BioStation 3

GUÍA DE USUARIO DE

Versión 1.13

Español
ES 102.00.BS3

suprema
SECURITY & BIOMETRICS

CONTENIDO

Instrucciones de Seguridad 4

Información de cumplimiento 4

Primeros Pasos 8

Componentes 8

Nombre y función de cada parte 9

Cables y conectores 11

Método correcto de enrolamiento y autenticación facial 18

Nota sobre el uso de códigos QR y la licencia del dispositivo 19

Instalación 20

Fijar el soporte y el producto 20

Conexión de la fuente de alimentación 30

Conexión de red 32

Conexión de entrada 33

Conexión del relé 34

Conectar como independiente 36

Conectar Secure I/O 2 38

Conexión Wiegand 39

Cómo Usar 40

Menú de Administrador 40

Usuario 42

Autenticación 46

Ajustes 54

Registros de eventos 72

Solución de Problemas 74

Verifique estos elementos antes de reportar una falla 74

Especificaciones del Producto 76

Credenciales 76

General 76

Capacidad 78

Interfaz 78

Eléctrico 79

Dimensiones y peso 80

Información Reglamentaria 82

Regulaciones y licencias 82

Información de cumplimiento de la FCC 83

Información de IC 84

Declaración de conformidad de la UE (CE) 84

Apéndices 85

Descargos de responsabilidad 85

Aviso de derechos de autor 86

Licencia de código abierto 86

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.

No conecte la fuente de alimentación y la alimentación PoE+ juntas.

- 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.

Al conectar alimentación PoE+, asegúrese de hacerlo según los estándares PoE+ o PoE++.

- El uso de PoE estándar puede provocar que los dispositivos funcionen de forma inestable o sufran daños permanentes.

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.

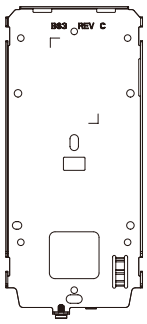
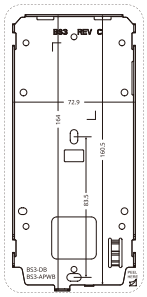
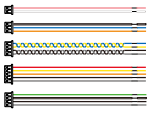
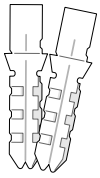
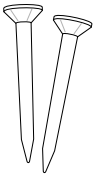
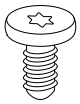
- El dispositivo puede funcionar incorrectamente.

> **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.

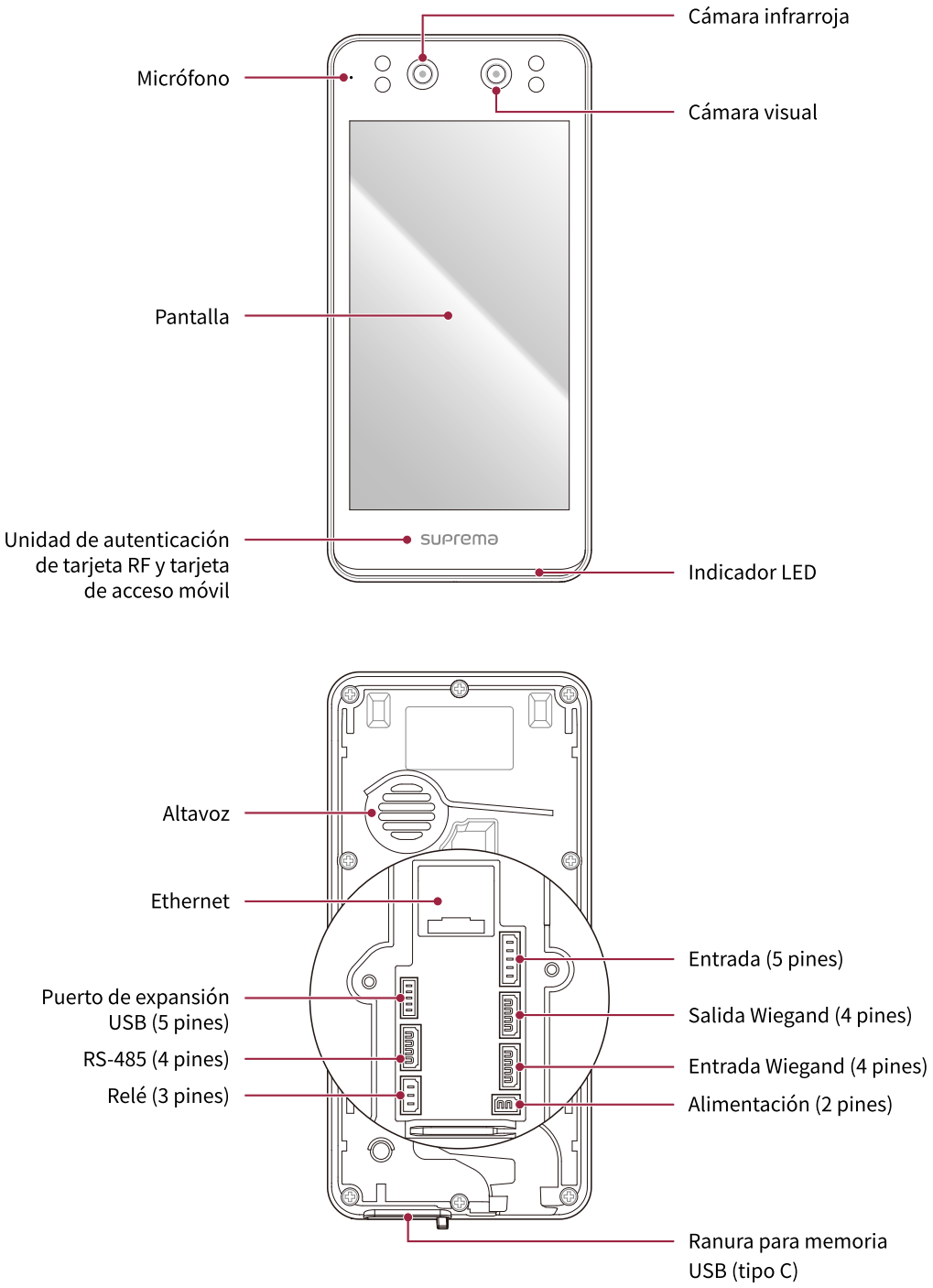
Componentes

				
BioStation 3	Soporte de pared	Plantilla de perforación	Guía rápida	Cables de conexión
				
Diodo	Resistencia de 120 Ω	Anclajes de PVC x2	Tornillos de fijación x2	Tornillo de fijación del soporte (en forma de estrella)

Información

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

Nombre y función de cada parte



- **Micrófono**: Transmite la voz del usuario cuando el interfono está conectado.
  - Cubrir u obstruir el micrófono puede interferir con la transmisión de la voz.
- **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.

- **Indicador LED**: Indica el estado operativo del dispositivo mediante el color del LED.
  - Verde: autenticación exitosa.
  - Rojo: autenticación fallida.
  - Azul: Operación normal.
  - Azul/verde intermitente:
    - Al configurar **DHCP** para usar, no se puede obtener la dirección IP.
    - Cuando está en modo **Slave**, la conexión con el dispositivo maestro se desconecta.
  - Parpadeo rojo/morado: El dispositivo está bloqueado.
  - Parpadeo amarillo: Esperando entrada.
- **Altavoz**: Emite sonido.
- **Ethernet**: Conecta el cable Ethernet.
- **Entrada (5 pines)**: Conecta el cable de entrada.
- **Puerto de expansión USB (5 pines)**: Conecta otros productos accesorios.
- **Salida Wiegand (4 pines)**: Conecta el cable de salida Wiegand.
- **Entrada Wiegand (4 pines)**: Conecta el cable de entrada Wiegand.
- **RS-485 (4 pines)**: Conecta el cable RS-485.
- **Relé (3 pines)**: Conecta el cable del relé.
- **Alimentación (2 pines)**: Conecta el cable de alimentación.
- **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	INPUT2	Naranja
4	INPUT GND	Negro
5	SH GND	Gris

Entrada Wiegand



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

Salida Wiegand



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

Configurar administrador maestro Productos orientados a CE

La función **Master Admin** mejora los privilegios administrativos generales del dispositivo para aumentar la seguridad del dispositivo y evitar el acceso y los cambios de configuración no autorizados. Esta característica solo aplica a los **productos orientados a CE** para la región de la UE, y los **productos CE requieren inscribir al administrador maestro**. Solo el Master Administrator enrolled puede acceder al menú de administrador y cambiar los settings del dispositivo.

Información

- Esta característica es una política obligatoria para mejorar la seguridad de los **productos orientados a CE** en la región de la UE, y no es compatible con los **productos globales (no CE)**.
- El administrador maestro no puede eliminarse directamente y solo se eliminará durante **Factory Default**.

Política de soporte del administrador maestro Productos CE vs productos globales (sin CE)

La feature **Master Admin** se activa solo en **Productos CE con una etiqueta que tiene la marca CE**.

Use la etiqueta adhesiva en el rótulo posterior para identificar **Productos CE** y **productos Global (No CE)**. La feature funciona de manera diferente, como se indica a continuación.

- **Productos CE**: marca CE presente
- **productos Global (No CE)**: marca CE ausente

Categoría	Productos orientados a CE	Productos globales (sin CE)
Master Admin	Habilitado (no se puede deshabilitar)	No compatible
Admin 2-step Authentication	Obligatorio	No compatible
Longitud mínima del PIN	Al menos 8 dígitos	Al menos 4 dígitos

Cuando se conecta a BioStar X (o BioStar 2), el setting de Master Admin cambia según la compatibilidad del dispositivo, y la activación del menú de autenticación en dos pasos del administrador se sincroniza automáticamente.

Comportamiento durante la actualización del firmware

Cuando actualiza el firmware de un dispositivo existente, la compatibilidad con **Master Admin** y **Admin 2-step Authentication** puede variar según la combinación de la **versión anterior a la actualización** y la **versión objetivo**.

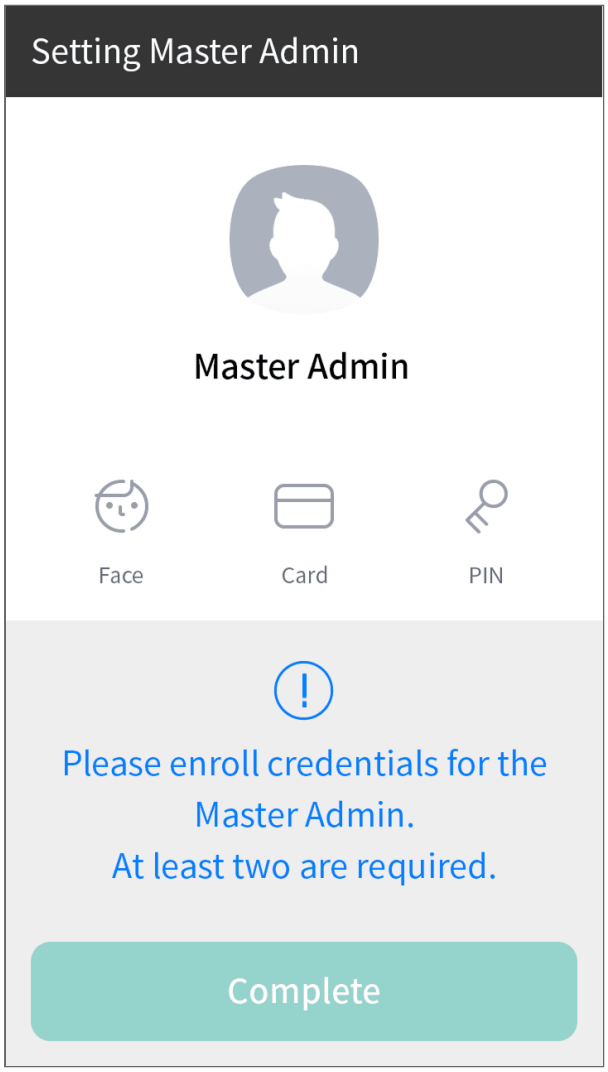
Contacte a Equipo de Soporte Técnico global de Suprema para obtener información detallada sobre la disponibilidad del soporte por versión.

Registrar Master Admin en un dispositivo nuevo

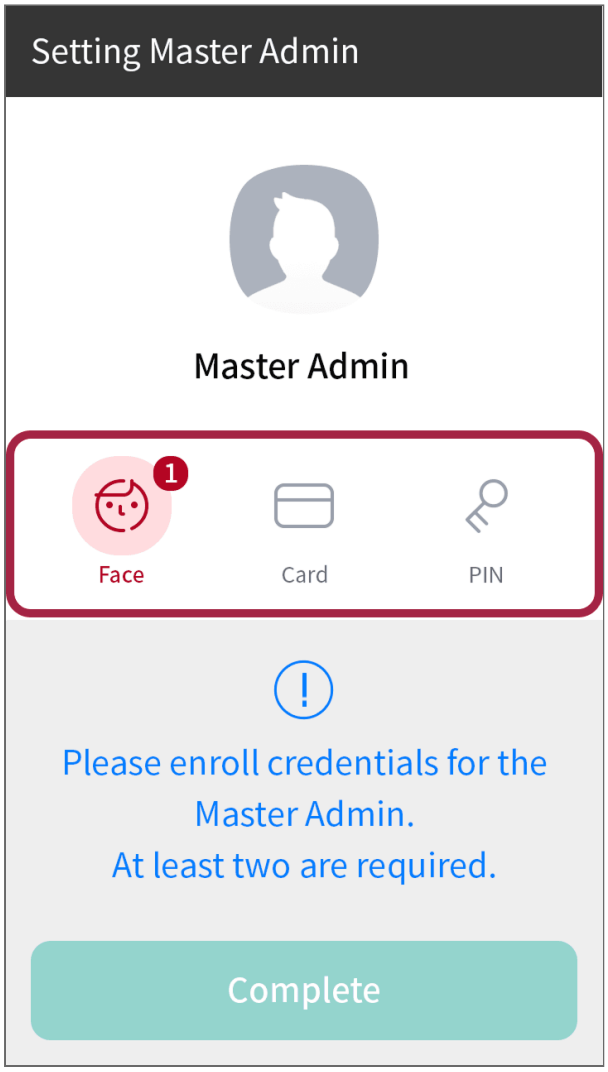
En un dispositivo nuevo para Productos CE, debe enrolar **Master Admin** desde el inicio. Si no lo enrola, el uso del dispositivo queda restringido.

> **Información**
>
> - En el primer arranque, aparece la pantalla de enrollment de **Master Admin**. Si no completa el enrollment, no puede pasar a la siguiente pantalla.
> - Aunque se conecte a BioStar X (o BioStar 2) y asigne un administrador para todo el dispositivo, debe inscribir **Master Admin** directamente en el dispositivo para usar todas las funciones.
> - Los dispositivos nuevos no pueden realizar degradaciones de firmware.

1. Cuando el dispositivo nuevo se inicie por primera vez, aparecerá la pantalla de registro de **Master Admin**.



2. Según la política de seguridad de la UE, **Master Admin** debe inscribir credenciales de al menos dos tipos. Seleccione e inscriba las dos credenciales deseadas.



Las credenciales que se pueden inscribir para **Master Admin** son las siguientes.

