AXIS C1410 Mk II Network Mini Speaker

Manual del usuario

Índice

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*.

Una descripción general de cómo funciona el audio en red.

Instalación

Cómo funciona

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*.

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 todos los controles y opciones de la interfaz web del dispositivo, consulte *Interfaz web, on page 14*.

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 65*.

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 65*.
   Después de un restablecimiento, el inicio seguro garantiza el estado del dispositivo.
2. Configure e instale el dispositivo.

Información general de la interfaz web

Este vídeo le ofrece información general de la interfaz web del dispositivo.

Interfaz web del dispositivo Axis

Configure su dispositivo

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 62* para identificar el botón de control.

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 58*.

Para más información sobre las opciones de ajustes, consulte *SIP, on page 45*.

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 59*.

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 58*.

Para más información sobre las opciones de ajustes, consulte *SIP, on page 45*.

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.

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)*.

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. Nómbrelo "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 audio cuando una cámara detecta movimiento

En este ejemplo se explica cómo configurar el dispositivo de audio para reproducir un clip de audio cuando una cámara de red Axis detecta movimiento.

Requisitos

- El dispositivo de audio Axis y la cámara de red Axis se encuentran en la misma red.
- La aplicación de detección de movimiento está configurada y en funcionamiento en la cámara.

1. Preparar un enlace al clip de audio:
   1.1. Vaya a **Audio** > **Audio clips (Audio > Clips de audio)**.
   1.2. Haga clic en ⋮ > **Create link (Crear enlace)** en un clip de audio.
   1.3. Configure el volumen y el número de veces que se debe repetir el clip.
   1.4. Haga clic en el icono de copia para copiar el enlace.
2. Cree una regla de acción:
   2.1. Vaya a **Settings (Ajustes)** > **Events (Eventos)** > **Recipients (Destinatarios)**.
   2.2. Haga clic en **+ Add recipient (+ Agregar destinatario)**.
   2.3. Escriba un nombre para el destinatario, por ejemplo, "Altavoz".
   2.4. Seleccione **HTTP** en la lista desplegable **Type (Tipo)**.
   2.5. Pegue el enlace configurado desde el dispositivo de audio en el campo **URL**.
   2.6. Introduzca el nombre de usuario y la contraseña del dispositivo de audio.
   2.7. Haga clic en **Save (Guardar)**.
   2.8. Vaya a **Rules (Reglas)** y haga clic en **+ Add a rule (+ Agregar una regla.**
   2.9. Introduzca un nombre para la regla de acción, por ejemplo, "Reproducir clip".
   2.10. En la lista **Condition (Condición)**, seleccione una alternativa de detección de movimiento en el vídeo en **Applications (Aplicaciones)**.

   Nota

   Si no hay opciones para la detección de movimiento en el vídeo, vaya a **Apps (Aplicaciones)**, haga clic en **AXIS Video Motion Detection** y active la detección de movimiento.

   2.11. En la lista **Action (Acción)**, seleccione **Send notification through HTTP (Enviar notificación a través de HTTP)**.
   2.12. En **Recipient (Destinatario)**, seleccione el destinatario.
   2.13. 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 **Descriptión (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 **Ringing (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 **Ringing (Sonando)**.
9. En la lista de acciones, seleccione **Answer call (Responder llamada)**.
10. Haga clic en **Save (Guardar)**.

Interfaz web

Para acceder a la interfaz web, escriba la dirección IP del dispositivo en un navegador web.

Nota

La compatibilidad con las características y ajustes descrita en esta sección varía entre dispositivos. Este icono  indica que la función o ajuste solo está disponible en algunos dispositivos.

 Mostrar u ocultar el menú principal.

 Acceda a las notas de la versión.

 Acceder a la ayuda del producto.

 Cambiar el idioma.

 Definir un tema claro o un tema oscuro.

 El menú de usuario contiene:

- Información sobre el usuario que ha iniciado sesión.
-  **Cambiar cuenta**: Cierre sesión en la cuenta actual e inicie sesión en una cuenta nueva.
-  **Cerrar sesión**: Cierre sesión en la cuenta actual.

 El menú contextual contiene:

- **Analytics data (Datos de analíticas)**: Puede compartir datos no personales del navegador.
- **Feedback (Comentarios)**: Puede enviarnos comentarios para ayudarnos a mejorar su experiencia de usuario.
- **Legal (Aviso legal)**: Lea información sobre cookies y licencias.
- **About (Acerca de)**: Puede consultar la información del dispositivo, como la versión de AXIS OS y el número de serie.

Estado

Información del sistema de audio

Esta información solo se muestra para dispositivos que pertenecen a un sitio AXIS Audio Manager Edge.

AXIS Audio Manager Edge: Lanzar AXIS Audio Manager Edge.

Localizar dispositivo

Muestra la información de localización del dispositivo, como el número de serie y la dirección IP.

Locate device (Localizar dispositivo): Reproduce un sonido que le ayuda a identificar el altavoz. En algunos productos, parpadea un LED en el dispositivo.

Pruebas con el altavoz

Muestra si el altavoz ha sido calibrado o no.

Comprobación del altavoz: : Calibrar el altavoz. Lo lleva a la página **Comprobación del altavoz** donde puede realizar la calibración y ejecutar la prueba de altavoces.

Información sobre el dispositivo

Muestra información sobre el dispositivo, como la versión del AXIS OS y el número de serie.

Actualización de AXIS OS: Actualizar el software en el dispositivo. Le lleva a la página de mantenimiento donde puede realizar la actualización.

Estado de sincronización de hora

Muestra la información de sincronización de NTP, como si el dispositivo está sincronizado con un servidor NTP y el tiempo que queda hasta la siguiente sincronización.

Configuración de NTP: Ver y actualizar los ajustes de NTP. Le lleva a la página **Time and location (Hora y localización)**, donde puede cambiar los ajustes de NTP.

Seguridad

Muestra qué tipo de acceso al dispositivo está activo y qué protocolos de cifrado están en uso y si se permite el uso de aplicaciones sin firmar. Las recomendaciones para los ajustes se basan en la guía de seguridad del AXIS OS.

Hardening guide (Guía de seguridad): Enlace a la *AXIS OS Hardening guide (guía de refuerzo del sistema operativo AXIS)*, donde encontrará más información sobre ciberseguridad en dispositivos Axis y prácticas recomendadas.

Clientes conectados

Muestra el número de conexiones y clientes conectados.

View details (Ver detalles): Consulte y actualice la lista de clientes conectados. La lista muestra la dirección IP, el protocolo, el puerto, el estado y PID/proceso de cada conexión.

Grabaciones en curso

Muestra las grabaciones en curso y el espacio de almacenamiento designado.

Grabaciones: Consulte las grabaciones en curso y filtradas y la fuente. Para obtener más información, consulte *Grabaciones, on page 20*

Muestra el espacio de almacenamiento en el que se guarda la grabación.

Analítica

AXIS Audio Analytics

Nivel de presión acústica

Show threshold and events in graph (Mostrar umbral y eventos en el gráfico): Active esta opción para mostrar en el gráfico cuándo se detecta un pico de sonido.

Umbral: Ajuste los valores umbral de detección. La aplicación registrará un evento de audio ante cualquier sonido que supere los valores umbral.

Detección de audio adaptativa

Show events in graph (Mostrar eventos en el gráfico): Active esta opción para mostrar en el gráfico cuándo se detecta un pico de sonido.

Umbral: Mueva el control deslizante para ajustar el umbral de detección. El umbral mínimo registrará incluso picos ligeros de sonido como una detección, mientras que el umbral máximo solo registrará picos significativos de sonido como detección.

Probar alarmas: Haga clic en **Probar** para desencadenar un evento de detección con fines de prueba.

Clasificación de audio

Show events in graph (Mostrar eventos en el gráfico) : Active esta opción para mostrar en el gráfico cuándo se detectó un tipo específico de sonido.

Classifications (Clasificaciones) : Seleccione los tipos de sonido que desea que detecte la aplicación.

Test alarms (Probar alarmas) : Haga clic en **Test (Probar)** para desencadenar un evento de detección ante un sonido específico con fines de prueba.

Audio

AXIS Audio Manager Edge

AXIS Audio Manager Edge: Lance la aplicación.

Seguridad de la instalaciones de audio

Certificado CA: Seleccione el certificado que se utilizará al agregar dispositivos a la instalación de audio. Debe habilitar la autenticación TLS en AXIS Audio Manager Edge.

Save (Guardar): Active y guarde la selección.

Configuración del dispositivo

Entrada: active o desactive la entrada de audio. Muestra el tipo de entrada.

Ganancia: Utilice el control deslizante para cambiar la ganancia. Haga clic en el icono de micrófono para silenciar o activar el audio.

Input type (Tipo de entrada) : Seleccione el tipo de entrada.

Power type (Tipo de alimentación) : Seleccione el tipo de alimentación.

Salida: Muestra el tipo de salida.

Ganancia: Utilice el control deslizante para cambiar la ganancia. Haga clic en el icono de altavoz para silenciar o activar el audio.

Flujo

Codificación: seleccione la codificación que se va a utilizar para el flujo de la fuente de entrada. Solo puede seleccionar la codificación si la entrada de audio está activada. Si la entrada de audio está desactivada, haga clic en **Enable audio input (Habilitar entrada de audio)** para activarla.

Cancelación de eco: Active esta función para eliminar ecos durante la comunicación bidireccional.

Clips de audio

Add clip (Agregar clip): Agregar un nuevo clip de audio. Puede utilizar archivos .au, .mp3, .opus, .vorbis y .wav.

Reproducir el clip de audio.

Detener la reproducción del clip de audio.

El menú contextual contiene:

- **Cambiar nombre**: Cambia el nombre del clip de audio.
- **Crear enlace**: Cree una URL que, cuando se utiliza, reproduce el clip de audio del dispositivo. Especifique el volumen y el número de veces que se debe reproducir el clip.
- **Descargar**: Descargue el clip de audio en el ordenador.
- **Eliminar**: Elimine el clip de audio del dispositivo.

Escuchar y grabar

Haga clic para escuchar.

Inicie una grabación continua del flujo de audio en directo. Vuelva a hacer clic para dejar de grabar. Si hay una grabación en curso, se reanudará automáticamente después de reiniciarse.

Nota

Solo puede escuchar y grabar si la entrada está activada para el dispositivo. Vaya a **Audio > Device settings (Audio > Ajustes del dispositivo)** para asegurarse de activar la entrada.

Muestra el almacenamiento configurado para el dispositivo. Debe haber iniciado sesión como administrador para configurar el almacenamiento.

Pruebas con el altavoz

Puede utilizar la prueba del altavoz para verificar de forma remota que el altavoz funciona como se ha diseñado.

Calibrate (Calibrar): Debe calibrar el altavoz antes de su primera prueba. Durante la calibración, el altavoz reproducirá una serie de tonos de prueba registrados por el micrófono integrado. Al calibrar el altavoz, se debe instalar en su posición final. Si mueve el altavoz más adelante o si su entorno cambia, por ejemplo, si se levanta o se derriba una pared, el altavoz se debe calibrar de nuevo.

Ejecutar la prueba: Reproduzca la misma serie de tonos de prueba que se reprodujeron durante la calibración y compárelos con los valores registrados de la calibración.

Luz

Descripción general

Estado de luz

Muestra las diferentes actividades luminosas que se ejecutan en el dispositivo. Puede disponer de hasta 10 actividades simultáneas en la lista de estado de la luz. Cuando dos o más actividades se ejecutan al mismo tiempo, la actividad que tiene la mayor prioridad muestra el estado de luz. Dicha fila se resaltará de color verde en la lista de estado.

Perfiles

Perfiles

Un perfil es una colección de configuraciones. Puede tener hasta 30 perfiles con diferentes prioridades y patrones. Los perfiles se muestran para ofrecer información general del nombre, la prioridad y los ajustes de la luz y la sirena.

Create (Crear): Haga clic para crear un perfil.

- **Vista previa/Detener vista previa**: Inicie o detenga una vista previa del perfil antes de guardarlo.

Nota

No es posible tener dos perfiles con el mismo nombre.

- **Name (Nombre)**: Introduzca un nombre para el perfil.
- **Descripción**: Introduzca una descripción del perfil.
- **Luz**: Seleccione en el menú desplegable qué tipo de **Pattern (Patrón)**, **Speed (Velocidad)**, **Intensity (Intensidad)** y **Color** de luz desea.
- **Siren (Sirena)**: Seleccione en el menú desplegable qué tipo de **Pattern (Patrón)** e **Intensity (Intensidad)** de sirena desea.
- Inicie o detenga una vista previa se solo la luz o la sirena.
- **Duration (Duración)**: Defina la duración de las actividades.
  - **Continuo**: una vez que se pone en marcha, funciona hasta que se detiene.
  - **Time (Hora)**: Establezca un tiempo determinado para la duración de la actividad.
  - **Repetitions (Repeticiones)**: Defina cuántas veces debe repetirse la actividad.
- **Priority (Prioridad)**: Ajuste la prioridad de una actividad a un número entre 1 y 10. Las actividades con un número de prioridad superior a 10 no pueden eliminarse de la lista de estado. Hay tres actividades con prioridad mayor que 10: **Maintenance (Mantenimiento)** (11), **Identify (Identificación)** (12) y **Health check (Control de estado)** (13).

Import (Importar): Agregue uno o más perfiles con configuración predefinida.

- **Add (Agregar)** : Agregue nuevos perfiles.
- **Delete and add (Eliminar y agregar)** : Se eliminan los perfiles antiguos y se pueden cargar perfiles nuevos.
- **Overwrite (Sobrescritura)**: Los perfiles actualizados sobrescriben los perfiles existentes.

Para copiar un perfil y guardarlo en otros dispositivos, seleccione uno o más perfiles y haga clic en **Export (Exportar)**. Se exporta un archivo .json.

Iniciar un perfil. El perfil y sus actividades aparecen en la lista de estados.

