AXIS TP3604-E Cellular Back Box

Manual del usuario

Índice

Instalación 3
Cómo funciona 4
Localice el dispositivo en la red 4
Compatibilidad con navegadores 4
Abrir la interfaz web del dispositivo 4
Crear una cuenta de administrador 4
Contraseñas seguras 4
Asegúrese de que no se ha manipulado el software del dispositivo 5
Configure su dispositivo 6
Gestión de tarjetas SIM 6
Configure el APN 6
Compruebe la intensidad de la señal y la dirección IP 6
Compruebe la conectividad 6
Compruebe los puertos de gestión 6
Activar el reenvío a la cámara 7
Configure la propiedad de la dirección IP de la cámara 7
Modo local 8
Modo de paso directo 8
Configurar reglas para eventos 9
Activar una acción 9
Activar una notificación al abrir el cerramiento 9
Interfaz web 11
Especificaciones 12
Guía de productos 12
Indicadores LED 12
Botones 13
Botón de control 13
Conectores 13
Conector de entrada PoE (PoE in) 13
Conector de red (PoE OUT) 13
Conector de corriente 13
Limpie su dispositivo 14
Localización de problemas 15
Restablezca la configuración predeterminada de fábrica 15
Opciones de AXIS OS 15
Comprobar la versión de AXIS OS 15
Actualización de AXIS OS 16
Problemas técnicos y posibles soluciones 16
Contactar con la asistencia técnica 18
Ciberseguridad 19
Gestión de las vulnerabilidades 19
Notificaciones de seguridad 19
Ciclo de vida seguro del producto 19

Instalación



El vídeo muestra cómo instalar la AXIS TP3604-E Cellular Back Box con las cámaras domo fijas de la serie AXIS P32 y las cámaras tipo bullet de la serie AXIS P14.

Para obtener instrucciones que abarquen todos los escenarios de instalación, así como información de seguridad, consulte la guía de instalación.

Cómo funciona

Localice el dispositivo en la red

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

Compatibilidad con navegadores

Puede utilizar el dispositivo con los siguientes navegadores:

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

✓: Recomendado

*: Asistencia con limitaciones

Abrir la interfaz web del dispositivo

1. Escriba el nombre de usuario y la contraseña. Si accede al dispositivo por primera vez, debe crear una cuenta de administrador. Consulte *Crear una cuenta de administrador, on page 4*.

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

Crear una cuenta de administrador

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

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

Contraseñas seguras

Importante

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

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

Para proteger sus datos le recomendamos encarecidamente que:

- Utilice una contraseña con al menos 8 caracteres, creada preferiblemente con un generador de contraseñas.
- No exponga la contraseña.

- Cambie la contraseña a intervalos periódicos y al menos una vez al año.

Asegúrese de que no se ha manipulado el software del dispositivo

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

1. Configure e instale el dispositivo.

Configure su dispositivo

Para configurar su dispositivo, debe seguir los siguientes pasos:

1. *Gestión de tarjetas SIM, on page 6*
2. Si su red requiere un nombre de punto de acceso (APN) explícito, *Configure el APN, on page 6*
3. *Compruebe la intensidad de la señal y la dirección IP, on page 6*
4. *Compruebe la conectividad, on page 6*
5. *Compruebe los puertos de gestión, on page 6*
6. *Activar el reenvío a la cámara, on page 7*

Gestión de tarjetas SIM

La gestión de la tarjeta SIM es obligatoria cuando el PIN de la tarjeta SIM está habilitado. Si el número de identificación personal (PIN) de la tarjeta SIM está desactivado, puede omitir este paso.

1. Introduzca la tarjeta SIM. Vaya a **Modem > SIM management > SIM status (Módem > Gestión de SIM > Estado de la SIM)** para verificar la detección del módem y la SIM.
2. Si el PIN de la tarjeta SIM está bloqueado, vaya a **Modem > SIM management > SIM PIN > Unlock (Módem > Gestión de SIM > PIN de la tarjeta SIM > Desbloquear)** para desbloquearla con el PIN correcto.

