Suprema Device Manager

USER GUIDE

Version 1.09

English
EN 102.00.DM

suprema
SECURITY & BIOMETRICS

CONTENTS

Getting Started 4

Minimum requirements 4

Initial Setup of the Device 6

Select device 6

Configuring app settings 6

Set Up IP Device 8

Change device settings 8

Connect device 11

Upgrade device firmware 12

Restart device 12

Initialize settings 13

Initialize device settings excluding network 13

Change device password 13

Set Up XPass D2 15

Add template 15

Apply template 23

Manage templates 24

Search and connect device 28

Upgrade device firmware 29

Restart device 12

Change admin password 30

Appendices 32

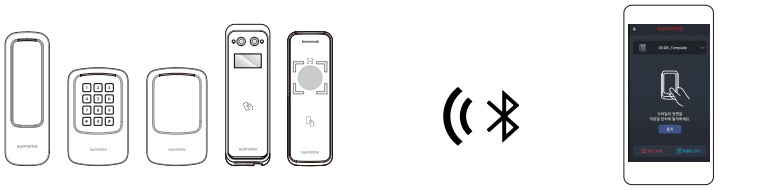
Disclaimers 32

Copyright Notice 33

Open Source License 33

Getting Started

Suprema Device Manager is a mobile application that uses BLE communication to configure Suprema's XPass D2, XPass 2, XPass 2 V2, BioEntry W3, and XPass Q2 devices.



XPass D2 / XPass 2 / XPass 2 V2 / BioEntry W3 / XPass Q2

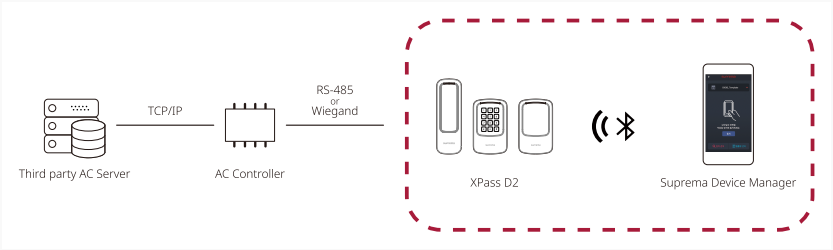
Suprema Device Manager

Administrators can connect to the server from a PC or set the device's network, server, RS-485 communication, card format, keypad settings, PIN, LED, and buzzer from a mobile device without physically disconnecting it, and can also use functions such as device restart, firmware upgrade, and device setting initialization.

For XPass D2, values set once can be saved as a template for quick and easy application to multiple devices.

Info

Using Suprema Device Manager allows on-site modification of the settings of XPass D2 configured with third-party controllers.



Minimum requirements

Mobile Device

Check if the mobile device supports BLE communication.

- Android 5.0 Lollipop or later
- iOS 15 or later

Device and Firmware

Check compatible devices and firmware versions.

- XPass D2 firmware version 1.1.0 or later
- XPass 2

  - XP2-MDPB, XP2-GDPB, XP2-GKDPB: firmware version 1.0.0 or later
  - XP2-MAPB: firmware version 1.4.1 or later
  - XP2-MAPB-H: firmware version 1.4.3 or later
- **XPass 2 V2** firmware version 1.0.0 or later
- **BioEntry W3** firmware version 1.0.1 or later
- **XPass Q2** firmware version 1.0.0 or later

Info

- Compatible devices and firmware are subject to change.
- If the device firmware version is lower than the versions listed above, upgrade the device firmware in BioStar X. When using the device as a slave, the connected master's firmware must also be the latest version compatible with BioStar 2 2.7.0 or later.
- For details on upgrading device firmware, see IP Device (Upgrade Device Firmware), XPass D2 (Upgrade Device Firmware), or the BioStar X Administrator Guide.

Initial Setup of the Device

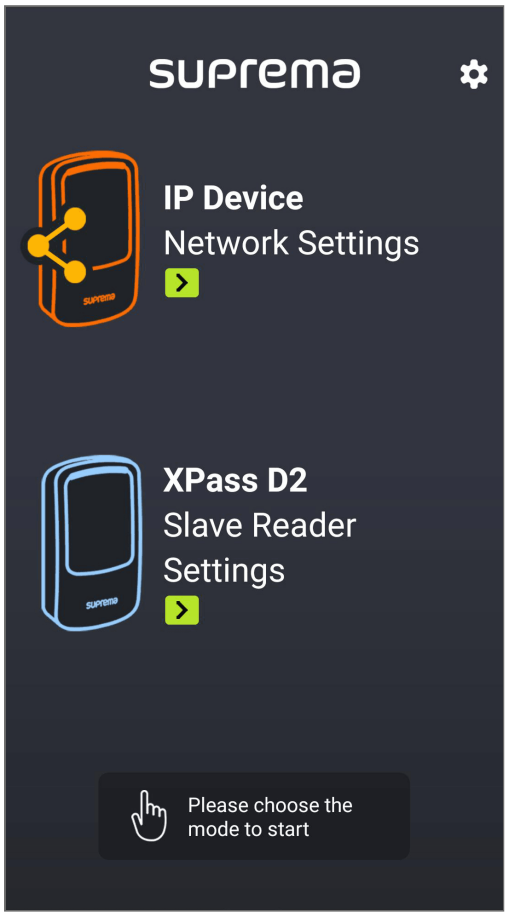
Guidance on how to select a device and manage app settings.

Select device

Select the device to configure using Suprema Device Manager.

You can select an IP device or XPass D2, and the options available for configuration will vary depending on the selected device.

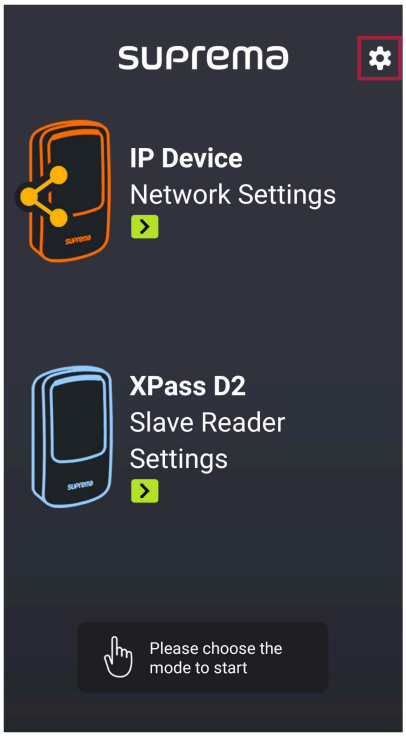
1. Install the **Suprema Device Manager** application on the mobile device of the device manager. Suprema Device Manager is available for download from the **App Store** and **Play Store**.
2. Run the Suprema Device Manager on your mobile device.
3. Select the device to configure.

