FaceStation F2

GUÍA DE USUARIO DE

Versión 1.14

Español
ES 102.00.FSF2

suprema
SECURITY & BIOMETRICS

CONTENIDO

Instrucciones de Seguridad 4

Información de cumplimiento 4

Primeros Pasos 8

Componentes 8

Nombre y función de cada parte 10

Cables y conectores 11

Método correcto de enrolamiento y autenticación facial 14

Instalación 17

Fijar el soporte y el producto 17

Conexión de la fuente de alimentación 22

Conexión de red 23

Conexión de entrada 24

Conexión del relé 25

Conectar como independiente 28

Conectar Secure I/O 2 30

Conexión Wiegand 31

Cómo Usar 32

Menú de Administrador 32

Usuario 34

Autenticación 39

Ajustes 49

Registros de eventos 63

Solución de Problemas 65

Verifique estos elementos antes de reportar una falla 65

Especificaciones del Producto 68

Credenciales 68

General 68

Capacidad 70

Interfaz 70

Eléctrico 71

Dimensiones y peso 72

Información Reglamentaria 74

Información de cumplimiento de la FCC 74

Información de IC 74

Declaración de conformidad de la UE (CE) 75

Apéndices 76

Descargos de responsabilidad 76

Aviso de derechos de autor 77

Licencia de código abierto 77

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.

Para cumplir con las normas IP65, asegúrese de usar una cubierta de cable después de conectar el producto y el cable. Se recomienda usar un gabinete cuando se instale en exteriores con exposición total.

- La disminución del rendimiento a prueba de agua y polvo puede provocar fallos.

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.

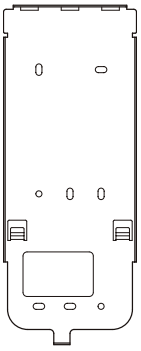
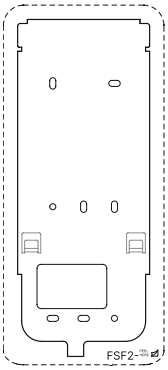
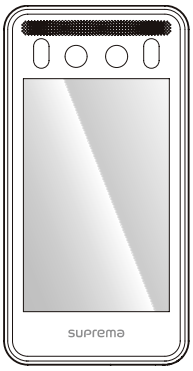
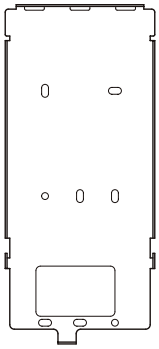
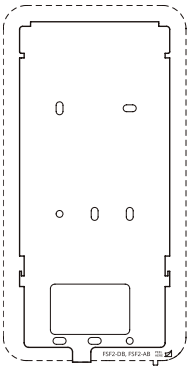
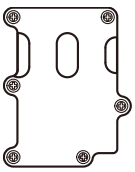
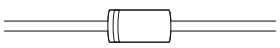
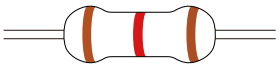
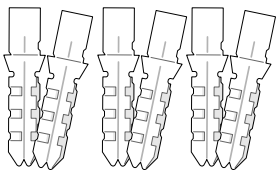
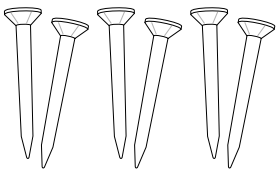
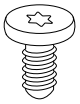
- El dispositivo puede funcionar incorrectamente.

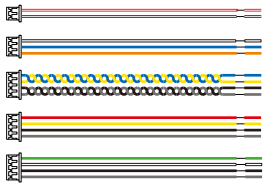
> **Batería RTC**
>
> Reemplazar por baterías no autorizadas o de tipo incorrecto puede representar un riesgo de explosión. Deseche las baterías conforme a las normativas locales o internacionales sobre residuos.

Primeros Pasos

Proporciona procedimientos iniciales para empezar con el dispositivo.

Componentes

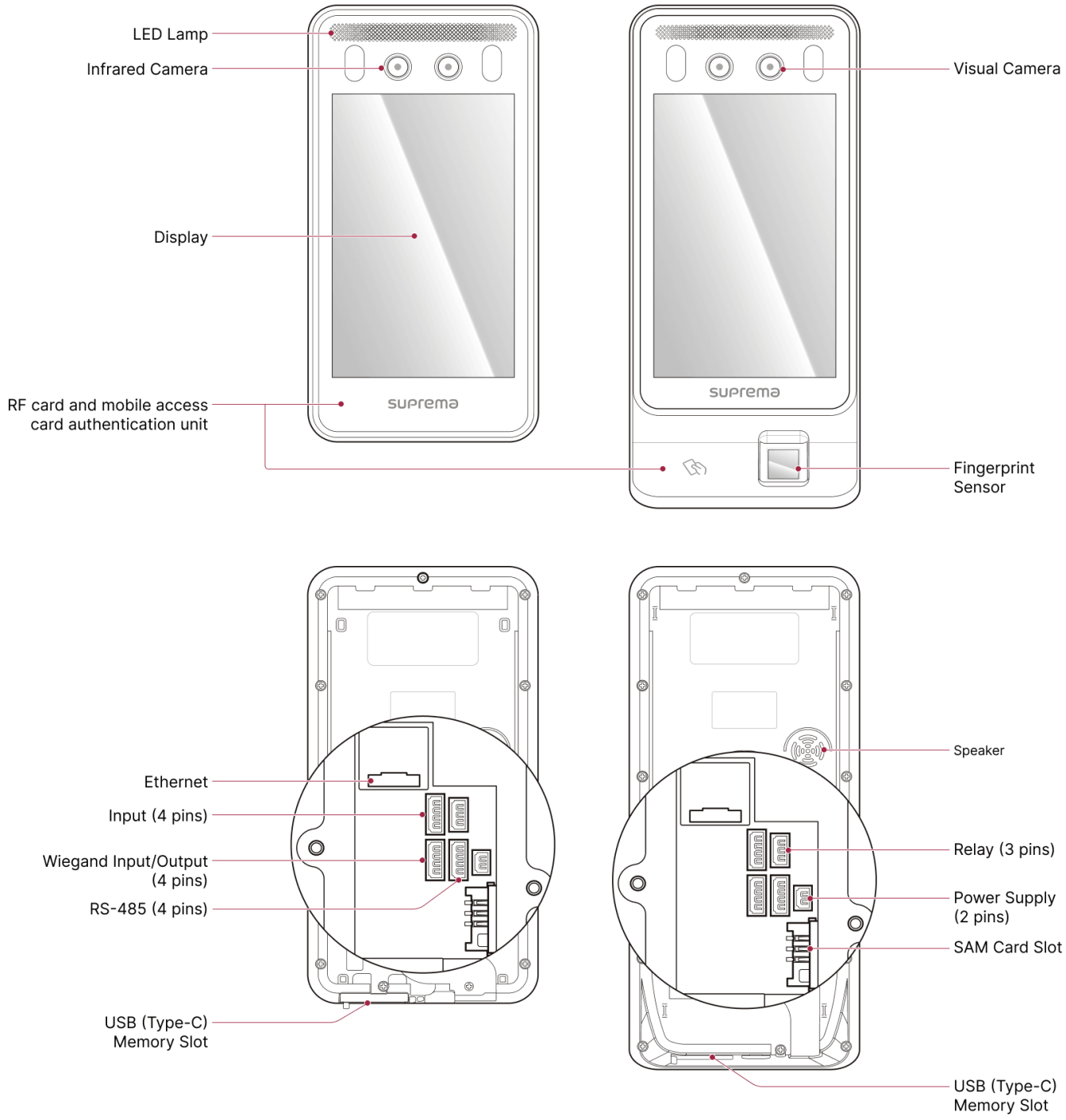
		
FaceStation F2 (FSF2-ODB)	Soporte de pared (FSF2-ODB)	Plantilla de perforación (FSF2-ODB)
		
FaceStation F2 (FSF2-DB, FSF2-AB)	Soporte de pared (FSF2-DB, FSF2-AB)	Plantilla de perforación (FSF2-DB, FSF2-AB)
		
Cubierta de cable	Diodo	Resistencia de 120 Ω
		

Anclaje de PVC x6	Tornillo de fijación x6	Tornillo de fijación del soporte (en forma de estrella)
		
Cables de conexión	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



- **Lámpara LED**: La lámpara LED se enciende cuando detecta a un usuario en la oscuridad.
- **Cámara infrarroja**: Captura la imagen facial infrarroja.
- **Cámara visual**: Captura una imagen facial real.
- **Pantalla**: Proporciona una interfaz de usuario para la operación.

- **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.
- **Unidad de reconocimiento de huellas**: FSF2-ODB La parte que reconoce la huella para el acceso.
- **Ethernet**: Conecta el cable Ethernet.
- **Entrada (4 pines)**: Conecta el cable de entrada.
- **Entrada/salida Wiegand (4 pines)**: Conecta el cable Wiegand de entrada/salida.
- **RS-485 (4 pines)**: Conecta el cable RS-485.
- **Altavoz**: Emite sonido.
- **Relé (3 pines)**: Conecta el cable del relé.
- **Alimentación (2 pines)**: Conecta el cable de alimentación.
- **Ranura para tarjeta SAM**: Se puede usar una tarjeta SAM.
- **Ranura para memoria USB (tipo C)**: Conecta la memoria USB.

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 60 a 100 cm entre el dispositivo y tu rostro al enrolar tu 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.

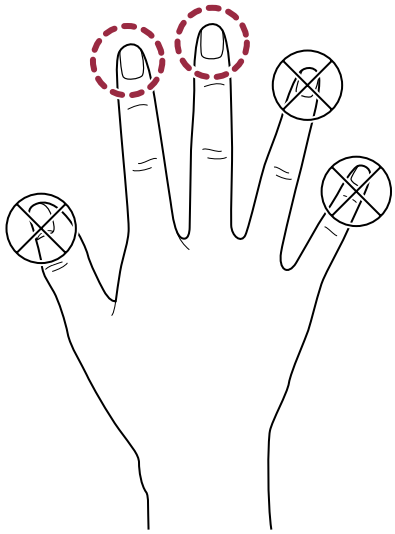
Precauciones para autenticar un rostro

- 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 90-100 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.

Método correcto de ingreso de huellas dactilares FSF2-ODB

Registre la huella correctamente para mejorar la tasa de autenticación de huellas dactilares. Este producto puede autenticar huellas dactilares incluso si cambian el ángulo y la posición de ingreso de la huella. Registre la huella teniendo en cuenta los siguientes aspectos para mejorar la tasa de autenticación.

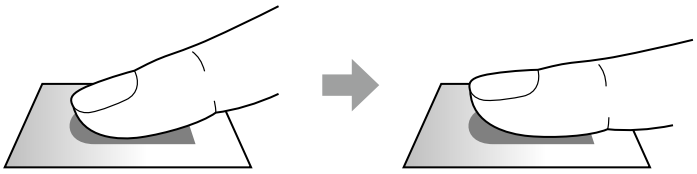
Selección de dedo para el ingreso de huella dactilar



- Para el caso de que la huella de un dedo específico no pueda utilizarse, por ejemplo, si el usuario sostiene una carga con una mano o se lesiona un dedo, se pueden registrar hasta 10 huellas dactilares por usuario.
- Si la huella de un usuario no se reconoce correctamente, registre el mismo dedo dos veces para mejorar la tasa de autenticación.
- Si un dedo tiene un corte o la huella está borrosa, seleccione otro dedo para la huella.
- Use el dedo índice o medio al escanear la huella. La tasa de autenticación puede reducirse si es difícil colocar otro dedo con precisión en el centro del sensor de huellas.

Método de registro de huellas dactilares

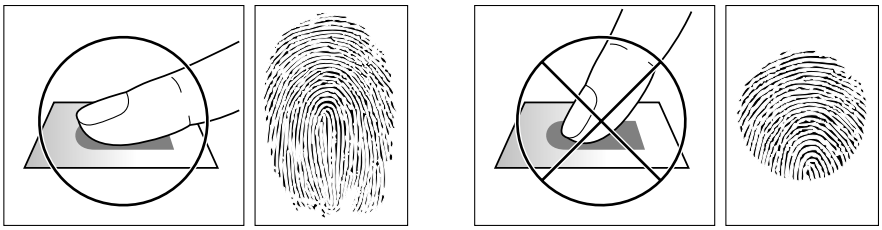
1. Cuando la pantalla muestre "Ingrese su huella", coloque el dedo que desea registrar en la unidad de reconocimiento de huellas y presiónelo suavemente para que la huella se autentique correctamente.



2. Cuando aparezca la pantalla de reingreso tras el beep, vuelva a escanear la huella del dedo registrado. (escanee dos veces la huella del dedo que va a registrar)

Precauciones para la inscripción de huellas dactilares

Cuando se reconoce una huella, se compara con la huella registrada inicialmente; por lo tanto, el registro inicial es el más importante. Tenga en cuenta los siguientes aspectos al registrar la huella.



- Coloque el dedo lo suficientemente profundo para que haga contacto completo con el sensor.
- Coloque el centro de la huella en el centro del sensor.
- Si un dedo tiene un corte o la huella está borrosa, seleccione otro dedo para la huella.
- Escanee la huella correctamente sin moverla, según las instrucciones de la pantalla.
- Si mantiene el dedo en posición vertical de modo que se reduzca el área de contacto con el sensor o cambia el ángulo del dedo, es posible que la autenticación de la huella no se realice.

Si la autenticación de huellas no funciona correctamente

Este producto puede autenticar huellas dactilares sin importar los cambios estacionales o el estado de los dedos. Sin embargo, la tasa de autenticación puede variar según el entorno externo o el método de ingreso de la huella. Si la autenticación de huellas no se realiza sin problemas, adopte las siguientes medidas.

- Si el dedo está mojado o sudoroso, séquelo y luego escanee la huella.
- Si el dedo está demasiado seco, sople sobre la yema y luego escanee la huella.
- Si el dedo tiene un corte, registre la huella de otro dedo.
- Como la huella dactilar inscrita inicialmente con frecuencia no se introduce correctamente, vuelva a registrarla siguiendo las Precauciones para el registro de huellas dactilares.

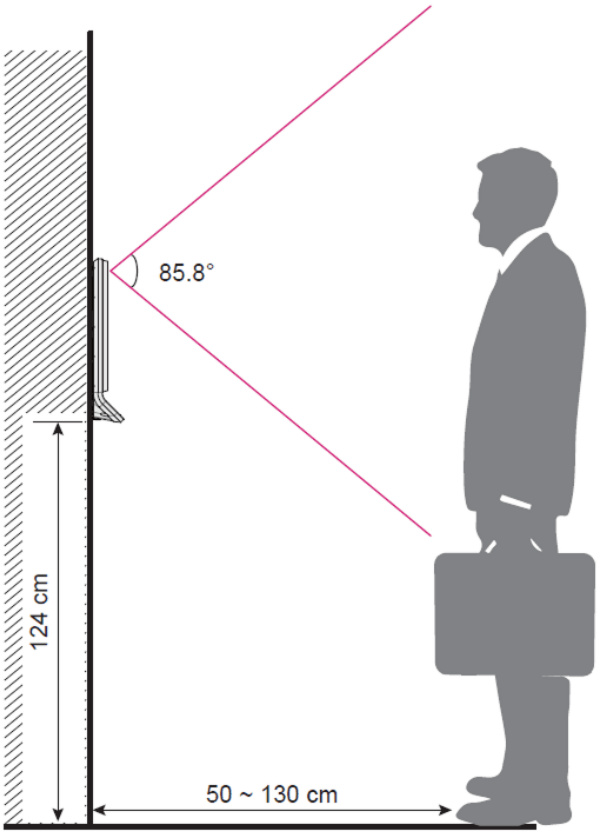
Instalación

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

Fijar el soporte y el producto

> **Información**
> Este documento describe el método de instalación basado en la forma del modelo FSF2-ODB. Utilice el mismo método para instalar los modelos FSF2-DB y FSF2-AB.