Elija **Edit (Editar)**, **Copy (Copiar)**, **Export (Exportar)** o **Delete (Eliminar)** el perfil.

Grabaciones

Haga clic para filtrar las grabaciones.

Desde: Mostrar grabaciones realizadas después de un determinado punto del tiempo.

Hasta: Mostrar grabaciones hasta un momento determinado.

Fuente: Mostrar grabaciones según la fuente. La fuente hace referencia al sensor.

Evento: Mostrar grabaciones en función de eventos.

Almacenamiento: Mostrar grabaciones según el tipo de almacenamiento.

Ongoing recordings (Grabaciones en curso): Muestra todas las grabaciones en curso en la cámara.

Inicia una grabación en el dispositivo.

Elija en qué dispositivo de almacenamiento guardar la grabación.

Detener una grabación en el dispositivo.

Las grabaciones activadas finalizarán cuando se detengan manualmente o cuando se apague el dispositivo.

Las **grabaciones continuas** seguirán hasta que se detengan manualmente. Aunque el aparato se apague, la grabación continuará cuando vuelva a encenderse.

Reproduzca la grabación.

Deje de reproducir la grabación.

Muestre u oculte información y opciones sobre la grabación.

Definir intervalo de exportación: si solo desea exportar parte de la grabación, introduzca un intervalo horario. Tenga en cuenta que si trabaja en una zona horaria distinta a la ubicación del dispositivo, el intervalo de tiempo se basa en la zona horaria del dispositivo.

Encrypt (Cifrar): Seleccione esta opción para definir una contraseña para las grabaciones exportadas. No será posible abrir el archivo exportado sin la contraseña.

Haga clic para eliminar una grabación.

Exportar: Exporte toda o una parte de la grabación.

Aplicaciones

Add app (Agregar aplicación): Instale una nueva aplicación.

Find more apps (Buscar más aplicaciones): Encuentre más aplicaciones para instalar. Se le mostrará una página de información general de las aplicaciones de Axis.

Permitir aplicaciones sin firma : Active esta opción para permitir la instalación de aplicaciones sin firma.

Consulte las actualizaciones de seguridad en las aplicaciones AXIS OS y ACAP.

Nota

El rendimiento del dispositivo puede empeorar si ejecuta varias aplicaciones al mismo tiempo.

Utilice el switch situado junto al nombre de la aplicación para iniciar o detener la aplicación.

Abrir: Acceda a los ajustes de la aplicación. que varían en función de la aplicación. Algunas aplicaciones no tienen ajustes.

El menú contextual puede contener una o más de las siguientes opciones:

- **Licencia de código abierto**: Consulte la información sobre las licencias de código abierto utilizadas en la aplicación.
- **App log (Registro de aplicación)**: Consulte un registro de los eventos de la aplicación. El registro resulta útil si se debe contactar con el servicio de soporte técnico.
- **Activate license with a key (Activar licencia con una clave)**: Si la aplicación requiere una licencia, tiene que activarla. Use esta opción si su dispositivo no tiene acceso a Internet.
  Si no dispone de clave de licencia, vaya a *axis.com/products/analytics*. Se necesita un código de licencia y el número de serie del producto de Axis para generar una clave de licencia.
- **Activate license automatically (Activar licencia automáticamente)**: Si la aplicación requiere una licencia, tiene que activarla. Use esta opción si su dispositivo tiene acceso a Internet. Se necesita un código para activar la licencia.
- **Deactivate the license (Desactivar la licencia)**: Desactive la licencia para sustituirla por otra, por ejemplo, al cambiar de licencia de prueba a licencia completa. Si desactiva la licencia, también la elimina del dispositivo.
- **Settings (Ajustes)**: Configure los parámetros.
- **Eliminar**: Permite eliminar la aplicación del dispositivo permanentemente. Si primero no desactiva la licencia, permanecerá activa.

Sistema

Hora y ubicación

Fecha y hora

El formato de fecha y hora depende de la configuración de idioma del navegador web.

Nota

Es aconsejable sincronizar la fecha y hora del dispositivo con un servidor NTP.

Synchronization (Sincronización): Seleccione una opción para la sincronización de la fecha y la hora del dispositivo.

- **Automatic date and time (Fecha y hora automáticas) (PTP)**: sincronice utilizando el protocolo de tiempo de precisión.
- **Fecha y hora automáticas (servidores NTS KE manuales)**: Sincronice con los servidores de establecimiento de claves NTP seguros conectados al servidor DHCP.
  - **Servidores NTS KE manuales**: Introduzca la dirección IP de un servidor NTP o de dos. Si usa dos servidores NTP, el dispositivo sincroniza y adapta la fecha y hora en función de la información de los dos.
  - **Trusted NTS KE CA certificates (Certificados CA NTS KE de confianza)**: Seleccione los certificados CA de confianza que se emplearán para la sincronización horaria NTS KE segura o no seleccione ninguno.
  - **Tiempo máximo de encuesta NTP**: Seleccione la cantidad máxima de tiempo que debe esperar el dispositivo antes de que sondee el servidor NTP para obtener una hora actualizada.
  - **Tiempo mínimo de encuesta NTP**: Seleccione la cantidad mínima de tiempo que debe esperar el dispositivo antes de que sondee el servidor NTP para obtener una hora actualizada.
- **Fecha y hora automáticas (los servidores NTP utilizan DHCP)**: Se sincroniza con los servidores NTP conectados al servidor DHCP.
  - **Servidores NTP alternativos**: Introduzca la dirección IP de un servidor alternativo o de dos.
  - **Tiempo máximo de encuesta NTP**: Seleccione la cantidad máxima de tiempo que debe esperar el dispositivo antes de que sondee el servidor NTP para obtener una hora actualizada.
  - **Tiempo mínimo de encuesta NTP**: Seleccione la cantidad mínima de tiempo que debe esperar el dispositivo antes de que sondee el servidor NTP para obtener una hora actualizada.
- **Fecha y hora automáticas (servidores NTP manuales)**: Se sincroniza con los servidores NTP que seleccione.
  - **Servidores NTP manuales**: Introduzca la dirección IP de un servidor NTP o de dos. Si usa dos servidores NTP, el dispositivo sincroniza y adapta la fecha y hora en función de la información de los dos.
  - **Tiempo máximo de encuesta NTP**: Seleccione la cantidad máxima de tiempo que debe esperar el dispositivo antes de que sondee el servidor NTP para obtener una hora actualizada.
  - **Tiempo mínimo de encuesta NTP**: Seleccione la cantidad mínima de tiempo que debe esperar el dispositivo antes de que sondee el servidor NTP para obtener una hora actualizada.
- **Custom date and time (Personalizar fecha y hora)**: Establezca manualmente la fecha y hora. Haga clic en **Get from system (Obtener del sistema)** para obtener una vez la configuración de fecha y hora desde su ordenador o dispositivo móvil.

Time zone (Zona horaria): Seleccione la zona horaria que desee utilizar. La hora se ajustará automáticamente para el horario de verano y el estándar.

- **DHCP**: Adopta la zona horaria del servidor DHCP. El dispositivo debe estar conectado a un servidor DHCP (v4 o v6) para poder seleccionar esta opción. Si ambas versiones están disponibles, el dispositivo prefiere las zonas horarias IANA sobre POSIX, y DHCPv4 sobre DHCPv6.
  - DHCPv4 utiliza la opción 100 para las zonas horarias POSIX y la opción 101 para las zonas horarias IANA.
  - DHCPv6 utiliza la opción 41 para POSIX y la opción 42 para IANA.
- **Manual**: Seleccione una zona horaria de la lista desplegable.

Nota

El sistema utiliza los ajustes de fecha y hora en todas las grabaciones, registros y ajustes del sistema.

Localización de dispositivo

Especifique el lugar en el que se encuentra el dispositivo. El sistema de gestión de vídeo puede utilizar esta información para colocar el dispositivo en un mapa.

- **Latitude (Latitud)**: Los valores positivos son el norte del ecuador.
- **Longitude (Longitud)**: Los valores positivos son el este del meridiano principal.
- **Heading (Rumbo)**: Introduzca la dirección de la brújula a la que apunta el dispositivo. 0 es al norte.
- **Label (Etiqueta)**: Especifique un nombre descriptivo para el dispositivo.
- **Save (Guardar)**: Haga clic para guardar la localización del dispositivo.

Red

IPv4

Asignar IPv4 automáticamente: Seleccione IPv4 IP automática (DHCP) para permitir que la red asigne automáticamente su dirección IP, máscara de subred y router, sin configuración manual. Recomendamos utilizar la asignación automática de IP (DHCP) para la mayoría de las redes.

IP address (Dirección IP): Introduzca una dirección IP única para el dispositivo. Las direcciones IP estáticas se pueden asignar de manera aleatoria dentro de redes aisladas, siempre que cada dirección asignada sea única. Para evitar conflictos, le recomendamos ponerse en contacto con el administrador de la red antes de asignar una dirección IP estática.

Subnet mask (Máscara de subred): Introduzca la máscara de subred para definir qué direcciones se encuentran dentro de la red de área local. Cualquier dirección fuera de la red de área local pasa por el router.

Router: Introduzca la dirección IP del router predeterminado (puerta de enlace) utilizada para conectar dispositivos conectados a distintas redes y segmentos de red.

Volver a la dirección IP estática si DHCP no está disponible: Seleccione si desea agregar una dirección IP estática para utilizarla como alternativa si DHCP no está disponible y no puede asignar una dirección IP automáticamente.

Nota

Si DHCP no está disponible y el dispositivo utiliza una reserva de dirección estática, la dirección estática se configura con un ámbito limitado.

IPv6

Assign IPv6 automatically (Asignar IPv6 automáticamente): Seleccione esta opción para activar IPv6 y permitir que el router de red asigne automáticamente una dirección IP al dispositivo.

Nombre de host

Asignar nombre de host automáticamente: Seleccione esta opción para que el router de red asigne automáticamente un nombre de host al dispositivo.

Hostname (Nombre de host): Introduzca el nombre de host manualmente para usarlo como una forma alternativa de acceder al dispositivo. El informe del servidor y el registro del sistema utilizan el nombre de host. Los caracteres permitidos son A–Z, a–z, 0–9 y -.

Active las actualizaciones de DNS dinámicas: Permite que el dispositivo actualice automáticamente los registros de su servidor de nombres de dominio cada vez que cambie la dirección IP del mismo.

Register DNS name (Registrar nombre de DNS): Introduzca un nombre de dominio único que apunte a la dirección IP de su dispositivo. Los caracteres permitidos son A–Z, a–z, 0–9 y -.

TTL: El tiempo de vida (Time to Live, TTL) establece cuánto tiempo permanece válido un registro DNS antes de que sea necesario actualizarlo.

Servidores DNS

Asignar DNS automáticamente: Seleccione esta opción para permitir que el servidor DHCP asigne dominios de búsqueda y direcciones de servidor DNS al dispositivo automáticamente. Recomendamos DNS automática (DHCP) para la mayoría de las redes.

Search domains (Dominios de búsqueda): Si utiliza un nombre de host que no esté completamente cualificado, haga clic en **Add search domain (Agregar dominio de búsqueda)** y escriba un dominio en el que se buscará el nombre de host que usa el dispositivo.

DNS servers (Servidores DNS): Haga clic en **Agregar servidor DNS** e introduzca la dirección IP del servidor DNS. Este servidor proporciona la traducción de nombres de host a las direcciones IP de su red.

Nota

Si DHCP está deshabilitado, las funciones que dependen de la configuración automática de la red, como el nombre de host, los servidores DNS, NTP y otras, podrían dejar de funcionar.

HTTP y HTTPS

HTTPS es un protocolo que proporciona cifrado para las solicitudes de página de los usuarios y para las páginas devueltas por el servidor web. El intercambio de información cifrado se rige por el uso de un certificado HTTPS, que garantiza la autenticidad del servidor.

Para utilizar HTTPS en el dispositivo, debe instalar un certificado HTTPS. Vaya a **System > Security (Sistema > Seguridad)** para crear e instalar certificados.

Allow access through (Permitir acceso mediante): Seleccione si un usuario tiene permiso para conectarse al dispositivo a través de **HTTP**, **HTTPS** o ambos protocolos **HTTP and HTTPS (HTTP y HTTPS)**.

Nota

Si visualiza páginas web cifradas a través de HTTPS, es posible que experimente un descenso del rendimiento, especialmente si solicita una página por primera vez.

HTTP port (Puerto HTTP): Especifique el puerto HTTP que se utilizará. El dispositivo permite el puerto 80 o cualquier puerto en el rango 1024-65535. Si ha iniciado sesión como administrador, también puede introducir cualquier puerto en el rango 1-1023. Si utiliza un puerto en este rango, recibirá una advertencia.

HTTPS port (Puerto HTTPS): Especifique el puerto HTTPS que se utilizará. El dispositivo permite el puerto 443 o cualquier puerto en el rango 1024-65535. Si ha iniciado sesión como administrador, también puede introducir cualquier puerto en el rango 1-1023. Si utiliza un puerto en este rango, recibirá una advertencia.

Certificado: Seleccione un certificado para habilitar HTTPS para el dispositivo.

Protocolos de detección de red

Bonjour®: Active esta opción para permitir la detección automática en la red.

Nombre de Bonjour: Introduzca un nombre descriptivo; será el que se muestre en la red. El nombre predeterminado es el nombre del dispositivo seguido de la dirección MAC.

UPnP®: Active esta opción para permitir la detección automática en la red.

Nombre de UPnP: Introduzca un nombre descriptivo; será el que se muestre en la red. El nombre predeterminado es el nombre del dispositivo seguido de la dirección MAC.

WS-Discovery: Active esta opción para permitir la detección automática en la red.

LLDP y CDP: Active esta opción para permitir la detección automática en la red. Si se desactiva LLDP y CPD puede afectar a la negociación de alimentación PoE. Para solucionar cualquier problema con la negociación de alimentación PoE, configure el switch PoE solo para la negociación de alimentación PoE del hardware.

