

# AXIS D4200-VE Network Strobe Speaker

## Índice

Presentación esquemática de la solución.....	4
.....	4
Instalación.....	5
Cómo funciona.....	6
.....	6
Localice el dispositivo en la red.....	6
Compatibilidad con navegadores.....	6
Abrir la interfaz web del dispositivo.....	6
Crear una cuenta de administrador.....	6
Contraseñas seguras.....	7
Asegúrese de que nadie ha manipulado el software del dispositivo.....	7
Configure su dispositivo.....	8
Configurar un perfil.....	8
Configurar un perfil con un archivo de audio de sirena personalizado.....	8
Importar o exportar un perfil.....	8
Configurar SIP directo (P2P).....	8
Configurar SIP a través de un servidor (PBX).....	9
Calibración y ejecución de un altavoz remoto.....	10
Configurar reglas para eventos.....	10
Activar una acción.....	10
Iniciar un perfil cuando se active una alarma.....	11
Iniciar un perfil a través de SIP.....	11
Uso de extensiones SIP para controlar más de un perfil.....	11
Ejecutar dos perfiles con diferentes prioridades.....	12
Activación de un altavoz estroboscópico a través de HTTP post si una cámara detecta movimiento.....	13
Activación de un altavoz estroboscópico a través de una entrada virtual si una cámara detecta movimiento.....	14
Activar el altavoz estroboscópico a través de MQTT cuando la cámara detecte movimiento.....	15
Enviar un correo electrónico si se produce un error de comprobación de altavoz.....	17
Reproducir clip personalizado al activar una alarma.....	18
Detener audio con DTMF.....	18
Configuración de audio para llamadas SIP entrantes.....	19
Interfaz web.....	21
Descubrir más.....	22
Protocolo de inicio de sesión (SIP).....	22
Peer-to-peer SIP (SIP de punto a punto):.....	22
Centralita telefónica privada (PBX).....	22
NAT transversal.....	23
Analíticas y aplicaciones.....	23
AXIS Audio Analytics.....	23
InformaCast®.....	24
Ciberseguridad.....	24
Servicio de notificación de seguridad de Axis.....	24
Gestión de las vulnerabilidades.....	24
Funcionamiento seguro de dispositivos Axis.....	24
Especificaciones.....	25
Guía de productos.....	25
Indicadores LED.....	26
Ranura para tarjeta SD.....	27
Botones.....	27
Botón de control.....	27
Interruptor del micrófono.....	27

Conectores .....	27
Conector de red.....	27
Conector de audio .....	27
Conector de E/S.....	28
Nombres de patrones de luz .....	29
Nombres de los patrones de sonido .....	30
Limpie su dispositivo .....	31
Localización de problemas .....	32
Restablecimiento a la configuración predeterminada de fábrica .....	32
Opciones de AXIS OS .....	32
Comprobar la versión de AXIS OS.....	32
Actualización de AXIS OS.....	33
Problemas técnicos y posibles soluciones .....	33
Consideraciones sobre el rendimiento.....	36
Contactar con la asistencia técnica .....	36

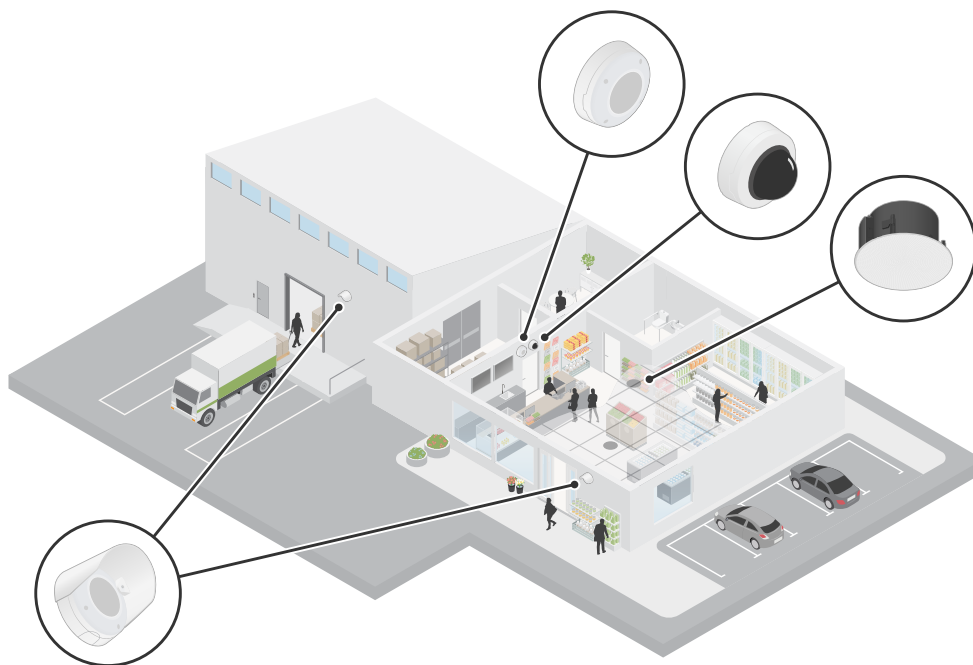
## Presentación esquemática de la solución

Este manual describe cómo lograr que el dispositivo sea accesible a su sistema de audio y cómo configurarlo directamente desde su interfaz.

Si utiliza un software de gestión de audio o vídeo, puede utilizar dicho software para configurar el dispositivo. Puede usar los siguientes programas de software de gestión para controlar su sistema de audio:

- **AXIS Audio Manager Edge:** software de gestión de audio para sistemas pequeños. Viene preinstalado en todos los dispositivos de audio con un firmware igual o superior a 10.0.
  - *Manual de usuario de AXIS Audio Manager Edge*
- **AXIS Audio Manager Pro:** software avanzado de gestión de audio para sistemas de gran tamaño.
  - *Manual de usuario AXIS Audio Manager Pro*
- **AXIS Camera Station Pro:** software avanzado de gestión de vídeo para sistemas de gran tamaño.
  - *Manual de usuario de AXIS Camera Station Pro*

Para obtener más información, consulte *Software de gestión de audio*.



## Instalación

### Importante

No instale el altavoz estroboscópico ni los dispositivos conectados a menos de 3 m del centro de la vía férrea. Este vídeo es un ejemplo de cómo instalar el AXIS D4200-VE Network Strobe Speaker.



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

## Cómo funciona

### ⚠ ADVERTENCIA

Los destellos o luces parpadeantes pueden provocar convulsiones en personas con epilepsia fotosensible.

### Localice el dispositivo en la red

Para localizar dispositivos de Axis en la red y asignarles direcciones IP en Windows®, utilice AXIS IP Utility o AXIS Device Manager. Ambas aplicaciones son gratuitas y pueden descargarse desde [axis.com/support](http://axis.com/support).

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

### Compatibilidad con navegadores

Puede utilizar el dispositivo con los siguientes navegadores:

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

✓: Recomendado

\*: Asistencia técnica con limitaciones

### Abrir la interfaz web del dispositivo

1. Abra un navegador y escriba la dirección IP o el nombre de host del dispositivo Axis. Si no conoce la dirección IP, use AXIS IP Utility o AXIS Device Manager para localizar el dispositivo en la red.
2. Escriba el nombre de usuario y la contraseña. Si accede al dispositivo por primera vez, debe crear una cuenta de administrador. Vea *Crear una cuenta de administrador, on page 6*.

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

### Crear una cuenta de administrador

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

1. Introduzca un nombre de usuario.
2. Introduzca una contraseña. Vea *Contraseñas seguras, on page 7*.
3. Vuelva a escribir la contraseña.
4. Aceptar el acuerdo de licencia.
5. Haga clic en **Add account (agregar cuenta)**.

### Importante

El dispositivo no tiene una cuenta predeterminada. Si pierde la contraseña de la cuenta de administrador, debe restablecer el dispositivo. Vea *Restablecimiento a la configuración predeterminada de fábrica, on page 32*.

## Contraseñas seguras

### Importante

Utilice HTTPS (habilitado por defecto) para configurar su contraseña u otros ajustes confidenciales a través de la red. HTTPS ofrece conexiones de red seguras y cifradas para proteger datos confidenciales, como las contraseñas.

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

Para proteger sus datos le recomendamos encarecidamente que:

- Utilice una contraseña con al menos 8 caracteres, creada preferiblemente con un generador de contraseñas.
- No exponga la contraseña.
- Cambie la contraseña a intervalos periódicos y al menos una vez al año.

## Asegúrese de que nadie ha manipulado el software del dispositivo

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


1. Restablezca la configuración predeterminada de fábrica. Vea *Restablecimiento a la configuración predeterminada de fábrica, on page 32*. Después de un restablecimiento, el inicio seguro garantiza el estado del dispositivo.
2. Configure e instale el dispositivo.

## Configure su dispositivo

### Configurar un perfil

Un perfil es una colección de configuraciones. Puede tener hasta 30 perfiles con diferentes prioridades y patrones.

Para establecer un nuevo perfil:


1. Vaya a **Profiles (Perfiles)** y haga clic en  **Create (Crear)**.
2. Introduzca un **Name (Nombre)** y una **Description (Descripción)**.
3. Seleccione la configuración de la **Light (Luz)** y la **Siren (Sirena)** que desea para el perfil.
4. Establezca la **Priority (Prioridad)** de la luz y la sirena y haga clic en **Save (Guardar)**.

Para editar un perfil, haga clic en  y seleccione **Edit (Editar)**.

