Suprema Device Manager

USER GUIDE

suprema
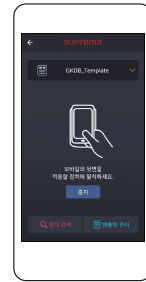SECURITY & BIOMETRICS

CONTENTS

Getting Started

Introduction

The Device Manager is a mobile application that can set XPass D2, XPass 2, and BioEntry W3 of Suprema using BLE connection.
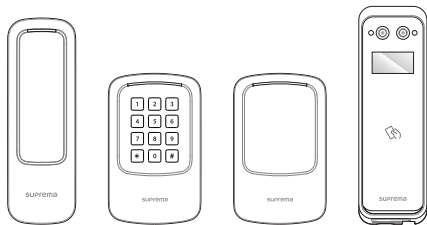
XPass D2 / XPass 2 / BioEntry W3   Suprema Device Manager

This application eliminates the need for administrators to access the server on the PC or physically disconnect the device. You can set the network, server, RS-485 connection, card format, keypad setting, PIN, LED and buzzer of the device directly from mobile device, and you can use additional functions such as device restart or firmware upgrade.

In addition, you can save the set values as a template and apply quickly and easily to multiple devices.

Device Manager allows you to instantly set the XPass D2 configured with 3rd party controllers in the field.

TCP/IP

RS-485
or
Wiegand

Third party AC Server   AC Controller   XPass D2   Suprema Device Manager
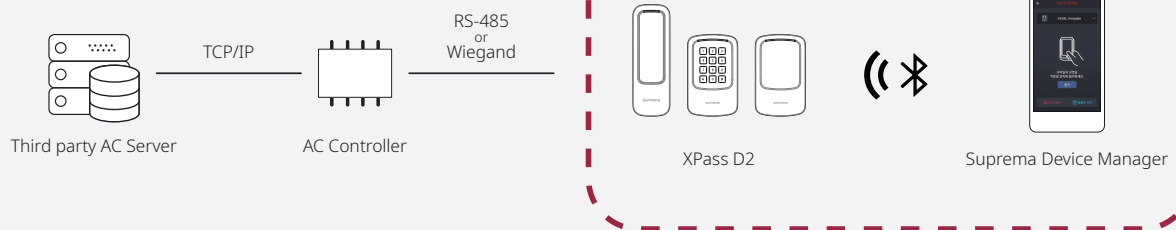
Minimum Requirements

Mobile Device

Check whether your mobile device supports BLE connection.

- Android 5.0 Lollipop OS or later
- iOS 9.0 or later

Device and Firmware

Check the compatible device and firmware version.

- XPass D2 FW 1.1.0 or later
- XPass 2
    - XP2-MDPB, XP2-GDPB, XP2-GKDPB: FW 1.0.0 or later
    - XP2-MAPB: FW 1.4.1 or later
- BioEntry W3 FW 1.0.1 or later

> - Compatible devices and firmware are subject to change.
> - If the firmware of the device is lower than the version in the above list, upgrade the firmware from BioStar 2. If you are using the device as a slave, the firmware of the connected master device must also be the latest version compatible with BioStar 2.7.0 or later.
> - For detailed contents regarding upgrading the device firmware, refer to the IP Device (Upgrading Firmware), XPass D2 (Upgrading Firmware), or the BioStar 2 Administrator Guide.
> - For more information about the devices, refer to the Suprema's home page (www.supremainc.com).

Selecting the Device

Choose the model to set up by Suprema Device Manager.

You can choose IP Device or XPass D2, and the items that can be set vary depending on the model you choose.

1   Download the **Supreme Device Manager** application to the mobile device. You can download the application from the **App Store** and **Play Store**.

2   Run Suprema Device Manager on your mobile device.

3   Select the model you want to set up.

4
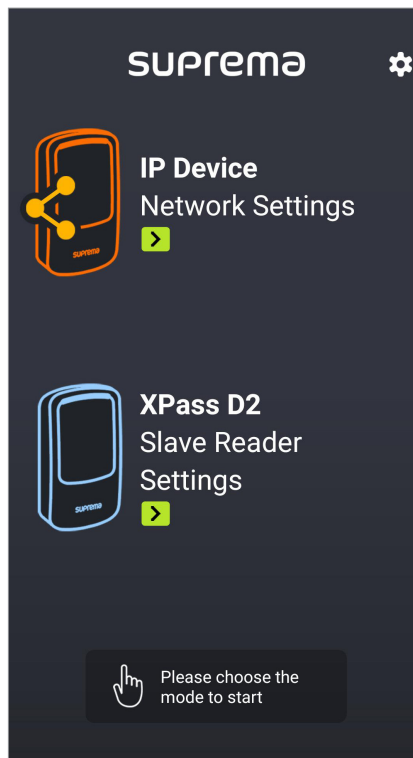
Setting the App

The device auto connection feature can be set, and the app version information can be checked.

1 Run Suprema Device Manager on your mobile device.

2 Select the ✿ on the main screen.
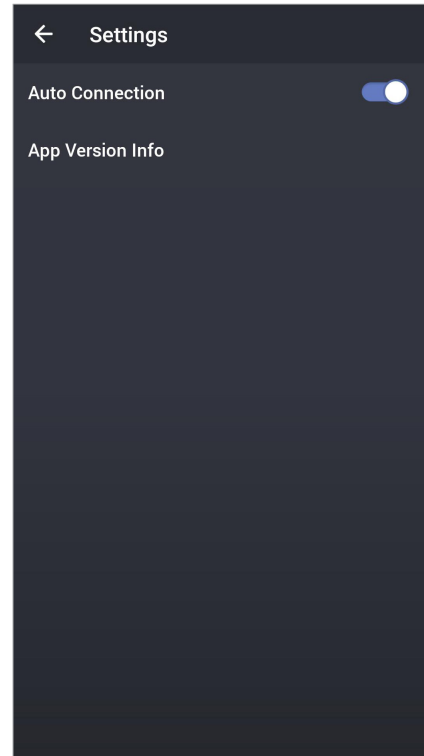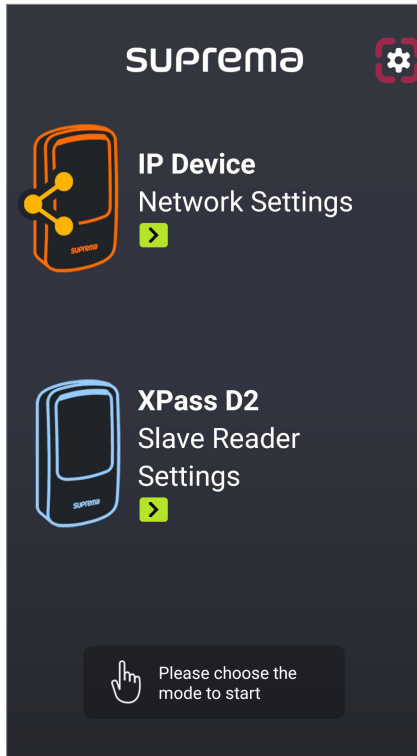
- **Auto Connection**: Enable or disable the device auto connection feature.
- **App Version Info**: Check the current version of the app and license information.

Setting the IP Device

You can change the settings of IP Device in the Suprema Device Manager. It is possible to apply the device setting much faster than setting the management program from the PC or using the command card.

> ℹ️ If the firmware version of the device is low, some settings may not be applied to the device. To apply the all settings, upgrade the firmware by referring to the Upgrading Firmware.

Changing the Settings

You can change the Network, Server, RS-485, LED / Buzzer and other settings.

> ℹ️ Biometric device only supports network and server settings.