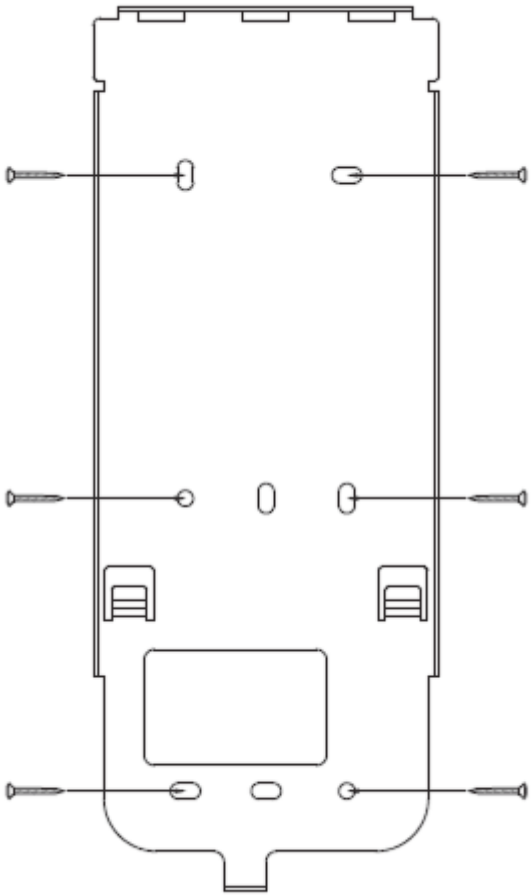
1. Determine la posición correcta para instalar el soporte usando la plantilla de perforación proporcionada.



Información

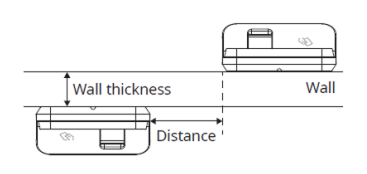
- La altura óptima para instalar el dispositivo es la siguiente.
  - FSF2-ODB: 124 cm
  - FSF2-DB, FSF2-AB: 127 cm
- Instale el dispositivo donde no reciba luz solar directa ni luz UV.
- Ajuste la posición de instalación para que el rostro no esté expuesto a la luz solar directa cuando el usuario intente autenticarse.

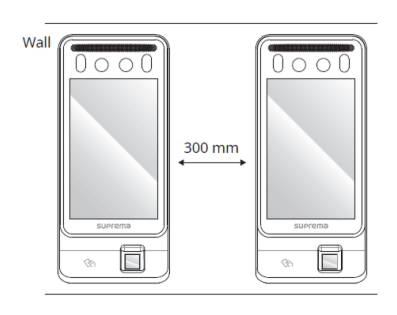
2. Asegura firmemente el soporte con los tornillos de fijación en el lugar donde se montará el producto.



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.

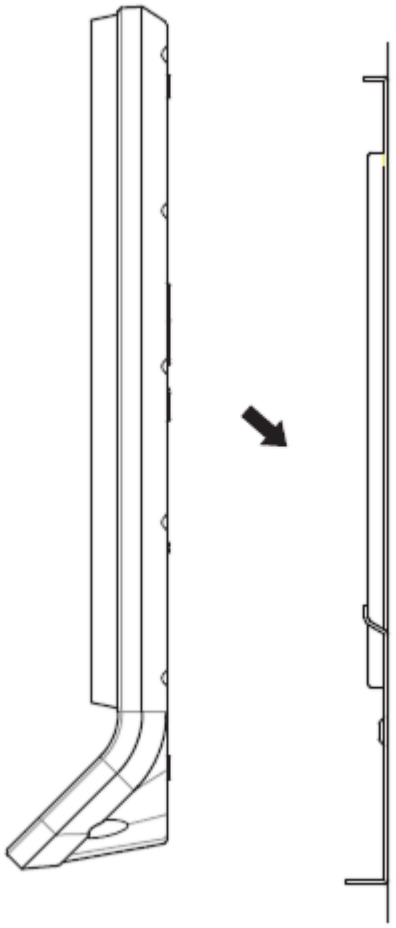




Espesor de pared	Distancia
100 mm	200 mm
120 mm	180 mm
150 mm	150 mm

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

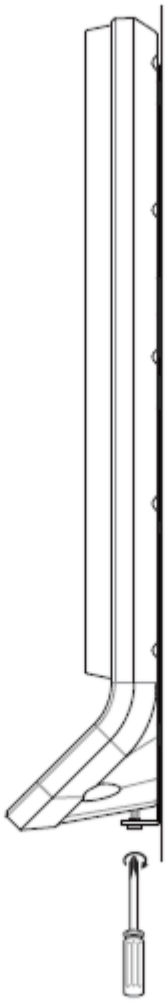
3. Después de instalar la cubierta del cable, apriete firmemente los seis tornillos de la cubierta y monte el producto en el soporte fijo.



Información

Asegúrate de que la cubierta del cable quede completamente cerrada después de conectarla al producto para mantener la resistencia al agua y al polvo (IP65).

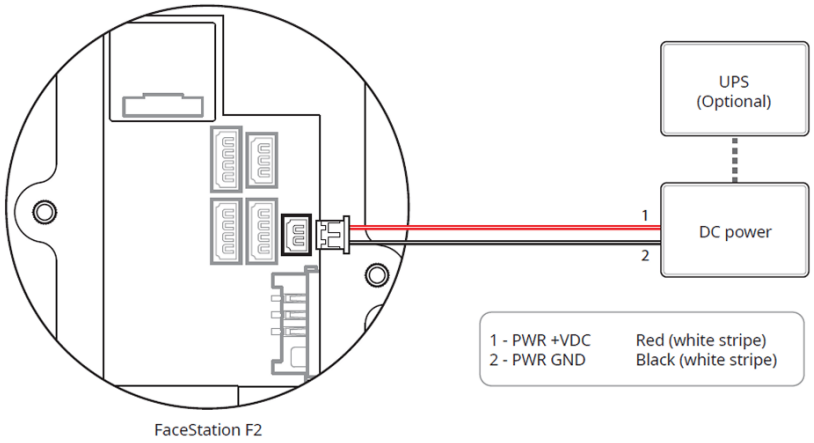
4. Gira los tornillos de fijación para ensamblar el producto con el soporte.



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.

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. Este producto admite alimentación de 24 VCC y 12 VCC; verifique la longitud máxima según la especificación del cable para asegurarse de que la unidad reciba alimentación adecuada.

Estándar de cable	Máx. longitud extendida	
	CC 12V	CC 24V
16 AWG	50 m	150 m
18 AWG	30 m	136 m
20 AWG	20 m	90 m

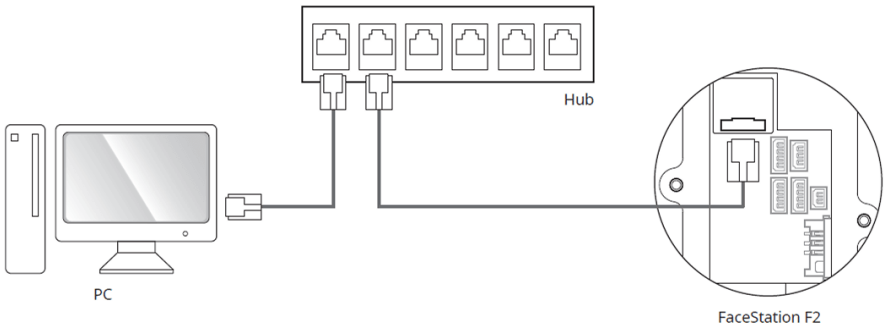
- NO extienda la longitud del cable de alimentación al usar el adaptador de alimentación.
- NO utilice CAT5 UTP de 2 hilos para la alimentación.

Conexión de red

TCP/IP

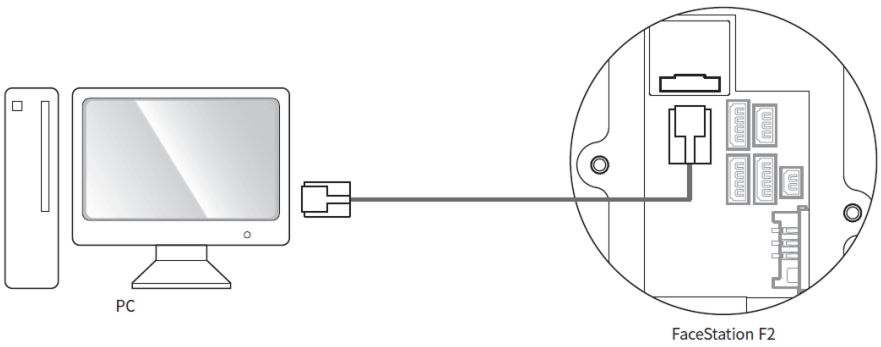
Conexión LAN (conexión a un concentrador)

Conéctese a un concentrador usando un cable CAT-5 estándar o superior.



Conexión LAN (conexión directa a una PC)

Este producto admite MDI/MDIX automático, por lo que puede conectarse directamente a una PC mediante un cable cruzado o un cable CAT-5 recto estándar o superior.



Información

Para un switch Ethernet gigabit, verifique la siguiente información.

- Utilice un cable CAT-5e UTP (par trenzado sin blindaje).
- Utilice los 4 pares (8 hilos) para la conexión de red.
- No use pares ni hilos del cable de red para otros fines.

Puertos y servicios de red

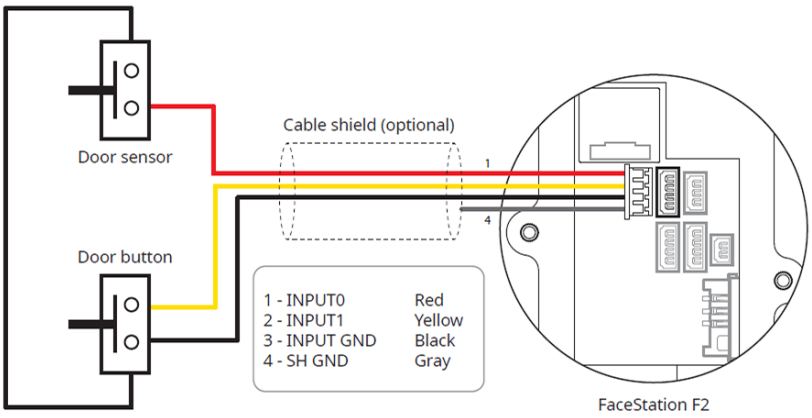
Este dispositivo usa los siguientes puertos para la comunicación de red y el funcionamiento estable del servicio.

Protocolo	Servicio
TCP	El dispositivo usa este puerto para comunicarse con el servidor y cambiar el estado operativo.
UDP	El dispositivo usa este puerto para detectar 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.

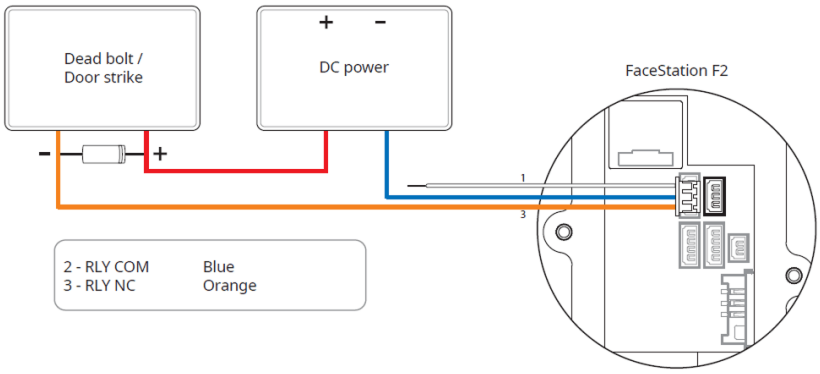
Conexión de entrada



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

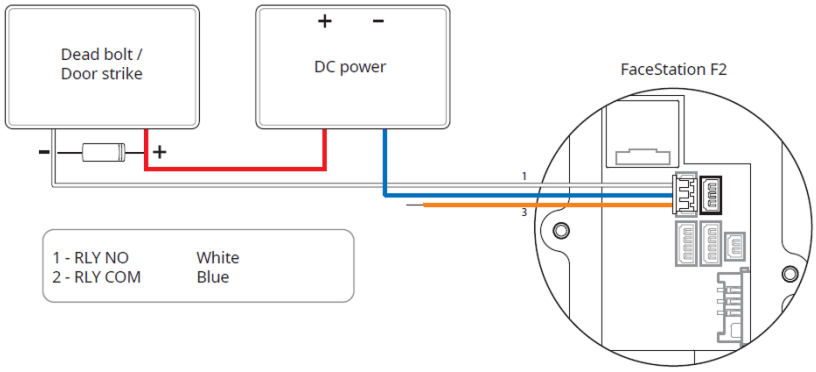
- Instale un diodo en ambos extremos del cable de la cerradura, como se muestra en la figura, para proteger el relé de la corriente inversa que se produce cuando la cerradura funciona.
- Utilice una fuente de alimentación independiente para el producto y la cerradura.
- Los lectores inteligentes independientes 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.



