Videoportero en red AXIS A8207-VE Mk II

Manual del usuario

Índice

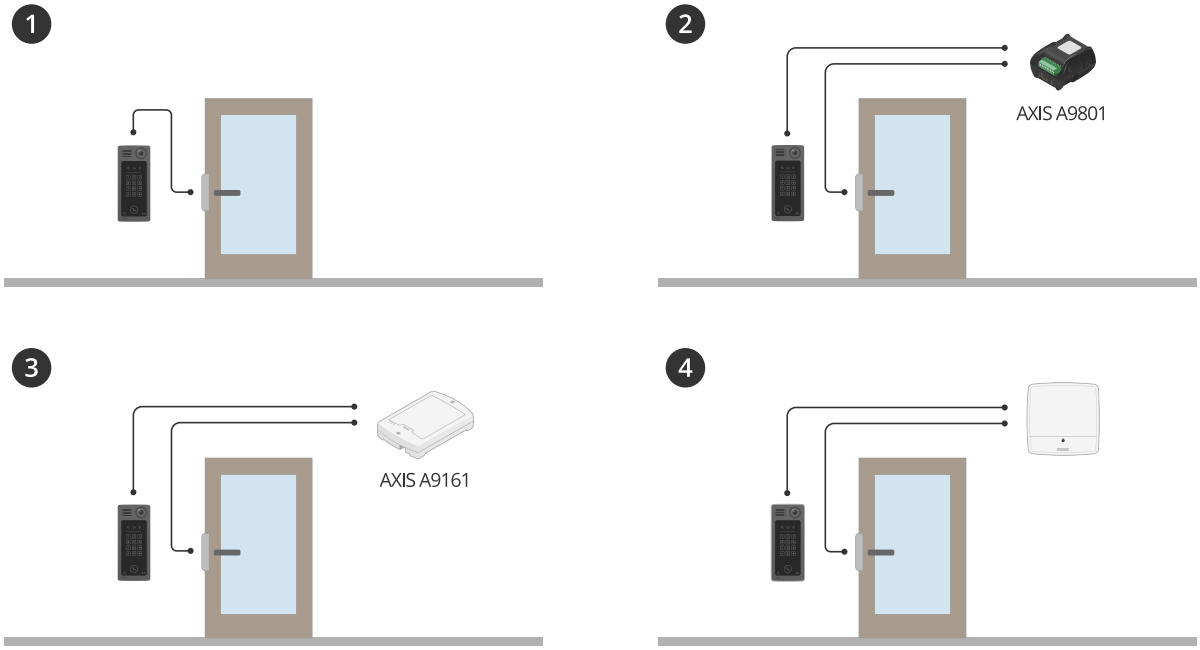
Presentación esquemática de la solución 4
Guía de productos 5
Instalación 7
Cómo funciona 8
- Localice el dispositivo en la red 8
  - Compatibilidad con navegadores 8
- Abrir la interfaz web del dispositivo 8
- Crear una cuenta de administrador 8
- Contraseñas seguras 9
- Asegúrese de que nadie ha manipulado el software del dispositivo 9
- Información general de la interfaz web 9

Configuración adicional 10
- Cambiar la contraseña root 10
- Configurar SIP directo (P2P) 10
- Configurar SIP a través de un servidor (PBX) 11
- Crear un contacto 11
- Configurar el botón de llamada 12
- Configurar como lector de tarjetas: conexión de red 12
- Configurar como lector de tarjetas: conexión con cable 12
- Utilizar datos protegidos en tarjetas para aumentar la seguridad 13
- Usar DTMF para desbloquear la puerta de un visitante 13
- Transmisión de vídeo en directo a un monitor 14
- Permitir que los propietarios de la credencial abran la puerta 14

Interfaz web 16
- Estado 16
- Vídeo 18
  - Instalación 20
  - Imagen 20
  - Flujo 26
  - Superposiciones 29
  - Máscaras de privacidad 31
- Comunicación 31
  - Lista de contactos 31
  - SIP 33
  - Llamadas 38
  - Llamadas VMS 39
- Analítica 39
  - Configuración de metadatos 39
- Lector 40
  - Conexión 40
  - Formato de salida 41
  - Tipos de chip 41
  - Número de identificación personal (PIN) 42
  - Lista de entrada 42
- Audio 43
  - Configuración del dispositivo 43
  - Flujo 44
  - Clips de audio 45
- Grabaciones 45
- Aplicaciones 46
- Sistema 47
  - Hora y ubicación 47
  - Comprobación de configuración 48

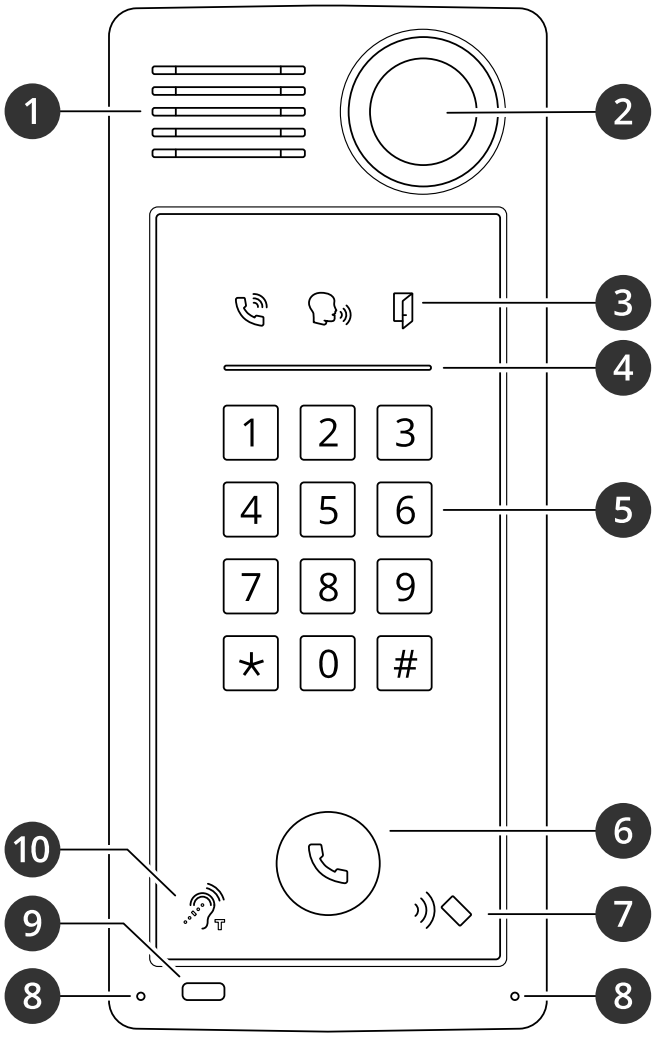
Red 48
Seguridad 53
Cuentas 57
Eventos 59
MQTT 64
Almacenamiento 67
Perfiles de transmisión 69
ONVIF 70
Detectores 73
Salida de vídeo 73
Accesorios 75
Registros 75
Configuración sencilla 76
Mantenimiento 77
Mantenimiento 77
solucionar problemas 78
Descubrir más 79
Voz por IP (VoIP) 79
Protocolo de inicio de sesión (SIP) 79
Peer-to-peer SIP (SIP de punto a punto): 79
Centralita telefónica privada (PBX) 80
Configurar reglas para eventos 81
Aplicaciones 81
Uso diario 82
Utilizar el teclado 82
Localización de problemas 83
Restablecimiento a la configuración predeterminada de fábrica 83
Comprobar la versión de AXIS OS 83
Actualización de AXIS OS 83
Problemas técnicos, consejos y soluciones 84
Consideraciones sobre el rendimiento 85
Especificaciones 86
Controles e indicadores del panel delantero 86
Iconos de indicador 86
Banda del indicador del lector de tarjetas 86
Botón de llamada 86
Indicadores LED 86
Ranura para tarjeta SD 86
Botones 86
Botón de control 86
Conectores 87
Conector HDMI 87
Conector de red 87
Conector de audio 87
Conector de relé 87
Conector de lector 88
Conector de E/S 88
Conector de alimentación 89
Información de seguridad 90
Niveles de peligro 90
Otros niveles de mensaje 90

Presentación esquemática de la solución

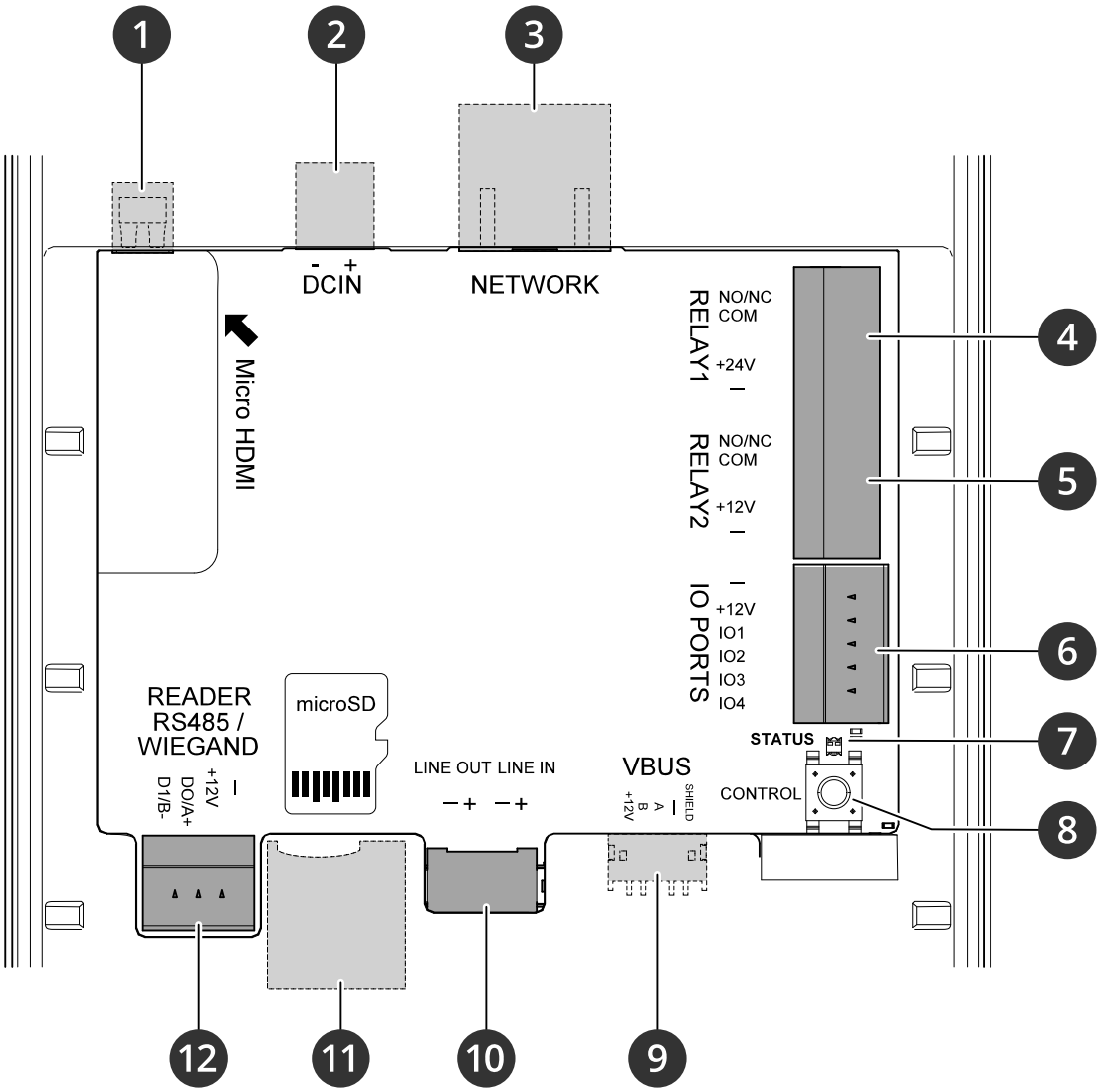


1 *Terminal de puerta*
2 *Videoportero combinado con AXIS A9801*
3 *Videoportero combinado con AXIS A9161*
4 *Videoportero combinado con un sistema de control de accesos; por ejemplo, AXIS A1001 o AXIS A1601*

Guía de productos

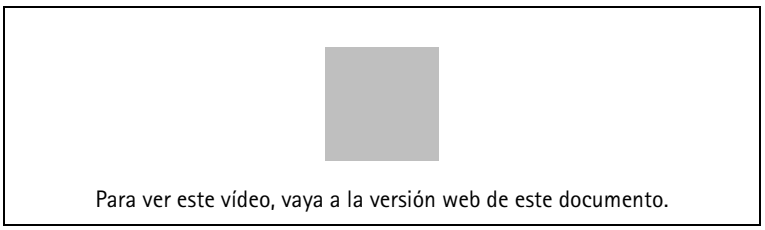


1 *Altavoz*
2 *Cámara*
3
4
5 *Teclado numérico*
6
7 *Icono de lector de tarjeta*
8 *Micrófono*
9 *Sensor PIR*
10 *Icono T-coil*



1 (microHDMI)
2
3 (PoE+)
4
5
6
7 LED de estado
8
9 2N VBUS (no en uso)
10
11 (microSD/microSDHC/microSDXC)
12

Instalación



Vídeo de instalación para el lector A8207-VE.