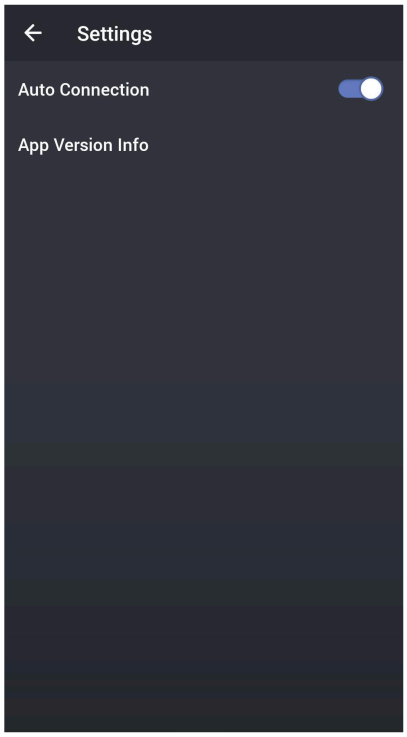


Configuring app settings

You can configure the automatic device connection feature or check the app version information.

1. Run the Suprema Device Manager on your mobile device.
2. Select ⚙ on the main screen.





- **Auto Connection**: You can enable or disable the automatic device connection feature.
- **App Version Info**: You can check the current app version and license information.

Set Up IP Device

You can change the settings of the IP device. You can change settings quickly and conveniently compared to changing settings via the management program on a PC or using command cards.

> **Info**
> Some settings may not apply if the device's firmware version is low. To apply all settings, refer to Upgrade device firmware to upgrade the firmware.

Change device settings

You can change the device's network, server, RS-485, LED and buzzer, and other settings.

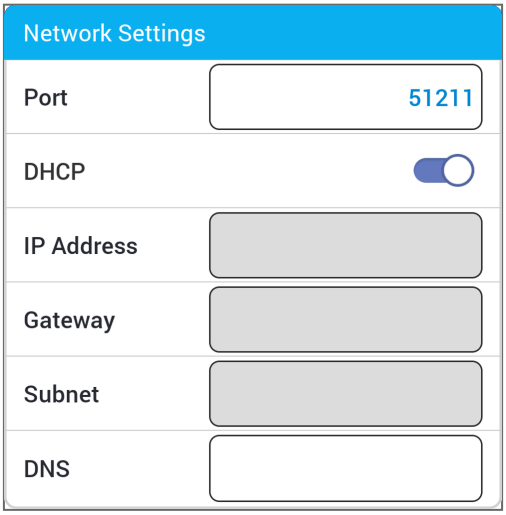
> **Info**
> Biometric devices only support network and server settings.

1. Enable Bluetooth on your mobile device and run Suprema Device Manager.
2. Select the IP device from the main screen.
3. Check the device ID to select the device from the list of connectable devices, or bring the mobile device closer to the device to connect.
4. After setting the device password, press **OK**. Tap  to display the entered password.

   > **Info**
   > - The device password can be set to a number of 6-32 characters.
   > - Be careful not to lose the device password. If you lose the device password, you must initialize the device to connect to it.

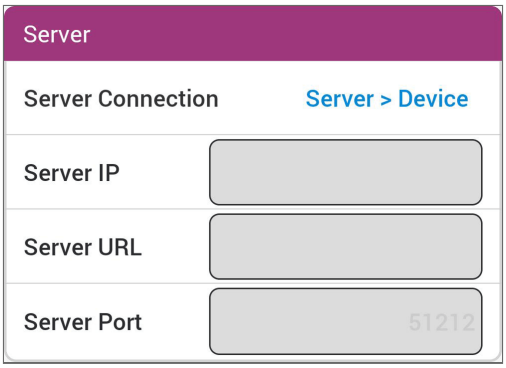
5. After setting each item, press **Apply Device** to save.

Network settings



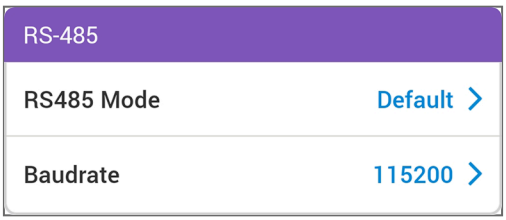
- **Port**: Enter the port that the device will use.
- **DHCP**: Enable this to allow the device to use dynamic IP. If you enable this option, you cannot enter network information manually.
- **IP Address**, **Gateway**, **Subnet**: Enter the network information for the device.
- **DNS**: Enter the DNS server address.

Server



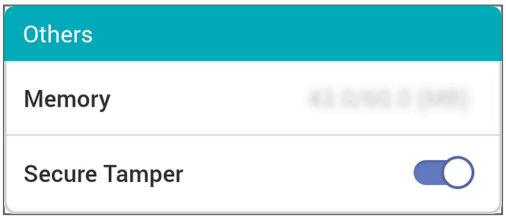
- **Server Connection**: You can set the server communication method. To search and connect the device from the server, select **Server > Device**. To set the server information to connect the device, select **Device > Server**.
- **Server IP**: Enter the server's IP address.
- **Server URL**: Enter the server's domain address.
- **Server Port**: Enter the server's port.

RS-485



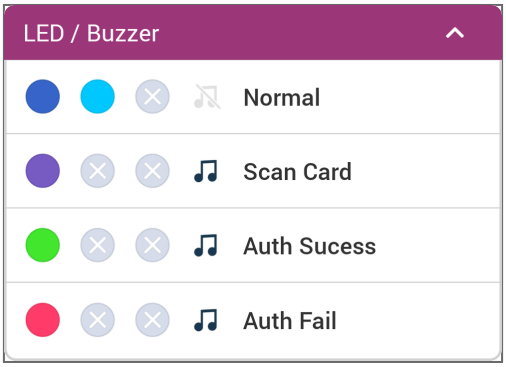
- **RS485 Mode**: Set the RS-485 mode.
- **Baudrate**: Set the RS-485 transmission speed.

Others



- **Memory**: You can check the memory usage status.
- **Secure Tamper**: If a tamper event occurs on the device, it can be set to delete all stored user information, logs, and security keys. To use the security tamper feature, activate it.

LED / Buzzer



- **Normal**: You can set the colors displayed on the device LED during normal operation.
- **Scan Card**: You can set the color displayed on the device LED and the number of times the buzzer sound plays when scanning a card.
- **Auth Sucess**: You can set the color displayed on the device LED and the number of times the buzzer sound plays upon successful authentication.
- **Auth Fail**: You can set the color displayed on the device LED and the number of times the buzzer sound plays upon failed authentication.

