

Controlador de accesos en red AXIS A1610 Network Door Controller

Manual del usuario

Controlador de accesos en red AXIS A1610 Network Door Controller

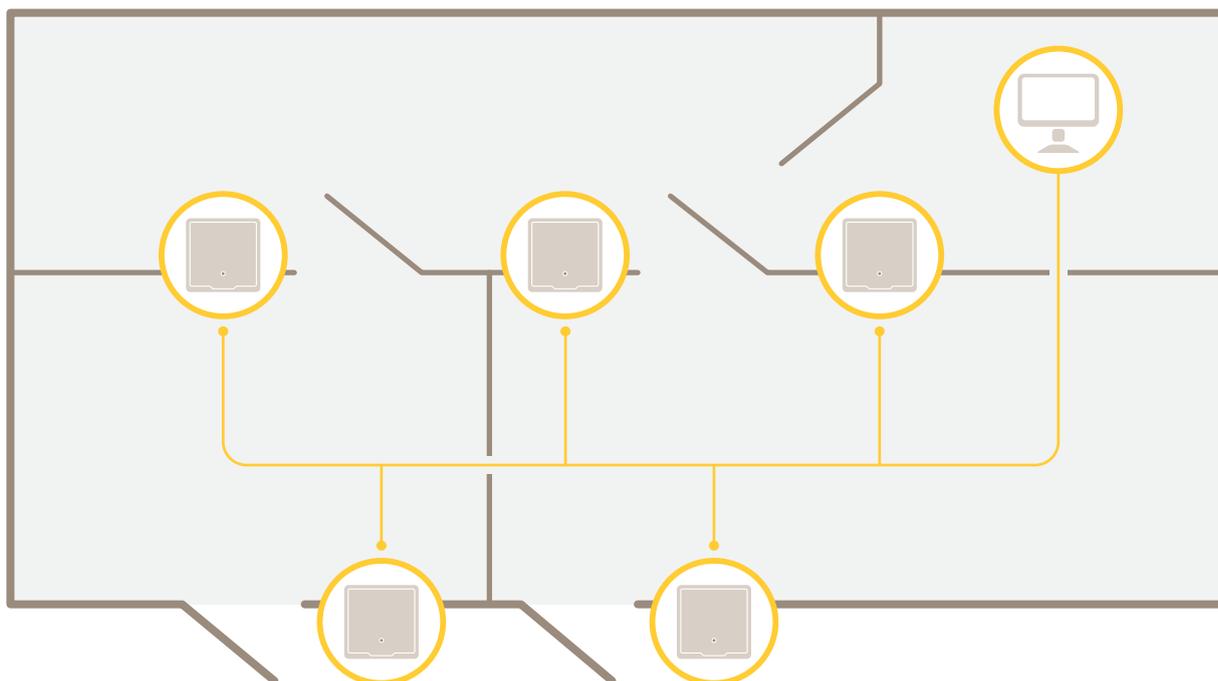
Índice

Descripción general de la solución	3
Procedimientos iniciales	5
Localice el dispositivo en la red	5
Abrir la interfaz web del dispositivo	5
Crear una cuenta de administrador	5
Contraseñas seguras	5
Comprobar que no se ha manipulado el software del dispositivo	6
Información general de la interfaz web	6
Configure su dispositivo	7
Interfaz web	8
Estado	8
Control de acceso	9
Sistema	9
Mantenimiento	20
Descubrir más	22
Ciberseguridad	22
Especificaciones	23
Información general del producto	23
Indicadores LED	23
Botones	24
Conectores	24
Solución de problemas	31
Restablecimiento a la configuración predeterminada de fábrica	31
Opciones de AXIS OS	31
Comprobar la versión de AXIS OS	31
Actualización de AXIS OS	31
Problemas técnicos, consejos y soluciones	32
Consideraciones sobre el rendimiento	33
Contacto con asistencia técnica	34

Controlador de accesos en red AXIS A1610 Network Door Controller

Descripción general de la solución

Descripción general de la solución



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

Controlador de accesos en red AXIS A1610 Network Door Controller

Descripción general de la solución



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

Controlador de accesos en red AXIS A1610 Network Door Controller

Procedimientos iniciales

Procedimientos iniciales

Localice el dispositivo en la red

Para localizar dispositivos 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 **Ajustes > Safari > Avanzadas > Características 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 *Crear una cuenta de administrador en la página 5*.

