

AXIS D6310 Air Quality Sensor

Índice

Instalación	4
Cómo funciona	5
.....	5
Localice el dispositivo en la red.....	5
Compatibilidad con navegadores.....	5
Abrir la interfaz web del dispositivo	5
Crear una cuenta de administrador	5
Contraseñas seguras.....	6
Asegúrese de que nadie ha manipulado el software del dispositivo	6
Configure su dispositivo.....	7
Configurar el monitor de calidad del aire	7
Configurar el panel de control del sensor de calidad del aire	7
Configurar el sensor de calidad del aire.....	8
Descargar estadísticas de datos del sensor.....	8
Calibración ante el primer uso del dispositivo	9
Configurar un perfil.....	9
Configurar un perfil con un archivo de audio de sirena personalizado.....	9
Importar o exportar un perfil	10
Configurar SIP directo (P2P).....	10
Configurar SIP a través de un servidor (PBX).....	11
Configurar reglas para eventos	11
Activar una acción.....	12
Grabar vídeo cuando detecta el uso de vapers.....	12
Reproducir clip de audio cuando el nivel de CO2 sea demasiado alto.....	12
Activar un perfil de luz y sirena mediante el sensor PIR.....	13
Iniciar un perfil cuando se active una alarma.....	13
Iniciar un perfil a través de SIP.....	14
Uso de extensiones SIP para controlar más de un perfil.....	14
Ejecutar dos perfiles con diferentes prioridades.....	15
Activar un perfil de luz y sirena mediante publicación HTTP cuando una cámara detecte movimiento	15
Activar un perfil de luz y sirena mediante entrada virtual cuando una cámara detecte movimiento	17
Activar un perfil de luz y sirena en MQTT cuando una cámara detecte movimiento.....	18
Enviar un correo electrónico si se produce un error de comprobación de altavoz	19
Reproducir clip personalizado al activar una alarma	20
Detener audio con DTMF	21
Configuración de audio para llamadas SIP entrantes	22
Interfaz web.....	23
Estado.....	23
Vídeo	24
Flujo.....	24
Sensor de calidad del aire.....	25
Panel.....	25
Ajustes	29
Estadísticas.....	31
Análítica	31
AXIS Audio Analytics.....	31
Audio.....	32
Configuración del dispositivo	32
Flujo.....	33
Clips de audio	33
Mejora de audio	33

Descripción general	33
Perfiles.....	34
Grabaciones.....	36
Medios.....	37
Aplicaciones	37
Sistema.....	38
Hora y ubicación	38
Red	39
Seguridad	43
Cuentas.....	48
Eventos	51
MQTT	56
SIP.....	59
Almacenamiento	64
Perfiles de transmisión	65
ONVIF.....	66
Detectores	69
Ajustes de energía	69
Accesorios	69
Registros	70
Configuración sencilla.....	71
Mantenimiento.....	72
Mantenimiento	72
solucionar problemas	73
Especificaciones.....	74
Guía de productos	74
.....	74
LED de estado	75
Botones.....	75
Botón de control	75
Interruptor del micrófono	75
Conectores	75
Conector de red.....	75
Conector de E/S.....	75
Conector RS485/RS422	76
Nombres de patrones de luz	77
Nombres de patrones de sirena	77
Limpie su dispositivo	79
Localización de problemas	80
Restablecimiento a la configuración predeterminada de fábrica	80
Problemas técnicos, consejos y soluciones.....	80
Consideraciones sobre el rendimiento.....	81
Contactar con la asistencia técnica	82

Instalación

Importante

- Manténgase al menos a 1,5 metros de las zonas con respiraderos importantes o fuentes de contaminación. Esto incluye rejillas de ventilación, puertas, ventanas, zonas de preparación de alimentos, etc.
- Instale el dispositivo en un lugar que permita la libre circulación del aire.
- Para garantizar una detección eficaz de vapores o tabaco, instale el dispositivo en el techo a una altura de entre 2,4 y 2,7 metros del suelo.
- Para garantizar una supervisión eficaz de la calidad del aire y control ambiental, instale el dispositivo a una altura de entre 0,9 y 1,8 metros del suelo.

Para obtener instrucciones de instalación detalladas, consulte la guía de instalación.

Cómo funciona

⚠ ADVERTENCIA

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

Localice el dispositivo en la red

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

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 .

Para obtener descripciones de todos los controles y opciones de la interfaz web del dispositivo, consulte .

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 .
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 .