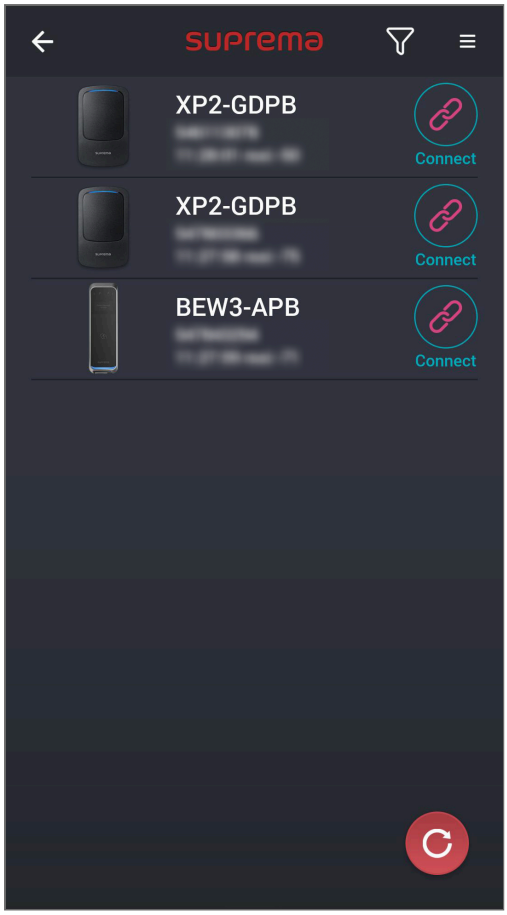
Info

- LED can be set to display a maximum of three colors in alternating patterns. Press the slot to choose a color.
- Selecting skips the color sequence for that slot and displays the color set for the next slot.

Connect device

You can search for and connect to installed IP devices nearby. When connected to Suprema Device Manager, you can upgrade the device's firmware, restart the device, initialize settings, initialize device settings excluding network settings, change the administrator password, and use various features.

1. Enable Bluetooth on your mobile device and run Suprema Device Manager.
2. Select the IP device from the main screen. A list of connectable devices will appear.



3. Select a device by checking the device ID in the device list or bring your mobile device close to the device to connect.
4. Enter the connection password. Tap to display the entered password.
5. Press **OK** to complete the device connection.

Info

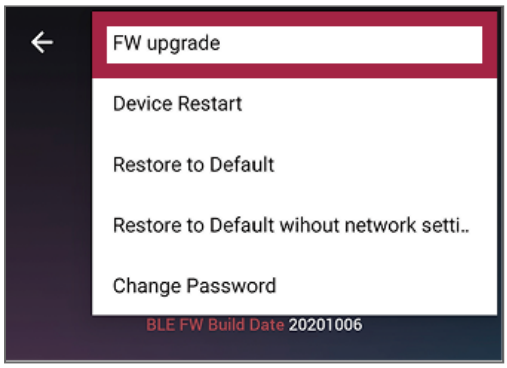
Device Filter: At the top of the device list screen, press to set it to display only the desired devices in the list.

Upgrade device firmware

You can easily upgrade the device's firmware.

> **Info**
>
> - To upgrade the firmware, you need to download the firmware file to your mobile device. The latest firmware can be downloaded from the Suprema Download Center.
> - During the firmware upgrade, keep the distance between the device and mobile device within 1m.
> - Only XPass 2 and XPass 2 V2 include support for the firmware upgrade feature.

1. Refer to Connect device to connect to the device for firmware upgrade.
2. Tap ⋮ → **FW upgrade**.

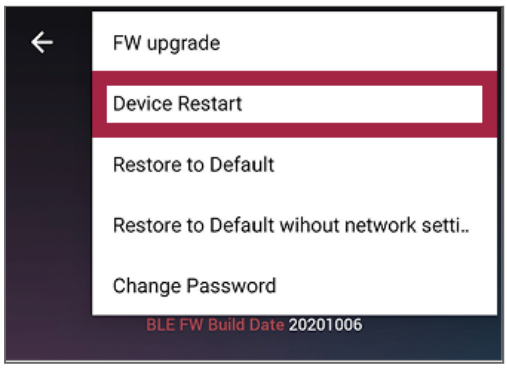


3. Select the firmware from the path where the firmware file is saved. The firmware upgrade is in progress.
4. Press **OK** to complete the firmware upgrade.

Restart device

You can restart the device.

1. Refer to Connect device to connect to the device to restart.
2. Tap ⋮ → **Device Restart**.



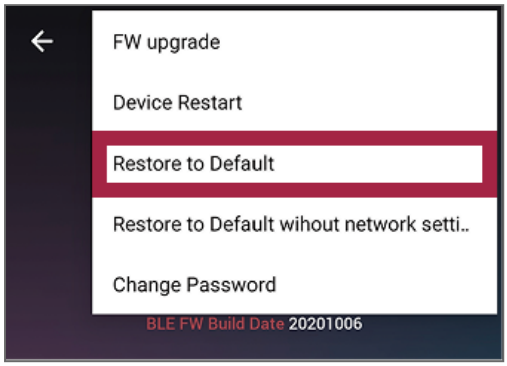
3. When you restart the device, the BLE communication connection with the mobile device will be disconnected. To reconnect automatically, enable the **Auto Connection** feature. For detailed configuration instructions, refer to

Configuring app settings.

Initialize settings

You can initialize device settings.

1. Refer to Connect device to connect to the device to initialize the settings.
2. Tap ⋮ → **Restore to Default**.

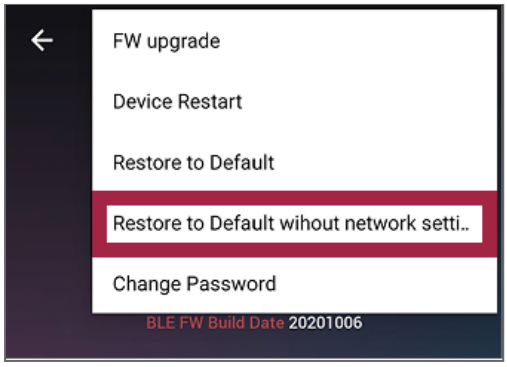


3. If the device is initialized, all settings are restored to their default values. Press **OK** to continue.

Initialize device settings excluding network

You can initialize device settings excluding network settings.

1. Refer to Connect device to connect to the device to initialize device settings excluding network settings.
2. Tap ⋮ → **Restore to Default without network settings**.



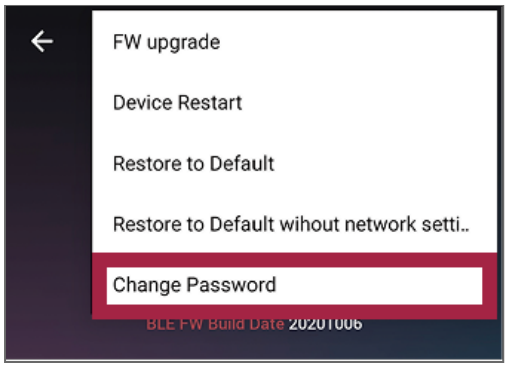
3. If you initialize device settings excluding network, the remaining settings excluding the network will be initialized. Press **OK** to continue.

