X-Station 2 Suprema CLUe

GUÍA DE USUARIO DE

Versión 1.01

Español
ES 102.00.XS2SC

suprema
SECURITY & BIOMETRICS

CONTENIDO

Instrucciones de Seguridad 4

Información de cumplimiento 4

Primeros Pasos 8

Componentes 8

Nombre y función de cada parte 10

Notas sobre QR/código de barras y licencia del dispositivo 15

Instalación 18

Fijar el soporte y el producto 18

Conexión de la fuente de alimentación 21

Conexión de red 22

Conexión de entrada 23

Conexión del relé 24

Conectar como independiente 27

Conectar Secure I/O 2 28

Conexión Wiegand 29

Cómo Usar 30

Menú de Administrador 30

Usuario 31

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 66

Información de cumplimiento de la FCC 66

Información de IC 67

Declaración de conformidad de la UE (CE) 67

Apéndices 68

Descargos de responsabilidad 68

Aviso de derechos de autor 69

Licencia de código abierto 69

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 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.

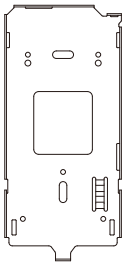
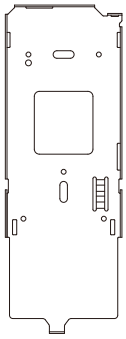
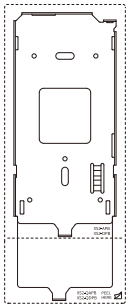
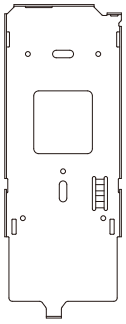
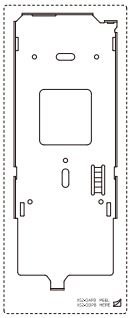
- El dispositivo puede funcionar incorrectamente.

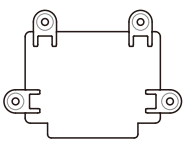
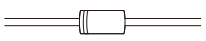
> **Batería RTC**
>
> Reemplazar por baterías no autorizadas o de tipo incorrecto puede representar un riesgo de explosión. Deseche las baterías conforme a las normativas locales o internacionales sobre residuos.

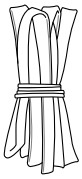
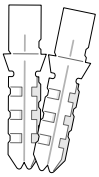
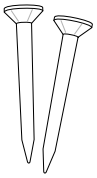
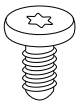
Primeros Pasos

Proporciona procedimientos iniciales para empezar con el dispositivo.

Componentes

				
X-Station 2 (XS2-DPB, XS2-APB)	Soporte de pared (XS2-QDPB, XS2-QAPB)	X-Station 2 (XS2-QDPB, XS2-QAPB)	Soporte de pared (XS2-DPB, XS2-APB)	Plantilla de perforación (XS2-DPB, XS2-APB, XS2-QDPB, XS2-QAPB)
				
X-Station 2 (XS2-ODPB, XS2-OAPB)	Soporte de pared (XS2-ODPB, XS2-OAPB)	Plantilla de perforación (XS2-ODPB, XS2-OAPB)	Guía rápida	Guía de software de código abierto

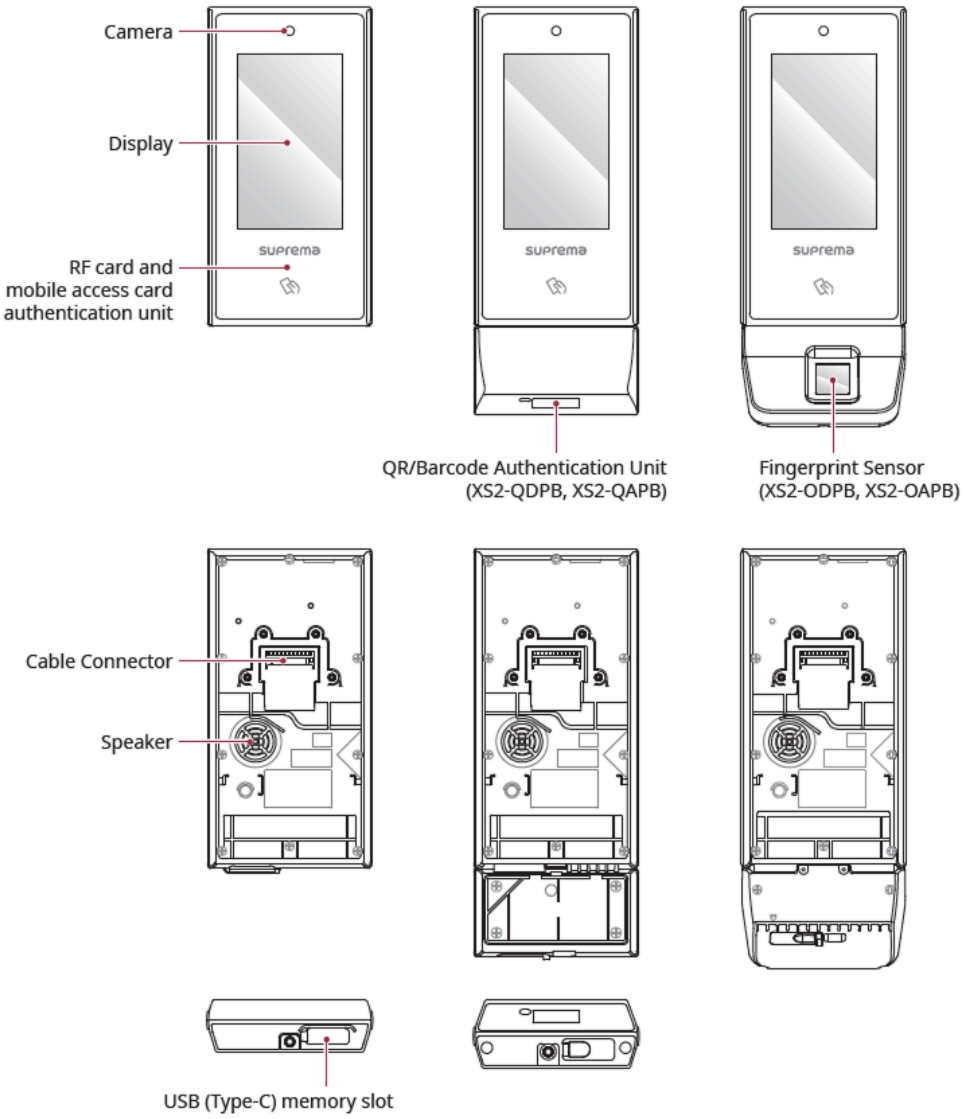
			
Cables de conexión	Cubierta de cable	Resistencia de 120 Ω	Diodo

			
Tubo termorretráctil	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.

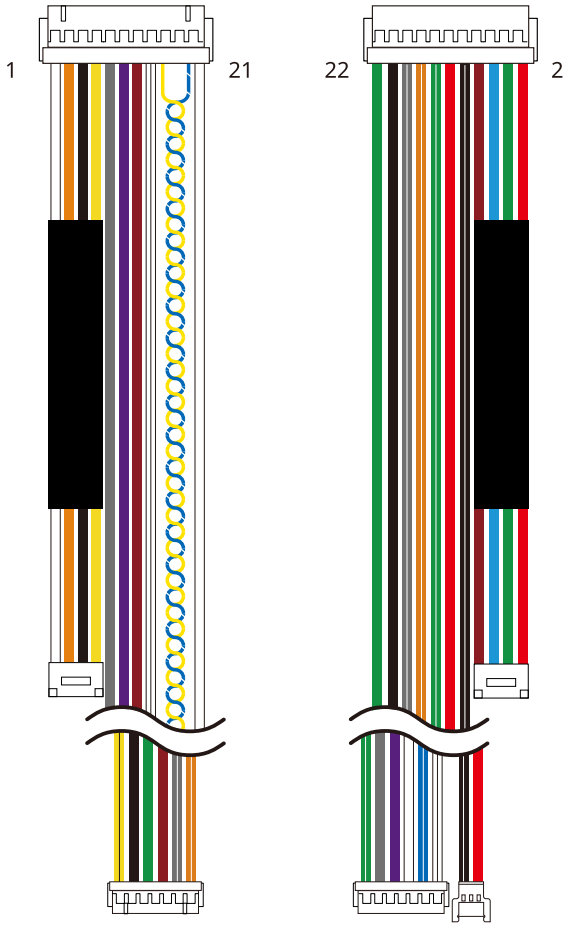
Nombre y función de cada parte



- **Cámara**: Registre su foto o deje un registro de imagen.
- **Pantalla**: Proporciona una interfaz de usuario para la operación.
- **Unidad de autenticación de tarjeta RF y tarjeta de acceso móvil**: parte para escanear una tarjeta RFID o una tarjeta de acceso móvil para la entrada.
- **Unidad de reconocimiento de QR/código de barras**: XS2-QDPB, XS2-QAPB Escanea credenciales de QR/código de barras para el acceso.
- **Unidad de reconocimiento de huellas dactilares**: XS2-ODPB, XS2-OAPB Parte que reconoce la huella dactilar para el acceso.
- **Conector de cable**: Conecta el cable.

  Alimentación / RS-485 / Ethernet + PoE / Relé / Wiegand entrada/salida / entrada
- **Altavoz**: Emite sonido.
- **Ranura para memoria USB (tipo C)**: Conecta la memoria USB.

Cables y conectores



Cable	Pin	Nombre	Color
RJ-45 (Ethernet + PoE)	1	ENET TXP	Blanco
	3	ENET TXN	Naranja
	5	ENET RXP	Negro
	7	ENET RXN	Amarillo
Entrada	9	INPUT GND	Gris
	11	INPUT0	Morado
	13	INPUT1	Marrón
RS-485	15	485 GND	Blanco (franja negra)
	17	485 TRXN	Amarillo (franja negra)
	19	485 TRXP	Azul (franja blanca)
Wiegand	21	WG D1	Blanco
	22	WG D0	Verde
	20	WG GND	Negro
Relé	18	RLY NO	Gris (franja blanca)
	16	RLY NC	Naranja (franja blanca)
	14	RLY COM	Verde (franja blanca)
Alimentación	12	PWR +VDC	Rojo

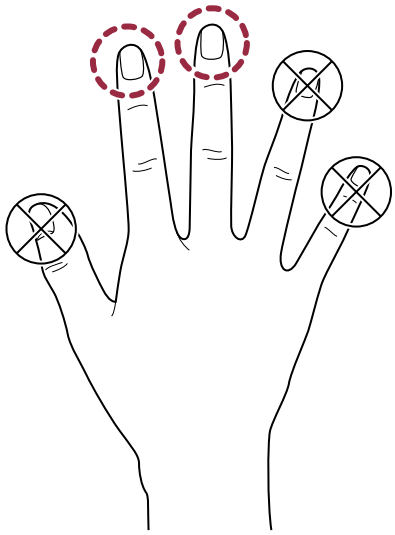
Cable	Pin	Nombre	Color
	10	PWR GND	Negro (franja blanca)
RJ-45 (Ethernet + PoE)	8	VB2	Marrón
	6	VB2	Azul
	4	VB1	Verde
	2	VB1	Rojo

Método correcto de ingreso de huellas dactilares

XS2-ODPB, XS2-OAPB

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

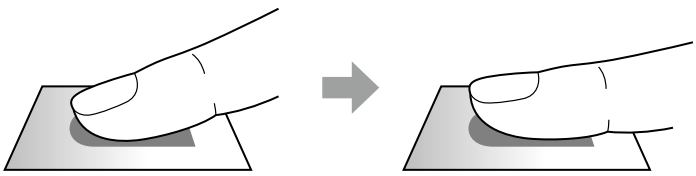
Selección de dedo para el ingreso de huella dactilar



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

Método de registro de huellas dactilares

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

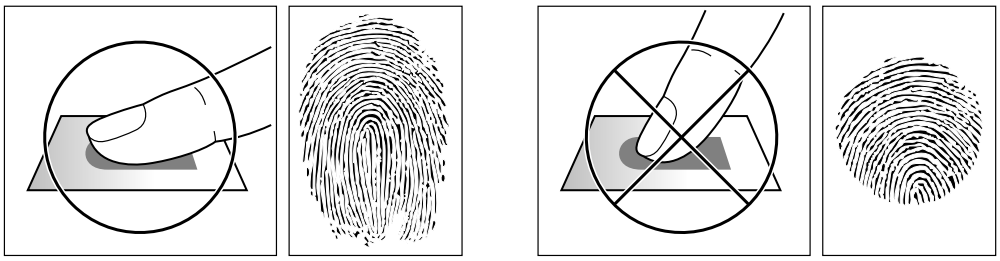


2. Cuando aparezca la pantalla de reingreso tras el beep, vuelva a escanear la huella del dedo registrado. (escanee dos

veces la huella del dedo que va a registrar)

