

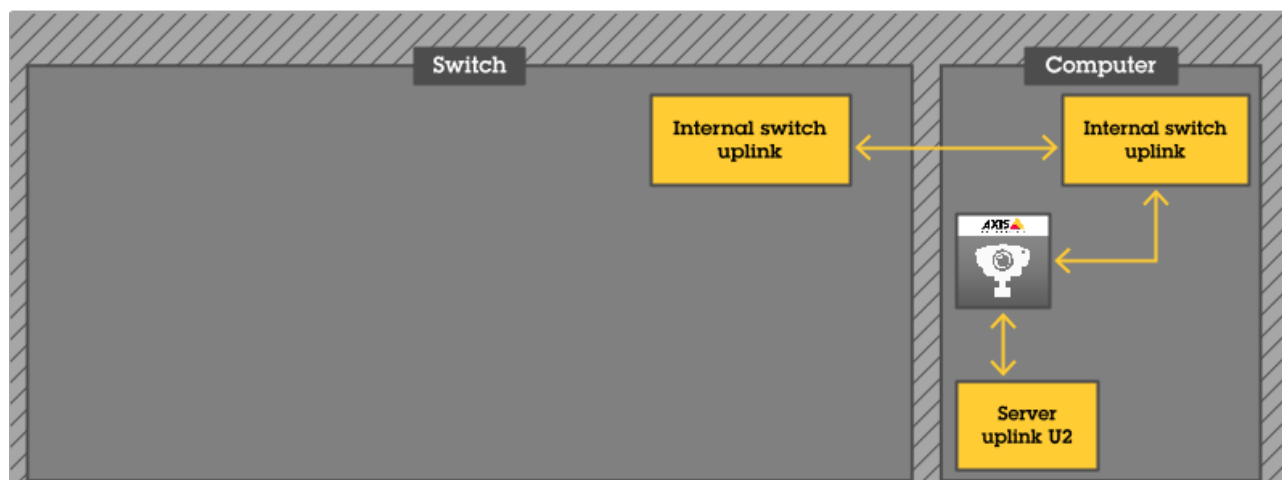
AXIS Camera Station S2108 Appliance

Sobre su dispositivo

El equipo AXIS Camera Station S2108 Appliance es una solución de grabación todo en uno con switch PoE integrado, diseñado para ofrecer una videovigilancia fiable de alta definición y compatible con cámaras con una resolución de hasta 4K. Para una instalación rápida y sencilla, el dispositivo está preconfigurado y precargado con el software de gestión de vídeo AXIS Camera Station, incluidas las licencias y todo el software de sistema necesario. AXIS Camera Station ofrece una interfaz de usuario intuitiva que permite a los usuarios aprovechar al máximo la amplia gama de cámaras de videovigilancia y otros productos IP de Axis. Con el sistema operativo almacenado en una unidad de estado sólido (SSD) y una garantía de hardware de 5 años, el dispositivo proporciona una solución de vigilancia fiable.

Un dispositivo AXIS Camera Station S2108 Appliance consta de dos partes:

- **Switch:** Switch de alimentación a través de Ethernet (PoE) incorporado.
- **Equipo:** Precargado con todo el software necesario, debe crear una solución de vigilancia que incluya el software de gestión de vídeo AXIS Camera Station.

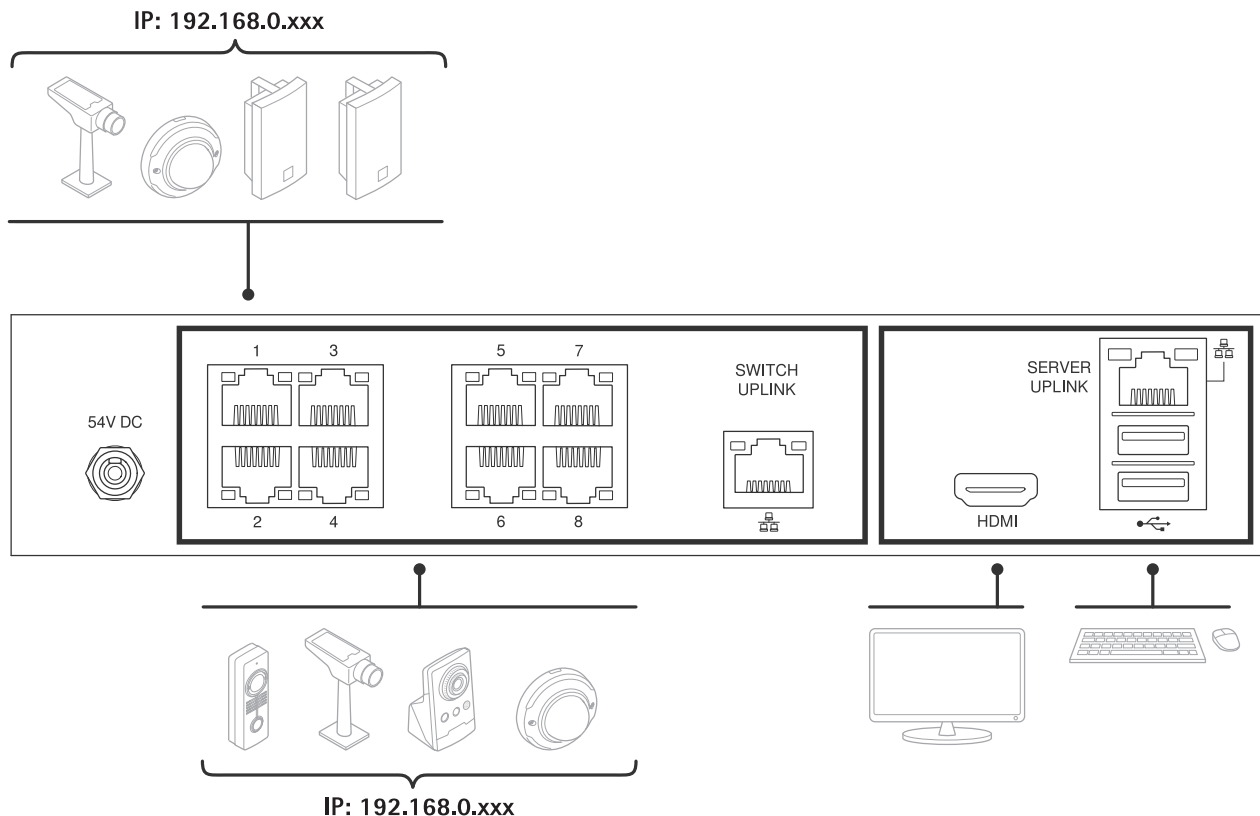


- El switch y el ordenador son dos partes separadas.
- El switch y el ordenador se comunican a través de los conectores internos de enlace ascendente: uno se encuentra en la placa de circuitos impresos de alimentación del switch y el otro en la placa base del ordenador.
- El enlace ascendente del servidor es una interfaz de red externa que se puede conectar a una red existente.
- Los dispositivos conectados al enlace ascendente del servidor no pueden comunicarse con los dispositivos conectados al switch directamente.
- Los dispositivos conectados al enlace ascendente del servidor pueden comunicarse con los dispositivos conectados al switch a través de AXIS Camera Station.

Ejemplos de configuración

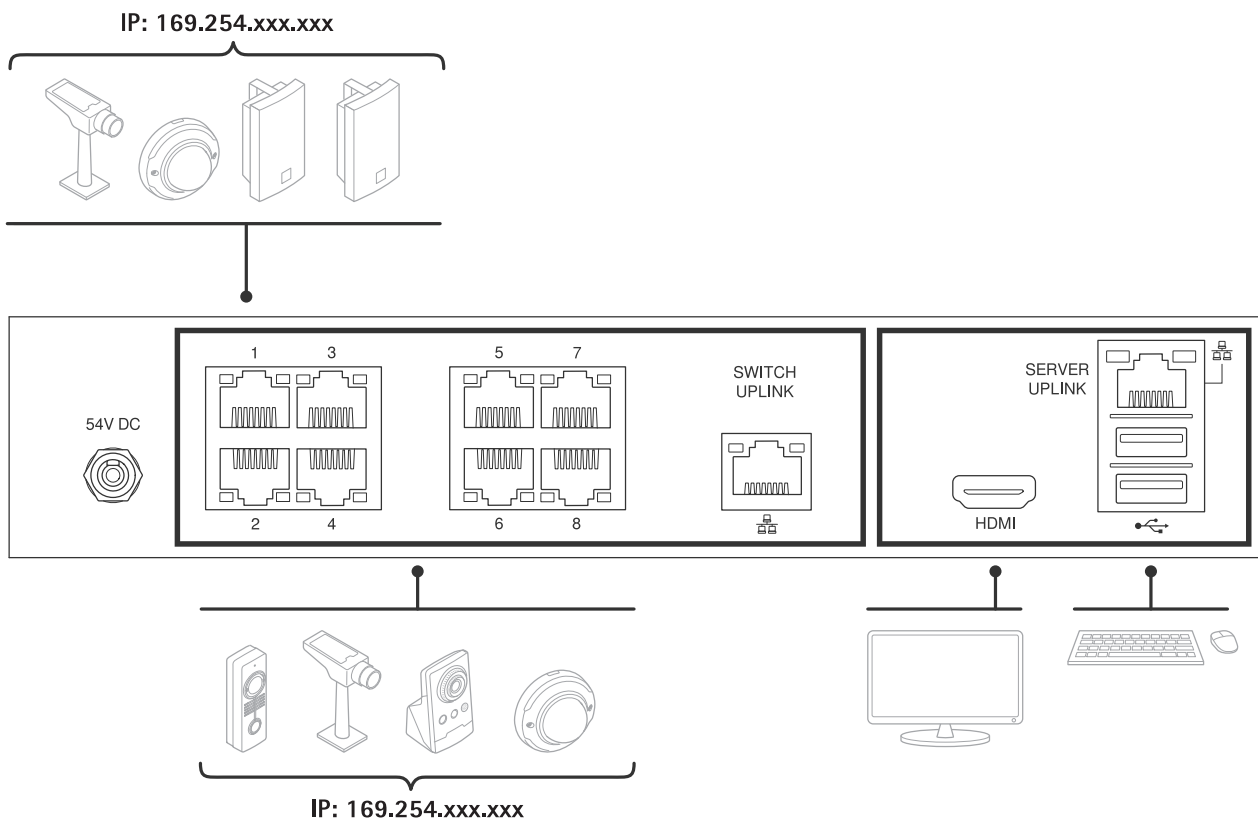
Asignar una dirección estática a cada dispositivo

Puede crear una red independiente asignando una dirección IP estática a cada dispositivo y al dispositivo AXIS S2108 Appliance. La red no tendrá interconectividad con otra red externa salvo que los parámetros de las dos redes sean iguales. De todas formas, el ordenador puede conectarse a Internet a través del puerto de enlace ascendente del servidor. Cuando los dispositivos se conecten a los puertos PoE con alimentación, tomarán la dirección de enlace local y necesitarán un conjunto de IP fija que coincida con la del dispositivo AXIS S2108 Appliance.