Configure el APN

Nota

Solo debe seguir este paso si su red requiere un APN (nombre de punto de acceso) explícito.

Para realizar un ajuste de APN explícito, vaya a **Modem > Cellular network > APN (Módem > Red móvil > APN)**.

Compruebe la intensidad de la señal y la dirección IP

Nota

Este paso requiere acceso a la red móvil.

1. Compruebe la intensidad de la señal en **System > Modem > Cellular network > Radio parameters > Signal strength index (Sistema > Módem > Red móvil > Parámetros de radio > Índice de intensidad de la señal)**. De tres a cuatro barras indican que la calidad de la señal es buena.
2. En **System > Modem > Cellular network > User equipment IP address (Sistema > Módem > Red móvil > Dirección IP del equipo de usuario)**, compruebe que se haya recibido una dirección IP de la red móvil.

Compruebe la conectividad

Nota

Este paso requiere acceso a la red móvil.

1. Vaya a **System > Modem > Cellular network > Test cellular connection (Sistema > Módem > Red móvil > Probar conexión móvil)**. Introduzca un nombre de host o una dirección IP.
2. Verifique que la prueba de conexión se haya realizado correctamente.

Compruebe los puertos de gestión

Antes de encender el modo de enrutamiento definitivo, compruebe los puertos de gestión de la caja de conexión.

1. Vaya a **Cellular routing > Back box management ports (Enrutamiento móvil > Puertos de gestión de la caja de conexión)**.

2. Cambie los puertos si la red no admite los valores predeterminados.

Activar el reenvío a la cámara

El último paso consiste en activar el reenvío a la cámara.

1. Vaya a **Cellular routing > Main mode (Enrutamiento móvil > Modo principal)** y haga clic en **Enable forwarding to connected device (Habilitar reenvío al dispositivo conectado)**.

Una vez habilitado el reenvío, los puertos de servicio habituales se reenvían a la cámara, y la gestión del dispositivo central continúa disponible a través de los puertos de gestión reservados.

2. Compruebe el acceso a la cámara: en un navegador web, introduzca la dirección IP del móvil seguida del número de puerto 80: `http://<cellular-ip-address>:80`.
3. Compruebe el acceso al back box: en un navegador web, introduzca la dirección IP del móvil seguida del número de puerto 11080 (el puerto predeterminado de gestión del back box para HTTP), `http://<cellular-ip-address>:11080`.

Configure la propiedad de la dirección IP de la cámara

Nota

Este paso es opcional y solo es necesario si necesita modificar el comportamiento predeterminado de la subred o ajustarlo.

Una red móvil asigna únicamente una dirección IP, y esa dirección está vinculada a la identidad de la tarjeta SIM. Una instalación normal consta de una caja de conexión y una cámara conectada a ella. El modo DHCP determina qué dirección IP se asigna a la cámara. Esta es la decisión clave a la hora de elegir el modo de funcionamiento de un servidor DHCP.

De forma predeterminada (modo local), la dirección IP móvil permanece en la unidad central y a la cámara se le asigna una dirección IP privada de la red local de la unidad central. Continúa siendo posible acceder a la cámara sin problemas desde la red móvil. En la mayoría de las instalaciones, esto es todo lo que se necesita y garantiza que la cámara permanezca aislada de forma segura en una red privada.

La diferencia resulta evidente cuando una herramienta analiza la dirección IP desde la propia perspectiva de la cámara. Si un VMS lee la dirección IP que indica la cámara, o si la cámara está configurada para mostrar su dirección IP en una superposición de vídeo, esa será la dirección IP privada de la LAN de la cámara, no la dirección IP pública de la red móvil que utiliza el mundo exterior para conectarse a ella. Las direcciones no coinciden porque la IP móvil pertenece a la identidad de la tarjeta SIM que tiene la caja de conexión, no a la cámara.