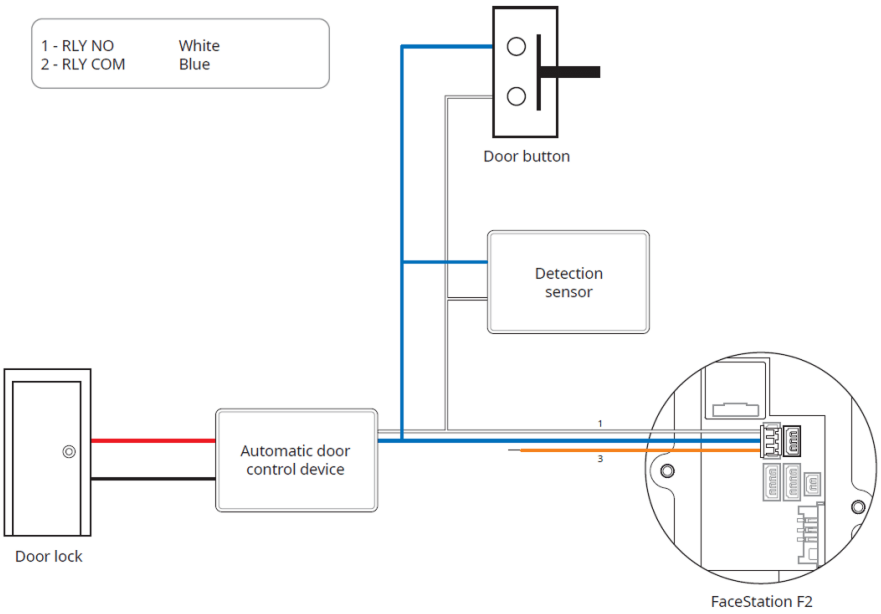
Precaución

- 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

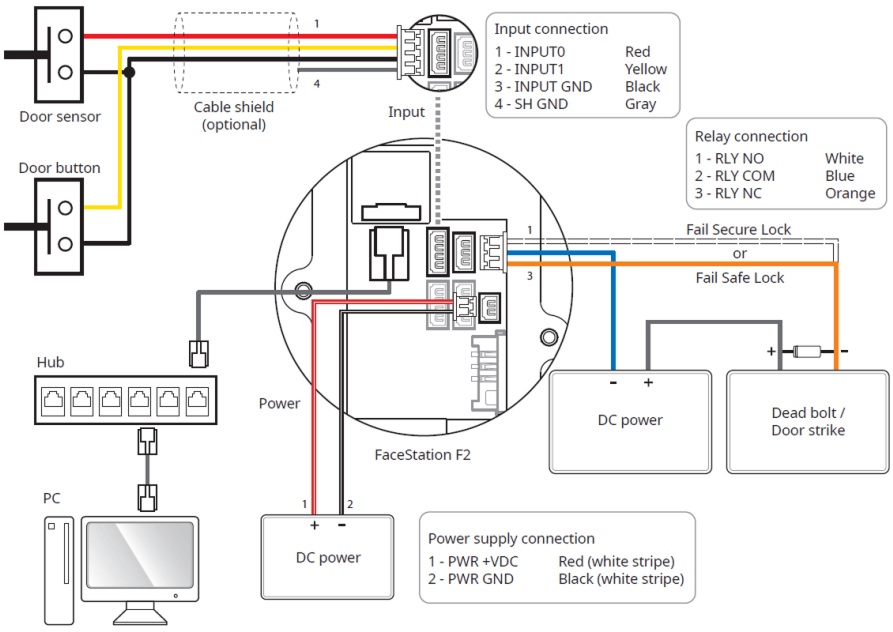
Preste atención a la dirección de instalación del diodo. Instale el diodo cerca de la cerradura.

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.

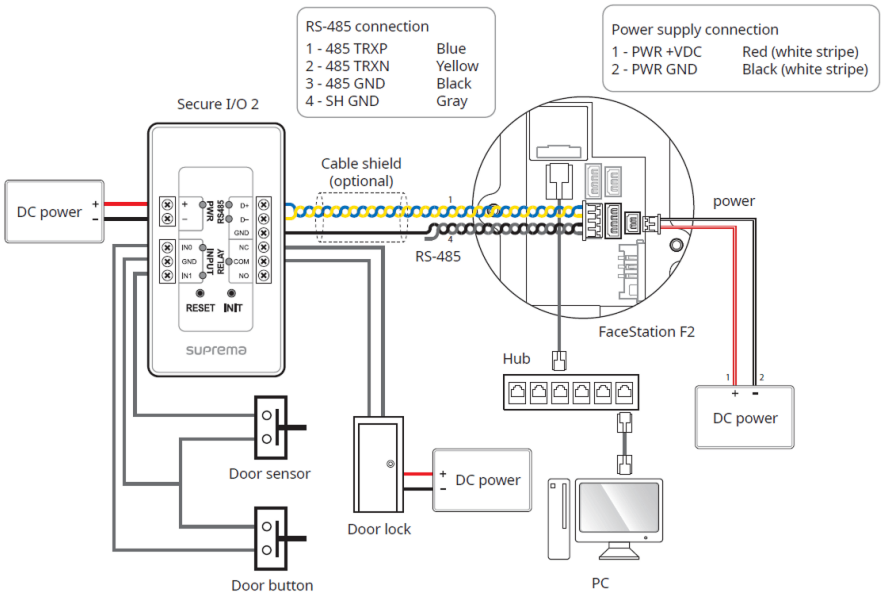
Información

- 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 F2, no se puede agregar otro FaceStation F2 como esclavo.
- Si el dispositivo de autenticación por huella digital es el dispositivo maestro, no se puede agregar FaceStation F2 como dispositivo esclavo.
- Cuando se conecta FaceStation F2 como dispositivo esclavo mientras FaceStation F2 es el dispositivo maestro, solo se puede agregar un FaceStation F2 como dispositivo esclavo.
- Cuando FaceStation F2 es el dispositivo maestro y otro FaceStation F2 se conecta a él como esclavo, se puede conectar adicionalmente un Secure I/O 2 y un DM-20 cada uno.
- Cuando FaceStation F2 es el dispositivo maestro y otro FaceStation F2 está conectado a él como esclavo, no se pueden conectar OM-120 adicionales.
- FaceStation F2 no puede utilizarse como dispositivo esclavo cuando BioStation 3 es el dispositivo maestro y viceversa.
- 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.

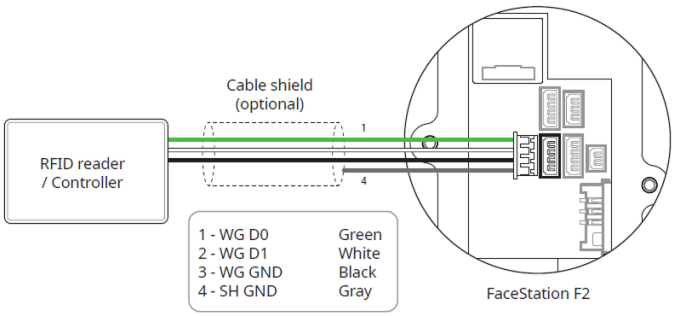


Información

- 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 F2, no se puede agregar otro FaceStation F2 como esclavo.
- Si el dispositivo de autenticación por huella digital es el dispositivo maestro, no se puede agregar FaceStation F2 como dispositivo esclavo.
- Cuando se conecta FaceStation F2 como dispositivo esclavo mientras FaceStation F2 es el dispositivo maestro, solo se puede agregar un FaceStation F2 como dispositivo esclavo.
- Cuando FaceStation F2 es el dispositivo maestro y otro FaceStation F2 se conecta a él como esclavo, se puede conectar adicionalmente un Secure I/O 2 y un DM-20 cada uno.
- Cuando FaceStation F2 es el dispositivo maestro y otro FaceStation F2 está conectado a él como esclavo, no se pueden conectar OM-120 adicionales.
- FaceStation F2 no puede utilizarse como dispositivo esclavo cuando BioStation 3 es el dispositivo maestro y viceversa.
- 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

Use como dispositivo de entrada o salida Wiegand.



Cómo Usar

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

Menú de Administrador

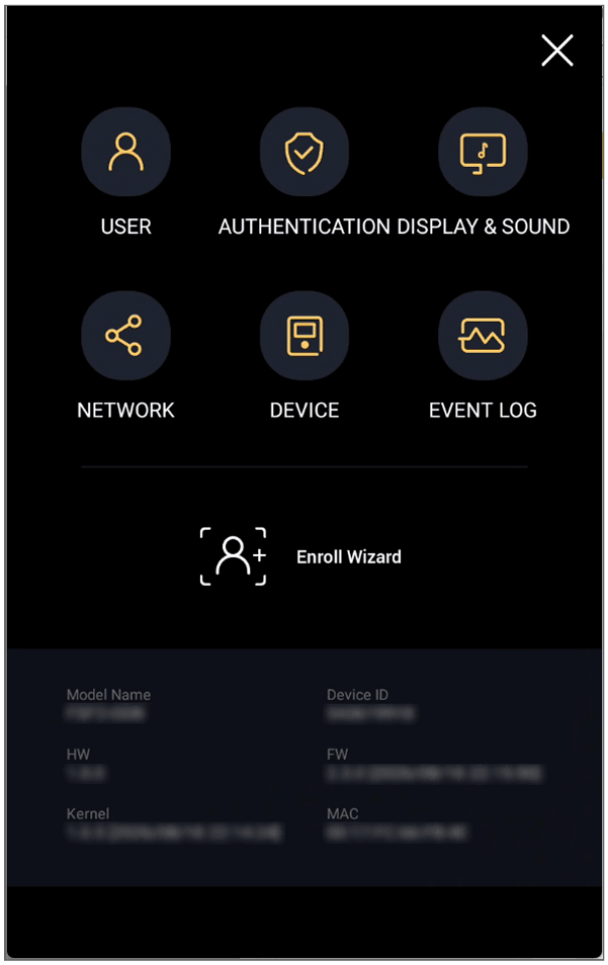
Proporciona orientación sobre los menús principales y las funciones accesibles con privilegios de administrador.

Menú completo

1. Presione y autentíquese con la credencial de nivel de administrador.

   En la pantalla del menú, revise la información del dispositivo o presione **Enroll Wizard** para inscribir a un usuario de inmediato.

2. Selecciona el menú deseado.



Información

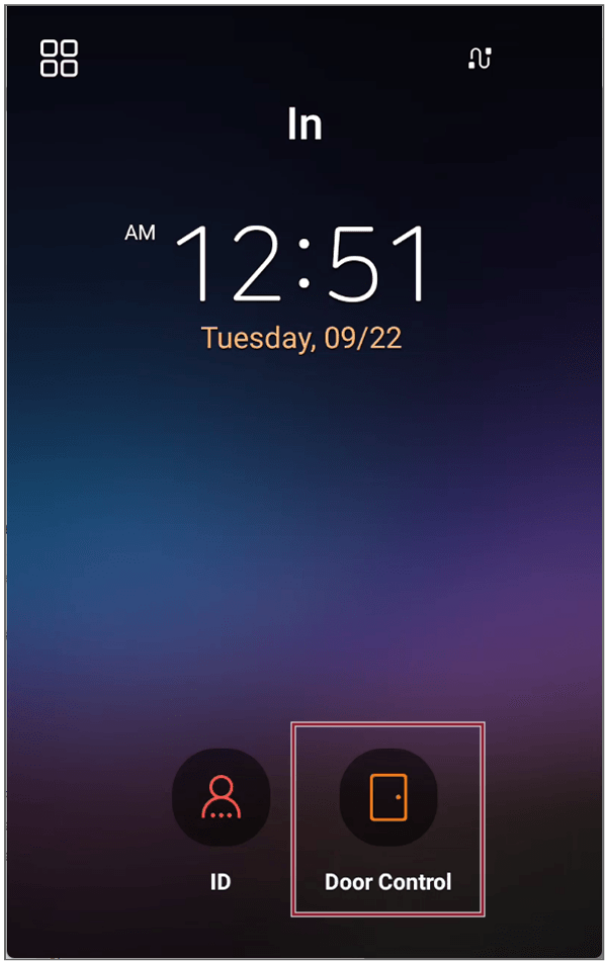
Si no se designa un administrador, haz clic en para mostrar la pantalla del menú.

Control de Puerta

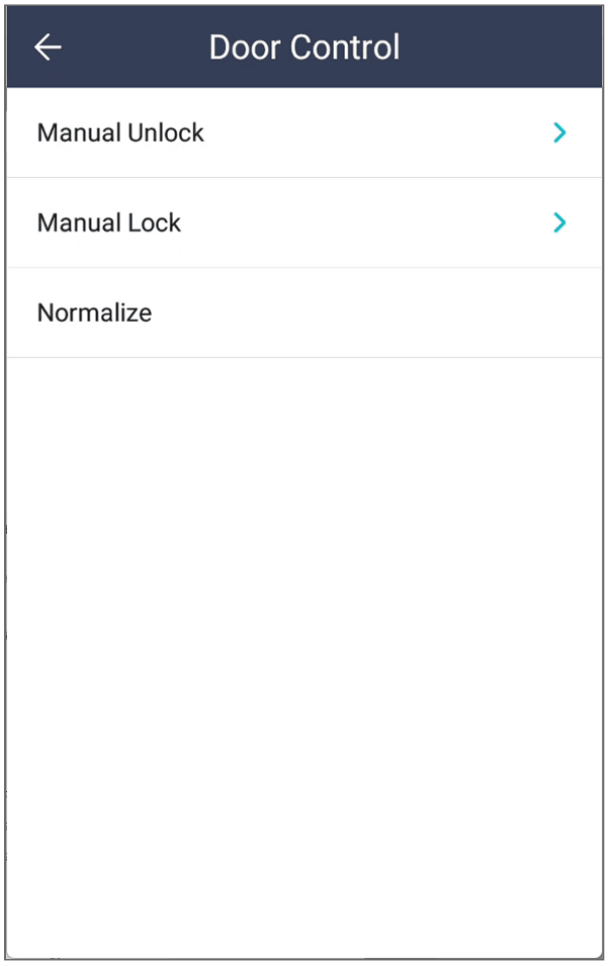
Puede abrir, bloquear o desbloquear manualmente la puerta conectada.

> **Información**
>
> - Solo puede controlar la puerta cuando el dispositivo esté configurado como dispositivo maestro.
> - Utilice **Administrator** o **Configuration** para controlar la puerta.

1. Seleccione **Door Control** en la pantalla principal.



2. Autentica usando el método de privilegio de administrador.
3. Seleccione el método de control de la puerta que desee.



- **Manual Unlock**: Establezca el tiempo para la apertura inmediata de la puerta o para mantenerla abierta.
- **Manual Lock**: Establezca el tiempo para el cierre inmediato de la puerta o para mantenerla bloqueada.
- **Normalize**: Cancele la apertura manual o la retención manual del bloqueo.

> **Información**
> Establezca los tiempos de apertura manual y de retención manual del bloqueo entre 1 y 86,400 segundos.

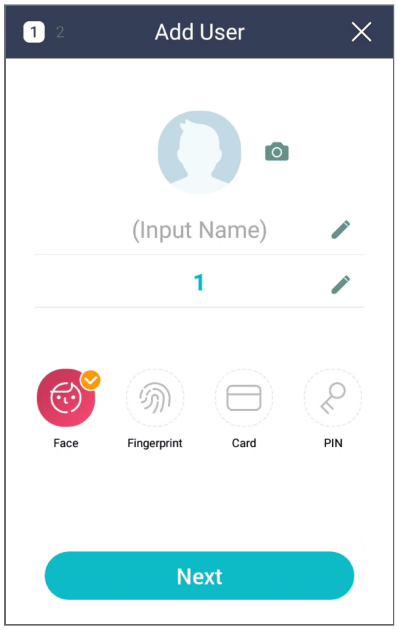
Usuario

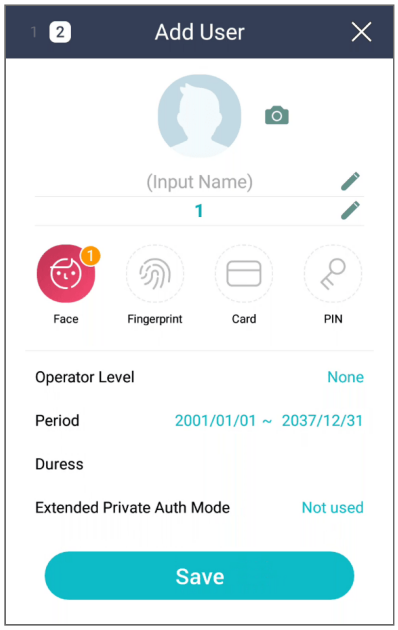
Describe cómo registrar, editar, eliminar y gestionar usuarios.

Registrar información de usuario

Registre información de usuario que incluya datos de autenticación biométrica.

