AXIS I8307-VE Network Intercom

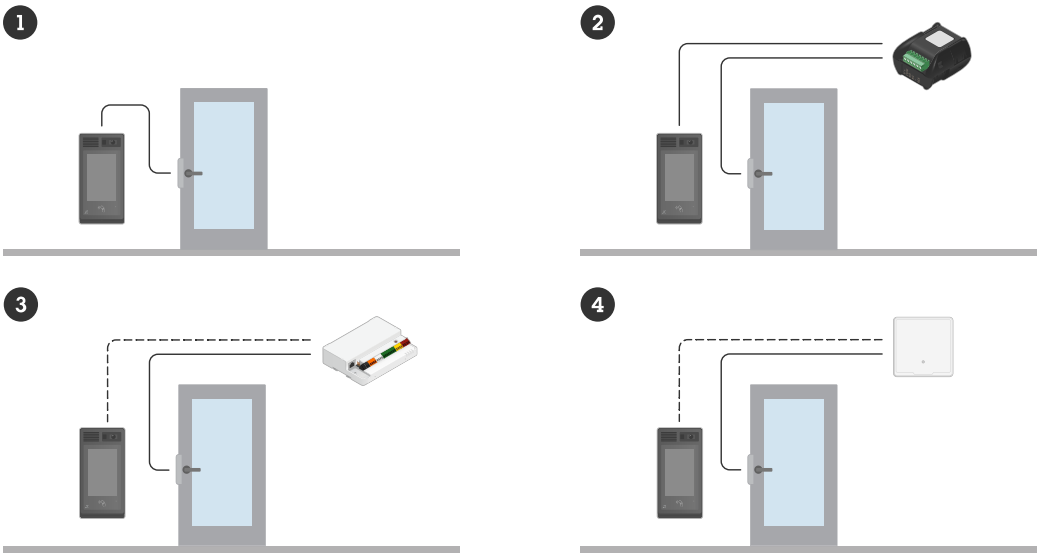
Manual del usuario

Índice

Presentación esquemática de la solución 4
Instalación 5
Modo de vista previa 5
Cómo funciona 6
Localice el dispositivo en la red 6
Compatibilidad con navegadores 6
Abrir la interfaz web del dispositivo 6
Crear una cuenta de administrador 6
Contraseñas seguras 7
Asegúrese de que no se ha manipulado el software del dispositivo 7
Configure su dispositivo 8
Calibración y ejecución de un altavoz remoto 8
Configurar SIP directo (P2P) 8
Configurar SIP a través de un servidor (PBX) 9
Crear un contacto 10
Añadir un botón de llamada a la pantalla 10
Configurar como lector 10
Utilice la lista de entrada para permitir que los titulares de credenciales abran la puerta 11
Configúrelo como lector de tarjetas mediante un controlador de puerta 11
Utilizar datos protegidos en tarjetas para aumentar la seguridad 13
Usar DTMF para mostrar un mapa en la pantalla 13
Interfaz web 15
Descubrir más 16
Voz por IP (VoIP) 16
Protocolo de inicio de sesión (SIP) 16
Peer-to-peer SIP (SIP de punto a punto): 16
Centralita telefónica privada (PBX) 17
NAT transversal 18
Configurar reglas para eventos 18
Analíticas y aplicaciones 18
AXIS Client for Unified Communication Systems 18
Especificaciones 19
Guía de productos 19
Indicadores LED 20
Ranura para tarjeta SD 21
Botones 21
Botón de control 21
Conectores 21
Conector de red 21
Conector de audio 21
Conector de relé 21
Conector de lector 22
Conector de E/S 23
Conector de corriente 23
Conectar los equipos 25
Un relé alimentado por PoE (12 V) 25
Dos relés alimentados por PoE (12 V) 25
Un relé alimentado por PoE (12 V) + un relé alimentado por fuente de alimentación externa 26
Un relé alimentado por PoE (12 V) + un contacto libre de potencial del relé 26
Cerradura de seguridad negativa de 12 V alimentada mediante PoE+ desde el intercomunicador 27
Cerradura de seguridad negativa alimentada por fuente de alimentación externa 27
Un relé alimentado por PoE (24 V) + un contacto libre de potencial del relé 28
Lector conectado al controlador de puerta mediante OSDP 28

Lector conectado al controlador de puerta mediante Wiegand 29
Lector conectado al controlador de puerta Axis mediante lector VAPIX 29
Localización de problemas 30
Restablezca la configuración predeterminada de fábrica 30
Opciones de AXIS OS 30
Comprobar la versión de AXIS OS 30
Actualización de AXIS OS 31
Problemas técnicos y posibles soluciones 31
Consideraciones sobre rendimiento 33
Contactar con la asistencia técnica 34
Información de seguridad 35
Niveles de peligro 35
Otros niveles de mensaje 35
Ciberseguridad 36
Gestión de las vulnerabilidades 36
Notificaciones de seguridad 36
Ciclo de vida seguro del producto 36

Presentación esquemática de la solución



1 *Intercomunicadores*
2 *Intercomunicador combinado con AXIS A9801*
3 *Intercomunicador combinado con AXIS A9210*
4 *Intercomunicador combinado con un sistema de control de acceso*

Instalación



Modo de vista previa

El modo de vista previa es ideal para los instaladores cuando se ajusta con precisión la vista de la cámara durante la instalación. No es necesario iniciar sesión para acceder a la vista de cámara en modo de vista previa. Solo está disponible en el estado de configuración predeterminada de fábrica durante un tiempo limitado para encender el dispositivo.



Este vídeo demuestra cómo utilizar el modo de vista previa.

Cómo funciona

Localice el dispositivo en la red

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

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

Compatibilidad con navegadores

Puede utilizar el dispositivo con los siguientes navegadores:

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

✓: Recomendado

*: Asistencia 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 desconoce 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. Consulte *Crear una cuenta de administrador, on page 6*.

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 7*.
3. Vuelva a escribir la contraseña.
4. Aceptar el acuerdo de licencia.
5. Haga clic en **Add account (agregar cuenta)**.

Importante

El dispositivo no tiene una cuenta predeterminada. Si pierde la contraseña de la cuenta de administrador, debe restablecer el dispositivo. Consulte *Restablezca la configuración predeterminada de fábrica, on page 30*.

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.

Asegúrese de que no se 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. Consulte *Restablezca la configuración predeterminada de fábrica, on page 30*.
   Después de un restablecimiento, el inicio seguro garantiza el estado del dispositivo.
2. Configure e instale el dispositivo.

Configure su dispositivo

En esta sección se tratarán todas las configuraciones importantes que un instalador tiene que hacer para poner en funcionamiento el producto una vez que se haya completado la instalación del hardware.

Calibración y ejecución de un altavoz remoto

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

Nota

La prueba se debe calibrar desde el lugar en el que está montado. Si el altavoz se mueve o su entorno local cambia, por ejemplo, si se levanta o se derriba una pared, el altavoz se debe calibrar de nuevo

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

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

Nota

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

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

Nota

También es posible ejecutar la calibración pulsando el botón de control del dispositivo físico. Consulte *Guía de productos, on page 19* para identificar el botón de control.

Configurar SIP directo (P2P)

VoIP (Voz por IP) es un conjunto de tecnologías que permite la comunicación multimedia y por voz a través de redes IP. Para obtener más información, consulte *Voz por IP (VoIP), on page 16*.

En este dispositivo, VoIP se habilita a través del protocolo SIP. Para obtener más información sobre SIP, consulte *Protocolo de inicio de sesión (SIP), on page 16*.

Existen dos tipos de configuraciones para SIP. De punto a punto (p2P) directo es una de ellos. 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 información sobre cómo realizar la configuración, consulte *Peer-to-peer SIP (SIP de punto a punto):, on page 16*.

1. Vaya a **Communication > SIP > Settings (Comunicación > SIP > Ajustes)** y seleccione **Enable SIP (Habilitar SIP)**.
2. Para permitir que el dispositivo reciba llamadas entrantes, seleccione **Allow incoming calls (Permitir llamadas entrantes)**.