### Configurar un perfil con un archivo de audio de sirena personalizado

Puede configurar un perfil con un archivo de audio personalizado. Puede guardar archivos de audio de hasta 100 MB en el dispositivo. Para archivos de audio más grandes, utilice una tarjeta SD si el dispositivo cuenta con una ranura para tarjetas SD.

Subir un archivo de audio:


1. Vaya a **Media (Medios)** y haga clic en  **Add (Añadir)**.
2. Seleccione el archivo desde su ordenador.
3. Seleccione la **Storage location (Ubicación de almacenamiento)**.
4. Haga clic en **Save (Guardar)**.

Para usar el archivo de audio en un perfil:

1. Vaya a **Profiles (Perfiles)** y cree un perfil. Para obtener más información, consulte *Configurar un perfil, on page 8*.
2. Cuando configure la **Siren (Sirena)**, seleccione el archivo de audio cargado como **Pattern (Patrón)**.

### Importar o exportar un perfil

Si desea utilizar un perfil con configuraciones predefinidas, puede importarlo:

1. Vaya a **Profiles (Perfiles)** y haga clic en  **Importar**.
2. Desplácese hasta localizar el archivo o arrastre y coloque el archivo que desee importar.
3. Haga clic en **Save (Guardar)**.

Para copiar uno o más perfiles y guardar en otros dispositivos, puede exportarlos:

1. seleccione los perfiles.
2. Haga clic en **Exportar**.
3. Desplácese para localizar los archivos .json.

### Configurar SIP directo (P2P)

Utilice la configuración de punto a punto cuando la comunicación se realice entre unos pocos agentes de usuario dentro de la misma red IP y no necesite funciones adicionales que pueda proporcionar un servidor PBX.

Para comprender mejor el funcionamiento de par a par, consulte *Peer-to-peer SIP (SIP de punto a punto)*; on page 22.

Para más información sobre las opciones de ajustes, consulte .

1. Vaya a **System (Sistema) > SIP > SIP settings (Ajustes SIP)** y seleccione **Enable SIP (Habilitar SIP)**.
2. Para permitir que el dispositivo reciba llamadas entrantes, seleccione **Allow incoming calls (Permitir llamadas entrantes)**.
3. En **Gestión de Llamadas**, defina el tiempo de espera y la duración de la llamada.
4. En **Ports (Puertos)**, introduzca los números de los puertos.
  - **SIP port (Puerto SIP)**: puerto de red utilizado para la comunicación SIP. El tráfico de señalización a través de este puerto no está cifrado. El puerto predeterminado es el 5060. Si es necesario, introduzca un número de puerto diferente.
  - **TLS port (Puerto TLS)**: puerto de red utilizado para la comunicación SIP cifrada. El tráfico de señalización a través de este puerto está cifrado con Transport Layer Security (TLS). El puerto predeterminado es el 5061. Si es necesario, introduzca un número de puerto diferente.
  - **RTP start port (Puerto de inicio RTP)**: introduzca el puerto utilizado para la primera transmisión de medios RTP en una llamada SIP. El puerto de inicio predeterminado para el transporte de medios es 4000. Algunos cortafuegos pueden bloquear el tráfico RTP en determinados números de puerto. Un número de puerto debe estar entre 1024 y 65535.
5. En **NAT traversal (NAT transversal)**, seleccione los protocolos que desea activar.

### Nota

Utilice NAT transversal cuando el dispositivo se conecta a la red desde un router NAT o un firewall. Para obtener más información vea *NAT transversal*, on page 23.

6. En **Audio**, seleccione al menos un códec de audio con la calidad de audio requerida para las llamadas SIP. Arrastre y coloque para cambiar la prioridad.
7. En **Additional (Adicional)**, seleccione opciones adicionales.
  - **UDP-to-TCP switching (Conmutación de UDP a TCP)**: seleccione esta opción para permitir que las llamadas cambien los protocolos de transporte de UDP (User Datagram Protocol) a TCP (Transmission Control Protocol) temporalmente. El motivo para cambiar es evitar la fragmentación y el cambio puede realizarse si la solicitud está a 200 bytes de la unidad de transmisión máxima (MTU) o es mayor de 1300 bytes.
  - **Allow via rewrite (Permitir mediante reescritura)**: seleccione para enviar la dirección IP local en lugar de la dirección IP pública del rúter.
  - **Allow contact rewrite (Permitir la reescritura de contactos)**: seleccione para enviar la dirección IP local en lugar de la dirección IP pública del rúter.
  - **Register with server every (Registro en el servidor cada)**: establezca la frecuencia con la que desea que el dispositivo se registre en el servidor SIP en relación con las cuentas SIP existentes.
  - **DTMF payload type (Tipo de carga útil DTMF)**: cambia el tipo de carga útil predeterminada para DTMF.
8. Haga clic en **Save (Guardar)**.

## Configurar SIP a través de un servidor (PBX)

Utilice un servidor PBX cuando los agentes usuarios se comuniquen dentro y fuera de la red IP. Se pueden agregar características adicionales a la configuración en función del proveedor del PBX. Para comprender mejor el funcionamiento de par a par, consulte *Centralita telefónica privada (PBX)*, on page 22.

Para más información sobre las opciones de ajustes, consulte .

1. Solicite la siguiente información de su proveedor de PBX:
  - ID de usuario
  - Dominio

- Contraseña
  - ID de autenticación
  - ID del emisor de la llamada
  - Registrador
  - Puerto de inicio RTP
2. Para agregar una cuenta nueva, vaya a **System (Sistema) > SIP > SIP accounts (Cuentas SIP)** y haga clic en **+ Account (Cuenta)**.
  3. Introduzca los datos que ha recibido de su proveedor PBX.
  4. Seleccione **Registered (Registrado)**.
  5. Seleccionar un modo de transporte.
  6. Haga clic en **Save (Guardar)**.
  7. Configure los ajustes de SIP de la misma forma que para el punto a punto. Consulte *Configurar SIP directo (P2P)*, on page 8 para obtener más información.

### Calibración y ejecución de un altavoz remoto

Puede ejecutar una prueba de altavoces para verificar, desde una ubicación remota, que un altavoz funciona como está previsto. El altavoz realiza la prueba reproduciendo una serie de tonos de prueba registrados por el micrófono integrado. Cada vez que se ejecuta la prueba, los valores registrados se comparan con los valores que se registraron durante la calibración.

#### Nota

La prueba se debe calibrar desde el lugar en el que está montado. Si el altavoz se mueve o si su entorno local cambia, por ejemplo, si se construye o se elimina una pared, el altavoz debe volver a calibrarse.

Durante la calibración, se recomienda que alguien esté presente físicamente en el sitio de instalación para escuchar los tonos de comprobación y asegurarse de que los tonos de comprobación no están apagados o bloqueados por cualquier obstrucción no deseada en la ruta acústica del altavoz.

1. Vaya a la interfaz del dispositivo > **Audio > Speaker test (Comprobación de altavoz)**.
2. Para calibrar el dispositivo de audio, haga clic en **Calibrate (Calibrar)**.

#### Nota

Una vez que el producto Axis esté calibrado, la prueba de los altavoces puede ejecutarse en cualquier momento.

3. Para ejecutar la prueba de los altavoces, haga clic en **Run the test (Ejecutar la comprobación)**.

#### Nota

También es posible ejecutar la calibración pulsando el botón de control del dispositivo físico. Consulte *Guía de productos*, on page 25 para identificar el botón de control.

### Configurar reglas para eventos

Puede crear reglas para que el dispositivo realice acciones cuando se produzcan determinados eventos. Una regla consta de condiciones y acciones. Las condiciones se pueden utilizar para activar las acciones. Por ejemplo, el dispositivo puede reproducir un clip de audio según una programación o cuando recibe una llamada, o puede enviar un correo electrónico si cambia su dirección IP.

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

### Activar una acción

1. Vaya a **System > Events (Sistema > Eventos)** y agregue una regla. La regla determina cuándo debe realizar el dispositivo determinadas acciones. Puede configurar reglas como programadas, recurrentes o activadas manualmente.

2. Introduzca un **Name (Nombre)**.
3. Seleccione la **Condition (Condición)** que debe cumplirse para que se active la acción. Si especifica varias condiciones para la regla, deben cumplirse todas ellas para que se active la acción.
4. En **Action (Acción)**, seleccione qué acción debe realizar cuando se cumplan las condiciones.

**Nota**

- Si realiza cambios a una regla activa, esta debe iniciarse de nuevo para que los cambios surtan efecto.

### Iniciar un perfil cuando se active una alarma

En este ejemplo se explica cómo activar una alarma cuando la señal de entrada digital está cambiada.

Configure la entrada de dirección para el puerto:

1. Vaya a **System (Sistema) > Accessories (Accesorios) > I/O ports (Puertos de E/S)**.
2. Vaya a **Port 1 (Puerto 1) > Normal state (Estado normal)** y haga clic en **Circuit closed (Circuito cerrado)**.

Crear una regla:

1. Vaya a **System (Sistema) > Events (Eventos)** y agregue una regla.
2. Escriba un nombre para la regla.
3. En la lista de condiciones, seleccione **I/O (E/S) > Digital input is active (La entrada digital está activa)**.
4. Seleccione **Port 1 (Puerto 1)**.
5. En la lista de acciones, seleccione **Run light and siren profile while the rule is active (Ejecutar perfil de luz y sirena mientras la regla esté activa)**.
6. Seleccione el perfil que desea iniciar.
7. Haga clic en **Save (Guardar)**.

### Iniciar un perfil a través de SIP

En este ejemplo se explica cómo activar una alarma a través de SIP.

