

AXIS A9210 Network I/O Relay Module

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 técnica 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 no conoce 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. Vea *Crear una cuenta de administrador, on page 2*.

Para obtener descripciones de todas las funciones y configuraciones 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 un nombre de usuario.
2. Introduzca una contraseña. Vea *Contraseñas seguras, on page 3*.
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. Vea *Restablecimiento a la configuración predeterminada de fábrica, on page 15*.

Contraseñas seguras

Importante

Utilice HTTPS (habilitado por defecto) para configurar su contraseña u otros ajustes confidenciales a través de la red. HTTPS ofrece conexiones de red seguras y cifradas para proteger 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 nadie 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. Vea *Restablecimiento a la configuración predeterminada de fábrica, on page 15*.
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

Configurar un puerto de E/S

1. Vaya a **Device > I/Os and relays > AXIS A9210 > I/Os** (Dispositivo > E/S y relés > relés de red AXIS A9210 > E/Ss).
2. Haga clic  para expandir la configuración del puerto de E/S.
3. Cambiar el nombre del puerto.
4. Configurar el estado normal. Haga clic  para circuito abierto o  para circuito cerrado.
5. Para configurar el puerto de E/S como entrada:
 - 5.1. En **Direction (Dirección)**, haga clic .
 - 5.2. Para supervisar el estado de entrada, active **Supervised (Supervisado)**. Vea *Entradas con supervisión, on page 14*.

Nota

En las API, los puertos de E/S supervisados funcionan de forma diferente a los puertos de entrada supervisados. Para obtener más información, vaya a la *biblioteca VAPIX®*.

6. Para configurar el puerto de E/S como salida:
 - 6.1. En **Direction (Dirección)**, haga clic .
 - 6.2. Para ver las URL para activar y desactivar los dispositivos conectados, vaya a **Toggle port URL (Alternar URL de puerto)**.

Configurar un relé

1. Vaya a **Device > I/Os and relays > AXIS A9210 > Relays** (Dispositivo > E/S y relés > relés de red AXIS A9210 > relés).
2. Haga clic  para expandir la configuración del relé.
3. Active el **Relay (relé)**.
4. Cambiar el nombre del relé.
5. Para ver las URL para activar y desactivar el relé, vaya a **Toggle port URL (Alternar URL de puerto)**.

Configurar reglas para eventos

Para obtener más información, consulte *Get started with rules for events (Introducción a las reglas para eventos)*.

Activar una acción

1. Vaya a **System > Events (Sistema > Eventos)** y agregue una regla. La regla determina cuándo debe realizar el dispositivo determinadas acciones. Puede configurar reglas como programadas, recurrentes o activadas manualmente.
2. Introduzca un **Name (Nombre)**.
3. Seleccione la **Condition (Condición)** que debe cumplirse para que se active la acción. Si especifica varias condiciones para la regla, deben cumplirse todas ellas para que se active la acción.
4. En **Action (Acción)**, seleccione qué acción debe realizar cuando se cumplan las condiciones.

Nota

- Si realiza cambios a una regla activa, esta debe iniciarse de nuevo para que los cambios surtan efecto.

Interfaz web

Para leer sobre todas las funciones y configuraciones 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

Analíticas y aplicaciones

Las analíticas y aplicaciones permiten sacar el máximo partido a su dispositivo Axis. AXIS Camera Application Platform (ACAP) es una plataforma abierta que permite a terceros desarrollar analíticas y otras apps para dispositivos Axis. Las apps pueden preinstalarse en el dispositivo, pueden descargarse de forma gratuita o por un precio de licencia.

Para encontrar los manuales de usuario de analíticas y apps de Axis, visite help.axis.com.

Supervisión de puertas AXIS

Esta aplicación supervisa el estado de la puerta, mostrando si esta se encuentra abierta o cerrada y si permanece abierta mucho tiempo. Por ejemplo, utilice esta opción en una puerta de seguridad contra incendios que no requiera un bloqueo pero en la que debe saber si está abierta.

Una puerta normal dispone de un sensor de posición de puerta, REX, junto con cierres y lectores, lo que requiere un controlador de puerta.

Una puerta de supervisión solo requiere un sensor de posición de puerta y REX, y se puede supervisar empleando un módulo de relé de E/S de red. Cada módulo de relé de E/S de red permite conectar hasta cinco puertas de supervisión.