Para obtener descripciones de todos los controles y opciones de la interfaz web del dispositivo, consulte *Interfaz web en la página 8*.

Crear una cuenta de administrador

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

1. Escriba un nombre de usuario.
2. Escriba una contraseña. Vea *Contraseñas seguras en la página 5*.
3. Vuelva a escribir la contraseña.
4. Aceptar el acuerdo de licencia.
5. Haga clic en **Add account (agregar cuenta)**.

Importante

El dispositivo no tiene una cuenta predeterminada. Si pierde la contraseña de la cuenta de administrador, debe restablecer el dispositivo. Vea *Restablecimiento a la configuración predeterminada de fábrica en la página 31*.

Controlador de accesos en red AXIS A1610 Network Door Controller

Procedimientos iniciales

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 *Restablecimiento a la configuración predeterminada de fábrica en la página 31*.

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.



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

help.axis.com/?&pid=81253§ion=web-interface-overview

Interfaz web del dispositivo Axis

Controlador de accesos en red AXIS A1610 Network Door Controller

Configure su dispositivo

Configure su dispositivo

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

Controlador de accesos en red AXIS A1610 Network Door Controller

Interfaz web

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.

-  Muestre u oculte el menú principal.
-  Acceda a las notas de la versión.
-  Acceda a la ayuda del producto.
-  Cambie el idioma.
-  Defina 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.
 - **Interfaz de dispositivo existente**: Cambie la interfaz web del dispositivo a la versión existente.

Estado

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.

Ajustes de NTP: Ver y actualizar los ajustes de NTP. Le lleva a la página **Fecha y hora**, donde puede cambiar los ajustes de NTP.

Información del 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.

Interfaz web

Control de acceso

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 (Apertura de carcasa)  : 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 K Ω parallel resistor and a 4.7 K Ω serial resistor** (Primera conexión en paralelo con una resistencia de 22 K Ω en paralelo y una resistencia de 4,7 K Ω 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

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.

Sistema

Hora y ubicación

Fecha y hora

El formato de fecha y hora depende de los ajustes 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 entrada 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.

Controlador de accesos en red AXIS A1610 Network Door Controller

Interfaz web

- **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 entrada 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.

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.

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.

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: Escriba 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

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.

Nombre de host: Escriba 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 -.

Servidores DNS

Controlador de accesos en red AXIS A1610 Network Door Controller

Interfaz web

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.

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.

Servidores DNS: Haga clic en **Agregar servidor DNS** y escriba la dirección IP del servidor DNS. Este servidor proporciona la traducción de nombres de host a las direcciones IP de su red.

HTTP and HTTPS (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): Escriba el HTTP port (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 escribir cualquier puerto en el rango 1-1023. Si utiliza un puerto en este rango, recibirá una advertencia.

HTTPS port (Puerto HTTPS): Escriba 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 escribir cualquier puerto en el rango 1-1023. Si utiliza un puerto en este rango, recibirá una advertencia.

Certificate (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.

Bonjour name (Nombre de Bonjour): Escriba 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.

UPnP name (Nombre de UPnP): Escriba 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.

One-click cloud connection (Conexión a la nube con un solo 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.

Controlador de accesos en red AXIS A1610 Network Door Controller

Interfaz web

Allow O3C (Permitir O3C):

- **One-click (Un clic):** Estos son los ajustes predeterminados. 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.
- **Always (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 (Ajustes del proxy): Si es necesario, escriba los ajustes del proxy para conectarse al servidor proxy.

Host: Escriba la dirección del servidor proxy.

Port (Puerto): Escriba el número de puerto utilizado para acceder.

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

Authentication method (Método de autenticación):

- **Basic (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 Basic (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 **public (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 **write (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](#).

Controlador de accesos en red AXIS A1610 Network Door Controller

Interfaz web

- **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.

