

AXIS Device Manager Extend

Manual del usuario

AXIS Device Manager Extend

Índice

| | |
|--|----|
| Acerca de | 3 |
| Información general de la solución | 4 |
| Requisitos previos | 7 |
| Procedimientos iniciales | 9 |
| Registrar una cuenta MyAxis | 9 |
| Instalación del cliente y activación de su cuenta | 9 |
| Instalar el host en el extremo | 10 |
| Reclamar el host en el extremo | 10 |
| Gestionar dispositivos | 11 |
| Agregar dispositivos detectados a un host en el extremo | 11 |
| Eliminar dispositivos | 12 |
| Iniciar sesión en sus dispositivos. | 12 |
| Configuración | 13 |
| Activación de acceso remoto | 13 |
| Eliminar una instalación | 13 |
| Agregar usuarios a su organización | 13 |
| Eleva el rol del usuario | 13 |
| Eliminar usuarios | 14 |
| Gestión de firmware | 15 |
| Gestionar firmware en función del modelo de dispositivo | 15 |
| Gestionar el firmware de dispositivos de un host en el extremo | 15 |
| Ver actualizaciones de firmware en curso y completadas | 15 |
| Policies (Políticas) | 16 |
| Crear y aplicar una política de seguridad | 16 |
| Crear y aplicar una política de aplicación | 16 |
| Editar una política | 17 |
| Eliminar una política | 17 |
| Solución de problemas | 18 |
| Cómo configurar los ajustes de cortafuegos | 18 |

AXIS Device Manager Extend

Acerca de

Acerca de

La solución AXIS Device Manager Extend proporciona a los administradores del sistema una interfaz para identificar, configurar y trabajar con dispositivos de Axis en las redes de su organización.

La aplicación de escritorio AXIS Device Manager Extend

La aplicación de escritorio es un programa de utilidad de software que se puede utilizar como interfaz de usuario, bajo demanda o siempre disponible, para la administración del sistema. Se puede ejecutar en un equipo dedicado junto con un host en el extremo local o de forma independiente del host en el extremo de un portátil conectado de forma remota. El cliente presenta al usuario el estado general del sistema disponible y las acciones de gestión disponibles.

Host en el extremo

El componente de host en el extremo de AXIS Device Manager Extend es un servicio de gestión local siempre disponible que es responsable de mantener dispositivos locales como cámaras. El host en el extremo de AXIS Device Manager Extend actúa también como un enlace al servicio de gestión remota de Axis, en el que la misma funcionalidad de API admite la gestión remota de instalaciones a través de la plataforma de servicio de Axis.

AXIS Device Manager Extend

Información general de la solución

Información general de la solución

AXIS Device Manager Extend con acceso local y remoto

- 1 *Axis*
- 2 *IAM (MyAxis)*
- 3 *Datos de la organización*
- 4 *Cliente local*
- 5 *Host en el extremo*
- 6 *Dispositivos*
- 7 *VMS*
- 8 *TURN*
- 9 *Señalización*
- 10 *Cliente remoto*
- 11 *Servidores WebRTC con acceso remoto*
- 12 *Instalación 1*

| Conexión | URL e IP | Puerto | Protocolo | Comentario |
|----------|--|---|----------------------------------|--|
| A | prod.adm.connect.axis.com (52.224.128.152 o 40.127.155.231) | 443 | HTTPS | Obligatorio |
| B | Detección de HTTP (de cliente a hosts en el extremo) Transferencia de datos (entre cliente y hosts en el extremo) Detección de multicast (de cliente a hosts en el extremo) Detección de multicast (de hosts en el extremo a cliente) | 37080 37443 6801 6801 | HTTP HTTPS UDP UDP | Necesario para aprovisionar la instalación. Opcional después del aprovisionamiento. |
| C | Transferencia de datos (entre el host en el extremo y los dispositivos) Detección de unicast Detección de multicast Detección de HTTP | 80/puerto personalizado, 443 1900 1900, 5353 80,443 | HTTP, HTTPS SSDP, Bonjour | Obligatorio |
| D | signaling.prod.webrtc.connect.axis.com *.turn.prod.webrtc.connect.axis.com | 443 443, 5349 | HTTPS HTTPS, DTLS (UDP y TCP) | Se basa en el estándar WebRTC Opcional y desactivado de forma predeterminada |
| E | De punto a punto (P2P) | 49152-65535 | DTLS (UDP y TCP) | |