1 Activate Bluetooth on your mobile device and run Suprema Device Manager.

2 Select IP Device on the main screen.

3 Check the device ID in the list of connectable devices and select the device. Or place your mobile device close to the device which you want to connect.

4 Set the device password and tap **OK**. Tap 👁️ to display the entered password on the screen.

> ℹ️ • The device password can be set from 6 to 32 characters.
> • Be careful not to forget the device password. If you forgot the device password, the device factory reset will be necessary to connect to the device.

5 Edit the necessary items in the **Network** tab.

Network Settings	
Port	51211
DHCP	🔵
IP Address	
Gateway	
Subnet	
DNS	

- **Port**: Enter a port to be used by the device.
- **DHCP**: Select this option to allow the device to use a dynamic IP address. If this option is selected, network settings cannot be entered.
- **IP Address**, **Gateway**, **Subnet**: Enter network settings of the device.
- **DNS**: Enter a DNS server address.

6

6 Edit the necessary items in the **Server** tab.

Server	
Server Connection	Server > Device
Server IP	
Server URL	
Server Port	51212

- **Server Connection**: You can set the server communication method. Select **Server** > **Device** to search and connect devices on the server. To enter the server information directly on the device and connect to the server, select **Device** > **Server**.

- **Server IP**: Enter the IP address of the BioStar 2.

- **Server URL**: Enter the domain name of the BioStar 2.

- **Server Port**: Enter the port number of the BioStar 2 server.

7 Edit the necessary items in the **RS-485** tab.

| RS-485	
RS485 Mode	Default ❭
Baudrate	115200 ❭

- **RS485 Mode**: Set the RS-485 mode.

- **Baudrate**: Set a baud rate of the RS-485 connection.

8 Edit the necessary items in the **Others** tab.

Others	
Memory	43.0/60.0 (MB)
Secure Tamper	◯

- **Memory**: View the status of memory usage.

- **Secure Tamper**: If a tamper event occurs on the device, you can set to delete the entire user information, the entire log, and the security key stored on the device. To use the secure tamper, enable this option.

9 Edit the necessary items in the **LED / Buzzer** tab.
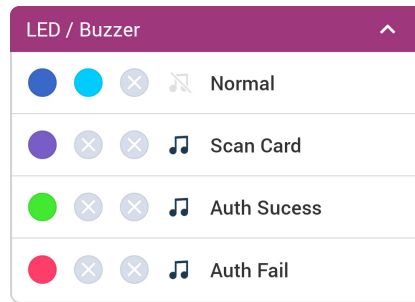
LED / Buzzer	^
🔵 🔵 ⊗ 🎵̸	Normal
🟣 ⊗ ⊗ 🎵	Scan Card
🟢 ⊗ ⊗ 🎵	Auth Sucess
🔴 ⊗ ⊗ 🎵	Auth Fail

- **Normal**: You can set the color that is normally displayed on the device LED.

- **Scan Card**: You can set the LED color and the number of times the Buzzer plays when scanning the card to the device.

- **Auth Sucess**: You can set the LED color and the number of times the Buzzer plays when the authentication is successful.

- **Auth Fail**: You can set the LED color and the number of times the Buzzer plays when the authentication is failed.

> ℹ️ You can set the LED to display repeatedly up to three colors. Tap the slot to select a color.
> If you select ⊗, that slot is skipped and the color of next slot is displayed.

10 To save the template settings, tap **Apply Device**.

Connecting the Device

The Suprema Device Manager allows you to search for and connect Suprema's access control and time & attendance devices installed nearby. If you connect to the Device Manager, you can use various functions such as upgrading the firmware of the device, restarting the device, restoring to default, restoring to default without network, and changing the device password.

1 Activate Bluetooth on your mobile device and run Suprema Device Manager.

2 Select IP Device on the main screen. A list of connectable devices appears.
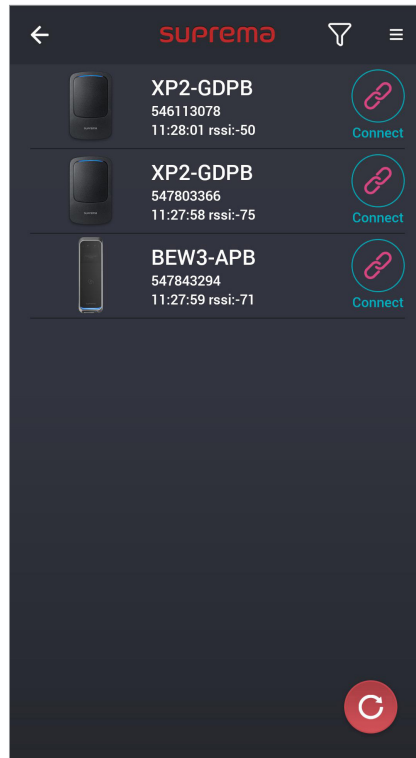
3 Check the device ID in the list of connectable devices and select the device. Or place your mobile device close to the device which you want to connect.

4 Set the device password and tap **OK**. Tap 👁 to display the entered password on the screen.

5 Click **OK** to complete the device connection.

> ⓘ **Device Filter**: Tap the ▽ at the top of the device list screen to display only the desired devices in the list.

Upgrading Firmware

You can easily upgrade the firmware of the device using the Suprema Device Manager.

> • To upgrade the firmware, you need to download the firmware file to your mobile device. You can download the firmware file from the Suprema's home page (www.supremainc.com).
> • Keep the distance between the device and the mobile device within 1 m during firmware upgrade.

1 Connect the device that you want to upgrade the firmware by referring to Connecting the Device.
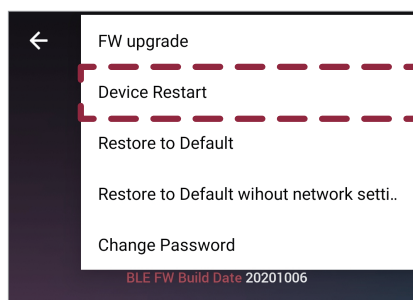
2 Tap ⋮ → **FW upgrade**.
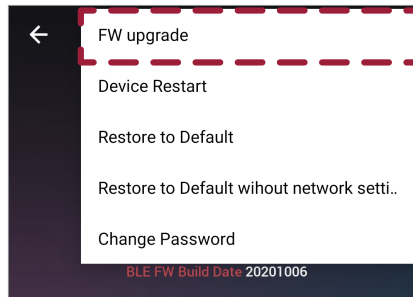
3 Select the firmware from the path where the firmware file is stored. The firmware upgrade will proceed.

4 Tap **OK** to complete the firmware upgrade.

Restarting the Device

You can restart the device using the Suprema Device Manager.

1 Connect the device that you want to restart by referring to Connecting the Device.

2 Tap ⋮ → **Device Restart**.

3 If you restart the device, the BLE with the mobile device is disconnected. To automatically reconnect, enable the **Auto Connect** feature. For detailed instructions, refer to Setting the App.

Restoring the Factory Defaults

You can reset the device settings using the Suprema Device Manager.

1 Connect the device that you want to reset by referring to Connecting the Device.

2 Tap ⋮→ **Restore to Default**.
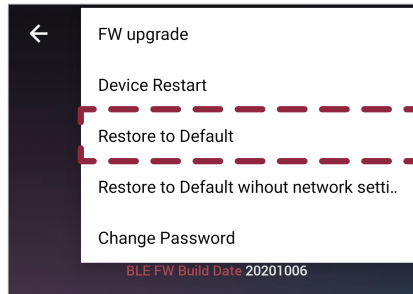
3 All of the device settings are restored to the default values. Tap **OK** to continue.

Restoring to Default Without Network Settings

You can reset the device settings exclude the network using the Suprema Device Manager.

