BioStation 2a

GUÍA DE USUARIO DE

Versión 1.04

Español
ES 102.00.BS2A

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 ingreso de huellas dactilares 17

Instalación 19

Fijar el soporte y el producto 19

Conexión de la fuente de alimentación 21

Conexión de red 22

Conexión de entrada 23

Conexión del relé 24

Conectar como independiente 26

Conectar Secure I/O 2 28

Conexión Wiegand 29

Cómo Usar 30

Menú de Administrador 30

Usuario 32

Autenticación 35

Ajustes 41

Registros de eventos 54

Solución de Problemas 57

Verifique estos elementos antes de reportar una falla 57

Especificaciones del Producto 59

Credenciales 59

General 59

Capacidad 60

Interfaz 61

Eléctrico 61

Dimensiones y peso 62

Información Reglamentaria 64

Información de cumplimiento de la FCC 64

Declaración de conformidad de la UE (CE) 65

Apéndices 66

Descargos de responsabilidad 66

Aviso de derechos de autor 67

Licencia de código abierto 67

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.

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 60 °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.

Este producto utiliza un botón capacitivo. Si está lloviendo o hay mucha humedad en la superficie del producto, séquelo con un paño seco antes de usarlo.

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

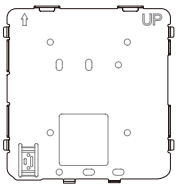
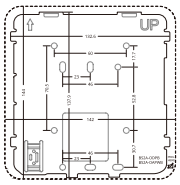
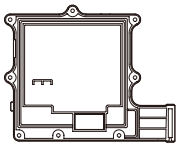
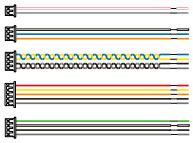
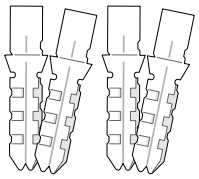
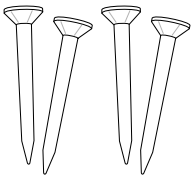
- El dispositivo puede funcionar incorrectamente.

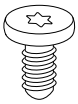
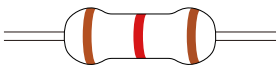
> **Batería RTC**
>
> Reemplazar por baterías no autorizadas o de tipo incorrecto puede representar un riesgo de explosión. Deseche las baterías conforme a las normativas locales o internacionales sobre residuos.

Primeros Pasos

Proporciona procedimientos iniciales para empezar con el dispositivo.

Componentes

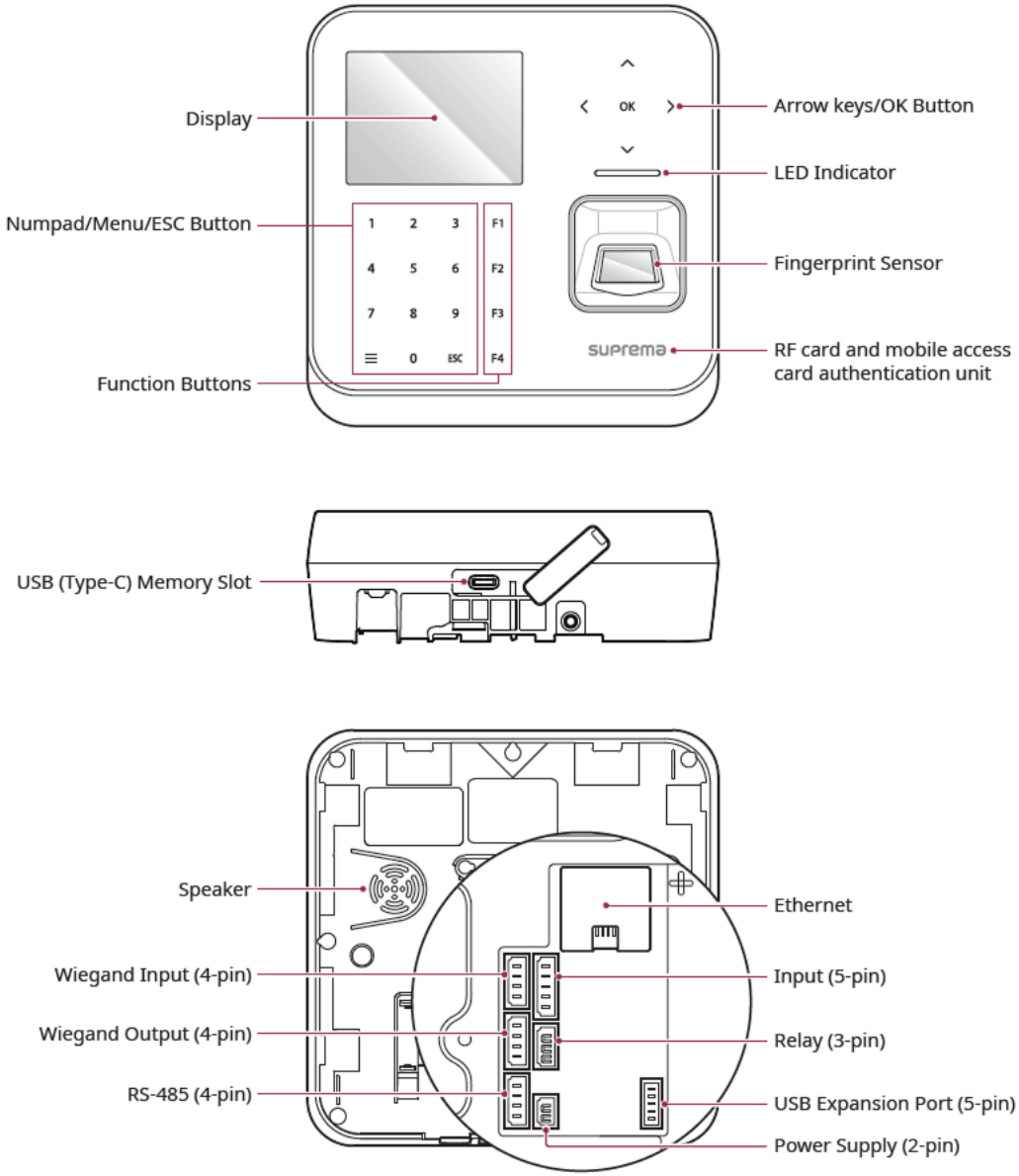
			
BioStation 2a	Soporte de pared	Plantilla de perforación	Cubierta de cable
			
Cables de conexión	Guía rápida	Anclajes de PVC x4	Tornillos de fijación x4

		
Tornillo de fijación del soporte (en forma de estrella)	Resistencia de 120 Ω	Diodo

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



- **Pantalla**: Proporciona una interfaz de usuario para la operación.
- **Botón Número/Menú/ESC**
  - **0-9**: Ingresar números/caracteres, seleccionar menús
  - ☰: Ingresar al menú
  - **ESC**: Regresar a la pantalla anterior, cancelar ingreso
- **Botón Función**: Se usa como tecla funcional de control de asistencia o para seleccionar submenú.
- **Botón Dirección/OK**
  - ^: Cambiar tipo de carácter, establecer inicio/fin de guardia
  - v: Cambiar tipo de carácter, seleccionar evento de asistencia para registro

  - ‹ : Eliminar números/caracteres, autenticar con ID
  - › : Insertar símbolo, definir elemento, seleccionar código de operación
  - **OK**: Seleccionar elemento/guardar ajuste, activar menú de teclas
- **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.
- **Unidad de reconocimiento de huella dactilar**: La parte que reconoce la huella dactilar para acceso.
- **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.
- **Ranura para memoria USB (tipo C)**: Conecta la memoria USB.
- **Altavoz**: Emite sonido.
- **Entrada Wiegand (4 pines)**: Conecta el cable de entrada Wiegand.
- **Salida Wiegand (4 pines)**: Conecta el cable de salida Wiegand.
- **RS-485 (4 pines)**: Conecta el cable RS-485.
- **Ethernet**: Conecta el cable Ethernet.
- **Entrada (5 pines)**: Conecta el cable de entrada.
- **Relé (3 pines)**: Conecta el cable del relé.
- **Puerto de expansión USB (5 pines)**: Conecta otros productos accesorios.
- **Alimentación (2 pines)**: Conecta el cable de alimentación.

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**.

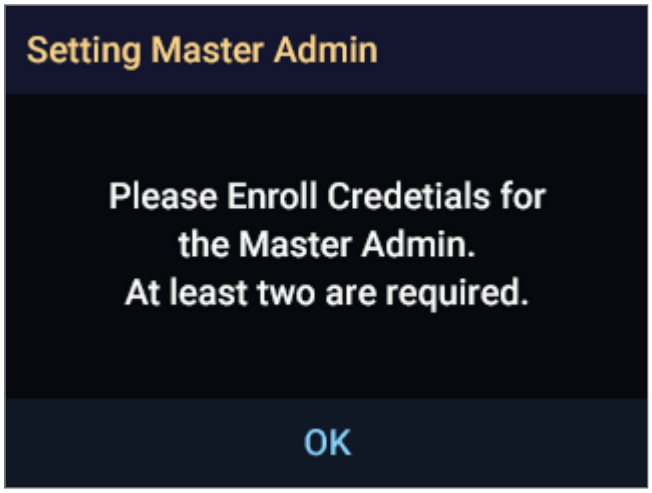
Contacte a Equipo de Soporte Técnico global de Suprema para obtener información detallada sobre la disponibilidad del soporte por versión.

Registrar Master Admin en un dispositivo nuevo

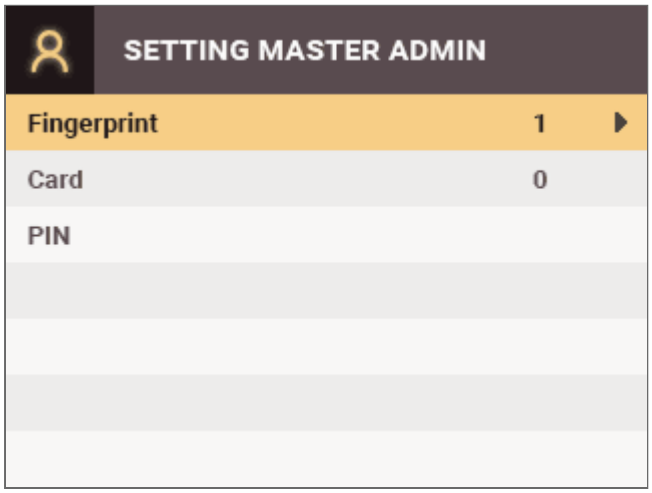
En un dispositivo nuevo para Productos CE, debe enrolar **Master Admin** desde el inicio. Si no lo enrola, el uso del dispositivo queda restringido.

> **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**. Presione **OK** para iniciar la inscripción.



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.



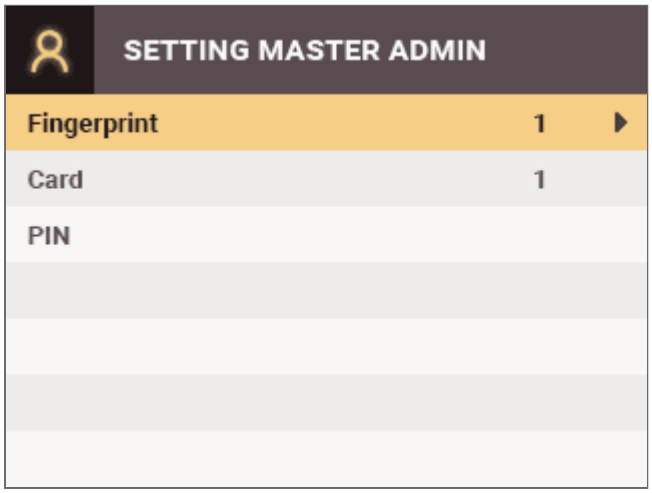
Las credenciales que se pueden inscribir para **Master Admin** son las siguientes.

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 **OK** para completar la inscripción 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.