1. Presione y autentíquese con la credencial de nivel de administrador.
2. Seleccione **USER** → y configure los elementos deseados. La información de uso de usuarios aparece.





- : Registre una foto de usuario.
- **Nombre**: Introduzca el nombre de usuario. Ingrese hasta 48 caracteres, incluidos símbolos especiales (`~` `!` `@` `#` `$` `%` `^` `&` `(` `)` `-` `_` `=` `+` `[` `]` `{` `}` `;` `.` `'`). No se permiten nombres que comiencen con `&` `@` `~`.
- **ID**: Ingrese un número entre 1 y 4294967295 para registrar un ID de usuario. Si **User ID Type** está establecido en **Alphanumeric**, ingrese hasta 32 caracteres con caracteres alfanuméricos y ciertos símbolos (`_` `-` `.`). Los ID no pueden incluir espacios. Use puntos (`.`), pero el ID no puede ser un solo punto (`.`) ni dos puntos (`..`).
- **Face**: Registre un rostro para la autenticación del usuario. Presione **Face** → **Next** y siga las instrucciones en pantalla para registrar su rostro. Haga clic en + para inscribir más rostros. Consulte Inscribir rostros de usuario para obtener más información sobre el registro de rostros.
- **Fingerprint**: FSF2-ODB Inscriba una huella para la autenticación del usuario. Presione **Fingerprint** → **Next** y siga las instrucciones en pantalla para inscribir una huella. Presione + para inscribir más huellas. Para obtener más información sobre el registro de huellas, consulte Inscripción de huella digital de usuario.
- **Card**: Inscriba una tarjeta para la autenticación del usuario. Presione **Card** → **Next** y escanee la tarjeta que se asignará al usuario en la sección de autenticación de tarjeta RF. Haga clic en + para inscribir más tarjetas.
- **PIN**: Ingrese el PIN que desea usar. Presione **PIN** → **Next** e introduzca el PIN que desea usar. Para confirmarlo, introduzca el PIN nuevamente y luego presione **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**: Utilice los menús **AUTHENTICATION**, **DISPLAY & SOUND**, **DEVICE**, **NETWORK**, **EVENT LOG**.
> – **User Management**: Puede usar los menús **USER**, **EVENT LOG**.

- **Period**: Configure la duración de uso de la cuenta de usuario.
- **Duress**: FSF2-ODB Seleccione para inscribir una huella de coacción. Si alguien lo coacciona o necesita abrir la puerta por la fuerza, autenticar con esta huella enviará una señal de alarma a BioStar X.
- **Extended Private Auth Mode**: Configura el modo ampliado de autenticación personal. Con el modo de autenticación personal extendido, es posible combinar métodos de autenticación, incluidos rostro y huella, para cada usuario. De lo contrario, utilice el modo de autenticación básico del dispositivo.

> **Información**
> El registro de huellas solo está disponible en el producto FSF2-ODB.

3. Presione **Save** para completar el registro de la información del usuario.

Inscribir rostros de usuario

1. Presione y autentíquese con la credencial de nivel de administrador.
2. Seleccione **USER** → .
3. Presione **Face** → **Next**.
4. Ajuste la distancia entre el rostro y la pantalla y mire directamente a la cámara del dispositivo.
5. Cuando la captura se complete, presione **OK** → **Save**. Para volver a tomar la foto de su rostro, presione **Re-Shot**.

Información

- Los datos de visual face de este producto no son compatibles con las plantillas de face de FaceStation 2 ni con las de FaceLite.
- Inscriba el rostro del usuario en el dispositivo y en masa en BioStar X. Cargue una foto o importe un archivo CSV. Envíe a un usuario un enlace para inscribir su rostro en su dispositivo móvil personal. Para obtener información detallada sobre cada método de registro, consulte la Guía del Administrador de BioStar X.
- Para usar correctamente la función Visual Face, tome una foto siguiendo las instrucciones a continuación.
  - Mantén una distancia de 60 a 100 cm entre el dispositivo y tu rostro al enrolar tu 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.

Inscripción de huella digital de usuario FSF2-ODB

1. Presione y autentíquese con la credencial de nivel de administrador.
2. Seleccione **USER** → .
3. Presione **Fingerprint** → **Next**.
4. Después de escanear la huella del dedo que se va a inscribir, escanee nuevamente la huella del mismo dedo.

Información

- El registro de huellas solo está disponible en el producto FSF2-ODB.
- Coloque el dedo lo suficientemente profundo para que haga contacto completo con el sensor.
- Coloque el centro de la huella en el centro del sensor.
- Si un dedo tiene un corte o la huella está borrosa, seleccione otro dedo para la huella.
- Ingrese con precisión según las instrucciones en pantalla al autenticar huellas.
- Si mantiene el dedo en posición vertical de modo que se reduzca el área de contacto con el sensor o cambia el ángulo del dedo, es posible que la autenticación de la huella no se realice.

Modificar información de usuario

El gestor de usuarios o el administrador pueden modificar la información de usuario registrada. Agregue el rostro, la huella digital o la tarjeta del usuario y modifique el PIN y el nivel.

1. Presione y autentíquese con la credencial de nivel de administrador.
2. Haga clic en **USER** → .
3. Seleccione los términos de búsqueda. Busque usuarios con **All**, **User ID**, **Name**, **Face**, **Fingerprint**, **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**
>
> - La búsqueda por huella solo está disponible en el producto FSF2-ODB.
> - **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

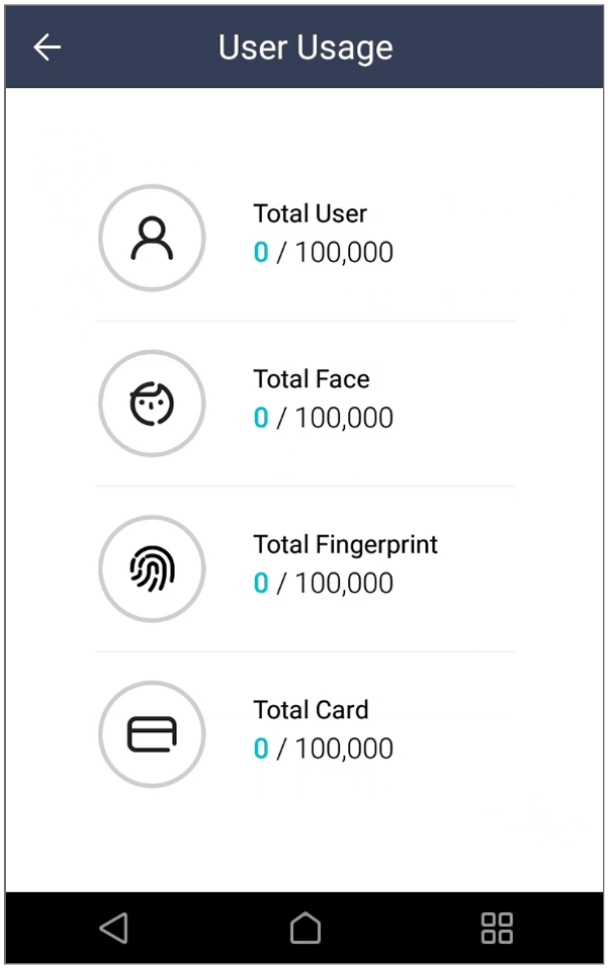
Elimine todos los usuarios registrados a la vez.

1. Presione y autentíquese con la credencial de nivel 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

Vea de un vistazo la cantidad de usuarios, rostros, huellas y tarjetas inscritos.

1. Presione y autentíquese con la credencial de nivel de administrador.
2. Presione **USER** → . La información de uso de usuarios aparece.



Información
La cantidad de huellas solo se puede verificar en el producto FSF2-ODB.

Autenticación

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

Modo de autenticación

Configura el modo de autenticación. Utilice rostro, huella, PIN, tarjeta e ID en combinación como modos de autenticación y configure también el horario para cada modo.

Información
La autenticación por huella solo está disponible en el producto FSF2-ODB.

Registrar modo de autenticación

1. Presione y autentíquese con la credencial de nivel de administrador.

2. Presione **AUTHENTICATION** → **Auth Mode** → .
3. Seleccione y elija el método de autenticación que desea usar. Seleccione del mismo modo el método de autenticación adicional y combínelo.
4. Configure **Schedule**.

> **Información**
>
> - Combine los métodos de autenticación seleccionados para autenticar todos en orden o elija autenticar solo algunos de ellos. Por ejemplo, si se combinan como + + , deberá autenticar la tarjeta, rostro y PIN; cuando se combinan como + / , deberá autenticar la tarjeta y luego ingresar el rostro o el PIN.
> - **Schedule** se puede configurar en BioStar X. Si no hay un horario configurado, solo se pueden seleccionar **Not Use** y **Always**.
> - Para más información sobre la configuración de **Schedule**, consulte la Guía del administrador de BioStar X.

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

Modificar modo de autenticación

1. Presione y autentíquese con la credencial de nivel 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. Presione y autentíquese con la credencial de nivel de administrador.
2. Presione **AUTHENTICATION** → **Auth Mode**.
3. Pulsa y selecciona el modo de autenticación que deseas eliminar. Es posible seleccionar varias opciones.
4. Presione **OK**, luego **OK** para eliminar el elemento seleccionado. Presiona **Cancel** para regresar a la pantalla anterior.

Autenticación en servidor

Configura la autenticación en servidor. El uso de la autenticación en servidor significa que la autenticación del usuario se realiza en BioStar X y no en el dispositivo. La autenticación en servidor puede ser útil cuando hay demasiada información de usuarios en el dispositivo o cuando se instala fuera de la puerta de entrada.

1. Presione y autentíquese con la credencial de nivel de administrador.
2. Presione **AUTHENTICATION** y luego active **Server Matching**.

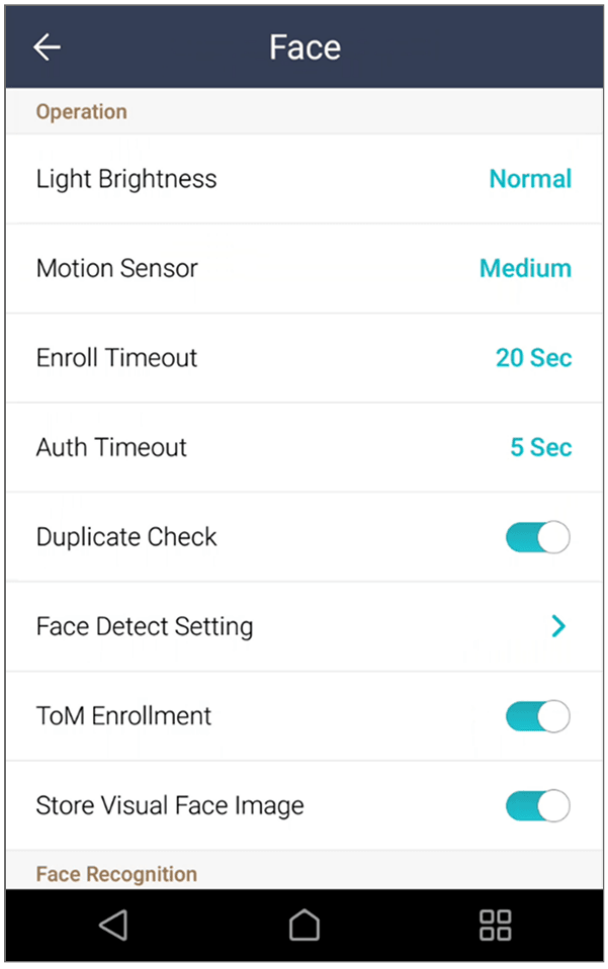
- FSF2-ODB: **Server Matching (Fingerprint, Card, ID)**
- FSF2-DB, FSF2-AB: **Server Matching (Card, ID)**

> **Información**
>
> - **Server Matching** solo puede usar huella, tarjeta 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.

Rostro

Cambie la configuración de la autenticación facial.

1. Presione y autentíquese con la credencial de nivel de administrador.
2. Selecciona **AUTHENTICATION** → **Face**.
3. Cambie el elemento deseado.



- **Light Brightness**: Permite ajustar manualmente el brillo de la luz del dispositivo. Ajuste el brillo con **Normal** o **High** o seleccione **Not Use** para apagar la luz.
- **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.

- **Enroll Timeout**: Si el rostro no se registra dentro del tiempo establecido, el registro se cancelará.
- **Auth Timeout**: Si la autenticación no se completa dentro del tiempo establecido, la autenticación falla.
- **Duplicate Check**: Permite verificar rostros duplicados durante el registro de rostro.
- **Face Detect Setting**: Defina la posición y el tamaño del área donde el dispositivo detecta rostros durante la autenticación facial.

> **Información**
> Para un rendimiento óptimo, se recomienda usar los valores predeterminados de las subopciones de **Face Detect Setting**. Los valores predeterminados de cada opción son los siguientes:
> – Ángulo máximo de orientación de la cabeza: 15
> – Distancia de detección: mín. 30 cm, máx. 100 cm
> – Búsqueda amplia: desactivada

- **ToM Enrollment**: Al activar **ToM Enrollment**, podrá enrolar la **Template on Mobile** emitida por BioStar X. **Template on Mobile** permite la autenticación biométrica sin almacenar datos de usuario en el servidor BioStar X, Airfob Portal o dispositivo, al guardar la plantilla biométrica del usuario en una tarjeta de acceso móvil.

> **Información**
> Para más información sobre **Template on Mobile**, consulta la Guía del administrador de BioStar X.

- **Store Visual Face Image**: Configure para almacenar tanto las imágenes reales como las plantillas en Visual Face, o para guardar solo las plantillas sin imágenes. Si se desactiva, se eliminarán todas las imágenes almacenadas de rostros visuales y los rostros visuales enrolados posteriormente almacenarán solo las plantillas, sin imágenes.

> **Información**
> Después de desactivar esta configuración, conéctate a BioStar 2 v2.9.7 o superior o a BioStar X.

- **Security Level**: Configura el nivel de seguridad para la autenticación 1:N.
- **Operation Mode**: Configure el modo de funcionamiento del dispositivo para la autenticación facial.
  - **Fusion Matching**: La coincidencia visual e infrarroja funciona conjuntamente para aumentar la precisión de la autenticación facial.
  - **Fast Matching**: Los usuarios pueden autenticarse rápidamente mientras caminan dentro del rango de autenticación del dispositivo.
- **Fake Detection**: Evite la autenticación de usuarios con rostros falsificados, como fotografías. Se activa cuando **Operation Mode** está configurado en **Fusion Matching**.

> **Información**
> Con luz solar intensa, se recomienda usar la función **Fake Detection** como **Normal**.

- **Advanced Settings**: Permite cambiar ajustes avanzados de autenticación facial, como la detección de mascarilla y las funciones de la cámara térmica.
  - **Check Mode**: Permite establecer el modo de confirmación según la finalidad.