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

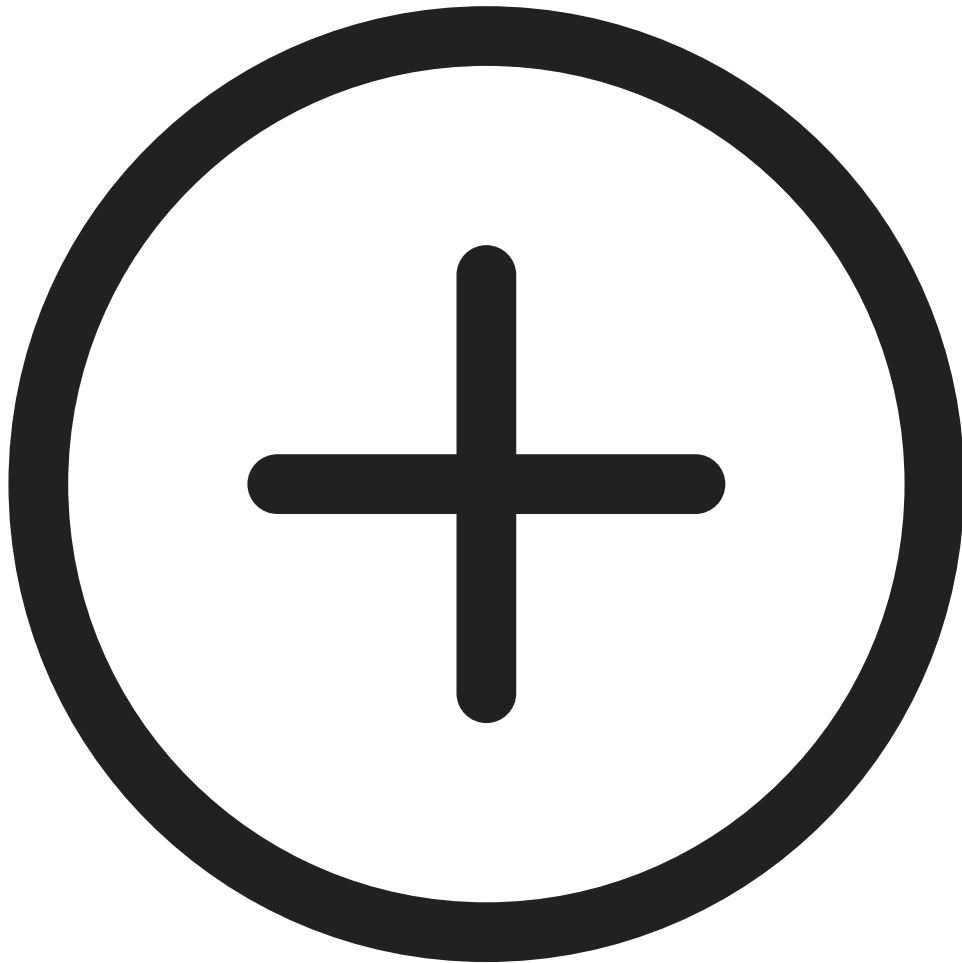
Configure su dispositivo

Configurar el monitor de calidad del aire

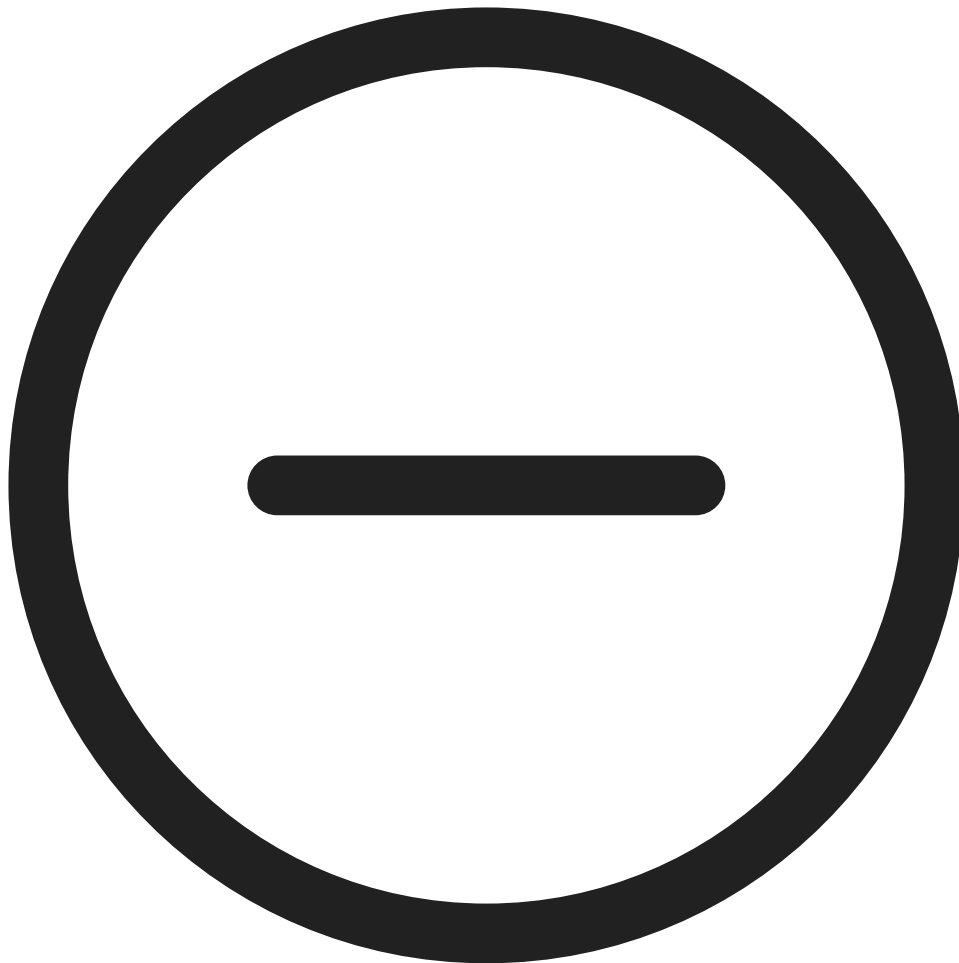
Configurar el panel de control del sensor de calidad del aire

En la página web del dispositivo, vaya a Air quality monitor (Monitor de calidad del aire) > Dashboard (Panel de instrumentos):

- Para editar el nombre del panel, haga clic en  a la izquierda.
- Para mostrar los datos en el panel, haga clic en  Edit (Editar) >



- Para ocultar los datos en el panel, haga clic en  Edit (Editar) >



Configurar el sensor de calidad del aire

En la página web del dispositivo, vaya a **Air quality sensor (Sensor de calidad del aire) > Settings (Ajustes)**.

- Establezca los umbrales de temperatura, humedad, CO₂, NO_x, PM_{1.0}, PM_{2.5}, PM_{4.0}, PM_{10.0}, VOC y AQI; consulte .
- Establezca las unidades de temperatura; consulte .
- Establezca la sensibilidad de detección de vapeo; consulte .
- Establezca el tiempo de retención de almacenamiento; consulte .
- Establezca la frecuencia de metadatos en la nube; consulte .
- Establezca el periodo de validación; consulte .

Descargar estadísticas de datos del sensor

Puede exportar hasta 365 días de estadísticas del sensor a un archivo CSV y usarlo en aplicaciones como Microsoft® Excel.

1. En la página web del dispositivo, visite **Air quality monitor (Monitor de calidad del aire) > Statistics (Estadísticas) > Sensor Data Statistics (Estadísticas de datos del sensor)**.
2. Escoja un rango de fechas:
 - **Custom range (Rango personalizado)**: En las listas **From (Desde)** y **To (Hasta)**, seleccione las fechas de inicio y fin (hasta 365 días).
 - **Predefined range (Rango predefinido)**: En la lista **Predefined date range (Rango de fechas predefinido)**, seleccione un periodo disponible.

Nota

Si se seleccionan tanto un rango personalizado como uno predefinido, este último tendrá prioridad.

Nota

El rango máximo de descarga está limitado por el tiempo de retención configurado en .

3. En la lista **Source (Fuente)**, seleccione la fuente deseada; para exportar los datos de todas las fuentes, haga clic en **Download all data (Descargar todos los datos)**.
4. Haga clic en **Download data (Descargar datos)** para exportar las estadísticas seleccionadas.

Nota

Haga clic en **Download all data (Descargar todos los datos)** para exportar los datos de todas las fuentes dentro del periodo seleccionado.

Calibración ante el primer uso del dispositivo

Nota

- La precisión total del CO2 requerirá 2 días la primera vez que se use el dispositivo.
- El AQI (Índice de calidad del aire) necesitará 12 horas para ser funcional la primera vez que use el dispositivo. El AQI mostrará **Calculating (Calculando)** hasta que disponga de datos suficientes. Se requiere el tiempo de calibración cada vez que se reinicia el dispositivo.
- La precisión total de VOC se obtiene después de que el dispositivo haya permanecido en funcionamiento una hora. Se requiere el tiempo de calibración cada vez que se reinicia el dispositivo.
- La precisión total de NOx se obtiene después de que el dispositivo haya permanecido en funcionamiento 6 horas. Se requiere el tiempo de calibración cada vez que se reinicia el dispositivo.

Configurar un perfil

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

Para establecer un nuevo perfil:

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

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

Configurar un perfil con un archivo de audio de sirena personalizado

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

Subir un archivo de audio:

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

Para usar el archivo de audio en un perfil:

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

Importar o exportar un perfil

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

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

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

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

Configurar SIP directo (P2P)

Utilice la configuración de punto a punto cuando la comunicación se realice entre unos pocos agentes de usuario dentro de la misma red IP y no necesite funciones adicionales que pueda proporcionar un servidor PBX. Para comprender mejor el funcionamiento de par a par, consulte .

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 .

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 .

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 para obtener más información.

Configurar reglas para eventos

Para obtener más información, consulte nuestra guía *Introducción a las reglas de eventos*.

Activar una acción

1. Vaya a **System > Events (Sistema > Eventos)** y agregue una regla. La regla determina cuándo debe realizar el dispositivo determinadas acciones. Puede configurar reglas como programadas, recurrentes o activadas manualmente.
2. Introduzca un **Name (Nombre)**.
3. Seleccione la **Condition (Condición)** que debe cumplirse para que se active la acción. Si especifica varias condiciones para la regla, deben cumplirse todas ellas para que se active la acción.
4. En **Action (Acción)**, seleccione qué acción debe realizar el dispositivo cuando se cumplan las condiciones.

Nota

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

Grabar vídeo cuando detecta el uso de vapors

El siguiente ejemplo explica cómo configurar un sensor de calidad del aire para que grabe vídeo en el almacenamiento en red cuando detecte el uso de vapors.

1. En la página web del sensor de calidad del aire, vaya a **Settings (Ajustes) > System (Sistema) > Storage (Almacenamiento)** para comprobar que el almacenamiento de red esté debidamente configurado.
2. Vaya a **Settings > System > Events (Ajustes > Sistema > Eventos)** y añada una regla. Introduzca la siguiente información:
 - **Name (Nombre)**: Escriba un nombre para la regla.
 - **Condition (Condición)**: **Air quality monitor (Monitor de calidad del aire) > Vaping or smoking detected (Detectado uso de vapors o tabaco)**.
 - **Action (Acción)**: **Recordings (Grabaciones) > Record video (Grabar vídeo)**.
 - **Almacenamiento**: **Network storage (Almacenamiento de red)**. Asegúrese de que el almacenamiento en red esté debidamente configurado.
 - **Cámara**: Seleccione un área de visión de la cámara.
 - **Stream profile (Perfil de flujo)**: Seleccione un perfil de transmisión o **Create a stream profile (Crear un perfil de transmisión)**.
 - **Prebuffer (Búfer anterior)** y **Postbuffer (Búfer posterior)**: Configure los valores deseados.
3. Haga clic en **Save (Guardar)**.

Reproducir clip de audio cuando el nivel de CO2 sea demasiado alto

Este ejemplo explica cómo reproducir un clip de audio cuando el nivel de CO2 es demasiado alto.

Crear una regla

1. En la página web, vaya a **Events (Eventos) > Rules (Reglas) > Add a rule (Añadir una regla)** para crear una regla.
2. Introduzca la siguiente información:
 - **Name (Nombre)**: Escriba un nombre para la regla.
 - **Conditions (Condiciones)**: **Air quality monitor (Monitor de calidad del aire) > Air quality outside acceptable range (Calidad del aire fuera del rango aceptable)**
 - **Sensor**: **CO2**
 - **Action (Acción)**: **Reproducción de secuencia de audio**
 - **Clip**: seleccione un clip de audio.
3. Haga clic en **Save (Guardar)**.

Configuración del intervalo de alarma del nivel de CO2

- En la página web, vaya a **Air quality monitor (Monitor de calidad del aire) > Settings (Ajustes) > CO2**.
- Introduzca los datos **MIN (MÍN.)** y **MAX (MÁX.)** para configurar el rango de CO2.

Activar un perfil de luz y sirena mediante el sensor PIR

Este ejemplo detalla cómo activar un perfil de luz y sirena mediante el sensor PIR. Consulte para conocer la ubicación de las luces (LED de señalización) y la sirena.