Connected clients (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.

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 obtener un certificado emitido por una autoridad de certificación.
- **Certificados AC**
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.



Add certificate (Agregar certificado): Haga clic aquí para agregar un certificado.

- **More (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  :

Controlador de accesos en red AXIS A1610 Network Door Controller

Interfaz web

- **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.

IEEE 802.1x e IEEE 802.1AE MACsec

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).

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. La opción predeterminada es EAP-TLS. EAP-PEAP/MSCHAPv2 es una opción más segura.

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.

Certificado CA: 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.

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.

Los ajustes solo están disponibles si utiliza EAP-TLS como método de autenticación:

Mode (Modo)

- **Dynamic CAK / EAP-TLS**: La opción predeterminada. Después de una conexión segura, el dispositivo busca MACsec en la red.
- **CAK estática/clave precompartida (PSK)**: Seleccione para configurar el nombre y el valor de la clave para conectarse a la red.

Los ajustes solo están disponibles si utiliza EAP-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.

Prevent brute-force attacks (Evitar ataques de fuerza bruta)

Controlador de accesos en red AXIS A1610 Network Door Controller

Interfaz web

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.
- **Port (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 establecido la hora para 0, las reglas se activarán inmediatamente.

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 **Pending rules (Reglas pendientes)** y **Active rules (Reglas activas)** hasta que ha transcurrido el tiempo establecido, o hasta que las confirma. Si no las confirma, solo aparece en **Pending rules (Reglas pendientes)** y el cortafuegos 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

Controlador de accesos en red AXIS A1610 Network Door Controller

Interfaz web

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



Agregar 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.
 - Agregar aplicaciones
- **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.

MQTT

MQTT (Message Queuing Telemetry Transport) es un protocolo de mensajería estándar para Internet of things (IoT). Se diseñó para integración simplificada de 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 *Portal AXIS OS*.

ALPN

Controlador de accesos en red AXIS A1610 Network Door Controller

Interfaz web

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 (Intermediario)

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

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

Port (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.

Connect message (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.

Controlador de accesos en red AXIS A1610 Network Door Controller

Interfaz web

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.

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.

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



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



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.

Controlador de accesos en red AXIS A1610 Network Door Controller

Interfaz web

Accesorios

I/O ports (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.

Port (Puerto)

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.

 **Supervised (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.

Logs (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 el 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.

Logs (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

Controlador de accesos en red AXIS A1610 Network Door Controller

Interfaz web

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 **Download (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).

Port (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 CA): Consulte los ajustes actuales o añada un certificado.

Mantenimiento

Restart (Reiniciar): Reiniciar el dispositivo. La configuración actual no se verá afectada. Las aplicaciones en ejecución se reinician automáticamente.

Restore (Restaurar): *Casi todos* los ajustes vuelven a los valores predeterminados de fábrica. Después deberá 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
- Enrutador predeterminado
- Máscara de subred
- Configuración de 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.

Controlador de accesos en red AXIS A1610 Network Door Controller

Interfaz web

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 dispositivos 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.

Controlador de accesos en red AXIS A1610 Network Door Controller

Descubrir más

Descubrir más

Ciberseguridad

Sistema operativo firmado

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

Arranque seguro

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

Axis Edge Vault

Por su parte, Axis Edge Vault proporciona una plataforma de ciberseguridad de 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. Se basa en una sólida base de módulos de computación criptográficos (elemento seguro y TPM) y seguridad SoC (TEE y arranque seguro), combinados con experiencia en seguridad de dispositivos locales.

ID de dispositivo de AXIS

La posibilidad de verificar el origen del dispositivo es esencial para establecer la fiabilidad de la identidad del dispositivo. Cuando se fabrican, los dispositivos con Axis Edge Vault reciben un certificado de ID de dispositivo de Axis único y proporcionado en la fábrica que cumple la norma IEEE 802.1AR. Funciona como un pasaporte que prueba el origen del dispositivo. El ID de dispositivo se almacena de forma segura y permanente en el almacén de claves seguro como certificado firmado por un certificado root 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.