AVISO

Cuando se permiten las llamadas entrantes, el dispositivo acepta llamadas desde cualquier dispositivo conectado a la red. Si se puede acceder al dispositivo desde una red pública o desde Internet, le recomendamos que no permita las llamadas entrantes.

3. Haga clic en **Call handling (Gestión de llamadas)**.
4. En **Calling timeout (Tiempo de espera de llamada)**, establezca el número de segundos que debe durar una llamada antes de finalizarla si no hay respuesta.
5. Si ha permitido las llamadas entrantes, defina el número de segundos antes del tiempo de espera para dichas llamadas **Incoming call timeout (Tiempo de espera de llamadas entrantes)**.

6. Haga clic en **Ports (Puertos)**.
7. Introduzca el número de **SIP port (Puerto SIP)** y el número de **TLS port (Puerto TLS)**.

Nota

- **SIP port (Puerto SIP)**: para sesiones SIP. El tráfico de señalización a través de este puerto no está cifrado. El puerto predeterminado es el 5060.
- **TLS port (Puerto TLS)**: para sesiones SIPS y sesiones SIP protegidas por TLS. El tráfico de señalización a través de este puerto se cifra empleando Transport Layer Security (TLS). El puerto predeterminado es el 5061.
- **RTP start port (Puerto de inicio RTP)**: el puerto utilizado para la primera transmisión de medios RTP en una llamada SIP. El puerto de inicio predeterminado es 4000. Algunos firewalls pueden bloquean el tráfico RTP en determinados números de puerto. El número de puerto debe estar entre 1024 y 65535.

8. Haga clic en **NAT transversal**.
9. Seleccione los protocolos que desea activar para NAT transversal.

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 transversal, on page 18*.

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

Configurar SIP a través de un servidor (PBX)

VoIP (Voz por IP) es un conjunto de tecnologías que permite la comunicación multimedia y por voz a través de redes IP. Para obtener más información, consulte *Voz por IP (VoIP), on page 16*.

En este dispositivo, VoIP se habilita a través del protocolo SIP. Para obtener más información sobre SIP, consulte *Protocolo de inicio de sesión (SIP), on page 16*.

Existen dos tipos de configuraciones para SIP. Emplear un servidor PBX es una de ellas. Utilice un servidor PBX cuando la comunicación se realice entre un número infinito de agentes de usuario dentro y fuera de la red IP. Se pueden añadir funciones adicionales a la configuración en función del proveedor de PBX. Para obtener más información, consulte *Centralita telefónica privada (PBX), on page 17*.

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. Vaya a **Communication> SIP > Accounts (Comunicación > SIP > Cuentas)** y haga clic en **+ Add account (+ Agregar cuenta)**.
3. Introduzca un **Name (Nombre)** para la cuenta.
4. Seleccione **Registered (Registrado)**.
5. Seleccionar un modo de transporte.
6. Agregue la información de cuenta del proveedor del PBX.
7. Haga clic en **Save (Guardar)**.
8. Configure los ajustes SIP de la misma manera que para una red par a par, véase *Configurar SIP directo (P2P), on page 8*. Utilice el puerto de inicio RTP del proveedor PBX.

Crear un contacto

En este ejemplo se explica cómo crear un nuevo contacto en la lista de contactos. Antes de comenzar, active SIP en **Communication > SIP (Comunicación > SIP)**.

Para crear un nuevo contacto:

1. Vaya a **Communication > Contact list (Comunicación > Lista de contactos)**.
2. Haga clic en **+ Add contact (+ Agregar contacto)**.
3. Introduzca el nombre y apellidos del contacto.
4. Introduzca la dirección SIP del contacto.

Nota

Para obtener información acerca de las direcciones SIP, consulte *Protocolo de inicio de sesión (SIP), on page 16*.

5. Seleccione la cuenta SIP desde la que desea llamar.

Nota

Las opciones de disponibilidad se definen en **System (Sistema)** > **Eventos (Eventos)** > **Schedules (Programaciones)**.

6. Seleccione la disponibilidad del **contacto**. Si hay una llamada cuando el contacto no está disponible, la llamada se cancela a menos que haya un contacto de reserva.

Nota

Una reserva es un contacto al que se envía la llamada si el contacto original no responde o no está disponible.

7. En **Fallback (Reserva)**, seleccione **None (Ninguno)**.
8. Haga clic en **Save (Guardar)**.

Añadir un botón de llamada a la pantalla

Este ejemplo explica cómo configurar la pantalla para mostrar un botón que los visitantes puedan pulsar para llamar a recepción.

Antes de empezar

- Crear el contacto de recepción. Para consultar las instrucciones, vea *Crear un contacto, on page 10*.

1. Vaya a **Display (Pantalla)> Pages (Páginas)**.
2. En **Default Homepage (Página de inicio predeterminada)**, haga clic en ⋮ y seleccione **Edit (Editar)**.
3. Haga clic en **+ Agregar**.
4. En la lista **Type (Tipo)**, seleccionar **Button (Botón)**.
5. En la lista de contactos, seleccionar la recepción.
6. Seleccionar el tamaño del botón.
7. Para guardar el botón, haga clic en **Save (Guardar)**.
8. Para guardar la página de inicio predeterminada, haga clic en **Save (Guardar)**.

Configurar como lector

Puede configurar su intercomunicador como lector para permitir que los titulares de credenciales abran la puerta.

Mediante la función de lista de entrada, el intercomunicador almacena las credenciales localmente y puede actuar como lector independiente para hasta cincuenta titulares de credenciales.

Al conectar el intercomunicador a un controlador de puerta, el intercomunicador puede continuar almacenando hasta cincuenta credenciales, y si la credencial solicitada se encuentra en la lista de entrada, el intercomunicador gestionará los permisos de acceso. Si la credencial solicitada no se encuentra en la lista de entrada y la opción **Use connected door controller (Usar controlador de puerta conectado)** está activada, la solicitud se reenviará al controlador de puerta, que a su vez gestionará los permisos de acceso.

Utilice la lista de entrada para permitir que los titulares de credenciales abran la puerta

Con la lista de entrada, puede hacer posible que los titulares de credenciales utilicen estas para activar acciones, como abrir una puerta. En este ejemplo se explica cómo añadir un titular de la credencial que puede utilizar su tarjeta para abrir la puerta 10 veces.

Requisitos previos

- Asegúrese de que el tipo de chip correcto esté activo en **Reader > Chip types (Lector > Tipos de chip)**.

Active la lista de entrada y agregue un soporte de credencial:

1. Vaya a **Reader > Entry list (Lector > Lista de entrada)**.
2. Active **Use Entry list (Usar lista de entradas)**.
3. Haga clic en **+ Add credential holder (Agregar soporte de la credencial)**.
4. Introduzca el nombre y apellidos del titular de las credenciales. El nombre debe ser único.
5. Seleccione **Card (Tarjeta)**.
6. Pase la tarjeta del titular de la credencial en el dispositivo y haga clic en **Get latest (Obtener último)**.
7. Mantenga la condición de evento **Access granted (Acceso concedido)**.
8. En **Valid to (Válido para)**, seleccione **Number of times (Número de veces)**.
9. En **Number of times (Número de veces)**, introduzca 10.
10. Haga clic en **Save (Guardar)**.

Crear una regla:

1. Vaya a **System > Events (Sistema > Eventos)**.
2. En **Rules (Reglas)**, haga clic en **+ Add a rule (Agregar una regla)**.
3. En **Name (Nombre)**, introduzca Open door (Puerta abierta).
4. En la lista de condiciones, seleccione **Entry list > Access granted (Lista de entradas > Acceso concedido)**.
5. En la lista de acciones, seleccione **I/O > Toggle I/O once (E/S > Conmutar E/S una sola vez)**.
6. En la lista de puertos, seleccione **Door (Puerta)**.
7. En **State (Estado)**, seleccione **Activo (Active)**.
8. Defina la duración en 00:00:07.
9. Haga clic en **Save (Guardar)**.

