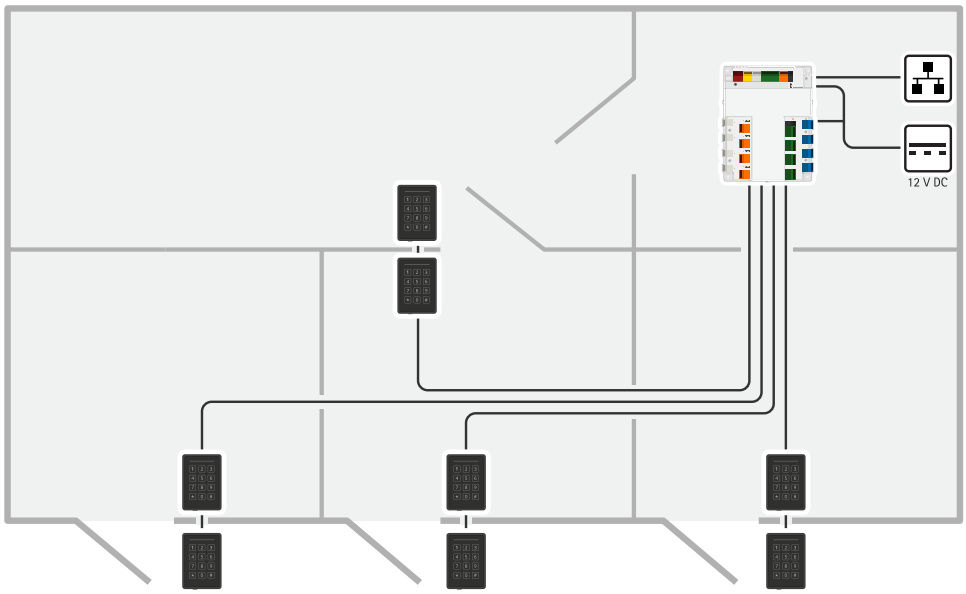
AXIS A1710-B Network Door Controller

Manual del usuario

Índice

Presentación esquemática de la solución



El controlador de puerta en red puede conectarse fácilmente a su red IP existente. Cada controlador de puerta en red puede encender y controlar hasta 8 lectores y 4 bloqueos.

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

*Para utilizar la interfaz web AXIS OS con iOS 15 o iPadOS 15, vaya a
Settings > Safari > Advanced > Experimental Features (Configuración > Safari > Avanzada > Funciones experimentales) y desactive NSURLSession Websocket.

Si necesita más información sobre los navegadores recomendados, visite el *portal de AXIS OS*.

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 .

Para obtener descripciones de todos los controles y opciones de la interfaz web del dispositivo, consulte .

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 .
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 .

Contraseñas seguras

Importante

Los dispositivos de Axis envían la contraseña definida inicialmente en texto abierto a través de la red. Para proteger su dispositivo tras el primer inicio de sesión, configure una conexión HTTPS segura y cifrada y, a continuación, cambie la contraseña.

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.

Comprobar 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. Vea .
   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.

Interfaz web

Para acceder a la interfaz web, escriba la dirección IP del dispositivo en un navegador web.

Nota

La compatibilidad con las características y ajustes descrita en esta sección varía entre dispositivos. Este icono  indica que la función o ajuste solo está disponible en algunos dispositivos.

 Mostrar u ocultar el menú principal.

 Acceda a las notas de la versión.

 Acceder a la ayuda del producto.

 Cambiar el idioma.

 Definir un tema claro o un tema oscuro.

 El menú de usuario contiene:

- Información sobre el usuario que ha iniciado sesión.
-  **Cambiar cuenta**: Cierre sesión en la cuenta actual e inicie sesión en una cuenta nueva.
-  **Cerrar sesión**: Cierre sesión en la cuenta actual.

 El menú contextual contiene:

- **Analytics data (Datos de analíticas)**: Puede compartir datos no personales del navegador.
- **Feedback (Comentarios)**: Puede enviarnos comentarios para ayudarnos a mejorar su experiencia de usuario.
- **Legal (Aviso legal)**: Lea información sobre cookies y licencias.
- **About (Acerca de)**: Puede consultar la información del dispositivo, como la versión de AXIS OS y el número de serie.

Estado

Conexión de puerta

Puerta: Muestra el estado de las puertas conectadas.

Información sobre el dispositivo

Muestra información del dispositivo, como la versión del AXIS OS y el número de serie.

Actualización de AXIS OS: Actualizar el software en el dispositivo. Le lleva a la página de mantenimiento donde puede realizar la actualización.

Estado de sincronización de hora

Muestra la información de sincronización de NTP, como si el dispositivo está sincronizado con un servidor NTP y el tiempo que queda hasta la siguiente sincronización.

Configuración de NTP: Ver y actualizar los ajustes de NTP. Le lleva a la página **Time and location (Hora y localización)**, donde puede cambiar los ajustes de NTP.

Seguridad

Muestra qué tipo de acceso al dispositivo está activo y qué protocolos de cifrado están en uso y si se permite el uso de aplicaciones sin firmar. Las recomendaciones para los ajustes se basan en la guía de seguridad del sistema operativo AXIS.

Hardening guide (Guía de seguridad): Enlace a la *guía de seguridad del sistema operativo AXIS*, en la que podrá obtener más información sobre ciberseguridad en dispositivos Axis y prácticas recomendadas.

Clientes conectados

Muestra el número de conexiones y clientes conectados.

View details (Ver detalles): Consulte y actualice la lista de clientes conectados. La lista muestra la dirección IP, el protocolo, el puerto, el estado y PID/proceso de cada conexión.

Dispositivo

Alarmas

Device motion (Movimiento del dispositivo): Active esta opción para desencadenar una alarma en el sistema cuando se detecte un movimiento del dispositivo.

Casing open (Carcasa abierta) : Active esta opción para desencadenar una alarma en el sistema cuando se detecte una carcasa del controlador de puerta abierta. Desactive este ajuste para los controladores de puerta básicos.

External tamper (Manipulación externa) : Con esta opción se desencadena una alarma en el sistema si se detecta una manipulación externa. Por ejemplo, cuando alguien abre o cierra el armario externo.

- **Supervised input (Entrada supervisada)** : Active la supervisión del estado de entrada y configure las resistencias de final de línea.
  - Para utilizar la primera conexión paralela, seleccione **Parallel first connection with a 22 KΩ parallel resistor and a 4.7 KΩ serial resistor (Primera conexión en paralelo con una resistencia de 22 KΩ en paralelo y una resistencia de 4,7 KΩ en serie)**.
  - Para utilizar la primera conexión en serie, seleccione **Serial first connection (Primera conexión en serie)** y seleccione los valores de la resistencia en la lista desplegable **Resistor values (Valores de resistencia)**.

Periféricos

Lectores

Add reader (Agregar lector): Haga clic para agregar un nuevo lector.

Name (Nombre): Introduzca el nombre del lector.

Lector: Seleccione un lector de la lista desplegable.

IP address (Dirección IP): Introduzca la dirección IP del lector manualmente.

Nombre de usuario: Introduzca el nombre de usuario del lector.

Contraseña: Introduzca la contraseña de usuario del lector.

Ignore server certificate verification (Ignorar verificación de certificado de servidor): Active esta opción para ignorar la verificación.

Cerraduras inalámbricas

Necesita una licencia para utilizar esta función.

Conectar concentrador de comunicaciones: Haga clic para conectar los bloqueos inalámbricos.

Actualizar lectores

Actualizar lectores: Haga clic para actualizar los lectores a una nueva versión de AXIS OS. La característica solo puede actualizar los lectores compatibles cuando estén en línea.

Aplicaciones

Add app (Agregar aplicación): Instale una nueva aplicación.

Find more apps (Buscar más aplicaciones): Encuentre más aplicaciones para instalar. Se le mostrará una página de información general de las aplicaciones de Axis.

Permitir aplicaciones sin firma : Active esta opción para permitir la instalación de aplicaciones sin firma.

Permitir aplicaciones con privilegios de root : Active esta opción para permitir a las aplicaciones con privilegios root el acceso completo al dispositivo.

Consulte las actualizaciones de seguridad en las aplicaciones AXIS OS y ACAP.

Nota

El rendimiento del dispositivo puede empeorar si ejecuta varias aplicaciones al mismo tiempo.

Utilice el switch situado junto al nombre de la aplicación para iniciar o detener la aplicación.

