlador adicional > Opciones del sistema > Puertos y dispositivos > Puertos de E/S)**.
2. Seleccione **Salida** en el elemento deseado de la lista desplegable **Tipo de puerto de E/S** e introduzca un **Nombre**.
3. Seleccione el **Estado Normal** del puerto de salida E/S y haga clic en **Guardar**.
4. Vaya a **Events > Action Rules (Eventos > Reglas de acción)** y haga clic en **Añadir**.

5. Seleccione **Puerta** en la lista desplegable **Activador**.
6. Seleccione **Alarma de puerta** en la lista desplegable.
7. Seleccione la puerta deseada en la lista desplegable.
8. Seleccione **Puerta forzada** en la lista desplegable.
9. Si lo desea, seleccione una **Programación** y **Condiciones adicionales**. Consulte a continuación.
10. En **Acciones**, seleccione **Puerto de salida** en la lista desplegable **Tipo**.
11. Seleccione el puerto de salida deseado en la lista desplegable **Puerto**.
12. Establezca el estado en **Activo**.
13. Seleccione **Duración** e **Ir después al estado opuesto**. A continuación, introduzca la duración deseada de la acción.
14. Haga clic en **OK (Aceptar)**.

Para utilizar más de un activador para la regla de acción, seleccione **Condiciones adicionales** y haga clic en **Añadir** para añadir desencadenadores adicionales. Al utilizar condiciones adicionales, todas las condiciones deben cumplirse para que se active la acción.

Para evitar que una acción se active repetidamente, se puede establecer un tiempo mínimo de espera en **Esperar al menos**. Introduzca el tiempo en horas, minutos y segundos, durante el cual debe ignorarse el activador antes de que la regla de acción se pueda activar de nuevo.

Para obtener más información, consulte la ayuda integrada del producto.

Activadores

Entre los **activadores** y **condiciones** de regla de acción disponibles se incluyen:

- **Access Point (Punto de acceso)**
  - **Access Point Enabled (Punto de acceso activado)**: activa una regla de acción cuando se configura un dispositivo de punto de acceso como un lector o un dispositivo REX; por ejemplo, si se completa la configuración del hardware o se añade un tipo de identificación.
- **Configuration (Configuración)**
  - **Access Point Changed (Punto de acceso cambiado)**: activa una regla de acción cuando se cambia la configuración de un dispositivo de punto de acceso como un lector o un dispositivo REX; por ejemplo, si se configura el hardware o se modifica un tipo de identificación para cambiar la manera de poder acceder a una puerta.
  - **Access Point Removed (Punto de acceso eliminado)**: activa una regla de acción cuando se restablece la configuración del hardware de un dispositivo de punto de acceso, como un lector o un dispositivo REX.
  - **Area Changed (Área cambiada)**: no compatible con esta versión de AXIS Entry Manager. Debe configurarse mediante un cliente, como un sistema de gestión de acceso, a través de la interfaz de programación de aplicaciones VAPIX®, que es compatible con esta función y utiliza dispositivos que pueden proporcionar las señales necesarias. Activa la regla de acción cuando se cambia un área de acceso.
  - **Area Removed (Área eliminada)**: no compatible con esta versión de AXIS Entry Manager. Debe configurarse mediante un cliente, como un sistema de gestión de acceso, a través de la interfaz de programación de aplicaciones VAPIX®, que es compatible con esta función y utiliza dispositivos que pueden proporcionar las señales necesarias. Activa la regla de acción cuando se elimina un área de acceso del sistema.
  - **Door Changed (Puerta cambiada)**: activa una regla de acción cuando se cambia la configuración de la puerta, por ejemplo su nombre, o si se añade una puerta al sistema. Esto se puede usar, por ejemplo, para enviar una notificación cuando se instala y configura una puerta.

  - **Door Removed (Puerta eliminada)**: activa una regla de acción cuando se elimina una puerta del sistema. Esto, por ejemplo, se puede usar para enviar una notificación cuando se elimina una puerta del sistema.

- **Door (Puerta)**
  - **Battery Alarm (Alarma de batería)**: activa una regla de acción cuando es la batería de una puerta inalámbrica se está agotando o se ha agotado.
  - **Door Alarm (Alarma de puerta)**: activa una regla de acción cuando el monitor de puerta indica que la puerta se ha forzado para abrirse, ha permanecido abierta durante demasiado tiempo o falla de alguna manera. Esto se puede usar, por ejemplo, para enviar una notificación cuando alguien pretende acceder de manera forzada.
  - **Door Double-Lock Monitor (Monitor de doble cerradura de puerta)**: activa una regla de acción solo cuando el estado de la cerradura secundaria cambia a bloqueado o desbloqueado.
  - **Door Lock Monitor (Monitor de cerradura de puerta)**: activa una regla de acción cuando el estado de la cerradura normal cambia a bloqueado o desbloqueado. Por ejemplo, se activa un error cuando el monitor de la puerta detecta que esta está abierta, aunque la cerradura esté bloqueada.
  - **Door Mode (Modo de puerta)**: activa una regla de acción cuando se cambia el estado de la puerta. Por ejemplo, si se ha accedido a la puerta o se ha bloqueado; o bien, si la puerta está en modo de desbloqueo. Consulte la ayuda en línea para ver descripciones más detalladas de estos modos.
  - **Door Monitor (Monitor de puerta)**: activa una regla de acción cuando el estado del monitor de puerta cambia. Esto, por ejemplo, se puede usar para enviar una notificación cuando un monitor de puerta indica que la puerta está abierta o cerrada.
  - **Door Tamper (Manipulación de puerta)**: activa una regla de acción cuando el monitor de puerta detecta que la conexión está interrumpida, por ejemplo si alguien corta los cables al monitor de la puerta. Para usar este activador, asegúrese de que esté seleccionada la opción **Enable supervised inputs (Activar entradas supervisadas)** y de que estén instaladas las resistencias de final de línea en los puertos de entrada del conector de la puerta correspondiente. Para obtener más información, consulte *Cómo usar entradas supervisadas en la página 17*.
  - **Door Warning (Advertencia de puerta)**: activa una regla de acción antes de que la alarma Puerta abierta durante demasiado tiempo se dispare. Se puede usar, por ejemplo, para enviar una señal de advertencia de que el controlador de la puerta enviará la alarma real, la alarma de puerta abierta durante demasiado tiempo, si la puerta no se cierra en el tiempo especificado a tal efecto. Para obtener más información acerca de la advertencia de puerta abierta durante demasiado tiempo, consulte *Cómo configurar monitores y cerraduras de puerta en la página 14*.
  - **Lock Jammed (Cerradura atascada)**: activa una regla de acción cuando la cerradura de una puerta inalámbrica está físicamente bloqueada.

- **Event Logger (Registro de eventos)**: controla todos los eventos del controlador de la puerta, por ejemplo cuando un usuario pasa una tarjeta o abre una puerta. Si está activado **Global events (Eventos globales)**, el registro de eventos controla todos los eventos de todos los controladores del sistema. Para configurar qué alarmas y eventos pueden activar una regla de acción, vaya a **Setup > Configure Event and Alarm Logs (Configuración > Configurar registros de eventos y alarmas)**. El registro de eventos está compartido en el sistema y puede almacenar hasta 30 000 eventos. Cuando se llega al límite, el registro de eventos emplea la regla FIFO (primero en entrar, primero en salir). Esto implica que el primer evento registrado será el primero en sobrescribirse.
  - **Alarm (Alarma)**: activa una regla de acción cuando de dispara una de las alarmas especificadas. El administrador del sistema puede configurar qué eventos son más importantes que el resto y seleccionar si un evento particular debería disparar una alarma o no.
  - **Dropped Alarms (Alarmas no registradas)**: activa una regla de acción cuando no se pueden grabar nuevas alarmas en los registros de alarmas. Por ejemplo, si existen tantas alarmas simultáneas que el registro de eventos no tiene capacidad suficiente. Cuando no se registra una alarma, puede enviarse una notificación al operador.
  - **Dropped Events (Eventos no registrados)**: activa una regla de acción cuando no se pueden grabar nuevos eventos en los registros de eventos. Por ejemplo, si existen tantos eventos simultáneos que el registro de eventos no tiene capacidad suficiente. Cuando no se registra un evento, puede enviarse una notificación al operador.

- **Hardware**
  - **Network (Red)**: activa una regla de acción cuando se pierde la conexión de red. Seleccione **Yes (Sí)** para activar la regla de acción si se pierde la conexión de red. Seleccione **No** para activar la regla de acción cuando se recupera la conexión de red. Seleccione **IPv4/v6 address removed dirección** (Dirección IPv4/v6 eliminada) o **New IPv4/v6 address** (Nueva dirección IPv4/v6) para activar una acción cuando cambia la dirección IP.
  - **Peer Connection (Punto de conexión)**: activa una regla de acción cuando el producto de Axis ha establecido una conexión con otro controlador de puerta, si se pierde la conexión de red entre los dispositivos o si falla el emparejamiento de controladores de puerta. Puede utilizarse, por ejemplo, para enviar una notificación cuando un controlador de puerta ha perdido la conexión de red.
- **Input Signal (Señal de entrada)**
  - **Digital Input Port (Puerto de entrada digital)**: activa una regla de acción cuando un puerto de E/S recibe una señal de un dispositivo conectado. Consulte *Puertos de E/S en la página 63*.
  - **Manual Trigger (Activador manual)**: activa una regla de acción cuando se activa el activador manual. Puede usarse mediante un cliente, como un sistema de gestión de acceso, a través de la interfaz de programación de aplicaciones VAPIX®, para iniciar o detener manualmente la regla de acción.
  - **Virtual Inputs (Entradas digitales)**: activa una regla de acción cuando cambia el estado de una de las entradas virtuales. Puede usarse mediante un cliente, como un sistema de gestión de acceso, a través de la interfaz de programación de aplicaciones VAPIX®, para disparar acciones. Las entradas virtuales, por ejemplo, se pueden conectar a botones de la interfaz de usuario del sistema de gestión.
- **Schedule (Programación)**
  - **Interval (Intervalo)**: activa una regla de acción a la hora de inicio del programador y permanece activo hasta que llega la hora de finalización de la programación.
  - **Pulse (Impulso)**: activa una regla de acción cuando se produce un evento único. Es decir, un evento que ocurre en un momento específico y no tiene duración.
- **System (Sistema)**
  - **System Ready (Sistema preparado)**: activa una regla de acción cuando el sistema está listo. Por ejemplo, el producto Axis puede detectar el estado del sistema y enviar una notificación cuando se ha iniciado el sistema.