1 Connect the device that you want to reset without network settings by referring to Connecting the Device.

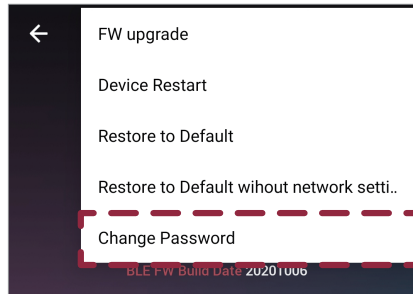**2** Tap ⋮→ **Restore to Default without network setti.. **.
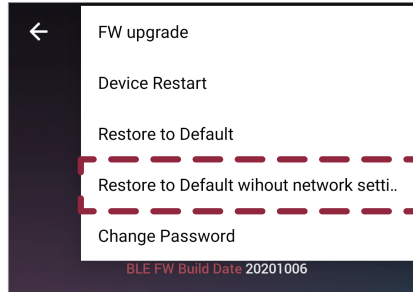
3 All of the device settings without network settings are restored to the default values. Tap **OK** to continue.

Changing Password

You can change the password of the device.

1   Connect the device that you want to change the password by referring to Connecting the Device.

2   Tap ⋮ → **Change Password**.

> ← FW upgrade
>
> Device Restart
>
> Restore to Default
>
> Restore to Default wihout network setti..
>
> Change Password
>
> BLE FW Build Date 20201006

3   Enter the current password and the new password.

> ← **Change Password**
>
> Please set a passwrod
>
> Current password input
>
> Enter a new password
>
> Enter a confirm password
>
> Caution! If you forgot your password,
> The device factory reset will be
> necessary.
>
> Cancel   OK

4   Tap **OK** to complete the password change.

> ⓘ
> - The device password can be set from 6 to 32 characters.
> - Be careful not to forget the Admin Password. If you forgot the Admin Password, the device factory reset will be necessary to apply the template.

Setting the XPass D2

You can configure the settings to apply to the XPass D2 in advance as a template in the Suprema Device Manager and then apply them directly to individual devices. It is possible to apply the device setting much faster than setting the management program from the PC or using the command card.

> If the firmware version of the device is low, some settings may not be applied to the device. To apply the all settings, upgrade the firmware by referring to the Upgrading Firmware.

Adding Templates

You can set the RS-485, card format, keypad setting, PIN, LED, and buzzer and then save them as a template. The template allows you to quickly and easily apply settings to devices without having to set up multiple individual devices each time.

1 Run Suprema Device Manager on your mobile device.

2 Select XPass D2 on the main screen.

3 Tap **Template Management** → ⊕.
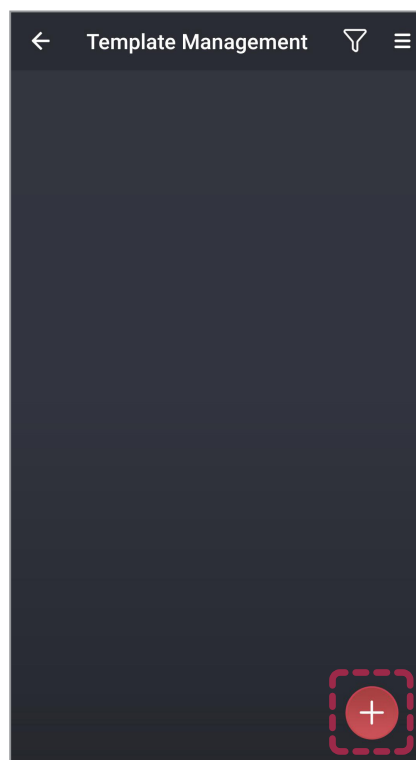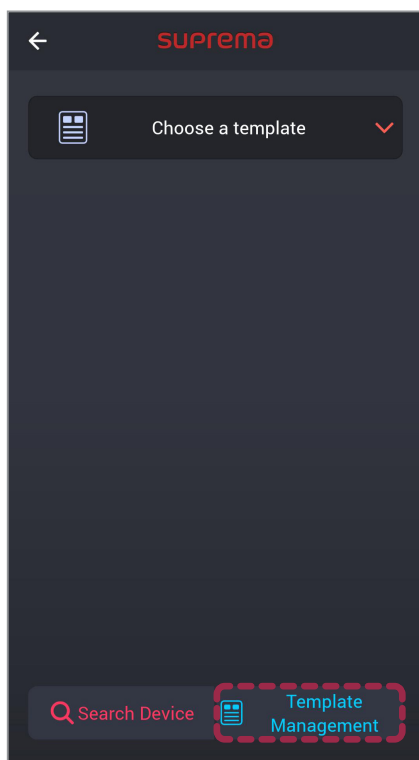
4 Select the model name for which you want to add a template.

5   Enter **Template Name** and **Admin Password**.

Template Name
Admin Password

- **Template Name**: Enter a template name.

- **Admin Password**: Enter an administrator password.

> ℹ️
> - Be careful not to forget the Admin Password. If you forgot the Admin Password, the device factory reset will be necessary to apply the template.
> - For details about changing the Admin Password, refer to Changing Administrator Password.

6   Set the RS-485 connection in the **Interface** tab.

Interface	⌃
RS-485	
OSDP	0
Baudrate	115200

- **OSDP**: Set the OSDP address to be used for connection between the device and the master device. You can set it to a number from 0 to 126.

- **Baudrate**: Set a baud rate of the RS-485 connection.

7   Set the **Card Type** in the **Authentication** tab.

Authentication	⌃
Card Type	❯

- **Card Type**: You can set the type of card used by the device.
    - **CSN Card**: You can select the CSN card type and set the byte order.
    - **Suprema Smart Card Layout**: You can select the type of smart card issued by Suprema.
    - **Custom Smart Card Layout**: You can select the type of smart card issued by a 3rd party.
    - **Mobile**: You can set the type of mobile card.

> ℹ️
> When Byte Order is set to **MSB**, the device reads a card ID from the highest byte to the lowest byte. For example, the highest byte of the card ID 0x12345678 is 0x12 and the device sequentially reads 0x12, 0x34, 0x56 and 0x78. When the option is set to **LSB**, the device reads a card ID from the lowest byte to the highest byte.

8 Set the necessary items in the **Wiegand Card Format** tab.

Wiegand Card Format	⌃
Format	
26bit SIA Standard-H10301	⟩
Setting	
Pulse width (us)	40
Pulse interval (us)	10000

- **Format**: You can configure the format for reading card data. The card data is processed in the set Wiegand format.

  - **New Wiegand Format**: If the desired format is not there, can press the ➕ button to add a new Wiegand format.

← **New Wiegand Format** ✓
Name   Input value
Total Bits   Input value
ID field

Start Bit	End Bit
⊕ Add	

Parity field

| Type	Position	Start Bit	End Bit
⊕ Add			

  – **Name**: Enter a Wiegand format name.

  – **Total Bits**: Enter the total bit count.

  – **ID field**: Enter a Start Bit and End Bit of the ID to use. Click **+Add** to add an ID field.

  – **Parity field**: Enter a Position, Start Bit, and End Bit of the Parity field to use. Click **+Add** to add a parity field.

> ⓘ You must enter the total bit to add a parity bit.

- **Pulse width (µs)**: You can set the pulse width of the Wiegand signal.

- **Pulse interval (µs)**: You can set the pulse interval of the Wiegand signal.

