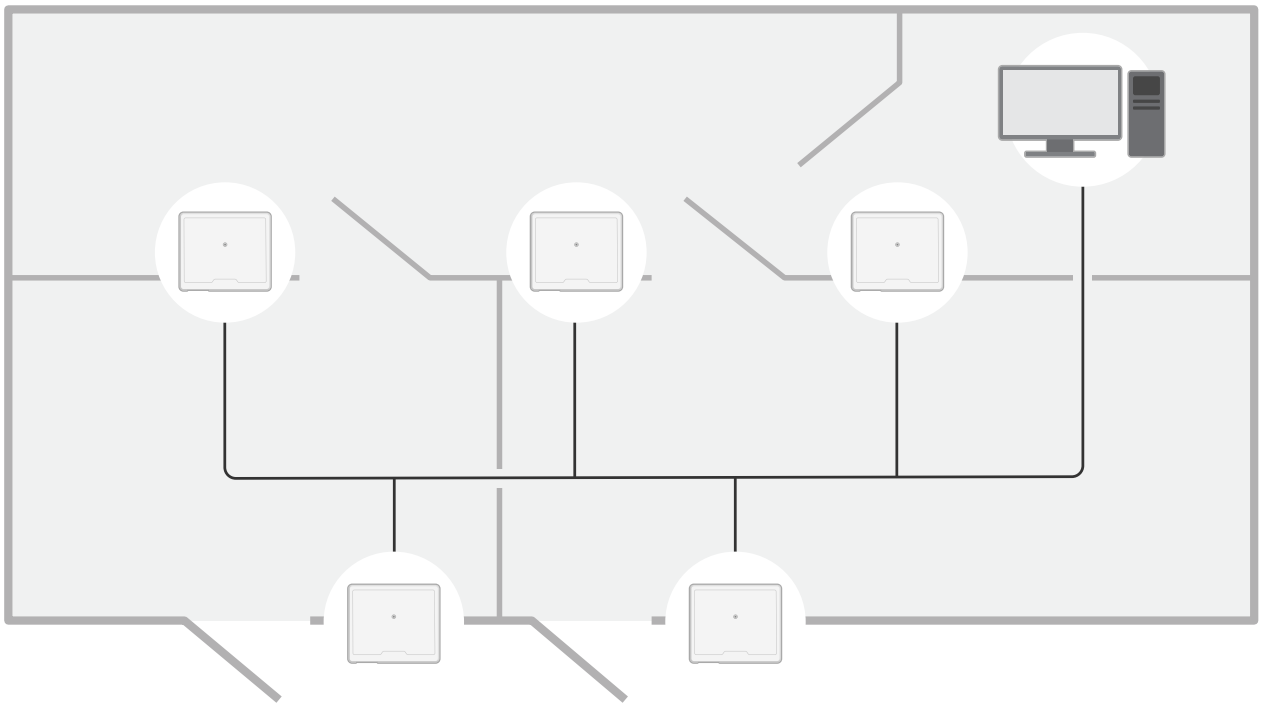
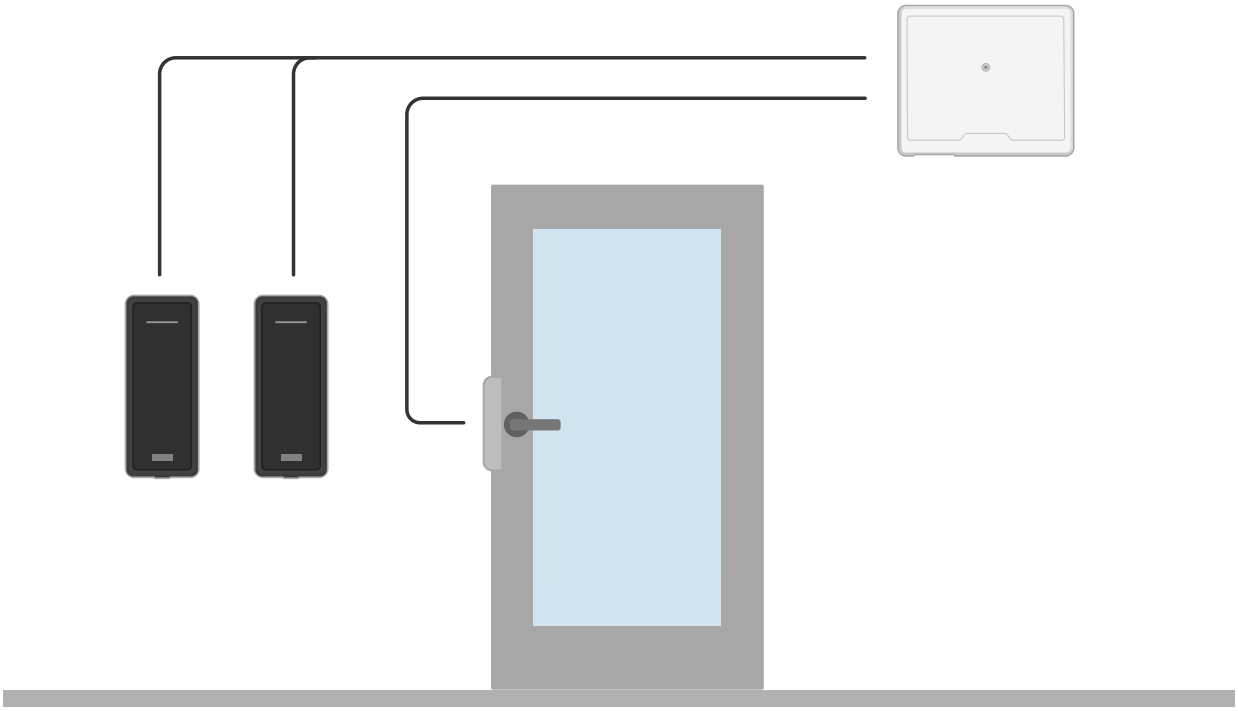
Índice