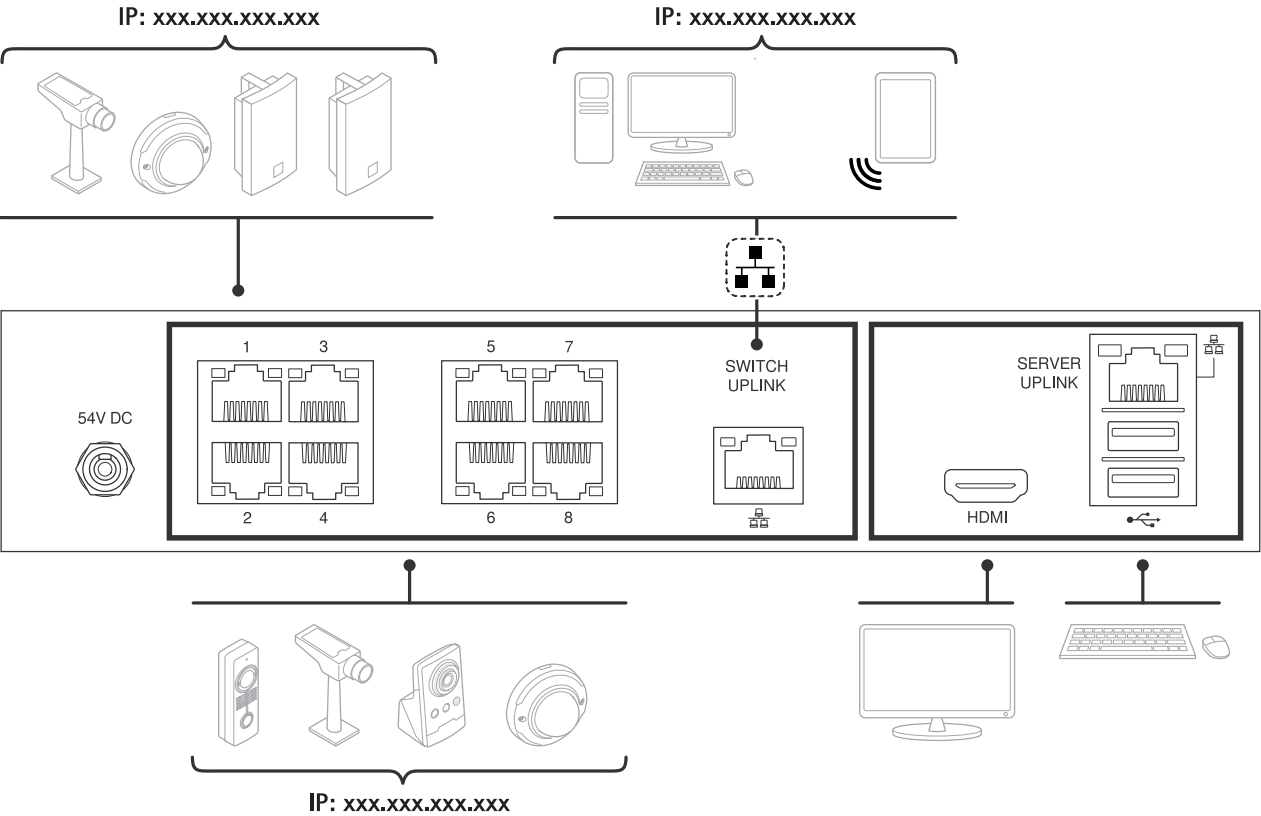
Utilizar la dirección local

Puede crear una red independiente utilizando la dirección de enlace local en cada dispositivo y el dispositivo AXIS S2108 Appliance. La red no tendrá interconectividad con otra red externa. De todas formas, el ordenador puede conectarse a Internet a través del puerto de enlace ascendente del servidor. Cuando los dispositivos se conecten a los puertos PoE con alimentación, tomarán la dirección de enlace local y AXIS Camera Station podrá localizarlos en el dispositivo AXIS S2108 Appliance.



Utilizar un servidor DHCP de otra red

El dispositivo AXIS S2108 Appliance y los dispositivos conectados pueden unirse si hay una red y un servidor DHCP conectados al enlace ascendente del switch. De esta forma, todos los dispositivos conectados tendrán una dirección IP del rango del servidor DHCP. Si hay conectividad a Internet disponible en esa red, también estará disponible para el dispositivo AXIS S2108 Appliance. De lo contrario, el ordenador puede conectarse a Internet de forma independiente a través del puerto de enlace ascendente del servidor. Cuando los dispositivos se conecten a los puertos PoE con alimentación, tomarán la dirección DHCP si el servidor DHCP está activo.



Cómo funciona

El flujo de trabajo estándar para configurar un servidor de grabación de AXIS Camera Station es:

1. *Instalar su dispositivo*
2. Configuración inicial de Windows®: Después de instalar el dispositivo, se le guiará mediante unos pasos para configurar la región, el idioma, la disposición del teclado, una cuenta de administrador y su contraseña.
3. Configuración inicial del grabador de Axis: Una vez abierta la configuración inicial de Windows, se abre AXIS Recorder Toolbox que le guiará a través de algunos pasos para configurar los ajustes básicos y necesarios, por ejemplo, el nombre del ordenador, la fecha y la hora y la red. Vea *Configuración inicial del grabador de Axis, on page 15*.
4. Configure Windows®. Se recomienda que haga lo siguiente:
 - Actualizar Windows® a la última versión. Vea .
 - Crear una cuenta de usuario estándar. Vea *Crear una cuenta de usuario, on page 21*.
5. Actualice AXIS Camera Station a la última versión.
 - Si su sistema está en línea: abra la aplicación AXIS Recorder Toolbox y haga clic en **Update AXIS Camera Station (Actualizar AXIS Camera Station)**.
 - Si su sistema no está conectado: vaya a *axis.com* y descargue la versión más reciente.
6. Inicie el cliente de AXIS Camera Station.
7. *Conectar con el servidor de AXIS Camera Station*
8. *Configurar AXIS Camera Station, on page 16*

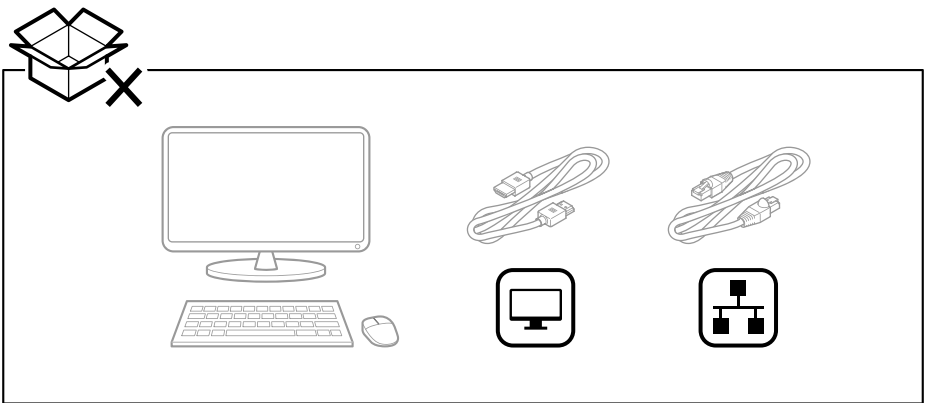
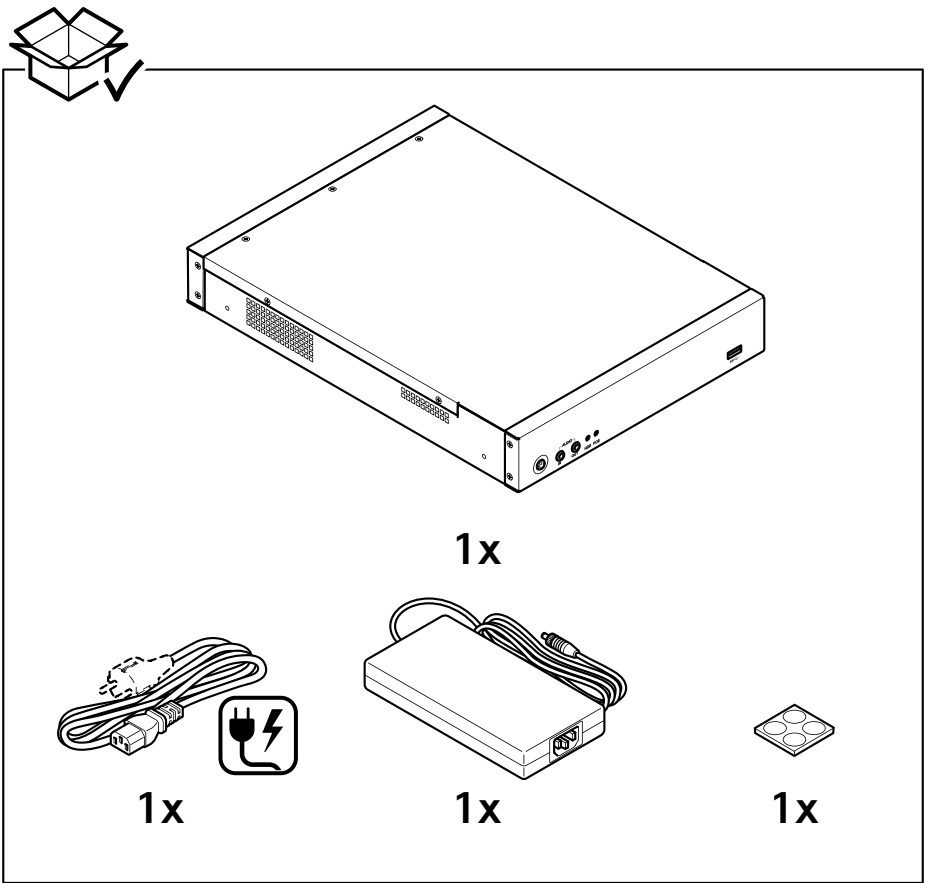
Instalar su dispositivo