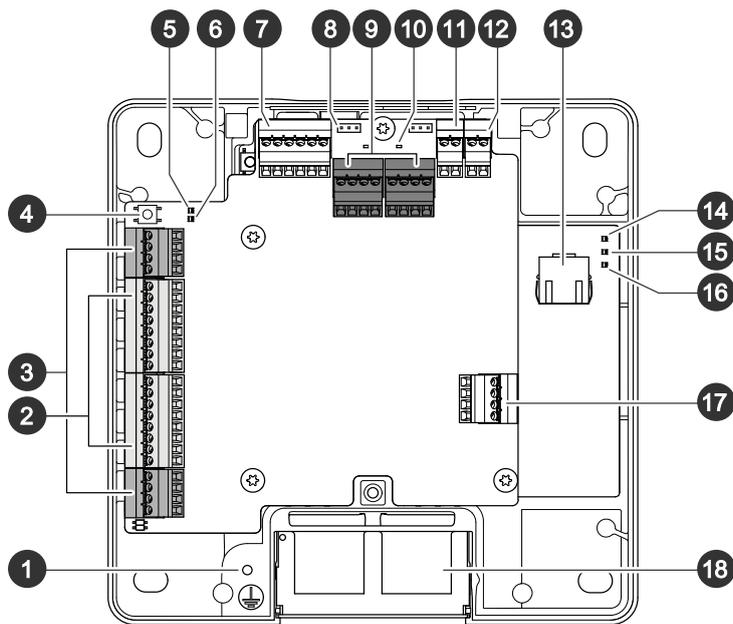
Para obtener más información sobre las características de ciberseguridad de los dispositivos Axis, vaya a axis.com/learning/white-papers y busque ciberseguridad.

Controlador de accesos en red AXIS A1610 Network Door Controller

Especificaciones

El texto marcado UL solo es válido para instalaciones UL 294.

Información general del producto



- 1 Posición de masa
- 2 Conector de lector, 2x
- 3 Conector de puerta, 2x
- 4 Botón de control
- 5 Led de sobrecorriente del relé
- 6 LED de sobrecorriente de lector
- 7 Conector auxiliar
- 8 Puente de relé, 2x
- 9 Conector de relé, 2x
- 10 LED de relé, 2x
- 11 Entrada de alimentación de seguridad de 12 V
- 12 Conector de alimentación
- 13 Conector de red
- 14 Alimentación de LED
- 15 LED de estado
- 16 LED de red
- 17 Conector externo
- 18 Cubierta de cable reversible

Controlador de accesos en red AXIS A1610 Network Door Controller

Especificaciones

Indicadores LED

LED	Color	Indicación
Red	Verde	Fijo para indicar una conexión a una red de 100 MBits/s. Parpadea cuando hay actividad de red.
	Ámbar	Fijo para indicar una conexión a una red de 10 MBits/s. Parpadea cuando hay actividad de red.
	Apagado	No hay conexión a la red.
Estado	Verde	Fijo en verde para indicar un funcionamiento normal.
	Ámbar	Fijo durante el inicio y al restaurar valores de configuración.
	Rojo	Parpadea despacio si se ha producido un error en una actualización.
Alimentación	Verde	Funcionamiento normal.
	Ámbar	Parpadea en verde/ámbar durante la actualización del firmware.
Sobrecorriente de relé	Rojo	Fijo con cortocircuito o si se ha detectado sobretensión.
	Apagado	Funcionamiento normal.
Sobrecorriente del lector	Rojo	Fijo con cortocircuito o si se ha detectado sobretensión.
	Apagado	Funcionamiento normal.
Relé	Verde	Relé activo. ¹
	Apagado	Relé inactivo.

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

Nota

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

Botones

Botón de control

El botón de control se utiliza para lo siguiente:

- Restablecer el producto a los ajustes predeterminados de fábrica. Consulte *Restablecimiento a la configuración predeterminada de fábrica en la página 31*.

Conectores

Conector de red

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

UL: La alimentación a través de Ethernet (PoE) se debe suministrar mediante un inyector de alimentación 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 incluidos en la lista UL 294 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.

