

# AXIS Device Manager

## Índice

Acerca de AXIS Device Manager .....	3
Cómo funciona .....	4
Instalación del software.....	4
Conectar a un servidor.....	4
Conectar a varios servidores .....	4
Configurar el servidor .....	5
Configuración inicial .....	5
Gestionar dispositivos.....	6
Agregar dispositivos .....	6
Eliminar dispositivos.....	6
Sustituir dispositivos .....	6
Restaurar dispositivos.....	6
Instalación de aplicaciones.....	7
Configuración.....	8
Gestión de puntos de restauración .....	8
Crear un punto de restauración.....	8
Crear puntos de restauración automáticos.....	8
Gestionar múltiples credenciales.....	8
Instalación de certificados.....	9
Acerca de los certificados.....	9
Crear una autoridad de certificación (CA).....	9
Activar HTTPS.....	10
Activar 802.1X .....	10
Configure los ajustes SIP.....	11
Gestionar cuentas SIP.....	12
Añadir cuentas SIP.....	12
Eliminar cuentas SIP .....	13
Habilitar metadatos en dispositivos.....	14
Gestión del software del dispositivo.....	15
Actualizaciones al AXIS OS.....	15
Localización de problemas .....	16
Lista de componentes de software .....	16
Contactar con la asistencia técnica.....	16
Proceso de escalada.....	16

### Acerca de AXIS Device Manager

AXIS Device Manager es una aplicación de software de instalación y gestión para productos Axis. El software puede buscar dispositivos automáticamente en la red, asignar direcciones IP, establecer contraseñas, mostrar estados de conexión, gestionar actualizaciones de firmware, certificados y configuración de varios dispositivos.

AXIS Device Manager se compone de:

- **AXIS Device Manager Service Control:** el servidor que gestiona toda la comunicación con los productos de Axis
- **AXIS Device Manager Client:** la interfaz de usuario front-end que permite realizar la gestión remota desde internet o la red de empresa

Se pueden conectar varios clientes al mismo servidor. Un cliente puede estar conectado a varios servidores al mismo tiempo.

Igualmente, AXIS Device Manager resulta muy útil para reforzar su sistema y la seguridad de este. Para obtener más información, consulte la *AXIS Device Manager Security Guide (Guía de seguridad de AXIS Device Manager)*.

## Cómo funciona

### Instalación del software

Para instalar AXIS Device Manager 5, asegúrese de que dispone de todos los derechos de administrador en el equipo en el que realice la instalación y, a continuación, haga lo siguiente:

1. Vaya a la página del producto en [axis.com](http://axis.com) y descargue el instalador de la aplicación de escritorio de AXIS Device Manager
2. Ejecute el instalador y siga las instrucciones que aparecen en pantalla.

#### Nota

Si aún no está instalado, se instalará Microsoft .NET 4.8 Framework (incluido en el archivo de instalación). Este proceso tardará varios minutos. Microsoft .NET 4.8 Framework también puede instalarse a través de Windows Update antes de la instalación de AXIS Device Manager.

### Conectar a un servidor

Cuando inicie AXIS Device Manager por primera vez, se le pedirá que se conecte a un servidor. El servidor puede ejecutarse en la máquina local o en un servidor remoto.

Para iniciar sesión como usuario local de Windows:

1. Seleccione **This computer (Este ordenador)**.
2. Marque **Log on as current user (Iniciar sesión como usuario actual)** para iniciar sesión con sus credenciales actuales.

Para iniciar sesión como otro usuario en el servidor o en el dominio:

- Seleccione **Other user (Otro usuario)**.
- En **Other user (Otro usuario)**, introduzca las credenciales de esa cuenta.
- Marque **Remember me (Recordarme)** para omitir este paso la próxima vez que ejecute el cliente.
- Haga clic en **Log on (Iniciar sesión)**.

#### Nota

Para borrar las credenciales guardadas de todos los servidores, vaya a la pantalla de inicio de sesión y seleccione **Delete saved passwords (Eliminar contraseñas guardadas)**.

Para iniciar sesión en un servidor remoto:

1. Seleccione **Servidor remoto**.
2. Seleccione un servidor de la lista desplegable o introduzca la dirección IP o DNS en el campo.
3. Introduzca las credenciales
4. Haga clic en **Log on (Iniciar sesión)**.

#### Nota

Esta opción no puede utilizarse para iniciar sesión en un servidor remoto desde un equipo que no forme parte de un dominio de Windows.

### Conectar a varios servidores

Puede conectarse a varios servidores con AXIS Device Manager. Cuando haya iniciado sesión en un servidor, podrá cambiar de servidor en el menú principal.

1. Vaya al menú principal > Servers (Servidores) > New connection (Nueva conexión)
2. Elija conectarse a su ordenador o a un servidor remoto como se ha descrito anteriormente.

### Configurar el servidor

Una vez instalado AXIS Device Manager Server en su ordenador, el control de servicios permite iniciar y detener el servidor, así como modificar su configuración.

