AXIS Device Manager Extend

Manual del usuario

Índice

Acerca de 3
Acerca de las organizaciones 4
Presentación esquemática de la solución 5
Requisitos 10
Cómo funciona 12
    Registrar una cuenta MyAxis 12
    Instalación del cliente y activación de su cuenta 12
    Crear una organización 12
    Instalar el host en el extremo 12
    Reclamar el host en el extremo 12
Gestionar dispositivos 14
    Agregar dispositivos detectados a un host en el extremo 14
        Añadir dispositivos desde direcciones IP 14
        Agregar dispositivos desde intervalo IP 14
        Agregar dispositivos desde un archivo 14
    Eliminar dispositivos 15
    Iniciar sesión en sus dispositivos. 15
Configuración 16
    Activación de acceso remoto 16
    Eliminar una instalación 16
    Agregar usuarios a su organización 16
    Acerca de los roles de usuario 16
    Elevar el rol del usuario 17
    Eliminar usuarios 17
Gestión de AXIS OS 18
    Gestionar las versiones de AXIS OS en función del modelo 18
    Gestionar AXIS OS en un host local. 18
    Ver las actualizaciones de AXIS OS en curso y finalizadas 18
Políticas 19
    Crear y aplicar una política de seguridad 19
    Crear y aplicar una política de aplicación 19
    Editar una política 20
    Eliminar una política 20
Gestionar licencias 21
    Obtener una licencia del producto 21
Localización de problemas 22
    Cómo configurar los ajustes de cortafuegos 22

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 extremos 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

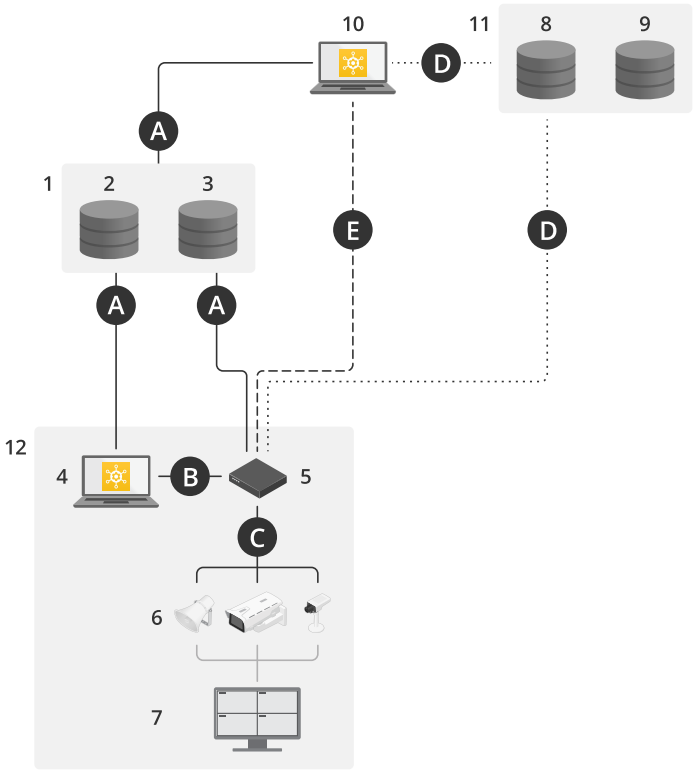
El componente de host en el extremo de AXIS Device Manager Extend es un servicio de gestión local siempre disponible que es responsable de mantener dispositivos locales como cámaras. El host en el extremo de AXIS Device Manager Extend actúa también como un enlace al servicio de gestión remota de Axis,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

Acerca de las organizaciones

La organización es una representación virtual de las instalaciones del sistema de Axis y está en el centro de los servicios en la nube. Una organización aloja todos los dispositivos y las cuentas de usuario de una empresa en una categoría que regula el acceso y garantiza la máxima seguridad. Al mismo tiempo, permite una gestión flexible de usuarios y dispositivos tanto para pequeños negocios como para grandes empresas.

- Cuando crea una nueva organización, se convierte en su propietario. La organización conecta el sistema a los usuarios del servicio en la nube de Axis.
- Puede invitados a los usuarios a la organización. Consulte *Agregar usuarios a su organización, on page 16*.
- Puede asignar distintas funciones a los usuarios.
- La organización contiene una carpeta predeterminada en la que puede empezar a desarrollar la estructura de la estructura que mejor se ajuste a sus necesidades. Puede estructurar la organización en carpetas y subcarpetas. Normalmente, una carpeta representa la instalación física o la ubicación de un sistema dentro de una organización.
- Gestione sus licencias para su sistema dentro de su organización.
- Para crear una organización, necesita una cuenta My Axis.