Controlador de accesos en red AXIS A1610 Network Door Controller

Especificaciones

Prioridad de potencia

Este dispositivo puede recibir alimentación mediante una entrada de PoE o CC. Consulte *Conector de red en la página 24* y *Conector de alimentación en la página 30*.

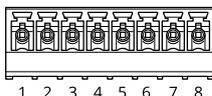
- Cuando PoE y CC se conectan antes de que se encienda el dispositivo, PoE se utiliza para la alimentación.
- PoE y CC están conectados y PoE está conectado actualmente. Cuando se pierde PoE, el dispositivo utiliza CC para proporcionar alimentación sin reiniciar.
- PoE y CC están conectados y CC está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

Conector de lector

Dos bloques de terminales de 8 pines, ambos compatibles con los protocolos RS485 y Wiegand para la comunicación con el lector.

Los valores especificados de salida de potencia se comparten entre los dos puertos de lector. Esto significa que se reservan 500 mA a 12 V CC para todos los lectores conectados al controlador de puerta.

Seleccione el protocolo que desea utilizar en la página web del producto.



Configurado para RS485

Función	Pin	Nota	Especificaciones
Tierra CC (GND)	1		0 V CC
Salida de CC (+12 V)	2	Proporciona alimentación al lector.	12 V CC, máx. 500 mA combinados para todos los lectores
RX/TX	3-4	Full-duplex: RX. Half-duplex: RX/TX.	
TX	5-6	Full duplex: TX.	
Configurable (entrada o salida)	7-8	Entrada digital: conéctela al pin 1 para activarla o bien déjela suelta (desconectada) para desactivarla.	De 0 a 30 V CC máx.
		Salida digital: Si se utiliza con una carga inductiva, como un relé, conecte un diodo en paralelo a la carga como protección contra transitorios de tensión.	De 0 a 30 V CC máx., colector abierto, 100 mA

Controlador de accesos en red AXIS A1610 Network Door Controller

Especificaciones

Importante

- Cuando el controlador alimenta el lector, la longitud de cable cualificada es de hasta 200 m.
- Si el controlador no alimenta el lector, la longitud de cable cualificada para datos del lector es de hasta 1000 m (3280,8 ft) si se cumplen los siguientes requisitos de cable: 1 par trenzado con blindaje, AWG 20-16.

Configurado para Wiegand

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

Importante

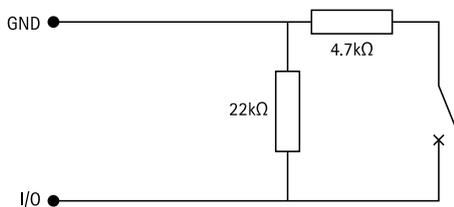
- Cuando el controlador alimenta el lector, la longitud de cable cualificada es de hasta 150 m.
- Si el controlador no alimenta el lector, la longitud de cable cualificada para datos del lector es de hasta 150 m si se cumple el siguiente requisito de cable: AWG 20-16.

Entradas supervisadas

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 .

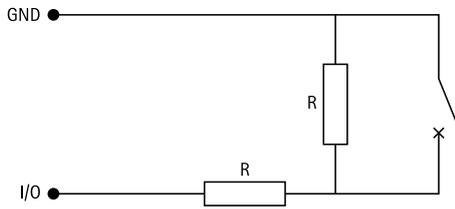


Serial first connection (Primera conexión en serie)

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 .

Controlador de accesos en red AXIS A1610 Network Door Controller

Especificaciones



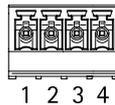
Nota

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

Conector de puerta

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

El monitor de puerta admite supervisión con resistencias de final de línea. Si se interrumpe la conexión, se activa una alarma. Para usar entradas supervisadas, instale las resistencias de final de línea. Use el diagrama de conexión para las entradas supervisadas. Consulte *Entradas supervisadas en la página 26*.



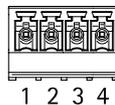
Función	Pin	Notas	Especificaciones
Tierra CC	1, 3		0 V CC
Entrada	2, 4	Para comunicarse con el monitor de puerta. Entrada digital o entrada supervisada – Conectar a pin 1 o 3 respectivamente para activar o dejar suelta (desconectada) para desactivar.	De 0 a 30 V CC máx.