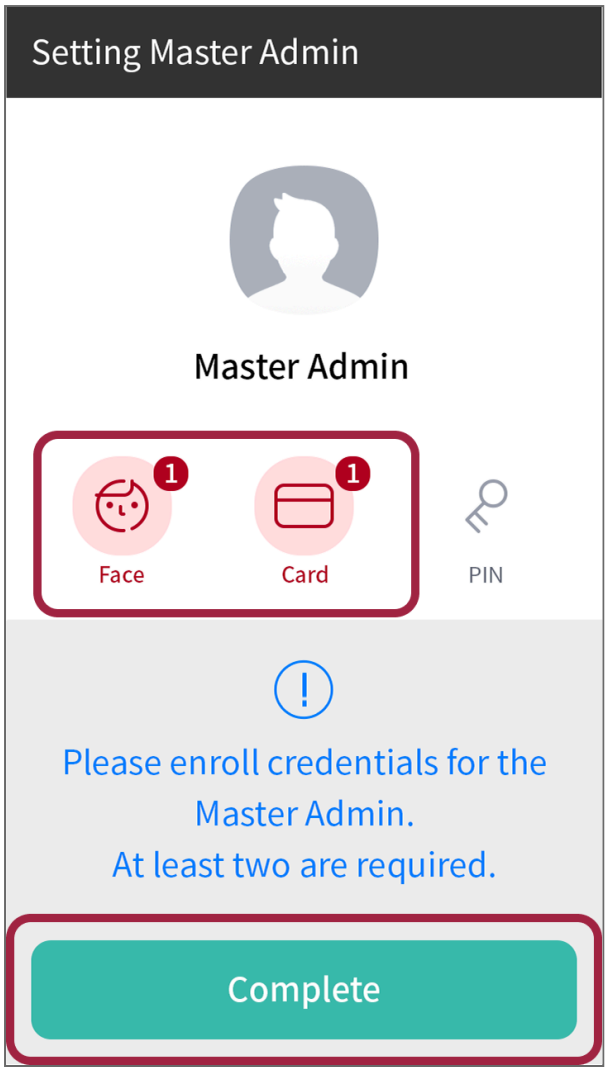
Tipo de credencial	Número de inscripciones	Condiciones
Tarjeta	Hasta 4	Admite solo tipos CSN y Wiegand No se permite la inscripción duplicada dentro del mismo tipo
Rostro	Hasta 2	Inscriba solo en dispositivos con el mismo algoritmo
Fingerprint	Hasta 2	-
PIN	1	Al menos 8 dígitos (se aplica la normativa CE)

Condiciones de enrolamiento

- Debe enrolar al menos dos tipos de credenciales.
- Todas las credenciales compatibles con el dispositivo pueden utilizarse como medios de autenticación.

3. Después de inscribir dos o más tipos de credenciales, presione el botón **Complete** para completar el registro de

Master Admin.



Información adicional

- **Cuando se enrola un PIN mediante el software BioStar**

  Los productos Global (No CE) que no admiten el Master Administrator pueden enrolar un PIN de al menos 4 dígitos directamente en el dispositivo. Sin embargo, al enrolar usuarios mediante BioStar X (o BioStar 2), las siguientes versiones requieren un PIN de al menos 8 dígitos.

  – BioStar 2 v2.9.11 o posterior

  – BioStar X v1.0.0 a v1.0.2

  Los usuarios enrolados con un PIN de 4 dígitos en las versiones anteriores no pueden asignarse como administradores del dispositivo.

- **Cambio manual de la clave hash del dispositivo**

  Al cambiar manualmente la clave hash del dispositivo, aparecerá un mensaje de advertencia que indicará que los PIN de Master Admin se eliminarán. Confirme el mensaje antes de continuar.

- **Restricción de transmisión de imágenes biométricas RS-485**

  Las imágenes de credenciales biométricas no se transmiten por comunicación RS-485, por lo que aparecen imágenes sustitutas al ver el rostro del Master Admin registrado en dispositivos esclavos.

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.

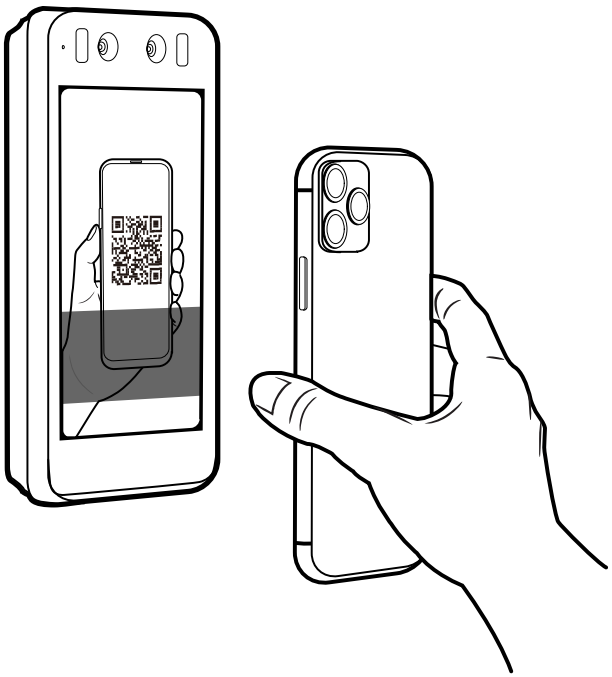
Precauciones para autenticar un rostro

- 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 60~100 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.

Nota sobre el uso de códigos QR y la licencia del dispositivo

Cómo escanear un código QR

Emite un código QR a un usuario y úsalo como método de autenticación. Escanea correctamente el código QR siguiendo las instrucciones en la pantalla para aumentar la tasa de reconocimiento.



- Mantén la distancia entre la cámara del dispositivo y el código QR a 30~40 cm.
- Coloca el código QR en el centro de la pantalla de escaneo del dispositivo.
- Al autenticar con el código QR descargado en tu smartphone, ajusta el brillo de tu smartphone para que el dispositivo pueda leer el código QR con claridad.

Notas sobre la licencia del dispositivo

- El uso de la autenticación mediante código QR requiere una licencia de dispositivo aparte. Contacta al lugar de compra para obtener una licencia de dispositivo.
- El archivo de licencia del dispositivo está cifrado y no puede modificarse de forma arbitraria.
- Las licencias de dispositivo se emiten según el ID del dispositivo. Si el ID del dispositivo se cambia de manera inusual, no se proporciona servicio de garantía para la licencia.

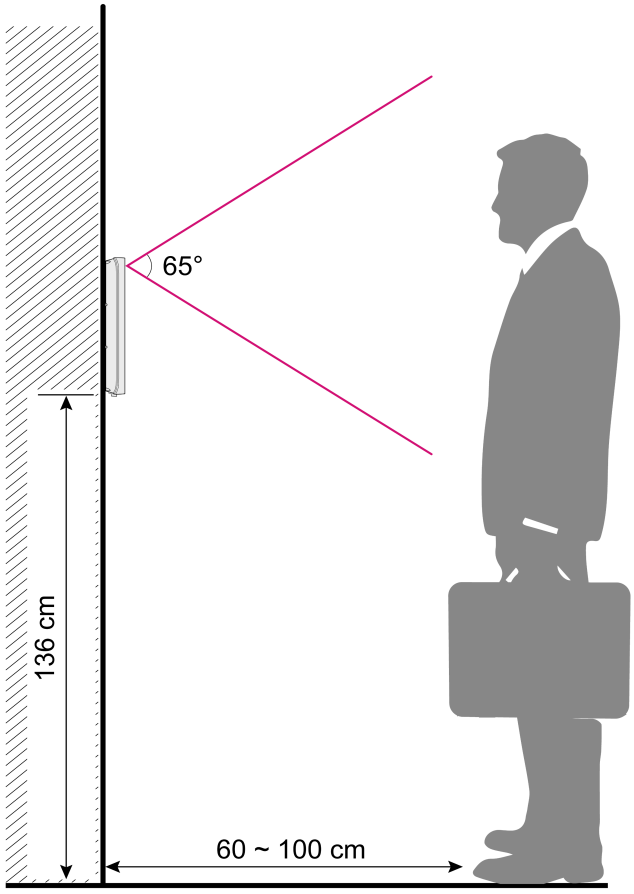
Instalación

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

Fijar el soporte y el producto

Soporte general

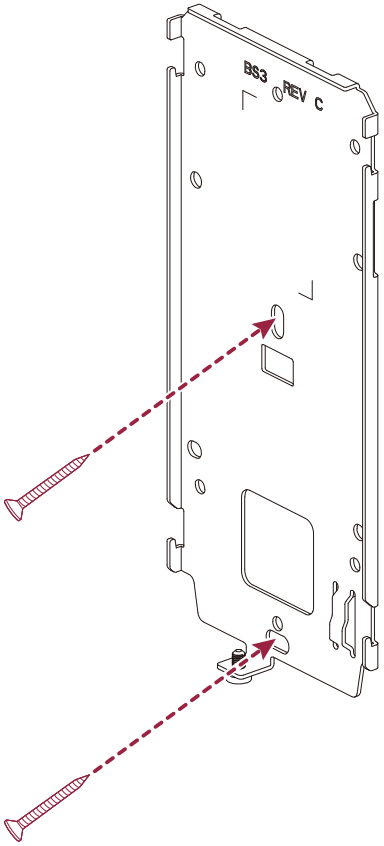
1. Determine la posición correcta para instalar el soporte usando la plantilla de perforación proporcionada.



Información

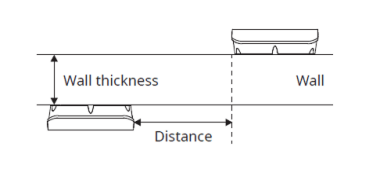
- La altura óptima para instalar el dispositivo es de 136 cm.
- Instale el dispositivo donde no reciba luz solar directa ni luz UV.
- Ajuste la posición de instalación para que el rostro no esté expuesto a la luz solar directa cuando el usuario intente autenticarse.

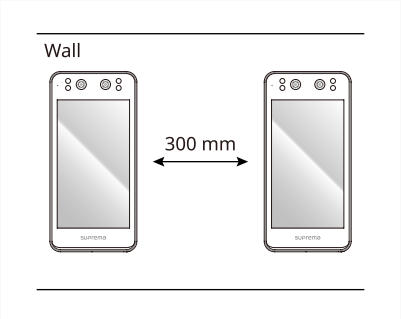
2. Asegura firmemente el soporte con los tornillos de fijación en el lugar donde se montará el producto.



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.

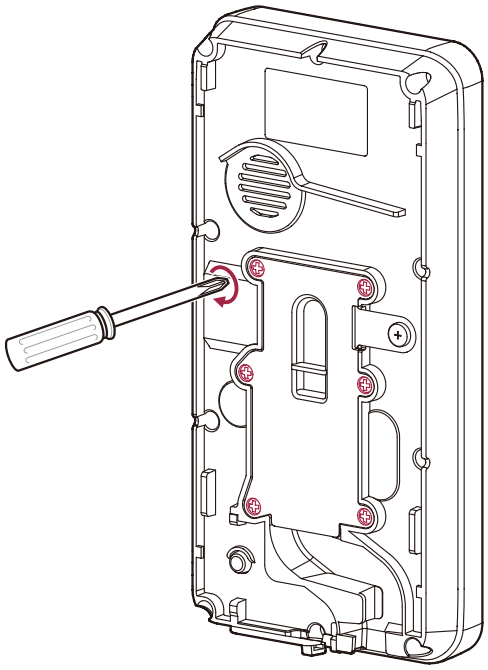




Espesor de pared	Distancia
100 mm	200 mm
120 mm	180 mm
150 mm	150 mm

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

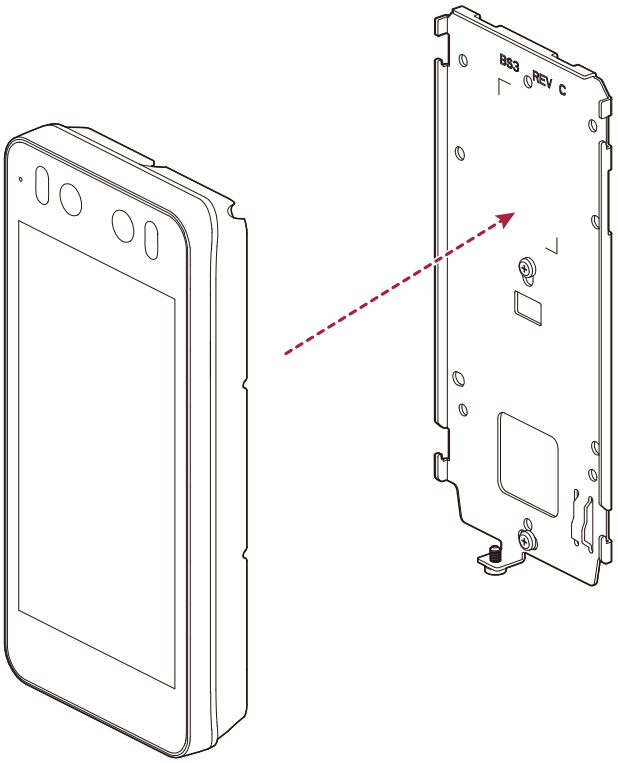
3. Después de colocar la cubierta del cable, apriete firmemente los seis tornillos de la cubierta para asegurarlo.



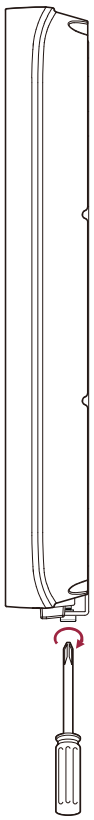
Información

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. Monta el producto en el soporte fijado.



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



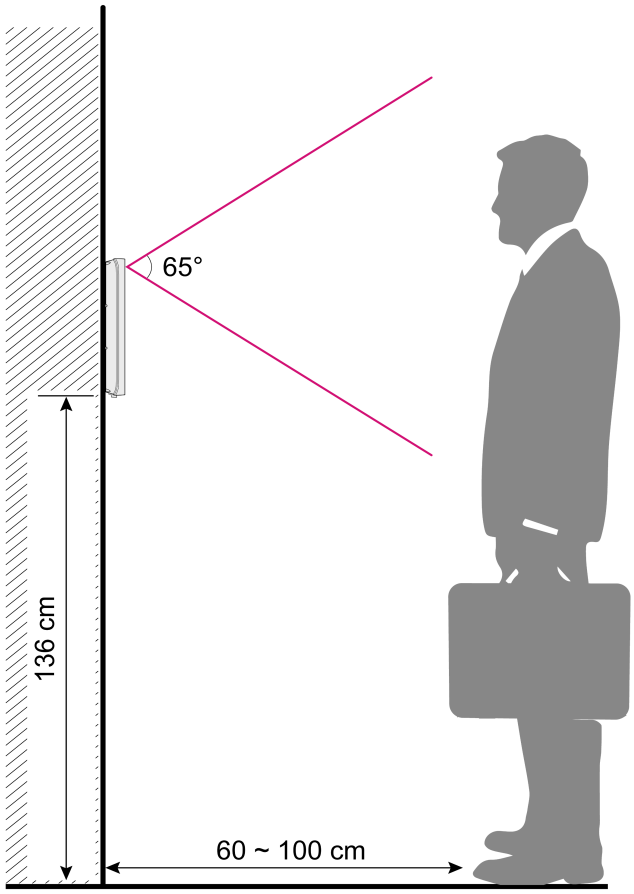
Información

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

Soporte inclinable

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

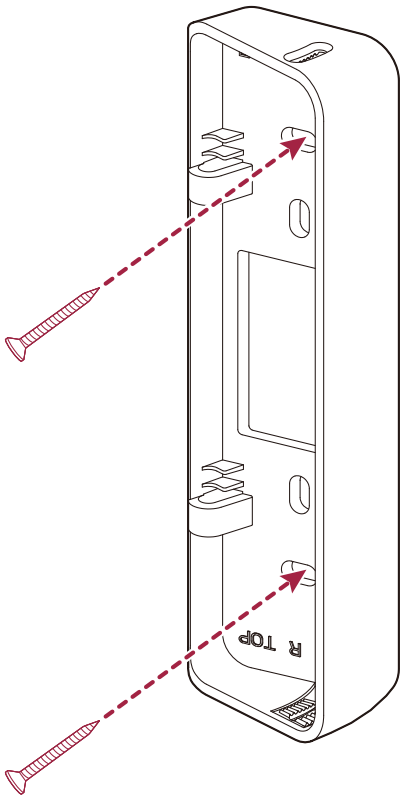
1. Determine la posición correcta para instalar el soporte usando la plantilla de perforación proporcionada.