Abrir: Acceda a los ajustes de la aplicación. que varían en función de la aplicación. Algunas aplicaciones no tienen ajustes.

El menú contextual puede contener una o más de las siguientes opciones:

- **Licencia de código abierto**: Consulte la información sobre las licencias de código abierto utilizadas en la aplicación.
- **App log (Registro de aplicación)**: Consulte un registro de los eventos de la aplicación. El registro resulta útil si se debe contactar con el servicio de soporte técnico.
- **Activate license with a key (Activar licencia con una clave)**: Si la aplicación requiere una licencia, tiene que activarla. Use esta opción si su dispositivo no tiene acceso a Internet.
  Si no dispone de clave de licencia, vaya a *axis.com/products/analytics*. Se necesita un código de licencia y el número de serie del producto de Axis para generar una clave de licencia.
- **Activate license automatically (Activar licencia automáticamente)**: Si la aplicación requiere una licencia, tiene que activarla. Use esta opción si su dispositivo tiene acceso a Internet. Se necesita un código para activar la licencia.
- **Deactivate the license (Desactivar la licencia)**: Desactive la licencia para sustituirla por otra, por ejemplo, al cambiar de licencia de prueba a licencia completa. Si desactiva la licencia, también la elimina del dispositivo.
- **Settings (Ajustes)**: Configure los parámetros.
- **Eliminar**: Permite eliminar la aplicación del dispositivo permanentemente. Si primero no desactiva la licencia, permanecerá activa.

Nota

AXIS Door Controller Extension ACAP viene preinstalado en el sistema. Se requiere una licencia para utilizarlo.

Sistema

Hora y ubicación

Fecha y hora

El formato de fecha y hora depende de la configuración de idioma del navegador web.

Nota

Es aconsejable sincronizar la fecha y hora del dispositivo con un servidor NTP.

Synchronization (Sincronización): Seleccione una opción para la sincronización de la fecha y la hora del dispositivo.

- **Fecha y hora automáticas (servidores NTS KE manuales)**: Sincronice con los servidores de establecimiento de claves NTP seguros conectados al servidor DHCP.
  - **Servidores NTS KE manuales**: Introduzca la dirección IP de un servidor NTP o de dos. Si usa dos servidores NTP, el dispositivo sincroniza y adapta la fecha y hora en función de la información de los dos.
  - **Tiempo máximo de encuesta NTP**: Seleccione la cantidad máxima de tiempo que debe esperar el dispositivo antes de que sondee el servidor NTP para obtener una hora actualizada.
  - **Tiempo mínimo de encuesta NTP**: Seleccione la cantidad mínima de tiempo que debe esperar el dispositivo antes de que sondee el servidor NTP para obtener una hora actualizada.
- **Fecha y hora automáticas (los servidores NTP utilizan DHCP)**: Se sincroniza con los servidores NTP conectados al servidor DHCP.
  - **Servidores NTP alternativos**: Introduzca la dirección IP de un servidor alternativo o de dos.
  - **Tiempo máximo de encuesta NTP**: Seleccione la cantidad máxima de tiempo que debe esperar el dispositivo antes de que sondee el servidor NTP para obtener una hora actualizada.
  - **Tiempo mínimo de encuesta NTP**: Seleccione la cantidad mínima de tiempo que debe esperar el dispositivo antes de que sondee el servidor NTP para obtener una hora actualizada.
- **Fecha y hora automáticas (servidores NTP manuales)**: Se sincroniza con los servidores NTP que seleccione.
  - **Servidores NTP manuales**: Introduzca la dirección IP de un servidor NTP o de dos. Si usa dos servidores NTP, el dispositivo sincroniza y adapta la fecha y hora en función de la información de los dos.
  - **Tiempo máximo de encuesta NTP**: Seleccione la cantidad máxima de tiempo que debe esperar el dispositivo antes de que sondee el servidor NTP para obtener una hora actualizada.
  - **Tiempo mínimo de encuesta NTP**: Seleccione la cantidad mínima de tiempo que debe esperar el dispositivo antes de que sondee el servidor NTP para obtener una hora actualizada.
- **Custom date and time (Personalizar fecha y hora)**: Establezca manualmente la fecha y hora. Haga clic en **Get from system (Obtener del sistema)** para obtener una vez la configuración de fecha y hora desde su ordenador o dispositivo móvil.

Time zone (Zona horaria): Seleccione la zona horaria que desee utilizar. La hora se ajustará automáticamente para el horario de verano y el estándar.

- **DHCP**: Adopta la zona horaria del servidor DHCP. El dispositivo debe estar conectado a un servidor DHCP para poder seleccionar esta opción.
- **Manual**: Seleccione una zona horaria de la lista desplegable.

Nota

El sistema utiliza los ajustes de fecha y hora en todas las grabaciones, registros y ajustes del sistema.

Localización de dispositivo

Especifique el lugar en el que se encuentra el dispositivo. El sistema de gestión de vídeo puede utilizar esta información para colocar el dispositivo en un mapa.

- **Format (Formato)**: Seleccione el formato que desea utilizar para introducir la latitud y longitud de su dispositivo.
- **Latitude (Latitud)**: Los valores positivos son el norte del ecuador.
- **Longitude (Longitud)**: Los valores positivos son el este del meridiano principal.
- **Heading (Rumbo)**: Introduzca la dirección de la brújula a la que apunta el dispositivo. 0 es al norte.
- **Label (Etiqueta)**: Especifique un nombre descriptivo para su dispositivo.
- **Save (Guardar)**: Haga clic para guardar la localización del dispositivo.

Red

IPv4

Asignar IPv4 automáticamente: Seleccione esta opción para que el router de red asigne automáticamente una dirección IP al dispositivo. Recomendamos IP automática (DHCP) para la mayoría de las redes.

IP address (Dirección IP): Introduzca una dirección IP única para el dispositivo. Las direcciones IP estáticas se pueden asignar de manera aleatoria dentro de redes aisladas, siempre que cada dirección asignada sea única. Para evitar conflictos, le recomendamos ponerse en contacto con el administrador de la red antes de asignar una dirección IP estática.

Subnet mask (Máscara de subred): Introduzca la máscara de subred para definir qué direcciones se encuentran dentro de la red de área local. Cualquier dirección fuera de la red de área local pasa por el router.

Router: Introduzca la dirección IP del router predeterminado (puerta de enlace) utilizada para conectar dispositivos conectados a distintas redes y segmentos de red.

Volver a la dirección IP estática si DHCP no está disponible: Seleccione si desea agregar una dirección IP estática para utilizarla como alternativa si DHCP no está disponible y no puede asignar una dirección IP automáticamente.

Nota

Si DHCP no está disponible y el dispositivo utiliza una reserva de dirección estática, la dirección estática se configura con un ámbito limitado.

IPv6

Assign IPv6 automatically (Asignar IPv6 automáticamente): Seleccione esta opción para activar IPv6 y permitir que el router de red asigne automáticamente una dirección IP al dispositivo.

Nombre de host

Asignar nombre de host automáticamente: Seleccione esta opción para que el router de red asigne automáticamente un nombre de host al dispositivo.

Hostname (Nombre de host): Introduzca el nombre de host manualmente para usarlo como una forma alternativa de acceder al dispositivo. El informe del servidor y el registro del sistema utilizan el nombre de host. Los caracteres permitidos son A–Z, a–z, 0–9 y -.

Active las actualizaciones de DNS dinámicas: Permite que el dispositivo actualice automáticamente los registros de su servidor de nombres de dominio cada vez que cambie la dirección IP del mismo.

Register DNS name (Registrar nombre de DNS): Introduzca un nombre de dominio único que apunte a la dirección IP de su dispositivo. Los caracteres permitidos son A–Z, a–z, 0–9 y -.

TTL: El tiempo de vida (Time to Live, TTL) establece cuánto tiempo permanece válido un registro DNS antes de que sea necesario actualizarlo.

Servidores DNS

Asignar DNS automáticamente: Seleccione esta opción para permitir que el servidor DHCP asigne dominios de búsqueda y direcciones de servidor DNS al dispositivo automáticamente. Recomendamos DNS automática (DHCP) para la mayoría de las redes.

Search domains (Dominios de búsqueda): Si utiliza un nombre de host que no esté completamente cualificado, haga clic en **Add search domain (Agregar dominio de búsqueda)** y escriba un dominio en el que se buscará el nombre de host que usa el dispositivo.