El modo de paso directo resuelve este problema tomando la única dirección IP que la red móvil asigna al decodificador y reenviándola a la cámara. Con la función de paso directo habilitada, la cámara tiene exactamente la misma dirección IP que la red móvil, por lo que la dirección que indica la cámara (y que se muestra en una superposición de vídeo) es la misma que se utiliza para acceder a ella de forma remota. Dado que la cámara cuenta ahora con la identidad móvil, esta elección también cambia la forma en que la cámara puede comunicarse con otros equipos de usuario (UE) de la red móvil.

En el resto de esta sección se describe cada modo con detalle.

Puede acceder a la cámara conectada a la caja de conexión a través de la IP móvil en los puertos estándar (`80/443/554/22`) y también a través de los puertos de gestión reservados (por ejemplo,`11080/11443/11554/11022`).

La diferencia entre el modo Local y el modo de Paso directo:

Modo local

- A la cámara se le ha asignado una subred local privada.
- La dirección IP interna de la cámara es distinta de la dirección IP accesible a través de la red móvil.
- En caso de duda, utilice el modo DHCP local.

Modo de paso directo

- A la cámara se le asigna la dirección IP móvil.

Modo local

Active el modo local

1. En **Cellular routing > Advanced DHCP configuration > DHCP server mode (Enrutamiento móvil > Configuración avanzada de DHCP > Modo del servidor DHCP)**, seleccione **Local**.
2. Compruebe que la dirección IP local de la cámara no entre en conflicto con ninguna otra dirección IP accesible de la red: **Cellular routing > Advanced DHCP configuration > Local private network configuration (Enrutamiento móvil > Configuración avanzada de DHCP > Configuración de la red privada local)**
3. Si es preciso, cambie la dirección IP en **Cellular routing > Advanced DHCP configuration > Local private network configuration (Enrutamiento móvil > Configuración avanzada de DHCP > Configuración de la red privada local)**. Utilice el mismo valor para la **Starting IP address (Dirección IP inicial)** y la **Ending IP address (Dirección IP final)**.
4. Haga clic en **Save (Guardar)**.

Modo de paso directo

Si los UE (equipos de usuario, es decir, las cámaras) no se comunican entre sí y el tráfico siempre procede de otra LAN del VMS hacia los UE, no existe una ruta de UE a UE para el enmascaramiento de IP. En ese caso, se considera que el paso directo es seguro desde el punto de vista del enmascaramiento de IP.

A grandes rasgos, esto significa que la red móvil se amplía hacia el lado de la cámara. Esto resulta útil cuando la cámara debe aparecer directamente en la dirección IP asociada al móvil.

Riesgo importante: Enmascaramiento de IP en modo de paso directo

Esta descripción de los riesgos se aplica a las configuraciones con una sola cámara. Incluso con una sola cámara, la función de paso directo continúa necesitando dos direcciones IP en la subred del lado de la LAN:

- Una dirección IP para la cámara.
- Una dirección IP para el servidor DHCP de la caja de conexión en el lado de Ethernet.

Escenario 1: subred mínima por UE `(/30)`

En este modelo, cada UE dispone de una subred pequeña e independiente.

- Un servidor de alojamiento `(/30)` ofrece dos direcciones IP de host utilizables.
- La cámara utiliza una dirección IP.

La dirección IP libre la utiliza internamente el servidor DHCP de la caja de conexión.

Recomendación para el escenario 1:

- Mantenga todas las subredes de los dispositivos de usuario (UE) separadas.
- Asegúrese de que cada subred de UE sea única. No permita que las subredes se solapen entre los UE.

Escenario 2: Subred compartida más grande con muchos UE

En algunas implementaciones se utiliza una única subred de mayor tamaño compartida por varios UE. El riesgo de enmascaramiento surge si la cámara intenta conectarse con otro dispositivo de usuario (UE) que utilice la misma dirección IP que la del servidor DHCP de la caja de conexión. En ese caso, es posible que el tráfico se dirija a la dirección local del equipo de red local en lugar de al UE remoto al que está destinado.

Recomendación para el escenario 2:

- Compruebe la dirección IP del servidor DHCP del router en el ajuste de paso directo.
- Asegúrese de que esta dirección IP no se haya asignado a ningún otro dispositivo UE.
- Asegúrese de que esta dirección IP no se asigne a ninguna tarjeta SIM en el portal de servicios de la red.