Crear un perfil de luz y sirena:

1. En la página web del dispositivo, vaya a **Profiles (Perfiles) > Create (Crear)**.
2. Introduzca la siguiente información:
 - **Name (Nombre):** Perfil 1
 - **Descripción:** Añada la descripción del perfil.
 - **Luz:** Seleccione **Pattern (Patrón)**, **Speed (Velocidad)**, **Intensity (Intensidad)**, **Color** y **Duration (Duración)**.
 - **Siren (Sirena):** Seleccione **Pattern (Patrón)**, **Intensity (Intensidad)** y **Duration (Duración)**.

Nota

Los perfiles con números más altos tienen mayor prioridad.

- **Priority (Prioridad):** Seleccionar **Light priority (Prioridad de luz)** y **Siren priority (Prioridad de sirena)**.

Cree un evento :

1. Vaya a **System (Sistema) > Events (Eventos) > Rules (Reglas)** y añada una regla.
2. Introduzca la siguiente información:
 - **Name (Nombre):** Activar los LED de señalización y la sirena.
 - **Condition (Condición):** sensor PIR.
 - **Action (Acción):** Ejecutar perfil de luz y sirena
 - **Profile (Perfil):** Perfil 1
 - **Action (Acción):** Start (Inicio)
3. Haga clic en **Save (Guardar)**.

Iniciar un perfil cuando se active una alarma

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

Configure la entrada de dirección para el puerto:

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

Crear una regla:

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

6. Seleccione el perfil que desea iniciar.
7. Haga clic en **Save (Guardar)**.

Iniciar un perfil a través de SIP

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

Activar SIP:

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

Crear una regla:

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

Uso de extensiones SIP para controlar más de un perfil

Activar SIP:

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

Crear una regla para iniciar un perfil:

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

Crear una regla para detener un perfil:

1. Vaya a **System (Sistema) > Events (Eventos)** y agregue una regla.
2. Escriba un nombre para la regla.

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

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

Ejecutar dos perfiles con diferentes prioridades

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

Nota

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

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

Crear perfiles:

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

Crear una regla:

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

Activar un perfil de luz y sirena mediante publicación HTTP cuando una cámara detecte movimiento

Este ejemplo explica cómo conectar una cámara al sensor de calidad del aire y activar un perfil de luz y sirena en el sensor cuando la aplicación AXIS Motion Guard, instalada en la cámara, detecte movimiento.

Antes de empezar:

- Cree un nuevo usuario con la función de operador o administrador en el sensor de calidad del aire.
- Cree un perfil en el sensor de calidad del aire llamado: "Perfil de luz y sirena".
- Configure AXIS Motion Guard en la cámara y cree un perfil llamado: "Perfil de cámara".
- Asegúrese de utilizar AXIS Device Assistant con la versión de firmware 10.8.0 o posterior.

Cree un destinatario en la cámara:

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

Cree dos reglas en la cámara:

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

```
{  "apiVersion": "1.0",  "method": "start",  "params": {    "profile": "Light and siren profile"  } }
```

Asegúrese de introducir la misma información en **"profile"** : <> como hizo cuando creó el perfil en el sensor de calidad del aire; en este caso: "Perfil de luz y sirena".

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

```
{  "apiVersion": "1.0",  "method": "stop",  "params": {    "profile": "Light and siren profile"  } }
```

Asegúrese de introducir la misma información en **"profile"** : <> como hizo cuando creó el perfil en el sensor de calidad del aire; en este caso: "Perfil de luz y sirena".

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

Activar un perfil de luz y sirena mediante entrada virtual cuando una cámara detecte movimiento

Este ejemplo explica cómo conectar una cámara al sensor de calidad del aire y activar un perfil de luz y sirena en el sensor cuando la aplicación AXIS Motion Guard, instalada en la cámara, detecte movimiento.

Antes de empezar:

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

Cree dos destinatarios en la cámara:

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

Cree dos reglas en la cámara:

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

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

Crear una regla en el sensor de calidad del aire:

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

Activar un perfil de luz y sirena en MQTT cuando una cámara detecte movimiento

Este ejemplo explica cómo conectar una cámara al sensor de calidad del aire y activar un perfil de luz y sirena en dicho sensor cuando la cámara detecte movimiento.

Antes de empezar:

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

Configure el cliente MQTT en la cámara:

1. En la interfaz web de la cámara, vaya a **System > MQTT > MQTT client > Broker (Sistema > MQTT > Cliente MQTT > Intermediario)** e introduzca la siguiente información:
 - **Host:** Dirección IP de intermediario
 - **Client ID (ID de cliente):** Por ejemplo, cámara 1
 - **Protocol (Protocolo):** El protocolo con el que se establece el intermediario
 - **Puerto:** El número de puerto utilizado por el intermediario
 - El **Username (Nombre de usuario)** y la **Password (Contraseña)** del intermediario.
2. Haga clic en **Save (Guardar)** y **Connect (Conectar)**.

Cree dos reglas en la cámara para la publicación MQTT:

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

- Seleccione **Invert this condition** (Invertir esta condición).
 - **Action (Acción):** MQTT > Send MQTT publish message (MQTT > Enviar mensaje de publicación MQTT)
 - **Topic (Tema):** Movimiento
 - **Payload (Carga):** Desactivado
 - **QoS:** 0, 1 o 2
5. Haga clic en **Save (Guardar)**.

Configure el cliente MQTT en el sensor de calidad del aire:

1. En la interfaz web del sensor de calidad del aire, vaya a **System (Sistema) > MQTT > MQTT client (Cliente MQTT) > Broker (Intermediario)** e introduzca la siguiente información:
 - **Host:** Dirección IP de intermediario
 - **Client ID (ID de cliente):** sirena 1
 - **Protocol (Protocolo):** El protocolo con el que se establece el intermediario
 - **Puerto:** El número de puerto utilizado por el intermediario
 - **Username (Nombre de usuario) y Password (Contraseña)**
2. Haga clic en **Save (Guardar)** y **Connect (Conectar)**.
3. Vaya a **MQTT subscriptions (Suscripciones MQTT)** y agregue una suscripción. Introduzca la siguiente información:
 - **Filtro de suscripción:** Movimiento
 - **Tipo de suscripción:** Con estado
 - **QoS:** 0, 1 o 2
4. Haga clic en **Save (Guardar)**.

Cree una regla en el sensor de calidad del aire para suscripciones MQTT:

1. Vaya a **System > Events > Rules (Sistema > Eventos > Reglas)** y añada una regla.
2. Introduzca la siguiente información:
 - **Name (Nombre):** Movimiento detectado
 - **Condition (Condición):** MQTT > Stateful (MQTT > Con estado)
 - **Filtro de suscripción:** Movimiento
 - **Payload (Carga):** On (Encendido)
 - **Action (Acción):** Light and siren > Run light and siren profile while the rule is active (Luz y sirena > Ejecutar perfil de luz y sirena mientras la regla está activa)
 - **Profile (Perfil):** Seleccione el perfil que desea que esté activo.
3. Haga clic en **Save (Guardar)**.

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

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

1. Establezca una programación para la prueba del altavoz:
 - 1.1. Vaya a la interfaz del dispositivo > **System (Sistema) > Events (Eventos) > Schedules (Programación)**.
 - 1.2. Cree una programación que comience a las 18:00 y termine a las 18:01 todos los días. Nómbralo "Diario a las 18:00".
2. Crear un destinatario de correo electrónico:

- 2.1. Vaya a la interfaz del dispositivo > **System (Sistema)** > **Events (Eventos)** > **Recipients (Destinatarios)**.
- 2.2. Haga clic en **Add recipient (Agregar destinatario)**.
- 2.3. Nombre el destinatario "Destinatarios de la prueba del altavoz"
- 2.4. En **Type (Tipo)**, select (seleccione) **Email (Correo electrónico)**.
- 2.5. En **Send email to (Enviar correo electrónico a)**, introduzca las direcciones de los destinatarios. Utilice comas para separar múltiples direcciones.
- 2.6. Introduzca los datos de la cuenta de correo electrónico del remitente.
- 2.7. Haga clic en **Test (Probar)** para enviar un correo electrónico de prueba.

