AXIS D4100-VE Mk II Network Strobe Siren

Manual del usuario

Índice

Instalación 4
..... 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 5
Configure su dispositivo 7
Apague el modo de mantenimiento después de instalar la sirena 7
Encienda el modo de mantenimiento 7
Configurar un perfil 7
Importar o exportar un perfil 7
Configurar SIP directo (P2P) 7
Configurar SIP a través de un servidor (PBX) 8
Configurar reglas para eventos 9
Activar una acción 9
Iniciar un perfil cuando se active una alarma 9
Iniciar un perfil a través de SIP 9
Uso de extensiones SIP para controlar más de un perfil 10
Ejecutar dos perfiles con diferentes prioridades 11
Activación de una sirena estroboscópica a través de una entrada virtual si una cámara detecta movimiento 11
Activación de una sirena estroboscópica a través de HTTP post si una cámara detecta movimiento 13
Activar la sirena estroboscópica a través de MQTT cuando la cámara detecta movimiento 14
Interfaz web 16
Descubrir más 17
Protocolo de inicio de sesión (SIP) 17
Peer-to-peer SIP (SIP de punto a punto): 17
Centralita telefónica privada (PBX) 17
NAT transversal 17
Especificaciones 18
Guía de productos 18
..... 18
Indicadores LED 18
Botones 18
Botón de control 18
Conectores 19
Conector de red 19
Conector de E/S 19
Nombres de patrones de luz 20
Nombres de los patrones de sonido 20
Limpie su dispositivo 22
Localización de problemas 23
Restablezca la configuración predeterminada de fábrica 23
Opciones de AXIS OS 23
Comprobar la versión de AXIS OS 23
Actualización de AXIS OS 24
Problemas técnicos y posibles soluciones 24
..... 26
Consideraciones sobre rendimiento 26

Contactar con la asistencia técnica 26
Ciberseguridad 27
Gestión de las vulnerabilidades 27
Notificaciones de seguridad 27
Ciclo de vida seguro del producto 27

Instalación



Cómo funciona

⚠ ADVERTENCIA

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

Localice el dispositivo en la red

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 con limitaciones

Abrir la interfaz web del dispositivo

1. Escriba el nombre de usuario y la contraseña. Si accede al dispositivo por primera vez, debe crear una cuenta de administrador. Consulte *Crear una cuenta de administrador, on page 5*.

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

Crear una cuenta de administrador

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

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

Contraseñas seguras

Importante

Utilice HTTPS (habilitado por defecto) para establecer su contraseña u otras configuraciones confidenciales a través de la red. El protocolo HTTPS habilita conexiones a la red seguras y cifradas, protegiendo así los 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.

Configure su dispositivo

Apague el modo de mantenimiento después de instalar la sirena

⚠ PRECAUCIÓN

Para proteger al instalador de los daños en la vista y del desperfectos producidos por la luz brillante, se recomienda que el modo de mantenimiento esté en funcionamiento al instalar el dispositivo.

La primera vez que instala el dispositivo, se enciende el modo de mantenimiento de forma predeterminada. Cuando el dispositivo está en modo de mantenimiento, la sirena no produce sonido y la luz proporciona patrones de luz blancas que pulsan.

Vaya a **Overview (Información general)** > **Maintenance (Mantenimiento)** para desactivar **Maintenance mode (Modo de mantenimiento)**.

Encienda el modo de mantenimiento

Para realizar el servicio del dispositivo, vaya a **Overview (Información general)** > **Maintenance (Mantenimiento)** y active **Maintenance mode (Modo de mantenimiento)**. A continuación, se pausan las actividades de luz y sirena comunes.

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)**.

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 obtener más información sobre las opciones de ajustes, consulte *SIP*.

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, consulte *NAT traversal*.

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 temporalmente los protocolos de transporte de UDP (User Datagram Protocol) a TCP (Transmission Control Protocol). 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 obtener más información sobre las opciones de ajustes, consulte *SIP*.

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. Para obtener más información, consulte *SIP*.

