

AXIS C1410 Mk II Network Mini Speaker

Índice

Presentación esquemática de la solución.....	4
.....	4
Instalación.....	5
.....	5
Cómo funciona.....	6
Localice el dispositivo en la red.....	6
Compatibilidad con navegadores.....	6
Abrir la interfaz web del dispositivo	6
Crear una cuenta de administrador	6
Contraseñas seguras.....	7
Asegúrese de que nadie ha manipulado el software del dispositivo	7
Información general de la interfaz web.....	7
Configure su dispositivo.....	8
Calibración y ejecución de un altavoz remoto.....	8
Configurar SIP directo (P2P)	8
Configurar SIP a través de un servidor (PBX).....	9
Configurar reglas para eventos	9
Enviar un correo electrónico si se produce un error de comprobación de altavoz	10
Reproducir audio cuando una cámara detecta movimiento	11
Detener audio con DTMF	11
Configuración de audio para llamadas SIP entrantes	12
Interfaz web.....	14
Descubrir más.....	15
Protocolo de inicio de sesión (SIP).....	15
Peer-to-peer SIP (SIP de punto a punto):	15
Centralita telefónica privada (PBX).....	15
NAT transversal.....	16
Análíticas y aplicaciones.....	16
AXIS Audio Analytics.....	16
AXIS Client for Unified Communication Systems	17
Ciberseguridad.....	17
Axis Edge Vault	17
SO firmado	17
Arranque seguro.....	17
Almacén de claves seguro.....	17
ID de dispositivo de Axis.....	17
Sistema de archivos cifrado	18
Servicio de notificación de seguridad de Axis.....	18
Gestión de las vulnerabilidades	18
Funcionamiento seguro de dispositivos Axis	18
Especificaciones.....	19
Guía de productos	19
Indicadores LED.....	19
Botones.....	20
Botón de control	20
Interruptor de desactivación de micrófono	20
Conectores	20
Conector de red.....	20
Comandos API	21
Localización de problemas	22
Restablecimiento a la configuración predeterminada de fábrica	22
Opciones de AXIS OS	22
Comprobar la versión de AXIS OS.....	22

Actualización de AXIS OS	23
Problemas técnicos y posibles soluciones	23
Consideraciones sobre el rendimiento.....	26
Contactar con la asistencia técnica	26

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*.



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

Una descripción general de cómo funciona el audio en red.

Instalación



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

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

Crear una cuenta de administrador

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

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

Importante

El dispositivo no tiene una cuenta predeterminada. Si pierde la contraseña de la cuenta de administrador, debe restablecer el dispositivo. Vea *Restablecimiento a la configuración predeterminada de fábrica*, on page 22.

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 22*.
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 19 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 15.

Para más información sobre las opciones de ajustes, consulte .

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

Nota

Utilice NAT transversal cuando el dispositivo se conecta a la red desde un router NAT o un firewall. Para obtener más información vea *NAT transversal*, on page 16.

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 15.

Para más información sobre las opciones de ajustes, consulte .

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

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 **Description (Descripción)**, introduzca "detener audio".
8. Haga clic en **Save (Guardar)**.
9. Vaya a **System (Sistema) > Events (Eventos) > Rules (Reglas)** y haga clic en **+ Add a rule (Agregar una regla)**.
10. En **Name (Nombre)**, introduzca "Detener audio DTMF".
11. En **Condition (Condición)**, seleccione **DTMF**.
12. En **DTMF Event ID (Identificación evento)**, seleccione **stop audio (detener audio)**.
13. En **Action (Acción)**, seleccione **Stop playing audio clip (Detener reproducción de fragmento de audio)**.
14. Haga clic en **Save (Guardar)**.

Configuración de audio para llamadas SIP entrantes

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

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

Habilitar ajustes SIP:

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

Reproducción de audio cuando se recibe una llamada SIP:

1. Vaya a **Settings > System > Events > Rules (Ajustes > Sistema > Eventos > Reglas)** y añada una regla.
2. Escriba un nombre para la regla.
3. En la lista de condiciones, seleccione **State (Estado)**.
4. En la lista de estados, seleccione **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 **Ringling** (Sonando).
9. En la lista de acciones, seleccione **Answer call** (Responder llamada).
10. Haga clic en **Save** (Guardar).

Interfaz web

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

Descubrir más

Protocolo de inicio de sesión (SIP)

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

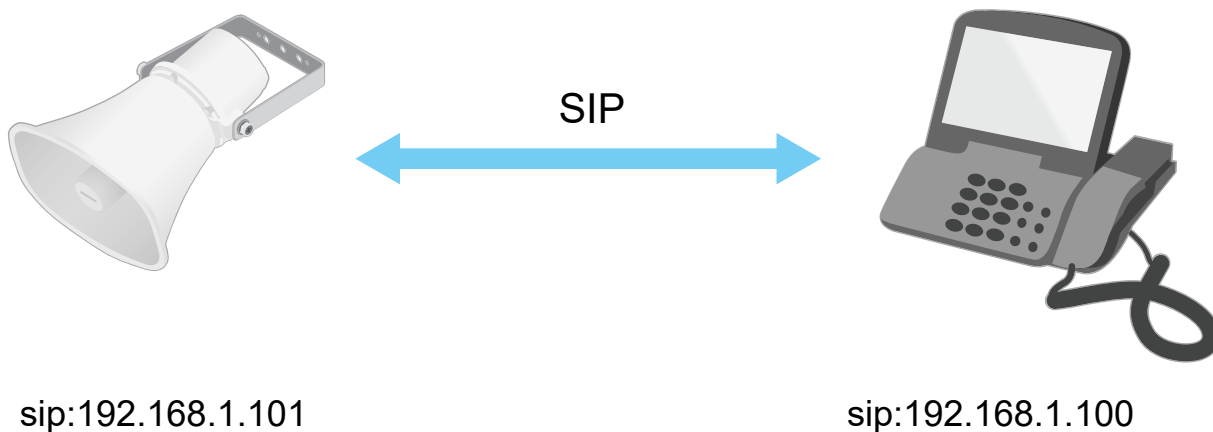
El audio o el vídeo real se intercambian entre los agentes de usuario SIP con un protocolo de transporte, por ejemplo, RTP (protocolo de transporte en tiempo real).