Nota

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

- 2.8. Haga clic en **Save (Guardar)**.
3. Configurar una prueba de altavoz automatizada:
 - 3.1. Vaya a la interfaz del dispositivo > **System (Sistema)** > **Events (Eventos)** > **Rules (Reglas)**.
 - 3.2. Haga clic en **Add a rule (Agregar una regla)**.
 - 3.3. Introduzca un nombre para la regla.
 - 3.4. En **Condition (Condición)**, seleccione **(Schedule) Programación** y escoja entre la lista de activadores
 - 3.5. En **Schedule (Programación)**, seleccione su programación ("Diaria a las 18:00").
 - 3.6. En **Action (Acción)**, seleccione **Run automatic speaker test (Ejecutar comprobación automática de altavoz)**.
 - 3.7. Haga clic en **Save (Guardar)**.
4. Configuración de la condición para el envío de un correo electrónico cuando la prueba del altavoz falla:
 - 4.1. Vaya a la interfaz del dispositivo > **System (Sistema)** > **Events (Eventos)** > **Rules (Reglas)**.
 - 4.2. Haga clic en **Add a rule (Agregar una regla)**.
 - 4.3. Introduzca un nombre para la regla.
 - 4.4. En **Condition (Condición)**, seleccione **Speaker test result (Resultado de la comprobación del altavoz)**.
 - 4.5. En **Speaker test status (Estado de prueba del altavoz)**, seleccione **Didn't pass the test (No ha pasado la comprobación)**.
 - 4.6. En **Action (Acción)**, seleccione **Send notification to email (Enviar notificación por correo electrónico)**.
 - 4.7. En **Recipient (Destinatario)**, seleccione su destinatario ("Destinatarios de prueba de altavoz")
 - 4.8. Introduzca un asunto y un mensaje y haga clic en **Save (Guardar)**.

Reproducir clip personalizado al activar una alarma

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

Subir un archivo de audio:

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

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

Cree un perfil con el archivo de audio:

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

Configure la entrada de dirección para el puerto:

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

Crear una regla:

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

Detener audio con DTMF

En este ejemplo se explica cómo:

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

Configuración de audio para llamadas SIP entrantes

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

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

Habilitar ajustes SIP:

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

Reproducción de audio cuando se recibe una llamada SIP:

1. Vaya a **Settings > System > Events > Rules (Ajustes > Sistema > Eventos > Reglas)** y añada una regla.
2. Escriba un nombre para la regla.
3. En la lista de condiciones, seleccione **State (Estado)**.
4. En la lista de estados, seleccione **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.

Estado

Información sobre el dispositivo

Muestra información del 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 sistema operativo AXIS.

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

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.

Estado de alimentación

Muestra información del estado de alimentación. La información varía en función del producto.

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



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

Cientes 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.

Vídeo

Flujo

General

Resolución: Seleccione la resolución de imagen apta para la escena de vigilancia. Una mayor resolución aumenta el ancho de banda y el almacenamiento.

Velocidad de imagen: Para evitar problemas de ancho de banda en la red o para reducir el tamaño de almacenamiento, puede limitar la velocidad de fotogramas a un número fijo. Si deja la velocidad de fotogramas en cero, la velocidad se mantendrá en el máximo nivel de velocidad posible según las condiciones actuales. Una velocidad de fotogramas más alta requiere más ancho de banda y capacidad de almacenamiento.

P-frames: Un fotograma P es una imagen pronosticada que solo muestra los cambios en la imagen con respecto al fotograma anterior. Introduzca el número deseado de fotogramas P. Cuanto mayor es el número, menos ancho de banda se necesita. Sin embargo, si hay congestión en la red, puede haber un declive notable en la calidad del vídeo.

Compression (Compresión): Utilice el control deslizante para ajustar la compresión de imagen. Cuanto mayor sea la compresión, menor será la velocidad de fotogramas y la calidad de imagen. Una compresión menor mejora la calidad de la imagen, pero requiere más ancho de banda y espacio de almacenamiento al grabar.

Vídeo firmado  : Active esta opción para agregar la función de vídeo firmado a los vídeos. El vídeo firmado protege el vídeo contra manipulaciones mediante la adición de firmas criptográficas.

Control de velocidad de bits

- **Promedio:** Seleccione esta opción para ajustar automáticamente la velocidad de bits durante más tiempo y proporcionar la mejor calidad de imagen posible en función del almacenamiento disponible.
 -  Haga clic para calcular la velocidad de bits de destino en función del almacenamiento, el tiempo de retención y el límite de velocidad de bits disponibles.
 - **Velocidad de bits objetivo:** Introduzca la velocidad de bits de destino deseada.
 - **Tiempo de conservación:** Introduzca el número de días que guardar las grabaciones.
 - **Almacenamiento:** Muestra el almacenamiento estimado que se puede ser usado para el flujo.
 - **Velocidad de bits máxima:** Active esta función para establecer un límite de velocidad de bits.
 - **Bitrate limit (Límite de velocidad de bits):** Introduzca un límite de velocidad de bits mayor que la velocidad de bits de destino.
- **Máximo:** Seleccione para establecer una velocidad de bits instantánea máxima del flujo en función del ancho de banda de la red.
 - **Máximo:** Introduzca la velocidad de bits máxima.
- **Variable:** Seleccione esta opción para permitir que la velocidad de bits varíe en función del nivel de actividad de la escena. Más actividad requiere más ancho de banda. Recomendamos esta opción para la mayoría de situaciones.

Audio

Include (Incluir): Active esta opción para usar audio en el flujo de vídeo.

Fuente  : Seleccione la fuente de audio que desea utilizar.

Estéreo  : Active esta opción para incluir audio integrado y audio de un micrófono externo.

Sensor de calidad del aire

Panel

Datos del sensor en tiempo real

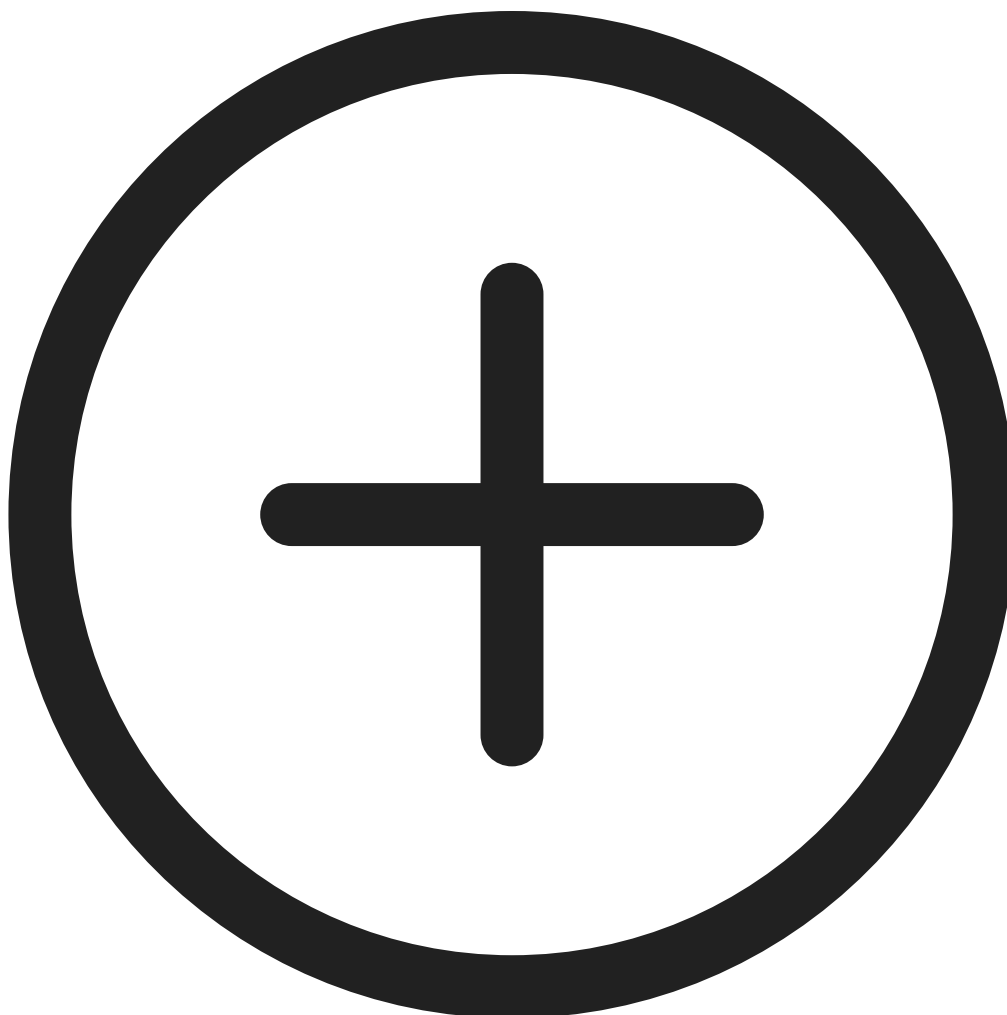
Muestra los datos del sensor en tiempo real.