Vídeo de instalación para el relé A8207-VE.

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

*Para utilizar la interfaz web AXIS OS con iOS 15 o iPadOS 15, vaya a
Settings > Safari > Advanced > Experimental Features (Configuración > Safari > Avanzada > Funciones experimentales) y desactive NSURLSession Websocket.

Abrir la interfaz web del dispositivo

1. Abra un navegador y escriba la dirección IP o el nombre de host del dispositivo Axis.
   Si no conoce la dirección IP, use AXIS IP Utility o AXIS Device Manager para localizar el dispositivo en la red.
2. Escriba el nombre de usuario y la contraseña. Si accede al dispositivo por primera vez, debe crear una cuenta de administrador. Vea .

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

Crear una cuenta de administrador

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

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

Importante

El dispositivo no tiene una cuenta predeterminada. Si pierde la contraseña de la cuenta de administrador, debe restablecer el dispositivo. Vea .

Contraseñas seguras

Importante

Los dispositivos de Axis envían la contraseña definida inicialmente en texto abierto a través de la red. Para proteger su dispositivo tras el primer inicio de sesión, configure una conexión HTTPS segura y cifrada y, a continuación, cambie la contraseña.

La contraseña del dispositivo es la principal protección para sus datos y servicios. Los dispositivos de Axis no imponen una política de contraseñas ya que pueden utilizarse en distintos tipos de instalaciones.

Para proteger sus datos le recomendamos encarecidamente que:

- Utilice una contraseña con al menos 8 caracteres, creada preferiblemente con un generador de contraseñas.
- No exponga la contraseña.
- Cambie la contraseña a intervalos periódicos y al menos una vez al año.

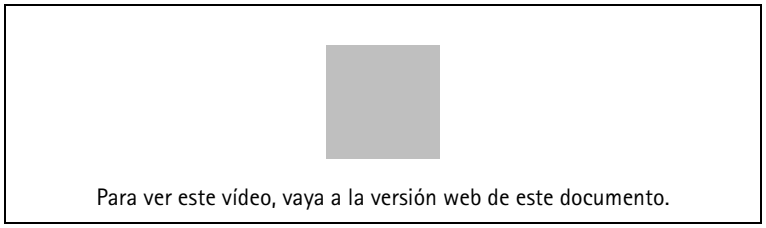
Asegúrese de que nadie ha manipulado el software del dispositivo

Para asegurarse de que el dispositivo tiene el AXIS OS original o para volver a controlar el dispositivo tras un incidente de seguridad:

1. Restablezca la configuración predeterminada de fábrica. Vea .
   Después de un restablecimiento, el inicio seguro garantiza el estado del dispositivo.
2. Configure e instale el dispositivo.

Información general de la interfaz web

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



Interfaz web del dispositivo Axis

Configuración adicional

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.

Cambiar la contraseña root

1. Inicie sesión en la interfaz del dispositivo y vaya a **Sistema > Usuarios**.
2. Para el usuario raíz, haga clic en ⋮ **> Update user (Actualizar usuario)**.
3. Introduzca una nueva contraseña y haga clic en Save (Guardar).

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, vea .

En este dispositivo, VoIP se habilita a través del protocolo SIP. Para obtener más información sobre SIP, consulte

Existen dos tipos de configuración para SIP: directa o de igual a igual (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 información sobre cómo realizar la configuración, consulte .

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 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 vea .

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, vea .

En este dispositivo, VoIP se habilita a través del protocolo SIP. Para obtener más información sobre SIP, consulte

Existen dos tipos de configuraciones para SIP. Una de ellas es un servidor PBX. 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, vea .

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 . 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 .

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)**.

Configurar el botón de llamada

De forma predeterminada, el botón de llamada está configurado para hacer llamadas de VMS (software de gestión de vídeo). Si desea conservar esta configuración, solo tiene que añadir el intercomunicador en red de Axis al VMS.

Este ejemplo explica cómo configurar el sistema para llamar a un contacto de la lista de contactos cuando un visitante pulsa el botón de llamada.

1. Vaya a **Communication > Calls > Call button (Comunicación > Llamadas > Botón Llamada)**.
2. En **Recipients (Destinatarios)**, elimine **VMS**.
3. En **Recipients (Destinatarios)**, seleccione un contacto existente o cree uno nuevo.

Para desactivar el botón de llamada, apague **Enable call button (Habilitar botón de llamada)**.

Configurar como lector de tarjetas: conexión de red

Para utilizar el videoportero como lector de tarjetas, debe 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. Vea .

Configurar el videoportero de puerta 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)**.

Configurar como lector de tarjetas: conexión con cable

Para utilizar el videoportero como lector de tarjetas, debe 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 videoportero a un controlador de puerta.
  Consulte los esquemas de cableado eléctrico, que puede descargar de *axis.com/products/axis-a8207-ve-mk-ii/support*.
- 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 videoportero de puerta 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 desbloquear la puerta de un visitante

Cuando un visitante realiza una llamada desde el videoportero, la persona que responde puede utilizar la señalización multifrecuencia de doble tono (DTMF) de su dispositivo SIP para desbloquear la puerta. El controlador de puerta desbloquea y bloquea la puerta.

En este ejemplo se explica cómo:

- definir la señal DTMF en el videoportero

- configurar el videoportero para:
  - pedir al controlador de puerta que desbloquee la puerta, **o bien**
  - desbloquear la puerta mediante el relé interno.

Puede configurar todos los ajustes en la página web del videoportero.

Antes de empezar

- Permitir llamadas SIP desde el dispositivo y crear una cuenta SIP. Vea y .

Definir la señal DTMF en el videoportero

1. Vaya a **Communication (Comunicación) > SIP > DTMF**.
2. Haga clic en **+ Add sequence (Agregar secuencia)**.
3. En **Sequence (Secuencia)**, introduzca 1.
4. En **Description (Descripción)**, introduzca Unlock door (Desbloquear puerta).
5. En **Accounts (Cuentas)**, seleccione la cuenta SIP.
6. Haga clic en **Save (Guardar)**.

Configurar el videoportero para desbloquear la puerta mediante el relé interno

7. Vaya a **System > Events > Rules (Sistema > Eventos > Reglas)** y añada una regla.
8. En el campo **Name (Nombre)**, introduzca DTMF unlock door (Desbloquear puerta por DTMF).
9. En la lista de condiciones, en el apartado **Call (Llamada)**, seleccione **DTMF** y **Unlock door (Desbloquear puerta)**.
10. En la lista de acciones, en **E/S**, seleccione **Toggle I/O once (Alternar E/S una vez)**.
11. En la lista de puertos, seleccione **Relay 1 (Relé 1)**.
12. Cambie **Duration (Duración)** a 00:00:07, lo que significa que la puerta está abierta durante 7 segundos.
13. Haga clic en **Save (Guardar)**.

Transmisión de vídeo en directo a un monitor

El dispositivo puede transmitir vídeo en directo a un monitor HDMI sin conexión de red. Utilice el monitor para ver quién está en la puerta.

1. Conecte un monitor externo al conector HDMI.
2. Ajuste la configuración de HDMI en **Sistema > Salida de vídeo**.

Permitir que los propietarios de la credencial abran la puerta

Con la lista de entradas, puede hacer posible que los titulares de las credenciales utilicen su tarjeta o PIN 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

- 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)**.

Interfaz web

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

Nota

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

Mostrar u ocultar el menú principal.

Acceda a las notas de la versión.

Acceder a la ayuda del producto.

Cambiar el idioma.

Definir un tema claro o un tema oscuro.

El menú de usuario contiene:

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

El menú contextual contiene:

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

Estado

Información sobre el dispositivo

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

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

Estado de sincronización de hora

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

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

Seguridad

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

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

Clientes conectados

Muestra el número de conexiones y clientes conectados.

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

Grabaciones en curso

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

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

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

Vídeo

Haga clic para reproducir el flujo de vídeo en directo.

Haga clic para congelar el flujo de vídeo en directo.

Haga clic para tomar una instantánea del flujo de vídeo en directo. El archivo se guarda en la carpeta "Descargas" de su equipo. El nombre del archivo de imagen será [snapshot_YYYY_MM_DD_HH_MM_SS.jpg]. El tamaño de la instantánea depende de la compresión que aplique el buscador web en el que se recibe la instantánea. En consecuencia, el tamaño puede no corresponder al del ajuste de compresión definido en el dispositivo.

Haga clic para mostrar puertos de salida de E/S. Utilice el switch para abrir o cerrar el circuito de un puerto, por ejemplo, para probar seguridad positiva.

Haga clic para encender o apagar la iluminación de IR.

Haga clic para encender o apagar la luz blanca.

Haga clic para acceder a los controles en pantalla:

- **Predefined controls (Controles predefinidos)**: Active esta opción para utilizar los controles disponibles en pantalla.
- **Custom controls (Controles personalizados)**: Haga clic en **Add custom control (Agregar control personalizado)** para agregar un control a la pantalla.

Inicia el limpiador. Cuando se inicia la secuencia, la cámara se mueve a la posición configurada para recibir el pulverizador de lavado. Cuando se completa toda la secuencia de lavado, la cámara vuelve a su posición anterior. Este icono solo está visible cuando el limpiador está conectado y configurado.

Inicia la escobilla limpiadora.

Haga clic y seleccione una posición predefinida para ir a esa posición predefinida en la visualización en directo. O bien, haga clic en **Setup (Configuración)** para ir a la página de posición predefinida.

Agrega o elimina un área de recuerdo de enfoque. Cuando añade una zona de recuerdo de enfoque, la cámara guarda los ajustes de enfoque en ese rango específico de panorámica/inclinación. Cuando haya configurado una zona de recuerdo de enfoque y la cámara entre en dicha dona en la visualización en directo, la cámara recordará el enfoque guardado anteriormente. Será suficiente cubrir la mitad del área para que la cámara recuerde el enfoque.

Haga clic para seleccionar una ronda de vigilancia y, a continuación, haga clic en **Start (Iniciar)** para reproducir la ronda de vigilancia. O bien, haga clic en **Setup (Configuración)** para ir a la página de rondas de vigilancia.

Haga clic para encender manualmente el calefactor durante un periodo de tiempo seleccionado.

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

Haga clic para mostrar el almacenamiento configurado para el dispositivo. Debe haber iniciado sesión como administrador para configurar el almacenamiento.

Haga clic para acceder a más ajustes:

- **Formato de vídeo**: Seleccione el formato de codificación que se utilizará en la visualización en directo.
- **Reproducción automática**: Active la reproducción automática de un flujo de vídeo silenciado siempre que abra el dispositivo en una nueva sesión.
- **Información de transmisión del cliente**: Active esta función para mostrar información dinámica sobre el flujo de vídeo que utiliza el navegador que muestra el flujo de vídeo en directo. La información de velocidad de bits difiere de la información que se muestra en una superposición de texto, debido a las distintas fuentes de información. La velocidad de bits de la información de flujo del cliente es la velocidad de bits del último segundo y procede del controlador de codificación del dispositivo. La velocidad de bits de la superposición es la velocidad de bits media de los últimos 5 segundos, que procede del navegador. Ambos valores cubren solo el flujo de vídeo sin formato y no el ancho de banda adicional generado al transmitirse a través de la red a través de UDP/TCP/HTTP.
- **Transmisión adaptativa**: Active esta función para adaptar la resolución de imagen a la resolución de visualización real del cliente de visualización, para mejorar la experiencia del usuario y evitar una posible sobrecarga del hardware del cliente. El flujo adaptativo solo se aplica cuando visualiza el flujo de vídeo en directo en la interfaz web en un navegador. Cuando la transmisión adaptativa está activada, la velocidad de fotogramas máxima es de 30 imágenes por segundo. Si toma una instantánea mientras el flujo adaptativo está activado, utilizará la resolución de imagen seleccionada por la transmisión adaptativa.
- **Cuadrícula de nivel**: Haga clic en para mostrar la cuadrícula de nivel. La cuadrícula le ayuda a decidir si la imagen está alineada horizontalmente. Haga clic en para ocultarlo.
- **Pixel counter (Contador de píxeles)**: haga clic en para mostrar el contador de píxeles. Arrastre y cambie el tamaño del recuadro que contiene su área de interés. También puede definir el tamaño de píxel del recuadro en los campos **Width (Anchura)** y **Height (Altura)**.
- **Refresh (Actualizar)**: haga clic en para actualizar la imagen estática de la visualización en directo.
- **Controles PTZ** : Active esta función para mostrar los controles PTZ en la visualización en directo.

Haga clic para mostrar la visualización en directo a resolución completa. Si la resolución completa es superior al tamaño de la pantalla, utilice la imagen más pequeña para navegar en la imagen.

Haga clic para mostrar el flujo de vídeo en directo en pantalla completa. Presione ESC para salir del modo de pantalla completa.

Instalación

Capture mode (Modo de captura) : un modo de captura es una configuración predefinida que define cómo captura las imágenes la cámara. Si cambia el modo de captura, puede afectar a muchos otros ajustes, como áreas de visión y máscaras de privacidad.

Mounting position (Posición de montaje) : la orientación de la imagen puede cambiar en función de cómo monte la cámara.