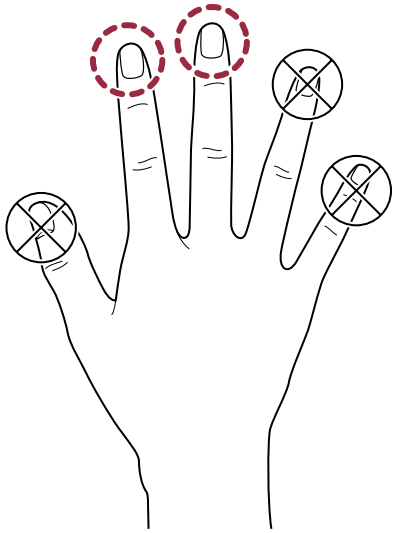
- **Restricción de transmisión de imágenes biométricas RS-485**

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 ingreso de huellas dactilares

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

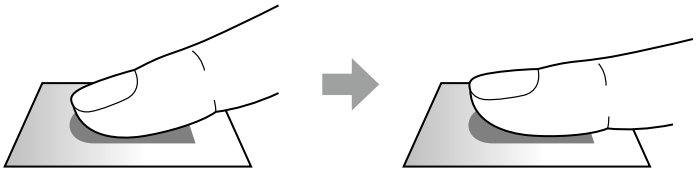
Selección de dedo para el ingreso de huella dactilar



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

Método de registro de huellas dactilares

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

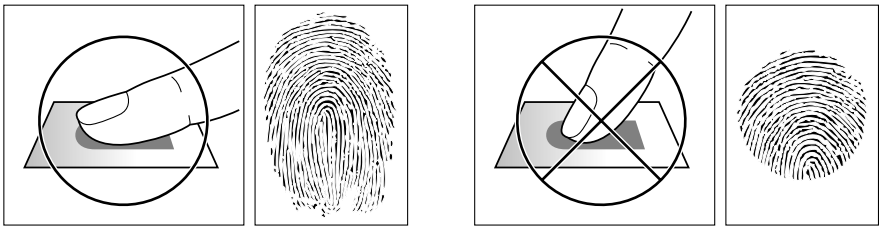


2. Cuando aparezca la pantalla de reingreso tras el beep, vuelva a escanear la huella del dedo registrado. (escanee dos

veces la huella del dedo que va a registrar)

Precauciones para la inscripción de huellas dactilares

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



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

Si la autenticación de huellas no funciona correctamente

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

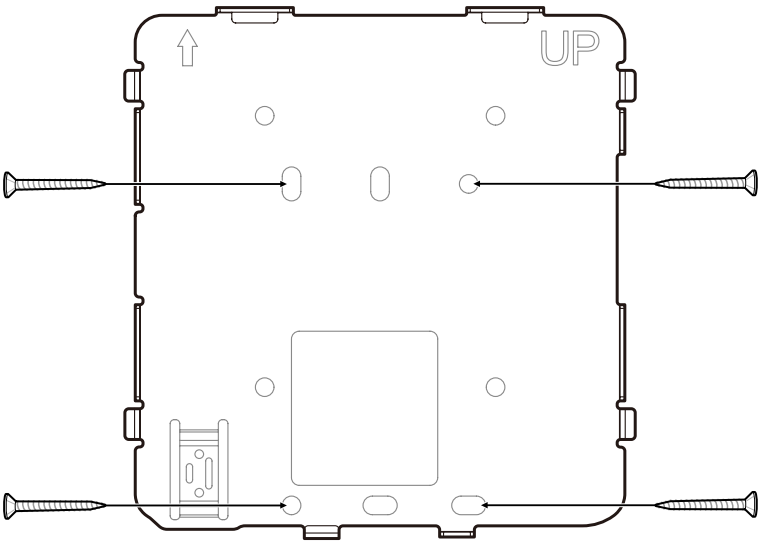
- Si el dedo está mojado o sudoroso, séquelo y luego escanee la huella.
- Si el dedo está demasiado seco, sople sobre la yema y luego escanee la huella.
- Si el dedo tiene un corte, registre la huella de otro dedo.
- Como la huella dactilar inscrita inicialmente con frecuencia no se introduce correctamente,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

Instalación

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

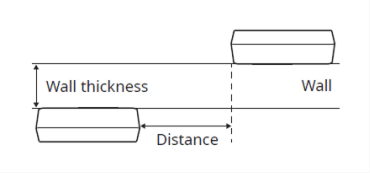
Fijar el soporte y el producto

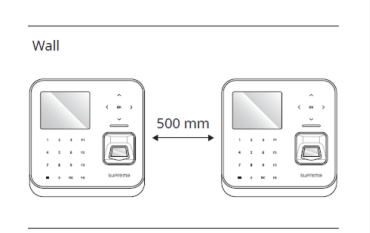
1. Determine la posición correcta para instalar el soporte usando la plantilla de perforación proporcionada. Asegura firmemente el soporte con los tornillos de fijación en el lugar donde se montará el producto.



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.

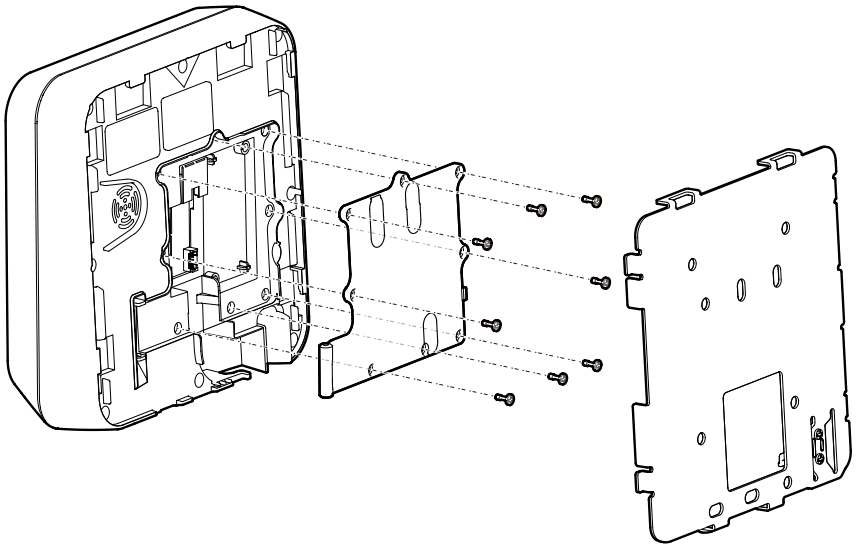




Espesor de pared	Distancia
100 mm	500 mm
120 mm	400 mm
150 mm	300 mm

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

2. Ensamble la cubierta del cable y luego instale el producto en el soporte asegurado.

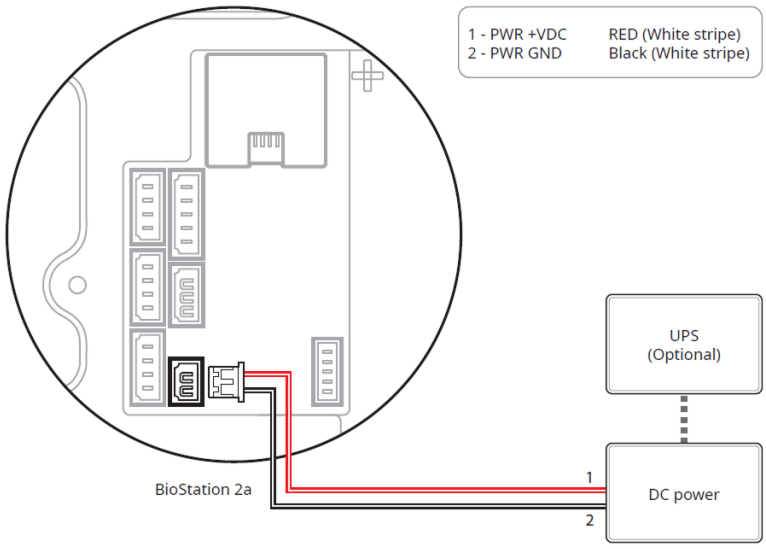


> **Información**
> Use la cubierta del cable después de conectar el producto y los cables para cumplir con las clasificaciones IP65 de resistencia al agua y al polvo.

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

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

Conexión de la fuente de alimentación



Precaución

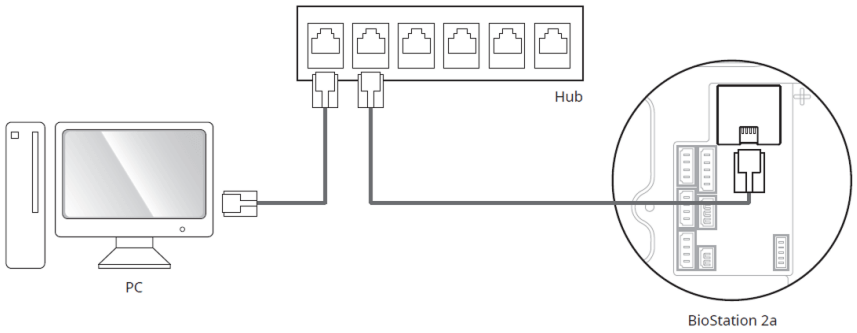
- NO conecte el dispositivo a la fuente de alimentación de CC (o adaptador) y a la alimentación PoE al mismo tiempo.
- Use un adaptador de alimentación aprobado por IEC/EN 62368-1 que admita un consumo de energía mayor que el del producto. Si desea conectar y usar otro dispositivo al adaptador de alimentación, 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.
- NO extienda la longitud del cable de alimentación al usar el adaptador de alimentación.

Conexión de red

TCP/IP

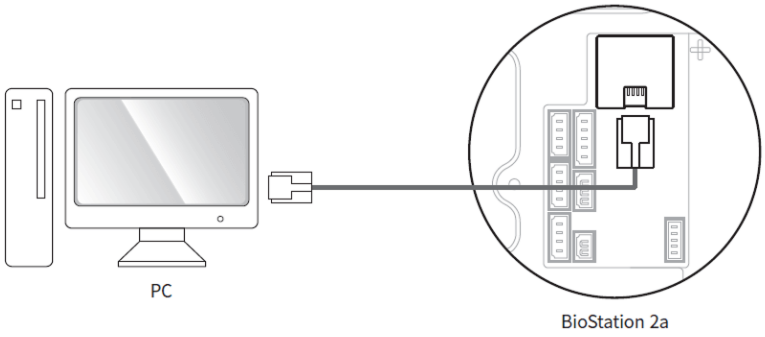
Conexión LAN (conexión a un concentrador)

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.



Puertos y servicios de red

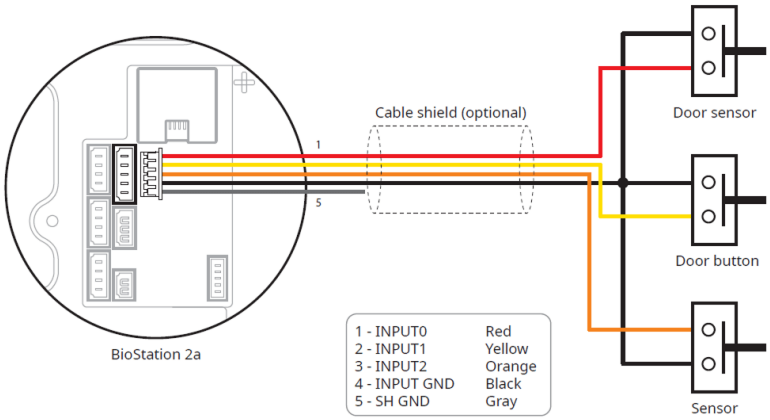
Este dispositivo usa los siguientes puertos para la comunicación de red y el funcionamiento estable del servicio.