Configúrelo como lector de tarjetas mediante un controlador de puerta

Conexión de red

Para utilizar el intercomunicador como lector de tarjetas, puede conectarlo a un controlador de puerta. El controlador de puerta almacena todas las credenciales y realiza un seguimiento de a quién se permite cruzar la puerta. En este ejemplo, conectamos los dispositivos a través de la red. También modificamos los tipos de tarjeta permitidos.

Importante

La conexión de red solo funciona con los controladores de puerta Axis. Para conectarse a un controlador de puerta que no sea de Axis, debe conectar físicamente los dispositivos con cables. Consulte *Conexión por cable, on page 12*.

Configurar el intercomunicador como lector de tarjetas

1. Vaya a **Reader (Lector) > Connection (Conexión)**.
2. Seleccione el tipo de protocolo **Lector VAPIX**.
3. Seleccione el protocolo para la comunicación con el controlador de puerta.

Nota

Recomendamos activar **Verificar certificado** si está usando **HTTPS**.

4. Introduzca la dirección IP para el controlador de puerta.
5. Escriba las credenciales para el controlador de puerta.
6. Haga clic en **Connect (Conectar)**.
7. Seleccione el lector de entrada para la puerta adecuada.
8. Haga clic en **Save (Guardar)**.

Conexión por cable

Para utilizar el videoportero como lector de tarjetas, puede conectarlo a un controlador de puerta. El controlador de puerta almacena todas las credenciales y realiza un seguimiento de a quién se permite cruzar la puerta. En este ejemplo, conectamos los dispositivos con cables, utilizamos el protocolo Wiegand, activamos el avisador acústico y empleamos un puerto de E/S para el LED. También modificamos los tipos de tarjeta permitidos.

Importante

Utilice puertos de E/S que no estén ya en uso. Si utiliza puertos de E/S que ya están en uso, los eventos creados para estos puertos dejarán de funcionar.

Antes de empezar

- Conecte el intercomunicador a un controlador de puerta.
  Consulte los planos del cableado eléctrico, que encontrará en *Conectar los equipos, on page 25*.
- Configure el hardware del controlador de puerta empleando el protocolo Wiegand para el lector. Para obtener instrucciones, consulte el manual de usuario del controlador de puerta.

Configurar el intercomunicador como lector de tarjetas

1. Vaya a **Reader (Lector) > Connection (Conexión)**.
2. Seleccione **Wiegand** como tipo de protocolo.
3. Active **Beeper**.
4. En **Input for beeper (Entrada para el avisador acústico)**, seleccione **I3**.
5. En **Input used for LED control (Entrada utilizada para el control LED)**, seleccione **1**.
6. En **Input for LED1 (Entrada para LED1)**, seleccione **I1**.
7. Seleccione los colores que se utilizarán para cada estado.
8. En **Formato KeyPress**, seleccione **FourBit**.
9. Haga clic en **Save (Guardar)**.
10. Vaya a **Lector > Tipos de chip** y active los tipos de chip que desee utilizar.

Nota

Puede mantener el conjunto de tipos de chip predeterminado, pero le recomendamos que modifique la lista según sus necesidades específicas.

11. Haga clic en **Agregar conjunto de datos** para especificar los conjuntos de datos para los distintos tipos de chip.
12. Haga clic en **Save (Guardar)**.

Utilizar datos protegidos en tarjetas para aumentar la seguridad

Para aumentar la seguridad en su sistema de control de acceso, puede elegir utilizar datos de tarjeta seguros almacenados en algunos tipos de tarjetas. Los datos están protegidos por una clave confidencial. Para leer los datos de la tarjeta, es necesario almacenar la clave secreta y otra información sobre la tarjeta en el dispositivo.

1. Vaya a **Lector > Tipos de chip**.
2. En **Data sets (Conjuntos de datos)**, seleccione el tipo de chip que desea editar y haga clic en **Add data set (Agregar conjunto de datos)**.
3. Introduzca información sobre los datos de la tarjeta. La información que debe introducirse dependerá del tipo de tarjeta y de la forma en la que se inscribió.
4. Si utiliza los protocolos OSDP o Wiegand, seleccione **Use as UID (Usar como UID)** para enviar los datos seguros como UID/CSN en lugar de como UID/CSN de tarjeta normal.
5. Para permitir que las tarjetas que cumplan con los datos de tarjeta especificados se envíen al controlador de acceso, seleccione **Datos obligatorios**. El lector ignora las tarjetas que no cumplen los requisitos.
6. Haga clic en **Save (Guardar)**.

Usar DTMF para mostrar un mapa en la pantalla

Cuando un visitante llama desde el intercomunicador y necesita indicaciones, quien contesta puede usar la señalización DTMF (multifrecuencia bitono) para mostrar un mapa en la pantalla del intercomunicador.

En este ejemplo se explica cómo:

- Subir una imagen de mapa al intercomunicador.
- Crear una página que contenga la imagen del mapa en el intercomunicador.
- Definir la secuencia DTMF en el intercomunicador.
- Configurar el intercomunicador para que muestre la página del mapa durante 30 segundos como respuesta a la secuencia DTMF.

Antes de empezar

- Permitir llamadas SIP desde el dispositivo y crear una cuenta SIP. Para consultar instrucciones, vea *Configurar SIP directo (P2P), on page 8* y *Configurar SIP a través de un servidor (PBX), on page 9*.

Cargar imagen del mapa

1. Ir a **Media (Medios)**.
2. Haga clic en **+ Agregar**.
3. Arrastrar y soltar una imagen que muestre un mapa del edificio. La resolución de imagen recomendada es de 480 x 800 píxeles y la máxima, de 2048 x 2048 píxeles.
4. Haga clic en **Save (Guardar)**.

Crear una página de mapa para la visualización

5. Vaya a **Display (Pantalla)> Pages (Páginas)**.
6. Haga clic en **+ Agregar**.
7. Escriba un nombre para la página, por ejemplo Map page (Página del mapa).
8. Haga clic en **+ Agregar**.
9. En la lista de tipos, seleccione **Image (Imagen)**.
10. Escriba un nombre para la imagen, por ejemplo Map image (Imagen del mapa).
11. En la lista de imágenes, seleccione la imagen del mapa.
12. Haga clic en **Save (Guardar)**.
13. Vuelva a hacer clic en **Save (Guardar)**.

Definir la secuencia DTMF

14. Vaya a **Communication (Comunicación) > SIP > DTMF**.
15. Haga clic en **+ Add sequence (Agregar secuencia)**.
16. En **Sequence (Secuencia)**, escriba 9.
17. En **Description (Descripción)**, escriba Show map (Mostrar mapa).
18. Seleccione una cuenta.
19. Haga clic en **Save (Guardar)**.

Crear una regla

20. Vaya a **System > Events > Rules (Sistema > Eventos > Reglas)** y añada una regla.
21. Escriba un nombre para la regla, por ejemplo, Use DTMF to show map (Usar DTMF para mostrar el mapa).
22. En la lista de condiciones, seleccione **Call (Llamar) > DTMF**.
23. En la lista de ID de eventos DTMF, seleccione **Show map (Mostrar mapa)**.
24. En la lista de acciones, seleccione **Display (Pantalla) > Show page (Mostrar página)**.
25. En la lista de páginas, seleccione **Map page (Página del mapa)**.
26. En **Duration (Duración)**, introduzca 00:00:30 para mostrar el mapa durante 30 segundos.
27. 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)*.