    Seleccione el botón de radio **Yes (Sí)** para activar la regla de acción cuando el producto esté en estado preparado. Tenga en cuenta que la regla solo se activará cuando todos los servicios necesarios, como el sistema de eventos, se hayan iniciado.
- **Time (Tiempo)**
  - **Recurrence (Repetición)**: activa una regla de acción supervisando las repeticiones que han sido creadas. Este activador se puede utilizar para iniciar acciones repetitivas, como enviar notificaciones cada hora. Seleccione un patrón de repetición o cree uno nuevo. Para obtener más información acerca de cómo configurar un patrón de repetición, consulte *Cómo configurar repeticiones en la página 52*.
  - **Use Schedule (Programación de uso)**: activa una regla de acción de acuerdo con la programación seleccionada. Consulte *Cómo crear programaciones en la página 52*.

Acciones

Puede configurar varias acciones:

- **Output Port (Puerto de salida)**: activa un puerto de E/S para controlar un dispositivo externo.
- **Send Notification (Enviar notificación)**: envía un mensaje de notificación a un destinatario.
- **Status LED (LED de estado)**: el LED de estado puede configurarse para que emita un destello durante el tiempo que dure la regla de acción o durante el tiempo en segundos que se haya establecido. El LED de estado se puede usar durante la instalación y configuración para comprobar visualmente si los ajustes de los activadores, como el activador de puerta

abierta durante demasiado tiempo, funcionan correctamente. Para establecer el color del destello del LED de estado, seleccione un **LED Color (Color de LED)** en la lista desplegable.

Cómo añadir destinatarios

El producto puede enviar mensajes para notificar a los destinatarios acerca de eventos y alarmas. Pero antes de que el producto puede enviar mensajes de notificación, se deben definir uno o varios destinatarios. Para obtener más información sobre las opciones disponibles, consulte *Tipos de destinatario en la página 51*.

Para añadir un destinatario:

1. Vaya a **Setup > Additional Controller Configuration > Events > Recipients (Configuración > Configuración de controlador adicional > Eventos > Destinatarios)** y haga clic en **Añadir**.
2. Introduzca un nombre descriptivo.
3. Seleccione un **tipo** de destinatario.
4. Introduzca la información necesaria para el tipo de destinatario.
5. Haga clic en **Prueba** para probar la conexión con el destinatario.
6. Haga clic en **OK (Aceptar)**.

Tipos de destinatario

Están disponibles los siguientes tipos destinatario:

HTTP

HTTPS

Correo electrónico

TCP

Cómo configurar destinatarios de correo electrónico

Los destinatarios de correo electrónico se pueden configurar seleccionando uno de los proveedores de correo electrónico enumerados o especificando el servidor SMTP, el puerto y la autenticación utilizada, por ejemplo, por un servidor de correo electrónico corporativo.

Nota

Algunos proveedores de correo electrónico cuentan con filtros de seguridad que evitan que los usuarios reciban o archivos adjuntos de gran tamaño, que reciban correos programados, etc. Compruebe la política de seguridad del proveedor de correo electrónico para evitar problemas de entrega y bloqueos en las cuentas de correo electrónico.

Para configurar un destinatario de correo electrónico mediante uno de los proveedores enumerados:

1. Vaya a **Events > Recipients (Eventos > Destinatarios)** y haga clic en **Add (Añadir)**.
2. Introduzca un **Name (Nombre)** y seleccione **Email (Correo electrónico)** en la lista **Type (Tipo)**.
3. Introduzca las direcciones de correo electrónico a las que se enviarán mensajes de correo electrónico en el campo **To (Para)**. Utilice comas para separar múltiples direcciones.
4. Seleccione un proveedor de correo electrónico en la lista **Provider (Proveedor)**.
5. Introduzca la ID de usuario y la contraseña de la cuenta de correo electrónico.
6. Haga clic en **Test (Probar)** para enviar un correo electrónico de prueba.

Para configurar un destinatario de correo electrónico mediante, por ejemplo, un servidor de correo electrónico corporativo, siga las instrucciones anteriores, pero seleccione **User defined (Definido por el usuario)** como **Provider (Proveedor)**. Introduzca la

dirección de correo electrónico que aparecerá como remitente en el campo **From (De)**. Seleccione **Advanced settings (Configuración avanzada)** y especifique el servidor SMTP, el puerto y el método de autenticación. Opcionalmente, seleccione **Use encryption (Utilizar cifrado)** para enviar mensajes de correo electrónico a través de una conexión cifrada. El certificado de servidor puede ser validado mediante los certificados disponibles en el producto de Axis. Para obtener información sobre cómo cargar certificados, consulte *Certificados en la página 56*.

Cómo crear programaciones

Las programaciones se pueden utilizar como activadores de reglas de acción o como condiciones adicionales. Utilice una de las programaciones predefinidas o cree una nueva programación según se describe a continuación.

Para crear una nueva programación:

1. Vaya a **Setup > Additional Controller Configuration > Events > Schedules (Configuración > Configuración de controlador adicional > Eventos > Programaciones)** y haga clic en **Añadir**.
2. Introduzca un nombre descriptivo y la información necesaria para una programación diaria, semanal, mensual o anual.
3. Haga clic en **OK (Aceptar)**.

Para utilizar la programación en una regla de acción, seleccione la programación en la lista desplegable **Programación** en la página de configuración de la regla de acción.

Cómo configurar repeticiones

Las repeticiones se utilizan para activar la reglas de acción varias veces, por ejemplo, cada 5 minutos o cada hora.

Para configurar una repetición:

1. Vaya a **Setup > Additonal Controller Configuration > Events > Recurrences (Configuración > Configuración de controlador adicional > Eventos > Repeticiones)** y haga clic en **Añadir**.
2. Especifique un nombre descriptivo y un patrón de repetición.
3. Haga clic en **OK (Aceptar)**.

Para usar la repetición en una regla de acción, seleccione en primer lugar **Tiempo** en la lista desplegable **Activador** en la página Configuración de regla de acción y, a continuación, seleccione la repetición en la segunda lista desplegable.

Para modificar o eliminar las repeticiones, seleccione la repetición en la **Lista de repeticiones** y haga clic en **Modificar** o en **Eliminar**.

Información del lector

Los lectores utilizan luces LED e indicadores acústicos para enviar información al usuario (la persona que accede o intenta acceder a la puerta). El controlador de puerta puede activar una serie de mensajes informativos, algunos de los cuales se han preconfigurado en el controlador de puerta y son compatibles con la mayoría de lectores.

Los lectores presentan diferentes respuestas LED, pero por lo general utilizan distintas secuencias de luces fijas y parpadeantes de color rojo, verde y ámbar.

Los lectores también pueden utilizar indicadores acústicos de un solo tono para enviar mensajes mediante distintas secuencias de señales acústicas cortas y largas.

La tabla siguiente muestra los eventos preconfigurados en el controlador de puerta para activar la información del lector y sus señales de información más habituales. Las señales informativas de los lectores de Axis se presentan en la guía de instalación proporcionada con el lector de Axis.

Evento	Wiegand LED dual	Wiegand LED único	OSDP	Patrón de indicador acústico	Estado
Inactivo[1]	Desactivado	Rojo	Rojo	Silencioso	Normal

Configuración de eventos y alarmas

Se requiere PIN	Rojo/verde intermitente	Rojo/verde intermitente	Rojo/verde intermitente	Dos pitidos cortos	Se requiere PIN
Acceso permitido	Verde	Verde	Verde	Señal sonora	Acceso permitido
Acceso denegado	Rojo	Rojo	Rojo	Señal sonora	Acceso denegado

1. Se pasa a estado inactivo cuando la puerta está cerrada y la cerradura esté bloqueada.

Los mensajes de información distintos de los anteriores se deben configurar mediante un cliente, como un sistema de gestión de acceso, a través de la interfaz de programación de aplicaciones VAPIX®, que es compatible con esta función y utiliza lectores capaces de proporcionar las señales requeridas. Para obtener más información, consulte la información del usuario proporcionada por el desarrollador del sistema de gestión de acceso y por el fabricante del lector.

Reports (Informes)

La página de informes permite ver, imprimir y exportar informes que contienen diferentes tipos de información acerca del sistema. Para obtener más información acerca de los informes, consulte *Tipos de informe en la página 54*.

Ver, imprimir y exportar informes

Para abrir la página de informes, haga clic en **Reports (Informes)**.

Para ver un informe, haga clic en **View and print (Ver e imprimir)**.

Para imprimir un informe:

1. Haga clic en **View and print (Ver e imprimir)**.
2. Seleccione las columnas que se incluirán en el informe. De forma predeterminada se seleccionan todas las columnas.
3. Si desea limitar el alcance del informe, introduzca un filtro en el campo de filtro correspondiente. Por ejemplo, puede filtrar usuarios por grupo el al que pertenecen, puertas por sus programaciones o grupos por puertas a las que tienen acceso.

   Para obligar a obtener resultados exactos, entrecomille el texto del filtro, por ejemplo, "Juan".
4. Si desea ordenar los elementos del informe en un orden diferente, haga clic en  en la columna correspondiente. Para cambiar entre orden estándar e inverso, active los botones de clasificación.

