

Device Manager

USER GUIDE

Version 1.02
English

EN 102.00.DM V1.02A

Contents

Getting Started	3
Introduction	3
Minimum Requirements	4
Mobile Device.....	4
Device and Firmware.....	4
Selecting the Device	5
Setting the XPass 2	6
Changing the Settings	6
Connecting the Device.....	9
Restarting the Device.....	9
Restoring the Factory Defaults.....	9
Restoring to Default without network settings.....	10
Changing Password	10
Setting the XPass D2	12
Adding Templates.....	12
Applying Templates.....	15
Managing Templates	16
Editing Templates	16
Deleting Templates.....	17
Search and Connect Devices.....	18
Upgrading Firmware.....	19
Restarting Device.....	20
Checking Card Information	20
Changing Administrator Password.....	21
Appendices	22
Disclaimers	22
Copyright notice.....	22

Getting Started

Introduction

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



XPass D2 / XPass 2



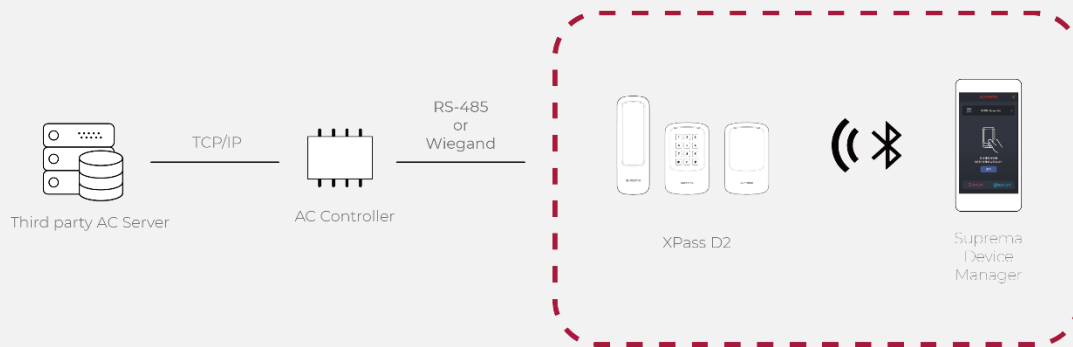
Suprema
Device
Manager

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, 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.

NOTE

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



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.

- XPD2-MDB FW 1.1.0 or later
- XPD2-GDB FW 1.1.0 or later
- XPD2-GKDB FW 1.1.0 or later
- XP2-MDPB FW 1.0.0 or later
- XP2-GDPB FW 1.0.0 or later
- XP2-GKDPB FW 1.0.0 or later

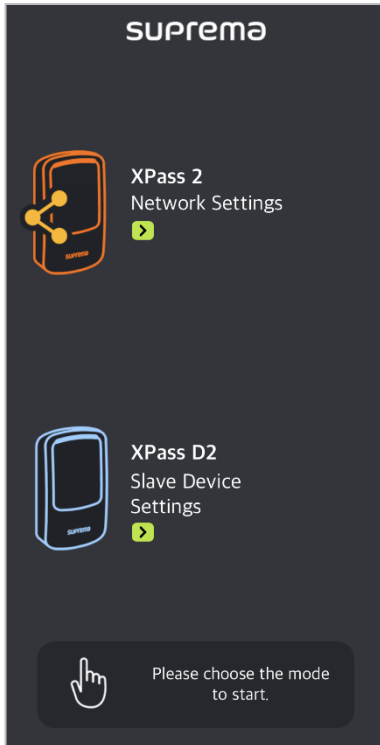
NOTE

- 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 details about upgrading the device firmware, refer to 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 Device Manager. You can choose XPass 2 or XPass D2, and the items that can be set vary depending on the model you choose.

1. Run the Device Manager.
2. Select the model you want to set up.




Setting the XPass 2

You can change the settings of XPass 2 in the 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.

Changing the Settings

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

1. Activate the Bluetooth on your mobile device and run the Device Manager.
2. Select XPass 2 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.