Nota

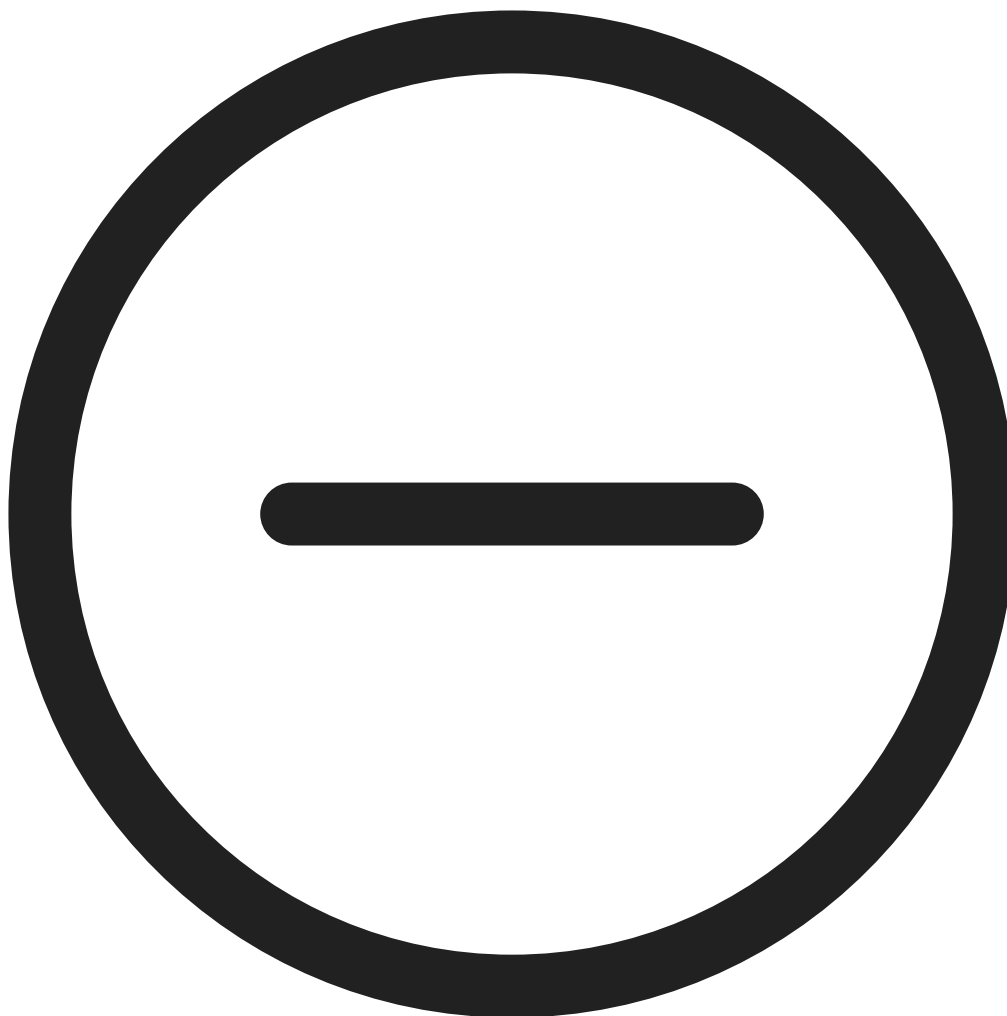
- La precisión total del CO2 requerirá 2 días la primera vez que se use el dispositivo.
- El AQI (Índice de calidad del aire) necesitará 12 horas para ser funcional la primera vez que use el dispositivo. El AQI mostrará **Calculating (Calculando)** hasta que disponga de datos suficientes. Se requiere el tiempo de calibración cada vez que se reinicia el dispositivo.
- La precisión total de VOC se obtiene después de que el dispositivo haya permanecido en funcionamiento una hora. Se requiere el tiempo de calibración cada vez que se reinicia el dispositivo.
- La precisión total de NOx se obtiene después de que el dispositivo haya permanecido en funcionamiento 6 horas. Se requiere el tiempo de calibración cada vez que se reinicia el dispositivo.

 : Haga clic para ajustar el nombre del panel de control.

 Editar: Haga clic para mostrar u ocultar los datos.



: Haga clic para añadir datos al panel de control.



: Haga clic para eliminar datos del panel de control.

Temperatura: ver la temperatura en tiempo real del sensor de calidad del aire.

Humidity (Humedad): ver la humedad en tiempo real del sensor de calidad del aire.

CO2: ver el dióxido de carbono en tiempo real.

El significado de los colores de las barras de estado de CO2 es este:

- **Verde (0–1 000):** Bueno. Los datos se consideran satisfactorios.
- **Naranja (1 001–2 000): perjudicial para grupos sensibles.** Los miembros de grupos sensibles pueden experimentar efectos sobre su salud. El público en general tiene menos probabilidades de verse afectado.
- **Rojo (2 001–5 000): perjudicial.** Todos pueden empezar a experimentar efectos sobre la salud; los miembros de grupos sensibles pueden experimentar efectos más graves.
- **Morado (5 001–40 000): muy perjudicial.** Advertencias sanitarias de situaciones de emergencia. El público en general tiene más probabilidades de verse afectado.

NOx: Visualice el óxido nítrico y el dióxido de nitrógeno en tiempo real.

El significado de los colores de las barras de estado de NOx es este:

- **Verde (0–30): Bueno.** Los datos se consideran satisfactorios.
- **Amarillo (31–150): Moderado.** Los datos son aceptables. Puede representar un problema de salud moderado para un número muy pequeño de personas que son inusualmente sensibles.
- **Naranja (151–300): perjudicial para grupos sensibles.** Todos pueden empezar a experimentar efectos sobre la salud; los miembros de grupos sensibles pueden experimentar efectos más graves.
- **Rojo (301–500): perjudicial.** Todos pueden empezar a experimentar efectos sobre la salud; los miembros de grupos sensibles pueden experimentar efectos más graves.

PM 1.0: ver la materia particulada 1.0 en tiempo real.

PM 2.5: ver la materia particulada 2.5 en tiempo real.

El significado de los colores de las barras de estado de PM 2.5 es este:

- **Verde (0–9): Bueno.** Los datos se consideran satisfactorios.
- **Amarillo (9,1–35,4): Moderado.** Los datos son aceptables. Puede representar un problema de salud moderado para un número muy pequeño de personas que son inusualmente sensibles.
- **Naranja (35,5–55,4): perjudicial para grupos sensibles.** Todos pueden empezar a experimentar efectos sobre la salud; los miembros de grupos sensibles pueden experimentar efectos más graves.
- **Rojo (55,5–125,4): perjudicial.** Todos pueden empezar a experimentar efectos sobre la salud; los miembros de grupos sensibles pueden experimentar efectos más graves.
- **Morado (125,5–225,4): muy perjudicial.** Advertencias sanitarias de situaciones de emergencia. El público en general tiene más probabilidades de verse afectado.
- **Granate (225,5–1 000): Peligroso.** Condiciones de emergencia. El público en general tiene más probabilidades de verse afectado.

PM 4.0: ver la materia particulada 4.0 en tiempo real.

PM 10.0: ver la materia particulada 10.0 en tiempo real.

El significado de los colores de las barras de estado de PM 10.0 es este:

- **Verde (0–54): Bueno.** Los datos se consideran satisfactorios.
- **Amarillo (55–154): Moderado.** Los datos son aceptables. Puede representar un problema de salud moderado para un número muy pequeño de personas que son inusualmente sensibles.
- **Naranja (155–254): perjudicial para grupos sensibles.** Todos pueden empezar a experimentar efectos sobre la salud; los miembros de grupos sensibles pueden experimentar efectos más graves.
- **Rojo (255–354): perjudicial.** Todos pueden empezar a experimentar efectos sobre la salud; los miembros de grupos sensibles pueden experimentar efectos más graves.
- **Morado (355–424): muy perjudicial.** Advertencias sanitarias de situaciones de emergencia. El público en general tiene más probabilidades de verse afectado.
- **Granate (425–1 000): Peligroso.** Condiciones de emergencia. El público en general tiene más probabilidades de verse afectado.

Vapeo/Tabaco: ver el uso detectado/no detectado de vapores o tabaco.

El significado de los colores de las barras de estado de Vapeo/Tabaco es este:

- **Verde: Undetected (No detectado).** No se detecta la actividad sospechosa de uso de vapores o tabaco.
- **Rojo: Detected (Detectado).** Se detecta la actividad sospechosa de uso de vapores o tabaco.

VOC: ver índice de compuestos orgánicos volátiles.

El significado de los colores de las barras de estado de VOC es este:

- **Verde (0–100): Bueno.** Los datos se consideran satisfactorios.
- **Amarillo (101–300): Moderado.** Los datos son aceptables. Puede representar un problema de salud moderado para un número muy pequeño de personas que son inusualmente sensibles.

- **Naranja (301–400): perjudicial para grupos sensibles.** Todos pueden empezar a experimentar efectos sobre la salud; los miembros de grupos sensibles pueden experimentar efectos más graves.
- **Rojo (401–500): perjudicial.** Todos pueden empezar a experimentar efectos sobre la salud; los miembros de grupos sensibles pueden experimentar efectos más graves.

AQI: ver el índice de calidad del aire.