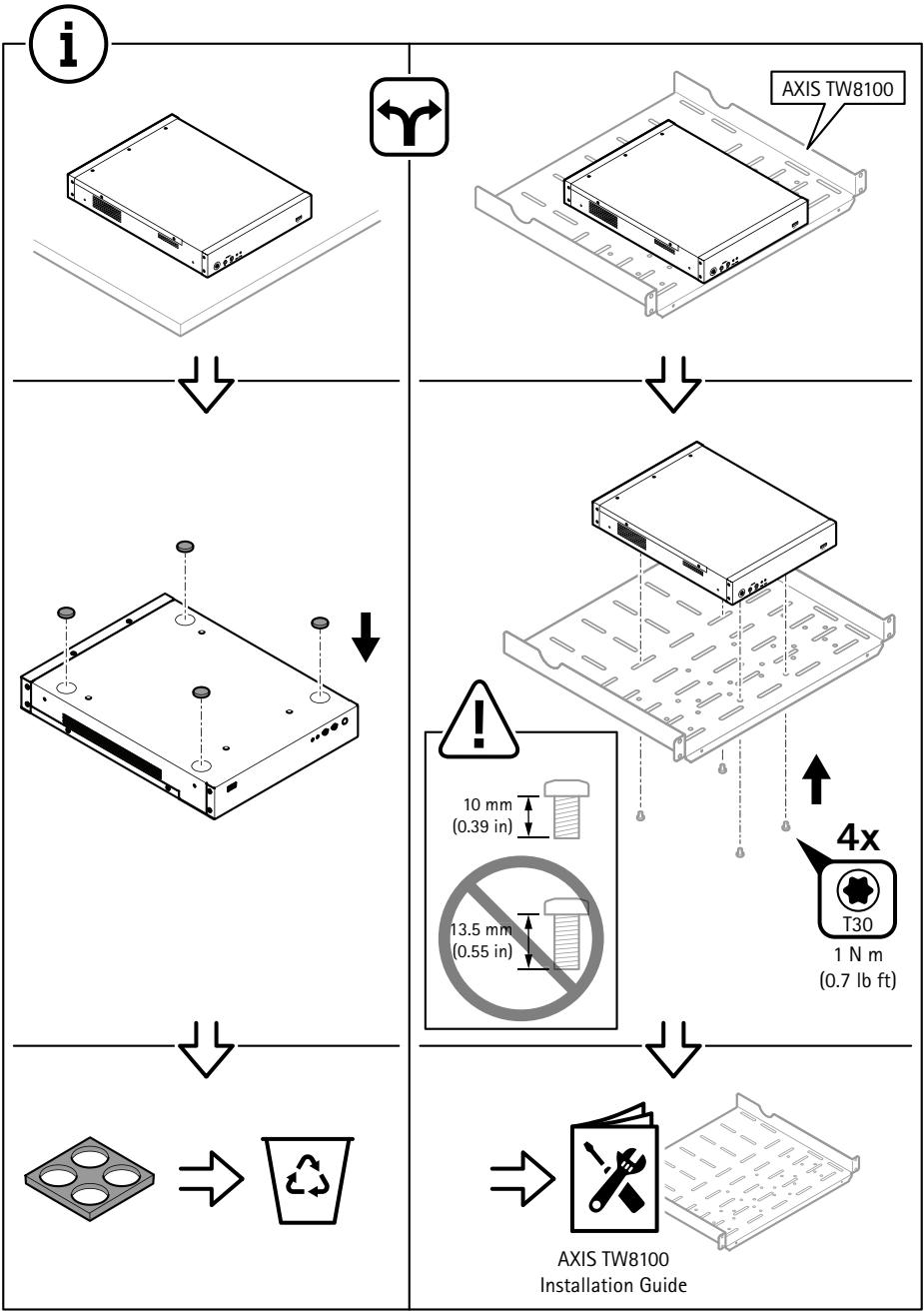
Antes de la instalación

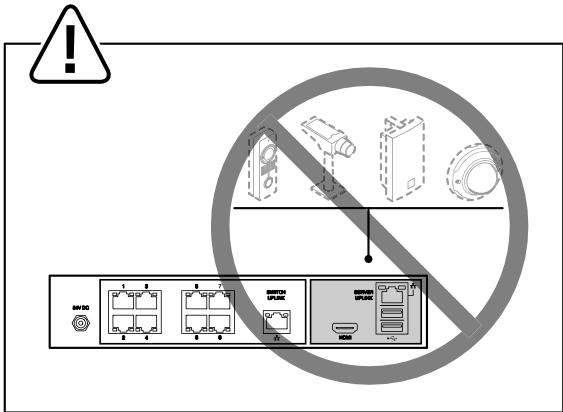
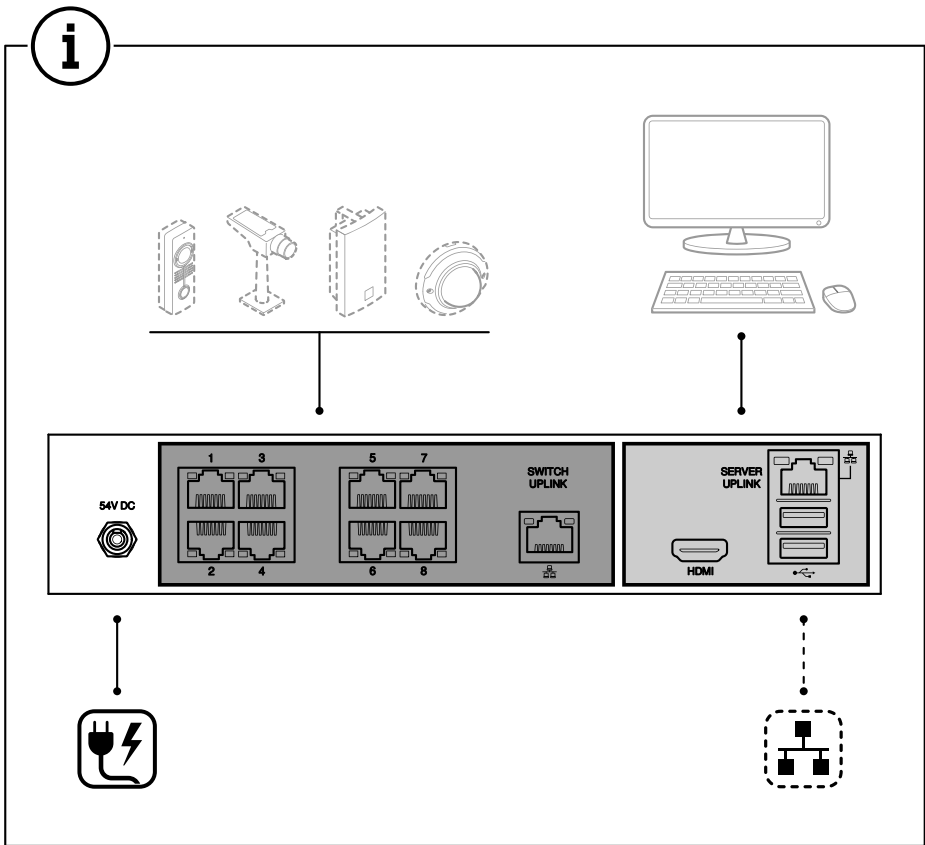
- Prepare los accesorios adicionales que utilizará para la instalación: monitor, ratón, teclado y cable de red.
- Comprenda el uso de diferentes cuentas de usuario.

En la siguiente tabla se muestran las cuentas de usuario que se pueden utilizar para la instalación, configuración y funcionamiento del sistema Axis.

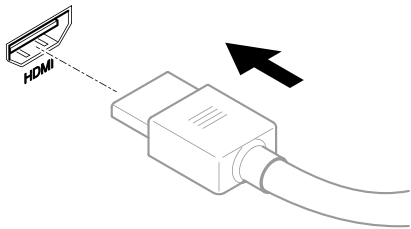
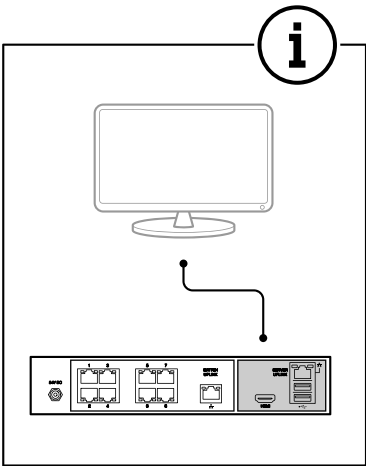
Cuenta de usuario	Descripción	Nota
MyAxis	Se utiliza para descargar el software más reciente, acceder al sistema de licencias, Axis Secure Remote Access y System Health Monitoring.	Registrado desde <i>my.axis.com</i> .
Windows®		
Administrador de Windows®	Privilegios de administrador en Windows®. Recomendamos no usarlos como administrador de AXIS Camera Station.	Se ha creado durante la configuración inicial de Windows®.
Usuario de Windows® con privilegios de administrador de AXIS Camera Station	De la configuración o solución de problemas se debe encargar un usuario de Windows® con privilegios de administrador concedidos en AXIS Camera Station por un integrador o administrador del sistema.	Se ha creado en la configuración de Windows®.
Usuario de Windows® con privilegios de operador u observador en AXIS Camera Station	Un usuario de Windows® con privilegios de operador u observador en AXIS Camera Station.	Se ha creado en la configuración de Windows®.
Dispositivo		
Administrador de dispositivos	Utilizado por el administrador para acceder a la cámara desde el sistema de gestión de vídeo o la página web del dispositivo.	Se crea a partir de la página web del dispositivo o al agregar el dispositivo a AXIS Camera Station.



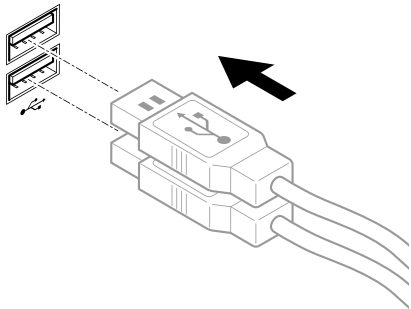
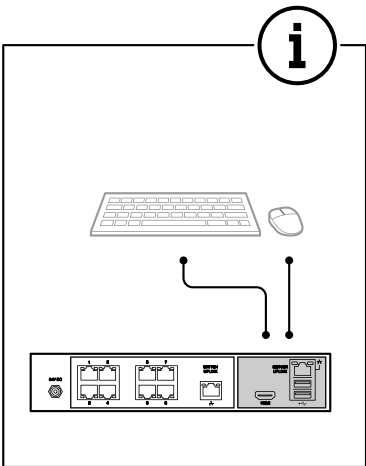