    Muestra los elementos en orden estándar (ascendente).

    Muestra los elementos en orden inverso (descendente).
5. Haga clic en **Print selected columns (Imprimir columnas seleccionadas)**.

Para exportar un informe, haga clic en **Export CSV file (Exportar archivo CSV)**.

El informe se exporta como archivo de valores separados por comas (CSV) e incluye todas las columnas y elementos posibles para el tipo de informe. A menos que se especifique lo contrario, el archivo exportado (*.csv) se guarda en la carpeta de descargas predeterminada. Se puede seleccionar una carpeta de descargas en la configuración de usuario del navegador web.

Nota

Solo se muestran en los informes los usuarios que disponen de credenciales.

Tipos de informe

Están disponibles los siguientes tipos informe:

- Programaciones de acceso. Para obtener más información sobre los tipos de programación de acceso y opciones, consulte *página 32* y *página 33*.
- Grupos. Para obtener más información acerca de las credenciales de grupo, consulte *página 34*.
- Puertas. Para obtener más información acerca de puertas y tipos de identificación, consulte *página 35* y *página 36*.
- Usuarios. Para obtener más información sobre credenciales de usuario, consulte *página 41*.
- Controladores de puerta. Para obtener más información sobre los controladores conectados y sus tipos de identificación, consulte *página 27*. Para obtener más información acerca de las opciones de tiempo de los monitores de puerta, consulte *página 16*.

Opciones del sistema

Seguridad

Usuarios

El control de acceso de usuario está activado de forma predeterminada y se pueden configurar en **Setup > Additional Controller Configuration > System Options > Security > Users (Configuración > Configuración de controlador adicional > Opciones del sistema > Seguridad > Usuarios)**. Un administrador puede configurar otros usuarios asignándoles nombres de usuario y contraseñas.

La lista de usuarios muestra los usuarios autorizados y grupos de usuarios (niveles de acceso):

- **Los administradores** tienen acceso sin restricciones a todos los ajustes. El administrador puede añadir, modificar y eliminar otros usuarios.

Nota

Tenga en cuenta que, cuando la opción **Cifrado y sin cifrar** está activada, el servidor web cifrará la contraseña. Esta es la opción predeterminada para una unidad nueva o para una unidad restablecida a los ajustes predeterminados de fábrica.

En **Configuración de contraseña HTTP/RTSP**, seleccione el tipo de contraseña permitida. Puede que necesite permitir contraseñas no cifradas si hay clientes de visualización que no admiten cifrado o si ha actualizado el firmware y los clientes actuales admiten cifrado, pero se debe volver a iniciar sesión para configurarlos a fin de utilizar esta funcionalidad.

ONVIF

ONVIF es un foro abierto del sector que proporciona y promueve interfaces estandarizadas para una eficiente interoperabilidad de los productos de seguridad físicos basados en IP.

Al crear un usuario, se permite automáticamente la comunicación ONVIF. Utilice el nombre de usuario y la contraseña en todas las comunicaciones ONVIF con el producto. Consulte *www.onvif.org* para obtener más información.

Filtro de direcciones IP

El filtrado de direcciones IP se habilita en la página **Setup > Additional Controller Configuration > System Options > Security > IP Address Filter (Configuración > Configuración de controlador adicional > Opciones del sistema > Seguridad > Filtro de direcciones IP)**. Una vez activado, el acceso al producto de Axis está permitido o denegado a las direcciones IP enumeradas. Seleccione en la lista **Allow (Permitir)** o **Deny (Denegar)** y haga clic en **Apply (Aplicar)** para habilitar el filtrado de direcciones IP.

El administrador puede añadir a la lista hasta 256 entradas de direcciones IP (una única entrada puede incluir varias direcciones IP).

HTTPS

HTTPS (HyperText Transfer Protocol over Secure Socket Layer, o HTTP por SSL) es un protocolo web que proporciona navegación cifrada. Los usuarios y clientes también pueden utilizar HTTPS para comprobar que se tiene acceso al dispositivo correcto. El nivel de seguridad proporcionado por HTTPS se considera adecuado para la mayoría de intercambios comerciales.

El producto de Axis puede configurarse para solicitar HTTPS cuando los administradores inician sesión.

Para poder usar HTTPS, debe haber instalado un certificado HTTPS. Vaya a **Setup > Additional Controller Configuration > System Options > Security > Certificates (Configuración > Configuración de controlador adicional > Opciones del sistema > Seguridad > Certificados)** para instalar y administrar certificados. Consulte *Certificados en la página 56*.

Para habilitar HTTPS en el producto de Axis:

1. Vaya a **Setup > Additional Controller Configuration > System Options > Security > HTTPS (Configuración > Configuración de controlador adicional > Opciones del sistema > Seguridad > HTTPS)**
2. Seleccione un certificado HTTPS en la lista de certificados instalados.
3. Opcionalmente, haga clic en **Ciphers (Cifrados)** y seleccione los algoritmos de cifrado que se utilizarán para SSL.

4. Establezca la **HTTPS Connection Policy (Política de conexión HTTPS)** para los distintos grupos de usuarios.
5. Haga clic en **Save (Guardar)** para activar la configuración.

Para acceder al producto de Axis a través del protocolo deseado, introduzca en el campo de dirección del navegador `https://` para el protocolo HTTPS y `http://` para el protocolo HTTP.

Se puede cambiar el puerto HTTPS en la página **System Options > Network > TCP/IP > Advanced (Opciones del sistema > Red > TCP/IP > Avanzadas)** página.

IEEE 802.1X

IEEE 802.1X es un estándar para el control de admisión de red basada en puertos que proporciona una autenticación segura de los dispositivos de red conectados e inalámbricos. IEEE 802.1X se basa en el protocolo de autenticación extensible, EAP.

Para acceder a una red protegida por IEEE 802.1X, los dispositivos deben autenticarse. Un servidor de autenticación lleva a cabo esta autenticación, normalmente un **servidor RADIUS**; por ejemplo, FreeRADIUS y Microsoft Internet Authentication Server.

En la implementación de Axis, el producto de Axis y el servidor de identificación se identifican ellos mismos con certificados digitales utilizando EAP-TLS (protocolo de autenticación extensible - seguridad de la capa de transporte). Los certificados son proporcionados por una **Autoridad de Certificación** (AC). Se necesita:

- Un certificado de la AC para autenticar el servidor de autenticación.
- Un certificado de cliente con firma AC para autenticar el producto de Axis.

Para crear e instalar certificados, vaya a **Setup > Additional Controller Configuration > System Options > Security > Certificates (Configuración > Configuración de controlador adicional > Opciones del sistema > Seguridad > Certificados)** para instalar y administrar certificados. Consulte *Certificados en la página 56*.

Para permitir el acceso del producto a una red protegida por IEEE 802.1X:

1. Vaya a **Setup > Additional Controller Configuration > System Options > Security > IEEE 802.1X (Configuración > Configuración de controlador adicional > Opciones del sistema > Seguridad > IEEE 802.1X)**.
2. Seleccione un **CA Certificate (Certificado de AC)** y un **Client Certificate (Certificado de cliente)** de las listas de certificados instalados.
3. En **Settings (Ajustes)**, seleccione la versión EAPOL y proporcione la identidad EAP asociada al certificado de cliente.
4. Marque la casilla para activar IEEE 802.1X y haga clic en **Save (Guardar)**.

Nota

Para que la autenticación funcione correctamente, la configuración de fecha y hora del producto de Axis se debe sincronizar con un servidor NTP. Consulte *Fecha y hora en la página 57*.

Certificados

Los certificados se utilizan para autenticar los dispositivos de una red. Las aplicaciones más habituales incluyen la navegación web cifrada (HTTPS), la protección de la red mediante IEEE 802.1X y los mensajes de notificación, por ejemplo a través de correo electrónico. Se pueden utilizar dos tipos de certificados con los productos de Axis:

Server/Client certificates (Certificados de servidor-cliente) - Autenticar el producto Axis. Un certificado **Server/Client (Servidor-Cliente)** puede ser autofirmado o emitido por una autoridad de certificación (AC). Un certificado firmado por el propio producto ofrece protección limitada y se puede utilizar antes de que se obtenga un certificado emitido por una AC.

Certificados AC - Autenticar certificados entre iguales, por ejemplo, el certificado de un servidor de autenticación en caso de que el producto de Axis se conecte a una red protegida IEEE 802.1X. El producto de Axis se proporciona con varios certificados AC preinstalados.

Nota

- Si el producto se restablece a la configuración predeterminada de fábrica, se eliminarán todos los certificados, excepto los certificados AC preinstalados.
- Si el producto se restablece a la configuración predeterminada de fábrica, se reinstalarán todos los certificados, excepto los certificados AC preinstalados.

Cómo crear un certificado autofirmado

1. Vaya a **Setup > Additional Controller Configuration > System Options > Security > Certificates (Configuración > Configuración de controlador adicional > Opciones del sistema > Seguridad > Certificados)**.
2. Haga clic en **Create self-signed certificate (Crear certificado autofirmado)** y proporcione la información solicitada.

Cómo crear e instalar un certificado firmado por una autoridad de certificación

1. Cree un certificado autofirmado; consulte .
2. Vaya a **Setup > Additional Controller Configuration > System Options > Security > Certificates (Configuración > Configuración de controlador adicional > Opciones del sistema > Seguridad > Certificados)**.
3. Haga clic en **Create certificate signing request (Crear solicitud de firma de certificado)** y proporcione la información solicitada.
4. Copie la solicitud con formato PEM y envíela a la autoridad de certificación de su elección.
5. Cuando se devuelva el certificado firmado, haga clic en **Install certificate (Instalar certificado)** y cargue el certificado).

Cómo instalar certificados adicionales de una autoridad de certificación

1. Vaya a **Setup > Additional Controller Configuration > System Options > Security > Certificates (Configuración > Configuración de controlador adicional > Opciones del sistema > Seguridad > Certificados)**.
2. Haga clic en **Install certificate (Instalar certificado)** y cargue el certificado.