Información

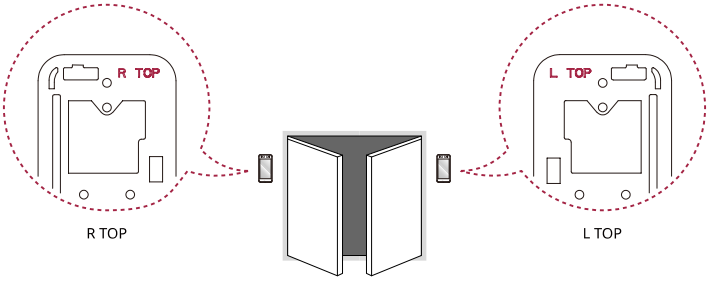
- La altura óptima para instalar el dispositivo es de 136 cm.
- Instale el dispositivo donde no reciba luz solar directa ni luz UV.
- Ajuste la posición de instalación para que el rostro no esté expuesto a la luz solar directa cuando el usuario intente autenticarse.

2. Use los tornillos de montaje del soporte inclinable para fijar firmemente la parte trasera del soporte inclinable en la ubicación de instalación (pared).



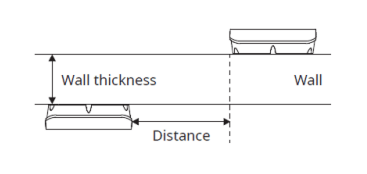
Según la ubicación de instalación, instale el soporte inclinable con la orientación superior e inferior como se indica a continuación.

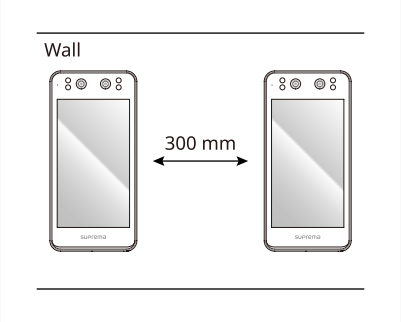
- Al instalarlo en el lado izquierdo de la entrada: instálelo de modo que la marca "R TOP" quede hacia arriba
- Al instalarlo en el lado derecho de la entrada: instálelo de modo que la marca "L TOP" quede hacia arriba



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.

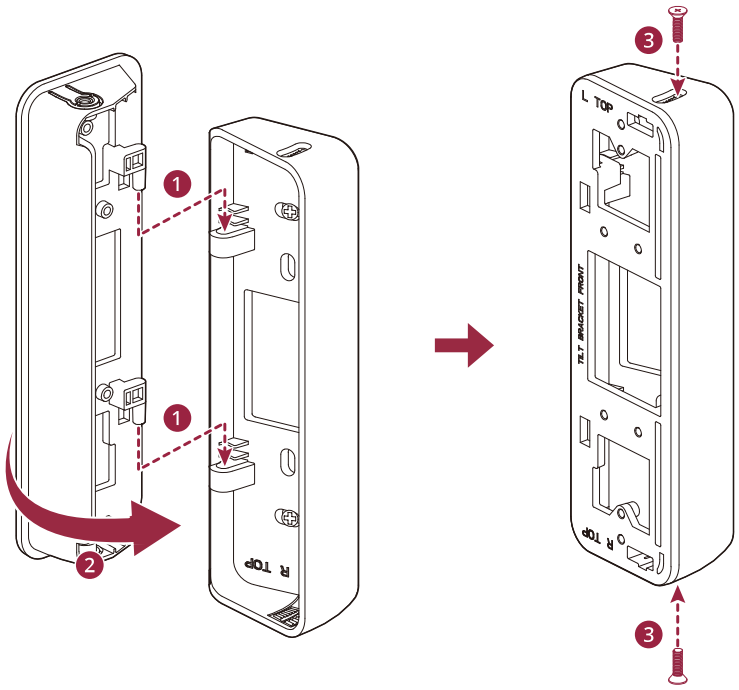




Espesor de pared	Distancia
100 mm	200 mm
120 mm	180 mm
150 mm	150 mm

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

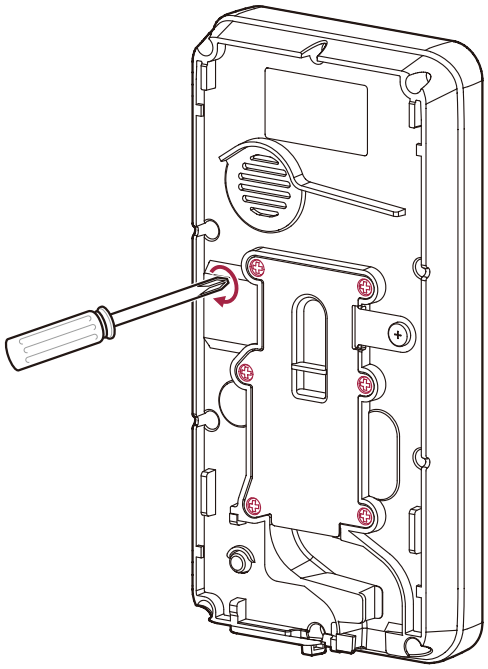
3. Una la parte frontal del soporte inclinable con la ranura de la parte trasera, ciérrelo y fíjelo con dos tornillos en los orificios superiores e inferiores.



Información

Si aprieta demasiado los tornillos, no se puede ajustar el ángulo. Apriete los tornillos al nivel adecuado.

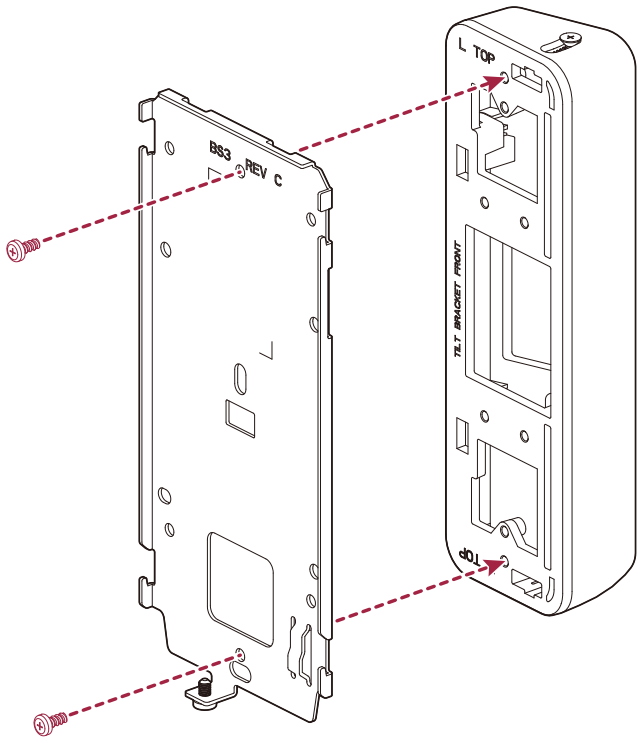
4. Después de colocar la cubierta del cable, apriete firmemente los seis tornillos de la cubierta para asegurarlo.



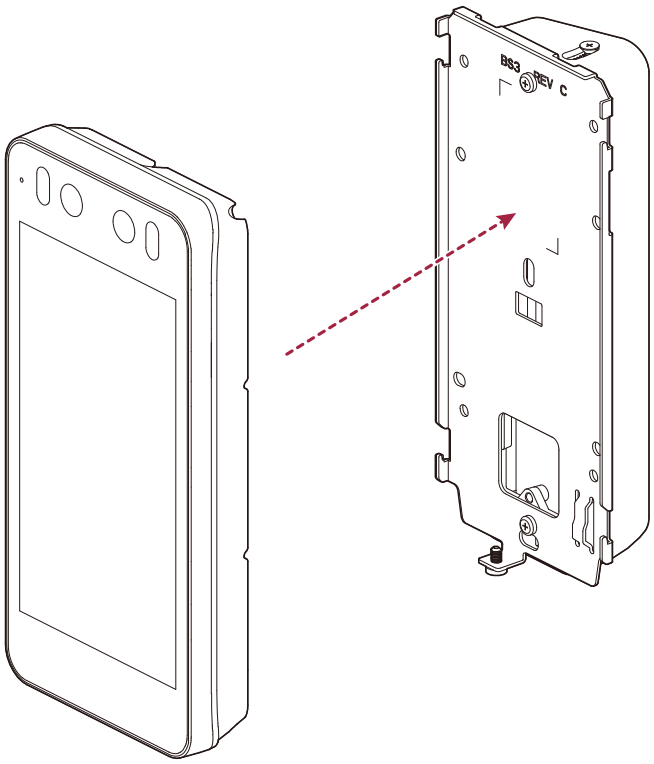
Información

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).

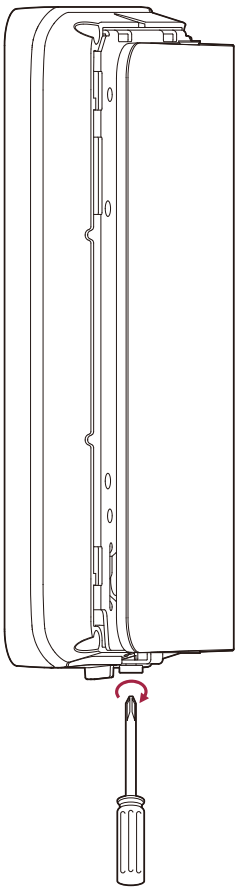
5. Fije firmemente el soporte de montaje en pared encima del soporte inclinable.



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



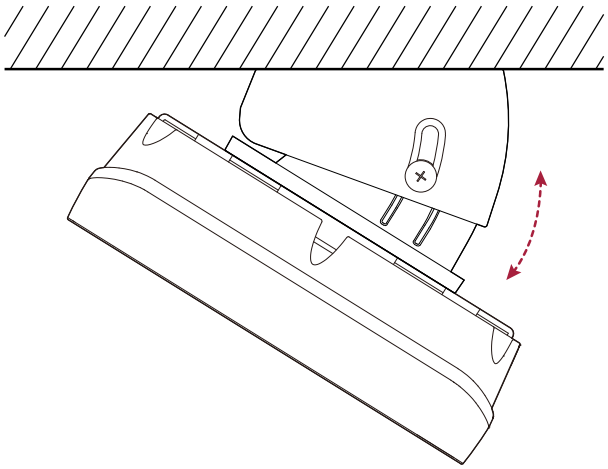
7. Apriete los tornillos de fijación del producto para ensamblarlo con el soporte de montaje en pared.



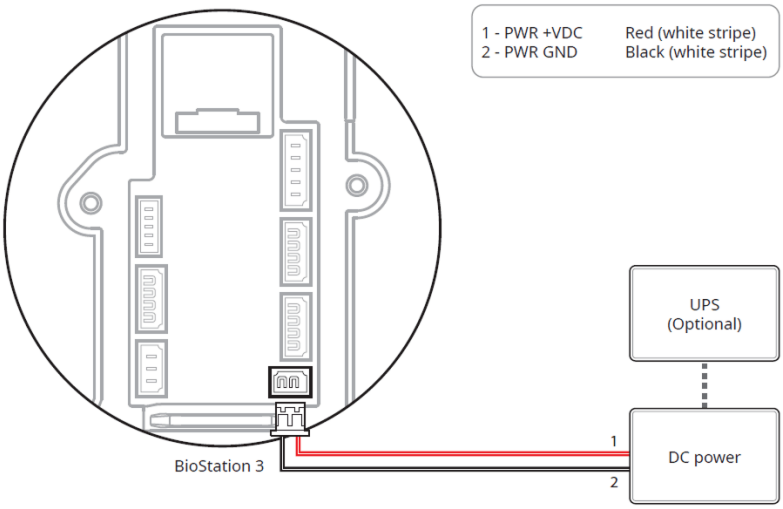
Información

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

8. Ajuste el soporte inclinable al ángulo deseado.



Conexión de la fuente de alimentación



Precaución

- NO conecte el dispositivo a la fuente de alimentación de CC (o adaptador) y a la alimentación PoE al mismo tiempo.
- 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

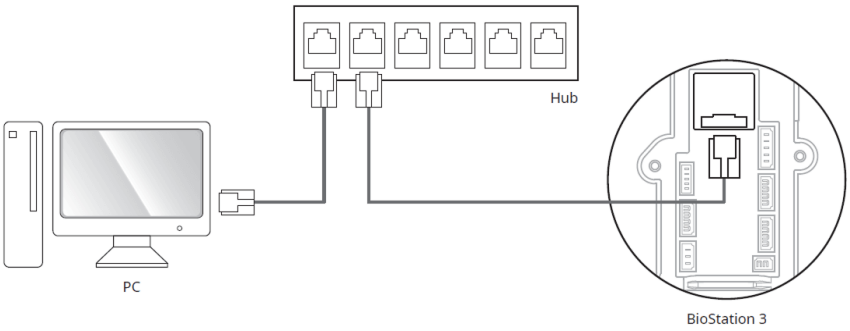
- NO extienda la longitud del cable de alimentación al usar el adaptador de alimentación.
- NO utilice CAT5 UTP de 2 hilos para la alimentación.

Conexión de red

TCP/IP

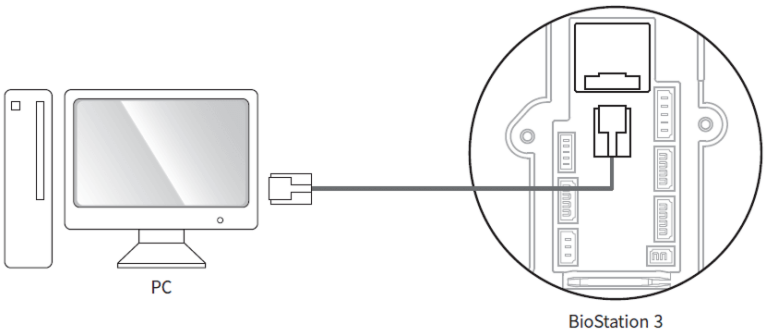
Conexión LAN (conexión a un concentrador)

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

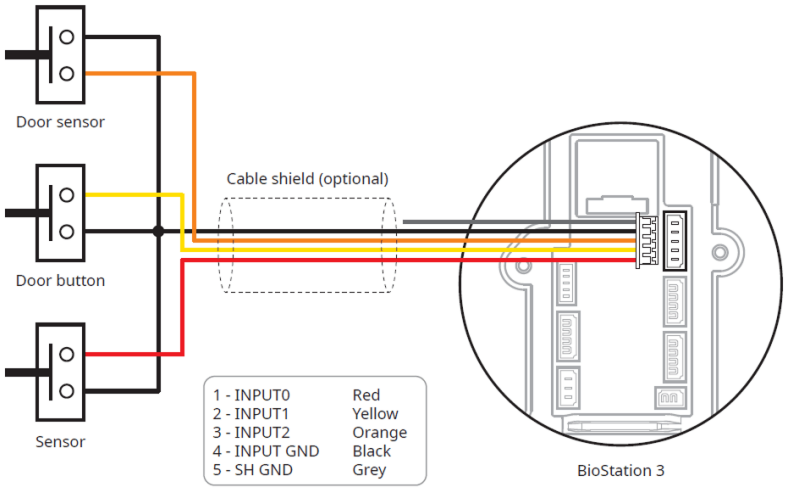
Este dispositivo usa los siguientes puertos para la comunicación en red y el funcionamiento estable del servicio.

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 proporcionan las características de red estándar del producto. Al configurar reglas del firewall o ajustes de seguridad de red, permita estos puertos.