Activar SIP:

1. Vaya a **Settings (Ajustes) > SIP > SIP settings (Ajustes SIP)**.
2. Seleccione **Enable SIP (Habilitar SIP)** y **Allow incoming calls (Permitir llamadas entrantes)**.
3. Haga clic en **Save (Guardar)**.

Crear una regla:

1. Vaya a **System (Sistema) > Events (Eventos)** y agregue una regla.
2. Escriba un nombre para la regla.
3. En la lista de condiciones, seleccione **Call (Llamar) > State (Estado)**.
4. En la lista de estado, seleccione **Active (Activo)**.
5. En la lista de acciones, seleccione **Run light and siren profile while the rule is active (Ejecutar perfil de luz y sirena mientras la regla esté activa)**.
6. Seleccione el perfil que desea iniciar.
7. Haga clic en **Save (Guardar)**.

### Uso de extensiones SIP para controlar más de un perfil

Activar SIP:

1. Vaya a **Settings (Ajustes) > SIP > SIP settings (Ajustes SIP)**.

2. Seleccione **Enable SIP (Habilitar SIP)** y **Allow incoming calls (Permitir llamadas entrantes)**.
3. Haga clic en **Save (Guardar)**.

Crear una regla para iniciar un perfil:

1. Vaya a **System (Sistema) > Events (Eventos)** y agregue una regla.
2. Escriba un nombre para la regla.
3. En la lista de condiciones, seleccione **Call (Llamar) > State change (Cambio de estado)**.
4. En la lista de motivos, seleccione **Accepted by device (Aceptado por dispositivo)**.
5. En **Call direction (Dirección de llamada)**, seleccione **Incoming (Entrante)**.
6. En **Local SIP URI (URI SIP local)**, escriba `< sip:[Ext]@[IP address]>`, donde [Ext] es la extensión que se usa para el perfil y [dirección IP] es la dirección del dispositivo. Por ejemplo, `sip:1001@192.168.0.90`.
7. En la lista de acciones, seleccione **Light and Siren (Luz y sirena) > Run light and siren profile (Ejecutar perfil de luz y sirena)**.
8. Seleccione el perfil que desea iniciar.
9. Seleccione la acción **Start (Iniciar)**.
10. Haga clic en **Save (Guardar)**.

Crear una regla para detener un perfil:

1. Vaya a **System (Sistema) > Events (Eventos)** y agregue una regla.
2. Escriba un nombre para la regla.
3. En la lista de condiciones, seleccione **Call (Llamar) > State change (Cambio de estado)**.
4. En la lista de motivos, seleccione **Terminated (Terminado)**.
5. En **Call direction (Dirección de llamada)**, seleccione **Incoming (Entrante)**.
6. En **Local SIP URI (URI SIP local)**, escriba `sip:[Ext]@[IP address]` (`sip:[Ext]@[dirección IP]`), donde [Ext] es la extensión que se usa para el perfil y [dirección IP] es la dirección del dispositivo. Por ejemplo, `sip:1001@192.168.0.90`.
7. En la lista de acciones, seleccione **Light and Siren (Luz y sirena) > Run light and siren profile (Ejecutar perfil de luz y sirena)**.
8. Seleccione el perfil que desea detener.
9. Seleccione la acción **Stop (Detener)**.
10. Haga clic en **Save (Guardar)**.

Repita los pasos para crear reglas de inicio y detención para cada perfil que quiera controlar mediante SIP.

## Ejecutar dos perfiles con diferentes prioridades

Si ejecuta dos perfiles con diferentes prioridades, el perfil con un número de prioridad más alto interrumpirá al perfil con un número de prioridad menor.

### Nota

Si ejecuta dos perfiles con la misma prioridad, el perfil más reciente cancelará al anterior.

En este ejemplo se explica cómo configurar el dispositivo para que muestre un perfil con prioridad 4 sobre otro perfil con prioridad 3 cuando se activa mediante el puerto de E/S digital.

Crear perfiles:

1. Cree un perfil con prioridad 3.
2. Cree otro perfil con prioridad 4.

Crear una regla:

1. Vaya a **System (Sistema) > Events (Eventos)** y agregue una regla.
2. Escriba un nombre para la regla.
3. En la lista de condiciones, seleccione **I/O (E/S) > Digital input is active (La entrada digital está activa)**.
4. Seleccione un puerto.
5. En la lista de acciones, seleccione **Run light and siren profile while the rule is active (Ejecutar perfil de luz y sirena mientras la regla esté activa)**.
6. Seleccione el perfil que tiene el número de prioridad más alto.
7. Haga clic en **Save (Guardar)**.
8. Vaya a **Profiles (Perfiles)** e inicie el perfil con el número de prioridad más bajo.

### Activación de un altavoz estroboscópico a través de HTTP post si una cámara detecta movimiento

Este ejemplo explica cómo conectar una cámara al altavoz estroboscópico, y cómo activar un perfil cada vez que la aplicación AXIS Motion Guard, instalada en la cámara, detecte movimiento.

Antes de empezar:

- Cree un nuevo usuario con la función de operador o administrador en el altavoz estroboscópico.
- Cree un perfil en el altavoz estroboscópico llamado: "Strobe speaker profile" (Perfil de altavoz estroboscópico).
- Configure AXIS Motion Guard en la cámara y cree un perfil llamado: "Perfil de cámara".
- Asegúrese de utilizar AXIS Device Assistant con la versión de firmware 10.8.0 o posterior.

Cree un destinatario en la cámara:

1. En la interfaz del dispositivo de la cámara, vaya a **System > Events > Recipients (Sistema > Eventos > Destinatarios)** y agregue un destinatario.
2. Introduzca la siguiente información:
  - **Name (Nombre):** Altavoz estroboscópico
  - **Tipo:** HTTP
  - **URL:** `http://<IPaddress>/axis-cgi/siren_and_light.cgi`  
Sustituya la <IPaddress> (Dirección IP) por la dirección del altavoz estroboscópico.
  - El nombre de usuario y contraseña del nuevo usuario del altavoz estroboscópico.
3. Haga clic en **Test (Probar)** para asegurarse de que todos los datos son válidos.
4. Haga clic en **Save (Guardar)**.

Cree dos reglas en la cámara:

1. Vaya a **Rules (Reglas)** y añada una regla.
2. Introduzca la siguiente información:
  - **Name (Nombre):** Activar el altavoz estroboscópico con movimiento
  - **Condition (Condición):** **Applications (Aplicaciones) > Motion Guard: Camera profile (Perfil de la cámara)**
  - **Action (Acción):** **Notificaciones > Enviar notificación a través de HTTP**
  - **Recipient (Destinatario):** **Strobe speaker (Altavoz estroboscópico)**.  
La información debe ser la misma que ha introducido anteriormente en **Events > Recipients > Name (Eventos > Destinatarios > Nombre)**.
  - **Método:** **Post (Publicar)**
  - **Cuerpo:**

```
{ "apiVersion": "1.0", "method": "start", "params": {
"profile": "Strobe speaker profile" } }
```

Asegúrese de introducir la misma información en "profile" (perfil) : <>' como hizo cuando creó el perfil en el altavoz estroboscópico; en este caso: "Strobe speaker profile" (Perfil del altavoz estroboscópico).

3. Haga clic en **Save (Guardar)**.
4. Agregue otra regla con la siguiente información:
  - **Name (Nombre):** Desactivar el altavoz estroboscópico con movimiento
  - **Condition (Condición):** Applications (Aplicaciones) > Motion Guard: Camera profile (Perfil de la cámara)
  - Seleccione **Invert this condition (Invertir esta condición)**.
  - **Action (Acción):** Notificaciones > Enviar notificación a través de HTTP
  - **Recipient (Destinatario):** Altavoz estroboscópico  
La información debe ser la misma que ha introducido anteriormente en Events > Recipients > Name (Eventos > Destinatarios > Nombre).
  - **Método:** Post (Publicar)
  - **Cuerpo:**

```
{ "apiVersion": "1.0", "method": "stop", "params": { "profile": "Strobe speaker profile" } }
```

Asegúrese de introducir la misma información en "profile" (perfil) : <>' como hizo cuando creó el perfil en el altavoz estroboscópico; en este caso: "Strobe speaker profile" (Perfil del altavoz estroboscópico).

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

### Activación de un altavoz estroboscópico a través de una entrada virtual si una cámara detecta movimiento

Este ejemplo explica cómo conectar una cámara al altavoz estroboscópico, y cómo activar un perfil cada vez que la aplicación AXIS Motion Guard, instalada en la cámara, detecte movimiento.

Antes de empezar:

- Cree una nueva cuenta con los privilegios de operador o administrador en el altavoz estroboscópico.
- Cree un perfil en el altavoz estroboscópico.
- Configure AXIS Motion Guard en la cámara y cree un perfil llamado "Perfil de cámara".

Cree dos destinatarios en la cámara:

1. En la interfaz del dispositivo de la cámara, vaya a **System > Events > Recipients (Sistema > Eventos > Destinatarios)** y agregue un destinatario.
2. Introduzca la siguiente información:
  - **Name (Nombre):** Activate virtual port (Activar puerto virtual)
  - **Tipo:** HTTP
  - **URL:** http://<IPaddress>/axis-cgi/virtualinput/activate.cgi  
Sustituya la <IPaddress> (Dirección IP) por la dirección del altavoz estroboscópico.
  - La cuenta y la contraseña de la cuenta del altavoz estroboscópico recién creada.
3. Haga clic en **Test (Probar)** para asegurarse de que todos los datos son válidos.
4. Haga clic en **Save (Guardar)**.
5. Agregue un segundo destinatario con la siguiente información:
  - **Name (Nombre):** Deactivate virtual port (Desactivar puerto virtual)
  - **Tipo:** HTTP
  - **URL:** http://<IPaddress>/axis-cgi/virtualinput/deactivate.cgi  
Sustituya la <IPaddress> (Dirección IP) por la dirección del altavoz estroboscópico.
  - La cuenta y la contraseña de la cuenta del altavoz estroboscópico recién creada.
6. Haga clic en **Test (Probar)** para asegurarse de que todos los datos son válidos.