Presentación esquemática de la solución 2
Instalación 3
..... 3
Cómo funciona 4
Localice el dispositivo en la red 4
Compatibilidad con navegadores 4
Abrir la interfaz web del dispositivo 4
Crear una cuenta de administrador 4
Contraseñas seguras 5
Asegúrese de que no se ha manipulado el software del dispositivo 5
Información general de la interfaz web 5
Configure su dispositivo 6
Door override (Anulación de puerta) 6
Perfil LED OSDP 6
Formato de tarjeta 7
Interfaz web 9
Descubrir más 10
Ciberseguridad 10
SO firmado 10
Arranque seguro 10
Axis Edge Vault 10
ID de dispositivo de Axis 10
Especificaciones 11
Guía de productos 11
..... 11
Indicadores LED 11
Botones 12
Botón de control 12
Conectores 12
Conector de red 12
Prioridad de potencia 12
Conector de lector 12
Conector de puerta 14
Conector de relé 14
Conector auxiliar 15
Conector externo 16
Conector de alimentación 17
Entradas con supervisión 17
Localización de problemas 18
Restablezca la configuración predeterminada de fábrica 18
Opciones de AXIS OS 18
Comprobar la versión de AXIS OS 18
Actualización de AXIS OS 19
Problemas técnicos y posibles soluciones 19
Contactar con la asistencia técnica 21
Ciberseguridad 22
Gestión de las vulnerabilidades 22
Notificaciones de seguridad 22
Ciclo de vida seguro del producto 22

Presentación esquemática de la solución



El controlador de puerta en red se puede conectar fácilmente y recibirá alimentación de su red IP ya existente sin necesidad de cableado especial.



Cada controlador de puerta en red es un dispositivo inteligente fácil de montar junto a una puerta. Puede proporcionar alimentación y controlar hasta dos lectores.

Instalación



Cómo funciona

Localice el dispositivo en la red

Para localizar dispositivos de Axis en la red y asignarles direcciones IP en Windows®, utilice AXIS IP Utility o AXIS Device Manager. Ambas aplicaciones son gratuitas y pueden descargarse desde *axis.com/support*.

Para obtener más información acerca de cómo encontrar y asignar direcciones IP, vaya a *How to assign an IP address and access your device (Cómo asignar una dirección IP y acceder al dispositivo)*.

Compatibilidad con navegadores

Puede utilizar el dispositivo con los siguientes navegadores:

	Chrome™	Edge™	Firefox®	Safari®
Windows®	✓	✓	*	*
macOS®	✓	✓	*	*
Linux®	✓	✓	*	*
Otros sistemas operativos	*	*	*	*

✓: Recomendado

*: Asistencia con limitaciones

Abrir la interfaz web del dispositivo

1. Abra un navegador y escriba la dirección IP o el nombre de host del dispositivo Axis.
   Si desconoce la dirección IP, use AXIS IP Utility o AXIS Device Manager para localizar el dispositivo en la red.
2. Escriba el nombre de usuario y la contraseña. Si accede al dispositivo por primera vez, debe crear una cuenta de administrador. Consulte *Crear una cuenta de administrador, on page 4*.

Para obtener descripciones de todas las funciones y ajustes de la interfaz web de los dispositivos con AXIS OS, consulte la *AXIS OS web interface help (Ayuda de la interfaz web de AXIS OS)*.

Crear una cuenta de administrador

La primera vez que inicie sesión en el dispositivo, debe crear una cuenta de administrador.

1. Introduzca una cuenta.
2. Introduzca una contraseña. Consulte *Contraseñas seguras, on page 5*.
3. Vuelva a escribir la contraseña.
4. Aceptar el acuerdo de licencia.
5. Haga clic en **Add account (agregar cuenta)**.

Importante

El dispositivo no tiene una cuenta predeterminada. Si pierde la contraseña de la cuenta de administrador, debe restablecer el dispositivo. Consulte *Restablezca la configuración predeterminada de fábrica, on page 18*.

Contraseñas seguras

Importante

Utilice HTTPS (habilitado por defecto) para establecer su contraseña u otras configuraciones confidenciales a través de la red. El protocolo HTTPS habilita conexiones a la red seguras y cifradas, protegiendo así los datos confidenciales, como las contraseñas.

La contraseña del dispositivo es la principal protección para sus datos y servicios. Los dispositivos de Axis no imponen una política de contraseñas ya que pueden utilizarse en distintos tipos de instalaciones.

Para proteger sus datos le recomendamos encarecidamente que:

- Utilice una contraseña con al menos 8 caracteres, creada preferiblemente con un generador de contraseñas.
- No exponga la contraseña.
- Cambie la contraseña a intervalos periódicos y al menos una vez al año.

Asegúrese de que no se ha manipulado el software del dispositivo

Para asegurarse de que el dispositivo tiene el AXIS OS original o para volver a controlar el dispositivo tras un incidente de seguridad:

1. Restablezca la configuración predeterminada de fábrica. Consulte *Restablezca la configuración predeterminada de fábrica, on page 18*.
   Después de un restablecimiento, el inicio seguro garantiza el estado del dispositivo.
2. Configure e instale el dispositivo.

Información general de la interfaz web

Este vídeo le ofrece información general de la interfaz web del dispositivo.



Interfaz web del dispositivo Axis

Configure su dispositivo

Para obtener información sobre cómo configurar su dispositivo, consulte el *manual del usuario de AXIS Camera Station* o soluciones de terceros.

Door override (Anulación de puerta)

Importante

Esta función controla directamente los relés de las puertas y anula la configuración de los relés en AXIS Camera Station. Úselo únicamente si el soporte técnico de Axis se lo ha indicado.