AXIS Device Manager Extend con configuración en varias instalaciones mediante acceso remoto y local

- 1 *Axis*
- 2 *IAM (MyAxis)*
- 3 *Datos de la organización*
- 4 *Cliente local*
- 5 *Host en el extremo*
- 6 *Dispositivos*
- 7 *VMS*
- 8 *TURN*
- 9 *Señalización*
- 10 *Cliente remoto*

AXIS Device Manager Extend

Información general de la solución

- 11 *Servidores WebRTC con acceso remoto*
- 12 *Instalación 1*
- 13 *Instalación 2*
- 14 *Instalación 3*

| Conexión | URL e IP | Puerto | Protocolo | Comentario |
|----------|--|---|----------------------------------|--|
| A | prod.adm.connect.axis.com (52.224.128.152 o 40.127.155.231) | 443 | HTTPS | Obligatorio |
| B | Detección de HTTP (de cliente a hosts en el extremo) Transferencia de datos (entre cliente y hosts en el extremo) Detección de multicast (de cliente a hosts en el extremo) Detección de multicast (de hosts en el extremo a cliente) | 37080 37443 6801 6801 | HTTP HTTPS UDP UDP | Necesario para aprovisionar la instalación. Opcional después del aprovisionamiento. |
| C | Transferencia de datos (entre el host en el extremo y los dispositivos) Detección de unicast Detección de multicast Detección de HTTP | 80/puerto personalizado, 443 1900 1900, 5353 80,443 | HTTP, HTTPS SSDP, Bonjour | Obligatorio |
| D | signaling.prod.webrtc.connect.axis.com *.turn.prod.webrtc.connect.axis.com | 443 443, 5349 | HTTPS HTTPS, DTLS (UDP y TCP) | Se basa en el estándar WebRTC Opcional y desactivado de forma predeterminada |
| E | De punto a punto (P2P) | 49152-65535 | DTLS (UDP y TCP) | |

AXIS Device Manager Extender con acceso local y remoto usando una conexión VPN

- 1 *Axis*
- 2 *IAM (MyAxis)*
- 3 *Datos de la organización*
- 4 *Cliente local*
- 5 *Host en el extremo*
- 6 *Dispositivos*
- 7 *VMS*
- 8 *TURN*
- 9 *Señalización*
- 10 *Cliente remoto*
- 11 *Servidores WebRTC con acceso remoto*
- 12 *Instalación 1*
- 13 *Instalación 2*
- 14 *Instalación 3*

| Conexión | URL e IP | Puerto | Protocolo | Comentario |
|----------|---|--------|-----------|-------------|
| A | prod.adm.connect.axis.com (52.224.128.152 o 40.127.155.231) | 443 | HTTPS | Obligatorio |

AXIS Device Manager Extend

Información general de la solución

| | | | | |
|---|--|---|----------------------------------|--|
| B | Detección de HTTP (de cliente a hosts en el extremo) Transferencia de datos (entre cliente y hosts en el extremo) Detección de multicast (de cliente a hosts en el extremo) Detección de multicast (de hosts en el extremo a cliente) | 37080 37443 6801 6801 | HTTP HTTPS UDP UDP | Necesario para aprovisionar la instalación. Opcional después del aprovisionamiento. |
| C | Transferencia de datos (entre el host en el extremo y los dispositivos) Detección de unicast Detección de multicast Detección de HTTP | 80/puerto personalizado, 443 1900 1900, 5353 80,443 | HTTP, HTTPS SSDP, Bonjour | Obligatorio |
| D | signaling.prod.webrtc.connect.axis.com *.turn.prod.webrtc.connect.axis.com | 443 443, 5349 | HTTPS HTTPS, DTLS (UDP y TCP) | Se basa en el estándar WebRTC Opcional y desactivado de forma predeterminada |
| E | De punto a punto (P2P) | 49152-65535 | DTLS (UDP y TCP) | |

- Un requisito adicional es un DNS público como DNS de Google: 8.8.8.8/8.8.4.4 o Cloudflare DNS: 1.1.1.1
- Se necesitan conexiones A y C para admitir todas las funciones del sistema AXIS Device Manager Extend.
- La aplicación se está desarrollando en la actualidad, por lo que es aconsejable permitir que la aplicación de escritorio AXIS Device Manager Extend y los hosts en el extremo tengan acceso de cortafuegos a las conexiones de red salientes.