Proxies globales

Http proxy (Proxy http): Especifique un host proxy global o una dirección IP según el formato permitido.

Https proxy (Proxy https): Especifique un host proxy global o una dirección IP según el formato permitido.

Formatos permitidos para proxies http y https:

- http(s)://host:puerto
- http(s)://usuario@host:puerto
- http(s)://user:pass@host:puerto

Nota

Reinicie el dispositivo para aplicar los ajustes globales del proxy.

No proxy (Sin proxy): Utilice **No proxy (Sin proxy)** para evitar los proxies globales. Introduzca una de las opciones de la lista, o introduzca varias separadas por una coma:

- Dejar vacío
- Especifique una dirección IP
- Especifique una dirección IP en formato CIDR
- Especifique un nombre de dominio, por ejemplo: www.<nombre de dominio>.com
- Especifique todos los subdominios de un dominio concreto, por ejemplo .<nombre de dominio>.com

Conexión a la nube con un clic

La conexión One-Click Cloud (O3C), junto con un servicio O3C, ofrece acceso seguro y sencillo a Internet para acceder al vídeo en directo o grabado desde cualquier ubicación. Para obtener más información, consulte *axis.com/end-to-end-solutions/hosted-services*.

Allow O3C (Permitir O3C):

- **Un clic**: esta es la opción predeterminada. Presione el botón de control del dispositivo para conectarse a O3C. Según el modelo del dispositivo, mantenga pulsado o pulse y suelte el botón hasta que el LED de estado parpadee. Registre el dispositivo en el servicio O3C en un plazo de 24 horas para activar la opción **Siempre** y mantenerse conectado. Si no lo registra, el dispositivo se desconectará de O3C.
- **Siempre**: El dispositivo intenta conectarse continuamente a un servicio O3C a través de Internet. Una vez registrado el dispositivo, permanece conectado. Utilice esta opción si el botón de control está fuera de su alcance.
- **No**: desconecta el servicio O3C.

Proxy settings (Configuración proxy): Si es necesario, escriba los ajustes del proxy para conectarse al servidor proxy.

Host: Introduzca la dirección del servidor proxy.

Puerto: Introduzca el número de puerto utilizado para acceder.

Inicio de sesión y **Contraseña**: En caso necesario, escriba un nombre de usuario y la contraseña del servidor proxy.

Authentication method (Método de autenticación):

- **Básico**: Este método es el esquema de autenticación más compatible con HTTP. Es menos seguro que el método **Digest** porque envía el nombre de usuario y la contraseña sin cifrar al servidor.
- **Digest**: Este método de autenticación es más seguro porque siempre transfiere la contraseña cifrada a través de la red.
- **Automático**: Esta opción permite que el dispositivo seleccione el método de autenticación automáticamente en función de los métodos admitidos. Da prioridad al método **Digest** por delante del **Básico**.

Owner authentication key (OAK) (Clave de autenticación de propietario [OAK]): Haga clic en **Get key (Obtener clave)** para obtener la clave de autenticación del propietario. Esto solo es posible si el dispositivo está conectado a Internet sin un cortafuegos o proxy.

SNMP

El protocolo de administración de red simple (SNMP) permite gestionar dispositivos de red de manera remota.

SNMP: Seleccione la versión de SNMP a usar.

- **v1 and v2c (v1 y v2c)**:
  - **Read community (Comunidad de lectura)**: Introduzca el nombre de la comunidad que tiene acceso de solo lectura a todos los objetos SNMP compatibles. El valor predeterminado es **público**.
  - **Write community (Comunidad de escritura)**: Escriba el nombre de la comunidad que tiene acceso de lectura o escritura a todos los objetos SNMP compatibles (excepto los objetos de solo lectura). El valor predeterminado es **escritura**.
  - **Activate traps (Activar traps)**: Active esta opción para activar el informe de trap. El dispositivo utiliza traps para enviar mensajes al sistema de gestión sobre eventos importantes o cambios de estado. En la interfaz web puede configurar traps para SNMP v1 y v2c. Las traps se desactivan automáticamente si cambia a SNMP v3 o desactiva SNMP. Si utiliza SNMP v3, puede configurar las traps a través de la aplicación de gestión de SNMP v3.
  - **Trap address (Dirección trap)**: introduzca la dirección IP o el nombre de host del servidor de gestión.
  - **Trap community (Comunidad de trap)**: Introduzca la comunidad que se utilizará cuando el dispositivo envía un mensaje trap al sistema de gestión.
  - **Traps**:
    - **Cold start (Arranque en frío)**: Envía un mensaje trap cuando se inicia el dispositivo.
    - **Link up (Enlace hacia arriba)**: Envía un mensaje trap cuando un enlace cambia de abajo a arriba.
    - **Link down (Enlace abajo)**: Envía un mensaje trap cuando un enlace cambia de arriba a abajo.
    - **Authentication failed (Error de autenticación)**: Envía un mensaje trap cuando se produce un error de intento de autenticación.

Nota

Todas las traps Axis Video MIB se habilitan cuando se activan las traps SNMP v1 y v2c. Para obtener más información, consulte *AXIS OS Portal > SNMP*.

- **v3**: SNMP v3 es una versión más segura que ofrece cifrado y contraseñas seguras. Para utilizar SNMP v3, recomendamos activar HTTPS, ya que la contraseña se envía a través de HTTPS. También evita que partes no autorizadas accedan a traps SNMP v1 y v2c sin cifrar. Si utiliza SNMP v3, puede configurar las traps a través de la aplicación de gestión de SNMP v3.
  - **Privacy (Privacidad)**: Seleccione el cifrado que desea usar para proteger sus datos SNMP.
  - **Password for the account "initial" (contraseña para la cuenta "Inicial")**: Introduzca la contraseña de SNMP para la cuenta denominada "Initial". Aunque la contraseña se puede enviar sin activar HTTPS, no lo recomendamos. La contraseña de SNMP v3 solo puede establecerse una vez, y preferiblemente solo cuando esté activado HTTPS. Una vez establecida la contraseña, dejará de mostrarse el campo de contraseña. Para volver a establecer la contraseña, debe restablecer el dispositivo a su configuración predeterminada de fábrica.

Seguridad

Certificados

Los certificados se utilizan para autenticar los dispositivos de una red. Un dispositivo admite dos tipos de certificados:

- **Client/server certificates (Certificados de cliente/servidor)**
  Un certificado de cliente/servidor valida la identidad del dispositivo de Axis y puede firmarlo el propio dispositivo o emitirlo una autoridad de certificación (CA). Un certificado firmado por el propio producto ofrece protección limitada y se puede utilizar antes de que se obtenga un certificado emitido por una autoridad de certificación.
- **Certificados CA**
  Puede utilizar un certificado de la autoridad de certificación (AC) para autenticar un certificado entre iguales, por ejemplo, para validar la identidad de un servidor de autenticación cuando el dispositivo se conecta a una red protegida por IEEE 802.1X. El dispositivo incluye varios certificados de autoridad de certificación preinstalados.

Se admiten estos formatos:

- Formatos de certificado: .PEM, .CER y .PFX
- Formatos de clave privada: PKCS#1 y PKCS#12

Importante

Si restablece el dispositivo a los valores predeterminados de fábrica, se eliminarán todos los certificados. Los certificados CA preinstalados se vuelven a instalar.

Agregar certificado: Haga clic aquí para añadir un certificado. Se abre una guía paso a paso.

- **Más** : Mostrar más campos que rellenar o seleccionar.
- **Almacenamiento de claves seguro**: Seleccione esta opción para usar **Trusted Execution Environment (SoC TEE)**, **Secure element (Elemento seguro)** o **Trusted Platform Module 2.0** para almacenar la clave privada de forma segura. Para obtener más información sobre el almacén de claves seguro que desea seleccionar, vaya a *help.axis.com/axis-os#cryptographic-support*.
- **Tipo de clave**: Seleccione la opción predeterminada o un algoritmo de cifrado diferente en la lista desplegable para proteger el certificado.

El menú contextual contiene:

- **Certificate information (Información del certificado)**: Muestra las propiedades de un certificado instalado.
- **Delete certificate (Eliminar certificado)**: Se elimina el certificado.
- **Create certificate signing request (Crear solicitud de firma de certificado)**: Se crea una solicitud de firma de certificado que se envía a una autoridad de registro para solicitar un certificado de identidad digital.

Almacenamiento de claves seguro :

- **Trusted Execution Environment (SoC TEE)**: seleccione esta opción para utilizar SoC TEE para el almacenamiento seguro de claves.
- **Elemento seguro (CC EAL6+, FIPS 140-3 Level 3)** : Seleccione para utilizar un elemento seguro para un almacén de claves seguro.
- **Trusted Platform Module 2.0 (CC EAL4+, FIPS 140-2 nivel 2)** : Seleccione para usar TPM 2.0 para el almacén de claves seguro.

Política criptográfica

La política criptográfica define cómo se utiliza el cifrado para proteger los datos.

Activa: Seleccione la política criptográfica que se aplicará al dispositivo:

- **Predeterminado - OpenSSL**: Seguridad y rendimiento equilibrados para uso general.
- **FIPS - Política para el cumplimiento de FIPS 140-2**: cifrado conforme con FIPS 140-2 para sectores regulados.

Control y cifrado de acceso a la red

IEEE 802.1x

IEEE 802.1x es un estándar IEEE para el control de admisión de red basada en puertos que proporciona una autenticación segura de los dispositivos de red conectados e inalámbricos. IEEE 802.1x se basa en el protocolo de autenticación extensible, EAP.

Para acceder a una red protegida por IEEE 802.1x, los dispositivos de red deben autenticarse ellos mismos. Un servidor de autenticación lleva a cabo la autenticación, normalmente un servidor RADIUS (por ejemplo, FreeRADIUS y Microsoft Internet Authentication Server).

IEEE 802.1AE MACsec

IEEE 802.1AE MACsec es un estándar IEEE para la seguridad del control de acceso a medios (MAC) que define la confidencialidad e integridad de los datos sin conexión para protocolos independientes de acceso a medios.

Certificados

Si se configura sin un certificado de la autoridad de certificación, la validación de certificados del servidor se deshabilita y el dispositivo intentará autenticarse a sí mismo independientemente de la red a la que esté conectado.

Si se usa un certificado, en la implementación de Axis, el dispositivo y el servidor de autenticación se autentican ellos mismos con certificados digitales utilizando EAP-TLS (protocolo de autenticación extensible - seguridad de la capa de transporte).

Para permitir que el dispositivo acceda a una red protegida mediante certificados, debe instalar un certificado de cliente firmado en el dispositivo.

Authentication method (Método de autenticación): Seleccione un tipo de EAP utilizado para la autenticación.

Client certificate (Certificado del cliente): Seleccione un certificado de cliente para usar IEEE 802.1x. El servidor de autenticación utiliza el certificado para validar la identidad del cliente.

CA Certificates (Certificados de la autoridad de certificación): Seleccione certificados CA para validar la identidad del servidor de autenticación. Si no se selecciona ningún certificado, el dispositivo intentará autenticarse a sí mismo, independientemente de la red a la que esté conectado.

EAP identity (Identidad EAP): Introduzca la identidad del usuario asociada con el certificado de cliente.

EAPOL version (Versión EAPOL): Seleccione la versión EAPOL que se utiliza en el switch de red.

Use IEEE 802.1x (Utilizar IEEE 802.1x): Seleccione para utilizar el protocolo IEEE 802.1x.

Estos ajustes solo están disponibles si utiliza **IEEE 802.1x PEAP-MSCHAPv2** como método de autenticación:

- **Contraseña**: Escriba la contraseña para la identidad de su usuario.
- **Versión de Peap**: Seleccione la versión de Peap que se utiliza en el switch de red.
- **Label (Etiqueta)**: Seleccione 1 para usar el cifrado EAP del cliente; seleccione 2 para usar el cifrado PEAP del cliente. Seleccione la etiqueta que utiliza el switch de red cuando utilice la versión 1 de Peap.

Estos ajustes solo están disponibles si utiliza **IEEE 802.1ae MACsec (CAK estática/clave precompartida)** como método de autenticación:

- **Nombre de clave de asociación de conectividad de acuerdo de claves:** Introduzca el nombre de la asociación de conectividad (CKN). Debe tener de 2 a 64 caracteres hexadecimales (divisibles por 2). La CKN debe configurarse manualmente en la asociación de conectividad y debe coincidir con los dos extremos del enlace para activar inicialmente MACsec.
- **Clave de asociación de conectividad de acuerdo de claves**: Introduzca la clave de la asociación de conectividad (CAK). Debe tener una longitud de 32 o 64 caracteres hexadecimales. La CAK debe configurarse manualmente en la asociación de conectividad y debe coincidir con los dos extremos del enlace para activar inicialmente MACsec.

Evitar ataques de fuerza bruta

Blocking (Bloqueo): Active esta función para bloquear ataques de fuerza bruta. Un ataque de fuerza utiliza un sistema de ensayo y error para descubrir información de inicio de sesión o claves de cifrado.

Blocking period (Período de bloqueo): Introduzca el número de segundos para bloquear un ataque de fuerza bruta.

Blocking conditions (Condiciones de bloqueo): Introduzca el número de fallos de autenticación permitidos por segundo antes de que se inicie el bloqueo. Puede definir el número de fallos permitidos tanto a nivel de página como de dispositivo.

Firewall

Firewall: Encender para activar el firewall.

Política predeterminada: Seleccione cómo desea que el firewall gestione las solicitudes de conexión no cubiertas por las reglas.

- **ACCEPT (Aceptar):** Permite todas las conexiones al dispositivo. Esta opción está establecida de forma predeterminada.
- **DROP (Soltar):** Bloquea todas las conexiones al dispositivo.

Para realizar excepciones a la política predeterminada, puede crear reglas que permitan o bloqueen las conexiones al dispositivo desde direcciones, protocolos y puertos específicos.