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

Información

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

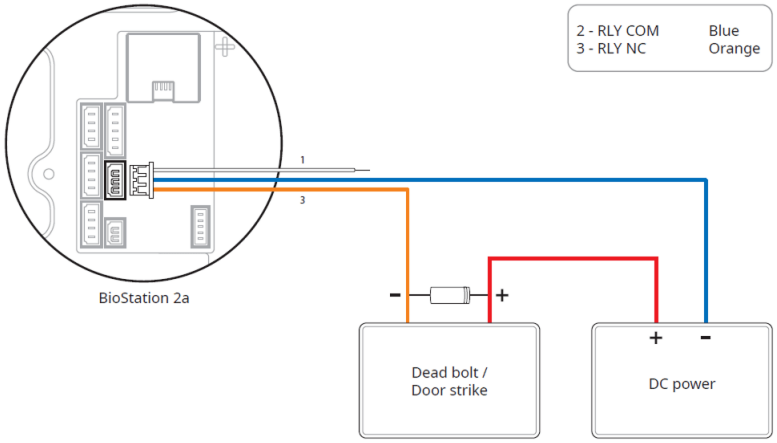
Conexión de entrada



Conexión del relé

Cerradura fail safe

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



Precaución

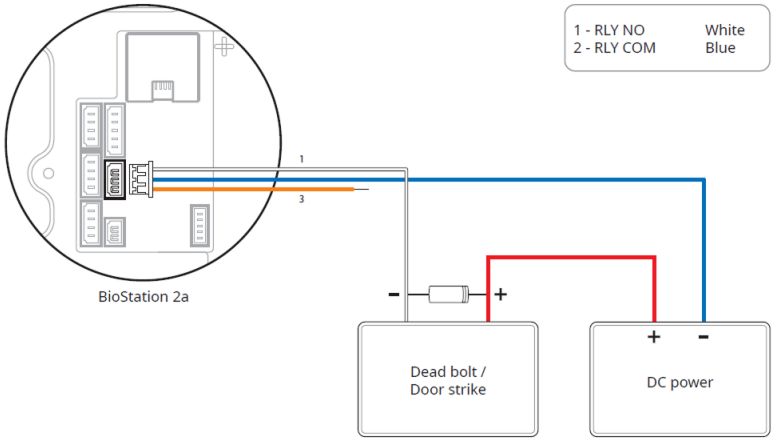
- Instale un diodo en ambos extremos del cable de la cerradura, como se muestra en la figura, para proteger el relé de la corriente inversa que se produce cuando la cerradura funciona.
- Utilice una fuente de alimentación independiente para el producto y la cerradura.
- Los lectores inteligentes independientes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

Información

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

Cerradura fail secure

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



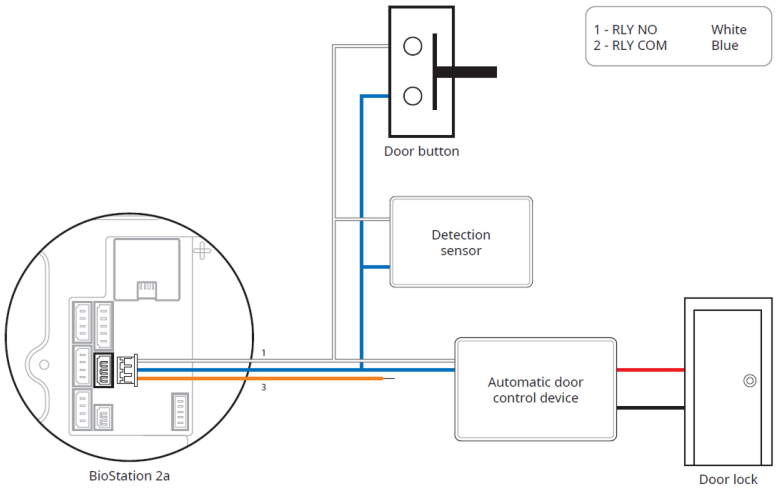
Precaución

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

Información

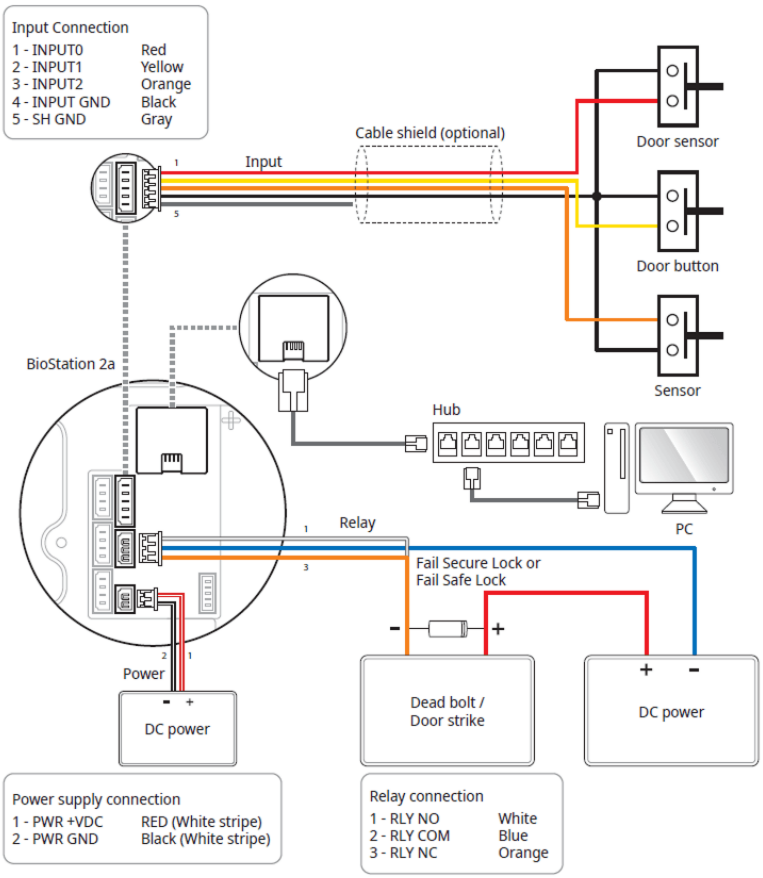
Preste atención a la dirección de instalación del diodo. Instale el diodo cerca de la cerradura.

Conexión de puerta automática



Conectar como independiente

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



Precaución

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

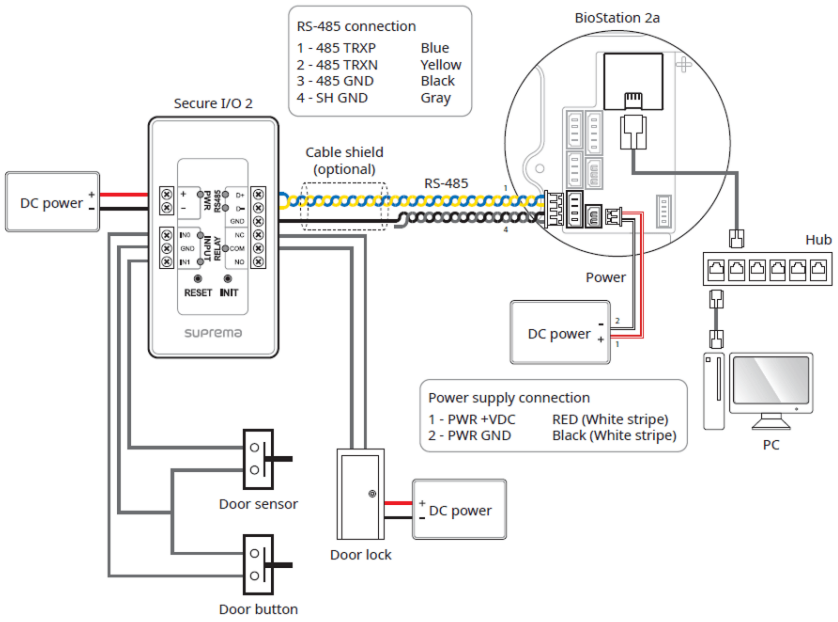
Información

- El dispositivo puede utilizarse como controlador de múltiples puertas con los dispositivos esclavos mediante el cable RS-485. Los dispositivos esclavos se utilizan como lectores ficticios y la autenticación se realiza en el dispositivo maestro.
- Si se conecta XPass o XPass 2 al dispositivo maestro, solo se puede usar la autenticación con tarjeta.
- El número máximo de dispositivos esclavos que se pueden conectar varía según el método de autenticación, el número de usuarios y el número de dispositivos. Ten en cuenta también que la cantidad de dispositivos esclavos afecta el rendimiento de autenticación.
- Conecte hasta 31 dispositivos esclavos a un dispositivo maestro. El ancho de banda de RS-485 permite conectar hasta 7 dispositivos de autenticación por huella.
- Para más información, comuníquese con el Equipo de soporte técnico de Suprema.

Conectar Secure I/O 2

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

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

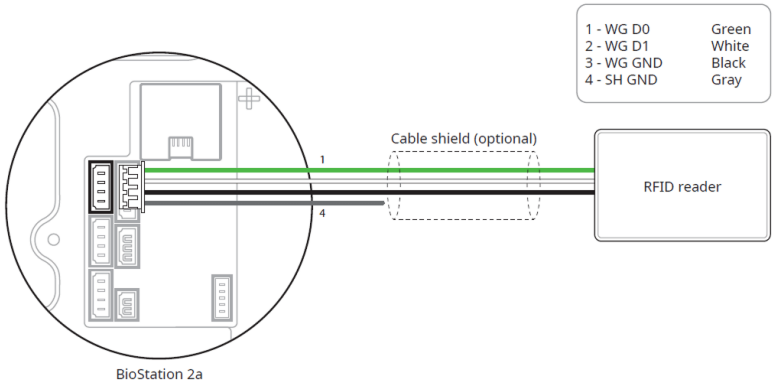


Información

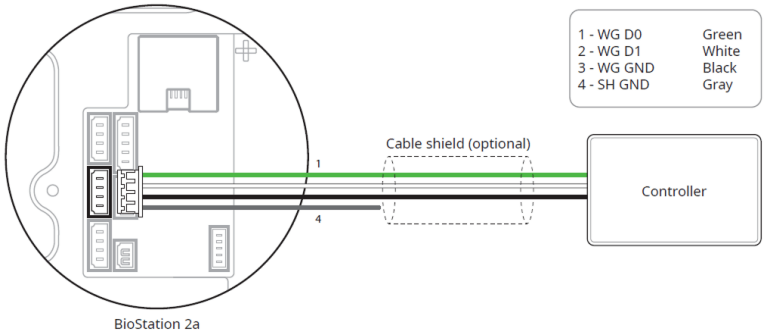
- El dispositivo puede utilizarse como controlador de múltiples puertas con los dispositivos esclavos mediante el cable RS-485. Los dispositivos esclavos se utilizan como lectores ficticios y la autenticación se realiza en el dispositivo maestro.
- Si se conecta XPass o XPass 2 al dispositivo maestro, solo se puede usar la autenticación con tarjeta.
- El número máximo de dispositivos esclavos que se pueden conectar varía según el método de autenticación, el número de usuarios y el número de dispositivos. Ten en cuenta también que la cantidad de dispositivos esclavos afecta el rendimiento de autenticación.
- Conecte hasta 31 dispositivos esclavos a un dispositivo maestro. El ancho de banda de RS-485 permite conectar hasta 7 dispositivos de autenticación por huella.
- Para más información, comuníquese con el Equipo de soporte técnico de Suprema.

Conexión Wiegand

Se usa como dispositivo de entrada Wiegand.



Se usa como dispositivo de salida Wiegand.



Cómo Usar

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

Menú de Administrador

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

Menú completo

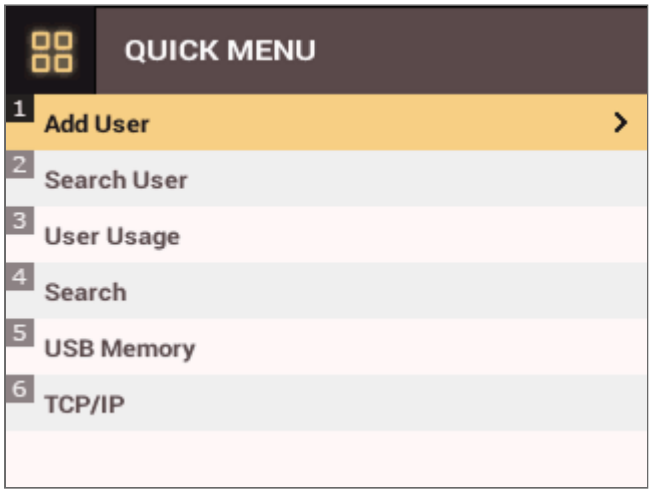
1. Presione ☰ y autentíquese con la credencial de administrador.
2. Selecciona el menú deseado.



> **Información**
>
> Si no hay un administrador designado, al presionar ☰ se mostrará la pantalla de menú.

Menú rápido

1. Mantén presionado ☰ por más de 1 segundo y luego suéltalo. Autentica usando el método de privilegio de administrador.
2. Selecciona el menú deseado.

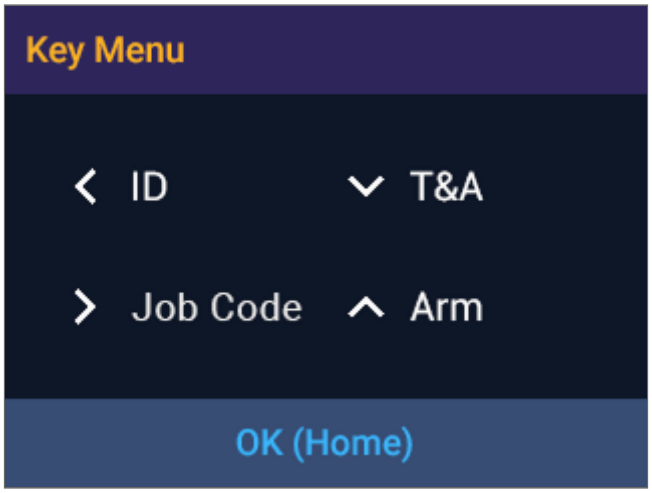


Información

Si no hay un administrador designado, al mantener presionado ☰ aparecerá la pantalla de menú rápido.