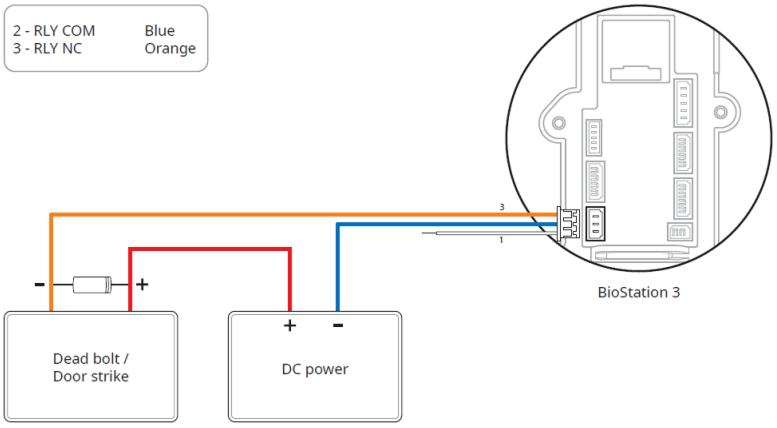
Conexión de entrada



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

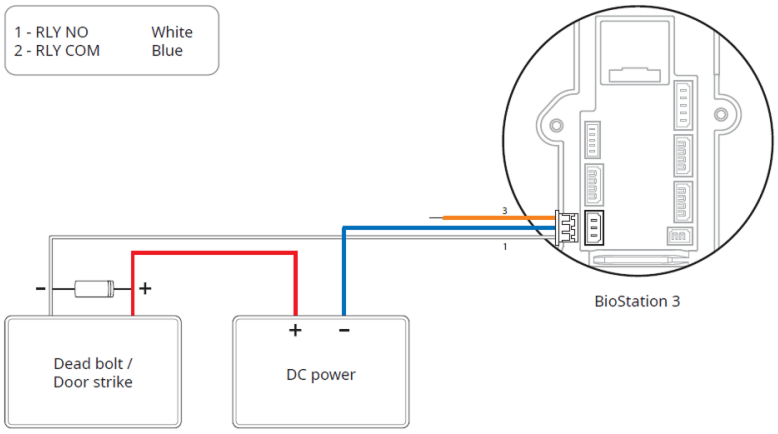
- Instale un diodo en ambos extremos del cable de la cerradura, como se muestra en la figura, para proteger el relé de la corriente inversa que se produce cuando la cerradura funciona.
- Utilice una fuente de alimentación independiente para el producto y la cerradura.
- Los lectores inteligentes independientes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



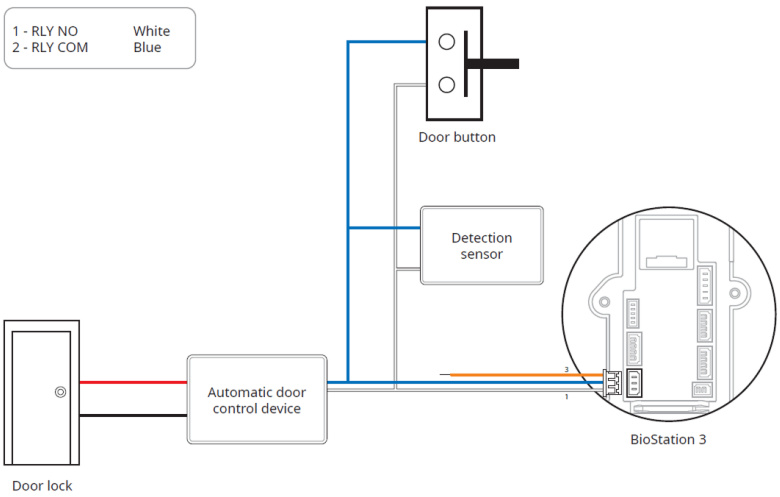
Precaución

- 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

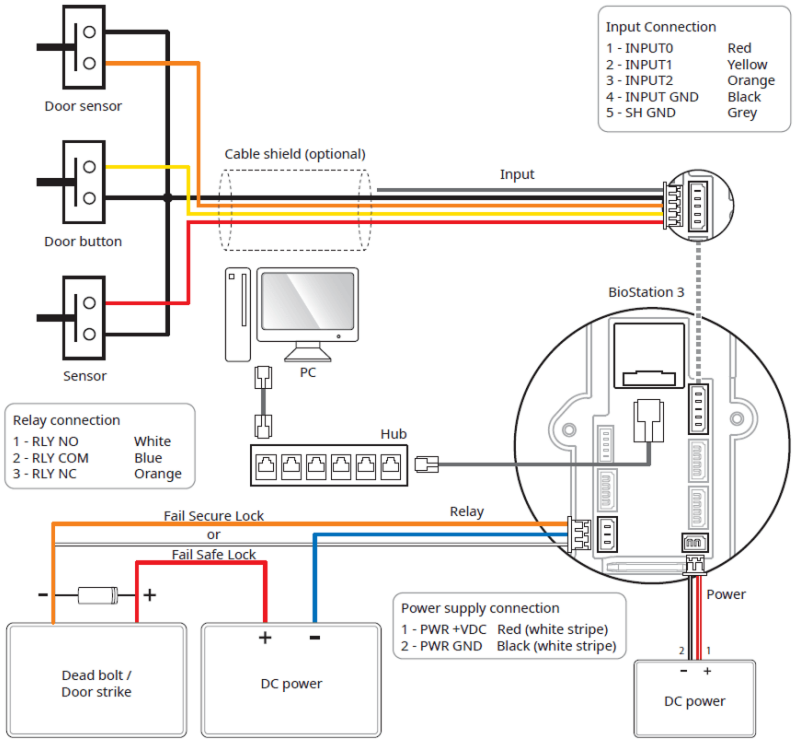
Preste atención a la dirección de instalación del diodo. Instale el diodo cerca de la cerradura.

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.

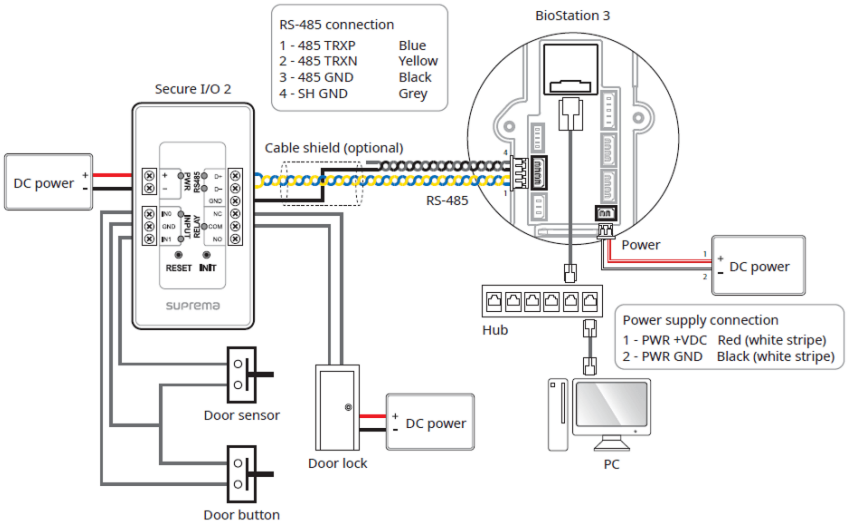
Información

- 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.
- BioStation 3 no puede utilizarse como dispositivo esclavo cuando FaceStation 2, FaceLite 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.

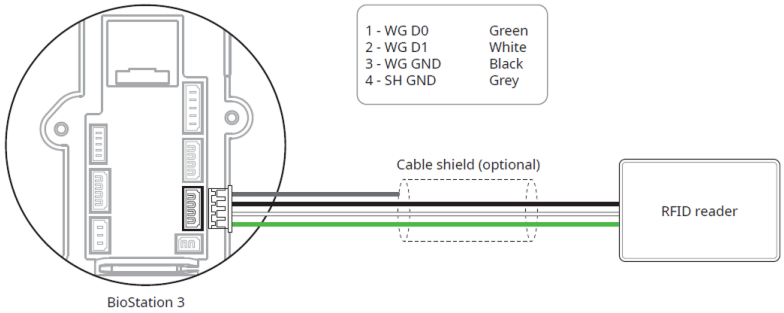


Información

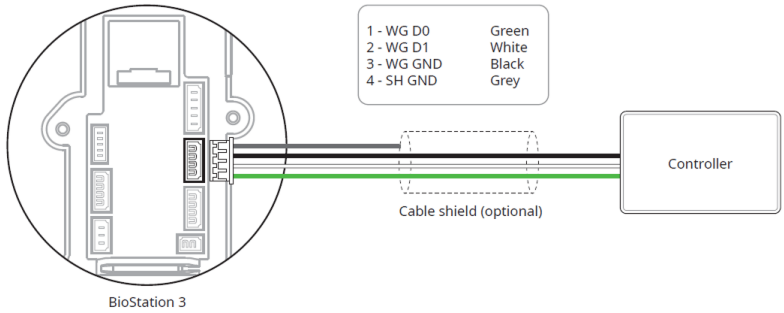
- El dispositivo puede utilizarse como controlador de múltiples puertas con los dispositivos esclavos mediante el cable RS-485. Los dispositivos esclavos se utilizan como lectores ficticios y la autenticación se realiza en el dispositivo maestro.
- BioStation 3 no puede utilizarse como dispositivo esclavo cuando FaceStation 2, FaceLite 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

Se usa como dispositivo de entrada Wiegand.



Se usa como dispositivo de salida Wiegand.



Cómo Usar

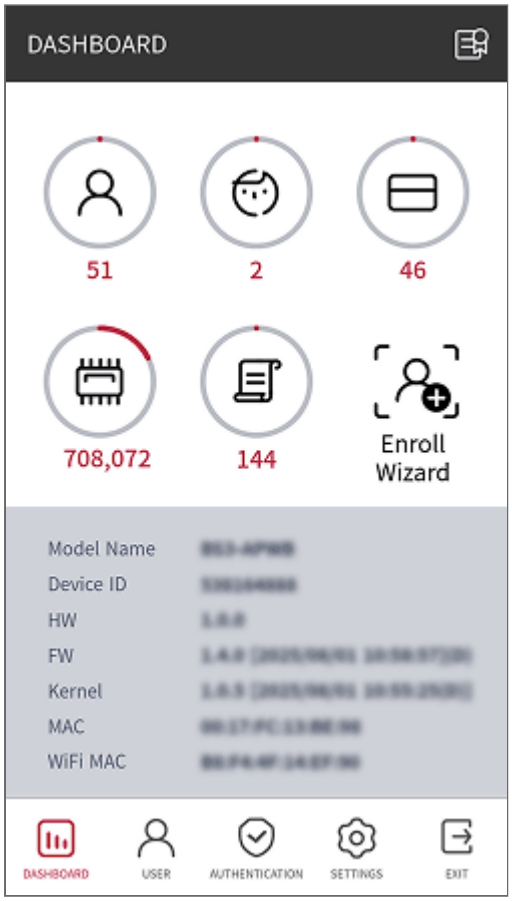
Proporciona orientación sobre cómo utilizar las funciones principales del dispositivo de manera efectiva.

Menú de Administrador

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

TABLERO

1. Presione y autentíquese con la credencial de nivel Administrador.
   Verifique el estado y la información del dispositivo en **DASHBOARD**. Como alternativa, presione **Enroll Wizard** para registrar directamente a un usuario.
2. Seleccione el menú deseado en la parte inferior del panel de control para registrar un usuario o configurar un dispositivo.



Información

- Si no se ha designado un administrador, al presionar se mostrará la pantalla de **DASHBOARD**.
- **WiFi MAC** solo se puede confirmar en el modelo BS3-APWB.

Control de Puerta

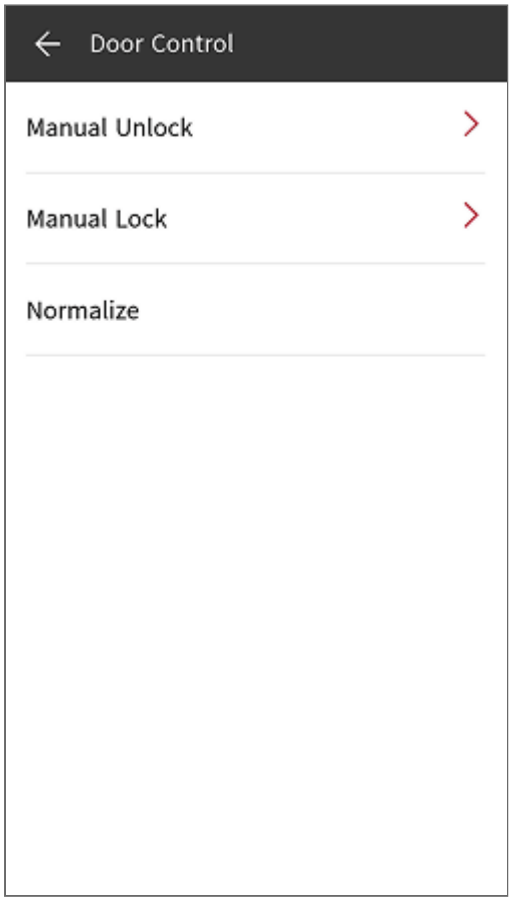
Puede abrir, bloquear o desbloquear manualmente la puerta conectada.

> **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** 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.

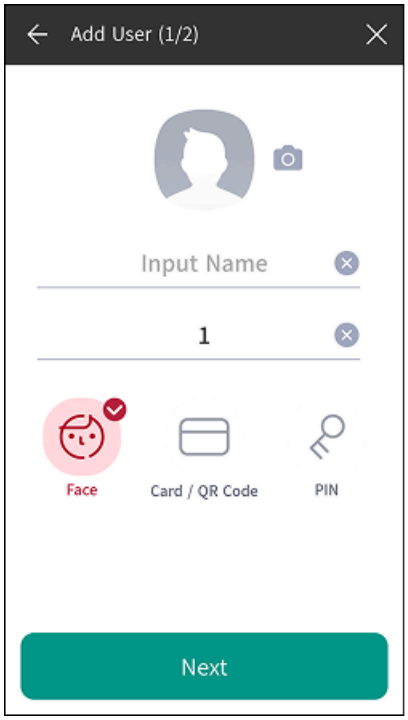
Usuario

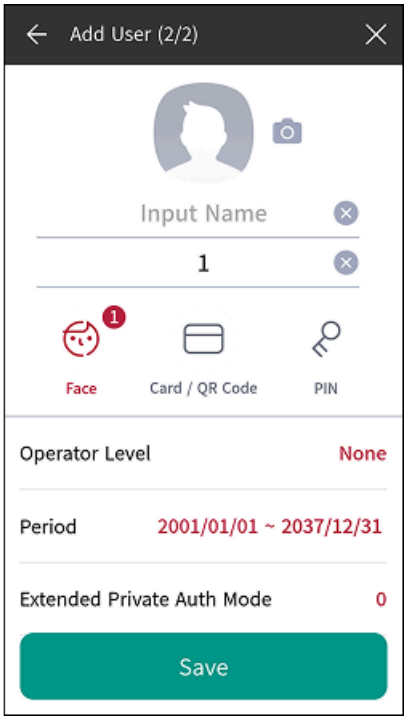
Describe cómo registrar, editar, eliminar y gestionar usuarios.

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 el elemento deseado. 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. Presione para añadir más rostros. Consulte Inscribir rostros de usuario para obtener más información sobre el registro de rostros.
- **Card / QR Code**: Registre una tarjeta para la autenticación del usuario. Presione **Card / QR Code** → **Next**, luego escanee la tarjeta en la unidad de autenticación de tarjetas RF para asignarla al usuario. Presione **Card / QR Code** → para registrar 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**. Ingrese un PIN de entre 4 y 16 dígitos para evitar que se exponga.

> **Información**
> Al usar la función **Master Admin**, ingrese un número de al menos 8 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.
- **Extended Private Auth Mode**: Configura el modo ampliado de autenticación personal. Este modo le permite combinar métodos de autenticación del usuario, incluidos ambos rostros. De lo contrario, utilice el modo de autenticación básico del dispositivo.