+ New rule (Nueva regla): Haga clic para crear una regla.

Rule type (Tipo de regla):

- **FILTER (Filtro)**: Seleccione esta opción para permitir o bloquear conexiones de dispositivos que coincidan con los criterios definidos en la regla.
  - **Policy (Directiva)**: Seleccione **Accept (Aceptar)** o **Drop (Soltar)** para la regla del firewall.
  - **IP range (Intervalo IP)**: Seleccione para especificar el rango de direcciones que desee permitir o bloquear. Utilice IPv4/IPv6 en **Start (Inicio)** y **End (Fin)**.
  - **IP address (Dirección IP)**: Introduzca la dirección que desee permitir o bloquear. Utilice el formato IPv4/IPv6 o CIDR.
  - **Protocol (Protocolo)**: Seleccione el protocolo de red (TCP, UDP o Ambos) que desee permitir o bloquear. Si selecciona un protocolo, también deberá especificar un puerto.
  - **MAC**: Introduzca la dirección MAC del dispositivo que desee permitir o bloquear.
  - **Port range (Intervalo de puertos)**: Seleccione esta opción para especificar el rango de puertos que desee permitir o bloquear. Añádalos en **Start (Inicio)** y **End (Fin)**.
  - **Puerto**: Introduzca el número de puerto que desee permitir o bloquear. Los números de puerto deben situarse estar entre 1 y 65535.
  - **Traffic type (Tipo de tráfico)**: Seleccione el tipo de tráfico que desee permitir o bloquear.
    - **UNICAST**: Tráfico de un único emisor a un único destinatario.
    - **BROADCAST (Transmisión)**: Tráfico de un único emisor a todos los dispositivos de la red.
    - **MULTICAST**: Tráfico de uno o varios emisores a uno o varios destinatarios.
- **LIMIT (Límites)**: Seleccione esta opción para aceptar conexiones de dispositivos que coincidan con los criterios definidos en la regla, pero aplique límites para reducir el tráfico excesivo.
  - **IP range (Intervalo IP)**: Seleccione para especificar el rango de direcciones que desee permitir o bloquear. Utilice IPv4/IPv6 en **Start (Inicio)** y **End (Fin)**.
  - **IP address (Dirección IP)**: Introduzca la dirección que desee permitir o bloquear. Utilice el formato IPv4/IPv6 o CIDR.
  - **Protocol (Protocolo)**: Seleccione el protocolo de red (TCP, UDP o Ambos) que desee permitir o bloquear. Si selecciona un protocolo, también deberá especificar un puerto.
  - **MAC**: Introduzca la dirección MAC del dispositivo que desee permitir o bloquear.
  - **Port range (Intervalo de puertos)**: Seleccione esta opción para especificar el rango de puertos que desee permitir o bloquear. Añádalos en **Start (Inicio)** y **End (Fin)**.
  - **Puerto**: Introduzca el número de puerto que desee permitir o bloquear. Los números de puerto deben situarse estar entre 1 y 65535.
  - **Unit (Unidad)**: Seleccione el tipo de conexiones que desee permitir o bloquear.
  - **Period (Periodo)**: Seleccione el periodo de tiempo relacionado con **Amount (Cantidad)**.
  - **Amount (Cantidad)**: Determine el número máximo de veces que se permite que un dispositivo se conecte dentro del **Period (Periodo)**. La cantidad máxima es 65535.

- **Burst (Ráfaga)**: Introduzca el número de conexiones que pueden superar la **Amount (Cantidad)** establecida una vez durante el **Period (Periodo)** establecido. Una vez alcanzado el número, solo se permitirá la cantidad determinada durante el periodo establecido.
- **Traffic type (Tipo de tráfico)**: Seleccione el tipo de tráfico que desee permitir o bloquear.
  - **UNICAST**: Tráfico de un único emisor a un único destinatario.
  - **BROADCAST (Transmisión)**: Tráfico de un único emisor a todos los dispositivos de la red.
  - **MULTICAST**: Tráfico de uno o varios emisores a uno o varios destinatarios.

Test rules (Prueba de reglas): Haga clic para probar las reglas que haya definido.

- **Test time in seconds (Tiempo de prueba en segundos)**: Defina un límite de tiempo para probar las reglas.
- **Roll back (Restaurar)**: Haga clic para restablecer el firewall a su estado anterior, antes de haber probado las reglas.
- **Apply rules (Aplicar reglas)**: Haga clic para activar las reglas sin realizar pruebas. No le recomendamos esta opción.

Certificado de AXIS OS con firma personalizada

Para instalar en el dispositivo software de prueba u otro software personalizado de Axis, necesita un certificado de AXIS OS firmado personalizado. El certificado verifica que el software ha sido aprobado por el propietario del dispositivo y por Axis. El software solo puede ejecutarse en un dispositivo concreto identificado por su número de serie único y el ID de su chip. Solo Axis puede crear los certificados de AXIS OS firmados personalizados, ya que Axis posee la clave para firmarlos.

Install (Instalar): Haga clic para instalar el certificado. El certificado se debe instalar antes que el software.

El menú contextual contiene:

- **Delete certificate (Eliminar certificado)**: Se elimina el certificado.

Cuentas

Cuentas

Add account (Añadir cuenta): Haga clic para agregar una nueva cuenta. Puede agregar hasta 100 cuentas.

Cuenta: introduzca un nombre de cuenta único.

Nueva contraseña: introduzca una contraseña para la cuenta. Las contraseñas deben tener entre 1 y 64 caracteres. La contraseña solo admite caracteres ASCII imprimibles (códigos de 32 a 126), por ejemplo, letras, números, signos de puntuación y algunos símbolos.

Repetir contraseña: Introduzca la misma contraseña de nuevo.

Privilegios:

- **Administrador**: Tiene acceso completo a todos los ajustes. Los administradores también pueden agregar, actualizar y eliminar otras cuentas.
- **Operator (Operador)**: Tiene acceso a todos los ajustes excepto:
  - Todos los ajustes del **sistema**.
- **Viewer (Visualizador)**: No tiene acceso para cambiar ajustes.

El menú contextual contiene:

Actualizar cuenta: Editar las propiedades de la cuenta.

Eliminar cuenta: Elimine la cuenta. No puede eliminar la cuenta de root.

Acceso anónimo

Permitir la visualización anónima: Active esta opción para permitir que todos los usuarios accedan al dispositivo como visores sin tener que registrarse con una cuenta.

Allow anonymous PTZ operating (Permitir funcionamiento PTZ anónimo) : Active esta opción para permitir que los usuarios anónimos giren, inclinen y acerquen el zoom a la imagen.

Cuentas SSH

Add SSH account (Agregar cuenta SSH): Haga clic para agregar una nueva cuenta SSH.

- **Habilitar SSH**: Active el uso del servicio SSH.

Cuenta: introduzca un nombre de cuenta único.

Nueva contraseña: introduzca una contraseña para la cuenta. Las contraseñas deben tener entre 1 y 64 caracteres. La contraseña solo admite caracteres ASCII imprimibles (códigos de 32 a 126), por ejemplo, letras, números, signos de puntuación y algunos símbolos.

Repetir contraseña: Introduzca la misma contraseña de nuevo.

Comentario: Introduzca un comentario (opcional).

El menú contextual contiene:

Actualizar cuenta SSH: Editar las propiedades de la cuenta.

Eliminar cuenta SSH: Elimine la cuenta. No puede eliminar la cuenta de root.

Host virtual

Add virtual host (Agregar host virtual): Haga clic para agregar un nuevo host virtual.

Habilitada: Seleccione esta opción para usar este host virtual.

Server name (Nombre del servidor): Introduzca el nombre del servidor. Utilice solo los números 0-9, las letras A-Z y el guión (-).

Puerto: Introduzca el puerto al que está conectado el servidor.

Tipo: Seleccione el tipo de autenticación que desea usar. Seleccione entre **Basic**, **Digest**, **Open ID** y **Client Credential Grant**.

HTTPS: seleccione esta opción para utilizar HTTPS.

El menú contextual contiene:

- **Actualizar host virtual**
- **Eliminar host virtual**

Configuración de concesión de credenciales de cliente

Admin claim (Reclamación de administrador): Introduzca un valor para la función de administrador.

Verification URL (URL de verificación): Introduzca el enlace web para la autentificación de punto de acceso de API.

Operator claim (Reclamación de operador): Introduzca un valor para la función de operador.

Require claim (Requerir solicitud): Introduzca los datos que deberían estar en el token.

Viewer claim (Reclamación de visor): Introduzca el valor de la función de visor.

Save (Guardar): Haga clic para guardar los valores.

Configuración de OpenID

Importante

Si no puede utilizar OpenID para iniciar sesión, utilice las credenciales Digest o Basic que usó al configurar OpenID para iniciar sesión.

Client ID (ID de cliente): Introduzca el nombre de usuario de OpenID.

Outgoing Proxy (Proxy saliente): Introduzca la dirección de proxy de la conexión de OpenID para usar un servidor proxy.

Admin claim (Reclamación de administrador): Introduzca un valor para la función de administrador.

Provider URL (URL de proveedor): Introduzca el enlace web para la autenticación de punto de acceso de API. El formato debe ser https://[insertar URL]/.well-known/openid-configuration

Operator claim (Reclamación de operador): Introduzca un valor para la función de operador.

Require claim (Requerir solicitud): Introduzca los datos que deberían estar en el token.

Viewer claim (Reclamación de visor): Introduzca el valor de la función de visor.

Remote user (Usuario remoto): Introduzca un valor para identificar usuarios remotos. Esto ayudará a mostrar el usuario actual en la interfaz web del dispositivo.

Scopes (Ámbitos): Ámbitos opcionales que podrían formar parte del token.

Client secret (Secreto del cliente): Introduzca la contraseña de OpenID.

Save (Guardar): Haga clic para guardar los valores de OpenID.

Enable OpenID (Habilitar OpenID): Active esta opción para cerrar la conexión actual y permitir la autenticación del dispositivo desde la URL del proveedor.

Eventos

Reglas

Una regla define las condiciones que desencadena el producto para realizar una acción. La lista muestra todas las reglas actualmente configuradas en el producto.

Nota

Puede crear hasta 256 reglas de acción.

Agregar una regla: Cree una regla.

Name (Nombre): Introduzca un nombre para la regla.

Esperar entre acciones: Introduzca el tiempo mínimo (hh:mm:ss) que debe pasar entre las activaciones de regla. Resulta útil si la regla se activa, por ejemplo, en condiciones del modo diurno/nocturno, para evitar que pequeños cambios de luz durante el amanecer y el atardecer activen la regla varias veces.

Condition (Condición): Seleccione una condición de la lista. Una condición se debe cumplir para que el dispositivo realice una acción. Si se definen varias condiciones, todas ellas deberán cumplirse para que se active la acción. Para obtener información sobre condiciones específicas, consulte *Introducción a las reglas para eventos*.

Utilizar esta condición como activador: Seleccione esta primera función de condición solo como activador inicial. Una vez que se activa la regla, permanecerá activa mientras se cumplen todas las demás condiciones, independientemente del estado de la primera condición. Si no selecciona esta opción, la regla estará activa siempre que se cumplan el resto de condiciones.

Invert this condition (Invertir esta condición): Seleccione si desea que la condición sea la opuesta a su selección.

Agregar una condición: Haga clic para agregar una condición adicional.

Action (Acción): Seleccione una acción de la lista e introduzca la información necesaria. Para obtener información sobre acciones específicas, consulte *Introducción a las reglas para eventos*.

Su producto puede tener algunas de las siguientes reglas preconfiguradas:

Front-facing LED Activation: LiveStream (Activación de LED frontal: Transmisión en directo): cuando el micrófono está encendido y se recibe una transmisión en directo, el LED frontal del dispositivo de audio se pone en verde.

Front-facing LED Activation: Recording (Activación de LED frontal: Grabación): cuando el micrófono está encendido y hay una grabación en curso, el LED frontal del dispositivo de audio se pone en verde.

Front-facing LED Activation: SIP (Activación de LED frontal: SIP): cuando el micrófono está encendido y hay activa una llamada SIP, el LED frontal del dispositivo de audio se pone en verde. Debe habilitar SIP en el dispositivo de audio antes de que se pueda desencadenar este evento.

Pre-announcement tone: Play tone on incoming call (Tono de preaviso: Reproducir tono al recibir llamada entrante): cuando se realiza una llamada SIP al dispositivo de audio, el dispositivo reproduce un fragmento de audio predefinido. Debe habilitar SIP para el dispositivo de audio. Para que la persona que realiza la llamada SIP escuche un tono de llamada mientras el dispositivo de audio reproduce el fragmento de audio, debe configurar la cuenta SIP del dispositivo para no responder a la llamada automáticamente.

Pre-announcement tone: Answer call after incoming call-tone (Tono de preaviso: contestar llamada después del tono de llamada entrante): cuando el fragmento de audio ha finalizado, se responde a la llamada SIP entrante. Debe habilitar SIP para el dispositivo de audio.

Loud ringer (Timbre alto) : cuando se realiza una llamada SIP al dispositivo de audio, se reproduce un fragmento de audio predefinido mientras la regla esté activa. Debe habilitar SIP para el dispositivo de audio.

Destinatarios

Puede configurar el dispositivo para notificar a los destinatarios acerca de los eventos o enviar archivos.

Nota

Si configura su dispositivo para utilizar FTP o SFTP, no cambie ni elimine el número de secuencia único que se añade a los nombres de archivo. Si lo hace, solo se podrá enviar una imagen por evento.

La lista muestra todos los destinatarios configurados actualmente en el producto, además de información sobre su configuración.

Nota

Puede crear hasta 20 destinatarios.

Agregar un destinatario: Haga clic para agregar un destinatario.

Name (Nombre): Introduzca un nombre para el destinatario.