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

Cree dos reglas en la cámara:

1. Vaya a **Rules (Reglas)** y añada una regla.
2. Introduzca la siguiente información:
  - **Name (Nombre):** Activar IO1 virtual
  - **Condition (Condición):** Applications (Aplicaciones) > Motion Guard: Camera profile (Perfil de la cámara)
  - **Action (Acción):** Notificaciones > Enviar notificación a través de HTTP
  - **Recipient (Destinatario):** Activate virtual port (Activar puerto virtual)
  - **Query string suffix (Sufijo de la cadena de consulta):** schemaversion=1&tport=1
3. Haga clic en **Save (Guardar)**.
4. Agregue otra regla con la siguiente información:
  - **Name (Nombre):** Desactivar IO1 virtual
  - **Condition (Condición):** Applications (Aplicaciones) > Motion Guard: Camera profile (Perfil de la cámara)
  - Seleccione **Invert this condition (Invertir esta condición)**.
  - **Action (Acción):** Notificaciones > Enviar notificación a través de HTTP
  - **Recipient (Destinatario):** Deactivate virtual port (Desactivar puerto virtual)
  - **Query string suffix (Sufijo de la cadena de consulta):** schemaversion=1&tport=1
5. Haga clic en **Save (Guardar)**.

Crear una regla en el altavoz estroboscópico:

1. En la interfaz web del altavoz estroboscópico, vaya a **System > Events (Sistema > Eventos)** y añada una regla.
2. Introduzca la siguiente información:
  - **Name (Nombre):** activador en entrada virtual 1
  - **Condition (Condición):** I/O (E/S) > Virtual input (Entrada virtual)
  - **Port (Puerto):** 1
  - **Action (Acción):** Light and siren > Run light and siren profile while the rule is active (Luz y sirena > Ejecutar perfil de luz y sirena mientras la regla está activa)
  - **Profile (Perfil):** seleccionar el perfil recién creado
3. Haga clic en **Save (Guardar)**.

### **Activar el altavoz estroboscópico a través de MQTT cuando la cámara detecte movimiento**

Este ejemplo ilustra cómo conectar una cámara al altavoz estroboscópico mediante MQTT y activar un perfil en el altavoz cuando detecte movimiento.

Antes de empezar:

- Cree un perfil en el altavoz estroboscópico.
- Configure un intermediario de MQTT y obtenga la dirección IP, el nombre de usuario y la contraseña del intermediario.
- Asegúrese de que la aplicación de detección de movimiento esté configurada y en funcionamiento en la cámara.

Configure el cliente MQTT en la cámara:

1. En la interfaz web de la cámara, vaya a **System > MQTT > MQTT client > Broker (Sistema > MQTT > Cliente MQTT > Intermediario)** e introduzca la siguiente información:
  - **Host:** Dirección IP de intermediario

- **Client ID (ID de cliente):** Por ejemplo, cámara 1
- **Protocol (Protocolo):** El protocolo con el que se establece el intermediario
- **Puerto:** El número de puerto utilizado por el intermediario
- El **Username (Nombre de usuario)** y la **Password (Contraseña)** del intermediario.

2. Haga clic en **Save (Guardar)** y **Connect (Conectar)**.

Cree dos reglas en la cámara para la publicación MQTT:

1. Vaya a **System > Events > Rules (Sistema > Eventos > Reglas)** y añada una regla.
2. Introduzca la siguiente información:
  - **Name (Nombre):** Movimiento detectado
  - **Condition (Condición):** Applications > Motion alarm (Aplicaciones > Alarma de movimiento)
  - **Action (Acción):** MQTT > Send MQTT publish message (MQTT > Enviar mensaje de publicación MQTT)
  - **Topic (Tema):** Movimiento
  - **Payload (Carga):** Encendido
  - **QoS:** 0, 1 o 2

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

4. Agregue otra regla con la siguiente información:
  - **Name (Nombre):** Sin movimiento
  - **Condition (Condición):** Applications > Motion alarm (Aplicaciones > Alarma de movimiento)
    - Seleccione **Invert this condition (Invertir esta condición)**.
  - **Action (Acción):** MQTT > Send MQTT publish message (MQTT > Enviar mensaje de publicación MQTT)
  - **Topic (Tema):** Movimiento
  - **Payload (Carga):** Apagado
  - **QoS:** 0, 1 o 2

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

Configure el cliente MQTT en el altavoz estroboscópico:

1. En la interfaz web del altavoz estroboscópico, vaya a **System > MQTT > MQTT client > Broker (Sistema > MQTT > Cliente MQTT > Intermediario)** e introduzca la siguiente información:
  - **Host:** Dirección IP de intermediario
  - **Client ID (ID de cliente):** sirena 1
  - **Protocol (Protocolo):** El protocolo con el que se establece el intermediario
  - **Puerto:** El número de puerto utilizado por el intermediario
  - **Username (Nombre de usuario)** y **Password (Contraseña)**

2. Haga clic en **Save (Guardar)** y **Connect (Conectar)**.

3. Vaya a **MQTT subscriptions (Suscripciones MQTT)** y agregue una suscripción. Introduzca la siguiente información:
  - **Filtro de suscripción:** Movimiento
  - **Tipo de suscripción:** Con estado
  - **QoS:** 0, 1 o 2

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

Crear una regla en el altavoz para suscripciones MQTT:

1. Vaya a **System > Events > Rules (Sistema > Eventos > Reglas)** y añada una regla.
2. Introduzca la siguiente información:

- **Name (Nombre):** Movimiento detectado
- **Condition (Condición):** MQTT > Stateful (MQTT > Con estado)
- **Filtro de suscripción:** Movimiento
- **Payload (Carga):** Encendido
- **Action (Acción):** Light and siren > Run light and siren profile while the rule is active (Luz y sirena > Ejecutar perfil de luz y sirena mientras la regla está activa)
- **Profile (Perfil):** Seleccione el perfil que desea que esté activo.

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

### Enviar un correo electrónico si se produce un error de comprobación de altavoz

En este ejemplo, el dispositivo de audio se ha configurado para enviar un correo electrónico a un destinatario definido cuando se produce un error en la comprobación del altavoz. La prueba del altavoz está configurada para que se realice todos los días a las 18:00 horas.

1. Establezca una programación para la prueba del altavoz:
  - 1.1. Vaya a la interfaz del dispositivo > **System (Sistema)** > **Events (Eventos)** > **Schedules (Programación)**.
  - 1.2. Cree una programación que comience a las 18:00 y termine a las 18:01 todos los días. Nómbralo "Diario a las 18:00".
2. Crear un destinatario de correo electrónico:
  - 2.1. Vaya a la interfaz del dispositivo > **System (Sistema)** > **Events (Eventos)** > **Recipients (Destinatarios)**.
  - 2.2. Haga clic en **Add recipient (Agregar destinatario)**.
  - 2.3. Nombre el destinatario "Destinatarios de la prueba del altavoz"
  - 2.4. En **Type (Tipo)**, select (seleccione) **Email (Correo electrónico)**.
  - 2.5. En **Send email to (Enviar correo electrónico a)**, introduzca las direcciones de los destinatarios. Utilice comas para separar múltiples direcciones.
  - 2.6. Introduzca los datos de la cuenta de correo electrónico del remitente.
  - 2.7. Haga clic en **Test (Probar)** para enviar un correo electrónico de prueba.

#### Nota

Algunos proveedores de correo electrónico cuentan con filtros de seguridad que evitan que los usuarios reciban o archivos adjuntos de gran tamaño, que reciban correos programados, etc. Compruebe la política de seguridad del proveedor de correo electrónico para evitar problemas de entrega y bloqueos en las cuentas de correo electrónico.


- 2.8. Haga clic en **Save (Guardar)**.
3. Configurar una prueba de altavoz automatizada:
  - 3.1. Vaya a la interfaz del dispositivo > **System (Sistema)** > **Events (Eventos)** > **Rules (Reglas)**.
  - 3.2. Haga clic en **Add a rule (Agregar una regla)**.
  - 3.3. Introduzca un nombre para la regla.
  - 3.4. En **Condition (Condición)**, seleccione **(Schedule) Programación** y escoja entre la lista de activadores
  - 3.5. En **Schedule (Programación)**, seleccione su programación ("Diaria a las 18:00").
  - 3.6. En **Action (Acción)**, seleccione **Run automatic speaker test (Ejecutar comprobación automática de altavoz)**.
  - 3.7. Haga clic en **Save (Guardar)**.
4. Configuración de la condición para el envío de un correo electrónico cuando la prueba del altavoz falla:

- 4.1. Vaya a la interfaz del dispositivo > System (Sistema) > Events (Eventos) > Rules (Reglas).
- 4.2. Haga clic en Add a rule (Agregar una regla).
- 4.3. Introduzca un nombre para la regla.
- 4.4. En Condition (Condición), seleccione Speaker test result (Resultado de la comprobación del altavoz).
- 4.5. En Speaker test status (Estado de prueba del altavoz), seleccione Didn't pass the test (No ha pasado la comprobación).
- 4.6. En Action (Acción), seleccione Send notification to email (Enviar notificación por correo electrónico).
- 4.7. En Recipient (Destinatario), seleccione su destinatario ("Destinatarios de prueba de altavoz").
- 4.8. Introduzca un asunto y un mensaje y haga clic en Save (Guardar).