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.

Modificar información de usuario

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

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

Información

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

Eliminar todos los usuarios

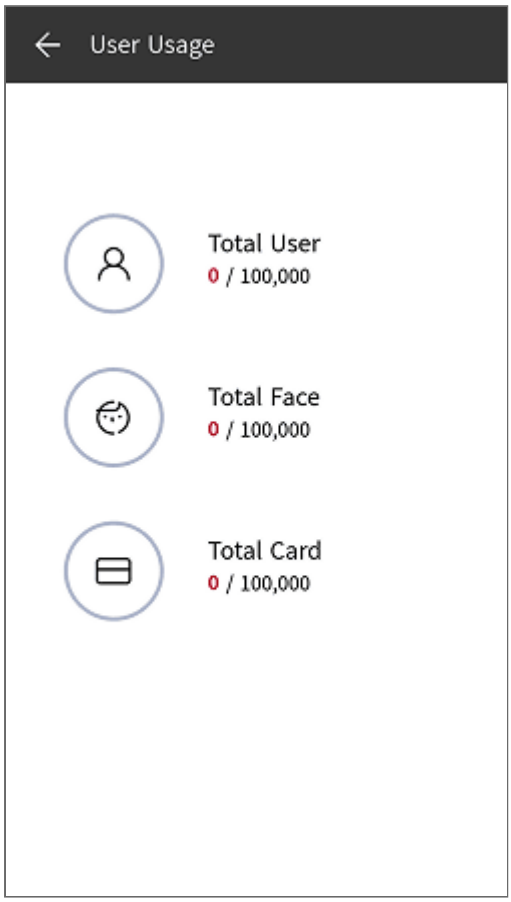
Elimine todos los usuarios registrados a la vez.

1. 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

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

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



Autenticación

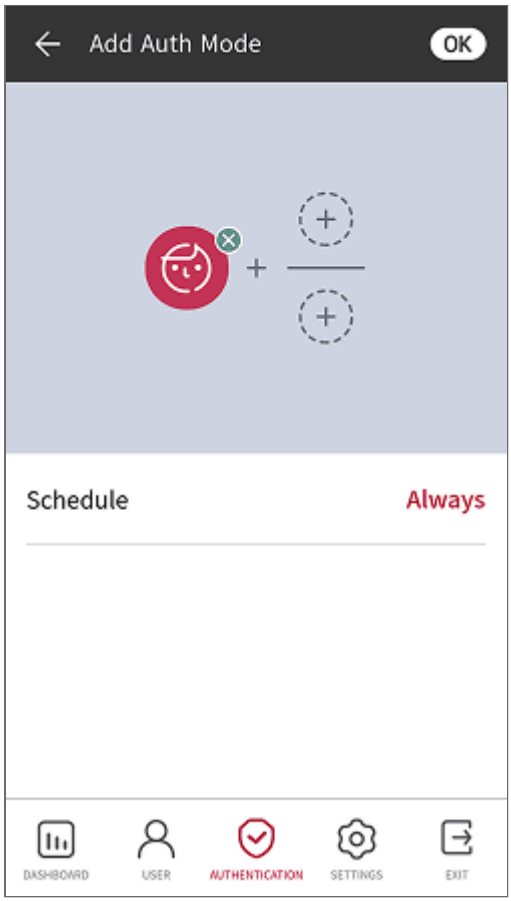
Describe los métodos de autenticación compatibles y los procedimientos de autenticación.

Modo de autenticación

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

Registrar modo de autenticación

1. Presione y autentíquese con la credencial de nivel de administrador.
2. Presione **AUTHENTICATION** → **Auth Mode**.
3. Seleccione .
4. Al pulsar , aparecerá en la pantalla la credencial que se puede añadir. Selecciona las credenciales que deseas añadir. Pulsa mientras la credencial esté añadida para eliminarla.



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

Categoría	Descripción
Rostro	- : Este modo utiliza únicamente autenticación facial. - + : Este modo requiere autenticación facial seguida de la introducción de un PIN.

Categoría	Descripción
Tarjeta / Código QR	- : Este modo utiliza solo la autenticación por tarjeta / código QR. - + : Este modo requiere autenticación con tarjeta / código QR seguida de autenticación facial. - + : Este modo requiere autenticación mediante tarjeta / código QR seguida de ingreso de PIN. - + / : Este modo requiere autenticación con tarjeta / código QR seguida de autenticación facial o introducción de PIN. - + + : Este modo utiliza autenticación facial y PIN después de la autenticación con tarjeta / código QR.
ID	- + : Este modo requiere la introducción de ID seguida de autenticación facial. - + : Este modo requiere ingresar un ID seguido de ingreso de PIN. - + / : Este modo requiere la introducción de ID seguida de autenticación facial o introducción de PIN. - + + : Este modo utiliza autenticación facial y PIN después de la introducción de ID.

Información

- **Schedule** se puede configurar en BioStar X. Si no se establece un horario, solo se puede seleccionar **Always**.
- Para más información sobre la configuración de **Schedule**, consulte la Guía del administrador de BioStar X.
- Haga clic en **AUTHENTICATION** y active **Operation** con **QR Authentication** para usar la autenticación **QR Code**; se requiere una licencia de dispositivo independiente. Para obtener más información, consulta Licencia.

6. 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

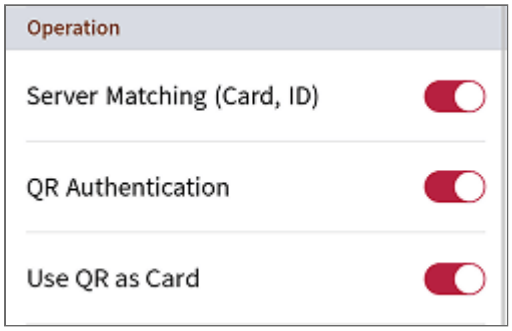
1. Presione y autentíquese con la credencial de nivel de administrador.
2. Presione **AUTHENTICATION** → **Auth Mode**.

3. Pulsa y selecciona el modo de autenticación que deseas eliminar. Es posible seleccionar varias opciones.
4. Pulsa **OK** para eliminar el elemento seleccionado.

Operación

Puede configurar opciones relacionadas con la autenticación, como **Server Matching** y **QR Authentication**.

1. Presione y autentíquese con la credencial de nivel de administrador.
2. Presione **AUTHENTICATION**, luego habilite las opciones deseadas en **Operation**.



- **Server Matching (Card, ID)**: El uso de la autenticación en servidor significa que BioStar X autentica a los usuarios, no el dispositivo. Esto resulta útil cuando el dispositivo almacena grandes cantidades de información de usuarios. También ayuda a evitar exponer en el exterior un dispositivo que almacena información de credenciales.

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

- **QR Authentication**: Configure si se utiliza la autenticación por código QR a través de la cámara del dispositivo.

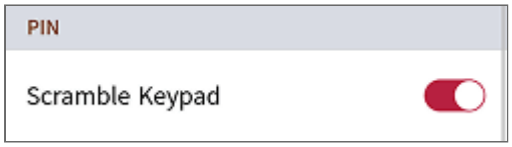
  > **Información**
  >
  > Se requiere una licencia de dispositivo independiente para usar **QR Authentication**. Para obtener más información, consulta Licencia.

- **Use QR as Card**: Configure la autenticación con un código QR con los datos de la tarjeta CSN o Wiegand del usuario. Solo se puede configurar cuando **QR Authentication** está activado.

PIN

Configura si se utiliza el teclado aleatorio al ingresar contraseñas.

1. Presione y autentíquese con la credencial de nivel de administrador.
2. Después de pulsar **AUTHENTICATION**, establece si se usa **PIN** en **Scramble Keypad**.

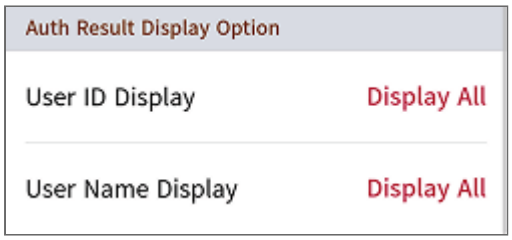


- **Scramble Keypad**: Las posiciones de las teclas numéricas pueden mezclarse aleatoriamente al ingresar una contraseña para evitar filtraciones.

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. Después de pulsar **AUTHENTICATION**, cambia los elementos deseados en **Auth Result Display Option**.

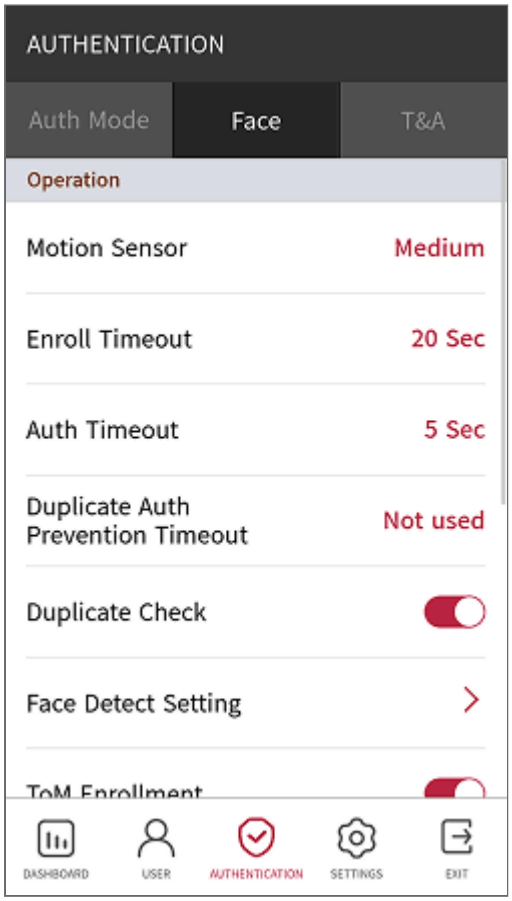


- **User ID Display**: Seleccione cómo se muestra el ID de usuario en la pantalla de resultados de autenticación del dispositivo.
  - **Display All**: Muestra el ID completo del usuario.
  - **Mask All but First Letter**: Muestra solo la primera letra del ID de usuario.
  - **Hide All**: No mostrar el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

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.



- **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 Auth Prevention Timeout**: Evita la autenticación duplicada durante el tiempo establecido cuando el sistema detecta de nuevo el mismo rostro. Configúrelo en **Not used** o de 3 a 60 segundos.

> **Información**
> El ajuste **Duplicate Auth Prevention Timeout** solo está disponible en el dispositivo maestro.

- **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**
  > - El rendimiento de la función anti-spoofing facial se ha mejorado para aprobar la prueba iBeta Level 1 ISO 30107-3 de detección de ataques de presentación.
  > - Con luz solar intensa, se recomienda usar la función **Fake Detection** como **Normal**.

- **Advanced Settings**: Cambie las configuraciones avanzadas para la autenticación facial, como la detección de mascarillas.
  - **Mask Detection**: Configure si se utiliza la detección de mascarillas.
  - **Detection Mode**: Defina el método para comprobar si se lleva mascarilla. Se activa cuando **Mask Detection** está configurado en **Enabled**.

> **Información**
>
> – **Require Mask (Hard)**: A los usuarios que no usan mascarilla se les niega la autenticación y se registra un evento de incumplimiento de uso de mascarilla.
> – **Require Mask (Soft)**: Los usuarios que no usan mascarilla aún pueden autenticarse, pero se registra un evento de incumplimiento de uso de mascarilla.
> – **Require No Mask**: Solo los usuarios que no usan mascarilla pueden autenticarse y, cuando se utiliza este modo, el modo de verificación de mascarilla se fija en **Check Before Authentication**.

– **Mask Detection Level**: Establece la sensibilidad para detectar el uso de mascarilla. Se activa cuando **Mask Detection** está configurado en **Enabled**.

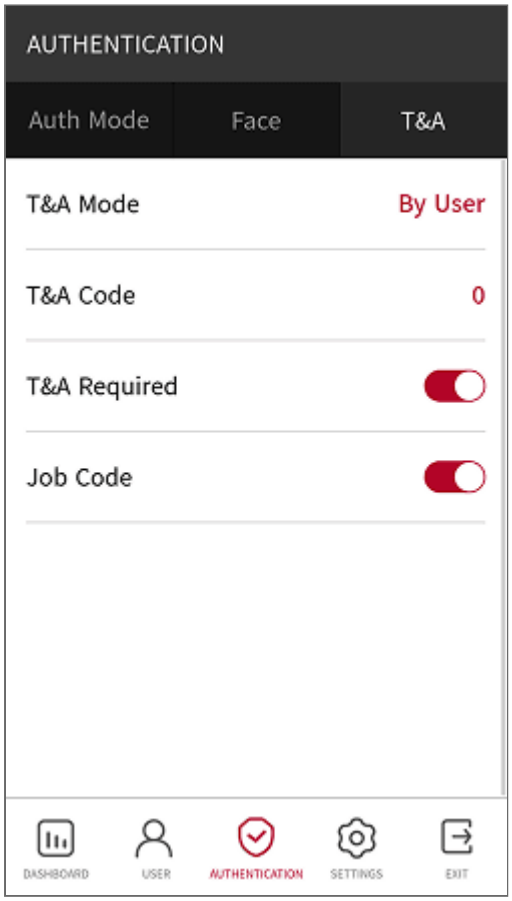
– **Check Mode**: Establece el modo de confirmación según el propósito del dispositivo.

> **Información**
>
> – **Check After Authentication**: Después de la autenticación, verifica si el usuario lleva mascarilla.
> – **Check Before Authentication**: Autentica después de comprobar si el usuario lleva mascarilla.
> – **Check Only**: El dispositivo solo se puede usar para comprobar si se lleva mascarilla. Cuando este modo está activado, cualquier usuario que lleve mascarilla puede acceder, sin importar la autenticación.

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**.
3. Cambie el elemento deseado.



- **T&A Mode**: Configura cómo usar el modo de asistencia.
- **T&A Code**: Registra eventos de T&A. Selecciona **T&A Code** → ⊕ para registrar eventos de asistencia y luego configura el icono que se mostrará en la pantalla, **T&A Event Name** y **Schedule**.
- **T&A Required**: Configure para que el usuario tenga que seleccionar un evento de T&A al autenticarse. Disponible cuando **T&A Mode** está configurado en **By User**.
- **Fixed T&A Key**: Configura para usar solo un evento de T&A seleccionado por el administrador. Disponible cuando **T&A Mode** está configurado en **Fixed**.
- **Job Code**: Configure si se usará el código de puesto.

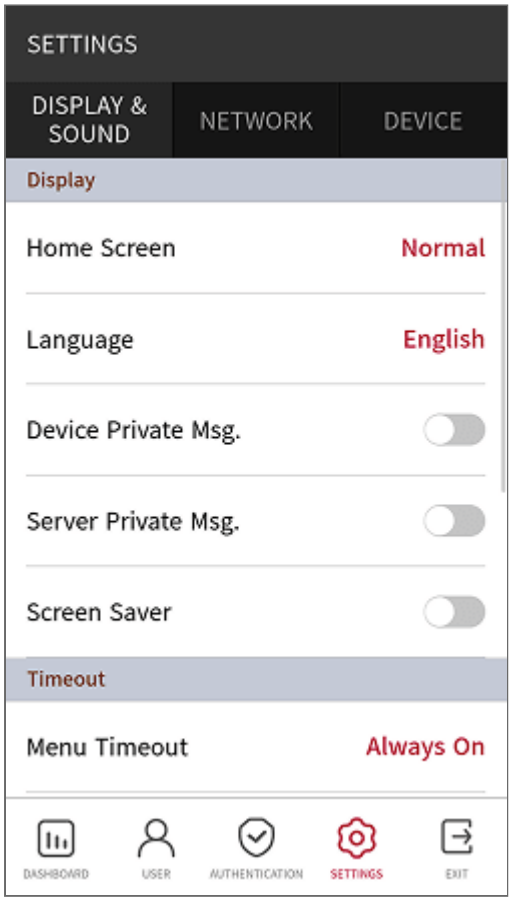
Ajustes

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

Pantalla y sonido

Cambie los ajustes de pantalla y sonido del dispositivo.