1. Detenga el servicio Secure Entry en AXIS Camera Station.
2. En la interfaz web del controlador de puerta, vaya a **Advanced (Avanzado) > Door override (Anulación de puerta)**.
3. Lea atentamente la información de la página y, a continuación, haga clic en **I understand (Entendido)**.
4. Encienda la **Door override (Anulación de puerta)** y haga clic en **Enable (Habilitar)**.
5. Diríjase al relé de la puerta, haga clic en **Lock (Bloquear)**, **Unlock (Desbloquear)** o **Access (Acceso)** para bloquear la puerta, desbloquear la puerta o conceder acceso.
6. Diríjase al relé que desea configurar y haga clic en **Activate (Activar)** o **Deactivate (Desactivar)** para activar o desactivar el relé.

Perfil LED OSDP

Puede personalizar los perfiles de los LED de su lector OSDP para definir las luces y los sonidos que se utilizan en función de los distintos eventos. Para consultar la lista completa de perfiles, véase *LED profiles (Perfiles LED)*.

Establecer niveles de luz y audio

1. Vaya a **Peripherals (Periféricos)** > **Readers (Lectores)** > **OSDP LED profile (Perfil LED OSDP)**.
2. Despliegue el menú **Light and audio levels (Niveles de luz y audio)**.
3. Utilice el control deslizante para ajustar la intensidad de la tira de LED, la retroiluminación LED y el sonido.
4. Haga clic en **Save (Guardar)**.

Nota

Al cambiar los niveles de luz y audio, los ajustes se actualizan en todos los lectores conectados al controlador.

Comprobar los ajustes de los LED del OSDP:

Puede utilizar el menú **OSDP LED test (Prueba LED de OSDP)** para consultar los ajustes de audio e iluminación de cualquiera de sus perfiles de lector.

Para comprobar los ajustes de sus perfiles LED de OSDP:

1. Vaya a **Peripherals (Periféricos)** > **Readers (Lectores)** > **OSDP LED profile (Perfil LED OSDP)**.
2. Despliegue el menú **OSDP LED test (Prueba LED de OSDP)**.
3. Elija un indicador LED.
4. Elija el lector que desea probar.
5. Haga clic en **Iniciar**.
6. Haga clic **Edit feedback (Editar respuesta)** para cambiar los ajustes de luz y audio de su perfil.
   - Elija un nuevo color en el menú desplegable **Color**.
   - Elija una frecuencia de audio en el menú desplegable **Audio**, si procede.

- También puede restablecer los ajustes del perfil haciendo clic en **Reset to default values (Restablecer valores predeterminados)**.
- Haga clic en **Save (Guardar)**.

Cambiar los ajustes del perfil LED de OSDP:

1. Vaya a **Peripherals (Periféricos)** > **Readers (Lectores)** > **OSDP LED profile (Perfil LED OSDP)**.
2. Acceda al **OSDP LED profile (Perfil LED de OSDP)**.
3. Haga clic en  junto al perfil que desea editar.
4. Edite los ajustes correspondientes:
   - Elija el comportamiento que seguirán sus LED en el menú desplegable **Behaviour (Comportamiento)**.
   - Elija el color de sus LED en el menú desplegable **Color**.
   - Establezca la **Duration on (Duración de encendido)** y la **Duration off (Duración de apagado)** de sus LED.
   - Establezca la **Recurrence (Periodicidad)** de la respuesta del LED.
   - En el menú desplegable **Audio**, elija la **Beep duration, on (Duración del pitido, encendido)** y la **Beep duration, off (Duración del pitido, apagado)** y determine la**Recurrence (Periodicidad)** de la respuesta del avisador acústico. Asegúrese de que la **Beep duration, on (Duración del pitido, encendido)** y la **Beep duration, off (Duración del pitido, apagado)** sean iguales.
5. Haga clic en **Save (Guardar)**.

Importar ajustes existentes desde otro controlador

1. Vaya a **Peripherals (Periféricos)** > **Readers (Lectores)** > **OSDP LED profile (Perfil LED OSDP)**.
2. Haga clic en **Import (Importar)**.
3. Seleccione el archivo que desea subir.
4. Haga clic en **Import (Importar)**.

Exportar los ajustes actuales

1. Vaya a **Peripherals (Periféricos)** > **Readers (Lectores)** > **OSDP LED profile (Perfil LED OSDP)**.
2. Haga clic en **Export (Exportar)**.
3. Elija dónde desea guardar el archivo JSON y haga clic en **Save (Guardar)**.

Formato de tarjeta

Esta función está destinada exclusivamente a usuarios expertos. En cuanto se encienda el **Card format (Formato de tarjeta**:

- Si utiliza una credencial de 37 bits, se eliminan los últimos 5 bits.
- Si utiliza una credencial de 64 bits (código QR), se elimina la primera secuencia de 24 bits.

Puede utilizar tanto los datos de ejemplo como el lector de tarjetas para ver las credenciales.

1. Vaya a **Advanced (Avanzado)** > **Card format (Formato de tarjeta)**.
2. Lee la advertencia y haz clic en **I understand (Lo entiendo)** para habilitar el **Card format (Formato de tarjeta)**.
3. En el menú desplegable **Reader data visualization (Visualización de datos del lector)**, elija su lector.
4. Haga clic en **Get reader data (Obtener datos del lector)** o en **Use sample data (Utilizar datos de ejemplo)** para generar una salida de tarjeta. Se aplicará a todos los titulares de tarjetas registrados en el dispositivo.

5. Active la opción **Trim reader data (Recortar datos del lector)** para eliminar los bits finales de las credenciales de la tarjeta.
6. Haga clic en **Enable (Activar)**.

Interfaz web

Para obtener información sobre todas las funciones y ajustes disponibles en la interfaz web de los dispositivos con AXIS OS, vaya a *AXIS OS web interface help (Ayuda de la interfaz web de AXIS OS)*.

Descubrir más

Ciberseguridad

Para obtener información sobre ciberseguridad específica de un producto, consulte la hoja de datos del producto en axis.com.