Frecuencia de la red eléctrica: para minimizar el parpadeo de la imagen, seleccione la frecuencia que utiliza la región. En las regiones americanas, suele ser 60 Hz y en el resto del mundo, suele ser 50 Hz. Si no está seguro de cuál es la frecuencia de la red eléctrica de su región, póngase en contacto con las autoridades locales.

Imagen

Aspecto

Perfil de escena : Seleccione un perfil de escena que se ajuste a su escenario de vigilancia. Un perfil de escena optimiza los ajustes de la imagen, incluidos el nivel de color, el brillo, la nitidez, el contraste y el contraste local, para un entorno o propósito específico.

- **Forense** : Adecuado para fines de vigilancia.
- **Interiores** : Apto para entornos de interior.
- **Exteriores** : Apto para entornos de exterior.
- **Vívido** : Útil para fines de demostración.
- **Información general del tráfico** : Adecuado para la supervisión del tráfico de vehículos.
- **Matrícula** : Adecuado para capturar matrículas.

Saturation (Saturación): Utilice el control deslizante para ajustar la intensidad del color. Puede obtener, por ejemplo, una imagen en escala de grises.

Contrast (Contraste): Utilice el control deslizante para ajustar la diferencia entre las áreas de luz y de oscuridad.

Brightness (Brillo): Utilice el control deslizante para ajustar la intensidad de la luz. Esto puede hacer que los objetos sean más fáciles de ver. El brillo se aplica después de capturar la imagen y no afecta a la información de la imagen. Para obtener más detalles de una zona oscura, normalmente es mejor aumentar la ganancia o el tiempo de exposición.

Sharpness (Nitidez): Utilice el control deslizante para que los objetos en la imagen aparezcan con mayor nitidez mediante el ajuste del contraste de los bordes. Si aumenta la nitidez, podría aumentar la velocidad de bits y la cantidad de espacio de almacenamiento necesaria también.

Wide Dynamic Range

WDR : Active para que se vean las áreas brillantes y oscuras de la imagen.

Contraste local : Utilice el control deslizante para ajustar el contraste de la imagen. Cuanto mayor es el valor, mayor es el contraste entre las áreas oscuras y luminosas.

Mapeado de tonos : Utilice el control deslizante para ajustar la cantidad de mapeado de tonos que se aplica a la imagen. Si el valor es cero, solo se aplica la corrección gamma estándar, mientras que un valor más alto aumenta la visibilidad de las partes más oscuras y más brillantes de la imagen.

Balance de blancos

Si la cámara detecta la temperatura de color de la luz entrante, puede ajustar la imagen para hacer que los colores tengan un aspecto más natural. Si no es suficiente, puede seleccionar una fuente de luz adecuada de la lista.

El ajuste de balance de blancos automático se adapta a los cambios gradualmente para reducir el riesgo de parpadeo de color. Si cambia la iluminación o cuando se pone en marcha por primera vez la cámara, pueden necesitarse hasta 30 segundos para la adaptación a la nueva fuente de luz. Si en una escena hay varios tipos de fuentes de luz, esto es, con diferente temperatura de color, para el algoritmo de balance de blancos automático se toma como referencia la fuente de luz dominante. Para ignorar este comportamiento se puede seleccionar un ajuste de balance de blancos fijo que corrija la fuente de luz que desea utilizar como referencia.

Entorno de luz:

- **Automático**: Compensación e identificación automáticas del color de la fuente de luz. Es el ajuste recomendado y se puede utilizar en la mayoría de las situaciones.
- **Automático: exterior** : Compensación e identificación automáticas del color de la fuente de luz. Es el ajuste recomendado y se puede utilizar en la mayoría de las situaciones en exteriores.
- **Interior personalizado** : Ajuste de color fijo para habitaciones con luz artificial que no sea luz fluorescente e idóneo para una temperatura de color normal, de alrededor de 2800 K.
- **Exterior personalizado** : Ajuste de color fijo para ambientes soleados con una temperatura de color de alrededor de 5500 K.
- **Fijo: fluorescente 1**: Ajuste de color fijo para iluminación fluorescente con una temperatura de color de alrededor de 4000 K.
- **Fijo: fluorescente 2**: Ajuste de color fijo para iluminación fluorescente con una temperatura de color de alrededor de 3000 K.
- **Fijo: interior**: Ajuste de color fijo para habitaciones con luz artificial que no sea luz fluorescente e idóneo para una temperatura de color normal, de alrededor de 2800 K.
- **Fijo: exterior 1**: Ajuste de color fijo para ambientes soleados con una temperatura de color de alrededor de 5500 K.
- **Fijo: exterior 2**: Ajuste de color fijo para ambientes nublados con una temperatura de color de alrededor de 6500 K.
- **Farola: mercurio** : Ajuste de color fijo para emisión ultravioleta de las luces de vapor de mercurio habituales en el alumbrado vial.
- **Farola: sodio** : Ajuste de color fijo que compensa el naranja amarillento de las luces de vapor de sodio habituales en la iluminación callejera.
- **Mantener la corriente**: Mantenga los ajustes actuales y no compense los cambios de luz.
- **Manual** : Fije el balance de blancos mediante un objeto blanco. Arrastre el círculo a un objeto que la cámara deba interpretar como blanco en la imagen de visualización en directo. Utilice los controles deslizantes **Red balance (Balance de rojo)** y **Blue balance (Balance de azul)** para ajustar manualmente el balance de blancos.

Exposición

Seleccione un modo de exposición para reducir rápidamente los efectos irregulares cambiantes de la imagen; por ejemplo, el parpadeo generado por distintos tipos de fuentes de luz. Le recomendamos que utilice el modo de exposición automática o la misma frecuencia que la red de alimentación.

Modo de exposición:

- **Automático**: La cámara ajusta la abertura, la ganancia y el obturador automáticamente.
- **Apertura automática** : La cámara ajusta la apertura y la ganancia automáticamente. El obturador está fijo.
- **Obturador automático** : La cámara ajusta el obturador y la ganancia automáticamente. La apertura está fija.
- **Mantener la corriente**: Fija los ajustes de exposición actuales.
- **Sin parpadeo** : La cámara ajusta la apertura y la ganancia automáticamente, y utiliza solo las siguientes velocidades de obturación: 1/50 s (50 Hz) y 1/60 s (60 Hz).
- **Sin parpadeo 50 Hz** : La cámara ajusta la apertura y la ganancia automáticamente, y utiliza la velocidad de obturación de 1/50 s.
- **Sin parpadeo 60 Hz** : La cámara ajusta la apertura y la ganancia automáticamente, y utiliza la velocidad de obturación de 1/60 s.
- **Parpadeo reducido** : Esto es lo mismo que sin parpadeo, pero en este caso la cámara podría usar cualquier velocidad de obturación más rápida que 1/100 s (50 Hz) y 1/120 s (60 Hz) para escenas más luminosas.
- **Parpadeo reducido 50 Hz** : Esto es lo mismo que sin parpadeo, pero en este caso la cámara podría usar cualquier velocidad de obturación más rápida que 1/100 s para escenas más luminosas.
- **Parpadeo reducido 60 Hz** : Esto es lo mismo que sin parpadeo, pero en este caso la cámara podría usar cualquier velocidad de obturación más rápida que 1/120 s para escenas más luminosas.
- **Manual** : La abertura, la ganancia y el obturador están fijos.

Zona de exposición : Utilice las zonas de exposición para optimizar la exposición en una parte de la escena seleccionada, por ejemplo, el área delante de una puerta de entrada.

Nota

Las zonas de exposición están relacionadas con la imagen original (sin girar) y los nombres de las zonas se refieren a esa imagen. Por ejemplo, esto significa que, si el flujo de vídeo tiene una rotación de 90°, la zona **superior** será la zona **derecha** en el flujo y la **izquierda** será la **inferior**.

- **Automático**: Adecuado para la mayoría de situaciones.
- **Centro**: Usa una zona fija en el centro de la imagen para calcular la exposición. El área tiene un tamaño y una posición fijos en la visualización en directo.
- **Completo** : Usa toda la visualización en directo para calcular la exposición.
- **Superior** : Usa una zona de un tamaño y una posición fijos en la parte superior de la imagen para calcular la exposición.
- **Inferior** : Usa una zona de un tamaño y una posición fijos en la parte inferior de la imagen para calcular la exposición.
- **Izquierda** : Usa una zona de un tamaño y una posición fijos en la parte izquierda de la imagen para calcular la exposición.

- **Derecha** : Usa una zona de un tamaño y una posición fijos en la parte derecha de la imagen para calcular la exposición.
- **Punto**: Usa una zona de un tamaño y una posición fijos en la visualización en directo para calcular la exposición.
- **Custom (Personalizado)**: Usa una zona de la visualización en directo para calcular la exposición. Puede ajustar el tamaño y la posición del área.

Obturador máximo: Seleccione la velocidad de obturación para ofrecer la mejor imagen posible. Las bajas velocidades de obturación (tiempo de exposición más prolongado) podrían provocar distorsión por movimiento ante cualquier movimiento y una velocidad de obturación demasiado alta podría afectar a la calidad de imagen. Este parámetro se utiliza junto con la ganancia máxima para mejorar la imagen.

Ganancia máxima: Seleccione la ganancia máxima adecuada. Si aumenta la ganancia máxima, mejora el nivel visible de detalle en las imágenes oscuras, aunque también aumenta el nivel de ruido. Más ruido también puede provocar un uso mayor del ancho de banda y del espacio de almacenamiento. Si establece la ganancia máxima en un valor alto, las imágenes pueden diferir mucho si las condiciones de luz varían en gran medida entre el día y la noche. Este parámetro se utiliza junto con el obturador máximo para mejorar la imagen.

Exposición adaptada al movimiento : Seleccione esta opción para reducir el desenfoque de movimiento en condiciones de poca luz.

Blur-noise trade-off (Compensación de desenfoque-ruido): Use el control deslizante para ajustar la prioridad entre distorsión por movimiento y ruido. Si desea priorizar el ancho de banda bajo y tener menos ruido a expensas de los detalles de los objetos en movimiento, mueva el control deslizante hacia **Bajo ruido**. Si desea priorizar la conservación de detalles de objetos en movimiento a expensas del ruido y el ancho de banda, mueva el control, deslizante hacia **Baja distorsión por movimiento**.

Nota

Puede cambiar la exposición mediante el ajuste del tiempo de exposición o la ganancia. Si aumenta el tiempo de exposición, se traduce en más distorsión por movimiento y, si aumenta la ganancia, se traduce en más ruido. Si ajusta la **compensación de desenfoque-ruido** hacia **Bajo ruido**, la exposición automática priorizará tiempos de exposición más largos sobre el aumento de ganancia y, lo contrario, si ajusta la compensación hacia **Distorsión por movimiento**. La ganancia y el tiempo de exposición terminarán alcanzando sus valores máximos en condiciones de poca luz, independientemente de la prioridad establecida.

Apertura de bloqueo : Active esta función para mantener el tamaño de apertura definido por el control deslizante **Apertura**. Apague para permitir que la cámara ajuste automáticamente el tamaño de apertura. Por ejemplo, puede bloquear la apertura para las escenas con condiciones de iluminación permanentes.

Abertura : Utilice el control deslizante para ajustar el tamaño de apertura, es decir, cuánta luz atraviesa el objetivo. Para permitir que entre más luz en el sensor y, de este modo, producir una imagen más luminosa en condiciones de poca luz, mueva el control deslizante hacia **Abierto**. Una apertura abierta también reduce la profundidad de campo, lo que implica que los objetos más cercanos o los más alejados de la cámara se pueden mostrar desenfocados. Para permitir que más imagen esté enfocada, mueva el control deslizante hacia **Cerrado**.

Nivel de exposición: Utilice el control deslizante para ajustar la exposición de imagen.

Anticondensación : Active para detectar los efectos de la niebla y elimínelos automáticamente para obtener una imagen más clara.

Nota

Recomendamos no activar **Desempañado** en escenas con bajo contraste, grandes variaciones de nivel de luz o cuando el enfoque automático esté ligeramente desactivado. Esto puede afectar a la calidad de imagen, por ejemplo, aumentando el contraste. Además, un exceso de luz puede afectar negativamente a la calidad de la imagen cuando el desempañado está activo.

Flujo

General

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

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

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

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

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

Zipstream

Zipstream es una tecnología de reducción de la velocidad de bits optimizada para la videovigilancia. Reduce la velocidad de bits media de una transmisión H.264 o H.265 en tiempo real. Axis Zipstream aplica una alta velocidad de bits en escenas con muchas regiones de interés, por ejemplo, en escenas con objetos en movimiento. Cuando la escena es más estática, Zipstream aplica una velocidad de bits inferior y por lo tanto reduce el almacenamiento requerido. Para obtener más información, consulte *Reducción de la velocidad de bits con Axis Zipstream*

Seleccione la **Strength (Potencia)** de reducción de velocidad de bits:

- **Apagado**: Sin reducción de la velocidad de bits.
- **Bajo**: Sin degradación visible de la calidad en la mayor parte de las escenas. Esta es la opción predeterminada y se puede utilizar en todo tipo de escenas para reducir la velocidad de bits.
- **Medio**: Efectos visibles en algunas escenas a través de menos ruido y un nivel de detalle levemente inferior en regiones de menor interés, por ejemplo, sin movimiento.
- **Alto**: Efectos visibles en algunas escenas a través de menos ruido y un nivel de detalle inferior en regiones de menor interés, por ejemplo, sin movimiento. Recomendamos este nivel para dispositivos conectados a la nube y dispositivos que utilizan almacenamiento local.
- **Más alto**: Efectos visibles en algunas escenas a través de menos ruido y un nivel de detalle inferior en regiones de menor interés, por ejemplo, sin movimiento.
- **Extremo**: Efectos visibles en la mayoría de las escenas. La velocidad de bits se ha optimizado para el menor almacenamiento posible.