Para configurar el servidor:

1. Haga doble clic en el icono para abrir **AXIS Device Manager Service Control**
2. Marque la casilla **Modify settings (Modificar ajustes)**
3. Asigne un nombre al servidor. El nombre del servidor lo identifica y se muestra en el cliente AXIS Device Manager cuando este está conectado a más de un servidor. El nombre predeterminado es el del ordenador donde se instaló el software.
4. Introduzca el puerto HTTP. El número de puerto HTTP predeterminado es: 55762
5. Introduzca el puerto TCP. El número de puerto TCP predeterminado es: 55764

#### Nota

El número de puerto del servidor debe encontrarse entre 1024 y 65533. El número de puerto TCP será siempre el número de puerto del servidor más 2. Por ejemplo, si el número de puerto del servidor es 55765, el número de puerto TCP será 55767.

#### Nota

En instalaciones de mayor envergadura, recomendamos AXIS Device Manager Service Administration. Se trata de una aplicación de consola que se puede utilizar desde la línea de comandos o desde un script por lotes para iniciar y detener el servicio, realizar copias de seguridad de la base de datos, etc. La aplicación de consola "AdmAdminConsole.exe" se encuentra en el directorio de instalación del servidor.

### Configuración inicial

Para empezar, tiene que hacer lo siguiente:

- Agregar dispositivos y crear cuentas de usuario, consulte: *Agregar dispositivos, on page 6*
- Reforzar la ciberseguridad de su sistema. Vea *Instalación de certificados, on page 9*

## Gestionar dispositivos

### Agregar dispositivos

AXIS Device Manager busca automáticamente en la red los dispositivos conectados e intenta iniciar sesión en todos los dispositivos. La lista de dispositivos encontrados muestra la dirección del dispositivo (dirección IP o nombre de host), el número de serie, el modelo y el estado. El número de serie (S/N) está impreso en la etiqueta del producto.

Para agregar dispositivos de la lista:

1. Seleccione los dispositivos que desee añadir y haga clic en **Next (Siguiente)**.
2. Seleccione **Use host name when possible (Usar nombre de host cuando sea posible)**. Si un dispositivo se añade mediante su nombre de host, este se utilizará para todas las comunicaciones posteriores con el dispositivo. Si no hay ningún nombre de host disponible, se utilizará la dirección IP.
3. Ajuste la contraseña para dispositivos sin contraseña. Si no debe ajustarse una contraseña, seleccione **Skip (Omitir)**.
4. Haga clic en **Next (Siguiente)**.

La página «Ready to add devices» (Listo para agregar dispositivos) muestra los dispositivos que se van a agregar.

5. Haga clic en **Finish (Finalizar)** para agregar los dispositivos.

### Eliminar dispositivos

Para quitar dispositivos de la lista:

1. Vaya a **Device management (Gestión de dispositivos)**.
2. Seleccione los dispositivos.
3. Haga clic con el botón derecho y seleccione **Remove (Quitar)**.
4. Haga clic en **Yes (Sí)**.

### Sustituir dispositivos

Para sustituir un dispositivo en AXIS Device Manager, conecte un dispositivo nuevo y reutilice la configuración del dispositivo existente. El dispositivo sustituido se eliminará si la operación se realiza correctamente. Debe haber al menos un punto de restauración disponible para ese dispositivo, consulte *Crear un punto de restauración*, on page 8. No se restaurarán puntos en el dispositivo nuevo.

1. Vaya a **Device management (Gestión de dispositivos)**.
2. Vaya a la barra de herramientas y haga clic en el icono de reemplazar dispositivo.
3. Seleccione el dispositivo que desee sustituir y haga clic en **OK (Aceptar)**.
4. Seleccione el dispositivo por el que lo desee sustituir y haga clic en **OK (Aceptar)**.
5. Haga clic en **Next (Siguiente)** para recuperar la configuración de un dispositivo desde el último punto de restauración.
6. Vaya a **Parameters (Parámetros) > Additional Settings (Ajustes adicionales)** y seleccione los parámetros y ajustes a aplicar.
7. Haga clic en **Next (Siguiente)**.
8. Haga clic en **Finish (Finalizar)** para aplicar sus ajustes.

### Restaurar dispositivos

Es posible restablecer uno o varios dispositivos a un punto de restauración creado anteriormente. Para restaurar dispositivos, cada uno de ellos debe tener al menos un punto de restauración disponible. De forma predeterminada, se crean puntos de restauración automáticos y se eliminan continuamente cada noche para

todos los dispositivos del servidor seleccionado. Se guarda un número determinado de los últimos puntos de restauración automática a efectos de restaurarlos.

Restaurar dispositivos a un punto de restauración anterior:

1. Vaya al espacio de trabajo **Device management (Gestión de dispositivos)**.
2. Seleccione uno o varios dispositivos para restaurar.
3. Haga clic con el botón derecho del ratón y seleccione **Backup / Restore (Copia de seguridad/ Restauración) > Restore to a Previous Time (Restaurar a un momento anterior)** en el menú desplegable.
4. Seleccione un punto de restauración en la lista de los puntos de restauración más recientes disponibles y haga clic en **Next (Siguiete)**.
5. Revise los ajustes de cada dispositivo y haga clic en **Finish (Finalizar)**.