Para obtener información detallada sobre ciberseguridad en AXIS OS, lea la *Guía de endurecimiento de AXIS OS*.

SO firmado

El sistema operativo firmado lo implementa el proveedor del software que firma la imagen de AXIS OS con una clave privada. Cuando la firma se une al sistema operativo, el dispositivo validará el software antes de instalarlo. Si el dispositivo detecta que la integridad del software está comprometida, se rechazará la actualización de AXIS OS.

Arranque seguro

El arranque seguro es un proceso de arranque que consta de una cadena ininterrumpida de software validado criptográficamente, comenzando por la memoria inmutable (ROM de arranque). Al estar basado en el uso del sistema operativo firmado, el arranque seguro garantiza que un dispositivo pueda iniciarse solo con un software autorizado.

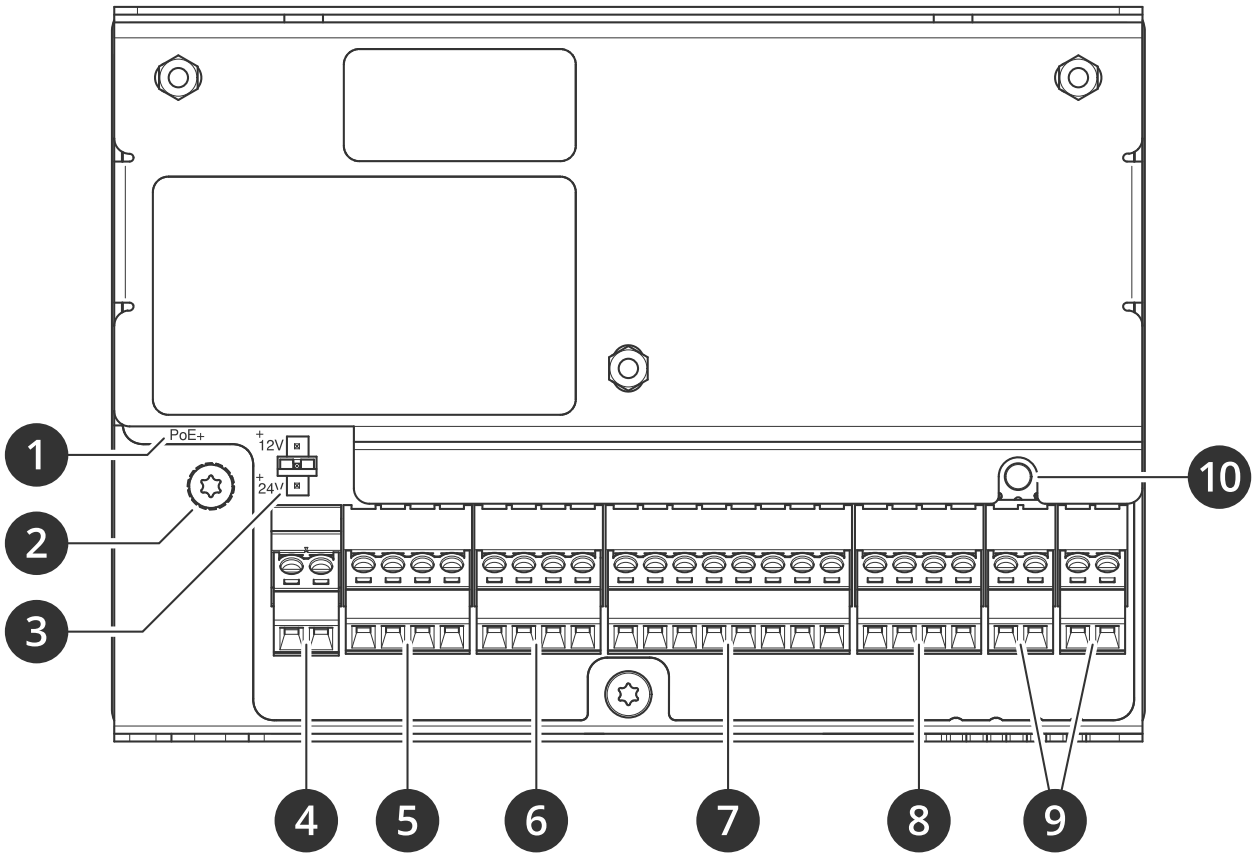
Axis Edge Vault

Axis Edge Vault es una plataforma de ciberseguridad basada en hardware que protege el dispositivo Axis. Ofrece características que garantizan la identidad e integridad del dispositivo y protegen su información confidencial frente a accesos no autorizados. Tiene dos sólidos pilares: los módulos de computación criptográfica (elemento seguro y TPM) y la seguridad del SoC (TEE y arranque seguro), combinados con una amplia experiencia en la seguridad de los dispositivos en el extremo.

ID de dispositivo de Axis

la posibilidad de verificar el origen del dispositivo es fundamental para poder confiar en su identidad. Durante la producción, se asigna a los dispositivos con Axis Edge Vault un certificado de ID de dispositivo de Axis único y conforme con el estándar IEEE 802.1AR en la propia fábrica. Es como una especie de pasaporte para demostrar el origen del dispositivo. El ID de dispositivo se guarda de forma segura y permanente en el almacén de claves seguro como certificado firmado por el certificado raíz de Axis. La infraestructura de TI del cliente puede utilizar el ID de dispositivo en la incorporación segura automatizada de dispositivos y en la identificación segura de dispositivos

Guía de productos



1 *Conector de red*
2 *Posición de toma de tierra*
3 *Puente de relé*
4 *Conector de alimentación*
5 *Conector de relé*
6 *Conector de puerta*
7 *Conector de lector*
8 *Conector auxiliar*
9 *Conectores externos*
10 *Botón de control*

Indicadores LED

LED	Color	Indicación
Estado	Verde	Fijo 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.
Red	Verde	Fijo para indicar una conexión a una red de 100 MBits/s. Parpadea para indicar actividad en la red.
	Ámbar;	Fijo para indicar una conexión a una red de 10 MBits/s. Parpadea para indicar actividad en la red.
	Apagado	No hay conexión a la red.