Change device password

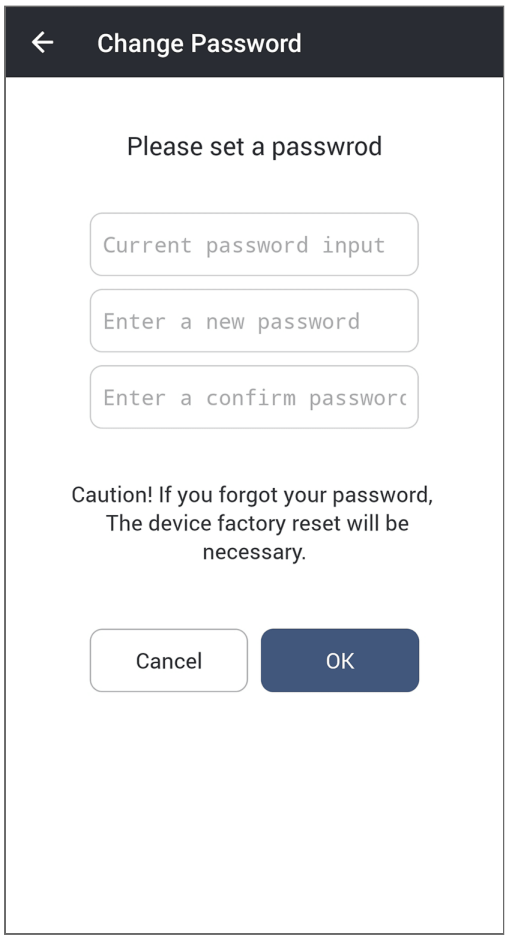
You can change the device's password.

1. Refer to Connect device to connect to the device to change password.

2. Tap ⋮ → **Change Password**.



3. Enter the current password and the new password you will use.



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

Info

- The device password can be set to a number of 6-32 characters.
- Be careful not to lose the device password. If you lose the device password, you must initialize the device to connect to it.

Set Up XPass D2

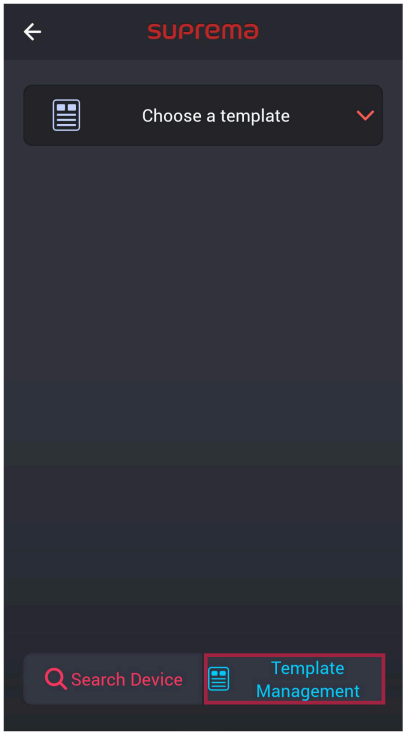
You can configure settings to apply to XPass D2 as a template and then directly apply them to individual devices. You can apply settings much faster than by accessing the management program on a PC or using command cards.

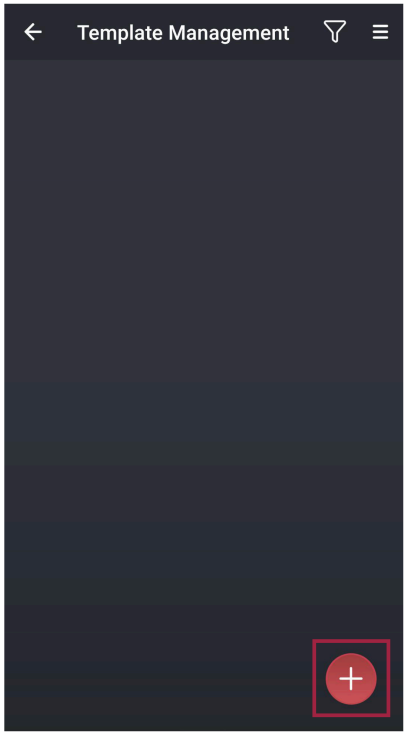
> **Info**
> Some settings may not apply if the device's firmware version is low. To apply all settings, upgrade the firmware. See Upgrade device firmware.

Add template

You can set RS-485 communication, card format, keypad settings, PIN, LED, and buzzer before adding them as a template. Adding a template allows you to quickly and easily apply settings without configuring each individual device every time.

1. Run the Suprema Device Manager on your mobile device.
2. Select XPass D2 on the main screen.
3. Tap **Template Management** → ⊕.





4. Select the device model for which you want to create the template.
5. After configuring each item, click **Save** to save the template.

> **Info**
> You can add up to 100 templates.

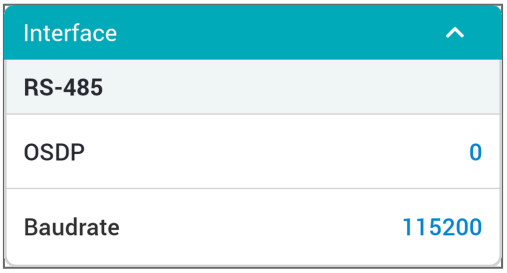
Set Template Name and Admin Password



- **Template Name**: Enter the desired template name.
- **Admin Password**: Enter the administrator password.

> **Info**
>
> - The administrator password can be set to 6-32 digits.
> - Be careful not to lose the administrator password. If you lose the administrator password, you will need to initialize the device to connect to the device with the applied template.
> - For more information on changing the administrator password, refer to Change admin password.

Interface



- **OSDP**: Set the OSDP address to be used in communication between the device and the master device. Can be set to numbers from 0~126.
- **Baudrate**: Set the RS-485 transmission speed.

Authentication

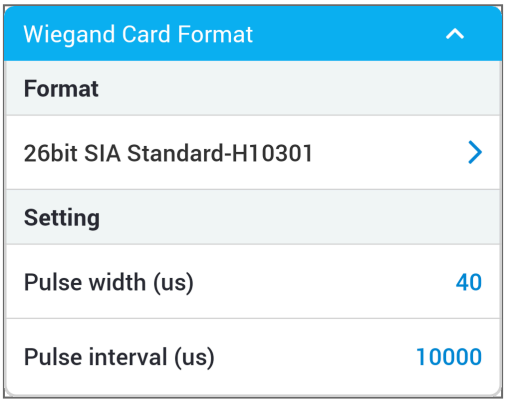


- **Card Type**: You can set the type of card to be used by the device.
  - **CSN Card**: You can select the CSN card type and set the byte order.
  - **Suprema Smart Card**: You can select the types of smart cards issued by Suprema.
  - **Custom Smart Card**: You can select the types of smart cards issued by third parties.
  - **Mobile**: You can set the mobile card type.