Configurar reglas para eventos

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

Activar una acción

1. Vaya **System (Sistema)** > **Events (Eventos)** y haga clic en **Add a rule (+Añadir 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. Seleccione qué **Action (Acción)** debe realizar cuando se cumplan las condiciones.

Iniciar un perfil cuando se active una alarma

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

Configure la entrada de dirección para el puerto:

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

Crear una regla:

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

Iniciar un perfil a través de SIP

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

Activar SIP:

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

Crear una regla:

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

Uso de extensiones SIP para controlar más de un perfil

Activar SIP:

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

Crear una regla para iniciar un perfil:

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

Crear una regla para detener un perfil:

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

8. Seleccione el perfil que desea detener.
9. Seleccione la acción **Stop (Detener)**.
10. Haga clic en **Save (Guardar)**.

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

Ejecutar dos perfiles con diferentes prioridades

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

Nota

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

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

Crear perfiles:

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

Crear una regla:

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

Activación de una sirena estroboscópica a través de una entrada virtual si una cámara detecta movimiento

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

Antes de empezar:

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

Creación de 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 <IPaddress> (dirección IP) con la dirección de la sirena estroboscópica.

- El nombre y la contraseña de la cuenta de la sirena estroboscópica 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 <IPaddress> (dirección IP) con la dirección de la sirena estroboscópica.
   - El nombre y la contraseña de la cuenta de la sirena estroboscópica 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)**: **Notifications > Send notification through HTTP (Notificaciones > Enviar notificación a través de HTTP)**
   - **Recipient (Destinatario)**: **Activate virtual port (Activar puerto virtual)**
   - **Query string suffix (Sufijo de cadena query)**: 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)**: **Notifications > Send notification through HTTP (Notificaciones > Enviar notificación a través de HTTP)**
   - **Recipient (Destinatario)**: **Deactivate virtual port (Desactivar puerto virtual)**
   - **Query string suffix (Sufijo de cadena query)**: schemaversion=1&port=1
5. Haga clic en **Save (Guardar)**.

Cree una regla en la sirena estroboscópica:

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

Activación de una sirena estroboscópica a través de HTTP post si una cámara detecta movimiento

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

Antes de empezar:

- Cree un nuevo usuario con la función de operador o administrador en la sirena estroboscópica.
- Cree un perfil en la sirena estroboscópica llamado: "Perfil de sirena estroboscópica".
- 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)**: Sirena estroboscópica
   - **Tipo**: **HTTP**
   - **URL**: http://<IPaddress>/axis-cgi/siren_and_light.cgi
     Sustituya <IPaddress> (dirección IP) con la dirección de la sirena estroboscópica.
   - El nombre de usuario y contraseña del nuevo usuario de la sirena estroboscópica.
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 la sirena estroboscópica con movimiento
   - **Condition (Condición)**: **)Applications (Aplicaciones) > Motion Guard: Camera profile (Perfil de la cámara)**
   - **Action (Acción)**: **Notifications > Send notification through HTTP (Notificaciones > Enviar notificación a través de HTTP)**
   - **Destinatario**: **Sirena estroboscópica**.
     La información debe ser la misma que ha introducido anteriormente en **Events > Recipients > Name (Eventos > Destinatarios > Nombre)**.
   - **Method (Método)**: **Post**
   - **Cuerpo**:

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

Asegúrese de introducir la misma información en **"profile" : <>** que cuando creó el perfil en la sirena estroboscópica; en este caso: "Perfil de sirena estroboscópica".

3. Haga clic en **Save (Guardar)**.
4. Agregue otra regla con la siguiente información:
   - **Name (Nombre)**: Desactivar la sirena estroboscópica con movimiento
   - **Condition (Condición)**: **)Applications (Aplicaciones) > Motion Guard: Camera profile (Perfil de la cámara)**
   - Seleccione **Invert this condition (Invertir esta condición)**.
   - **Action (Acción)**: **Notifications > Send notification through HTTP (Notificaciones > Enviar notificación a través de HTTP)**

- **Destinatario: Sirena estroboscópica**
  La información debe ser la misma que ha introducido anteriormente en **Events > Recipients > Name (Eventos > Destinatarios > Nombre)**.
- **Method (Método): Post**
- **Cuerpo**:

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

Asegúrese de introducir la misma información en **"profile" : <>** que cuando creó el perfil en la sirena estroboscópica; en este caso: "Perfil de sirena estroboscópica".