NOTE

- 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	
Port	<input type="text" value="51211"/>
DHCP	<input checked="" type="checkbox"/>
IP Address	<input type="text"/>
Gateway	<input type="text"/>
Subnet	<input type="text"/>
DNS	<input type="text"/>

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

Server	
Server Connection	Server > Device >
Server IP	<input type="text"/>
Server URL	<input type="text"/>
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	42.0 MB/60.0 MB
Secure Tamper	<input type="checkbox"/>


- **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	<input type="radio"/> <input type="radio"/> <input type="radio"/> <input type="radio"/>
Scan Card	<input type="radio"/> <input type="radio"/> <input type="radio"/> <input type="radio"/>
Auth Success	<input type="radio"/> <input type="radio"/> <input type="radio"/> <input type="radio"/>
Auth Fail	<input type="radio"/> <input type="radio"/> <input type="radio"/> <input type="radio"/>

- **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 Success:** 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.


NOTE

- 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

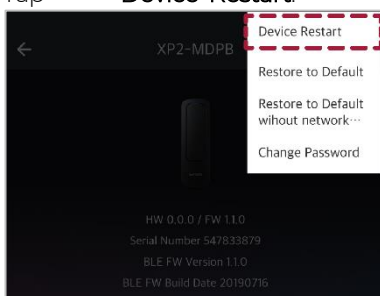
The Device Manager allows you to search for and connect Suprema's access control and time & attendance devices installed nearby. If you connect to the Device Manager, you can use various functions such as restarting the device, restoring to default, restoring to default without network, and changing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

1. Activate the Bluetooth on your mobile device and run the Device Manager.
2. Select XPass 2 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.

Restarting the Device

You can restart the device using the Device Manager.


1. Connect the device that you want to restart by referring to [Connecting the Device](#).
2. Tap  > **Device Restart**.

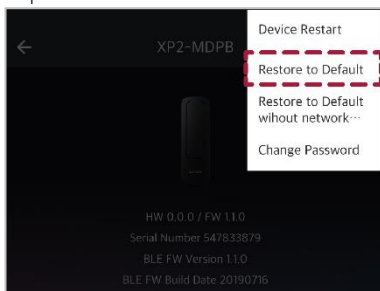


3. If you restart the device, the BLE with the mobile device is disconnected. Tap **OK** to reconnect.

Restoring the Factory Defaults

You can reset the device settings using Device Manager.


1. Connect the device that you want to restart by referring to [Connecting the Device](#).
2. Tap  > **Restore to Default**.

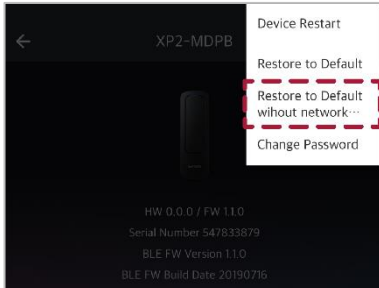


3. All of the device settings are restored to the default values. Tap **OK** to continue.

Restoring to Default without network settings

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


1. Connect the device that you want to restart by referring to [Connecting the Device](#).
2. Tap  > Restore to Default without network...

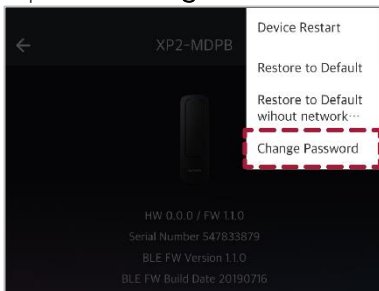


3. All of the device settings without network settings are restored to the default values. Tap **OK** to continue.

Changing Password

You can change the password of the device.

1. Connect the device that you want to restart by referring to [Connecting the Device](#).
2. Tap  > Change Password.



3. Enter the current password and the new password.

 A screenshot of the 'Change Password' dialog box. The title bar says 'Change Password' with a close button (X). The main text reads 'Please set a password'. There are three input fields: 'Current password input', 'Enter a new password', and another 'Enter a new password'. Each field has a toggle icon on the right. At the bottom, there is a 'Caution! If you forgot your password, The device factory reset will be necessary.' message and two buttons: 'Cancel' and 'OK'.

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

NOTE

- 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.