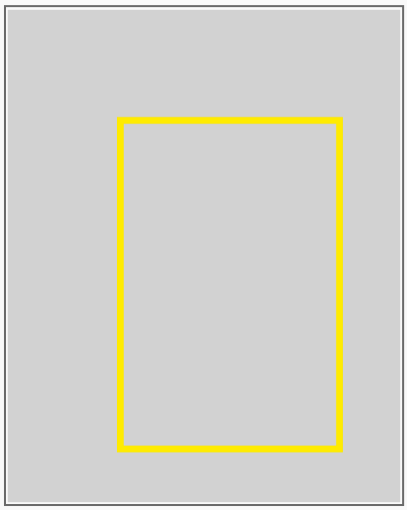
    > **Información**
    >
    > Al usar **Mask Detection** o **Thermal Camera**, configure **Check Mode** según la finalidad del dispositivo.
    >
    > - **Check After Authentication**: Después de la autenticación, verifica si el usuario lleva mascarilla o mide la temperatura.
    > - **Check Before Authentication**: Después de comprobar si el usuario lleva mascarilla o de medir la temperatura, realiza la autenticación. Al usar este modo, los usuarios sin mascarilla o con temperatura superior al estándar no pueden autenticarse.
    > - **Check Only**: El dispositivo solo sirve para verificar si se lleva mascarilla o para medir la temperatura. Al usar este modo, los usuarios que lleven mascarilla o que estén por debajo de la temperatura estándar pueden ingresar sin autenticación.

  - **Authentication Fail Sound**: Permite definir el estado de notificación para fallos de autenticación debidos a la ausencia de mascarilla o a temperatura superior al estándar.
  - **Mask Detection**: Configure si se utiliza la detección de mascarillas.
    - **Enabled (Hard)**: Los usuarios sin mascarilla serán rechazados y el evento sin mascarilla se registrará en los registros.
    - **Enabled (Soft)**: Los usuarios sin mascarilla aún podrán autenticarse, pero se registrará un evento sin mascarilla.
- **Thermal Camera**: Puede establecer si se utilizará la cámara térmica.
  - **Enabled (Hard)**: Los usuarios con temperatura superior al rango estándar serán rechazados y el evento se registrará como temperatura superior al estándar.
  - **Enabled (Soft)**: Los usuarios con temperatura superior al rango estándar aún podrán autenticarse, pero el evento se registrará como temperatura superior al estándar.

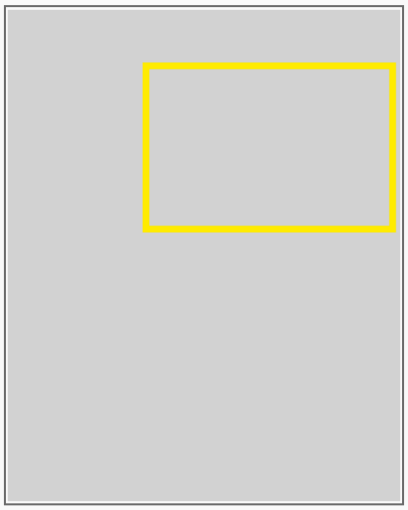
Información

- Cuando **Thermal Camera** se ajusta a **Enabled**, se activan las opciones avanzadas de la cámara térmica.
  - **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. Los usuarios con temperatura superficial inferior a **Low Threshold Temperature** serán rechazados. **Low Threshold Temperature** puede establecerse en un rango de 1℃~45℃ y no puede configurarse por encima de **High Threshold Temperature**.
  - **High Threshold Temperature**: Puede establecer la temperatura máxima de referencia para restringir el acceso. Los usuarios con temperatura superficial superior a **High Threshold Temperature** serán rechazados. **High Threshold Temperature** puede establecerse en un rango de 1℃~45℃ y no puede configurarse por debajo de **Low Threshold Temperature**.
  - **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**: Establece si el video infrarrojo se muestra en la pantalla del dispositivo.
  - **Dynamic ROI**: Configura el dispositivo para que detecte automáticamente la zona de interés (ROI) para medir la temperatura del usuario. Por ejemplo, si hay otras luces instaladas cerca, esta opción permite que la cámara térmica detecte y mida la temperatura del usuario en lugar de esa iluminación.
  - **Camera Configuration**: Establece opciones detalladas de la cámara para una medición precisa.

- Cuando **Thermal Camera** se ajusta a **Enabled**, configura opciones detalladas de la cámara térmica para una medición precisa según el entorno de instalación.
  - **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(%)**: Permite configurar manualmente la ROI (región de interés) cuando **Dynamic ROI** está ajustado a **Not Use**. Ajuste la ubicación y el tamaño de la ROI para especificar el área donde la cámara térmica medirá la temperatura. **ROI X(%)** indica las posiciones izquierda y derecha de la región de interés; cuanto mayor sea este valor, más se desplazará la región hacia la derecha de la pantalla. **ROI Y(%)** indica las posiciones superior e inferior de la región de interés; cuanto mayor sea este valor, más se desplazará la región hacia arriba. **ROI Width(%)** y **ROI Height(%)** indican el tamaño de la región de interés; al aumentar ambos valores, el área para medir la temperatura se amplía. Por ejemplo, si los valores de **ROI X(%)**, **ROI Y(%)**, **ROI Width(%)**, **ROI Height(%)** se cambian de los valores predeterminados a 40, 15, 70 y 40 respectivamente, la región de interés cambiará como se muestra a continuación.



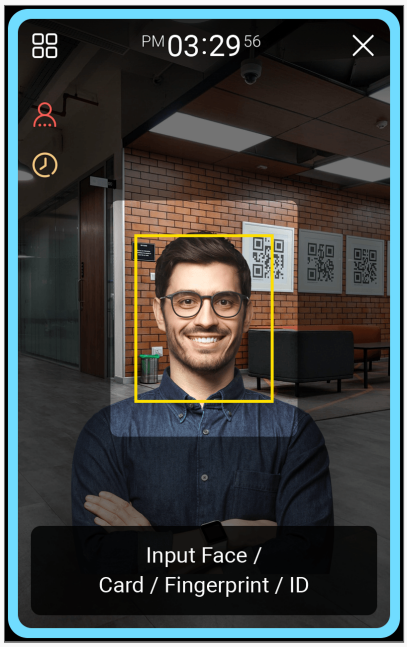
Si la ROI está configurada con el valor predeterminado



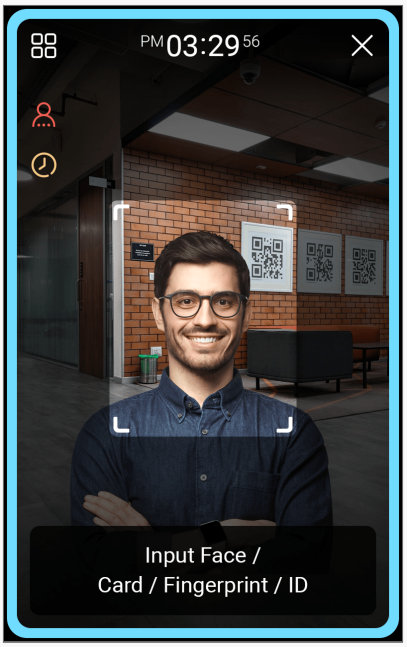
ROI X(%), ROI Y(%), ancho de ROI (%), alto de ROI (%) Cuando los valores se cambian a 40, 15, 70 y 40, respectivamente

  - **Skin Temperature Compensation**: Configure la cámara termográfica para corregir la temperatura de forma autónoma, teniendo en cuenta el uso ambiental del dispositivo y la temperatura circundante.
  - **Skin Temperature Correction**: Ajuste las mediciones de temperatura para que aumenten o disminuyan en un valor constante según el entorno de uso del producto. Por ejemplo, si la lectura de temperatura siempre se mide 0.1℃ más alta, establezca el valor de corrección de temperatura en -0.1.
  - **FW**: Si la cámara termográfica está correctamente conectada, se mostrará la versión del firmware de dicha cámara.
- Para un rendimiento óptimo, se recomienda usar los valores predeterminados en las subopciones de **Camera Configuration**. Los valores predeterminados de cada opción son los siguientes:
  - **Distance(cm)**: 100
  - **Emissivity**: 0.98
  - **ROI X(%)**: 30
  - **ROI Y(%)**: 25
  - **ROI Width(%)**: 50
  - **ROI Height(%)**: 55

Cuando use el ROI como configuración predeterminada, se mostrará una guía amarilla en el área de ROI de la pantalla durante la autenticación, como se muestra a continuación. Cuando el rostro del usuario esté alineado dentro de esa área durante la autenticación, se podrán realizar mediciones de temperatura precisas. Cuando cambie la configuración manualmente o use un ROI dinámico, la guía amarilla no se mostrará.



Si la ROI está configurada con el valor predeterminado



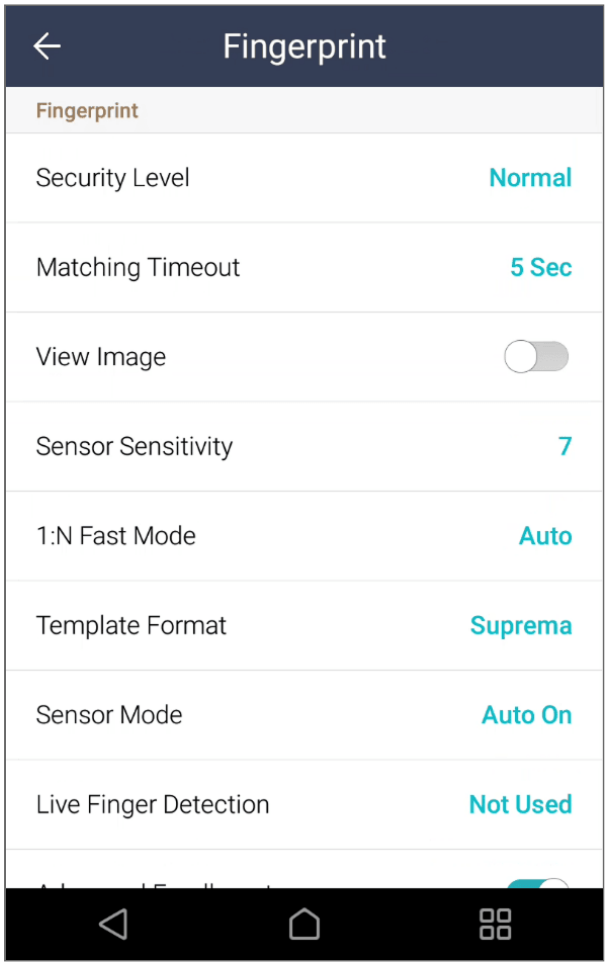
Al cambiar la configuración de ROI o usar ROI dinámico

- Las funciones de autenticación con mascarilla y de cámara termográfica no están disponibles en los dispositivos esclavos.
- La cámara termográfica es compatible con TCM10-FSF2.

Huella dactilar FSF2-ODB

Cambia los ajustes de autenticación por huella digital.

1. Presione y autentíquese con la credencial de nivel de administrador.
2. Seleccione **AUTHENTICATION** → **Fingerprint**.
3. Cambie el elemento deseado.

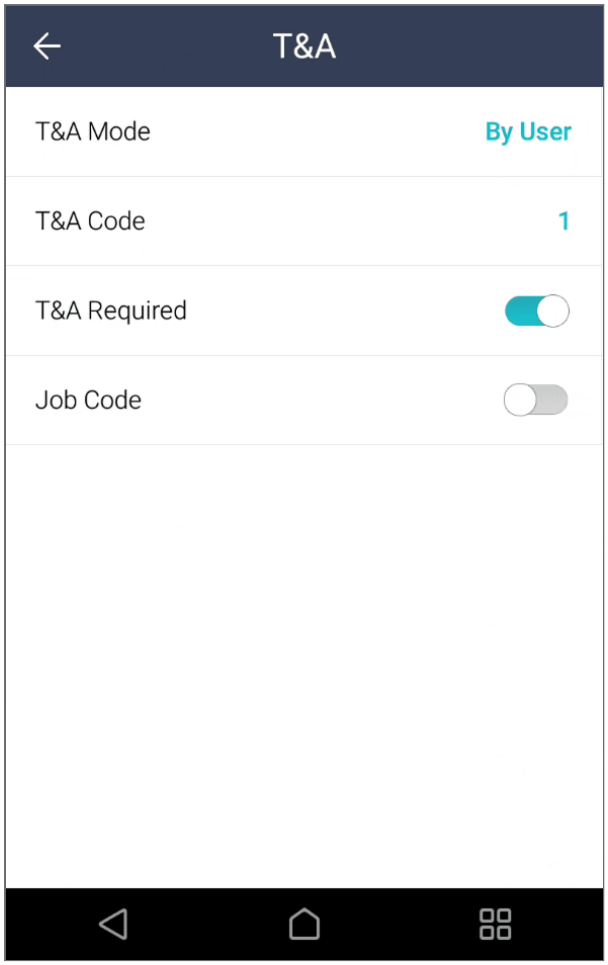


- **Security Level**: Configura el nivel de seguridad para la autenticación 1:N.
- **Matching Timeout**: Configura el tiempo de espera para la correspondencia de huellas. Si la autenticación no se completa dentro del tiempo especificado, fallará.
- **View Image**: Se puede ver la imagen original de la huella escaneada.
- **Sensor Sensitivity**: Configura la sensibilidad del sensor de reconocimiento de huellas. Establece la sensibilidad más alta para obtener información de huella dactilar precisa.
- **1:N Fast Mode**: Configura la velocidad de la autenticación por huella. Al seleccionar **Auto**, la velocidad de autenticación se ajusta según el total de plantillas de huellas almacenadas en el dispositivo.
- **Template Format**: Configura el formato de plantilla de huella. **SUPREMA** está configurado por defecto. Al cambiar el formato de la plantilla, las huellas digitales guardadas anteriormente quedarán inutilizables, así que tenga cuidado al modificarlo.
- **Sensor Mode**: Configura en **Auto On** para encender el sensor de huella cuando detecte el dedo del usuario. Al configurarse en **Always On**, el sensor permanece encendido aunque no se estén escaneando huellas.
- **Live Finger Detection**: Configura el nivel de detección de huellas falsas. Niveles más altos de detección de huellas falsas pueden aumentar las tasas de rechazo de las huellas reales.
- **Advanced Enrollment**: Evalúa la calidad de las huellas escaneadas para guardar información de alta calidad. Habilite la notificación para avisar al usuario cuando la calidad de la huella digital sea baja, ayudándole a escanearla correctamente.
- **Duplicate Check**: Verifica huellas duplicadas durante el enrolamiento.

T&A (Tiempo y Asistencia)

Configura cómo registrar el modo T&A.

1. Presione y autentíquese con la credencial de nivel de administrador.
2. Selecciona **AUTHENTICATION** → **T&A Mode**.
3. Cambie el elemento deseado.

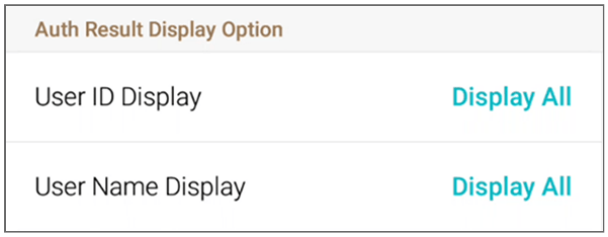


- **T&A Mode**: Configura cómo usar el modo de asistencia.
- **T&A Code**: Registra eventos de T&A. Para registrar eventos de asistencia, seleccione **T&A Code** → y luego configure el icono para que se muestre en pantalla, Nombre de Evento de T&A y Programación.
- **T&A Required**: Configure para que 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.