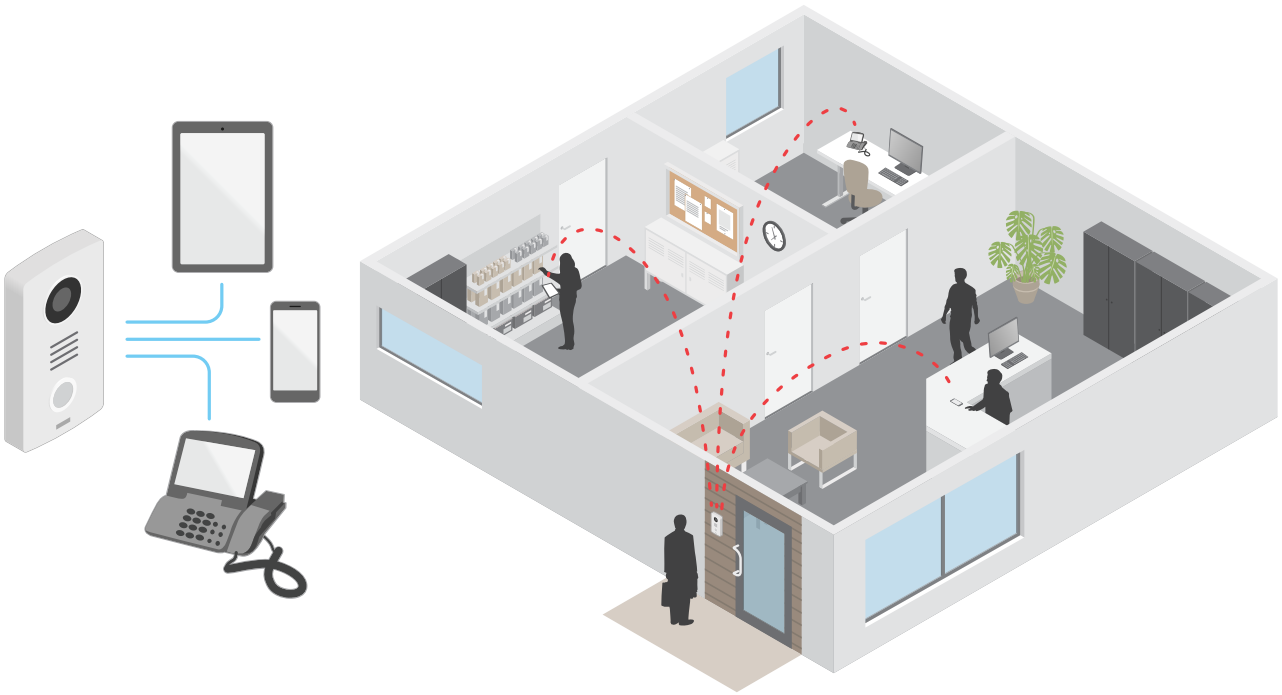
Descubrir más

Voz por IP (VoIP)

Voz por IP (VoIP) es un conjunto de tecnologías que permite la comunicación por voz y las sesiones multimedia a través de redes IP como Internet. En las llamadas telefónicas tradicionales, las señales analógicas se envían a través de las transmisiones de circuitos a través de la red telefónica pública conmutada (PSTN). En una llamada VoIP, las señales analógicas se convierten en señales digitales para poder enviarlas en paquetes de datos a través de redes IP locales o de Internet.

En el producto de Axis, VoIP se habilita a través del protocolo de inicio de sesión (SIP) y de la señalización multifrecuencia de doble tono (DTMF).

Ejemplo:



Al pulsar el botón de llamada en un intercomunicador Axis, se inicia una llamada a uno o varios destinatarios predefinidos. Cuando un destinatario responde, se establece una llamada. La voz y el vídeo se transmiten a través de tecnologías VoIP.

Protocolo de inicio de sesión (SIP)

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

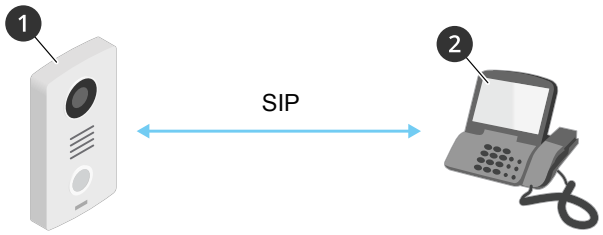
El audio o el vídeo real se intercambian entre los agentes de usuario SIP con un protocolo de transporte, por ejemplo, RTP (protocolo de transporte en tiempo real).

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

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

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

Ejemplo:



1 *User agent A - intercomunicador. Dirección IP: sip:192.168.1.101*
2 *User agent B - teléfono habilitado para SIP. Dirección IP: sip:192.168.1.100*

Puede configurar el intercomunicador de Axis para que llame, por ejemplo, a un teléfono habilitado para SIP en la misma red mediante una configuración de SIP de punto a punto.

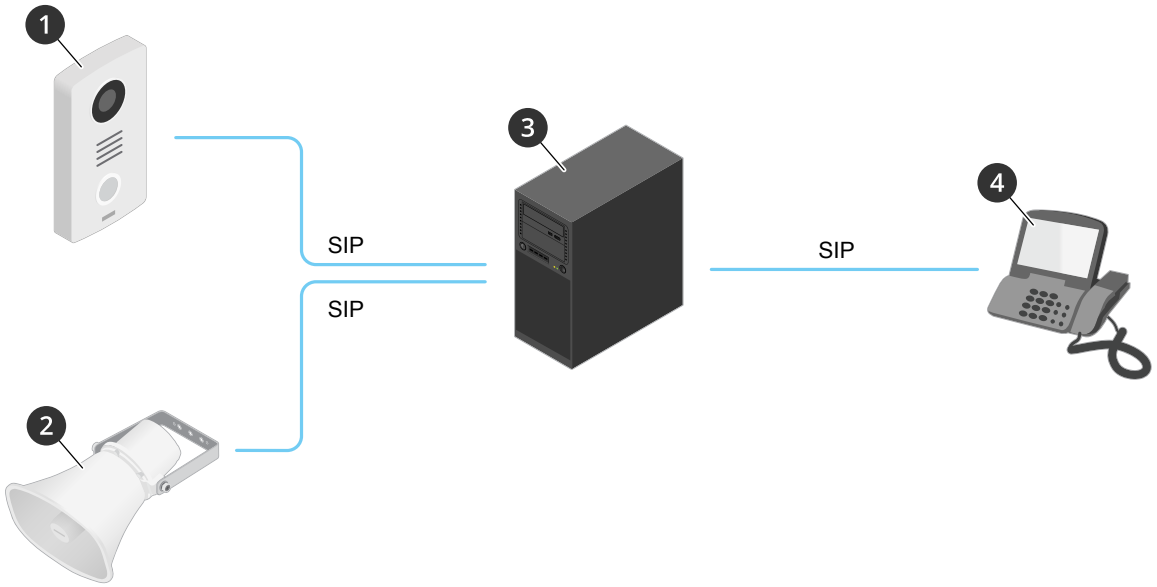
Centralita telefónica privada (PBX)

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

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

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

Ejemplo:



1 *sip:mydoor@company.com*
2 *sip:myspeaker@company.com*
3 ***PBX** sip.company.com*
4 *sip:office@company.com*

Al pulsar el botón de llamada en un intercomunicador Axis, la llamada se envía a través de una o varias PBX a una dirección SIP, ya sea en la red IP local o a través de Internet.

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.

Configurar reglas para eventos

Puede crear reglas para que el dispositivo realice una acción cuando se produzcan determinados eventos. Una regla consta de condiciones y acciones. Las condiciones se pueden utilizar para activar las acciones. Por ejemplo, el dispositivo puede iniciar una grabación o enviar un correo electrónico cuando detecta movimiento o mostrar un texto superpuesto mientras está grabando.

