Suprema Device Manager

GUÍA DE USUARIO DE

Versión 1.09

Español
ES 102.00.DM

suprema
SECURITY & BIOMETRICS

CONTENIDO

Primeros Pasos 4

Requisitos mínimos 4

Configuración Inicial del Dispositivo 6

Seleccionar dispositivo 6

Configurar los ajustes de la aplicación 6

Configurar dispositivo IP 8

Cambiar configuración del dispositivo 8

Conectar dispositivo 11

Actualizar el firmware del dispositivo 12

Reiniciar dispositivo 12

Inicializar la configuración 13

Inicializar la configuración del dispositivo excepto la de red 13

Cambiar la contraseña del dispositivo 14

Configurar XPass D2 16

Agregar plantilla 16

Aplicar plantilla 24

Gestionar plantillas 25

Buscar y conectar dispositivo 29

Actualizar el firmware del dispositivo 30

Reiniciar dispositivo 12

Cambiar contraseña de administrador 31

Apéndices 33

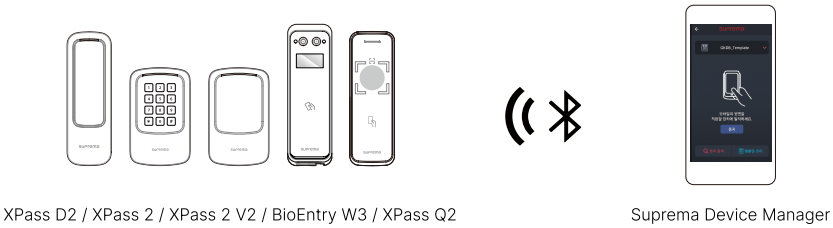
Descargos de responsabilidad 33

Aviso de derechos de autor 34

Licencia de código abierto 34

Primeros Pasos

Suprema Device Manager es una aplicación móvil que utiliza comunicación BLE para configurar los dispositivos XPass D2, XPass 2, XPass 2 V2, BioEntry W3 y XPass Q2 de Suprema.



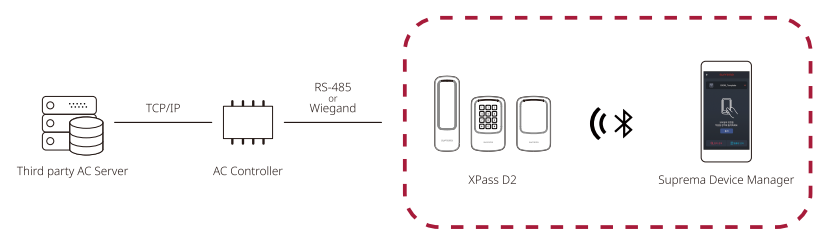
XPass D2 / XPass 2 / XPass 2 V2 / BioEntry W3 / XPass Q2 — Suprema Device Manager

Los administradores pueden conectarse al servidor desde una PC o configurar la red del dispositivo, servidor, comunicación RS-485, formato de tarjeta, ajustes del teclado, PIN, LED y zumbador desde un dispositivo móvil sin desconectarlo físicamente, y también pueden usar funciones como reinicio del dispositivo, actualización de firmware e inicialización de la configuración del dispositivo.

Para XPass D2, los valores configurados una vez pueden guardarse como plantilla para aplicarlos de forma rápida y sencilla a varios dispositivos.

Información

El uso de Suprema Device Manager permite modificar in situ la configuración del XPass D2 integrado con controladoras de terceros.



Requisitos mínimos

Dispositivo móvil

Compruebe si el dispositivo móvil admite comunicación BLE.

- Android 5.0 Lollipop o posterior
- iOS 15 o posterior

Dispositivo y firmware

Verifica los dispositivos y las versiones de firmware compatibles.

- XPass D2 versión del firmware 1.1.0 o posterior

- **XPass 2**
  - XP2-MDPB, XP2-GDPB, XP2-GKDPB: versión de firmware 1.0.0 o posterior
  - XP2-MAPB: versión de firmware 1.4.1 o posterior
  - XP2-MAPB-H: versión de firmware 1.4.3 o posterior
- **XPass 2 V2** versión del firmware 1.0.0 o posterior
- **BioEntry W3** versión del firmware 1.0.1 o posterior
- **XPass Q2** versión del firmware 1.0.0 o posterior

Información

- Los dispositivos y firmware compatibles están sujetos a cambios.
- Si la versión de firmware del dispositivo es inferior a las versiones indicadas anteriormente, actualice el firmware del dispositivo en BioStar X. Cuando el dispositivo se utilice como esclavo, el firmware del maestro conectado también debe ser la versión más reciente compatible con BioStar 2 2.7.0 o posterior.
- Para más detalles sobre cómo actualizar el firmware del dispositivo, consulta Dispositivo IP (Actualizar el firmware del dispositivo), XPass D2 (Actualizar el firmware del dispositivo) o la Guía del administrador de BioStar X.

Configuración Inicial del Dispositivo

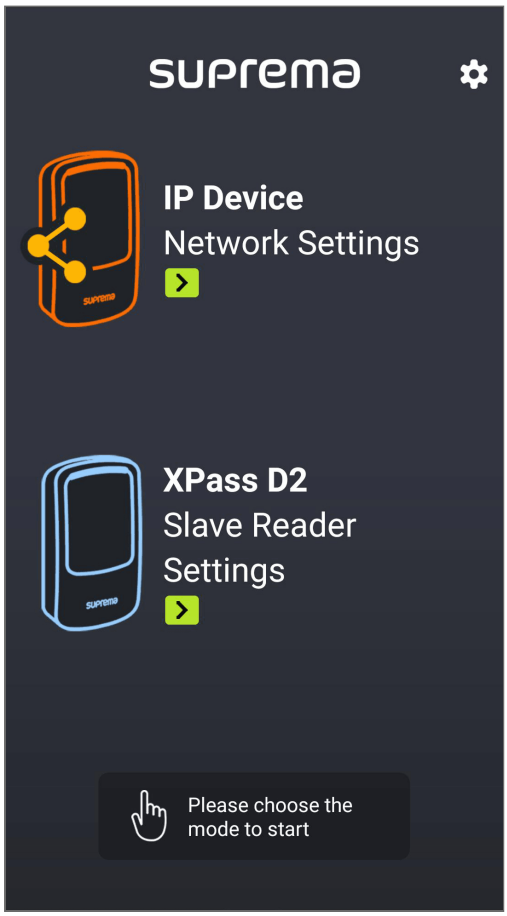
Guía sobre cómo seleccionar un dispositivo y gestionar la configuración de la aplicación.

Seleccionar dispositivo

Seleccione el dispositivo que desea configurar con Suprema Device Manager.

Seleccione un dispositivo IP o XPass D2; las opciones de configuración disponibles varían según el dispositivo seleccionado.

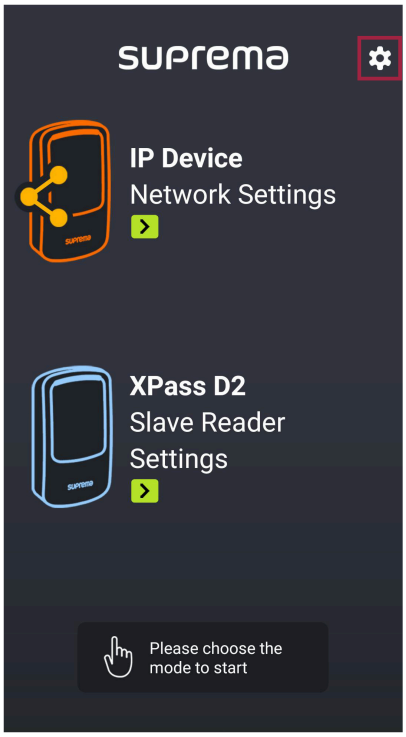
1. Instale la aplicación **Suprema Device Manager** en el dispositivo móvil del administrador. Suprema Device Manager está disponible para descargar en la **App Store** y la **Play Store**.
2. Ejecuta Suprema Device Manager en el dispositivo móvil.
3. Seleccione el dispositivo que desea configurar.

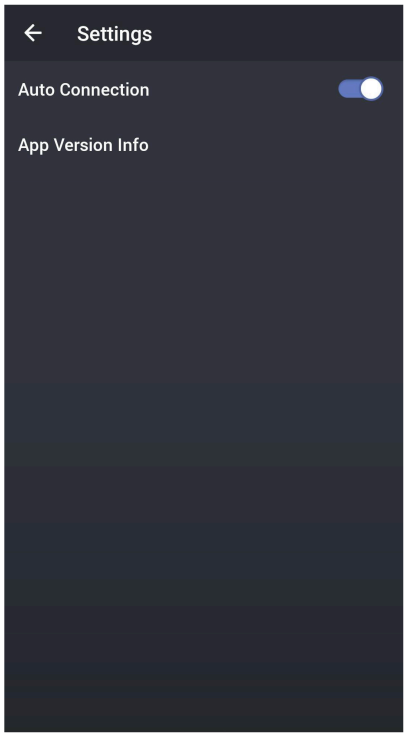


Configurar los ajustes de la aplicación

Configure la función de conexión automática del dispositivo o consulte la información de la versión de la aplicación.