Importante

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

Conector de relé

Dos 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
Masa CC (GND)	1		0 V CC

Controlador de accesos en red AXIS A1610 Network Door Controller

Especificaciones

NO	2	Normalmente abierto. Para conectar dispositivos de relés. Conecte una cerradura con seguridad ante fallos entre NO y Tierra CC. Los dos pins de relé tienen separación galvánica del resto del circuito si no se utilizan los puentes.	Corriente máxima = 2 A por relé Tensión máxima = 30 V CC
COM	3	Común	
NC	4	Normalmente cerrado. Para conectar dispositivos de relés. Conecte una cerradura con protección ante fallos entre NC y Tierra CC. Los dos pins de relé tienen separación galvánica del resto del circuito si no se utilizan los 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 ¹	Potencia máxima a 24 V CC
CC IN	1800 mA	750 mA
PoE	900 mA	410 mA

1. La alimentación se comparte entre los dos relés y E/S AUX 12 V CC.

AVISO

Si la cerradura no está polarizada, le recomendamos agregar un diodo de retorno externo.

Conector auxiliar

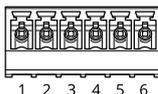
Utilice el conector auxiliar con dispositivos externos, por ejemplo, en combinación con detección de movimiento, activación de eventos y notificaciones de alarma. Además del punto de referencia de 0 V CC y la alimentación (salida de CC), el conector auxiliar ofrece la interfaz para:

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

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

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

Bloque de terminales de 6 pines

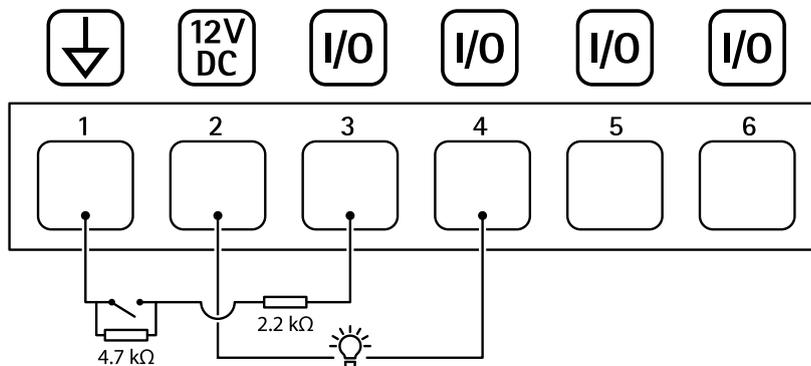


Función	Pin	Notas	Especificaciones
Tierra CC	1		0 V CC
Salida de CC	2	Se puede utilizar para conectar el equipo auxiliar. Nota: Este pin solo puede utilizarse como salida de alimentación y en el lado seguro, ya que comparte alimentación con los relés.	12 V CC Carga máx. = 50 mA para cada E/S

Controlador de accesos en red AXIS A1610 Network Door Controller

Especificaciones

Configurable (entrada o salida)	3-6	Entrada digital o entrada supervisada: conéctela al pin 1 para activarla, o bien déjela suelta (sin conectar) para desactivarla. Para usar la entrada supervisada, instale las resistencias de final de línea. Consulte el diagrama de conexiones para obtener información sobre cómo conectar las resistencias.	De 0 a 30 V CC máx.
		Salida digital: conectada internamente a pin 1 (tierra CC) cuando está activa; y suelta (desconectada), cuando está inactiva. Si se utiliza con una carga inductiva, por ejemplo, un relé, conecte un diodo en paralelo a la carga como protección contra transitorios de tensión. Cada E/S puede conducir una carga externa de 12 V CC, 50 mA (máx.), si se utiliza una salida interna de 12 V CC (pin 2). En caso de usar conexiones de colector abierto en combinación con una fuente de alimentación externa, las E/S pueden gestionar el suministro de CC de 0 – 30 V CC, 100 mA.	De 0 a 30 V CC máx., colector abierto, 100 mA

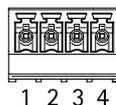


- 1 Masa CC
- 2 Salida de CC 12 V, 50 mA máx.
- 3 E/S configurada como entrada supervisada
- 4 E/S configurada como salida
- 5 E/S configurable
- 6 E/S configurable

Conector externo

Bloque de terminales de 4 pines para conectar dispositivos externos, 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/antiincendios.