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

Analíticas y aplicaciones

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

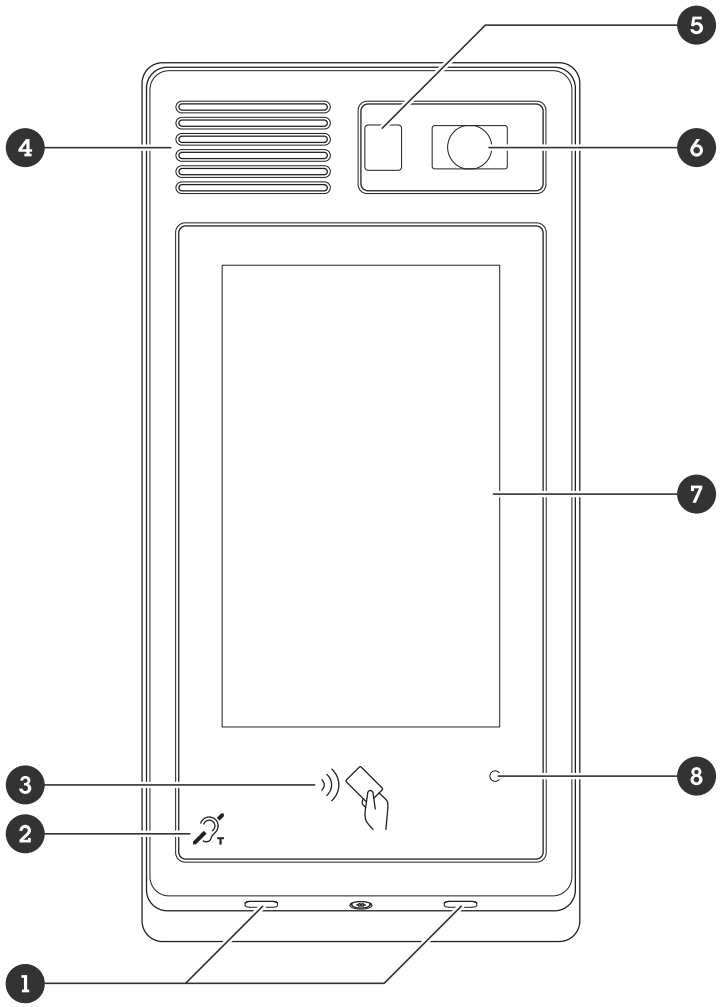
Para encontrar los manuales de usuario de analíticas y apps de Axis, visite *help.axis.com*.

AXIS Client for Unified Communication Systems

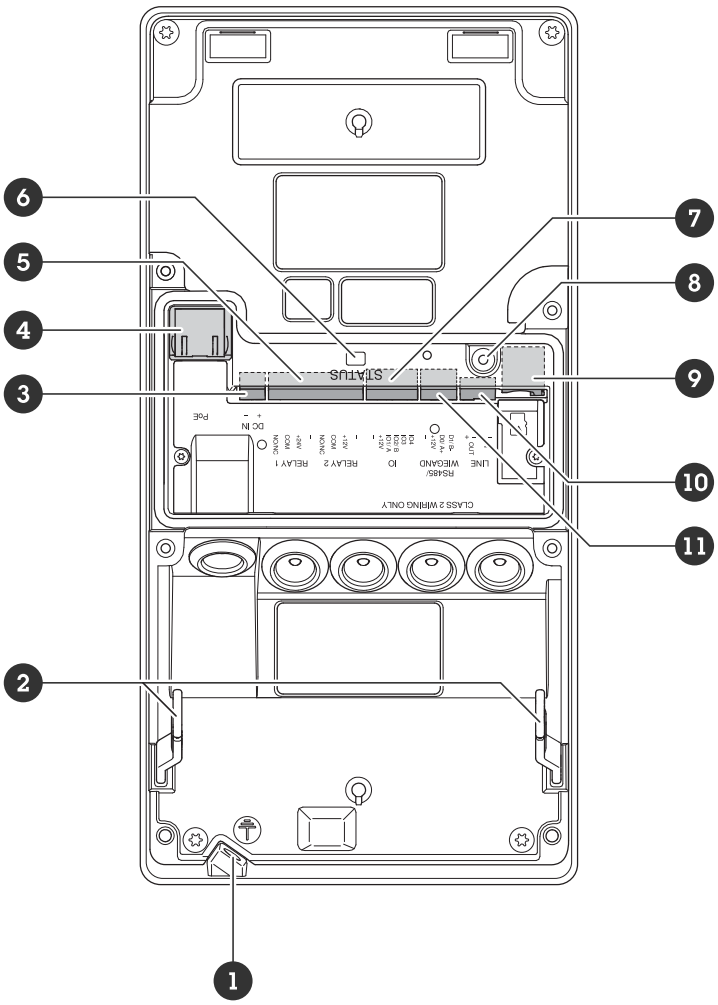
Con esta aplicación, puede realizar llamadas entre dispositivos Axis habilitados para SIP y cuentas vinculadas de Microsoft® Teams. Para obtener más información, consulte el *manual de usuario de AXIS Client for Unified Communication Systems*.

Especificaciones

Guía de productos



1 *Micrófono (2)*
2 *T-coil*
3 *Lector de RFID*
4 *Altavoz*
5 *Sensor de PIR*
6 *Cámara*
7 *Pantalla*
8 *Sensor lumínico*



1 *Tornillo de toma de tierra*
2 *Bisagras de instalación*
3 *Conector de corriente*
4 *Conector de red*
5 *Conector de relé (2)*
6 *LED de estado*
7 *Conector de E/S*
8 *Botón de control*
9 *Ranura para tarjetas SD (microSD)*
10 *Conector de audio*
11 *Conector de lector*

Indicadores LED

LED de estado	Indicación
Verde	Fijo para indicar un funcionamiento normal.

Ranura para tarjeta SD

AVISO

- Riesgo de daños en la tarjeta SD. No utilice herramientas afiladas, objetos metálicos ni ejerza una fuerza excesiva al introducir o eliminar la tarjeta SD. Utilice los dedos para introducir y eliminar la tarjeta.
- Riesgo de pérdida de datos y grabaciones dañadas. Desmonte la tarjeta SD desde la interfaz web del dispositivo antes de retirarla. No extraiga la tarjeta SD mientras el producto esté en funcionamiento.

Este dispositivo admite tarjetas microSD/microSDHC/microSDXC.

Para conocer las recomendaciones sobre tarjetas SD, consulte *axis.com*.

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

Botones

Botón de control

El botón de control se utiliza para lo siguiente:

- Restablecer el producto a la configuración predeterminada de fábrica. Consulte *Restablezca la configuración predeterminada de fábrica, on page 30*.

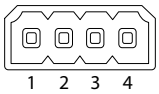
Conectores

Conector de red

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

Conector de audio

Bloque de terminales de 4 pines para entrada y salida de audio.

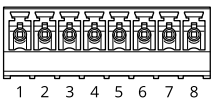


Función	Pasador	Notas
Entrada de línea	1	Entrada de línea (mono)
Toma de tierra (GND)	2	Tierra de audio
Salida de línea	3	Salida de línea
Toma de tierra (GND)	4	Tierra de audio

Conector de relé

Bloque de terminales de 8 pines para relés de estado sólido que se puede utilizar de las siguientes formas:

- Como relé estándar que abre y cierra circuitos auxiliares.
- Para controlar directamente un bloqueo.
- Para controlar un bloqueo a través de un relé de seguridad. El uso de un relé de seguridad en el lado seguro de la puerta previene el puenteado.



Función	Pasador	Notas	Especificaciones
NO/NC	1	Normalmente abierto/normalmente cerrado Para conectar dispositivos de relés. Los dos pines de relé están separados de forma galvanizada del resto del circuito.	Corriente máx. 1 A Voltaje máx. 30 V CC
COM	2	Común	
24 V CC	3	Para conectar el equipo auxiliar. Nota: Este pin solo se puede utilizar como salida de alimentación.	Tensión de salida 24 V CC Corriente máx. 50 mA[1] Corriente máx. 300 mA[2]
Tierra CC	4		0 V CC
NO/NC	5	Normalmente abierto/normalmente cerrado Para conectar dispositivos de relés. Los dos pines de relé están separados de forma galvanizada del resto del circuito.	Corriente máx. 1 A Voltaje máx. 30 V CC
COM	6	Común	
12 V CC	7	Para conectar el equipo auxiliar. Nota: Este pin solo se puede utilizar como salida de alimentación.	Tensión de salida: 12 V CC . Corriente máxima: 100 mA[1] Corriente máx. 600 mA[2]
Tierra CC	8		0 V CC

Conector de lector

Bloque de terminales de 4 pines para conectar lector externo.