AXIS Device Manager Extend

Requisitos previos

Requisitos previos

Sistemas operativos compatibles:

- Windows 10 Pro y Enterprise
- Windows 11 Pro y Enterprise
- Windows Server 2016, 2019 y 2022 (sistema basado en x64)
- Privilegio de administrador del sistema necesario para cambios en la instalación y la configuración.

Recomendación mínima del sistema:

- CPU: Intel Core i5
- RAM: 4 GB
- Red: 100 Mbps

Conectividad a Internet

Nota

La aplicación AXIS Device Manager Extend precisa que la conectividad a Internet disponga de certificados que la identifiquen como perteneciente a la organización creada y asociada a la cuenta de MyAxis utilizada en la instalación. En cualquier caso, para disfrutar de ciertas características como la información de garantía y la compatibilidad multisitio, necesita una conexión a Internet. Además, el cliente o el controlador de la instalación solo se actualizan automáticamente en el modo con conexión.

Hora y fecha sincronizadas

Nota

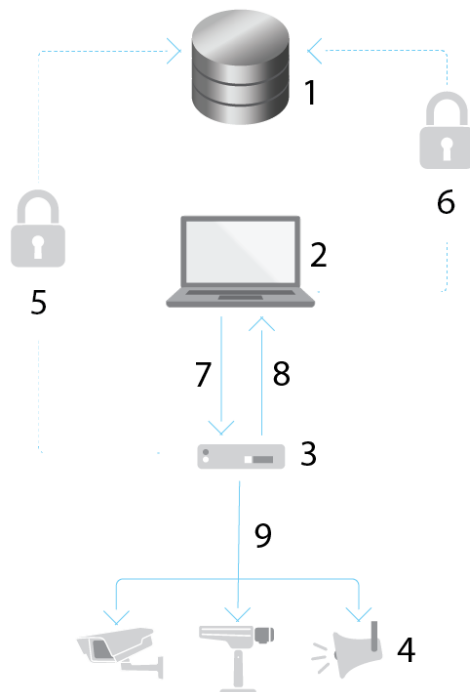
Asegúrese de que todos los componentes del sistema estén sincronizados; de lo contrario, podría producirse un error de autenticación de certificados entre host en el extremo y el cliente o el back-end. Se recomienda que todos los equipos host estén sincronizados con un servidor horario de red común para evitar problemas potenciales.

Puertos de red abiertos:

Para establecer conexiones seguras de la aplicación de escritorio AXIS Device Manager Extend con el host en el extremo, la detección de host en el extremo y Axis Remote Service.

AXIS Device Manager Extend

Requisitos previos



- 1 *Axis Service Platform*
- 2 *Aplicación de escritorio AXIS Device Manager Extend*
- 3 *Host en el extremo*
- 4 *Dispositivos*
- 5 *HTTPS (puerto 443)*
- 6 *HTTPS (puerto 443)*
- 7 *HTTPS (puerto 37443), detección de multicast UDP (puerto 6801), detección de HTTP (puerto 37080)*
- 8 *Detección de multidifusión UDP (puerto 6801)*
- 9 *HTTPS y HTTP (puerto 443 y 80), detección de multidifusión –SSDP (puerto 1900) – Bonjour (puerto 5353), detección de unidifusión (puerto 1900), detección HTTP (puerto 80 y 443)*

Acceso a la red saliente

La aplicación se está desarrollando en la actualidad, por lo que es aconsejable permitir que la aplicación de escritorio AXIS Device Manager Extend y los hosts en el extremo tengan acceso de cortafuegos a las conexiones de red salientes.

AXIS Device Manager Extend

Procedimientos iniciales

Procedimientos iniciales



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

help.axis.com/?etpiald=63389&tsection=get-started


Instalar el software, crear una organización y agregar dispositivos

Registrar una cuenta MyAxis

Registre una cuenta MyAxis en axis.com/my-axis/login.

Puede proteger mejor su cuenta MyAxis mediante la activación de la autenticación multifactor (MFA). MFA es un sistema de seguridad que agrega otra capa de verificación para garantizar la identidad del usuario.

