FaceStation 2

GUÍA DE USUARIO DE

Versión 1.29

Español
ES 102.00.FS2

suprema
SECURITY & BIOMETRICS

CONTENIDO

Instrucciones de Seguridad 4

Información de cumplimiento 4

Primeros Pasos 8

Componentes 8

Nombre y función de cada parte 9

Cables y conectores 10

Método correcto de enrolamiento y autenticación facial 12

Instalación 14

Fijar el soporte y el producto 14

Conexión de la fuente de alimentación 21

Conexión de red 22

Conexión de entrada 23

Conexión del relé 24

Conectar como independiente 26

Conectar Secure I/O 2 27

Conexión Wiegand 29

Cómo Usar 30

Menú de Administrador 30

Usuario 30

Autenticación 34

Ajustes 38

Registros de eventos 48

Solución de Problemas 50

Verifique estos elementos antes de reportar una falla 50

Especificaciones del Producto 52

Credenciales 52

General 52

Capacidad 53

Interfaz 53

Eléctrico 54

Dimensiones y peso 55

Información Reglamentaria 57

Información de cumplimiento de la FCC 57

Información de IC 57

Declaración de conformidad de la UE (CE) 58

Apéndices 59

Descargos de responsabilidad 59

Aviso de derechos de autor 60

Licencia de código abierto 60

Instrucciones de Seguridad

Lea estas instrucciones de seguridad antes de usar el producto para evitar lesiones a usted y a otros y para prevenir daños a la propiedad.

El término «producto» en este manual se refiere al producto y a cualquier elemento suministrado con él.

Información de cumplimiento

Alerta

Se utiliza para indicar información de advertencia que, si se ignora durante el uso del producto, podría causar lesiones graves o la muerte.

Precaución

Se utiliza para indicar información de precaución que, si se ignora durante el uso del producto, puede provocar lesiones leves o daños al producto.

Información

Se utiliza para proporcionar notas o información adicional durante el uso del producto.

Nota

Se utiliza para proporcionar notas o información adicional durante el uso del producto.

⚠ Advertencia

Instalar

Tenga especial cuidado con el cableado incorrecto cuando use fuentes de alimentación de alta capacidad.

- Un cableado incorrecto puede provocar incendios graves, descargas eléctricas o daños al producto.

No permita que los usuarios instalen o reparen el producto de manera arbitraria.

- Puede causar incendios, descargas eléctricas o lesiones.
- No se proporcionará servicio de reparación gratuito si el producto resulta dañado debido a la instalación o reparación arbitraria por parte del usuario.

No instale el producto en lugares expuestos a la luz solar directa, humedad, polvo o hollín, ni donde pueda haber fugas de gas.

- Puede causar incendios o descargas eléctricas.

Al instalar el producto en exteriores, asegúrese de colocarlo en un área sombreada y bien ventilada.

No use un gabinete completamente sellado al instalar el producto en exteriores.

- La temperatura interna del gabinete puede aumentar debido a la luz solar directa, lo que puede provocar incendios, descargas eléctricas o daños al producto.

No instale el producto en lugares donde se genere calor, como cerca de calefactores.

- El sobrecalentamiento puede provocar incendios o descargas eléctricas.

No instale en lugares húmedos.

- La humedad puede provocar descargas eléctricas o daños al producto.

No instale en lugares con interferencia electromagnética.

- Puede provocar descargas eléctricas o daños al producto.

Uso

No permita que líquidos como agua, bebidas o productos químicos entren en el producto.

- Puede provocar incendios, descargas eléctricas o daños al producto.

No use adaptadores de corriente o enchufes dañados ni tomacorrientes flojos.

- Si las conexiones son inestables, pueden provocar incendios o descargas eléctricas.

No doble ni rompa en exceso el cable de alimentación.

- Puede causar incendios o descargas eléctricas.

⚠ Precaución

Instalar

Lea este manual detenidamente antes de instalar el producto para garantizar una instalación segura y correcta.

Al conectar cables de alimentación y conectores, asegúrese de apagar la alimentación de todos los dispositivos antes de cablear y conectar.

- Los dispositivos pueden funcionar incorrectamente.

Antes de conectar la alimentación al producto, revise nuevamente el manual para asegurarse de que el cableado sea correcto y luego conecte la alimentación.

No instale el producto en lugares expuestos directamente a la luz solar o ultravioleta.

- Puede provocar daños, mal funcionamiento, decoloración o deformación del producto.

No deje cables de alimentación en pasillos.

- Puede provocar lesiones corporales o daños al producto.

No instale cerca de objetos magnéticos fuertes como imanes, televisores, monitores CRT o altavoces.

- El dispositivo puede funcionar incorrectamente.

Al instalar varios dispositivos, asegúrese de respetar la distancia mínima de separación.

- Puede afectar el rendimiento RF y BLE de otros dispositivos, provocando que funcionen incorrectamente.

Use un adaptador de corriente con aprobación IEC/EN 62368-1 y con capacidad superior al consumo de energía del dispositivo terminal. Se recomienda usar los adaptadores de corriente vendidos por Suprema.

- El uso de una fuente de alimentación inadecuada puede provocar el mal funcionamiento de los dispositivos.
- Consulte la sección Alimentación en las especificaciones del producto para conocer el consumo máximo de corriente.

Asegúrese de que el producto y Secure I/O 2, así como la cerradura eléctrica (dispositivo de bloqueo electrónico), utilicen fuentes de alimentación separadas.

- Los dispositivos pueden funcionar incorrectamente.

Uso

No deje caer el producto ni lo someta a golpes.

- El dispositivo puede funcionar incorrectamente.

Asegure que no se interrumpa el suministro eléctrico durante las actualizaciones de firmware del producto.

- El dispositivo puede funcionar incorrectamente.

Administre la contraseña para que otros no la conozcan y cámbiela regularmente.

- Esto puede provocar acceso no autorizado.

No presione los botones (panel táctil) del producto con fuerza ni use herramientas puntiagudas para hacerlo.

- El dispositivo puede funcionar incorrectamente.

Use el producto dentro de -20 °C a 50 °C y guárdelo a temperaturas adecuadas, ni demasiado bajas ni demasiado altas.

- El dispositivo puede funcionar incorrectamente.

Tenga cuidado al limpiar el producto.

- Limpie suavemente la superficie del producto con un paño limpio y seco.
- Si va a desinfectar el producto, humedezca un paño limpio con la cantidad adecuada de alcohol desinfectante y limpie suavemente la superficie del producto. Use alcohol desinfectante que contenga 70-75 % de alcohol isopropílico y un paño suave, limpio y sin pelusa.
- No aplique desinfectante directamente sobre el producto.

No utilice el producto para fines distintos a su uso previsto.

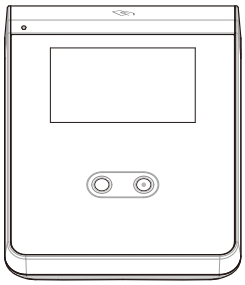
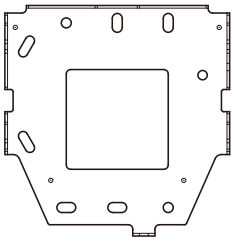
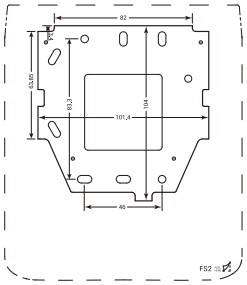
- El dispositivo puede funcionar incorrectamente.

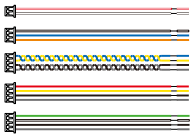
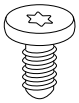
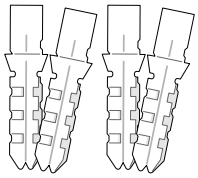
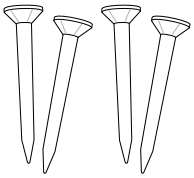
> **Batería RTC**
>
> Reemplazar por baterías no autorizadas o de tipo incorrecto puede representar un riesgo de explosión. Deseche las baterías conforme a las normativas locales o internacionales sobre residuos.

Primeros Pasos

Proporciona procedimientos iniciales para empezar con el dispositivo.

Componentes

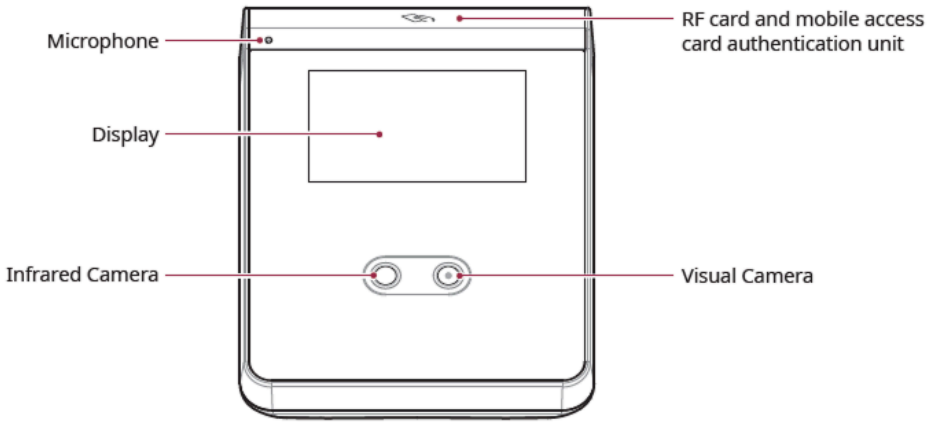
		
FaceStation 2	Soporte de pared	Plantilla de perforación

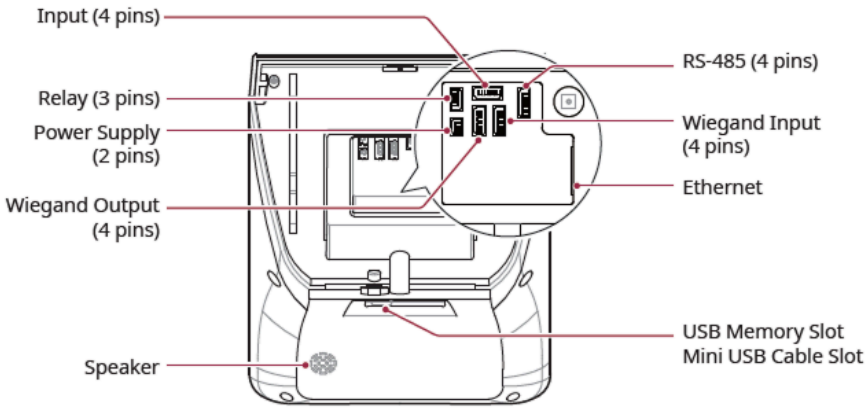
			
Cables de conexión	Diodo	Resistencia de 120 Ω	Tornillo de fijación del soporte (en forma de estrella)
			
Anclajes de PVC x4	Tornillos de fijación x4	Guía rápida	Guía de software de código abierto

Información

- Los componentes pueden variar según el entorno de instalación.
- Al ensamblar el producto con el soporte, puedes usar el tornillo de fijación del soporte incluido (en forma de estrella) en lugar del tornillo de fijación del producto para aumentar la seguridad.

Nombre y función de cada parte





- **Micrófono**: Transmite la voz del usuario cuando el interfono está conectado.
  - Cubrir u obstruir el micrófono puede interferir con la transmisión de la voz.
- **Pantalla**: Proporciona una interfaz de usuario para la operación.
- **Cámara infrarroja**: Captura la imagen facial infrarroja.
- **Cámara visual**: Captura una imagen facial real.
- **Unidad de autenticación de tarjeta RF y tarjeta de acceso móvil**: parte para escanear una tarjeta RFID o una tarjeta de acceso móvil para la entrada.
- **Altavoz**: Emite sonido.

- **Ranura para memoria USB**: Conecta la memoria USB.
  - La cámara térmica Suprema (TCM10-FS2) no se puede usar simultáneamente con la memoria USB.
- **Ranura para cable mini USB**: Compatibilidad disponible próximamente.
- **Entrada (4 pines)**: Conecta el cable de entrada.
- **RS-485 (4 pines)**: Conecta el cable RS-485.
- **Relé (3 pines)**: Conecta el cable del relé.
- **Alimentación (2 pines)**: Conecta el cable de alimentación.
- **Ethernet**: Conecta el cable Ethernet.
- **Entrada Wiegand (4 pines)**: Conecta el cable de entrada Wiegand.
- **Salida Wiegand (4 pines)**: Conecta el cable de salida Wiegand.

Cables y conectores

Alimentación



Pin	Nombre	Color
1	PWR +VDC	Rojo (franja blanca)
2	PWR GND	Negro (franja blanca)

Relé



Pin	Nombre	Color
1	RLY NO	Blanco
2	RLY COM	Azul
3	RLY NC	Naranja

RS-485



Pin	Nombre	Color
1	485 TRXP	Azul
2	485 TRXN	Amarillo
3	485 GND	Negro
4	SH GND	Gris

Entrada



Pin	Nombre	Color
1	INPUT0	Rojo
2	INPUT1	Amarillo
3	INPUT GND	Negro
4	SH GND	Gris

Entrada y salida Wiegand



Pin	Nombre	Color
1	WG D0	Verde
2	WG D1	Blanco
3	WG GND	Negro
4	SH GND	Gris

Método correcto de enrolamiento y autenticación facial

Precauciones para enrolar rostros

- Mantén una distancia de 40 a 80 cm entre el dispositivo y tu rostro al enrolar un rostro.
- No cambies tu expresión facial.
- No uses mascarillas, sombreros ni parches para los ojos.
- No enroles un rostro con mascarilla. Podría aumentar la tasa de aceptación errónea (FAR) si se enrolan rostros con y sin mascarilla.
- No inclines la cabeza hacia arriba ni hacia abajo.
- No uses maquillaje pesado.
- No cierres los ojos.
- Asegúrate de que ambos hombros aparezcan correctamente en la pantalla.
- Permanece quieto y enrola tu rostro mirando fijamente la pantalla.
- Asegúrate de que no aparezcan dos rostros en la pantalla. Enrola a una persona a la vez.
- Si no sigues las instrucciones en pantalla, el enrolamiento facial podría tardar más o fallar.

Precauciones para autenticar un rostro

- Asegúrese de que el rostro aparezca en el centro de la pantalla del dispositivo. Cuando se muestre la guía, siga las instrucciones en pantalla para autenticar el rostro.
- Si parte del rostro está cubierta con un sombrero, mascarilla, parche ocular o gafas de sol, la autenticación puede fallar.

No cubra el rostro; permita que el dispositivo reconozca tanto las cejas como el rostro.

- Autentique a una distancia de 40~80 cm del dispositivo.
- Asegúrate de que ambos hombros aparezcan correctamente en la pantalla. La autenticación puede fallar si los hombros no están a la misma altura. Permanezca quieto y luego autentique el rostro.