Función	Pasador	Notas	Especificaciones
Tierra CC	1		0 V CC
12 V CC	2	Para conectar el equipo auxiliar. Nota: Este pin solo se puede utilizar como salida de alimentación.	Tensión de salida 12 V CC
D0/A+	3	Wiegand: Salida DATA0 RS485: A+	
D1/B-	4	Wiegand: Salida DATA1 RS485: B-	

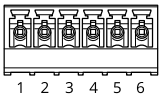
1. *Alimentación a través de Ethernet IEEE 802.3af/802.3at Tipo 1 Clase 3.*
2. *Cuando se recibe corriente de alimentación a través de Ethernet Plus (PoE+) IEEE 802.3at Tipo 2 Clase 4 o entrada de corriente continua.*

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:

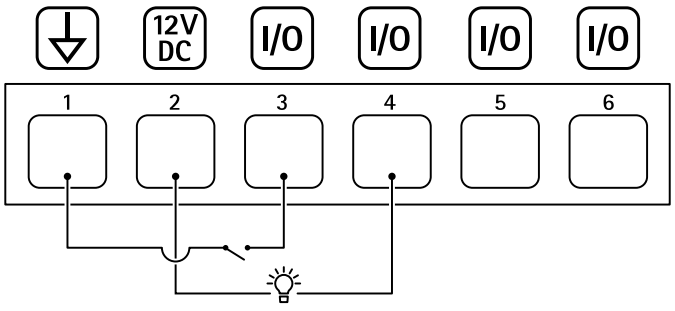
Entrada digital – Conectar dispositivos que puedan alternar entre circuitos cerrados y abiertos, por ejemplo, sensores PIR, contactos de puertas y ventanas o detectores de cristales rotos.

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.



Función	Pasador	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)	3–6	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*
5 *E/S configurable*
6 *E/S configurable*

Conector de corriente

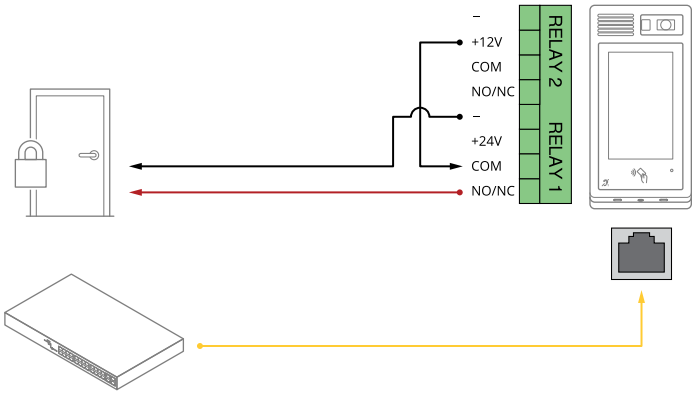
Bloque de terminales de 2 pines para la entrada de alimentación de CC. Use una fuente de alimentación limitada (LPS) que cumpla los requisitos de seguridad de baja tensión (SELV) con una potencia nominal de salida limitada a ≤100 W o una corriente nominal de salida limitada a ≤5 A.



Función	Pasador	Notas	Especificaciones
Tierra CC	1		0 V CC
Entrada CC	2	Para alimentar el controlador cuando no se use la alimentación a través de Ethernet. Nota: Este pin solo se puede utilizar como entrada de alimentación.	18-28 V CC, 22 W máx. Carga máxima en las salidas 9 W

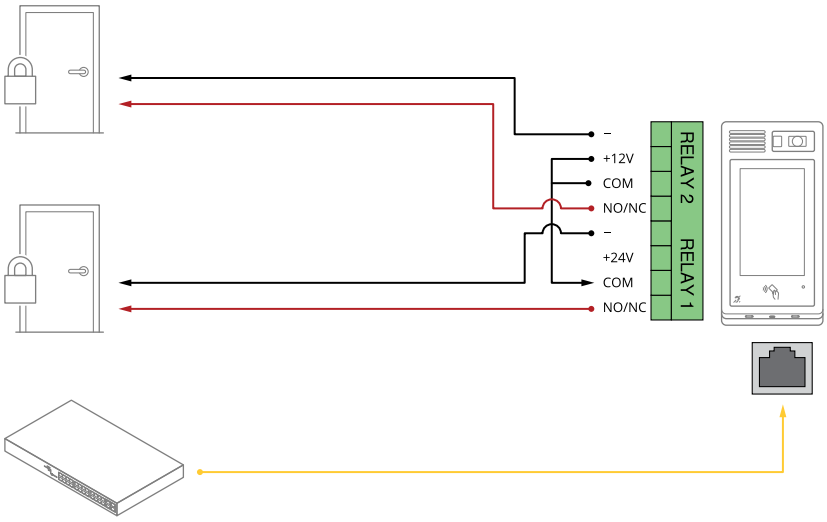
Conectar los equipos

Un relé alimentado por PoE (12 V)



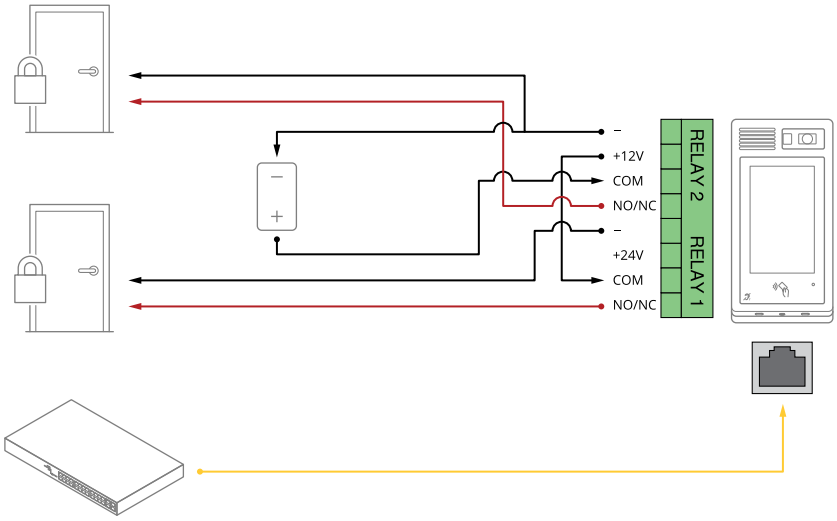
1. Para comprobar el estado del relé, vaya a **System > Accessories (Sistema > Accesorios)** y encuentre el puerto de relé.
2. Establezca **Normal state (Estado normal)** en:
   -  para un bloqueo de seguridad negativa.
   -  para un bloqueo de seguridad positiva.

Dos relés alimentados por PoE (12 V)



1. Para comprobar el estado del relé, vaya a **System > Accessories (Sistema > Accesorios)** y encuentre el puerto de relé.
2. Establezca **Normal state (Estado normal)** en:
   -  para un bloqueo de seguridad negativa.
   -  para un bloqueo de seguridad positiva.

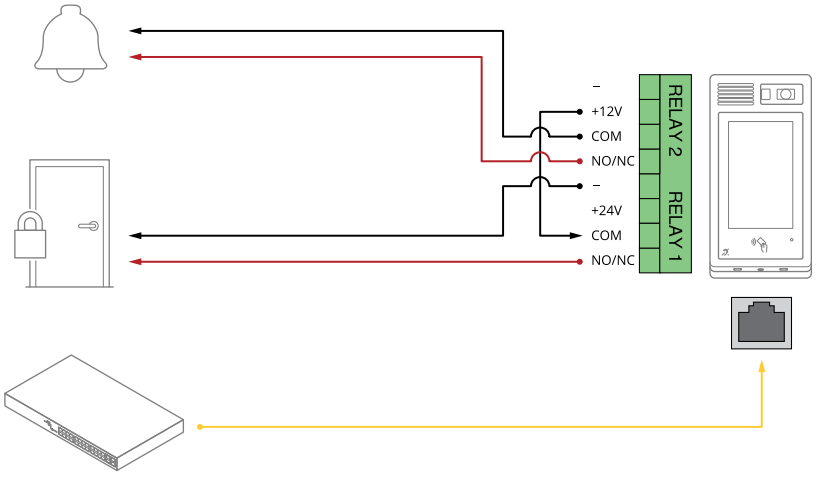
Un relé alimentado por PoE (12 V) + un relé alimentado por fuente de alimentación externa



1. Para comprobar el estado del relé, vaya a **System > Accessories (Sistema > Accesorios)** y encuentre el puerto de relé.
2. Establezca **Normal state (Estado normal)** en:
   -  para un bloqueo de seguridad negativa.
   -  para un bloqueo de seguridad positiva.