1. Ejecuta Suprema Device Manager en el dispositivo móvil.
2. Seleccione ⚙ en la pantalla principal.





- **Auto Connection**: Active o desactive la función de conexión automática del dispositivo.
- **App Version Info**: Consulte la versión actual de la aplicación y la información de la licencia.

Configurar dispositivo IP

Puede cambiar la configuración del dispositivo IP. Puede cambiar la configuración de forma más rápida y cómoda que al usar el programa de administración en una PC o las tarjetas de comando.

> **Información**
> Es posible que ciertos ajustes no se apliquen si la versión del firmware del dispositivo es antigua. Consulta Actualizar el firmware del dispositivo para aplicar todos los ajustes.

Cambiar configuración del dispositivo

Puede cambiar la configuración de red, del servidor, de RS-485, del LED y del zumbador, y otros ajustes.

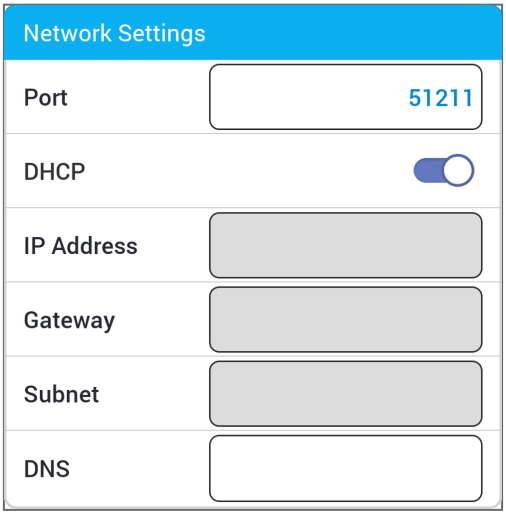
> **Información**
> Los dispositivos biométricos solo admiten las configuraciones de red y servidor.

1. Active el Bluetooth en su dispositivo móvil y ejecute Suprema Device Manager.
2. Seleccione el dispositivo IP desde la pantalla principal.
3. Verifique el ID del dispositivo para seleccionarlo en la lista de dispositivos conectables o acerque el dispositivo móvil al equipo para conectarlo.
4. Después de establecer la contraseña del dispositivo, presione **OK**. Toque  para mostrar la contraseña ingresada.

   > **Información**
   > - La contraseña del dispositivo puede establecerse con una longitud de 6-32 caracteres.
   > - Tenga cuidado de no perder la contraseña del dispositivo. Si pierde la contraseña del dispositivo, deberá inicializar el equipo para poder conectarse a él.

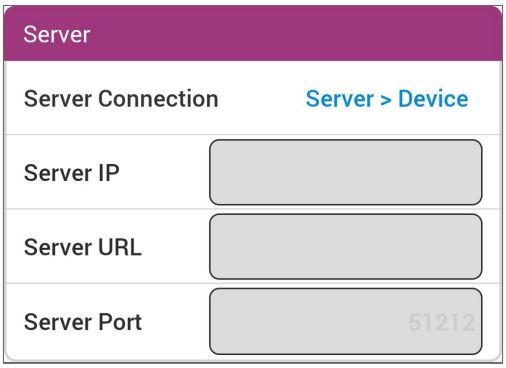
5. Después de configurar cada elemento, presione **Apply Device** para guardar.

Configuración de red



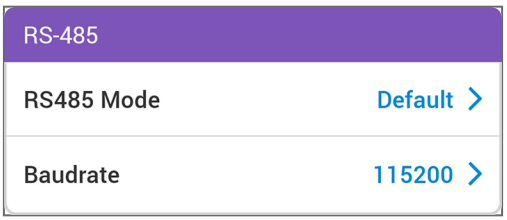
- **Port**: Introduzca el puerto que utilizará el dispositivo.
- **DHCP**: Active esta opción para que el dispositivo use IP dinámica. Si activa esta opción, no podrá introducir la información de red manualmente.
- **IP Address**, **Gateway**, **Subnet**: Introduzca la información de red del dispositivo.
- **DNS**: Introduzca la dirección del servidor DNS.

Servidor



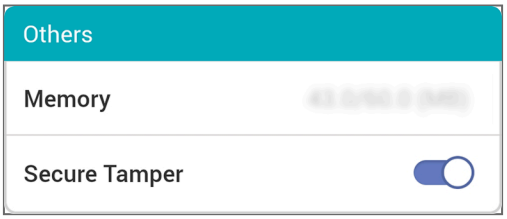
- **Server Connection**: Configure el método de comunicación del servidor. Para buscar y conectar el dispositivo desde el servidor, seleccione **Server > Device**. Para establecer la información del servidor para conectar el dispositivo, seleccione **Device > Server**.
- **Server IP**: Ingrese la dirección IP del servidor.
- **Server URL**: Ingrese el dominio del servidor.
- **Server Port**: Ingrese el puerto del servidor.

RS-485



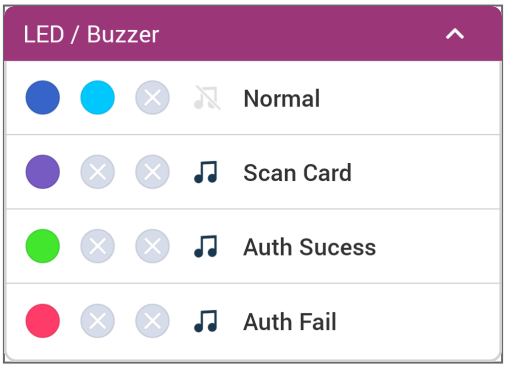
- **RS485 Mode**: Configure el modo RS-485.
- **Baudrate**: Establece la velocidad de transmisión RS-485.

Otros



- **Memory**: Puede verificar el uso de la memoria.
- **Secure Tamper**: Si ocurre un evento de manipulación en el dispositivo, puede configurarse para eliminar toda la información de usuario, los registros y las claves de seguridad almacenadas. Active la función de manipulación de seguridad para utilizarla.

LED / zumbador



- **Normal**: Configure los colores que se mostrarán en el LED del dispositivo durante el funcionamiento normal.
- **Scan Card**: Configure el color que se mostrará en el LED del dispositivo y la cantidad de veces que suena el zumbador al escanear una tarjeta.
- **Auth Sucess**: Configure el color que se mostrará en el LED del dispositivo y la cantidad de veces que suena el zumbador cuando la autenticación es correcta.
- **Auth Fail**: Configure el color que se mostrará en el LED del dispositivo y la cantidad de veces que suena el zumbador cuando la autenticación falla.

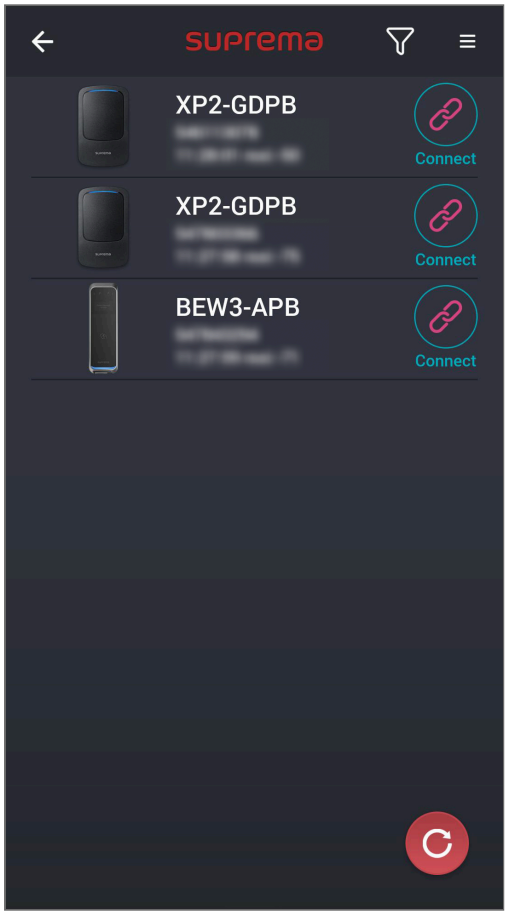
Información

- El LED puede configurarse para mostrar un máximo de tres colores en patrones alternos. Presione la ranura para elegir un color.
- Al seleccionar , se omite la secuencia de color de esa ranura y se muestra el color configurado para la siguiente ranura.

Conectar dispositivo

Puede buscar y conectarse a los dispositivos IP instalados cercanos. Cuando esté conectado a Suprema Device Manager, podrá actualizar el firmware del dispositivo, reiniciarlo, inicializar la configuración, inicializar la configuración del dispositivo excepto la de red, cambiar la contraseña de administrador y usar varias funciones.