15

9 Set the necessary items in the **Suprema Smart Card Layout** tab.
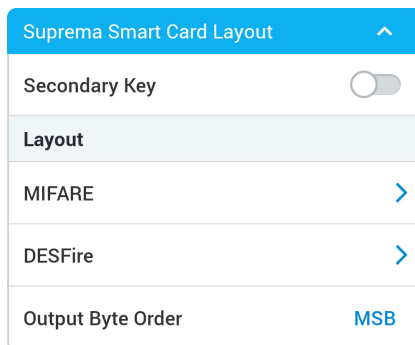
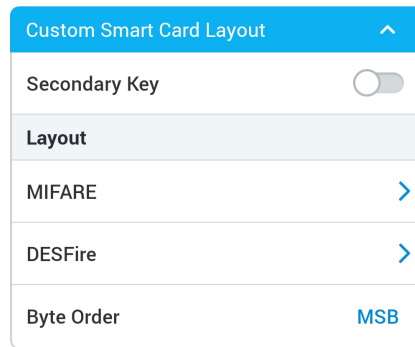| Suprema Smart Card Layout	⌃
Secondary Key	
Layout	
MIFARE	❯
DESFire	❯
Output Byte Order	MSB

- **Secondary Key**: You can set whether or not to use the secondary key. When a secondary key is set, authentication is carried out using the secondary key when the primary key of the card does not match.

- **MIFARE**: You can set the MIFARE card.
  - **Primary Key**: Key which encrypts the communication between the smart key and the card reader.
  - **Secondary Key**: When a secondary key is set, authentication is carried out using the secondary key when the primary key of the card does not match. The secondary Key of MIFARE is displayed only when you activate the **Secondary Key**.
  - **Start Block Index**: Select the start block where each template will be saved. This block is the index of block where user information will be saved. If the user already has the smart key, set available block for saving. Setting is available only for MIFARE.

- **DESFire**: You can set the DESFire card.
  - **DESFire Advanced**: You can use a DESFire card issued by a 3rd party.
  - **Primary Key**: Key which encrypts the communication between the smart key and the card reader.
  - **Secondary Key**: When a secondary key is set, authentication is carried out using the secondary key when the primary key of the card does not match. The secondary Key of DESFire is displayed only when you activate the **Secondary Key**.
  - **App ID**: Set the application ID. This plays a role of directory which includes file ID. Setting is available only for DESFire.
  - **File ID**: Set the file ID. Setting is available only for DESFire.
  - **Encryption Type**: It is possible to set the encryption type to DES/3DES or AES. Setting is available only for DESFire.

- **Output Byte Order**: You can set the smart card output byte order.

> ⓘ
> - To use **DESFire Advanced**, enter the information for **App Master Key**, **App Master Key Index**, **File Read Access Key**, **File Read Access Key Index**, **App ID**, **File ID**, and **Encryption Type** correctly.
> - **App Master Key** and **File Read Access Key** can only be entered in hexadecimal numbers up to 32 bytes.
> - When Byte Order is set to **MSB**, the device reads a card ID from the highest byte to the lowest byte. For example, the highest byte of the card ID 0x12345678 is 0x12 and the device sequentially reads 0x12, 0x34, 0x56 and 0x78. When the option is set to **LSB**, the device reads a card ID from the lowest byte to the highest byte.

16

10 Set the necessary items in the **Custom Smart Card Layout** tab.

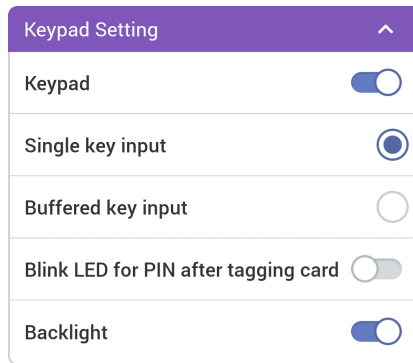| Custom Smart Card Layout	⌃
Secondary Key	⬤
Layout	
MIFARE	›
DESFire	›
Byte Order	MSB

- **Secondary Key**: You can set whether or not to use the secondary key. When a secondary key is set, authentication is carried out using the secondary key when the primary key of the card does not match.

- **MIFARE**: You can set the MIFARE card.
  - **Primary Key**: Key which encrypts the communication between the smart key and the card reader.
  - **Secondary Key**: When a secondary key is set, authentication is carried out using the secondary key when the primary key of the card does not match. The secondary Key of MIFARE is displayed only when you activate the **Secondary Key**.
  - **Block Index**: Select the start block where each template will be saved. This block is the index of block where user information will be saved. If the user already has the smart key, set available block for saving. Setting is available only for MIFARE.
  - **Skip Bytes**: You can set the starting point for reading the card number.
  - **Data Size**: (When the set **Primary Key** and **Secondary Key** are the same as the set value of the card) You can set the data size of the card to be read.

- **DESFire**: You can set the DESFire card.
  - **DESFire Advanced**: You can use a DESFire card issued by a 3rd party.
  - **Primary Key**: Key which encrypts the communication between the smart key and the card reader.
  - **Secondary Key**: When a secondary key is set, authentication is carried out using the secondary key when the primary key of the card does not match. The secondary Key of DESFire is displayed only when you activate the **Secondary Key**.
  - **App ID**: Set the application ID. This plays a role of directory which includes file ID. Setting is available only for DESFire.
  - **File ID**: Set the file ID. Setting is available only for DESFire.
  - **Encryption Type**: It is possible to set the encryption type to DES/3DES or AES. Setting is available only for DESFire.
  - **Skip Bytes**: You can set the starting point for reading the card number.
  - **Data Size**: (When the set **Primary Key** and **Secondary Key** are the same as the set value of the card) You can set the data size of the card to be read.

- **Byte Order**: You can set th smart card output byte order.

> - To use **DESFire Advanced**, enter the information for **App Master Key**, **App Master Key Index**, **File Read Access Key**, **File Read Access Key Index**, **App ID**, **File ID**, and **Encryption Type** correctly.
> - **App Master Key** and **File Read Access Key** can only be entered in hexadecimal numbers up to 32 bytes.
> - When Byte Order is set to **MSB**, the device reads a card ID from the highest byte to the lowest byte. For example, the highest byte of the card ID 0x12345678 is 0x12 and the device sequentially reads 0x12, 0x34, 0x56 and 0x78. When the option is set to **LSB**, the device reads a card ID from the lowest byte to the highest byte.

11 Set the necessary items in the **Keypad Setting** tab.

| Keypad Setting	⌄
Keypad	⬤
Single key input	◉
Buffered key input	◯
Blink LED for PIN after tagging card	⬤
Backlight	⬤

- **Keypad**: You can set whether or not to use the keypad. Enabling the keypad allows authentication by entering the card ID on the keypad.

- **Single key input**: When a user enters a card ID on the keypad, the device sends the ID value each time a key is pressed.

- **Buffered key input**: When a user enters a card ID on the keypad, the entire ID value will be sent at once after pressing all the keys and then pressing the # key.

- **Blink LED for PIN after tagging card**: When the device's auth mode is set to Card+PIN, if a user tags a card, the device's LED operates to induce PIN input.

- **Backlight**: You can turn the backlight of the keypad on or off.

> - The **Keypad Setting** is displayed only on the template setting of the XPD2-GKDB.
> - **Backlight** is only supported on XPD2-GKDB hardware V02M, firmware v1.7.1 or later.
> - The values entered through the device's keypad are transmitted in 4-bits. When the keypad is enabled, it is sent the same as the card ID according to the Wiegand card format.

12 Set the **Secure Tamper** in the **Others** tab.

Others	⌄
Secure Tamper	◯
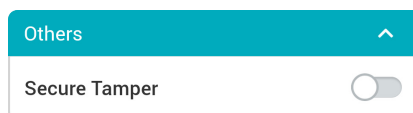
- **Secure Tamper**: If a tamper event occurs on the device, you can set to delete the security key stored on the device. To use the secure tamper, enable this option.