Optimize for storage (Optimizar para almacenamiento): Active esta función para minimizar la velocidad de bits mientras se mantiene la calidad. La optimización no se aplica al flujo que se muestra en el cliente web. Solo se puede utilizar si VMS admite fotogramas B. Si activa **Optimize for storage (Optimizar para almacenamiento)**, también se activa **Dynamic GOP (GOP dinámico)**.

FPS dinámico (imágenes por segundo): Active esta opción para permitir que el ancho de banda varíe en función del nivel de actividad de la escena. Más actividad requiere más ancho de banda.

Lower limit (Límite inferior): Introduzca un valor para ajustar la velocidad de fotogramas entre el mínimo de imágenes por segundo y la transmisión predeterminada basada en el movimiento de la escena. Recomendamos que utilice un límite inferior en las escenas con muy poco movimiento, donde las imágenes por segundo podrían caer a 1 o menos.

Grupo de imágenes dinámico (GOP) (grupo de imágenes): Active esta función para ajustar dinámicamente el intervalo entre fotogramas I en función del nivel de actividad de la escena.

Upper limit (Límite superior): Introduzca una longitud de GOP máxima, es decir, el número máximo de fotogramas P entre dos fotogramas I. Un fotograma I es un fotograma de imagen independiente de otros fotogramas.

Control de velocidad de bits

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

Orientación

Duplicar: Actívela para reflejar la imagen.

Audio

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

Fuente : Seleccione la fuente de audio que desea utilizar.

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

Superposiciones

: Haga clic para agregar una superposición. Seleccione el tipo de superposición de la lista desplegable:

- **Texto**: Seleccione esta opción para mostrar un texto integrado en la imagen de visualización en directo y visible en todas las vistas, grabaciones e instantáneas. Puede introducir su propio texto e incluir también modificadores preconfigurados para que se muestren automáticamente, por ejemplo, la hora, la fecha y la velocidad de fotogramas.
  - : Haga clic para agregar el modificador de fecha `%F` para mostrarla en formato aaaa-mm-dd.
  - : Haga clic para agregar el modificador de hora `%X` para mostrarla en formato hh:mm:ss (reloj de 24 horas).
  - **Modificadores**: Haga clic para seleccionar los modificadores de la lista para agregarlos al cuadro de texto. Por ejemplo, el modificador `%a` muestra el día de la semana.
  - **Size (Tamaño)**: Seleccione el tamaño de fuente deseado.
  - **Appearance (Aspecto)**: Seleccione el color del texto y del fondo; por ejemplo, texto blanco sobre fondo negro (valor predeterminado).
  - : Seleccione la posición de la superposición en la imagen o haga clic en la superposición y arrástrela para moverla en la visualización en directo.
- **Imagen**: Seleccione esta opción para mostrar una imagen estática superpuesta sobre el flujo de vídeo. Puede utilizar los archivos .bmp, .png, .jpeg o .svg.
  Para cargar una imagen, haga clic en **Imágenes**. Antes de cargar una imagen, puede elegir:
  - **Escala con resolución**: Seleccione esta opción para escalar automáticamente la superposición de imagen de modo que se ajuste a la resolución de vídeo.
  - **Usar transparencia**: Seleccione e introduzca el valor hexadecimal RGB para ese color. Utilice el formato RRGGBB. Ejemplos de valores hexadecimales: FFFFFF para el blanco, 000000 para el negro, FF0000 para el rojo, 6633FF para el azul y 669900 para el verde. Solo para imágenes .bmp.
- **Scene annotation (Anotación de escena)** : Seleccione para mostrar una superposición de texto en la transmisión de vídeo que permanece en la misma posición, incluso cuando la cámara se desplaza o inclina en otra dirección. Puede optar por mostrar solo la superposición dentro de ciertos niveles de zoom.
  - : Haga clic para agregar el modificador de fecha `%F` para mostrarla en formato aaaa-mm-dd.
  - : Haga clic para agregar el modificador de hora `%X` para mostrarla en formato hh:mm:ss (reloj de 24 horas).
  - **Modificadores**: Haga clic para seleccionar los modificadores de la lista para agregarlos al cuadro de texto. Por ejemplo, el modificador `%a` muestra el día de la semana.
  - **Size (Tamaño)**: Seleccione el tamaño de fuente deseado.
  - **Appearance (Aspecto)**: Seleccione el color del texto y del fondo; por ejemplo, texto blanco sobre fondo negro (valor predeterminado).
  - : Seleccione la posición de la superposición en la imagen o haga clic en la superposición y arrástrela para moverla en la visualización en directo. La superposición se guarda y permanece en las coordenadas de giro e inclinación de esta posición.

- **Anotación entre niveles de zoom (%)**: Establezca los niveles de zoom en los que se mostrará la superposición.
- **Símbolo de anotación**: Seleccione un símbolo que aparezca en lugar de la superposición cuando la cámara no esté dentro de los niveles de zoom establecidos.

- **Streaming indicator (Indicador de transmisión)** : Seleccione esta opción para mostrar una animación superpuesta sobre el flujo de vídeo. La animación indica que el flujo de vídeo se realiza en directo, aunque la escena no contiene ningún movimiento.
  - **Appearance (Aspecto)**: Seleccione el color de la animación y del fondo; por ejemplo, animación roja sobre un fondo transparente (valor predeterminado).
  - **Size (Tamaño)**: Seleccione el tamaño de fuente deseado.
  - : Seleccione la posición de la superposición en la imagen o haga clic en la superposición y arrástrela para moverla en la visualización en directo.

- **Widget: Linegraph (Gráfico lineal)** : Muestre un gráfico que muestre cómo cambia un valor medido con el tiempo.
  - **Title (Título)**: introduzca un nombre para el widget.
  - **Modificador de superposición**: Seleccione un modificador de superposición como fuente de datos. Si ha creado superposiciones MQTT, se ubicarán al final de la lista.
  - : Seleccione la posición de la superposición en la imagen o haga clic en la superposición y arrástrela para moverla en la visualización en directo.
  - **Size (Tamaño)**: Seleccione el tamaño de la superposición.
  - **Visible en todos los canales**: Desactívelo para mostrar solo el canal seleccionado en la actualidad. Actívelo para mostrar en todos los canales activos.
  - **Actualizar intervalo**: Elija el tiempo entre actualizaciones de datos.
  - **Transparency (Transparencia)**: Establezca la transparencia de toda la superposición.
  - **Transparencia de fondo**: Establezca la transparencia solo del fondo de la superposición.
  - **Puntos**: Actívelo para agregar un punto a la línea del gráfico cuando se actualicen los datos.
  - Eje X
    - **Label (Etiqueta)**: Introduzca la etiqueta de texto para el eje x.
    - **Ventana de tiempo**: Introduzca el tiempo que se visualizarán los datos.
    - **Unidad de tiempo**: Introduzca una unidad de tiempo para el eje x.
  - Eje Y
    - **Label (Etiqueta)**: Introduzca la etiqueta de texto para el eje y.
    - **Escala dinámica**: Actívelo para que la escala se adapte automáticamente a los valores de los datos. Desactívelo para introducir valores manualmente para una escala fija.
    - **Umbral mínimo de alarma** y **Umbral máximo de alarma**: Estos valores agregarán líneas de referencia horizontales al gráfico, lo que facilitará ver cuando el valor de los datos sube o baja demasiado.

- **Widget: Meter (Medidor)** : Muestra un gráfico de barras que muestra el valor de datos medido más recientemente.
  - **Title (Título)**: introduzca un nombre para el widget.
  - **Modificador de superposición**: Seleccione un modificador de superposición como fuente de datos. Si ha creado superposiciones MQTT, se ubicarán al final de la lista.

- : Seleccione la posición de la superposición en la imagen o haga clic en la superposición y arrástrela para moverla en la visualización en directo.
- **Size (Tamaño)**: Seleccione el tamaño de la superposición.
- **Visible en todos los canales**: Desactívelo para mostrar solo el canal seleccionado en la actualidad. Actívelo para mostrar en todos los canales activos.
- **Actualizar intervalo**: Elija el tiempo entre actualizaciones de datos.
- **Transparency (Transparencia)**: Establezca la transparencia de toda la superposición.
- **Transparencia de fondo**: Establezca la transparencia solo del fondo de la superposición.
- **Puntos**: Actívelo para agregar un punto a la línea del gráfico cuando se actualicen los datos.
- Eje Y
  - **Label (Etiqueta)**: Introduzca la etiqueta de texto para el eje y.
  - **Escala dinámica**: Actívelo para que la escala se adapte automáticamente a los valores de los datos. Desactívelo para introducir valores manualmente para una escala fija.
  - **Umbral mínimo de alarma** y **Umbral máximo de alarma**: Estos valores agregarán líneas de referencia horizontales al gráfico de barras, lo que facilitará ver cuando el valor de los datos sube o baja demasiado.

Máscaras de privacidad

: Haga clic para crear una nueva máscara de privacidad.

Máscaras de privacidad: Haga clic para cambiar el color de todas las máscaras de privacidad o para eliminar todas las máscaras de privacidad de forma permanente.

Mask x (Máscara x): Haga clic para renombrar, deshabilitar o eliminar permanentemente la máscara.

Comunicación

Lista de contactos

Contactos

Haga clic aquí para descargar la lista de contactos como archivo json.

Haga clic aquí para importar una lista de contactos (json).

Add contact (Añadir contacto): Haga clic para agregar un nuevo contacto a la lista.

Upload image (Cargar imagen) : Haga clic para cargar una imagen representativa del contacto.

First name (Nombre): Introduzca el nombre del contacto.

Last name (Apellidos): Introduzca los apellidos del contacto.

Speed dial (Marcación rápida) : Introduzca un número de marcación rápida disponible para el contacto. Este número se usa para llamar al contacto desde el dispositivo.

Dirección SIP: Si utiliza SIP, introduzca la dirección IP o extensión del contacto.

: Haga clic para realizar una llamada de prueba. La llamada termina automáticamente cuando se contesta.

Cuenta SIP: Si utiliza SIP, seleccione la cuenta SIP que quiera usar para la llamada del dispositivo al contacto.

Availability (Disponibilidad): Seleccione el calendario de la disponibilidad del contacto. Puede añadir o ajustar programaciones en **System (Sistema) > Events (Eventos) > Schedules (Programaciones)**. Si se intenta realizar una llamada cuando el contacto no está disponible, la llamada se cancela a menos que haya un contacto de reserva.

Fallback (Reserva): Si es necesario, seleccione un contacto de reserva de la lista.

Notas: Añada información opcional sobre el contacto.

El menú contextual contiene:

Edit contact (Editar contacto): Edite las propiedades del contacto.

Delete contact (Eliminar contacto): Elimine el contacto.

Grupos

Haga clic aquí para descargar la lista de contactos como archivo json.

Haga clic aquí para importar una lista de contactos (json).

Add group (Añadir grupo): Haga clic para crear un nuevo grupo de contactos ya existentes.

Upload image (Cargar imagen) : Haga clic para cargar una imagen representativa del grupo.

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

Use for group calls only (Usar solo para llamadas de grupo): Active esta opción si quiere usar el grupo solo para llamadas de grupo. Desactive esta opción si desea añadir contactos individuales a un grupo pero no usar el grupo para llamadas de grupo.

Speed dial (Marcación rápida): Introduzca un número de marcado rápido disponible para el grupo. Este número se usa para llamar al grupo desde el dispositivo. Solo para grupos de llamada de grupo.

Recipients (Destinatarios): Seleccione los contactos que desea incluir en el grupo. Las llamadas se realizarán a todos los destinatarios a la vez. El número máximo de destinatarios es seis.

Fallback (Reserva): Si es necesario, seleccione un contacto de reserva de la lista. Solo para grupos de llamada de grupo.

Notas: Añada información opcional sobre el grupo.

El menú contextual contiene:

Edit group (Editar grupo): Edite las propiedades del grupo.

Delete group (Eliminar grupo): Elimine el grupo.

SIP

Ajustes

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

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

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

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

Gestión de llamadas

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

Puertos

Un número de puerto debe estar entre 1024 y 65535.

- **Puerto SIP**: el puerto de red empleado para la comunicación SIP. El tráfico de señalización a través de este puerto no está cifrado. El puerto predeterminado es el 5060. Si es necesario, introduzca un número de puerto diferente.
- **TLS port (Puerto TLS)**: el puerto de red empleado para la comunicación SIP cifrada. El tráfico de señalización a través de este puerto está cifrado con Transport Layer Security (TLS). El puerto predeterminado es el 5061. Si es necesario, introduzca un número de puerto diferente.
- **Puerto de inicio RTP**: el puerto de red utilizado para la primera transmisión de medios RTP en una llamada SIP. El puerto de inicio predeterminado es el 4000. Algunos cortafuegos bloquean el tráfico RTP en determinados números de puerto.