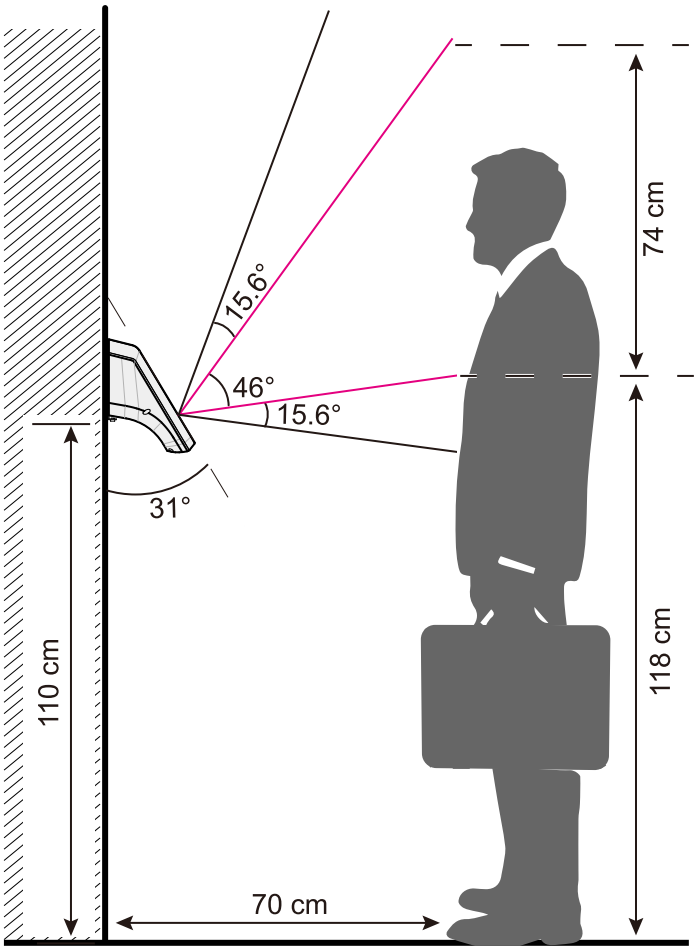
Instalación

Ofrece los procedimientos completos de instalación y ejemplos de conexión necesarios para el dispositivo.

Fijar el soporte y el producto

Soporte general

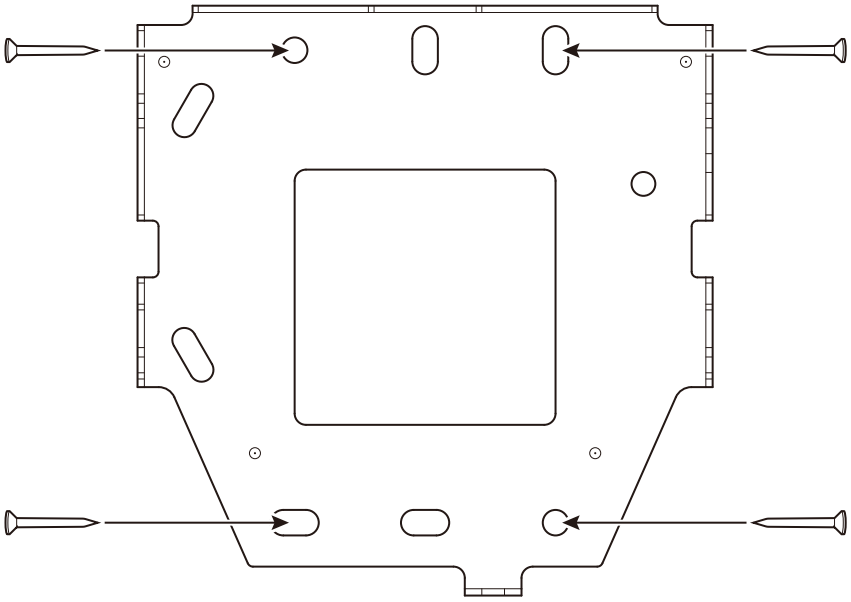
1. Determine la posición correcta para instalar el soporte usando la plantilla de perforación proporcionada.



Información

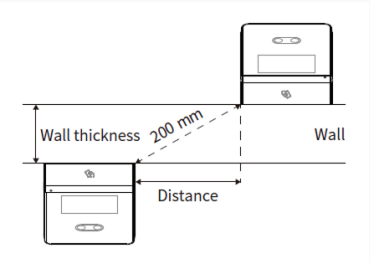
- La altura óptima para instalar el dispositivo es de 110 cm.
- Instale el dispositivo donde no reciba luz solar directa ni luz UV.
- Ajuste la posición de instalación para que el rostro no esté expuesto a la luz solar directa cuando el usuario intente autenticarse.

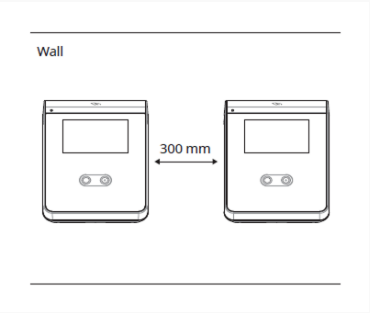
2. Asegura firmemente el soporte con los tornillos de fijación en el lugar donde se montará el producto.



Información

- Si instalas el producto en una pared de concreto, perfora un agujero, inserta un anclaje de PVC y sujétalo con un tornillo de fijación.
- Para evitar interferencias de RF, se debe mantener una distancia mínima de separación.

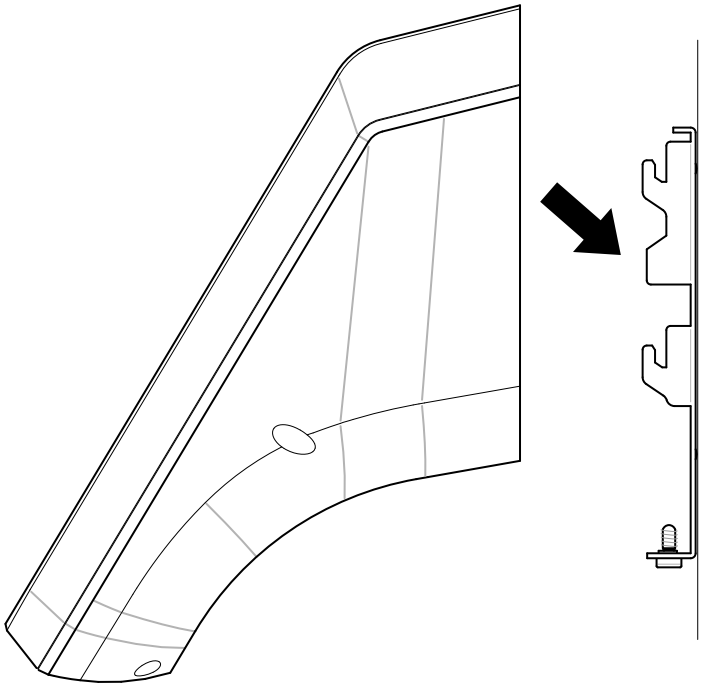




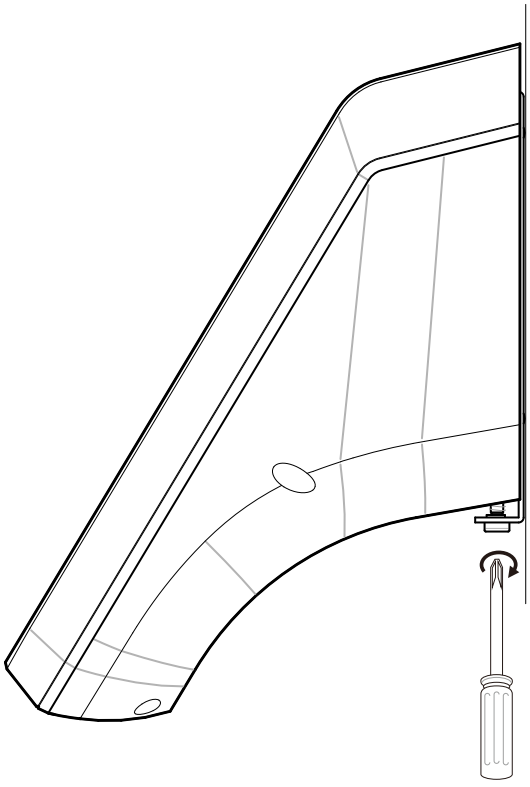
Espesor de pared	Distancia
100 mm	283 mm
120 mm	275 mm
150 mm	260 mm

- Al utilizar una credencial de acceso móvil, instala los dispositivos manteniendo una distancia mínima de 1 m entre ellos para evitar interferencias BLE.

3. Monta el producto en el soporte fijado.



4. Gira los tornillos de fijación para ensamblar el producto con el soporte.



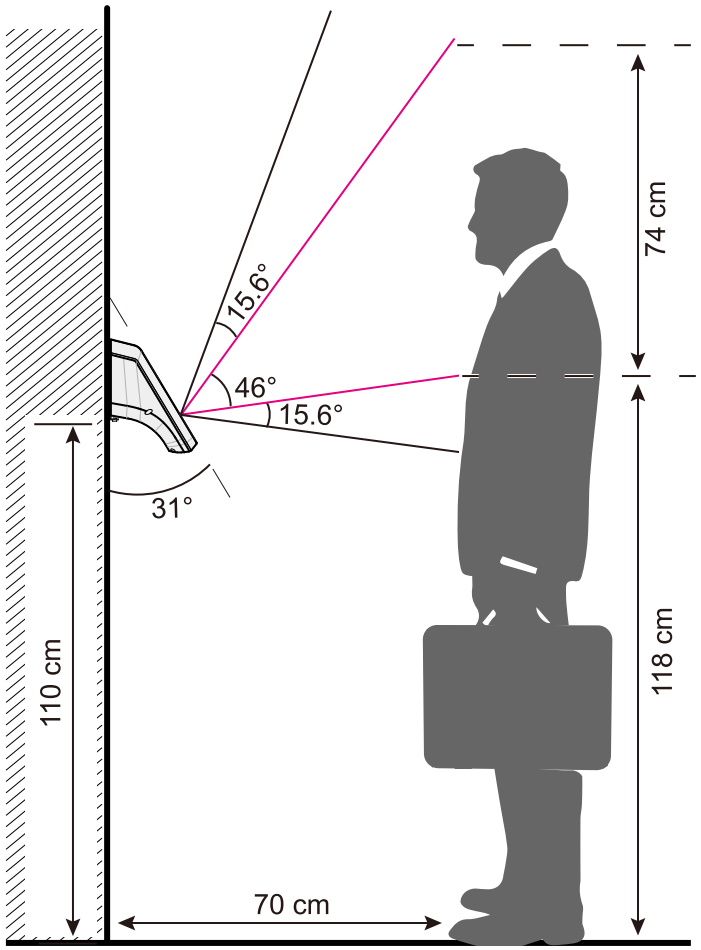
Información

Al ensamblar el producto con el soporte, puedes usar el tornillo de fijación del soporte incluido (en forma de estrella) en lugar del tornillo de fijación del producto para aumentar la seguridad.

Soporte inclinable

Use el soporte inclinable dedicado para ajustar el ángulo de autenticación según el entorno de instalación. El soporte inclinable se vende por separado.

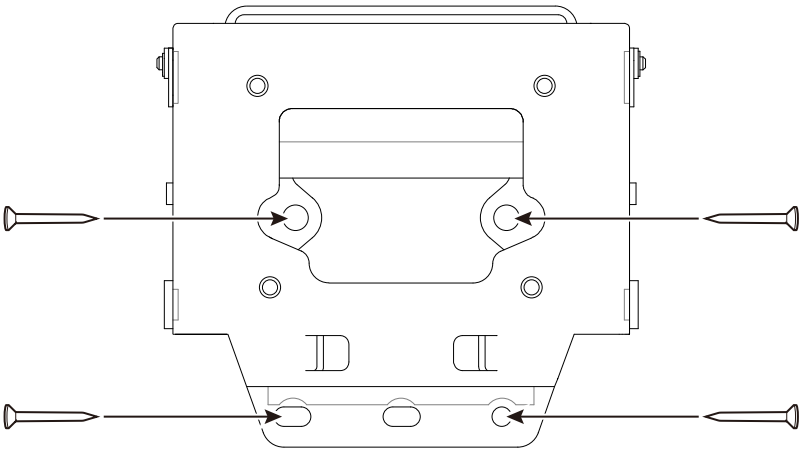
1. Determine la posición correcta para instalar el soporte usando la plantilla de perforación proporcionada.



Información

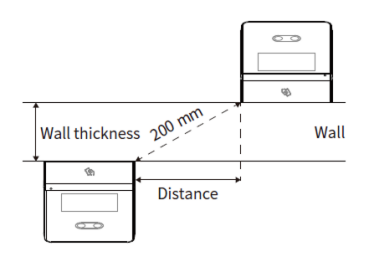
- La altura óptima para instalar el dispositivo es de 110 cm.
- Instale el dispositivo donde no reciba luz solar directa ni luz UV.
- Ajuste la posición de instalación para que el rostro no esté expuesto a la luz solar directa cuando el usuario intente autenticarse.

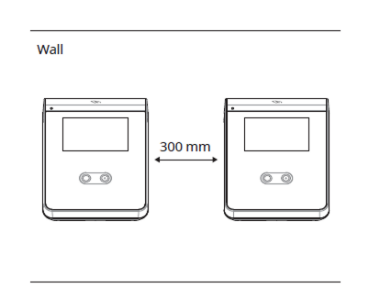
2. Asegure firmemente el soporte de inclinación al lugar de instalación (pared) usando los tornillos de fijación para el soporte de inclinación.



Información

- Si instalas el producto en una pared de concreto, perfora un agujero, inserta un anclaje de PVC y sujétalo con un tornillo de fijación.
- Para evitar interferencias de RF, se debe mantener una distancia mínima de separación.

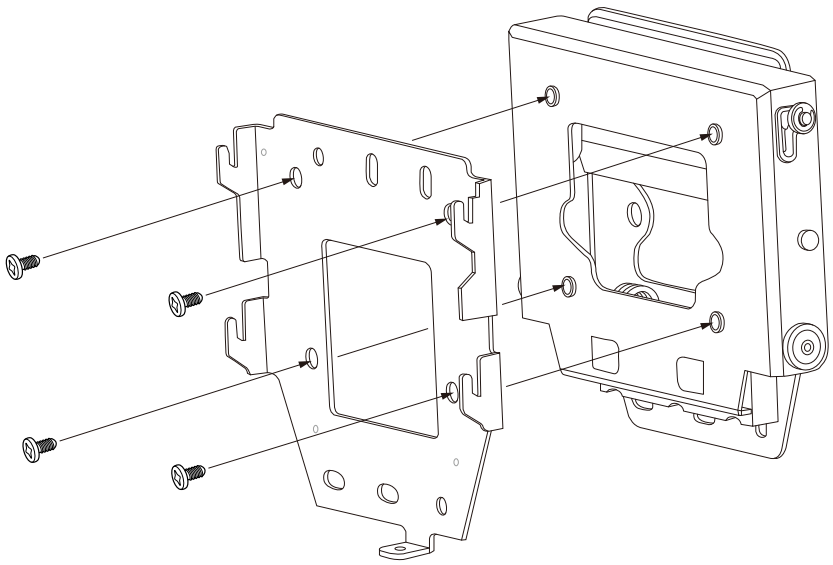




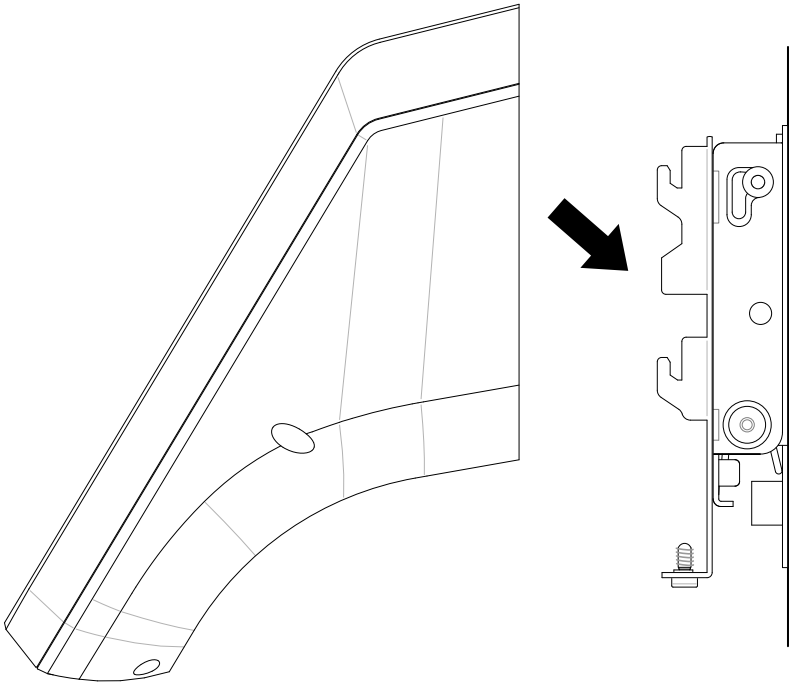
Espesor de pared	Distancia
100 mm	283 mm
120 mm	275 mm
150 mm	260 mm

- Al utilizar una credencial de acceso móvil, instala los dispositivos manteniendo una distancia mínima de 1 m entre ellos para evitar interferencias BLE.