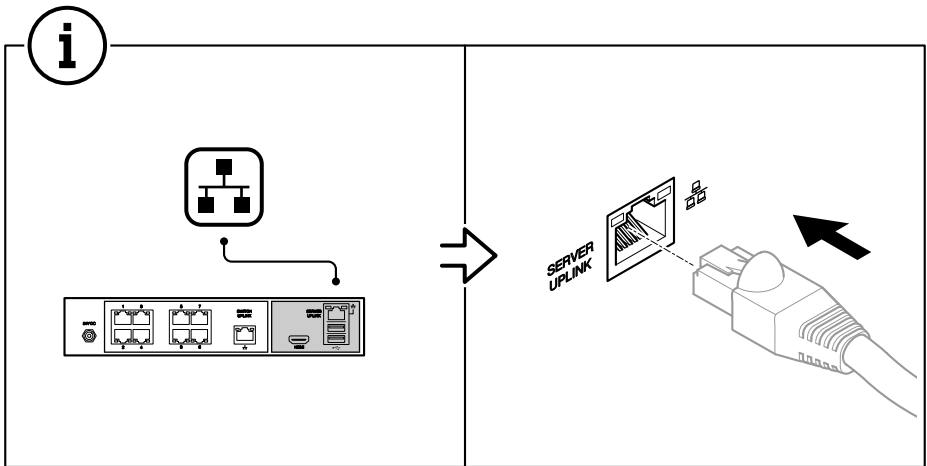
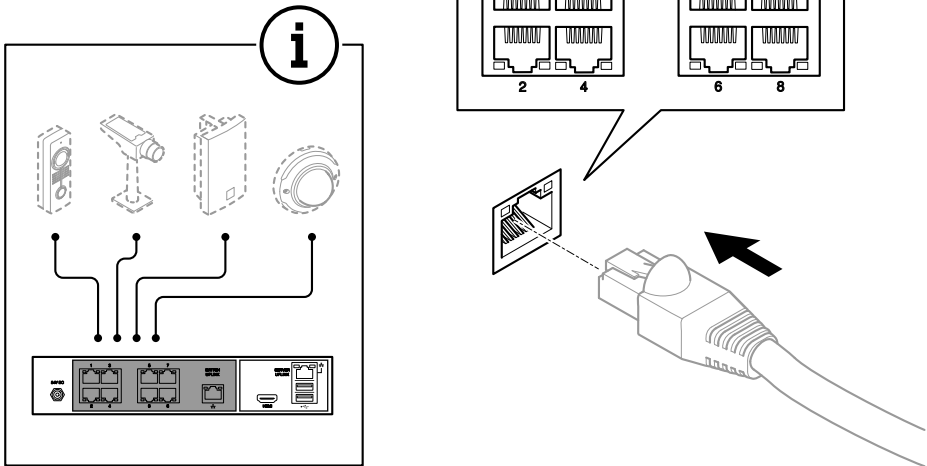
1.1



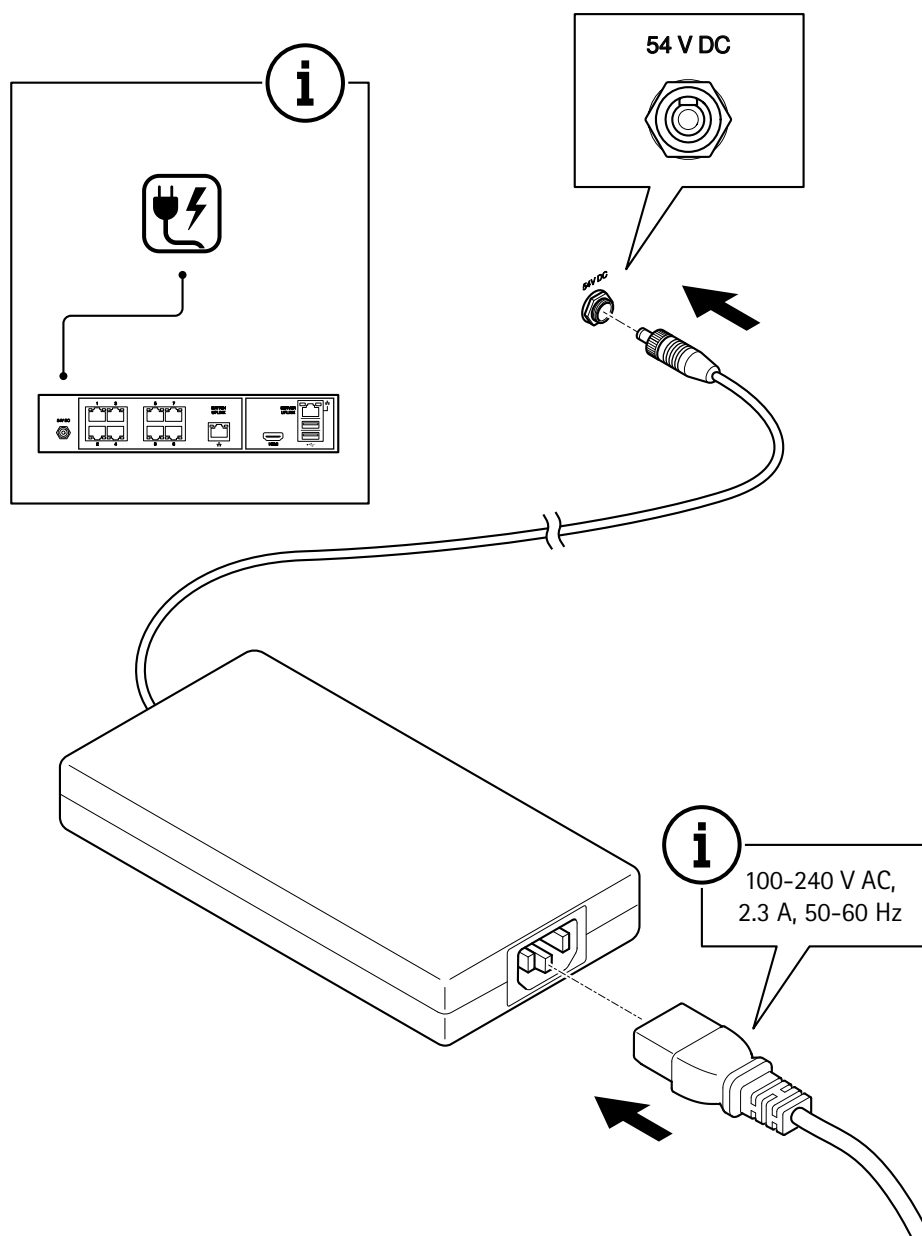
1.2



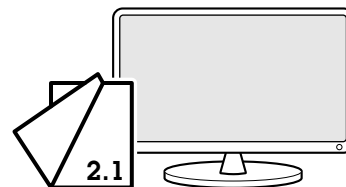
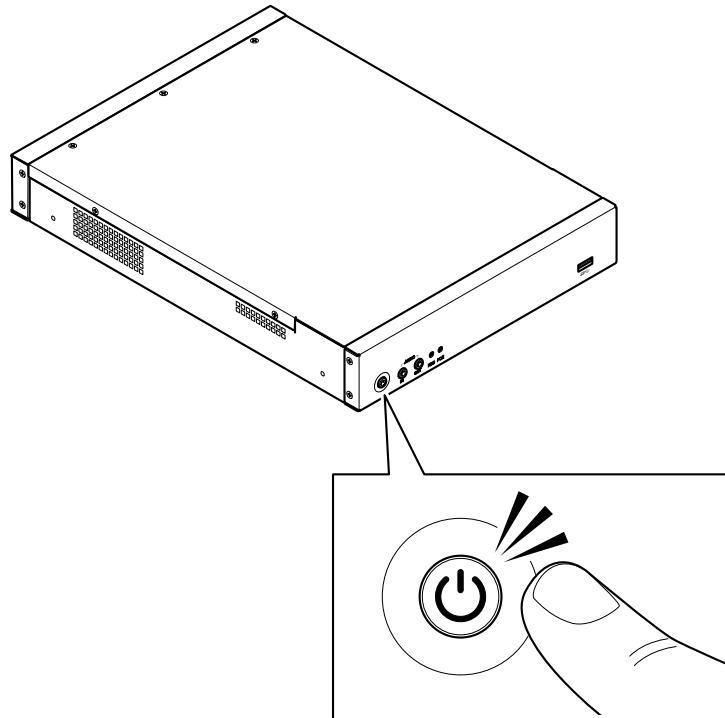
1.3



1.4



1.5



Configure su dispositivo

Configuración inicial del grabador de Axis

Una vez que haya configurado Windows®, AXIS Recorder Toolbox se abre automáticamente y lo guía con el asistente de primera configuración. En este asistente, puede configurar varios ajustes básicos y necesarios antes de gestionar su dispositivo en AXIS Recorder Toolbox.

1. Seleccione un tema **Light (Claro)** o **Dark (Oscuro)** y haga clic en **Next (Siguiente)** (si está disponible para el producto).
2. Cambie el nombre del equipo si lo desea y haga clic en **Next (Siguiente)**.
3. En **Date and time (Fecha y hora)**, configure los siguientes ajustes y haga clic en **Next (Siguiente)**.
 - Seleccionar una zona horaria.
 - Para configurar un servidor NTP, seleccione **NTP server (Servidor NTP)** e introduzca la dirección del servidor NTP.
 - Para configurarlo manualmente, seleccione **Manual** y una fecha y una hora.
4. En **Network settings (Ajustes de red)**, configure los siguientes ajustes y haga clic en **Next (Siguiente)**.
 - «**Use automatic IP settings (DHCP) (Usar la configuración IP automática —DHCP—)**» y «**Use automatic DNS settings (Usar la configuración de DNS automática)**» se activan de forma predeterminada.
 - Si el dispositivo está conectado a una red con un servidor DHCP, se mostrarán automáticamente la dirección IP, la máscara de subred, la puerta de enlace y el DNS preferido asignados.
 - Si su dispositivo no está conectado a una red o no hay ningún servidor DHCP disponible, introduzca manualmente la dirección IP, la máscara de subred, la puerta de enlace y el DNS preferido en función de los requisitos de la red.
5. Haga clic en **Finish (Finalizar)**. Si ha cambiado el nombre del equipo, AXIS Recorder Toolbox le pedirá que reinicie el dispositivo.

Iniciar sesión en el servidor

Con el cliente de AXIS Camera Station, puede conectar con varios servidores o con un único servidor instalado en el equipo local o en otra parte de la red. Se puede conectar a los servidores de AXIS Camera Station de diferentes maneras:

Últimos servidores usados – Conéctese a los servidores usados en la sesión anterior.

Este equipo – Conéctese al servidor instalado en el mismo equipo que el cliente.

Servidor remoto – Vea *Conectar a un servidor remoto, on page 16*.

AXIS Secure Remote Access – Vea *Iniciar sesión en AXIS Secure Remote Access, on page 16*.

Nota

Al intentar conectarse a un servidor por primera vez, el cliente comprueba el ID del certificado del servidor. Para asegurarse de que se está conectando al servidor correcto, coteje manualmente el ID del certificado con el que se muestra en AXIS Camera Station Service Control.

Lista de servidores	Para conectarse a servidores de una lista de servidores, seleccione uno del menú desplegable de la Lista de servidores . Haga clic en  para crear o editar las listas de servidores.
Importar la lista de servidores	Para importar un archivo de lista de servidores exportado desde AXIS Camera Station, haga clic en Import server list (Importar lista de servidores) y examine hasta un archivo .msl.