Fecha y hora

Los ajustes de fecha y hora del producto Axis se configuran en **System Options > Date & Time (Configuración > Configuración de controlador adicional > Opciones del sistema > Fecha y hora)**.

Hora actual del servidor muestra la fecha y hora actuales (formato de 24 horas).

Para cambiar los ajustes de fecha y hora, seleccione el **Modo horario** en **Nueva hora del servidor**:

- **Sincronizar con hora del ordenador**: establece la fecha y hora de acuerdo con el reloj del equipo. Con esta opción, la fecha y la hora se establecen una vez y no se actualizan automáticamente.
- **Sincronizar con servidor NTP**: la fecha y la hora se obtienen de un servidor NTP. Con esta opción, la configuración de fecha y hora se actualiza continuamente. Para obtener información sobre la configuración NTP, consulte *Configuración NTP en la página 60*.

  Si utiliza un nombre de host para el servidor NTP, se debe configurar un servidor DNS. Consulte *Configuración DNS en la página 60*.
- **Configurar manualmente**: permite configurar manualmente la fecha y hora.

Si utiliza un servidor NTP, seleccione su **Zona horaria** en la lista desplegable. En caso necesario, marque **Ajustar automáticamente entre horario de verano e invierno**.

Red

Ajustes básicos de TCP/IP

El producto de Axis admite IP versión 4 (IPv4).

El producto de Axis puede obtener una dirección IPv4 de los siguientes modos:

- **Dirección IP dinámica**: **Obtain IP address via DHCP (Obtener dirección IP a través de DHCP)** está activado de forma predeterminada. Esto significa que se configura el producto Axis para que obtenga automáticamente la dirección IP a través de Dynamic Host Configuration Protocol (DHCP).

  DHCP permite a los administradores de red administrar y automatizar la asignación de direcciones IP de forma centralizada.

- **Dirección IP estática** : para utilizar una dirección IP estática, seleccione **Use the following IP address (Usar la siguiente dirección IP)** y especifique la dirección IP, la máscara de subred y el router predeterminado. A continuación, haga clic en **Save (Guardar)**.

DHCP solo debe habilitarse si se utiliza la notificación de dirección IP dinámica o si DHCP puede actualizar un servidor DNS que permite acceder al producto de Axis por su nombre (nombre de host).

Si DHCP está habilitado y no se puede acceder al producto, ejecute AXIS IP Utility para buscar en la red los productos Axis conectados, o restablezca el producto a la configuración predeterminada de fábrica y, a continuación, vuelva a realizar la instalación. Para obtener información sobre cómo restablecer los valores predeterminados de fábrica, consulte *página 65*.

ARP/Ping

La dirección IP del producto se puede asignar usando ARP y Ping. Para consultar las instrucciones, vea *Asignar una dirección IP usando ARP/Ping en la página 58*.

El servicio ARP/Ping está activado de forma predeterminada, pero se desactiva automáticamente transcurridos dos minutos desde el inicio del producto o tan pronto como se asigna una dirección IP. Para volver a asignar la dirección IP usando ARP/Ping, el producto debe reiniciarse a fin de habilitar ARP/Ping durante otros dos minutos.

Para deshabilitar el servicio, vaya a **Setup > Additional Controller Configuration > System Options > Network > TCP/IP > Basic (Configuración > Configuración de controlador adicional > Opciones del sistema > Red > TCP/IP > Básica)** y desmarque la opción **Enable ARP/Ping setting of IP address (Habilitar ajuste ARP/Ping de dirección IP)**.

Cuando el servicio esté deshabilitado seguirá siendo posible hacer ping en el producto.

Asignar una dirección IP usando ARP/Ping

La dirección IP del dispositivo se puede asignar usando ARP/Ping. El comando se debe emitir en un plazo de 2 minutos a partir de la conexión de la fuente de alimentación.

1. Adquiera una dirección IP estática gratis en el mismo segmento de red que el equipo.
2. Localice el número de serie (S/N) en la etiqueta del dispositivo.
3. Abra el símbolo del sistema e introduzca los siguientes comandos:

   Sintaxis Linux/Unix

   ```
   arp -s <dirección IP> <número de serie> temp
   ping -s 408 <dirección IP>
   ```

   Ejemplo de Linux/Unix

   ```
   arp -s 192.168.0.125 00:40:8c:18:10:00 temp
   ping -s 408 192.168.0.125
   ```

   Sintaxis de Windows (es posible que deba ejecutar el símbolo del sistema como administrador)

```
arp -s <dirección IP> <número de serie>
ping -l 408 -t <dirección IP>
```

Ejemplo de Windows (es posible que deba ejecutar el símbolo del sistema como administrador)

```
arp -s 192.168.0.125 00-40-8c-18-10-00
ping -l 408 -t 192.168.0.125
```

4. Reinicie el dispositivo. Para ello, debe desconectar y volver a conectar el conector de red.
5. Cierre el símbolo del sistema cuando el dispositivo responda con `Reply from 192.168.0.125:...` o similar.
6. Abra un navegador y escriba `http://<dirección IP>` en el campo de la dirección.

Para conocer otros métodos de asignación de direcciones IP, consulte el documento *Cómo asignar una dirección IP y acceder al dispositivo* en *www.axis.com/support*.

Nota

- Para abrir el símbolo del sistema en Windows, abra el menú **Start (Inicio)** y busque `cmd`.
- Para usar el comando ARP en Windows 8/Windows 7/Windows Vista, haga clic en el botón derecho del icono del símbolo del sistema y seleccione **Run as administrator (Ejecutar como administrador)**.
- Para abrir el símbolo del sistema en Mac OS X, abra la **utilidad Terminal** desde **Aplicación > Utilidades**.

AXIS Video Hosting System (AVHS)

AVHS, utilizado en combinación con un servicio AVHS, ofrece acceso seguro y sencillo a Internet para poder acceder a la gestión del controlador y los registros desde cualquier ubicación. Para obtener más información y asistencia para localizar un proveedor de servicios AVHS, acceda a www.axis.com/hosting.

Los ajustes de AVHS se configuran en **Setup > Additional Controller Configuration > System Options > Network > TCP IP > Basic (Configuración > Configuración de controlador adicional > Opciones del sistema > Red > TCP IP > Básica)**. La posibilidad de conectarse a un servicio AVHS está activada de forma predeterminada. Para deshabilitarla, desmarque la casilla **Habilitar AVHS**.

Habilitar un solo clic – Mantenga pulsado el botón de control del producto (consulte *Información general del producto en la página 3*) durante aproximadamente 3 segundos para conectar a un servicio AVHS a través de Internet. Una vez registrado, debe habilitarse **Siempre** y el producto de Axis permanecerá conectado al servicio AVHS. Si no se registra el producto en un plazo de 24 horas desde el momento en que se pulsó el botón, el producto se desconectará del servicio AVHS.

Siempre – El producto de Axis intentará conectarse continuamente al servicio AVHS a través de Internet. Una vez registrado, el producto permanecerá conectado al servicio. Esta opción puede utilizarse cuando el producto ya está instalado y no es posible o no es conveniente utilizar la instalación en un solo clic.

Nota

El soporte de AVHS depende de la disponibilidad de suscripciones de proveedores de servicios.

Servicio AXIS Internet Dynamic DNS

El servicio AXIS Internet Dynamic DNS asigna un nombre de host para facilitar el acceso al producto. Para obtener más información, consulte *www.axiscam.net*.

Para registrar el producto de Axis en el servicio AXIS Internet Dynamic DNS, vaya a **Setup > Additional Controller Configuration > System Options > Network > TCP/IP > Basic (Configuración > Configuración de controlador adicional > Opciones del sistema > Red > TCP/IP > Básica)**. En **Servicios**, haga clic en el botón **Configuración** de AXIS Internet Dynamic DNS Service (requiere acceso a Internet). El nombre de dominio registrado actualmente en el servicio AXIS Internet Dynamic DNS para el producto se puede eliminar en cualquier momento.

Nota

AXIS Internet Dynamic DNS Service requiere IPv4.

Configuración avanzada TCP/IP

Configuración DNS

DNS (Domain Name Service) proporciona la traducción de nombres de host a direcciones IP. Los ajustes DNS se configuran desde **Setup > Additional Controller Configuration > System Options > Network > TCP/IP > Advanced (Configuración > Configuración de dispositivo adicional > Opciones de sistema > red > TCP/IP > Avanzada)**.

Seleccione **Obtain DNS server address via DHCP (Obtener dirección de servidor DNS a través de DHCP)** para utilizar la configuración de DNS proporcionada por el servidor DHCP.

Para realizar la configuración manual, seleccione **Use the following DNS server address (Usar la siguiente dirección del servidor DNS)** y especifique los elementos siguientes:

Nombre de dominio – Introduzca los dominios donde se buscará el nombre de host utilizado por el producto Axis. Se pueden introducir múltiples dominios separados por punto y coma. El nombre de host siempre es la primera parte de un nombre de dominio completamente cualificado, por ejemplo, `myserver` es el nombre de host en el nombre de dominio completamente cualificado `myserver.mycompany.com`, donde `mycompany.com` es el nombre de dominio.

Servidor DNS principal y secundario – Introduzca las direcciones IP de los servidores DNS principal y secundario. El servidor DNS secundario es opcional y se utilizará cuando el principal no esté disponible.

Configuración NTP

NTP (Network Time Protocol) se utiliza para sincronizar la hora de reloj de los dispositivos de una red. Los ajustes NTP se configuran desde **Configuración > Configuración de dispositivo adicional > Opciones de sistema > red > TCP/IP > Avanzada (Setup > Additional Controller Configuration > System Options > Network > TCP/IP > Advanced)**.

Seleccione **Obtain NTP server address via DHCP (Obtener dirección de servidor NTP a través de DHCP)** para utilizar la configuración de NTP proporcionada por el servidor DHCP.