Tipo: Seleccione de la lista:

- **FTP**
  - **Host**: Introduzca la dirección IP o el nombre de host del servidor. Si introduce un nombre de host, asegúrese de que se ha especificado un servidor DNS en **Sistema > Red > IPv4 e IPv6**.
  - **Puerto**: Introduzca el número de puerto utilizado por el servidor FTP. El valor por defecto es 21.
  - **Carpeta**: Introduzca la ruta al directorio en el que desea almacenar los archivos. Si el directorio aún no existe en el servidor FTP, obtendrá un mensaje de error al realizar la carga de archivos.
  - **Nombre de usuario**: Introduzca el nombre de usuario para el inicio de sesión.
  - **Contraseña**: Introduzca la contraseña para el inicio de sesión.
  - **Utilice nombre de archivo temporal**: Seleccione esta opción para cargar archivos con nombres de archivo temporales generados automáticamente. Los archivos se renombran por los nombres deseados cuando se completa la carga. Si la carga se ha anulado o interrumpido, no obtendrá archivos dañados. Sin embargo, es probable que se sigan recibiendo los archivos temporales. De este modo, sabrá que todos los archivos que tienen el nombre deseado son correctos.
  - **Usar FTP pasivo**: En circunstancias normales, el producto simplemente solicita al servidor FTP de destino que abra la conexión de datos. El dispositivo inicia activamente el control FTP y las conexiones de datos al servidor de destino. Normalmente esto es necesario si existe un cortafuegos entre el dispositivo y el servidor FTP de destino.
- **HTTP**
  - **URL**: Introduzca la dirección de red al servidor HTTP y la secuencia de comandos que gestionará la solicitud. Por ejemplo, http://192.168.254.10/cgi-bin/notify.cgi.
  - **Nombre de usuario**: Introduzca el nombre de usuario para el inicio de sesión.
  - **Contraseña**: Introduzca la contraseña para el inicio de sesión.
  - **Proxy**: Active e introduzca la información requerida si es necesario pasar un servidor proxy para conectarse al servidor HTTP.
- **HTTPS**
  - **URL**: Introduzca la dirección de red al servidor HTTPS y la secuencia de comandos que gestionará la solicitud. Por ejemplo, https://192.168.254.10/cgi-bin/notify.cgi.
  - **Validar certificado del servidor**: Seleccione para validar el certificado creado por el servidor HTTPS.
  - **Nombre de usuario**: Introduzca el nombre de usuario para el inicio de sesión.
  - **Contraseña**: Introduzca la contraseña para el inicio de sesión.
  - **Proxy**: Active e introduzca la información requerida si es necesario pasar un servidor proxy para conectarse al servidor HTTPS.
- **Almacenamiento de red**
  Puede agregar almacenamiento de red, como almacenamiento en red tipo NAS (almacenamiento en red) y usarlo como destinatario para almacenar archivos. Los archivos se almacenan en formato Matroska (MKV).
  - **Host**: Introduzca la dirección IP o el nombre de host del almacenamiento de red.
  - **Recurso compartido**: Escriba el nombre del recurso compartido en el host.

- **Carpeta**: Introduzca la ruta al directorio en el que desea almacenar los archivos.
- **Nombre de usuario**: Introduzca el nombre de usuario para el inicio de sesión.
- **Contraseña**: Introduzca la contraseña para el inicio de sesión.

- SFTP
  - **Host**: Introduzca la dirección IP o el nombre de host del servidor. Si introduce un nombre de host, asegúrese de que se ha especificado un servidor DNS en **Sistema > Red > IPv4 e IPv6**.
  - **Puerto**: Introduzca el número de puerto utilizado por el servidor SFTP. El predeterminado es 22.
  - **Carpeta**: Introduzca la ruta al directorio en el que desea almacenar los archivos. Si el directorio aún no existe en el servidor SFTP, obtendrá un mensaje de error al realizar la carga de archivos.
  - **Nombre de usuario**: Introduzca el nombre de usuario para el inicio de sesión.
  - **Contraseña**: Introduzca la contraseña para el inicio de sesión.
  - **Tipo de clave pública del host SSH (MD5)**: Introduzca la huella de la clave pública del host remoto (una cadena de 32 dígitos hexadecimales). El cliente de SFTP es compatible con servidores SFTP que emplean tipos de clave del host SSH-2 con RSA, DSA, ECDSA y ED25519. RSA es el método preferido durante la negociación, seguido de ECDSA, ED25519 y DSA. Asegúrese de introducir la clave de host MD5 correcta que utiliza el servidor SFTP. Si bien el dispositivo Axis admite claves hash MD5 y SHA-256, recomendamos usar SHA-256 debido a una seguridad más sólida que MD5. Para obtener más información sobre cómo configurar un servidor SFTP con un dispositivo Axis, vaya al Portal *de AXIS OS*.
  - **Tipo de clave pública del host SSH (SHA256)**: Ingrese la huella digital de la clave pública del host remoto (una cadena codificada en Base64 de 43 dígitos). El cliente de SFTP es compatible con servidores SFTP que emplean tipos de clave del host SSH-2 con RSA, DSA, ECDSA y ED25519. RSA es el método preferido durante la negociación, seguido de ECDSA, ED25519 y DSA. Asegúrese de introducir la clave de host MD5 correcta que utiliza el servidor SFTP. Si bien el dispositivo Axis admite claves hash MD5 y SHA-256, recomendamos usar SHA-256 debido a una seguridad más sólida que MD5. Para obtener más información sobre cómo configurar un servidor SFTP con un dispositivo Axis, vaya al Portal *de AXIS OS*.
  - **Utilice nombre de archivo temporal**: Seleccione esta opción para cargar archivos con nombres de archivo temporales generados automáticamente. Los archivos se renombran por los nombres deseados cuando se completa la carga. Si la carga se ha anulado o interrumpido, no obtendrá archivos dañados. Sin embargo, es probable que se sigan recibiendo los archivos temporales. De este modo, sabrá que todos los archivos que tienen el nombre deseado son correctos.

- SIP o VMS :
  SIP: Seleccione esta opción para realizar una llamada SIP.
  VMS: Seleccione esta opción para realizar una llamada de VMS.
  - **Desde cuenta SIP**: Seleccione de la lista.
  - **A dirección SIP**: Introduzca la dirección SIP.
  - **Prueba**: Haga clic para comprobar que los ajustes de la llamada funcionan.
- Correo electrónico
  - **Enviar correo electrónico a**: Introduzca la dirección de correo electrónico a la que enviar correos electrónicos. Para especificar varias direcciones de correo electrónico, utilice comas para separarlas.
  - **Enviar correo desde**: Introduzca la dirección de correo electrónico del servidor emisor.
  - **Nombre de usuario**: Introduzca el nombre de usuario del servidor de correo. Deje este campo vacío si el servidor de correo no necesita autenticación.

- **Contraseña**: Introduzca la contraseña del servidor de correo. Deje este campo vacío si el servidor de correo no necesita autenticación.
- **Servidor de correo electrónico (SMTP)**: Introduzca el nombre del servidor SMTP, por ejemplo, smtp.gmail.com, smtp.mail.yahoo.com.
- **Puerto**: Introduzca el número de puerto para el servidor SMTP, usando valores entre 0 y 65535. El valor por defecto es 587.
- **Cifrado**: Para usar el cifrado, seleccione SSL o TLS.
- **Validar certificado del servidor**: Si utiliza el cifrado, seleccione esta opción para validar la identidad del dispositivo. El certificado puede firmarlo el propio producto o emitirlo una autoridad de certificación (CA).
- **Autentificación POP**: Active para introducir el nombre del servidor POP, por ejemplo, pop.gmail.com.

Nota

Algunos proveedores de correo electrónico tienen filtros de seguridad que evitan que los usuarios reciban o vean grandes cantidades de adjuntos, que reciban mensajes de correo electrónico programados, etc. Compruebe la política de seguridad del proveedor de correo electrónico para evitar que su cuenta de correo quede bloqueada o que no reciba correos electrónicos esperados.

- **TCP**
  - **Host**: Introduzca la dirección IP o el nombre de host del servidor. Si introduce un nombre de host, asegúrese de que se ha especificado un servidor DNS en **Sistema > Red > IPv4 e IPv6**.
  - **Puerto**: Introduzca el número de puerto utilizado para acceder al servidor.

Comprobación: Haga clic en probar la configuración.

⋮ El menú contextual contiene:

Ver destinatario: Haga clic para ver todos los detalles del destinatario.

Copiar destinatario: Haga clic para copiar un destinatario. Cuando copia, puede realizar cambios en el nuevo destinatario.

Eliminar destinatario: Haga clic para eliminar el destinatario de forma permanente.

Horarios

Se pueden usar programaciones y pulsos como condiciones en las reglas. La lista muestra todas las programaciones y pulsos configurados actualmente en el producto, además de información sobre su configuración.

+ **Agregar programación**: Haga clic para crear una programación o pulso.

Activadores manuales

Puede usar el activador manual para desencadenar manualmente una regla. El activador manual se puede utilizar, por ejemplo, para validar acciones durante la instalación y configuración de productos.

MQTT

MQTT (Message Queuing Telemetry Transport) es un protocolo de mensajería estándar para Internet of things (IoT). Se diseñó para simplificar la integración del IoT y se utiliza en una amplia variedad de sectores para conectar dispositivos remotos con una huella de código pequeña y un ancho de banda de red mínimo. El cliente MQTT del software de dispositivos de Axis puede simplificar la integración de los datos y eventos producidos en el dispositivo con sistemas que no sean software de gestión de vídeo (VMS).

Configure el dispositivo como cliente MQTT. La comunicación MQTT se basa en dos entidades, los clientes y el intermediario. Los clientes pueden enviar y recibir mensajes. El intermediario es responsable de dirigir los mensajes entre los clientes.

Puede obtener más información sobre MQTT en la *base de conocimiento de AXIS OS*.

ALPN

ALPN es una extensión de TLS/SSL que permite seleccionar un protocolo de aplicación durante la fase de enlace de la conexión entre el cliente y el servidor. Se utiliza para habilitar el tráfico MQTT a través del mismo puerto que se utiliza para otros protocolos, como HTTP. En algunos casos, es posible que no haya un puerto dedicado abierto para la comunicación MQTT. Una solución en tales casos es utilizar ALPN para negociar el uso de MQTT como protocolo de aplicación en un puerto estándar, permitido por los cortafuegos.

Cliente MQTT

Conectar: Active o desactive el cliente MQTT.

Estado: Muestra el estado actual del cliente MQTT.

Broker

Host: introduzca el nombre de host o la dirección IP del servidor MQTT.

Protocol (Protocolo): Seleccione el protocolo que desee utilizar.

Puerto: Introduzca el número de puerto.

- 1883 es el valor predeterminado de **MQTT a través de TCP**
- 8883 es el valor predeterminado de **MQTT a través de SSL**
- 80 es el valor predeterminado de **MQTT a través de WebSocket**
- 443 es el valor predeterminado de **MQTT a través de WebSocket Secure**

Protocol ALPN: Introduzca el nombre del protocolo ALPN proporcionado por su proveedor de MQTT. Esto solo se aplica con MQTT a través de SSL y MQTT a través de WebSocket Secure.

Nombre de usuario: Introduzca el nombre de cliente que utilizará la cámara para acceder al servidor.

Contraseña: Introduzca una contraseña para el nombre de usuario.

Client ID (ID de cliente): Introduzca una ID de cliente. El identificador de cliente que se envía al servidor cuando el cliente se conecta a él.

Clean session (Limpiar sesión): Controla el comportamiento en el momento de la conexión y la desconexión. Si se selecciona, la información de estado se descarta al conectar y desconectar.

Proxy HTTP: Una URL con una longitud máxima de 255 bytes. Puede dejar el campo vacío si no desea utilizar un proxy HTTP.

Proxy HTTPS: Una URL con una longitud máxima de 255 bytes. Puede dejar el campo vacío si no desea utilizar un proxy HTTPS.

Keep alive interval (Intervalo de Keep Alive): Habilita al cliente para detectar si el servidor ya no está disponible sin tener que esperar a que se agote el tiempo de espera de TCP/IP.

Timeout (Tiempo de espera): El intervalo de tiempo está en segundos para permitir que se complete la conexión. Valor predeterminado: 60

Device topic prefix (Prefijo de tema del dispositivo): se utiliza en los valores por defecto del tema en el mensaje de conexión, en el mensaje LWT de la pestaña **MQTT client (Cliente MQTT)** y, en las condiciones de publicación de la pestaña **MQTT publication (Publicación MQTT)** ".

Reconnect automatically (Volver a conectar automáticamente): especifica si el cliente debe volver a conectarse automáticamente tras una desconexión.

Mensaje de conexión

Especifica si se debe enviar un mensaje cuando se establece una conexión.

Enviar mensaje: Active esta función para enviar mensajes.

Usar predeterminado: Desactive esta opción para introducir su propio mensaje predeterminado.

Topic (Tema): Introduzca el tema para el mensaje predeterminado.

Payload (Carga): Introduzca el contenido para el mensaje predeterminado.

Retain (Retener): Seleccione esta opción para mantener el estado del cliente en este **Tema**

QoS: Cambie la capa de QoS para el flujo de paquetes.

Mensaje de testamento y últimas voluntades

El testamento y últimas voluntades (LWT) permite a un cliente proporcionar un testimonio junto con sus credenciales al conectar con el intermediario. Si el cliente se desconecta de forma no voluntaria (quizá porque no dispone de fuente de alimentación), puede permitir que el intermediario entregue un mensaje a otros clientes. Este mensaje de LWT tiene el mismo formato que un mensaje normal y se enruta a través de la misma mecánica.

Enviar mensaje: Active esta función para enviar mensajes.

Usar predeterminado: Desactive esta opción para introducir su propio mensaje predeterminado.

Topic (Tema): Introduzca el tema para el mensaje predeterminado.

Payload (Carga): Introduzca el contenido para el mensaje predeterminado.

Retain (Retener): Seleccione esta opción para mantener el estado del cliente en este **Tema**

QoS: Cambie la capa de QoS para el flujo de paquetes.