Menú de teclas

Presiona el botón **OK** para mostrar la pantalla del menú de teclas. Ingresa presionando **Key Menu** o el botón direccional correspondiente al menú deseado en la pantalla de inicio.



- **ID**: La autenticación de ID se puede realizar según lo establecido en **ID**.
- **T&A**: Selecciona un evento T&A para autenticar.
- **Job Code**: Puedes seleccionar el código laboral del usuario.
- **Arm**: Inicia o detén la seguridad.

Información

Si está en el estado **Arm**, no se puede ingresar a **Key Menu**. Desactiva la seguridad presionando el botón ^ en la pantalla de inicio.

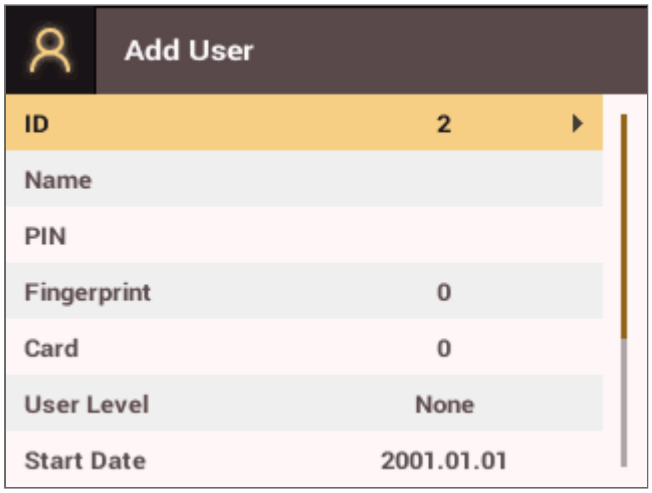
Usuario

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 administrador.
2. Seleccione **USER** → **Add User** y luego presione **OK**.



3. Seleccione el elemento deseado y presione el botón ›. Después de configurar el elemento, presione **OK** para registrar la información de usuario.
   - **ID**: Ingrese un número entre 1 y 4294967295 para registrar un ID de usuario. Si **User ID Type** está configurado en **Alphanumeric**, puede usar una combinación de caracteres alfanuméricos y los símbolos `_` `-` como ID, con un máximo de 32 caracteres.
   - **Name**: Ingrese el nombre de usuario usando los botones numéricos. Presione los botones ^ / v para seleccionar letras o números y presione **F1/F2** para ver más caracteres.
   - **PIN**: Ingrese el PIN que desea usar. Ingrese el PIN y presione **OK**. Para confirmar, ingrese el PIN nuevamente y presione **OK**. Para evitar filtraciones, ingrese un PIN de 4 a 16 dígitos.

     > **Información**
     > Al usar la función **Master Admin**, ingrese un número de al menos 8 dígitos.

   - **Fingerprint**: Inscriba una huella digital para la autenticación del usuario. Después de escanear la huella digital del dedo que se va a inscribir, vuelva a escanear la huella del mismo dedo.
   - **Card**: Inscriba una tarjeta para la autenticación del usuario. Escanee la tarjeta que desea asignar al usuario.
   - **User Level**: Seleccione los permisos que desea asignar al usuario.

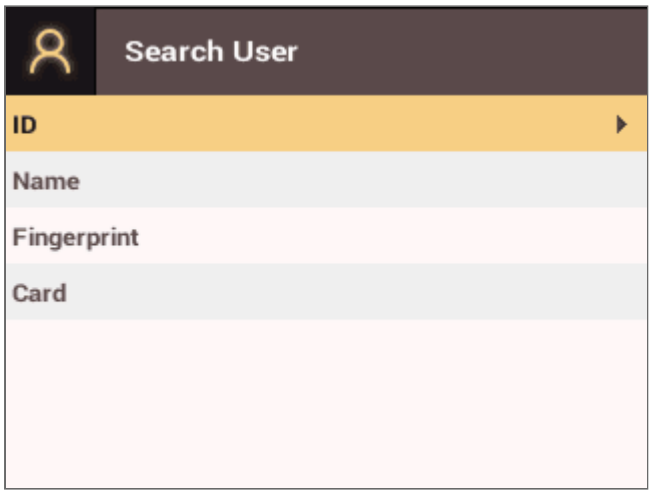
> **Información**
>
> Los menús disponibles varían según el nivel de usuario establecido.
>
> – **None**: Este es un nivel de usuario general y el menú no está disponible.
> – **Administrator**: Puede usar todos los menús.
> – **Configuration**: Puede usar los menús **AUTHENTICATION**, **DISPLAY & SOUND**,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

- **Start Date**: Configure la fecha de inicio de uso de la cuenta de usuario. Presione los botones numéricos para ingresar la fecha. Utilice el botón ‹ para eliminar la fecha ingresada y el botón › para insertar un separador.
- **Expiration Date**: Configure la fecha de finalización de uso de la cuenta de usuario. Presione los botones numéricos para ingresar la fecha. Utilice el botón ‹ para eliminar la fecha ingresada y el botón › para insertar un separador.
- **Security Level**: Configure el nivel de seguridad para la autenticación 1:1.
- **Duress**: Seleccione para inscribir una huella de coacción. Si alguien lo coacciona o necesita abrir la puerta por la fuerza, autenticar con esta huella enviará una señal de alarma a BioStar X.
- **Private Auth Mode**: Puede cambiar el método de autenticación para cada usuario. Seleccione el elemento deseado y cambie el ajuste con los botones ‹ / ›.

Modificar información de usuario

El administrador de usuarios o el superadministrador puede modificar la información de usuario registrada. Agregue la huella digital o la tarjeta del usuario y modifique el PIN y los permisos.

1. Presione ☰ y autentíquese con la credencial de administrador.
2. Seleccione **USER** → **Search User** y luego presione **OK**.



3. Seleccione el método de búsqueda que desea usar y presione el botón ›. Busque usuarios con **ID**, **Name**, **Fingerprint**, **Card**.
   - Si presiona **OK** sin seleccionar un método de búsqueda, aparecerá la lista completa de usuarios.
4. Seleccione el usuario que desea modificar y presione **F2**. Consulte Registrar información de usuario para modificar la

información.

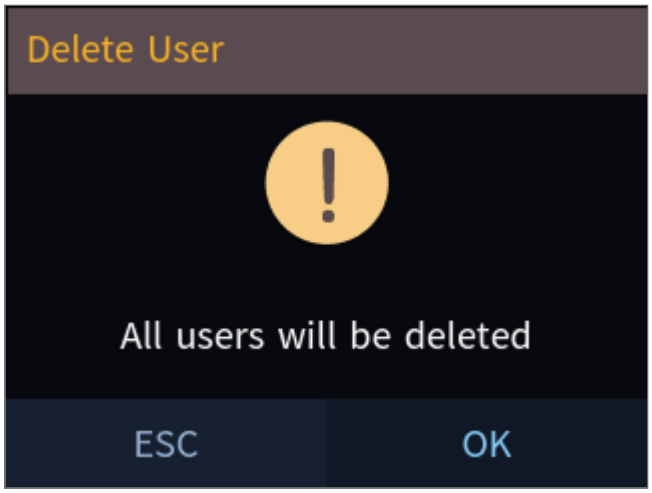
- Para eliminar un usuario, presione **F3** y luego **OK**.

> **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 administrador.
2. Seleccione **USER** → **Delete User** y luego presione **OK**.

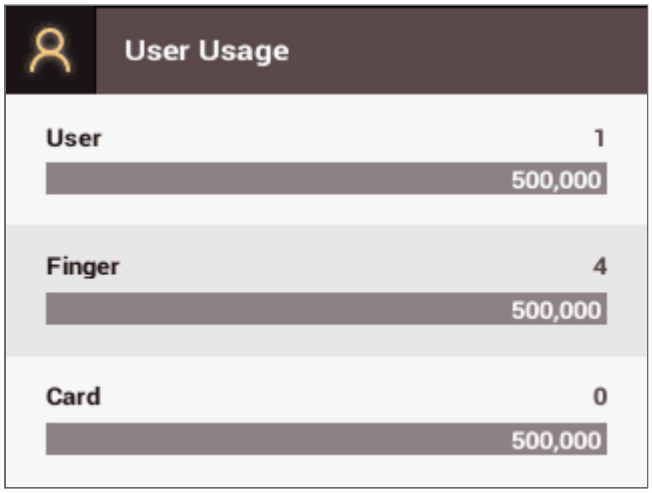


3. Presione **OK** para eliminar a todos los usuarios. Presione **ESC** para regresar a la pantalla anterior.

Ver uso de usuarios

Vea de un vistazo la cantidad de usuarios, huellas digitales y tarjetas inscritas.

1. Presione ☰ y autentíquese con la credencial de administrador.
2. Seleccione **USER** → **User Usage** y luego presione **OK**. La información de uso de usuarios aparece.



Autenticación

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

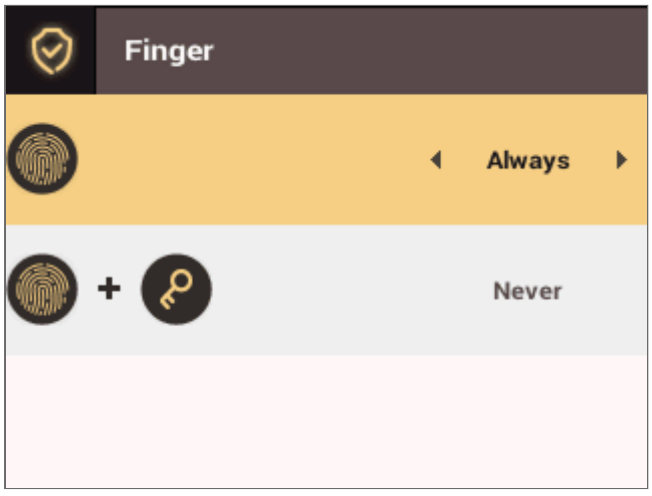
Modo de autenticación

Configura el modo de autenticación. Combina **Fingerprint**, **PIN**, **Card** y **ID** para el modo de autenticación y establece horarios para cada modo de autenticación.

Modo de autenticación por huella

Define horarios para cada método de autenticación que use huellas.

1. Presione ☰ y autentíquese con la credencial de administrador.
2. Seleccione **AUTHENTICATION** → **Auth Mode** → **Finger** y luego presione **OK**.



3. Seleccione el elemento deseado y presione < / > para establecer la programación.
   - : Modo que utiliza únicamente huellas dactilares.
   - + : Modo que autentica mediante huellas dactilares seguido del ingreso de PIN.

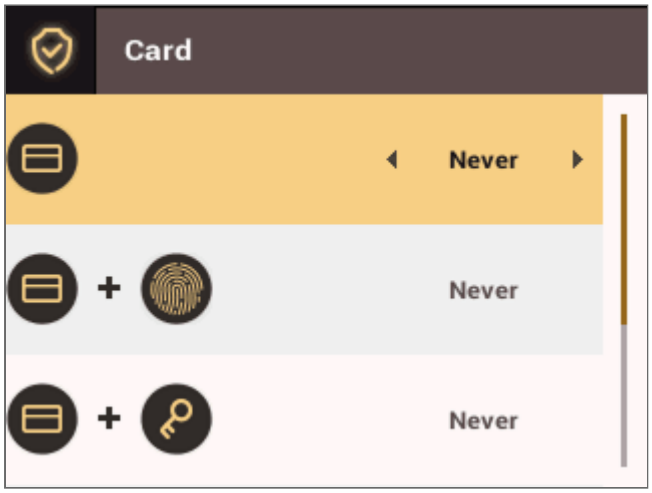
4. Pulsa **OK** para guardar la configuración.

> **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.

Modo de autenticación por tarjeta

Define horarios para cada método de autenticación que use tarjetas.

1. Presione ☰ y autentíquese con la credencial de administrador.
2. Seleccione **AUTHENTICATION** → **Auth Mode** → **Card** y luego presione **OK**.