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

Activar la sirena estroboscópica a través de MQTT cuando la cámara detecta movimiento

Este ejemplo explica cómo conectar una cámara a la sirena estroboscópica a través de MQTT y cómo activar un perfil cada vez que la aplicación AXIS Motion Guard, instalada en la cámara, detecte movimiento.

Antes de empezar:

- Cree un perfil en la sirena estroboscópica.
- Configure un intermediario de MQTT y obtenga la dirección IP, el nombre de usuario y la contraseña del intermediario.
- Configure AXIS Motion Guard en la cámara.

Configuración del cliente MQTT en la cámara:

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

- **Action (Acción)**: **MQTT > Send MQTT publish message (MQTT > Enviar mensaje de publicación MQTT)**
- **Topic (Tema)**: Movimiento
- **Payload (Carga)**: Apagado
- **QoS**: 0, 1 o 2

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

Configure el cliente MQTT en la sirena estroboscópica:

1. En la interfaz del dispositivo de la sirena estroboscópica, vaya a **System > MQTT > MQTT client > Broker (Sistema > MQTT > Cliente MQTT> Intermediario)** e introduzca la siguiente información:
   - **Host**: Dirección IP de intermediario
   - **Client ID (ID de cliente)**: sirena 1
   - **Protocol (Protocolo)**: El protocolo con el que se establece el intermediario
   - **Port (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 la sirena 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)**
   - **Subscription filter (Filtro de suscripción)**: **Motion (Movimiento)**
   - **Payload (Carga)**: Encendido
   - **Action (Acción)**, **Light and siren (Luz y sirena) > Run light and siren profile while the rule is active (Ejecutar perfil de luz y sirena mientras la regla esté activa)**
   - **Profile (Perfil)**: Seleccione el perfil que desea que esté activo.
3. Haga clic en **Save (Guardar)**.

Interfaz web

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

Descubrir más

Protocolo de inicio de sesión (SIP)

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

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

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

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

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

Centralita telefónica privada (PBX)

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

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

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

NAT transversal

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

Nota

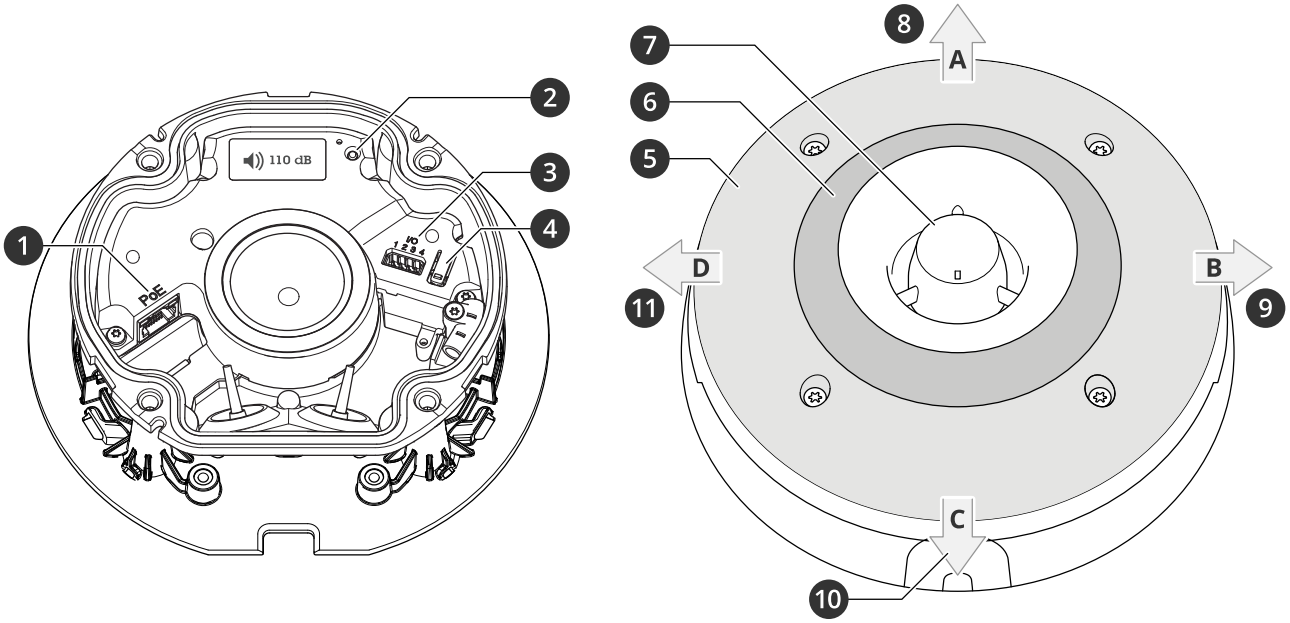
El router debe ser compatible con NAT transversal y UPnP®.