Activar MFA:

1. Inicie sesión con sus credenciales de MyAxis.
2. Vaya a  seleccione **Account settings (Ajustes de cuenta)**.
3. Haga clic en **Security settings (Ajustes de seguridad)**.
4. Active la verificación en 2 pasos.

Se le redirigirá a una página de inicio de sesión.

5. Inicie sesión con sus credenciales de MyAxis.

Ahora MFA está activa.

Iniciar sesión con MFA activa:

1. Inicie sesión en su cuenta MyAxis.

Se le enviará un correo electrónico.

2. Abra el correo electrónico y haga clic en **Authenticate (Autenticar)**.

Si no ha recibido ningún correo electrónico, compruebe si está en la carpeta de correo no deseado. Si no está, póngase en contacto con el servicio de asistencia técnica de TI.

Instalación del cliente y activación de su cuenta

Vaya a la página del producto en axis.com y descargue el instalador de la aplicación de escritorio de AXIS Device Manager Extend

1. Localice dónde ha descargado la aplicación y haga clic para instalarla.
2. Seleccione **client (Cliente)** y haga clic en **Install (Instalar)**.

AXIS Device Manager Extend

Procedimientos iniciales

3. Inicie sesión en su cuenta MyAxis.
4. Confirme su dirección de correo electrónico para completar la activación.
5. Cree una organización o únase a una existente.

Instalar el host en el extremo

El host en el extremo y el cliente de escritorio se incluyen en el instalador de AXIS Device Manager Extend. Recomendamos instalar el host en el extremo en un servidor lo más cerca posible de sus dispositivos.

1. Elija el servidor en el que quiera instalar el host en el extremo.
2. Ejecute el instalador en el servidor y seleccione instalar solo el controlador en el extremo.

Reclamar el host en el extremo

Para crear una conexión segura con los dispositivos desde la aplicación de escritorio AXIS Device Manager Extend, primero debe reclamar un host en extremo para la organización.

1. Haga clic en un host en el extremo con el estado **Unclaimed (Sin reclamar)**.
 - 1.1 Haga clic en **Add new edge host (Agregar nuevo host en el extremo)** si no hay ninguno en la lista.
 - 1.2 Escriba la dirección IP en la que está el host en el extremo.
2. Escriba el nombre del host en el extremo.
3. Agregue una descripción opcional (recomendado).
4. Haga clic en **Claim edge host (Reclamar host en el extremo)**.

AXIS Device Manager Extend

Gestionar dispositivos

Gestionar dispositivos

Agregar dispositivos detectados a un host en el extremo

1. Vaya a **Edge hosts (Hosts en el extremo)**.
2. Seleccione un host en el extremo en la lista a la que quiere agregar dispositivos.
3. Vaya a **Devices > Discovered (Dispositivos > Detectados)**.
4. Seleccione los dispositivos que desee agregar o seleccione todos los dispositivos activando la casilla de la parte superior de la columna de selección.
5. Haga clic en **Add devices to edge host (Agregar dispositivos al host en el extremo)**.

Los dispositivos se muestran en la pestaña **Managed (Gestionados)** y su estado se puede consultar en **Edge host overview (Información general sobre host en el extremo)**.

Añadir dispositivos desde direcciones IP

Agregue dispositivos que no se descubran automáticamente desde subredes, direcciones IP o un rango de direcciones IP.

Agregar dispositivos de un intervalo de IP

1. Vaya a un host en el extremo reclamado por su organización.
2. Vaya a **Settings > Device discovery options (Ajustes > Detección de dispositivos)**.
3. Haga clic en **Add by IP (Agregar por IP)**.
4. Seleccione **Manual entry (Entrada manual)**.
5. Introduzca el intervalo de IP.
6. Haga clic en **Add IP addresses (Agregar direcciones IP)**.
7. Vaya a **Devices > Discovered (Dispositivos > Detectados)**.
8. Seleccione los dispositivos que desee agregar o seleccione todos los dispositivos activando la casilla de la parte superior de la columna de selección.
9. Haga clic en **Add devices (Agregar dispositivos)**.