Opciones de visualización del resultado de autenticación

Configura la opción de visualización del resultado de autenticación.

1. Presione y autentíquese con la credencial de nivel de administrador.
2. Seleccione **AUTHENTICATION**.
3. Configure los elementos deseados en **Auth Result Display Option**.



- **User ID Display**: Seleccione cómo se muestra el ID de usuario en la pantalla de resultados de autenticación del dispositivo.
  - **Display All**: Muestra el ID completo del usuario.
  - **Mask All but First Letter**: Muestra solo la primera letra del ID de usuario.
  - **Hide All**: No mostrar el ID de usuario.
- **User Name Display**: Seleccione cómo se muestra el nombre del usuario en la pantalla de resultados de autenticación del dispositivo.
  - **Display All**: Muestra el nombre de usuario completo.
  - **Mask All but First Letter**: Muestra solo la primera letra del nombre del usuario.
  - **Hide All**: No mostrar el nombre del usuario.

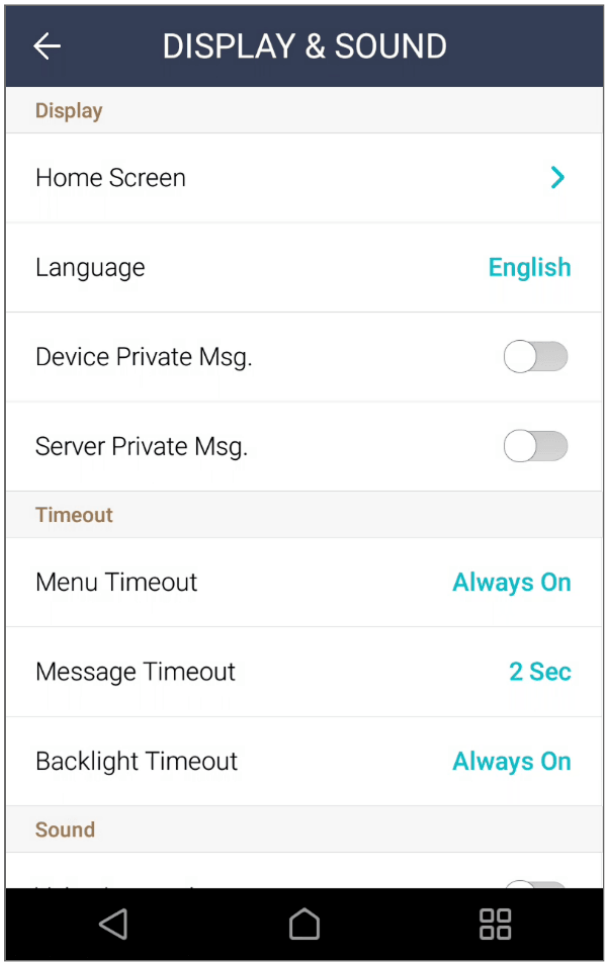
Ajustes

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

Pantalla y sonido

Cambie los ajustes de pantalla y sonido del dispositivo.

1. Presione y autentíquese con la credencial de nivel 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.
- **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.

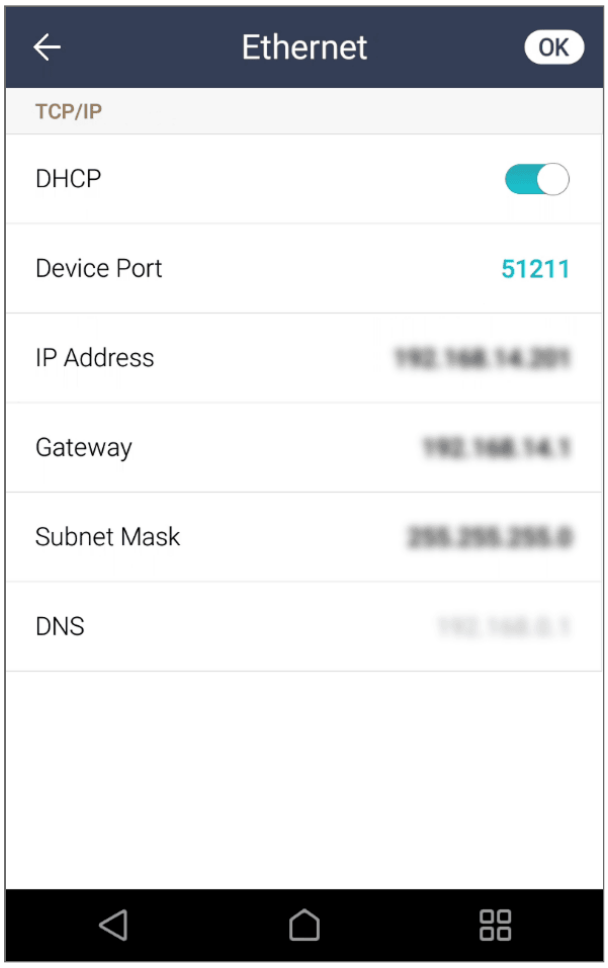
> **Información**
>
> Para obtener más información sobre el SDK de dispositivos BioStar, consulte la página del SDK de dispositivos BioStar en la base de conocimientos de Suprema.

Ajustes de comunicación

Cambie los ajustes de red del dispositivo, como Ethernet, servidor, OSDP, etc.

Ethernet

1. Presione y autentíquese con la credencial de nivel de administrador.
2. Seleccione **NETWORK** → **Ethernet**.
3. Cambie el elemento deseado.



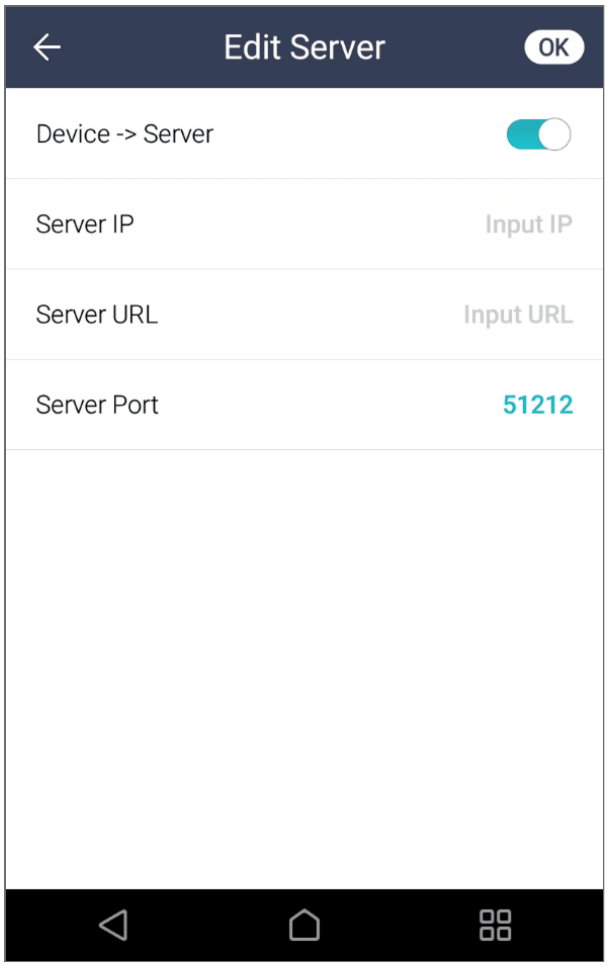
- **DHCP**: Configure si se utiliza DHCP. Desactive la configuración DHCP para permitir que los usuarios modifiquen **Device Port**, **IP Address**, **Gateway** y **Subnet Mask**.
- **Device Port**: Configure el puerto del dispositivo.
- **IP Address**: Compruebe la dirección IP del dispositivo. Para 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.

Servidor

1. Presione y autentíquese con la credencial de nivel de administrador.
2. Seleccione **NETWORK** → **Server**.
3. Cambie el elemento deseado.

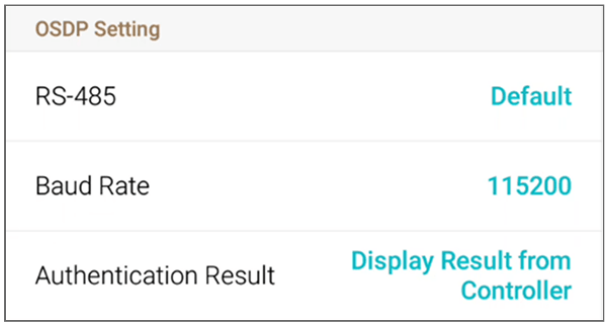


- **Device → Server**: Envíe directamente una señal de conexión desde el dispositivo a un servidor con la información ingresada. Cuando **Device → Server** está habilitado, el usuario puede ingresar **Server IP**, **Server URL** y **Server Port**.
- **Server IP**: Ingrese la dirección IP de la PC donde 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.

Ajustes de OSDP

1. Presione y autentíquese con la credencial de nivel de administrador.
2. Seleccione **NETWORK**.
3. Configure el elemento deseado en **OSDP Setting**.



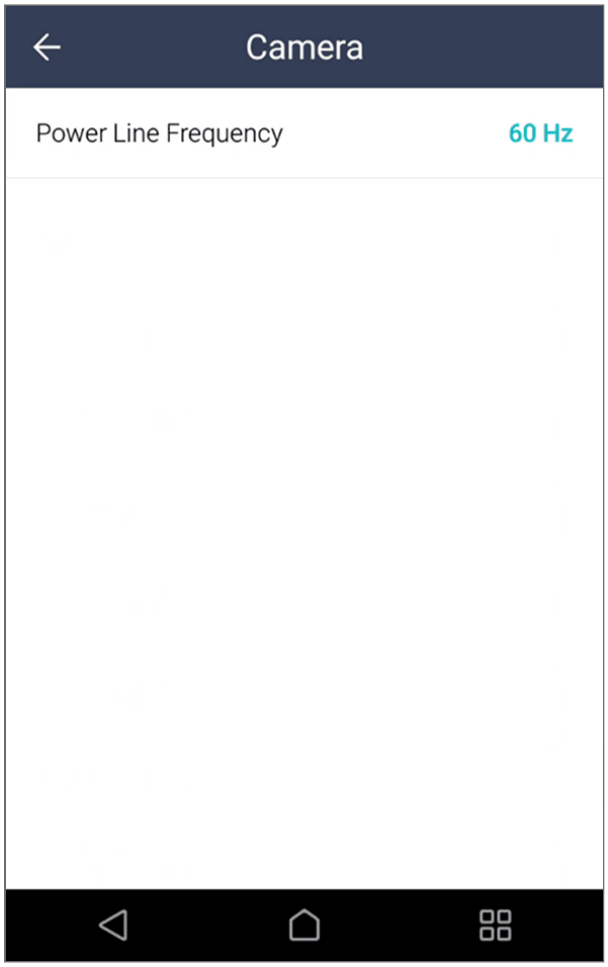
- **RS-485**: Seleccione el modo RS-485.
- **Baud Rate**: Seleccione la velocidad en baudios deseada.
- **Authentication Result**: Al usar **Intelligent Slave**, seleccione mostrar en pantalla los resultados de autenticación de controladores o dispositivos de terceros. Esta opción puede utilizarse cuando el modo de **RS-485** está configurado en **Default** o **Slave**.

Dispositivo

Cámara

Configure la frecuencia para evitar el parpadeo del video.

1. Presione y autentíquese con la credencial de nivel de administrador.
2. Presione **DEVICE** → **Camera**.

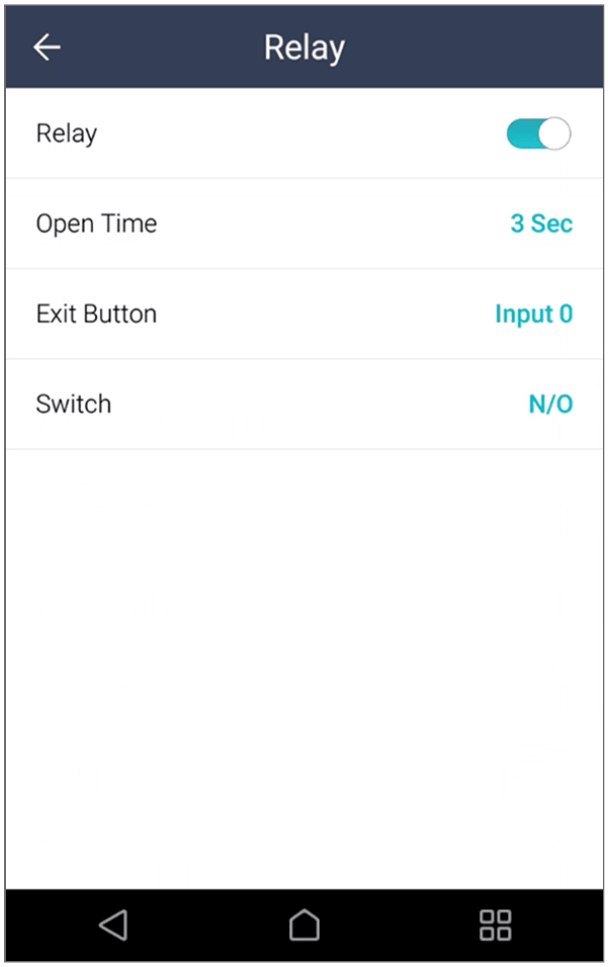


- **Power Line Frequency**: Configure la frecuencia a 50 Hz o 60 Hz para evitar que el video parpadee según las condiciones de iluminación ambiental.

Relé

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

1. Presione y autentíquese con la credencial de nivel de administrador.
2. Haga clic en **DEVICE** → **Relay**.

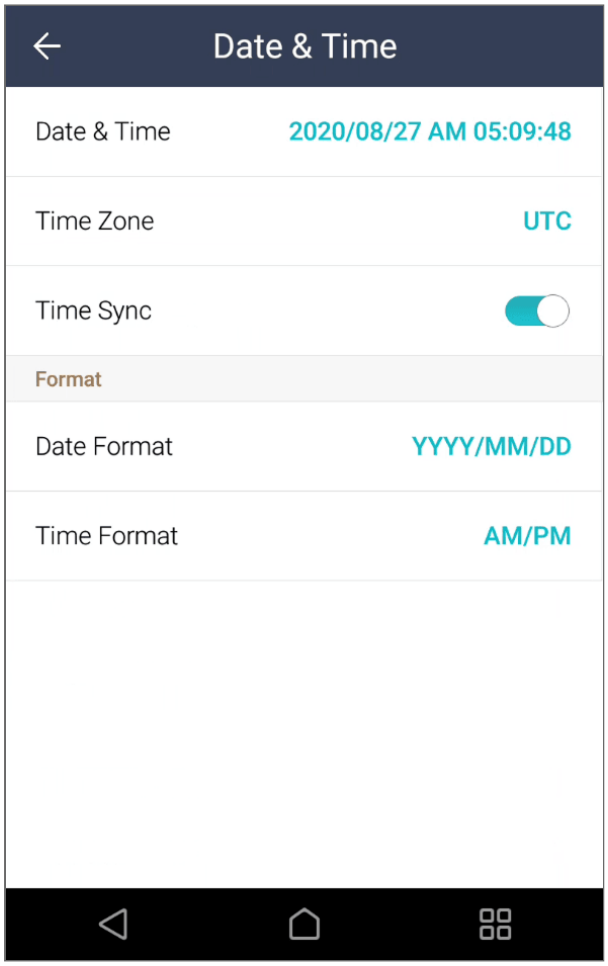


- **Relay**: Configure si el relé está habilitado. Habilitar el ajuste de relé permite configurar **Open Time** y **Exit Button**.
- **Open Time**: Establece la duración que la puerta permanece abierta cuando se ha realizado la autenticación de usuario estándar.
- **Exit Button**: Selecciona el puerto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

Fecha y hora

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

1. Presione y autentíquese con la credencial de nivel de administrador.
2. Haz clic en **DEVICE** → **Date & Time**.
3. Cambie el elemento deseado.