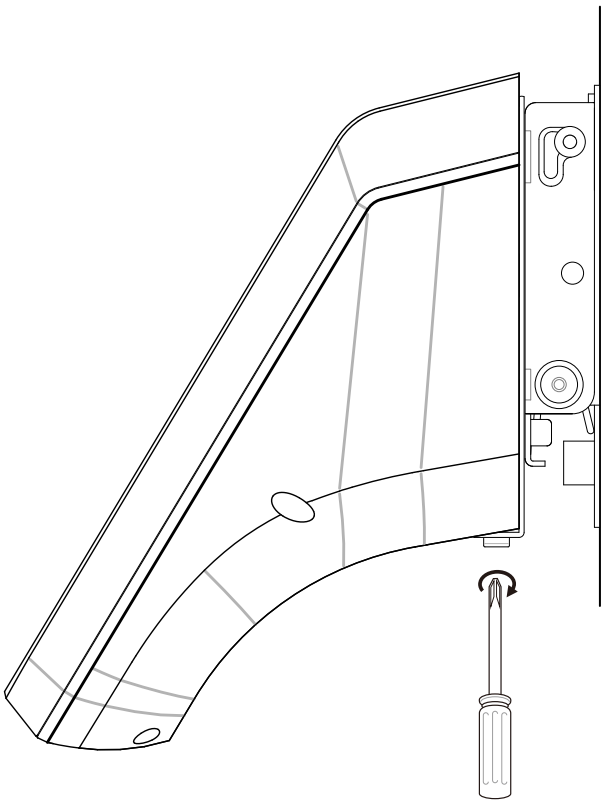
3. Fije firmemente el soporte de montaje en pared encima del soporte inclinable.



4. Monte el producto en el soporte de montaje en pared fijado.



5. Apriete los tornillos de fijación del producto para ensamblarlo con el soporte de montaje en pared.

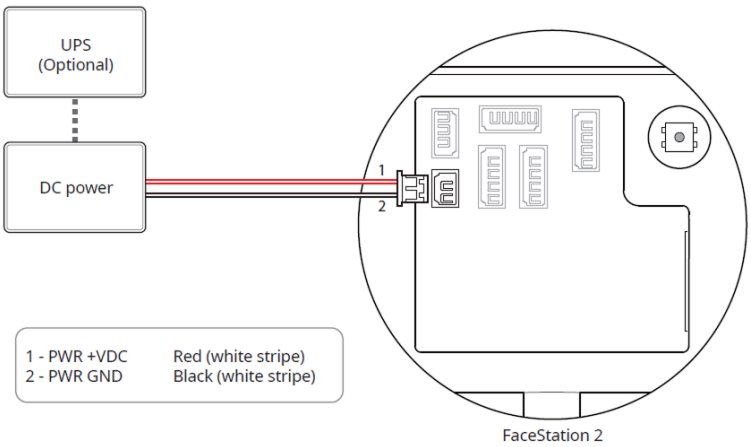


Información

Al ensamblar el producto con el soporte, puedes usar el tornillo de fijación del soporte incluido (en forma de estrella) en lugar del tornillo de fijación del producto para aumentar la seguridad.

6. Ajuste el soporte inclinable al ángulo deseado.

Conexión de la fuente de alimentación



Precaución

- Use un adaptador de alimentación aprobado por IEC/EN 62368-1 que admita un consumo de energía mayor que el del producto. Si desea conectar y usar otro dispositivo al adaptador de alimentación, utilice un adaptador con una capacidad de corriente igual o mayor que el consumo total requerido por el terminal y el otro dispositivo.
  - Consulte la sección Alimentación en las especificaciones del producto para conocer el consumo máximo de corriente.
- Use una fuente de alimentación independiente para Secure I/O 2, la cerradura eléctrica y el producto, respectivamente. Si conecta y usa la misma fuente de alimentación para estos dispositivos, estos pueden funcionar incorrectamente.
- Al conectar la alimentación, tenga en cuenta la distancia entre el dispositivo y la fuente de alimentación. Conecte el dispositivo lo más cerca posible de la fuente de alimentación para que la longitud del cable sea mínima. Si las conexiones de los cables se realizan de forma incorrecta, el dispositivo puede funcionar incorrectamente. Se recomienda usar un cable de 16 AWG o 18 AWG si el producto está lejos de la fuente de alimentación. La distancia de conexión puede variar según el estándar del cable utilizado y el entorno de instalación.

Estándar de cable	Máx. longitud extendida
16 AWG	150 m
18 AWG	136 m
20 AWG	90 m

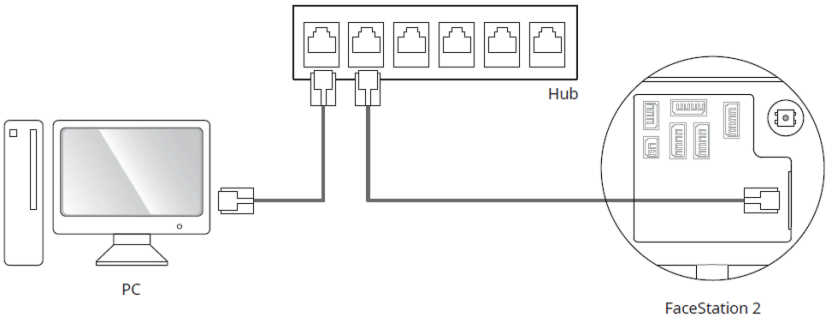
- NO extienda la longitud del cable de alimentación al usar el adaptador de alimentación.
- NO utilice CAT5 UTP de 2 hilos para la alimentación.

Conexión de red

TCP/IP

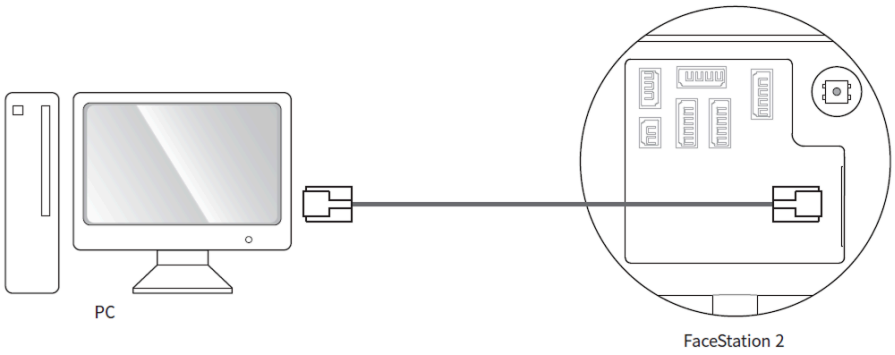
Conexión LAN (conexión a un concentrador)

Conecte el producto a un concentrador con un cable CAT-5 estándar.



Conexión LAN (conexión directa a una PC)

Este dispositivo cuenta con función automática MDI/MDIX, por lo que puede conectarse directamente a una PC utilizando un cable CAT-5 recto estándar o un cable cruzado.



Información

Consulte la siguiente información al utilizar un conmutador de red gigabit.

- Utilice un cable CAT-5e UTP (unidad de par trenzado sin blindaje).
- Utilice los 4 pares (8 hilos) del cable para la conexión de red.
- NO utilice el par de cables para otro propósito.

Puertos y servicios de red

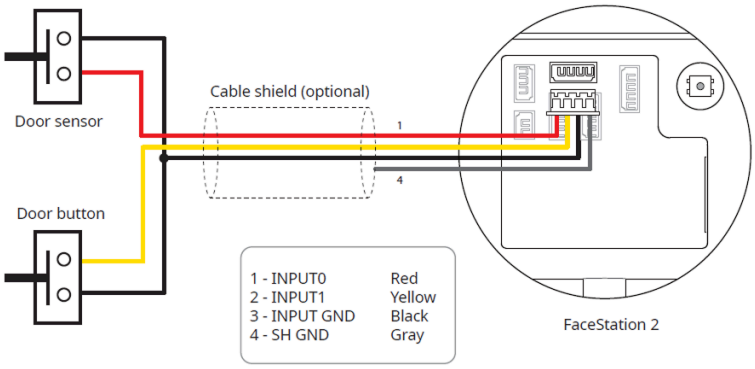
Este dispositivo usa los siguientes puertos para la comunicación en red y el funcionamiento estable del servicio.

Protocolo	Descripción del servicio
TCP	Se utiliza para los servicios de comunicación entre el servidor y el dispositivo, así como para el servicio de cambio de estado operativo del dispositivo.
UDP	Se usa para el servicio de detección del dispositivo, que permite buscar dispositivos en la red.

Información

Estos puertos se utilizan para proporcionar las funciones normales de red del producto. Al configurar reglas de firewall o ajustes de seguridad de red, permite el uso de estos puertos.

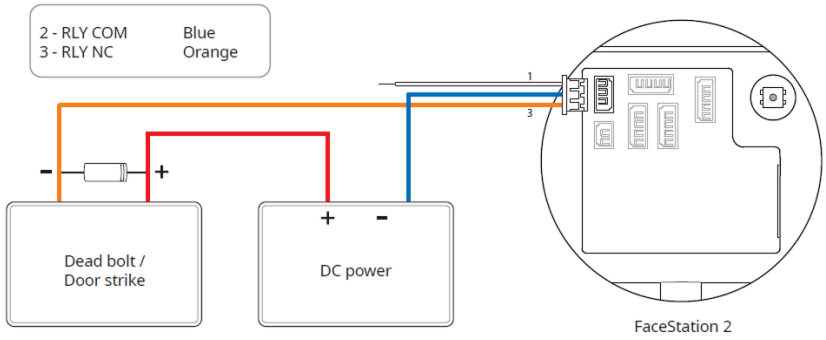
Conexión de entrada



Conexión del relé

Cerradura fail safe

Para utilizar la cerradura Fail Safe, conecte el relé N/C como se muestra en la figura a continuación. Normalmente circula corriente a través del relé de la cerradura Fail Safe. Cuando se activa el relé y se bloquea el flujo de corriente, la puerta se abrirá. Si se corta la alimentación del producto debido a un fallo de energía o a un factor externo, la puerta se abrirá.



Precaución

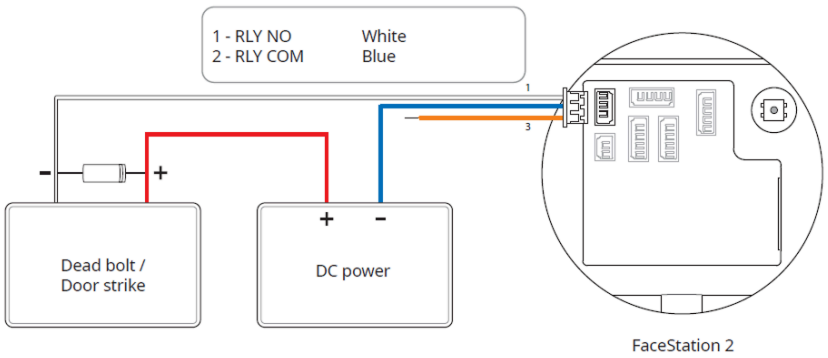
- Instale un diodo en ambos extremos del cable de la cerradura, como se muestra en la figura, para proteger el relé de la corriente inversa que se produce cuando la cerradura funciona.
- Utilice una fuente de alimentación independiente para el producto y la cerradura.
- Los lectores inteligentes independientes de Suprema contienen relés internos que pueden bloquear/desbloquear puertas directamente sin controladores externos para mayor comodidad. Sin embargo, para aplicaciones de control de acceso que requieren seguridad, NO se recomienda utilizar el relé interno de un lector a fin de evitar manipulaciones que puedan desbloquear la puerta. Para estas aplicaciones, se recomienda encarecidamente usar una unidad de relé independiente para el control de la cerradura, como Secure I/O 2, DM-20 o CoreStation de Suprema, instaladas en el lado seguro de la puerta.

Información

Preste atención a la dirección de instalación del diodo. Instale el diodo cerca de la cerradura.

Cerradura fail secure

Conecte el relé N/O como se muestra en la figura para usar la cerradura fail secure. Normalmente no circula corriente a través del relé para la cerradura Fail Secure. Cuando el relé activa el flujo de corriente, la puerta se abrirá. Si el suministro eléctrico del producto se interrumpe debido a un corte de energía o a un factor externo, la puerta se bloqueará.



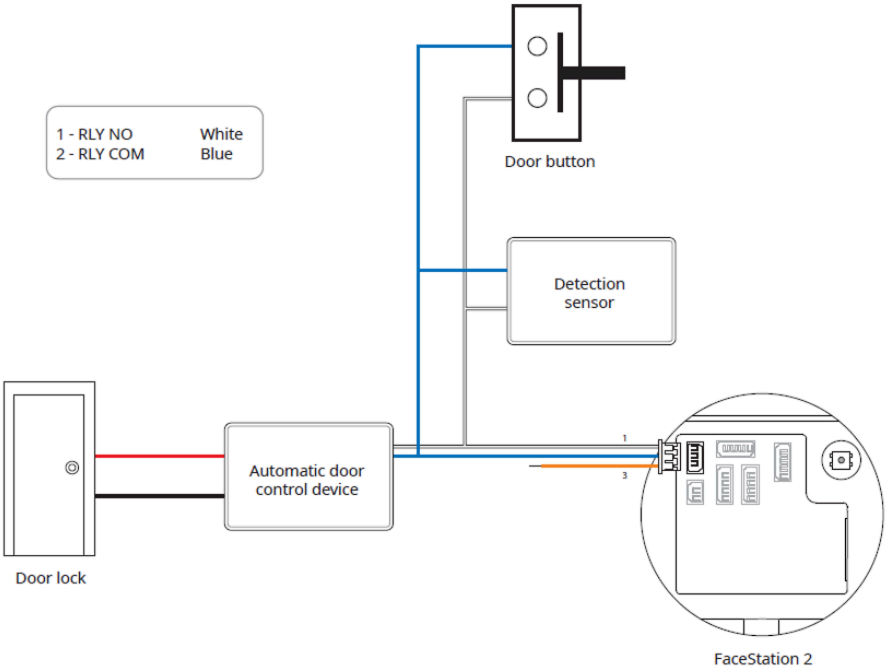
Precaución

- Instale un diodo en ambos extremos del cable de la cerradura, como se muestra en la figura, para proteger el relé de la corriente inversa que se produce cuando la cerradura funciona.
- Utilice una fuente de alimentación independiente para el producto y la cerradura.
- Los lectores inteligentes independientes de Suprema contienen relés internos que pueden bloquear/desbloquear puertas directamente sin controladores externos para mayor comodidad. Sin embargo, para aplicaciones de control de acceso que requieren seguridad, NO se recomienda utilizar el relé interno de un lector a fin de evitar manipulaciones que puedan desbloquear la puerta. Para estas aplicaciones, se recomienda encarecidamente usar una unidad de relé independiente para el control de la cerradura, como Secure I/O 2, DM-20 o CoreStation de Suprema, instaladas en el lado seguro de la puerta.