Eliminar contraseñas guardadas	Para eliminar los nombres de usuario y las contraseñas guardados de todos los servidores conectados, haga clic en Delete saved passwords (Eliminar contraseñas guardadas) .
Modificar la configuración proxy del cliente	Es posible que tenga que cambiar los ajustes del proxy del cliente para conectarse a un servidor, haga clic en Change client proxy settings (Cambiar ajustes del proxy del cliente) .

Conectar a un servidor remoto

1. Seleccione **Servidor remoto**.
2. Seleccione un servidor de la lista desplegable **Remote server (Servidor remoto)** o introduzca la dirección IP o DNS. Si el servidor no aparece en la lista, haga clic en  para actualizar la lista de todos los servidores remotos disponibles. Si el servidor está configurado para aceptar clientes en un puerto diferente del número de puerto predeterminado 55754, introduzca la dirección IP seguida del número de puerto, por ejemplo, 192.168.0.5:46001.
3. Realice una de las acciones siguientes:
 - Seleccione **Log in as current user (Iniciar sesión como usuario actual)** para iniciar sesión como el usuario actual de Windows®.
 - Desmarque **Log in as current user (Iniciar sesión como usuario actual)** y haga clic en **Log in (Iniciar sesión)**. Seleccione **Other user (Otro usuario)** y facilite otro nombre de usuario y contraseña para iniciar sesión con credenciales diferentes.

Iniciar sesión en AXIS Secure Remote Access

Importante

Para mejorar la seguridad y la funcionalidad, estamos actualizando **Axis Secure Remote Access (v1)** a **Axis Secure Remote Access v2**. Suspendemos la versión actual el 1 de diciembre de 2025, por lo que le recomendamos firmemente actualizar a **Axis Secure Remote Access v2** antes de esa fecha.

¿Qué supone esto para su sistema **AXIS Camera Station S2108 Appliance**?

- Después del 1 de diciembre de 2025, ya no podrá acceder de forma remota a su sistema utilizando **Axis Secure Remote Access (v1)**.
- Para utilizar **Axis Secure Remote Access v2**, debe actualizar a la versión 6.8 de **AXIS Camera Station Pro**. Esta actualización es actualmente gratuita para todos los usuarios de **AXIS Camera Station 5** hasta el 1 de marzo de 2026.

Nota

- Al intentar conectarse a un servidor mediante **Axis Secure Remote Access**, el servidor no puede actualizar el cliente automáticamente.
 - Si el servidor proxy se encuentra entre el dispositivo de red y el servidor de **AXIS Camera Station S2108 Appliance**, debe configurar los ajustes de proxy en Windows en el servidor de **AXIS Camera Station S2108 Appliance** para acceder al servidor mediante **AXIS Secure Remote Access**.
1. Haga clic en el enlace **Iniciar sesión en AXIS Secure Remote Access**.
 2. Introduzca las credenciales de la cuenta de My Axis.
 3. Haga **Sign in (Iniciar sesión)**.
 4. Haga clic en **Grant (Autorizar)**.

Configurar AXIS Camera Station

Este tutorial le guía por los pasos básicos necesarios para que su sistema esté listo y en funcionamiento.

Antes de empezar:

- Configurar la red en función de la instalación. Vea *Configuración de red*, on page 18.
- Si es necesario, configure los puertos del servidor. Vea *Configuración del puerto del servidor*, on page 19.
- Tenga en cuenta los aspectos de seguridad. Vea *Consideraciones de seguridad*.

Una vez realizada la configuración necesaria, ya puede empezar a trabajar con AXIS Camera Station:

1. *Inicie el sistema de gestión de vídeo*, on page 17
2. *Agregar dispositivos*, on page 17
3. *Configurar el método de grabación*, on page 17
4. *Ver vídeo en directo*, on page 17
5. *Visualización de grabaciones*, on page 17
6. *Agregar marcadores*, on page 18
7. *Exportar grabaciones*, on page 18
8. *Reproducir y verificar las grabaciones en AXIS File Player*, on page 18

Inicie el sistema de gestión de vídeo

Haga doble clic en el icono de cliente de AXIS Camera Station para iniciar el cliente. Al iniciar al cliente por primera vez, intentará iniciar sesión en el servidor de AXIS Camera Station instalado en el mismo equipo que el cliente.

Puede conectar varios servidores de AXIS Camera Station de diferentes maneras.

Agregar dispositivos

La página *Add devices* (Agregar dispositivos) se abre la primera vez que inicia AXIS Camera Station. AXIS Camera Station busca dispositivos conectados en la red y muestra una lista de los dispositivos encontrados.

1. Seleccione las cámaras que desea agregar de la lista. Si no puede encontrar la cámara, haga clic en **Manual search (Búsqueda manual)**.
2. Haga clic en **Añadir**.
3. Seleccione **Configuración rápida** o **Configuración del Espacio de diseño**. Haga clic en **Next (Siguiente)**.
4. Utilice los ajustes predeterminados y asegúrese de que el método de grabación está establecido en **None (Ninguno)**. Haga clic en **Instalar**.

Configurar el método de grabación

1. Vaya a **Configuración > Grabaciones y eventos > Método de grabación**.
2. Seleccione una cámara.
3. Active **Motion detection (Detección de movimiento)** o **Continuous (Continuo)** o ambos.
4. Haga clic en **Aplicar**.

Ver vídeo en directo

1. Abra una pestaña **Live view (Visualización en directo)**.
2. Seleccione una cámara para ver el vídeo en directo.

Visualización de grabaciones

1. Abra una pestaña **Recordings (Grabaciones)**.
2. Seleccione la cámara desde la que desea ver las grabaciones.

Agregar marcadores

1. Ir a grabación.
2. En la línea temporal, amplíe o reduzca la vista de la línea temporal y coloque el marcador en la posición deseada.
3. Haga clic en .
4. Introduzca un nombre y una descripción para el marcador. Utilice palabras clave para facilitar la búsqueda del marcador.
5. Seleccione **Impedir eliminar grabación** para bloquear la grabación.

Nota

Para desbloquear la grabación, desactive la opción **Prevent recording deletion (Impedir eliminar la grabación)** o elimine el marcador.

6. Haga clic en **OK (Aceptar)** para guardar el marcador.

Exportar grabaciones

1. Abra una pestaña **Recordings (Grabaciones)**.
2. Seleccione la cámara desde la que desea exportar grabaciones.
3. Haga clic en  para mostrar los marcadores de selección.
4. Arrastre los marcadores para incluir las grabaciones que desea exportar.
5. Haga clic en  para abrir la pestaña **Export (Exportar)**.
6. Haga clic en **Export... (Exportar...)**

Reproducir y verificar las grabaciones en AXIS File Player

1. Vaya a la carpeta con las grabaciones exportadas.
2. Haga doble clic en la aplicación **AXIS File Player**.
3. Haga clic en  para mostrar las notas de la grabación.
4. Para verificar la firma digital:
 - 4.1. Vaya a **Herramientas > Verificar firma digital**.
 - 4.2. Seleccione **Validate with password (Validar con contraseña)** e introduzca la contraseña.
 - 4.3. Haga clic en **Verify (Verificar)** para consultar los resultados de la verificación.

Nota

- Una firma digital no es lo mismo que un vídeo firmado. El vídeo firmado permite rastrear una grabación hasta la cámara de la que procede, para poder verificar que no ha sido manipulada. Consulte *Vídeo firmado* y el manual de usuario de la cámara para obtener más información.
- Si los archivos guardados no tienen ninguna conexión con una base de datos de **AXIS Camera Station** (archivos no indexados), será preciso convertirlos para poder reproducirlos en **AXIS File Player**. Contacte con el equipo de asistencia técnica de Axis si necesita ayuda para convertir sus archivos.

Configuración de red

Configure los ajustes del proxy o del cortafuegos antes de utilizar **AXIS Camera Station** si el cliente de **AXIS Camera Station**, el servidor de **AXIS Camera Station** y los dispositivos de red conectados están instalados en redes diferentes.

Configuración proxy del cliente

Cuando un servidor proxy separa el cliente y el servidor, configure los ajustes del proxy del cliente.

1. Abra el cliente de AXIS Camera Station.
2. Haga clic en **Change client proxy settings (Cambiar configuración proxy del cliente)**.
3. Cambie los ajustes proxy del cliente.
4. Haga clic en **OK**.

Ajustes de proxy del servidor

Cuando un servidor proxy separa los dispositivos de red y el servidor, configure los ajustes del proxy del servidor.

1. Abra el control del servicio de AXIS Camera Station.
2. Seleccione **Modificar ajustes**.
3. En la sección de configuración de Proxy, utilice el valor predeterminado **System account internet option (Opción de internet de cuenta del sistema)** o bien seleccione **Use manual proxy settings (Utilizar configuración manual de proxy)**.
4. Haga clic en **Save (Guardar)**.

NAT y Firewall

Cuando un NAT, cortafuegos o similar separa el cliente y el servidor, configure el NAT o cortafuegos para asegurarse de que el HTTP port (Puerto HTTP), el puerto TCP y el puerto de transmisión especificados en el Control de servicio de AXIS Camera Station puedan cruzar el cortafuegos o el NAT. Póngase en contacto con el administrador de la red para obtener instrucciones sobre cómo configurar el NAT o el cortafuegos.

Configuración del puerto del servidor

El servidor de AXIS Camera Station usa los puertos 55752 (HTTP), 55754 (TCP), 55756 (comunicación móvil) y 55757 (transmisión móvil) para la comunicación entre el servidor y el cliente. Puede cambiar los puertos en Control del Servicio de AXIS Camera Station, si es necesario.

Consideraciones de seguridad

Para evitar el acceso no autorizado a las cámaras y grabaciones:

- Utilice contraseñas seguras para todos los dispositivos de red (cámaras, codificadores de vídeo y dispositivos auxiliares).
- Instale el servidor de AXIS Camera Station S2108 Appliance, las cámaras, los codificadores de vídeo y los dispositivos auxiliares en una red segura independiente de la red de trabajo. Puede instalar el cliente de AXIS Camera Station S2108 Appliance en un equipo de otra red, por ejemplo, una red con acceso a Internet.
- Asegúrese de que todos los usuarios tienen contraseñas seguras.

Autorizar un sistema en línea

Tanto el cliente de AXIS Camera Station como el servidor deben tener conexión a Internet.

1. Vaya a **Configuración > Licencias > Gestión**.
2. Asegúrese de que la opción **Manage licenses online (Gestionar licencias en línea)** está activada.
3. Inicie sesión en su cuenta MyAxis.
4. La clave de licencia se genera automáticamente y aparece en **License keys (Claves de licencia)**.
5. Si ha adquirido claves de licencia de forma independiente, introduzca la clave de licencia en **Add license key (Agregar clave de licencia)**.
6. Haga clic en **Añadir**.
7. En el cliente de AXIS Camera Station, compruebe que las claves de licencia aparecen en **Configuration > Licenses > Keys (Configuración > Licencias > Claves)**.