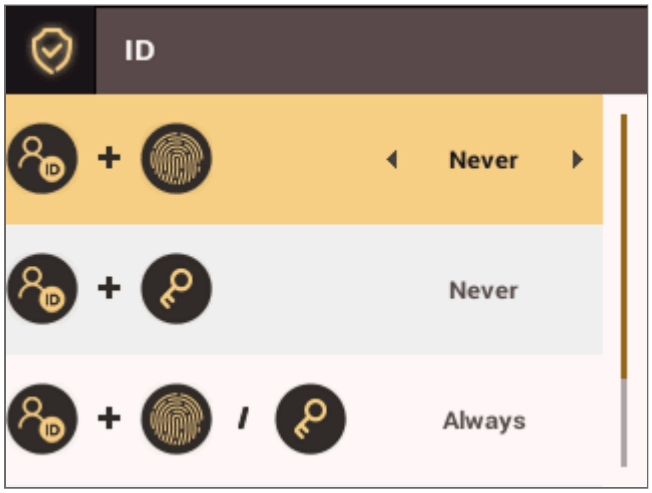
3. Seleccione el elemento deseado y presione < / > para establecer la programación.
   - : Modo que utiliza únicamente tarjetas.
   - + : Modo que autentica mediante tarjetas y luego huellas dactilares.
   - + : Modo que autentica mediante tarjetas y luego ingreso de PIN.
   - + / : Modo que autentica mediante tarjetas y luego huellas dactilares o ingreso de PIN.
   - + + : Modo que utiliza tanto la autenticación de huella dactilar como la entrada de PIN después de usar una tarjeta.
4. Pulsa **OK** para guardar la configuración.

> **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.

Modo de autenticación por ID

Define horarios para cada método de autenticación que use ID.

1. Presione ☰ y autentíquese con la credencial de administrador.
2. Seleccione **AUTHENTICATION** → **Auth Mode** → **ID** y luego presione **OK**.



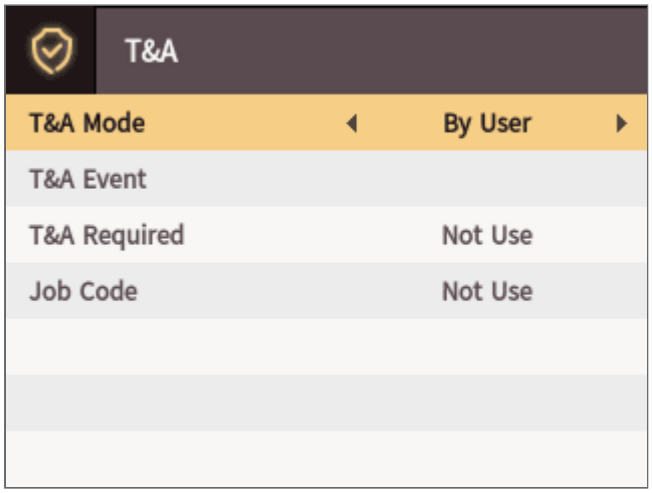
3. Seleccione el elemento deseado y presione < / > para establecer la programación.
   - + : Modo que autentica mediante ID y luego huellas dactilares.
   - + : Modo que autentica mediante ID y luego ingreso de PIN.
   - + / : Modo que autentica mediante ID y luego huellas dactilares o ingreso de PIN.
   - + + : Modo que utiliza tanto la autenticación de ID como la entrada de PIN después de usar una huella dactilar.
4. Pulsa **OK** para guardar la configuración.

> **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.

Modo de asistencia

Configura cómo registrar el modo T&A.

1. Presione ☰ y autentíquese con la credencial de administrador.
2. Seleccione **AUTHENTICATION** → **T&A**, y luego haga clic en **OK**.

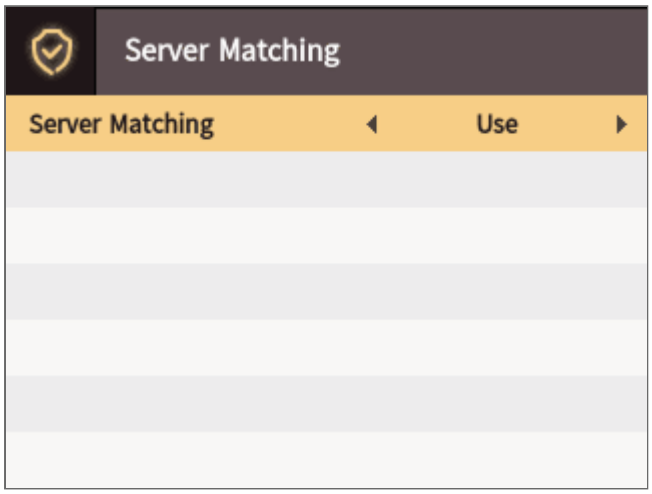


3. Seleccione el elemento deseado y presione < / > para cambiar la configuración.
   - **T&A Mode**: Configura cómo usar el modo de asistencia.
   - **T&A Event**: Permite revisar los eventos de asistencia.
   - **T&A Required**: Configure para que el usuario tenga que seleccionar un evento de T&A al autenticarse.
   - **Job Code**: Configure si se usará el código de puesto.
4. Pulsa **OK** para guardar la configuración.

Autenticación en servidor

Configura la autenticación en servidor. Cuando se utiliza la autenticación en servidor, la autenticación se realiza en BioStar X sin autenticación en el dispositivo. Se puede usar cuando el dispositivo tiene demasiada información de usuarios o cuando el dispositivo está instalado en exteriores.

1. Presione ☰ y autentíquese con la credencial de administrador.
2. Seleccione **AUTHENTICATION** → **Server Matching** y luego presione **OK**.



3. Presione < / > para cambiar la configuración.
4. Pulsa **OK** para guardar la configuración.

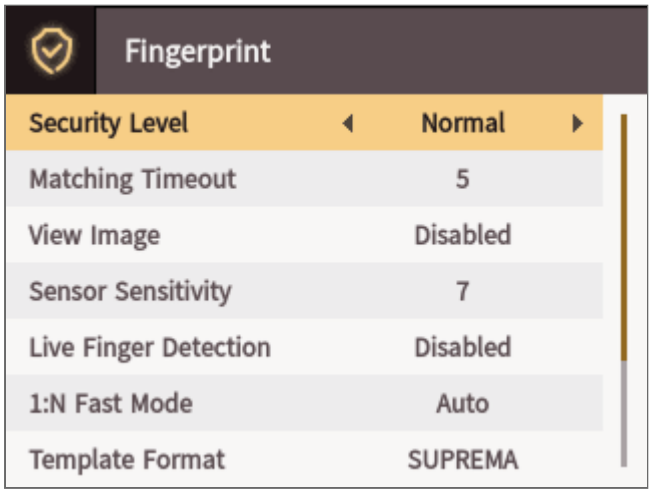
Información

- Solo puede usar **Server Matching** con **Fingerprint**, **Card** y **ID**.
- Si usa **Server Matching**, debe activar la coincidencia de servidor tanto en el dispositivo como en BioStar X. Para obtener información detallada sobre la configuración de coincidencia de servidor en BioStar X, consulte la Guía del administrador de BioStar X.

Ajustes de huella

Cambia los ajustes de autenticación por huella digital.

1. Presione ☰ y autentíquese con la credencial de administrador.
2. Seleccione **AUTHENTICATION** → **Fingerprint** y luego presione **OK**.



3. Seleccione el elemento deseado y presione < / > para cambiar la configuración.
   - **Security Level**: Configura el nivel de seguridad para la autenticación 1:N.
   - **Matching Timeout**: Configura el tiempo de espera para la correspondencia de huellas. Si la autenticación no se completa dentro del tiempo especificado, fallará.
   - **View Image**: Se puede ver la imagen original de la huella escaneada.
   - **Sensor Sensitivity**: Configura la sensibilidad del sensor de reconocimiento de huellas. Establece la sensibilidad más alta para obtener información de huella dactilar precisa.
   - **Live Finger Detection**: Configura el nivel de detección de huellas falsas. Niveles más altos de detección de huellas falsas pueden aumentar las tasas de rechazo de las huellas reales.
   - **1:N Fast Mode**: Configura la velocidad de la autenticación por huella. Al seleccionar **Auto**, la velocidad de autenticación se ajusta según el total de plantillas de huellas almacenadas en el dispositivo.
   - **Template Format**: Configura el formato de plantilla de huella. **SUPREMA** está configurado por defecto. Al cambiar el formato de la plantilla, las huellas digitales guardadas anteriormente quedarán inutilizables, así que tenga cuidado al modificarlo.

> **Información**
> Elimina toda la información de huellas dactilares de los usuarios y luego cambia el formato de la plantilla. Si hay información de huellas dactilares registrada, no es posible cambiar el formato de la plantilla.

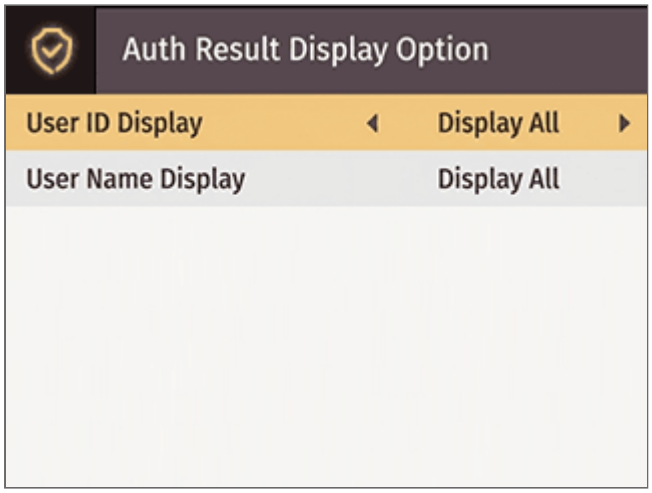
- **Sensor Mode**: Configura en **Auto On** para encender el sensor de huella cuando detecte el dedo del usuario. Al configurarse en **Always On**, el sensor permanece encendido aunque no se estén escaneando huellas.
- **Advanced Enrollment**: Evalúa la calidad de las huellas escaneadas para guardar información de alta calidad. Habilite la notificación para avisar al usuario cuando la calidad de la huella digital sea baja, ayudándole a escanearla correctamente.
- **Duplicate Check**: Verifica huellas duplicadas durante el enrolamiento.

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

Opciones de visualización del resultado de autenticación

Configura la opción de visualización del resultado de autenticación.

1. Presione ☰ y autentíquese con la credencial de administrador.
2. Seleccione **AUTHENTICATION** → **Auth Result Display Option** y presione **Aceptar**.



3. Seleccione el elemento deseado y presione < / > para cambiar la configuración.
   - **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.

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

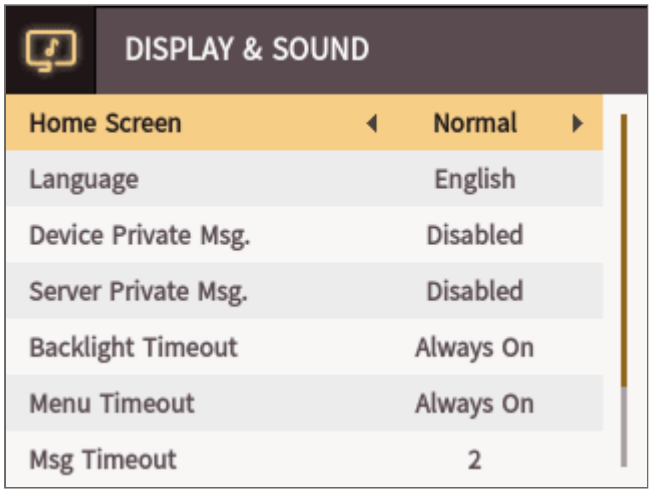
Ajustes

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 administrador.
2. Seleccione **DISPLAY & SOUND** y luego presione **OK**.



3. Seleccione el elemento deseado y presione < / > para cambiar la configuración.

   - **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.
   - **Backlight Timeout**: Configure el tiempo (s) para apagar la iluminación de la pantalla.
   - **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.
   - **Msg Timeout**: Configure el tiempo (s) para que un mensaje de configuración completada o de notificación desaparezca automáticamente.
   - **Voice Instruction**: Permite usar guía por voz en lugar de tonos de notificación.

- **Volume**: Configure el volumen.

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

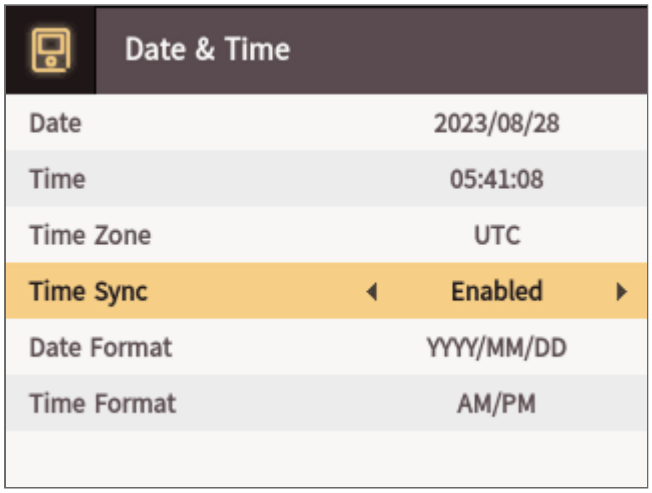
> **Información**
> Para obtener más información sobre el SDK de dispositivos BioStar, consulte la página del SDK de dispositivos BioStar en la base de conocimientos de Suprema.