1. Presione ⊞ y autentíquese con la credencial de nivel de administrador.
2. Presione **SETTINGS** → **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 al disminuir el brillo de la pantalla cuando el dispositivo no está en uso.
- **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.
- **Intercom Speaker Volume**: Ajuste el volumen de salida del altavoz cuando use el intercomunicador IP.
- **Intercom Microphone Volume**: Ajuste el volumen de entrada del micrófono cuando use el intercomunicador IP.

Información

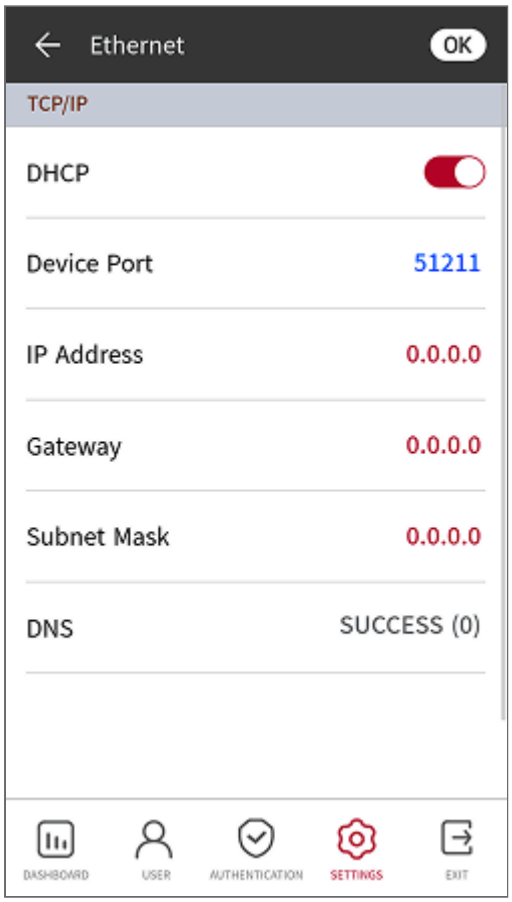
Para obtener más información sobre el SDK de dispositivos BioStar, consulte la página del SDK de dispositivos BioStar en la base de conocimientos de Suprema.

Red

Cambie 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 **SETTINGS** → **NETWORK** → **Ethernet**.
3. Cambie el elemento deseado.



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

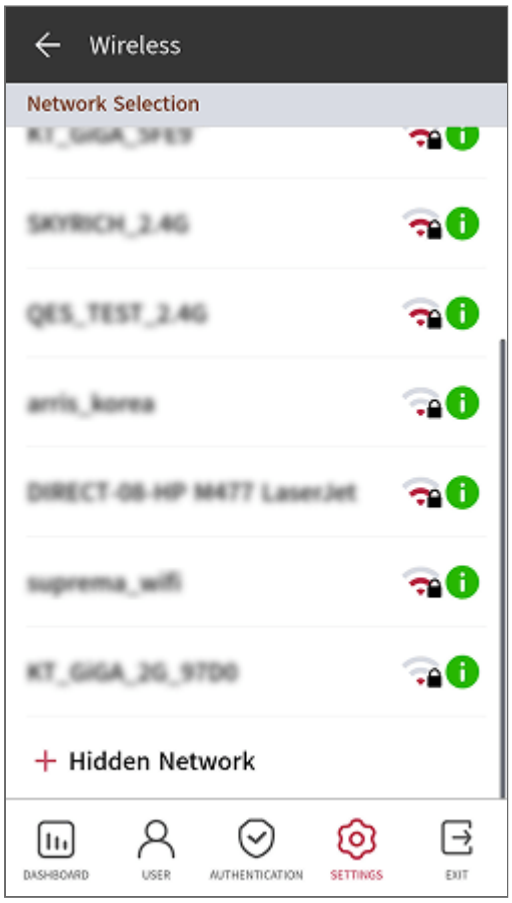
- **DNS**: Configure la dirección del servidor DNS.

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

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

LAN inalámbrica

1. Presione y autentíquese con la credencial de nivel de administrador.
2. Selecciona **SETTINGS** → **NETWORK** → **Wireless**.
3. Se mostrará la lista de redes disponibles para conectarse.



- **Hidden Network**: Agrega y conéctate a una red inalámbrica ingresando la información de red manualmente.
  - **SSID**: Ingresa el SSID. El SSID puede tener hasta 32 caracteres e incluir caracteres alfanuméricos (distingue mayúsculas y minúsculas) y caracteres especiales.
  - **Password**: Ingrese la contraseña. La contraseña solo puede incluir caracteres alfanuméricos y especiales.

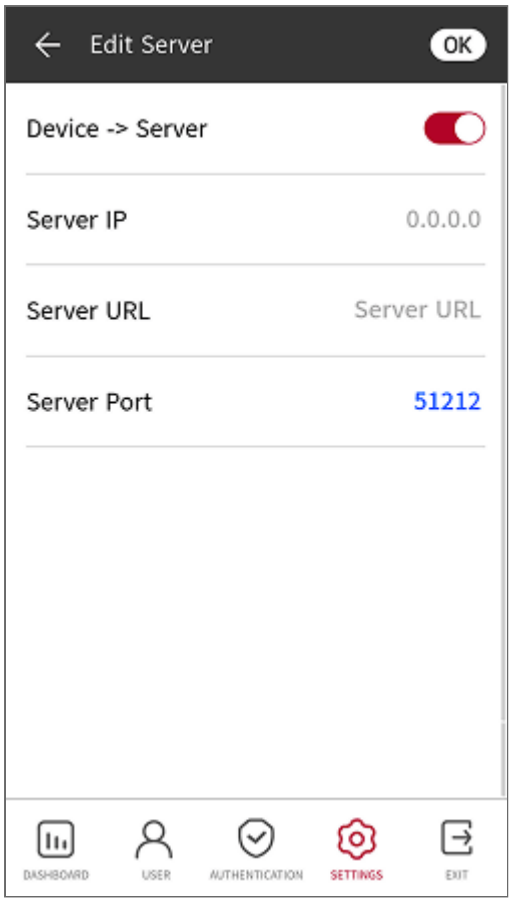
4. Seleccione la red a la que desea conectarse e ingrese la contraseña. Al presionar **OK**, se establecerá la conexión a la red inalámbrica.
5. Presiona en la red inalámbrica que deseas usar y luego desactiva la configuración DHCP para permitir que los usuarios modifiquen **IP Address**, **Gateway** y **Subnet Mask**.

Información

- **Wireless** solo está disponible para el modelo BS3-APWB.
- **Wireless** no se puede usar con **Ethernet**.
- Se requiere un enrutador inalámbrico para conectar **Wireless**. Para obtener información sobre la instalación y configuración del enrutador inalámbrico, consulte el manual del usuario del enrutador.

Servidor

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

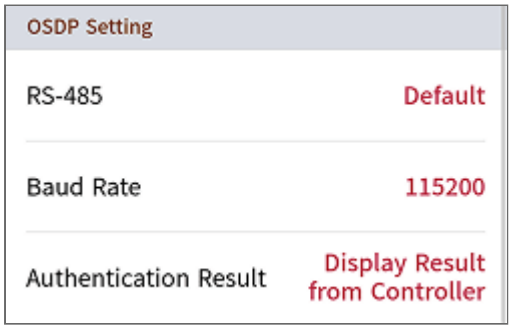


- **Device** → **Server**: Envíe directamente una señal de conexión desde el dispositivo a un servidor con la información ingresada. Cuando **Device** → **Server** está habilitado, el usuario puede ingresar **Server IP**, **Server URL** y **Server Port**.
- **Server IP**: Ingrese la dirección IP de la 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. Selecciona **SETTINGS** → **NETWORK**.
3. Configure el elemento deseado en **OSDP Setting**.



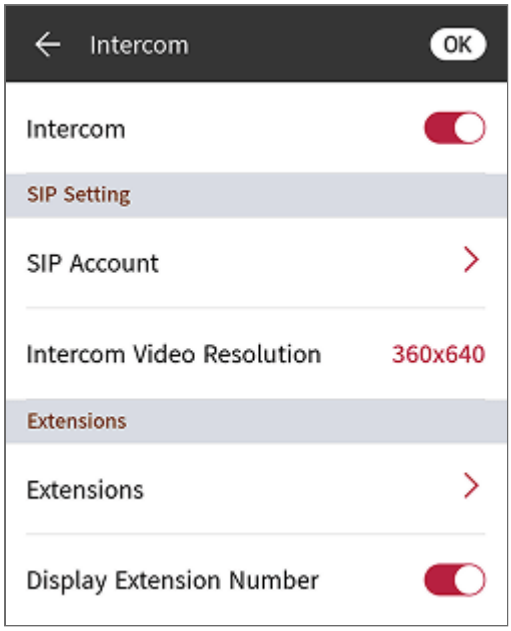
- **RS-485**: Seleccione el modo RS-485.
- **Baud Rate**: Seleccione la velocidad en baudios deseada.
- **Authentication Result**: Al usar **Intelligent Slave**, seleccione mostrar en pantalla los resultados de autenticación de controladores o dispositivos de terceros. Esta opción puede utilizarse cuando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

Dispositivo

Intercomunicador IP

Configura la cuenta y las extensiones del intercomunicador.

1. Presione y autentíquese con la credencial de nivel de administrador.
2. Seleccione **SETTINGS** → **DEVICE** → **Intercom**.



- **Intercom**: Configure si el intercomunicador está habilitado. Al habilitar la configuración del intercomunicador, puede configurar **SIP Account** y **Extensions**.
- **SIP Account**: Ingrese cada dato para que el dispositivo se registre en el servidor SIP.
- **Intercom Video Resolution**: Seleccione la resolución de salida de video del intercomunicador en el dispositivo.
- **Extensions**: Agregue, elimine o edite números de extensión.
- **Display Extension Number**: Configure si se mostrarán los números de extensión.

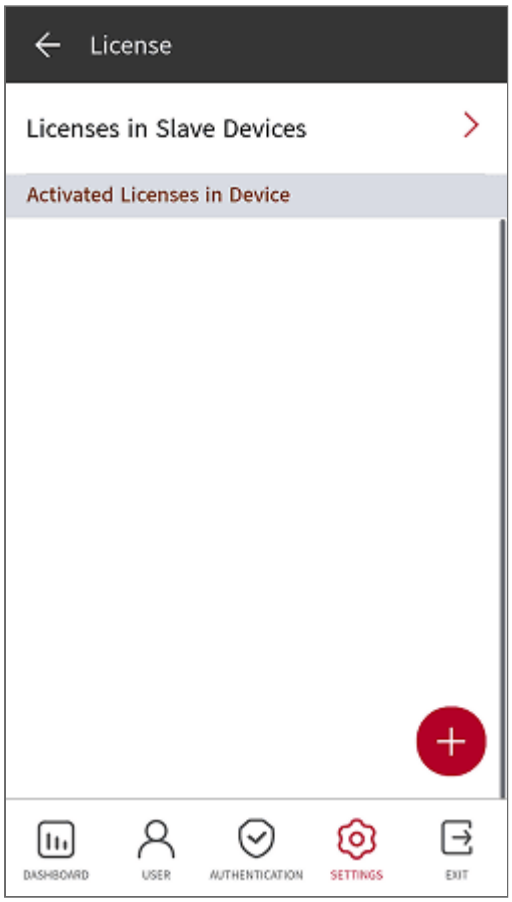
> **Información**
>
> - Si **Display Name** no está configurado, no será posible distinguir los receptores.
> - Los números de extensión solo pueden incluir caracteres alfanuméricos (distingue mayúsculas y minúsculas) y los caracteres especiales `+` `-` `@` `.`.

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

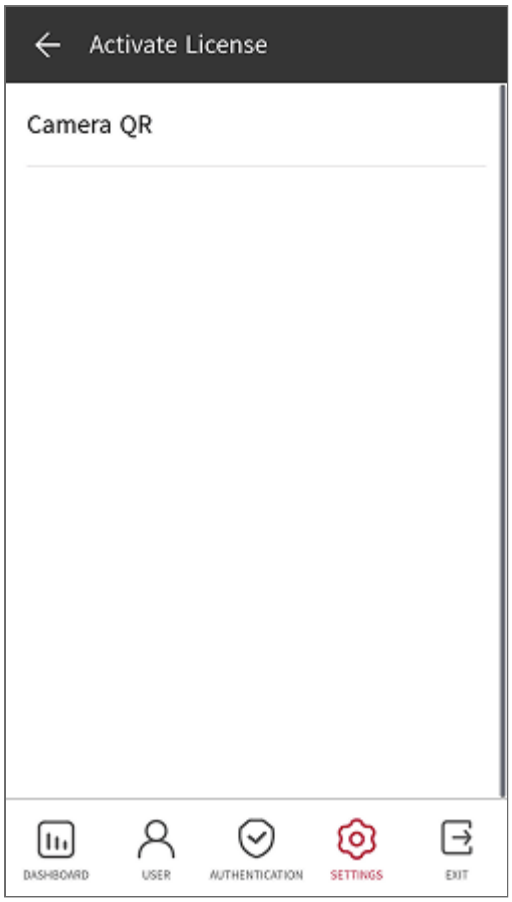
Licencia

Activa la licencia del dispositivo o revisa **Licenses in Slave Devices** y **Activated Licenses in Device**.

1. Presione y autentíquese con la credencial de nivel de administrador.
2. Seleccione **SETTINGS** → **DEVICE** → **License**.
3. Para activar la licencia del dispositivo, conecte el USB con la licencia al dispositivo y seleccione .



4. Las licencias que se pueden activar aparecen en la pantalla. Activa la licencia deseada.



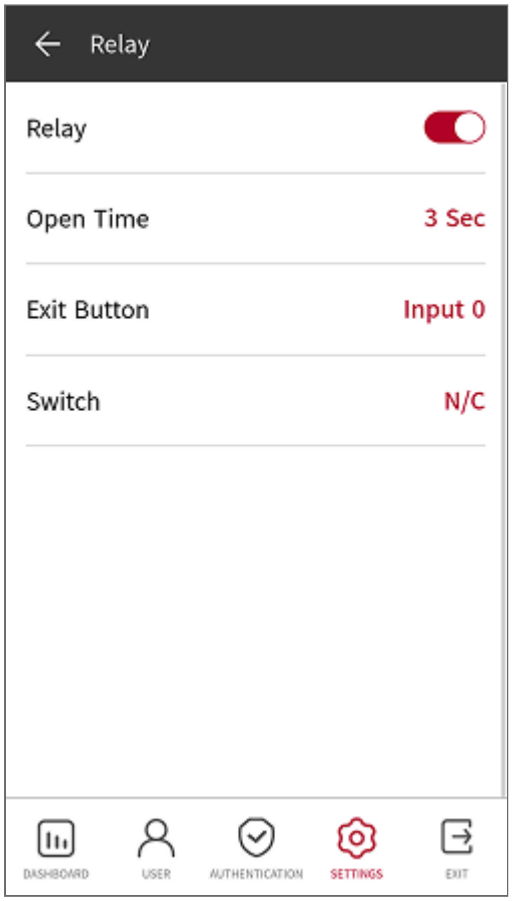
Información

- Contacta al lugar de compra para obtener una licencia de dispositivo.
- Hay una función disponible por licencia de dispositivo.
- Es posible incluir varias licencias de dispositivo en un solo archivo de licencia de dispositivo. (Admite hasta 100)
- El archivo de licencia del dispositivo está cifrado y no puede modificarse de forma arbitraria.
- Las licencias de dispositivo se emiten según el ID del dispositivo. Si el ID del dispositivo se cambia de manera inusual, no se proporciona servicio de garantía para la licencia.