Agregar dispositivos desde un archivo

1. Vaya a un host en el extremo reclamado por su organización.
2. Vaya a **Settings > Device discovery options (Ajustes > Detección de dispositivos)**.
3. Haga clic en **Add by IP (Agregar por IP)**.
4. Seleccione **Import from file (Importar desde archivo)**.
5. Seleccione un archivo de datos separados por comas (. CSV) con las direcciones IP.
6. Haga clic en **Import (Importar)**.
7. Vaya a **Devices > Discovered devices (Dispositivos > Dispositivos detectados)**.
8. Seleccione los dispositivos que desee agregar o seleccione todos los dispositivos activando la casilla de la parte superior de la columna de selección.

AXIS Device Manager Extend

Gestionar dispositivos

9. Haga clic en **Add devices (Agregar dispositivos)**.

Nota

El archivo debe tener:
Un encabezado para la columna de direcciones IP.
Una única columna.
Un máximo de 25 600 direcciones IP.

Eliminar dispositivos



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

help.axis.com/?&pid=63389&tsection=remove-devices

Eliminar dispositivos de un host en el extremo

1. Haga clic en **Edge hosts (Hosts en el extremo)**.
2. Seleccione un host en el extremo.
3. Vaya a **Devices (Dispositivos)**.
4. Seleccione los dispositivos que desee eliminar o seleccione todos los dispositivos activando la casilla de la parte superior de la columna de selección.
5. Haga clic en el icono **Remove devices from edge host (Eliminar dispositivos del host en el extremo)** en el menú de acciones.
6. Haga clic en **Remove (Eliminar)**.

Los dispositivos eliminados se pueden encontrar en **Devices > Discovered (Dispositivos > Detectados)**.

Iniciar sesión en sus dispositivos.

1. Haga clic en **Edge hosts (Hosts en el extremo)**.
2. Seleccione un host en el extremo.
3. Vaya a **Devices > Managed (Dispositivos > Gestionados)**.
4. Seleccione los dispositivos a los que desee acceder o seleccione todos los dispositivos activando la casilla de la parte superior de la columna de selección.
5. Haga clic en **Log in (Iniciar sesión)** para iniciar sesión automáticamente en varios dispositivos.
6. Escriba el nombre de usuario y la contraseña.
7. Haga clic en **Log in (Iniciar sesión)**.

Nota

Si el nombre de usuario y la contraseña son correctos, en **Status (Estado)** se mostrará **Reachable (Localizado)**.

AXIS Device Manager Extend

Configuración

Configuración

Activación de acceso remoto

Si la configuración del cortafuegos bloquea las conexiones salientes, es posible que tenga que introducir una conexión proxy para acceder a la instalación de forma remota.

1. Seleccione el host en el extremo en el que desea activar el acceso remoto.
2. Vaya a **Settings > Edge hosts connections (Ajustes > Conexiones de hosts en el extremo)**.
3. Active **Allow remote access to edge host (Permitir el acceso remoto al host en el extremo)**.
4. Si necesita escribir una dirección proxy para acceder a Internet, escriba una dirección en **Proxy address (Dirección proxy)**.

Se le notificará cuando la conexión esté activa.

Nota

Para que la conexión sea compatible con los hosts en el extremo en otras redes, es posible que tenga que agregar la siguiente configuración a la "lista permitida" del cortafuegos de red corporativa: Endpoint Port Protocol signaling.prod.webrtc.connect.axis.com 443 HTTPS *.turn.prod.webrtc.connect.axis.com 443 HTTPS webRTC (Turn and P2P) 5349, 49152 - 65535 DTLS (UDP and TCP)

Eliminar una instalación

Antes de eliminar un host en el extremo de la organización, debe *Eliminar dispositivos en la página 12* pertenecientes a ese host. Los dispositivos se pueden encontrar en **Devices > Discovered (Dispositivos > Detectados)**.

1. Haga clic en **Edge hosts (Hosts en el extremo)**.
2. Seleccione el host en el extremo con las teclas de flecha o desplace el ratón sobre él con el puntero.
3. Haga clic en **...** y seleccione **Remove edge host (Eliminar host en el extremo)** en el menú desplegable.
4. Active **I'm aware of the risks. (Soy consciente de los riesgos.)**
5. Haga clic en **Remove (Eliminar)**.