Dispositivo

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 administrador.
2. Seleccione **DEVICE** → **Date & Time** y luego presione **OK**.



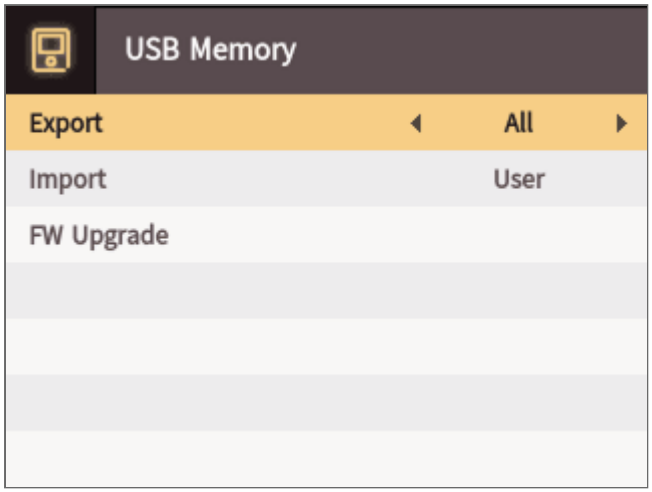
3. Seleccione el elemento deseado y presione < / > para cambiar la configuración.
   - **Date**: Verifique la fecha actual. Para modificarla manualmente, desactive **Time Sync**.
   - **Time**: Verifique la hora actual. Para modificarla manualmente, desactive **Time Sync**.
   - **Time Zone**: Ajuste 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**.
4. Pulsa **OK** para guardar la configuración.

> **Información**
> Ingrese la fecha y la hora presionando los botones numéricos. Elimine el valor ingresado con el botón < e ingrese el delimitador con el botón > .

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 administrador.
2. Seleccione **DEVICE** → **USB Memory** y luego presione **OK**.



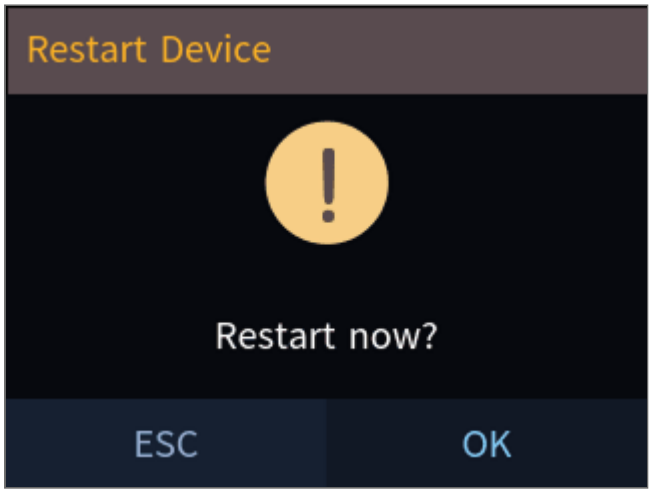
3. Seleccione el elemento deseado para continuar.
   - **Export**: Seleccione la información que desea exportar a la memoria USB conectada. Seleccione el elemento y luego presione **OK**.
   - **Import**: Importe la información de usuarios desde la memoria USB conectada. Seleccione el elemento y luego presione **OK**.
   - **FW Upgrade**: Si el archivo de firmware está guardado en la memoria USB conectada, presione **OK** para actualizar el firmware.

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

Reiniciar dispositivo

Reinicia el dispositivo.

1. Presione ☰ y autentíquese con la credencial de administrador.
2. Seleccione **DEVICE** → **Restart Device** y luego presione **OK**.

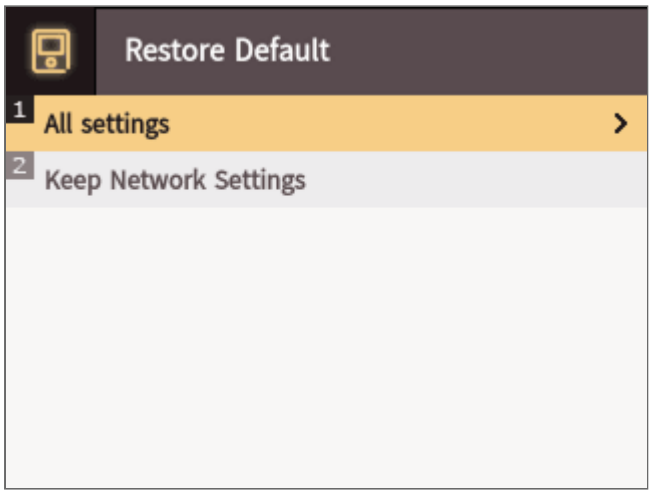


3. Presione **OK** para reiniciar el dispositivo. Presione **ESC** para regresar a la pantalla anterior.

Restablecimiento

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

1. Presione ☰ y autentíquese con la credencial de administrador.
2. Seleccione **DEVICE** → **Restore Default** y luego presione **OK**.



3. Seleccione el elemento deseado para continuar.
   - **All settings**: Inicializa todos los ajustes almacenados en el dispositivo. Presione **OK** para inicializar todas las configuraciones del dispositivo. Presione **ESC** para regresar a la pantalla anterior.
   - **Keep Network Settings**: Inicializa todos los ajustes excepto los de red. Presione **OK** para inicializar todas las configuraciones excepto las de red. Presione **ESC** 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.
4. La ejecución de **Restore Default** reinicia el dispositivo.

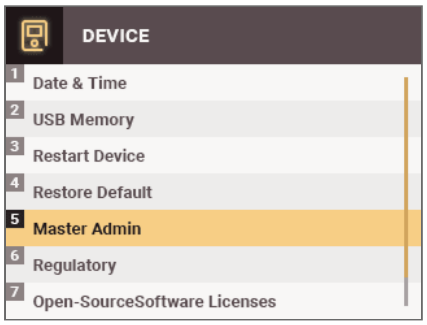
Información

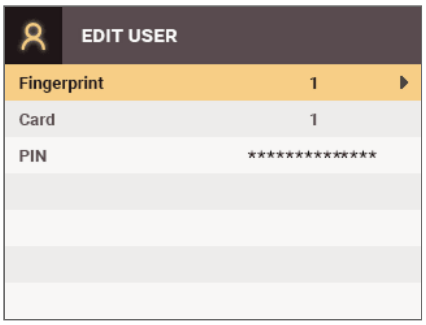
- Al restablecer, el nivel de operador también se restablecerá. Después de restablecer, vuelve a configurar el nivel de operador.
- El ajuste de idioma no cambiará después de restablecer.
- El menú **Factory Default** puede utilizarse cuando el certificado raíz está guardado en el dispositivo.
- El menú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

Administrador maestro Productos orientados a CE

Cambie el método de autenticación del administrador maestro.

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





Información

- Debe enrolar al menos dos tipos de credenciales.
- Esta función está disponible solo en dispositivos nuevos con firmware v1.2.0 o superior.

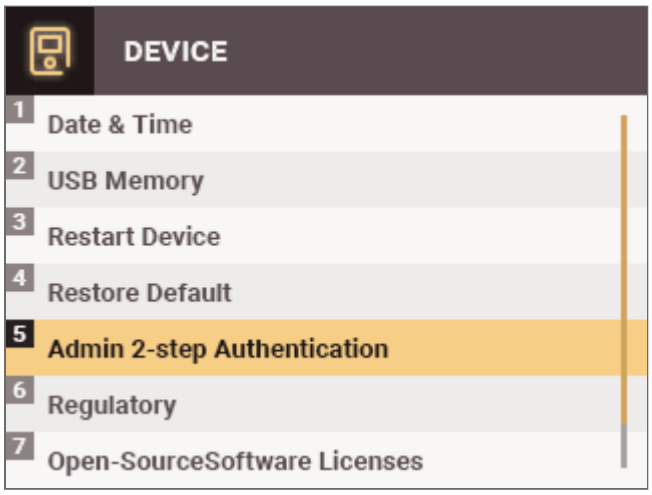
Autenticación de dos factores del administrador Productos orientados a CE

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 administrador.
2. Seleccione **DEVICE** → **Admin 2-step Authentication**.

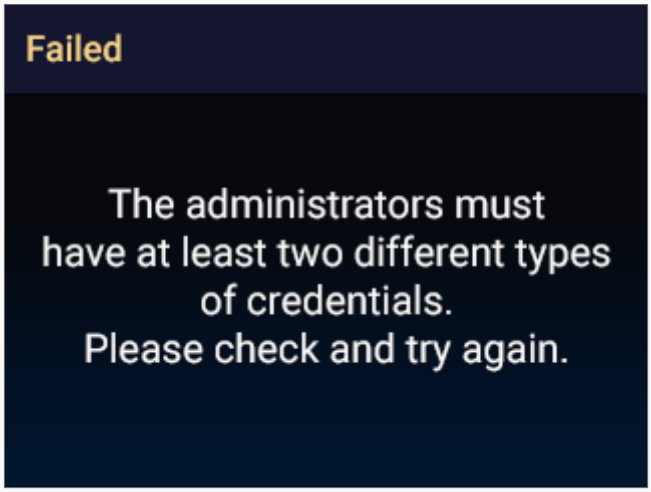


Información

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

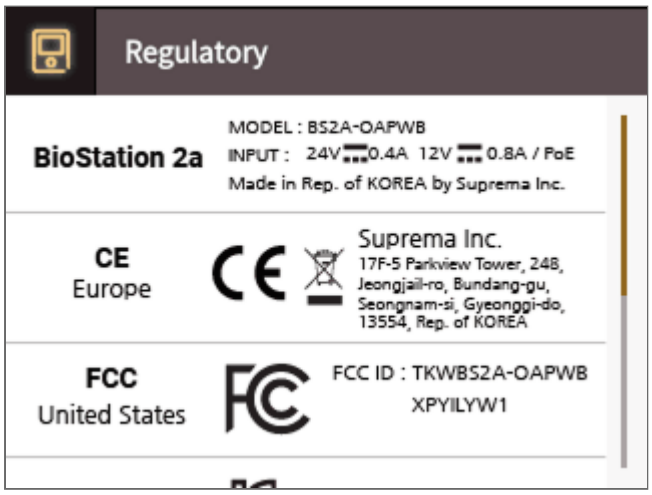
Si activa **Admin 2-step Authentication** y elimina las credenciales de todos los administradores hasta dejar menos de dos tipos, no podrá acceder al menú de administrador cuando BioStar X o BioStar 2 no estén disponibles. Por lo tanto, tenga especial cuidado al eliminar credenciales de administrador.

Normativa

Verifique las certificaciones reglamentarias y las marcas de cumplimiento en el producto.

- CE / FCC / KC / UKCA / RCM

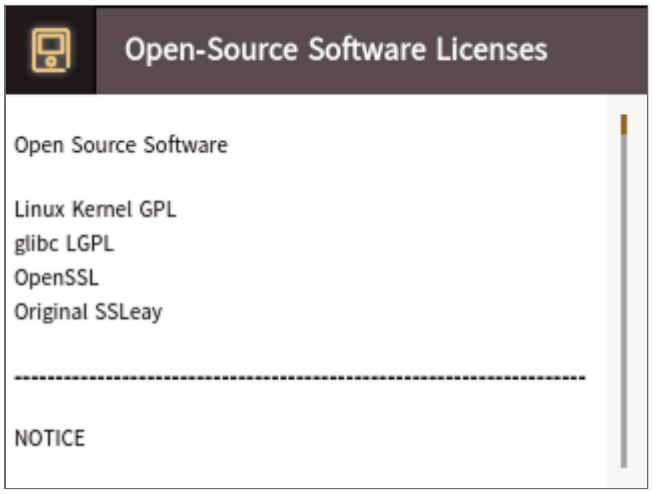
1. Presione ☰ y autentíquese con la credencial de administrador.
2. Seleccione **DEVICE** → **Regulatory** y luego presione **OK**. Verifique las certificaciones reglamentarias.



Licencia de software de código abierto

Verifique la licencia en el producto.

1. Presione ☰ y autentíquese con la credencial de administrador.
2. Seleccione **DEVICE** → **Open-Source Software Licenses** y luego presione **OK**. Verifique la licencia.