1. Active el Bluetooth en su dispositivo móvil y ejecute Suprema Device Manager.
2. Seleccione el dispositivo IP desde la pantalla principal. Aparecerá una lista de dispositivos conectables.



3. Seleccione un dispositivo verificando el ID en la lista de dispositivos o acerque su dispositivo móvil al dispositivo para conectarlo.
4. Ingrese la contraseña de conexión. Toque para mostrar la contraseña ingresada.
5. Presione **OK** para completar la conexión del dispositivo.

Información

Device Filter: En la parte superior de la pantalla de la lista de dispositivos, pulse para mostrar únicamente los dispositivos deseados en la lista.

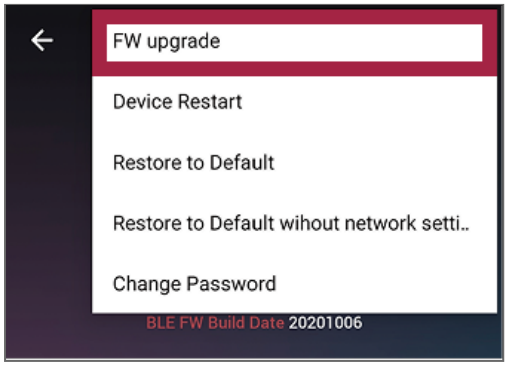
Actualizar el firmware del dispositivo

Actualice fácilmente el firmware del dispositivo.

Información

- Descargue el archivo de firmware en su dispositivo móvil para actualizar el firmware. Puede descargar el firmware más reciente desde el Centro de descargas de Suprema.
- Durante la actualización del firmware, mantenga una distancia menor a 1 m entre el dispositivo y el dispositivo móvil.
- Solo XPass 2 y XPass 2 V2 incluyen soporte para la actualización de firmware.

1. Consulte Conectar dispositivo para conectarse al dispositivo y actualizar el firmware.
2. Toque → **FW upgrade**.

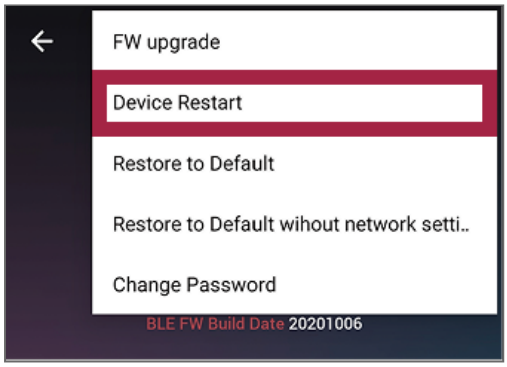


3. Seleccione el firmware desde la ruta donde se guardó el archivo de firmware. La actualización del firmware está en curso.
4. Presione **OK** para completar la actualización del firmware.

Reiniciar dispositivo

Reinicie el dispositivo.

1. Consulte Conectar dispositivo para conectarse al dispositivo y reiniciarlo.
2. Toque → **Device Restart**.

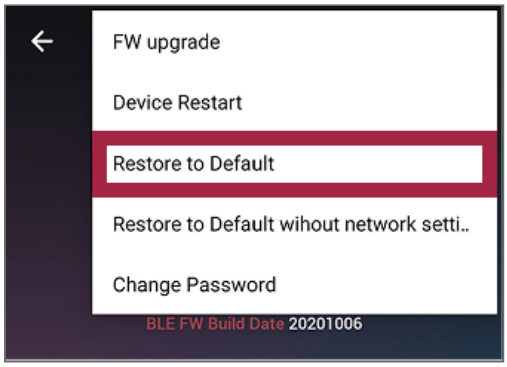


3. Al reiniciar el dispositivo, la conexión de comunicación BLE con el dispositivo móvil se desconectará. Habilite la función **Auto Connection** para reconectar automáticamente. Para obtener instrucciones detalladas de configuración, consulte Configurar los ajustes de la aplicación.

Inicializar la configuración

Puede inicializar la configuración del dispositivo.

1. Consulte Conectar dispositivo para conectarse al dispositivo e inicializar la configuración.
2. Toque ⋮ → **Restore to Default**.

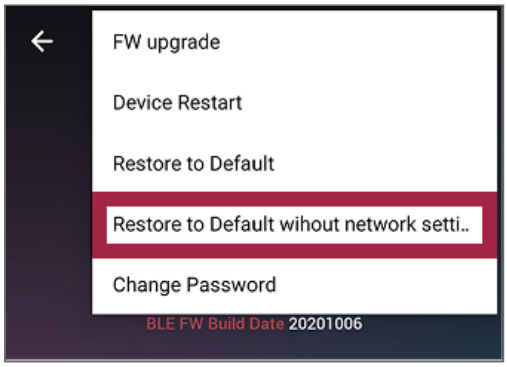


3. Si el dispositivo se inicializa, todos los ajustes se restauran a sus valores predeterminados. Presione **OK** para continuar.

Inicializar la configuración del dispositivo excepto la de red

Puede inicializar la configuración del dispositivo excepto la de red.

1. Consulte Conectar dispositivo para conectarse al dispositivo e inicializar la configuración del dispositivo excepto la de red.
2. Toque ⋮ → **Restore to Default without network settings**.



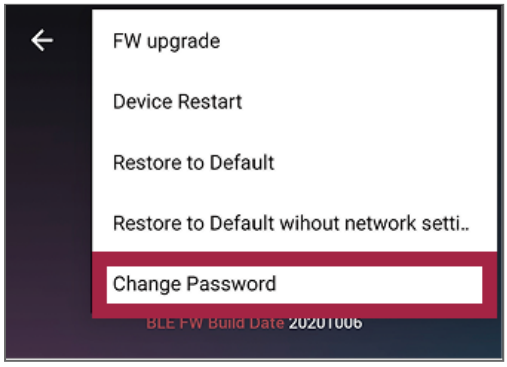
3. Si inicializa la configuración del dispositivo excepto la de red, se inicializarán las demás configuraciones. Presione **OK** para continuar.

Cambiar la contraseña del dispositivo

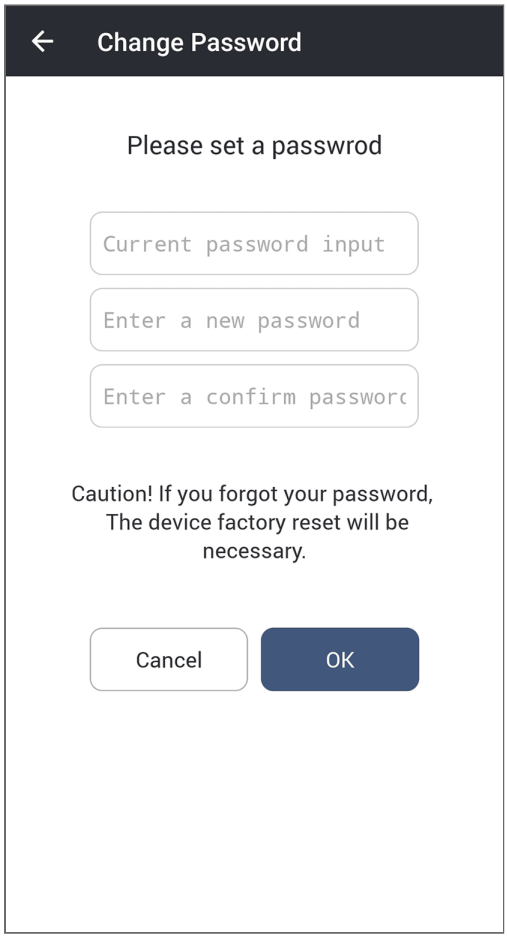
Puede cambiar la contraseña del dispositivo.

1. Consulte Conectar dispositivo para conectarse al dispositivo y cambiar la contraseña.

2. Toque ⋮ → **Change Password**.



3. Ingrese la contraseña actual y la nueva contraseña que utilizará.



4. Presione **OK** para completar el cambio de contraseña.

Información

- La contraseña del dispositivo puede establecerse con una longitud de 6-32 caracteres.
- Tenga cuidado de no perder la contraseña del dispositivo. Si pierde la contraseña del dispositivo, deberá inicializar el equipo para poder conectarse a él.