### Instalación de aplicaciones

Una aplicación es software que se puede descargar e instalar en dispositivos Axis. Las apps pueden instalarse en dispositivos compatibles con AXIS Camera Application Platform. Estas aportan funcionalidad al dispositivo, por ejemplo, capacidades de detección, reconocimiento, seguimiento y recuento. Las aplicaciones deben descargarse primero desde [www.axis.com](http://www.axis.com) o el sitio web del proveedor de la aplicación. Algunas aplicaciones también requieren una versión específica del AXIS OS o un modelo de dispositivo concreto. Si la app requiere una licencia, el archivo de la clave de licencia puede instalarse al mismo tiempo que la app o posteriormente usando la página de configuración de los dispositivos. Si una app no se puede instalar, vaya a [www.axis.com](http://www.axis.com) y compruebe si el modelo y la versión del AXIS OS son compatibles con AXIS Camera Application Platform.

Para instalar una app:

1. Vaya a [axis.com](http://axis.com) y descargue la app
2. Vaya a **Browse to Application (Buscar aplicación)**
3. Haga clic en **Browse (Examinar)** y vaya a su carpeta de descargas
4. Seleccione la aplicación y haga clic en **Next (Siguiete)**

Si la aplicación requiere una licencia para iniciarse, deberá tener un archivo de licencia ya descargado; de lo contrario, haga clic en **No** y continúe en el paso 8:

5. Seleccione **Yes (Sí)** y haga clic en **Next (Siguiete)**
6. Haga clic en **Browse (Examinar)** y seleccione el archivo de licencia.
7. Haga clic en **Next (Siguiete)**.
8. Seleccione el tipo de instalación que desea:
  - **Versión anterior de la aplicación** instala una versión anterior de las aplicaciones.
  - **Sobrescritura de la aplicación** vuelve a instalar las aplicaciones.

#### Nota

La instalación de una versión anterior o la sobrescritura de la aplicación restablece la configuración de la aplicación en los dispositivos.

#### Preparado para instalar

Se muestran los dispositivos donde se instalarán las apps. Si las apps ya se han instalado en algunos dispositivos, se sobrescribirán las existentes. Si se sobrescribe, se eliminarán todos los ajustes de la app.

9. Haga clic en **Finalizar**

## Configuración

### Gestión de puntos de restauración

Un punto de restauración es una configuración guardada del dispositivo que puede utilizarse para hacer copias de seguridad y restaurar los ajustes del dispositivo. Los puntos de restauración se crean automáticamente cada noche para todos los dispositivos reconfigurados en un servidor. Si no se ha modificado ningún ajuste de un dispositivo desde el último punto de restauración, no se creará otro nuevo. Para aprovechar al máximo la capacidad de almacenamiento, los puntos de restauración más antiguos se eliminan automáticamente. Se guarda un número determinado de los últimos puntos de restauración automática a efectos de restaurarlos.

#### Crear un punto de restauración

Para crear un punto de restauración manual:

- Vaya al espacio de trabajo **Device management (Gestión de dispositivos)**.
- Seleccione uno o varios dispositivos para restaurar.
- Haga clic con el botón derecho y seleccione **Backup/Restore (Copia de seguridad/Restauración) > Create Restore Points (Crear puntos de restauración)**.
- Escriba una descripción que identifique el punto de restauración.
- Haga clic en **OK**.

#### Nota

Los puntos de restauración que se crean manualmente no se eliminan de forma automática.

#### Crear puntos de restauración automáticos

Si tiene más de un servidor, seleccione el servidor que desea configurar en la lista de servidores.

- Vaya a **Options (Opciones) > Restore point settings (Ajustes de puntos de restauración)**.
- Seleccione **Create restore points automatically (Crear puntos de restauración automáticamente)** para habilitar la creación automática de puntos de restauración.
- Introduzca el número de puntos de restauración automáticos que desea guardar y haga clic en **OK (Aceptar)**.

### Gestionar múltiples credenciales

Esta función proporciona a AXIS Device Manager credenciales para una cuenta de administrador de los dispositivos.

#### Escribir las credenciales del dispositivo manualmente

Si elige introducir las credenciales del dispositivo manualmente, estas se actualizarán en AXIS Device Manager para los dispositivos seleccionados.

- Seleccione uno o más dispositivos
- Haga clic con el botón derecho del ratón y seleccione **Advanced (Avanzado) > Enter Device Credentials (Introducir credenciales del dispositivo)** en el menú desplegable.

#### Nota

Las credenciales que no sea posible verificar que funcionan en el dispositivo no se actualizarán. Debe utilizarse la misma contraseña y nombre de usuario para todos los dispositivos que participen en esta operación.

#### Utilizar un archivo CSV para diferentes credenciales

Mediante el uso de un archivo CSV, puede utilizar contraseñas y nombres de usuario independientes para cada dispositivo. La dirección MAC, dirección IP o dirección de host se utiliza para asignar las filas del archivo CSV a los dispositivos correspondientes en la base de datos de Axis Device Manager.