Información

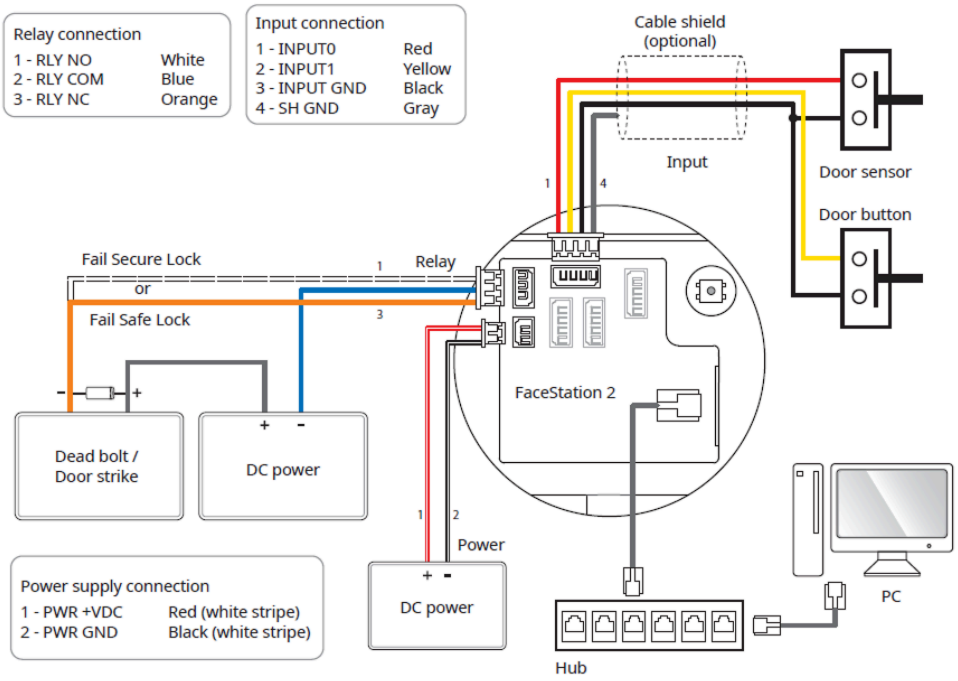
Preste atención a la dirección de instalación del diodo. Instale el diodo cerca de la cerradura.

Conexión de puerta automática



Conectar como independiente

El producto puede conectarse directamente a la cerradura, el botón y el sensor de puerta sin necesidad de conectar un dispositivo de E/S adicional.



Precaución

Los lectores inteligentes independientes de Suprema contienen relés internos que pueden bloquear/desbloquear puertas directamente sin controladores externos para mayor comodidad. Sin embargo, para aplicaciones de control de acceso que requieren seguridad, NO se recomienda utilizar el relé interno de un lector a fin de evitar manipulaciones que puedan desbloquear la puerta. Para estas aplicaciones, se recomienda encarecidamente usar una unidad de relé independiente para el control de la cerradura, como Secure I/O 2, DM-20 o CoreStation de Suprema, instaladas en el lado seguro de la puerta.

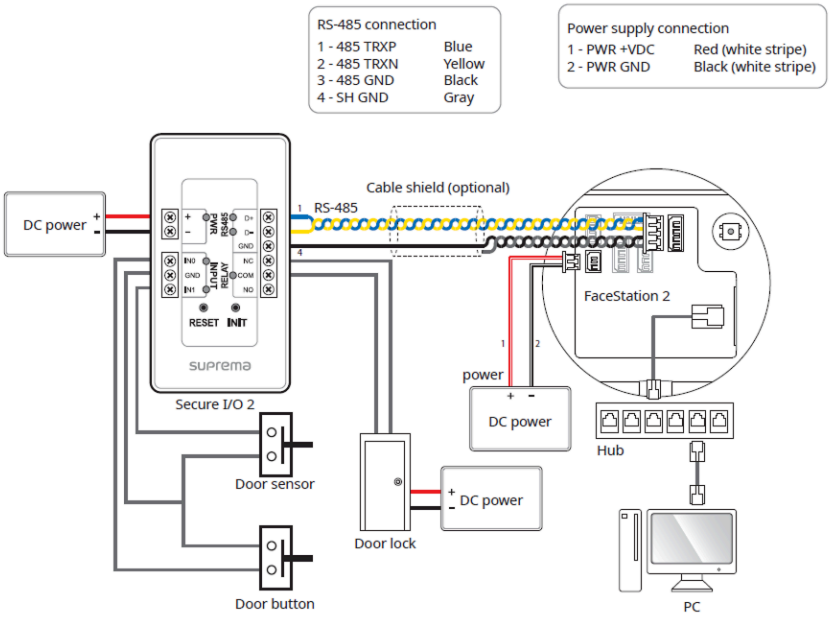
Información

- El dispositivo puede utilizarse como controlador de múltiples puertas con los dispositivos esclavos mediante el cable RS-485. Los dispositivos esclavos se utilizan como lectores ficticios y la autenticación se realiza en el dispositivo maestro.
- Si un dispositivo de autenticación por huella digital está configurado como esclavo en FaceStation 2, no se puede agregar otro FaceStation 2 como esclavo.
- Si el dispositivo de autenticación por huella digital es el dispositivo maestro, no se puede agregar FaceStation 2 como dispositivo esclavo.
- Cuando se conecta FaceStation 2 como dispositivo esclavo mientras FaceStation 2 es el dispositivo maestro, solo se puede agregar un FaceStation 2 como dispositivo esclavo.
- Cuando FaceStation 2 es el dispositivo maestro y otro FaceStation 2 se conecta a él como esclavo, se puede conectar adicionalmente un Secure I/O 2 y un DM-20 cada uno.
- Cuando FaceStation 2 es el dispositivo maestro y otro FaceStation 2 está conectado a él como esclavo, no se pueden conectar OM-120 adicionales.
- El número máximo de dispositivos esclavos que se pueden conectar varía según el método de autenticación, el número de usuarios y el número de dispositivos. Ten en cuenta también que la cantidad de dispositivos esclavos afecta el rendimiento de autenticación.
- Conecte hasta 31 dispositivos esclavos a un dispositivo maestro. El ancho de banda de RS-485 permite conectar hasta 7 dispositivos de autenticación por huella.
- Para más información, comuníquese con el Equipo de soporte técnico de Suprema.

Conectar Secure I/O 2

Secure I/O 2 es un dispositivo de E/S que se puede conectar al producto con el cable RS-485. La seguridad puede mantenerse incluso si se pierde la conexión entre el producto y Secure I/O 2 o si el suministro de energía al producto se interrumpe debido a factores externos.

- Utilice un par trenzado AWG24 con una longitud máxima de 1.2 km para el cable RS-485.
- Se recomienda usar cables RS-485 con una impedancia característica de 120 Ω.
- Si se conecta mediante una cadena en serie RS-485, conecte la resistencia de terminación (120 Ω) en ambos extremos de la conexión en cadena. Si se conecta en la línea media, el nivel de señal se reducirá y el rendimiento de comunicación se verá afectado. Asegúrese de conectarlas en ambos extremos de la conexión en cadena.

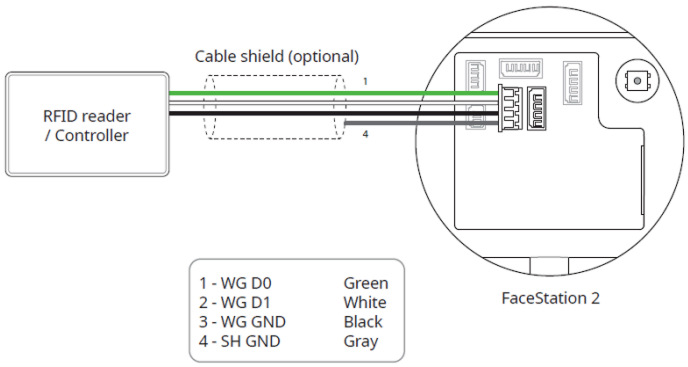


Información

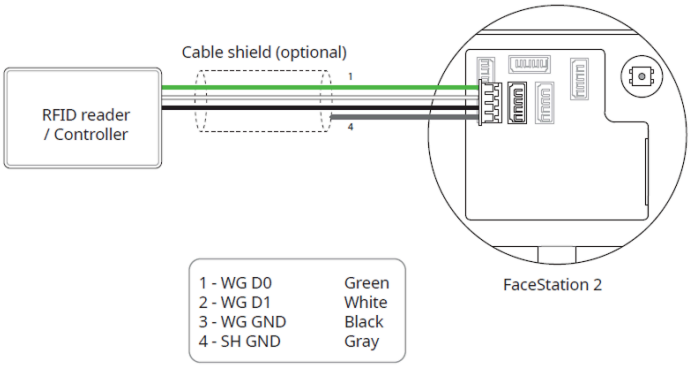
- El dispositivo puede utilizarse como controlador de múltiples puertas con los dispositivos esclavos mediante el cable RS-485. Los dispositivos esclavos se utilizan como lectores ficticios y la autenticación se realiza en el dispositivo maestro.
- Si un dispositivo de autenticación por huella digital está configurado como esclavo en FaceStation 2, no se puede agregar otro FaceStation 2 como esclavo.
- Si el dispositivo de autenticación por huella digital es el dispositivo maestro, no se puede agregar FaceStation 2 como dispositivo esclavo.
- Cuando se conecta FaceStation 2 como dispositivo esclavo mientras FaceStation 2 es el dispositivo maestro, solo se puede agregar un FaceStation 2 como dispositivo esclavo.
- Cuando FaceStation 2 es el dispositivo maestro y otro FaceStation 2 se conecta a él como esclavo, se puede conectar adicionalmente un Secure I/O 2 y un DM-20 cada uno.
- Cuando FaceStation 2 es el dispositivo maestro y otro FaceStation 2 está conectado a él como esclavo, no se pueden conectar OM-120 adicionales.
- El número máximo de dispositivos esclavos que se pueden conectar varía según el método de autenticación, el número de usuarios y el número de dispositivos. Ten en cuenta también que la cantidad de dispositivos esclavos afecta el rendimiento de autenticación.
- Conecte hasta 31 dispositivos esclavos a un dispositivo maestro. El ancho de banda de RS-485 permite conectar hasta 7 dispositivos de autenticación por huella.
- Para más información, comuníquese con el Equipo de soporte técnico de Suprema.

Conexión Wiegand

Se usa como dispositivo de entrada Wiegand.



Se usa como dispositivo de salida Wiegand.



Cómo Usar

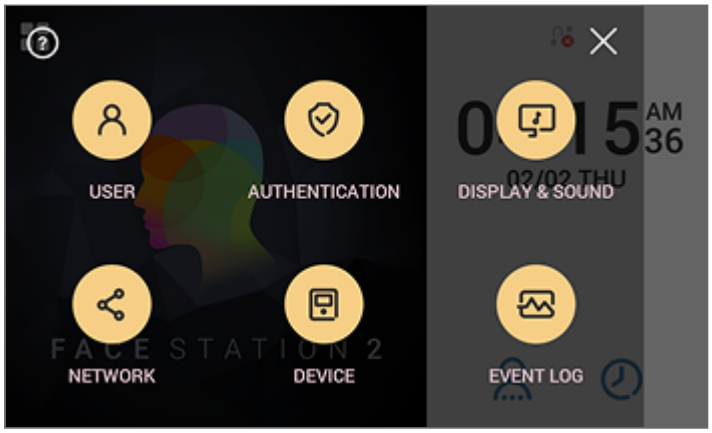
Proporciona orientación sobre cómo utilizar las funciones principales del dispositivo de manera efectiva.

Menú de Administrador

Proporciona orientación sobre los menús principales y las funciones accesibles con privilegios de administrador.

Menú completo

1. Haz clic en y autentícate con privilegios de administrador.
2. Selecciona el menú deseado.



> **Información**
>
> Si no se especifica un administrador, al hacer clic en aparece la pantalla del menú.

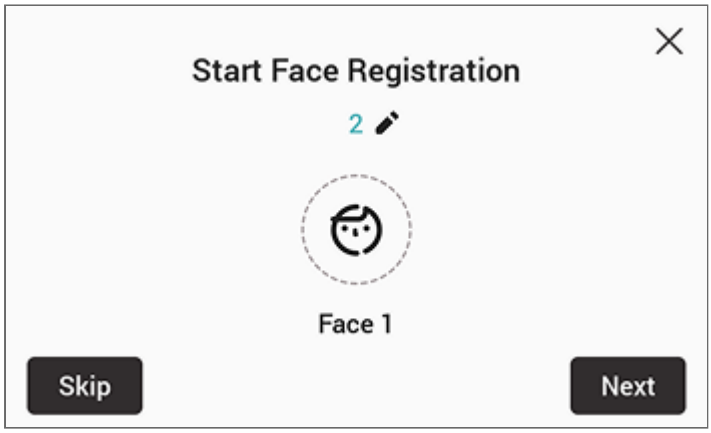
Usuario

Describe cómo registrar, editar, eliminar y gestionar usuarios.

Registrar información de usuario

Registre información de usuario que incluya datos de autenticación biométrica.

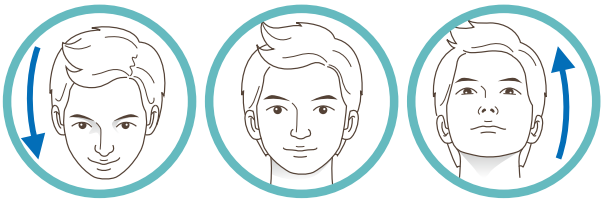
1. Haz clic en y autentícate con privilegios de administrador.
2. Haga clic en **USER** → . El asistente de registro de rostro se iniciará.



3. Haz clic en **Next** para continuar con el asistente de registro de rostro. Para omitir, presiona **Skip** y verifica el paso **5**.
4. Si presionaste **Next**, sigue las instrucciones en pantalla para registrar tu rostro. El registro de rostro consta de un total de 3 pasos.
    1. Registro de rostro frontal



    2. Mueve el rostro arriba y abajo



    3. Mueve el rostro a la izquierda y a la derecha

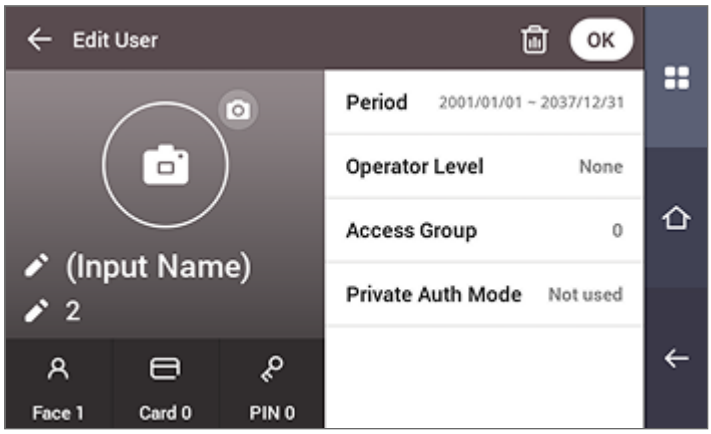


El uso del asistente de registro de rostro solo registrará el rostro del usuario. Una vez completado el registro de rostro, selecciona al usuario para establecer información adicional.