Configurar XPass D2

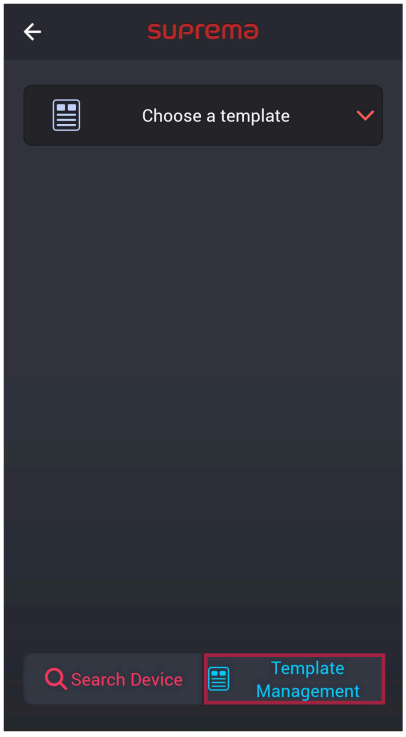
Configura ajustes para aplicar a XPass D2 como plantilla y aplícalos directamente a dispositivos individuales. Aplica los ajustes mucho más rápido que al acceder al programa de gestión en un PC o usar tarjetas de comando.

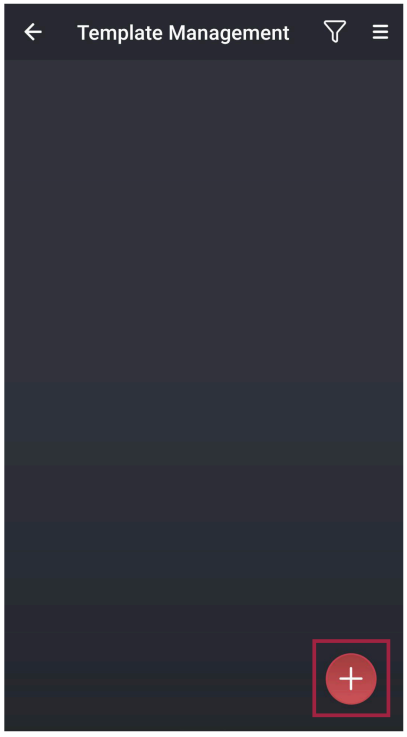
> **Información**
> Es posible que ciertos ajustes no se apliquen si la versión del firmware del dispositivo es antigua. Para aplicar todos los ajustes, actualice el firmware. Consulte Actualizar el firmware del dispositivo.

Agregar plantilla

Configura la comunicación RS-485, el formato de tarjeta, los ajustes del teclado, el PIN, el LED y el zumbador antes de agregarlos como plantilla. Agregar una plantilla permite aplicar ajustes de forma rápida y sencilla sin configurar cada dispositivo individual cada vez.

1. Ejecuta Suprema Device Manager en el dispositivo móvil.
2. Selecciona XPass D2 en la pantalla principal.
3. Toca **Template Management** → (+).





4. Selecciona el modelo de dispositivo para el que deseas crear la plantilla.
5. Después de configurar cada elemento, toca **Save** para guardar la plantilla.

> **Información**
> Se pueden agregar hasta 100 plantillas.

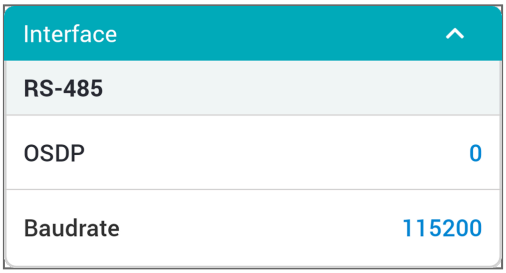
Establecer nombre de plantilla y contraseña de administrador



- **Template Name**: Ingresa el nombre de plantilla deseado.
- **Admin Password**: Ingresa la contraseña de administrador.

> **Información**
>
> - La contraseña de administrador puede tener de 6 a 32 dígitos.
> - Ten cuidado de no perder la contraseña de administrador. Si pierdes la contraseña de administrador, será necesario inicializar el dispositivo para conectarte al dispositivo con la plantilla aplicada.
> - Para obtener más información sobre cómo cambiar la contraseña de administrador, consulta Cambiar contraseña de administrador.

Interfaz



- **OSDP**: Establece la dirección OSDP que se utilizará en la comunicación entre el dispositivo y el dispositivo maestro. Se puede configurar con números del 0 al 126.
- **Baudrate**: Establece la velocidad de transmisión RS-485.

Autenticación

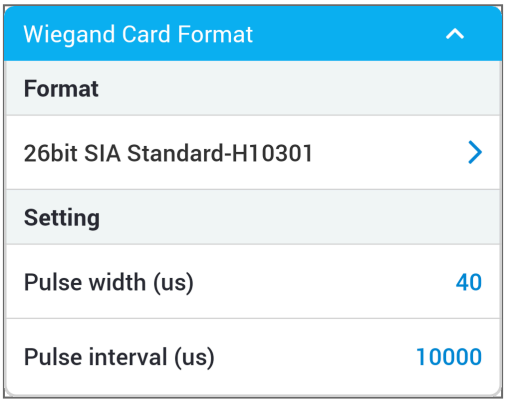


- **Card Type**: Configura el tipo de tarjeta que usará el dispositivo.
  - **CSN Card**: Selecciona el tipo de tarjeta CSN y establece el orden de bytes.
  - **Suprema Smart Card**: Selecciona los tipos de tarjetas inteligentes emitidas por Suprema.
  - **Custom Smart Card**: Selecciona los tipos de tarjetas inteligentes emitidas por terceros.
  - **Mobile**: Configura el tipo de tarjeta móvil.

Información

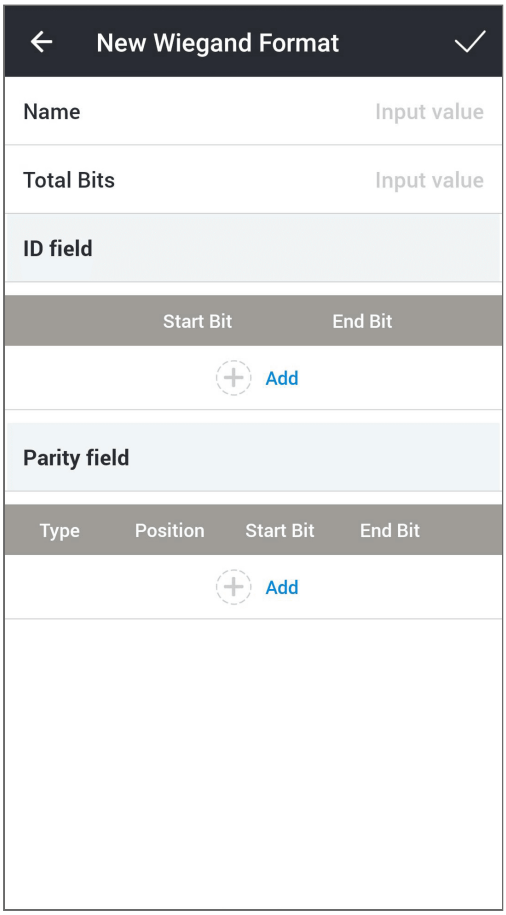
Cuando se establece en **MSB**, los datos de la tarjeta se procesan de izquierda a derecha, procesando secuencialmente del byte más grande al más pequeño al guardar el número de serie de la tarjeta (CSN). **LSB** procesa el número de serie de la tarjeta (CSN) del byte más pequeño al más grande al guardarlo.

Formato Tarjeta Wiegand



- **Format**: Establece el formato de tarjeta Wiegand que se especificará para el dispositivo. Los datos de la tarjeta se procesan según el formato establecido.

- **New Wiegand Format**: Si el formato deseado no está disponible, toca + para agregar un nuevo formato Wiegand.

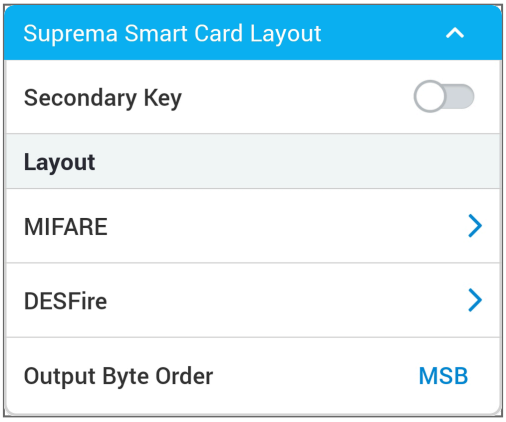


  - **Name**: Ingresa el nombre del formato Wiegand deseado.
  - **Total Bits**: Ingresa el número total de bits.
  - **ID field**: Ingresa los bits inicial y final del ID que deseas usar. Toca ⊕ **Add** para agregar un campo de ID.
  - **Parity field**: Ingresa la posición del campo de paridad y los bits inicial y final que deseas usar. Toca ⊕ **Add** para agregar un campo de paridad.

    > **Información**
    > Para agregar un campo de paridad, ingresa el número total de bits.

- **Pulse width (µs)**: Configura el ancho de pulso de la señal Wiegand.
- **Pulse interval (µs)**: Configura el intervalo de pulso de la señal Wiegand.