DNS servers (Servidores DNS): Haga clic en **Agregar servidor DNS** e introduzca la dirección IP del servidor DNS. Este servidor proporciona la traducción de nombres de host a las direcciones IP de su red.

HTTP y HTTPS

HTTPS es un protocolo que proporciona cifrado para las solicitudes de página de los usuarios y para las páginas devueltas por el servidor web. El intercambio de información cifrado se rige por el uso de un certificado HTTPS, que garantiza la autenticidad del servidor.

Para utilizar HTTPS en el dispositivo, debe instalar un certificado HTTPS. Vaya a **System > Security (Sistema > Seguridad)** para crear e instalar certificados.

Allow access through (Permitir acceso mediante): Seleccione si un usuario tiene permiso para conectarse al dispositivo a través de **HTTP**, **HTTPS** o ambos protocolos **HTTP and HTTPS (HTTP y HTTPS)**.

Nota

Si visualiza páginas web cifradas a través de HTTPS, es posible que experimente un descenso del rendimiento, especialmente si solicita una página por primera vez.

HTTP port (Puerto HTTP): Especifique el puerto HTTP que se utilizará. El dispositivo permite el puerto 80 o cualquier puerto en el rango 1024-65535. Si ha iniciado sesión como administrador, también puede introducir cualquier puerto en el rango 1-1023. Si utiliza un puerto en este rango, recibirá una advertencia.

HTTPS port (Puerto HTTPS): Especifique el puerto HTTPS que se utilizará. El dispositivo permite el puerto 443 o cualquier puerto en el rango 1024-65535. Si ha iniciado sesión como administrador, también puede introducir cualquier puerto en el rango 1-1023. Si utiliza un puerto en este rango, recibirá una advertencia.

Certificado: Seleccione un certificado para habilitar HTTPS para el dispositivo.

Protocolos de detección de red

Bonjour®: Active esta opción para permitir la detección automática en la red.

Nombre de Bonjour: Introduzca un nombre descriptivo; será el que se muestre en la red. El nombre predeterminado es el nombre del dispositivo seguido de la dirección MAC.

UPnP®: Active esta opción para permitir la detección automática en la red.

Nombre de UPnP: Introduzca un nombre descriptivo; será el que se muestre en la red. El nombre predeterminado es el nombre del dispositivo seguido de la dirección MAC.

WS-Discovery: Active esta opción para permitir la detección automática en la red.

LLDP y CDP: Active esta opción para permitir la detección automática en la red. Si se desactiva LLDP y CPD puede afectar a la negociación de alimentación PoE. Para solucionar cualquier problema con la negociación de alimentación PoE, configure el switch PoE solo para la negociación de alimentación PoE del hardware.

Proxies globales

Http proxy (Proxy http): Especifique un host proxy global o una dirección IP según el formato permitido.

Https proxy (Proxy https): Especifique un host proxy global o una dirección IP según el formato permitido.

Formatos permitidos para proxies http y https:

- http(s)://host:puerto
- http(s)://usuario@host:puerto
- http(s)://user:pass@host:puerto

Nota

Reinicie el dispositivo para aplicar los ajustes globales del proxy.

No proxy (Sin proxy): Utilice **No proxy (Sin proxy)** para evitar los proxies globales. Introduzca una de las opciones de la lista, o introduzca varias separadas por una coma:

- Dejar vacío
- Especifique una dirección IP
- Especifique una dirección IP en formato CIDR
- Especifique un nombre de dominio, por ejemplo: www.<nombre de dominio>.com
- Especifique todos los subdominios de un dominio concreto, por ejemplo .<nombre de dominio>.com

Conexión a la nube con un clic

La conexión One-Click Cloud (O3C), junto con un servicio O3C, ofrece acceso seguro y sencillo a Internet para acceder al vídeo en directo o grabado desde cualquier ubicación. Para obtener más información, consulte *axis.com/end-to-end-solutions/hosted-services*.

Allow O3C (Permitir O3C):

- **Un clic**: Esta es la configuración predeterminada. Mantenga pulsado el botón de control en el dispositivo para conectar con un servicio O3C a través de Internet. Debe registrar el dispositivo en el servicio O3C en un plazo de 24 horas después de pulsar el botón de control. De lo contrario, el dispositivo se desconecta del servicio O3C. Una vez que registre el dispositivo, **Always (Siempre)** quedará habilitado y el dispositivo permanecerá conectado al servicio O3C.
- **Siempre**: El dispositivo intenta conectarse continuamente a un servicio O3C a través de Internet. Una vez que registre el dispositivo, permanece conectado al servicio O3C. Utilice esta opción si el botón de control del dispositivo está fuera de su alcance.
- **No**: Deshabilita el servicio O3C.

Proxy settings (Configuración proxy): Si es necesario, escriba los ajustes del proxy para conectarse al servidor proxy.

Host: Introduzca la dirección del servidor proxy.

Puerto: Introduzca el número de puerto utilizado para acceder.

Inicio de sesión y **Contraseña**: En caso necesario, escriba un nombre de usuario y la contraseña del servidor proxy.

Authentication method (Método de autenticación):

- **Básico**: Este método es el esquema de autenticación más compatible con HTTP. Es menos seguro que el método **Digest** porque envía el nombre de usuario y la contraseña sin cifrar al servidor.
- **Digest**: Este método de autenticación es más seguro porque siempre transfiere la contraseña cifrada a través de la red.
- **Automático**: Esta opción permite que el dispositivo seleccione el método de autenticación automáticamente en función de los métodos admitidos. Da prioridad al método **Digest** por delante del **Básico**.

Owner authentication key (OAK) (Clave de autenticación de propietario [OAK]): Haga clic en **Get key (Obtener clave)** para obtener la clave de autenticación del propietario. Esto solo es posible si el dispositivo está conectado a Internet sin un cortafuegos o proxy.

SNMP

El protocolo de administración de red simple (SNMP) permite gestionar dispositivos de red de manera remota.

SNMP: Seleccione la versión de SNMP a usar.

- **v1 and v2c (v1 y v2c)**:
  - **Read community (Comunidad de lectura)**: Introduzca el nombre de la comunidad que tiene acceso de solo lectura a todos los objetos SNMP compatibles. El valor predeterminado es **público**.
  - **Write community (Comunidad de escritura)**: Escriba el nombre de la comunidad que tiene acceso de lectura o escritura a todos los objetos SNMP compatibles (excepto los objetos de solo lectura). El valor predeterminado es **escritura**.
  - **Activate traps (Activar traps)**: Active esta opción para activar el informe de trap. El dispositivo utiliza traps para enviar mensajes al sistema de gestión sobre eventos importantes o cambios de estado. En la interfaz web puede configurar traps para SNMP v1 y v2c. Las traps se desactivan automáticamente si cambia a SNMP v3 o desactiva SNMP. Si utiliza SNMP v3, puede configurar las traps a través de la aplicación de gestión de SNMP v3.
  - **Trap address (Dirección trap)**: introduzca la dirección IP o el nombre de host del servidor de gestión.
  - **Trap community (Comunidad de trap)**: Introduzca la comunidad que se utilizará cuando el dispositivo envía un mensaje trap al sistema de gestión.
  - **Traps**:
    - **Cold start (Arranque en frío)**: Envía un mensaje trap cuando se inicia el dispositivo.
    - **Warm start (Arranque templado)**: Envía un mensaje trap cuando cambia una configuración SNMP.
    - **Link up (Enlace hacia arriba)**: Envía un mensaje trap cuando un enlace cambia de abajo a arriba.
    - **Authentication failed (Error de autenticación)**: Envía un mensaje trap cuando se produce un error de intento de autenticación.

Nota

Todas las traps Axis Video MIB se habilitan cuando se activan las traps SNMP v1 y v2c. Para obtener más información, consulte *AXIS OS Portal > SNMP*.

- **v3**: SNMP v3 es una versión más segura que ofrece cifrado y contraseñas seguras. Para utilizar SNMP v3, recomendamos activar HTTPS, ya que la contraseña se envía a través de HTTPS. También evita que partes no autorizadas accedan a traps SNMP v1 y v2c sin cifrar. Si utiliza SNMP v3, puede configurar las traps a través de la aplicación de gestión de SNMP v3.
  - **Password for the account "initial" (contraseña para la cuenta "Inicial")**: Introduzca la contraseña de SNMP para la cuenta denominada "Initial". Aunque la contraseña se puede enviar sin activar HTTPS, no lo recomendamos. La contraseña de SNMP v3 solo puede establecerse una vez, y preferiblemente solo cuando esté activado HTTPS. Una vez establecida la contraseña, dejará de mostrarse el campo de contraseña. Para volver a establecer la contraseña, debe restablecer el dispositivo a su configuración predeterminada de fábrica.