Info

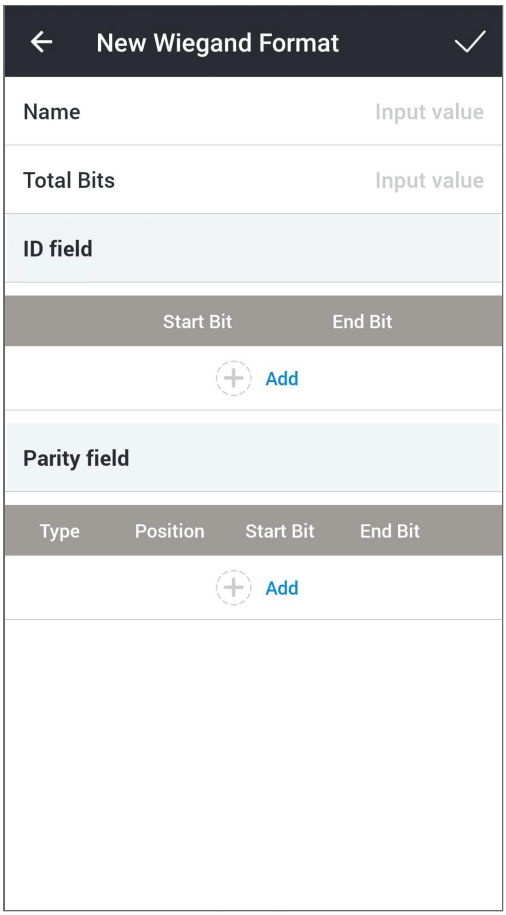
When set to **MSB**, card data is processed in left-to-right order, sequentially processing from large byte to small byte order when saving the card's serial number (CSN). **LSB** processes the card's serial number (CSN) from small byte to large byte order when saving it.

Wiegand Card Format



- **Format**: You can set the Wiegand card format to be specified for the device. The card data is processed according to the set format.

- **New Wiegand Format**: If the desired format is not available, you can click + to add a new Wiegand format.

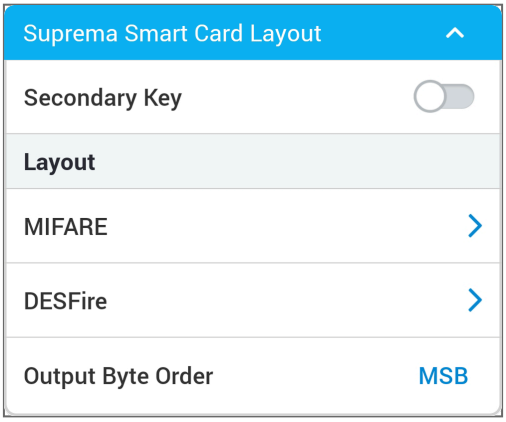


  - **Name**: Enter the name of the desired Wiegand format.
  - **Total Bits**: Enter the total number of bits.
  - **ID field**: Enter the start and end bits of the ID you wish to use. Tap **Add** to add an ID field.
  - **Parity field**: Enter the position of the parity field and the start and end bits you wish to use. Tap **Add** to add a parity field.

    Info
    To add a parity field, enter the total bits.

- **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.

Suprema Smart Card Layout

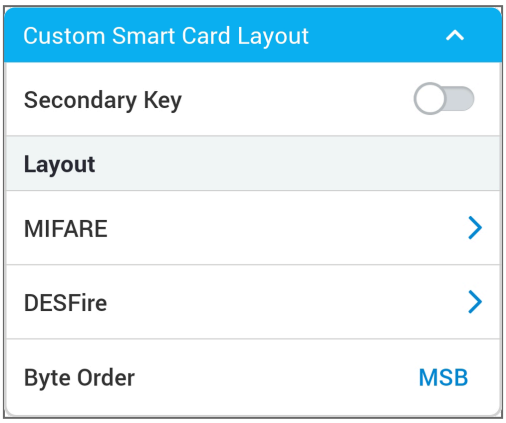


- **Secondary Key**: You can set whether to use the auxiliary site key. By setting the auxiliary site key, you can use it for authentication when the card's main key does not match.
- **MIFARE**: You can set up MIFARE cards.
  - **Security Level**: You can set the encryption type to SL1 or SL3.
  - **Primary Key**: The key that encrypts communication between smart cards and the device.
  - **Secondary Key**: You can use it to authenticate when the card's main site key does not match. The auxiliary site key field is only displayed when **Secondary Key** from the previous depth is activated.
  - **Start Block Index**: Select the starting block where each template will be stored. This block is the index of the block where user information is stored; set it to a storable block if the user is already using the smart card. Can only be set for MIFARE.
- **DESFire**: You can set up DESFire cards.
  - **DESFire Advanced**: You can use DESFire cards issued by third parties. Only DESFire can be configured.
  - **Primary Key**: The key that encrypts communication between smart cards and the device.
  - **Secondary Key**: You can use it to authenticate when the card's main site key does not match. The auxiliary site key field is only displayed when **Secondary Key** from the previous depth is activated.
  - **App ID**: Set the application ID. Serves as a kind of directory that includes a file ID. Only DESFire can be configured.
  - **File ID**: Set the file ID. Only DESFire can be configured.
  - **Encryption Type**: You can set the encryption type to DES/3DES or AES.
  - **Enforce EV2/EV3 Secure Messaging**: Enable this option to force secure messaging when authenticating to the device with DESFire EV2 or EV3 cards. This option is only available when **Encryption Type** is set to AES.
- **Output Byte Order**: You can set the byte order for smart card output.

Info

- To use **DESFire Advanced**, please accurately enter the information for **App Master Key**, **App Master Key Index**, **File Read Access Key**, **File Read Access Key Index**, **App ID**, **File ID**, **Encryption Type**.
- **App Master Key**, **File Read Access Key** can only accept up to 32 bytes of hexadecimal.
- When set to **MSB**, card data is processed in left-to-right order, sequentially processing from large byte to small byte order when saving the card's serial number (CSN). **LSB** processes the card's serial number (CSN) from small byte to large byte order when saving it.

Custom Smart Card Layout



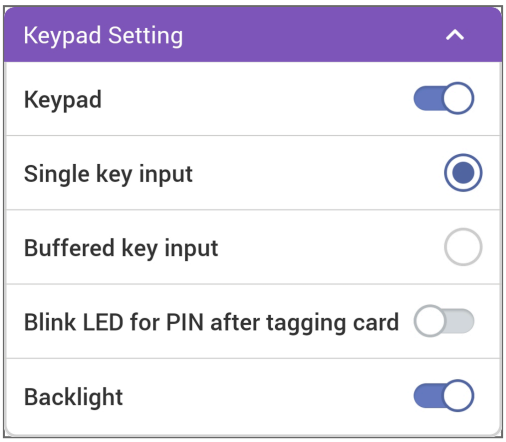
- **Secondary Key**: You can set whether to use the auxiliary site key. By setting the auxiliary site key, you can use it for authentication when the card's main key does not match.
- **MIFARE**: You can set up MIFARE cards.
  - **Security Level**: You can set the encryption type to SL1 or SL3.
  - **Primary Key**: The key that encrypts communication between smart cards and the device.
  - **Secondary Key**: You can use it to authenticate when the card's main site key does not match. The auxiliary site key field is only displayed when **Secondary Key** from the previous depth is activated.
  - **Block Index**: Select the starting block where each template will be stored. This block is the index of the block where user information is stored; set it to a storable block if the user is already using the smart card. Can only be set for MIFARE.
  - **Skip Bytes**: You can set the starting point for reading the card number.
  - **Data Size**: (If the set values of **Primary Key** and **Secondary Key** are the same as the values of the card) You can set the size of the data to read from the card.
- **DESFire**: You can set up DESFire cards.
  - **DESFire Advanced**: You can use DESFire cards issued by third parties. Only DESFire can be configured.
  - **Primary Key**: The key that encrypts communication between smart cards and the device.
  - **Secondary Key**: You can use it to authenticate when the card's main site key does not match. The auxiliary site key field is only displayed when **Secondary Key** from the previous depth is activated.
  - **App ID**: Set the application ID. Serves as a kind of directory that includes a file ID. Only DESFire can be configured.