Precauciones para el registro de huellas dactilares

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



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

Si la autenticación de huellas no funciona correctamente

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

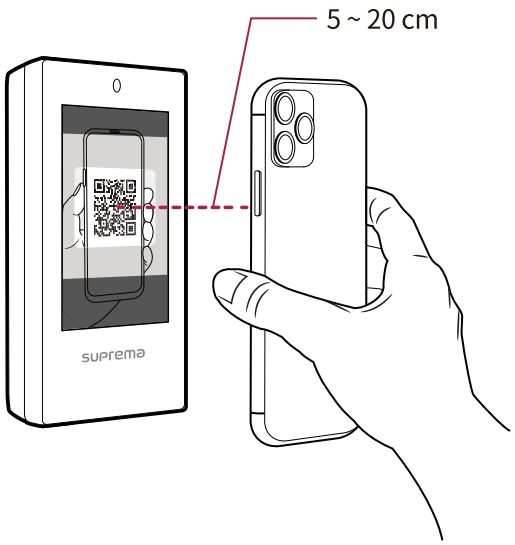
- Si el dedo está mojado o sudoroso, séquelo y luego escanee la huella.
- Si el dedo está demasiado seco, sople sobre la yema y luego escanee la huella.
- Si el dedo tiene un corte, registre la huella de otro dedo.
- Como la huella dactilar inscrita inicialmente con frecuencia no se introduce correctamente,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

Notas sobre QR/código de barras y licencia del dispositivo

Método correcto de autenticación con QR/código de barras

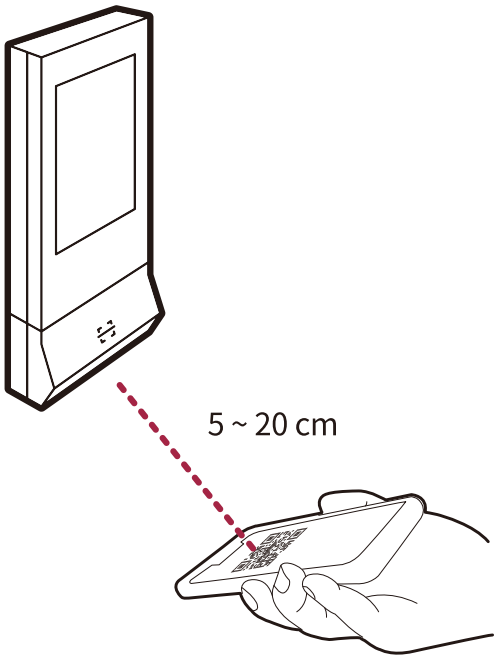
Emita un QR/código de barras al usuario para usarlo como medio de autenticación. Escanee el QR/código de barras correctamente según las indicaciones en la pantalla para mejorar la tasa de reconocimiento.

XS2-DPB, XS2-APB



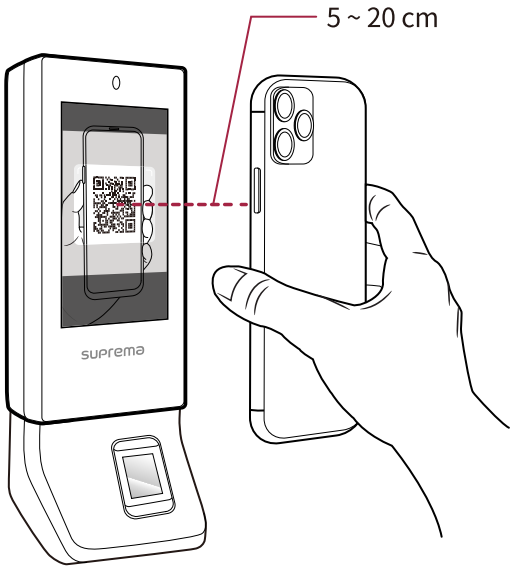
- Mantenga la distancia entre la cámara del dispositivo y el QR/código de barras a 5-20 cm.
- Coloque el QR/código de barras de modo que quede centrado en la pantalla de escaneo del dispositivo.
- Si autentica con un QR/código de barras descargado en un dispositivo móvil, ajuste el brillo del dispositivo para que la pantalla sea claramente visible.
- Si no sigue las instrucciones en la pantalla, el reconocimiento del QR/código de barras puede ser lento o fallar.

XS2-QDPB, XS2-QAPB



- Mantenga la distancia entre la unidad de reconocimiento de QR/código de barras del dispositivo y el QR/código de barras a 5-20 cm.
- Asegúrese de que la unidad de reconocimiento de QR/código de barras del dispositivo esté horizontal con respecto al QR/código de barras que se escanea y coloque el haz guía en el centro del QR/código de barras.
- Si autentica con un QR/código de barras descargado en un dispositivo móvil, ajuste el brillo del dispositivo para que la pantalla sea claramente visible.
- Si no sigue las instrucciones en la pantalla, el reconocimiento del QR/código de barras puede ser lento o fallar.

XS2-ODPB, XS2-OAPB



- Mantenga la distancia entre la cámara del dispositivo y el QR/código de barras a 5-20 cm.
- Coloque el QR/código de barras de modo que quede centrado en la pantalla de escaneo del dispositivo.

- Si autentica con un QR/código de barras descargado en un dispositivo móvil, ajuste el brillo del dispositivo para que la pantalla sea claramente visible.
- Si no sigue las instrucciones en la pantalla, el reconocimiento del QR/código de barras puede ser lento o fallar.

Notas sobre la licencia del dispositivo

- Para usar métodos de autenticación adicionales con QR/código de barras se requiere una licencia de dispositivo independiente. 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.

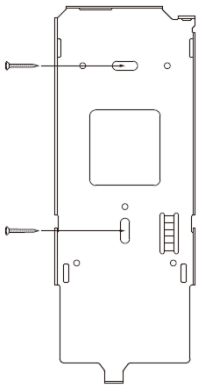
Instalación

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

Fijar el soporte y el producto

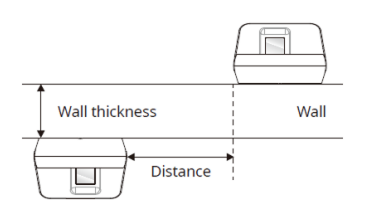
> **Información**
> Este documento explica el método de instalación basado en el factor de forma XS2-ODPB y XS2-OAPB. Instale los modelos XS2-DPB, XS2-APB, XS2-QDPB y XS2-QAPB de la misma manera.

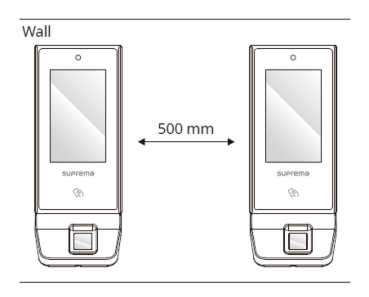
1. Determine la posición correcta para instalar el soporte usando la plantilla de perforación proporcionada. Asegura firmemente el soporte con los tornillos de fijación en el lugar donde se montará el producto.



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.

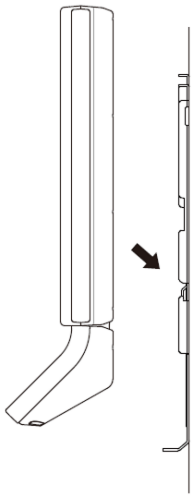




Espesor de pared	Distancia
100 mm	500 mm
120 mm	400 mm
150 mm	300 mm

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

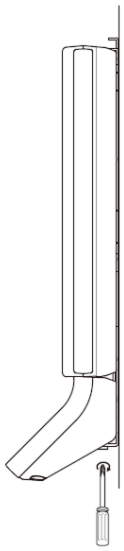
2. Después de colocar la cubierta del cable, gire los cuatro tornillos instalados en la cubierta para asegurarla firmemente y monte el producto en el soporte fijo.



Información

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

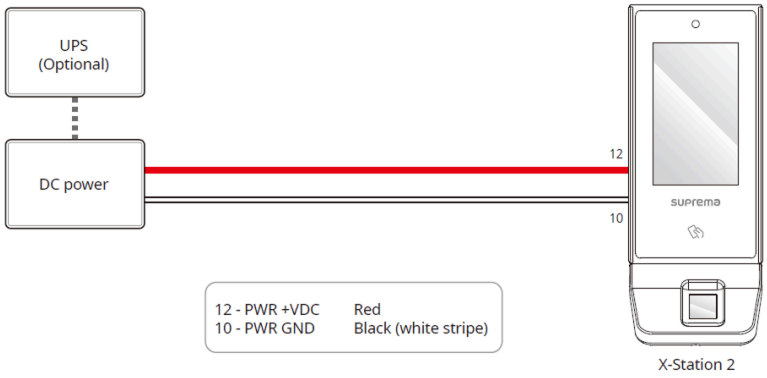
3. Gira los tornillos de fijación para ensamblar el producto con el soporte.



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

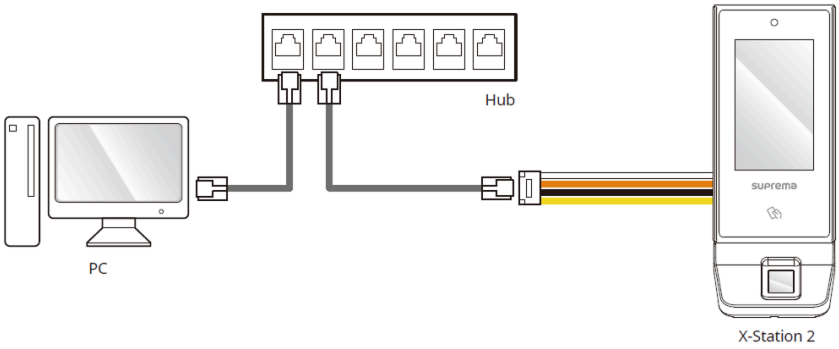
- NO conecte el dispositivo a la fuente de alimentación de CC (o adaptador) y a la alimentación PoE al mismo tiempo.
- Use un adaptador de alimentación aprobado por IEC/EN 62368-1 que admita un consumo de energía mayor que el del producto. Si desea conectar y usar otro dispositivo al adaptador de alimentación, 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.
- NO utilice CAT5 UTP de 2 hilos para la alimentación.

Conexión de red

TCP/IP

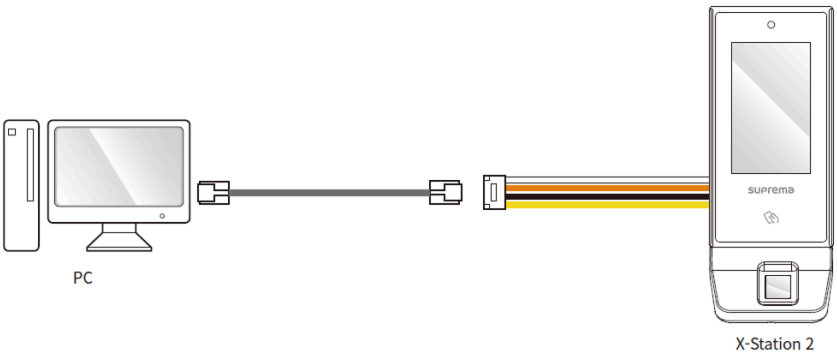
Conexión LAN (conexión a un concentrador)

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



Conexión LAN (conexión directa a una PC)

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



Puertos y servicios de red

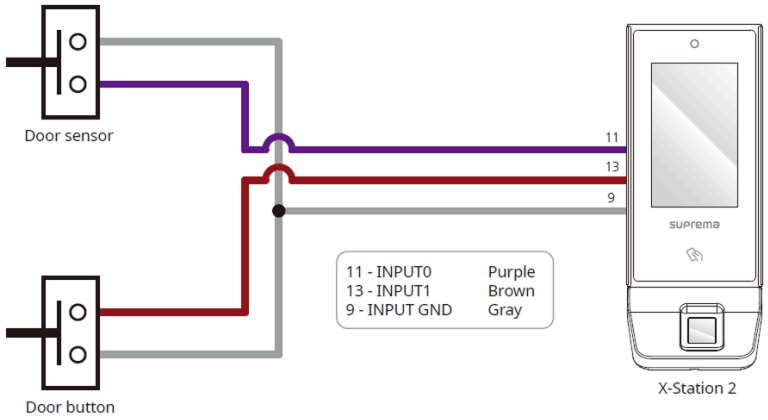
Este dispositivo usa los siguientes puertos para la comunicación en red y el funcionamiento estable del servicio.