Presentación esquemática de la solución

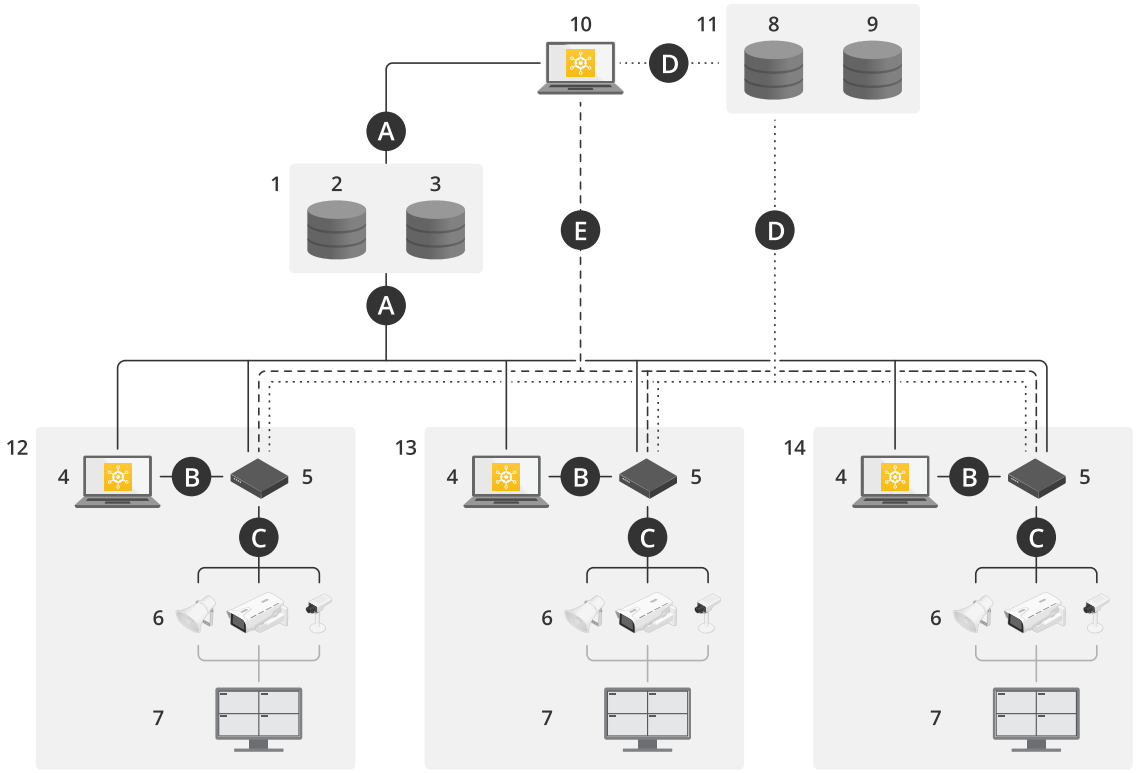


AXIS Device Manager Extend con acceso local y remoto

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, cep.connect.axis.com (52.224.128.152, 40.127.155.231, 75.2.119.140, 99.83.133.42)	443, 8443	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)	37080 37443 6801 6801	HTTP HTTPS UDP UDP	Necesaria para el aprovisionamiento del sitio. Opcional después de aprovisionamiento.

	Detección de multicast (de hosts en el extremo a cliente)			
C	Transferencia de datos (entre el host local y los dispositivos) Detección unicast Detección multicast Detección 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)	