  - **File ID**: Set the file ID. Only DESFire can be configured.
  - **Encryption Type**: You can set the encryption type to DES/3DES or AES.
  - **Skip Bytes**: You can set the starting point for reading the card number.
  - **Data Size**: (If the set values of **Primary Key** and **Secondary Key** are the same as the values of the card) You can set the size of the data to read from the card.
  - **Enforce EV2/EV3 Secure Messaging**: Enable this option to force secure messaging when authenticating to the device with DESFire EV2 or EV3 cards. This option is only available when **Encryption Type** is set to AES.

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

> **Info**
>
> - To use **DESFire Advanced**, please accurately enter the information for **App Master Key**, **App Master Key Index**, **File Read Access Key**, **File Read Access Key Index**, **App ID**, **File ID**, **Encryption Type**.
> - **App Master Key**, **File Read Access Key** can only accept up to 32 bytes of hexadecimal.
> - When set to **MSB**, card data is processed in left-to-right order, sequentially processing from large byte to small byte order when saving the card's serial number (CSN). **LSB** processes the card's serial number (CSN) from small byte to large byte order when saving it.

Keypad Setting

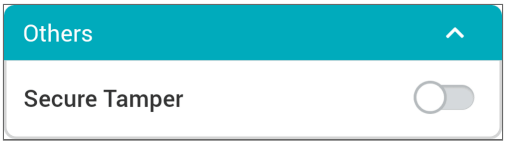


- **Keypad**: You can set whether to use the keypad. When the keypad is activated, you can authenticate by entering the card ID using the keypad.
- **Single key input**: Each time you press a key while entering the card ID on the keypad, the value will be sent.
- **Buffered key input**: When entering the card ID on the keypad, all keys need to be pressed, and then press the `#` key to send the entire value at once.
- **Blink LED for PIN after tagging card**: When the device's authentication mode is set to card + PIN, pressing the card will activate the LED to prompt the user to enter the PIN.
- **Backlight**: You can turn the keypad backlight on or off.

Info

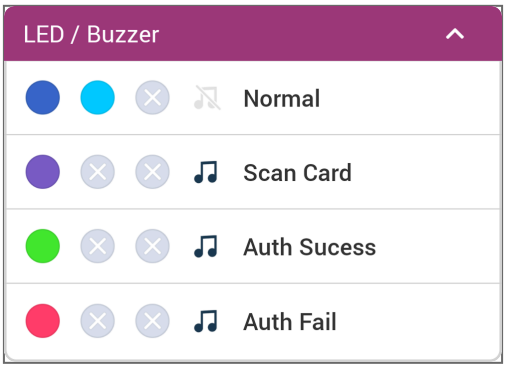
- **Keypad Setting** is only displayed on the template setting screen of the XPD2-GKDB device.
- **Backlight** is only supported on XPD2-GKDB hardware V02M and firmware version v1.7.1 or higher.
- Values entered through the keypad are transmitted in 4-bit units by default. Card IDs entered through the keypad are sent in the same format as the Wiegand card format.

Others



- **Secure Tamper**: You can set it so that when a tamper event occurs in the device, the security key stored in the device will be deleted. To use the security tamper feature, activate it.

LED / Buzzer



- **Normal**: You can set the colors displayed on the device LED during normal operation.
- **Scan Card**: You can set the color displayed on the device LED and the number of times the buzzer sound plays when scanning a card.
- **Auth Sucess**: You can set the color displayed on the device LED and the number of times the buzzer sound plays upon successful authentication.
- **Auth Fail**: You can set the color displayed on the device LED and the number of times the buzzer sound plays upon failed authentication.

Info

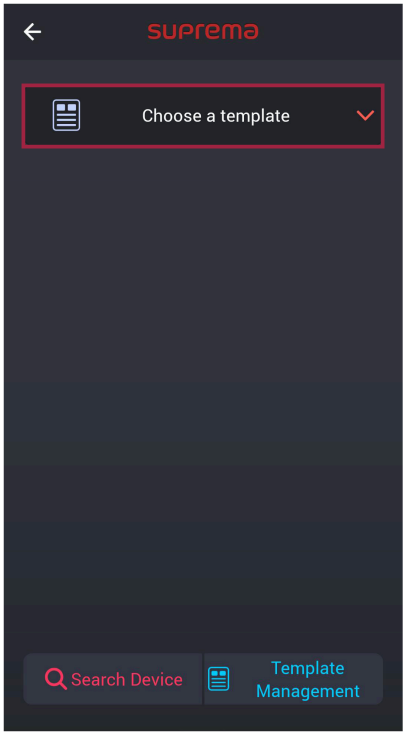
- LED can be set to display a maximum of three colors in alternating patterns. Press the slot to choose a color.
- Selecting ⊗ skips the color sequence for that slot and displays the color set for the next slot.

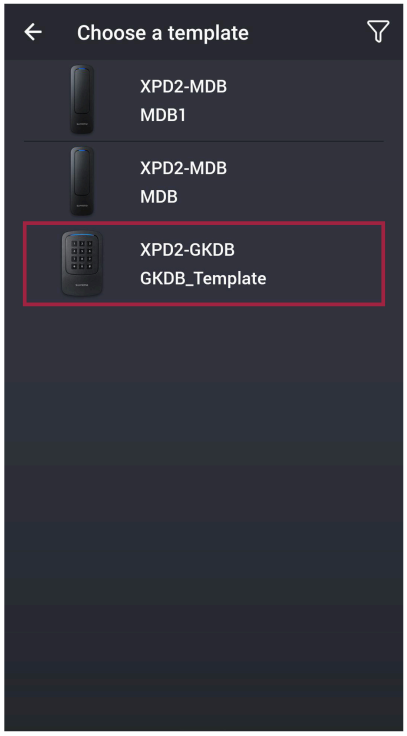
Apply template

The added templates can be applied uniformly to multiple devices via BLE communication.