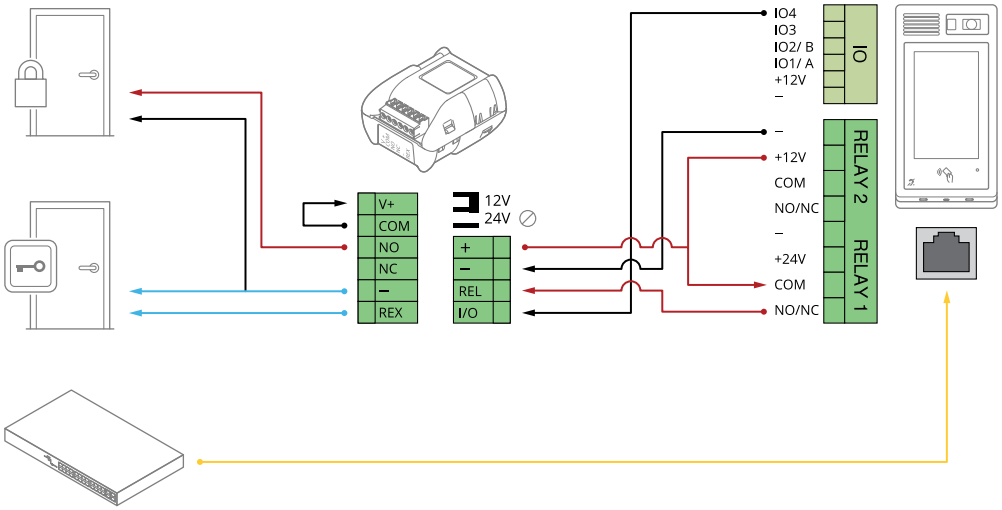
Un relé alimentado por PoE (12 V) + un contacto libre de potencial del relé

El contacto libre de potencial puede ser, por ejemplo, un timbre de puerta.



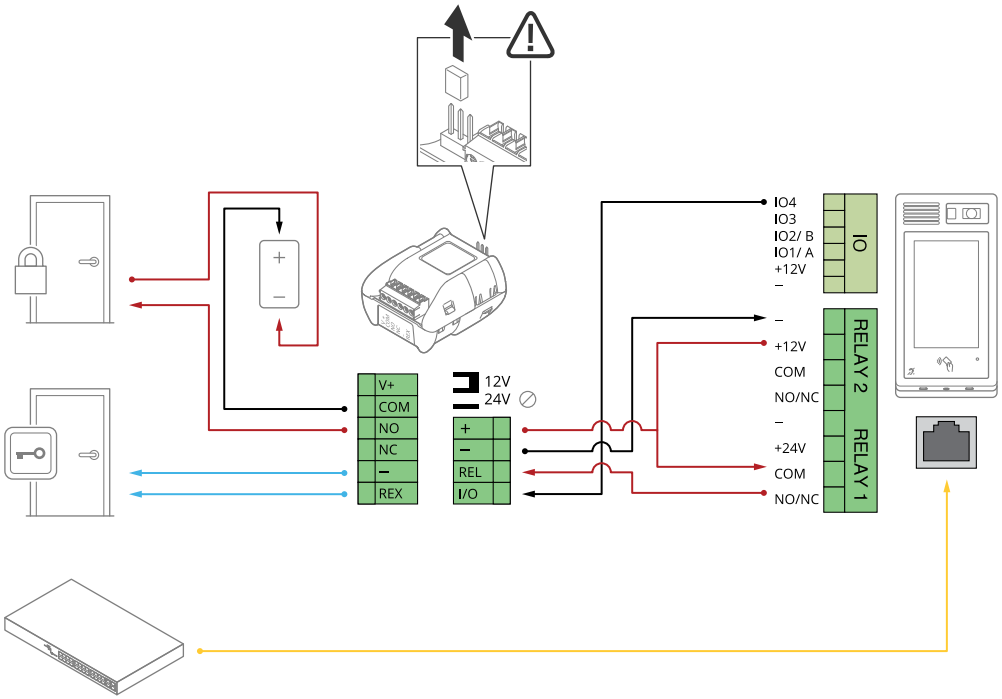
1. Para comprobar el estado del relé, vaya a **System > Accessories (Sistema > Accesorios)** y encuentre el puerto de relé.
2. Establezca **Normal state (Estado normal)** en:
   -  para un bloqueo de seguridad negativa.
   -  para un bloqueo de seguridad positiva.

Cerradura de seguridad negativa de 12 V alimentada mediante PoE+ desde el intercomunicador



1. Para comprobar el estado del relé, vaya a **System > Accessories (Sistema > Accesorios)** y encuentre el puerto de relé.
2. Establezca **Normal state (Estado normal)** en:
   - para un bloqueo de seguridad negativa.
   - para un bloqueo de seguridad positiva.

Cerradura de seguridad negativa alimentada por fuente de alimentación externa

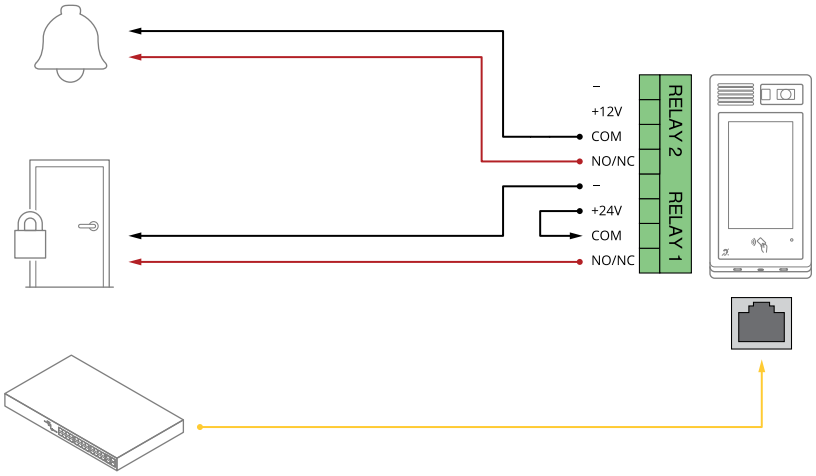


1. Para comprobar el estado del relé, vaya a **System > Accessories (Sistema > Accesorios)** y encuentre el puerto de relé.
2. Establezca **Normal state (Estado normal)** en:
   - para un bloqueo de seguridad negativa.

–  para un bloqueo de seguridad positiva.

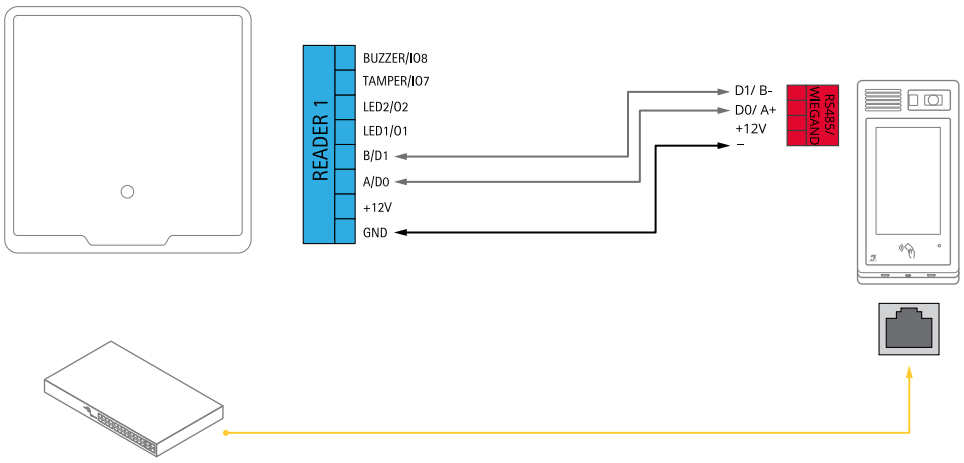
Un relé alimentado por PoE (24 V) + un contacto libre de potencial del relé

El contacto libre de potencial puede ser, por ejemplo, un timbre de puerta.