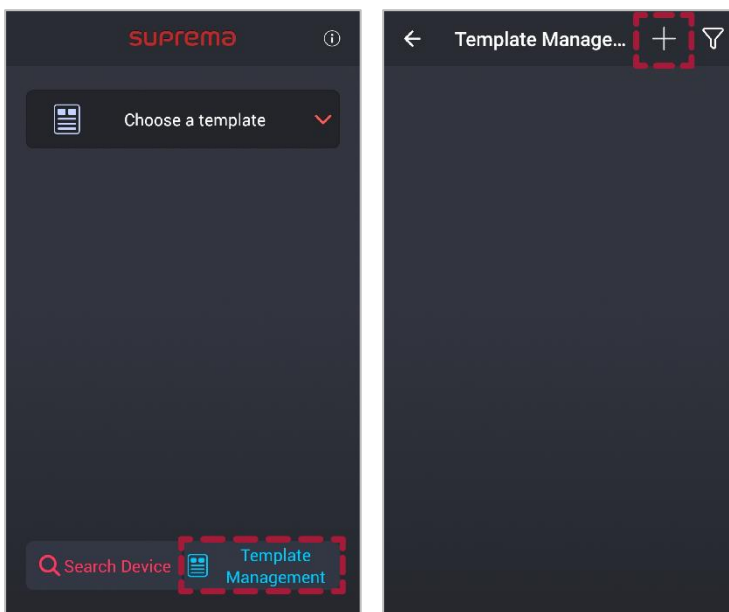
Setting the XPass D2

You can configure the settings to apply to the XPass D2 in advance as a template in the 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.

Adding Templates

You can set the RS-485, card format, 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. Activate the Bluetooth on your mobile device and run the Device Manager.
2. Select XPass D2 on the main screen.
3. Tap **Template Management** > **+**.



4. Select the device model 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.

NOTE

- 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.

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 Wiegand Card Format.

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. If there is no format you want, tap **+** to add a new format.
 - **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.

NOTE

- 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.

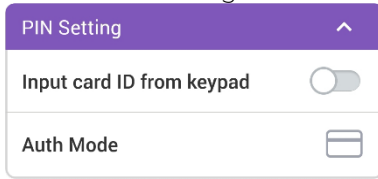
8. Set the Smart Card Format.

Smart Card Format	
Secondary Key	<input type="checkbox"/>
Format	
MIFARE	>
DESFire / Mobile	>

- **Secondary Key:** It is possible to set whether or not to use the secondary website key. When a secondary site key is set, authentication is carried out using the secondary website key when the basic site key of the card does not match.
- **MIFARE:** You can set the Primary Key, Secondary Key, and Start Block Index for the MIFARE card. The secondary Key of MIFARE is displayed only when you activate the Secondary Key.
- **DESFire / Mobile:** You can set the Primary Key, Secondary Key, APP ID, and File ID for the DESFire and Mobile card. The

secondary key of DESFire and Mobile is displayed only when you activate the secondary key.

9. Set the PIN Setting.

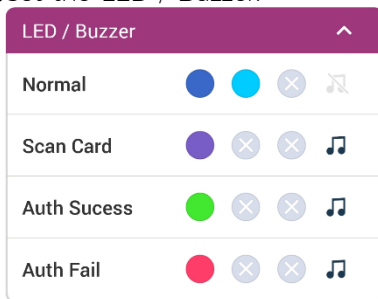


- **Input card ID from keypad:** You can authenticate by entering the card ID directly into the device.
- **Auth Mode:** You can set the authentication mode of the device. Authentication mode can be set as card or PIN + card.

NOTE


- The PIN Setting is displayed only on the template setting of the XPD2-GKDB.
- The values entered through the device's keypad are transmitted in 4-bits. When **Input card ID from keypad** is enabled, it is sent the same as the card ID according to the Wiegand card format.

10. Set the LED / Buzzer.



- **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 Success:** 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.

NOTE

- 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.