NAT transversal

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

Nota

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

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

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

Audio y vídeo

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

Nota

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

- **Dirección de audio**: Seleccione las direcciones de audio permitidas.
- **Modo de paqueteización** H.264: Seleccione qué modo de paquetización que desea utilizar.
  - **Automático**: (Recomendado) El dispositivo decide qué modo de paquetización se va a utilizar.

  - **None (Ninguno)**: No se ha establecido ningún modo de paquetización. Este modo se suele interpretar como modo **0**.
  - **0**: Modo no intercalado.
  - **1**: Modo de unidad NAL individual.
- **Dirección de vídeo**: Seleccione las direcciones de vídeo permitidas.

Adicional

- **Cambiar de UDP a TCP**: Seleccione para permitir que las llamadas cambien de protocolo de transporte de UDP (Protocolo de Datagramas de Usuario) a TCP (Protocolo de Control de la Transmisión) temporalmente. El motivo para cambiar es evitar la fragmentación y el cambio puede realizarse si la solicitud está a 200 bytes de la unidad de transmisión máxima (MTU) o es mayor de 1300 bytes.
- **Permitir mediante reescritura**: Seleccione para enviar la dirección IP local en lugar de la dirección IP pública del router.
- **Permitir reescribir contacto**: Seleccione para enviar la dirección IP local en lugar de la dirección IP pública del router.
- **Registrar con servidor cada**: establezca la frecuencia con la que desea que el dispositivo se registre con el servidor SIP para las cuentas SIP existentes.
- **Tipo de carga útil MFDT**: Cambia el tipo de carga útil predeterminado para MFDT.
- **Máximo de retransmisiones**: Puede establecer la cantidad máxima de veces que el dispositivo intenta conectarse al servidor SIP antes de dejar de intentarlo.
- **Segundos hasta la recuperación a prueba de fallos**: Puede establecer la cantidad de segundos hasta que el dispositivo intenta volver a conectarse al servidor SIP principal después de haber conmutado por error a un servidor SIP secundario.

Cuentas

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

La cuenta se ha registrado correctamente con el servidor SIP.

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

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

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

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

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

DTMF

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

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

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

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

Protocolos

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

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

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

Llamada de prueba

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

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

Lista de acceso

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

Policy (Directiva):

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

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

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

Llamadas

Botón de llamada

Utilizar el botón de llamada: Active esta opción para poder usar el botón de llamada.

Funcionalidad del botón durante una llamada: Seleccione la funcionalidad del botón de llamada una vez iniciada una llamada desde el dispositivo.

- **Finalizar la llamada**: Cuando un visitante pulsa el botón de llamada durante una llamada saliente, termina la llamada. Utilice esta opción para que los visitantes puedan finalizar una llamada en cualquier momento.
- **Sin funcionalidad hasta que la llamada haya finalizado**: Cuando un visitante pulsa el botón de llamada durante una llamada saliente, no pasa nada. Utilice esta opción para prohibir a los visitantes finalizar una llamada.
- **Espera antes de finalizar la llamada**: Cuando un visitante pulsa el botón de llamada en el periodo de tiempo configurado en **Espera (segundos)** tras iniciar una llamada, no ocurre nada. Si ha transcurrido el tiempo de espera, al pulsar el botón de llamada termina la llamada. Utilice esta opción para evitar que los visitantes finalicen llamadas por error al pulsar dos veces.
  - **Espera (segundos)**: introduzca el tiempo que debe transcurrir antes de pulsar el botón de llamada por segunda vez para finalizar la llamada.

Standby light (Luz de espera): Seleccione una de las opciones de la luz integrada que rodea el botón de llamada.

- **Automático** : El dispositivo enciende y apaga la luz integrada en función de la luz ambiental.
- **On (Encendido)**: La luz integrada siempre está encendida cuando el dispositivo está en modo de reposo.
- **Apagado**: La luz integrada siempre está apagada cuando el dispositivo está en modo de reposo.

Recipients (Destinatarios): Seleccione o cree contactos a los que se debe llamar cuando un usuario pulse el botón de llamada. Si añade más de un destinatario, todos recibirán la llamada a la vez. El número máximo de destinatarios de llamadas SIP es seis, pero el número de destinatarios de llamadas VMS es ilimitado.

Fallback (Reserva): Agregue un contacto de reserva de la lista por si no responde ninguno de los destinatarios.

General

Audio

Nota

- El clip de audio seleccionado solo se reproduce cuando se realiza una llamada.
- Si cambia el clip de audio o la ganancia durante una llamada en curso, no estará en activo hasta la siguiente llamada.

Ringtone (Tono de llamada): Seleccione el clip de audio que se reproducirá cuando alguien haga una llamada al dispositivo. Utilice el control deslizante para ajustar la ganancia.

Ringback tone (Tono de llamada): Seleccione el clip de audio que se reproducirá cuando alguien haga una llamada desde el dispositivo. Utilice el control deslizante para ajustar la ganancia.

Llamadas VMS

Llamadas VMS

Allow calls in the video management software (VMS) (Permitir llamadas en el software de gestión de vídeo [VMS]): Seleccione esta opción para permitir llamadas desde el dispositivo al VMS. Puede realizar llamadas VMS aunque SIP esté apagado.

Tiempo de espera de llamada: Defina la duración máxima de una llamada en curso si nadie responde.

Analítica

Configuración de metadatos

Productores de metadatos RTSP

Se muestran las aplicaciones que transmiten metadatos y los canales que utilizan.

Nota

Estos ajustes corresponden al flujo de metadatos RTSP que utilizan ONVIF XML. Los cambios que se hagan aquí no afectan a la página de visualización de metadatos.

Productor: La aplicación que genera los metadatos. Debajo de la aplicación hay una lista de los tipos de metadatos que transmite la aplicación desde el dispositivo.

Canal: El canal que utiliza la aplicación. Active esta casilla para activar la secuencia de metadatos. Desactive esta casilla por motivos de compatibilidad o de gestión de recursos.

Lector

Conexión

Protocolo de lector

Reader protocol type (Tipo de protocolo de lector): Seleccione el protocolo que se debe usar para la función de lector.

- **VAPIX reader (Lector VAPIX)**: Solo se puede utilizar con controladores de puerta Axis.
  - **Protocol (Protocolo)**: Seleccione **HTTPS** o **HTTP**.
  - **Door controller address (Dirección del controlador de puerta)**: Introduzca la dirección IP para el controlador de puerta.
  - **Nombre de usuario**: Introduzca el nombre de usuario del controlador de puerta.
  - **Contraseña**: Introduzca la contraseña del controlador de puerta.
  - **Conectar**: Haga clic aquí para conectarse al controlador de puerta.
  - **Select reader (Seleccionar lector)**: Seleccione el lector de entrada para la puerta adecuada.
- **OSDP**:
  - **OSDP address (Dirección OSDP)**: Introduzca la dirección del lector OSDP. 0 es la dirección predeterminada y más común para lectores individuales.
- **Wiegand** :
  - **Beeper (Indicador acústico)**: Active esta opción para activar la entrada de indicador acústico.
  - **Input for beeper (Entrada de indicador acústico)**: Seleccione el puerto de E/S que se usa para el indicador acústico.
  - **Input used for LED control (Entrada utilizada para el control LED)**: Seleccione cuántos puertos de E/S se deben usar para controlar la información LED del dispositivo.
  - **Input for LED1/LED2 (Entrada para LED1/LED2)**: Seleccione qué puertos de E/S utilizar para la entrada de LED.
  - **Idle color (Color inactivo)**: Si no se utiliza ningún puerto de E/S para controlar el LED, se puede seleccionar un color estático para que se muestre en la tira del indicador del lector de tarjetas.
  - **Color for state low/high (Color para estado bajo/alto)**: Si se utiliza un puerto de E/S para el control LED, se deben seleccionar los colores que se mostrarán para el estado bajo y el estado alto respectivamente.
  - **Idle color/LED1 color/LED2 color/LED1 + LED2 color (Color inactivo/Color de LED1/Color de LED2/Color de LED1 + LED2)**: Si se utilizan dos puertos de E/S para el control LED, seleccione los colores que se deben mostrar para inactivo, LED1, LED2 y LED1 + LED2, respectivamente.
  - **Keypress format (Formato Keypress)**: Decida cómo formatear el PIN cuando se envía a la unidad de control de acceso.
    - **FourBit**: El número de identificación personal (PIN) `1234` se codifica y se envía como 0x1 0x2 0x3 0x4. Este es el comportamiento predeterminado y más común.
    - **EightBitZeroPadded**: El PIN `1234` se codifica y se envía como 0x01 0x02 0x03 0x04.
    - **EightBitInvertPadded**: El PIN `1234` se codifica y se envía como 0xE1 0xD2 0xC3 0xB4.
    - **Wiegand26**: El PIN se codifica en formato Wiegand26 con un código de instalación de 8 bits y un identificador de 16 bits.
    - **Wiegand34**: El PIN se codifica en un formato Wiegand34 con un código de instalación de 16 bits y un identificador de 16 bits.

- **Wiegand37**: El PIN se codifica en formato Wiegand37 (H10302) con un identificador de 35 bits.
- **Wiegand37FacilityCode**: El PIN se codifica en un formato Wiegand37 (H10304) con un código de instalación de 16 bits y un identificador de 19 bits.

– **Facility code (Código de instalación)**: Introduzca el código de instalación que se debe enviar. Esta opción solo está disponible en algunos formatos de pulsación de tecla.

Formato de salida

Select data format (Seleccionar formato de datos): Seleccione el formato en el que se enviarán los datos de la tarjeta a la unidad de control de acceso.

- **Raw (Sin formato)**: Los datos de la tarjeta se transmiten tal y como están.
- **Wiegand26**: Los datos de la tarjeta se codifican en formato Wiegand26 con un código de instalación de 8 bits y un identificador de 16 bits.
- **Wiegand34**: Los datos de la tarjeta se codifican en formato Wiegand34 con un código de instalación de 16 bits y un identificador de 16 bits.
- **Wiegand37**: Los datos de la tarjeta se codifican en formato Wiegand37 (H10302) con un identificador de 35 bits.
- **Wiegand37FacilityCode**: Los datos de la tarjeta se codifican en formato Wiegand37 (H10304) con un código de instalación de 16 bits y un identificador de 19 bits.
- **Custom (Personalizado)**: Defina un formato personalizado.

Facility code override mode (Modo de anulación de código de instalación): Seleccione una opción para anular el código de la instalación.

- **Automático**: El código de la instalación no se anula y se crea un código de instalación a partir de la detección automática de los datos de entrada. Se usa el código de instalación original de la tarjeta o el código se crear a partir de los bits sobrantes de un número de tarjeta.
- **Optional (Opcional)**: Se usa el código de instalación creado a partir de los datos de entrada o lo anula con un valor opcional configurado.
- **Override (Anulación)**: Se anula siempre con un código de instalación determinado.

Tipos de chip

Tipos de chip

Activate chip type (Activar tipo de chip): Seleccione un tipo de chip de la lista para activarlo.

La opción **Active chip types (Tipos de chip activos)** contiene la lista de todos los tipos de chip activos e indica si los chips usan conjuntos de datos predeterminados o personalizados.

El menú contextual contiene:

- **Deactivate (Desactivar)**: Active esta opción para eliminar un tipo de chip de la lista de tipos de chip activos.

Conjuntos de datos

Invert byte order for all chip types using the full card serial number (CSN) (Invertir el orden de los bytes para todos los tipos de chip utilizando el número de serie completo de la tarjeta [CSN]): Active esta opción para invertir el orden de los bytes del número de serie de la tarjeta. El número de serie de la tarjeta son los datos predeterminados.

Invert byte order for all chip types using secure card data (Invertir orden de bytes para todos los tipos de chip utilizando datos de tarjeta segura): Active esta opción para revertir el orden de bytes de los datos de tarjeta segura para los tipos de chip que utilizan un conjunto de datos personalizado.

Add data set (Agregar conjunto de datos): Seleccione un tipo de chip y haga clic para agregar un conjunto de datos. Para datos personalizados.

- **Name of data set (Nombre del conjunto de datos)**: Cambie el nombre del conjunto de datos de forma que le ayude a identificar los datos. El nombre debe ser único. Funciona como ID, por ejemplo en la API.
- **Habilitada**: Desactive esta opción para dejar de utilizar el conjunto de datos sin eliminarlo.
- **Required data (Datos obligatorios)**: Si no se puede acceder a los datos de tarjeta segura por algún motivo, el dispositivo no envía ningún dato al controlador de puerta cuando este ajuste está activado. Desactive esta opción para enviar el CSN al controlador de puerta cuando no se puede acceder a datos de la tarjeta segura.
- **Use as authenticator (Usar como autenticador)**: Desactive esta opción si no desea utilizar datos de la tarjeta segura como autenticación y enviarlos solo como metadatos válidos para el protocolo VAPIX.
- **Offset (bits) (Desplazamiento [bits])**: Introduzca la posición de inicio de los datos. 0 significa que la posición de inicio es el primer bit.
- **Length (bits) (Longitud [bits])**: Introduzca la longitud de los datos. 0 significa que se leerá cualquier longitud de datos.
- **Use data on card (Usar los datos de la tarjeta)**: Active esta opción para utilizar datos de la tarjeta segura. Desactive el uso de CSN en lugar de los datos de la tarjeta segura.