### Reproducir clip personalizado al activar una alarma

Este ejemplo ilustra cómo activar un archivo de audio personalizado cuando cambia la señal de entrada digital.

Subir un archivo de audio:

1. Vaya a Media (Medios) y haga clic en  Add (Añadir).
2. Haga clic para explorar y seleccionar el archivo de audio de su ordenador.
3. Seleccione la Storage location (Ubicación de almacenamiento).
4. Haga clic en Save (Guardar).

Cree un perfil con el archivo de audio:

1. Vaya a Profiles (Perfiles) y haga clic en  Create (Crear).
2. Introduzca Name (Nombre) y seleccione el patrón de luz para el perfil.
3. En la sección de la sirena, seleccione el archivo de audio cargado.
4. Seleccione Intensity (Intensidad) y Duration (Duración).
5. Haga clic en Save (Guardar).

Configure la entrada de dirección para el puerto:

1. Vaya a System (Sistema) > Accessories (Accesorios) > I/O ports (Puertos de E/S).
2. Vaya a Port 1 (Puerto 1) > Normal state (Estado normal) y haga clic en Circuit closed (Circuito cerrado).


Crear una regla:

1. Vaya a System (Sistema) > Events (Eventos) y agregue una regla.
2. Introduzca un nombre para la regla.
3. En la lista de condiciones, seleccione I/O (E/S) > Digital input is active (La entrada digital está activa).
4. Seleccione Port 1 (Puerto 1).
5. En la lista de acciones, seleccione Run light and siren profile while the rule is active (Ejecutar perfil de luz y sirena mientras la regla esté activa).
6. Seleccione el perfil con el archivo de audio cargado.
7. Haga clic en Save (Guardar).

### Detener audio con DTMF

En este ejemplo se explica cómo:

- Configurar DTMF en un dispositivo.


- Configure un evento para que detenga el audio cuando se envíe un comando DTMF al dispositivo.
1. Vaya a **Settings (Ajustes) > SIP > SIP settings (Ajustes SIP)**.
  2. Asegúrese de que **Enable SIP (Activar SIP)** esté encendido.  
Si tiene que activarlo, recuerde hacer clic en **Save (Guardar)** después.
  3. Vaya a **SIP accounts (Cuentas SIP)**.
  4. Junto a la cuenta SIP, haga clic en  > **Edit (Editar)**.
  5. En **DTMF**, haga clic en **+ DTMF sequence (Secuencia DTMF)**.
  6. En **Sequence (Secuencia)**, introduzca "1".
  7. En **Description (Descripción)**, introduzca "detener audio".
  8. Haga clic en **Save (Guardar)**.
  9. Vaya a **System (Sistema) > Events (Eventos) > Rules (Reglas)** y haga clic en **+ Add a rule (Agregar una regla)**.
  10. En **Name (Nombre)**, introduzca "Detener audio DTMF".
  11. En **Condition (Condición)**, seleccione **DTMF**.
  12. En **DTMF Event ID (Identificación evento)**, seleccione **stop audio (detener audio)**.
  13. En **Action (Acción)**, seleccione **Stop playing audio clip (Detener reproducción de fragmento de audio)**.
  14. Haga clic en **Save (Guardar)**.

### Configuración de audio para llamadas SIP entrantes

Puede configurar una regla para que se reproduzca un clip de audio cuando reciba una llamada SIP.

También puede configurar una regla adicional que responda automáticamente a la llamada SIP cuando haya finalizado el clip de audio. Esto puede resultar útil en casos en los que el operador de la alarma quiera llamar la atención de alguien cercano a un dispositivo de audio y establecer una línea de comunicación. Para ello, realiza una llamada SIP al dispositivo de audio, que reproducirá un clip de audio para avisar a las personas cercanas al dispositivo de audio. Cuando se haya detenido la reproducción del clip de audio, el dispositivo de audio responde automáticamente a la llamada SIP y se puede realizar la comunicación entre el operador de la alarma y las personas cercanas al dispositivo de audio.

Habilitar ajustes SIP:

1. vaya a la interfaz del altavoz introduciendo su dirección IP en un navegador web.
2. Vaya a **System (Sistema) > SIP > SIP settings (Ajustes SIP)** y seleccione **Enable SIP (Habilitar SIP)**.
3. Para permitir que el dispositivo reciba llamadas entrantes, seleccione **Allow incoming calls (Permitir llamadas entrantes)**.
4. Haga clic en **Save (Guardar)**.
5. Vaya a **SIP accounts (Cuentas SIP)**.
6. Junto a la cuenta SIP, haga clic en  > **Edit (Editar)**.
7. Desmarque **Answer automatically (Responder automáticamente)**.

Reproducción de audio cuando se recibe una llamada SIP:

1. Vaya a **Settings > System > Events > Rules (Ajustes > Sistema > Eventos > Reglas)** y añada una regla.
2. Escriba un nombre para la regla.
3. En la lista de condiciones, seleccione **State (Estado)**.
4. En la lista de estados, seleccione **Ringling (Sonando)**.
5. En la lista de acciones, seleccione **Play audio clip (Reproducir clip de audio)**.
6. En la lista de clips, seleccione el clip de audio que desee reproducir.

7. Seleccione cuántas veces desea repetir el clip de audio. 0 significa "reproducir una vez".
8. Haga clic en **Save (Guardar)**.

Conteste a la llamada SIP automáticamente después de que el clip de audio haya finalizado:

1. Vaya a **Settings > System > Events > Rules (Ajustes > Sistema > Eventos > Reglas)** y añada una regla.
2. Escriba un nombre para la regla.
3. En la lista de condiciones, seleccione **Audio clip playing (Reproducir clip de audio)**.
4. Compruebe **Use this condition as a trigger (Utilizar esta condición como activador)**.
5. Compruebe **Invert this condition (Invertir esta condición)**.
6. Haga clic en **+ Add a condition (+ Agregar una condición)** para agregar una segunda condición al evento.
7. En la lista de condiciones, seleccione **State (Estado)**.
8. En la lista de estados, seleccione **Ringling (Sonando)**.
9. En la lista de acciones, seleccione **Answer call (Responder llamada)**.
10. Haga clic en **Save (Guardar)**.

## Interfaz web

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

## Descubrir más

### Protocolo de inicio de sesión (SIP)

El protocolo de inicio de sesión (SIP) se utiliza para configurar, mantener y terminar llamadas VoIP. Puede realizar llamadas entre dos o más partes, denominadas agentes de usuario SIP. Para realizar una llamada SIP, puede utilizar, por ejemplo, teléfonos SIP, softphones o dispositivos Axis habilitados para SIP.

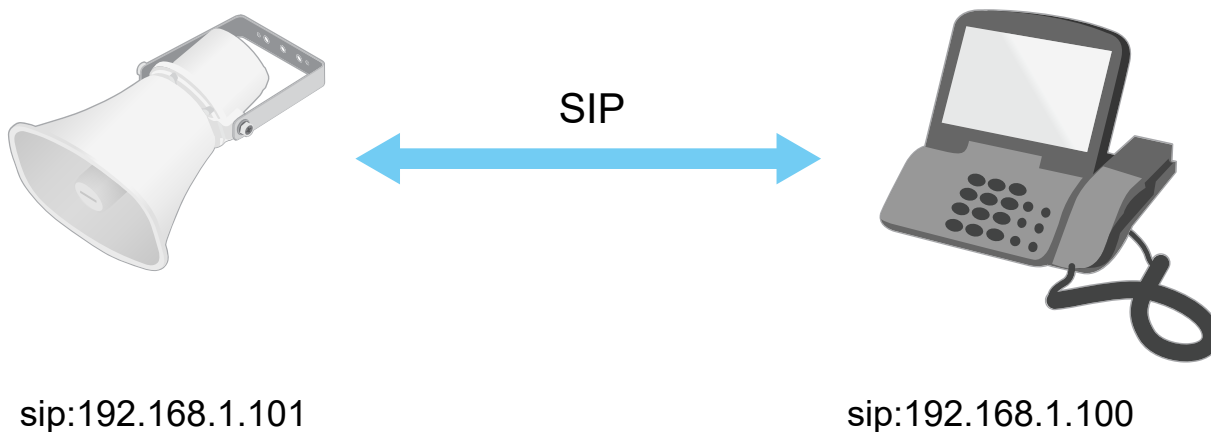
El audio o el vídeo real se intercambian entre los agentes de usuario SIP con un protocolo de transporte, por ejemplo, RTP (protocolo de transporte en tiempo real).

Puede realizar llamadas en redes locales mediante una configuración de punto a punto o a través de redes mediante un servidor PBX.

#### Peer-to-peer SIP (SIP de punto a punto):

El tipo más básico de comunicación SIP tiene lugar directamente entre dos o más agentes de usuario SIP. Esto se denomina SIP de punto a punto (P2PSIP). Si tiene lugar en una red local, solo se necesitan las direcciones SIP de los agentes de usuario. En este caso, una dirección SIP típica sería `sip:<local-ip>`.

Ejemplo:



Puede configurar un teléfono habilitado para SIP para llamar a un dispositivo de audio en la misma red mediante una configuración de SIP de punto a punto.