Función	Pin	Notas	Especificaciones
Tierra CC	1, 3		0 V CC

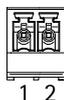
Controlador de accesos en red AXIS A1610 Network Door Controller

Especificaciones

Configurable (entrada o salida)	2, 4	Entrada digital: conéctela al pin 1 o 3 para activarla, o bien déjela suelta (desconectada) para desactivarla.	De 0 a 30 V CC máx.
		Salida digital: conéctela al pin 1 o 3 para activarla o bien déjela suelta (desconectada) para desactivarla. 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

Conector de alimentación

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



Función	Pin	Notas	Especificaciones
0 V CC (-)	1		0 V CC
Entrada de CC	2	Para alimentar el controlador cuando no se use la alimentación a través de Ethernet. Nota: Este pin solo se puede utilizar como entrada de alimentación.	10,5–28 V CC, 36 W máx.

UL: Una fuente de alimentación UL 294, UL 293 o UL 603 debe suministrar la alimentación de CC, en función de la aplicación, con las clasificaciones adecuadas.

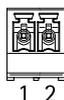
Entrada de alimentación de seguridad de 12 V

Para una solución de reserva mediante una batería con cargador integrado. Entrada 12 V CC.

UL: El conector no ha sido evaluado conforme a UL.

Importante

Cuando se utiliza la entrada de batería, se debe conectar en serie un fusible de fusión lenta externo de 3 A.



Función	Pin	Notas	Especificaciones
0 V CC (-)	1		0 V CC
Entrada de batería	2	Para alimentar el controlador de puerta cuando no hay otras fuentes de alimentación disponibles. Nota: Este pin solo se puede utilizar como alimentación de la batería. Solo para la conexión a SAI (UPS).	11 – 13,7 V CC, máx. 36 W

Solución de problemas

Solución 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 *Información general del producto en la página 23*.
3. Mantenga pulsado el botón de control durante 25 segundos hasta que el indicador LED de estado se ponga en ámbar por segunda vez.
4. Suelte el botón de control. El proceso finaliza cuando el indicador LED de estado se pone verde. El producto se ha restablecido a la configuración predeterminada de fábrica. Si no hay ningún servidor DHCP disponible en la red, la dirección IP predeterminada será 192.168.0.90.
5. Utilice las herramientas del software de instalación y gestión para asignar una dirección IP, establecer la contraseña y acceder al producto.

También puede restablecer los parámetros a la configuración predeterminada de fábrica a través de la interfaz web del dispositivo. Vaya a **Maintenance (Mantenimiento) > Factory default (Configuración predeterminada de fábrica)** y haga clic en **Default (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)**.

Solución de problemas

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.
--	--

Controlador de accesos en red AXIS A1610 Network Door Controller

Solución de problemas

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): <ul style="list-style-type: none">• Si recibe: Reply from <IP address> (Responder desde <dirección IP>): bytes=32; time=10... significa que la dirección IP podría estar en uso por otro dispositivo de la red. Solicite una nueva dirección IP al administrador de red y vuelva a instalar el 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 <i>Restablecimiento a la configuración predeterminada de fábrica en la página 31</i> .
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 Companion: 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. <ul style="list-style-type: none">• 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/intermediario es compatible con ALPN, se puede negociar el uso de MQTT en un puerto abierto, como 443. Consulte con su proveedor de servidor/intermediario para ver si ALPN es compatible y qué protocolo y puerto ALPN utilizar.
---	--

Consideraciones sobre el rendimiento

Los siguientes factores son los más importantes que se deben considerar:

Controlador de accesos en red AXIS A1610 Network Door Controller

Solución de problemas

- Un uso denso de la red debido a una infraestructura deficiente afecta al ancho de banda.

Contacto con asistencia técnica

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