Autorizar un sistema fuera de línea

1. Vaya a Configuración > Licencias > Gestión.
2. Desactive Manage licenses online (Gestionar licencias en línea).
3. Haga clic en Exportar archivo de sistema.
4. Guarde el archivo de sistema en una unidad flash USB.
5. Inicie sesión en su cuenta MyAxis.
6. Haga clic en Upload system file (Cargar archivo de sistema) para cargar el archivo de sistema guardado en la unidad flash USB.
7. La clave de licencia se genera automáticamente y se muestra en License keys (Claves de licencia).
8. Si ha adquirido claves de licencia de forma independiente, introduzca la clave de licencia en Add license key (Agregar clave de licencia).
9. Haga clic en Añadir.
10. En License keys (Claves de licencia), haga clic en Download license file (Descargar archivo de licencia) y guarde el archivo en una unidad flash USB.
11. En el cliente de AXIS Camera Station, vaya a Configuration > Licenses > Management (Configuración > Licencias > Gestión).
12. Haga clic en Import license file (Importar archivo de licencia) y seleccione el archivo de licencia en su unidad flash USB.
13. Compruebe que las claves de licencia aparecen en Configuration > Licenses > Keys (Configuración > Licencias > Claves).

Gestionar cuentas de usuario locales de Windows®

Crear una cuenta de usuario

Para ayudar a mantener sus datos personales e información más segura, le recomendamos que añada una contraseña para cada cuenta local.

Importante

Una vez que cree una contraseña para una cuenta local, no la olvide. No hay forma de recuperar una contraseña perdida para las cuentas locales.

1. Vaya a **Settings > Accounts > Other people > Add someone else to this PC** (Configuración > Cuentas > Otros usuarios > Agregar otra persona a este equipo).
2. Haga clic en **I don't have this person's sign-in information** (No tengo los datos de inicio de sesión de esta persona).
3. Haga clic en **Add a user without a Microsoft account** (Agregar un usuario sin cuenta Microsoft).
4. Introduzca un nombre de usuario, contraseña y recordatorio de contraseña.
5. Haga clic en **Next (Siguiente)** y siga las instrucciones.

Crear una cuenta de administrador

1. Vaya a **Settings > Accounts > Other people** (Configuración > Cuentas > Otros usuarios).
2. Vaya a la cuenta que desea cambiar y haga clic en **Change account type** (Cambiar tipo de cuenta).
3. Vaya a **Account type (Tipo de cuenta)** y seleccione **Administrator (Administrador)**.
4. Haga clic en **OK**.
5. Reinicie el dispositivo e inicie sesión con la nueva cuenta de administrador.

Crear un grupo de usuarios local

1. Vaya a **Computer Management (Gestión del equipo)**.
2. Vaya a **Local Users and Groups > Group** (Usuarios locales y Grupos > Grupo).
3. Haga clic con el botón derecho en **Group (Grupo)** y seleccione **New Group (Nuevo Grupo)**.
4. Introduzca un nombre de grupo y una descripción.
5. Agregue a los miembros del grupo:
 - 5.1. Haga clic en **Añadir**.
 - 5.2. Haga clic en **Avanzado**.
 - 5.3. Encuentre la cuenta o cuentas de usuario que desea agregar al grupo y haga clic en **OK**.
 - 5.4. Haga clic en **OK** otra vez.
6. Haga clic en **Create (Crear)**.

Quitar una cuenta de usuario

Importante

Quando se quita una cuenta, se elimina la cuenta de usuario de la pantalla de inicio de sesión. También se eliminan todos los archivos, ajustes y datos de programa almacenados en la cuenta de usuario.

1. Vaya a **Settings > Accounts > Other people** (Configuración > Cuentas > Otros usuarios).
2. Vaya a la cuenta que desea eliminar y haga clic en **Remove (Quitar)**.

Cambiar la contraseña de una cuenta de usuario

1. Iniciar sesión con una cuenta de administrador.

2. Vaya a **User Accounts > User Accounts > Manage another account in sequence** (Cuentas de usuario > Cuentas de usuario > Gestionar otra cuenta en la secuencia). Verá una lista con todas las cuentas de usuario en el dispositivo.
3. Seleccione la cuenta de usuario cuya contraseña desea cambiar.
4. Haga clic en **Change the password** (Cambiar la contraseña).
5. Introduzca la nueva contraseña y haga clic en **Change password** (Cambiar contraseña).

Crear un disco de restablecimiento de contraseña para una cuenta de usuario

Recomendamos crear un disco de restablecimiento de contraseña en una unidad flash USB. Con esto, puede restablecer la contraseña. Sin un disco de restablecimiento de contraseña, no se puede restablecer la contraseña.

Nota

Si utiliza Windows® 10 o posterior, puede agregar preguntas de seguridad a la cuenta local en caso de que olvide la contraseña, de modo que no tenga que crear un disco para restablecer la contraseña. Para esto, vaya a **Start (Inicio)** y haga clic en **Settings > Sign-in options > Update your security questions** (Configuración > Opciones de inicio de sesión > Actualizar preguntas de seguridad).

1. Inicie sesión en su dispositivo con una cuenta de usuario local. No puede crear un disco de restablecimiento de contraseña para una cuenta conectada.
2. Conecte una unidad flash USB vacía en el dispositivo.
3. Desde el campo de búsqueda de Windows®, vaya a **Create a password reset disk** (Crear un disco de restablecimiento de contraseña).
4. En el asistente de configuración de **Contraseña olvidada**, haga clic en **Next (Siguiente)**.
5. Seleccione su unidad flash USB y haga clic en **Next (Siguiente)**.
6. Introduzca la contraseña actual y haga clic en **Next (Siguiente)**.
7. Siga las instrucciones en la pantalla.
8. Extraiga la unidad flash USB y manténgala en un lugar seguro. No tiene que crear un nuevo disco cuando cambie la contraseña, aunque la cambie varias veces.

Gestionar las cuentas de usuario de AXIS Camera Station

Permisos de usuario

Vaya a **Configuration > Security > User permissions** (Configuración > Seguridad > Permisos de usuario) para visualizar los usuarios y grupos en AXIS Camera Station S2108 Appliance.

Nota

Los administradores del equipo que ejecuta el servidor AXIS Camera Station S2108 Appliance obtienen automáticamente privilegios de administrador en AXIS Camera Station S2108 Appliance. No puede cambiar ni quitar los privilegios del grupo de administradores.

Antes de añadir un usuario o grupo, asegúrese de que esté registrado en el equipo local o que tenga una cuenta de usuario de Windows® Active Directory. Para agregar usuarios o grupos, consulte *Agregar usuarios o grupos*.

Cuando un usuario pertenece a un grupo, recibe permisos del rol de mayor nivel que se le haya asignado individualmente o al grupo. Por ejemplo, un usuario con acceso a la cámara X que también pertenece a un grupo con acceso a las cámaras Y y Z, tendrá acceso a las tres cámaras.

	Indica que la entrada es un usuario individual.
	Indica que la entrada es un grupo.
Nombre	El nombre de usuario que aparece en el equipo local o Active Directory.
Dominio	Es el dominio al que pertenece el usuario o grupo.
Función	El rol de acceso asignado al usuario o grupo. Valores posibles: Administrador, Operador y Visor.
Detalles	Información detallada sobre el usuario según aparece en el equipo local o en Active Directory.
Servidor	Es el servidor al que pertenece el usuario o grupo.

Agregar usuarios o grupos

Los usuarios y grupos de Microsoft Windows® y Active Directory pueden acceder a AXIS Camera Station S2108 Appliance. Para agregar un usuario a AXIS Camera Station S2108 Appliance, debe agregar usuarios o un grupo a Windows®.

Añadir un usuario en Windows® 10 y 11:

- Pulse la tecla de Windows + X y seleccione **Computer Management (Gestión de equipos)**.
- En la ventana **Computer Management (Gestión de equipos)**, vaya a **Local Users and Groups (Usuarios y grupos locales) > Users (Usuarios)**.
- Haga clic con el botón derecho en **Users (Usuarios)** y seleccione **New user (Nuevo usuario)**.
- En el cuadro de diálogo emergente, introduzca los datos del nuevo usuario y desactive **User must change password at next login** (El usuario debe cambiar la contraseña en el próximo inicio de sesión).
- Haga clic en **Create (Crear)**.

Si utiliza un dominio de Active Directory, consulte con su administrador de red.

Agregar usuarios o grupos

1. Vaya a **Configuration > Security > User permissions** (Configuración > Seguridad > Permisos de usuario).
2. Haga clic en **Añadir**. La lista recoge los usuarios y grupos disponibles.
3. En **Scope (Ámbito)**, seleccione dónde se deben buscar usuarios y grupos.

4. En **Show (Mostrar)**, seleccione esta opción para mostrar usuarios o grupos. Es posible que los resultados de la búsqueda no aparezcan si el número de usuarios o grupos es excesivo. Utilice el filtro para acotar los resultados.
5. Seleccione los usuarios o grupos y haga clic en **Agregar**.

Ámbito	
Servidor	Seleccione esta opción para buscar usuarios o grupos en el equipo local.
Dominio	Seleccione esta opción para buscar usuarios o grupos en Active Directory.
Servidor seleccionado	Si está conectado a varios servidores de AXIS Camera Station S2108 Appliance, seleccione uno donde buscar usuarios o grupos.

Configurar un usuario o grupo

1. Seleccione un usuario o grupo en la lista.
2. En **Role (Rol)**, seleccione **Administrator (Administrador)**, **Operator (Operador)** o **Viewer (Visor)**.
3. Si ha seleccionado **Operator (Operador)** o **Viewer (Visor)**, puede configurar los privilegios de usuario o grupo. Vea *Privilegios de usuario o grupo*.
4. Haga clic en **Save (Guardar)**.

Eliminar un usuario o grupo

1. Seleccione un usuario o un grupo.
2. Haga clic en **Remove (Eliminar)**.
3. En el diálogo emergente, haga clic en **Aceptar** para eliminar el usuario o el grupo.

Privilegios de usuario o grupo

Existen tres roles que se pueden asignar a un usuario o grupo. Para ver cómo definir el rol de un usuario o un grupo, consulte *Agregar usuarios o grupos*.

Administrador – Acceso completo a todo el sistema, incluido acceso al vídeo en directo y grabado de todas las cámaras, a todos los puertos de E/S y a todas las vistas. Este rol es necesario para acceder a la configuración del sistema.

Operador – Puede seleccionar cámaras, vistas y puertos de E/S para obtener acceso a vídeos en directo y grabados. Un operador tiene acceso completo a todas las funciones de AXIS Camera Station S2108 Appliance excepto la configuración del sistema.