Seguridad

Certificados

Los certificados se utilizan para autenticar los dispositivos de una red. Un dispositivo admite dos tipos de certificados:

- **Client/server certificates (Certificados de cliente/servidor)**
  Un certificado de cliente/servidor valida la identidad del dispositivo de Axis y puede firmarlo el propio dispositivo o emitirlo una autoridad de certificación (CA). Un certificado firmado por el propio producto ofrece protección limitada y se puede utilizar antes de que se obtenga un certificado emitido por una autoridad de certificación.
- **Certificados CA**
  Puede utilizar un certificado de la autoridad de certificación (AC) para autenticar un certificado entre iguales, por ejemplo, para validar la identidad de un servidor de autenticación cuando el dispositivo se conecta a una red protegida por IEEE 802.1X. El dispositivo incluye varios certificados de autoridad de certificación preinstalados.

Se admiten estos formatos:

- Formatos de certificado: .PEM, .CER y .PFX
- Formatos de clave privada: PKCS#1 y PKCS#12

Importante

Si restablece el dispositivo a los valores predeterminados de fábrica, se eliminarán todos los certificados. Los certificados CA preinstalados se vuelven a instalar.

Agregar certificado: Haga clic aquí para añadir un certificado.

- **Más** : Mostrar más campos que rellenar o seleccionar.
- **Almacenamiento de claves seguro**: Seleccione usar el **Elemento seguro** o **Trusted Platform Module 2.0** para almacenar la clave privada de forma segura. Para obtener más información sobre el almacén de claves seguro que desea seleccionar, vaya a *help.axis.com/en-us/axis-os#cryptographic-support*.
- **Tipo de clave**: Seleccione la opción predeterminada o un algoritmo de cifrado diferente en la lista desplegable para proteger el certificado.

El menú contextual contiene:

- **Certificate information (Información del certificado)**: Muestra las propiedades de un certificado instalado.
- **Delete certificate (Eliminar certificado)**: Se elimina el certificado.
- **Create certificate signing request (Crear solicitud de firma de certificado)**: Se crea una solicitud de firma de certificado que se envía a una autoridad de registro para solicitar un certificado de identidad digital.

Almacenamiento de claves seguro :

- **Elemento seguro (CC EAL6+)**: Seleccione para utilizar un elemento seguro para un almacén de claves seguro.
- **Trusted Platform Module 2.0 (CC EAL4+, FIPS 140-2 nivel 2)**: Seleccione para usar TPM 2.0 para el almacén de claves seguro.

Control y cifrado de acceso a la red

IEEE 802.1x

IEEE 802.1x es un estándar IEEE 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 de red deben autenticarse ellos mismos. Un servidor de autenticación lleva a cabo la autenticación, normalmente un servidor RADIUS (por ejemplo, FreeRADIUS y Microsoft Internet Authentication Server).

IEEE 802.1AE MACsec

IEEE 802.1AE MACsec es un estándar IEEE para la seguridad del control de acceso a medios (MAC) que define la confidencialidad e integridad de los datos sin conexión para protocolos independientes de acceso a medios.

Certificados

Si se configura sin un certificado de la autoridad de certificación, la validación de certificados del servidor se deshabilita y el dispositivo intentará autenticarse a sí mismo independientemente de la red a la que esté conectado.

Si se usa un certificado, en la implementación de Axis, el dispositivo y el servidor de autenticación se autentican ellos mismos con certificados digitales utilizando EAP-TLS (protocolo de autenticación extensible - seguridad de la capa de transporte).

Para permitir que el dispositivo acceda a una red protegida mediante certificados, debe instalar un certificado de cliente firmado en el dispositivo.

Authentication method (Método de autenticación): Seleccione un tipo de EAP utilizado para la autenticación.

Client certificate (Certificado del cliente): Seleccione un certificado de cliente para usar IEEE 802.1x. El servidor de autenticación utiliza el certificado para validar la identidad del cliente.

CA Certificates (Certificados de la autoridad de certificación): Seleccione certificados CA para validar la identidad del servidor de autenticación. Si no se selecciona ningún certificado, el dispositivo intentará autenticarse a sí mismo, independientemente de la red a la que esté conectado.

EAP identity (Identidad EAP): Introduzca la identidad del usuario asociada con el certificado de cliente.

EAPOL version (Versión EAPOL): Seleccione la versión EAPOL que se utiliza en el switch de red.

Use IEEE 802.1x (Utilizar IEEE 802.1x): Seleccione para utilizar el protocolo IEEE 802.1x.

Estos ajustes solo están disponibles si utiliza **IEEE 802.1x PEAP-MSCHAPv2** como método de autenticación:

- **Contraseña**: Escriba la contraseña para la identidad de su usuario.
- **Versión de Peap**: Seleccione la versión de Peap que se utiliza en el switch de red.
- **Label (Etiqueta)**: Seleccione 1 para usar el cifrado EAP del cliente; seleccione 2 para usar el cifrado PEAP del cliente. Seleccione la etiqueta que utiliza el switch de red cuando utilice la versión 1 de Peap.

Estos ajustes solo están disponibles si utiliza **IEEE 802.1ae MACsec (CAK estática/clave precompartida)** como método de autenticación:

- **Nombre de clave de asociación de conectividad de acuerdo de claves:** Introduzca el nombre de la asociación de conectividad (CKN). Debe tener de 2 a 64 caracteres hexadecimales (divisibles por 2). La CKN debe configurarse manualmente en la asociación de conectividad y debe coincidir con los dos extremos del enlace para activar inicialmente MACsec.
- **Clave de asociación de conectividad de acuerdo de claves**: Introduzca la clave de la asociación de conectividad (CAK). Debe tener una longitud de 32 o 64 caracteres hexadecimales. La CAK debe configurarse manualmente en la asociación de conectividad y debe coincidir con los dos extremos del enlace para activar inicialmente MACsec.

Evitar ataques de fuerza bruta

Blocking (Bloqueo): Active esta función para bloquear ataques de fuerza bruta. Un ataque de fuerza utiliza un sistema de ensayo y error para descubrir información de inicio de sesión o claves de cifrado.

Blocking period (Período de bloqueo): Introduzca el número de segundos para bloquear un ataque de fuerza bruta.

Blocking conditions (Condiciones de bloqueo): Introduzca el número de fallos de autenticación permitidos por segundo antes de que se inicie el bloqueo. Puede definir el número de fallos permitidos tanto a nivel de página como de dispositivo.

Firewall

Activar: Encienda el cortafuegos.

Política predeterminada: Seleccione el estado predeterminado para el cortafuegos.

- **Allow (Permitir):** Permite todas las conexiones al dispositivo. Esta opción está establecida de forma predeterminada.
- **Deny (Denegar):** Deniega todas las conexiones al dispositivo.

Para hacer excepciones a la política predeterminada, puede crear reglas que permiten o deniegan las conexiones al dispositivo desde direcciones, protocolos y puertos específicos.

- **Dirección**: Introduzca una dirección en formato IPv4/IPv6 o CIDR a la que desee permitir o denegar el acceso.
- **Protocol (Protocolo)**: Seleccione un protocolo al que desee permitir o denegar el acceso.
- **Puerto**: Introduzca un número de puerto al que desee permitir o denegar el acceso. Puede agregar un número de puerto entre 1 y 65535.
- **Policy (Directiva)**: Seleccione la política de la regla.

: Haga clic para crear otra regla.

Agregar reglas: Haga clic para agregar las reglas que haya definido.

- **Tiempo en segundos:** Defina un límite de tiempo para probar las reglas. El límite de tiempo predeterminado se establece en 300 segundos. Para activar las reglas inmediatamente, defina la hora en 0 segundos.
- **Confirmar reglas:** Confirme las reglas y su límite de tiempo. Si ha establecido un límite de tiempo de más de 1 segundo, las reglas estarán activas durante este periodo. Si ha ajustado la hora en 0, las reglas se activarán de inmediato.