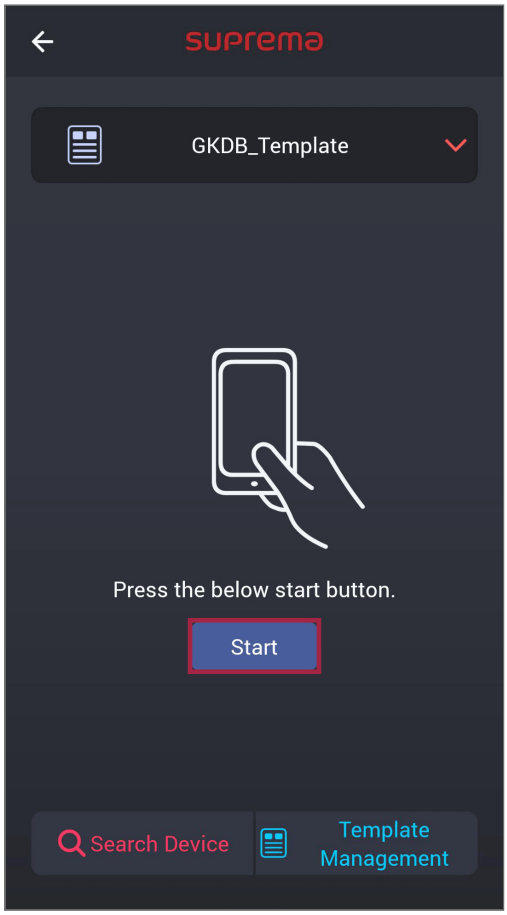
> **Info**
> Some settings may not apply if the device's firmware version is low. To apply all settings, upgrade the firmware. See Upgrade device firmware.

1. Enable Bluetooth on your mobile device and run Suprema Device Manager.
2. Select XPass D2 on the main screen.
3. Click **Choose a template**. A list of available templates will appear.





4. Select the desired template from the list of templates.
5. Click **Start** to continue.



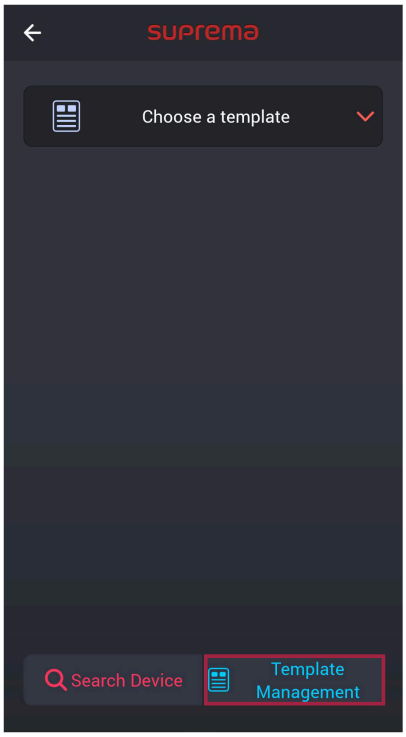
6. Make sure the back of your mobile device touches the device to which you want to apply the template.
7. Once the template application is complete, click **OK**.

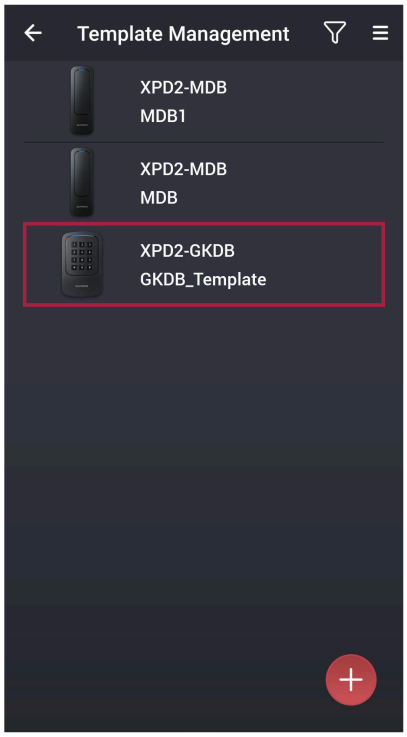
> **Info**
>
> - Settings changed using Suprema Device Manager are only applied to the device and will not be synchronized with the server.
> - If the device is connected to the master device or if the Wiegand output settings have changed, it cannot be connected to Suprema Device Manager with the main key. To connect with Suprema Device Manager, you must initialize the device.

Manage templates

Edit template

1. Run the Suprema Device Manager on your mobile device.
2. Select XPass D2 on the main screen.
3. Click **Template Management**.

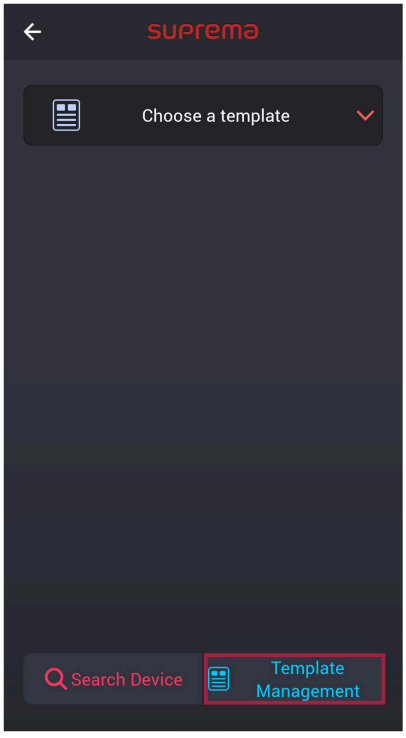


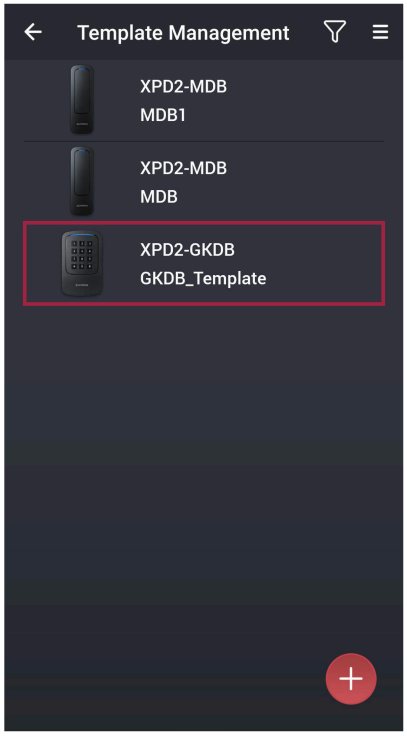


4. Select the template you want to edit from the list of templates.
5. Refer to Add template to edit the template.
6. To save the changed settings, click **Save**; to save as a new template, click **Save as new template**.