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

Información

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

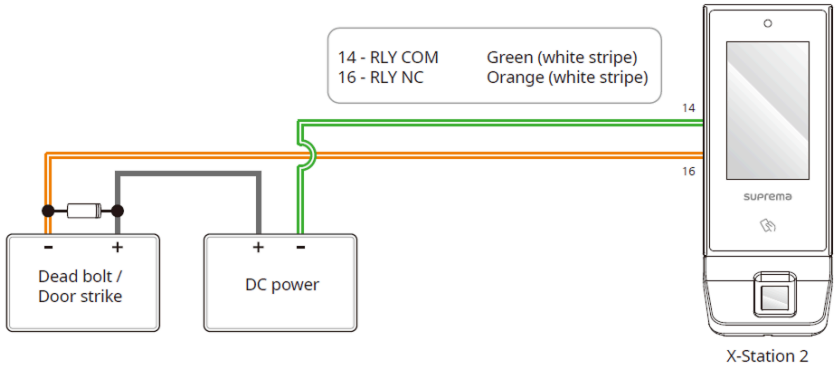
Conexión de entrada



Conexión del relé

Cerradura fail safe

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



Precaución

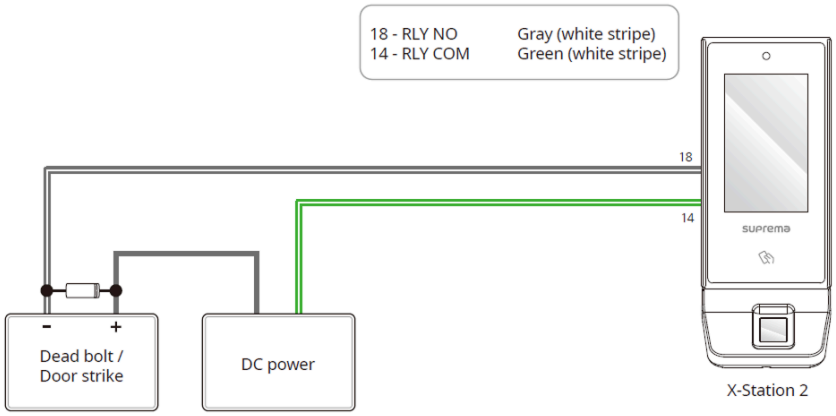
- Instale un diodo en ambos extremos del cable de la cerradura, como se muestra en la figura, para proteger el relé de la corriente inversa que se produce cuando la cerradura funciona.
- Utilice una fuente de alimentación independiente para el producto y la cerradura.
- Los lectores inteligentes independientes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

Información

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

Cerradura fail secure

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



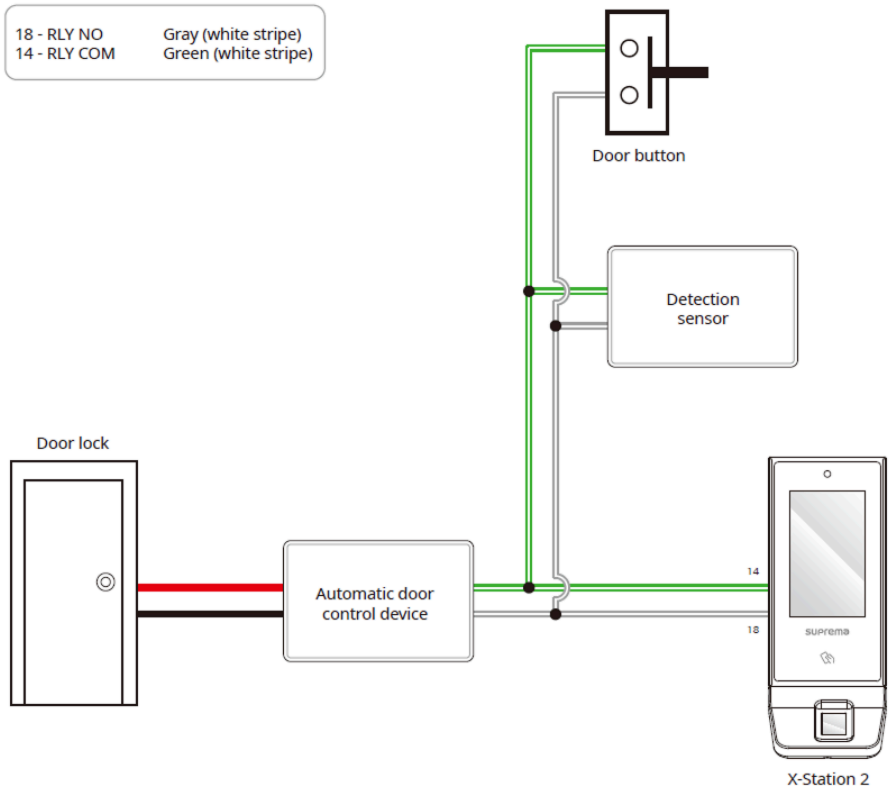
Precaución

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

Información

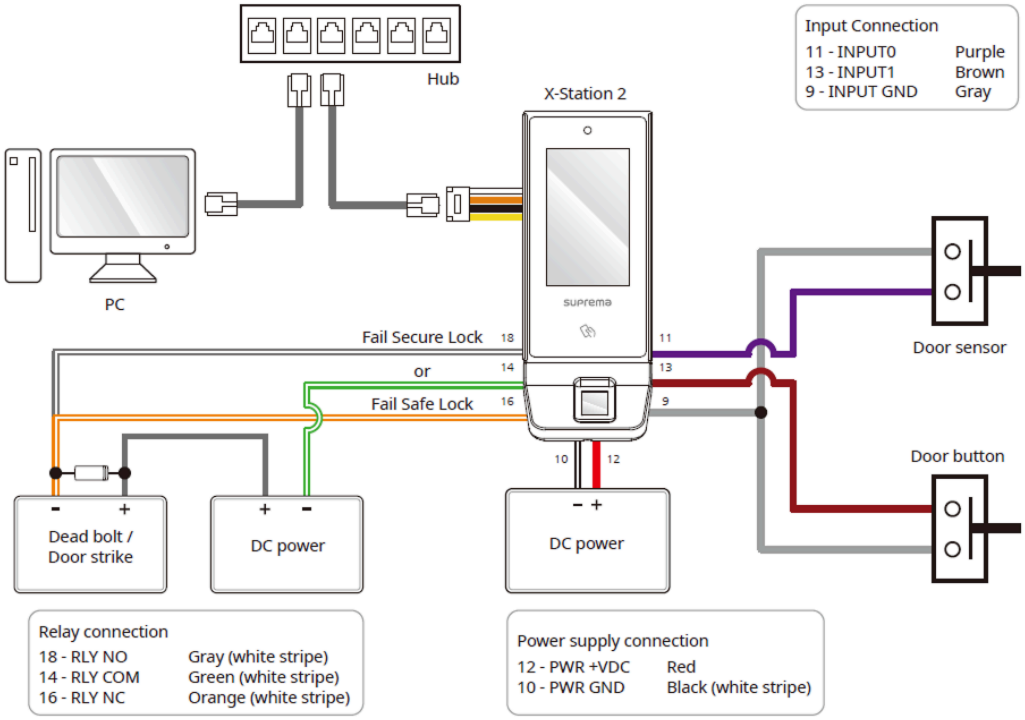
Preste atención a la dirección de instalación del diodo. Instale el diodo cerca de la cerradura.

Conexión de puerta automática



Conectar como independiente

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



Precaución

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

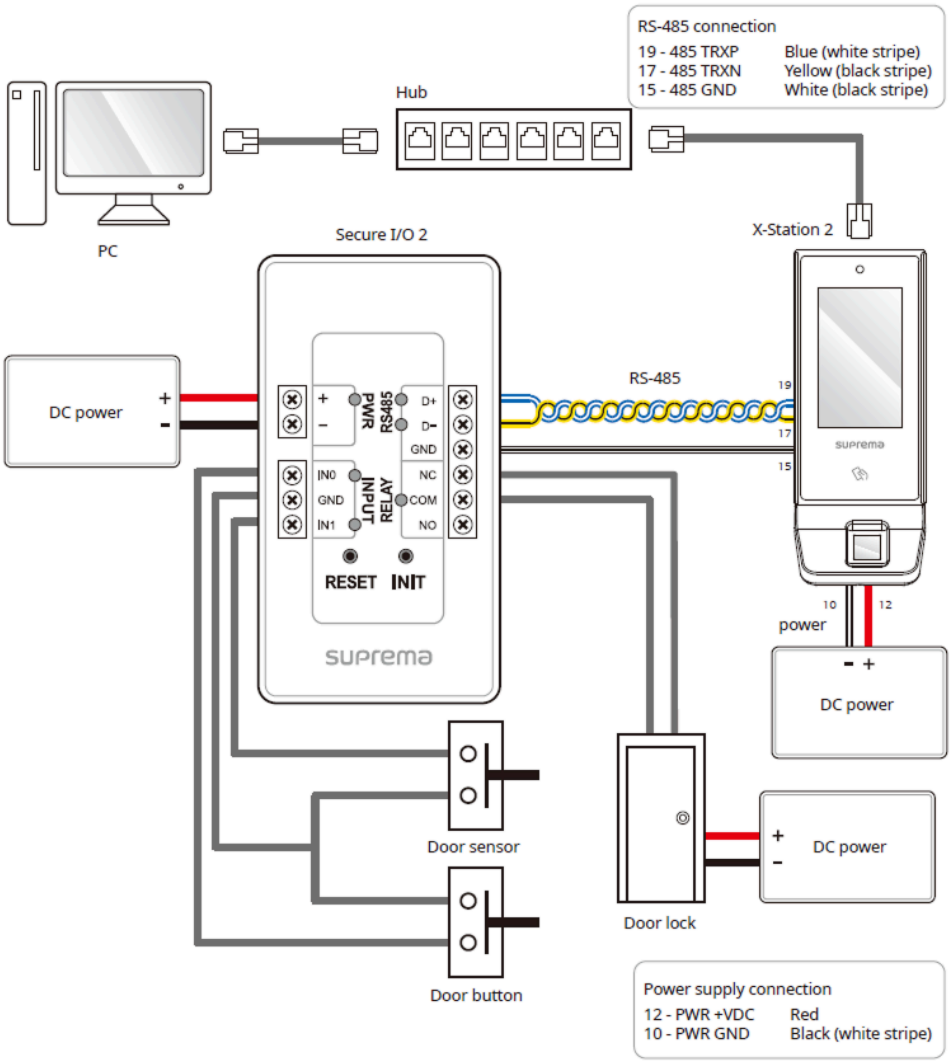
Información

- El dispositivo puede utilizarse como controlador de múltiples puertas con los dispositivos esclavos mediante el cable RS-485. Los dispositivos esclavos se utilizan como lectores ficticios y la autenticación se realiza en el dispositivo maestro.
- 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.

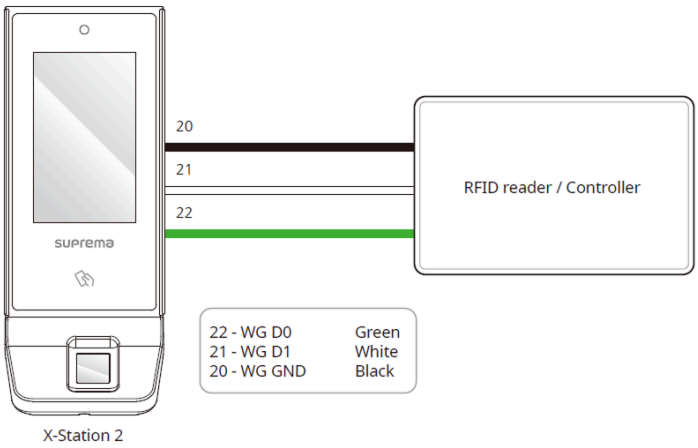


Información

- 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.
- El número máximo de dispositivos esclavos que se pueden conectar varía según el método de autenticación, el número de usuarios y el número de dispositivos. Ten en cuenta también que la cantidad de dispositivos esclavos afecta el rendimiento de autenticación.
- Conecte hasta 31 dispositivos esclavos a un dispositivo maestro. El ancho de banda de RS-485 permite conectar hasta 7 dispositivos de autenticación por huella.
- Para más información, comuníquese con el Equipo de soporte técnico de Suprema.

Conexión Wiegand

Use como dispositivo de entrada o salida Wiegand.