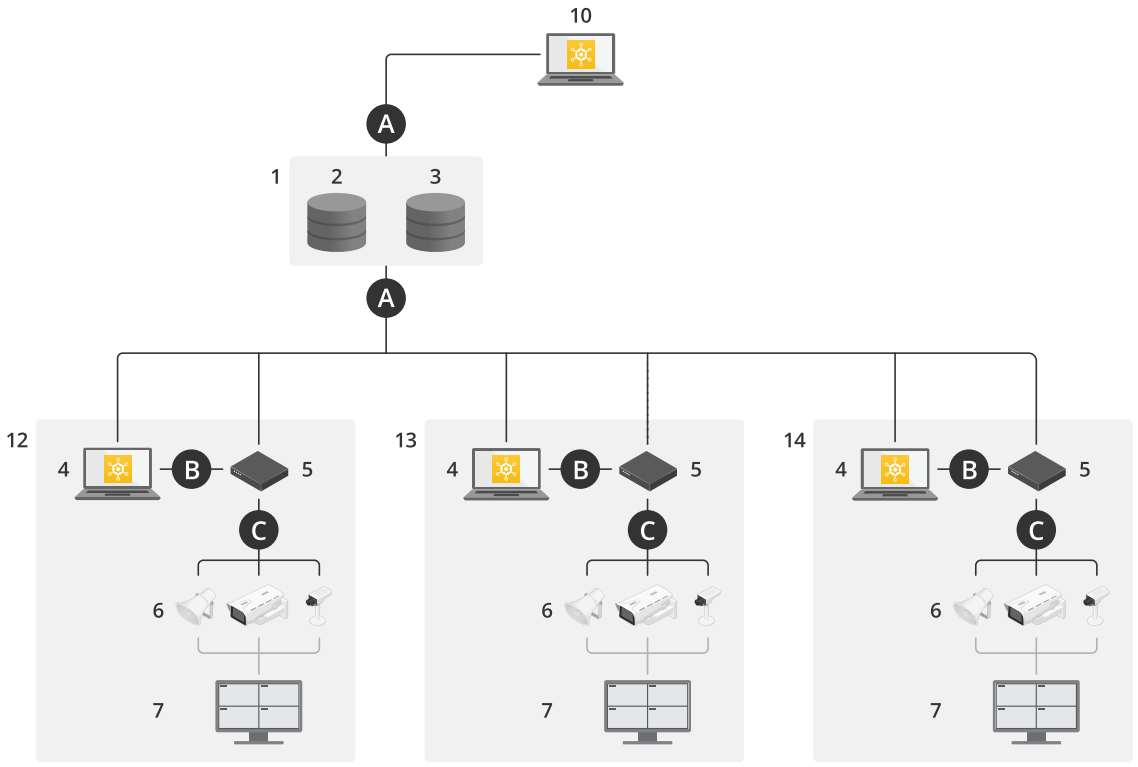


AXIS Device Manager Extend con configuración en varias instalaciones mediante acceso remoto y local

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*
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, cep.connect.axis.com (52.224.128.152, 40.127.155.231, 75.2.119.140, 99.83.133.42)	443, 8443	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	Necesaria para el aprovisionamiento del sitio. Opcional después de aprovisionamiento.
C	Transferencia de datos (entre el host local y los dispositivos) Detección unicast Detección multicast Detección 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 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, cep.connect.axis.com (52.224.128.152, 40.127.155.231, 75.2.119.140, 99.83.133.42)	443, 8443	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)	37080 37443 6801 6801	HTTP HTTPS UDP UDP	Necesaria para el aprovisionamiento del sitio. Opcional después de aprovisionamiento.

	Detección de multicast (de hosts en el extremo a cliente)			
C	Transferencia de datos (entre el host local y los dispositivos) Detección unicast Detección multicast Detección 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 DNS de Cloudflare: 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.

Requisitos

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 host local solo se actualizan automáticamente en el modo con conexión.

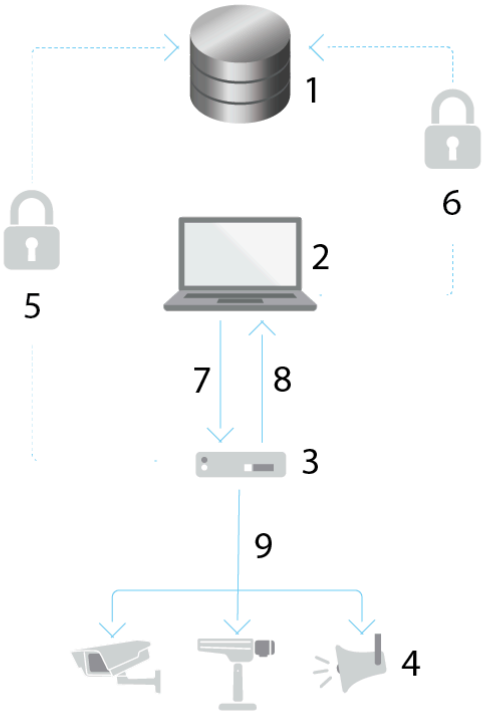
Hora y fecha sincronizadas

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.



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.