Limitations (Limitaciones)

La aplicación solo está disponible en AXIS A9210. REX solo se puede conectar a las E/S 1 y E/S 2, no es posible configurar REX en las E/S 3, E/S 4 o E/S 5.

Configuración de la Supervisión de puertas AXIS

Nombre	Descripción
Puerta	El número de la puerta.
Entrada DPS	La entrada DPS de la puerta.
Entrada REX	La entrada REX de la puerta.
Door open-too-long time (sec) [Tiempo de apertura de la puerta demasiado largo (s)]	El número de segundos que se permite que la puerta esté abierta.
Tiempo de acceso (s)	El número de segundos que la puerta deberá permanecer desbloqueada una vez concedido el permiso de acceso.
Estado	El estado de la puerta.

Ciberseguridad

Para obtener información específica sobre ciberseguridad, consulte la ficha técnica del producto en axis.com.

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

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.

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.

Almacén de claves seguro

Un entorno protegido contra manipulaciones para la protección de claves privadas y la ejecución segura de operaciones criptográficas. Impide el acceso sin autorización y las extracciones maliciosas en caso de incidentes de seguridad. En función de los requisitos de seguridad, un dispositivo Axis puede tener uno o varios módulos de computación criptográfica basados en hardware, el lugar donde se encuentra el almacén de claves seguro protegido por el hardware. En función de los requisitos de seguridad, un dispositivo Axis puede tener uno o varios módulos de computación criptográficos basados en hardware, como un TPM 2.0 (Módulo de plataforma segura) o un elemento seguro, o un TEE (Entorno de ejecución de confianza), que ofrecen un almacén de claves seguro protegido por hardware. Además, algunos productos Axis cuentan con un almacén de claves seguro con certificación FIPS 140-2 Nivel 2.

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.

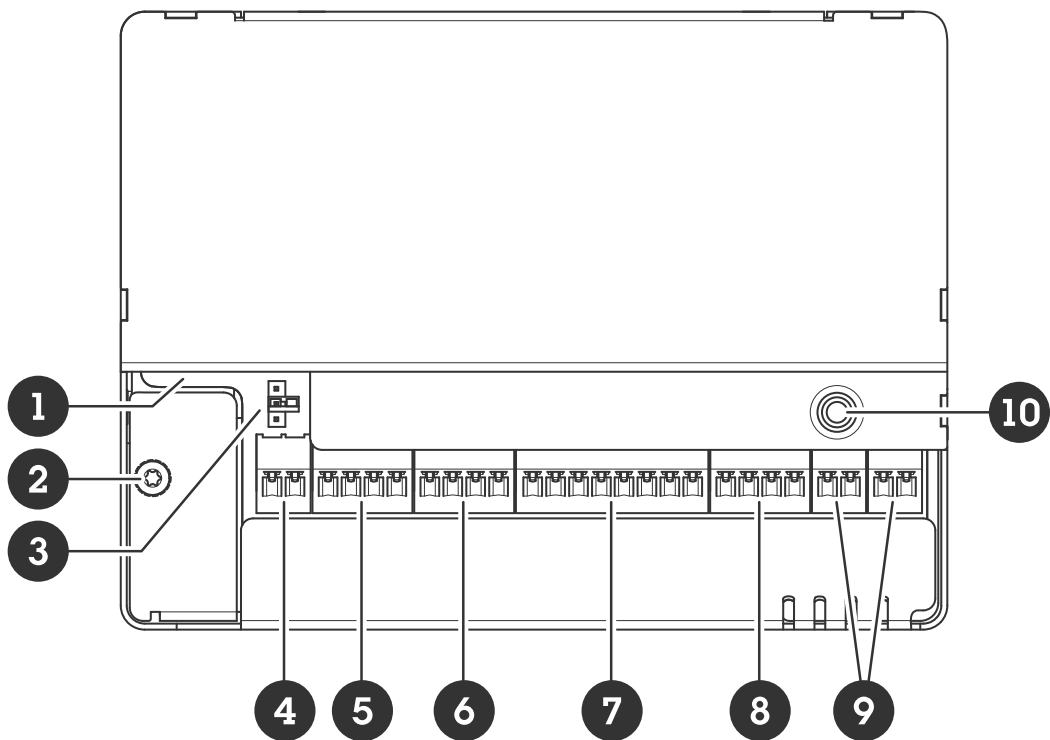
Sistema de archivos cifrado

El almacén de claves seguro impide la filtración maliciosa de información y evita que pueda manipularse la configuración aplicando un potente cifrado al sistema de archivos. Esto garantiza que no se puedan extraer ni manipular datos almacenados en el sistema de archivos cuando no se use el dispositivo, durante un acceso no autorizado al dispositivo o si alguien roba el dispositivo Axis. Durante el proceso de arranque seguro, se descifra el sistema de archivos de lectura/escritura y el dispositivo Axis puede montarlo y utilizarlo.