Para realizar la configuración manual, seleccione **Use the following NTP server address (Usar la siguiente dirección de servidor NTP)** e introduzca el nombre de host o la dirección IP del servidor NTP.

Configuración de nombre de host

El producto de Axis es accesible a través de un nombre de host en lugar de una dirección IP. El nombre de host suele ser el mismo que el nombre DNS asignado. El nombre de host se configura desde **Setup > Additional Controller Configuration > System Options > Network > TCP/IP > Advanced (Configuración > Configuración de dispositivo adicional > Opciones de sistema > red > TCP/IP > Avanzada)**.

Seleccione **Obtain host name via IPv4 DHCP (Obtener nombre de host a través de DHCP IPv4)** para utilizar el nombre de host proporcionado por el servidor DHCP que se ejecuta en IPv4.

Seleccione **Use the host name (Utilizar el nombre de host)** para establecer manualmente el nombre de host.

Seleccione **Enable dynamic DNS updates (Activar actualizaciones dinámicas de DNS)** para actualizar dinámicamente los servidores DNS locales siempre que cambie la dirección IP del producto de Axis. Consulte la ayuda en línea para obtener más información.

Dirección de enlace local IPv4

Link-Local Address (Dirección de enlace local) se activa de forma predeterminada y asigna al producto de Axis una dirección IP adicional que se puede utilizar para acceder al producto desde otros hosts en el mismo segmento de la red local. El producto puede tener una IP de enlace local y al mismo tiempo una dirección IP estática o proporcionada por DHCP.

Esta función se puede deshabilitar en **Setup > Additional Controller Configuration > System Options > Network > TCP/IP > Advanced (Configuración > Configuración del controlador adicional > Opciones del sistema > Red > TCP/IP > Avanzada)**.

Opciones del sistema

HTTP

El puerto HTTP utilizado por el producto de Axis se puede cambiar en **Setup > Additional Controller Configuration > System Options > Network > TCP/IP > Advanced (Configuración > Configuración de controlador adicional > Opciones del sistema > Red > TCP/IP > Avanzada)**. Además del puerto predeterminado, que es 80, se puede utilizar cualquier puerto entre 1024 y 65535.

HTTPS

El puerto HTTPS utilizado por el producto de Axis se puede cambiar en **Setup > Additional Controller Configuration > System Options > Network > TCP/IP > Advanced (Configuración > Configuración de controlador adicional > Opciones del sistema > Red > TCP/IP > Avanzada)**. Además del puerto predeterminado, que es 443, se puede utilizar cualquier puerto entre 1024 y 65535.

Para activar HTTPS, vaya a **Setup > Additional Controller Configuration > System Options > Security > HTTPS (Configuración > Configuración de controlador adicional > Opciones del sistema > Seguridad > HTTPS)**. Para obtener más información, consulte *HTTPS en la página 55*.

NAT transversal (asignación de puertos) para IPv4

Un router de red permite a los dispositivos en una red privada (LAN) compartir una única conexión a Internet. Esto se realiza redirigiendo el tráfico de red desde la red privada hacia el "exterior", es decir, hacia internet. La seguridad de la red privada (LAN) es mayor, ya que la mayoría de los routers están preconfigurados para detener los intentos de acceso a la red privada (LAN) desde la red pública (internet).

Utilice **NAT transversal** cuando el producto Axis se encuentra en una intranet (LAN) y se desea que esté disponible desde el otro lado (WAN) de un router NAT. Con la NAT transversal configurada correctamente, se envía al producto todo el tráfico HTTP a un puerto externo HTTP en el router NAT.

NAT transversal se configura desde **Setup > Additional Controller Configuration > System Options > Network > TCP/IP > Advanced (Configuración > Configuración de dispositivo adicional > Opciones de sistema > red > TCP/IP > Avanzada)**.

Nota

- La NAT transversal debe ser compatible con el router para poder funcionar. El router debe ser compatible también con UPnP®.
- En este contexto, un router hace referencia a cualquier dispositivo de enrutamiento de red, como un router NAT, un router de red, una puerta de enlace de Internet, un router de banda ancha, un dispositivo de uso compartido de banda ancha o un software, como un cortafuegos.

Activar/desactivar – Si se activa, el producto de AXIS tratará de configurar la asignación de puertos de un router NAT de la red mediante UPnP. Tenga en cuenta que UPnP debe estar habilitado en el producto (consulte **Setup > Additional Controller Configuration > System Options > Network > UPnP (Configuración > Configuración de controlador adicional > Opciones del sistema > Red > UPnP)**).

Utilizar router NAT seleccionado manualmente – Seleccione esta opción para seleccionar manualmente un router NAT y escriba en el campo la dirección IP para el router. Si no se especifica ningún router, el producto busca automáticamente routers NAT en su red. Si se encuentra más de un router, se selecciona el router predeterminado.

Puerto HTTP alternativo – Seleccione esta opción para definir manualmente un puerto HTTP externo. Introduzca un puerto dentro del rango 1024-65535. Si el campo del puerto está vacío o contiene la configuración predeterminada, que es 0, se seleccionará automáticamente un número de puerto al habilitar NAT transversal.

Nota

- Un puerto HTTP alternativo puede utilizarse o estar activo incluso si la función de NAT transversal está desactivada. Esto resulta útil si el router NAT no admite UPnP y se necesita configurar manualmente la redirección de puertos en el router NAT.
- Si se intenta introducir manualmente un puerto que ya está en uso, automáticamente se selecciona otro puerto disponible.
- En este campo se indica si el puerto está seleccionado automáticamente. Para cambiarlo, introduzca un nuevo número de puerto y haga clic en **Guardar**.

FTP

El servidor FTP que se ejecuta en el producto de Axis permite la carga de nuevo firmware, aplicaciones de usuario, etc. El servidor FTP se puede deshabilitar en **Setup > Additional Controller Configuration > System Options > Network > TCP/IP > Advanced (Configuración > Configuración de controlador adicional > Red > TCP/IP > Avanzada)**.

RTSP

El servidor RTSP que se ejecuta en el producto de Axis permite a un cliente conectado iniciar una transmisión de evento. Se puede cambiar el número de puerto RTSP en **Setup > Additional Controller Configuration > System Options > Network > TCP/IP > Advanced (Configuración > Configuración de controlador adicional > Opciones del sistema > Red > TCP/IP > Avanzada)**. El puerto predeterminado es 554.

Nota

La retransmisión de eventos no estará disponible si se desactiva el servidor RTSP.

SOCKS

SOCKS es un protocolo de proxy de red. El producto de Axis puede configurarse para utilizar un servidor SOCKS a fin de llegar a redes situadas detrás de un cortafuegos o un servidor proxy. Esta funcionalidad resulta útil si el producto de Axis se encuentra en una red local detrás de un firewall y las notificaciones, cargas, alarmas, etc. deben enviarse a un destino situado fuera de la red local (por ejemplo, Internet).

SOCKS se configura en **Setup > Additional Controller Configuration > System Options > Network > SOCKS (Configuración > Configuración de controlador adicional > Opciones de sistema > Red > SOCKS)**. Consulte la ayuda en línea para obtener más información.

QoS (Calidad de Servicio)

QoS (calidad de servicio) garantiza un nivel determinado de un recurso especificado al tráfico seleccionado en una red. Una red con QoS establece las prioridades del tráfico de red y ofrece una mayor fiabilidad de la red mediante el control de la cantidad de ancho de banda que puede usar una aplicación.

La configuración de QoS se ajusta en **Setup > Additional Controller Configuration > System Options > Network > QoS (Configuración > Configuración de controlador adicional > Opciones de sistema > Red > QoS)**. Utilizando valores DSCP (Differentiated Services Codepoint), el producto de Axis puede marcar eventos/alarmas y gestión de tráfico.

SNMP

El protocolo de administración de red simple (SNMP) permite gestionar dispositivos de red de manera remota. Una comunidad SNMP es el grupo de dispositivos y estación de administración que ejecuta SNMP. Los nombres de comunidad se utilizan para identificar grupos.

Para habilitar y configurar SNMP en el producto de Axis, vaya a la página **Setup > Additional Controller Configuration > System Options > Network > SNMP (Configuración > Configuración de controlador adicional > Opciones del sistema > Red > SNMP)**.

En función del nivel de seguridad requerido, seleccione la versión de SNMP que se utilizará.

El producto Axis utiliza traps para enviar mensajes al sistema de gestión ante eventos importantes y cambios de estado. Marque **Activar traps** e introduzca la dirección IP a la que se debe enviar el mensaje trap y la **Comunidad trap** que debe recibir el mensaje.

Nota

Si HTTPS está habilitado, SNMP v1 y SNMP v2c deben desactivarse.

El producto Axis utiliza **traps para SNMP v1/v2** a fin de enviar mensajes al sistema de gestión ante eventos importantes y cambios de estado. Marque **Activar traps** e introduzca la dirección IP a la que se debe enviar el mensaje trap y la **Comunidad trap** que debe recibir el mensaje.

Están disponibles las traps siguientes:

- Arranque en frío

- Arranque templado
- Vincular
- Error de autenticación

SNMP v3 proporciona cifrado y contraseñas seguras. Para usar traps con SNMP v3, se requiere una aplicación de administración de SNMP v3.

Para usar SNMP v3, HTTPS debe estar activado; consulte *HTTPS en la página 55*. Para habilitar SNMP v3, active la casilla de verificación y proporcione la contraseña del usuario inicial.

Nota

La contraseña inicial solo se puede establecer una vez. Si se pierde la contraseña, se deberá restablecer el producto Axis a su configuración predeterminada de fábrica; consulte *Restablecimiento a la configuración predeterminada de fábrica en la página 65*.

UPnP

El producto de Axis incluye compatibilidad con UPnP®. UPnP está activado de forma predeterminada y el producto es detectado automáticamente por los sistemas operativos y clientes compatibles con este protocolo.