Diseño de Tarjeta Inteligente Suprema

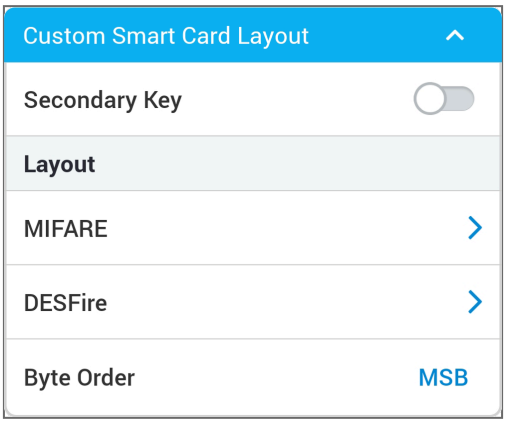


- **Secondary Key**: Define si se utilizará la clave de sitio auxiliar. Al establecer la clave de sitio auxiliar, se puede usar para la autenticación cuando la clave principal de la tarjeta no coincide.
- **MIFARE**: Configura tarjetas MIFARE.
  - **Security Level**: Puedes configurar el tipo de cifrado en SL1 o SL3.
  - **Primary Key**: Clave que cifra la comunicación entre las tarjetas inteligentes y el dispositivo.
  - **Secondary Key**: Úsala para autenticar cuando la clave principal de sitio de la tarjeta no coincide. El campo de clave de sitio auxiliar solo se muestra cuando **Secondary Key** del nivel anterior está activado.
  - **Start Block Index**: Selecciona el bloque inicial donde se almacenará cada plantilla. Este bloque es el índice del bloque donde se almacena la información del usuario; configúrelo en un bloque almacenable si el usuario ya usa la tarjeta inteligente. Solo se puede configurar para MIFARE.
- **DESFire**: Configura tarjetas DESFire.
  - **DESFire Advanced**: Utiliza tarjetas DESFire emitidas por terceros. Solo se puede configurar DESFire.
  - **Primary Key**: Clave que cifra la comunicación entre las tarjetas inteligentes y el dispositivo.
  - **Secondary Key**: Úsala para autenticar cuando la clave principal de sitio de la tarjeta no coincide. El campo de clave de sitio auxiliar solo se muestra cuando **Secondary Key** del nivel anterior está activado.
  - **App ID**: Establece el ID de aplicación. Funciona como una especie de directorio que incluye un ID de archivo. Solo se puede configurar DESFire.
  - **File ID**: Establece el ID de archivo. Solo se puede configurar DESFire.
  - **Encryption Type**: Configura el tipo de cifrado en DES/3DES o AES.
  - **Enforce EV2/EV3 Secure Messaging**: Habilite esta opción para forzar mensajería segura al autenticarse en el dispositivo con tarjetas DESFire EV2 o EV3. Solo puede activarse cuando **Encryption Type** está configurado como AES.
- **Output Byte Order**: Configure el orden de bytes para la salida de tarjeta inteligente.

Información

- Ingrese correctamente la información de **App Master Key**, **App Master Key Index**, **File Read Access Key**, **File Read Access Key Index**, **App ID**, **File ID**, **Encryption Type** para utilizar **DESFire Advanced**.
- **App Master Key**, **File Read Access Key** solo aceptan hasta 32 bytes en hexadecimal.
- Cuando se establece en **MSB**, los datos de la tarjeta se procesan de izquierda a derecha, procesando secuencialmente del byte más grande al más pequeño al guardar el número de serie de la tarjeta (CSN). **LSB** procesa el número de serie de la tarjeta (CSN) del byte más pequeño al más grande al guardarlo.

Diseño de Tarjeta Inteligente Personalizada

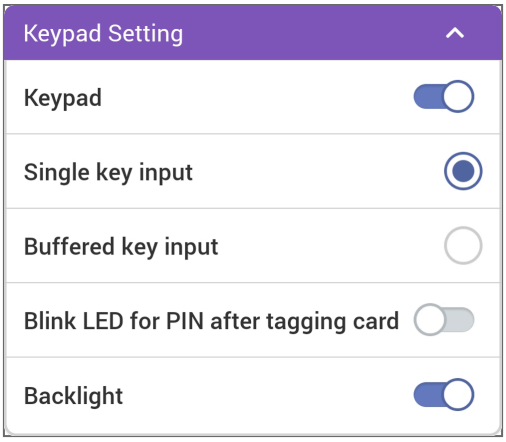


- **Secondary Key**: Define si se utilizará la clave de sitio auxiliar. Al establecer la clave de sitio auxiliar, se puede usar para la autenticación cuando la clave principal de la tarjeta no coincide.
- **MIFARE**: Configura tarjetas MIFARE.
  - **Security Level**: Puedes configurar el tipo de cifrado en SL1 o SL3.
  - **Primary Key**: Clave que cifra la comunicación entre las tarjetas inteligentes y el dispositivo.
  - **Secondary Key**: Úsala para autenticar cuando la clave principal de sitio de la tarjeta no coincide. El campo de clave de sitio auxiliar solo se muestra cuando **Secondary Key** del nivel anterior está activado.
  - **Block Index**: Seleccione el bloque inicial donde se almacenará cada plantilla. Este bloque es el índice del bloque donde se almacena la información del usuario; configúrelo en un bloque almacenable si el usuario ya usa la tarjeta inteligente. Solo se puede configurar para MIFARE.
  - **Skip Bytes**: Configure el punto de inicio para leer el número de tarjeta.
  - **Data Size**: Configure el tamaño de los datos que se leerán de la tarjeta (si los valores establecidos de **Primary Key** y **Secondary Key** son iguales a los de la tarjeta).
- **DESFire**: Configura tarjetas DESFire.
  - **DESFire Advanced**: Utiliza tarjetas DESFire emitidas por terceros. Solo se puede configurar DESFire.
  - **Primary Key**: Clave que cifra la comunicación entre las tarjetas inteligentes y el dispositivo.
  - **Secondary Key**: Úsala para autenticar cuando la clave principal de sitio de la tarjeta no coincide. El campo de clave de sitio auxiliar solo se muestra cuando **Secondary Key** del nivel anterior está activado.

  - **App ID**: Establece el ID de aplicación. Funciona como una especie de directorio que incluye un ID de archivo. Solo se puede configurar DESFire.
  - **File ID**: Establece el ID de archivo. Solo se puede configurar DESFire.
  - **Encryption Type**: Configura el tipo de cifrado en DES/3DES o AES.
  - **Skip Bytes**: Configure el punto de inicio para leer el número de tarjeta.
  - **Data Size**: Configure el tamaño de los datos que se leerán de la tarjeta (si los valores establecidos de **Primary Key** y **Secondary Key** son iguales a los de la tarjeta).
  - **Enforce EV2/EV3 Secure Messaging**: Habilite esta opción para forzar mensajería segura al autenticarse en el dispositivo con tarjetas DESFire EV2 o EV3. Solo puede activarse cuando **Encryption Type** está configurado como AES.
- **Byte Order**: Configure el orden de bytes para la salida de tarjeta inteligente.

> **Información**
>
> - Ingrese correctamente la información de **App Master Key**, **App Master Key Index**, **File Read Access Key**, **File Read Access Key Index**, **App ID**, **File ID**, **Encryption Type** para utilizar **DESFire Advanced**.
> - **App Master Key**, **File Read Access Key** solo aceptan hasta 32 bytes en hexadecimal.
> - Cuando se establece en **MSB**, los datos de la tarjeta se procesan de izquierda a derecha, procesando secuencialmente del byte más grande al más pequeño al guardar el número de serie de la tarjeta (CSN). **LSB** procesa el número de serie de la tarjeta (CSN) del byte más pequeño al más grande al guardarlo.

Configuración del teclado



- **Keypad**: Configure si se utilizará el teclado. Cuando el teclado está activado, autentíquese ingresando el ID de la tarjeta con el teclado.
- **Single key input**: Envía el valor cada vez que se presiona una tecla al ingresar el ID de la tarjeta en el teclado.
- **Buffered key input**: Al ingresar el ID de la tarjeta en el teclado, presione todas las teclas necesarias y luego presione la tecla `#` para enviar todo el valor de una vez.
- **Blink LED for PIN after tagging card**: Cuando el modo de autenticación del dispositivo está configurado en tarjeta + PIN, al presentar la tarjeta se activa el LED para solicitar al usuario que ingrese el PIN.
- **Backlight**: Encienda o apague la retroiluminación del teclado.