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. Seleccione **SETTINGS** → **DEVICE** → **Relay**.

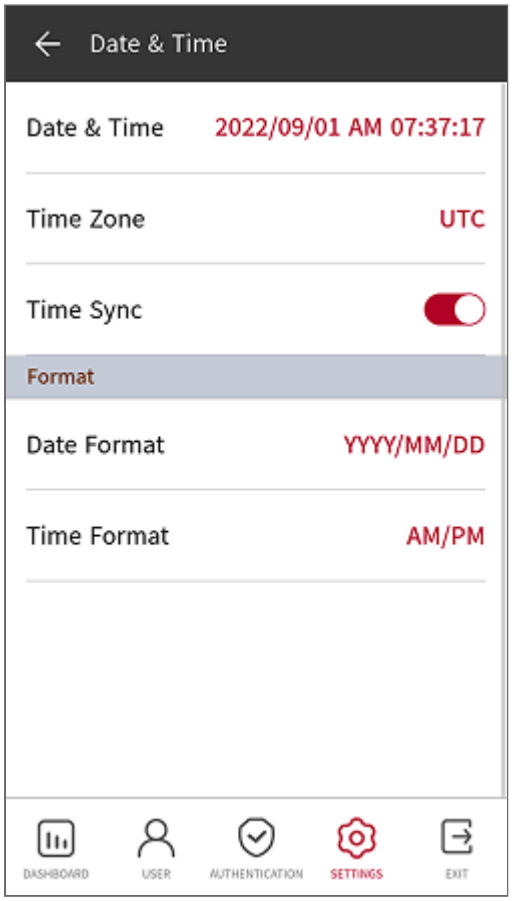


- **Relay**: Configure si el relé está habilitado. Para configurar **Open Time** y **Exit Button**, active esta opción.
- **Open Time**: Establece la duración que la puerta permanece abierta cuando se ha realizado la autenticación de usuario estándar.
- **Exit Button**: Seleccione el puerto de entrada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

Fecha y hora

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

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

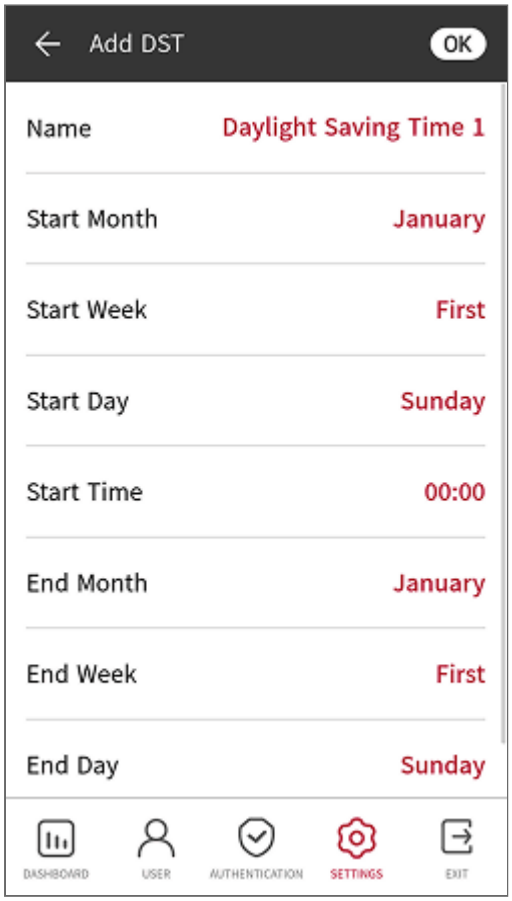


- **Date & Time**: Compruebe la fecha y hora actuales. Para modificarla manualmente, desactive **Time Sync**.
- **Time Zone**: Ajuste la referencia horaria de la ubicación actual.
- **Time Sync**: Sincronice el servidor y la hora. Si desea sincronizar el servidor y la hora, habilite **Time Sync**.
- **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. Seleccione **SETTINGS** → **DEVICE** → **Daylight Saving Time** y luego presione para añadir un horario de verano adicional.
3. Cambie el elemento deseado.



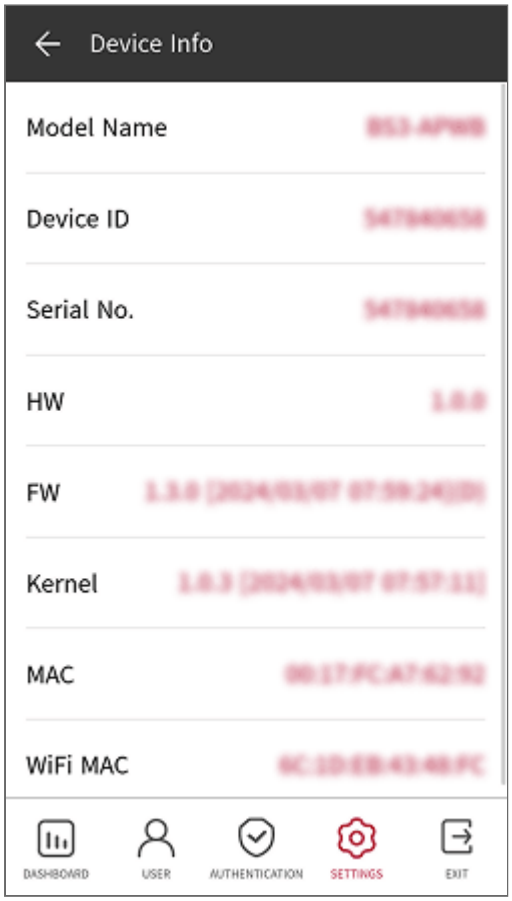
- **Name**: Establece el nombre del horario de verano.
- **Start Month** / **Start Week** / **Start Day** / **Start Time**: Configure los detalles sobre cuándo comienza el horario de verano.
- **End Month** / **End Week** / **End Day** / **End Time**: Configure los detalles sobre cuándo termina el horario 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. Seleccione **SETTINGS** → **DEVICE** → **Device Info**. Vea la información de **Model Name**, **Device ID**, **Serial No.**, **HW**, **FW**, **Kernel**, **MAC** y **WiFi MAC**.



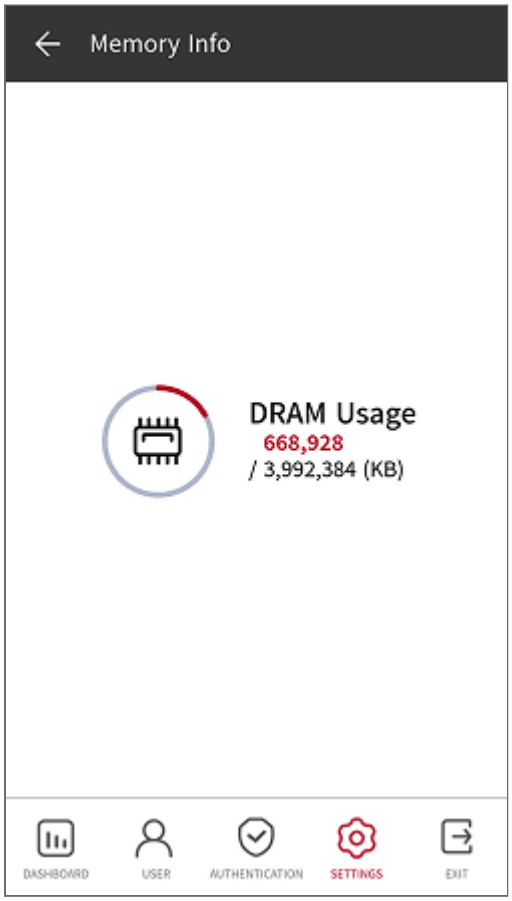
Información

- Mantenga presionado **MAC** para mostrar la información **FAS_IR_SP** que indica la versión del algoritmo de anti-suplantación facial. Si presiona **FAS_IR_SP**, puede ver el valor hash completo en un mensaje emergente.
- **WiFi MAC** solo se puede confirmar en el modelo BS3-APWB.

Información de memoria

Consulta el estado de uso de la memoria.

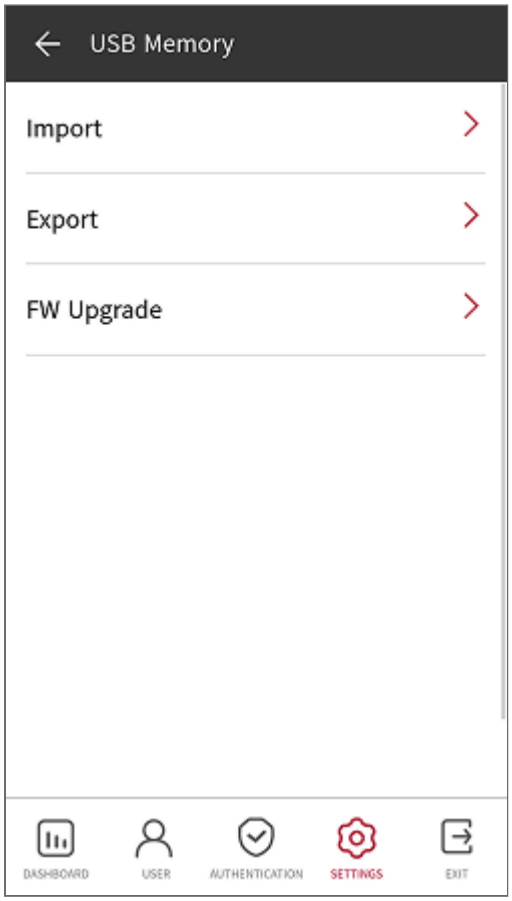
1. Presione y autentíquese con la credencial de nivel de administrador.
2. Seleccione **SETTINGS** → **DEVICE** → **Memory Info**. Consulta el estado de uso de memoria del dispositivo.



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. Seleccione **SETTINGS** → **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.

Información

- 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.

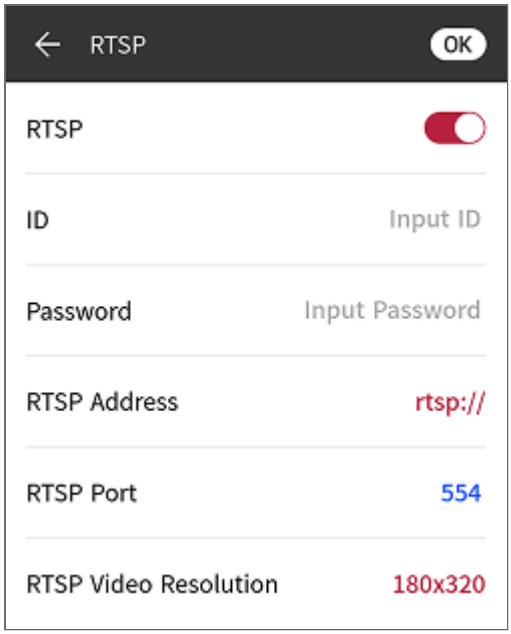
1. Presione y autentíquese con la credencial de nivel de administrador.
2. Selecciona **SETTINGS** → **DEVICE**.

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.

RTSP

Conecta un sistema de gestión de video (VMS) de terceros para monitorear los videos filmados con la cámara visual del producto.

1. Presione y autentíquese con la credencial de nivel de administrador.
2. Seleccione **SETTINGS** → **DEVICE** → **RTSP**.
3. Selecciona el elemento deseado y cambia el ajuste.



- **RTSP**: Configure si RTSP está habilitado o no. Cuando RTSP está habilitado, el usuario puede configurar **ID**, **Password**, **RTSP Address**, **RTSP Port** y **RTSP Video Resolution**.
- **ID**: Ingrese el ID. El ID puede tener hasta 32 caracteres, en una combinación de caracteres alfanuméricos (distingue mayúsculas y minúsculas) y los símbolos `-` `_`.
- **Password**: Ingrese la contraseña. La contraseña puede tener de 8 a 32 caracteres en una combinación de letras (mayúsculas y minúsculas) y números.
- **RTSP Address**: Ingrese la dirección RTSP.
- **RTSP Port**: Ingrese el puerto RTSP.
- **RTSP Video Resolution**: Seleccione la resolución de la salida de video RTSP desde el dispositivo.

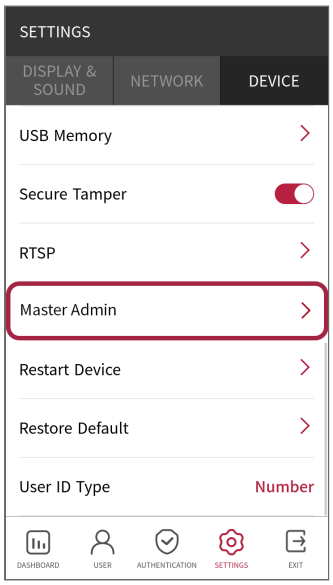
Información

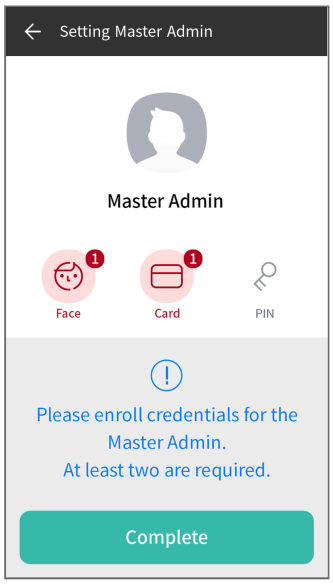
Cuando el dispositivo está configurado como dispositivo esclavo, es posible que la función RTSP no esté disponible.

Administrador maestro Productos orientados a CE

Cambie el método de autenticación del administrador maestro.

1. Presione y autentíquese con la credencial de nivel de administrador.
2. Seleccione **SETTINGS** → **DEVICE** → **Master Admin**.
3. Configure los métodos de autenticación deseados.





Información

- Debe enrolar al menos dos tipos de credenciales.
- Esta función solo está disponible en dispositivos con firmware versión 1.4.0 o superior.

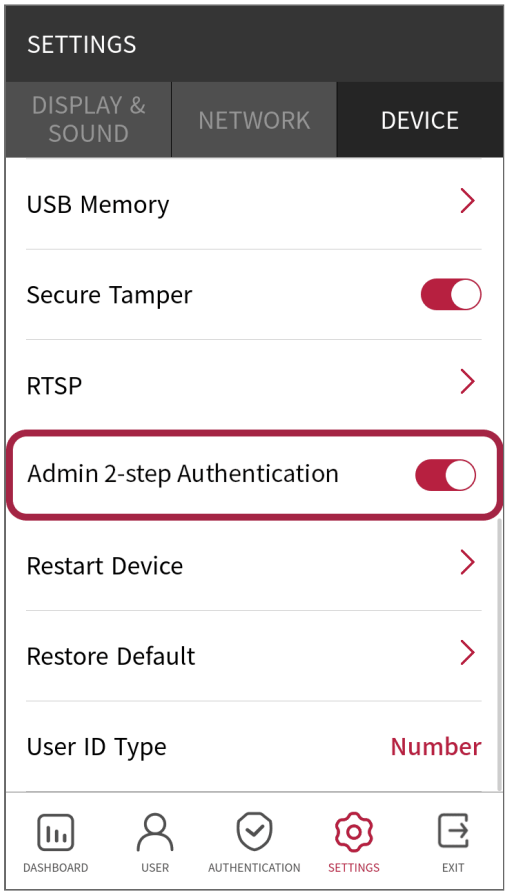
Autenticación de dos factores del administrador Productos orientados a CE

Un producto CE actualizado mediante firmware no ofrece settings de **Master Admin**, pero puede usar la opción **Admin 2-step Authentication** para mejorar los privilegios generales del administrador y la seguridad del dispositivo.