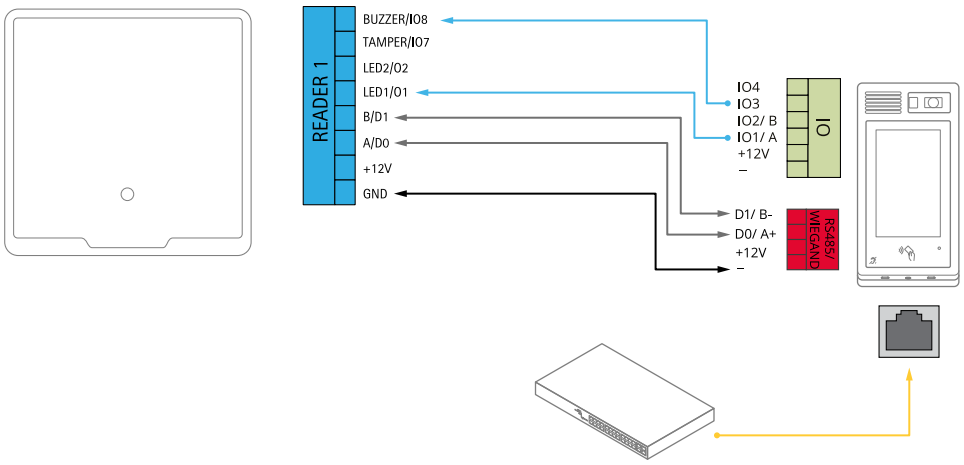
1. Para comprobar el estado del relé, vaya a **System > Accessories (Sistema > Accesorios)** y encuentre el puerto de relé.
2. Establezca **Normal state (Estado normal)** en:
   –  para un bloqueo de seguridad negativa.
   –  para un bloqueo de seguridad positiva.

Lector conectado al controlador de puerta mediante OSDP



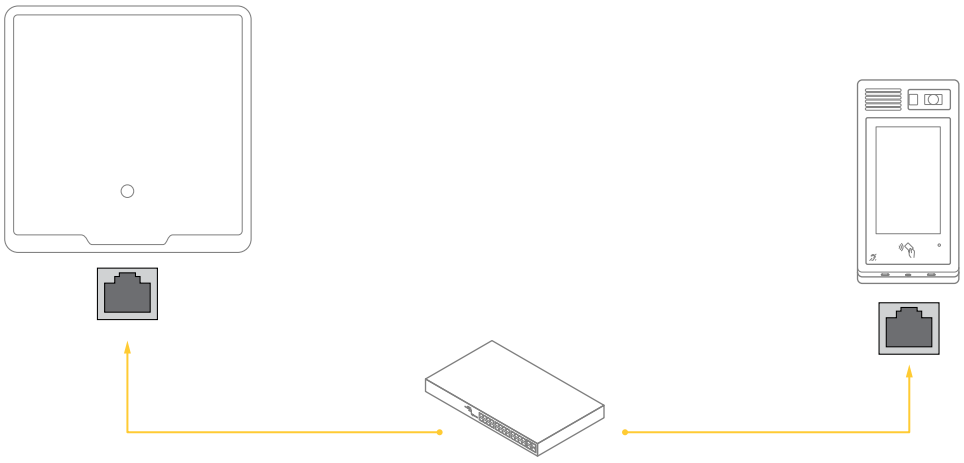
1. Vaya a **Reader (Lector) > Connection (Conexión) > Reader protocol (Protocolo de lector)**.
2. Ajuste el **Reader protocol type (Tipo de protocolo de lector)** a **OSDP** y haga clic en **Save (Guardar)**.

Lector conectado al controlador de puerta mediante Wiegand



1. Vaya a **Reader (Lector) > Connection (Conexión) > Reader protocol (Protocolo de lector)**.
2. Ajuste el **Reader protocol type (Tipo de protocolo de lector)** a **Wiegand**.
3. Active **Beeper**.
4. En **Input for beeper (Entrada para el avisador acústico)**, seleccione **I3**.
5. En **Input used for LED control (Entrada utilizada para el control LED)**, seleccione **1**.
6. En **Input for LED1 (Entrada para LED1)**, seleccione **I1**.
7. Ajuste otros parámetros y haga clic en **Save (Guardar)**.

Lector conectado al controlador de puerta Axis mediante lector VAPIX



1. Vaya a **Reader (Lector) > Connection (Conexión) > Reader protocol (Protocolo de lector)**.
2. Ajuste el **Reader protocol type (Tipo de protocolo de lector)** a **VAPIX reader (Lector VAPIX)**.
3. Conectar a un controlador de puerta 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 19*.
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 30*.

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 6*.

No se puede acceder externamente al dispositivo.

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

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

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

Problemas con 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*.

Consideraciones sobre rendimiento

A la hora de configurar su sistema, es importante considerar de qué modo afectan al rendimiento los diferentes ajustes y situaciones. Algunos factores afectan al ancho de banda (velocidad de bits), otros afectan a la velocidad de fotogramas y otros, a ambos.

Los factores más importantes a tener en cuenta son:

- La resolución de imagen alta o los niveles bajos de compresión hacen que las imágenes contengan mayor cantidad de datos, lo que afecta, a su vez, al ancho de banda.
- El acceso por parte de un gran número de clientes Motion JPEG o unicast H.264/H.265/AV1 afecta al ancho de banda.
- La visualización simultánea de distintas transmisiones (resolución, compresión) por parte de distintos clientes afecta tanto a la velocidad de fotogramas como al ancho de banda.
  Utilice transmisiones idénticas cuando sea posible para mantener una velocidad de imagen alta. Se pueden utilizar perfiles de transmisión para asegurar que las transmisiones sean idénticas.
- El acceso a transmisiones de vídeo con distintos códecs afecta simultáneamente a la velocidad de fotogramas y al ancho de banda. Para un rendimiento óptimo, utilice flujos con el mismo códec.
- El uso de numerosas configuraciones de eventos afecta a la carga de la CPU del producto, lo que a su vez afecta a la velocidad de imagen.
- El uso de HTTPS podría reducir la velocidad de imagen, especialmente en las transmisiones Motion JPEG.
- Un uso denso de la red debido a una infraestructura deficiente afecta al ancho de banda.
- La visualización en ordenadores cliente de bajo rendimiento disminuye la percepción del rendimiento y afecta a la velocidad de imagen.

- La ejecución simultánea de varias aplicaciones de la plataforma de aplicaciones para cámaras AXIS (ACAP) puede afectar a la velocidad de fotogramas y al rendimiento en general.

Contactar con la asistencia técnica

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

Información de seguridad

Niveles de peligro

⚠ PELIGRO
Indica una situación peligrosa que, si no se evita, provocará lesiones graves o la muerte.

⚠ ADVERTENCIA
Indica una situación peligrosa que, si no se evita, puede provocar lesiones graves o la muerte.

⚠ PRECAUCIÓN
Indica una situación peligrosa que, si no se evita, puede provocar lesiones moderadas o leves.

AVISO
Indica una situación peligrosa que, si no se evita, puede provocar daños materiales.

Otros niveles de mensaje

Importante
Indica información importante que es fundamental para que el producto funcione correctamente.

Nota
Indica información útil que ayuda a aprovechar el producto al máximo.

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.

T10213214_es

2026-10 (M12.2)

© 2025 – 2026 Axis Communications AB