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

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

Especificaciones

Guía de productos



1 *Conector de red PoE*
2 *Indicador LED de estado*
3 *Conector de E/S*
4 *Botón de control*
5 *LED blancos*
6 *LED RGBA (rojo, azul, verde, ámbar) LEDs*
7 *Siren (Sirena):*
8 *Dirección de la luz A*
9 *Dirección de la luz B*
10 *Dirección de la luz C*
11 *Dirección de la luz D*

Indicadores LED

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

Botones

Botón de control

El botón de control se utiliza para lo siguiente:

- Restablecer el producto a la configuración predeterminada de fábrica. Consulte *Restablezca la configuración predeterminada de fábrica, on page 23*.
- Conectarse a un servicio de conexión a la nube (O3C) de un solo clic a través de Internet. Para conectarse, presione y suelte el botón y espere a que el LED de estado parpadee tres veces en verde.

Conectores

Conector de red

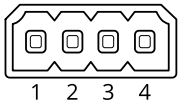
Conector Ethernet RJ45 con alimentación a través de Ethernet (PoE).

Conector de E/S

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.

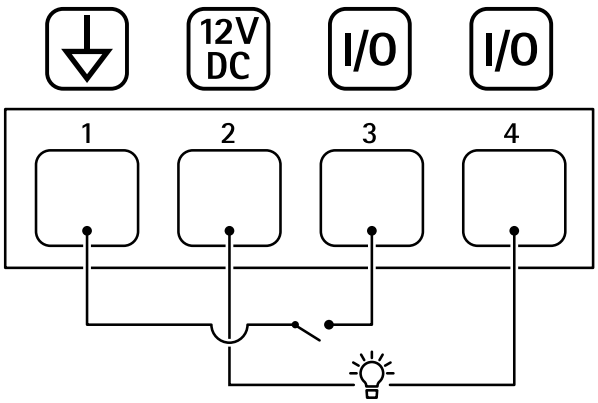
Salida digital – Conectar dispositivos externos como relés y LED. Los dispositivos conectados se pueden activar mediante la interfaz de programación de aplicaciones VAPIX®, mediante un evento o desde la interfaz web del dispositivo.

Bloque de terminales de 4 pines



Función	PIN	Notas	Especificaciones
Tierra CC	1		0 V CC
Salida de CC	2	⚠ Se puede utilizar para alimentar equipos auxiliares. Nota: Este pin solo se puede utilizar como salida de alimentación.	12 V CC Carga máx. = 50 mA
Configurable (entrada o salida)	3-4	Entrada digital: conéctela al pin 1 para activarla, o bien déjela suelta (sin conectar) para desactivarla.	0 a máx. 30 V CC
		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 un máximo de 30 V CC, colector abierto, 100 mA

Ejemplo:



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

Nombres de patrones de luz

Apagado
Fijo
Blanco fijo + color de destello
Alternativo
Pulse (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
Parpadeo 1 vez en blanco + color fijo
Parpadeo 3 veces en blanco + color fijo
Dirección A + color fijo
Dirección B + color fijo
Dirección C + color fijo
Dirección D + color fijo
Girar blanco + color fijo
Girar blanco de cola + color fijo
Blanco aleatorio + color fijo
Blanco brillante + color fijo
Blanco fijo + color fijo

Nombres de los patrones de sonido

Apagado
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: 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 y jabón suave no abrasivo.