13 Edit the necessary items in the **LED / Buzzer** tab.
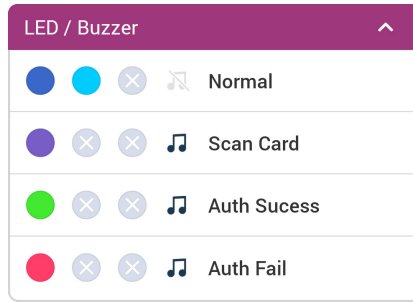
- **Normal**: You can set the color that is normally displayed on the device LED.

- **Scan Card**: You can set the LED color and the number of times the Buzzer plays when scanning the card to the device.

- **Auth Sucess**: You can set the LED color and the number of times the Buzzer plays when the authentication is successful.

- **Auth Fail**: You can set the LED color and the number of times the Buzzer plays when the authentication is failed.

> You can set the LED to display repeatedly up to three colors. Tap the slot to select a color.
>
> If you select ⓧ, that slot is skipped and the color of next slot is displayed.

14 To save the template settings, tap **Save**.

> You can add up to 100 templates.

Applying Templates

The templates can be applied equally to multiple devices using BLE.

> ℹ️ If the firmware version of the device is low, some settings may not be applied to the device. To apply the all settings, upgrade the firmware by referring to the Upgrading Firmware.

1 Activate Bluetooth on your mobile device and run Suprema Device Manager.

2 Select XPass D2 on the main screen.

3 Tap **Choose a template**. A list of selectable templates appears.
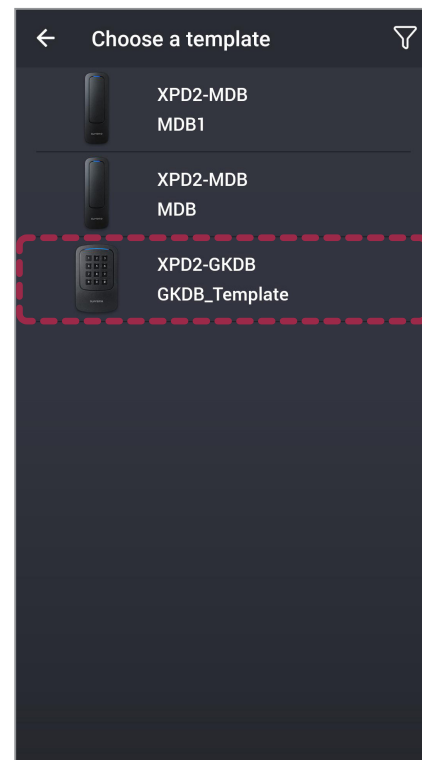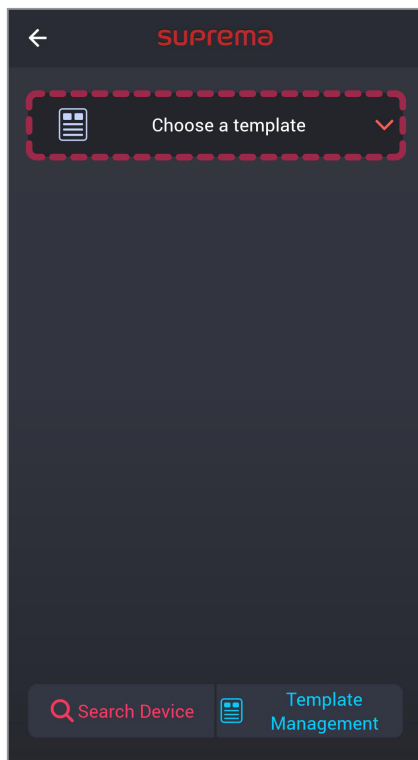
4 Select the template in the templates list.

5 Tap **Start**.
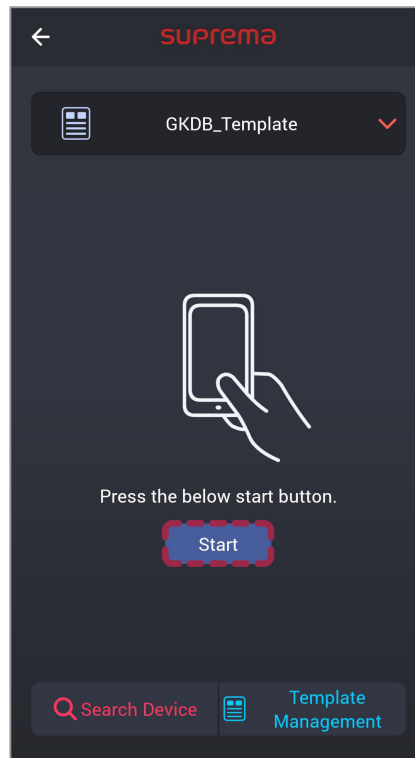
6 Place the back of your mobile device to the device to which you want to apply the template.

7 When you are finished applying the template, tap **OK**.

> ⓘ
> - Settings that you changed using the Suprema Device Manager apply only to the device and are not synchronized to the server.
> - If the device is connected to the master device or if the Wiegand output settings have been changed, you can not connect with Suprema Device Manager using the default key. To connect with Suprema Device Manager, reset the device.