Ten en cuenta lo siguiente al registrar tu rostro.

- Mantén una distancia de 40 a 80 cm entre el dispositivo y tu rostro al enrolar un rostro.
- No cambies tu expresión facial.
- No uses mascarillas, sombreros ni parches para los ojos.
- No enroles un rostro con mascarilla. Podría aumentar la tasa de aceptación errónea (FAR) si se enrolan rostros con y sin mascarilla.
- No inclines la cabeza hacia arriba ni hacia abajo.
- No uses maquillaje pesado.
- No cierres los ojos.
- Asegúrate de que ambos hombros aparezcan correctamente en la pantalla.
- Permanece quieto y enrola tu rostro mirando fijamente la pantalla.
- Asegúrate de que no aparezcan dos rostros en la pantalla. Enrola a una persona a la vez.
- Si no sigues las instrucciones en pantalla, el enrolamiento facial podría tardar más o fallar.

5. Si presionaste **Skip**, selecciona el elemento deseado y configúralo.



- : Permite registrar una foto de usuario.
- **Nombre**: Introduzca el nombre de usuario.
- **ID**: Ingrese un número entre 1 y 4294967295 para registrar un ID de usuario. Si **User ID Type** está configurado en **Alphanumeric**, puede usar una combinación de caracteres alfanuméricos y los símbolos `_` `-` como ID, con un máximo de 32 caracteres.
- **Face**: Registre un rostro para la autenticación del usuario. Presiona y sigue las instrucciones en pantalla para registrar tu rostro. Haga clic en para inscribir más rostros.
- **Card**: Inscriba una tarjeta para la autenticación del usuario. Presiona y escanea la tarjeta para asignarla al usuario en la sección de autenticación de tarjeta RF. Haga clic en para inscribir más tarjetas.
- **PIN**: Ingrese el PIN que desea usar. Ingresa el PIN que deseas usar, confírmalo ingresándolo nuevamente y presiona **OK**. Para evitar filtraciones, ingrese un PIN de 4 a 16 dígitos.
- **Operator Level**: Seleccione los permisos que desea asignar al usuario.

> **Información**
>
> Los menús disponibles varían según el nivel de usuario establecido.
>
> – **None**: Este es un nivel de usuario general y el menú no está disponible.
>
> – **Administrator**: Puede usar todos los menús.
>
> – **Configuration**: Puede usar los menús **AUTHENTICATION**, **DISPLAY & SOUND**, **DEVICE**, **NETWORK**, **EVENT LOG**.
>
> – **User Management**: Puede usar los menús **USER**, **EVENT LOG**.

- **Face Group**: Permite seleccionar un grupo para el rostro del usuario. Los grupos de rostro solo se pueden usar si **Group Matching** está habilitado y únicamente se pueden registrar en BioStar X.
- **Access Group**: Permite verificar el grupo de acceso del usuario. Los grupos de acceso solo se pueden registrar en BioStar X.
- **Private Auth Mode**: Permite configurar un modo de autenticación personal. El uso del modo de autenticación personal permite combinar métodos de autenticación, incluida la autenticación facial, para cada usuario. De lo contrario, utilice el modo de autenticación básico del dispositivo.

6. Presiona **OK** para completar el registro de la información del usuario.

Modificar información de usuario

El gestor de usuarios o el administrador pueden modificar la información de usuario registrada. Se puede añadir una tarjeta o rostro y modificar el PIN y el nivel.

1. Haz clic en y autentícate con privilegios de administrador.
2. Haga clic en **USER** → .
3. Seleccione los términos de búsqueda. Busque usuarios utilizando **All**, **User ID**, **Name**, **Face**, **Card**.
4. Seleccione el usuario que desea modificar.
5. Modifique la información consultando Registrar información de usuario y presione **OK**.
   - Para eliminar un usuario, seleccione y luego presione **OK**.

> **Información**
>
> **Access Group** se puede registrar en BioStar X. Para obtener información detallada sobre cómo registrar un Grupo de Acceso, consulte la Guía del Administrador de BioStar X.

Eliminar todos los usuarios

Elimine todos los usuarios registrados a la vez.

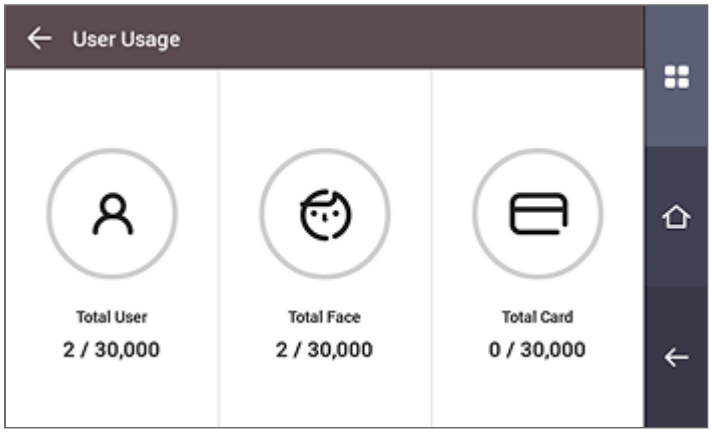
1. Haz clic en y autentícate con privilegios de administrador.
2. Selecciona **USER** → .

3. Seleccione **Delete All** para verificar y luego presione **OK**.
4. Para eliminar a todos los usuarios, presione **OK**.

Ver uso de usuarios

Puede ver de un vistazo la cantidad de usuarios, rostros y tarjetas registrados.

1. Haz clic en y autentícate con privilegios de administrador.
2. Haga clic en **USER** → . La información de uso de usuarios aparece.



Autenticación

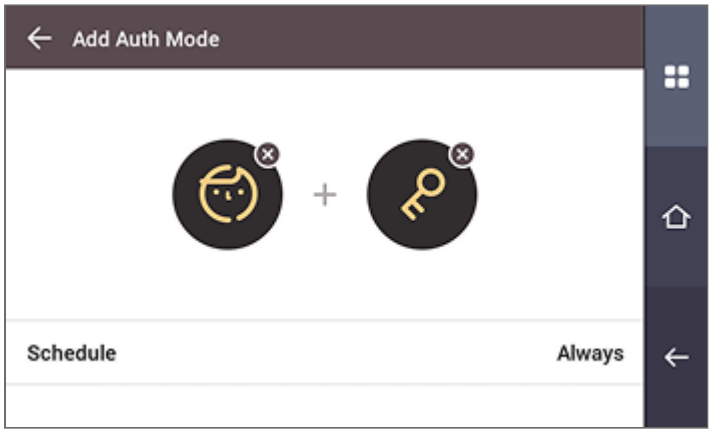
Describe los métodos de autenticación compatibles y los procedimientos de autenticación.

Modo de autenticación

Configura el modo de autenticación. Puedes combinar **Face**, **PIN**, **Card** y **ID** para el modo de autenticación, y también puedes configurar los horarios para cada modo de autenticación.

Registrar modo de autenticación

1. Haz clic en y autentícate con privilegios de administrador.
2. Presione **AUTHENTICATION** → **Auth Mode**.
3. Selecciona .
4. Presione para ver las credenciales que se pueden agregar en la pantalla. Selecciona las credenciales que deseas añadir. Selecciona las credenciales que deseas añadir.



5. Después de configurar el modo de autenticación deseado, configura **Schedule**.

Categoría	Descripción
Rostro	- : Este modo usa solo autenticación facial. - + : Este modo primero autentica con rostro y luego ingresa el PIN.
tarjeta	- : Este modo usa solo autenticación con tarjeta. - + : Este modo autentica con tarjeta y luego con rostro. - + : Este modo autentica con tarjeta y luego ingresa el PIN. - + / : Este modo autentica con tarjeta y luego con rostro o ingresa el PIN. - + + : Este modo usa autenticación facial y entrada de PIN después de autenticar con tarjeta.
ID	- + : Este modo ingresa el ID y luego autentica con rostro. - + : Este modo ingresa el ID y luego ingresa el PIN. - + / : Este modo ingresa el ID y luego autentica con rostro o ingresa el PIN. - + + : Este modo usa autenticación facial y entrada de PIN después de ingresar el ID.

Información

- **Schedule** se puede configurar en BioStar X. Si no se establece un horario, solo se puede seleccionar **Always**.
- Para más información sobre la configuración de **Schedule**, consulte la Guía del administrador de BioStar X.

6. Pulsa **OK** para guardar la configuración.

Modificar modo de autenticación

1. Haz clic en y autentícate con privilegios de administrador.
2. Presione **AUTHENTICATION** → **Auth Mode**.

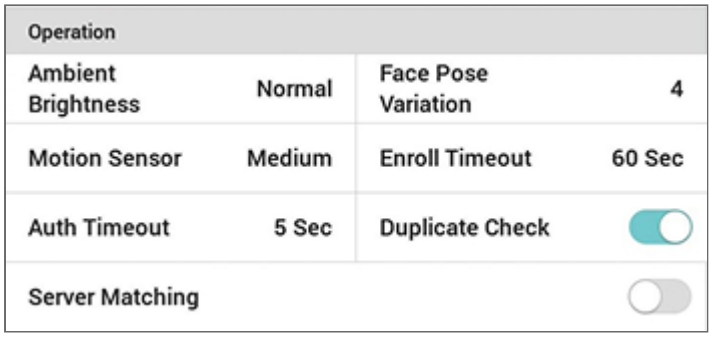
3. Selecciona el modo de autenticación que deseas modificar.
4. Modifica el modo de autenticación consultando Registrar modo de autenticación y pulsa **OK**.

Eliminar modo de autenticación

1. Haz clic en y autentícate con privilegios de administrador.
2. Presione **AUTHENTICATION** → **Auth Mode**.
3. Pulsa y selecciona el modo de autenticación que deseas eliminar. Es posible seleccionar varias opciones.
4. Pulsa **OK** para eliminar el elemento seleccionado.

Operación

1. Haz clic en y autentícate con privilegios de administrador.
2. Después de pulsar **AUTHENTICATION**, cambia el elemento deseado en **Operation**.



- **Ambient Brightness**: Ajusta la intensidad del LED IR detectando el brillo ambiental. Cambie los ajustes según el entorno de instalación.
- **Motion Sensor**: Establece la sensibilidad para detectar movimiento alrededor del dispositivo. Cuando **Motion Sensor** está ajustado en **Off**, toque la pantalla para autenticar el rostro.
- **Auth Timeout**: Si la autenticación no se completa dentro del tiempo establecido, la autenticación falla.
- **Server Matching**: Cuando se configura la autenticación en servidor, el dispositivo no realiza la autenticación del usuario; BioStar X realiza la autenticación del usuario. Se puede usar cuando el dispositivo tiene demasiada información de usuarios o cuando el dispositivo está instalado en exteriores.

> **Información**
>
> – **Server Matching** solo puede usar tarjetas e ID.
>
> – Si usa **Server Matching**, habilite la coincidencia con el servidor tanto en el dispositivo como en BioStar X. Para obtener información detallada sobre la configuración de la coincidencia con servidor en BioStar X, consulte la Guía del administrador de BioStar X.

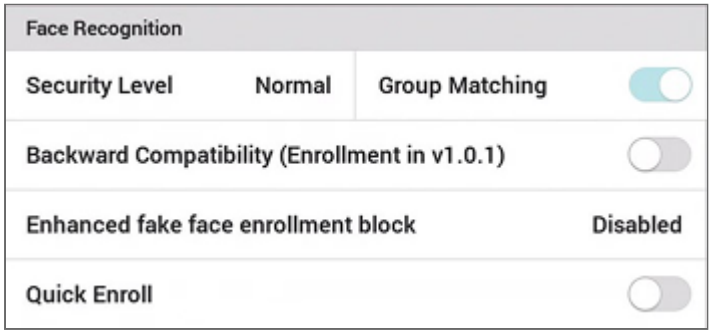
- **Face Pose Variation**: Establece la sensibilidad para la posición, el ángulo y la distancia del rostro al registrar un rostro. Establezca en alto para plantillas de rostro precisas.
- **Enroll Timeout**: Si el rostro no se registra dentro del tiempo establecido, el registro se cancelará.

- **Duplicate Check**: Permite verificar rostros duplicados durante el registro de rostro.

Autenticación facial

Cambie la configuración de la autenticación facial.

1. Haz clic en y autentícate con privilegios de administrador.
2. Después de presionar **AUTHENTICATION**, cambie el elemento deseado en **Face Recognition**.



- **Security Level**: Configura el nivel de seguridad para la autenticación 1:N:.
- **Group Matching**: Permite verificar si se usa coincidencia de grupo. El uso de la coincidencia de grupo permite agrupar los rostros de varios usuarios para aumentar la velocidad de autenticación.
- **Backward Compatibility (Enrollment in v1.0.1)**: Habilite esta opción si el firmware del dispositivo que registra las plantillas de rostro es v1.0.1 o anterior.
- **Enhanced fake face enrollment block**: Puede prevenir el registro de usuarios con rostros falsificados, como fotografías. Establezca la intensidad de **Level 1** a **Level 3**; a medida que aumenta el nivel, la intensidad de la inspección se incrementa.
- **Quick Enroll**: Permite definir si se utiliza el registro facial rápido. Cuando el registro facial rápido está habilitado, el proceso de registro de rostro se establece en un paso; cuando está deshabilitado, se establece en tres pasos.

> **Información**
>
> – **Group Matching** se puede configurar en BioStar X.
>
> – Si **Enhanced fake face enrollment block** se establece en un nivel alto, el registro de rostros reales puede ser rechazado. Si el registro falla, inténtelo de nuevo o disminuya la intensidad de la inspección.
>
> – Para registrar plantillas de rostro de alta calidad, desactive **Quick Enroll**.

Modo de asistencia

Configura cómo registrar el modo T&A.

1. Haz clic en y autentícate con privilegios de administrador.
2. Haz clic en **AUTHENTICATION**, luego modifica el elemento deseado en **T&A Mode**.



- **T&A Mode**: Configura cómo usar el modo de asistencia.
- **T&A Code**: Registra eventos de T&A.
- **T&A Required**: Configure para que el usuario tenga que seleccionar un evento de T&A al autenticarse. Disponible cuando **T&A Mode** está configurado en **By User**.
- **Fixed T&A Key**: Configura para usar solo un evento de T&A seleccionado por el administrador. Disponible cuando **T&A Mode** está configurado en **Fixed**.
- **Job Code**: Configure si se usará el código de puesto.