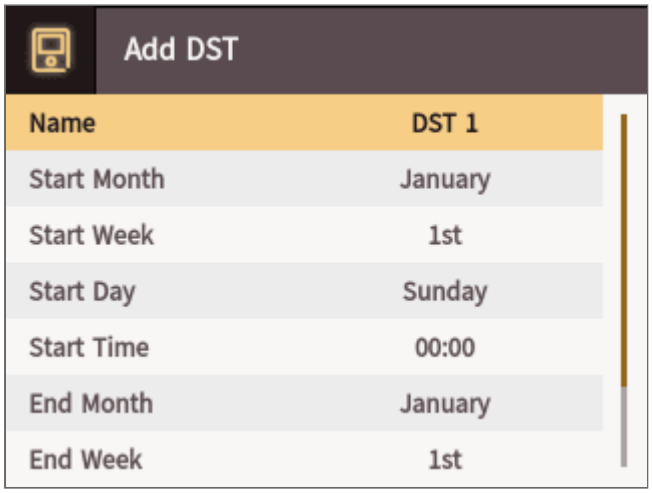


Otras configuraciones

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 administrador.
2. Seleccione **DEVICE** → **More Settings** → **Daylight Saving Time** y luego presione **OK**.
3. Seleccione **Add DST** y luego presione **OK**.

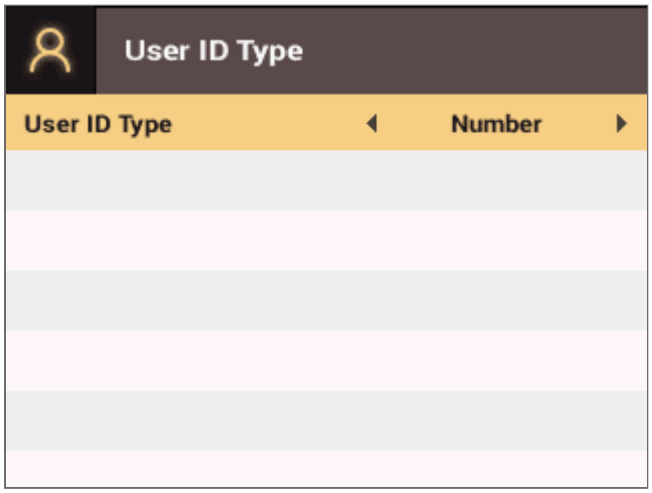


4. Seleccione el elemento deseado y presione < / > para cambiar la configuración.
   - **Name**: Establece el nombre del horario de verano.
   - **Start Month** / **Start Week** / **Start Day** / **Start Time**: Configure los detalles sobre cuándo comienza el horario de verano.
   - **End Month** / **End Week** / **End Day** / **End Time**: Configure los detalles sobre cuándo termina el horario de verano.
5. Pulsa **OK** para guardar la configuración.

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 administrador.
2. Seleccione **DEVICE** → **More Settings** → **User ID Type** y luego presione **OK**.

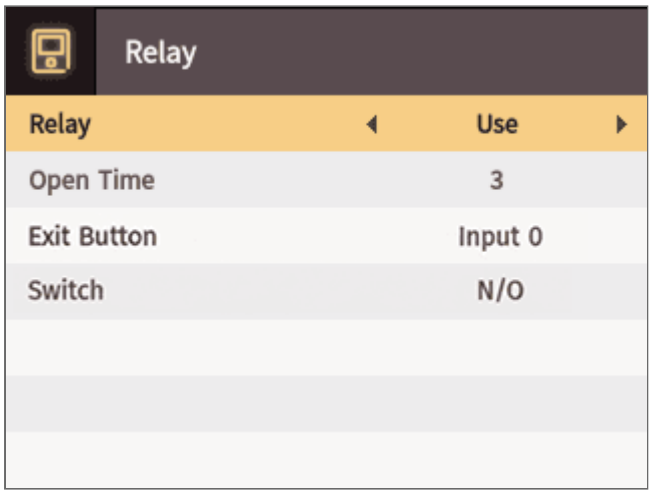


3. Presione < / > para cambiar la configuración.
   - **Number**: Ingrese un ID de usuario con solo números.
   - **Alphanumeric**: Ingrese un ID de usuario con caracteres alfanuméricos y los símbolos _ -.
4. Pulsa **OK** para guardar la configuración.

Relé

Configure los puertos de entrada de **Open Time** y **Exit Button** en el dispositivo. Útil cuando se utiliza como dispositivo independiente.

1. Presione ☰ y autentíquese con la credencial de administrador.
2. Seleccione **DEVICE** → **More Settings** → **Relay** y luego presione **OK**.



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

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 administrador.
2. Seleccione **DEVICE** → **More Settings** → **Secure Tamper** y luego presione **OK**.

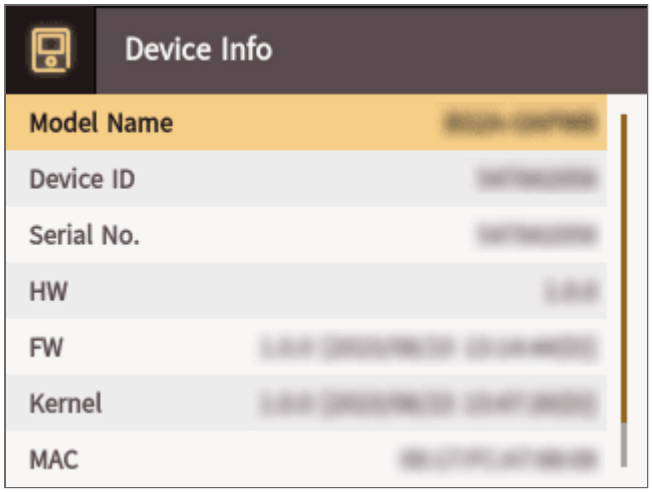


3. Para configurarlo para que elimine todos los usuarios, registros y claves seguras cuando ocurra un evento de sabotaje, presione < / > y establezca **Enabled**.
4. Pulsa **OK** para guardar la configuración.

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 administrador.
2. Seleccione **DEVICE** → **More Settings** → **Device Info** y luego presione **OK**. Vea la información de **Model Name**, **Device ID**, **Serial No.**, **HW**, **FW**, **Kernel**, **MAC** y **WiFi MAC**.



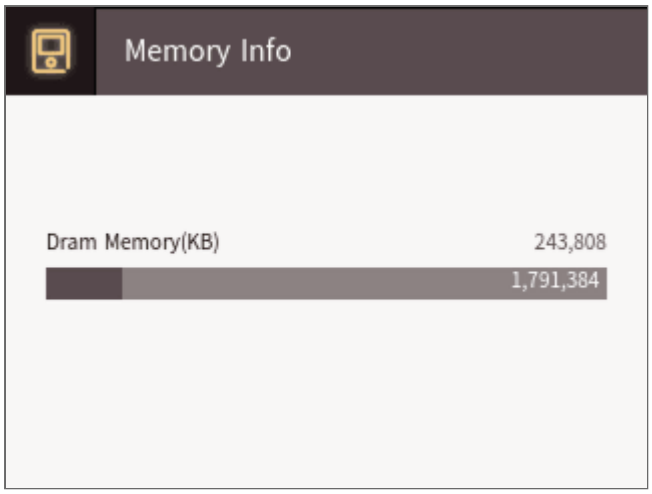
> **Información**
> **WiFi MAC** solo está disponible para el modelo BS2A-OAPWB.

Información de memoria

Consulta el estado de uso de la memoria.

1. Presione ☰ y autentíquese con la credencial de administrador.
2. Seleccione **DEVICE** → **More Settings** → **Memory Info** y luego presione **OK**. Consulta el estado de uso de memoria del

dispositivo.



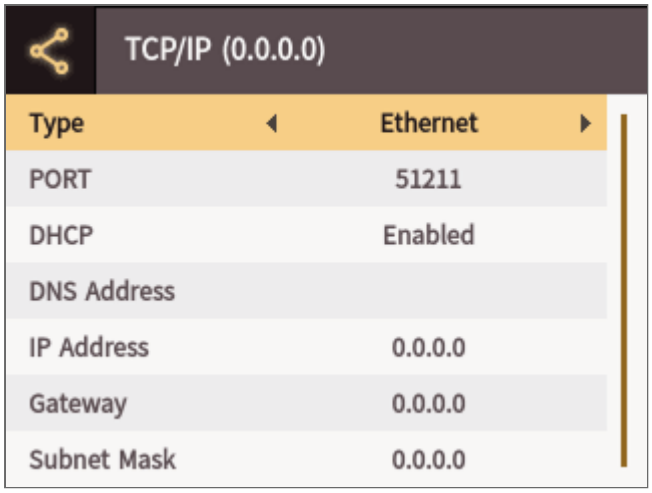
Red

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

TCP/IP

Ethernet

1. Presione ☰ y autentíquese con la credencial de administrador.
2. Seleccione **NETWORK** → **TCP/IP** y luego presione **OK**.
3. Presione ‹ / › en **Type** y seleccione **Ethernet**.



4. Cambie el elemento deseado.
   - **PORT**: Configure los puertos del dispositivo.
   - **DHCP**: Configure si se utiliza DHCP. Si la configuración DHCP está deshabilitada, se pueden modificar **IP Address**, **Gateway** y **Subnet Mask**.
   - **DNS Address**: Configure la dirección DNS.
   - **IP Address**: Compruebe la dirección IP del dispositivo. Para modificarla, desactive la configuración de DHCP.

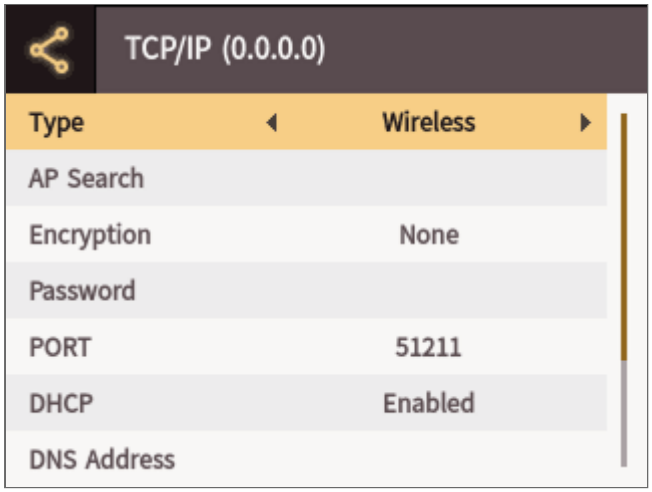
- **Gateway**: Compruebe la puerta de enlace del dispositivo. Para modificarla, desactive la configuración de DHCP.
- **Subnet Mask**: Compruebe la máscara de subred del dispositivo. Para modificarla, desactive la configuración de DHCP.

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

> **Información**
>
> - **Ethernet** no se puede usar con **Wireless**.
> - **IP Address**, **Gateway** y **Subnet Mask** se ingresan presionando los botones numéricos. Elimine el valor ingresado con el botón ‹ e ingrese el delimitador con el botón ›.

LAN inalámbrica

1. Presione ☰ y autentíquese con la credencial de administrador.
2. Seleccione **NETWORK** → **TCP/IP** y luego presione **OK**.
3. Presione ‹ / › en **Type** y seleccione **Wireless**.



4. Cambie el elemento deseado.
   - **AP Search**: Seleccione el AP al que desea conectarse.
   - **Encryption**: Se muestra el método de cifrado configurado en el AP.
   - **Password**: Ingrese la contraseña de acceso del AP.
   - **PORT**: Configure los puertos del dispositivo.
   - **DHCP**: Configure si se utiliza DHCP. Si la configuración DHCP está deshabilitada, se pueden modificar **IP Address**, **Gateway** y **Subnet Mask**.
   - **DNS Address**: Configure la dirección DNS.
   - **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

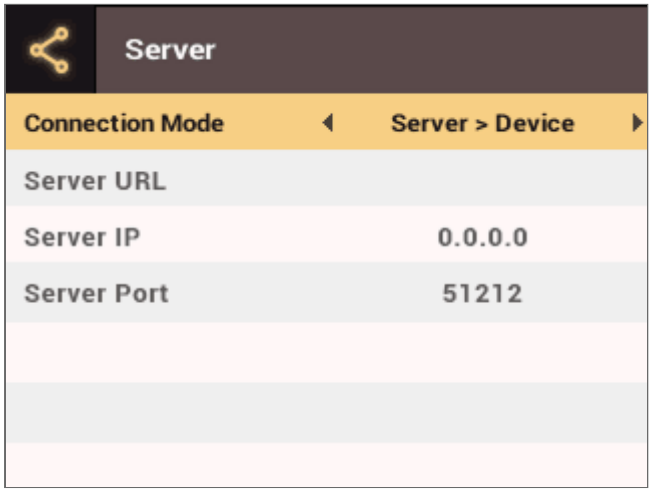
DHCP.