Managing Templates

Editing Templates

1   Run Suprema Device Manager on your mobile device.

2   Select XPass D2 on the main screen.
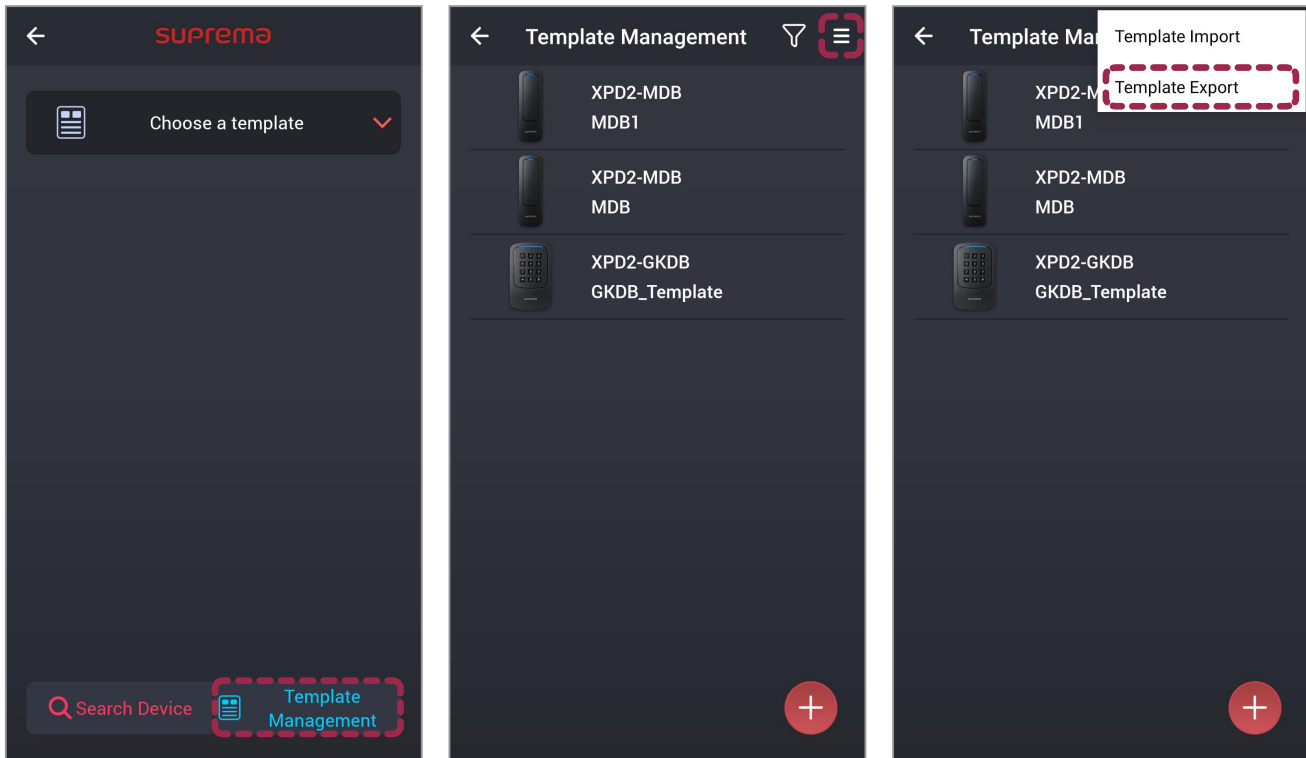
3   Tap **Template Management**.
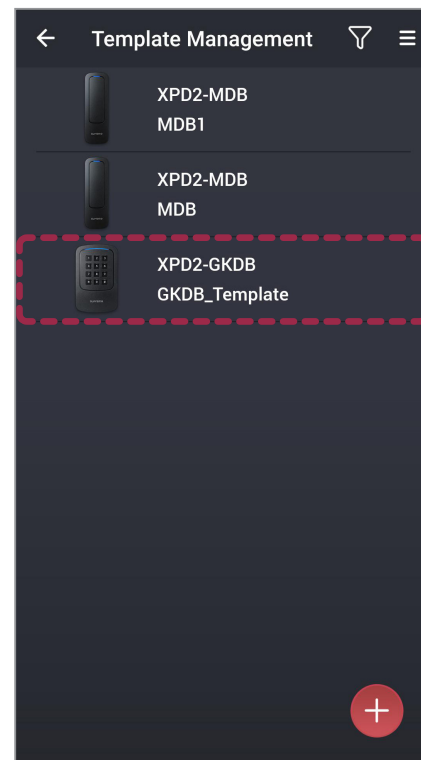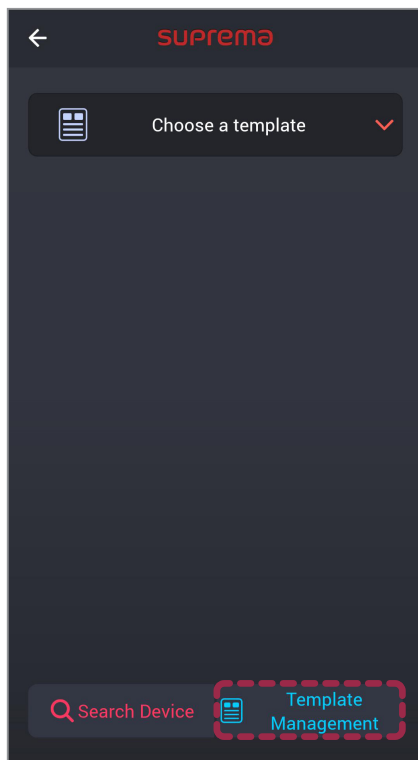
4   Select the template in the templates list.

5   Edit template by referring to Adding Templates.

6   To save the changed settings, tab **Save**. To save as a new template, tab **Save as new template**.

Deleting Templates

1 Run Suprema Device Manager on your mobile device.

2 Select XPass D2 on the main screen.

3 Tap **Template Management**.
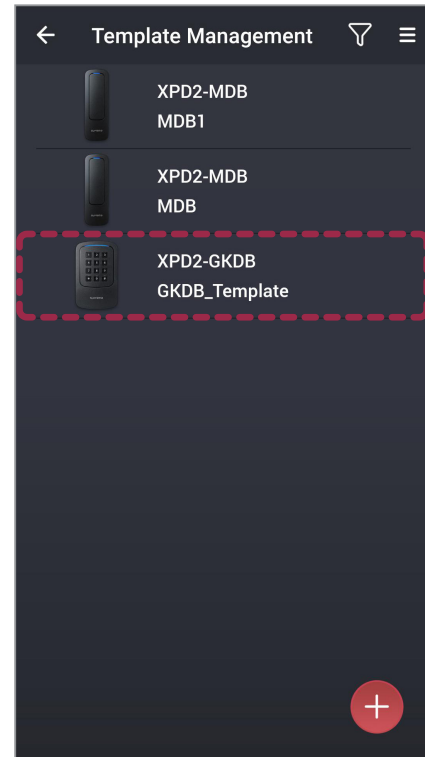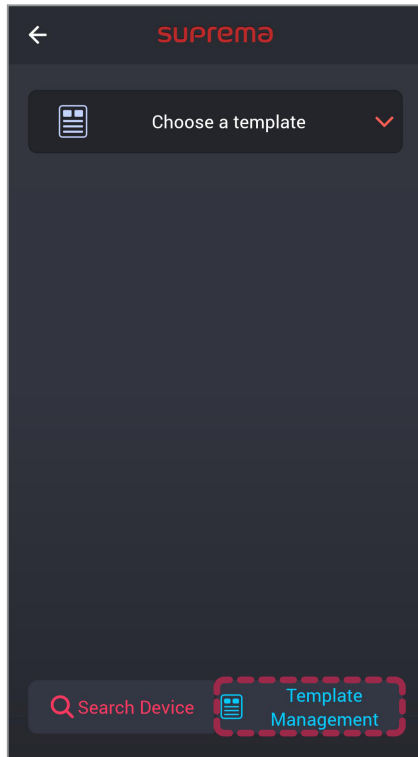
4 Select the template in the templates list.

5 To delete the template, tap 🗑 → **OK**.
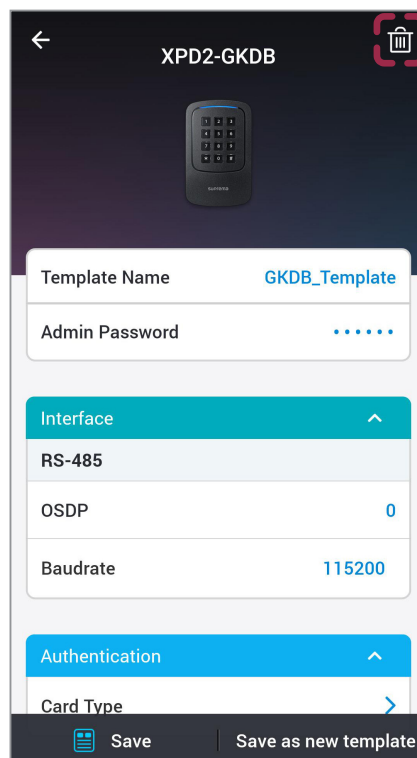
Exporting Templates

You can export templates for XPass D2 settings from the app.

1 Run Suprema Device Manager on your mobile device.

2 Select XPass D2 on the main screen.

3 Tap **Template Management**.

← suprema	← Template Management ▽ ☰	← Template Mar Template Import
📖 Choose a template ⌄	XPD2-MDB MDB1	XPD2-M Template Export MDB1
	XPD2-MDB MDB	XPD2-MDB MDB
	XPD2-GKDB GKDB_Template	XPD2-GKDB GKDB_Template
🔍 Search Device Template Management	⊕	⊕

4 Tap ☰ at the top of the template list screen and select **Template Export**.

**5** After selecting the template to export, tap ✓.
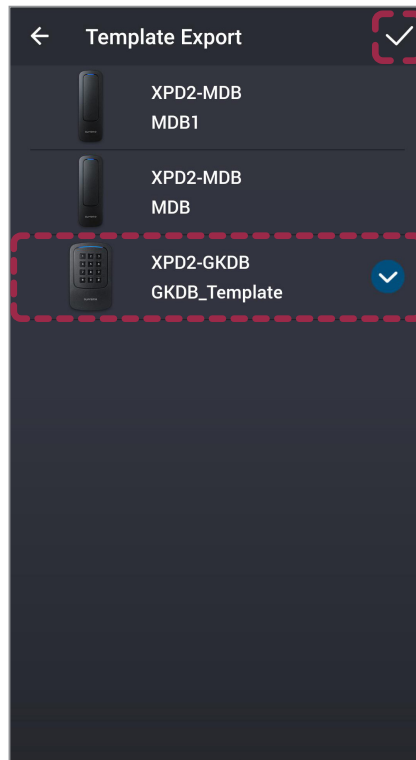
ℹ The template will be saved in the DeviceManager_TemplateFiles folder, which is created in the same location as the Suprema Device Manager application installation files.