Para obtener más información sobre las características de ciberseguridad de los dispositivos Axis, vaya a axis.com/learning/white-papers y busque ciberseguridad.

Especificaciones

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 1 entrada
- 7 RS485 y conector de E/S
- 8 Conector de E/S
- 9 Conector de 2 entrada
- 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.

Potencia	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. Vea *Restablecimiento a la configuración predeterminada de fábrica, on page 15*.
- Conectarse a un servicio de conexión a la nube (O3C) de un solo clic a través de Internet. Para conectarse, presione y suelte el botón y espere a que el LED de estado parpadee tres veces en verde.

Conectores

Conector de red

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

UL: La alimentación a través de Ethernet (PoE) se hará a través de Ethernet IEEE 802.3af/802.3at Tipo 1, Clase 3, o de alimentación a través de Ethernet Plus (PoE +) IEEE 802.3 at Tipo 2 Clase 4 que ofrezca 44–57 V CC, 15,4 W / 30 W. La alimentación a través de Ethernet (PoE) se ha evaluado conforme a UL con AXIS T8133 Midspan 30 W 1 puerto.

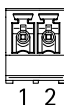
Prioridad de potencia

Este dispositivo puede recibir alimentación mediante una entrada de PoE o CC. Vea *Conector de red, on page 9* y *Conector de alimentación, on page 9*.

- 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 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.



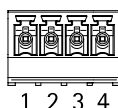
1. El relé está activo cuando COM está conectado a NO.

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.

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. Si se utiliza con una carga inductiva, por ejemplo, un bloqueo, conecte un diodo en paralelo a la carga como protección contra transitorios de tensión.



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.

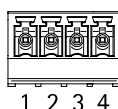
Se puede utilizar para conectar una cerradura entre los pines GND y NO, o GND y NC.

Fuente de alimentación	Potencia máxima a 12 V CC	Potencia máxima a 24 V CC
CC IN	2 000 mA	1 000 mA
PoE	350 mA	150 mA
PoE+	1100 mA	500 mA

Conector de 1 entrada

Un bloque de terminales de 4 pines para la entrada.

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. Vea *Entradas con supervisión*, on page 14.



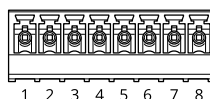
Función	Pin	Notas	Especificaciones
Tierra CC	1, 3		0 V CC
Entrada	2, 4	Entrada digital o entrada supervisada: conéctela al pin 1 o 3 respectivamente para activar, o dejar flotando (desconectado) para desactivar.	De 0 a 30 V CC máx.

Importante

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

RS485 y conector de E/S

Un bloque de terminales de 8 pines que incluye RS485 de 4 pines y E/S de 4 pines.



RS485

Función	Pin	Nota	Especificaciones
Tierra CC (GND)	1		0 V CC
Salida de CC (+12 V)	2	Suministra alimentación a los dispositivos auxiliares, por ejemplo, sensores Modbus.	12 V CC, máx. 200 mA
A	3		
B	4		

E/S

Función	Pin	Nota	Especificaciones
Salida digital	5	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.	De 0 a 30 V CC máx., colector abierto, 100 mA
Salida digital	6	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.	De 0 a 30 V CC máx., colector abierto, 100 mA
Entrada	7	Entrada digital o entrada supervisada: conéctela al pin 1 para activarla, o bien déjela suelta (sin conectar) para desactivarla.	0 a máx. 30 V CC
Salida digital	8	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.	De 0 a 30 V CC máx., colector abierto, 100 mA

Importante

- La longitud de cable cualificada para RS485 es de hasta 1000 m (3281 ft) si se cumplen los siguientes requisitos del cable: 1 par trenzado con blindaje, AWG 24, impedancia de 120 ohmios.
- La longitud del cable cualificado para E/S es de hasta 200 m (656 ft).