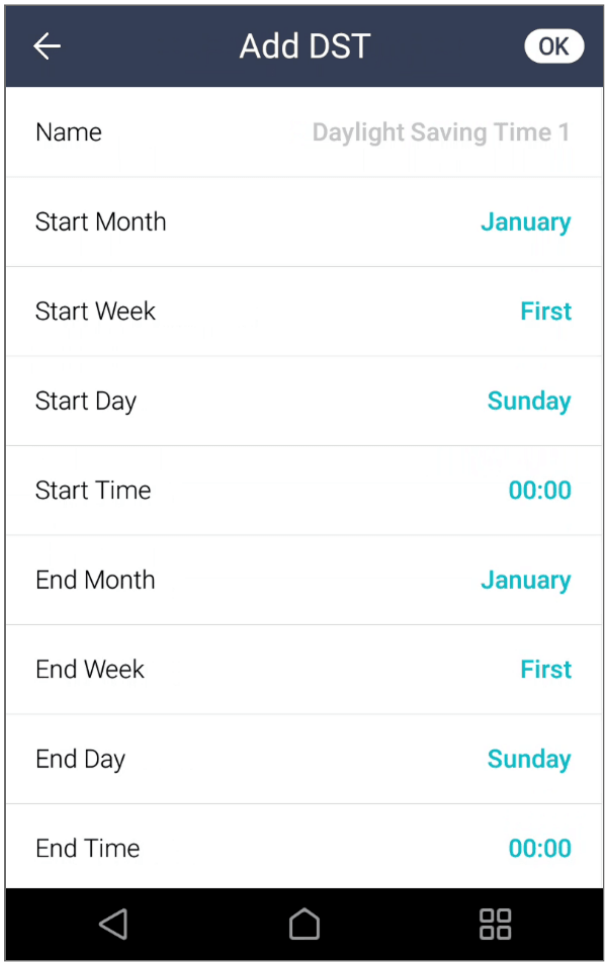


- **Date & Time**: Compruebe la fecha y hora actuales. Para modificarla manualmente, desactive **Time Sync**.
- **Time Zone**: Ajuste la referencia horaria de la ubicación actual.
- **Time Sync**: Sincronice el servidor y la hora. Si desea sincronizar el servidor y la hora, habilite **Time Sync**.
- **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. Presione y autentíquese con la credencial de nivel de administrador.
2. Haz clic en **DEVICE** → **Daylight Saving Time**, luego presiona para agregar el horario de verano.
3. Cambie el elemento deseado.



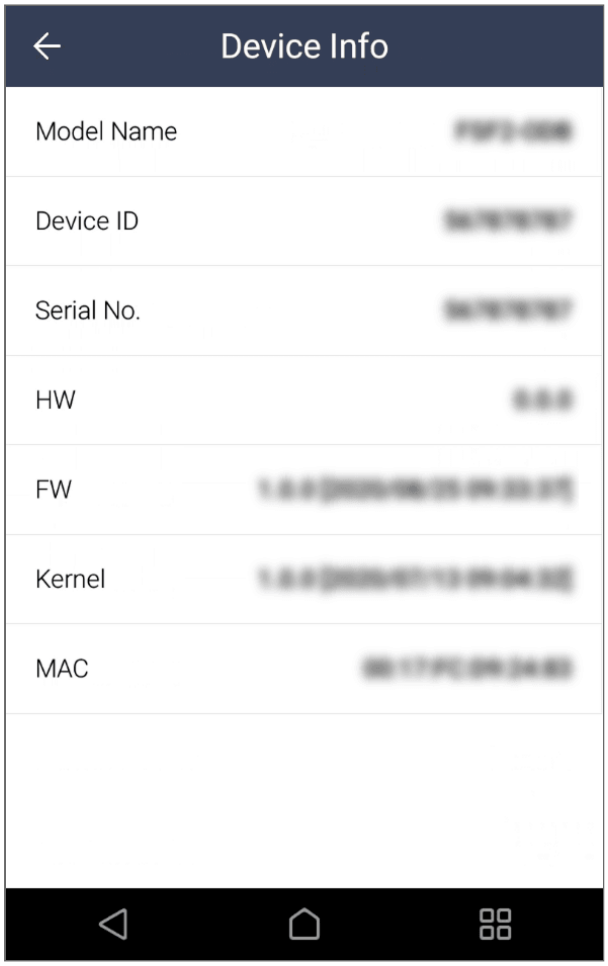
- **Name**: Establece el nombre del horario de verano.
- **Start Month** / **Start Week** / **Start Day** / **Start Time**: Configure los detalles sobre cuándo comienza el horario de verano.
- **End Month** / **End Week** / **End Day** / **End Time**: Configure los detalles sobre cuándo termina el horario 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.

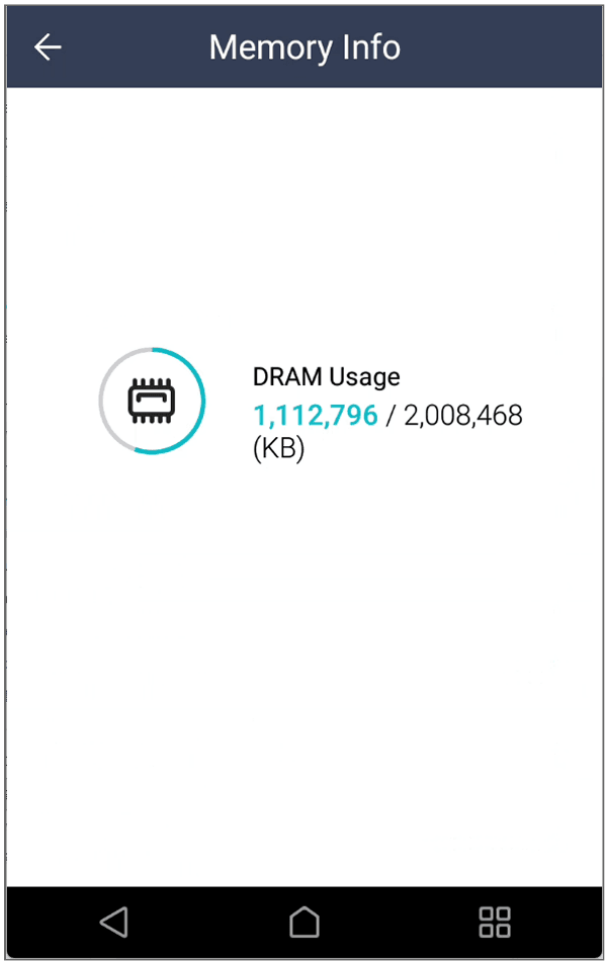
1. Presione y autentíquese con la credencial de nivel de administrador.
2. Selecciona **DEVICE** → **Device Info**. Verifica la información de **Model Name**, **Device ID**, **Serial No.**, **HW**, **FW**, **Kernel**, **MAC**.



Información de memoria

Consulta el estado de uso de la memoria.

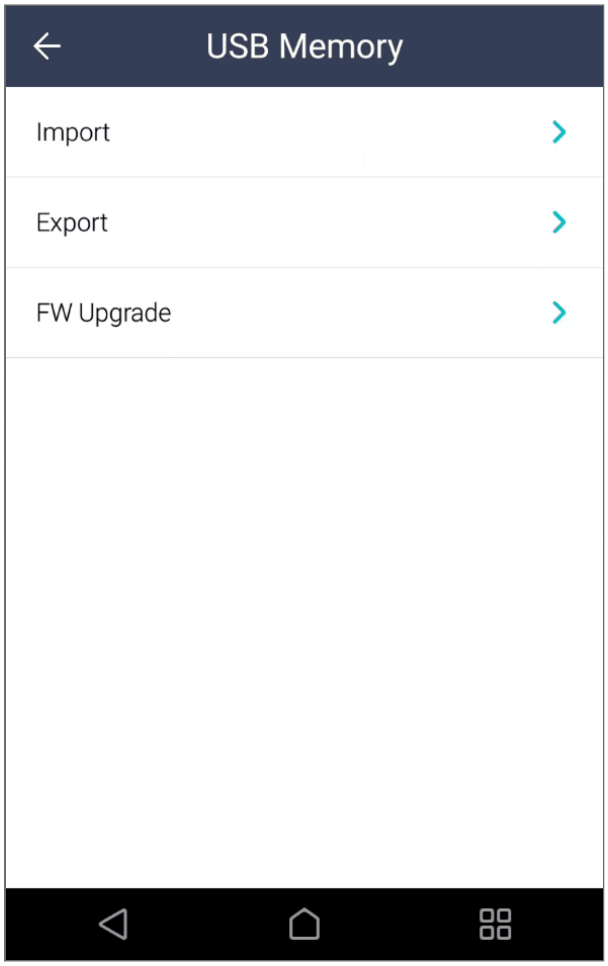
1. Presione y autentíquese con la credencial de nivel de administrador.
2. Selecciona **DEVICE** → **Memory Info**. Consulta el estado de uso de memoria del dispositivo.



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. Presione y autentíquese con la credencial de nivel de administrador.
2. Selecciona **DEVICE** → **USB Memory**.
3. Selecciona el elemento deseado y cambia el ajuste.



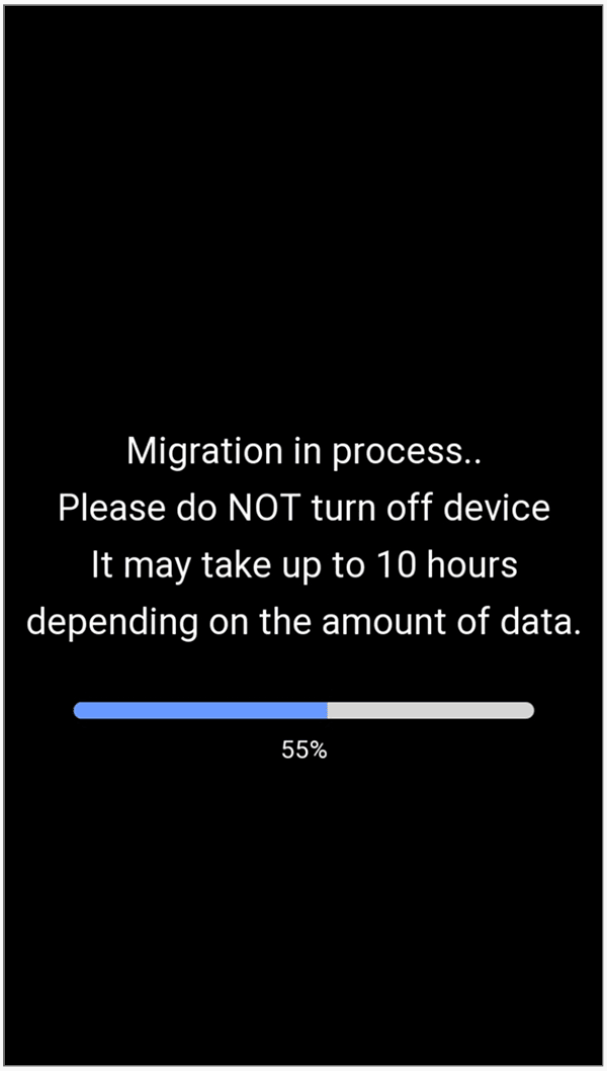
- **Import**: Importe la información de usuarios desde la memoria USB conectada.
- **Export**: Seleccione la información que desea exportar a la memoria USB conectada.
- **FW Upgrade**: Actualice el firmware si los archivos de firmware están guardados en la memoria USB conectada.

Precaución

- No desconecte la fuente de alimentación mientras se actualiza el firmware del dispositivo. El dispositivo puede funcionar incorrectamente.
- Utiliza BioStar X o BioStar Device SDK para actualizar el firmware de la versión v1.x.x a v2.x.x.
- Al actualizar el firmware con una unidad USB, primero configura el menú **DISPLAY & SOUND** a **Menu Timeout Always On** y luego continúa con la actualización. Además, no retires la unidad USB aunque aparezca un mensaje de fallo durante el proceso de actualización; espera hasta que aparezca un mensaje de éxito. El dispositivo se reiniciará automáticamente una vez finalizada la actualización.

Información

- Al actualizar el firmware de la versión 1.0.5 o inferior a la 1.1.0 o superior, se realizará una migración para extraer las plantillas faciales previamente enroladas; este proceso puede tardar hasta 10 horas según la cantidad de usuarios registrados.



- Se recomienda usar una unidad flash USB formateada en exFAT. Las unidades flash USB en formato FAT32 pueden funcionar incorrectamente cuando se almacenan más de 50,000 credenciales faciales.
- Verifica la cantidad de espacio libre en la unidad flash USB. Se requieren al menos 15 GB de espacio libre para guardar 100,000 credenciales faciales.

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. Presione y autentíquese con la credencial de nivel 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. Presione y autentíquese con la credencial de nivel 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. Presione y autentíquese con la credencial de nivel de administrador.
2. Selecciona **DEVICE** → **Restore Default**.
   - **All settings**: Inicializa todos los ajustes almacenados en el dispositivo. Presione **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** 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. Presione y autentíquese con la credencial de nivel 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 ciertos símbolos (`_` , `-` y `.`).
3. Después de cambiar al elemento deseado, presiona **OK**.

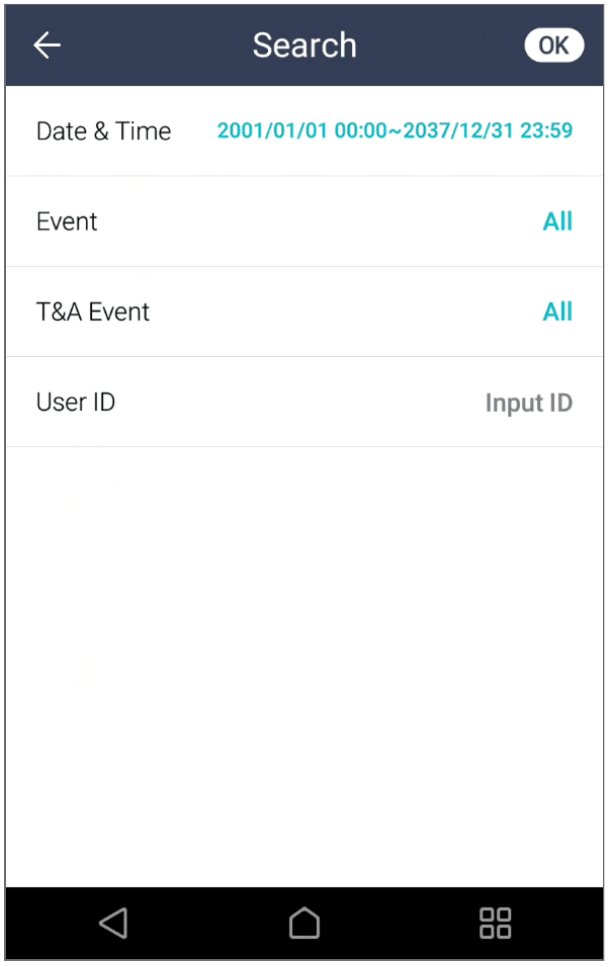
Registros de eventos

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

Busca registros de eventos

Configura condiciones para buscar registros.