Cuando se utiliza un archivo CSV, la interfaz de usuario le pide que especifique cómo interpretar las columnas del archivo CSV.

### Nota

Cómo especificar a qué dispositivo pertenece una fila del archivo CSV.

Una columna del archivo CSV debe contener direcciones MAC, direcciones IP o direcciones de host, por lo que debe especificar una columna del archivo CSV para que se interprete como dirección MAC o como dirección IP o de host. Este paso es necesario para especificar a qué dispositivo pertenecen los datos de una fila del archivo CSV. Además, se puede especificar una columna para que se interprete como Nombre del servidor. De este modo, se pueden distinguir las filas del archivo CSV que apuntan a dispositivos de diferentes servidores Axis Device Manager pero con la misma dirección IP o dirección de host. Si no se necesita esta distinción, no tiene sentido que haya una columna que se interprete como Nombre del servidor. En una configuración en la que un servidor utiliza la misma dirección IP o dirección de host para varios dispositivos, pero utiliza puertos para diferenciarlos entre sí, se puede especificar una columna para que se interprete como Puerto. Si no es necesario distinguir el puerto, normalmente no hay motivo para interpretar una columna como Puerto. Una opción para proporcionar el puerto en una columna específica consiste en indicar el puerto junto con la dirección IP o la dirección de alojamiento. La dirección IP o la dirección del host deben ir seguidas de dos puntos y del número de puerto.

## Instalación de certificados

### Acerca de los certificados

AXIS Device Manager proporciona los ajustes para la gestión de certificados de servidor/cliente. Los certificados de cliente se utilizan para IEEE 802.1X y los de servidor para HTTPS. Para aplicar cualquier cambio, seleccione los dispositivos adecuados en la opción «Device management» (Gestión de dispositivos) y, a continuación, seleccione la opción de habilitar o actualizar en el menú contextual.

### Crear una autoridad de certificación (CA)

Una autoridad de certificación permitirá habilitar HTTPS y IEEE 802.1X en dispositivos sin necesidad de instalar certificados de servidor y cliente. La CA instruye a los dispositivos para que creen certificados utilizando sus propias claves privadas, los firmen y los instalen.

Para crear una Autoridad de Certificación:

- Vaya a la pestaña **Configuration (Configuración)**.
- Vaya a **Security (Seguridad) > Certificates (Certificados)**
- En **Certificate authority (Autoridad de certificación)**, haga clic en **Generate... (Generar...)**.
- Escriba una frase de contraseña y confírmela.
- Haga clic en **OK**.

La CA se habrá generado y estará lista para usar.

### Nota

Su certificado root con firma propia y su clave privada, protegidos por una frase de contraseña de su elección. Un certificado generado por AXIS Device Manager durará 3 años. Si desea que AXIS Device Manager renueve los certificados de servidor/cliente de forma automática, debe marcar la casilla **Remember passphrase (Recordar frase de contraseña)**. Si no se ha configurado una CA, tendrá que crear certificados de servidor/cliente fuera de AXIS Device Manager. En ese caso, perderá las ventajas de la gestión automática de certificados.

**Import (Importar):** con la función «Importar», puede importar una CA existente que conste de un certificado público y una clave privada. Tendrá que proporcionar una frase de contraseña.

**Save to file (Guardar en archivo):** guarda el certificado público de la CA en formatos .cer o .crt. El archivo no contendrá la clave privada y, por tanto, no se cifrará.

**Backup (Copia de seguridad):** se recomienda realizar una copia de seguridad de una CA en caso de que se produzca un fallo de hardware. Si se selecciona esta opción, se realizará una copia de seguridad tanto del

certificado como de la clave privada de la CA utilizada por Axis Device Manager. Los datos de la copia de seguridad estarán protegidos por la frase de contraseña utilizada para generar la CA.

**Advertencia de caducidad de certificado** Se creará una notificación del sistema si un certificado ha caducado o está a punto de hacerlo. Esto se aplica a todos los certificados instalados en los dispositivos conectados, excepto los CA instalados fuera de AXIS Device Manager. La advertencia aparecerá como alarma del sistema, en la columna de estado de la gestión de dispositivos, como iconos en el cuadro de diálogo «View installed certificates» (Ver certificados instalados) y en el espacio de trabajo Configuration (Configuración).

Especifique la antelación con la que AXIS Device Manager debe emitir una notificación cuando la fecha de caducidad esté próxima. De forma predeterminada, los certificados de servidor y cliente generados por AXIS Device Manager se renovarán de forma automática siete días antes de que aparezca la advertencia de caducidad. Para recibir notificaciones cuando la CA está ajustada para caducar, la opción «Remember passphrase» (Recordar frase de contraseña) debe estar marcada.

### Activar HTTPS

Para habilitar HTTPS, debe haber un certificado de servidor en cada dispositivo. AXIS Device Manager puede utilizar una autoridad de certificación (CA) para firmar e instalar certificados de servidor para los dispositivos.