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

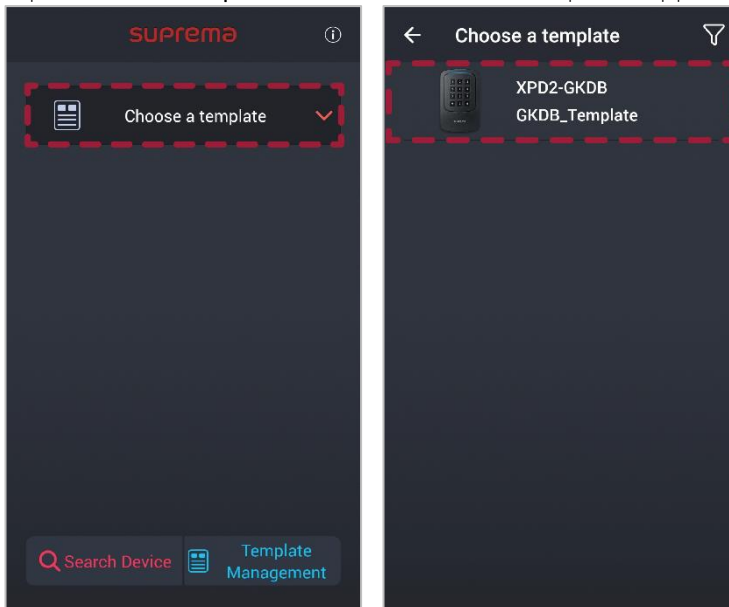
NOTE

- You can add up to 100 templates.

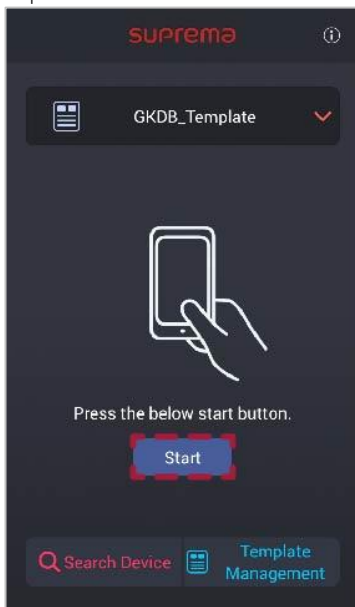
Applying Templates

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

1. Activate the Bluetooth on your mobile device and run the 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**.

NOTE

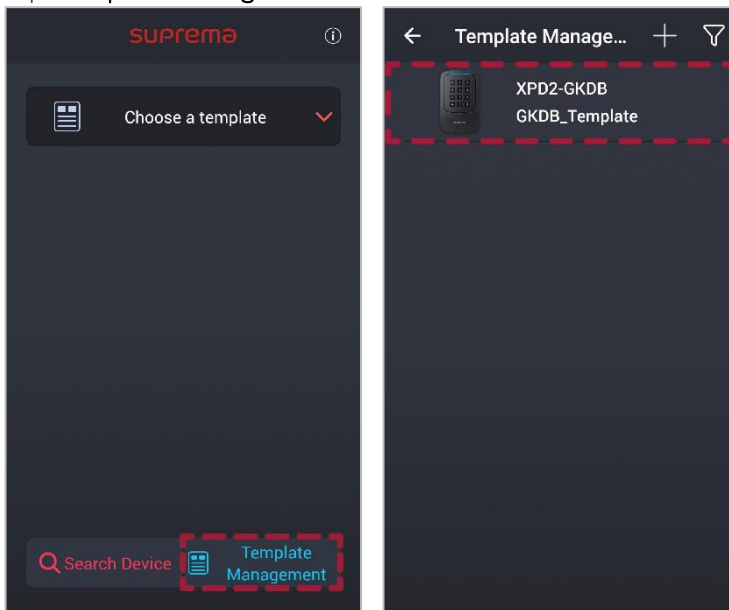
- Settings that you changed using the Device Manager apply only to the device and are not synchronized to the server.

- If the device is connected to the master device or if the Wiegand output settings have been changed, you can not connect with Device Manager using the default key. To connect with Device Manager, reset the device.