El resto de los ajustes son específicos del tipo de chip y se utilizan para definir cómo leer los datos de la tarjeta segura.

Número de identificación personal (PIN)

Los ajustes del PIN debe ser iguales que los configurados en la unidad de control de acceso.

Length (Longitud) (0–32): Introduzca el número de dígitos del PIN. Si los usuarios no están obligados a utilizar un PIN cuando utilizan el lector, ajuste la longitud a 0.

Timeout (seconds, 3–50) (Tiempo de espera [segundos, 3–50]): Especifique el número de segundos que deben transcurrir antes de que el dispositivo vuelva al modo inactivo cuando no se recibe el PIN.

Lista de entrada

Con la lista de entrada, puede configurar el dispositivo para permitir que los titulares de las credenciales utilicen su tarjeta o PIN para realizar acciones diferentes, como abrir una puerta. Las credenciales se almacenan localmente en el dispositivo. También puede combinar esta funcionalidad con un controlador de puerta externo.

Soportes de credenciales

Use Entry list (Utilizar lista de entrada): Active esta opción para utilizar la funcionalidad de lista de entrada.

Use connected door controller (Usar controlador de puerta conectado): Active esta función si el dispositivo ya está conectado a un controlador de puerta. Si alguien presenta una credencial que no existe en la lista de entradas, le enviaremos la solicitud al controlador de puerta conectado. No se envían las credenciales que están disponibles en la lista de entrada.

Add credential holder (Agregar soporte de credenciales): Haga clic para agregar un nuevo soporte de credenciales.

First name (Nombre): Introduzca su nombre.

Last name (Apellidos): Introduzca su apellido.

Credential type (Tipo de credencial):

- **PIN**:
  - **PIN**: Introduzca un PIN único o haga clic en **Generate (Generar)** para crear uno automáticamente.
- **Card (Tarjeta)**:
  - **UID**: Introduzca el UID y la longitud de bits de la tarjeta o haga clic en **Get latest (Obtener último)** para recuperar los datos del último barrido de tarjeta.

Event condition (Condiciones de evento): Seleccione una o más condiciones para activar cuando el titular de la credencial utilice su credencial. Para configurar la acción resultante, vaya a **System > Events (Sistema > Eventos)** y cree una regla con la misma condición que seleccione aquí.

Valid from (Válido desde): Seleccione **Current device time (Hora actual del dispositivo)** para activar la credencial inmediatamente. Borre para especificar cuándo activar la credencial.

Valid to (Válido hasta):

- **No end date (Sin fecha de finalización)**: La credencial es válida indefinidamente.
- **End date (Fecha de finalización)**: Especifique la fecha y hora en las que la credencial deja de ser válida.
- **Number of times (Número de veces)**: Especifique cuántas veces puede utilizar la credencial el titular de la credencial. El valor del campo se reduce a medida que se utiliza la credencial para mostrar el resto de usos.

Notas: Introduzca información opcional.

Suspend (Suspender): Seleccione esta opción para que la credencial sea temporalmente inválida.

Registro de eventos

El registro de eventos muestra una lista de los eventos de la lista de entrada. El tamaño máximo del archivo de registro es de 2 MB, lo que equivale aproximadamente a 6000 eventos.

Export all (Exportar todo): Haga clic para exportar todos los eventos de la lista. Para exportar solo un subconjunto, seleccione los eventos que le interesan. Los eventos se exportan a un archivo CSV.

Filter (Filtro): Haga clic para mostrar los eventos ocurridos durante un intervalo de tiempo específico.

: Escriba para buscar todo el contenido coincidente en la lista.

Audio

Configuración del dispositivo

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

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

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

Apply changes (Aplicar cambios) : Aplique su selección.

Cancelación de ruido: Active esta función para mejorar la calidad del audio eliminando el ruido de fondo.

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

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

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

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

Salida: Muestra el tipo de salida.

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

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

Flujo

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

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

Clips de audio

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

Reproducir el clip de audio.

Detener la reproducción del clip de audio.

El menú contextual contiene:

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

Grabaciones

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

Inicia una grabación en el dispositivo.

Elija en qué dispositivo de almacenamiento guardar la grabación.

Detener una grabación en el dispositivo.

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

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

Reproduzca la grabación.

Deje de reproducir la grabación.

Muestre u oculte información y opciones sobre la grabación.

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

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

Haga clic para eliminar una grabación.

Exportar: Exporte toda o una parte de la grabación.

Haga clic para filtrar las grabaciones.

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

Hasta: Mostrar grabaciones hasta un momento determinado.

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

Evento: Mostrar grabaciones en función de eventos.

Almacenamiento: Mostrar grabaciones según el tipo de almacenamiento.

Aplicaciones

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

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

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

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

Nota

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

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

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

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

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

Sistema

Hora y ubicación

Fecha y hora

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

Nota

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

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

- **Fecha y hora automáticas (servidores NTS KE manuales)**: Sincronice con los servidores de establecimiento de claves NTP seguros conectados al servidor DHCP.
  - **Servidores NTS KE manuales**: Introduzca la dirección IP de un servidor NTP o de dos. Si usa dos servidores NTP, el dispositivo sincroniza y adapta la fecha y hora en función de la información de los dos.
  - **Tiempo máximo de encuesta NTP**: Seleccione la cantidad máxima de tiempo que debe esperar el dispositivo antes de que sondee el servidor NTP para obtener una hora actualizada.
  - **Tiempo mínimo de encuesta NTP**: Seleccione la cantidad mínima de tiempo que debe esperar el dispositivo antes de que sondee el servidor NTP para obtener una hora actualizada.
- **Fecha y hora automáticas (los servidores NTP utilizan DHCP)**: Se sincroniza con los servidores NTP conectados al servidor DHCP.
  - **Servidores NTP alternativos**: Introduzca la dirección IP de un servidor alternativo o de dos.
  - **Tiempo máximo de encuesta NTP**: Seleccione la cantidad máxima de tiempo que debe esperar el dispositivo antes de que sondee el servidor NTP para obtener una hora actualizada.
  - **Tiempo mínimo de encuesta NTP**: Seleccione la cantidad mínima de tiempo que debe esperar el dispositivo antes de que sondee el servidor NTP para obtener una hora actualizada.
- **Fecha y hora automáticas (servidores NTP manuales)**: Se sincroniza con los servidores NTP que seleccione.
  - **Servidores NTP manuales**: Introduzca la dirección IP de un servidor NTP o de dos. Si usa dos servidores NTP, el dispositivo sincroniza y adapta la fecha y hora en función de la información de los dos.
  - **Tiempo máximo de encuesta NTP**: Seleccione la cantidad máxima de tiempo que debe esperar el dispositivo antes de que sondee el servidor NTP para obtener una hora actualizada.
  - **Tiempo mínimo de encuesta NTP**: Seleccione la cantidad mínima de tiempo que debe esperar el dispositivo antes de que sondee el servidor NTP para obtener una hora actualizada.
- **Custom date and time (Personalizar fecha y hora)**: Establezca manualmente la fecha y hora. Haga clic en **Get from system (Obtener del sistema)** para obtener una vez la configuración de fecha y hora desde su ordenador o dispositivo móvil.

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

- **DHCP**: Adopta la zona horaria del servidor DHCP. El dispositivo debe estar conectado a un servidor DHCP para poder seleccionar esta opción.
- **Manual**: Seleccione una zona horaria de la lista desplegable.

Nota

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

Localización de dispositivo

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

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

Comprobación de configuración

Imagen interactiva del dispositivo: Haga clic en los botones de la imagen para simular pulsaciones en el teclado. De esta forma, puede probar configuraciones o solucionar problemas de hardware sin tener acceso físico al dispositivo.

Latest credentials (Credenciales más recientes) : Muestra información sobre las credenciales que se registraron por última vez.

Muestre los datos de credenciales más recientes.

El menú contextual contiene:

- **Reverse UID (Invertir UID)**: Invertir el orden de bytes del UID.
- **Revert UID (Revertir UID)**: Revertir el orden de bytes del UID al orden original.
- **Copy to clipboard (Copiar en el portapapeles)**: Copiar el UID.

Check credentials (Comprobar credenciales) : Introduzca un UID o un PIN y envíelo para comprobar las credenciales. El sistema responderá del mismo modo que si utilizara las credenciales en el dispositivo. Si se necesitan UID y PIN, comience introduciendo el UID.

Red

IPv4

Asignar IPv4 automáticamente: Seleccione esta opción para que el router de red asigne automáticamente una dirección IP al dispositivo. Recomendamos IP automática (DHCP) para la mayoría de las redes.

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

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

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

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

Nota

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

IPv6

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

Nombre de host

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

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

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

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

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

Servidores DNS

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

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

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

HTTP y HTTPS

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

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

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

Nota

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

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

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

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

Protocolos de detección de red

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

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

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

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

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

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

Proxies globales

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

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

Formatos permitidos para proxies http y https:

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

Nota

Reinicie el dispositivo para aplicar los ajustes globales del proxy.

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

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

Conexión a la nube con un clic

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

Allow O3C (Permitir O3C):

- **Un clic**: Esta es la configuración predeterminada. Mantenga pulsado el botón de control en el dispositivo para conectar con un servicio O3C a través de Internet. Debe registrar el dispositivo en el servicio O3C en un plazo de 24 horas después de pulsar el botón de control. De lo contrario, el dispositivo se desconecta del servicio O3C. Una vez que registre el dispositivo, **Always (Siempre)** quedará habilitado y el dispositivo permanecerá conectado al servicio O3C.
- **Siempre**: El dispositivo intenta conectarse continuamente a un servicio O3C a través de Internet. Una vez que registre el dispositivo, permanece conectado al servicio O3C. Utilice esta opción si el botón de control del dispositivo está fuera de su alcance.
- **No**: Deshabilita el servicio O3C.

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

Host: Introduzca la dirección del servidor proxy.

Puerto: Introduzca el número de puerto utilizado para acceder.

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

Authentication method (Método de autenticación):

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

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

SNMP

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

SNMP: Seleccione la versión de SNMP a usar.

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

Nota

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

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

Clientes conectados

Muestra el número de conexiones y clientes conectados.

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

Seguridad

Certificados

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

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

Se admiten estos formatos:

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

Importante

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

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

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

El menú contextual contiene:

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

Almacenamiento de claves seguro :

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

Control y cifrado de acceso a la red

IEEE 802.1x

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

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

IEEE 802.1AE MACsec

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

Certificados

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

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

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

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

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

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

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

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

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

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

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

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

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

Evitar ataques de fuerza bruta

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

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

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

Firewall

Activar: Encienda el cortafuegos.

Política predeterminada: Seleccione el estado predeterminado para el cortafuegos.

- **Allow (Permitir):** Permite todas las conexiones al dispositivo. Esta opción está establecida de forma predeterminada.
- **Deny (Denegar):** Deniega todas las conexiones al dispositivo.

Para hacer excepciones a la política predeterminada, puede crear reglas que permiten o deniegan las conexiones al dispositivo desde direcciones, protocolos y puertos específicos.

- **Dirección**: Introduzca una dirección en formato IPv4/IPv6 o CIDR a la que desee permitir o denegar el acceso.
- **Protocol (Protocolo)**: Seleccione un protocolo al que desee permitir o denegar el acceso.
- **Puerto**: Introduzca un número de puerto al que desee permitir o denegar el acceso. Puede agregar un número de puerto entre 1 y 65535.
- **Policy (Directiva)**: Seleccione la política de la regla.

: Haga clic para crear otra regla.

Agregar reglas: Haga clic para agregar las reglas que haya definido.

- **Tiempo en segundos:** Defina un límite de tiempo para probar las reglas. El límite de tiempo predeterminado se establece en 300 segundos. Para activar las reglas inmediatamente, defina la hora en 0 segundos.
- **Confirmar reglas:** Confirme las reglas y su límite de tiempo. Si ha establecido un límite de tiempo de más de 1 segundo, las reglas estarán activas durante este periodo. Si ha ajustado la hora en 0, las reglas se activarán de inmediato.

Reglas pendientes: Información general de las reglas probadas recientemente que aún no ha confirmado.

Nota

Las reglas que tienen un límite de tiempo aparecen en **Active rules (Reglas activas)** hasta que se agota el temporizador mostrado o hasta que las confirme. Si no las confirma, aparecerán en **Pending rules (Reglas pendientes)** una vez que se agote el temporizador y el firewall volverá a los ajustes definidos anteriormente. Si los confirma, sustituirán las reglas activas actuales.

Confirmar reglas: Haga clic para activar las reglas pendientes.

Activar reglas: Información general de las reglas que ejecuta actualmente en el dispositivo.

: Haga clic para eliminar una regla activa.

: Haga clic para eliminar todas las reglas, tanto pendientes como activas.

Certificado de AXIS OS con firma personalizada

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

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

El menú contextual contiene:

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

Cuentas

Cuentas

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

Cuenta: introduzca un nombre de cuenta único.

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

Repetir contraseña: Introduzca la misma contraseña de nuevo.