Reglas pendientes: Información general de las reglas probadas recientemente que aún no ha confirmado.

Nota

Las reglas que tienen un límite de tiempo aparecen en **Active rules (Reglas activas)** hasta que se agota el temporizador mostrado o hasta que las confirme. Si no las confirma, aparecerán en **Pending rules (Reglas pendientes)** una vez que se agote el temporizador y el firewall volverá a los ajustes definidos anteriormente. Si los confirma, sustituirán las reglas activas actuales.

Confirmar reglas: Haga clic para activar las reglas pendientes.

Activar reglas: Información general de las reglas que ejecuta actualmente en el dispositivo.

: Haga clic para eliminar una regla activa.

: Haga clic para eliminar todas las reglas, tanto pendientes como activas.

Certificado de AXIS OS con firma personalizada

Para instalar en el dispositivo software de prueba u otro software personalizado de Axis, necesita un certificado de AXIS OS firmado personalizado. El certificado verifica que el software ha sido aprobado por el propietario del dispositivo y por Axis. El software solo puede ejecutarse en un dispositivo concreto identificado por su número de serie único y el ID de su chip. Solo Axis puede crear los certificados de AXIS OS firmados personalizados, ya que Axis posee la clave para firmarlos.

Install (Instalar): Haga clic para instalar el certificado. El certificado se debe instalar antes que el software.

El menú contextual contiene:

- **Delete certificate (Eliminar certificado)**: Se elimina el certificado.

Cuentas

Cuentas

Add account (Añadir cuenta): Haga clic para agregar una nueva cuenta. Puede agregar hasta 100 cuentas.

Cuenta: introduzca un nombre de cuenta único.

Nueva contraseña: introduzca una contraseña para la cuenta. Las contraseñas deben tener entre 1 y 64 caracteres. La contraseña solo admite caracteres ASCII imprimibles (códigos de 32 a 126), por ejemplo, letras, números, signos de puntuación y algunos símbolos.

Repetir contraseña: Introduzca la misma contraseña de nuevo.

Privilegios:

- **Administrador**: Tiene acceso completo a todos los ajustes. Los administradores también pueden agregar, actualizar y eliminar otras cuentas.
- **Operator (Operador)**: Tiene acceso a todos los ajustes excepto:
  - Todos los ajustes del **sistema**.
- **Viewer (Visualizador)**: No tiene acceso para cambiar ajustes.

El menú contextual contiene:

Actualizar cuenta: Editar las propiedades de la cuenta.

Eliminar cuenta: Elimine la cuenta. No puede eliminar la cuenta de root.

Cuentas SSH

Add SSH account (Agregar cuenta SSH): Haga clic para agregar una nueva cuenta SSH.

- **Restrinja el acceso root**: Active esta opción para restringir la funcionalidad que requiere acceso root.
- **Habilitar SSH**: Active el uso del servicio SSH.

Cuenta: introduzca un nombre de cuenta único.

Nueva contraseña: introduzca una contraseña para la cuenta. Las contraseñas deben tener entre 1 y 64 caracteres. La contraseña solo admite caracteres ASCII imprimibles (códigos de 32 a 126), por ejemplo, letras, números, signos de puntuación y algunos símbolos.

Repetir contraseña: Introduzca la misma contraseña de nuevo.

Comentario: Introduzca un comentario (opcional).

El menú contextual contiene:

Actualizar cuenta SSH: Editar las propiedades de la cuenta.

Eliminar cuenta SSH: Elimine la cuenta. No puede eliminar la cuenta de root.

Host virtual

Add virtual host (Agregar host virtual): Haga clic para agregar un nuevo host virtual.

Habilitada: Seleccione esta opción para usar este host virtual.

Server name (Nombre del servidor): Introduzca el nombre del servidor. Utilice solo los números 0-9, las letras A-Z y el guión (-).

Puerto: Introduzca el puerto al que está conectado el servidor.

Tipo: Seleccione el tipo de autenticación que desea usar. Seleccione entre **Basic**, **Digest** y **Open ID**.

El menú contextual contiene:

- **Update (Actualizar)**: Actualice el host virtual.
- **Eliminar**: Elimine el host virtual.

Disabled (Deshabilitado): El servidor está deshabilitado.

Configuración de OpenID

Importante

Si no puede utilizar OpenID para iniciar sesión, utilice las credenciales Digest o Basic que usó al configurar OpenID para iniciar sesión.

Client ID (ID de cliente): Introduzca el nombre de usuario de OpenID.

Outgoing Proxy (Proxy saliente): Introduzca la dirección de proxy de la conexión de OpenID para usar un servidor proxy.

Admin claim (Reclamación de administrador): Introduzca un valor para la función de administrador.

Provider URL (URL de proveedor): Introduzca el enlace web para la autenticación de punto de acceso de API. El formato debe ser https://[insertar URL]/.well-known/openid-configuration

Operator claim (Reclamación de operador): Introduzca un valor para la función de operador.

Require claim (Requerir solicitud): Introduzca los datos que deberían estar en el token.

Viewer claim (Reclamación de visor): Introduzca el valor de la función de visor.

Remote user (Usuario remoto): Introduzca un valor para identificar usuarios remotos. Esto ayudará a mostrar el usuario actual en la interfaz web del dispositivo.

Scopes (Ámbitos): Ámbitos opcionales que podrían formar parte del token.

Client secret (Secreto del cliente): Introduzca la contraseña de OpenID.

Save (Guardar): Haga clic para guardar los valores de OpenID.

Enable OpenID (Habilitar OpenID): Active esta opción para cerrar la conexión actual y permitir la autenticación del dispositivo desde la URL del proveedor.

MQTT

MQTT (Message Queuing Telemetry Transport) es un protocolo de mensajería estándar para Internet of things (IoT). Se diseñó para simplificar la integración del IoT y se utiliza en una amplia variedad de sectores para conectar dispositivos remotos con una huella de código pequeña y un ancho de banda de red mínimo. El cliente MQTT del software de dispositivos de Axis puede simplificar la integración de los datos y eventos producidos en el dispositivo con sistemas que no sean software de gestión de vídeo (VMS).

Configure el dispositivo como cliente MQTT. La comunicación MQTT se basa en dos entidades, los clientes y el intermediario. Los clientes pueden enviar y recibir mensajes. El intermediario es responsable de dirigir los mensajes entre los clientes.

Puede obtener más información sobre MQTT en la *AXIS OS Knowledge Base*.

ALPN

ALPN es una extensión de TLS/SSL que permite seleccionar un protocolo de aplicación durante la fase de enlace de la conexión entre el cliente y el servidor. Se utiliza para habilitar el tráfico MQTT a través del mismo puerto que se utiliza para otros protocolos, como HTTP. En algunos casos, es posible que no haya un puerto dedicado abierto para la comunicación MQTT. Una solución en tales casos es utilizar ALPN para negociar el uso de MQTT como protocolo de aplicación en un puerto estándar, permitido por los cortafuegos.

Cliente MQTT

Conectar: Active o desactive el cliente MQTT.

Estado: Muestra el estado actual del cliente MQTT.

Broker

Host: introduzca el nombre de host o la dirección IP del servidor MQTT.

Protocol (Protocolo): Seleccione el protocolo que desee utilizar.

Puerto: Introduzca el número de puerto.

- 1883 es el valor predeterminado de **MQTT a través de TCP**
- 8883 es el valor predeterminado de **MQTT a través de SSL**
- 80 es el valor predeterminado de **MQTT a través de WebSocket**
- 443 es el valor predeterminado de **MQTT a través de WebSocket Secure**

Protocol ALPN: Introduzca el nombre del protocolo ALPN proporcionado por su proveedor de MQTT. Esto solo se aplica con MQTT a través de SSL y MQTT a través de WebSocket Secure.

Nombre de usuario: Introduzca el nombre de cliente que utilizará la cámara para acceder al servidor.

Contraseña: Introduzca una contraseña para el nombre de usuario.

Client ID (ID de cliente): Introduzca una ID de cliente. El identificador de cliente que se envía al servidor cuando el cliente se conecta a él.

Clean session (Limpiar sesión): Controla el comportamiento en el momento de la conexión y la desconexión. Si se selecciona, la información de estado se descarta al conectar y desconectar.

Proxy HTTP: Una URL con una longitud máxima de 255 bytes. Puede dejar el campo vacío si no desea utilizar un proxy HTTP.