Managing Templates

Editing Templates

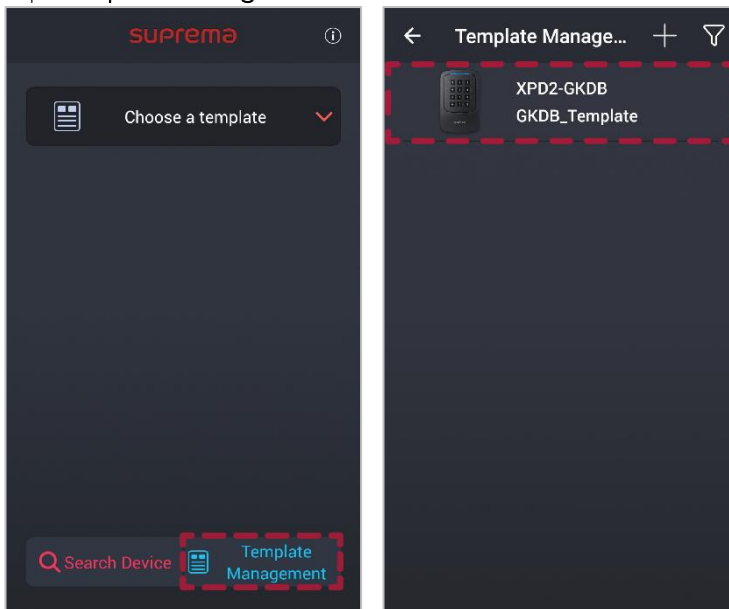
1. Run the Device Manager.
2. Select XPass D2 on the main screen.
3. Tap Template Management.




4. Select the template in the templates list.
5. Edit template by referring to [Adding Templates](#).
6. To save the changed settings, tap **Save**.

Deleting Templates

1. Run the Device Manager.
2. Select XPass D2 on the main screen.
3. Tap Template Management.

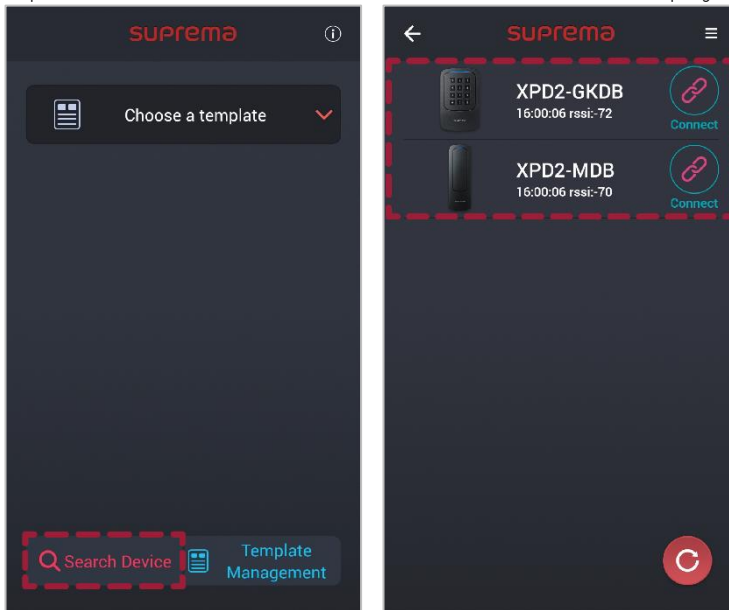



4. Select the template in the templates list.
5. To delete the template, tap  > OK.

Search and Connect Devices

The 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, checking card information, and changing the template password.

1. Activate the Bluetooth on your mobile device and run the 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. Select the device in the devices list or place the mobile device closer to the device 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.

Upgrading Firmware

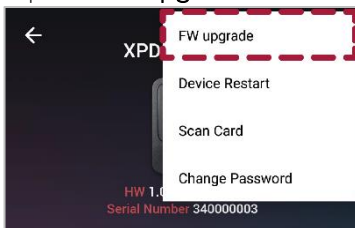
You can easily upgrade the firmware of the device using the Device Manager.

NOTE

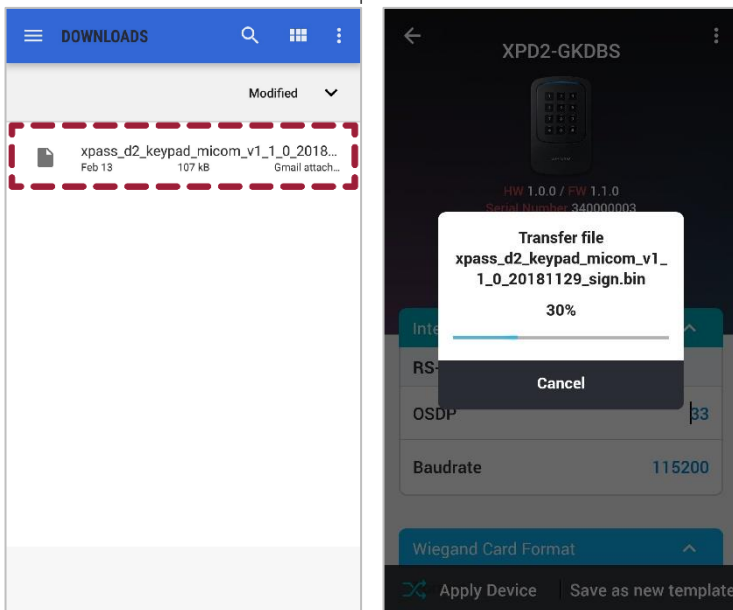
- To upgrade the firmware, you need to download the firmware file to your mobile device. You can download the firmware file from the Suprema's home page (www.supremainc.com).
- Keep the distance between the device and the mobile device within 1 m during firmware upgrade.