Alimentación	Verde	Funcionamiento normal.
	Ámbar;	Parpadea en verde/ámbar durante la actualización del firmware.
Relé	Verde	Relé activo.[1]
	Apagado	Relé inactivo.

Botones

Botón de control

El botón de control se utiliza para lo siguiente:

- Restablecer el producto a la configuración predeterminada de fábrica. Consulte *Restablezca la configuración predeterminada de fábrica, on page 18*.

Conectores

Conector de red

Conector Ethernet RJ45 con alimentación a través de Ethernet Plus (PoE+).

UL: La alimentación a través de Ethernet (PoE) debe suministrarse mediante un inyector de Ethernet IEEE 802.3af/802.3at Tipo 1 Clase 3 o de Ethernet Plus (PoE+) IEEE 802.3at Tipo 2 Clase 4 que suministra 44–57 V CC, 15,4/30 W. La alimentación a través de Ethernet (PoE) se ha evaluado mediante UL con un AXIS T8133 Midspan 30 W 1-port.

Prioridad de potencia

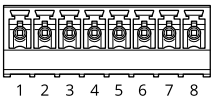
Este dispositivo puede recibir alimentación mediante una entrada de PoE o CC. Vea *Conector de red, on page 12* y *Conector de alimentación, on page 17*.

- Cuando PoE y CC se conectan antes de que se encienda el dispositivo, PoE se utiliza para la alimentación.
- PoE y CC están conectados y PoE está conectado actualmente. Cuando se pierde PoE, el dispositivo utiliza CC para proporcionar alimentación sin reiniciar.
- PoE y CC están conectados y CC está conectado actualmente. Cuando se pierde CC, el dispositivo se reinicia y utiliza PoE para proporcionar alimentación.
- Cuando se utiliza CC durante el inicio y se conecta PoE una vez que se ha iniciado el dispositivo, se utiliza CC para la alimentación.
- Cuando se utiliza PoE durante el inicio y se conecta CC una vez que se ha iniciado el dispositivo, se utiliza PoE para la alimentación.

Conector de lector

Un bloque de terminales de 8 pines, ambos compatibles con los protocolos OSDP y Wiegand para la comunicación con el lector.

Puede conectar hasta dos lectores OSDP (multipunto) o un lector Wiegand. Se reservan 500 mA a 12 V CC para todos los lectores conectados al controlador de puerta.



Configurado para un lector OSDP

1. *El relé está activo cuando COM está conectado a NO.*

Función	Pin	Nota	Especificaciones
Tierra CC (GND)	1		0 V CC
Salida de CC (+12 V)	2	Proporciona alimentación al lector.	12 V CC, máx. 500 mA
A	3	Semidúplex	
B	4	Semidúplex	

Configurado para dos lectores OSDP (multiconexión)

Función	Pin	Nota	Especificaciones
Tierra CC (GND)	1		0 V CC
Salida de CC (+12 V)	2	Proporciona alimentación a ambos lectores.	12 V CC, máx. 500 mA combinados para ambos lectores
A	3	Semidúplex	
B	4	Semidúplex	

Importante

- Cuando el controlador alimenta el lector, la longitud de cable cualificada es de hasta 200 m (656 ft). Verificado solo para lectores de Axis.
- Si el controlador no alimenta el lector, la longitud de cable cualificada para datos del lector es de hasta 1000 m (3280,8 ft) si se cumplen los siguientes requisitos de cable: 1 par trenzado con blindaje AWG 24, impedancia 120 ohm. Verificado solo para lectores de Axis.

Configurado para un lector Wiegand

Función	Pin	Nota	Especificaciones
Tierra CC (GND)	1		0 V CC
Salida de CC (+12 V)	2	Proporciona alimentación al lector.	12 V CC, máx. 500 mA
D0	3		
D1	4		
LED 1	5	LED rojo	
LED 2	6	LED verde	
MANIPULACIÓN	7	Entrada digital: conéctela al pin 1 para activarla, o bien déjela suelta (sin conectar) para desactivarla.	0 a máx. 30 V CC
AVISADOR ACÚSTICO	8	Salida digital: Si se utiliza con una carga inductiva, como un relé, conecte un diodo en paralelo a la carga como protección contra transitorios de tensión.	De 0 a 30 V CC máx., colector abierto, 100 mA

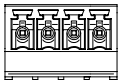
Importante

- Cuando el controlador alimenta el lector, la longitud de cable cualificada es de hasta 150 m.
- Si el controlador no alimenta el lector, la longitud de cable cualificada para datos del lector es de hasta 150 m si se cumple el siguiente requisito de cable: AWG 22.

Conector de puerta

Un bloque de terminales de 4 pines para dispositivos de monitor de puerta (entrada digital).

El monitor de puerta admite supervisión con resistencias de final de línea. Si se interrumpe la conexión, se activa una alarma. Para utilizar entradas con supervisión, debe instalar resistencias de fin de línea. Use el diagrama de conexión para las entradas supervisadas. Consulte *page 17*.



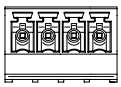
Función	Pin	Notas	Especificaciones
Tierra CC	1, 3		0 V CC
Entrada	2, 4	Para la comunicación con el monitor de la puerta. Entrada digital o entrada supervisada: conéctela al pin 1 o 3 respectivamente para activarla, o déjela flotando (desconectada) para desactivarla.	De 0 a 30 V CC máx.

Importante

La longitud de cable cualificada es de hasta 200 m (656 pies) si se cumplen los siguientes requisitos de cable: AWG 24.