AVISO

- Los productos químicos agresivos pueden dañar el dispositivo. No utilice productos químicos como un limpiacristales o acetona para limpiar el dispositivo.
- Evite limpiar en contacto directo con la luz o a temperaturas elevadas, ya que puede provocar manchas.

1. Utilice un aerosol de aire comprimido para quitar el polvo y la suciedad suelta del dispositivo.
2. Si es necesario, limpie el dispositivo con un paño de microfibra suave humedecido con agua tibia y jabón suave y no abrasivo.
3. Para eliminar cualquier resto de producto, limpie el dispositivo con un paño suave de microfibra humedecido con agua tibia.
4. Para evitar que queden manchas, seque el dispositivo con un paño limpio y no abrasivo.

Consulte el documento técnico *Chemical resistance to common cleaning agents (Resistencia química a productos de limpieza habituales)* para obtener más información sobre la limpieza de dispositivos Axis.

Localización de problemas

Restablezca la configuración predeterminada de fábrica

Importante

Hay que valorar bien es necesario restablecer la configuración predeterminada de fábrica. Todos los valores, incluida la dirección IP, se restablecerán a la configuración predeterminada de fábrica.

Para restablecer el producto a la configuración predeterminada de fábrica:

1. Desconecte la alimentación del producto.
2. Mantenga pulsado el botón de control mientras vuelve a conectar la alimentación. Consulte *Guía de productos, on page 18*.
3. Mantenga pulsado el botón de control durante 15-30 segundos hasta que el indicador LED de estado parpadee en color ámbar.
4. Suelte el botón de control. El proceso finalizará cuando el indicador LED de estado se ilumine en color verde. Si no hay ningún servidor DHCP en la red, la dirección IP del dispositivo será una de las siguientes de forma predeterminada:
   - **Dispositivos con AXIS OS 12.0 y versiones posteriores:** obtenidos de la subred de direcciones de enlace local (169.254.0.0/16)
   - **Dispositivos con AXIS OS 11.11 y anterior:** 192.168.0.90/24
5. Utilice las herramientas del software de instalación y gestión para asignar una dirección IP, configurar la contraseña y acceder al dispositivo.
   Las herramientas de software de instalación y gestión están disponibles en las páginas de servicio técnico de *axis.com/support*.

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

Opciones de AXIS OS

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

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

Comprobar la versión de AXIS OS

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

Para comprobar la versión de AXIS OS:

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

Actualización de AXIS OS

Importante

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

Nota

- Al actualizar el dispositivo con el AXIS OS más reciente en la pista activa, el producto obtiene las últimas funciones disponibles. Lea siempre las instrucciones de actualización y las notas de versión disponibles en cada nueva versión antes de la actualización. Para encontrar el AXIS OS y las notas de versión más recientes, consulte *axis.com/support/device-software*.

1. Descargue en su ordenador el archivo de AXIS OS, disponible de forma gratuita en *axis.com/support/device-software*.
2. Inicie sesión en el dispositivo como administrador.
3. Vaya a **Maintenance > AXIS OS upgrade (mantenimiento > actualización de AXIS OS)** y haga clic en **Upgrade (actualizar)**.

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

Problemas técnicos y posibles soluciones

Problemas para actualizar AXIS OS

Error en la actualización de AXIS OS

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

Problemas tras la actualización de AXIS OS

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

Problemas al configurar la dirección IP

No se puede configurar la dirección IP

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

Problemas de acceso al dispositivo

No puede iniciar sesión accediendo al dispositivo desde un navegador

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

Si ha olvidado la contraseña de la cuenta de administrador, deberá restablecer el dispositivo a la configuración de fábrica. Para consultar las instrucciones, vea *Restablezca la configuración predeterminada de fábrica, on page 23*.