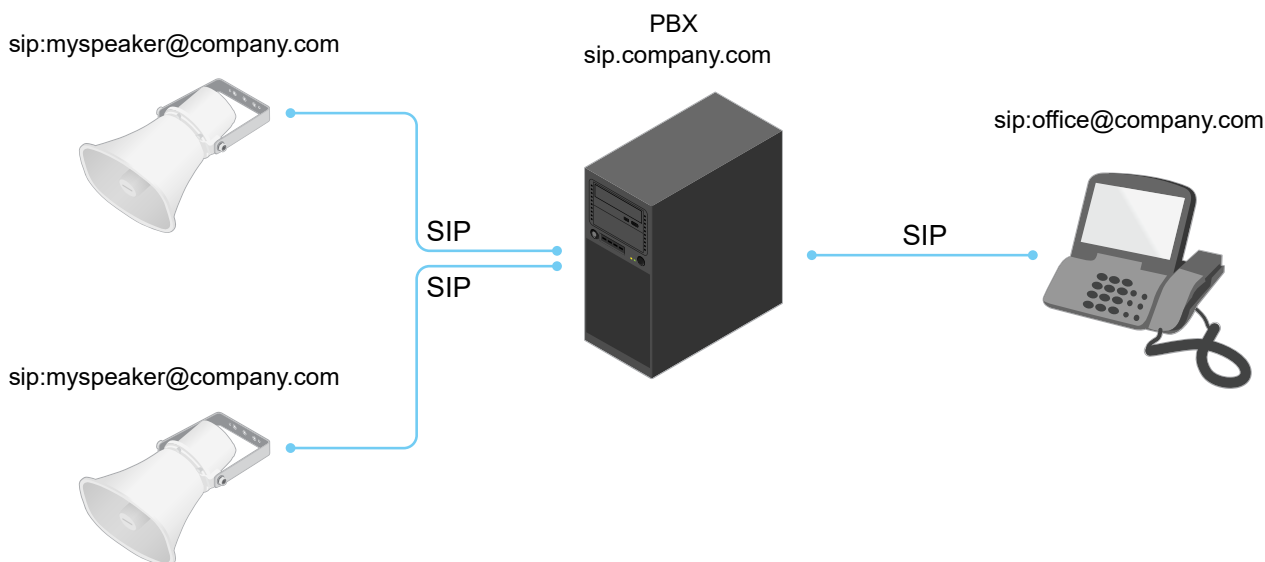
### Centralita telefónica privada (PBX)

Cuando realiza llamadas SIP fuera de su red IP local, un cambio de Centralita telefónica privada (PBX) puede actuar como un hub central. El componente principal de una Centralita Telefónica Privada es un servidor SIP, que también se conoce como proxy SIP o registrador. Un PBX funciona como una centralita tradicional, que muestra el estado actual del cliente y permite, por ejemplo, las transferencias de llamadas, el correo de voz y las redirecciones.

El servidor SIP de PBX puede configurarse como una entidad local o fuera de la instalación. Puede estar alojado en una intranet o en un proveedor de servicios externo. Cuando realiza llamadas SIP entre redes, las llamadas se dirigen a través de un conjunto de PBX, que consultan la ubicación de la dirección SIP a la que se dirige.

Cada agente de usuario SIP se registra en el PBX y, a continuación, puede llegar a los demás marcando la extensión correcta. En este caso, una dirección SIP típica sería `sip:<user>@<domain>` o `sip:<user>@<registrar-ip>`. La dirección SIP es independiente de su dirección IP y el PBX permite el acceso al dispositivo siempre que esté registrado en el PBX.

Ejemplo:



### NAT transversal

Utilice NAT (traducción de direcciones de red) transversal cuando el dispositivo de Axis se encuentra en una red privada (LAN) y desee acceder desde fuera de la red.

#### Nota

El router debe ser compatible con NAT transversal y UPnP®.

Cada protocolo de recorrido de NAT puede utilizarse por separado o en diferentes combinaciones, en función del entorno de red.

- **ICE** El protocolo ICE (Interactive Connectivity Establishment) aumenta las posibilidades de encontrar la ruta más eficiente para una correcta comunicación entre dispositivos de punto de acceso. Si habilita también STUN y TURN, mejora las posibilidades del protocolo ICE.
- **STUN** - STUN (Session Traversal Utilities for NAT) es un protocolo de red servidor-cliente que permite que el dispositivo de Axis determine si está situado detrás de un NAT o un firewall y, en tal caso, obtener la asignación de una dirección IP pública y un número de puerto asignado para conexiones a hosts remotos. Introduzca la dirección del servidor STUN, por ejemplo, una dirección IP.
- **TURN** - TURN (Traversal Using Relays around NAT) es un protocolo que permite que un dispositivo detrás de un router NAT o un firewall reciba datos de entrada desde otros hosts a través de TCP o UDP. Introduzca la dirección del servidor TURN y la información de inicio de sesión.

### Analíticas y aplicaciones

Las analíticas y aplicaciones permiten sacar el máximo partido a su dispositivo Axis. AXIS Camera Application Platform (ACAP) es una plataforma abierta que permite a terceros desarrollar analíticas y otras apps para dispositivos Axis. Las apps pueden preinstalarse en el dispositivo, pueden descargarse de forma gratuita o por un precio de licencia.

Para encontrar los manuales de usuario de analíticas y apps de Axis, visite [help.axis.com](http://help.axis.com).

### AXIS Audio Analytics

AXIS Audio Analytics detecta un aumento repentino del volumen del sonido y tipos específicos de sonidos como chillidos o gritos dentro del intervalo de dispositivos en los que se ha instalado. Estas detecciones se pueden configurar para desencadenar una respuesta, por ejemplo, grabación de vídeo, reproducción de un mensaje de audio o aviso al personal de seguridad. Para obtener más información sobre cómo funciona la aplicación, consulte el *manual de usuario de AXIS Audio Analytics*.

### InformaCast®

InformaCast es una plataforma que permite enviar mensajes de emergencia y comunicarse a través de los canales de comunicación que su organización ya tiene implementados, incluyendo los altavoces de red Axis. El sistema de notificación masiva InformaCast emite alertas de audio intrusivas en todas sus instalaciones. Para obtener más información sobre la Aplicación, consulte *AXIS Speaker Functionality for Singlewire InformaCast*.

### Ciberseguridad

Para obtener información específica sobre ciberseguridad, consulte la ficha técnica del producto en [axis.com](http://axis.com).

Para obtener información detallada sobre ciberseguridad en AXIS OS, lea la *Guía de endurecimiento de AXIS OS*.

### Servicio de notificación de seguridad de Axis

Axis ofrece un servicio de notificación con información sobre vulnerabilidad y otros asuntos relacionados con la seguridad de los dispositivos Axis. Para recibir notificaciones, puede suscribirse en [axis.com/security-notification-service](http://axis.com/security-notification-service).

### Gestión de las vulnerabilidades

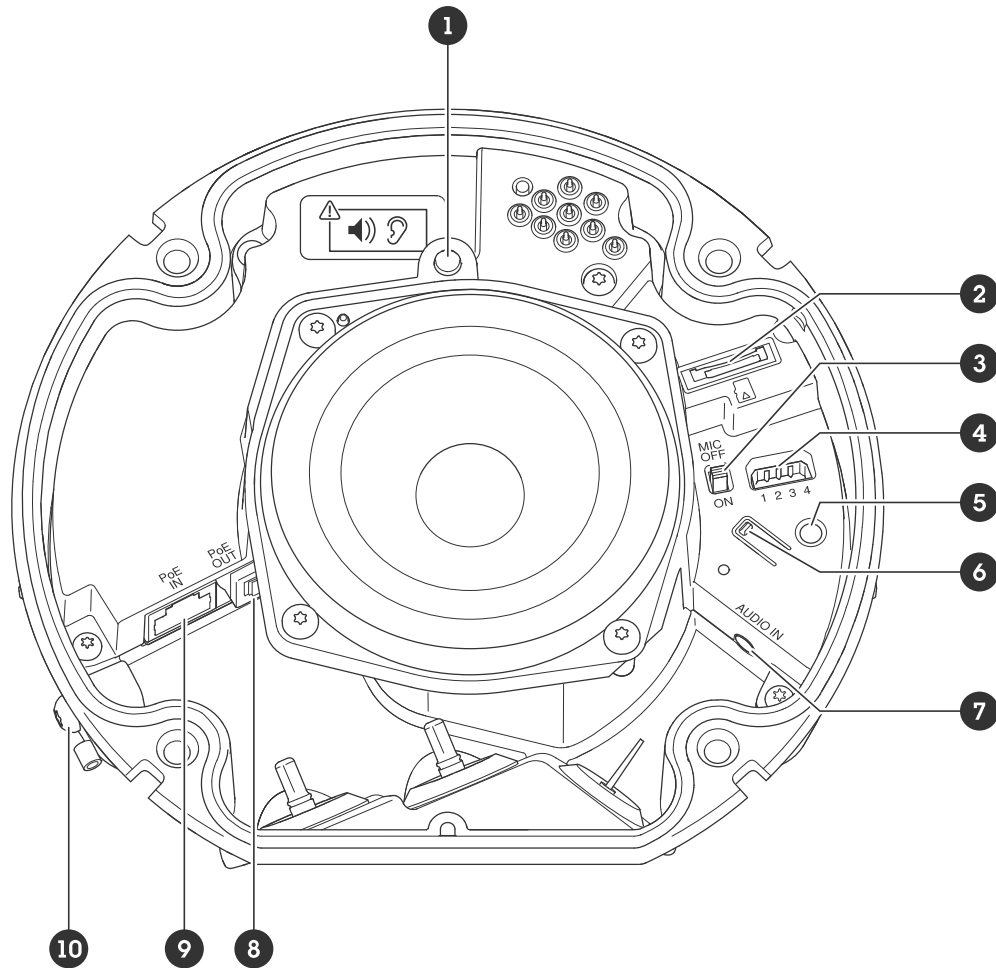
Para minimizar el riesgo de exposición de los clientes, Axis, como **autoridad de numeración común (CNA) de vulnerabilidades y exposiciones comunes (CVE)**, sigue los estándares del sector para gestionar y responder a las vulnerabilidades detectadas en nuestros dispositivos, software y servicios. Para obtener más información sobre la política de gestión de vulnerabilidades de Axis, cómo informar de vulnerabilidades, vulnerabilidades ya detectadas y los correspondientes avisos de seguridad, consulte [axis.com/vulnerability-management](http://axis.com/vulnerability-management).