Proxy HTTPS: Una URL con una longitud máxima de 255 bytes. Puede dejar el campo vacío si no desea utilizar un proxy HTTPS.

Keep alive interval (Intervalo de Keep Alive): Habilita al cliente para detectar si el servidor ya no está disponible sin tener que esperar a que se agote el tiempo de espera de TCP/IP.

Timeout (Tiempo de espera): El intervalo de tiempo está en segundos para permitir que se complete la conexión. Valor predeterminado: 60

Device topic prefix (Prefijo de tema del dispositivo): se utiliza en los valores por defecto del tema en el mensaje de conexión, en el mensaje LWT de la pestaña **MQTT client (Cliente MQTT)** y, en las condiciones de publicación de la pestaña **MQTT publication (Publicación MQTT)** ".

Reconnect automatically (Volver a conectar automáticamente): especifica si el cliente debe volver a conectarse automáticamente tras una desconexión.

Mensaje de conexión

Especifica si se debe enviar un mensaje cuando se establece una conexión.

Enviar mensaje: Active esta función para enviar mensajes.

Usar predeterminado: Desactive esta opción para introducir su propio mensaje predeterminado.

Topic (Tema): Introduzca el tema para el mensaje predeterminado.

Payload (Carga): Introduzca el contenido para el mensaje predeterminado.

Retain (Retener): Seleccione esta opción para mantener el estado del cliente en este **Tema**

QoS: Cambie la capa de QoS para el flujo de paquetes.

Mensaje de testamento y últimas voluntades

El testamento y últimas voluntades (LWT) permite a un cliente proporcionar un testimonio junto con sus credenciales al conectar con el intermediario. Si el cliente se desconecta de forma no voluntaria (quizá porque no dispone de fuente de alimentación), puede permitir que el intermediario entregue un mensaje a otros clientes. Este mensaje de LWT tiene el mismo formato que un mensaje normal y se enruta a través de la misma mecánica.

Enviar mensaje: Active esta función para enviar mensajes.

Usar predeterminado: Desactive esta opción para introducir su propio mensaje predeterminado.

Topic (Tema): Introduzca el tema para el mensaje predeterminado.

Payload (Carga): Introduzca el contenido para el mensaje predeterminado.

Retain (Retener): Seleccione esta opción para mantener el estado del cliente en este **Tema**

QoS: Cambie la capa de QoS para el flujo de paquetes.

Publicación MQTT

Usar prefijo de tema predeterminado: Seleccione esta opción para utilizar el prefijo de tema predeterminado, que se define en el prefijo de tema del dispositivo en la pestaña **Cliente MQTT**.

Incluir nombre de tema: Seleccione esta opción para incluir el tema que describe la condición en el tema de MQTT.

Incluir espacios de nombres de tema: Seleccione esta opción para incluir los espacios de nombres de los temas ONVIF en el tema MQTT.

Include serial number (Incluir número de serie): seleccione esta opción para incluir el número de serie del dispositivo en la carga útil de MQTT.

Add condition (Agregar condición): Haga clic para agregar una condición.

Retain (Retener): define qué mensajes MQTT se envían como retenidos.

- **None (Ninguno)**: envíe todos los mensajes como no retenidos.
- **Property (Propiedad)**: envíe únicamente mensajes de estado como retenidos.
- **Todo**: Envíe mensajes con estado y sin estado como retenidos.

QoS: Seleccione el nivel deseado para la publicación de MQTT.

Suscripciones MQTT

Add subscription (Agregar suscripción): Haga clic para agregar una nueva suscripción MQTT.

Filtro de suscripción: Introduzca el tema de MQTT al que desea suscribirse.

Usar prefijo de tema del dispositivo: Agregue el filtro de suscripción como prefijo al tema de MQTT.

Tipo de suscripción:

- **Sin estado**: Seleccione esta opción para convertir mensajes MQTT en mensajes sin estado.
- **Con estado**: Seleccione esta opción para convertir los mensajes MQTT en una condición. El contenido se utiliza como estado.

QoS: Seleccione el nivel deseado para la suscripción a MQTT.

Accesorios

Puertos de E/S

Use la entrada digital para conectar seguridad positiva que pueda alternar entre circuitos abiertos y cerrados, por ejemplo, sensores PIR, contactos de puertas o ventanas y detectores de cristales rotos.

Use la salida digital para establecer conexión con dispositivos externos, como relés y LED. Puede activar los dispositivos conectados a través de la interfaz de programación de aplicaciones VAPIX® o la interfaz web.

Puerto

Name (Nombre): Edite el texto para cambiar el nombre del puerto.

Direction (Dirección):  indica que el puerto es un puerto de entrada.  indica que el puerto es un puerto de salida. Si el puerto es configurable, puede hacer clic en los iconos para cambiar entre entrada y salida.

Normal state (Estado normal): Haga clic  para circuito abierto y  para circuito cerrado.

Current state (Estado actual): muestra el estado actual del puerto. La entrada o salida se activa cuando el estado actual difiere del estado normal. Una entrada del dispositivo tiene el circuito abierto cuando está desconectado o cuando hay una tensión superior a 1 V CC.

Nota

Durante el reinicio, se abre el circuito de salida. Cuando termina el reinicio, el circuito vuelve a la posición normal. Si modifica algún ajuste de esta página, los circuitos de salida recuperan las posiciones normales, con independencia de los activadores activos.

Supervisado  : Active esta opción para que sea posible detectar y activar acciones si alguien manipula la conexión con dispositivos de E/S digital. Además de detectar si una entrada está abierta o cerrada, también puede detectar si alguien la ha manipulado (mediante un corte o cortocircuito). La supervisión de la conexión requiere hardware adicional (resistencias de final de línea) en el bucle de E/S externa.

Registros

Informes y registros

Informes

- **Ver informe del servidor del dispositivo**: Consulte información acerca del estado del producto en una ventana emergente. El registro de acceso se incluye automáticamente en el informe del servidor.
- **Download the device server report (Descargar informe del servidor del dispositivo)**: Se crea un archivo .zip que contiene un archivo de texto con el informe del servidor completo en formato UTF–8 y una instantánea de la imagen de visualización en directo actual. Incluya siempre el archivo. zip del informe del servidor si necesita contactar con el servicio de asistencia.
- **Download the crash report (Descargar informe de fallos)**: Descargar un archivo con la información detallada acerca del estado del servidor. El informe de fallos incluye información ya presente en el informe del servidor, además de información detallada acerca de la corrección de fallos. Este informe puede incluir información confidencial, como trazas de red. Puede tardar varios minutos en generarse.

Registros

- **View the system log (Ver registro del sistema)**: Haga clic para consultar información acerca de eventos del sistema como inicio de dispositivos, advertencias y mensajes críticos.
- **View the access log (Ver registro de acceso)**: Haga clic para ver todos los intentos incorrectos de acceso al dispositivo, por ejemplo, si se utiliza una contraseña de inicio de sesión incorrecta.

Rastreo de red

Importante

Un archivo de rastreo de red puede contener información confidencial, por ejemplo, certificados o contraseñas.

Un archivo de rastreo de red puede ayudar a solucionar problemas mediante la grabación de la actividad en la red.

Trace time (Tiempo de rastreo): Seleccione la duración del rastreo en segundos o minutos y haga clic en **Descargar**.

Registro de sistema remoto

Syslog es un estándar de registro de mensajes. Permite que el software que genera los mensajes, el sistema que los almacena y el software que los notifica y analiza sean independientes. Cada mensaje se etiqueta con un código de instalación, que indica el tipo de software que genera el mensaje y tiene un nivel de gravedad.

Server (Servidor): Haga clic para agregar un nuevo servidor.

Host: introduzca el nombre de host o la dirección IP del servidor.

Format (Formato): Seleccione el formato de mensaje de syslog que quiera utilizar.

- Axis
- RFC 3164
- RFC 5424

Protocol (Protocolo): Seleccione el protocolo que desee utilizar:

- UDP (el puerto predeterminado es 514).
- TCP (el puerto predeterminado es 601).
- TLS (el puerto predeterminado es 6514).

Puerto: Modifique el número de puerto para usar otro puerto.

Severity (Gravedad): Seleccione los mensajes que se enviarán cuando se activen.

CA certificate set (Conjunto de certificados de CA): Consulte los ajustes actuales o añada un certificado.