Información

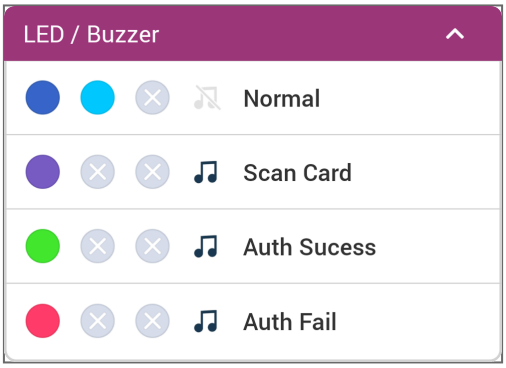
- **Keypad Setting** solo se muestra en la pantalla de configuración de plantillas del dispositivo XPD2-GKDB.
- **Backlight** solo es compatible con el hardware XPD2-GKDB V02M y la versión de firmware v1.7.1 o superior.
- Los valores ingresados mediante el teclado se transmiten en unidades de 4 bits de forma predeterminada. Los ID de tarjetas ingresados mediante el teclado se envían en el mismo formato que el formato de tarjeta Wiegand.

Otros



- **Secure Tamper**: Configure para que, cuando se produzca un evento de manipulación en el dispositivo, la clave de seguridad almacenada en el dispositivo se elimine. Active la función de manipulación de seguridad para utilizarla.

LED / zumbador



- **Normal**: Configure los colores que se mostrarán en el LED del dispositivo durante el funcionamiento normal.
- **Scan Card**: Configure el color que se mostrará en el LED del dispositivo y la cantidad de veces que suena el zumbador al escanear una tarjeta.
- **Auth Sucess**: Configure el color que se mostrará en el LED del dispositivo y la cantidad de veces que suena el zumbador cuando la autenticación es correcta.
- **Auth Fail**: Configure el color que se mostrará en el LED del dispositivo y la cantidad de veces que suena el zumbador cuando la autenticación falla.

Información

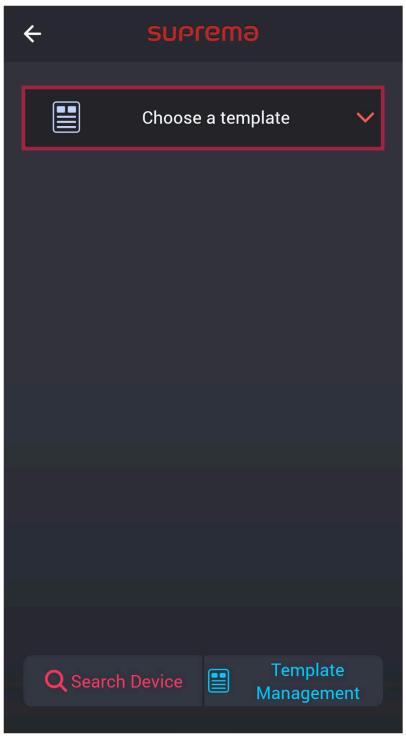
- El LED puede configurarse para mostrar un máximo de tres colores en patrones alternos. Presione la ranura para elegir un color.
- Al seleccionar , se omite la secuencia de color de esa ranura y se muestra el color configurado para la siguiente ranura.

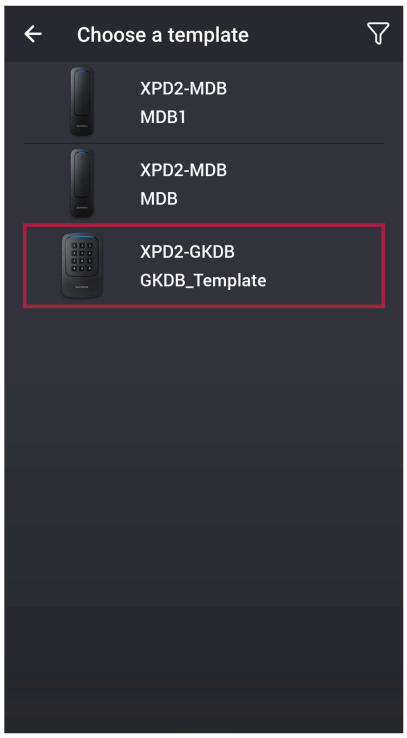
Aplicar plantilla

Las plantillas añadidas pueden aplicarse de manera uniforme a varios dispositivos mediante comunicación BLE.

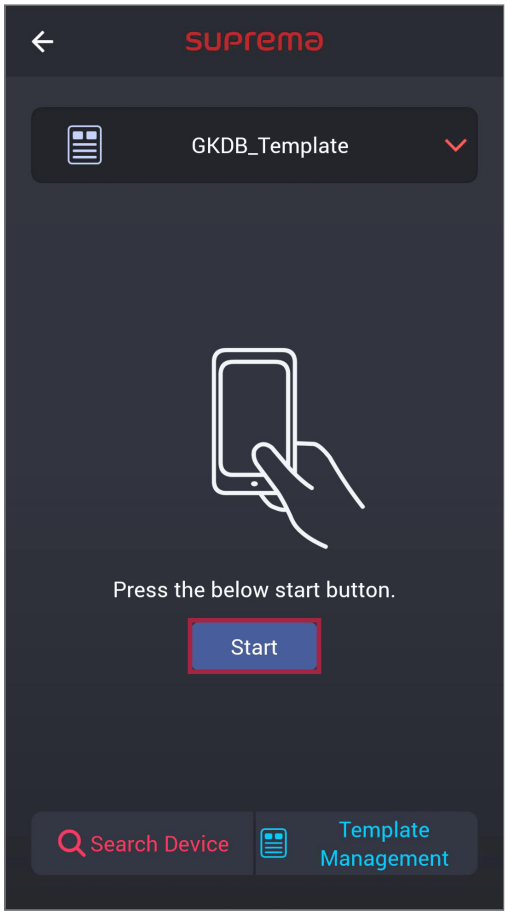
> **Información**
> Es posible que ciertos ajustes no se apliquen si la versión del firmware del dispositivo es antigua. Para aplicar todos los ajustes, actualice el firmware. Consulte Actualizar el firmware del dispositivo.

1. Active el Bluetooth en su dispositivo móvil y ejecute Suprema Device Manager.
2. Selecciona XPass D2 en la pantalla principal.
3. Haga clic en **Choose a template**. Aparecerá una lista de plantillas disponibles.





4. Seleccione la plantilla deseada de la lista de plantillas.
5. Haga clic en **Start** para continuar.



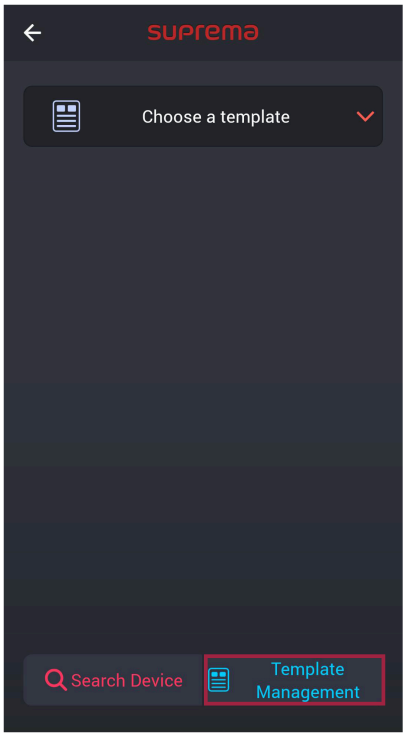
6. Asegúrese de que la parte posterior de su dispositivo móvil toque el dispositivo al que desea aplicar la plantilla.
7. Una vez completada la aplicación de la plantilla, haga clic en **OK**.

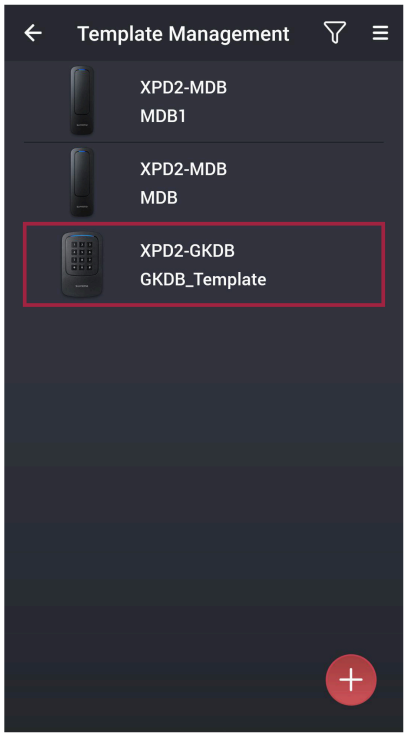
> **Información**
>
> - Los ajustes modificados mediante Suprema Device Manager solo se aplican al dispositivo y no se sincronizarán con el servidor.
> - Si el dispositivo está conectado al dispositivo maestro o si la configuración de salida Wiegand ha cambiado, no se puede conectar a Suprema Device Manager con la clave principal. Inicialice el dispositivo para conectarlo con Suprema Device Manager.

Gestionar plantillas

Editar plantilla

1. Ejecuta Suprema Device Manager en el dispositivo móvil.
2. Selecciona XPass D2 en la pantalla principal.
3. Haga clic en **Template Management**.