Se puede desactivar UPnP en **Setup > Additional Controller Configuration > System Options > Network > UPnP (Configuración > Configuración de controlador adicional > Opciones del sistema > Red > UPnP)**.

Bonjour

El producto de Axis incluye compatibilidad con Bonjour. Bonjour está activado de forma predeterminada y el producto es detectado automáticamente por los sistemas operativos y clientes compatibles con este protocolo.

Se puede desactivar Bonjour en **Setup > Additional Controller Configuration > System Options > Network > Bonjour (Configuración > Configuración de controlador adicional > Opciones del sistema > Red > Bonjour)**.

Puertos y dispositivos

Puertos de E/S

El conector auxiliar en el producto de Axis ofrece dos puertos de entrada y salida configurables para la conexión de dispositivos externos. Para obtener información sobre cómo conectar dispositivos externos, consulte la Guía de instalación, disponible en *www.axis.com*

Los puertos de E/S se configuran en **Setup > Additional Controller Configuration > System Options > Ports & Devices > I/O Ports (Configuración > Configuración de controlador adicional > Opciones del sistema > Puertos y dispositivos > Puertos de E/S)**. Seleccione la dirección del puerto (**Input (Entrada)** o **Output (Salida)**). Los puertos pueden tener nombres descriptivos y su **Estado Normal** se puede configurar como **Circuito abierto** o **Circuito a tierra**.

Estado de puerto

La lista que se encuentra en la página **System Options > Ports & Devices > Port Status (Opciones del sistema > Puertos y dispositivos > Estado de puerto)** muestra el estado de los puertos de entrada y salida del producto.

Mantenimiento

El producto de Axis ofrece varias funciones de mantenimiento. Están disponibles en **Setup > Additional Controller Configuration > Setup > System Options > Maintenance (Configuración > Configuración del controlador adicional > Configuración > Opciones del sistema > Mantenimiento)**.

Haga clic en **Restart (Reiniciar)** para realizar un reinicio adecuado del producto Axis si este no se comporta como se espera. No afectará a la configuración actual.

Nota

Un reinicio borra todas las entradas en el informe del servidor.

Haga clic en **Restore (Restaurar)** para restablecer la mayoría de los ajustes a los valores predeterminados de fábrica. Los siguientes ajustes no se verán afectados:

- el protocolo de arranque (DHCP o estático)
- la dirección IP estática
- el router predeterminado
- la máscara de subred
- la hora del sistema
- los ajustes de IEEE 802.1X

Haga clic en **Default (Predeterminada)** para restablecer todos los valores, incluida la dirección IP, a los valores predeterminados de fábrica. Este botón debe utilizarse con precaución. El producto de Axis también se puede restablecer a los valores predeterminados de fábrica con el botón de control; consulte *Restablecimiento a la configuración predeterminada de fábrica en la página 65*

Para obtener información sobre la actualización del firmware, consulte *Cómo actualizar el firmware en la página 67*.

Hacer una copia de seguridad de los datos de la aplicación

Para hacerlo, vaya a **Setup > Create a backup (Configuración > Crear una copia de seguridad)**. Se copian los datos de usuarios, credenciales, grupos y programaciones. Cuando se crea una copia de seguridad, se guarda un archivo con los datos en el ordenador.

Vaya a **Setup > Upload a backup (Configuración < Cargar una copia de seguridad)** para usar un archivo de copia de seguridad creado anteriormente y restaurar los datos de la aplicación. Para poder cargar el archivo, tiene que restablecer los ajustes predeterminados de fábrica en el dispositivo. Para consultar las instrucciones, vea *Restablecimiento a la configuración predeterminada de fábrica en la página 65*.

Soporte técnico

Soporte de vista general

La página **Setup > Additional Controller Configuration > System Options > Support > Support Overview (Configuración > Configuración de controlador adicional > Opciones del sistema > Soporte > Soporte de vista general)** proporciona información para la localización de problemas e información de contacto en caso de necesitar asistencia técnica.

Consulte también *Solución de problemas en la página 67*.

Descripción general del sistema

Para obtener una visión general de la configuración y el estado del producto de Axis, vaya a **Setup > Additional Controller Configuration > System Options > Support > System Overview (Configuración > Configuración de controlador adicional > Opciones del sistema > Soporte > Descripción general del sistema**. Entre la información disponible se encuentra la versión de firmware, la dirección IP, los ajustes de red y de seguridad, los ajustes de eventos y los elementos recientes del registro.

Registros e informes

La página **Setup > Additional Controller Configuration > System Options > Support > Logs & Reports (Configuración > Configuración de controlador adicional > Opciones del sistema > Soporte > Registros e informes)** genera registros e informes de utilidad para análisis y resolución de problemas del sistema. Si se pone en contacto con el soporte técnico de Axis, incluya un Informe del sistema junto con su consulta.

Registro del sistema – Proporciona información sobre eventos del sistema.

Registro de acceso – Enumera todos los intentos fallidos de acceder al producto. También se puede configurar el registro de acceso para obtener una lista de todas las conexiones al producto (consulte a continuación).

Ver informe del servidor – Proporciona información acerca del estado del producto en una ventana emergente. El registro de acceso se incluye automáticamente en el informe del servidor.

Descargar informe del servidor – Crea un archivo .zip que incluye un archivo de texto en formato UTF–8 con un informe completo del servidor. Seleccione la opción **Incluir captura desde visualización en directo** para incluir una instantánea de la visualización en directo del producto. El archivo .zip debe adjuntarse siempre que se contacte con el servicio técnico.

Lista de parámetros – Muestra los parámetros del producto y su configuración actual. Puede resultar útil para solucionar problemas o al ponerse en contacto con el servicio técnico de Axis.

Lista de conexiones – Enumera a todos los clientes que están accediendo actualmente a transmisiones de medios.

Informe de fallos – Genera un archivo con la información de depuración. El informe tarda varios minutos en generarse.

Los niveles de registro para los registros del sistema y de acceso se configuran en **Setup > Additional Controller Configuration > System Options > Support > Logs & Reports > Configuration (Configuración > Configuración del controlador adicional > Opciones del sistema > Soporte > Informes y registros > Configuración)**. El registro de acceso se puede configurar para obtener una lista de todas las conexiones al producto (seleccione Críticas, advertencias e información).

Avanzada

Secuencias de comandos

Las secuencias de comandos permiten a los usuarios experimentados personalizar y utilizar sus propias secuencias de comandos.

AVISO

Un uso incorrecto puede causar comportamientos inesperados y pérdida de contacto con el producto de Axis.

Axis recomienda encarecidamente no utilizar esta función, a menos que se comprendan las consecuencias. El servicio técnico de Axis no proporciona asistencia para problemas relacionados con secuencias de comandos personalizadas.

Para abrir el editor de secuencias de comandos, vaya a **Setup > Additional Controller Configuration > System Options > Advanced > Scripting (Configuración > Configuración de controlador adicional > Opciones del sistema > Avanzadas > Secuencias de comandos)**. Si una secuencia de comandos causa problemas, restablezca el producto a su configuración predeterminada de fábrica; consulte *página 65*.

Para obtener más información, visite *www.axis.com/developer*.

Carga de archivos

Se pueden cargar archivos, como páginas web e imágenes, en el producto de Axis y utilizarlos como ajustes personalizados. Para cargar un archivo, vaya a **Setup > Additional Controller Configuration > System Options > Advanced > File Upload (Configuración > Configuración de controlador adicional > Opciones del sistema > Avanzadas > Cargar archivos)**.

Se puede acceder a los archivos cargados en `http://<dirección IP>/local/<usuario>/<nombre de archivo>`, donde `<usuario>` es el grupo del usuario seleccionado (administrador) para el archivo cargado.

Restablecimiento a la configuración predeterminada de fábrica

Importante

Es preciso tener cuidado si se va a restablecer la configuración predeterminada de fábrica. Todos los valores, incluida la dirección IP, se restablecerán a la configuración predeterminada de fábrica.

Para restablecer el producto a la configuración predeterminada de fábrica:

1. Desconecte la alimentación del producto.

2. Mantenga pulsado el botón de control mientras vuelve a conectar la alimentación. Consulte *Información general del producto en la página 3*.
3. Mantenga pulsado el botón de control durante 25 segundos hasta que el indicador LED de estado se ponga en ámbar por segunda vez.
4. Suelte el botón de control. El proceso finaliza cuando el indicador LED de estado se pone verde. El producto se ha restablecido a la configuración predeterminada de fábrica. Si no hay ningún servidor DHCP disponible en la red, la dirección IP predeterminada será `192.168.0.90`.
5. Utilice las herramientas del software de instalación y gestión para asignar una dirección IP, establecer la contraseña y acceder al producto.

También es posible restablecer los parámetros a los valores predeterminados de fábrica mediante la interfaz web. Vaya a **Setup > Additional Controller Configuration > Setup > System Options > Maintenance (Configuración > Configuración del dispositivo adicional > Opciones del sistema > Opciones del sistema > Mantenimiento)** y haga clic en **Default (Predeterminado)**.

Solución de problemas

Cómo comprobar el firmware actual

El firmware es un tipo de software que determina la funcionalidad de los dispositivos de red. Una de las acciones que deberá llevar a cabo en primer lugar a la hora de solucionar problemas será comprobar la versión actual del firmware. La versión más reciente podría contener una corrección que solucione su problema concreto.

La versión de firmware actual instalada en el producto de Axis se muestra en la página de vista general.

Cómo actualizar el firmware

Importante

- Su distribuidor se reserva el derecho de realizar cobros por cualquier reparación relativa a una actualización incorrectamente realizada por el usuario.
- Al actualizar el firmware se guarda la configuración preconfigurada y personalizada (en caso de que esta función esté disponible en el firmware), si bien Axis Communications AB no puede garantizarlo.
- Si instala una versión de firmware anterior, a continuación deberá restablecer el producto a la configuración predeterminada de fábrica.