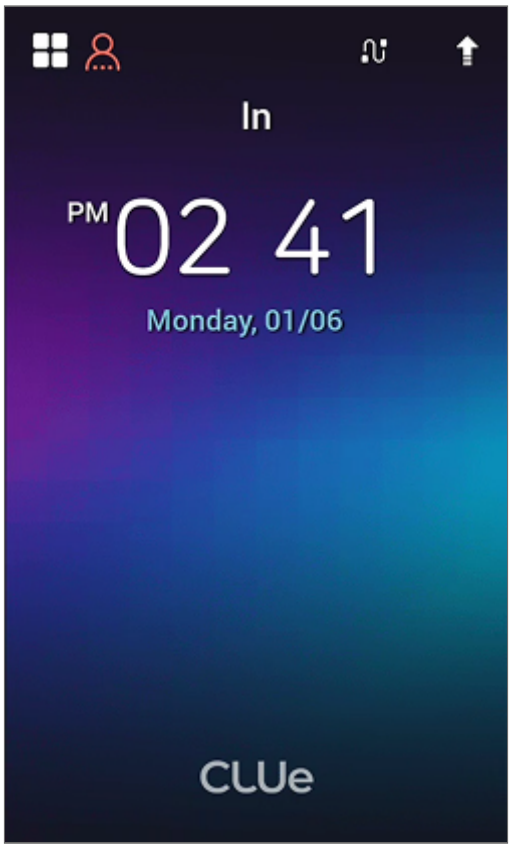
Cómo Usar

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

Menú de Administrador

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

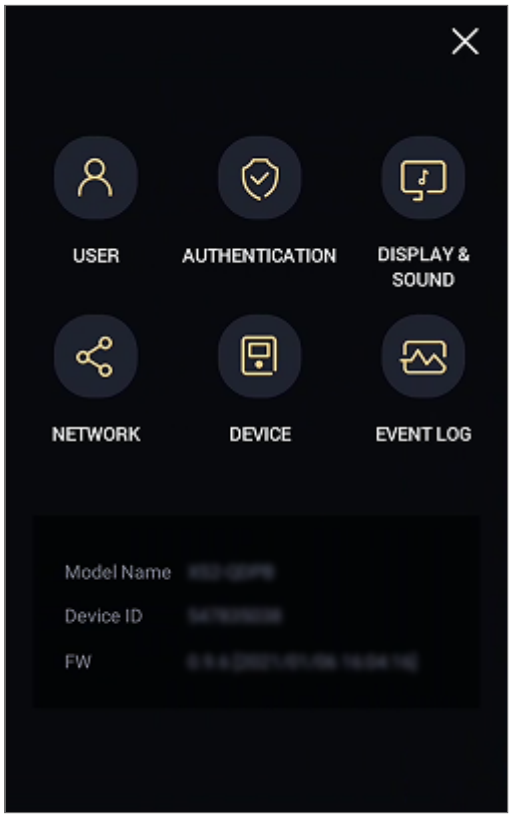
Icono superior



Nombre	Descripción de la función
(Conectando a Suprema CLUe)	Icono que indica que el dispositivo se está conectando a Suprema CLUe
(Suprema CLUe)	Icono que indica que el dispositivo está conectado a Suprema CLUe
(RS-485)	Icono que indica que la comunicación RS-485 está conectada
(TCP/IP)	Icono que indica el estado de conexión de la comunicación TCP/IP

Menú completo

1. Presiona , ingresa la contraseña y accede al menú.
2. Selecciona el menú deseado.



Información

Si **Menu Password** no está configurado, presione para abrir la pantalla del menú. Para obtener detalles sobre cómo configurar la contraseña, consulta Contraseña del menú.

Usuario

Describe cómo registrar, editar, eliminar y gestionar usuarios.

Información

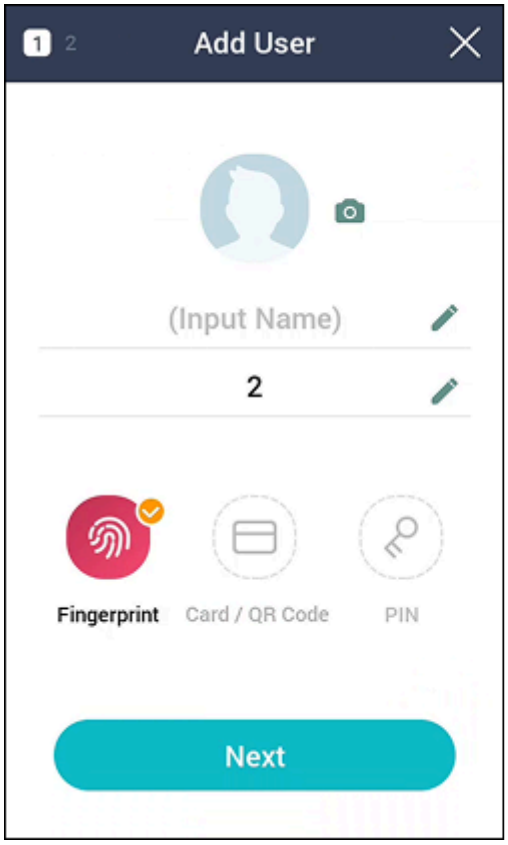
Cuando se usa el modo Suprema CLUe, el enroll, la edición y la eliminación de usuarios están disponibles solo en el servidor Suprema CLUe, no en el dispositivo.

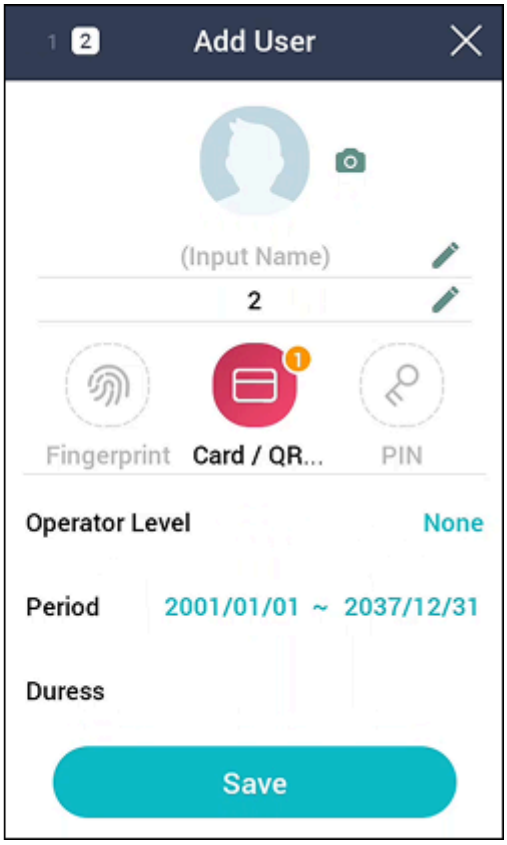
Registrar información de usuario

Registre información de usuario que incluya datos de autenticación biométrica.

1. Presiona , ingresa la contraseña y accede al menú.

2. Seleccione **USER** → ⊕ y configure los elementos deseados. La información de uso de usuarios aparece.





- 📷: Registre una foto de usuario.
- **Nombre**: Introduzca el nombre de usuario.
- **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.
- **Fingerprint**: XS2-ODPB, XS2-OAPB Registre una huella digital para la autenticación del usuario. Presione **Fingerprint** → **Next** y siga las instrucciones en pantalla para inscribir una huella. Presione ⊕ para inscribir más huellas. Para obtener más información sobre el registro de huellas, consulte Registro de huella digital de usuario.
- **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. Haga clic en ⊕ para inscribir más tarjetas.
- **PIN**: Ingrese el PIN que desea usar. Presione **PIN** → **Next** e introduzca el PIN que desea usar. Para confirmarlo, introduzca el PIN nuevamente y luego presione **OK**. Para evitar filtraciones, ingrese un PIN de 4 a 16 dígitos.

> **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**: Puede usar los menús **AUTHENTICATION**, **DISPLAY & SOUND**, **DEVICE**, **NETWORK**, **EVENT LOG**.
>
> – **User Management**: Puede usar los menús **USER**, **EVENT LOG**.

- **Period**: Configure la duración de uso de la cuenta de usuario.
- **Duress**: XS2-ODPB, XS2-OAPB Seleccione para registrar una huella digital 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.

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

Registro de huella digital de usuario XS2-ODPB, XS2-OAPB

1. Presiona , ingresa la contraseña y accede al menú.
2. Haga clic en **USER** → .
3. Seleccione **Fingerprint** → **Next**.
4. Después de escanear la huella del dedo que se va a inscribir, escanee nuevamente la huella del mismo dedo.

> **Información**
>
> - El registro de huellas digitales solo está disponible para los productos XS2-ODPB y XS2-OAPB.
> - Coloque el dedo lo suficientemente profundo para que haga contacto completo con el sensor.
> - Coloque el centro de la huella en el centro del sensor.
> - Si un dedo tiene un corte o la huella está borrosa, seleccione otro dedo para la huella.
> - Ingrese con precisión según las instrucciones en pantalla al autenticar huellas.
> - Si mantiene el dedo en posición vertical de modo que se reduzca el área de contacto con el sensor o cambia el ángulo del dedo, es posible que la autenticación de la huella no se realice.

Modificar información de usuario

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

1. Presiona , ingresa la contraseña y accede al menú.
2. Haga clic en **USER** → .

3. Seleccione los términos de búsqueda. Busque usuarios con **All**, **User ID**, **Name**, **Fingerprint**, **Card / QR Code**.
4. Seleccione el usuario que desea modificar.
5. Modifique la información consultando Registrar información de usuario y presione **OK**.
   - Seleccione y presione **OK** para eliminar un usuario.

> **Información**
>
> - La búsqueda por huella digital está disponible solo en XS2-ODPB y XS2-OAPB.
> - **Access Group** se puede enrollar en el servidor Suprema CLUe.

Eliminar todos los usuarios

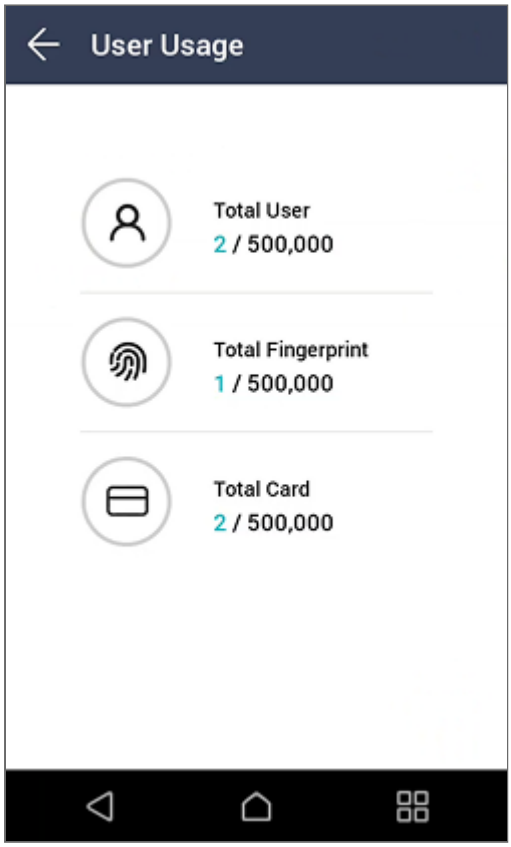
Elimine todos los usuarios registrados a la vez.

1. Presiona , ingresa la contraseña y accede al menú.
2. Selecciona **USER** → .
3. Seleccione **Delete All** para verificar y luego presione **OK**.
4. Para eliminar a todos los usuarios, presione **OK**.

Ver uso de usuarios

Vea los usuarios registrados y el recuento de tarjetas de un vistazo.

1. Presiona , ingresa la contraseña y accede al menú.
2. Haga clic en **USER** → . La información de uso de usuarios aparece.



> **Información**
> El número de huellas digitales solo puede verificarse en los productos XS2-ODPB y XS2-OAPB.

Autenticación

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

> **Información**
> Si usas el modo Suprema CLUe, solo puedes enrollar, editar y eliminar los modos de autenticación en el servidor Suprema CLUe, no en el dispositivo.

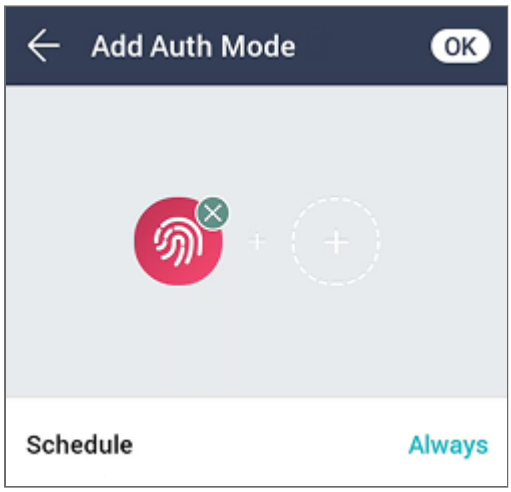
Modo de autenticación

Configura el modo de autenticación. Puedes combinar **Fingerprint**, **PIN**, **Card / QR Code** y **ID** para el modo de autenticación, y también puedes configurar horarios para cada uno de los modos de autenticación.

> **Información**
> La autenticación por huella digital solo está disponible para los productos XS2-ODPB y XS2-OAPB.