Cómo funciona

Registrar una cuenta MyAxis

1. Registre una cuenta **My Axis** en *axis.com/my-axis/login*.
2. Elija uno de los métodos de autentificación multifactor (MFA): **Authenticator App (TOTP)** o **Email (Correo electrónico)** y siga las instrucciones en pantalla. MFA es un sistema de seguridad que añade una etapa adicional de verificación para garantizar la identidad del usuario.

Instalación del cliente y activación de su cuenta

Visite la página del producto en axis.com y descargue la aplicación de escritorio Axis Device Management

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

Crear una organización

Para agregar dispositivos al sistema, tiene que formar parte de una organización. De esta forma, mantiene y protege sus dispositivos de forma segura en una o varias instalaciones. Si aún no es miembro de una organización, aparecerá un asistente de configuración que le guiará durante el proceso.

Para crear una organización:

1. Inicie sesión en su cuenta MyAxis.
2. Siga las instrucciones del asistente de configuración.

Para crear más organizaciones:

- Vaya al menú desplegable con el nombre de su organización.
- Seleccione **+ Create new organization (Crear nueva organización)**
- Siga las instrucciones del asistente de configuración.

Instalar el host en el extremo

Visite la página del producto en axis.com y descargue el servidor de borde (servidor Axis Device Management)..

1. Elija el servidor en el que quiera instalar el host en el extremo. Recomendamos instalar el host local en un servidor lo más cerca posible de sus dispositivos.
2. Ejecute el instalador en el servidor.

Reclamar el host en el extremo

Para crear una conexión segura con los dispositivos desde la aplicación de escritorio Axis Device Management, primero deberá solicitar un servidor de borde a su 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)**.

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 desde intervalo 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 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.
9. Haga clic en **Add devices** .

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

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)**.

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 asegurar la conexión a hosts locales en otras redes, es posible que tenga que agregar la siguiente configuración a la «lista de permitidos» de su cortafuegos de red corporativa: Protocolo de puerto final signaling.prod.webrtc.connect.axis.com 443 HTTPS *.turn.prod.webrtc.connect.axis.com 443 HTTPS webRTC (Turn y P2P) 5349, 49152 - 65535 DTLS (UDP y TCP)

Eliminar una instalación

Antes de eliminar un host en el extremo de la organización, debe *Eliminar dispositivos, on page 15* pertenecientes a ese host. Los dispositivos se pueden encontrar en **Devices > Discovered (Dispositivos > Detectados)**.

1. Haga clic en **Edge hosts (Hosts locales)**.
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 al panel My Systems (Mis sistemas).
3. Vaya a **ORGANIZATION > Users (ORGANIZACIÓN > Usuarios)**.
4. Haga clic en **Invite users (Invitar usuarios)**.
5. Siga las instrucciones en pantalla en el asistente de configuración.
   - Si ha seleccionado **Operator (Operador)** o **Viewer (Visor)**, seleccione a qué carpetas tendrán acceso los usuarios. Tenga en cuenta que las funciones **Admin (Administrador)** tienen acceso a todas las carpetas de la organización.

Nota

El usuario recibirá un correo electrónico de invitación que podrá utilizar para iniciar sesión en My Systems. Si el usuario no tiene una cuenta My Axis, deberá utilizar ese correo electrónico para registrarse y poder acceder a la organización. Las invitaciones pueden revocarse mientras se espera la aceptación.

Acerca de los roles de usuario

Los roles de usuario determinan el acceso que un usuario tiene a los sistemas de la organización. Las características disponibles varían en función del rol del usuario.

Admin

Los administradores tienen acceso a todo el sistema. Esto incluye la gestión de usuarios, dispositivos, licencias, vídeos y otros contenidos.

También pueden incorporar dispositivos que utilizan AXIS Camera Station Pro. Los administradores pueden gestionar la supervisión del servidor de AXIS Camera Station Pro en My Systems.

Operador

Los operadores pueden supervisar la transmisión de vídeo en directo, controlar dispositivos y acceder a grabaciones para su reproducción. Obtienen información general de los usuarios de la organización y sus respectivos roles. Los operadores también pueden gestionar la supervisión del servidor de AXIS Camera Station Pro en My Systems.

Visitante

Los visores pueden supervisar la transmisión de vídeo en directo, pero no pueden controlar dispositivos ni acceder a grabaciones. Obtienen información general de los usuarios de la organización y sus respectivos roles.