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.

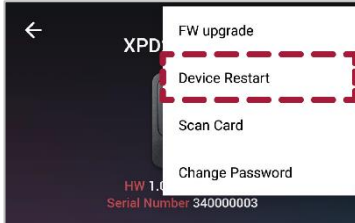


4. Tap OK to complete the firmware upgrade.

Restarting Device

You can restart the device using the Device Manager.


1. Connect the device that you want to restart by referring to [Search and Connect Devices](#).
2. Tap  > Device Restart.

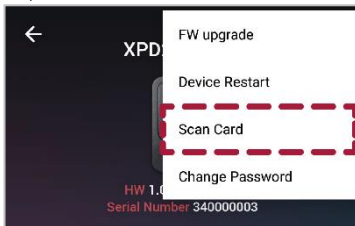


3. If you restart the device, the BLE with the mobile device is disconnected. Tap **OK** to reconnect.

Checking Card Information

You can check the card ID by scanning the card directly to the device.

1. Connect the device that you want to use for card scanning by referring to [Search and Connect Devices](#).
2. Tap  > Scan Card.



3. Place a card on the selected device. The card ID is displayed on the screen.



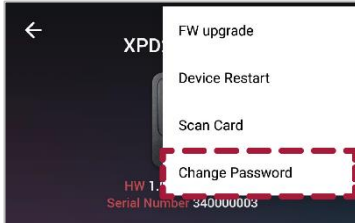
NOTE

- **Scan Card** is available only when using CSN card.

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.

NOTE

- 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

- The information in this manual is provided with regard to the Suprema's products.
- The right to use is acknowledged only for products included in the terms and conditions of the sales agreement guaranteed by Suprema. The right of license to other intellectual property rights not discussed in this manual is not acknowledged.
- Suprema does not guarantee or hold responsibility for the suitability and commerciality of the product for a specific purpose, or the infringement of patent, copyright, or other intellectual property rights with regard to sales or usage of Suprema's products.
- Do not use a Suprema product in situations related to medical, rescue of human lives, or maintenance of life, as a person may get injured or lose his/her life due to product malfunction. If an accident occurs while a consumer is using the product under the situations described as examples above, employees, subsidiaries, branches, affiliated companies and distributors of Suprema do not accept responsibility nor will they reimburse for all related direct and indirect expenses or expenditure including attorney fees even if the consumer has discovered any shortcomings in the product design or manufacturing process and claims this as a significant fault.
- Suprema may modify the product size and specifications at any time without proper notice in order to improve the safety, function and design of the product. Designers must keep in mind that functions or descriptions indicated as "to be implemented" or "undefined" may change at any time. Suprema will implement or define such functions or descriptions in the near future and Suprema accepts no responsibility for compatibility issues and any other problems arising from such compatibility issues.
- If you wish to obtain the newest specifications before ordering the product, contact Suprema through a Sales Representative or local distributor of Suprema.

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.

The logo for Suprema, featuring the word "suprema" in a bold, lowercase, sans-serif font. Below it, the words "SECURITY & BIOMETRICS" are written in a smaller, uppercase, sans-serif font. The entire logo is set against a dark red rectangular background.

suprema
SECURITY & BIOMETRICS

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

©2021 Suprema Inc. Suprema and identifying product names and numbers herein are registered trade marks of Suprema, Inc. All non-Suprema brands and product names are trademarks or registered trademarks of their respective companies. Product appearance, build status and/or specifications are subject to change without notice.