Registrar modo de autenticación

1. Presiona , ingresa la contraseña y accede al menú.
2. Presione **AUTHENTICATION** → **Auth Mode**.
3. Selecciona .
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
Huella	* : Este modo utiliza solo huella digital. - + : Este modo requiere ingresar un PIN después de la autenticación por huella digital.
Tarjeta / Código QR	* : Este modo utiliza solo la autenticación por tarjeta / código QR. - + : Este modo requiere autenticación mediante tarjeta / código QR seguida de autenticación por huella digital. - + : Este modo requiere autenticación mediante tarjeta / código QR seguida de ingreso de PIN. - + / : Este modo permite autenticación mediante tarjeta / código QR seguida de huella digital o ingreso de PIN. - + + : Este modo requiere autenticación por huella digital y ingreso de PIN después de la autenticación mediante tarjeta / código QR.

Categoría	Descripción
ID	* ID + huella: Este modo requiere ingresar un ID seguido de autenticación por huella digital. - ID + llave: Este modo requiere ingresar un ID seguido de ingreso de PIN. - ID + huella / llave: Este modo permite ingresar un ID seguido de autenticación por huella digital o ingreso de PIN. - ID + huella + llave: Este modo requiere autenticación por huella digital y ingreso de PIN después de ingresar un ID.

> **Información**
>
> - **Schedule** se puede configurar en el servidor Suprema CLUe. Si no se establece un horario, solo se puede seleccionar **Always**.
> - Para usar la autenticación **QR/Barcode** en los modelos XS2-DPB, XS2-APB, XS2-ODPB y XS2-OAPB, activa **QR/Barcode** en **AUTHENTICATION** → **QR/Barcode Operation** y adquiere una licencia de dispositivo adicional. Para obtener más información, consulta Licencia.

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

Modificar modo de autenticación

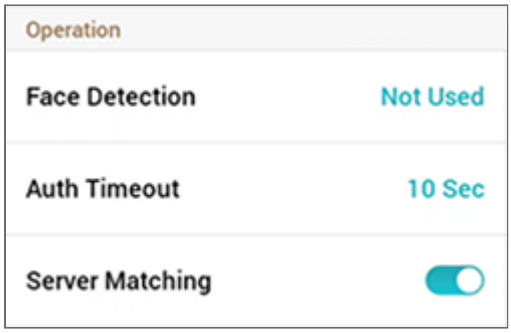
1. Presiona , ingresa la contraseña y accede al menú.
2. Presione **AUTHENTICATION** → **Auth Mode**.
3. Selecciona el modo de autenticación que deseas modificar.
4. Modifica el modo de autenticación consultando Registrar modo de autenticación y pulsa **OK**.

Eliminar modo de autenticación

1. Presiona , ingresa la contraseña y accede al menú.
2. Presione **AUTHENTICATION** → **Auth Mode**.
3. Pulsa y selecciona el modo de autenticación que deseas eliminar. Es posible seleccionar varias opciones.
4. Pulsa **OK** para eliminar el elemento seleccionado.

Operación

1. Presiona , ingresa la contraseña y accede al menú.
2. Después de pulsar **AUTHENTICATION**, cambia el elemento deseado en **Operation**.



- **Face Detection**: Cuando usas la función de detección de rostro, puede detectar un rostro humano real. Después de autenticarte con una tarjeta, un código QR o un PIN, el rostro debe detectarse para que la autenticación tenga éxito.
- **Auth Timeout**: Si la autenticación no se completa dentro del tiempo establecido, la autenticación fallará. Se puede configurar entre 3 y 20 segundos.
- **Server Matching**: Cuando configuras la coincidencia con el servidor, autentica al usuario del dispositivo o al usuario de Suprema CLUe según el modo de autenticación configurado. Se puede usar cuando el dispositivo tiene demasiada información de usuarios o cuando el dispositivo está instalado en exteriores.

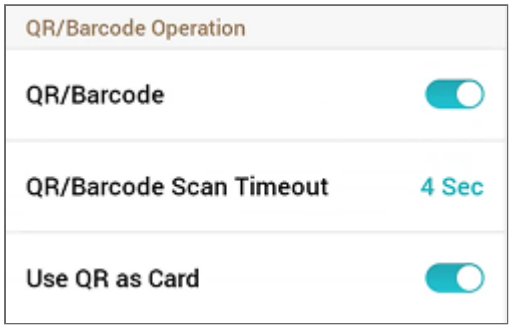
> **Información**
>
> – Si usas **Server Matching**, activa la coincidencia con el servidor en el dispositivo y en el servidor Suprema CLUe.
>
> – Si usas el modo Suprema CLUe, **Server Matching** se activa automáticamente.

Opciones de autenticación mediante QR/código de barras

Configura la autenticación por QR/código de barras.

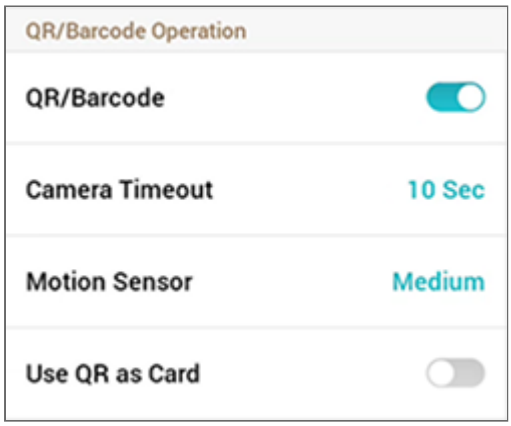
1. Presiona , ingresa la contraseña y accede al menú.
2. Después de presionar **AUTHENTICATION**, activa **QR/Barcode** en **QR/Barcode Operation**.

XS2-QDPB, XS2-QAPB



- **QR/Barcode**: Selecciona si se usa la autenticación por QR/código de barras.
- **QR/Barcode Scan Timeout**: Si el QR/código de barras no se escanea dentro del tiempo establecido, la autenticación falla. Establece entre 4 y 10 segundos.
- **Use QR as Card**: Configura la autenticación con un código QR que contenga los mismos datos que la tarjeta CSN o tarjeta Wiegand emitida al usuario.

XS2-DPB, XS2-APB, XS2-ODPB, XS2-OAPB



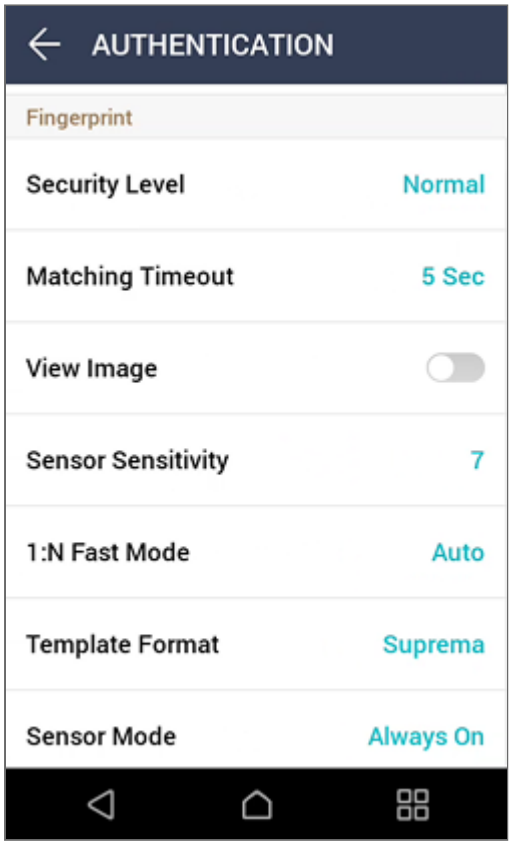
- **QR/Barcode**: Selecciona si se usa la autenticación por QR/código de barras.
- **Camera Timeout**: Si el QR/código de barras no se escanea dentro del tiempo establecido, la autenticación falla. Establece entre 3 y 20 segundos. Disponible solo cuando **QR/Barcode** está activado.
- **Motion Sensor**: Establece la sensibilidad para detectar movimiento alrededor del dispositivo. Disponible solo cuando **QR/Barcode** está activado.
- **Use QR as Card**: Configura la autenticación con un código QR que contenga los mismos datos que la tarjeta CSN o tarjeta Wiegand emitida al usuario. Disponible solo cuando **QR/Barcode** está activado.

> **Información**
> Para usar la autenticación **QR/Barcode** en los modelos XS2-DPB, XS2-APB, XS2-ODPB y XS2-OAPB, activa **QR/Barcode** en **AUTHENTICATION** → **QR/Barcode Operation** y adquiere una licencia de dispositivo adicional. Para obtener más información, consulta Licencia.

Configuraciones de huella digital XS2-ODPB, XS2-OAPB

Cambia los ajustes de autenticación por huella digital.

1. Presiona , ingresa la contraseña y accede al menú.
2. Tras presionar **AUTHENTICATION**, modifica los elementos deseados en **Fingerprint**.



- **Security Level**: Configura el nivel de seguridad para la autenticación 1:N:.
- **Matching Timeout**: Configura el tiempo de espera para la correspondencia de huellas. Si la autenticación no se completa dentro del tiempo especificado, fallará.
- **View Image**: Se puede ver la imagen original de la huella escaneada.
- **Sensor Sensitivity**: Configura la sensibilidad del sensor de reconocimiento de huellas. Establece la sensibilidad más alta para obtener información de huella dactilar precisa.
- **1:N Fast Mode**: Configura la velocidad de la autenticación por huella. Al seleccionar **Auto**, la velocidad de autenticación se ajusta según el total de plantillas de huellas almacenadas en el dispositivo.
- **Template Format**: Configura el formato de plantilla de huella. **SUPREMA** está configurado por defecto. Al cambiar el formato de la plantilla, las huellas digitales guardadas anteriormente quedarán inutilizables, así que tenga cuidado al modificarlo.

> **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.

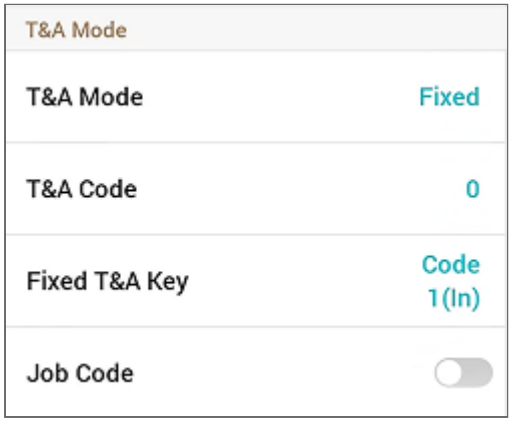
- **Sensor Mode**: Configura en **Auto On** para encender el sensor de huella cuando detecte el dedo del usuario. Al configurarse en **Always On**, el sensor permanece encendido aunque no se estén escaneando huellas.
- **Live Finger Detection**: Configura el nivel de detección de huellas falsas. Niveles más altos de detección de huellas falsas pueden aumentar las tasas de rechazo de las huellas reales.
- **Advanced Enrollment**: Evalúa la calidad de las huellas escaneadas para guardar información de alta calidad. Habilite la notificación para avisar al usuario cuando la calidad de la huella digital sea baja, ayudándole a escanearla correctamente.

- **Duplicate Check**: Verifica huellas duplicadas durante el enrolamiento.

Modo de asistencia

Configura cómo registrar el modo T&A.

1. Presiona , ingresa la contraseña y accede al menú.
2. Haz clic en **AUTHENTICATION**, luego modifica el elemento deseado en **T&A Mode**.



- **T&A Mode**: Configura cómo usar el modo de asistencia.
- **T&A Code**: Registra eventos de T&A. Para registrar eventos de asistencia, selecciona **T&A Code** → y configura los iconos que se mostrarán 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.

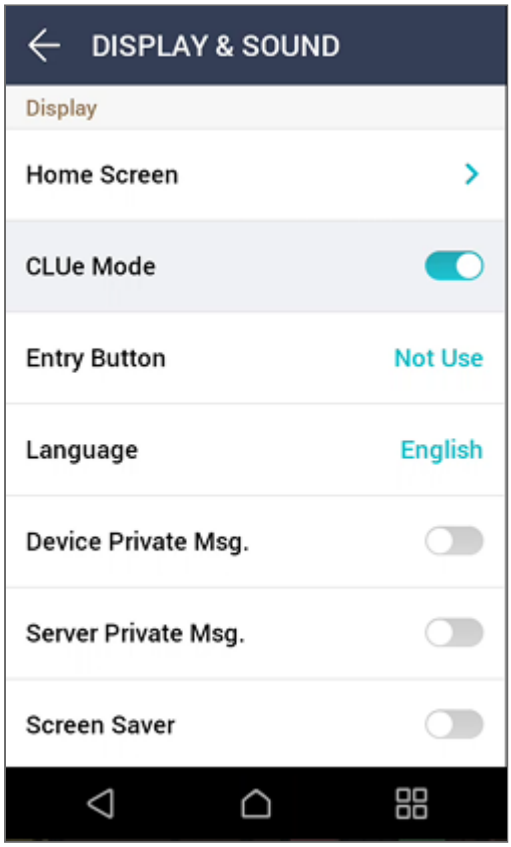
Ajustes

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

Pantalla y sonido

Cambie los ajustes de pantalla y sonido del dispositivo.