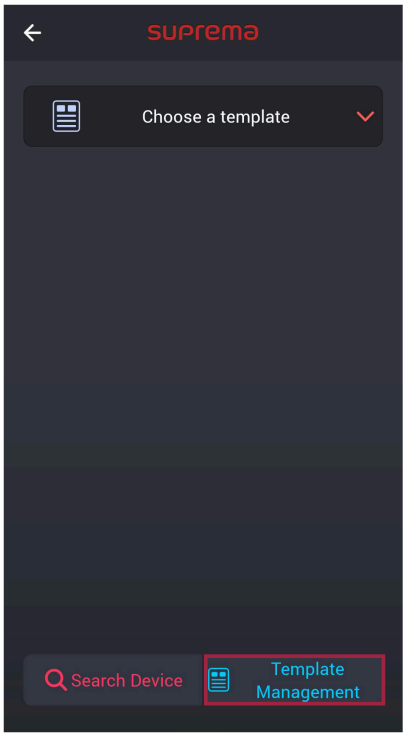


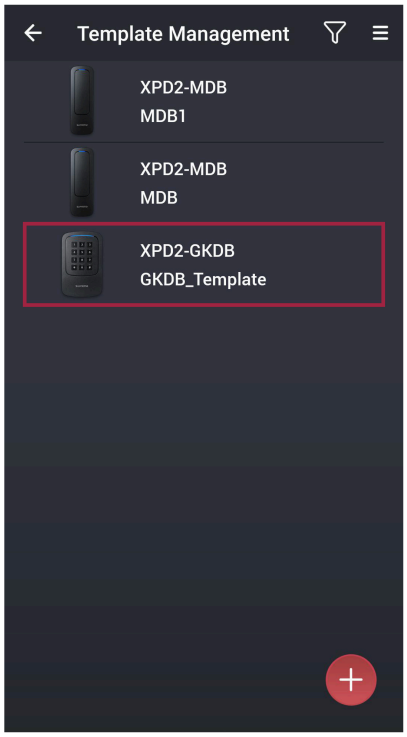


4. Seleccione la plantilla que desea editar de la lista de plantillas.
5. Consulte Agregar plantilla para editar la plantilla.
6. Para guardar los ajustes modificados, haga clic en **Save**; para guardarlos como una nueva plantilla, haga clic en **Save as new template**.

Eliminar plantilla

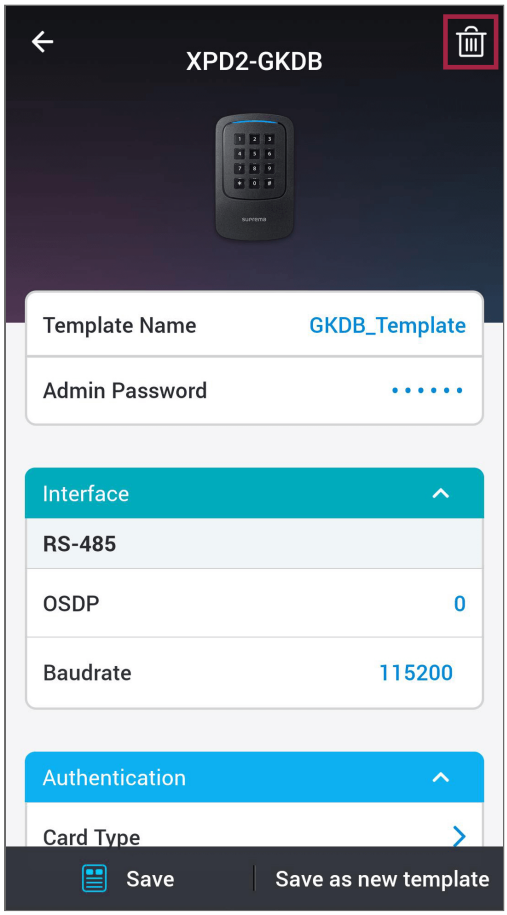
1. Ejecuta Suprema Device Manager en el dispositivo móvil.
2. Selecciona XPass D2 en la pantalla principal.
3. Haga clic en **Template Management**.





4. Seleccione la plantilla que desea eliminar de la lista de plantillas.

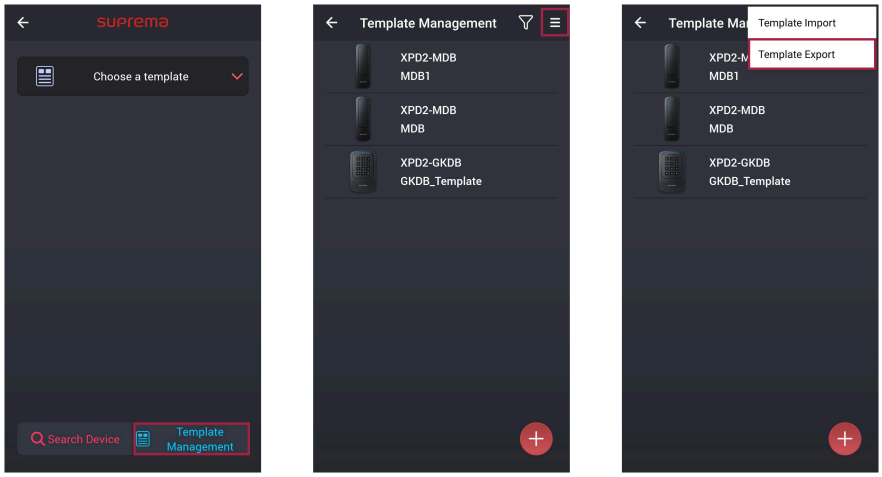
5. Toque → **OK** para eliminar una plantilla.



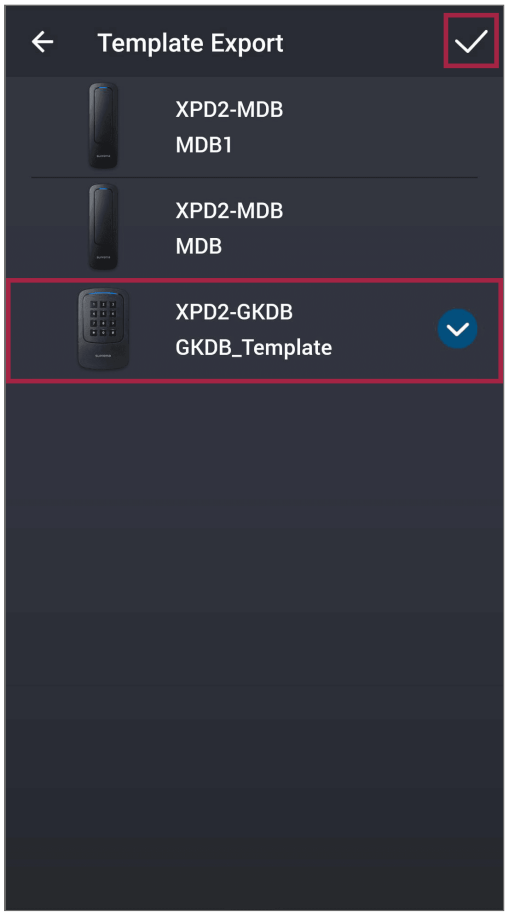
Exportar plantilla

Exporte plantillas para la configuración de XPass D2 desde la aplicación.

1. Ejecuta Suprema Device Manager en el dispositivo móvil.
2. Selecciona XPass D2 en la pantalla principal.
3. Haga clic en **Template Management**.



4. En la parte superior de la lista de plantillas, toque ☰ y seleccione **Template Export**.
5. Después de seleccionar la plantilla para exportar, toque ✓.

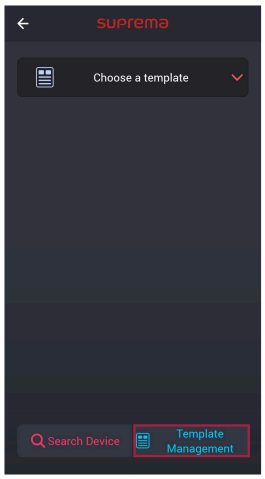


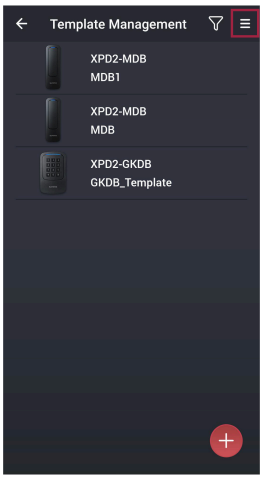
> **Información**
> Los archivos de plantilla se guardan en la siguiente carpeta de su dispositivo móvil.
> - **Android**: Download → DeviceManager_TemplateFiles
> - **iOS**: Device

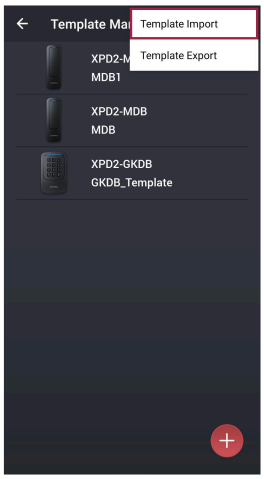
Importar plantilla

Importe plantillas para la configuración de XPass D2 en la aplicación.