Active el modo de paso directo

Nota

Es necesario tener acceso a una red móvil.

1. En **Cellular routing > Advanced DHCP configuration > DHCP server mode (Enrutamiento móvil > Configuración avanzada de DHCP > Modo de servidor DHCP)**, seleccione **Passthrough (Paso directo)**.
2. En **Cellular routing > Advanced DHCP configuration > Local private network configuration > Server IP and prefix length (Enrutamiento móvil > Configuración avanzada de DHCP > Configuración de la red privada local > Dirección IP del servidor y longitud del prefijo)**, compruebe que la dirección IP del servidor y la longitud del prefijo de subred seleccionadas automáticamente no entren en conflicto con otras direcciones IP accesibles.
3. Haga clic en **Save (Guardar)**.

Configurar reglas para eventos

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

Activar una acción

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

Activar una notificación al abrir el cerramiento

Este ejemplo detalla cómo configurar una notificación de correo electrónico al abrir la carcasa o cerramiento del dispositivo.

Añadir un destinatario de correo electrónico:

1. Vaya a **System > Events > Recipients (Sistema > Eventos > Destinatarios)** y haga clic en **Add recipient (Agregar destinatario)**.
2. Escriba un nombre para el destinatario.
3. Seleccione **Email (Correo electrónico)** como tipo de notificación.
4. Escriba la dirección de correo electrónico del destinatario.
5. Escriba la dirección de correo electrónico desde la que desea que la cámara envíe las notificaciones.
6. Proporcione los datos de inicio de sesión de la cuenta de correo electrónico de envío, junto con el nombre del host SMTP y el número de puerto.
7. Para probar la configuración de su correo electrónico, haz clic en **Test (Prueba)**.
8. Haga clic en **Save (Guardar)**.

Crear una regla:

9. Vaya a **Settings > Events > Rules (Ajustes > Eventos > Reglas)** y haga clic en **Añadir una regla**.
10. Escriba un nombre para la regla.
11. En la lista de condiciones, seleccione **Casing open (Apertura de carcasa)**.
12. En la lista de acciones, seleccione **Send notification to email (Enviar notificación a correo electrónico)**.
13. Seleccione un destinatario de la lista.
14. Escriba una línea de asunto y un mensaje para el correo electrónico.

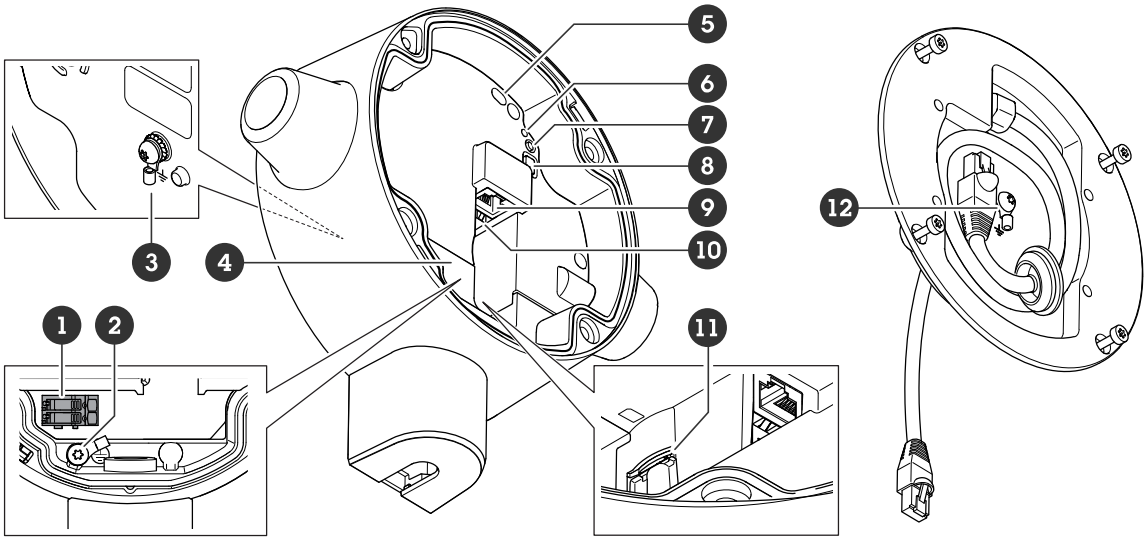
15. Haga clic en **Save (Guardar)**.