1. Presiona , ingresa la contraseña y accede al menú.
2. Haz clic en **DISPLAY & SOUND** y cambia el elemento deseado.



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

Información

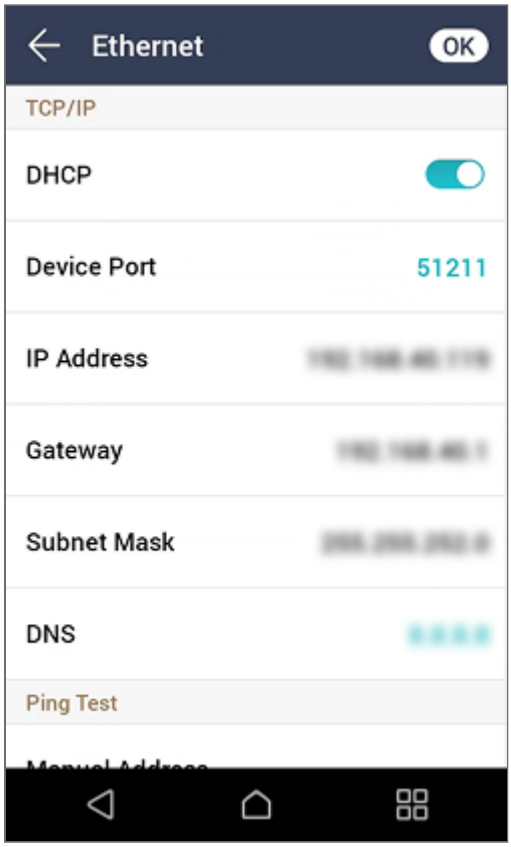
Para obtener más información sobre el SDK de dispositivos BioStar, consulte la página del SDK de dispositivos BioStar en la base de conocimientos de Suprema.

Red

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

Ethernet

1. Presiona , ingresa la contraseña y accede al menú.
2. Seleccione **NETWORK** → **Ethernet**.
3. Cambie el elemento deseado.



- **DHCP**: Configure si se utiliza DHCP. Desactive la configuración DHCP para permitir que los usuarios modifiquen **Device Port**, **IP Address**, **Gateway** y **Subnet Mask**.
- **Device Port**: Configure el puerto del dispositivo.
- **IP Address**: Compruebe la dirección IP del dispositivo. Para modificarla, desactive la configuración de DHCP.
- **Gateway**: Compruebe la puerta de enlace del dispositivo. Para modificarla, desactive la configuración de DHCP.
- **Subnet Mask**: Compruebe la máscara de subred del dispositivo. Para modificarla, desactive la configuración de DHCP.
- **DNS**: Configure la dirección del servidor DNS.

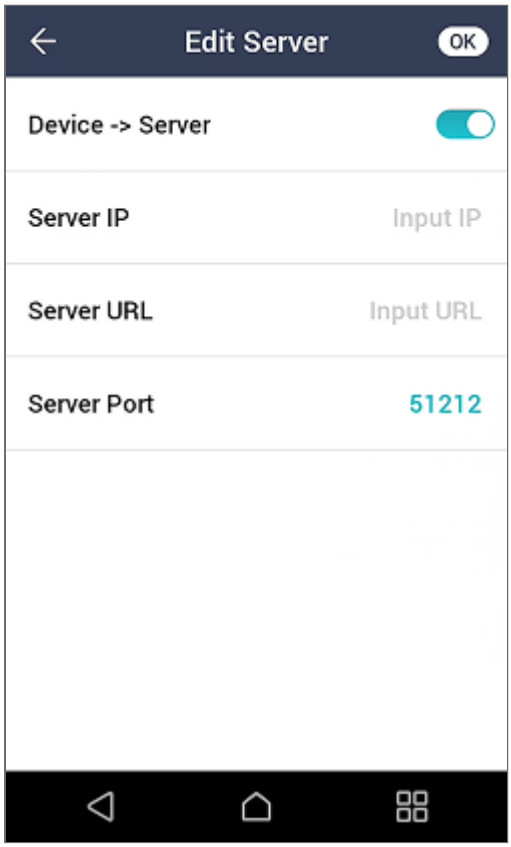
- **Manual Address**: Ingrese la dirección para la prueba de ping.
- **Timeout**: Ingrese el tiempo máximo de espera para la prueba de ping.
- **Ping Test**: Inicia la prueba de Ping.

> **Información**
> Seleccione un servidor DNS abajo para ejecutar la prueba de Ping.

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

Servidor

1. Presiona , ingresa la contraseña y accede al menú.
2. Seleccione **NETWORK** → **Server**.
3. Cambie el elemento deseado.



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

> **Información**
> Cuando usa el modo Suprema CLUe, el setting **Device → Server** queda fijo.

- **Server IP**: Para conectarse a Suprema CLUe, ingrese `127.0.0.1`.

- **Server URL**: Ingrese **Server URL** en lugar de **Server IP**.
- **Server Port**: Para conectarse a Suprema CLUe, ingrese `51212`.

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

Configuración de comunicación serial

1. Presiona , ingresa la contraseña y accede al menú.
2. Seleccione **NETWORK**.
3. Establezca la opción deseada en **Serial Setting**.



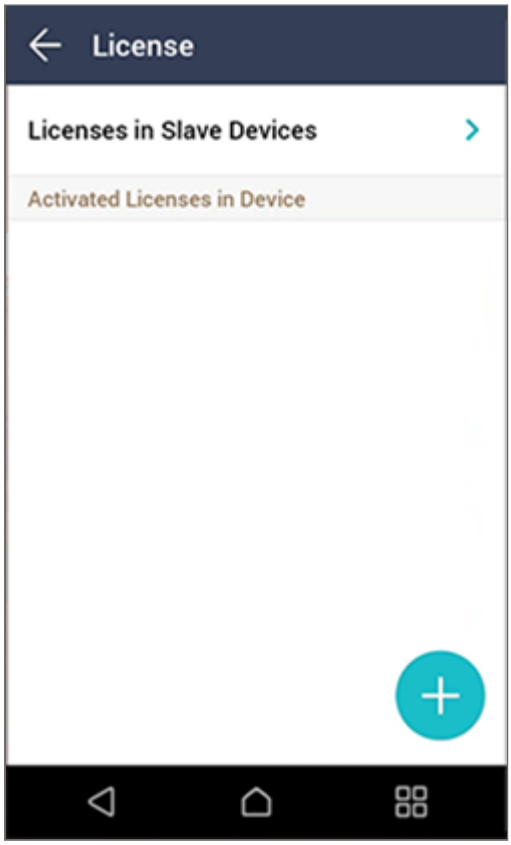
- **RS-485**: Seleccione el modo RS-485.
- **Baud Rate**: Seleccione la velocidad en baudios deseada.

Dispositivo

Licencia

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

1. Presiona , ingresa la contraseña y accede al menú.
2. Presiona **DEVICE** → **License**.
3. Conecta al dispositivo la USB que contiene la licencia y selecciona para activar la licencia del dispositivo.



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



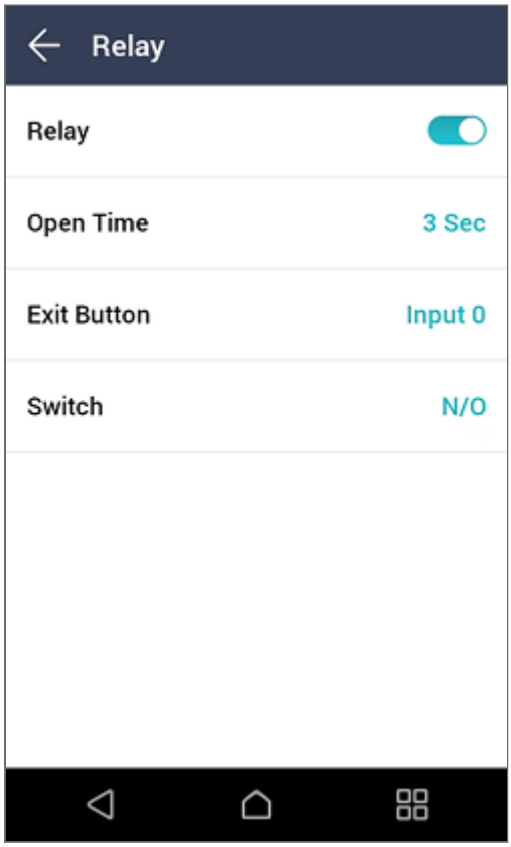
Información

- 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. Presiona , ingresa la contraseña y accede al menú.
2. Haga clic en **DEVICE** → **Relay**.

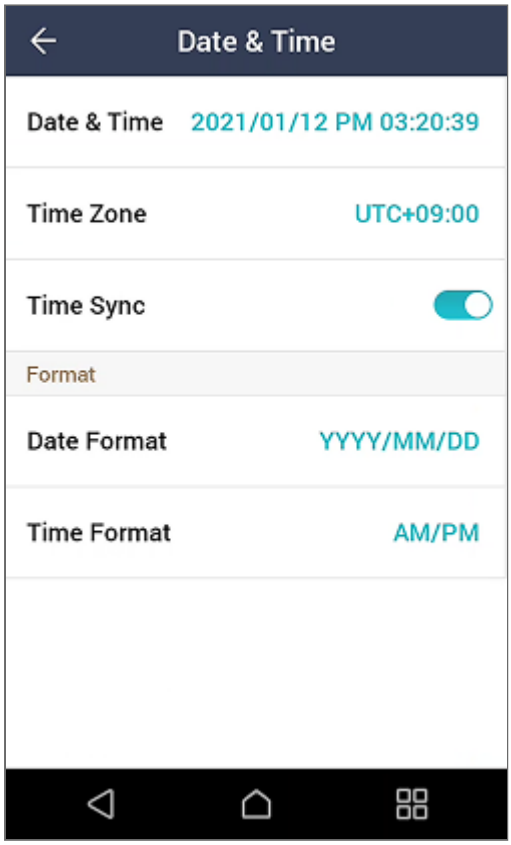


- **Relay**: Configure si el relé está habilitado. Habilitar el ajuste de relé permite configurar **Open Time** y **Exit Button**.
- **Open Time**: Establece la duración que la puerta permanece abierta cuando se ha realizado la autenticación de usuario estándar.
- **Exit Button**: Selecciona el puerto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

Fecha y hora

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

1. Presiona , ingresa la contraseña y accede al menú.
2. Haz clic en **DEVICE** → **Date & Time**.
3. Cambie el elemento deseado.

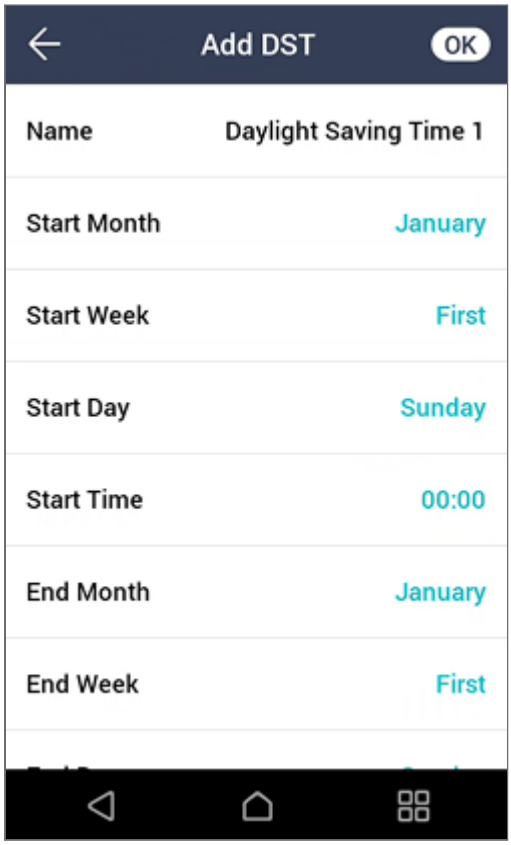


- **Date & Time**: Compruebe la fecha y hora actuales. Para modificarla manualmente, desactive **Time Sync**.
- **Time Zone**: Ajuste la referencia horaria de la ubicación actual.
- **Time Sync**: Sincronice el servidor y la hora. Si desea sincronizar el servidor y la hora, habilite **Time Sync**.
-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

Horario de verano

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

1. Presiona , ingresa la contraseña y accede al menú.
2. Haz clic en **DEVICE** → **Daylight Saving Time**, luego presiona para agregar el horario de verano.
3. Cambie el elemento deseado.