Mantenimiento

Restart (Reiniciar): Reiniciar el dispositivo. No afectará a la configuración actual. Las aplicaciones en ejecución se reinician automáticamente.

Restore (Restaurar): Casi todos los ajustes vuelven a los valores predeterminados de fábrica. Después deberás reconfigurar el dispositivo y las aplicaciones, reinstalar las que no vinieran preinstaladas y volver a crear los eventos y preajustes.

Importante

Los únicos ajustes que se guardan después de una restauración son:

- Protocolo de arranque (DHCP o estático)
- Dirección IP estática
- Router predeterminado
- Máscara de subred
- Configuración 802.1X
- Configuración de O3C
- Dirección IP del servidor DNS

Factory default (Predeterminado de fábrica): Todos los ajustes vuelven a los valores predeterminados de fábrica. Después, es necesario restablecer la dirección IP para poder acceder al dispositivo.

Nota

Todo el software de los dispositivos AXIS está firmado digitalmente para garantizar que solo se instala software verificado. Esto aumenta todavía más el nivel mínimo general de ciberseguridad de los dispositivo de Axis. Para obtener más información, consulte el documento técnico "Axis Edge Vault" en *axis.com*.

Actualización de AXIS OS: Se actualiza a una nueva versión de AXIS OS. Las nuevas versiones pueden contener mejoras de funciones, correcciones de errores y características totalmente nuevas. Le recomendamos que utilice siempre la versión de AXIS OS más reciente. Para descargar la última versión, vaya a *axis.com/support*.

Al actualizar, puede elegir entre tres opciones:

- **Standard upgrade (Actualización estándar)**: Se actualice a la nueva versión de AXIS OS.
- **Factory default (Predeterminado de fábrica)**: Se actualiza y todos los ajustes vuelven a los valores predeterminados de fábrica. Si elige esta opción, no podrá volver a la versión de AXIS OS anterior después de la actualización.
- **Autorollback (Restauración automática a versión anterior)**: Se actualiza y debe confirmar la actualización en el plazo establecido. Si no confirma la actualización, el dispositivo vuelve a la versión de AXIS OS anterior.

Restaurar AXIS OS: Se vuelve a la versión anterior de AXIS OS instalado.

Descubrir más

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*.

Servicio de notificación de seguridad de Axis

Axis ofrece un servicio de notificación con información sobre vulnerabilidad y otros asuntos relacionados con la seguridad de los dispositivos Axis. Para recibir notificaciones, puede suscribirse en *axis.com/security-notification-service*.

Gestión de las vulnerabilidades

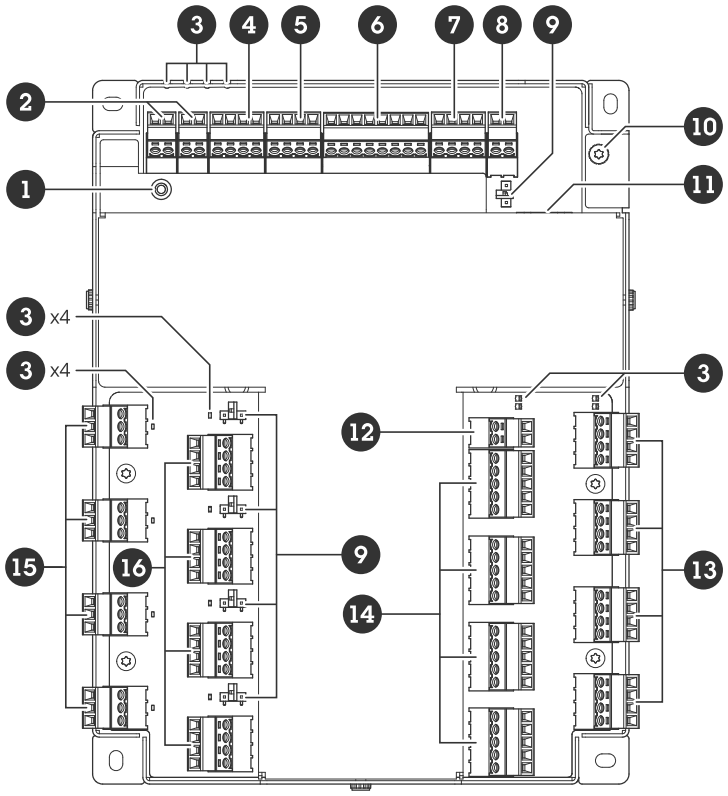
Para minimizar el riesgo de exposición de los clientes, Axis, como **autoridad de numeración común (CNA) de vulnerabilidades y exposiciones comunes (CVE)**, sigue los estándares del sector para gestionar y responder a las vulnerabilidades detectadas en nuestros dispositivos, software y servicios. Para obtener más información sobre la política de gestión de vulnerabilidades de Axis, cómo informar de vulnerabilidades, vulnerabilidades ya detectadas y los correspondientes avisos de seguridad, consulte *axis.com/vulnerability-management*.

Funcionamiento seguro de dispositivos Axis

Los dispositivos de Axis con ajustes predeterminados de fábrica se configuran previamente con mecanismos de protección predeterminados seguros. Recomendamos utilizar más configuración de seguridad al instalar el dispositivo. Para obtener más información sobre las guías de protección de Axis y otra documentación relacionada con la ciberseguridad, vaya a *axis.com/support/cybersecurity/resources*.

Especificaciones

Guía de productos



1 *Botón de control*
2 *Manipulación/alarma*
3 *LED*
4 *Conector auxiliar*
5 *Conector de salida*
6 *Conector de entrada*
7 *Conector de relé*
8 *Conector de alimentación (DC IN)*
9 *Puente de relé*
10 *Posición de toma de tierra*
11 *Conector de red*
12 *Conector de alimentación (DC IN PUERTA 1–4)*
13 *Conector de lector*
14 *Conector de puerta*
15 *Conector de relé AUX*
16 *Conector de relé de puerta*

Indicadores LED

LED	Color	Indicación
Estado (STAT)	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 (NET)	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 (PWR)	Verde	Funcionamiento normal.
	Ámbar	Parpadea en verde/ámbar durante la actualización del firmware.
Relé (RELÉ)	Verde	Relé activo. (*)
	Apagado	Relé inactivo.

LED PUERTA 1–4	**Color**	**Indicación**
Estado (STAT)	Verde	Parpadea (enciende durante 1 segundo, se paga durante 1 segundo) cuando está sin conexión.
	Verde	Parpadea (encendido durante 200 milisegundos, apagado durante 2 segundos) cuando está conectado.
	Rojo	Parpadea en verde/rojo durante la actualización del software del dispositivo.
Potencia (PWR)	Verde	Funcionamiento normal.
RS485 sobretensión (LECTOR OC)	Rojo	Fallo de sobretensión o subtensión en cualquier puerto RS485.
Sobretensión de relé (RELÉ OC)	Rojo	Fallo de sobretensión o subtensión en cualquier puerto de relé.
Relé (RELÉ)	Verde	Relé activo. (*)
	Apagado	Relé inactivo.
Relé AUX (RELÉ)	Verde	Relé activo. (*)
	Apagado	Relé inactivo.

(*) El relé está activo cuando COM está conectado a NO.

Botones

Botón de control

El botón de control se utiliza para lo siguiente:

- Restablecer el producto a la configuración predeterminada de fábrica. Vea .

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 AXIS 30 W Midspan.

Opciones de alimentación

Para alimentar el dispositivo, es necesario conectar los siguientes conectores:

1. PoE o DC IN. Consulte .
2. DC IN PUERTA 1–4 (obligatorio).

Prioridad de potencia

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

Conector de alimentación

Dos bloques de terminales de 2 pines para la entrada de alimentación de CC. Vea .

CC IN

Opcional para alimentar el dispositivo. Puede utilizar PoE en su lugar. Vea .

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.

DC IN PUERTA 1–4

Obligatorio para alimentar el dispositivo.

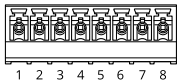
Función	Pin	Notas	Especificaciones
Tierra CC (GND)	1		0 V CC
Entrada CC	2	Obligatorio para alimentar el dispositivo. Nota: Este pin solo se puede utilizar como entrada de alimentación.	12 V CC, 96 W máx.

UL: Una fuente de alimentación UL 294, UL 603 o UL 2610 debe suministrar la alimentación de CC, en función de la aplicación, con las clasificaciones adecuadas.