También puede hacerlo manualmente:

1. Vaya a la pestaña **Device manager (Administrador de dispositivos)**
2. Haga clic con el botón derecho del ratón en los dispositivos y elija **Install server certificates (Instalar certificados de servidor)** para cada dispositivo en el menú contextual.

Solo puede haber un certificado de servidor presente en cada dispositivo antes de habilitar HTTPS. Los certificados sobrantes se pueden eliminar desde el menú contextual.

3. Después de instalar los certificados, puede habilitar HTTPS en el menú contextual.

#### Nota

Se puede establecer una conexión mediante HTTP si no está disponible una conexión segura (HTTPS). La finalidad de este paso es poder configurar dispositivos que aún no son seguros.

### Ignorar validación de certificado

AXIS Device Manager no se conectará a un dispositivo si su certificado no está validado. El certificado del servidor debe estar firmado por la autoridad de certificación activa en AXIS Device Manager o debe estar validado a través de Windows Certificate Store. Al seleccionar la opción «Ignore certificate validation» (Omitir validación de certificados), AXIS Device Manager no validará si el certificado enviado por el dispositivo es de confianza o no.

Para que AXIS Device Manager omita la validación de certificados:

- Vaya a la pestaña **Configuration (Configuración)**.
- En HTTPS, habilite **Ignore certificate validation (Omitir validación de certificados)**.

### Activar 802.1X

Para habilitar IEEE 802.1X, debe haber un certificado de cliente en cada dispositivo. AXIS Device Manager puede utilizar una autoridad de certificación (CA) para firmar e instalar certificados de cliente para los dispositivos.

También puede hacerlo de forma manual en Gestión de dispositivos si hace clic con el botón derecho del ratón en los dispositivos y elige instalar certificados de cliente para cada dispositivo en el menú contextual. Solo puede haber un certificado de cliente presente en cada dispositivo antes de habilitar IEEE 802.1X. Los certificados sobrantes se pueden eliminar desde el menú contextual. Después de instalar los certificados, puede habilitar IEEE 802.1X en el menú contextual.

También necesita un certificado CA de autenticación IEEE 802.1X para poder utilizar el protocolo IEEE 802.1X.

**EAPOL Version (Versión EAPOL):** seleccione la versión de protocolo de autenticación extensible (EAP) que desea utilizar.

**EAP identity (Identidad del EAP):** introduzca la dirección MAC del dispositivo, el nombre de host del dispositivo o texto personalizado.

**Custom (Personalizado):** introduzca cualquier texto que funcione como identidad del EAP.

**IEEE 802.1X authentication CA certificate (Certificado CA de autenticación de IEEE 802.1X):** además del certificado de cliente, se debe instalar una autenticación de certificado de autoridad certificadora IEEE 802.1X. Para activar IEEE 802.1X, solo se necesita el certificado público y no la clave privada, por lo que no es necesaria ninguna frase de contraseña. La autenticación de certificado CA IEEE 802.1X se instalará al habilitar o actualizar IEEE 802.1X..

**Import (Importar):** seleccione un certificado CA que se instalará en los dispositivos y se utilizará para validar el servidor de autenticación. El certificado CA puede ser creado por la CA en AXIS Device Manager o provenir de una fuente externa.

**View (Ver):** detalles del certificado CA utilizado durante el proceso de autenticación de IEEE 802.1X.

**Common name (Nombre común):** seleccione la identidad del EAP del dispositivo o la dirección IP del dispositivo. Si el campo personalizado se deja vacío, se seleccionará el nombre de host. Si hay algún problema relacionado con el nombre de host, se utilizará la dirección IP como nombre común.

### Configure los ajustes SIP

Para configurar los ajustes SIP y de puertos en los dispositivos seleccionados, utilice el asistente de configuración. El asistente de configuración permite conservar el valor presente en el dispositivo o introducir un valor que se aplicará a todos los dispositivos seleccionados. También puede cargar valores de un archivo CSV para aplicar valores específicos del dispositivo a los dispositivos seleccionados.

Use una fila del archivo CSV para cada dispositivo y una columna para cada parámetro que desee configurar. El asistente de configuración permite especificar qué valores se extraerán.

**Para usar un archivo CSV para la configuración específica de varios dispositivos:**

1. Vaya al espacio de trabajo **Device management (Gestión de dispositivos)**.
2. Elija los dispositivos que desea configurar.
3. Haga clic con el botón derecho y seleccione **Configure devices (Configurar dispositivos) > Advanced (Avanzado) > SIP configuration (Configuración SIP) > Settings (Ajustes)**.
4. Si desea utilizar un archivo CSV, verifique haber permitido el uso de archivos CSV. De lo contrario, proceda al punto 5.
  - 4.1. Haga clic en **Browse (Examinar)** y seleccione el archivo CSV que desea utilizar.
  - 4.2. Haga clic en **Next (Siguiente)**
  - 4.3. Seleccione los nombres de las columnas del archivo CSV en el menú desplegable.
  - 4.4. Seleccione la dirección MAC, la dirección IPv4 o la dirección de host de una columna del archivo CSV y asícielas con los dispositivos de las filas.
5. Haga clic en **Next (Siguiente)**.
6. Seleccione cualquiera de las siguientes configuraciones de SIP y puerto:
  - **Enable SIP (Habilitar SIP):** habilita SIP en los dispositivos seleccionados.
  - **Allow incoming SIP calls (Permitir llamadas SIP entrantes):** permite recibir llamadas SIP entrantes en sus dispositivos.
  - **SIP port (Puerto SIP) :** asigna un número de puerto para llamadas SIP.
  - **TLS Port (Puerto TLS):** asigna un número de puerto para el cifrado TLS.
  - **RTP start port (Puerto de inicio RTP):** asigna un número de puerto RTP al tráfico de audio.
7. Haga clic en **Next (Siguiente)**.
8. Seleccione cualquiera de las siguientes configuraciones de audio y llamada:

- **Audio direction (Dirección de audio):** elija entre **Send only (Solo enviar)**, **Receive only (Solo recibir)** o **Send and receive (Enviar y recibir)**.
  - **DTMF payload type (Tipo de carga útil DTMF):** elija el tipo de carga útil DTMF para transportar cifras, tonos y señales DTMF.
  - **Calling timeout (Tiempo de espera de llamada):** seleccione los segundos que se debe esperar hasta que finalice la llamada.
  - **Incoming call timeout (Tiempo de espera de llamada entrante):** seleccione los segundos que se debe esperar hasta que finalice el tiempo de espera de una llamada entrante.
  - **End calls after (Finalizar llamadas después de):** seleccione los segundos que se debe esperar hasta que una llamada entrante se finalice de forma automática. También puede optar por permitir una duración de llamada ilimitada.
9. Haga clic en **Next (Siguiente)**.
  10. Seleccione cualquiera de los siguientes parámetros para atravesar NAT (traducción de dirección de red):
    - **ICE Enable (Habilitar ICE):** habilita el establecimiento de conectividad interactiva (ICE) en los dispositivos seleccionados.
    - **TURN Enable (Habilitar TURN):** habilita el cruce mediante relés alrededor de la traducción de dirección de red (TURN).
    - **TURN server address (Dirección del servidor TURN):** introduzca la dirección del servidor TURN.
    - **TURN username (Nombre de usuario TURN):** introduzca el nombre de usuario en TURN.
    - **TURN password (Contraseña TURN):** introduzca la contraseña en TURN.
    - **STUN Enable (Habilitar STUN):** habilita las utilidades de cruce de sesión para la traducción de dirección de red (STUN).
    - **STUN server address (Dirección del servidor TURN):** introduzca la dirección del servidor STUN.
  11. Haga clic en **Next (Siguiente)**.
  12. Revise la configuración de los dispositivos de la lista.
  13. Si todo es correcto, haga clic en **Finish (Finalizar)**.

## Gestionar cuentas SIP

En Axis Device Manager puede configurar sus ajustes SIP y añadir o eliminar cuentas SIP.

### Añadir cuentas SIP

Para añadir cuentas SIP, debe especificarlas en un archivo CSV. Puede crear una plantilla en el asistente de configuración.

Para generar una plantilla:

1. Vaya al espacio de trabajo **Device management (Gestión de dispositivos)**.
2. Elija los dispositivos que desea configurar.
3. Haga clic con el botón derecho y seleccione **Configure devices (Configurar dispositivos) > Advanced (Avanzado) > SIP configuration (Configuración SIP) > Add SIP accounts (Añadir cuentas SIP)**.
4. Haga clic en **Generate template (Generar plantilla)**
5. Seleccione una ubicación donde guardar el archivo CSV.
6. Añada las cuentas al archivo. Utilice una fila para cada cuenta que desee añadir a un dispositivo. Puede añadir varias cuentas a un dispositivo.

El archivo CSV tiene el siguiente formato:

Nombre de columna	Descripción	Obligatorio/Opcional	Notas
deviceIdentifier	Dirección MAC, dirección IP o dirección de host	obligatorio	Esta columna especifica a qué dispositivo debe añadirse la cuenta. Puede tratarse de una dirección MAC, IPv4 o de host.
activo	Booleano	obligatorio	
makeDefault	Booleano	obligatorio	
answerAutomatically	Booleano	obligatorio	
nombre	cadena	obligatorio	
userId	cadena	obligatorio	
dominio	cadena	opcional	Si el archivo SSV no contiene esta columna, todas las cuentas se configurarán como punto a punto. Si la columna está presente, la cuenta será Punto a punto si la celda está vacía y Registrada si contiene información.
Contraseña	cadena	obligatorio	
authenticationId	cadena	obligatorio	
callerId	cadena	obligatorio	
registrar	cadena	opcional	
transportMode	udp o tcp	obligatorio	En MVP1, no se admite TLS.