Agregar usuarios a su organización

1. Seleccione la organización en la que quiera configurar los ajustes de usuario.
2. Vaya a **Users (Usuarios)**.
3. Haga clic en **Invite to organization (Invitar a la organización)**.
4. Introduzca la dirección de correo electrónico del usuario que quiera invitar a su organización.
5. Haga clic en **Send invite (Enviar invitación)**.

Nota

El usuario recibirá un correo electrónico de invitación que podrá utilizar para iniciar sesión en AXIS Device Manager Extend. El rol de usuario predeterminado es **Viewer (Observador)**. Si no dispone de una cuenta de MyAxis, debe utilizar este correo electrónico para registrarse y acceder a la organización. Las invitaciones pueden revocarse mientras se espera la aceptación.

Elevar el rol del usuario

1. Seleccione la organización en la que quiera configurar los ajustes de usuario.

AXIS Device Manager Extend

Configuración

2. Vaya a **Users (Usuarios)**.
3. Vaya a **Role (Rol)** en el usuario al que desea elevar.
4. Haga clic en el menú desplegable para seleccionar el nuevo rol.

Nota

El rol cambia inmediatamente una vez seleccionado. Por motivos de seguridad, las invitaciones se limitan al rol de espectador.

Eliminar usuarios

1. Seleccione la organización en la que quiera configurar los ajustes de usuario.
2. Vaya a **Users (Usuarios)**.
3. Desplace el puntero del ratón sobre el usuario que desee eliminar para que aparezca otro menú de opciones: ...
4. Haga clic en ... y seleccione **Remove user (Eliminar usuario)** en el menú desplegable.

AXIS Device Manager Extend

Gestión de firmware

Gestión de firmware

Con AXIS Device Manager Extend puede gestionar el firmware de varios dispositivos en cada organización.

Para obtener una lista de las actualizaciones de firmware disponibles para todos los dispositivos de su organización agrupadas por modelo, vaya a **Home > Firmware inventory (Inicio > Inventario de firmware)**. Para obtener una lista de las actualizaciones de firmware disponibles en un host en el extremo concreto, seleccione el host y vaya a **Firmware inventory (Inventario de firmware)**.

Gestionar firmware en función del modelo de dispositivo

Para gestionar el firmware por modelo de dispositivo en toda la organización:

1. Vaya a **Home > Firmware inventory (Inicio > Inventario de firmware)**.
2. Marque el modelo que quiera gestionar.
3. Haga clic en el menú desplegable **Upgrade to (Actualizar a)** para ver las opciones disponibles. Se preseleccionará el firmware más reciente.
4. Haga clic en **Upgrade (Actualizar)**.

Gestionar el firmware de dispositivos de un host en el extremo

Para gestionar el firmware de los dispositivos de un host en el extremo:

1. Vaya a **Edge hosts (Hosts en el extremo)**.
2. Haga clic en el host en el extremo al que desee acceder.
3. Vaya a **Devices (Dispositivos)**.
4. Seleccione los dispositivos que quiera gestionar.
5. Haga clic en el icono de **Firmware** en el menú de acciones.
6. Marque todos o solo algunos de los modelos de la lista.
7. Si desea cambiar el firmware seleccionado, haga clic en el firmware sugerido para ver qué está disponible para cada dispositivo. Se preseleccionará el firmware más reciente.
8. Haga clic en **Upgrade (Actualizar)**.

Ver actualizaciones de firmware en curso y completadas

Para ver las actualizaciones de firmware completadas:

1. Vaya a **Instalaciones**.
2. Haga clic en la instalación a la que desee acceder.
3. Vaya a **Tareas**

Para ver actualizaciones de firmware en curso:

4. Vaya a **Instalaciones**.
5. Haga clic en la instalación a la que desee acceder.
6. Vaya a **Tareas > Tareas en curso**

AXIS Device Manager Extend

Policies (Políticas)

Policies (Políticas)

Las políticas gestionan sus dispositivos automáticamente. Cree políticas para mantener la ciberseguridad en toda la instalación. También puede definir una política para instalar y actualizar aplicaciones automáticamente en sus dispositivos.

Crear y aplicar una política de seguridad

En este ejemplo de uso, se crea una política de seguridad básica y se aplica a un número determinado de dispositivos conectados a un host en el extremo.