Importing Templates

You can import templates for XPass D2 settings into the app.

1 Run Suprema Device Manager on your mobile device.

2 Select XPass D2 on the main screen.

3 Tap **Template Management**.
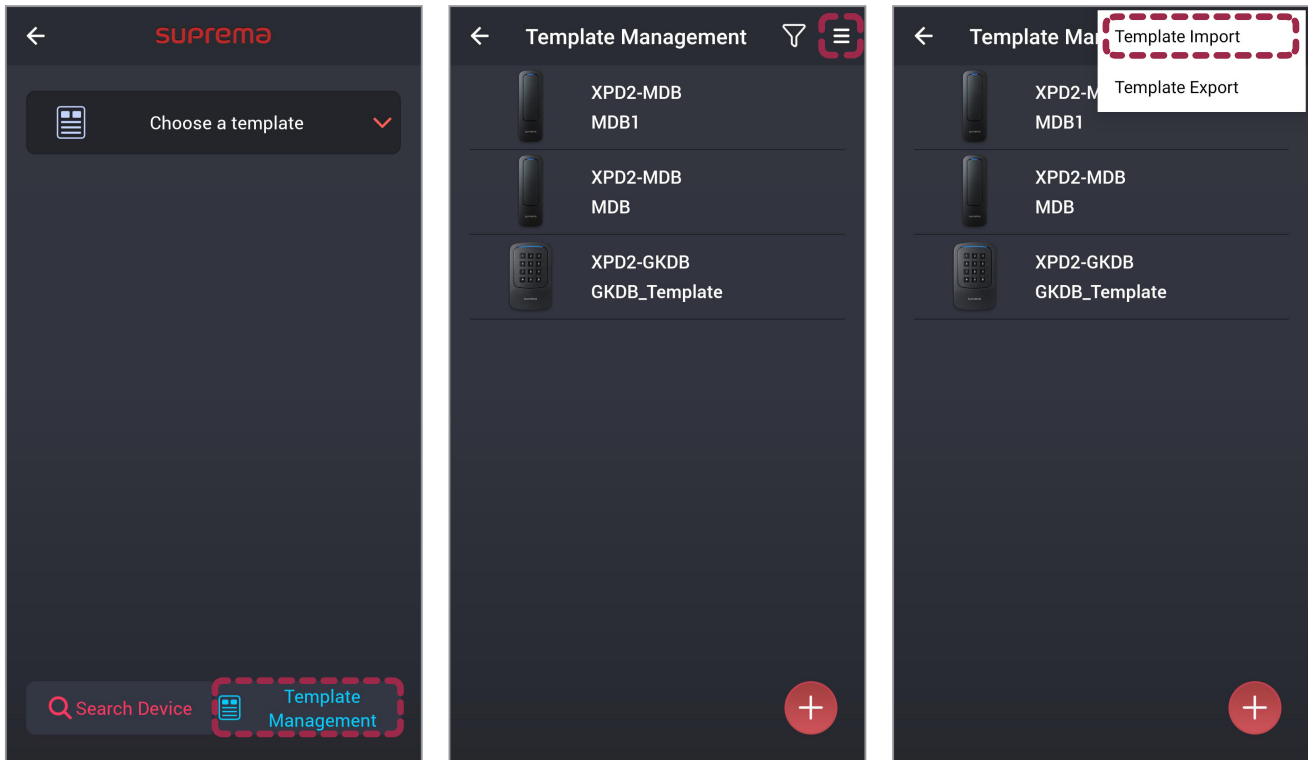
4 Tap ☰ at the top of the template list screen and select **Template Import**.

5 Select the template to import from the folder where the templates are stored.

> ℹ The template will be saved in the DeviceManager_TemplateFiles folder, which is created in the same location as the Suprema Device Manager application installation files.

26

Search and Connect Devices

The Suprema Device Manager allows you to search for and connect Suprema's access control and time & attendance devices installed nearby. If you connect to the Device Manager, you can use various functions such as upgrading the firmware of the device, restarting the device, and changing the template password.

1   Activate Bluetooth on your mobile device and run Suprema Device Manager.

2   Select XPass D2 on the main screen.

3   Tap **Search Device**. The list of connectable devices is displayed on the screen.
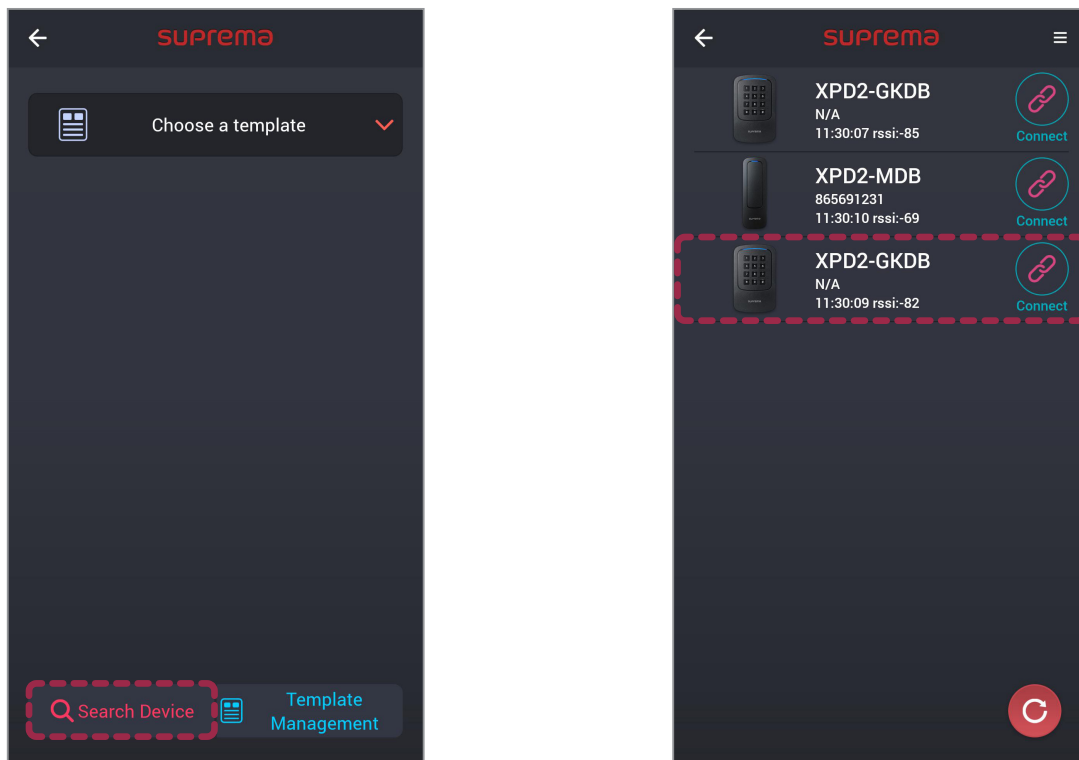
4   Check the device ID in the list of connectable devices and select the device. Or place your mobile device close to the device which you want to connect.