Conector de relé

Un bloque de terminales de 4 pines para relés de forma de contacto C que se pueden utilizar, por ejemplo, para controlar una cerradura o una interfaz para una puerta.



Función	Pin	Notas	Especificaciones
Tierra CC (GND)	1		0 V CC
NO	2	Normalmente abierto. Para conectar dispositivos de relés. Conecte un bloqueo de seguridad negativa entre NO y masa CC. Los dos pines de relé se separan de forma galvanizada del resto del circuito si no se utilizan puentes.	Corriente máx. = 2 A Voltaje máx. = 30 V CC
COM	3	Común	

NC	4	Normalmente cerrado. Para conectar dispositivos de relés. Conecte un bloqueo de seguridad negativa entre NC y masa CC. Los dos pines de relé se separan de forma galvanizada del resto del circuito si no se utilizan puentes.	

Puente de alimentación de relé

Cuando el puente de alimentación de relé está colocado, conecta 12 V CC o 24 V CC al pin COM del relé.

Se puede utilizar para conectar una cerradura entre los pines GND y NO, o GND y NC.

Fuente de alimentación	Potencia máxima a 12 V CC	Potencia máxima a 24 V CC
ENTRADA DE CC	1600 mA	800 mA
PoE	900 mA	450 mA

AVISO

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

Conector auxiliar

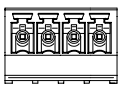
Utilice el conector auxiliar con dispositivos externos, por ejemplo, en combinación con detección de movimiento, activación de eventos y notificaciones de alarma. Además del punto de referencia de 0 V CC y la alimentación (salida de CC), el conector auxiliar ofrece la interfaz para:

Entrada digital – Conectar dispositivos que puedan alternar entre circuitos cerrados y abiertos, por ejemplo, sensores PIR, contactos de puertas y ventanas o detectores de cristales rotos.

Entrada supervisada – Permite detectar la manipulación de una señal digital.

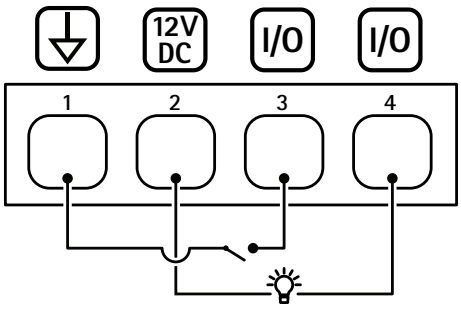
Salida digital – Conectar dispositivos externos como relés y LED. Los dispositivos conectados se pueden activar mediante la interfaz de programación de aplicaciones VAPIX® o desde la página web del producto.

Bloque de terminales de 4 pines



Función	Pin	Notas	Especificaciones
Tierra CC	1		0 V CC
Salida de CC	2	Se puede utilizar para alimentar equipos auxiliares. Nota: Este pin solo se puede utilizar como salida de alimentación.	12 V CC Carga máxima = 50 mA en total
Configurable (entrada o salida)	3-4	Entrada digital o entrada supervisada: conéctela al pin 1 para activarla o déjela suelta (sin conectar) para desactivarla. Para usar la entrada supervisada, instale las resistencias de final de línea. Consulte el diagrama de conexiones para obtener información sobre cómo conectar las resistencias.	De 0 a 30 V CC máx.

		Salida digital: conectada internamente a pin 1 (tierra CC) cuando está activa, y suelta (desconectada) cuando está inactiva. Si se utiliza con una carga inductiva, por ejemplo, un relé, conecte un diodo en paralelo a la carga como protección contra transitorios de tensión. Cada E/S puede conducir una carga externa de 12 V CC, 50 mA (máx. combinado), si se utiliza una salida interna de 12 V CC (pin 2). En caso de usar conexiones de colector abierto en combinación con una fuente de alimentación externa, las E/S pueden gestionar el suministro de CC de 0 – 30 V CC, 100 mA cada una.	De 0 a 30 V CC máx., colector abierto, 100 mA



1 *Tierra CC*
2 *Salida de CC 12 V*
3 *E/S configurada como entrada*
4 *E/S configurada como salida*

Conector externo

Dos bloques de terminales de 2 pines para seguridad positiva, como detectores de rotura de vidrio o de incendio.

UL: El conector no ha sido evaluado conforme a UL para el uso de una alarma antirrobo o antiincendios.



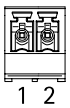
Función	Pin	Notas	Especificaciones
Tierra CC	1		0 V CC
MANIPULACIÓN	2	Entrada digital: conéctela al pin 1 para activarla, o bien déjela suelta (sin conectar) para desactivarla.	De 0 a 30 V CC máx.



Función	Pin	Notas	Especificaciones
Tierra CC	1		0 V CC
ALARMA	2	Entrada digital: conéctela al pin 1 para activarla, o bien déjela suelta (sin conectar) para desactivarla.	De 0 a 30 V CC máx.

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 seguridad de baja tensión (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
Tierra CC (GND)	1		0 V CC
Entrada CC	2	Para alimentar el dispositivo cuando no se use la alimentación a través de Ethernet. Nota: Este pin solo se puede utilizar como entrada de alimentación.	12 V CC, 36 W máx.

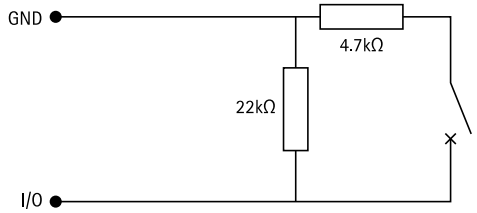
UL: Una fuente de alimentación UL 603 debe suministrar la alimentación de CC, en función de la aplicación, con las clasificaciones adecuadas.