Publicación MQTT

Usar prefijo de tema predeterminado: Seleccione esta opción para utilizar el prefijo de tema predeterminado, que se define en el prefijo de tema del dispositivo en la pestaña **Cliente MQTT**.

Include condition (Incluir condición): Seleccione esta opción para incluir el tema que describe la condición en el tema de MQTT.

Include namespaces (Incluir espacios de nombres): Seleccione esta opción para incluir los espacios de nombres de los temas ONVIF en el tema MQTT.

Include serial number (Incluir número de serie): seleccione esta opción para incluir el número de serie del dispositivo en la carga útil de MQTT.

Add condition (Agregar condición): Haga clic para agregar una condición.

Retain (Retener): define qué mensajes MQTT se envían como retenidos.

- **None (Ninguno)**: envíe todos los mensajes como no retenidos.
- **Property (Propiedad)**: envíe únicamente mensajes de estado como retenidos.
- **Todo**: Envíe mensajes con estado y sin estado como retenidos.

QoS: Seleccione el nivel deseado para la publicación de MQTT.

Suscripciones MQTT

Add subscription (Agregar suscripción): Haga clic para agregar una nueva suscripción MQTT.

Filtro de suscripción: Introduzca el tema de MQTT al que desea suscribirse.

Usar prefijo de tema del dispositivo: Agregue el filtro de suscripción como prefijo al tema de MQTT.

Tipo de suscripción:

- **Sin estado**: Seleccione esta opción para convertir mensajes MQTT en mensajes sin estado.
- **Con estado**: Seleccione esta opción para convertir los mensajes MQTT en una condición. El contenido se utiliza como estado.

QoS: Seleccione el nivel deseado para la suscripción a MQTT.

Superposiciones MQTT

Nota

Conéctese a un intermediario de MQTT antes de agregar los modificadores de superposición de MQTT.

Add overlay modifier (Agregar modificador de superposición): Haga clic para agregar un nuevo modificador de superposición.

Topic filter (Filtro de tema): Agregue el tema de MQTT que contiene los datos que desea mostrar en la superposición.

Data field (Campo de datos): Especifique la clave para la carga del mensaje que desea mostrar en la superposición, siempre y cuando el mensaje esté en formato JSON.

Modifier (Modificador): Utilice el modificador resultante cuando cree la superposición.

- Los modificadores que empiezan con **#XMP** muestran todos los datos recibidos del tema.
- Los modificadores que empiezan con **#XMD** muestran los datos especificados en el campo de datos.

SIP

Ajustes

Protocolo de inicio de sesión (SIP) se utiliza para sesiones de comunicación interactiva entre los usuarios. Las sesiones pueden incluir elementos de audio y vídeo.

Asistente de configuración de SIP: Haga clic para configurar SIP paso a paso.

Habilitar SIP: active esta opción para que sea posible iniciar y recibir llamadas SIP.

Permitir llamadas entrantes: Seleccione esta opción para permitir llamadas entrantes de otros dispositivos SIP.

Gestión de llamadas

- **Tiempo de espera de llamada**: Defina la duración máxima de una llamada en curso si nadie responde.
- **Duración de llamada entrante**: Defina el tiempo máximo que una llamada entrante puede durar (máx. 10 min.).
- **Terminar llamadas después**: Defina el tiempo máximo que una llamada puede durar (máx. 60 minutos). Seleccione **Duración de llamada infinita** si no desea limitar la longitud de una llamada.

Puertos

Un número de puerto debe estar entre 1024 y 65535.

- **Puerto SIP**: el puerto de red empleado 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)**: el puerto de red empleado 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.
- **Puerto de inicio RTP**: el puerto de red utilizado para la primera transmisión de medios RTP en una llamada SIP. El puerto de inicio predeterminado es el 4000. Algunos cortafuegos bloquean el tráfico RTP en determinados números de puerto.

NAT transversal

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

Nota

Para que NAT transversal funcione, el router debe ser compatible. El router debe ser compatible también con 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 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.

Audio

- **Audio codec priority (Prioridad de códec de audio)**: seleccione al menos un códec de audio con la calidad deseada para las llamadas SIP. Arrastre y coloque para cambiar la prioridad.

Nota

Los códecs seleccionados deben coincidir con el códec destinatario de la llamada, ya que el códec destinatario es fundamental cuando se realiza una llamada.

- **Dirección de audio**: Seleccione las direcciones de audio permitidas.

Adicional

- **Cambiar de UDP a TCP**: Seleccione para permitir que las llamadas cambien de protocolo de transporte de UDP (Protocolo de Datagramas de Usuario) a TCP (Protocolo de Control de la Transmisión)

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.

- **Permitir mediante reescritura**: Seleccione para enviar la dirección IP local en lugar de la dirección IP pública del router.
- **Permitir reescribir contacto**: Seleccione para enviar la dirección IP local en lugar de la dirección IP pública del router.
- **Registrar con servidor cada**: establezca la frecuencia con la que desea que el dispositivo se registre con el servidor SIP para las cuentas SIP existentes.
- **Tipo de carga útil MFDT**: Cambia el tipo de carga útil predeterminado para MFDT.
- **Máximo de retransmisiones**: Puede establecer la cantidad máxima de veces que el dispositivo intenta conectarse al servidor SIP antes de dejar de intentarlo.
- **Segundos hasta la recuperación a prueba de fallos**: Puede establecer la cantidad de segundos hasta que el dispositivo intenta volver a conectarse al servidor SIP principal después de haber conmutado por error a un servidor SIP secundario.

Cuentas

Todas las cuentas SIP actuales se muestran en **Cuentas SIP**. Para cuentas registradas, el círculo de color permite conocer el estado.

La cuenta se ha registrado correctamente con el servidor SIP.

Hay un problema con la cuenta. Algunos de los posibles motivos pueden ser un error de autorización, que las credenciales de la cuenta son incorrectos o que el servidor SIP no puede encontrar la cuenta.

La cuenta **De punto a punto** es una cuenta creada automáticamente. Puede eliminarla si crea, al menos, otra cuenta y la configura como cuenta predeterminada. La cuenta predeterminada se utiliza siempre al realizar una llamada de interfaz de programación de aplicación (API) VAPIX® sin especificar la cuenta SIP desde la que se llama.

Add account (Añadir cuenta): Haga clic para crear una nueva cuenta SIP.

- **Activa**: Seleccione esta opción para poder utilizar la cuenta.
- **Hacer predeterminado**: seleccione esta opción para marcar esta cuenta como predeterminada. Debe existir una cuenta predeterminada y solo puede haber una cuenta predeterminada.
- **Answer automatically (Responder automáticamente)**: seleccione esta opción para responder automáticamente a una llamada entrante.
- **Prioritize IPv6 over IPv4 (Priorizar IPv6 sobre IPv4)** : Seleccione esta opción para dar prioridad a las direcciones IPv6 sobre las direcciones IPv4. Esto resulta útil cuando se conecta a cuentas entre iguales o nombres de dominio que se resuelven en direcciones IPv4 e IPv6. Solo puede dar prioridad a IPv6 para los nombres de dominio que se asignan a direcciones IPv6.
- **Name (Nombre)**: Introduzca un nombre descriptivo. Puede ser, por ejemplo, un nombre y apellido, una función o una ubicación. El nombre no es único.
- **ID de usuario**: introduzca la extensión única o el número de teléfono asignado al dispositivo.
- **De punto a punto**: utilícelo para llamadas directas a otro dispositivo SIP de la red local.
- **Registered (Registrado)**: Utilícelo para llamadas a dispositivos SIP fuera de la red local, a través de un servidor SIP.
- **Dominio**: si se encuentra disponible, introduzca el nombre de dominio público. Se mostrará como parte de la dirección SIP al llamar a otras cuentas.
- **Contraseña**: introduzca la contraseña asociada a la cuenta SIP para la autenticación en el servidor SIP.
- **ID de autenticación**: introduzca el ID de autenticación utilizado para la autenticación en el servidor SIP. Si es el mismo que el ID de usuario, no es necesario especificar el ID de autenticación.
- **ID del emisor de la llamada**: El nombre que se presenta al destinatario de las llamadas realizadas desde el dispositivo.
- **Registrador**: introduzca la dirección IP del registro.
- **Modo de transporte**: seleccione el modo de transporte SIP para la cuenta: UPD, TCP o TLS.
- **Versión de TLS** (solo con el modo de transporte TLS): Seleccione la versión de TLS a usar. Las versiones **v1.2** y **v1.3** son las más seguras. **Automático** selecciona la versión más segura que el sistema puede manejar.
- **Cifrado de medios** (solo con el modo de transporte TLS): seleccione el tipo de cifrado de componentes multimedia (audio y vídeo) para las llamadas SIP.
- **Certificado** (solo con el modo de transporte TLS): Seleccione un certificado.
- **Verificar certificado del servidor** (solo con el modo de transporte TLS): compruebe para verificar el certificado del servidor.
- **Servidor SIP secundario**: active si desea que el dispositivo de Axis intente registrarse en un servidor SIP secundario si se produce un error de registro en el servidor SIP principal.

- **SIP secure (SIP segura)**: seleccione esta opción para utilizar el protocolo de inicio de sesión segura (SIPS). TLS SIPS utiliza el modo de transporte para cifrar el tráfico.
- **Proxies**
  - **Proxy**: haga clic para agregar un proxy.
  - **Priorizar**: si ha agregado dos o más proxies, haga clic para otorgarles prioridades.
  - **Dirección del servidor**: introduzca la dirección IP del servidor proxy SIP.
  - **Nombre de usuario**: si es necesario, introduzca el nombre de usuario para el servidor proxy SIP.
  - **Contraseña**: si es necesario, introduzca la contraseña para el servidor proxy SIP.
- **Vídeo**
  - **Área de visión**: seleccione el área de visión que desee utilizar para las llamadas de vídeo. Si no selecciona ninguna, se utiliza la vista nativa.
  - **Resolución**: seleccione la resolución que desee utilizar para las llamadas de vídeo. La resolución afecta al ancho de banda necesario.
  - **Velocidad de imagen**: seleccione el número de fotogramas por segundo para las llamadas de vídeo. La velocidad de fotogramas afecta al ancho de banda necesario.
  - **Perfil H.264**: Seleccione el perfil que desee utilizar para las llamadas de vídeo.

DTMF

Add sequence (Agregar secuencia): Haga clic para crear una nueva secuencia de multifrecuencia de doble tono (DTMF). Para crear una regla activada por tonos, vaya a **Events > Rules (Eventos > Reglas).**

Secuencia: Introduzca los caracteres para activar la regla. Caracteres admitidos: 0–9, A-D, # y *.

Descripción: Introduzca una descripción de la acción que la secuencia activará.

Accounts (Cuentas): Seleccione las cuentas que utilizarán la secuencia DTMF. Si selecciona **peer-to-peer (punto a punto)**, todas las cuentas de punto a punto compartirán la misma secuencia DTMF.

Protocolos

Seleccione los protocolos que se utilizarán para cada cuenta. Todas las cuentas de punto a punto comparten la misma configuración de protocolo.

Utilizar RTP (RFC2833): Active esta opción para permitir una señalización multifrecuencia de doble tono (MFDT), otras señales de tono y eventos de telefonía en paquetes RTP.

Use SIP INFO (Utilizar SIP INFO) (RFC2976): Active esta opción para incluir el método INFO en el protocolo SIP. El método INFO agrega información de capa de aplicación opcional, generalmente relacionada con la sesión.

Llamada de prueba

Cuenta SIP: Seleccione la cuenta desde la que desea realizar la llamada de prueba.

Dirección SIP: Introduzca una dirección SIP y haga clic en para realizar una llamada de prueba y comprobar que la cuenta funciona.

Controlador de multicast

Controlador de multicast de usuario: Active para activar el controlador de multicast.

Códec de audio: Seleccione un códec de audio.

Source (Fuente): Agregue una nueva fuente de controlador de multicast.

- **Label (Etiqueta)**: Introduzca el nombre de una etiqueta que no haya utilizado ya una fuente.
- **Source (fuente)**: Introduzca una fuente.
- **Puerto**: Introduzca un puerto.
- **Priority (Prioridad)**: Seleccione una prioridad.
- **Profile (Perfil)**: Seleccione un perfil.
- **Clave SRTP**: Introduzca una clave SRTP.

El menú contextual contiene:

Editar: Edite la fuente de controlador de multicast.

Eliminar: Elimine la fuente del controlador de multicast.

Almacenamiento

Almacenamiento de red

Network storage (Almacenamiento de red): Active para usar el almacenamiento de red.

Agregar almacenamiento de red: Haga clic para agregar un recurso compartido de red en el que guardar grabaciones.

- **Dirección**: Introduzca la dirección IP el nombre de host del servidor host, que suele ser un dispositivo de almacenamiento conectado a la red (NAS). Le recomendamos que configure el host para utilizar una dirección IP fija (que no sea DHCP, ya que las direcciones IP dinámicas pueden cambiar) o que utilice DNS. No se admiten los nombres SMB/CIFS de Windows.
- **Recurso compartido de red**: Escriba el nombre de una ubicación de recurso compartido en el servidor host. Varios dispositivos de Axis pueden utilizar el mismo recurso compartido de red, porque cada uno tiene su propia carpeta.
- **Usuario**: Si el servidor requiere un inicio de sesión, escriba el nombre de usuario. Para iniciar sesión en un servidor de dominio concreto, escriba `DOMAIN\username`.
- **Contraseña**: Si el servidor requiere un inicio de sesión, escriba la contraseña.
- **Versión de SMB**: Seleccione la versión del protocolo de almacenamiento SMB para conectarse al NAS. Si selecciona **Auto**, el dispositivo intentará negociar una de las versiones seguras SMB: 3.02, 3.0 o 2.1. Seleccione 1.0 o 2.0 para conectarse a almacenamiento en red tipo NAS más antiguo que no admita versiones superiores. Puede leer más sobre la compatibilidad con SMB en dispositivos Axis *aquí*.
- **Agregar recurso compartido sin pruebas**: Seleccione esta opción para agregar el recurso compartido de red aunque se detecte un error durante la prueba de conexión. El error puede ser, por ejemplo, que no se ha introducido una contraseña y el servidor la requiere.