El significado de los colores de las barras de estado del índice de calidad del aire es este:

- **Verde (0–50): Bueno.** Los datos se consideran satisfactorios.
- **Amarillo (51–100): Moderado.** Los datos son aceptables. Puede representar un problema de salud moderado para un número muy pequeño de personas que son inusualmente sensibles.
- **Naranja (101–150): perjudicial para grupos sensibles.** Todos pueden empezar a experimentar efectos sobre la salud; los miembros de grupos sensibles pueden experimentar efectos más graves.
- **Rojo (151–200): perjudicial.** Todos pueden empezar a experimentar efectos sobre la salud; los miembros de grupos sensibles pueden experimentar efectos más graves.
- **Morado (201–300): muy perjudicial.** Advertencias sanitarias de situaciones de emergencia. El público en general tiene más probabilidades de verse afectado.
- **Granate (301–500): Peligroso.** Condiciones de emergencia. El público en general tiene más probabilidades de verse afectado.

Ajustes

Umbral

Configura los datos del sensor de calidad del aire.

Temperatura: Ajuste la temperatura MIN (MÍN.) y MAX (MÁX.) dentro del intervalo de –10 a 45.

Humidity (Humedad): ajuste la humedad MIN (MÍN.) y MAX (MÁX.) dentro del rango de 0 a 100.

CO2: ajuste el dióxido de carbono MIN (MÍN.) y MAX (MÁX.) dentro del rango de 0 a 40 000.

NOx: Ajuste los valores MIN (MÍN.) y MAX (MÁX.) de óxido nítrico y dióxido de nitrógeno dentro del rango de 0 a 500.

PM1.0: ajuste la materia en partículas 1.0 MIN (MÍN.) y MAX (MÁX.) dentro del rango de 0 a 1 000.

PM2.5: ajuste la materia en partículas 2.5 MIN (MÍN.) y MAX (MÁX.) dentro del rango de 0 a 1 000.

PM4.0: ajuste la materia en partículas 4.0 MIN (MÍN.) y MAX (MÁX.) dentro del rango de 0 a 1 000.

PM10.0: ajuste la materia en partículas MIN (MÍN.) y MAX (MÁX.) dentro del rango de 0 a 1 000.

VOC: ajuste el índice de compuestos orgánicos volátiles MIN (MÍN.) y MAX (MÁX.) dentro del rango de 0 a 500.

AQI: ajuste el índice de calidad del aire MIN (MÍN.) y MAX (MÁX.) dentro del rango de 0 a 500.

Unidades de temperatura

Mostrar temperatura en: Centígrados o Fahrenheit

Sensibilidad de detección de vapeo

Configura la sensibilidad de detección de uso de vapors.

Low sensitivity (Baja sensibilidad), High sensitivity (Alta sensibilidad): Utilice el control deslizante para ajustar la diferencia entre baja y alta sensibilidad a la que el dispositivo debe emitir una alarma. Una alta sensibilidad significa que el dispositivo detectará incluso pequeñas cantidades de humo o vapeo y es más probable que emita una alerta; una baja sensibilidad significa que solo responderá a grandes cantidades de humo o vapeo, reduciendo así la posibilidad de emitir falsas alarmas.

Configuración de almacenamiento

- **Retention time 1 month, frequency 1 s (Tiempo de retención: 1 mes, frecuencia: 1 s):** sus datos se recopilan cada segundo y solo se conservan los de los últimos 30 días.
- **Retention time 3 months, frequency 5 s (Tiempo de retención: 3 meses, frecuencia: 5 s):** sus datos se recopilan cada 5 segundos y solo se conservan los de los últimos 90 días.
- **Retention time 1 year, frequency 10 s (Tiempo de retención: 1 año, frecuencia: 10 s):** sus datos se recopilan cada 10 segundos y solo se conservan los de los últimos 365 días.

Nota

Cambiar la opción de almacenamiento eliminará los datos existentes.

Frecuencia de metadatos en la nube

Las plataformas de terceros que desean suscribirse a los metadatos del sensor con una frecuencia de transmisión ajustable, utilizan la frecuencia de metadatos en la nube. Estos metadatos de la nube incluyen todos los datos de los sensores que recoge el panel.

Cloud metadata (Metadatos en la nube): Activar para usar metadatos de la nube.

Nota

Esta función está deshabilitada de forma predeterminada; no se envían metadatos del tema. Tras activar esta opción, los metadatos del tema se transmiten en el rango de frecuencia establecido a continuación.

Set frequency range (Establecer rango de frecuencia) (00:00:01 – 23:59:59): introduzca un valor para ajustar el rango de frecuencia.

Periodo de validación

Puede determinar un periodo de validación para los siguientes ajustes de configuración de calidad del aire. El periodo de validación actúa como un umbral de tiempo, y para que se active una alarma la lectura debe mantenerse por encima del límite del rango del periodo de validación.

Ejemplo

Si el periodo de validación de CO₂ es de 5 s, para que se active la alarma el nivel de CO₂ debe mantenerse por encima del límite durante los 5 s completos.

Determine el rango del periodo de validación (0-60 s) para los siguientes datos:

- Temperatura
- Humedad
- CO2
- NOx
- PM1.0
- PM2.5
- PM4.0
- PM10.0
- VOC
- AQI
- Vapear/fumar

Estadísticas

Estadísticas de datos del sensor

Puede exportar hasta 365 días de estadísticas del sensor a un archivo CSV y usarlo en aplicaciones como Microsoft® Excel.

- **Predefined date range (Rango de fechas predefinido):** para seleccionar el rango de fechas predefinido que desea descargar de la lista.
- **From (Desde) y To (Hasta):** para seleccionar el rango personalizado que desea descargar. Puede descargar datos de hasta 365 días.

Nota

Si se seleccionan tanto un rango personalizado como uno predefinido, este último tendrá prioridad.

Nota

El rango máximo de descarga está limitado por el tiempo de retención configurado en .

- **Select a source (Seleccionar una fuente):** para escoger la fuente que desea descargar.
- **Download data (Descargar datos):** para seleccionar **Download selected sensor data (Descargar datos del sensor seleccionado)** en el menú desplegable.
- **Download data for all sources (Descargar datos de todas las fuentes):** para exportar los datos de todas las fuentes dentro del periodo seleccionado.

El archivo se descargará en su carpeta de descargas. La descarga puede tardar cierto tiempo en función del tamaño del archivo.

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

Configuración del dispositivo

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

Input type (Tipo de entrada)  : Seleccione el tipo de entrada, por ejemplo, si es un micrófono interno o una entrada de línea.

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

Apply changes (Aplicar cambios)  : Aplique su selección.

Echo cancellation (Cancelación de eco)  : Active esta función para eliminar ecos durante la comunicación bidireccional.

Controles de ganancia independientes  : Active para ajustar la ganancia de forma independiente para los distintos tipos de entrada.

Control de ganancia automático  : Active para que la ganancia se adapte dinámicamente a los cambios en el sonido.

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

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.

Automatic volume control (Control automático del volumen)  : Active esta opción para que el dispositivo ajuste de forma automática y dinámica la ganancia en función del nivel de ruido ambiente. El control automático del volumen afecta a todas las salidas de audio, incluidas las de línea y telebobina.

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.

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.

Mejora de audio

Entrada

Ten Band Graphic Audio Equalizer (Ecualizador gráfico de audio de diez bandas): Active esta opción para ajustar el nivel de diferentes bandas de frecuencia dentro de una señal de audio. Esta característica es para usuarios avanzados con experiencia en configuración de audio.

Talkback range (Alcance de talkback)  : Elija el alcance de funcionamiento para recoger contenido de audio. El aumento del alcance de funcionamiento reduce las capacidades de comunicación bidireccional simultánea.

Voice enhancement (Mejora de la voz)  : Active esta función para mejorar el contenido de la voz en relación con otros sonidos.

Descripción general

Estado del LED de señalización

Muestra las diferentes actividades del LED de señalización que se ejecutan en el dispositivo. Puede tener hasta 10 actividades simultáneas en la lista de estado del LED de señalización. Cuando se ejecutan varias actividades a la vez, la actividad con la prioridad más alta muestra el estado del LED de señalización. Dicha fila se resaltará en la lista de estado.

Estado del altavoz de audio

Muestra las diferentes actividades del altavoz de audio que se ejecutan en el dispositivo. Puede disponer simultáneamente de hasta 10 actividades en la lista de estado del altavoz de audio. Cuando se ejecutan varias actividades a la vez, se reproduce la que tiene mayor prioridad. 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

Ongoing recordings (Grabaciones en curso): Mostrar todas las grabaciones en curso.

- Iniciar una grabación.
-  Seleccione una red de almacenamiento de red ya configurada.
- Detener una grabación.

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.

 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.

Medios

+ Add (agregar): Haga clic para añadir un nuevo archivo.

Storage location (Ubicación de almacenamiento): Seleccione si desea guardar el archivo en la memoria interna o en el almacenamiento integrado (tarjeta SD, si está disponible).



El menú contextual contiene:

- **Information (Información):** Ver información sobre el archivo.
- **Copy link (Copiar enlace):** Copiar el enlace a la ubicación del archivo en el dispositivo.
- **Eliminar:** Eliminar el archivo de la ubicación de almacenamiento.

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.