Entradas con supervisión

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

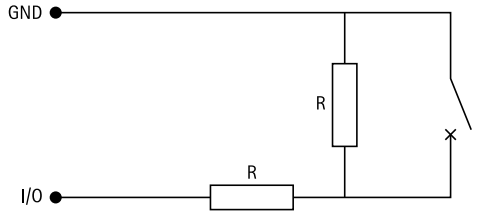
Primera conexión en paralelo

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



Primera conexión en serie

Los valores de la resistencia deben ser los mismos y los posibles son 1 kΩ, 2,2 kΩ, 4,7 kΩ y 10 kΩ .



Nota

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

Localización de problemas

Restablezca la configuración predeterminada de fábrica

Importante

Hay que valorar bien es necesario 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 *Guía de productos, on page 11*.
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 finalizará cuando el indicador LED de estado se ilumine en color verde. Si no hay ningún servidor DHCP en la red, la dirección IP del dispositivo será una de las siguientes de forma predeterminada:
   - **Dispositivos con AXIS OS 12.0 y versiones posteriores:** obtenidos de la subred de direcciones de enlace local (169.254.0.0/16)
   - **Dispositivos con AXIS OS 11.11 y anterior:** 192.168.0.90/24
5. Utilice las herramientas del software de instalación y gestión para asignar una dirección IP, configurar la contraseña y acceder al producto.

También puede restablecer los parámetros a la configuración predeterminada de fábrica a través de la interfaz web del dispositivo. Vaya a **Mantenimiento** > **Configuración predeterminada de fábrica** y haga clic en **Predeterminada**.

Opciones de AXIS OS

Axis ofrece gestión del software del producto según la vía activa o las vías de asistencia a largo plazo (LTS). La vía activa implica acceder de forma continua a todas las características más recientes del producto, mientras que las vías LTS proporcionan una plataforma fija con versiones periódicas dedicadas principalmente a correcciones de errores y actualizaciones de seguridad.

Se recomienda el uso de AXIS OS desde la vía activa si desea acceder a las características más recientes o si utiliza la oferta de sistemas de extremo a extremo de Axis. Las vías LTS se recomiendan si se usan integraciones de terceros que no se validan de manera continua para la última vía activa. Con LTS, los productos pueden preservar la ciberseguridad sin introducir modificaciones funcionales significativas ni afectar a las integraciones existentes. Para obtener información más detallada sobre la estrategia de software de dispositivos Axis, visite *axis.com/support/device-software*.

Comprobar la versión de AXIS OS

AXIS OS determina la funcionalidad de nuestros dispositivos. Cuando solucione un problema, le recomendamos que empiece comprobando la versión de AXIS OS actual. La versión más reciente podría contener una corrección que solucione su problema concreto.

Para comprobar la versión de AXIS OS:

1. Vaya a la interfaz web del dispositivo > **Status (estado)**.
2. Consulte la versión de AXIS OS en **Device info (información del dispositivo)**.

Actualización de AXIS OS

Importante

- Al actualizar el software del dispositivo, se guardan los ajustes preconfigurados y personalizados. Axis Communications AB no puede garantizar que se guarden los ajustes, incluso si las funciones están disponibles en la nueva versión del AXIS OS.
- A partir del AXIS OS 12.6, es preciso instalar todas las versiones LTS entre la versión actual de su dispositivo y la versión de destino. Por ejemplo, si la versión del software del dispositivo actualmente instalada es AXIS OS 11.2, deberá instalar la versión LTS AXIS OS 11.11 antes de poder actualizar el dispositivo a AXIS OS 12.6. Para obtener más información, consulte *AXIS OS lifecycle guide: Upgrade path (Guía de ciclo de vida de AXUS OS: ruta de actualización)*.
- Asegúrese de que el dispositivo permanece conectado a la fuente de alimentación durante todo el proceso de actualización.

Nota

- Al actualizar el dispositivo con el AXIS OS más reciente en la pista activa, 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 la actualización. Para encontrar el AXIS OS y las notas de versión más recientes, consulte *axis.com/support/device-software*.
- Puesto que la base de datos de usuarios, grupos, credenciales y otros datos se actualiza con la actualización del AXIS OS, el primer inicio podría tardar unos minutos en completarse. El tiempo necesario dependerá de la cantidad de datos.

1. Descargue en su ordenador el archivo de AXIS OS, disponible de forma gratuita en *axis.com/support/device-software*.
2. Inicie sesión en el dispositivo como administrador.
3. Vaya a **Maintenance > AXIS OS upgrade (mantenimiento > actualización de AXIS OS)** y haga clic en **Upgrade (actualizar)**.

Una vez que la actualización ha terminado, el producto se reinicia automáticamente.

4. Una vez reiniciado el producto, borre la caché del navegador web.

Problemas técnicos y posibles soluciones

Problemas para actualizar AXIS OS

Error en la actualización de AXIS OS

Cuando se produce un error en la actualización, el dispositivo vuelve a cargar la versión anterior. La causa más frecuente es que se ha cargado el archivo de AXIS OS incorrecto. Asegúrese de que el nombre del archivo de AXIS OS corresponde a su dispositivo e inténtelo de nuevo.

Problemas tras la actualización de AXIS OS

Si tiene problemas después de actualizar, vuelva a la versión instalada anteriormente desde la página de **Mantenimiento**.

Problemas al configurar la dirección IP

No se puede configurar la dirección IP

- Si la dirección IP prevista para el dispositivo y la dirección IP del ordenador utilizado para acceder al dispositivo se encuentran en subredes distintas, no podrá configurar la dirección IP. Póngase en contacto con el administrador de red para obtener una dirección IP.
- La dirección IP podría estar siendo utilizada por otro dispositivo. Para comprobarlo:
  1. Desconecte el dispositivo de Axis de la red.
  2. En una ventana de comando/DOS, escriba `ping` y la dirección IP del dispositivo.
  3. Si recibe: `Reply from <IP address>: bytes=32; time=10...`, significará 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 dispositivo.
  4. Si recibe: `Request timed out`, significa que la dirección IP está disponible para su uso con el dispositivo de Axis. Compruebe el cableado y vuelva a instalar el dispositivo.
- La IP podría estar siendo utilizada por otro dispositivo de la misma subred. Se utiliza la dirección IP estática del dispositivo 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 dispositivo.