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

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

Información del dispositivo

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

1. Presiona , ingresa la contraseña y accede al menú.
2. Selecciona **DEVICE** → **Device Info**. Vea la información de **Model Name**, **Device ID**, **Serial No.**, **HW**, **FW**, **Kernel**, **MAC** y **OSS Notice**.

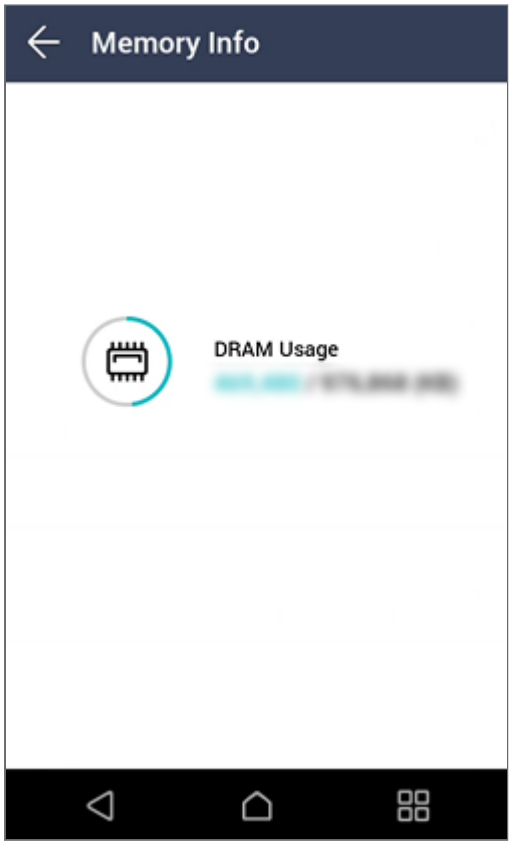


Información
Puede ver la información de licencia del dispositivo en **OSS Notice**.

Información de memoria

Consulta el estado de uso de la memoria.

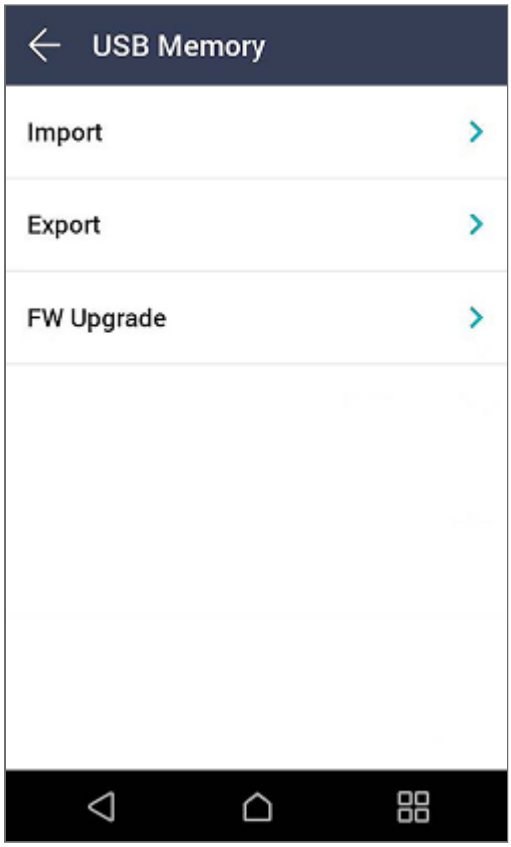
1. Presiona , ingresa la contraseña y accede al menú.
2. Selecciona **DEVICE** → **Memory Info**. Consulta el estado de uso de memoria del dispositivo.



Memoria USB

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

1. Presiona , ingresa la contraseña y accede al menú.
2. Selecciona **DEVICE** → **USB Memory**.
3. Selecciona el elemento deseado y cambia el ajuste.



- **Import**: Seleccione los elementos que desea importar desde la memoria USB conectada.
  - **USER**: Importe la información de usuarios.
  - **CLUe Resource**: Copie archivos de imagen al dispositivo.

    > **Información**
    > Puede copiar hasta 5 archivos de imagen a la vez.

- **Export**: Seleccione la información que desea exportar a la memoria USB conectada.
  - **All**: Exporte toda la información.
  - **USER**: Exporte la información de usuarios.
  - **Log**: Exporte la información de registros.
- **FW Upgrade**: Actualice el firmware si los archivos de firmware están guardados en la memoria USB conectada.

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

Sabotaje

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

1. Presiona , ingresa la contraseña y accede al menú.
2. Seleccione **DEVICE**.
3. Active **Secure Tamper** para eliminar los datos de todos los usuarios registrados, todos los registros y las claves seguras cuando ocurra un evento de manipulación.

Reiniciar dispositivo

Reinicia el dispositivo.

1. Presiona , ingresa la contraseña y accede al menú.
2. Selecciona **DEVICE** → **Restart Device**.
3. Presiona **OK** para reiniciar el dispositivo. Presiona **Cancel** para regresar a la pantalla anterior.

Restaurar valores predeterminados

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

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

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

Tipo de ID de usuario

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

1. Presiona , ingresa la contraseña y accede al menú.

2. Seleccione **DEVICE** → **User ID Type**.
   - **Number**: Ingrese un ID de usuario con solo números.
   - **Alphanumeric**: Ingrese un ID de usuario con caracteres alfanuméricos y los símbolos `_` `-`.
3. Pulsa **OK** para guardar la configuración.

Contraseña del menú

Establezca la contraseña del dispositivo.

1. Presiona , ingresa la contraseña y accede al menú.
2. Seleccione **DEVICE** → **Menu Password**.
3. Presione **OK** para establecer y guardar la contraseña.

> **Información**
>
> - Establezca la contraseña del dispositivo de 4~16 dígitos.
> - Tenga cuidado de no perder la contraseña del dispositivo. Si pierde la contraseña, inicialice el dispositivo para conectarse a él.

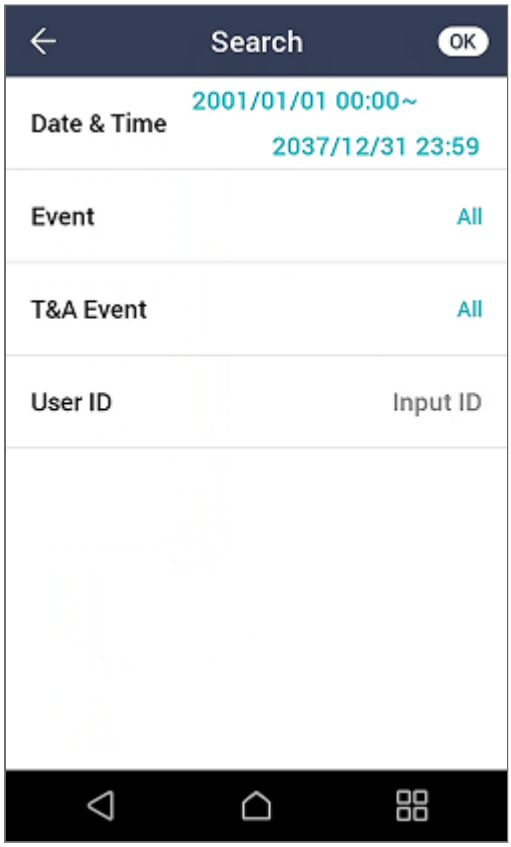
Registros de eventos

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

Busca registros de eventos

Configura condiciones para buscar registros.

1. Presiona , ingresa la contraseña y accede al menú.
2. Seleccione **EVENT LOG**. Todos los registros de eventos aparecen.
3. Presione para buscar un registro específico y cambiar la condición.



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

Eliminar todos los registros

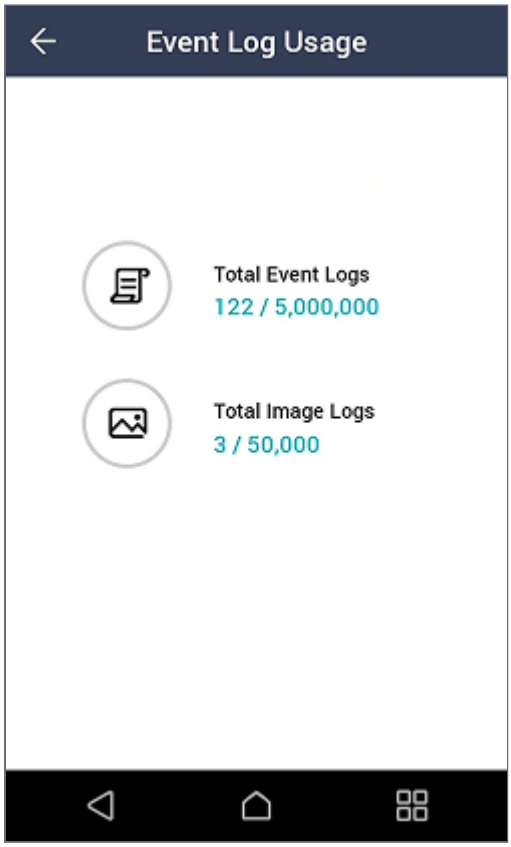
Elimina todos los registros guardados.

1. Presiona , ingresa la contraseña y accede al menú.
2. Seleccione **EVENT LOG**. Todos los registros de eventos aparecen.
3. Seleccione y haga clic en **OK** para eliminar todos los registros. Presiona **Cancel** para regresar a la pantalla anterior.

Ver uso de registros

Consulta el estado del uso de registros.

1. Presiona , ingresa la contraseña y accede al menú.
2. Haga clic en **EVENT LOG** → . Verifique el uso de los registros de eventos e imágenes del dispositivo.


Event Log Usage
Total Event Logs
122 / 5,000,000
Total Image Logs
3 / 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.

- Si pierde su PIN, 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.

QR/Código de Barras

Q. No se puede escanear un código QR/código de barras.

- Consulte Método correcto de autenticación con QR/código de barras y vuelva a intentarlo.
- **XS2-QDPB**, **XS2-QAPB**: Coloque el haz guía en el centro del código QR.
- **XS2-DPB**, **XS2-APB**, **XS2-ODPB**, **XS2-OAPB**: Coloque el código QR/código de barras en el centro de la pantalla de escaneo del dispositivo.
- Ajuste el brillo de su smartphone para que el dispositivo pueda leer el QR/código de barras claramente y vuelva a intentarlo.
- Si el problema persiste, comuníquese con el administrador que emitió el QR/código de barras.

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.

Especificaciones del Producto

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

Credenciales

Biométrico	**Huella** XS2-ODPB, XS2-OAPB • **Dimensiones de la imagen:300 x 400 píxeles** • **Resolución:500 dpi** • **Plantilla:SUPREMA / ISO19794-2 / ANSI-378** • **Extractor / Comparador:Con certificación y compatible con MINEX** • **Certificaciones del sensor:PIV del FBI e ID móvil FAP20 del FBI** • **Detección de huella dactilar viva:Compatible (basado en software)**	
Tarjeta RF	**XS2-DPB, XS2-QDPB, XS2-ODPB**	**125kHz EM y 13.56MHz MIFARE, MIFARE Plus, DESFire, DESFire EV1/EV2/EV3, FeliCa**
	XS2-APB, XS2-QAPB, XS2-OAPB	**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/HID Prox/MIFARE/DESFire/HID iCLASS: 50 mm, Felica: 30 mm**	
Móvil	**NFC, BLE**	
Teclado aleatorio (PIN)	**Soportado**	
QR/Código de Barras[2)]	**XS2-QDPB, XS2-QAPB**	**Soportado**
	XS2-DPB, XS2-APB, XS2-ODPB, XS2-OAPB	**Compatible**[3)]

General

CPU	**1.5 GHz Quad Core**
Memoria	**16 GB Flash + 1 GB RAM**

Chip criptográfico	**Soportado**	
Visualizar	**LCD en color IPS 4"**	
Resolución de pantalla	**480 x 800 píxeles**	
Sonido	**24 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**	
Tipo de cámara	**CMOS de 2M píxeles**	
Resolución de la cámara	**1600 x 1200 píxeles**	
Grado de protección IP	**IP65**	
Autenticación	**XS2-DPB, XS2-APB, XS2-QDPB, XS2-QAPB**	**CE, UKCA, KC, FCC, IC, RCM, BIS, ANATEL, SIG, TELEC, RoHS, REACH, WEEE**
	XS2-ODPB, XS2-OAPB	**CE, UKCA, KC, FCC, IC, RCM, BIS, ANATEL, SIG, RoHS, REACH, WEEE**

Capacidad

Máx. usuarios	**500,000**[4)]	
Máx. credenciales (1:N)	**XS2-ODPB, XS2-OAPB**	**Huella dactilar: 100,000**
Máx. credenciales (1:1)	**XS2-DPB, XS2-APB,**	• **Tarjeta: 500,000**