- **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 de NTS KE de confianza):** Seleccione los certificados CA de confianza que se usarán para la sincronización horaria segura de NTS KE 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 para poder seleccionar esta opción.
- **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 esta opción para que el router de red asigne automáticamente una dirección IP al dispositivo. Recomendamos IP automática (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.

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.
 - **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+):** 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.

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 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 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** y **Open ID**.



El menú contextual contiene:

- **Update (Actualizar):** Actualice el host virtual.
- **Eliminar:** Elimine el host virtual.

Disabled (Deshabilitado): El servidor está deshabilitado.

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 autenticación 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*.

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).
- **Autenticación 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**.

Incluir nombre de tema: Seleccione esta opción para incluir el tema que describe la condición en el tema de MQTT.

Incluir espacios de nombres de tema: 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.

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 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: UDP, 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.

Lista de acceso

Use access list (Usar lista de acceso): Active esta opción para restringir quién puede realizar llamadas al dispositivo.

Policy (Directiva):

- **Allow (Permitir):** Seleccione esta opción para permitir llamadas entrantes solo desde las fuentes de la lista de acceso.
- **Block (Bloquear):** Seleccione esta opción para bloquear llamadas entrantes desde las fuentes de la lista de acceso.



Add source (Agregar fuente): Haga clic para crear una nueva entrada en la lista de acceso.

Source SIP (Fuente SIP): Introduzca la ID del emisor de la llamada o la dirección del servidor SIP de la fuente.

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

Ignorar: Active para ignorar 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.

Perfiles de transmisión

Un perfil de flujo es un grupo de ajustes que afectan al flujo de vídeo. Puede utilizar perfiles de flujo en distintas situaciones, por ejemplo, al crear eventos y utilizar reglas para grabar.



Add stream profile (Agregar perfil de flujo): Haga clic para crear un perfil de flujo nuevo.

Preview (Vista previa): Una vista previa del flujo de vídeo con los ajustes del perfil de flujo que seleccione. La vista previa se actualiza cuando se modifican los ajustes de la página. Si el dispositivo tiene distintas áreas de visualización, puede cambiar el área de visualización en la lista desplegable de la esquina inferior izquierda de la imagen.

Name (Nombre): Agregue un nombre para su perfil.

Descripción: Agregue una descripción de su perfil.

Video codec (Código de vídeo): Seleccione el códec de vídeo que debe aplicarse al perfil.

Resolución: Consulte para obtener una descripción de este ajuste.

Velocidad de imagen: Consulte para obtener una descripción de este ajuste.

Compression (Compresión): Consulte para obtener una descripción de este ajuste.

Zipstream (Flujo zip)  : Consulte para obtener una descripción de este ajuste.

Optimize for storage (Optimizar para almacenamiento)  : Consulte para obtener una descripción de este ajuste.

Dynamic FPS (FPS dinámico)  : Consulte para obtener una descripción de este ajuste.

Dynamic GOP (GOP dinámico)  : Consulte para obtener una descripción de este ajuste.

Mirror (Duplicar)  : Consulte para obtener una descripción de este ajuste.

GOP length (Longitud de GOP)  : Consulte para obtener una descripción de este ajuste.

Control de velocidad de bits: Consulte para obtener una descripción de este ajuste.

Include overlays (Incluir superposiciones)  : Seleccione el tipo de superposiciones que desea incluir. Consulte para obtener información sobre cómo agregar superposiciones.

Include audio (Incluir audio)  : Consulte para obtener una descripción de este ajuste.

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.

Función:

- **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  : Seleccione el formato de codificación de audio para su 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.

Decodificador de audio  : Seleccione el formato de decodificación 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 todos 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.

Sensor de PIR

El sensor PIR mide la luz IR que irradian los objetos en su campo de visión.

Nivel de sensibilidad: Ajuste el nivel a un valor de 0-100, donde 0 es el nivel menos sensible y 100 es el más sensible.

Ajustes de energía

Estado de alimentación

Muestra información del estado de alimentación. La información varía en función del producto.

Accesorios

Puertos de E/S

Use la entrada digital para conectar seguridad positiva que pueda alternar entre circuitos abiertos y cerrados, por ejemplo, sensores PIR, contactos de puertas o ventanas y detectores de cristales rotos.

Use la salida digital para establecer conexión con dispositivos externos, como relés y LED. Puede activar los dispositivos conectados a través de la interfaz de programación de aplicaciones VAPIX® o la interfaz web.

Puerto

Name (Nombre): Edite el texto para cambiar el nombre del puerto.

Direction (Dirección):  indica que el puerto es un puerto de entrada.  indica que el puerto es un puerto de salida. Si el puerto es configurable, puede hacer clic en los iconos para cambiar entre entrada y salida.

Normal state (Estado normal): Haga clic  para circuito abierto y  para circuito cerrado.

Current state (Estado actual): muestra el estado actual del puerto. La entrada o salida se activa cuando el estado actual difiere del estado normal. Una entrada del dispositivo tiene el circuito abierto cuando está desconectado o cuando hay una tensión superior a 1 V CC.

Nota

Durante el reinicio, se abre el circuito de salida. Cuando termina el reinicio, el circuito vuelve a la posición normal. Si modifica algún ajuste de esta página, los circuitos de salida recuperan las posiciones normales, con independencia de los activadores activos.

Supervisado  : Active esta opción para que sea posible detectar y activar acciones si alguien manipula la conexión con dispositivos de E/S digital. Además de detectar si una entrada está abierta o cerrada, también puede detectar si alguien la ha manipulado (mediante un corte o cortocircuito). La supervisión de la conexión requiere hardware adicional (resistencias de final de línea) en el bucle de E/S externa.

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, autenticaciones 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 deberá 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 dispositivos 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

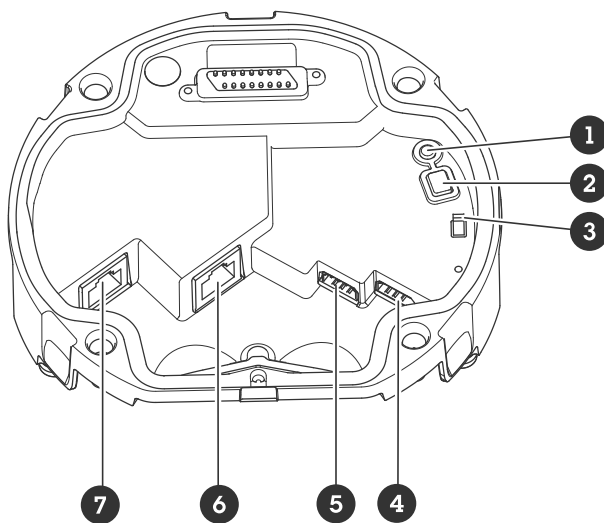
Un archivo de rastreo de red puede contener información confidencial, como certificados o contraseñas.

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

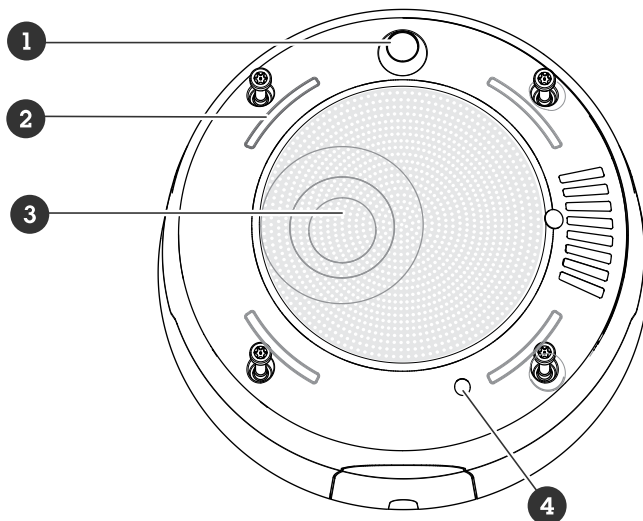
Trace time (Tiempo de rastreo): Seleccione la duración del rastreo en segundos o minutos y haga clic en **Descargar**.

Especificaciones

Guía de productos



- 1 Indicador LED de estado
- 2 Botón de control
- 3 Interruptor del micrófono
- 4 Conector de E/S
- 5 Conector RS-485
- 6 Conector de red (PoE OUT)
- 7 Conector de red (PoE IN)



- 1 Sensor de PIR
- 2 LED de señalización
- 3 Altavoz
- 4 Micrófono interno

LED de estado

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.

Botones

Botón de control

El botón de control se utiliza para lo siguiente:

- Restablecer el producto a la configuración predeterminada de fábrica. Vea .

Interruptor del micrófono

Consulte para conocer la ubicación del interruptor del micrófono.