Privilegios:

- **Administrador**: Tiene acceso completo a todos los ajustes. Los administradores también pueden agregar, actualizar y eliminar otras cuentas.
- **Operator (Operador)**: Tiene acceso a todos los ajustes excepto:
  - Todos los ajustes del **sistema**.
- **Viewer (Visualizador)**: Puede:
  - Ver y tomar instantáneas de una transmisión de vídeo.
  - Ver y exportar grabaciones.
  - Movimiento horizontal, vertical y zoom; con acceso a la **cuenta de PTZ**.

El menú contextual contiene:

Actualizar cuenta: Editar las propiedades de la cuenta.

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

Acceso anónimo

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

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

Cuentas SSH

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

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

Cuenta: introduzca un nombre de cuenta único.

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

Repetir contraseña: Introduzca la misma contraseña de nuevo.

Comentario: Introduzca un comentario (opcional).

El menú contextual contiene:

Actualizar cuenta SSH: Editar las propiedades de la cuenta.

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

Host virtual

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

Habilitada: Seleccione esta opción para usar este host virtual.

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

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

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

El menú contextual contiene:

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

Disabled (Deshabilitado): El servidor está deshabilitado.

Configuración de OpenID

Importante

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

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

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

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

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

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

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

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

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

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

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

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

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

Eventos

Reglas

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

Nota

Puede crear hasta 256 reglas de acción.

Agregar una regla: Cree una regla.

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

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

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

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

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

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

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

Destinatarios

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

Nota

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

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

Nota

Puede crear hasta 20 destinatarios.

Agregar un destinatario: Haga clic para agregar un destinatario.

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

Tipo: Seleccione de la lista:

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

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

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

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

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

Nota

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

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

Comprobación: Haga clic en probar la configuración.

⋮ El menú contextual contiene:

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

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

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

Horarios

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

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

Activadores manuales

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

MQTT

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

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

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

ALPN

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

Cliente MQTT

Conectar: Active o desactive el cliente MQTT.

Estado: Muestra el estado actual del cliente MQTT.

Broker

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

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

Puerto: Introduzca el número de puerto.

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

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

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

Contraseña: Introduzca una contraseña para el nombre de usuario.

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

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

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

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

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

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

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

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

Mensaje de conexión

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

Enviar mensaje: Active esta función para enviar mensajes.

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

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

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

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

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

Mensaje de testamento y últimas voluntades

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

Enviar mensaje: Active esta función para enviar mensajes.

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

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

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

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

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

Publicación MQTT

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

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

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

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

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

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

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

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

Suscripciones MQTT

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

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

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

Tipo de suscripción:

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

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

Superposiciones MQTT

Nota

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

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

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

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

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

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

Almacenamiento

Almacenamiento de red

Ignorar: Active para ignorar el almacenamiento de red.

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

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

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

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

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

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

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

Herramientas

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

Usar herramienta: Haga clic para activar la herramienta seleccionada.

Almacenamiento integrado

Importante

Riesgo de pérdida de datos y grabaciones dañadas. No extraiga la tarjeta SD mientras el dispositivo esté en funcionamiento. Desmonte la tarjeta SD para extraerla.

Unmount (Desmontar): Haga clic en esta opción para eliminar la tarjeta SD de forma segura.

Write protect (Protección contra escritura): Active esta opción para dejar de escribir en la tarjeta SD y evitar que se eliminen las grabaciones. El formato de una tarjeta SD protegida contra escritura no se puede cambiar.

Formato automático: Active esta función para formatear automáticamente una tarjeta SD que se acaba de insertar. El formato del sistema de archivos se cambia a ext4.

Ignorar: Active esta función para dejar de almacenar las grabaciones en la tarjeta SD. Si ignora la tarjeta SD, el dispositivo deja de reconocerla. Este ajuste solo está disponible para los administradores.

Tiempo de conservación: Seleccione el tiempo que desea guardar las grabaciones para limitar la cantidad de grabaciones antiguas o cumplir con las normativas en materia de almacenamiento de datos. Cuando la tarjeta SD está llena, elimina las grabaciones antiguas antes de que transcurra su tiempo de retención.

Herramientas

- **Check (Comprobar)**: Con esta opción se comprueban errores en la tarjeta SD.
- **Repair (Reparar)**: Se reparan los errores del sistema de archivos.
- **Format (Formato)**: Formatea la tarjeta SD para cambiar el sistema de archivos y borrar todos los datos. Solo puede formatear la tarjeta SD en el sistema de archivos ext4. Se necesita contar con una aplicación o un controlador ext4 de terceros para acceder al sistema de archivos desde Windows®.
- **Encrypt (Cifrar)**: Use esta herramienta para formatear la tarjeta SD y habilitar el cifrado. Borra todos los datos de la tarjeta SD. Se cifrará cualquier dato nuevo que almacene en la tarjeta SD.
- **Descifrar**: Use esta herramienta para formatear la tarjeta SD sin cifrado. Borra todos los datos de la tarjeta SD. No se cifrará ningún dato nuevo que almacene en la tarjeta SD.
- **Change password (Modificar contraseña)**: Se cambia la contraseña necesaria para cifrar la tarjeta SD.

Usar herramienta: Haga clic para activar la herramienta seleccionada.

Activador de desgaste: Defina un valor para el nivel de desgaste de la tarjeta SD al que desee activar una acción. El nivel de desgaste oscila entre el 0 y el 200 %. Una nueva tarjeta SD que nunca se haya utilizado tiene un nivel de desgaste del 0 %. Un nivel de desgaste del 100 % indica que la tarjeta SD está cerca de su vida útil prevista. Cuando el nivel de desgaste llega al 200 % existe un riesgo alto de fallos de funcionamiento de la tarjeta SD. Recomendamos ajustar el activador del desgaste entre un 80 y un 90 %. Esto le da tiempo a descargar cualquier grabación y a sustituir la tarjeta SD a tiempo antes de que se desgaste. El activador de desgaste le permite configurar un evento y recibir una notificación cuando el nivel de desgaste alcance su valor establecido.

Perfiles de transmisión

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

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

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

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

Descripción: Agregue una descripción de su perfil.

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

Resolución: Consulte para obtener una descripción de este ajuste.

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

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

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

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

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

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

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

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

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

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

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

ONVIF

Cuentas de ONVIF

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

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

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

Cuenta: introduzca un nombre de cuenta único.

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

Repetir contraseña: Introduzca la misma contraseña de nuevo.

Función:

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

El menú contextual contiene:

Actualizar cuenta: Editar las propiedades de la cuenta.

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

Perfiles multimedia de ONVIF

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

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

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

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

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

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

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

Nota

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

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

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

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

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

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

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

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

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

Metadatos: Seleccione los metadatos para incluir en su configuración.

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

PTZ : Seleccione los ajustes de PTZ para su configuración.

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

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

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

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

Detectores

Manipulación de la cámara

El detector de manipulación de la cámara genera una alarma cuando cambia la escena, por ejemplo cuando el objetivo se cubre, se pulveriza sobre el mismo o se desenfoca gravemente y el tiempo de **retraso al desencadenar** ha transcurrido. El detector de manipulación solo se activa cuando la cámara no se ha movido durante un mínimo de 10 segundos. Durante este periodo, el detector configura un modelo de escena que utiliza como comparación para detectar la manipulación en las imágenes actuales. Para que el modelo de escena se configure adecuadamente, asegúrese de que la cámara está enfocada, las condiciones de iluminación son correctas y la cámara no está orientada hacia una escena sin contornos, por ejemplo, una pared vacía. La manipulación de cámara se puede utilizar como una condición para desencadenar las acciones.

Retraso al desencadenar: Introduzca el tiempo mínimo durante el que las condiciones de manipulación deben estar activas antes de que se active la alarma. De este modo, se pueden evitar falsas alarmas para condiciones ya conocidas que afectan a la imagen.

Activar con imágenes oscuras: Es muy difícil generar alarmas si se pulveriza sobre el objetivo de la cámara, ya que no es posible distinguir este evento de otras situaciones en las que la imagen se oscurece de una forma similar, por ejemplo, cuando las condiciones de iluminación cambian. Active este parámetro para generar alarmas para todos los casos en los que la imagen se oscurezca. Cuando está desactivado, el dispositivo no genera ninguna alarma cuando la imagen se oscurece.

Nota

Para la detección de intentos de manipulación en escenas estáticas y no concurridas.

Detección de audio

Estos ajustes están disponibles para cada entrada de audio.

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

Detección de impactos

Detector de golpes: Active para generar una alarma si un objeto golpea el dispositivo o si se manipula.

Nivel de sensibilidad: Mueva el control deslizante para ajustar el nivel de sensibilidad al que el dispositivo debe generar una alarma. Un valor bajo significa que el dispositivo solo genera una alarma si el golpe es potente. Un valor alto significa que el dispositivo genera una alarma incluso cuando la manipulación sea ligera.

Salida de vídeo

HDMI

Puede conectar un monitor externo al dispositivo a través de un cable HDMI.

Fuente única

En el monitor externo se muestra una transmisión de una sola cámara.

- **Source (fuente)**: Seleccione solo una cámara.
- **Rotate image 180° (Girar la imagen 180°)**: Haga clic para girar la imagen.
- **Mirror image (Imagen reflejada)**: Haga clic para girar la imagen.
- **Dynamic overlays (Superposiciones dinámicas)** : Haga clic para superponer.

Vista cuádruple

Visualice las transmisiones de cuatro cámaras independientes al mismo tiempo en el monitor externo.

- **Sources (Fuentes)**: Seleccione una cámara diferente de cada una de las cuatro listas desplegables. La imagen situada junto a la fuente muestra el lugar en el que se mostrará el vídeo de dicha cámara en la pantalla.
- **Rotate image 180° (Girar la imagen 180°)**: Haga clic para girar todas las imágenes.

Lista de reproducción

Las transmisiones individuales de varias cámaras se alternan en el monitor externo.

- **Rotate image 180° (Girar la imagen 180°)**: Haga clic para girar la imagen desde todas las fuentes.
- +: Haga clic para agregar una cámara a la lista de reproducción.
- **Source (fuente)**: Seleccione la cámara deseada.
- **Duration (Duración)**: Defina cuánto tiempo (en mm:ss) se transmitirá la lista de reproducción desde esta cámara en cada rotación.
- **Mirror image (Imagen reflejada)**: Haga clic para girar la imagen.
- **Create (Crear)**: Haga clic para guardar.

Imagen en imagen

En el monitor externo se muestran dos transmisiones al mismo tiempo. Una transmisión llena el monitor y la otra es una imagen más pequeña. La **posición**, el **tamaño de la imagen** y los **bordes** son personalizables.

- **Imagen en imagen**

– **Source (fuente)**: Seleccione la cámara que transmitirá como la imagen más pequeña.
– **Rotate image 180° (Girar la imagen 180°)**: Haga clic para girar la imagen.
– **Mirror image (Imagen reflejada)**: Haga clic para girar la imagen.
– **Position (Posición)**: Seleccione en qué parte de la pantalla debería aparecer la imagen.
– **Picture size (Tamaño de imagen)**: Arrastre el control deslizante para definir el tamaño (% de pantalla) de la imagen.
– **Border (Borde)**: Haga clic para activar o desactivar los bordes de la imagen.
– : Arrastre el control deslizante para definir el grosor del borde completo.
– : Arrastre el control deslizante para definir el grosor del borde superior.
– : Arrastre el control deslizante para definir el grosor del borde derecho.

- : Arrastre el control deslizante para definir el grosor del borde inferior.
- : Arrastre el control deslizante para definir el grosor del borde izquierdo.
- **Color de borde**: Seleccione un color de borde.

• **Vista de mapa**

- **Source (fuente)**: Seleccione la cámara que transmitirá en la pantalla completa.
- **Rotate image 180° (Girar la imagen 180°)**: Haga clic para girar la imagen.
- **Mirror image (Imagen reflejada)**: Haga clic para girar la imagen.