Remove network storage (Eliminar almacenamiento de red): Haga clic para desinstalar, desvincular y eliminar la conexión con el recurso compartido de red. Así se eliminan todos los ajustes del recurso compartido de red.

Desvincular: Haga clic para desvincular y desconectar el recurso compartido de red.
Bind (Vincular): Haga clic para vincular y conectar el recurso compartido de red.

Unmount (Desmontar): Haga clic para desmontar el recurso compartido de red.
Mount (Montar): Haga clic para montar el recurso compartido de red.

Write protect (Protección contra escritura): Active esta opción para dejar de escribir en el recurso compartido de red y evitar que se eliminen las grabaciones. El formato de un recurso compartido de red protegido contra escritura no se puede cambiar.

Tiempo de conservación: Seleccione el tiempo que desea guardar las grabaciones para limitar la cantidad de grabaciones antiguas o cumplir con la normativa sobre almacenamiento de datos. Si se llena el almacenamiento de red, las grabaciones antiguas se eliminarán antes de que transcurra el periodo de tiempo seleccionado.

Herramientas

- **Test connection (Probar conexión)**: Pruebe la conexión con el recurso compartido de red.
- **Format (Formato)**: Formatee el recurso compartido de red, por ejemplo, cuando tenga que borrar rápidamente todos los datos. CIFS es la opción del sistema de archivos disponible.

Usar herramienta: Haga clic para activar la herramienta seleccionada.

ONVIF

Cuentas de ONVIF

ONVIF (Open Network Video Interface Forum) es un estándar de interfaz internacional que facilita que los usuarios finales, los integradores, los consultores y los fabricantes se beneficien de las distintas opciones que ofrece la tecnología de vídeo en red. ONVIF permite la interoperabilidad entre productos de distintos proveedores, proporciona mayor flexibilidad, costes reducidos y sistemas preparados para el futuro.

Al crear una cuenta ONVIF, se permite automáticamente la comunicación ONVIF. Utilice el nombre de cuenta y la contraseña para todas las comunicaciones ONVIF con el dispositivo. Para obtener más información, consulte la comunidad de desarrolladores de Axis en *axis.com*.

Agregar cuentas: Haga clic para agregar una nueva cuenta ONVIF.

Cuenta: introduzca un nombre de cuenta único.

Nueva contraseña: introduzca una contraseña para la cuenta. Las contraseñas deben tener entre 1 y 64 caracteres. La contraseña solo admite caracteres ASCII imprimibles (códigos de 32 a 126), por ejemplo, letras, números, signos de puntuación y algunos símbolos.

Repetir contraseña: Introduzca la misma contraseña de nuevo.

Privilegios:

- **Administrador**: Tiene acceso completo a todos los ajustes. Los administradores también pueden agregar, actualizar y eliminar otras cuentas.
- **Operator (Operador)**: Tiene acceso a todos los ajustes excepto:
  - Todos los ajustes del **sistema**.
  - Agregar aplicaciones.
- **Cuenta de medios**: Permite acceder solo al flujo de vídeo.

El menú contextual contiene:

Actualizar cuenta: Editar las propiedades de la cuenta.

Eliminar cuenta: Elimine la cuenta. No puede eliminar la cuenta de root.

Perfiles multimedia de ONVIF

Un perfil de medios ONVIF está formado por un conjunto de configuraciones que puede utilizar para cambiar la configuración de flujo de medios. Puede crear nuevos perfiles con su propio conjunto de configuraciones o utilizar perfiles preconfigurados para una configuración rápida.

Añadir perfil de medios: Haga clic para agregar un nuevo perfil de medios ONVIF.

Nombre de perfil: Agregue un nombre para el perfil multimedia.

Fuente de vídeo: Seleccione la fuente de video para su configuración.

- **Seleccionar configuración**: Seleccione de la lista una configuración definida por el usuario. Las configuraciones en la lista desplegable corresponden a los canales de video del dispositivo, incluidas vistas múltiples, áreas de visualización y canales virtuales.

Video encoder (Codificador de vídeo): Seleccione el formato de codificación de video para su configuración.

- **Seleccionar configuración**: Seleccione una configuración definida por el usuario de la lista y ajuste la configuración de codificación. Las configuraciones en la lista desplegable actúan como identificadores/nombres de la configuración del codificador de video. Seleccione el usuario del 0 al 15 para aplicar sus propios ajustes, o seleccione uno de los usuarios predeterminados si desea utilizar configuraciones predefinidas para un formato de codificación específico.

Nota

Habilite el audio en el dispositivo para tener la opción de seleccionar una fuente de audio y una configuración del codificador de audio.

Fuente de audio : Seleccione la fuente de entrada de audio para su configuración.

- **Seleccionar configuración**: Seleccione una configuración definida por el usuario de la lista y ajuste la configuración de audio. Las configuraciones de la lista desplegable corresponden a las entradas de audio del dispositivo. Si el dispositivo tiene una entrada de audio, es usuario0. Si el dispositivo tiene varias entradas de audio, habrá usuarios adicionales en la lista.

Codificador de audio : Selecciona el formato de codificación de audio para tu configuración.

- **Seleccionar configuración**: Seleccione una configuración definida por el usuario de la lista y ajuste la configuración de codificación de audio. Las configuraciones de la lista desplegable actúan como identificadores/nombres de la configuración del codificador de audio.

Descodificador de audio : Seleccione el formato de descodificación de audio para su configuración.

- **Seleccionar configuración**: Seleccione una configuración definida por el usuario de la lista y ajuste la configuración. Las configuraciones de la lista desplegable actúan como identificadores/nombres de la configuración.

Salida de audio : Seleccione el formato de salida de audio para su configuración.

- **Seleccionar configuración**: Seleccione una configuración definida por el usuario de la lista y ajuste la configuración. Las configuraciones de la lista desplegable actúan como identificadores/nombres de la configuración.

Metadatos: Seleccione los metadatos para incluir en su configuración.

- **Seleccionar configuración**: Seleccione una configuración definida por el usuario de la lista y ajuste la configuración de los metadatos. Las configuraciones de la lista desplegable actúan como identificadores/nombres de la configuración de metadatos.

PTZ : Seleccione los ajustes de PTZ para su configuración.

- **Seleccionar configuración**: Seleccione una configuración definida por el usuario de la lista y ajuste la configuración PTZ. Las configuraciones en la lista desplegable corresponden a los canales de video del dispositivo con soporte PTZ.

Create (Crear): Haga clic para guardar los ajustes y crear el perfil.

Cancelar: Haga clic para cancelar la configuración y borrar todas los ajustes.

profile_x: Haga clic en el nombre del perfil para abrir y editar el perfil preconfigurado.

Detectores

Detección de audio

Estos ajustes están disponibles para cada entrada de audio.

Nivel de sonido: Ajuste el nivel de sonido a un valor de 0-100, donde 0 es el nivel más sensible y 100 el menos sensible. Al configurar el nivel de sonido, utilice el indicador de actividad como guía. Al crear eventos, puede utilizar el nivel de sonido como una condición. Puede elegir desencadenar una acción si el nivel de sonido se eleva por encima o por debajo del valor establecido.

Registros

Informes y registros

Informes

- **Ver informe del servidor del dispositivo**: Consulte información acerca del estado del producto en una ventana emergente. El registro de acceso se incluye automáticamente en el informe del servidor.
- **Download the device server report (Descargar informe del servidor del dispositivo)**: Se crea un archivo .zip que contiene un archivo de texto con el informe del servidor completo en formato UTF–8 y una instantánea de la imagen de visualización en directo actual. Incluya siempre el archivo. zip del informe del servidor si necesita contactar con el servicio de asistencia.
- **Download the crash report (Descargar informe de fallos)**: Descargar un archivo con la información detallada acerca del estado del servidor. El informe de fallos incluye información ya presente en el informe del servidor, además de información detallada acerca de la corrección de fallos. Este informe puede incluir información confidencial, como trazas de red. Puede tardar varios minutos en generarse.

Registros

- **View the system log (Ver registro del sistema)**: Haga clic para consultar información acerca de eventos del sistema como inicio de dispositivos, advertencias y mensajes críticos.
- **View the access log (Ver registro de acceso)**: Haga clic para ver todos los intentos incorrectos de acceso al dispositivo, por ejemplo, si se utiliza una contraseña de inicio de sesión incorrecta.
- **View the audit log (Ver registro de auditoría)**: Haga clic para mostrar información sobre las actividades del usuario y del sistema, por ejemplo, autentificaciones y configuraciones correctas o fallidas.

Registro de sistema remoto

Syslog es un estándar de registro de mensajes. Permite que el software que genera los mensajes, el sistema que los almacena y el software que los notifica y analiza sean independientes. Cada mensaje se etiqueta con un código de instalación, que indica el tipo de software que genera el mensaje y tiene un nivel de gravedad.

Server (Servidor): Haga clic para agregar un nuevo servidor.

Host: introduzca el nombre de host o la dirección IP del servidor.

Format (Formato): Seleccione el formato de mensaje de syslog que quiera utilizar.

- Axis
- RFC 3164
- RFC 5424

Protocol (Protocolo): Seleccione el protocolo que desee utilizar:

- UDP (el puerto predeterminado es 514).
- TCP (el puerto predeterminado es 601).
- TLS (el puerto predeterminado es 6514).

Puerto: Modifique el número de puerto para usar otro puerto.

Severity (Gravedad): Seleccione los mensajes que se enviarán cuando se activen.

Tipo: Seleccione el tipo de registros que desea enviar.

Test server setup (Probar configuración del servidor): Envíe un mensaje de prueba a todos los servidores antes de guardar la configuración.

CA certificate set (Conjunto de certificados de CA): Consulte los ajustes actuales o añada un certificado.

Configuración sencilla

La configuración sencilla está destinada a usuarios con experiencia en la configuración de dispositivos Axis. La mayoría de los parámetros se pueden definir y editar desde esta página.

Mantenimiento

Mantenimiento

Restart (Reiniciar): Reiniciar el dispositivo. No afectará a la configuración actual. Las aplicaciones en ejecución se reinician automáticamente.

Restore (Restaurar): Casi todos los ajustes vuelven a los valores predeterminados de fábrica. Después deberás reconfigurar el dispositivo y las aplicaciones, reinstalar las que no vinieran preinstaladas y volver a crear los eventos y preajustes.

Importante

Los únicos ajustes que se guardan después de una restauración son:

- Protocolo de arranque (DHCP o estático)
- Dirección IP estática
- Router predeterminado
- Máscara de subred
- Configuración 802.1X
- Configuración de O3C
- Dirección IP del servidor DNS

Factory default (Predeterminado de fábrica): Todos los ajustes vuelven a los valores predeterminados de fábrica. Después, es necesario restablecer la dirección IP para poder acceder al dispositivo.

Nota

Todo el software de los dispositivos AXIS está firmado digitalmente para garantizar que solo se instala software verificado. Esto aumenta todavía más el nivel mínimo general de ciberseguridad de los dispositivo de Axis. Para obtener más información, consulte el documento técnico "Axis Edge Vault" en *axis.com*.

Actualización de AXIS OS: Se actualiza a una nueva versión de AXIS OS. Las nuevas versiones pueden contener mejoras de funciones, correcciones de errores y características totalmente nuevas. Le recomendamos que utilice siempre la versión de AXIS OS más reciente. Para descargar la última versión, vaya a *axis.com/support*.

Al actualizar, puede elegir entre tres opciones:

- **Standard upgrade (Actualización estándar)**: Se actualice a la nueva versión de AXIS OS.
- **Factory default (Predeterminado de fábrica)**: Se actualiza y todos los ajustes vuelven a los valores predeterminados de fábrica. Si elige esta opción, no podrá volver a la versión de AXIS OS anterior después de la actualización.
- **Automatic rollback (Restauración automática)**: Se actualiza y debe confirmar la actualización en el plazo establecido. Si no confirma la actualización, el dispositivo vuelve a la versión de AXIS OS anterior.

Restaurar AXIS OS: Se vuelve a la versión anterior de AXIS OS instalado.

solucionar problemas

Reset PTR (Restablecer PTR) : Restablezca el ajuste PTR si, por alguna razón, los ajustes de **Pan (Movimiento horizontal)**, **Tilt (Movimiento vertical)** o **Roll (Giro)** no funcionan de la forma prevista. Los motores PTR se calibran siempre en una cámara nueva. Sin embargo, la calibración se puede perder, por ejemplo, si la cámara pierde la alimentación o si los motores se mueven a mano. Al restablecer PTR, la cámara se vuelve a calibrar y vuelve a su posición predeterminada de fábrica.

Calibration (Calibración) : Haga clic en **Calibrate (Calibrar)** para recalibrar los motores de movimiento horizontal, movimiento vertical y giro a sus posiciones predeterminadas.

Ping: Para comprobar si el dispositivo puede llegar a una dirección específica, introduzca el nombre de host o la dirección IP del host al que desea hacer ping y haga clic en **Start (Iniciar)**.

Port check (Comprobación del puerto): Para verificar la conectividad del dispositivo con una dirección IP y un puerto TCP/UDP específicos, introduzca el nombre de host o la dirección IP y el número de puerto que desea comprobar; después, haga clic en **Start (Iniciar)**.

Rastreo de red

Importante

Un archivo de rastreo de red puede contener información confidencial, como certificados o contraseñas.

Un archivo de rastreo de red puede ayudar a solucionar problemas mediante la grabación de la actividad en la red.

Trace time (Tiempo de rastreo): Seleccione la duración del rastreo en segundos o minutos y haga clic en **Descargar**.

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.