	XS2-QDPB, XS2-QAPB	• **PIN: 500,000**
	XS2-ODPB, XS2-OAPB	• **Huella dactilar: 500,000** • **Tarjeta: 500,000** • **PIN: 500,000**
Máx. registros de texto	**5,000,000**	
Máx. registros de imágenes	**50,000**	

Interfaz

Ethernet	**Compatible (10/100 Mbps, MDI/MDI-X automática)**
Protocolo de red	**TCP, UDP**
RS-485	**1 canal maestro/esclavo (seleccionable)**
Protocolo de comunicación RS-485	**Compatible con OSDP V2**
Wiegand	**Entrada o salida de 1 canal (seleccionable)**
Entrada	**2 canales de entrada**
Relé	**1 relé**
USB	**USB 2.0 (Maestro)**
PoE	**Compatible (compatible con IEEE 802.3af)**
Tamper	**Soportado**

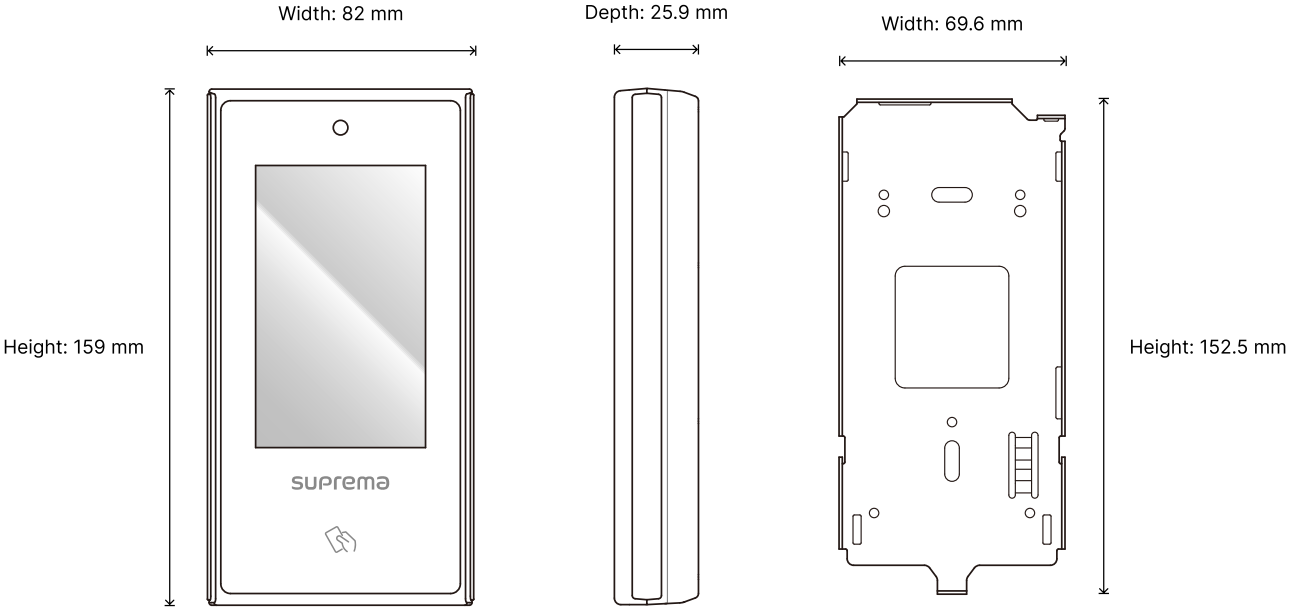
Eléctrico

Alimentación	**12 Vdc**	**Corriente: Máx. 0.8 A**

	24 Vdc	**Corriente: Máx. 0.5 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

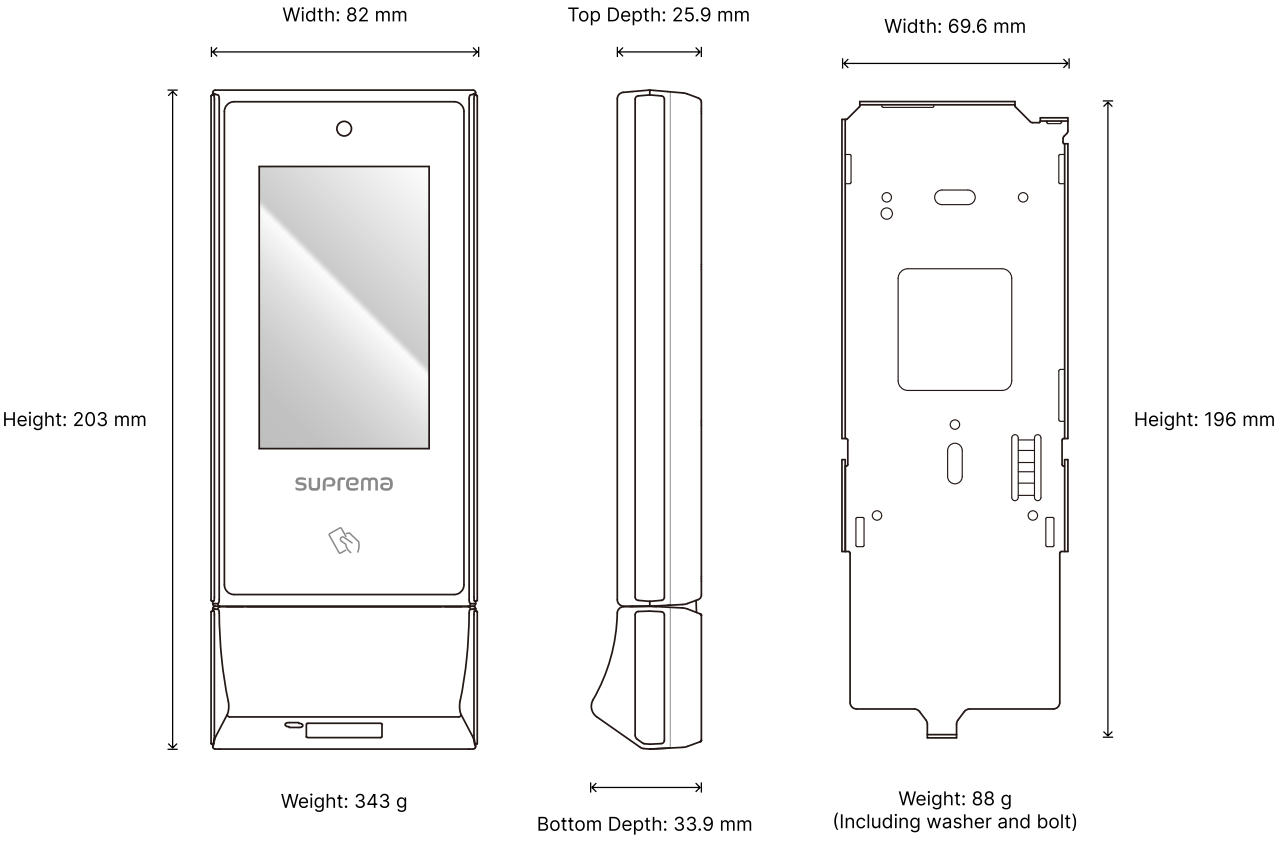
XS2-DPB, XS2-APB



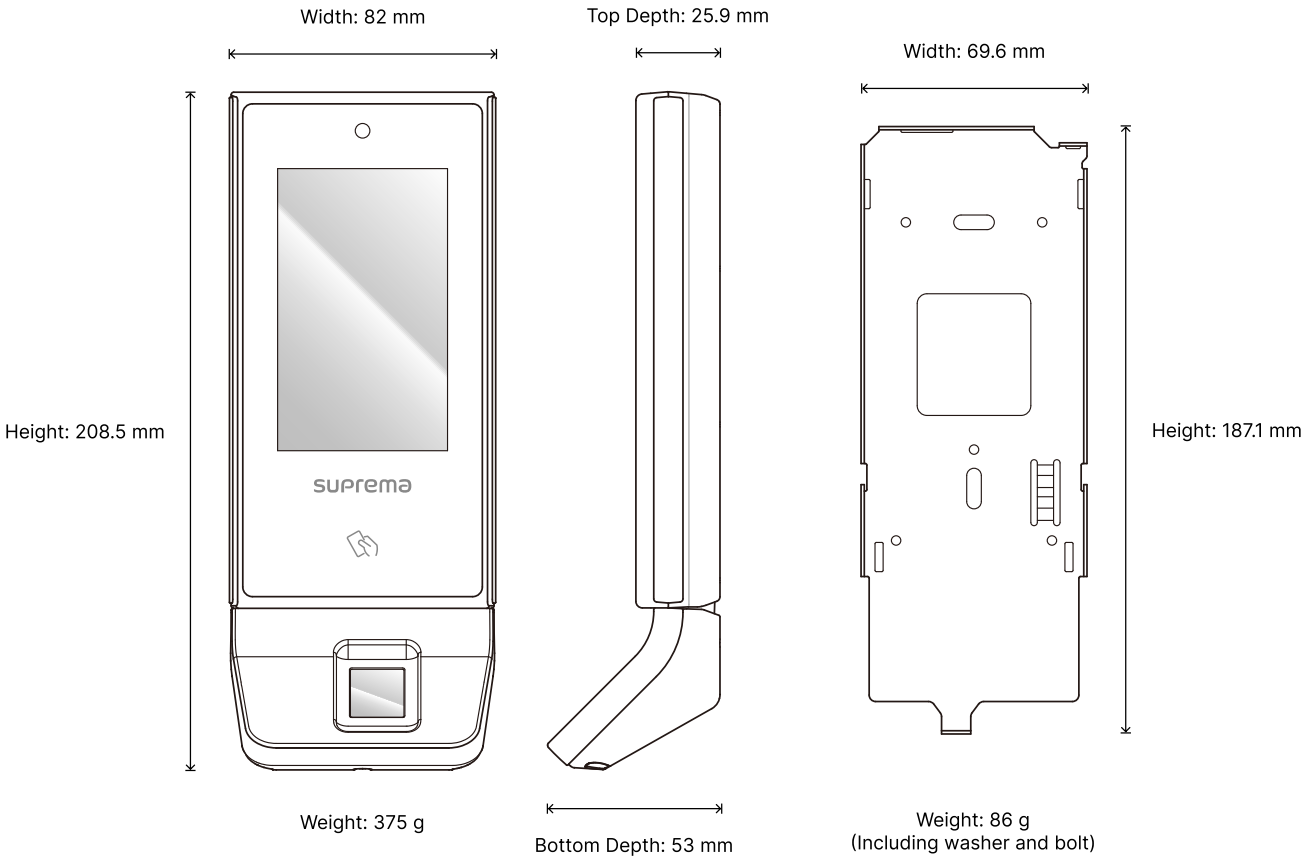
Weight: 280 g

Weight: 67 g
(Including washer and bolt)

XS2-QDPB, XS2-QAPB



XS2-ODPB, XS2-OAPB



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

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

3) Requiere una licencia de dispositivo por separado.

4) Número de usuarios registrados sin datos de credenciales.

Información

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

Información Reglamentaria

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

Información de cumplimiento de la FCC

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

El funcionamiento está sujeto a las siguientes dos condiciones:

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

Información

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

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

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

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

Información de IC

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

El funcionamiento está sujeto a las siguientes dos condiciones:

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

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

L'exploitation est autorisée aux deux conditions suivantes :

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

Declaración de conformidad de la UE (CE)

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

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

- Potencia de transmisión Bluetooth: -0.1 dBm
- Frecuencia Bluetooth: 2402~2480 MHz
- Frecuencia NFC: 13.56 MHz
- Frecuencia RFID: 13.56 MHz + 125 kHz

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

Suprema Inc.

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

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

Apéndices

Incluye avisos legales contenidos en el producto.

Descargos de responsabilidad

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

Aviso de derechos de autor

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

Licencia de código abierto

- El software de este producto se creó modificando la versión 4.x del kernel de Linux y la licencia del kernel de Linux se rige por la GPL. Para obtener más información sobre la licencia GPL, consulte la GNU General Public License.
- La biblioteca BoringSSL incluida en este producto se rige por la licencia OpenSSL y la licencia Original SSLeay. Para más información sobre la licencia BoringSSL, consulte la BoringSSL License.
- Este producto usa "OpenSSL", que está licenciado bajo las licencias OpenSSL y Original SSLeay. Para más información sobre las licencias OpenSSL y Original SSLeay, consulte la OpenSSL License y la Original SSLeay License.
- El AOSP incluido en este producto se rige por la licencia Apache 2.0. Para más información sobre la licencia Apache 2.0, consulte la Apache License.
- Comuníquese con el Equipo de Soporte Técnico de Suprema para descargar el código fuente modificado basado en el kernel de Linux 4.x y las bibliotecas BoringSSL, OpenSSL, Original SSLeay y AOSP incluidas en este producto.

Suprema Inc.

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

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

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

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