Visitante – Puede acceder al vídeo en directo de cámaras, puertos de E/S y vistas seleccionados. Un visor no tiene acceso a la configuración de vídeo grabado o del sistema.

Cámaras

Los siguientes privilegios de acceso están disponibles para grupos o usuarios con el rol **Operator (Operador)** o **Viewer (Visor)**.

Acceso	permite el acceso a la cámara y a todas las características de la cámara.
Vídeo	permite al usuario acceder a vídeo en directo desde la cámara.
Escuchar audio	Permite el acceso a la escucha desde la cámara.

Transmisión de audio	Permite el acceso para hablar con la cámara.
Grabación manual	Permitir iniciar y detener las grabaciones manualmente.
PTZ mecánica	permite el acceso a los controles PTZ mecánicos. Disponible únicamente para cámaras con PTZ mecánico.
Prioridad PTZ	Define la prioridad PTZ. Un número más bajo significa una mayor prioridad. Si no hay ninguna prioridad asignada, el valor es 0. Un administrador tiene la más alta prioridad. Cuando un rol con mayor prioridad opera una cámara PTZ, los demás no pueden operar la misma cámara durante 10 segundos de manera predeterminada. Disponible únicamente para cámaras con PTZ mecánico que tengan seleccionado Mechanical PTZ (PTZ mecánico) .

Vistas

Los siguientes privilegios de acceso están disponibles para grupos o usuarios con el rol **Operator (Operador)** o **Viewer (Visor)**. Puede seleccionar varias vistas y configurar los privilegios de acceso.

Acceso	Permitir acceso a las vistas en AXIS Camera Station S2108 Appliance.
Editar	Permite editar vistas en AXIS Camera Station S2108 Appliance.

E/S

Los siguientes privilegios de acceso están disponibles para grupos o usuarios con el rol **Operator (Operador)** o **Viewer (Visor)**.

Acceso	permite acceso total al puerto de E/S.
Lectura	Permite visualizar el estado del puerto de E/S sin modificarlo.
Escritura	Permite cambiar el estado del puerto de E/S.

Sistema

Los privilegios de acceso en gris en la lista no se pueden configurar. La marca de verificación implica que el usuario o grupo tiene este privilegio de forma predeterminada.

Los siguientes privilegios de acceso están disponibles para usuarios o grupos con el rol **Operator (Operador)**. **Take snapshots (Tomar instantáneas)** también está disponible para el rol **Viewer (Visor)**.

Tomar instantáneas	Permite tomar instantáneas en modo de visualización en directo y en modo de grabación.
Exportar grabaciones	Permite exportar grabaciones.
Generar informe de incidencias	Permite generar informes de incidencias.
Prevent access to recordings older than (Impedir el acceso a grabaciones anteriores a)	Impide acceder a grabaciones más antiguas que el número de minutos especificado. Los usuarios no

	encuentran estas grabaciones cuando realizan una búsqueda.
Acceder a alarmas, tareas y registros	Proporciona notificaciones de alarma y permite el acceso a la barra Alarms and tasks (Alarmas y tareas) y a la pestaña Logs (Registros) .
Access data search (Búsqueda de datos de acceso)	Permite buscar datos para realizar el seguimiento de lo que ocurrió en el momento del evento.
Añadir categorías a los eventos	Permitir añadir categorías de evento a la pestaña Recordings (Grabaciones) .
Eliminar categorías de evento	Permitir eliminar categorías de evento de la pestaña Recordings (Grabaciones) .

Control de acceso

Los siguientes privilegios de acceso están disponibles para usuarios o grupos con el rol **Operator (Operador)**. **Access Management (Gestión de acceso)** también está disponible para el rol **Viewer (Visor)**.

Configuración de control de acceso	Permite configurar puertas y zonas, perfiles de identificación, formatos de tarjeta y PIN, comunicación cifrada y servidor múltiple.
Gestión de acceso	Permite gestionar el acceso y acceder a los ajustes de Active Directory.

Los siguientes privilegios de acceso están disponibles para usuarios o grupos con el rol **Viewer (Visor)**.

Supervisión del estado del sistema

Los siguientes privilegios de acceso están disponibles para usuarios o grupos con el rol **Operator (Operador)**. **Access to system health monitoring (Acceso a supervisión del estado del sistema)** también está disponible para el rol **Viewer (Visor)**.

Configuration of system health monitoring (Configuración de Supervisión del estado del sistema)	Permite configurar la supervisión del estado del sistema.
Access to system health monitoring (Acceder a supervisión del estado del sistema)	Permite acceder a la supervisión del estado del sistema.

Gestione sus dispositivos

Actualizar certificados de arranque seguro

Microsoft retirará los certificados de arranque seguro de 2011 en junio de 2026 y los sustituirá por nuevos certificados de 2023. Para garantizar la seguridad de su grabadora, instale los certificados de 2023 antes de esa fecha.

La instalación de los certificados de 2023 requiere Windows 10 LTSC (Canal de servicio a largo plazo) o Windows 11 LTSC. Si su dispositivo está en garantía, pero ejecuta Windows 10 SAC (Canal semianual) en lugar de una versión LTSC, contacte con la asistencia técnica de Axis. Ellos podrán indicarle si puede actualizar a una versión LTSC antes de actualizar la BIOS o modificar cualquier certificado.

Nota

Después de junio de 2026, los dispositivos que no cuenten con los certificados de 2023 seguirán funcionando con normalidad, pero no recibirán las nuevas protecciones de seguridad para el proceso de arranque inicial, incluidas las actualizaciones del Administrador de arranque de Windows y las listas de revocación de nuevas vulnerabilidades.

Verifique el estado de su certificado.

Para verificar que los certificados de 2023 estén instalados y que el gestor de arranque de Windows se haya actualizado, utilice uno de los siguientes métodos:

Método 1:

1. Abra Registry Editor (Editor del registro).
2. Vaya a HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecureBoot\Servicing.
3. Compruebe el valor UEFICA2023Status. Si el valor indica **Updated (Actualizado)**, significará que el certificado de 2023 está instalado.

 (Default)	REG_SZ	(value not set)
 BucketHash	REG_SZ	5a3041a8e6c7476f988f369de06e65e224df7d53cf7f9...
 ConfidenceLevel	REG_SZ	No Data Observed - Action Required
 ConfidenceUpdateType	REG_DWORD	0x00000000 (0)
 LastParsedBucketDataVersion	REG_DWORD	0x0000000c (12)
 UEFICA2023Status	REG_SZ	Updated
 WindowsUEFICA2023Capable	REG_DWORD	0x00000002 (2)

Método 2:

1. Abra Windows Security (Seguridad de Windows).
2. Vaya a Device security (Seguridad del dispositivo).
3. En Secure boot (Arranque seguro), compruebe el mensaje de estado. Si el certificado está actualizado, la tarjeta mostrará: "El arranque seguro está activado y se han aplicado todas las actualizaciones de certificado necesarias. No se requieren más cambios en los certificados".



Secure boot

Secure Boot is on and all required certificate updates have been applied.
No further certificate changes are needed.

Nota

La seguridad de Windows solo muestra el estado del certificado si su dispositivo tiene instalada la actualización acumulativa del 14 de abril de 2026 o posterior. Si no ve ningún mensaje sobre el estado del certificado, instale la última actualización de Windows o utilice el Método 1.

Acciones recomendadas

Una actualización de la BIOS almacenará los certificados de 2023 de forma permanente en el firmware. Este es el método más fiable y el que recomendamos incluso si ya ha instalado los certificados a través de Windows Update.

Importante

Si solo instala los certificados a través de Windows Update y luego restablece las claves de arranque seguro de la BIOS a los valores predeterminados de fábrica, los certificados se perderán y el dispositivo no se iniciará con el arranque seguro activado. Actualice la BIOS para que los certificados sean permanentes antes de restablecer las claves de arranque seguro.

Actualizar el certificado a través de la BIOS

Instale la versión de BIOS indicada para su modelo, o una versión posterior. Puede descargarla desde la página del producto en Axis.com:

Modelo	Versión mínima de la BIOS
AXIS S2208	Por confirmar
AXIS S2212	Por confirmar
AXIS S2216	Por confirmar
AXIS S2224	Por confirmar
AXIS S2108	Z218-004
AXIS S2208 Mk II	Z670-005
AXIS S2212 Mk II	Z671-005
AXIS S2216 Mk II	Z672-005
AXIS S2224 Mk II	Z673-005

Actualizar el certificado a través de Windows Update

Si aún no existe una actualización de la BIOS disponible para su modelo, puede obtener los certificados de 2023 a través de Windows Update.

Importante

Los certificados instalados de esta manera se almacenan en la base de datos de arranque seguro actual, no en el firmware. Si restablece las claves de arranque seguro de la BIOS a los valores predeterminados de fábrica, perderá los certificados y es posible que el dispositivo no pueda arrancar con el arranque seguro activado. Instale una actualización de la BIOS tan pronto como esté disponible para su modelo, incluso si ya ha utilizado este método.

Para usar esta ruta:

1. Asegúrese de que su dispositivo ejecute Windows 10 LTSC o Windows 11 LTSC.
2. Instale todas las actualizaciones de Windows publicadas el 14 de abril de 2026 o después.
3. Vaya a **Windows Security (Seguridad de Windows) > Device security (Seguridad del dispositivo) > Secure Boot (Arranque seguro)** para comprobar el estado de su certificado.
4. Si el certificado no se actualiza tras instalar las últimas actualizaciones, compruebe el valor del registro **UEFICA2023Status**. Si su dispositivo continúa sin ser apto para la actualización automática, actualice la BIOS o contacte con la asistencia técnica de Axis.

Importante

No revoque manualmente el certificado de 2011 hasta que haya confirmado que todos los medios de recuperación, entornos de arranque y controladores de su entorno están firmados con el certificado de 2023.

Revocar el certificado de 2011 demasiado pronto impedirá que su dispositivo se inicie con el arranque seguro activado.

Comprobar la versión de BIOS

Para comprobar la versión de BIOS:

1. Encienda el dispositivo y pulse **DEL** varias veces hasta que aparezca el logotipo de Axis.
2. El número de versión se muestra como primera entrada en **Main (Principal)**.

Actualizar la BIOS

Siga las instrucciones incluidas en la guía de la BIOS, disponible en la página de descarga del archivo de la BIOS.

Actualización de Windows®

Windows® comprueba periódicamente si hay actualizaciones. Cuando hay una actualización disponible, el dispositivo descarga automáticamente la actualización, pero debe instalarla manualmente.

Nota

La grabación se interrumpirá durante un reinicio programado del sistema.

Para buscar actualizaciones manualmente:

1. Vaya a **Settings (Ajustes) > Windows Update**.
2. Haga clic en **Check for updates (Buscar actualizaciones)**.

Configurar los ajustes de Windows® Update

Es posible cambiar cómo y cuándo Windows® hace sus actualizaciones para adaptarse a sus necesidades.