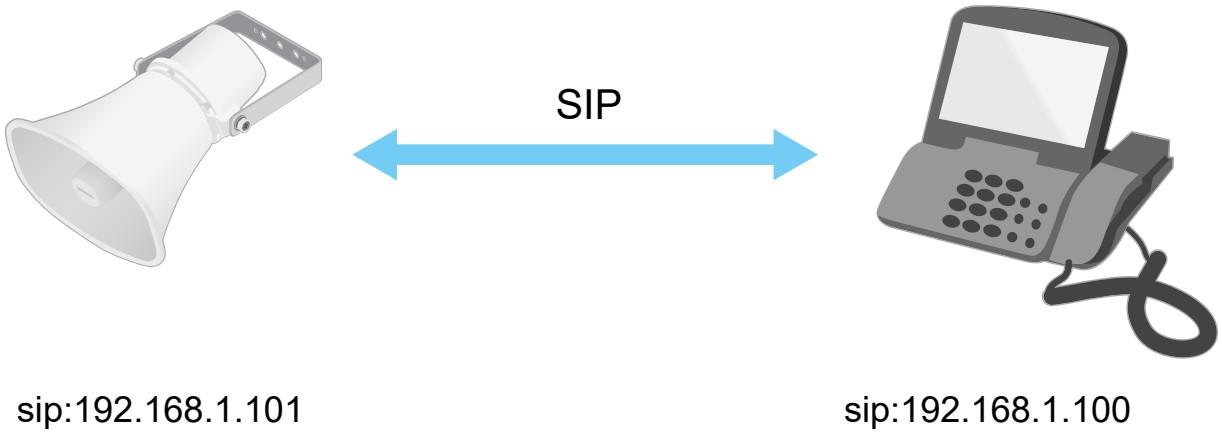
El audio o el vídeo real se intercambian entre los agentes de usuario SIP con un protocolo de transporte, por ejemplo, RTP (protocolo de transporte en tiempo real).

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.

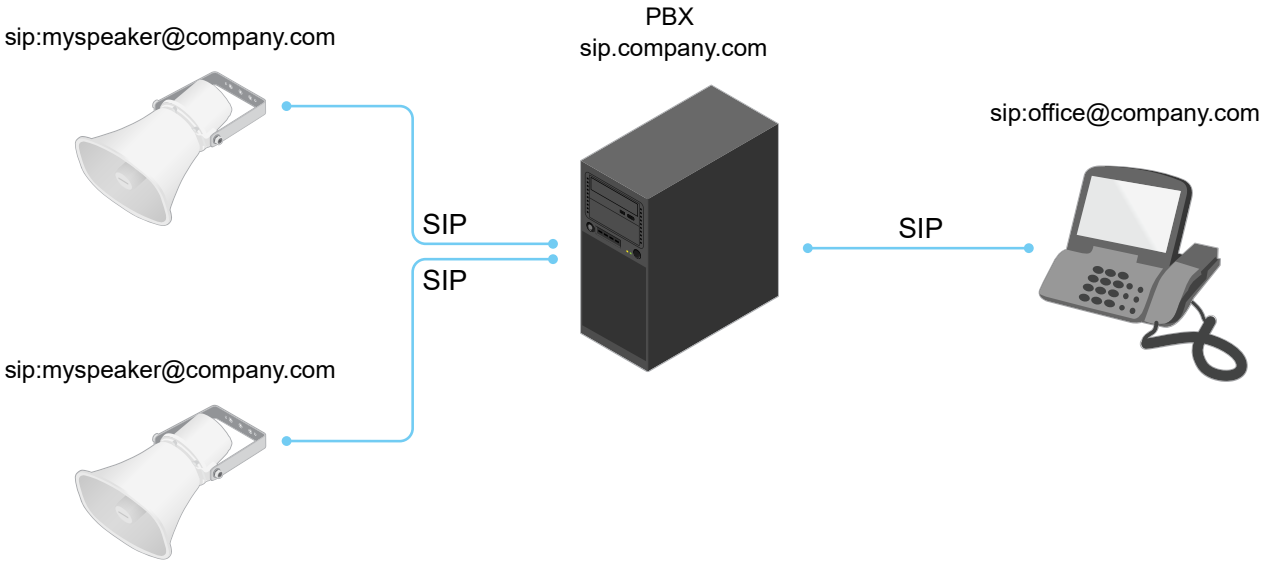
Centralita telefónica privada (PBX)

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*.

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*.

AXIS Client for Unified Communication Systems

Con esta aplicación, puede realizar llamadas entre dispositivos Axis habilitados para SIP y cuentas vinculadas de Microsoft® Teams. Para obtener más información, consulte el *manual de usuario de AXIS Client for Unified Communication Systems*.

Ciberseguridad

Para obtener información específica sobre ciberseguridad, consulte la ficha técnica del producto en axis.com.

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

Axis Edge Vault

Axis Edge Vault es una plataforma de ciberseguridad basada en hardware que protege el dispositivo Axis. Ofrece características que garantizan la identidad e integridad del dispositivo y protegen su información confidencial frente a accesos no autorizados. Tiene dos sólidos pilares: los módulos de computación criptográfica (elemento seguro y TPM) y la seguridad del SoC (TEE y arranque seguro), combinados con una amplia experiencia en la seguridad de los dispositivos en el extremo.

SO firmado

El sistema operativo firmado lo implementa el proveedor del software que firma la imagen de AXIS OS con una clave privada. Cuando la firma se une al sistema operativo, el dispositivo validará el software antes de instalarlo. Si el dispositivo detecta que la integridad del software está comprometida, se rechazará la actualización de AXIS OS.

Arranque seguro

El arranque seguro es un proceso de arranque que consta de una cadena ininterrumpida de software validado criptográficamente, comenzando por la memoria inmutable (ROM de arranque). Al estar basado en el uso del sistema operativo firmado, el arranque seguro garantiza que un dispositivo pueda iniciarse solo con un software autorizado.

Almacén de claves seguro

Un entorno protegido contra manipulaciones para la protección de claves privadas y la ejecución segura de operaciones criptográficas. Impide el acceso sin autorización y las extracciones maliciosas en caso de incidentes de seguridad. En función de los requisitos de seguridad, un dispositivo Axis puede tener uno o varios módulos de computación criptográfica basados en hardware, el lugar donde se encuentra el almacén de claves seguro protegido por el hardware. En función de los requisitos de seguridad, un dispositivo Axis puede tener uno o varios módulos de computación criptográficos basados en hardware, como un TPM 2.0 (Módulo de plataforma segura) o un elemento seguro, o un TEE (Entorno de ejecución de confianza), que ofrecen un almacén de claves seguro protegido por hardware. Además, algunos productos Axis cuentan con un almacén de claves seguro con certificación FIPS 140-2 Nivel 2.

ID de dispositivo de Axis

la posibilidad de verificar el origen del dispositivo es fundamental para poder confiar en su identidad. Durante la producción, se asigna a los dispositivos con Axis Edge Vault un certificado de ID de dispositivo de Axis único y conforme con el estándar IEEE 802.1AR en la propia fábrica. Es como una especie de pasaporte para demostrar el origen del dispositivo. El ID de dispositivo se guarda de forma segura y permanente en el almacén de claves seguro como certificado firmado por el certificado raíz de Axis. La infraestructura de TI del cliente puede utilizar el ID de dispositivo en la incorporación segura automatizada de dispositivos y en la identificación segura de dispositivos

Sistema de archivos cifrado

El almacén de claves seguro impide la filtración maliciosa de información y evita que pueda manipularse la configuración aplicando un potente cifrado al sistema de archivos. Esto garantiza que no se puedan extraer ni manipular datos almacenados en el sistema de archivos cuando no se use el dispositivo, durante un acceso no autorizado al dispositivo o si alguien roba el dispositivo Axis. Durante el proceso de arranque seguro, se descifra el sistema de archivos de lectura/escritura y el dispositivo Axis puede montarlo y utilizarlo.

Para obtener más información sobre las características de ciberseguridad de los dispositivos Axis, vaya a *axis.com/learning/white-papers* y busque ciberseguridad.

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*.

Gestión de las vulnerabilidades

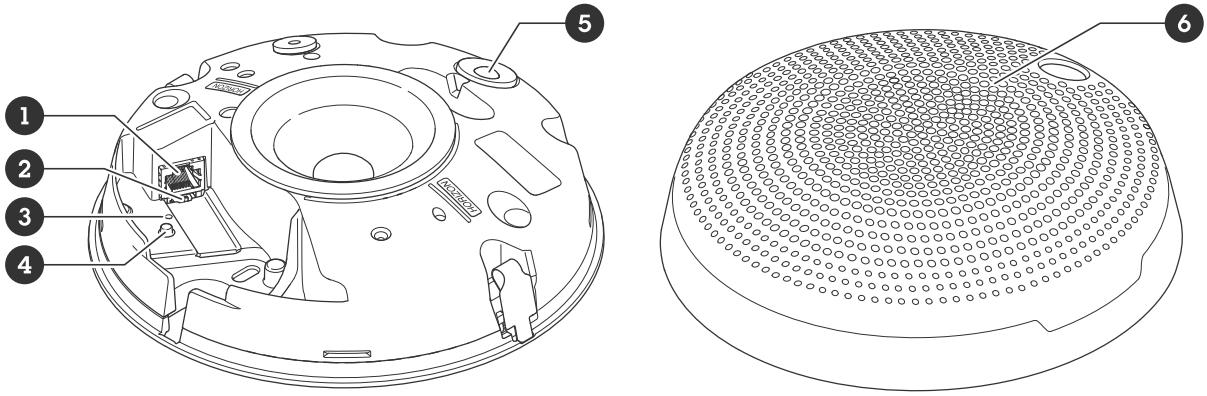
Para minimizar el riesgo de exposición de los clientes, Axis, como **autoridad de numeración común (CNA) de vulnerabilidades y exposiciones comunes (CVE)**, sigue los estándares del sector para gestionar y responder a las vulnerabilidades detectadas en nuestros dispositivos, software y servicios. Para 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*.

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 descubrir más sobre 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*.

Especificaciones

Guía de productos



1 *Conector de red*
2 *Interruptor del micrófono*
3 *Indicador LED de estado*
4 *Botón de control*
5 *Sensor PIR y LED frontal*
6 *Cubierta*

Indicadores LED

LED de estado	Indicación
Apagado	Apagado para indicar un funcionamiento normal.
Verde	Fijo durante 10 segundos para indicar un funcionamiento normal después de completar el inicio.
Ámbar	Fijo durante el inicio. Parpadea durante la actualización del software del dispositivo o el restablecimiento a la configuración predeterminada de fábrica.
Ámbar/rojo	Parpadea si la conexión a la red no está disponible o se ha perdido.
Rojo	Parpadea lentamente si la actualización ha fallado.
Rojo/verde	Parpadea rápidamente cuando se selecciona **Locate device (Localizar dispositivo)**.

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 65*.

Interruptor de desactivación de micrófono

Para conocer la ubicación del interruptor de desactivación de micrófono, consulte *Guía de productos, on page 62*.

El interruptor de desactivación de micrófono se utiliza mecánicamente para que el micrófono permanezca **ON (encendido)** u **OFF (apagado)**. La configuración predeterminada de fábrica para 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*.

Comandos API

VAPIX® es una API (interfaz de programación de aplicaciones) abierta de AXIS. Puede controlar casi todas las funciones disponibles en los dispositivos de AXIS través de VAPIX®. Para obtener acceso a la documentación completa de VAPIX®, únase a la comunidad de desarrolladores de AXIS en *axis.com/developer-community*

Introduzca los comandos en un navegador web y reemplace `<deviceIP>` con la dirección IP o el nombre de host de su dispositivo.

Importante

Los comandos de la API se ejecutan inmediatamente. Si restaura o restablece el dispositivo, se perderán todos los ajustes. Por ejemplo, las reglas de acción.

Ejemplo: Request
Reiniciar el dispositivo
Request
`http://<deviceIP>/axis-cgi/restart.cgi`

Ejemplo: Request
Restaurar el dispositivo. La solicitud devuelve la mayoría de los ajustes a los valores predeterminados, pero mantiene el número IP.
Request
`http://<deviceIP>/axis-cgi/factorydefault.cgi`

Ejemplo: Request
Restablecer el dispositivo. La solicitud devuelve todos los ajustes, incluido el número de IP, a los valores predeterminados.
Request
`http://<deviceIP>/axis-cgi/hardfactorydefault.cgi`

Ejemplo: Request
Consulte una lista de todos los parámetros del dispositivo.
Request
`http://<deviceIP>/axis-cgi/param.cgi?action=list`

Ejemplo: Request
Obtener un archivo de depuración
Request
`http://<deviceIP>/axis-cgi/debug/debug.tgz`

Ejemplo: Request
Obtener un informe de servidor
Request
`http://<deviceIP>/axis-cgi/serverreport.cgi`

Ejemplo: Request
Capturar una traza de la red de 300 segundos
Request
`http://<deviceIP>/axis-cgi/debug/debug.tgz?cmd=pcapdump&duration=300`

Ejemplo: Request
Activar FTP
Request
`http://<deviceIP>/axis-cgi/param.cgi?action=update&Network.FTP.Enabled=yes`

Ejemplo: Request
Desactivar FTP
Request
`http://<deviceIP>/axis-cgi/param.cgi?action=update&Network.FTP.Enabled=no`

Ejemplo: Request
Activar SSH
Request
`http://<deviceIP>/axis-cgi/param.cgi?action=update&Network.SSH.Enabled=yes`

Ejemplo: Request
Desactivar SSH
Request
`http://<deviceIP>/axis-cgi/param.cgi?action=update&Network.SSH.Enabled=no`

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 62*.
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*.

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*.

1. Descargue en su ordenador el archivo de AXIS OS, disponible de forma gratuita en *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 65*.

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*.

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 µ 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.

Si no encuentra aquí lo que busca, pruebe a visitar la sección de solución de problemas en *axis.com/support*.

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*.

T10208067_es

2026-01 (M10.2)