El servidor DHCP ha cambiado la dirección IP

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

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

Error de certificado cuando se utiliza IEEE 802.1X

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

El navegador no es compatible

Para obtener una lista de los navegadores recomendados, consulte *Compatibilidad con navegadores, on page 5*.

No se puede acceder externamente al dispositivo.

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

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

Para obtener instrucciones y descargas, vaya a *axis.com/vms*.

Problemas con MQTT

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

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

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

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

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

Problemas con el sonido	
El dispositivo no está tan alto como se esperaba	Compruebe que el dispositivo esté cerrado correctamente y que no haya obstrucciones en el altavoz exponencial ni en los elementos del altavoz.
El dispositivo no reproduce sonido	Compruebe si el dispositivo está en **Maintenance mode (Modo mantenimiento)**. Si está en modo de mantenimiento, apáguelo.

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

Consideraciones sobre rendimiento

Los factores más importantes a tener en cuenta son:

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

Contactar con la asistencia técnica

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

Ciberseguridad

La ciberseguridad contribuye a un ciclo de vida satisfactorio del producto con riesgos minimizados. Puede encontrar información detallada y documentación sobre nuestro enfoque en materia de ciberseguridad en *about our cybersecurity approach at axis.com/about-axis/cybersecurity*. Siga las directrices de ciberseguridad que se indican a continuación para recibir notificaciones de seguridad de Axis sobre el producto y para realizar la configuración de su producto de modo que garantice un ciclo de vida y una desinstalación seguros.

En *Axis Trust Center*, puede encontrar información sobre la implementación que hace Axis de las medidas de cumplimiento de seguridad, transparencia, protección de datos y privacidad.

Gestión de las vulnerabilidades

Axis es una *Common Vulnerability and Exposures (CVE) Numbering Authority (CNA) (autoridad numeradora de vulnerabilidades y exposiciones comunes (CVE) (CNA))*. Para minimizar su riesgo de exposición, satisfacemos las normas del sector a la hora de identificar y resolver vulnerabilidades en nuestros dispositivos, software y servicios. Consulte más información sobre nuestra política de gestión de vulnerabilidades o notifique una vulnerabilidad en *axis.com/vulnerability-management*.

Notificaciones de seguridad

Suscríbase a los correos electrónicos de notificaciones de seguridad de Axis en *axis.com/security-notification-service*. Le enviaremos información sobre vulnerabilidades, los avisos de seguridad correspondientes y otros asuntos relacionados con la seguridad de su producto Axis.

Ciclo de vida seguro del producto

Axis minimiza los riesgos a lo largo de la vida útil de nuestros productos mediante una gestión segura del ciclo de vida. Utilice nuestras guías de refuerzo en *help.axis.com* para configurar y operar sus productos Axis del modo más seguro y para encontrar información sobre:

Primer uso seguro – Los productos Axis vienen preconfigurados con un alto nivel de protección por defecto para permitir una inicialización segura y una comunicación cifrada desde el primer momento.

Uso previsto y errores de configuración comunes – Nuestras guías facilitan información sobre el uso previsto de los productos Axis, incluidos errores de uso comunes relacionados con la seguridad y errores de configuración que deben evitarse.

Gestión de vulnerabilidades y transparencia en la cadena de suministro – Con cada lanzamiento de software se publica una lista de materiales de software (SBOM) en *axis.com y* con el fin de revelar vulnerabilidades y mejorar la transparencia de la cadena de suministro.

Desinstalación y borrado seguro de datos – Para desinstalar un producto de forma segura cuando alcanza el término de su ciclo de vida, restablézcalo a los valores predeterminados de fábrica. Esto eliminará sus configuraciones, datos almacenados e información confidencial.

T10223803_es

2026-10 (M7.2)

© 2025 – 2026 Axis Communications AB