1. Presione y autentíquese con la credencial de nivel 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.

Eliminar todos los registros

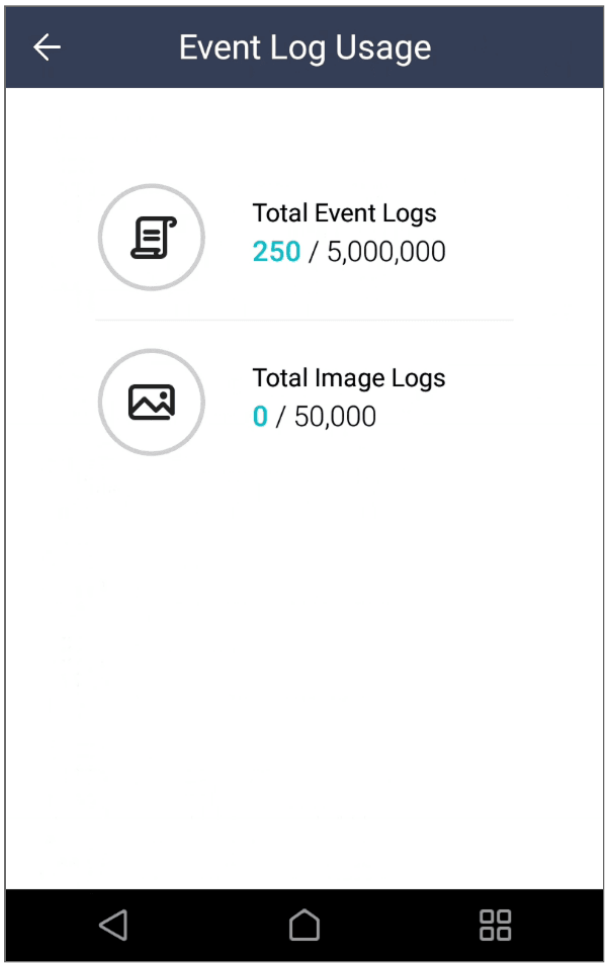
Elimina todos los registros guardados.

1. Presione y autentíquese con la credencial de nivel de administrador.
2. Seleccione **EVENT LOG**.
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. Presione y autentíquese con la credencial de nivel de administrador.
2. Haz 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 ha perdido el PIN de administrador, comuníquese con la empresa de instalación.

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

- Verifique si ingresó correctamente el PIN registrado.
- Verifique si cambió 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. Mask Detection está en Enabled, pero la autenticación facial no se realiza correctamente al usar una mascarilla.

- Autentique su rostro dos veces con la mascarilla bajada hasta la punta de la nariz. Luego, autentique su rostro nuevamente usando una mascarilla que cubra completamente la nariz. Si el problema persiste, comuníquese con la empresa de instalación.

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.

Huella

Q. La huella se ha registrado, pero la autenticación de huella no se realiza correctamente y se producen errores con frecuencia.

- Revisa el Método correcto de ingreso de huellas dactilares y vuelve a registrar la huella.
- Si su huella tiene un corte, el dispositivo puede reconocerla como la huella de otra persona.
- Si hay muchas huellas dactilares registradas, cambie **Matching Timeout** y vuelva a intentarlo.
- La tasa de autenticación puede variar para cada huella debido a diferentes características. Registre la huella de otro dedo.

Q. La autenticación de huella dejó de funcionar repentinamente.

- Verifique si el dedo o el sensor de huella tienen sudor, agua o polvo, y límpielos.
- Seque su dedo y el sensor de huella con una toalla seca y vuelva a intentarlo.
- Si su huella está demasiado seca, sopléela y vuelva a intentarlo.

Q. El sensor de huella no se enciende.

- Cuando **Sensor Mode** está en **Auto On**, el sensor solo se encenderá al colocar el dedo sobre él. Si desea que el sensor de huella esté siempre encendido, configure **Sensor Mode** en **Always On**.

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 ha perdido 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

- Distancia de autenticación[1]:De 0.3 a 1.3 m
- Altura de autenticación:De 1.4 a 1.9 m
- Velocidad de coincidencia:En un plazo de 0.5 segundos
- Detección de rostro vivo:Soportado

Huella FSF2-ODB

- Dimensiones de la imagen:300 x 400 píxeles
- Resolución:500 dpi
- Plantilla:SUPREMA / ISO19794-2 / ANSI-378
- Extractor / Comparador:Con certificación y compatible con MINEX
- Certificaciones del sensor:PIV del FBI e ID móvil FAP20 del FBI
- Detección de huella dactilar viva:Compatible (basado en software)

Tarjeta RF	FSF2-DB, FSF2-ODB	125kHz EM y 13.56MHz MIFARE, MIFARE Plus, DESFire, DESFire EV1/EV2/EV3[2], FeliCa
	FSF2-AB	125kHz EM, HID Prox y 13.56MHz MIFARE, MIFARE Plus, DESFire, DESFire EV1/EV2/EV3[2], FeliCa, iCLASS SE/SR/Seos
Rango de lectura RF[3]	EM/MIFARE/DESFire/HID iCLASS: 50 mm, HID Prox/FeliCa: 30 mm	
Móvil	NFC, BLE	

General

Nombre del modelo	FSF2-DB, FSF2-AB, FSF2-ODB
CPU	1.8 GHz Dual Core + 1.4 GHz Quad Core
Memoria	16 GB Flash + 2 GB RAM

Chip criptográfico	**Soportado**	
Visualizar	**LCD en color IPS 7"**	
Resolución de pantalla	**800 x 1280 píxeles**	
Sonido	**16 bit**	
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**	
Cámara	• **IR: 2M píxeles** • **Visual: 2M píxeles**	
Dimensiones (W x H x D)	**Dispositivo**	• **FSF2-DB, FSF2-AB: 119.8 x 233 x 23.5 (mm)** • **FSF2-ODB: 119.8 x 268.3 x 23.5 (Superior) / 49.6 (Inferior) (mm)**
	Soporte	• **FSF2-DB, FSF2-AB: 98.4 x 223.3 (mm)** • **FSF2-ODB: 98.4 x 251.4 (mm)**
Peso	**Dispositivo**	• **FSF2-DB, FSF2-AB: 585 g** • **FSF2-ODB: 670 g**
	Soporte	• **FSF2-DB, FSF2-AB: 181 g (incluye arandelas y tornillos)** • **FSF2-ODB: 205 g (incluye arandelas y tornillos)**
Grado de protección IP	**IP65**	
Autenticación	**CE, UKCA, KC, FCC, IC, RCM, BIS, ANATEL, SIG, RoHS, REACH, WEEE**	

Capacidad

Máx. usuarios	**100,000**[4)]	
Máx. credenciales (1:N)	**FSF2-DB, FSF2-AB**	**Rostro: 50,000**
	FSF2-ODB	• **Rostro: 50,000** • **Huella digital: 100,000**
Máx. credenciales (1:1)	**FSF2-DB, FSF2-AB**	• **Rostro: 100,000** • **Tarjeta: 100,000** • **PIN: 100,000**
	FSF2-ODB	• **Rostro: 100,000** • **Huella digital: 100,000** • **Tarjeta: 100,000** • **PIN: 100,000**
Máx. registros de texto	**5,000,000**	
Máx. registros de imágenes	**50,000**	

Interfaz

Ethernet	**Compatible (10/100 Mbps, MDI/MDI-X automática)**
Protocolo de red	**TCP, UDP**
RS-485	**1 canal maestro/esclavo (seleccionable)**
Protocolo de comunicación RS-485	**Compatible con OSDP V2**
Wiegand	**Entrada o salida de 1 canal (seleccionable)**
Entrada	**2 canales de entrada**
Relé	**1 relé**

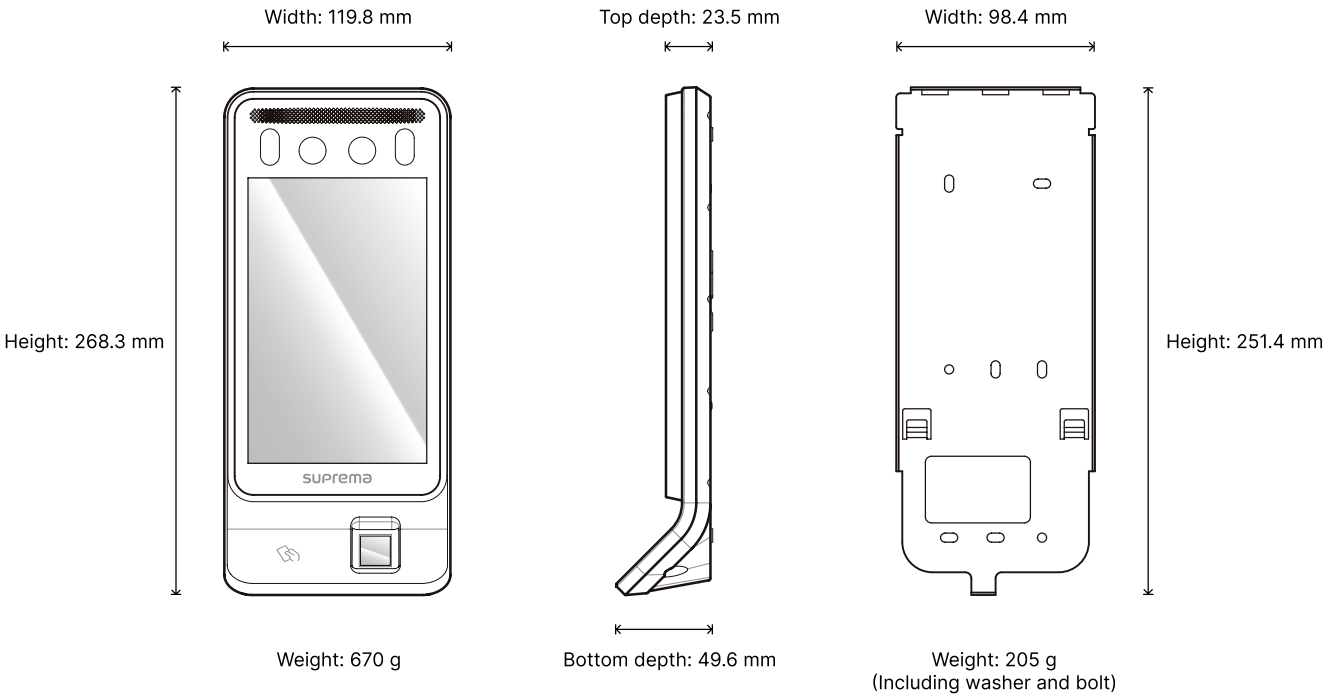
USB	**USB 2.0 (Maestro)**
Tamper	**Soportado**

Eléctrico

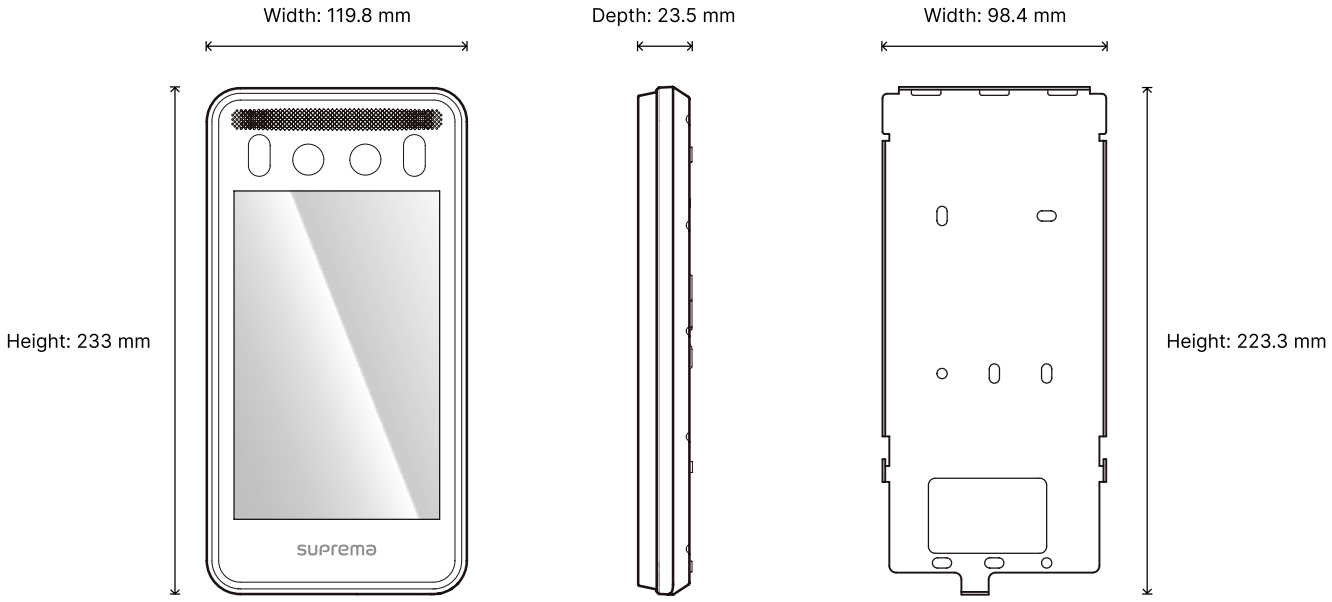
Alimentación	**12 Vdc**	**Corriente: Máx. 2.1 A**
	24 Vdc	**Corriente: Máx. 1 A**
Entrada de interruptor VIH	• **Mín.: 3 V** • **Máx.: 5 V**	
Entrada de interruptor VIL	**Máx.: 1 V**	
Resistencia pull-up del interruptor	**4.7 kΩ (los puertos de entrada se polarizan con 4.7 kΩ)**	
Salida Wiegand VOH	**Más 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

FSF2-ODB



FSF2-DB, FSF2-AB



1) La distancia mínima de autenticación facial especificada es la configuración predeterminada del producto, y la distancia de autenticación facial recomendada es de 0.5–1.3 m.

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

3) El rango de detección de RF puede variar según el entorno de instalación.

4) Número de usuarios registrados sin datos de credenciales.

Información

- Las especificaciones del producto están sujetas a cambios sin previo aviso para mejorar el rendimiento.
- Cuando FSF2-DB, FSF2-AB es el maestro, un esclavo equipado con un sensor de huellas digitales autentica huellas digitales.
  - Máx. Credenciales de huellas digitales (1:N): 100,000
  - 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: -0.1 dBm
- Frecuencia Bluetooth: 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 4.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.
- La biblioteca BoringSSL incluida en este producto se rige por la licencia OpenSSL y la licencia Original SSLeay. Para más información sobre la licencia BoringSSL, consulte la BoringSSL 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.
- Comuníquese con el Equipo de Soporte Técnico de Suprema para descargar el código fuente modificado basado en el kernel de Linux 4.x y las bibliotecas BoringSSL, OpenSSL, Original SSLeay y AOSP incluidas en este producto.

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.