### Funcionamiento seguro de dispositivos Axis

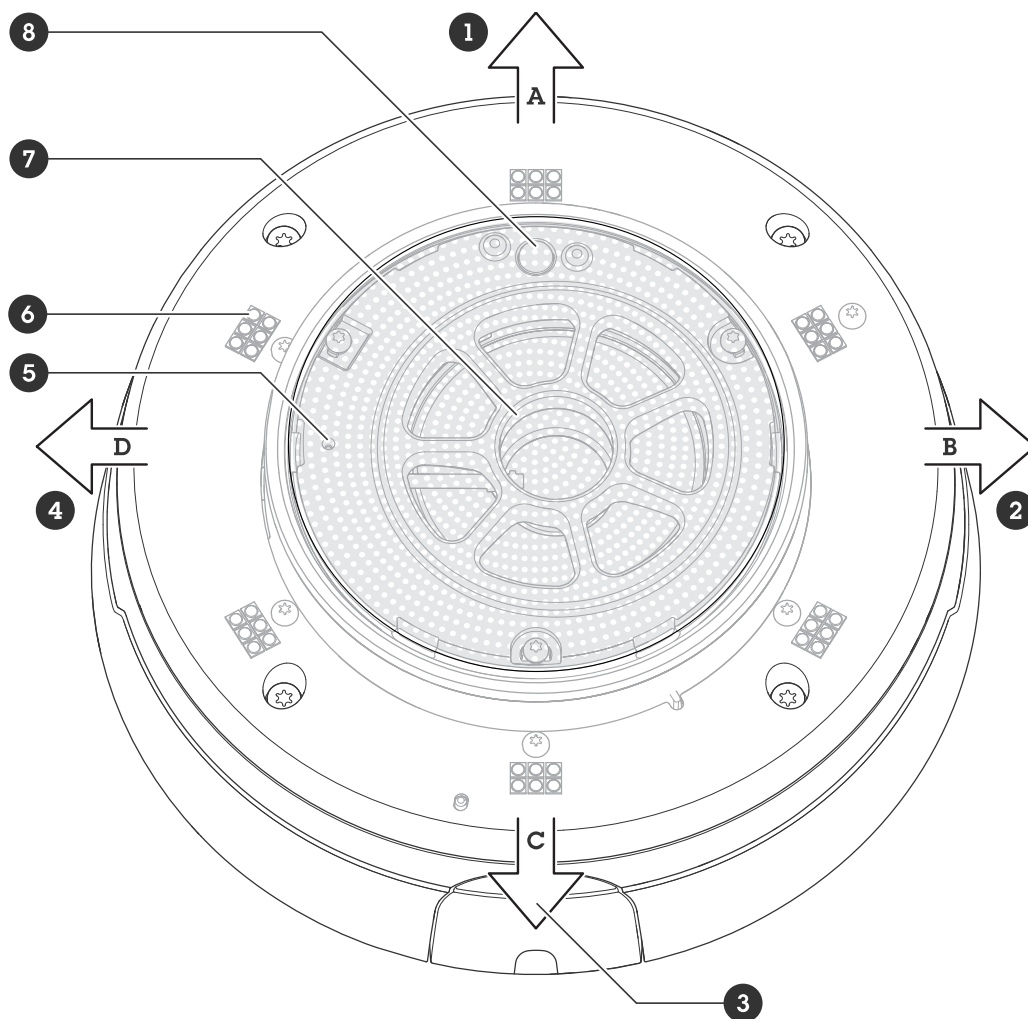
Los dispositivos de Axis con ajustes predeterminados de fábrica se configuran previamente con mecanismos de protección predeterminados seguros. Recomendamos utilizar más configuración de seguridad al instalar el dispositivo. Para conocer mejor el enfoque de Axis en materia de ciberseguridad, incluidas las buenas prácticas, los recursos y las directrices para la protección de sus dispositivos, vaya a [axis.com/about-axis/cybersecurity](http://axis.com/about-axis/cybersecurity).

## Especificaciones

## Guía de productos



- 1 LED de audio
- 2 Ranura para tarjeta microSD
- 3 Interruptor del micrófono
- 4 Conector de E/S
- 5 Indicador LED de estado
- 6 Botón de control
- 7 Conector de audio
- 8 Conector de red (PoE OUT)
- 9 Conector de red (PoE IN)
- 10 Tornillo de toma de tierra



- 1 Dirección de la luz A
- 2 Dirección de la luz B
- 3 Dirección de la luz C
- 4 Dirección de la luz D
- 5 Micrófono interno
- 6 LED de señalización
- 7 Altavoz
- 8 LED de audio

**Indicadores LED**

LED de estado	Indicación
Apagado	Conexión y funcionamiento normal.
Verde	Se muestra fijo durante diez segundos para indicar un funcionamiento normal después de completar el inicio.
Ámbar	Fijo durante el inicio, durante el restablecimiento de los ajustes predeterminados de fábrica o al restablecer la configuración.

## Ranura para tarjeta SD

### AVISO

- Riesgo de daños en la tarjeta SD. No emplee herramientas afiladas, objetos de metal ni demasiada fuerza al insertar o extraer la tarjeta SD. Utilice los dedos para insertar o extraer la tarjeta.
- Riesgo de pérdida de datos y grabaciones dañadas. Desmonte la tarjeta SD desde la interfaz web del dispositivo antes de retirarla. No extraiga la tarjeta SD mientras el producto esté en funcionamiento.

Para conocer las recomendaciones sobre tarjetas SD, consulte [axis.com](http://axis.com).



Los logotipos de microSD, microSDHC y microSDXC son marcas comerciales de SD-3C LLC. microSD, microSDHC, microSDXC son marcas comerciales o marcas comerciales registradas de SD-3C, LLC en Estados Unidos, en otros países o en ambos.

## Botones

### Botón de control

El botón de control se utiliza para lo siguiente:

- Calibrar la comprobación del altavoz. Pulse y suelte el botón de control y se reproducirá un tono de prueba.
- Restablecer el producto a la configuración predeterminada de fábrica. Vea *Restablecimiento a la configuración predeterminada de fábrica*, on page 32.
- Conectarse a un servicio de conexión a la nube (O3C) de un solo clic a través de Internet. Para conectarse, presione y suelte el botón y espere a que el LED de estado parpadee tres veces en verde.

### Interruptor del micrófono

Consulte *Guía de productos*, on page 25 para conocer la ubicación del interruptor del micrófono.

El interruptor del micrófono se utiliza mecánicamente para **ON (encender)** u **OFF (apagar)** el micrófono. La configuración predeterminada de fábrica de este interruptor es **ON (encendido)**.

## Conectores

### Conector de red

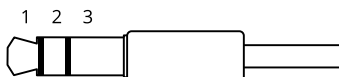
Conector Ethernet RJ45 con alimentación a través de Ethernet (PoE).

### AVISO

El dispositivo se conectará mediante un cable de red blindado (STP). Todos los cables que conectan el dispositivo a la red deben estar destinados a su uso específico. Asegúrese de que los dispositivos de red estén instalados conforme a las instrucciones del fabricante. Para obtener más información sobre los requisitos normativos, consulte la guía de instalación, disponible en [www.axis.com](http://www.axis.com).

### Conector de audio

- **Entrada de audio:** Entrada de 3,5 mm para micrófono digital, micrófono analógico mono, o entrada de línea de señal mono (se usa el canal izquierdo de una señal estéreo).



Entrada de audio

1 Punta	2 Anillo	3 Manguito
Micrófono no balanceado (con o sin alimentación de electret) o entrada de línea	Alimentación de electret si está seleccionada	Masa
Señal digital	Transformador de corriente si está seleccionado	Masa

**Nota**

La longitud máxima del cable conectado es de 30 m (98,4 pies).

**Conector de E/S**

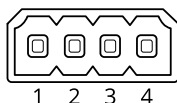
Utilice el conector de E/S con dispositivos externos en combinación con detección de movimiento, activación de eventos y notificaciones de alarma, por ejemplo. Además del punto de referencia de 0 V CC y la alimentación (salida de CC de 12 V), el conector de E/S ofrece una interfaz para:


**Entrada digital** – Conectar dispositivos que puedan alternar entre circuitos cerrados y abiertos, por ejemplo, sensores PIR, contactos de puertas y ventanas o detectores de cristales rotos.

**Entrada supervisada** – Permite detectar la manipulación de una señal digital.

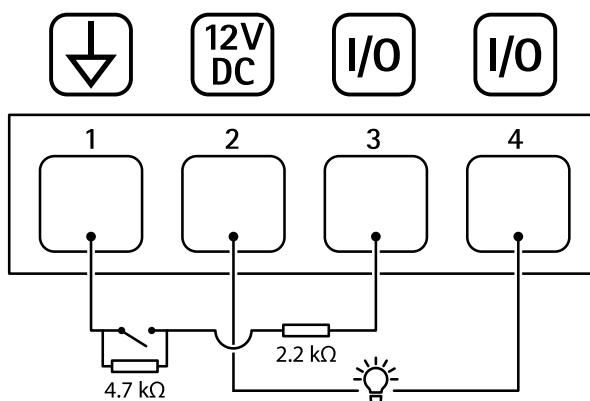
**Salida digital** – Conectar dispositivos externos como relés y LED. Los dispositivos conectados se pueden activar mediante la interfaz de programación de aplicaciones VAPIX®, mediante un evento o desde la interfaz web del dispositivo.