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

Conectores

Conector de red

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

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

Conector de E/S

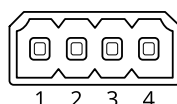
Utilice el conector de E/S con dispositivos externos en combinación con detección de movimiento, activación de eventos y notificaciones de alarma, por ejemplo. Además del punto de referencia de 0 V CC y la alimentación (salida de CC de 12 V), el conector de E/S ofrece una interfaz para:

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

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

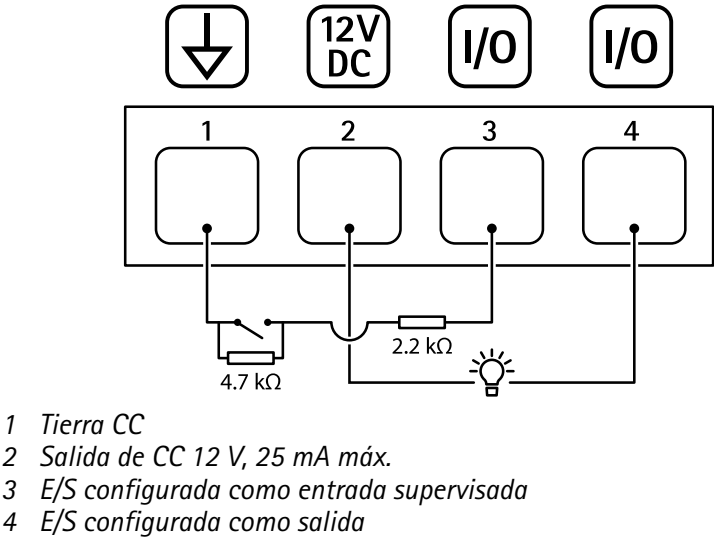
Salida digital – Conectar dispositivos externos como relés y LED. Los dispositivos conectados se pueden activar mediante la interfaz de programación de aplicaciones VAPIX®, mediante un evento o desde la interfaz web del dispositivo.

Bloque de terminales de 4 pines



Función	Pin	Notas	Especificaciones
Tierra CC	1		0 V CC
Salida de CC	2	⚠ Se puede utilizar para alimentar equipos auxiliares. Nota: Este pin solo se puede utilizar como salida de alimentación.	12 V CC Carga máx.: 25 mA
Configurable (entrada o salida)	3–4	Entrada digital o entrada supervisada: conéctela al pin 1 para activarla, o bien déjela suelta (sin conectar) para desactivarla. Para usar la entrada supervisada, instale las resistencias de final de línea. Consulte el diagrama de conexiones para obtener información sobre cómo conectar las resistencias.	De 0 a 30 V CC máx.
		Salida digital: conectada internamente a pin 1 (tierra CC) cuando está activa, y suelta (desconectada) cuando está inactiva. Si se utiliza con una carga inductiva, por ejemplo, un relé, conecte un diodo en paralelo a la carga como protección contra transitorios de tensión.	De 0 a 30 V CC máx., colector abierto, 100 mA

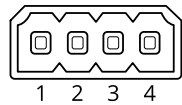
Ejemplo:



Conector RS485/RS422

Dos bloques de terminales de 2 pines para la interfaz serie RS485/RS422. El puerto serie puede configurarse para admitir:

- Semidúplex RS485 de dos cables
- Dúplex completo RS485 de cuatro cables
- Símples RS422 de dos cables
- Full-duplex RS422 de cuatro cables para comunicación punto a punto



Función	Pin	Notas
RS485/RS422 RX/TX A	1	(RX) para dúplex completo RS485/RS422 (RX/TX) Para RS485 semidúplex
RS485/RS422 RX/TX B	2	
RS485/RS422 TX A	3	(TX) para dúplex completo RS485/RS422
RS485/RS422 TX B	4	

Nombres de patrones de luz

Desactivado
Fijo
Alternativo
Impulso
Escalar 3 pasos
Parpadeo
Parpadeo 3 veces
Parpadeo 4 veces
Parpadeo 3 veces atenuación
Parpadeo 4 veces atenuación
Parpadeo 1 vez
Parpadeo 3 veces

Nombres de patrones de sirena

Desactivado
Alarma: Tono alto de alarma
Alarma: Tono bajo de alarma
Alarma: Ave
Alarma: Cuerno de barco
Alarma: Alarma de coche
Alarma: Alarma de coche rápida
Alarma: Reloj clásico
Alarma: Primer asistente
Alarma: Terror
Alarma: Industria
Alarma: Sonido único
Alarma: Sonido cuádruple suave
Alarma: Sonido triple suave

Alarma: Tono alto triple
Notificación: Aceptado
Notificación: Llamando
Notificación: Denegado
Notificación: Listo
Notificación: Entrada
Notificación: Error
Notificación: Prisa
Notificación: Mensaje
Notificación: Siguiente
Notificación: Abierto
Siren (Sirena): Alternativo
Siren (Sirena): Bullicioso
Siren (Sirena): Evacuación
Siren (Sirena): Tono descendente
Siren (Sirena): Inicio suave

Limpie su dispositivo

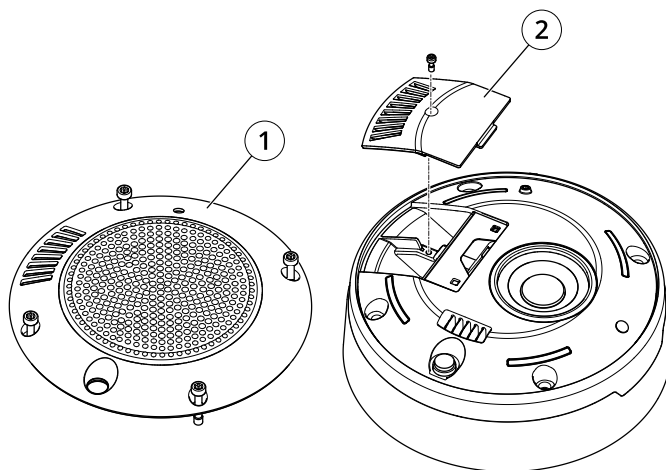
Puede limpiar su dispositivo con agua tibia.

AVISO

- Los productos químicos agresivos pueden dañar el dispositivo. No utilice productos químicos como un limpiacrystal o acetona para limpiar el dispositivo.
1. Utilice un aerosol de aire comprimido para quitar el polvo y la suciedad suelta del dispositivo.
 2. En caso necesario, utilice un paño suave de microfibra humedecido con agua tibia para limpiar el dispositivo.
 3. Para evitar que queden manchas, seque el dispositivo con un paño limpio y no abrasivo.

Nota

- Retire la cubierta (1) y la puerta (2).
- Use un cepillo para limpiar el polvo.



1 Cubierta

2 Puerta

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:

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**.

Problemas técnicos, consejos y soluciones

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

Problemas para actualizar AXIS OS

Fallo 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

El dispositivo se encuentra en una subred distinta	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 ya la utiliza otro dispositivo	Desconecte el dispositivo de Axis de la red. Ejecute el comando ping (en una ventana de comando/DOS, escriba <code>ping</code> y la dirección IP del dispositivo): - Si recibe lo siguiente: <code>Reply from <IP address>: bytes=32; time=10...</code> significa 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. - Si recibe lo siguiente: <code>Request timed out</code>, significa que la dirección IP está disponible para su uso con el dispositivo de Axis. Compruebe el cableado y vuelva a instalar el dispositivo.
Posible conflicto de dirección IP con 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.

No se puede acceder al dispositivo desde un navegador

No se puede iniciar sesión	Cuando HTTPS esté activado, asegúrese de utilizar el protocolo correcto (HTTP o HTTPS) al intentar iniciar sesión. Puede que tenga que escribir manualmente <code>http</code> o <code>https</code> en el campo de dirección del navegador. Si se pierde la contraseña para la cuenta de root, habrá que restablecer el dispositivo a los ajustes predeterminados de fábrica. Vea .
----------------------------	--

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 necesario, se puede asignar una dirección IP estática manualmente. 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 .

Se puede acceder al dispositivo localmente pero no externamente

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 5: versión de prueba de 30 días gratuita, ideal para sistemas de tamaño pequeño y medio.
- 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.

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

El cortafuegos bloquea el tráfico que utiliza el puerto 8883 por considerarse inseguro.	En algunos casos, el servidor/intermediario podría no proporcionar un puerto específico para la comunicación MQTT. Aun así, puede 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.
---	---

El dispositivo no se inicia después de conectarlo a otro producto

Clase de PoE incorrecta	Verifique que se utiliza una fuente de alimentación PoE de clase 4 cuando el dispositivo esté conectado a otro producto.
-------------------------	--

Los datos del sensor no son precisos

Los datos del sensor son inexactos	Los datos de AQI (Índice de calidad del aire), el CO ₂ , los VOC y el NO _x tardan un tiempo en estar operativos. Vea .
------------------------------------	--

Consideraciones sobre el rendimiento

Los siguientes factores son los más importantes que se deben considerar:

- Un uso denso de la red debido a una infraestructura deficiente afecta al ancho de banda.

Contactar con la asistencia técnica

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

T10222990_es

2025-09 (M2.4)

© 2025 Axis Communications AB