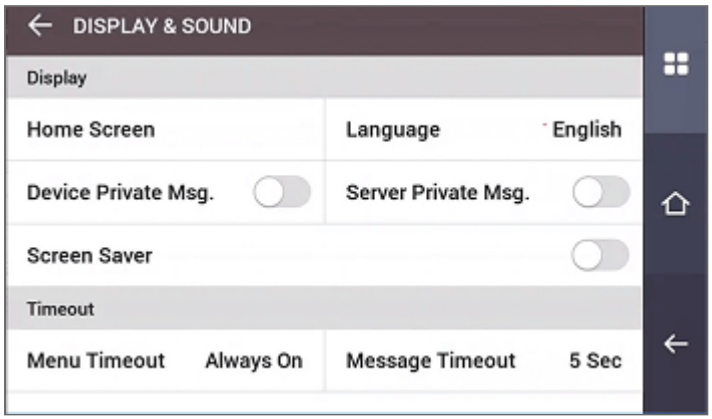
Ajustes

Proporciona instrucciones para configurar los ajustes del sistema y del dispositivo.

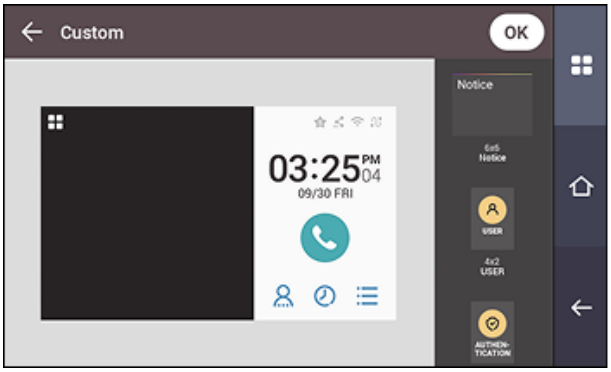
Pantalla y sonido

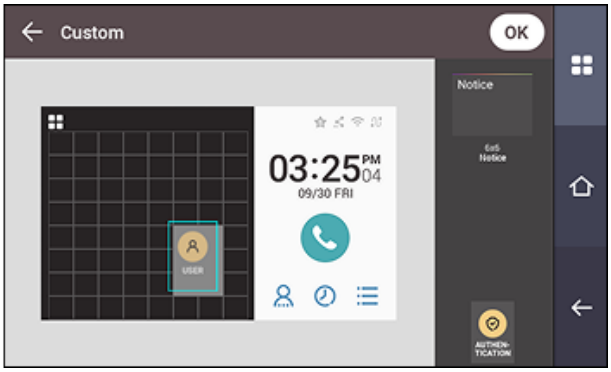
Cambie los ajustes de pantalla y sonido del dispositivo.

1. Haz clic en y autentícate con privilegios de administrador.
2. Haga clic en **DISPLAY & SOUND**.
3. Cambie el elemento deseado.



- **Home Screen**: Permite elegir los elementos que se mostrarán en el fondo de la pantalla de inicio. Al seleccionar el estilo personalizado, puede modificar la pantalla de inicio directamente. Mantenga presionado el objeto deseado y arrástrelo para editar la pantalla de inicio.





- **Language**: Permite seleccionar el idioma que se mostrará en la pantalla.
- **Device Private Msg.**: Configure si se utiliza un mensaje privado que se mostrará en la pantalla cuando el usuario se autentique. **Device Private Msg.** se puede configurar mediante el SDK de dispositivos BioStar. Si no se configura, no se mostrará ningún mensaje cuando la autenticación sea correcta, incluso si **Device Private Msg.** está habilitado en el dispositivo.
- **Server Private Msg.**: Configure si se utiliza un mensaje privado que se mostrará en la pantalla cuando el usuario se autentique. **Server Private Msg.** se puede configurar mediante la API de BioStar X. Si no se configura, no se mostrará ningún mensaje cuando la autenticación sea correcta, incluso si **Server Private Msg.** está habilitado en el dispositivo.
- **Screen Saver**: Configure si el protector de pantalla está habilitado. Reduce el consumo de energía innecesario al disminuir el brillo de la pantalla cuando el dispositivo no se utiliza.
- **Menu Timeout**: Configure el tiempo (s) para que la pantalla de menú desaparezca automáticamente. Si no se pulsa ningún botón durante el tiempo establecido, la pantalla regresará a la pantalla de inicio.
- **Message Timeout**: Configure el tiempo (s) para que un mensaje de configuración completada o de notificación desaparezca automáticamente.
- **Backlight Timeout**: Configure el tiempo (s) para apagar la iluminación de la pantalla.
- **Voice Instruction**: Permite usar guía por voz en lugar de tonos de notificación.
- **Volume**: Configure el volumen.

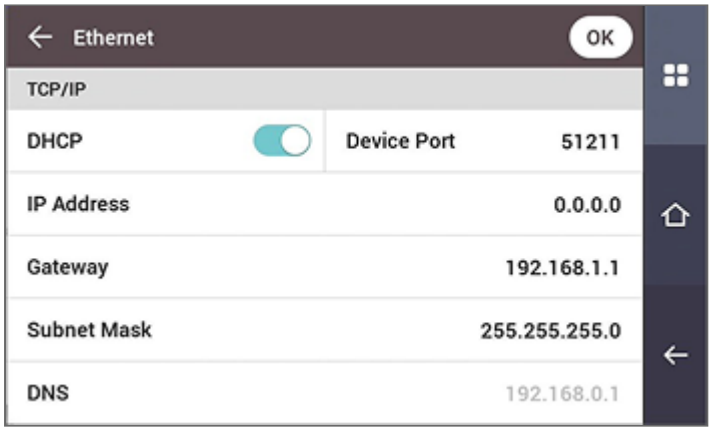
> **Información**
>
> Para obtener más información sobre el SDK de dispositivos BioStar, consulte la página del SDK de dispositivos BioStar en la base de conocimientos de Suprema.

Red

Cambie la configuración de comunicación de dispositivos como Ethernet, servidor y comunicación serial.

Ethernet

1. Haz clic en y autentícate con privilegios de administrador.
2. Seleccione **NETWORK** → **Ethernet**.
3. Cambie el elemento deseado.



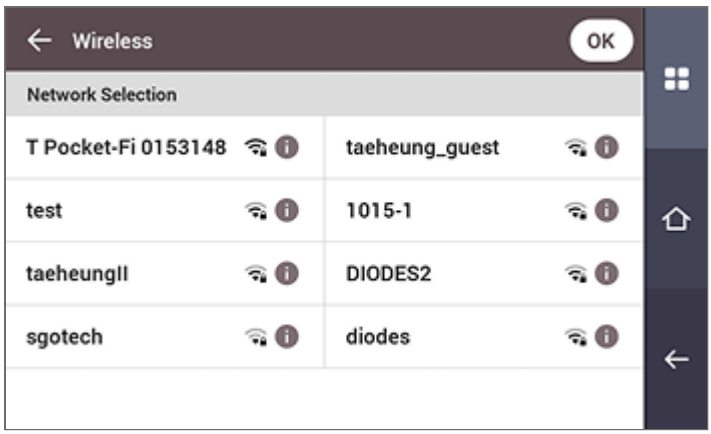
- **DHCP**: Configure si se utiliza DHCP. Si la configuración DHCP está deshabilitada, se pueden modificar **IP Address**, **Gateway** y **Subnet Mask**.
- **Device Port**: Configure el puerto del dispositivo.
- **IP Address**: Compruebe la dirección IP del dispositivo. Para modificarla, desactive la configuración de DHCP.
- **Gateway**: Compruebe la puerta de enlace del dispositivo. Para modificarla, desactive la configuración de DHCP.
- **Subnet Mask**: Compruebe la máscara de subred del dispositivo. Para modificarla, desactive la configuración de DHCP.
- **DNS**: Configure la dirección del servidor DNS.

4. Pulsa **OK** para guardar la configuración.

> **Información**
> **Ethernet** no se puede usar con **Wireless**.

Inalámbrico

1. Haz clic en y autentícate con privilegios de administrador.
2. Seleccione **NETWORK** → **Wireless**.
3. Se mostrará la lista de redes disponibles para conectarse.



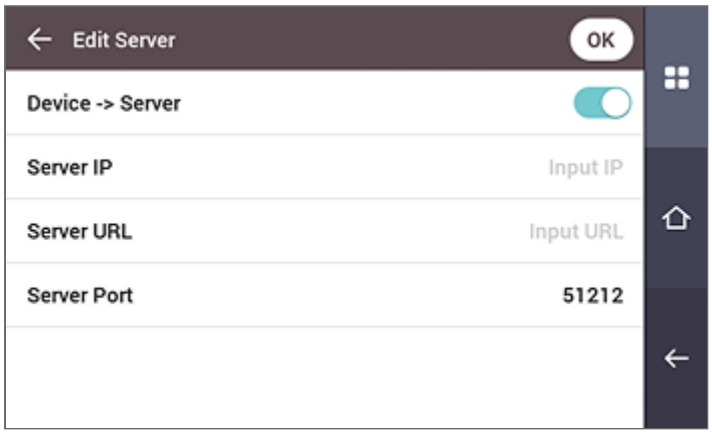
4. Seleccione la red a la que desea conectarse e ingrese la contraseña. Al presionar **OK**, se establecerá la conexión a la red inalámbrica.

5. Presiona en la red inalámbrica que deseas usar y desactiva DHCP para modificar **IP Address**, **Gateway** y **Subnet Mask**.

> **Información**
>
> - **Wireless** solo está disponible para el modelo FS2-AWB.
> - **Wireless** no se puede usar con **Ethernet**.
> - Se requiere un enrutador inalámbrico para conectar **Wireless**. Para obtener información sobre la instalación y configuración del enrutador inalámbrico, consulte el manual del usuario del enrutador.

Servidor

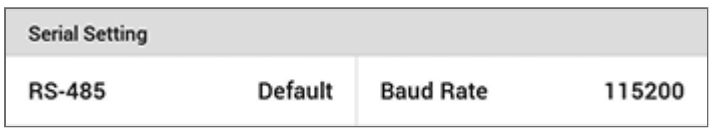
1. Haz clic en y autentícate con privilegios de administrador.
2. Seleccione **NETWORK** → **Server**.
3. Cambie el elemento deseado.



   - **Device → Server**: Envíe directamente una señal de conexión desde el dispositivo a un servidor con la información ingresada. Cuando **Device → Server** está habilitado, el usuario puede ingresar **Server IP**, **Server URL** y **Server Port**.
   - **Server IP**: Ingrese la dirección IP de la PC donde está instalado BioStar X.
   - **Server URL**: Ingrese **Server URL** en lugar de **Server IP**.
   - **Server Port**: Ingrese el puerto de la PC donde está instalado BioStar X.
4. Pulsa **OK** para guardar la configuración.

Configuración de comunicación serial

1. Haz clic en y autentícate con privilegios de administrador.
2. Presione **NETWORK** y cambie el elemento deseado en **Serial Setting**.



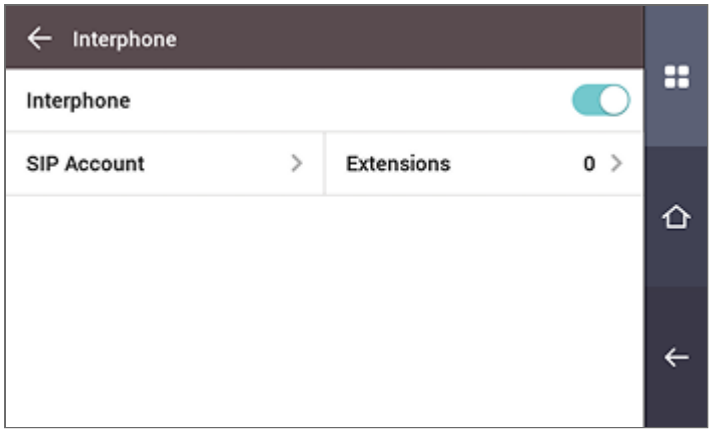
- **RS-485**: Seleccione el modo RS-485.
- **Baud Rate**: Seleccione la velocidad en baudios deseada.

Dispositivo

Interfono

Puede configurar la cuenta y las extensiones del intercomunicador SIP.

1. Haz clic en y autentícate con privilegios de administrador.
2. Haga clic en **DEVICE** → **Interphone**.



- **Interphone**: Puede definir si habilitar el intercomunicador. Al habilitar la configuración del intercomunicador, puede configurar **SIP Account** y **Extensions**.
- **SIP Account**: Ingrese cada dato para que el dispositivo se registre en el servidor SIP.
- **Extensions**: Agregue, elimine o edite números de extensión.

Relé

Configure los puertos de entrada de **Open Time** y **Exit Button** en el dispositivo.

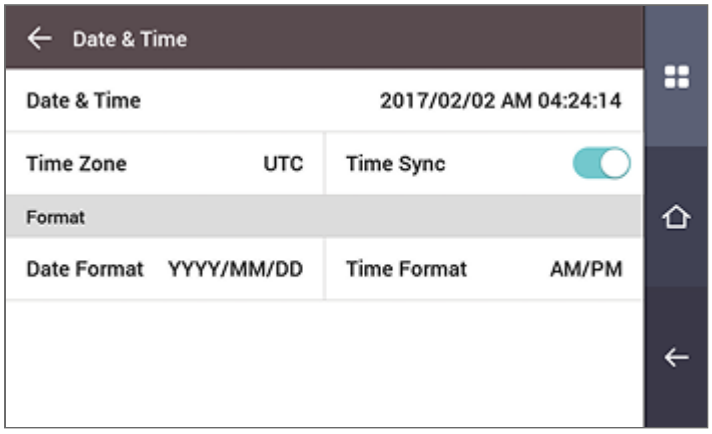
1. Haz clic en y autentícate con privilegios de administrador.
2. Haga clic en **DEVICE** → **Relay**.

- **Relay**: Configure si el relé está habilitado. Habilitar el ajuste de relé permite configurar **Open Time** y **Exit Button**.
- **Open Time**: Establece la duración que la puerta permanece abierta cuando se ha realizado la autenticación de usuario estándar.
- **Exit Button**: Selecciona el puerto de entrada conectado al botón de salida.
- **Switch**: Seleccione el tipo de interruptor (**N/O** o **N/C**) para el puerto de entrada del botón de salida.

Fecha y hora

Configura la fecha y la hora. Configura la fecha y la hora con precisión para recopilar datos de registro precisos.

1. Haz clic en y autentícate con privilegios de administrador.
2. Haz clic en **DEVICE** → **Date & Time**.
3. Cambie el elemento deseado.



- **Date & Time**: Compruebe la fecha y hora actuales. Para modificarla manualmente, desactive **Time Sync**.
- **Time Zone**: Ajuste la referencia horaria de la ubicación actual.
- **Time Sync**: Sincronice el servidor y la hora. Si desea sincronizar el servidor y la hora, habilite **Time Sync**.
- **Date Format**: Configure el formato de fecha. Seleccione **YYYY/MM/DD**, **MM/DD/YYYY** y **DD/MM/YYYY**.
- **Time Format**: Configure el formato de hora. Seleccione **AM/PM** y **24-Hour**.

Horario de verano

Aplica el horario de verano para usar el dispositivo. Configura correctamente la hora de inicio y fin.

1. Haz clic en y autentícate con privilegios de administrador.
2. Haz clic en **DEVICE** → **Daylight Saving Time**, luego presiona para agregar el horario de verano.
3. Cambie el elemento deseado.
   - **Name**: Consulta el nombre del horario de verano.
   - **Start Month** / **Start Week** / **Start Day** / **Start Time**: Configure los detalles sobre cuándo comienza el horario de verano.
   - **End Month** / **End Week** / **End Day** / **End Time**: Configure los detalles sobre cuándo termina el horario de verano.
4. Pulsa **OK** para guardar la configuración.