Problemas de acceso al dispositivo

No puede iniciar sesión accediendo al dispositivo desde un navegador

Cuando HTTPS esté habilitado, asegúrese de utilizar el protocolo correcto (HTTP o HTTPS) al intentar iniciar sesión. Es posible que deba escribir manualmente `http` o `https` en la barra de direcciones del navegador.

Si ha olvidado la contraseña de la cuenta de administrador, deberá restablecer el dispositivo a la configuración de fábrica. Para consultar las instrucciones, vea *Restablezca la configuración predeterminada de fábrica, on page 18*.

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 dispositivo en la red. Identifique el dispositivo utilizando el modelo o el número de serie, o por el nombre de DNS (si se ha configurado el nombre).

Si es preciso, puede asignar manualmente una dirección IP estática. Para ver las instrucciones, vaya a *axis.com/support*.

Error de certificado cuando se utiliza IEEE 802.1X

Para que la autentificación funcione correctamente, los ajustes de fecha y hora del dispositivo de Axis se deben sincronizar con un servidor NTP. Vaya a **Sistema > Fecha y hora**.

El navegador no es compatible

Para obtener una lista de los navegadores recomendados, consulte *Compatibilidad con navegadores, on page 4*.

No se puede acceder externamente al dispositivo.

Para acceder al dispositivo externamente, le recomendamos que use una de las siguientes aplicaciones para Windows®:

- AXIS Camera Station Edge: gratuito, ideal para sistemas pequeños con necesidades de vigilancia básicas.
- AXIS Camera Station Pro: versión de prueba de 90 días gratuita, ideal para sistemas de tamaño pequeño y medio.

Para obtener instrucciones y descargas, vaya a *axis.com/vms*.

Problemas con MQTT

No se puede conectar a través del puerto 8883 con MQTT a través de SSL

El firewall bloquea el tráfico que usa el puerto 8883 por considerarlo inseguro.

En algunos casos, el servidor/intermediario podría no proporcionar un puerto específico para la comunicación MQTT. Aun podría ser posible utilizar MQTT a través de un puerto utilizado normalmente para el tráfico HTTP/HTTPS.

- Si el servidor/intermediario es compatible con WebSocket/WebSocket Secure (WS/WSS), normalmente en el puerto 443, utilice este protocolo en su lugar. Consulte con el proveedor del servidor/intermediario para comprobar si es compatible con WS/WSS y qué puerto y basepath usar.
- Si el servidor/broker admite ALPN, el uso de MQTT puede negociarse a través de un puerto abierto, como 443. Consulte a su proveedor de servidores/brokers si admite ALPN y qué protocolo y puerto ALPN debe utilizar.

Si no encuentra aquí lo que busca, pruebe a visitar la sección de solución de problemas de *axis.com/support*.

Contactar con la asistencia técnica

Si necesita más ayuda, vaya a *axis.com/support*.

Ciberseguridad

La ciberseguridad contribuye a un ciclo de vida satisfactorio del producto con riesgos minimizados. Puede encontrar información detallada y documentación sobre nuestro enfoque en materia de ciberseguridad en *about our cybersecurity approach at axis.com/about-axis/cybersecurity*. Siga las directrices de ciberseguridad que se indican a continuación para recibir notificaciones de seguridad de Axis sobre el producto y para realizar la configuración de su producto de modo que garantice un ciclo de vida y una desinstalación seguros.

En *Axis Trust Center*, puede encontrar información sobre la implementación que hace Axis de las medidas de cumplimiento de seguridad, transparencia, protección de datos y privacidad.

Gestión de las vulnerabilidades

Axis es una *Common Vulnerability and Exposures (CVE) Numbering Authority (CNA) (autoridad numeradora de vulnerabilidades y exposiciones comunes (CVE) (CNA))*. Para minimizar su riesgo de exposición, satisfacemos las normas del sector a la hora de identificar y resolver vulnerabilidades en nuestros dispositivos, software y servicios. Consulte más información sobre nuestra política de gestión de vulnerabilidades o notifique una vulnerabilidad en *axis.com/vulnerability-management*.

Notificaciones de seguridad

Suscríbase a los correos electrónicos de notificaciones de seguridad de Axis en *axis.com/security-notification-servic*e. Le enviaremos información sobre vulnerabilidades, los avisos de seguridad correspondientes y otros asuntos relacionados con la seguridad de su producto Axis.

Ciclo de vida seguro del producto

Axis minimiza los riesgos a lo largo de la vida útil de nuestros productos mediante una gestión segura del ciclo de vida. Utilice nuestras guías de refuerzo en *help.axis.com* para configurar y operar sus productos Axis del modo más seguro y para encontrar información sobre:

Primer uso seguro – Los productos Axis vienen preconfigurados con un alto nivel de protección por defecto para permitir una inicialización segura y una comunicación cifrada desde el primer momento.

Uso previsto y errores de configuración comunes – Nuestras guías facilitan información sobre el uso previsto de los productos Axis, incluidos errores de uso comunes relacionados con la seguridad y errores de configuración que deben evitarse.

Gestión de vulnerabilidades y transparencia en la cadena de suministro – Con cada lanzamiento de software se publica una lista de materiales de software (SBOM) en *axis.com y* con el fin de revelar vulnerabilidades y mejorar la transparencia de la cadena de suministro.

Desinstalación y borrado seguro de datos – Para desinstalar un producto de forma segura cuando alcanza el término de su ciclo de vida, restablézcalo a los valores predeterminados de fábrica. Esto eliminará sus configuraciones, datos almacenados e información confidencial.

T10181041_es

2026-10 (M11.6)

© 2022 – 2026 Axis Communications AB