5   Enter the password. Tap 👁 to display the entered password on the screen.

6   Tap **OK**. The device connection is complete.

27

Upgrading Firmware

You can easily upgrade the firmware of the device using the Suprema Device Manager.

> ⓘ
> - To upgrade the firmware, you need to download the firmware file to your mobile device. You can download the firmware file from the Suprema's home page (www.supremainc.com).
> - Keep the distance between the device and the mobile device within 1 m during firmware upgrade.

1 Connect the device that you want to upgrade the firmware by referring to Search and Connect Devices.

2 Tap ⋮ → **FW upgrade**.
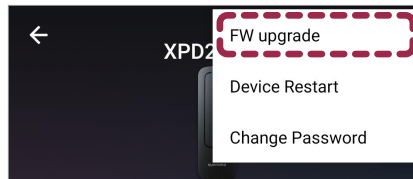
3 Select the firmware from the path where the firmware file is stored. The firmware upgrade will proceed.

4 Tap **OK** to complete the firmware upgrade.

Restarting Device

You can restart the device using the Suprema Device Manager.

1 Connect the device that you want to restart by referring to Search and Connect Devices.
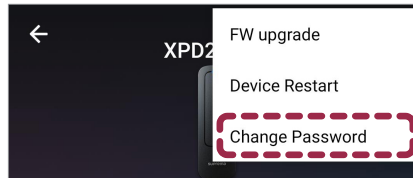
2 Tap ⋮ → **Device Restart**.
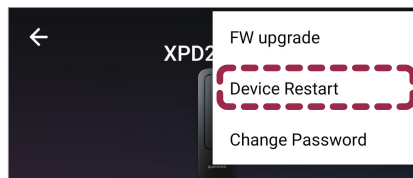
3 If you restart the device, the BLE with the mobile device is disconnected. To automatically reconnect, enable the **Auto Connect** feature. For detailed instructions, refer to Setting the App.
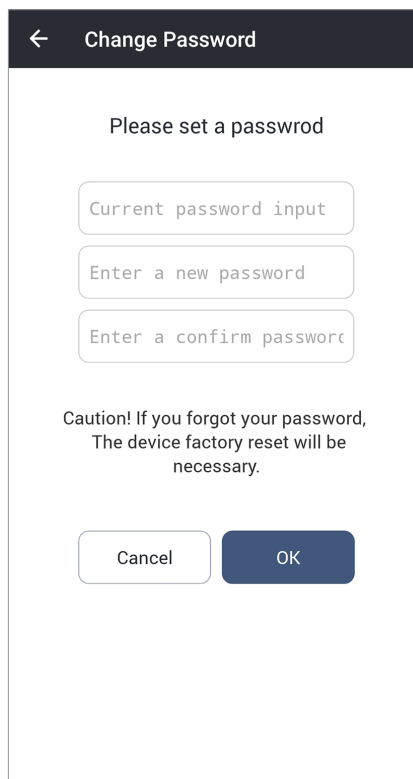
Changing Administrator Password

You can change the administrator password of the template.

1 Connect the device with the template whose password you want to change by referring to Search and Connect Devices.

2 Tap ⋮ → **Change Password**.

3 Enter the current password and the new password.

4 Tap **OK** to complete the password change.

> ℹ️ Be careful not to forget the Admin Password. If you forgot the Admin Password, the device factory reset will be necessary to apply the template.

Appendices

Disclaimers

- Information in this document is provided in connection with Suprema products.

- The right to use is acknowledged only for Suprema products included in the terms and conditions of use or sale for such products guaranteed by Suprema. No license, express or implied, by estoppel or otherwise, to any intellectual property is granted by this document.

- Except as expressly stated in an agreement between you and Suprema, Suprema assumes no liability whatsoever, and Suprema disclaims all warranties, express or implied including, without limitation, relating to fitness for a particular purpose, merchantability, or noninfringement.

- All warranties are VOID if Suprema products have been: 1) improperly installed or where the serial numbers, warranty date or quality assurance decals on the hardware are altered or removed; 2) used in a manner other than as authorized by Suprema; 3) modified, altered or repaired by a party other than Suprema or a party authorized by Suprema; or 4) operated or maintained in unsuitable environmental conditions.

- Suprema products are not intended for use in medical, lifesaving, life-sustaining applications, or other applications in which the failure of the Suprema product could create a situation where personal injury or death may occur. Should you purchase or use Suprema products for any such unintended or unauthorized application, you shall indemnify and hold Suprema and its officers, employees, subsidiaries, affiliates, and distributors harmless against all claims, costs, damages, and expenses, and reasonable attorney fees arising out of, directly or indirectly, any claim of personal injury or death associated with such unintended or unauthorized use, even if such claim alleges that Suprema was negligent regarding the design or manufacture of the part.

- Suprema reserves the right to make changes to specifications and product descriptions at any time without notice to improve reliability, function, or design.

- Personal information, in the form of authentication messages and other relative information, may be stored within Suprema products during usage. Suprema does not take responsibility for any information, including personal information, stored within Suprema's products that are not within Suprema's direct control or as stated by the relevant terms and conditions. When any stored information, including personal information, is used, it is the responsibility of the product users to comply with national legislation (such as GDPR) and to ensure proper handling and processing.

- You must not rely on the absence or characteristics of any features or instructions marked "reserved" or "undefined." Suprema reserves these for future definition and shall have no responsibility whatsoever for conflicts or incompatibilities arising from future changes to them.

- Except as expressly set forth herein, to the maximum extent permitted by law, the Suprema products are sold "as is".

- Contact your local Suprema sales office or your distributor to obtain the latest specifications and before placing your product order.

Copyright Notice

The copyright of this document is vested in Suprema. The rights of other product names, trademarks and registered trademarks are vested in each individual or organization that owns such rights.

Open-source Software License

This product contains open-source software. To request the source code covered under Android Open Source Project, Gson, TKCryptor, OCMapper, JKBigInteger, TODocumentPickerViewController, and other opensource licenses which require distribution of the source code, please visit support.supremainc.com.

You may obtain the source code for three years after our last shipment of this product on our website (support.supremainc.com).

If you want to obtain the source code in the physical medium, the cost of performing such distribution may be charged. This offer is valid to anyone in receipt of this information.

Open-source licenses and the corresponding license terms for open-source software contained in this product are as follows:

Android

Android - The Android Open Source Project

https://android.googlesource.com/platform/frameworks/support/

/*

* Copyright (C) 2012 The Android Open Source Project

*

* Licensed under the Apache License, Version 2.0 (the "License");

* you may not use this file except in compliance with the License.

* You may obtain a copy of the License at

*

*   http://www.apache.org/licenses/LICENSE-2.0

*

* Unless required by applicable law or agreed to in writing, software

* distributed under the License is distributed on an "AS IS" BASIS,

* WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.

* See the License for the specific language governing permissions and

* limitations under the License.

*/

Gson

https://github.com/google/gson

Copyright 2008 Google Inc.

Licensed under the Apache License, Version 2.0 (the "License");

you may not use this file except in compliance with the License.

You may obtain a copy of the License at

http://www.apache.org/licenses/LICENSE-2.0

Unless required by applicable law or agreed to in writing, software distributed under the License is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. See the License for the specific language governing permissions and limitations under the License.

iOS

TKCryptor

Copyright (c) 2014 Taras Kalapun <t.kalapun@gmail.com>

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

OCMapper

Copyright (c) 2013 Aryan Ghassemi. All rights reserved.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

JKBigInteger

TODocumentPickerViewController

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

For more information about Suprema's global branch offices,
visit the webpage below by scanning the QR code.
https://supremainc.com/en/about/global-office.asp