Información del dispositivo

Consulta el nombre del modelo, el ID del dispositivo, el número de serie, la versión del dispositivo y del firmware, el kernel y la dirección MAC.

1. Haz clic en y autentícate con privilegios de administrador.
2. Selecciona **DEVICE** → **Device Info**. Vea la información de **Model Name**, **Device ID**, **Serial No.**, **HW**, **FW**, **Kernel**, **MAC** y

WiFi MAC.

> **Información**
> El elemento **WiFi MAC** solo está disponible en el modelo FS2-AWB.

Información de memoria

Consulta el estado de uso de la memoria.

1. Haz clic en y autentícate con privilegios de administrador.
2. Selecciona **DEVICE** → **Memory Info**. Consulta el estado de uso de memoria del dispositivo.

Memoria USB

Conecta una memoria USB e importa la información de usuarios al dispositivo o exporta registros e información de usuarios desde el dispositivo. También puede actualizar el firmware.

1. Haz clic en y autentícate con privilegios de administrador.
2. Selecciona **DEVICE** → **USB Memory**.
3. Selecciona el elemento deseado y cambia el ajuste.
   - **Import**: Importe la información de usuarios desde la memoria USB conectada.
   - **Export**: Seleccione la información que desea exportar a la memoria USB conectada.
   - **FW Upgrade**: Actualice el firmware si los archivos de firmware están guardados en la memoria USB conectada.

> **Precaución**
> No desconecte la fuente de alimentación mientras se actualiza el firmware del dispositivo. El dispositivo puede funcionar incorrectamente.

Sabotaje

Configura si se utiliza el tamper de seguridad. Cuando el tamper está activado, establece la eliminación de todos los usuarios, todos los registros y la clave de seguridad.

1. Haz clic en y autentícate con privilegios de administrador.
2. Seleccione **DEVICE**.
3. Active **Secure Tamper** para eliminar los datos de todos los usuarios registrados, todos los registros y las claves seguras cuando ocurra un evento de manipulación.

Reiniciar dispositivo

Reinicia el dispositivo.

1. Haz clic en y autentícate con privilegios de administrador.
2. Selecciona **DEVICE** → **Restart Device**.
3. Presiona **OK** para reiniciar el dispositivo. Presiona **Cancel** para regresar a la pantalla anterior.

Restaurar valores predeterminados

Los ajustes del dispositivo, los ajustes de red y los niveles de operador se restablecerán.

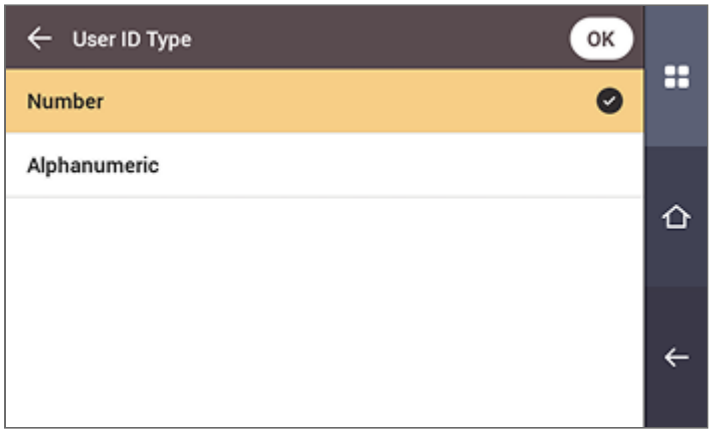
1. Haz clic en y autentícate con privilegios de administrador.
2. Selecciona **DEVICE** → **Restore Default**.
   - **All settings**: Inicializa todos los ajustes almacenados en el dispositivo. Presione **OK** → **OK** para inicializar todos los ajustes del dispositivo. Presiona **Cancel** para regresar a la pantalla anterior.
   - **Keep Network Settings**: Inicializa todos los ajustes excepto los de red. Presione **OK** → **OK** para inicializar todos los ajustes excepto los de red. Presiona **Cancel** para regresar a la pantalla anterior.
   - **Factory Default**: Elimina toda la información guardada en el dispositivo y el certificado raíz, y restaura los ajustes predeterminados.
   - **Delete the Root Certificate**: Elimina el certificado raíz guardado en el dispositivo.
3. Si continúas con **Restore Default**, el dispositivo se reiniciará.

> **Información**
>
> - Al restablecer, el nivel de operador también se restablecerá. Después de restablecer, vuelve a configurar el nivel de operador.
> - El ajuste de idioma no cambiará después de restablecer.
> - El menú **Factory Default** puede utilizarse cuando el certificado raíz está guardado en el dispositivo.
> - El menú **Delete the Root Certificate** puede utilizarse solo cuando el certificado raíz está guardado en el dispositivo y se ha designado un administrador.

Tipo de ID de usuario

Selecciona el tipo de ID de usuario que se va a registrar en el dispositivo.

1. Haz clic en y autentícate con privilegios de administrador.
2. Seleccione **DEVICE** → **User ID Type**.



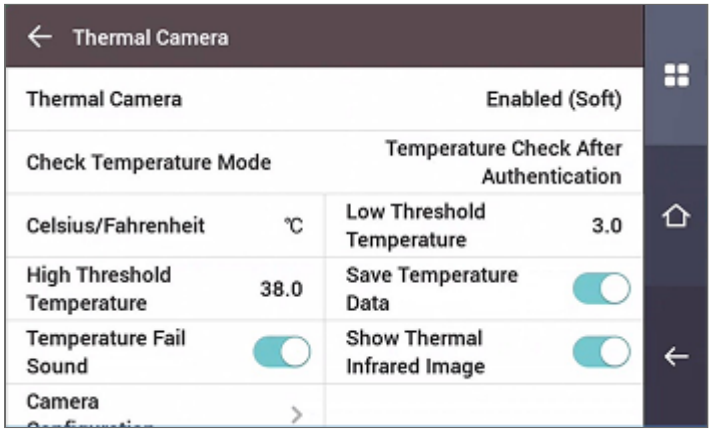
- **Number**: Ingrese un ID de usuario con solo números.
- **Alphanumeric**: Ingrese un ID de usuario con caracteres alfanuméricos y los símbolos _ -.

3. Después de cambiar al elemento deseado, presiona **OK**.

Cámara térmica

El dispositivo puede medir la temperatura de los usuarios que pasan por la entrada al vincularse con la cámara térmica y restringir el acceso a los usuarios que superen la temperatura de referencia.

1. Haz clic en y autentícate con privilegios de administrador.
2. Seleccione **DEVICE** → **Thermal Camera**.
3. Cambie el elemento deseado.



- **Thermal Camera**: Puede establecer si se utilizará la cámara térmica. Cuando se establece en **Enabled (Hard)**, a los usuarios que superen la temperatura de referencia se les negará la autenticación y se registrará el evento de temperatura excedida. Cuando se establece en **Enabled (Soft)**, los usuarios que superen la temperatura de referencia podrán autenticarse, pero se registrará el evento de temperatura excedida.
- **Check Temperature Mode**: Puede establecer el modo de comprobación de temperatura según el propósito.
  - **Temperature Check After Authentication**: Mide la temperatura del usuario después de que se realiza la autenticación.
  - **Temperature Check Before Authentication**: Mide la temperatura del usuario y luego realiza la autenticación. En este modo, los usuarios que superen la temperatura de referencia no podrán autenticarse.
  - **Check Temperature Only**: El dispositivo solo puede utilizarse para medir la temperatura. En este modo, todos

los usuarios por debajo de la temperatura de referencia pueden entrar, independientemente de la autenticación.

- **Celsius/Fahrenheit**: Puede establecer la unidad de visualización de la temperatura.
- **Low Threshold Temperature**: Puede establecer la temperatura mínima de referencia para restringir el acceso. A los usuarios con una temperatura superficial inferior a la temperatura mínima de referencia se les negará la autenticación.
  La temperatura mínima de referencia puede configurarse en el rango de 1 °C a 45 °C y debe ser superior a la temperatura máxima de referencia.
- **High Threshold Temperature**: Puede establecer la temperatura máxima de referencia para restringir el acceso. A los usuarios con una temperatura superficial superior a la temperatura máxima de referencia se les negará la autenticación.
  La temperatura máxima de referencia puede configurarse en el rango de 1 °C a 45 °C y debe ser inferior a la temperatura mínima de referencia.
- **Save Temperature Data**: Puede establecer si se guardará el registro de temperatura del usuario. Si utiliza esta opción, tanto el éxito de la autenticación como el valor de temperatura del usuario se guardarán en el registro; si no se utiliza, solo se registrará el éxito de la autenticación.
- **Show Thermal Infrared Image**: Puede establecer si se mostrará la imagen térmica en la pantalla del dispositivo.
- **Camera Configuration**: Puede establecer opciones detalladas para obtener mediciones precisas con la cámara.
  - **Distance(cm)**: Configure la distancia entre el usuario y la cámara térmica.
  - **Emissivity**: Configure la emisividad infrarroja.
  - **ROI X(%)**, **ROI Y(%)**, **ROI Width(%)**, **ROI Height(%)**: Si hay iluminación adicional instalada cerca, la cámara térmica puede configurarse para medir la temperatura del usuario en lugar de la de esa iluminación. Ajuste la posición y el tamaño del ROI (región de interés) para definir manualmente el área donde la cámara térmica medirá la temperatura.
  - **Skin Temperature Compensation**: Puede configurar la cámara térmica para calibrar automáticamente la temperatura según el entorno de uso y la temperatura ambiente.
  - **Skin Temperature Correction**: Puede ajustar las lecturas de temperatura a un valor fijo según el entorno de uso. Por ejemplo, en entornos donde la temperatura siempre se mide 0.1 °C más alta, establezca el valor de calibración de temperatura en -0.1.

Información

- Para un rendimiento óptimo, se recomienda utilizar los valores predeterminados de las subopciones de la configuración de la cámara. Los valores predeterminados de cada opción son los siguientes:
  - **Distance(cm)**: 100
  - **Emissivity**: 0.98
  - **ROI X(%)**: 47
  - **ROI Y(%)**: 45
  - **ROI Width(%)**: 15
  - **ROI Height(%)**: 10
- La cámara térmica es compatible con TCM10-FS2.

Registros de eventos

Describe cómo ver los registros de eventos generados por el dispositivo.

Busca registros de eventos

Configura condiciones para buscar registros.

1. Haz clic en y autentícate con privilegios de administrador.
2. Seleccione **EVENT LOG**. Todos los registros de eventos aparecen.
3. Presione para buscar un registro específico y cambiar la condición.

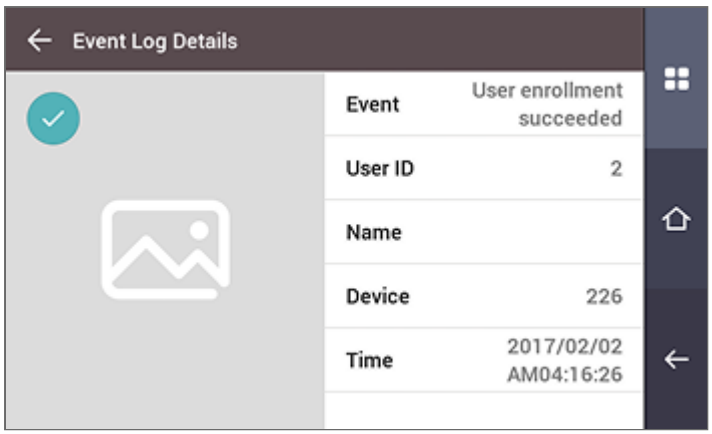


4. Establezca los criterios de búsqueda y haga clic en **OK** para mostrar los registros que coincidan con los criterios.

Ver detalles del registro de eventos

Consulta los detalles de los registros.

1. Haz clic en y autentícate con privilegios de administrador.
2. Seleccione **EVENT LOG**. Todos los registros de eventos aparecen.
3. Haz clic en el registro para consultar los detalles.



Eliminar todos los registros

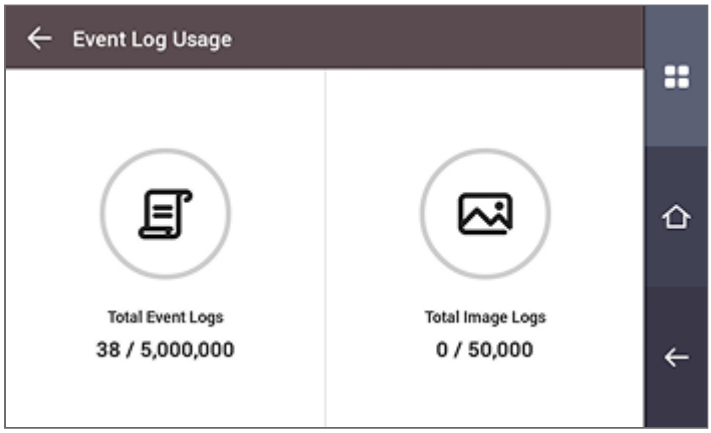
Elimina todos los registros guardados.

1. Haz clic en y autentícate con privilegios de administrador.
2. Seleccione **EVENT LOG**. Todos los registros de eventos aparecen.
3. Seleccione y haga clic en **OK** para eliminar todos los registros. Presiona **Cancel** para regresar a la pantalla anterior.

Ver uso de registros

Consulta el estado del uso de registros.

1. Haz clic en y autentícate con privilegios de administrador.
2. Haga clic en **EVENT LOG** → . Verifique el uso de los registros de eventos e imágenes del dispositivo.



Solución de Problemas

Este documento proporciona información para resolver problemas inesperados que puede encontrar al usar el dispositivo.

Verifique estos elementos antes de reportar una falla

Este documento proporciona información para resolver problemas inesperados que puede encontrar al usar el dispositivo.

Alimentación

Q. Se está suministrando energía, pero el dispositivo no funciona.

- Si el terminal y el soporte están muy separados, el dispositivo puede no funcionar debido al interruptor antisabotaje.
- Verifique el adaptador o el cable de alimentación.

PIN

Q. Perdí mi PIN.

- Para un PIN de usuario normal, solicítelo al administrador e introdúzcalo nuevamente.
- Si perdió el PIN de administrador, comuníquese con la empresa de instalación.

Q. Ingresé mi PIN y pulsé el botón OK, pero aún no puedo abrir la puerta.

- Verifique si ingresó el PIN registrado correctamente.
- Verifique si ha cambiado el PIN recientemente.
- Si no recuerda el PIN, solicítelo al administrador e introdúzcalo nuevamente.

Rostro

Q. El rostro está registrado pero la autenticación facial no se realiza correctamente y se producen errores con frecuencia.

- Consulte Precauciones para enrolar rostros y vuelva a registrarlo.
- Si hay muchos rostros registrados, cambie **Matching Timeout** y vuelva a intentarlo.

Q. La autenticación facial dejó de funcionar repentinamente.

- Consulte Precauciones para autenticar un rostro y vuelva a intentarlo.

Q. La cámara térmica no puede medir la temperatura.

- Verifique que la cámara térmica esté conectada correctamente al terminal.
- Mida la temperatura nuevamente sin cubrirse la frente. Si el problema persiste, comuníquese con la empresa de instalación.