Nota

- Una vez finalizado el proceso de actualización, el producto se reinicia automáticamente. Si reinicia manualmente el producto después de la actualización, espere 5 minutos, incluso si sospecha que la actualización ha fallado.
- Puesto que la base de datos de usuarios, grupos, credenciales y otros datos se actualiza con la actualización del firmware, el primer inicio puede tardar unos minutos en completarse. El tiempo necesario dependerá de la cantidad de datos.
- Al actualizar el producto de Axis con el firmware más reciente, el producto obtiene las últimas funciones disponibles. Lea siempre las instrucciones de actualización y las notas de versión disponibles en cada nueva versión antes de actualizar el firmware.

Controladores de puerta independientes:

1. Descargue a su ordenador el último archivo de firmware, disponible de forma gratuita en *www.axis.com/support*
2. Acceda a **Setup > Additional Controller Configuration > System Options > Maintenance (Configuración > Configuración de controlador adicional > Opciones del sistema > Mantenimiento)** en la página web del producto.
3. Bajo **Upgrade Server (Actualizar servidor)**, haga clic en **Choose file (Elegir archivo)** y localice el archivo en su equipo.
4. Si desea que el producto se restablezca automáticamente a los ajustes predeterminados de fábrica, al terminar la actualización marque la casilla de verificación **Default (Predeterminada)**.
5. Haga clic en **Upgrade (Actualizar)**.
6. Espere alrededor de 5 minutos a que el producto se actualice y se reinicie. A continuación, borre la caché del navegador.
7. Acceda al producto.

Controladores de puerta en un sistema:

Puede utilizar AXIS Device Manager o AXIS Camera Station para actualizar todos los controladores de puerta en un sistema. Visite *www.axis.com* para obtener más información.

Importante

- No seleccione la actualización secuencial.

Solución de problemas

Nota

- Todos los controladores de un sistema deben tener siempre la misma versión de firmware.
- Actualice todos los controladores en un sistema al mismo tiempo empleando la opción paralela en AXIS Device Manager o AXIS Camera Station.

Procedimiento de recuperación de emergencia

Si la conexión de alimentación o de red se pierde durante la actualización, se produce un error en el proceso y es posible que el producto no responda. El indicador de estado parpadea en rojo para señalar el error en la actualización. Para la recuperación del producto, siga estos pasos. El número de serie se encuentra en la etiqueta del producto.

1. En **UNIX/Linux**, escriba lo siguiente desde la línea de comandos:

   ```
   arp -s <dirección IP> <número de serie> temp
   ping -l 408 <dirección IP>
   ```

   En **Windows**, escriba lo siguiente en el símbolo de sistema/DOS Prompt (puede ser necesario ejecutar la línea de comandos como administrador):

   ```
   arp -s <dirección IP> <número de serie>
   ping -l 408 -t <dirección IP>
   ```

2. Si el producto no responde en 30 segundos, reinícielo y espere la respuesta. Pulse CTRL+C para detener el ping.
3. Abra un navegador y escriba la dirección IP del producto. En la página que se abrirá, utilice el botón **Browse (Examinar)** para seleccionar el archivo de actualización que se utilizará. A continuación, haga clic en **Load (Cargar)** para reiniciar el proceso de actualización.
4. Tras la actualización (entre 1 y 10 minutos), el producto se reinicia automáticamente y se muestra una luz verde fija en el indicador de estado.
5. Vuelva a instalar el producto de acuerdo con la guía de instalación.

Si tras el procedimiento de recuperación de emergencia no se logra que el producto vuelva a estar listo y en funcionamiento, póngase en contacto con el soporte técnico de Axis en *www.axis.com/support*

Síntomas, posibles causas y soluciones

Problemas al actualizar el firmware	
Error durante la actualización del firmware	Cuando se produce un error en la actualización del firmware, el producto vuelve a cargar el firmware anterior. Compruebe el archivo de firmware e inténtelo de nuevo.

Problemas al configurar la dirección IP	
Al utilizar ARP/Ping	Vuelva a intentar la instalación. La dirección IP debe establecerse durante un intervalo de dos minutos desde que se proporciona alimentación eléctrica al producto. Asegúrese de que la longitud de ping está establecida en 408. Para obtener instrucciones, consulte la guía de instalación en la página del producto en *axis.com*.
El producto se encuentra en una subred distinta	Si la dirección IP prevista para el producto y la dirección IP del ordenador utilizado para acceder al producto se encuentran en subredes distintas, no se podrá configurar la dirección IP. Póngase en contacto con el administrador de red para obtener una dirección IP.

Solución de problemas

La dirección IP ya la utiliza otro dispositivo	Desconecte el producto de Axis de la red. Ejecute el comando ping (en una ventana de comando/DOS, escriba `ping` y la dirección IP del producto): • Si recibe: `Reply from <IP address>: bytes=32; time=10...` significa que la dirección IP podría estar en uso por otro dispositivo de la red. Solicite una nueva dirección IP al administrador de red y vuelva a instalar el producto. • Si recibe: `Request timed out`, significa que la dirección IP está disponible para su uso con el producto de Axis. Compruebe el cableado y vuelva a instalar el producto.
Posible conflicto de dirección IP con otro dispositivo de la misma subred	Se utiliza la dirección IP estática del producto de Axis antes de que el servidor DHCP configure una dirección dinámica. Esto significa que, si otro dispositivo utiliza la misma dirección IP estática predeterminada, podría haber problemas para acceder al producto.

No se puede acceder al producto desde un navegador

No se puede iniciar sesión	Cuando HTTPS esté activado, asegúrese de que se utiliza el protocolo correcto (HTTP o HTTPS) al intentar iniciar sesión. Puede que tenga que escribir manualmente `http` o `https` en el campo de dirección del navegador. Si se pierde la contraseña del directorio raíz del usuario, habrá que restablecer el producto a su configuración predeterminada de fábrica. Consulte *Restablecimiento a la configuración predeterminada de fábrica en la página 65*.
El servidor DHCP ha cambiado la dirección IP	Las direcciones IP obtenidas de un servidor DHCP son dinámicas y pueden cambiar. Si la dirección IP ha cambiado, acceda a la utilidad AXIS IP Utility o AXIS Device Manager para localizar el producto en la red. Identifique el producto utilizando el modelo o el número de serie, o por su nombre de DNS (si se ha configurado el nombre). Si es necesario, se puede asignar una dirección IP estática manualmente. Para obtener instrucciones, consulte el documento *Cómo asignar una dirección IP y acceder al dispositivo* en la página de producto en *axis.com*
Error de certificado cuando se utiliza IEEE 802.1X	Para que la autenticación funcione correctamente, la configuración de fecha y hora del producto de Axis se debe sincronizar con un servidor NTP. Consulte *Fecha y hora en la página 57*.

Se puede acceder al producto localmente pero no externamente

Configuración del router	Para configurar el router a fin de permitir el tráfico de datos entrantes al producto Axis, active la función de NAT transversal, que tratará de configurar automáticamente el router para permitir el acceso al producto Axis, consulte *NAT transversal (asignación de puertos) para IPv4 en la página 61*. El router debe admitir UPnP®.
Protección de firewall	Pida al administrador de red que compruebe el firewall de Internet.
Se requieren routers predeterminados	Compruebe si debe configurar el router en **Setup > Network Settings (Configuración > Ajustes de red)** o **Setup > Additional Controller Configuration > System Options > Network > TCP/IP > Basic (Configuración > Configuración de controlador adicional > Opciones del sistema > Red > TCP/IP > Básica)**.

Los indicadores LED de red y de estado parpadean en rojo rápidamente

Error de hardware	Póngase en contacto con su distribuidor de Axis.

El producto no se inicia

El producto no se inicia	Si el producto no se inicia, mantenga el cable de red conectado y vuelva a introducir el cable de alimentación en el midspan.

Especificaciones

Conectores

Para obtener más información sobre las posiciones de los conectores, consulte .

Para ver los diagramas de conexión y obtener información sobre el gráfico de pines del hardware generado mediante la configuración de hardware, consulte *Diagramas de conexión en la página 74* y *Configuración del hardware en la página 13*.

En la siguiente sección, se describen las especificaciones técnicas de los conectores.

Conector de datos del lector

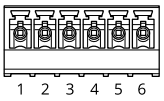
Bloque de terminales de 6 pines compatibles con los protocolos RS485 y Wiegand para la comunicación con el lector.

Los puertos RS485 admiten:

- Semidúplex RS485 de dos cables
- Dúplex completo RS485 de cuatro cables

Los puertos Wiegand admiten:

- Wiegand de dos cables



Función		Pin	Notas
RS485	A-	1	Para dúplex completo RS485 Para semidúplex RS485
	B+	2	
RS485	A-	3	Para dúplex completo RS485 Para semidúplex RS485
	B+	4	
Wiegand	D0 (datos 0)	5	Para Wiegand
	D1 (datos 1)	6	

Importante

Los puertos RS485 tienen una tasa de transmisión fija de 9600 bit/s.

Importante

La longitud de cable máxima recomendada es 30 m.

Importante

Los circuitos de salida de esta sección son de alimentación limitada de Clase 2.

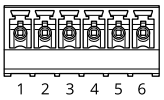
Conector de E/S del lector

Bloque de terminales de 6 pines para:

- Alimentación auxiliar (salida de CC)
- Entrada digital

- Salida digital
- 0 V CC (-)

Los 3 pines de los conectores de E/S del lector se pueden supervisar. Si se interrumpe la conexión, se activa un evento. Para usar entradas supervisadas, instale las resistencias de final de línea. Use el diagrama de conexión para las entradas supervisadas. Consulte *página 75*.