Accesorios

Puertos de E/S

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

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

Puerto

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

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

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

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

Nota

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

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

Registros

Informes y registros

Informes

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

Registros

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

Registro de sistema remoto

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

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

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

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

- Axis
- RFC 3164
- RFC 5424

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

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

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

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

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

Configuración sencilla

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

Mantenimiento

Mantenimiento

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

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

Importante

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

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

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

Nota

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

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

Al actualizar, puede elegir entre tres opciones:

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

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

solucionar problemas

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

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

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

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

Rastreo de red

Importante

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

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

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

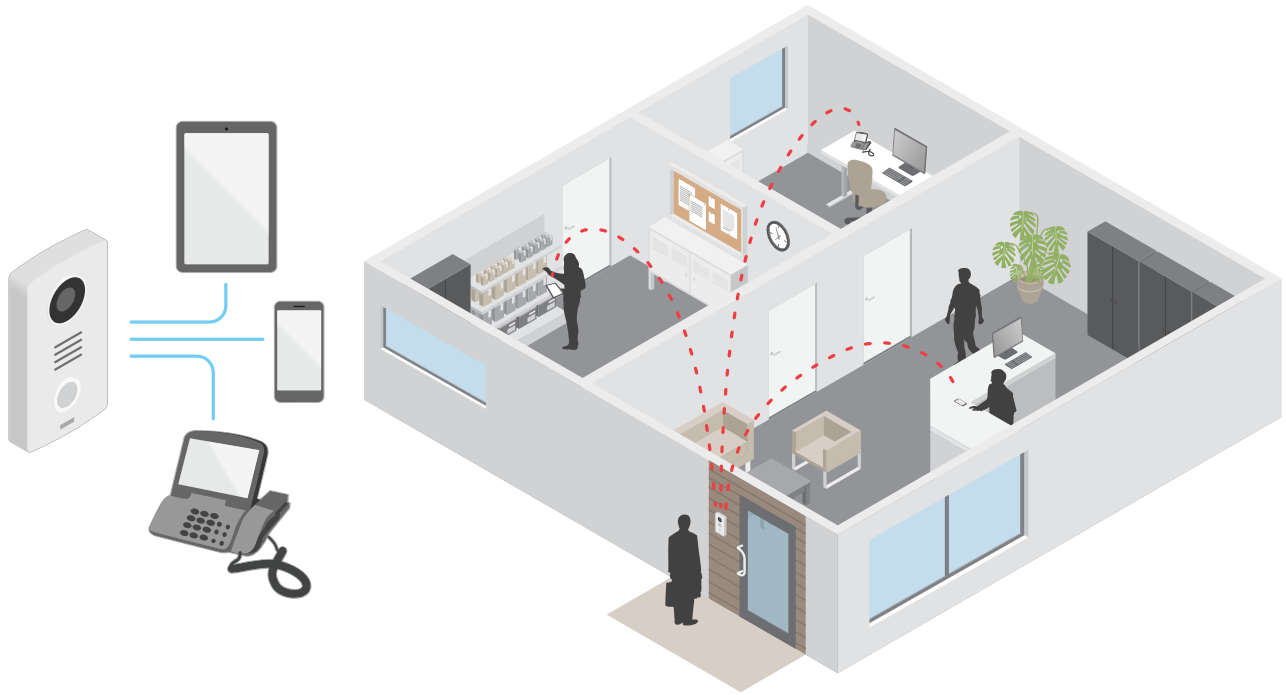
Descubrir más

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 videoportero 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.

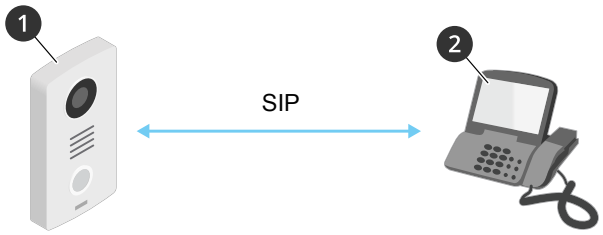
El audio o el vídeo real se intercambian entre los agentes de usuario SIP con un protocolo de transporte, por ejemplo, RTP (protocolo de transporte en tiempo real).

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 - videoportero. Dirección SIP: sip:192.168.1.101*
2 *User agent B - teléfono habilitado para SIP. Dirección SIP: sip:192.168.1.100*

Puede configurar el videoportero 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.

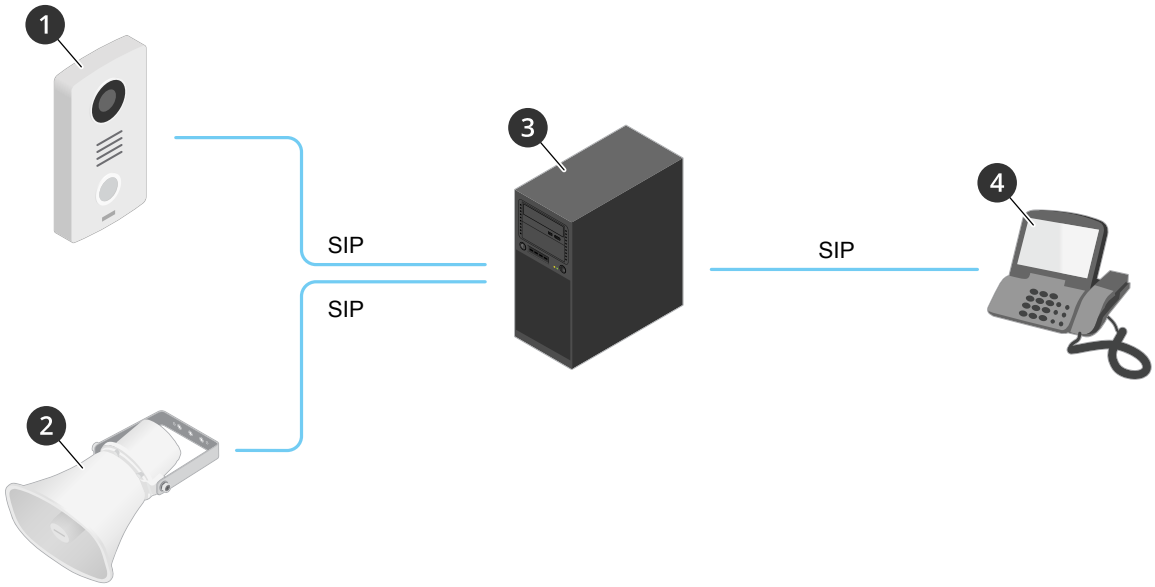
Centralita telefónica privada (PBX)

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. En este caso, una dirección SIP típica sería `sip:<user>@<domain>` o `sip:<user>@<registrar-ip>`. La dirección SIP es independiente de su dirección IP y el PBX permite el acceso al dispositivo siempre que esté registrado en el PBX.

Ejemplo:



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 videoportero AXIS, la llamada se envía a través de una o más PBX a una dirección SIP, ya sea en la red IP local o a través de Internet.

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 nuestra guía *Introducción a las reglas de eventos*.

Aplicaciones

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

Para encontrar los manuales de usuario de las aplicaciones de Axis, visite *help.axis.com*.

Uso diario

Utilizar el teclado

Quiero...	Acción
Llamar a alguien que me permita entrar en el edificio.	Prensa .
Llamar a una persona en el edificio.	Introduzca el número de marcado rápido de la persona y pulse .
Abrir la puerta con tarjeta y PIN.	Pase la tarjeta e introduzca el PIN.
Abrir la puerta con mi PIN.	Introduzca el PIN y pulse #.
Abrir la puerta con mi tarjeta.	Pase la tarjeta.

Localización de problemas

Restablecimiento a la configuración predeterminada de fábrica

Importante

Es preciso tener cuidado si se va a restablecer la configuración predeterminada de fábrica. Todos los valores, incluida la dirección IP, se restablecerán a la configuración predeterminada de fábrica.

Para restablecer el producto a la configuración predeterminada de fábrica:

1. Desconecte la alimentación del producto.
2. Mantenga pulsado el botón de control mientras vuelve a conectar la alimentación. Vea .
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 disponible en la red, la dirección IP del dispositivo adoptará de forma predeterminada una de las siguientes:
   - **Dispositivos con AXIS OS 12.0 y posterior:** Obtenido de la subred de dirección de enlace local (169.254.0.0/16)
   - **Dispositivos con AXIS OS 11.11 y anterior:** 192.168.0.90/24
5. Utilice las herramientas del software de instalación y gestión para asignar una dirección IP, configurar la contraseña y acceder al dispositivo.
   Las herramientas de software de instalación y gestión están disponibles en las páginas de servicio técnico en *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**.

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

- Cuando actualice el software del dispositivo se guardan los ajustes preconfigurados y personalizados (siempre que dicha función esté disponible en el AXIS OS nuevo), si bien Axis Communications AB no puede garantizarlo.
- 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, consejos y soluciones

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

Problemas al actualizar el firmware	
Error durante la actualización del firmware	Cuando se produce un error en la actualización del firmware, el dispositivo vuelve a cargar el firmware anterior. La causa más frecuente es que se ha cargado el firmware incorrecto. Asegúrese de que el nombre del firmware corresponde a su dispositivo e inténtelo de nuevo.

Problemas al configurar la dirección IP	
El dispositivo se encuentra en una subred distinta	Si la dirección IP prevista para el dispositivo y la dirección IP del ordenador utilizado para acceder al dispositivo se encuentran en subredes distintas, no podrá configurar la dirección IP. Póngase en contacto con el administrador de red para obtener una dirección IP.
La dirección IP ya la utiliza otro dispositivo	Desconecte el dispositivo de Axis de la red. Ejecute el comando ping (en una ventana de comando/DOS, escriba `ping` y la dirección IP del dispositivo): • Si recibe lo siguiente: `Reply from <IP address>: bytes=32; time=10...` significa que la dirección IP podría estar en uso por otro dispositivo de la red. Solicite una nueva dirección IP al administrador de red y vuelva a instalar el dispositivo. • Si recibe lo siguiente: `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.
Posible conflicto de dirección IP con otro dispositivo de la misma subred	Se utiliza la dirección IP estática del dispositivo de Axis antes de que el servidor DHCP configure una dirección dinámica. Esto significa que, si otro dispositivo utiliza la misma dirección IP estática predeterminada, podría haber problemas para acceder al dispositivo.

No se puede acceder al dispositivo desde un navegador	
No se puede iniciar sesión	Cuando HTTPS esté activado, asegúrese de utilizar el protocolo correcto (HTTP o HTTPS) al intentar iniciar sesión. Puede que tenga que escribir manualmente `http` o `https` en el campo de dirección del navegador. Si se pierde la contraseña del directorio raíz del usuario, habrá que restablecer el dispositivo a los ajustes predeterminados de fábrica. Consulte .
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).

Se puede acceder al dispositivo localmente pero no externamente

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

- AXIS Companion: gratuito, ideal para sistemas pequeños con necesidades de vigilancia básicas.
- AXIS Camera Station: versión de prueba gratuita de 30 días, ideal para sistemas de tamaño pequeño y mediano.

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

Consideraciones sobre el rendimiento

A la hora de configurar el sistema, es importante considerar de qué modo afectan al rendimiento los distintos ajustes y situaciones. Algunos factores afectan a la cantidad de ancho de banda (velocidad de bits) necesaria, otros pueden afectar a la velocidad de imagen, y otros a ambas. Si la carga de la CPU alcanza su nivel máximo, también afectará a la velocidad de los fotogramas.

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

- 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.

Especificaciones

Controles e indicadores del panel delantero

Al conectar el producto a la corriente eléctrica, los indicadores del panel frontal se encienden durante unos segundos.

Iconos de indicador

Icono	Indicación
	Azul fijo cuando se inicia la llamada saliente. Parpadea en azul cuando se inicia la llamada entrante.
	Ámbar fijo para una llamada en curso.
	Verde fijo cuando la puerta está abierta.

Banda del indicador del lector de tarjetas

La banda indica la información del lector.

Botón de llamada

Puede utilizar la luz integrada que rodea el botón de llamada para iluminar las caras de los visitantes.

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 emplee herramientas afiladas, objetos de metal ni demasiada fuerza al insertar o extraer la tarjeta SD. Utilice los dedos para insertar o extraer 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. Vea .

Conectores

Conector HDMI

Utilice el microHDMI™ para la conexión a una pantalla de vídeo o monitor público de visualización.

Conector de red

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

Conector de audio

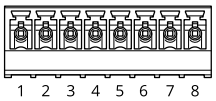
Bloque de terminales de 4 pines para entrada y salida de audio.

Función	Pin	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	Pin	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. 350 mA[2]
Tierra CC	4		0 V CC
NO/NC	5	Normalmente abierto/normalmente cerrado Para conectar dispositivos de relés.	Corriente máx. 1 A Voltaje máx. 30 V CC

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.*

		Los dos pines de relé están separados de forma galvanizada del resto del circuito.	
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 máx. 100 mA[3] Corriente máx. 700 mA[4]
Tierra CC	8		0 V CC

Conector de lector

Bloque de terminales de 4 pines para conectar lector externo.

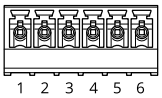
Función	Pin	Notas	Especificaciones
Tierra CC	1		0 V CC
12 V CC	2	Para conectar el equipo auxiliar. Nota: Este pin solo se puede utilizar como salida de alimentación.	Tensión de salida 12 V CC
D0/A+	3	Wiegand: salida DATA0 RS485: A+	
D1/B-	4	Wiegand: salida DATA1 RS485: B-	

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.

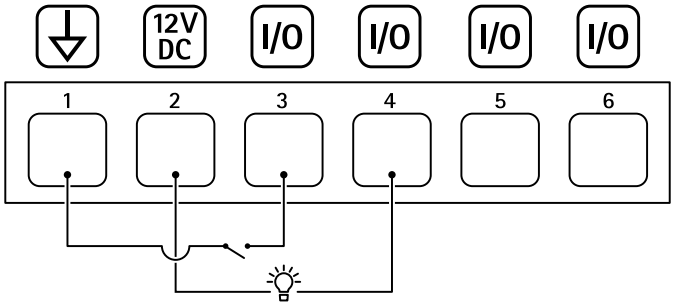


Función	Pin	Notas	Especificaciones
Tierra CC	1		0 V CC
Salida de CC	2	⚠ Se puede utilizar para alimentar equipos auxiliares.	12 V CC Carga máx. = 50 mA

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

		Nota: Este pin solo se puede utilizar como salida de alimentación.	
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 alimentación

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	Pin	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.	8-28 V CC, 22 W máx. Carga máxima en las salidas 9 W

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.

T10176599_es

2025-04 (M17.2)

© 2021 – 2025 Axis Communications AB