Interfaz web

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

Especificaciones

Guía de productos



1 *Conector de CA*
2 *Puesta a tierra de protección*
3 *Tornillo de tierra*
4 *Funda protectora (AC)*
5 *Detector de carcasa abierta*
6 *Botón de reinicio*
7 *LED de estado*
8 *Botón de control*
9 *Salida PoE (datos)*
10 *Entrada PoE*
11 *Ranura para tarjetas SIM*
12 *Tornillo de fijación a tierra (cámara)*

Indicadores LED

LED de estado en modo de configuración

LED de estado	Indicación
Apagado	El sensor IR de detección de la carcasa está cubierto.
Verde	Funcionamiento normal: la interfaz Ethernet está lista.
Ámbar;	Fijo durante el inicio. Parpadea durante la actualización del software del dispositivo o el restablecimiento a la configuración predeterminada de fábrica.
Ámbar/rojo	Sin conexión Ethernet y el módem está en proceso de configuración durante el arranque.
Rojo	Error de actualización del software del dispositivo.

LED de estado en modo conectado

LED de estado	Indicación
Apagado	El sensor IR de detección de la carcasa está cubierto.
Verde	El módem está conectado a la red.
Ámbar;	Fijo durante el inicio. Parpadea durante la actualización del software del dispositivo o el restablecimiento a la configuración predeterminada de fábrica.

Ámbar/rojo	El módem está en proceso de configuración durante el arranque.
Rojo	Error de actualización del software del dispositivo.

Botones

Botón de control

El botón de control se utiliza para lo siguiente:

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

Conectores

Conector de entrada PoE (PoE in)

Conector Ethernet RJ45 con alimentación a través de Ethernet (PoE) IEEE 802.3af/802.3at/802.3bt, Tipo 3 Clase 5.

Nota

Este conector solo se utiliza para la entrada de alimentación; no dispone de conexión a la red.

Nota

- Se requiere una entrada de CA para obtener una salida PoE conforme a la norma IEEE 802.3at, tipo 2, clase 4.
- Para una salida PoE conforme a la norma IEEE 802.3af, tipo 1, clase 3, se requiere una salida conforme a la norma IEEE 802.3at, tipo 2, clase 4 o superior.
- En el caso de una entrada PoE IEEE 802.3af Tipo 1 Clase 3, el dispositivo está operativo pero no tiene salida de potencia.

Nota

La longitud máxima del cable Ethernet es de 20 m.

Conector de red (PoE OUT)

Conector Ethernet RJ45.

Nota

- Se requiere una entrada de CA para obtener una salida PoE conforme a la norma IEEE 802.3at, tipo 2, clase 4.
- Para una salida PoE conforme a la norma IEEE 802.3af, tipo 1, clase 3, se requiere una salida conforme a la norma IEEE 802.3at, tipo 2, clase 4 o superior.
- En el caso de una entrada PoE IEEE 802.3af Tipo 1 Clase 3, el dispositivo está operativo pero no tiene salida de potencia.

Nota

La longitud máxima del cable Ethernet es de 20 m.

Conector de corriente

Bloque de bornes para la conexión de la alimentación de CA.

Nota

Se requiere una entrada de CA para obtener una salida PoE conforme a la norma IEEE 802.3at, tipo 2, clase 4.

Limpie su dispositivo

Puede limpiar su dispositivo con agua tibia y jabón suave no abrasivo.

AVISO

- Los productos químicos agresivos pueden dañar el dispositivo. No utilice productos químicos como un limpiacristales o acetona para limpiar el dispositivo.
- Evite limpiar en contacto directo con la luz o a temperaturas elevadas, ya que puede provocar manchas.