Elevar el rol del usuario

1. Seleccione la organización en la que quiera configurar los ajustes de usuario.
2. Vaya al panel My Systems (Mis sistemas).
3. En **ORGANIZATION (ORGANIZACIÓN)**, vaya a **Users (Usuarios)**.
4. Haga clic en el usuario que desea elevar y haga clic en **Roles and access (Roles y acceso)**.
5. Siga las instrucciones en pantalla en el asistente de configuración.

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 al panel My Systems (Mis sistemas).
3. En **ORGANIZATION (ORGANIZACIÓN)**, vaya a **Users (Usuarios)**.
4. Desplace el puntero del ratón sobre el usuario que desee eliminar para que aparezca otro menú de opciones: **...**
5. Haga clic en **...** y seleccione **Remove user (Eliminar usuario)** en el menú desplegable.

Eliminar varios usuarios

1. Seleccione los usuarios que quiera eliminar.
2. Haz clic en la papelera del menú de acciones.
3. Haga clic en **Remove (Eliminar)**.

Gestión de AXIS OS

La aplicación de escritorio Axis Device Management permite gestionar el sistema operativo de varios dispositivos de cada organización.

Para obtener una lista de las actualizaciones del sistema operativo AXIS que están disponibles para cada dispositivo de su organización agrupadas por modelo, vaya a **Home > AXIS OS inventory (Inicio > Inventario de AXIS OS)**. Para obtener una lista de las actualizaciones de AXIS OS disponibles en un host en el extremo concreto, seleccione el host y vaya a **AXIS OS inventory (Inventario de AXIS OS)**.

Gestionar las versiones de AXIS OS en función del modelo

Para gestionar AXIS OS por modelo en toda su organización:

1. Vaya a **Home > AXIS OS versions (Inicio > Versiones de AXIS SO)**.
2. Haga clic en el enlace de la versión recomendada de AXIS OS. Se abrirán las opciones de actualización de AXIS OS.
3. Haga clic en el menú desplegable **Upgrade to (Actualizar a)** para ver las opciones disponibles. Se preseleccionará la última versión de AXIS OS.
4. Haga clic en **Upgrade (Actualizar)**.

Gestionar AXIS OS en un host local.

Para gestionar AXIS OS en algunos o todos los dispositivos agregados a un host local:

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 **AXIS OS** en el menú de acciones.
6. Marque todos o solo algunos de los modelos de la lista.
7. Si desea cambiar la versión de AXIS OS, haga clic en la versión sugerida para ver qué está disponible para cada dispositivo. Se preseleccionará la última versión de AXIS OS.
8. Haga clic en **Actualizar**.

Ver las actualizaciones de AXIS OS en curso y finalizadas

Para ver las actualizaciones de software en curso de dispositivos conectados a un host en el extremo concreto:

1. Haga clic en **Edge hosts (Hosts en el extremo)**.
2. Haga clic en el host en el extremo al que desee acceder.
3. Vaya a **Log (Registro)**

Para ver las actualizaciones de software en curso:

4. Vaya a **Log > Ongoing tasks (Registro > Tareas en curso)**.

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 su política
7. Seleccione las aplicaciones que desee instalar y actualizar en sus dispositivos.
8. Seleccione el plazo de actualización en el menú desplegable.
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 **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.

Gestionar licencias

Obtener una licencia del producto

Para obtener una licencia de su producto, vaya a *My Systems > Licenses (Licencias)*. Para obtener más información sobre las licencias de los productos y servicios de Axis, consulte el *manual del usuario de My Systems*.

Localización de problemas

Cómo configurar los ajustes de cortafuegos

La aplicación de escritorio Axis Device Management requiere acceso al dominio axis.com y subdominios.

Para que el host en el extremo (edge) se comunique con los servicios Axis, incorpore las siguientes direcciones IP y puertos a la lista de permitidos del firewall de la organización:

- 40.127.155.231 (UE), puerto 443
- 52.224.128.152 y 40.127.155.231 (EE. UU.), puerto 443
- 75.2.119.140, puertos 443 y 8443
- 99.83.133.42, puertos 443 y 8443

Pueden usarse como alternativa los siguientes dominios (resueltos a las direcciones IP anteriores):

- prod.adm.connect.axis.com, puerto 443
- cep.connect.axis.com, puertos 443 y 8443

También debe permitir el tráfico DNS para la IP de su servidor DNS y el puerto predeterminado 53

Nota

Para obtener más información sobre la configuración de puertos, consulte el documento técnico de AXIS Device Manager Extend: *Configuraciones típicas del sistema*.

T10153497_es

2026-04 (M23.2)

© 2020 – 2026 Axis Communications AB