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

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

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

Ejemplo:



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

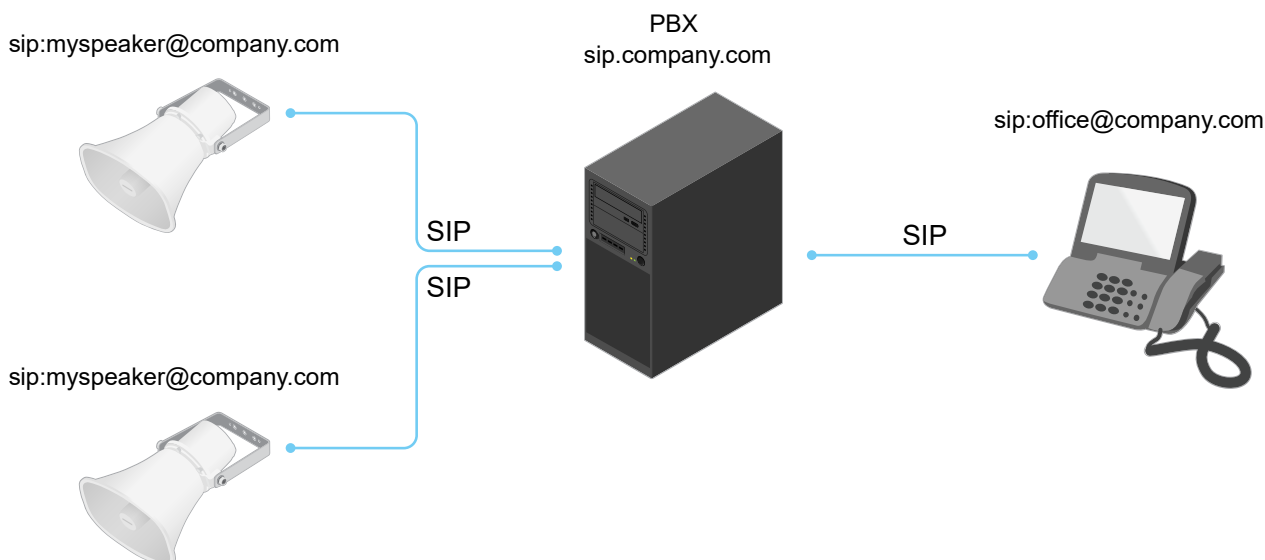
Centralita telefónica privada (PBX)

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

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

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

Ejemplo:



NAT transversal

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

Nota

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

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

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

Analíticas y aplicaciones

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

Para encontrar los manuales de usuario de analíticas y apps de Axis, visite help.axis.com.

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

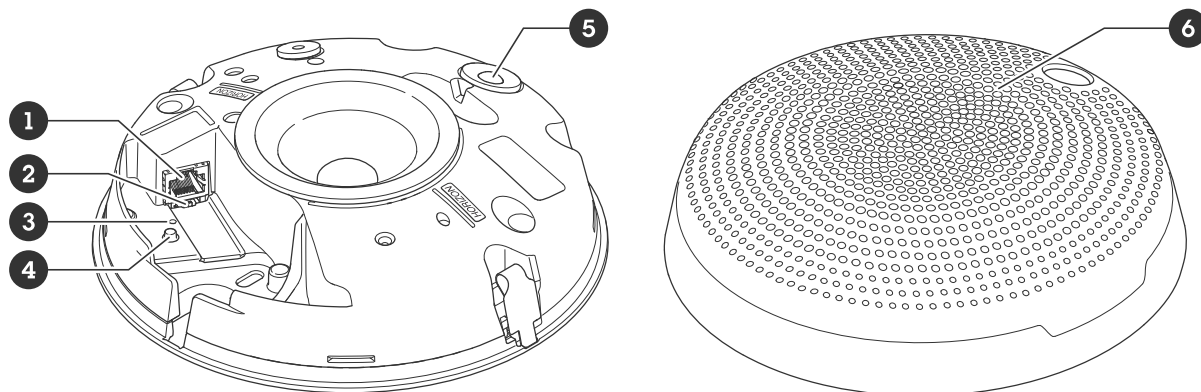
Para minimizar el riesgo de exposición de los clientes, Axis, como **autoridad de numeración común (CNA) de vulnerabilidades y exposiciones comunes (CVE)**, sigue los estándares del sector para gestionar y responder a las vulnerabilidades detectadas en nuestros dispositivos, software y servicios. Para 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 conocer mejor el enfoque de Axis en materia de ciberseguridad, incluidas las buenas prácticas, los recursos y las directrices para la protección de sus dispositivos, vaya a axis.com/about-axis/cybersecurity.

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 22.

Interruptor de desactivación de micrófono

Para conocer la ubicación del interruptor de desactivación de micrófono, consulte *Guía de productos*, on page 19.

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 19.
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 22*.

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.

Problemas con el funcionamiento del dispositivo

El calefactor delantero y el limpiaparabrisas no funcionan

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

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

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

2026-02 (M11.2)

© 2024 – 2026 Axis Communications AB