Q. La cámara térmica mide una temperatura inferior a la real.

- Si un usuario mide la temperatura después de estar expuesto al frío durante mucho tiempo, la cámara puede medir una temperatura inferior a la real. Espere de 1 a 2 minutos en el interior y vuelva a intentarlo. Si el problema persiste, comuníquese con la empresa de instalación.

Cerradura de puerta

Q. La puerta no se bloquea al cerrarla.

- La cerradura eléctrica puede estar fallando. Solicite una inspección a la empresa de instalación.

Hora

Q. De repente, la hora es incorrecta.

- El dispositivo cuenta con una batería interna, pero si no recibe alimentación durante mucho tiempo, la batería puede agotarse y provocar que la hora sea incorrecta. Puede corregirla consultando Fecha y hora.

Acceso de administrador

Q. Perdí mi PIN de administrador, por lo que no puedo acceder al modo de administrador.

- El administrador otorga un permiso de acceso en el dispositivo, por lo que solo él puede acceder al menú de administrador.
- Si perdió el PIN de administrador, comuníquese con la empresa de instalación.

Especificaciones del Producto

Incluye las especificaciones clave del producto, como tamaño, características y rendimiento.

Credenciales

Biométrico	**Rostro** • **Detección de rostro vivo:Soportado**	
Tarjeta RF	**FS2-D**	**125kHz EM y 13.56MHz MIFARE, MIFARE Plus, DESFire, DESFire EV1/EV2/EV3[1], FeliCa**
	FS2-AWB	**125kHz EM, HID Prox y 13.56MHz MIFARE, MIFARE Plus, DESFire, DESFire EV1/EV2/EV3[1], FeliCa, iCLASS SE/SR/Seos**
Rango de lectura RF[2]	**EM/HID Prox/MIFARE/DESFire/HID iCLASS/FeliCa: 30 mm**	
Móvil	**FS2-D**	**NFC**
	FS2-AWB	**NFC, BLE**

General

CPU	**1.4 GHz Quad Core**
Memoria	**8 GB Flash + 1 GB RAM**
Chip criptográfico	**Soportado**
Visualizar	**Pantalla TFT táctil en color de 4"**
Resolución de pantalla	**800 x 480 píxeles**
Sonido	**Procesador digital de señales de voz de 24 bits (cancelación de eco)**
Temperatura de funcionamiento	**De -20 °C a 50 °C**

Temperatura de almacenamiento	**De -40 °C a 70 °C**
Humedad de funcionamiento	**Del 0 % al 80 %, sin condensación**
Humedad de almacenamiento	**Del 0 % al 90 %, sin condensación**
Tipo de cámara	**CMOS**
Resolución de la cámara	**720 x 480 píxeles**
Ángulo de la cámara	• **Lente visual: 92.7° en diagonal** • **Lente de infrarrojos: 58° en diagonal**
Autenticación	**CE, UKCA, KC, FCC, IC, RCM, BIS, SIG, RoHS, REACH, WEEE**

Capacidad

Máx. usuarios	**30,000**[3)]
Máx. credenciales (1:N)	**Rostro: 4,000**
Máx. credenciales (1:1)	• **Rostro: 30,000** • **Tarjeta: 30,000** • **PIN: 30,000**
Máx. registros de texto	**5,000,000**
Máx. registros de imágenes	**50,000**

Interfaz

Ethernet	**Admitida (10/100/1000 Mbps, MDI/MDI-X automática)**

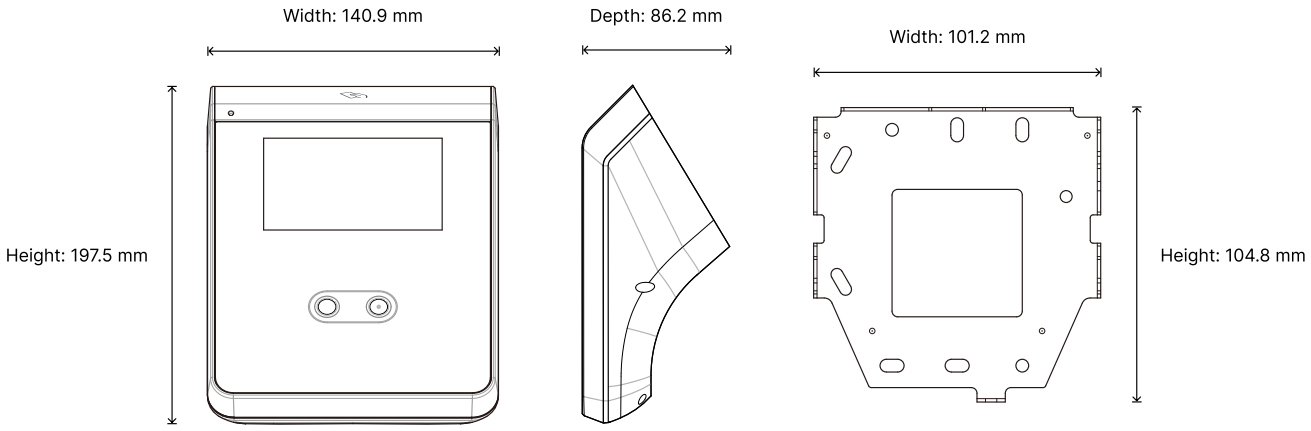
Wi-Fi	**FS2-D**	**No compatible**
	FS2-AWB	**Compatible (integrada, IEEE 802.11 b/g)**
Protocolo de red	**TCP, UDP**	
RS-485	**1 canal maestro/esclavo (seleccionable)**	
Protocolo de comunicación RS-485	**Compatible con OSDP V2**	
Wiegand	**Entrada de 1 canal, salida de 1 canal**	
Entrada	**2 canales de entrada**	
Relé	**1 relé**	
Interfono	**Soportado**	
USB	**USB 2.0 (Maestro)**	
Tamper	**Soportado**	

Eléctrico

Alimentación	**24 Vdc**	**Corriente: Máx. 1.2 A**
Entrada de interruptor VIH	• **Mín.: 3 V** • **Máx.: 5 V**	
Entrada de interruptor VIL	**Máx.: 1 V**	
Resistencia pull-up del interruptor	**4.7 kΩ (los puertos de entrada se polarizan con 4.7 kΩ)**	
Salida Wiegand VOH	**Más de 4.8 V**	

Salida Wiegand VOL	**Menos de 0.2 V**
Resistencia pull-up de salida Wiegand	**Polarización interna de 1 kΩ**
Relé	• **Carga resistiva de 2 A a 30 VCC** • **Carga inductiva de 1 A a 30 VCC**

Dimensiones y peso



1) Las tarjetas DESFire EV2/EV3 son compatibles con versiones anteriores de tarjetas DESFire EV1 y admiten las funciones de CSN y de tarjeta inteligente, incluidas las de la tarjeta DESFire EV1.

2) El alcance de lectura por RF variará según el entorno de instalación.

3) Basado en usuarios inscritos sin credenciales.

Información

- Las especificaciones del producto están sujetas a cambios sin previo aviso para mejorar el rendimiento.
- Cuando este producto funciona como dispositivo maestro, conectar un dispositivo con sensor de huellas como esclavo permite autenticar huellas mediante el dispositivo esclavo.
  - Máx. Credenciales de huella digital (1:N:): 10,000
  - Máx. Credenciales de huella digital (1:1:): 100,000

Información Reglamentaria

Proporciona información sobre las normativas y certificaciones que cumple el producto.

Información de cumplimiento de la FCC

ESTE DISPOSITIVO CUMPLE CON LA PARTE 15 DE LAS NORMAS DE LA FCC.

El funcionamiento está sujeto a las siguientes dos condiciones:

1. Este dispositivo no debe causar interferencias perjudiciales, y
2. Este dispositivo debe aceptar cualquier interferencia recibida, incluida la interferencia que pueda causar un funcionamiento no deseado.

Información

Este equipo ha sido probado y se determinó que cumple con los límites para un dispositivo digital Class A, de conformidad con la parte 15 de las normas de la FCC. Estos límites están diseñados para proporcionar una protección razonable contra interferencias perjudiciales cuando el equipo se opera en un entorno comercial. Este equipo genera, utiliza y puede irradiar energía de radiofrecuencia y, si no se instala y utiliza de acuerdo con el manual de instrucciones, puede causar interferencias perjudiciales en las comunicaciones por radio. El funcionamiento de este equipo en un área residencial probablemente cause interferencias perjudiciales; en tal caso, se requerirá que el usuario corrija la interferencia a su propio costo.

Cualquier cambio o modificación que no esté expresamente aprobado por la parte responsable del cumplimiento podría anular la autoridad del usuario para operar este equipo.

Este transmisor no debe colocarse ni operar junto con ninguna otra antena o transmisor.

Este equipo cumple con los límites de exposición a radiación establecidos por la FCC para un entorno no controlado. Este equipo debe instalarse y operarse manteniendo una distancia mínima de 20 cm entre el radiador y su cuerpo. No instale ni opere este dispositivo y su antena junto con ninguna otra antena o dispositivo de transmisión RF.

Información de IC

Este dispositivo cumple con las RSS exentas de licencia de Industry Canada.

El funcionamiento está sujeto a las siguientes dos condiciones:

1. Este dispositivo no debe causar interferencias, y
2. Este dispositivo debe aceptar cualquier interferencia recibida, incluidas las interferencias que puedan causar un funcionamiento no deseado.

Le présent appareil est conforme aux CNR d’Industrie Canada applicables aux appareils radio exempts de licence.

L’exploitation est autorisée aux deux conditions suivantes :

1. l'appareil ne doit pas produire de brouillage ;
2. l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

Declaración de conformidad de la UE (CE)

Este producto cuenta con la marca CE conforme a las disposiciones de la Directiva de Equipos Radioeléctricos (RED) 2014/53/UE.

Por la presente, Suprema Inc. declara que este producto cumple con los requisitos esenciales y otras disposiciones pertinentes de la Directiva de Equipos Radioeléctricos (RED) 2014/53/UE y lleva la marca CE. Este dispositivo es un equipo de radio Clase 1 según las instrucciones.

- Potencia de transmisión Bluetooth: FS2-AWB 0.049 mW
- Frecuencia Bluetooth: FS2-AWB 2402~2480 MHz
- Frecuencia NFC: 13.56 MHz
- Frecuencia RFID: 13.56 MHz + 125 kHz

Para obtener más información, contáctenos mediante los datos de contacto a continuación.

Suprema Inc.

Dirección: 17F Parkview Tower, 248, Jeongjail-ro, Bundang-gu, Seongnam-si, Gyeonggi-do, 13554, Rep. de COREA

Tel.: +82-31-783-4502 / Fax: +82-31-783-4503

Apéndices

Incluye avisos legales contenidos en el producto.

Descargos de responsabilidad

- La información de este sitio web se proporciona en relación con los productos de Suprema.
- El derecho de uso se reconoce únicamente para los productos de Suprema incluidos en los términos y condiciones de uso o venta de dichos productos garantizados por Suprema. Este sitio web no otorga ninguna licencia, expresa o implícita, por impedimento legal ni de ningún otro tipo, sobre ninguna propiedad intelectual.
- Salvo lo expresamente establecido en un acuerdo entre usted y Suprema, Suprema no asume ninguna responsabilidad y rechaza toda garantía, expresa o implícita, incluidas, entre otras, las relativas a la idoneidad para un fin particular, la comerciabilidad o la no infracción.
- Todas las garantías quedan ANULADAS si los productos de Suprema han sido: 1) instalados incorrectamente o si los números de serie, la fecha de garantía o las etiquetas de control de calidad del hardware han sido alterados o retirados; 2) utilizados de una manera distinta a la autorizada por Suprema; 3) modificados, alterados o reparados por un tercero que no sea Suprema o un tercero autorizado por Suprema; o 4) operados o mantenidos en condiciones ambientales inadecuadas.
- Los productos de Suprema no están destinados a usos médicos, de salvamento, de soporte vital ni a otras aplicaciones en las que la falla del producto de Suprema pudiera ocasionar lesiones personales o la muerte. Si compra o utiliza productos de Suprema para cualquiera de estas aplicaciones no previstas ni autorizadas, deberá indemnizar y eximir de responsabilidad a Suprema y a sus directores, empleados, subsidiarias, afiliadas y distribuidores por todos los reclamos, costos, daños y gastos, incluidos los honorarios razonables de abogados, derivados directa o indirectamente de cualquier reclamo por lesiones personales o muerte asociado con dicho uso no previsto o no autorizado, incluso si el reclamo alega que Suprema fue negligente en el diseño o la fabricación de la pieza.
- Suprema se reserva el derecho de realizar cambios en las especificaciones y descripciones de los productos en cualquier momento y sin previo aviso para mejorar la confiabilidad, la función o el diseño.
- La información personal, en forma de mensajes de autenticación y otra información relacionada, puede almacenarse en los productos de Suprema durante su uso. Suprema no se hace responsable de ninguna información, incluida la información personal, almacenada dentro de los productos de Suprema que no esté bajo el control directo de Suprema o según lo establecido en los términos y condiciones correspondientes. Cuando se utilice cualquier información almacenada, incluida la información personal, es responsabilidad de los usuarios del producto cumplir con la legislación nacional (como el RGPD) y garantizar su manipulación y tratamiento adecuados.
- No debe confiar en la ausencia o las características de ninguna función o instrucción marcada como "reservada" o "indefinida". Suprema las reserva para su definición futura y no tendrá ninguna responsabilidad por conflictos o incompatibilidades derivados de cambios posteriores en ellas.
- Salvo que se disponga expresamente en el presente documento y en la medida máxima permitida por la ley, los productos de Suprema se venden "tal cual".
- Comuníquese con la oficina de ventas local de Suprema o con su distribuidor para obtener las especificaciones más recientes y antes de realizar su pedido.

Aviso de derechos de autor

Los derechos de autor de este sitio web pertenecen a Suprema. Los derechos sobre otros nombres de productos, marcas comerciales y marcas registradas pertenecen a las personas u organizaciones propietarias.

Licencia de código abierto

- El software de este producto se creó modificando la versión 3.x del kernel de Linux y la licencia del kernel de Linux se rige por la GPL. Para obtener más información sobre la licencia GPL, consulte la GNU General Public License.
- Este producto usa "OpenSSL", que está licenciado bajo las licencias OpenSSL y Original SSLeay. Para más información sobre las licencias OpenSSL y Original SSLeay, consulte la OpenSSL License y la Original SSLeay License.
- El AOSP incluido en este producto se rige por la licencia Apache 2.0. Para más información sobre la licencia Apache 2.0, consulte la Apache License.
- El código fuente modificado basado en el kernel de Linux 3.x y el código fuente de AOSP incluido en este producto puede descargarse contactando al Equipo de Soporte Técnico de Suprema.

Suprema Inc.

17F Parkview Tower, 248, Jeongjail-ro, Bundang-gu, Seongnam-si, Gyeonggi-do, 13554, Rep. of KOREA

Tel: +82 31 783 4502 | Fax: +82 31 783 4503 | Inquiry: sales_sys@supremainc.com

Para obtener más información sobre las sucursales globales de Suprema,
visite la página web a continuación escaneando el código QR.
http://www.supremainc.com/en/about/contact-us.asp

© 2026 Suprema Inc. Suprema y los números y los nombres que identifican productos mencionados en este documento son marcas comerciales registradas de Suprema, Inc. Todas las marcas y los nombres de productos que no pertenecen a Suprema son marcas comerciales o marcas comerciales registradas de sus respectivas compañías. La apariencia del producto, el estado de la estructura o las especificaciones están sujetas a cambio sin previo aviso.