Cree una política de seguridad básica:

1. Vaya a **Edge hosts (Hosts en el extremo)**.
2. Haga clic en el host en el extremo al que desee acceder.
3. Vaya a **Devices (Dispositivos)**.
4. Haga clic en el icono + situado junto a **Policies (Políticas)**.
5. Seleccione **Basic security (Seguridad básica)** y haga clic en **Continue (Continuar)**.
6. Asigne un nombre a su política
7. Seleccione la configuración que se ajusta a sus necesidades de seguridad. Para el nivel de seguridad recomendado, mantenga el ajuste predeterminado.
 - Para cambiar la contraseña raíz de los dispositivos seleccionados, haga clic en **Device root password (Contraseña raíz del dispositivo)** y escriba la nueva contraseña raíz.
8. Haga clic en **Create (Crear)**.

Aplique la política:

1. Seleccione los dispositivos a los que quiera aplicar la directiva.
2. Haga clic en el icono de **Policy options (Opciones de políticas)** en el menú de acciones.
3. Seleccione la política de seguridad y haga clic en **Save (Guardar)**.

Crear y aplicar una política de aplicación

En este ejemplo de uso, se crea una política de aplicación y se aplica a un número determinado de dispositivos conectados a un host en el extremo.

1. Vaya a **Edge hosts (Hosts en el extremo)**.
2. Haga clic en el host en el extremo al que desee acceder.
3. Vaya a **Devices (Dispositivos)**.
4. Haga clic en el icono + situado junto a **Policies (Políticas)**.
5. Seleccione **Apps (Aplicaciones)** y haga clic en **Continue (Continuar)**.
6. Asigne un nombre a la política.
7. Seleccione las aplicaciones que desee instalar y actualizar en sus dispositivos.
8. Seleccione el plazo de actualización en el menú desplegable.

AXIS Device Manager Extend

Policies (Políticas)

9. Haga clic en **Create (Crear)**.

Aplique la política:

1. Seleccione los dispositivos a los que quiera aplicar la directiva.
2. Haga clic en el icono de **Policy options (Opciones de políticas)** en el menú de acciones.
3. Seleccione la política de aplicación que desee aplicar.
4. Haga clic en **Save (Guardar)**.

Nota

Las aplicaciones seleccionadas se volverán a instalar automáticamente si se eliminan.

Editar una política

Para editar una política existente:

1. Vaya a **Edge hosts (Hosts en el extremo)**.
2. Haga clic en el host en el extremo al que desee acceder.
3. Vaya a **Devices (Dispositivos)**.
4. Haga clic en ... junto a la política que quiera editar y seleccione **Edit policy (Editar política)** en el menú desplegable.
5. Edite los ajustes de la política como desee.
6. Haga clic en **Save (Guardar)**.

Eliminar una política

Para eliminar una política existente:

- Vaya a **Edge hosts (Hosts en el extremo)**.
- Haga clic en el host en el extremo al que desee acceder.
- Vaya a **Devices (Dispositivos)**.
- Haga clic en ... junto a la política que quiera editar y seleccione **Delete policy (Eliminar política)** en el menú desplegable.
- Haga clic en **Eliminar**

Nota

Cualquier dispositivo con esta directiva aplicada mantendrá la configuración de la directiva, pero la configuración ya no será persistente.

AXIS Device Manager Extend

Solución de problemas

Solución de problemas

Cómo configurar los ajustes de cortafuegos

El cliente de AXIS Device Manager Extend requiere acceso al dominio axis.com y a cualquier subdominio.

Para que el host en el extremo de AXIS Device Manager Extend se comuniquen con el servicio de Axis, las siguientes direcciones IP y puertos se deben agregar a la lista de permitidos del cortafuegos de la organización:

- 40.127.155.231 (UE), puerto 443
- 52.224.128.152 y 40.127.155.231 (EE. UU.), puerto 443
- Una IP de servidor DNS público, puerto 53

Otra opción es utilizar el dominio prod.adm.connect.axis.com (que es un registro de DNS A que apunta a las direcciones IP anteriores) en los ajustes del cortafuegos.

El host en el extremo de AXIS Device Manager Extend utiliza el nombre de dominio prod.adm.connect.axis.com para todas las solicitudes de salida.

Para que esto funcione, la red deberá utilizar un servidor DNS público y permitir la salida de tráfico hacia la dirección IP del servidor DNS (y el puerto predeterminado 53).