Nota

Todas las grabaciones en curso se interrumpirán durante un reinicio programado del sistema.

1. Abra la aplicación Ejecutar.
 - Vaya a **Windows System > Run (Sistema Windows > Ejecutar)**, o
2. Escriba `gpedit.msc` y haga clic en **OK (Aceptar)**. Se abrirá el Editor de directivas de grupo local.
3. Vaya a **Computer Configuration > Administrative Templates > Windows Components > Windows Update (Ajustes del ordenador > Plantillas administrativas > Componentes de Windows > Windows Update)**.
4. Configure las opciones según sea necesario, vea el ejemplo.

Ejemplo:

Para descargar e instalar automáticamente las actualizaciones sin la interacción del usuario y hacer que el dispositivo se reinicie, si es necesario, fuera del horario de oficina, utilice la siguiente configuración:

1. Abra **Always automatically restart at the scheduled time (Siempre se reinicia automáticamente a la hora programada)** y seleccione:
 - 1.1. **Habilitado**
 - 1.2. **The restart timer will give users this much time to save their work (minutes) (El temporizador de reinicio dará a los usuarios este tiempo para guardar su trabajo (minutos))**: 15.
 - 1.3. Haga clic en **OK**.
2. Abra **Configure Automatic Updates (Configurar actualizaciones automáticas)** y seleccione:
 - 2.1. **Habilitado**
 - 2.2. **Configure Automatic updates (Configurar actualizaciones automáticas)**: Descarga automática y programación de la instalación
 - 2.3. **Schedule Install day (Programar día de la instalación)**: Todos los domingos

- 2.4. Schedule Install time (Programar hora de la instalación): 00:00
- 2.5. Haga clic en OK.
3. Abra Allow Automatic Updates immediate installation (Permitir instalación inmediata de actualizaciones automáticas) y seleccione:
 - 3.1. Habilitado
 - 3.2. Haga clic en OK.

Administración de energía

El switch tiene una potencia disponible total de 105 W, que es la salida de alimentación máxima para todos los dispositivos conectados.

En casi todos los casos, los dispositivos conectados consumen menos energía que la solicitada. Para optimizar el uso de energía, el controlador PoE permite que los dispositivos conectados soliciten hasta 125 W y, al mismo tiempo, limita el uso de energía real a 105 W.

Por ejemplo, el switch puede alimentar 8 dispositivos PoE de clase 3.

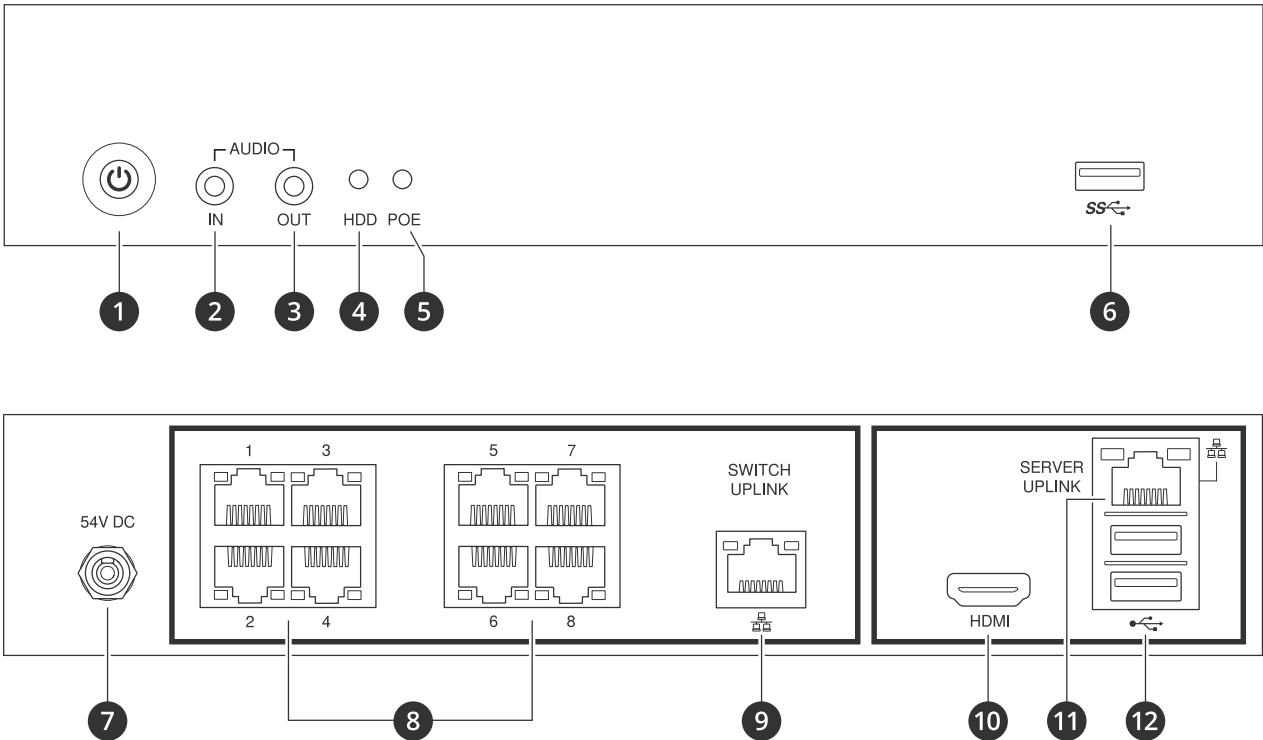
- Un dispositivo PoE de clase 3 solicita alimentación de 15,4 W.
- Ocho dispositivos PoE de clase 3 solicitan 8 x 15,4, es decir, una alimentación de 123,2 W. Esta cantidad se encuentra dentro del límite de 125 W que permite el controlador PoE.
- Un dispositivo PoE de clase 3 consume normalmente de 10 a 12 W.
- Ocho dispositivos PoE de clase 3 consume normalmente de 80 a 96 W. Esta cantidad se encuentra dentro del límite de 105 W de la potencia disponible total.

▲ ADVERTENCIA

- Si los dispositivos conectados solicitan una alimentación superior a 125 W:
 - El último dispositivo conectado no se iniciará.
 - El LED de sobrecarga de PoE se iluminará en rojo fijo hasta que se desenchufe el último dispositivo conectado o hasta que se libere la suficiente potencia disponible de PoE eliminando otros dispositivos.
- Si los dispositivos conectados consumen más de 105 W:
 - El último dispositivo encendido se apagará y tratará de reiniciarse.
 - El LED de sobrecarga PoE no se iluminará.

Guía de productos

Partes delantera y trasera



- 1 Botón de encendido/LED de encendido
- 2 Entrada de audio
- 3 Salida de audio
- 4 LED de actividad del disco duro
- 5 LED de estado de puertos PoE
- 6 Puerto USB 3.0
- 7 Conector de alimentación
- 8 Puertos PoE
- 9 Puerto de enlace ascendente de switch RJ45
- 10 Puerto HDMI
- 11 Puerto de enlace ascendente de servidor RJ45
- 12 Puertos USB 2.0

Especificaciones

LED frontales

Indicador LED	Color	Indicación
Potencia	Verde	Servidor en
Disco duro	Parpadea en ámbar	Actividad del disco duro
	Parpadea en rojo	Posible fallo del disco duro
Sobrecarga de PoE	Rojo	Por encima de la potencia disponible de PoE
	Apagado	OK

LED traseros

Actividad y velocidad de red	Color	Indicación
LED derecho	Ámbar	10/100 Mbit/s
	Verde ¹	1000 Mbit/s
LED izquierdo	Parpadea en verde	Actividad de red

1. Solo es válido para el enlace ascendente del switch y el enlace ascendente del servidor.

Localización de problemas

Ejecutar una recuperación del sistema

Si el dispositivo ha tenido un fallo completo del sistema, debe utilizar una imagen de recuperación para recrear el sistema Windows®. Para descargar el AXIS Network Video Recorder Recovery Kit, póngase en contacto con el Soporte Técnico de Axis y suministre el número de serie de su dispositivo.

Nota

El AXIS Network Video Recorder Recovery Kit está disponible en dos versiones:

- **sb11** — para dispositivos que aún utilizan el certificado de 2011.
- **sb23** — para dispositivos que hayan pasado a utilizar el certificado de 2023.

Antes de descargar el kit de recuperación, compruebe el estado de su certificado y seleccione la variante correspondiente. Si selecciona la variante incorrecta, la instalación no generará un resultado de arranque y deberá volver a empezar con la imagen correcta. Esto no dañará su dispositivo.

Si su dispositivo ya tiene instalado el certificado de 2023, la variante sb11 continúa siendo segura de usar, siempre y cuando el certificado de 2011 no haya sido revocado manualmente. Una vez revocado, solo funcionará el sb23.

Para recrear el sistema:

1. Descargue el kit de recuperación de AXIS Network Video Recorder y la herramienta de recuperación de ISO a USB de AXIS Network Video Recorder.
2. Inserte una unidad USB en su ordenador.
 - Utilice una unidad USB con un mínimo de 16 GB.
 - La unidad USB se formateará y se borrarán todos los datos existentes.
3. Ejecute la herramienta de recuperación de ISO a USB de AXIS Network Video Recorder y siga las instrucciones en pantalla.
La escritura de datos en la unidad USB tarda aproximadamente de 10 a 15 minutos. No extraiga la unidad USB hasta que el proceso se haya completado.
4. Una vez completada la herramienta de recuperación de ISO a USB de AXIS Network Video Recorder, tome la unidad USB y conéctela a su dispositivo.
5. Inicie su dispositivo.
6. Cuando vea la pantalla de bienvenida de Axis, pulse F12.
7. Haga clic en **UEFI: USB Drive (UEFI: unidad USB)**.
8. Navegue a su unidad de USB y pulse Intro. El sistema arranca en el kit de recuperación de AXIS Network Video Recorder.
9. Haga clic en **Reinstall Operating System (Reinstalar sistema operativo)**.
La recuperación toma aproximadamente de 10 a 15 minutos para completarse. Encontrará instrucciones detalladas en la descarga del kit de recuperación.

Resolución de problemas de AXIS Camera Station

Para obtener información sobre cómo solucionar los problemas de AXIS Camera Station, consulte el *Manual del usuario de AXIS Camera Station*.

¿Necesita más ayuda?

Enlaces útiles

- *Manual de usuario de AXIS Camera Station*
- *Iniciar sesión en AXIS Secure Remote Access*
- *Qué se debe incluir en una lista de permisos de antivirus para AXIS Camera Station*

Contactar con la asistencia técnica

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

T10181903_es

2026-07 (M7.2)

© 2022 – 2026 Axis Communications AB