1. Utilice un aerosol de aire comprimido para quitar el polvo y la suciedad suelta del dispositivo.
2. Si es necesario, limpie el dispositivo con un paño de microfibra suave humedecido con agua tibia y jabón suave y no abrasivo.
3. Para eliminar cualquier resto de producto, limpie el dispositivo con un paño suave de microfibra humedecido con agua tibia.
4. Para evitar que queden manchas, seque el dispositivo con un paño limpio y no abrasivo.

Consulte el documento técnico *Chemical resistance to common cleaning agents (Resistencia química a productos de limpieza habituales)* para obtener más información sobre la limpieza de dispositivos Axis.

Localización de problemas

Restablezca la configuración predeterminada de fábrica

Importante

Hay que valorar bien es necesario restablecer la configuración predeterminada de fábrica. Todos los valores, incluida la dirección IP, se restablecerán a la configuración predeterminada de fábrica.

Para restablecer el producto a la configuración predeterminada de fábrica:

1. Desconecte la alimentación del producto.
2. Mantenga pulsado el botón de control mientras vuelve a conectar la alimentación. Consulte *Guía de productos, on page 12*.
3. Mantenga pulsado el botón de control durante 15-30 segundos hasta que el indicador LED de estado parpadee en color ámbar.
4. Suelte el botón de control. El proceso finalizará cuando el indicador LED de estado se ilumine en color verde. Si no hay ningún servidor DHCP en la red, la dirección IP del dispositivo será una de las siguientes de forma predeterminada:
   - **Dispositivos con AXIS OS 12.0 y versiones posteriores:** obtenidos de la subred de direcciones de enlace local (169.254.0.0/16)
   - **Dispositivos con AXIS OS 11.11 y anterior:** 192.168.0.90/24
5. Utilice las herramientas del software de instalación y gestión para asignar una dirección IP, configurar la contraseña y acceder al dispositivo.
   Las herramientas de software de instalación y gestión están disponibles en las páginas de servicio técnico de *axis.com/support*.

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

Opciones de AXIS OS

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

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

Comprobar la versión de AXIS OS

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

Para comprobar la versión de AXIS OS:

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

Actualización de AXIS OS

Importante

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

Nota

- Al actualizar el dispositivo con el AXIS OS más reciente en la pista activa, el producto obtiene las últimas funciones disponibles. Lea siempre las instrucciones de actualización y las notas de versión disponibles en cada nueva versión antes de la actualización. Para encontrar el AXIS OS y las notas de versión más recientes, consulte *axis.com/support/device-software*.

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

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

Problemas técnicos y posibles soluciones

Problemas para actualizar AXIS OS

Error en la actualización de AXIS OS

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

Problemas tras la actualización de AXIS OS

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

Problemas al configurar la dirección IP

No se puede configurar la dirección IP

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

Problemas de acceso al dispositivo

No puede iniciar sesión accediendo al dispositivo desde un navegador

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

Si ha olvidado la contraseña de la cuenta de administrador, deberá restablecer el dispositivo a la configuración de fábrica. Para consultar las instrucciones, vea *Restablezca la configuración predeterminada de fábrica, on page 15*.

El servidor DHCP ha cambiado la dirección IP

Las direcciones IP obtenidas de un servidor DHCP son dinámicas y pueden cambiar. Si la dirección IP ha cambiado, acceda a la utilidad AXIS IP Utility o AXIS Device Manager para localizar el dispositivo en la red. Identifique el dispositivo utilizando el modelo o el número de serie, o por el nombre de DNS (si se ha configurado el nombre).

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

Error de certificado cuando se utiliza IEEE 802.1X

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

El navegador no es compatible

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

No se puede acceder externamente al dispositivo.

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

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

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

Problemas con MQTT

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

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

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

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

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

Contactar con la asistencia técnica

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

Ciberseguridad

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

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

Gestión de las vulnerabilidades

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

Notificaciones de seguridad

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

Ciclo de vida seguro del producto

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

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

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

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

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

T10233346_es

2026-10 (M2.2)

© 2026 Axis Communications AB