Información

- **Admin 2-step Authentication** se puede activar solo si todos los administradores enrolled tienen al menos dos tipos de credenciales.
  - El PIN no se puede usar como credencial independiente, por lo que la combinación ID + PIN no es compatible.
- El dispositivo actualizado mediante firmware no puede degradarse a una versión inferior después de la actualización.

1. Presione y autentíquese con la credencial de nivel de administrador.
2. Active **SETTINGS** → **DEVICE** → **Admin 2-step Authentication**.

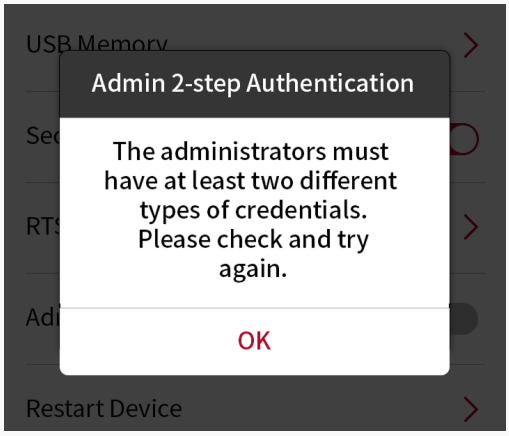


Información

Si no hay dos tipos de credenciales enroladas para todos los administradores, la activación falla y se muestra un mensaje de error.

Enrole dos tipos de credenciales para todos los administradores e inténtelo nuevamente.

- El PIN no se puede usar como credencial independiente, por lo que la combinación ID + PIN no es compatible.



Precaución

Si activa **Admin 2-step Authentication** y elimina las credenciales de todos los administradores hasta dejar menos de dos tipos, no podrá acceder al menú de administrador cuando BioStar X o BioStar 2 no estén disponibles. Por lo tanto, tenga especial cuidado al eliminar credenciales de administrador.

Reiniciar dispositivo

Reinicia el dispositivo.

1. Presione y autentíquese con la credencial de nivel de administrador.
2. Seleccione **SETTINGS** → **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. Seleccione **SETTINGS** → **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 **SETTINGS** → **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. Seleccione el elemento deseado.

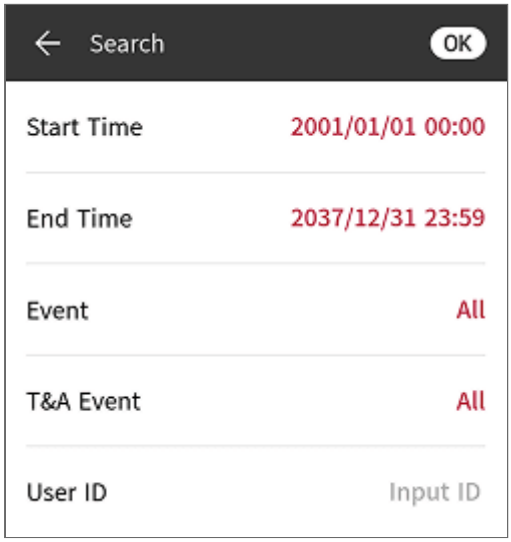
Registros de eventos

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 en **DASHBOARD**. 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

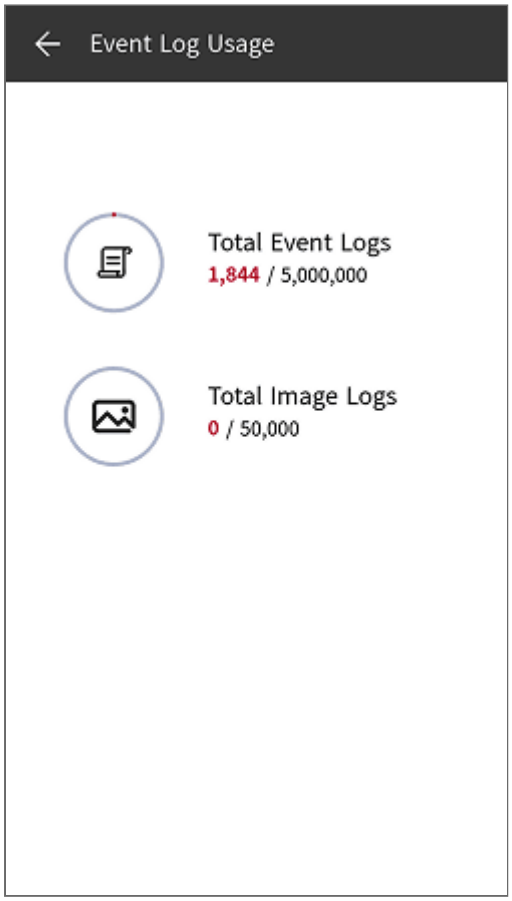
Elimina todos los registros guardados.

1. Presione y autentíquese con la credencial de nivel de administrador.
2. Seleccione en **DASHBOARD**. Todos los registros de eventos aparecen.
3. Seleccione y haga clic en **OK** para eliminar todos los registros. Presiona **Cancel** para regresar a la pantalla anterior.

Ver uso de registros

Consulta el estado del uso de registros.

1. Presione y autentíquese con la credencial de nivel de administrador.
2. Presione → en **DASHBOARD**. Verifique el uso de los registros de eventos e imágenes del dispositivo.


Event Log Usage
Total Event Logs
1,844 / 5,000,000
Total Image Logs
0 / 50,000

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 enrole el rostro nuevamente.
- 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.

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.

Administrador maestro (productos orientados a CE)

Q. ¿Es compatible la configuración de Administrador maestro después de una actualización de firmware desde un dispositivo existente?

- **Master Administrator solo es compatible en productos orientados a CE con una etiqueta con marca CE**. Use la etiqueta adhesiva en la parte posterior del producto para identificar productos **orientados a CE / globales (no CE)**. Para obtener detalles, consulte la Política de soporte del administrador maestro.

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 1.0 m** • **Altura de autenticación:De 1.4 a 1.9 m** • **Velocidad de coincidencia:En un plazo de 0.2 segundos** • **Detección de rostro vivo:Soportado**	
Tarjeta RF	**BS3-DB**	**125kHz EM y 13.56MHz MIFARE, MIFARE Plus, DESFire, DESFire EV1/EV2/EV3, FeliCa**
	BS3-APWB	**125kHz EM, HID Prox y 13.56MHz MIFARE, MIFARE Plus, DESFire, DESFire EV1/EV2/EV3, FeliCa, iCLASS SE/SR/Seos**
Rango de lectura RF[2]	**EM/HID Prox/MIFARE/DESFire/HID iCLASS: 30 mm, FeliCa: 15 mm**	
Móvil	**NFC, BLE**	
Teclado aleatorio (PIN)	**Soportado**	
QR/Código de Barras[3]	**Soportado[4]**	
Rango de lectura QR/ Código de barras[5]	**De 30 a 40 cm**	

General

Nombre del modelo	**BS3-DB, BS3-APWB**
CPU	**1.5 GHz Quad Core**
Memoria	**32 GB Flash + 4 GB RAM**

Chip criptográfico	**Soportado**	
Visualizar	**LCD en color IPS 5.5"**	
Resolución de pantalla	**720 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**	**82.5 x 171 x 23.4 (mm)**
	Soporte	**72.9 x 164 (mm)**
Peso	**Dispositivo**	• **BS3-DB: 370 g** • **BS3-APWB: 380 g**
	Soporte	**90 g (incluye arandelas y tornillos)**
Grado de protección IP	**IP65**	
Grado de protección IK	**IK06**	
Certificaciones	**CE, UKCA, KC, FCC, IC, RCM, BIS, SIG, RoHS, REACH, WEEE, MIC, TELEC**	

Capacidad

Máx. usuarios	**100,000**[6)]
Máx. credenciales (1:N)	**Rostro: 50,000**
Máx. credenciales (1:1)	• **Rostro: 100,000** • **Tarjeta: 100,000** • **PIN: 100,000**
Máx. registros de texto	**5,000,000**
Máx. registros de imágenes	**50,000**

Interfaz

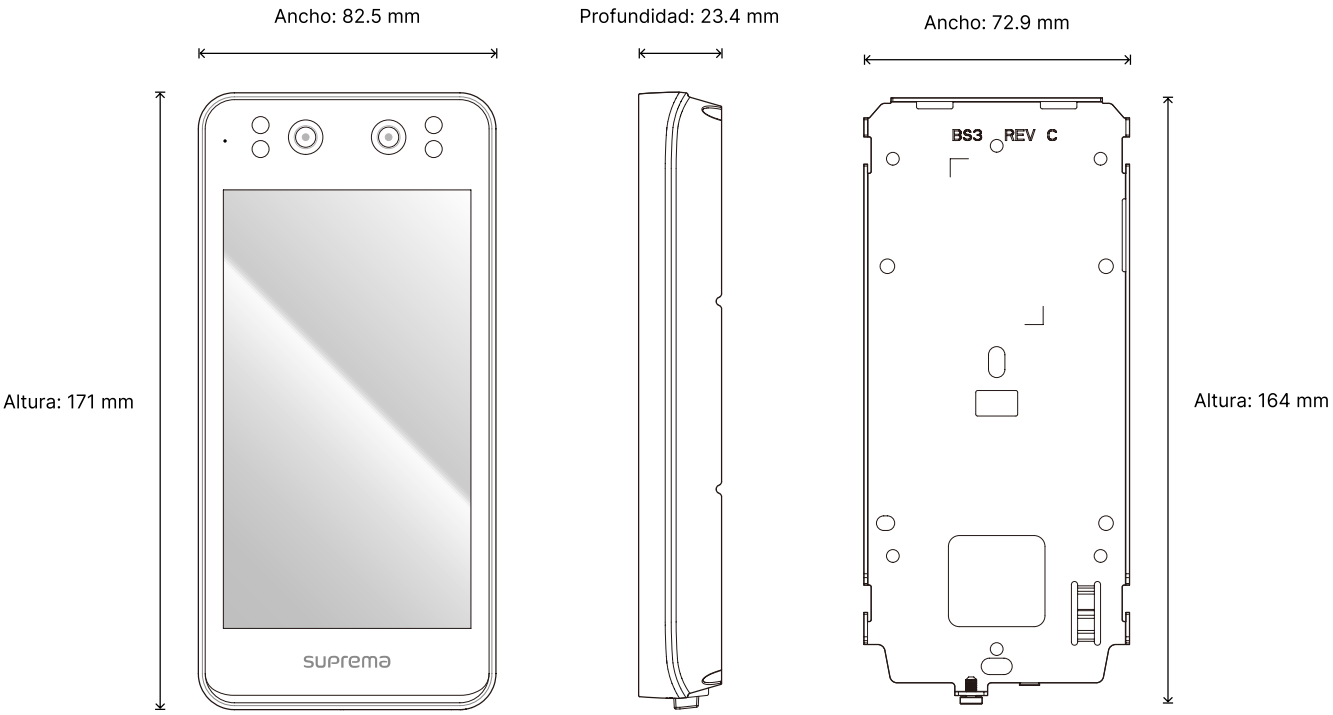
Ethernet	**Admitida (10/100/1000 Mbps, MDI/MDI-X automática)**	
Wi-Fi	**BS3-DB**	**No compatible**
	BS3-APWB	**Compatible (802.11 b/g/n 2.4 GHz)**
Protocolo de red	**TCP, UDP**	
RS-485	**1 canal maestro/esclavo (seleccionable)**	
Protocolo de comunicación RS-485	**Compatible con OSDP V2**	
Wiegand	**Entrada de 1 canal, salida de 1 canal**	
Entrada	**3 canales de entrada**	
Relé	**1 relé**	
PoE+[7)]	**BS3-DB**	**No compatible**
	BS3-APWB	**Compatible (compatible con IEEE 802.3at)**

Interfono	**Soportado**
RTSP	**Soportado**
USB	**USB 2.0 (Maestro)**
Puerto de expansión USB	**Soportado**
Tamper	**Soportado**

Eléctrico

Alimentación	**12 Vdc**	**Corriente: Máx. 1 A**
	24 Vdc	**Corriente: Máx. 0.7 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



Peso
- BS3-DB: 370 g
- BS3-APWB: 380 g

Peso: 90 g
(Incluyendo arandela y perno)

---

1) La distancia mínima de autenticación facial indicada es la configuración predeterminada del producto y la distancia recomendada de autenticación facial es de 0.6 a 1.0 m.

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

3) Admite códigos QR y de barras de hasta 32 cadenas de código ASCII.

4) Requiere una licencia aparte.

5) La distancia indicada para el reconocimiento de QR/código de barras es una distancia recomendada, y la distancia reconocible real puede variar según el tamaño del QR/código de barras y el entorno de instalación.

6) Número de usuarios registrados sin datos de credenciales.

7) Requiere alimentación PoE+ (IEEE 802.3at, 30 W) o PoE++ (IEEE 802.3bt, 60-100 W). No se admite PoE estándar (IEEE 802.3af, 15.4 W). El uso de PoE estándar puede provocar que los dispositivos funcionen de forma inestable o sufran daños permanentes. Antes de conectar el dispositivo, asegúrese de que su switch de red o inyector PoE sea compatible con PoE+ o PoE++.

Información

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

Información Reglamentaria

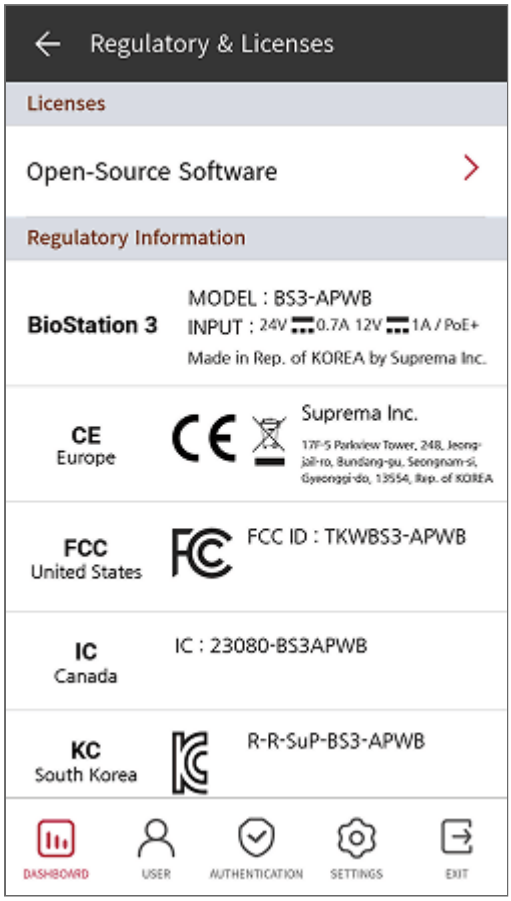
Proporciona información sobre las normativas y certificaciones que cumple el producto.

Regulaciones y licencias

Verifique la licencia, la certificación regulatoria y las marcas de cumplimiento en el producto.

- CE / FCC / IC / KC / UKCA / RCM / MIC / TELEC

1. Presione y autentíquese con la credencial de nivel de administrador.
2. En la esquina superior derecha, toque **DASHBOARD** y luego toque para verificar **Regulatory & Licenses**.



Información

Si no se ha designado un administrador, al presionar se mostrará la pantalla de **DASHBOARD**.

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 glibc incluida en este producto se rige por la LGPL. Para obtener más información sobre la licencia LGPL, consulte la GNU Lesser General Public License.
- Este producto usa "OpenSSL", que está licenciado bajo las licencias OpenSSL y Original SSLeay. Para más información sobre las licencias OpenSSL y Original SSLeay, consulte la OpenSSL License y la Original SSLeay License.
- El código fuente modificado basado en el kernel de Linux 4.x y la biblioteca glibc incluido en este producto puede descargarse contactando al Equipo de Soporte Técnico de Suprema.

Suprema Inc.

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

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

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

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