Conector de E/S

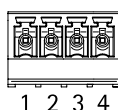
Utilice el conector auxiliar con dispositivos externos, por ejemplo, en combinación con detección de movimiento, activación de eventos y notificaciones de alarma. Además del punto de referencia de 0 V CC y la alimentación (salida de CC), el conector auxiliar ofrece la interfaz para:

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.

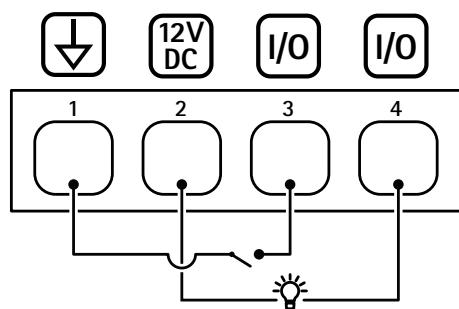
Entrada supervisada – Permite detectar la manipulación de una señal digital.

Salida digital – Para conectar dispositivos externos como relés y LED. Los dispositivos conectados pueden activarse 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 con la carga para protegerla contra transitorios de tensión. Las E/S son capaces de alimentar una carga externa de 12 V CC, 50 mA (máx. combinado), si se utiliza la 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

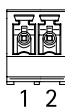


- 1 Tierra CC
- 2 Salida de CC 12 V
- 3 E/S configurada como entrada
- 4 E/S configurada como salida

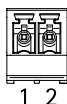
Conector de 2 entrada

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
Entrada	2	Entrada digital o entrada supervisada: conéctela al pin 1 para activarla o déjela suelta (sin conectar) para desactivarla.	De 0 a 30 V CC máx.



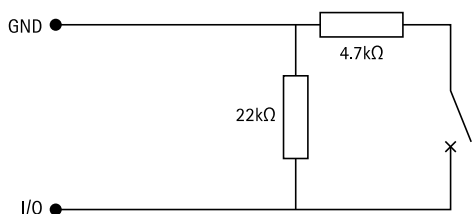
Función	Pin	Notas	Especificaciones
Tierra CC	1		0 V CC
Entrada	2	Entrada digital o entrada supervisada: conéctela al pin 1 para activarla o déjela suelta (sin conectar) para desactivarla.	De 0 a 30 V CC máx.

Entradas con supervisión

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

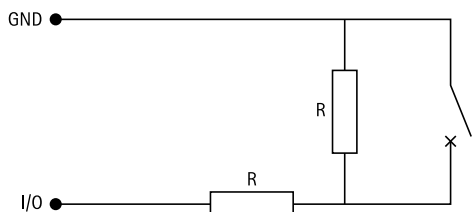
Parallel first connection (Primera conexión en paralelo)

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



Primera conexión en serie

Los valores de la resistencia deben ser los mismos y los posibles son 1 k Ω , 2,2 k Ω , 4,7 k Ω y 10 k Ω , 1 %, estándar de 1/4 vatio.



Nota

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

Estado	Descripción
Abierto	El switch supervisado está en modo abierto.
Cerrado	El switch supervisado está en modo cerrado.
Corto	El cable de E/S o Entrada 1-5 está en cortocircuito con tierra.
Cortar	El cable de E/S o de entrada 1-5 se corta y se deja abierto sin ruta actual a tierra.

Localización de problemas

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. Vea *Guía de productos*, on page 8.
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 disponible en la red, la dirección IP del dispositivo adoptará de forma predeterminada una de las siguientes:
 - **Dispositivos con AXIS OS 12.0 y posterior:** Obtenido de la subred de dirección 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 *Portal AXIS 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.
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.

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 lo siguiente: `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 *Restablecimiento a la configuración predeterminada de fábrica, on page 15*.

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 autenticación 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 2*.

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 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.

Problemas con el funcionamiento del dispositivo

El calefactor delantero y el limpiaparabrisas no funcionan

Si el calefactor delantero o el limpiaparabrisas no se encienden, compruebe que la cubierta superior esté correctamente fijada a la parte inferior de la unidad de alojamiento.

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

Contactar con la asistencia técnica

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

T10202445_es

2026-02 (M7.2)

© 2023 – 2026 Axis Communications AB