Bloque de terminales de 4 pines



Función	Pin	Notas	Especificaciones
Tierra CC	1		0 V CC
Salida de CC	2	 Se puede utilizar para alimentar equipos auxiliares. Nota: Este pin solo se puede utilizar como salida de alimentación.	12 V CC Carga máx.: 50 mA
Configurable (entrada o salida)	3-4	Entrada digital o entrada supervisada: conéctela al pin 1 para activarla, o bien déjela suelta (sin conectar) para desactivarla. Para usar la entrada supervisada, instale las resistencias de final de línea. Consulte el diagrama de conexiones para obtener información sobre cómo conectar las resistencias.	De 0 a 30 V CC máx.
		Salida digital: conectada internamente a pin 1 (tierra CC) cuando está activa, y suelta (desconectada) cuando está inactiva. Si se utiliza con una carga inductiva, por ejemplo, un relé, conecte un diodo en paralelo a la carga como protección contra transitorios de tensión.	De 0 a 30 V CC máx., colector abierto, 100 mA

**Ejemplo:**



- 1 Tierra CC
- 2 Salida de CC 12 V, 50 mA máx.
- 3 E/S configurada como entrada supervisada
- 4 E/S configurada como salida

**Nota**

La longitud máxima del cable conectado es de 30 m (98,4 pies).

**Nombres de patrones de luz**

Apagado
Fijo
Alternativo
Impulso
Escalar 3 pasos
Parpadeo
Parpadeo 3 veces
Parpadeo 4 veces
Parpadeo 3 veces atenuación
Parpadeo 4 veces atenuación
Parpadeo 1 vez
Parpadeo 3 veces
Dirección A
Dirección B
Dirección C
Dirección D
Rotate (Girar)
Aleatorio
Giro

## Nombres de los patrones de sonido

Alarma: Tono alto de alarma
Alarma: Tono bajo de alarma
Alarma: Ave
Alarma: Cuerno de barco
Alarma: Alarma de coche
Alarma: Alarma de coche rápida
Alarma: Reloj clásico
Alarma: Primer asistente
Alarma: Terror
Alarma: Industria
Alarma: Sonido único
Alarma: Sonido cuádruple suave
Alarma: Sonido triple suave
Alarma: Tono alto triple
Notificación: Aceptado
Notificación: Llamando
Notificación: Denegado
Notificación: Listo
Notificación: Entrada
Notificación: Error
Notificación: Prisa
Notificación: Mensaje
Notificación: Siguiendo
Notificación: Abierto
Siren (Sirena): Alternativo
Siren (Sirena): Bullicioso
Siren (Sirena): Evacuación
Siren (Sirena): Tono descendente
Siren (Sirena): Inicio suave

## Limpie su dispositivo

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

### **AVISO**

- Los productos químicos agresivos pueden dañar el dispositivo. No utilice productos químicos como un limpiacristales o acetona para limpiar el dispositivo.
  - No rocíe detergente directamente sobre el dispositivo. En su lugar, rocíe detergente sobre un paño no abrasivo y úselo para limpiar el dispositivo.
  - Evite limpiar en contacto directo con la luz o a temperaturas elevadas, ya que puede provocar manchas.
1. Utilice un aerosol de aire comprimido para quitar el polvo y la suciedad suelta del dispositivo.
  2. Si es necesario, limpie el dispositivo con un paño de microfibra suave humedecido con agua tibia y jabón suave y no abrasivo.
  3. Para evitar que queden manchas, seque el dispositivo con un paño limpio y no abrasivo.

## Localización de problemas

### Restablecimiento a la configuración predeterminada de fábrica

#### Importante

Es preciso tener cuidado si se va a restablecer la configuración predeterminada de fábrica. Todos los valores, incluida la dirección IP, se restablecerán a la configuración predeterminada de fábrica.

Para restablecer el producto a la configuración predeterminada de fábrica:

1. Desconecte la alimentación del producto.
2. Mantenga pulsado el botón de control mientras vuelve a conectar la alimentación. Vea *Guía de productos*, on page 25.
3. Mantenga pulsado el botón de control durante 10 segundos hasta que el indicador LED de estado se ponga en ámbar por segunda vez.
4. Suelte el botón de control. El proceso finalizará cuando el indicador LED de estado se ilumine en color verde. Si no hay ningún servidor DHCP disponible en la red, la dirección IP del dispositivo adoptará de forma predeterminada una de las siguientes:
  - **Dispositivos con AXIS OS 12.0 y posterior:** Obtenido de la subred de dirección de enlace local (169.254.0.0/16)
  - **Dispositivos con AXIS OS 11.11 y anterior:** 192.168.0.90/24
5. Utilice las herramientas del software de instalación y gestión para asignar una dirección IP, configurar la contraseña y acceder al producto.

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

### Opciones de AXIS OS

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

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

### Comprobar la versión de AXIS OS

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

Para comprobar la versión de AXIS OS:

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

## Actualización de AXIS OS

### Importante

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

### Nota

- Al actualizar el dispositivo con el AXIS OS más reciente en la pista activa, el producto obtiene las últimas funciones disponibles. Lea siempre las instrucciones de actualización y las notas de versión disponibles en cada nueva versión antes de la actualización. Para encontrar el AXIS OS y las notas de versión más recientes, consulte [axis.com/support/device-software](http://axis.com/support/device-software).
1. Descargue en su ordenador el archivo de AXIS OS, disponible de forma gratuita en [axis.com/support/device-software](http://axis.com/support/device-software).
  2. Inicie sesión en el dispositivo como administrador.
  3. Vaya a **Maintenance > AXIS OS upgrade (mantenimiento > actualización de AXIS OS)** y haga clic en **Upgrade (actualizar)**.

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

## Problemas técnicos y posibles soluciones

### Problemas para actualizar AXIS OS

#### Error en la actualización de AXIS OS

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

#### Problemas tras la actualización de AXIS OS

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

### Problemas al configurar la dirección IP

#### No se puede configurar la dirección IP

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

#### Problemas de acceso al dispositivo

##### No puede iniciar sesión accediendo al dispositivo desde un navegador

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

Si ha olvidado la contraseña de la cuenta de administrador, deberá restablecer el dispositivo a la configuración de fábrica. Para consultar las instrucciones, vea *Restablecimiento a la configuración predeterminada de fábrica, on page 32*.

##### El servidor DHCP ha cambiado la dirección IP

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

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

##### Error de certificado cuando se utiliza IEEE 802.1X

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

##### El navegador no es compatible

Para obtener una lista de los navegadores recomendados, consulte *Compatibilidad con navegadores, on page 6*.

**No se puede acceder externamente al dispositivo.**

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

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

Para obtener instrucciones y descargas, vaya a [axis.com/vms](http://axis.com/vms).

**Problemas con archivos de audio**

**No se puede subir el clip de medios**

Los siguientes formatos de clip de audio son compatibles:

- formato de archivo AU, codificado en Ley  $\mu$  y muestreado con 8 o 16 kHz.
- formato de archivo WAV, codificado en audio PCM. Es compatible con la codificación como mono o estéreo de 8 o 16 bits y frecuencia de muestreo de 8 a 48 kHz.
- Formato de archivo MP3, en mono o estéreo con velocidad de bits de 64 kbps a 320 kbps y frecuencia de muestreo de 8 a 48 kHz.

**Los clips de medios se reproducen con diferentes volúmenes**

Un archivo de sonido se graba con una ganancia determinada. Si sus clips de audio se han creado con ganancias diferentes, se reproducirán con un sonido diferente. Asegúrese de utilizar clips con la misma ganancia.

**Problemas con MQTT**

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

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

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

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

**Problemas con el funcionamiento del dispositivo**

**El calefactor delantero y el limpiaparabrisas no funcionan**

Si el calefactor delantero o el limpiaparabrisas no se encienden, compruebe que la cubierta superior esté correctamente fijada a la parte inferior de la unidad de alojamiento.

Si no encuentra aquí lo que busca, pruebe a visitar la sección de solución de problemas en [axis.com/support](http://axis.com/support).

Problemas con el sonido	
-------------------------	--

El dispositivo no está tan alto como se esperaba	Compruebe que el dispositivo esté cerrado correctamente y que no haya obstrucciones en el altavoz exponencial ni en los elementos del altavoz.
--	--

Problemas con la luz	
----------------------	--

El dispositivo no está tan brillante como se esperaba	Compruebe que se esté utilizando una fuente de alimentación de Clase de PoE 4. Compruebe la temperatura ambiente del dispositivo. Si el dispositivo se instala en un entorno de alta temperatura, las luces se atenuarán automáticamente.
---	--

## Consideraciones sobre el rendimiento

A la hora de configurar su sistema, es importante considerar cómo las distintas configuraciones y situaciones afectan al ancho de banda (velocidad de bits) requerido.

Los factores más importantes a tener en cuenta son:

- Un uso denso de la red debido a una infraestructura deficiente afecta al ancho de banda.
- La ejecución simultánea de varias aplicaciones de AXIS Camera Application Platform (ACAP) puede afectar al rendimiento en general.

## Contactar con la asistencia técnica

Si necesita más ayuda, vaya a [axis.com/support](http://axis.com/support).



T10217687\_es

2026-02 (M5.2)

© 2025 – 2026 Axis Communications AB