Función	Pin	Notas	Especificaciones
0 V CC (-)	1		0 V CC
Salida de CC	2	Para alimentar el equipo auxiliar. Nota: Este pin solo se puede utilizar como salida de alimentación.	12 V CC Carga máx. = 300 mA
Configurable (entrada o salida)	3–6	Entrada digital: conéctela al pin 1 para activarla o bien déjela suelta (desconectada) para desactivarla.	De 0 a 40 V CC máx.
		Salida digital: conéctela al pin 1 para activarla o bien déjela suelta (desconectada) para desactivarla. Si se utiliza con una carga inductiva (por ejemplo, un relé), debe conectarse un diodo en paralelo a la carga como protección ante transitorios de tensión.	De De 0 a 40 V CC máx., colector abierto, 100 mA

Importante

La longitud de cable máxima recomendada es 30 m.

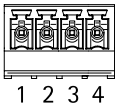
Importante

Los circuitos de salida de esta sección son de alimentación limitada de Clase 2.

Conector de puerta

Dos bloques de terminales de 4 pines para dispositivos de monitor de puerta (entrada digital).

Todos los pines de entrada de las puertas se pueden supervisar. Si se interrumpe la conexión, se activa una alarma. Para usar entradas supervisadas, instale las resistencias de final de línea. Use el diagrama de conexión para las entradas supervisadas. Consulte *página 75*.



Función	Pin	Notas	Especificaciones
0 V CC (-)	1, 3		0 V CC
Entrada	2, 4	Para comunicarse con el monitor de puerta. Entrada digital: conecte con el pin 1 o 3 respectivamente para activar o dejar suelta (desconectada) para desactivar. Nota: Este pin solo se puede utilizar como entrada.	De 0 a 40 V CC máx.

Importante

La longitud de cable máxima recomendada es 30 m.

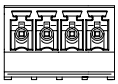
Especificaciones

Conector auxiliar

Bloque de terminales de E/S configurable de 4 pines para:

- Alimentación auxiliar (salida de CC)
- Entrada digital
- Salida digital
- 0 V CC (-)

Para ver un ejemplo del diagrama de conexiones, consulte *Diagramas de conexión en la página 74*.



Función	Pin	Notas	Especificaciones
0 V CC (-)	1		0 V CC
Salida de CC	2	Para conectar el equipo auxiliar. Nota: Este pin solo se puede utilizar como salida de alimentación.	3,3 V CC Carga máx. = 100 mA
Configurable (entrada o salida)	3–4	Entrada digital: conéctela al pin 1 para activarla o bien déjela suelta (desconectada) para desactivarla.	De 0 a 40 V CC máx.
		Salida digital: conéctela al pin 1 para activarla o bien déjela suelta (desconectada) para desactivarla. Si se utiliza con una carga inductiva (por ejemplo, un relé), debe conectarse un diodo en paralelo a la carga como protección ante transitorios de tensión.	De De 0 a 40 V CC máx., colector abierto, 100 mA

Importante

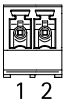
La longitud de cable máxima recomendada es 30 m.

Importante

Los circuitos de salida de esta sección son de alimentación limitada de Clase 2.

Conector de alimentación

Bloque de terminales de 2 pines para la entrada de alimentación de CC. Use una fuente de alimentación limitada (LPS) que cumpla los requisitos de tensión muy baja de seguridad (SELV) con una potencia nominal de salida limitada a ≤100 W o una corriente nominal de salida limitada a ≤5 A.



Función	Pin	Notas	Especificaciones
0 V CC (-)	1		0 V CC
Entrada de CC	2	Para alimentar el controlador cuando no se use la alimentación a través de Ethernet. Nota: Este pin solo se puede utilizar como entrada de alimentación.	10–28 V CC, máx. 36 W Carga máxima en salidas = 14 W

Especificaciones

Conector de red

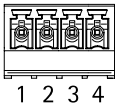
Conector Ethernet RJ45. Use cables de categoría 5e o superior.

Función	Especificaciones
Alimentación y Ethernet	Alimentación a través de Ethernet IEEE 802.3af802.3at Tipo 1 Clase 3, 44–57 V CC Carga máxima en las salidas = 7,5 W

Conector de alimentación de cerradura

Bloque de terminales de 4 pines para proporcionar alimentación a una o dos cerraduras (salida de CC). Este conector de bloqueo también podría usarse para proporcionar alimentación a dispositivos externos.

Conecte las cerraduras y las cargas a los pines según el gráfico de pines del hardware generado mediante la configuración de hardware.



Función	Pin	Notas	Especificaciones
0 V CC (-)	1, 3		0 V CC
0 V CC, suelto o 12 V CC	2, 4	Para controlar hasta dos bloqueos de 12 V. Uso del gráfico de pines del hardware. Consulte *Configuración del hardware en la página 13*.	12 V CC Carga máx. total = 500 mA

AVISO

Si la cerradura no está polarizada, le recomendamos añadir un diodo de regreso externo.

Importante

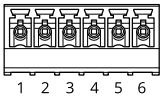
Los circuitos de salida de esta sección son de alimentación limitada de clase 2.

Conector de alimentación y relé

Bloque de terminales de 6 pines con relé integrado para:

- Dispositivos externos
- Alimentación auxiliar (salida de CC)
- 0 V CC (-)

Conecte las cerraduras y las cargas a los pines según el gráfico de pines del hardware generado mediante la configuración de hardware.



Función	Pin	Notas	Especificaciones
0 V CC (-)	1, 4		0 V CC

Relé	2–3	Para conectar dispositivos de relés. Uso del gráfico de pines del hardware. Consulte *Configuración del hardware en la página 13*. Los dos pines de relé están separados de forma galvanizada del resto del circuito.	Corriente máxima = 700 mA Tensión máxima = +30 V CC
12 V CC	5	Para alimentar el equipo auxiliar. Nota: Este pin solo se puede utilizar como salida de alimentación.	Tensión máxima = +12 V CC Carga máxima = 500 mA
24 V CC	6	No se utiliza	

AVISO

Si la cerradura no está polarizada, le recomendamos añadir un diodo de regreso externo.

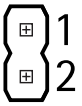
Importante

Los circuitos de salida de esta sección son de alimentación limitada de clase 2.

Cabezal con pines de la alarma antimanipulación

Dos cabezales con dos pines para funciones de bypass:

- Alarma antimanipulación posterior (TB)
- Alarma de manipulación frontal (TF)



Función	Pin	Notas
Alarma antimanipulación posterior	1–2	Para hacer el bypass simultáneamente a las alarmas de manipulación delantera y trasera, coloque puentes entre TB 1, TB 2 y TF 1, TF 2, respectivamente. Al aplicar un bypass a las alarmas antimanipulación, el sistema no identificará ningún intento de manipulación.
Alarma antimanipulación delantera	1–2	

Nota

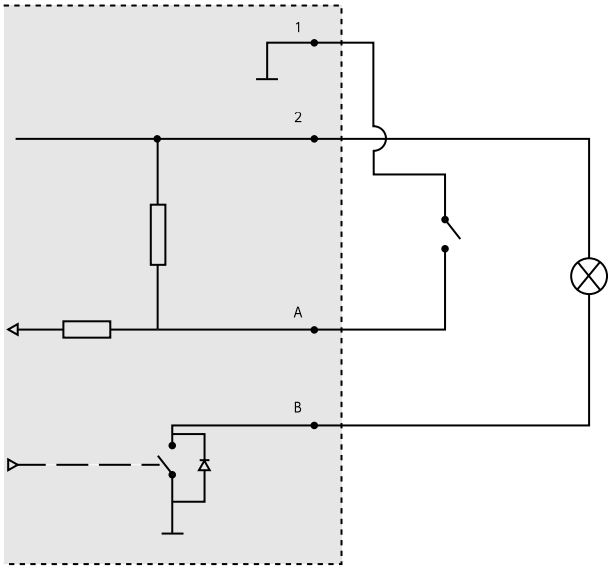
Las alarmas antimanipulación delantera y la trasera están conectadas de forma predeterminada. El activador de carcasa abierta se puede configurar para que realice una acción si el controlador de puerta está abierto o si se ha retirado de la pared o el techo. Para obtener más información sobre cómo configurar alarmas y eventos, consulte *Configuración de eventos y alarmas en la página 45*.

Diagramas de conexión

Conecte los dispositivos según el gráfico de pines del hardware generado mediante la configuración de hardware. Para obtener más información sobre la configuración del hardware y el gráfico de pines del hardware, consulte *Configuración del hardware en la página 13*.

Especificaciones

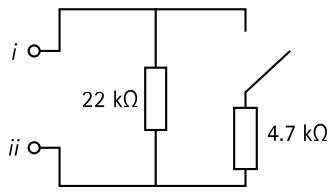
Conector auxiliar



1 *0 V CC (-)*
2 *Salida de CC: 3,3 V, máx 100 mA*
A *E/S configurada como entrada*
B *E/S configurada como salida*

Entradas supervisadas

Para usar entradas supervisadas, instale resistencias de final de línea según el siguiente diagrama.



i *Entrada*

ii *0 V CC (-)*

Nota

Se recomienda el uso de cables trenzados y blindados. Conecte el blindaje a 0 V CC.

Información de seguridad

Niveles de peligro

⚠PELIGRO

Indica una situación peligrosa que, si no se evita, provocará lesiones graves o la muerte.

⚠ADVERTENCIA

Indica una situación peligrosa que, si no se evita, puede provocar lesiones graves o la muerte.

⚠PRECAUCIÓN

Indica una situación peligrosa que, si no se evita, puede provocar lesiones moderadas o leves.

AVISO

Indica una situación peligrosa que, si no se evita, puede provocar daños materiales.

Otros niveles de mensaje

Importante

Indica información importante que es fundamental para que el producto funcione correctamente.

Nota

Indica información útil que ayuda a aprovechar el producto al máximo.

Manual del usuario
AXIS A1001 & AXIS Entry Manager

Ver. M25.2
Fecha: Diciembre 2023
N.º de pieza T10010336