Para añadir las cuentas a los dispositivos seleccionados:

- Vaya al espacio de trabajo **Device management (Gestión de dispositivos)**.
- Elija los dispositivos que desea configurar.
- Haga clic con el botón derecho y seleccione **Configure devices (Configurar dispositivos) > Advanced (Avanzado) > SIP configuration (Configuración SIP) > Add SIP accounts (Añadir cuentas SIP)**.
- Haga clic en **Browse (Examinar)**.
- Seleccione el archivo CSV al que añadió las cuentas.
- Haga clic en **Next (Siguiente)**
- Revise la configuración de los dispositivos de la lista.
- Si todo es correcto, haga clic en **Finish (Finalizar)**.

### Eliminar cuentas SIP

Para eliminar todas las cuentas SIP excepto la predeterminada en los dispositivos seleccionados:

1. Vaya al espacio de trabajo **Device management (Gestión de dispositivos)**.
2. Elija los dispositivos que desea configurar.
3. Haga clic con el botón derecho y seleccione **Configure devices (Configurar dispositivos) > Advanced (Avanzado) > SIP configuration (Configuración SIP) > Remove accounts (Eliminar cuentas)**.

4. En el asistente de configuración, marque **Remove all accounts except the default account on the selected devices** (Eliminar todas las cuentas excepto la predeterminada en los dispositivos seleccionados).
5. Haga clic en **Finish** (Finalizar).

### Habilitar metadatos en dispositivos

En este ejemplo, habilitaremos metadatos en varios dispositivos. Antes de realizar esta tarea, le recomendamos probarla en un dispositivo para evitar problemas con varios a la vez. Para habilitar metadatos en uno o más dispositivos:

1. Vaya al espacio de trabajo **Device management** (Gestión de dispositivos).
2. Seleccione los dispositivos en los que desea habilitar metadatos.
3. Haga clic con el botón derecho y seleccione **Configure devices** (Configurar dispositivos) > **Advanced** (Avanzado) > **Set configuration** (Establecer configuración).
4. Haga clic en **OK**
5. Seleccione **Set NTP servers** (Configurar servidores NTP) en el menú desplegable.
6. En el menú desplegable **Uri**, asegúrese de que el método sea **Post**.
7. En el campo de dirección, añada lo siguiente: **axis-cgi/analyticsmetadataconfig.cgi**
8. Añada el siguiente código en **Content** (Contenido):

```
{ "apiVersion": "1.0", "context": "my context", "method": "setEnabledProducers", "params": {  
  "producers": [ { "name": "objectanalytics", "videochannels": [ { "channel": 1, "enabled": true }  
  ] } ] }
```

9. Compruebe que **Content-Type** (Contenido-Tipo) es **application/json**
10. Haga clic en **Send** (Enviar).

#### Nota

Recuerde que AXIS Device Manager no devolverá respuesta al usar el método anterior. Revise siempre el panel **Tasks** (Tareas) en busca de errores. También puede usar un software específico como POSTMAN para probar la API con funcionalidad mejorada. Algunos VMS pueden tener limitaciones que solo permiten un productor a la vez, por lo que podría ser necesario deshabilitar los productores adicionales mediante la API antes mencionada.

## Gestión del software del dispositivo

### Actualizaciones al AXIS OS

Las nuevas versiones de AXIS OS pueden obtenerse de dos formas:

- Descargándolas con AXIS Device Manager (requiere acceso a internet)
- Importándolas desde un archivo (por ejemplo, en un disco duro o un dispositivo de memoria).

#### Nota

Le recomendamos seguir la ruta de actualización recomendada por AXIS OS. Más información en: <https://help.axis.com/axis-os#upgrade-path>

#### Actualización manual de AXIS OS

1. Seleccione los dispositivos que desea actualizar con una nueva versión de AXIS OS, haga clic con el botón derecho del ratón y seleccione **Upgrade firmware (Actualizar firmware)**.
2. Cuando se le indique que los dispositivos resultarán inaccesibles durante la actualización, haga clic en **Sí**.
3. Para actualizar la lista de versiones de firmware disponibles para descargar en el cuadro de diálogo **Upgrade firmware (Actualizar firmware)**, haga clic en **Check for Updates (Buscar actualizaciones)**.
4. Para examinar uno o varios archivos de versión de AXIS OS almacenados en el cliente local, haga clic en el botón **Browse (Examinar)**.
5. Seleccione los dispositivos y las versiones del AXIS OS que desea actualizar.
6. Para establecer la versión predeterminada de fábrica de los dispositivos seleccionados durante la actualización de AXIS OS, haga clic en la casilla de verificación **Factory default (Opción predeterminada de fábrica)**. Este paso es obligatorio cuando se revierte una actualización de algunas versiones de AXIS OS.
7. Haga clic en **OK (Aceptar)** para iniciar la actualización de los dispositivos seleccionados de la lista.

#### Nota

De forma predeterminada, las actualizaciones del AXIS OS se realizan simultáneamente para todos los dispositivos seleccionados. Puede modificar el orden de las actualizaciones en **Configuration (Configuración) > Connected Services (Servicios conectados) > Firmware upgrade settings (Ajustes de actualización de firmware)**.

#### Actualizaciones automáticas

El ajuste predeterminado de AXIS Device Manager 5 es no buscar ninguna actualización de firmware, pero puede configurarse para que compruebe automáticamente si existen actualizaciones disponibles de AXIS OS en el servidor o en axis.com.