1. Ejecuta Suprema Device Manager en el dispositivo móvil.
2. Selecciona XPass D2 en la pantalla principal.
3. Haga clic en **Template Management**.







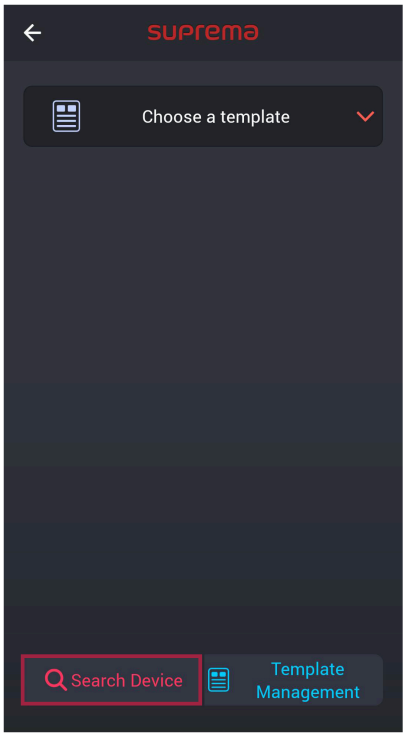
4. En la parte superior de la lista de plantillas, toque ☰ y seleccione **Template Import**.
5. Seleccione la plantilla que desea importar de la carpeta donde se almacenan las plantillas.

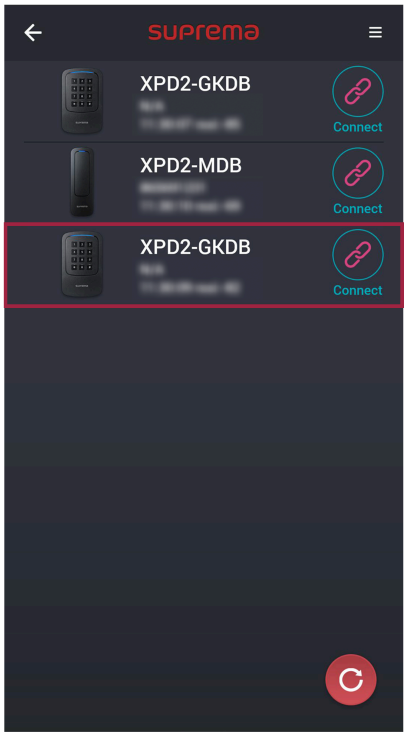
> **Información**
> Los archivos de plantilla se guardan en la siguiente carpeta de su dispositivo móvil.
> - **Android**: Download → DeviceManager_TemplateFiles
> - **iOS**: Device

Buscar y conectar dispositivo

Busque y conéctese a los XPass D2 instalados cercanos. Conéctese a Suprema Device Manager para actualizar el firmware del dispositivo o utilizar funciones como reiniciar el dispositivo o cambiar la contraseña de la plantilla.

1. Active el Bluetooth en su dispositivo móvil y ejecute Suprema Device Manager.
2. Selecciona XPass D2 en la pantalla principal.
3. Haga clic en **Search Device**. Aparecerá una lista de dispositivos conectables.





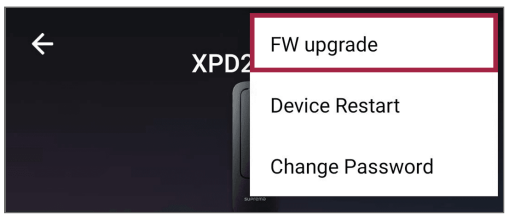
4. Seleccione un dispositivo verificando el ID en la lista de dispositivos o acerque su dispositivo móvil al dispositivo para conectarlo.
5. Ingrese la contraseña de conexión. Toque para mostrar la contraseña ingresada.
6. Presione **OK** para completar la conexión del dispositivo.

Actualizar el firmware del dispositivo

Actualice fácilmente el firmware del dispositivo.

> **Información**
>
> - Descargue el archivo de firmware en su dispositivo móvil para actualizar el firmware. Puede descargar el firmware más reciente desde el Centro de descargas de Suprema.
> - Durante la actualización del firmware, mantenga una distancia menor a 1 m entre el dispositivo y el dispositivo móvil.

1. Consulte Buscar y conectar dispositivo para conectar el dispositivo al que desea actualizar el firmware.
2. Toque → **FW upgrade**.



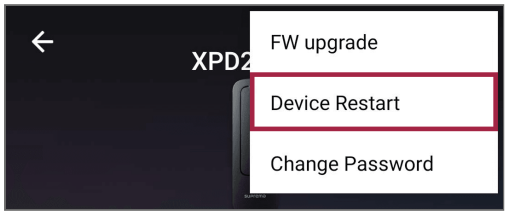
3. Seleccione el firmware desde la ruta donde se guardó el archivo de firmware. La actualización del firmware está en curso.

4. Presione **OK** para completar la actualización del firmware.

Reiniciar dispositivo

Reinicie el dispositivo.

1. Consulte Buscar y conectar dispositivo para conectar el dispositivo que desea reiniciar.
2. Toque ⋮ → **Device Restart**.

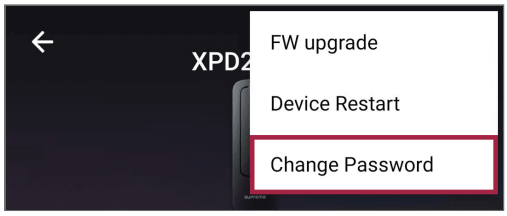


3. Al reiniciar el dispositivo, la conexión de comunicación BLE con el dispositivo móvil se desconectará. Habilite la función **Auto Connection** para reconectar automáticamente. Para obtener instrucciones detalladas de configuración, consulte Configurar los ajustes de la aplicación.

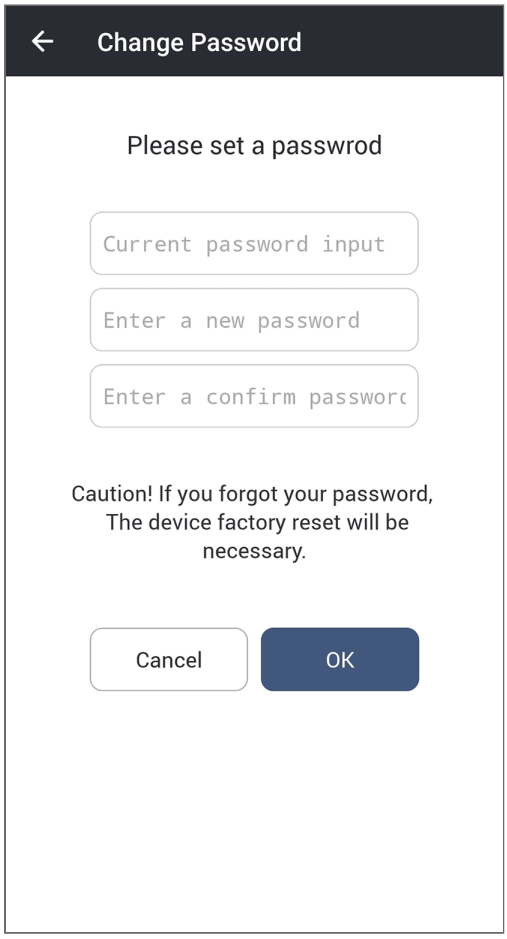
Cambiar contraseña de administrador

Cambie la contraseña de administrador de la plantilla.

1. Consulte Buscar y conectar dispositivo para conectar el dispositivo con la plantilla en la que desea cambiar la contraseña.
2. Toque ⋮ → **Change Password**.



3. Ingrese la contraseña actual y la nueva contraseña que utilizará.



4. Presione **OK** para completar el cambio de contraseña.

Información

- La contraseña de administrador puede tener de 6 a 32 dígitos.
- Ten cuidado de no perder la contraseña de administrador. Si pierdes la contraseña de administrador, será necesario inicializar el dispositivo para conectarte al dispositivo con la plantilla aplicada.

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

- Este producto contiene software de código abierto. El código fuente sujeto a las licencias GPL, LGPL, MPL y otras licencias de código abierto que requieren la distribución del código fuente puede solicitarse al Equipo de Soporte Técnico de Suprema.
- El código fuente de este producto puede solicitarse al Equipo de Soporte Técnico de Suprema durante 3 años a partir de la fecha de entrega final del producto.
- Si desea obtener el código fuente en un medio físico, podría cobrarse el costo de dicha distribución. Esta oferta es válida para cualquier persona que reciba esta información.
- Para más información sobre las licencias de Android e iOS incluidas en este producto, consulte Android y iOS.

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.