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

> **Información**
>
> - **Wireless** solo está disponible para el modelo BS2A-OAPWB.
> - **Wireless** no se puede usar con **Ethernet**.
> - **IP Address**, **Gateway** y **Subnet Mask** se ingresan presionando los botones numéricos. Elimine el valor ingresado con el botón < e ingrese el delimitador con el botón >.
> - 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 administrador.
2. Seleccione **NETWORK** → **Server** y luego presione **OK**.

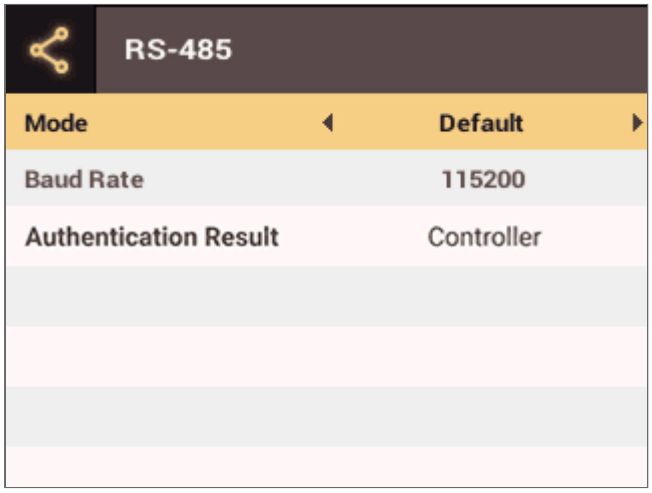


3. Presione < / > para cambiar la configuración.
   - **Connection Mode**: Al seleccionar **Device > Server**, se enviará una señal de conexión directamente a un servidor con la información ingresada desde el dispositivo. Cuando la configuración **Device > Server** está habilitada, el usuario puede ingresar **Server URL**, **Server IP**, **Server Port**.
   - **Server URL**: Ingrese **Server URL** en lugar de **Server IP**.
   - **Server IP**: Ingrese la dirección IP de la PC donde está instalado BioStar X.
   - **Server Port**: Ingrese el puerto de la PC donde está instalado BioStar X.
4. Pulsa **OK** para guardar la configuración.

> **Información**
>
> **Server IP**, **Server Port** pueden ingresarse presionando los botones numéricos. Elimine el valor ingresado con el botón < e ingrese el delimitador con el botón >.

RS-485

1. Presione ☰ y autentíquese con la credencial de administrador.
2. Seleccione **NETWORK** → **RS-485** y luego presione **OK**.



3. Seleccione el elemento deseado y presione < / > para cambiar la configuración.
   - **Mode**: Seleccione el modo de operación RS-485.
   - **Baud Rate**: Seleccione el rendimiento de comunicación deseado.
   - **Authentication Result**: Al usar **Intelligent Slave**, seleccione mostrar en pantalla los resultados de autenticación de controladores o dispositivos de terceros. Disponible cuando **Mode** está configurado en **Default** o **Slave**.
4. Pulsa **OK** para guardar la configuración.

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 administrador.
2. Seleccione **EVENT LOG** → **Search** y luego presione **OK**.

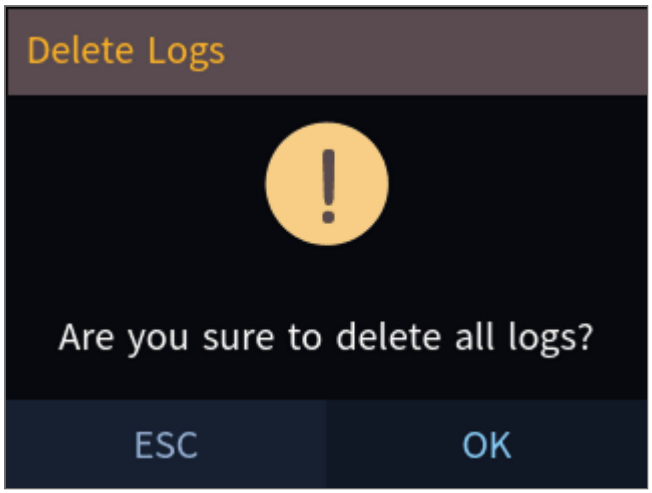


3. Seleccione el elemento deseado y presione < / > para cambiar la configuración. Al presionar **OK**, los registros que coinciden con las condiciones aparecen en la pantalla.
4. Presione **ESC** para regresar a la pantalla anterior.

Eliminar todos los registros

Elimina todos los registros guardados.

1. Presione ☰ y autentíquese con la credencial de administrador.
2. Seleccione **EVENT LOG** → **Delete All** y luego presione **OK**.

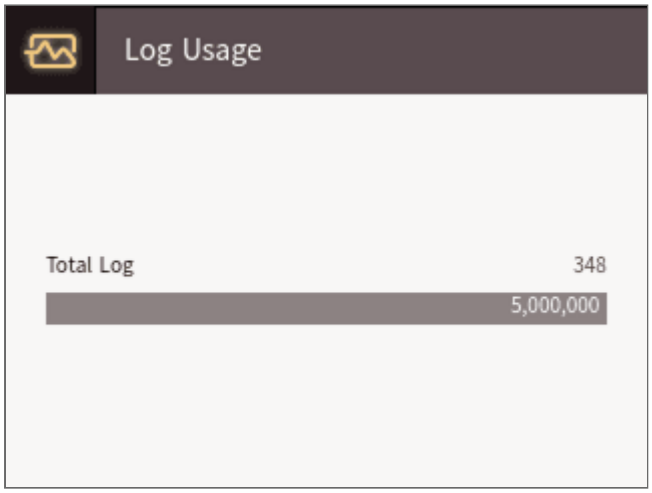


3. Pulsa **OK** para eliminar todos los registros. Presione **ESC** para regresar a la pantalla anterior.

Ver uso de registros

Consulta el estado del uso de registros.

1. Presione ☰ y autentíquese con la credencial de administrador.
2. Seleccione **EVENT LOG** → **Log Usage** y luego presione **OK**. Consulta el uso de registros del dispositivo.


Log Usage
Total Log
348
5,000,000

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.

Huella

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

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

Q. La autenticación de huella dejó de funcionar repentinamente.

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

Q. El sensor de huella no se enciende.

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

Cerradura de puerta

Q. La puerta no se bloquea al cerrarla.

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

Hora

Q. De repente, la hora es incorrecta.

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

Acceso de administrador

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

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

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	**Huella** • **Dimensiones de la imagen:272 x 320 píxeles** • **Profundidad de bits de la imagen:8 bits, 256 tonos de la escala de grises** • **Resolución:500 dpi** • **Plantilla:SUPREMA / ISO19794-2 / ANSI-378** • **Extractor / Comparador:Con certificación y compatible con MINEX** • **Detección de huella dactilar viva:Compatible (basado en software)**	
Tarjeta RF	**BS2A-ODPB**	**125kHz EM y 13.56MHz MIFARE, MIFARE Plus, DESFire, DESFire EV1/EV2/EV3, FeliCa**
	BS2A-OAPWB	**125kHz EM, HID Prox y 13.56MHz MIFARE, MIFARE Plus, DESFire, DESFire EV1/EV2/EV3, FeliCa, iCLASS SE/SR/Seos**
Rango de lectura RF[1)]	**EM/MIFARE/DESFire/HID iCLASS: 50 mm, HID Prox/FeliCa: 30 mm**	
Móvil	**NFC, BLE**	

General

Nombre del modelo	**BS2A-ODPB, BS2A-OAPWB**
CPU	**1.5 GHz Quad Core**
Memoria	**16 GB Flash + 2 GB RAM**
Chip criptográfico	**Soportado**
Visualizar	**Pantalla TFT-LCD en color de 2.8"**
Resolución de pantalla	**320 x 240 píxeles**

LED	**Multi-color**	
Sonido	**16 bit**	
Temperatura de funcionamiento	**De -20 °C a 60 °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**	
Dimensiones (W x H x D)	**Dispositivo**	**142 x 144 x 37.8 (Superior) / 45 (Inferior) (mm)**
	Soporte	**132.1 x 137.9 (mm)**
Peso	**Dispositivo**	**429 g**
	Soporte	**142 g (incluye arandelas y tornillos)**
Grado de protección IP	**IP65**	
Autenticación	**CE, UKCA, KC, FCC, RCM, SIG, RoHS, REACH, WEEE**	

Capacidad

Máx. usuarios	**500,000**[2)]
Máx. credenciales (1:N)	**Huella dactilar: 100,000**
Máx. credenciales (1:1)	• **Huella dactilar: 500,000** • **Tarjeta: 500,000** • **PIN: 500,000**
Máx. registros de texto	**5,000,000**

Interfaz

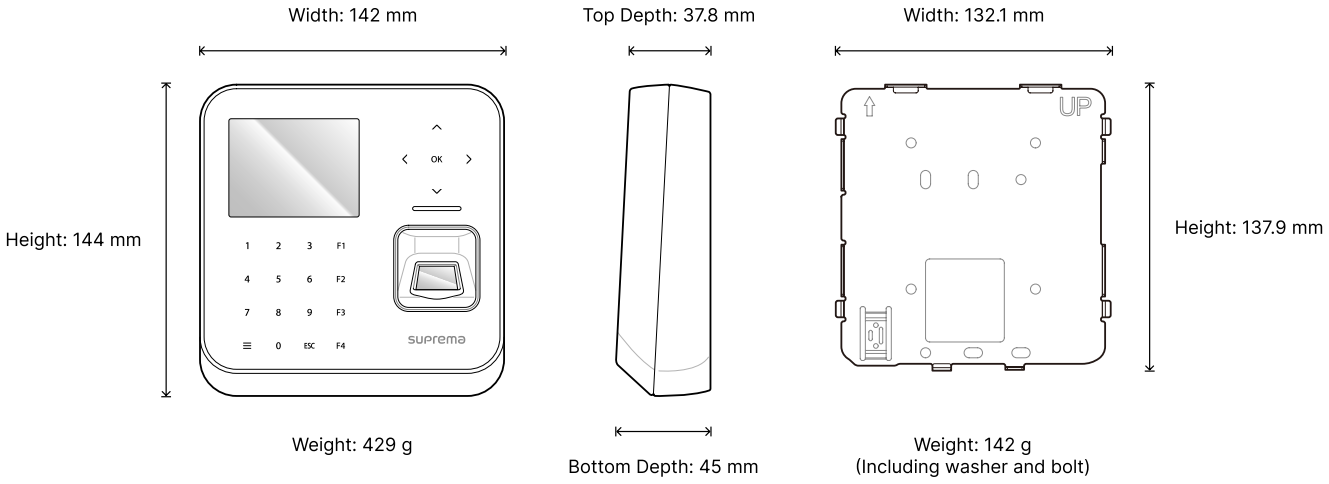
Ethernet	**Compatible (10/100 Mbps, MDI/MDI-X automática)**	
Wi-Fi	**BS2A-ODPB**	**No compatible**
	BS2A-OAPWB	**Compatible (802.11 b/g/n 2.4 GHz)**
Protocolo de red	**TCP, UDP**	
RS-485	**1 canal maestro/esclavo (seleccionable)**	
Protocolo de comunicación RS-485	**Compatible con OSDP V2**	
Wiegand	**Entrada de 1 canal, salida de 1 canal**	
Entrada	**3 canales de entrada**	
Relé	**1 relé**	
USB	**USB 2.0 (Maestro)**	
Puerto de expansión USB	**Soportado**	
PoE	**Compatible (compatible con IEEE 802.3af)**	
Tamper	**Soportado**	

Eléctrico

Alimentación	**12 Vdc**	**Corriente: Máx. 0.8 A**
	24 Vdc	**Corriente: Máx. 0.4 A**
Entrada de interruptor VIH	• **Mín.: 3 V** • **Máx.: 5 V**	

Entrada de interruptor VIL	**Máx.: 1 V**
Resistencia pull-up del interruptor	**4.7 kΩ (los puertos de entrada se polarizan con 4.7 kΩ)**
Salida Wiegand VOH	**Más de 4.8 V**
Salida Wiegand VOL	**Menos de 0.2 V**
Resistencia pull-up de salida Wiegand	**Polarización interna de 1 kΩ**
Relé	• **Carga resistiva de 2 A a 30 VCC** • **Carga inductiva de 1 A a 30 VCC**

Dimensiones y peso



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

2) Número de usuarios registrados sin datos de credenciales.

Información

Las especificaciones del producto están sujetas a cambios sin previo aviso para mejorar el rendimiento.

Información Reglamentaria

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

Información de cumplimiento de la FCC

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

El funcionamiento está sujeto a las siguientes dos condiciones:

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

Información

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

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

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

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

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.

- 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.