Para buscar manualmente las actualizaciones de AXIS OS, pulse el botón **Check now (Comprobar ahora)** en el menú de acciones.

#### Orden de actualización de AXIS OS

Las actualizaciones de AXIS OS pueden hacerse en todos los dispositivos a la vez o en un dispositivo tras otro.

- Para actualizar todos los dispositivos a la vez, seleccione el orden de actualización **Parallel (Paralelo)**.
- Para actualizar dispositivos uno tras otro, seleccione **Sequential (Secuencial)**. Esta opción tarda más, pero los dispositivos no se quedan sin conexión al mismo tiempo. También puede elegir detener una actualización secuencial si se produce un problema al marcar la casilla **Cancel all remaining upgrades if one device fails (Cancelar todas las actualizaciones restantes si un dispositivo falla)**.

## Localización de problemas

### Lista de componentes de software

Para obtener la lista de componentes de software (SBOM):

1. Vaya a *la página de asistencia técnica de AXIS Device Manager* en [axis.com](http://axis.com).
2. Haga clic en **LISTA DE COMPONENTES DE SOFTWARE**.

Para obtener más información sobre la SBOM, vaya al *AXIS OS Portal* en [axis.com](http://axis.com).

### Contactar con la asistencia técnica

Cuando se ponga en contacto con el soporte técnico, cree primero un ticket e incluya un archivo de informe del sistema para facilitar la localización de su problema concreto:

1. Vaya al menú principal.
2. Vaya a **Help (Ayuda) > System Report... (Informe del sistema)**
3. Guarde el archivo del informe en la carpeta que elija.
4. Vaya a [axis.com/support](http://axis.com/support).
5. Crear un ticket de soporte.
6. Adjunte el archivo a su ticket de soporte técnico.

#### Nota

Para crear un informe del sistema desde un sistema que no responde:

1. Ir a `C:\ProgramData\Axis Communications\`
2. Archive el contenido de la carpeta en un archivo .zip y adjúntelo al ticket de soporte técnico.

### Proceso de escalada

Si tiene incidencias que no se pueden resolver con esta guía, escale el problema a soporte en línea de Axis, consulte *soporte en línea de Axis*. Para que nuestro servicio técnico entienda la incidencia y pueda resolverla, debe incluir la siguiente información:

- Una descripción clara sobre cómo reproducir la incidencia o en qué circunstancias se produce.
- La hora y el nombre del dispositivo correspondiente o la dirección IP en la que se produce la incidencia.
- **AXIS Device Manager informe de sistema** generado inmediatamente después de producirse la incidencia. El informe del sistema debe generarse desde el cliente o el servidor donde se reprodujo la incidencia.
- Capturas de pantalla o grabaciones opcionales donde se muestre el problema.
- Si es necesario, incluya los archivos de la base de datos. Exclúyalas para que la carga vaya más rápido.

Algunos problemas requieren información adicional que el equipo de soporte solicita si es necesario.

#### Nota

Si el archivo es superior a 100 MB, por ejemplo, un rastreo de red o un archivo de la base de datos, use un archivo seguro mediante un servicio de uso compartido de archivos seguro en el que confíe para enviar el archivo.

Información adicional	
Registros de nivel de depuración	En ocasiones, usamos el registro de nivel de depuración para recopilar más información. Solo es así si lo solicita un ingeniero de soporte de Axis. Consulte las instrucciones en el servicio de <i>soporte en línea de Axis</i> .
Rastreo de red	Si lo solicita el ingeniero de soporte, genere trazas de red al crear el informe del sistema. Tome las trazas de red al mismo tiempo que se produce el problema, cuando este es reproducible. Recursos utilizados: <ul style="list-style-type: none"> <li>• Un seguimiento de red de 60 segundos tomado en la cámara (aplicable solo para firmware 5.20 y posteriores) Utilice el siguiente comando VAPIX para cambiar el inicio de sesión, la dirección IP y la duración (en segundos) si es necesario: <code>http://root:pass@192.168.0.90/axis-cgi/debug/debug.tgz?cmd=pcapdump&amp;duration=60</code></li> <li>• Un seguimiento de red de 10-30 segundos tomado en el servidor que muestra la comunicación entre el servidor y la cámara.</li> </ul>
Archivos de base de datos	En casos en los que tenemos que examinar o reparar manualmente la base de datos. Seleccione la opción <b>Include database in the report (Incluir base de datos en el informe)</b> antes de generar el informe del sistema.
Capturas de pantalla	Utilice las capturas de pantalla cuando se trate de un problema de la visualización en directo relacionado con la interfaz de usuario. Por ejemplo, si desea mostrar una línea temporal para las grabaciones o cuando es difícil describirla.
Grabaciones de pantalla	Utilice grabaciones de pantalla cuando resulte difícil describir el problema con palabras, por ejemplo, cuando hay muchas interacciones en la interfaz de usuario involucradas para reproducir el problema.

T10211981\_es

2026-03 (M5.2)

© 2024 – 2026 Axis Communications AB