Conector de entrada

Un bloque de terminales de 8 pines

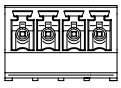
Las entradas digitales admiten la supervisión con resistencias de final de línea. Si se interrumpe la conexión, se activa una alarma. Para utilizar entradas con supervisión, debe instalar resistencias de fin de línea. Use el diagrama de conexión para las entradas supervisadas. Vea .



Función	Pin	Nota	Especificaciones
Tierra CC (GND)	1, 3, 5, 7		0 V CC
Entrada	2, 4, 6	Entrada digital: conéctela al pin 1 para activarla, o bien déjela suelta (sin conectar) para desactivarla. Posibilidad de supervisión. Vea .	0–30 V CC
+12 V CC	8		Máx. 190 mA

Conector de salida

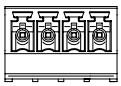
Un bloque de terminales de 4 pines



Función	Pin	Especificaciones
Tierra CC (GND)	1	0 V CC
Salida	2,3,4	Colector abierto, 0–30 V CC, 100 mA máx.

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.	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.	

Nota

El relé se separa 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	1 900 mA	1000 mA
PoE	150 mA	50 mA
PoE+	920 mA	420 mA

AVISO

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

Conector auxiliar

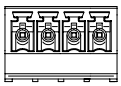
Utilice el conector auxiliar con dispositivos externos, por ejemplo, en combinación con detección de movimiento, activación de eventos y notificaciones de alarma. Además del punto de referencia de 0 V CC y la alimentación (salida de CC), el conector auxiliar ofrece la interfaz para:

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.

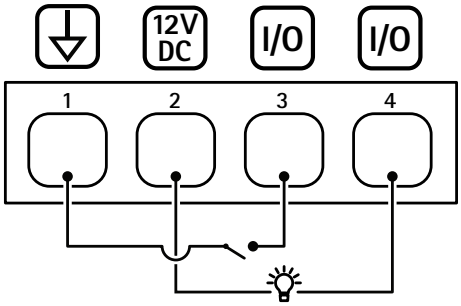
Entrada supervisada – Permite detectar la manipulación de una señal digital.

Salida digital – 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 = 250 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



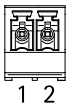
1 *Tierra CC*
2 *Salida de CC 12 V*
3 *E/S configurada como entrada*
4 *E/S configurada como salida*

Conector de manipulación/alarma

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. Posibilidad de supervisión. Vea .	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. Posibilidad de supervisión. Vea .	De 0 a 30 V CC máx.

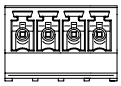
Conector de lector

Cuatro bloques de terminales de 4 pines que admiten el protocolo OSDP para la comunicación con el lector.

Puede conectar hasta ocho lectores OSDP o Wiegand. 2 A a 12 V CC están reservados para los lectores conectados a PUERTA 1-4.

Nota

Los lectores Wiegand requieren AXIS TA1101-B Wiegand to OSDP converter conectado entre el lector y el controlador.



Configurado para un lector OSDP

Función	Pin	Nota	Especificaciones
Tierra CC (GND)	1		0 V CC
Salida de CC (+12 V)	2	Proporciona alimentación al lector.	12 V CC, total combinado de 2 A para todos los conectores de lector.
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, total combinado de 2 A para todos los conectores de lector.
A	3	Semidúplex	
B	4	Semidúplex	

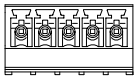
Importante

- Cuando el lector recibe alimentación del controlador, la longitud hábil del cable es de hasta 200 m (656 pies) si se cumple el siguiente requisito de cable: AWG 22-14. Verificado solo para lectores Axis.
- Cuando el lector no recibe alimentación del controlador, la longitud hábil del cable para datos de lector es de hasta 1000 m (3280,8 pies) si se cumplen los siguientes requisitos de cable: 1 par trenzado, AWG 26–14. Verificado solo para lectores Axis.

Conector de puerta

Cuatro bloques de terminales de 5 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. Vea .



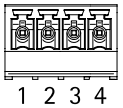
Función	Pin	Notas	Especificaciones
Tierra CC (GND)	1, 3		0 V CC
Entrada	2, 4	Para la comunicación con el monitor de la puerta. Entrada digital o entrada supervisada: conéctela al pin 1 o 3 respectivamente para activar, o dejar flotando (desconectado) para desactivar.	De 0 a 30 V CC máx.
+12 V CC	5	Suministra energía a dispositivos como sensores de puerta.	Total combinado de 400 mA para todos los conectores de puerta

Importante

La longitud de cable cualificada es de hasta 200 m si se cumplen los siguientes requisitos de cable: AWG 24–14.

Conector de relé de puerta

Cuatro bloques 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.	Corriente máx. = 4 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.	

Nota

El relé se separa 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
COM Total combinado de 46 W para todos los conectores de relé de puerta	Total combinado de 3,8 A para todos los conectores de relé de puerta	Total combinado de 1,5 A para todos los conectores de relé de puerta

AVISO

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

Conector de relé AUX

Cuatro bloques de terminales de 3 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
NO	1	Normalmente abierto. Para conectar dispositivos de relés. Conecte un bloqueo de seguridad negativa entre NO y masa CC.	Corriente máx. = 2 A Voltaje máx. = 30 V CC
COM	2	Común	

NC	3	Normalmente cerrado. Para conectar dispositivos de relés. Conecte un bloqueo de seguridad negativa entre NC y masa CC.	

Nota

El relé se separa de forma galvanizada del resto del circuito si no se utilizan puentes.

AVISO

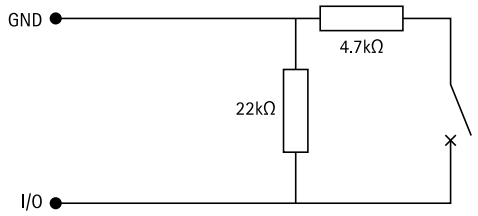
Si la cerradura no está polarizada, le recomendamos añadir un diodo de regreso externo.

Entradas con supervisión

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

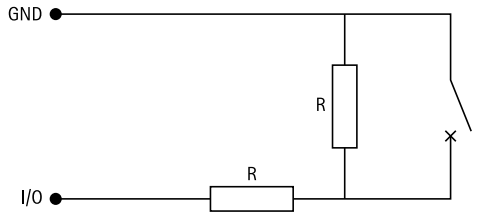
Parallel first connection (Primera conexión en paralelo)

Los valores de la resistencia deben ser de 4,7 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.

Estado	Descripción
Abierto	El switch supervisado está en modo abierto.
Cerrado	El switch supervisado está en modo cerrado.
Corto	El cable de E/S está en cortocircuito con tierra.
Cortar	El cable de E/S 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 .
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

- Cuando actualice el software del dispositivo se guardan los ajustes preconfigurados y personalizados

(siempre que dicha función esté disponible en el AXIS OS nuevo), si bien Axis Communications AB no puede garantizarlo.

- 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*.

Nota

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, consejos y soluciones

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

Problemas para actualizar AXIS OS

Fallo 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

El dispositivo se encuentra en una subred distinta	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 ya la utiliza otro dispositivo	Desconecte el dispositivo de Axis de la red. Ejecute el comando ping (en una ventana de comando/DOS, escriba `ping` y la dirección IP del dispositivo): • Si recibe: `Reply from <IP address>: bytes=32; time=10...` (Respuesta desde dirección IP: bytes=32; tiempo=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 dispositivo. • 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.
Posible conflicto de dirección IP con 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.

No se puede acceder al dispositivo desde un navegador

No se puede iniciar sesión	Cuando HTTPS esté activado, asegúrese de utilizar 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 para la cuenta de root, habrá que restablecer el dispositivo a los ajustes predeterminados de fábrica. Vea .
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 necesario, se puede asignar una dirección IP estática manualmente. 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**.

Se puede acceder al dispositivo localmente pero no externamente

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 5: versión de prueba de 30 días gratuita, ideal para sistemas de tamaño pequeño y medio.
- 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*.

No se puede conectar a través del puerto 8883 con MQTT a través de SSL	
El cortafuegos bloquea el tráfico que utiliza el puerto 8883 por considerarse inseguro.	En algunos casos, el servidor/intermediario podría no proporcionar un puerto específico para la comunicación MQTT. Aun así, puede 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.

Contactar con la asistencia técnica

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

T10217727_es

2025-03 (M9.3)