Delete template

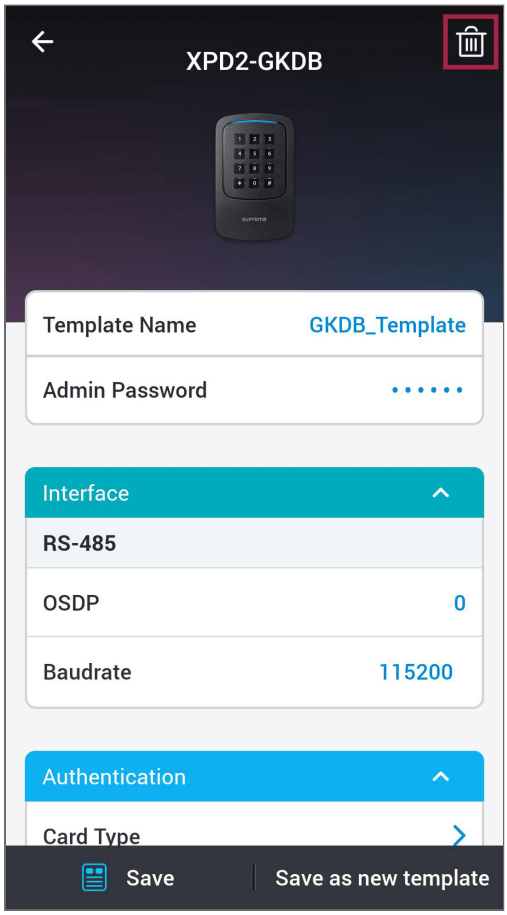
1. Run the Suprema Device Manager on your mobile device.
2. Select XPass D2 on the main screen.
3. Click **Template Management**.





4. Select the template you wish to delete from the list of templates.

5. Tap → **OK** to delete a template.



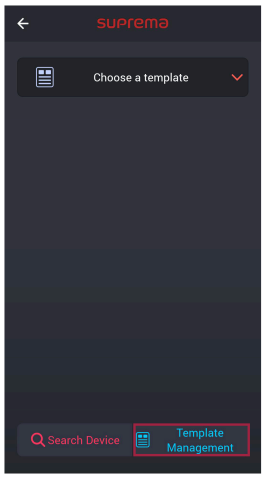
Export template

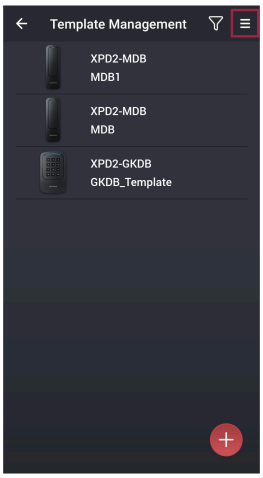
You can export templates for XPass D2 settings from the app.

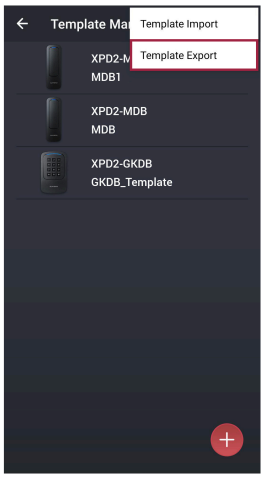
1. Run the Suprema Device Manager on your mobile device.

2. Select XPass D2 on the main screen.

3. Click **Template Management**.

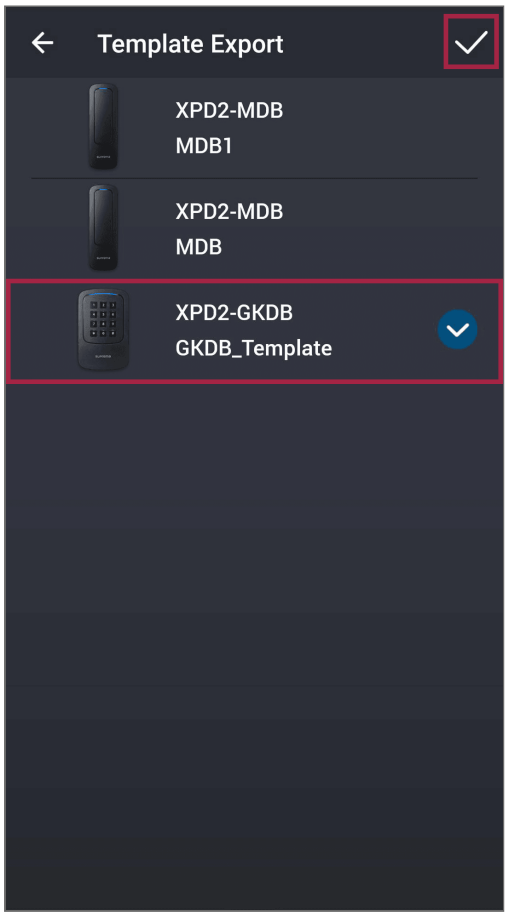






4. At the top of the template list, tap ☰ and select **Template Export**.

5. After selecting the template to export, tap ✓.

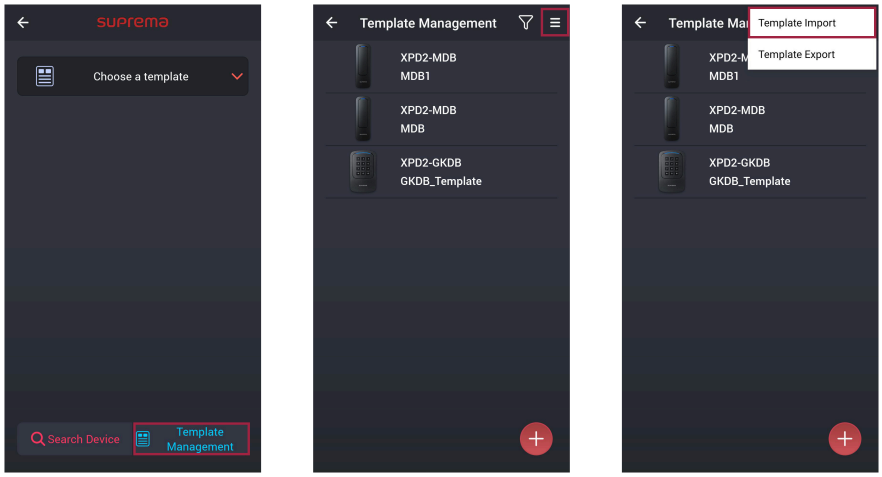


> **Info**
> Template files are saved to the following folder on your mobile device.
> - **Android**: Download → DeviceManager_TemplateFiles
> - **iOS**: Device

Import template

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

1. Run the Suprema Device Manager on your mobile device.
2. Select XPass D2 on the main screen.
3. Click **Template Management**.



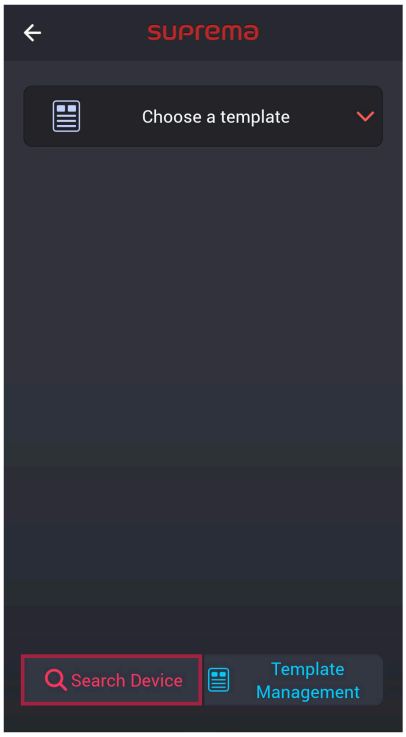
4. At the top of the template list, tap ☰ and select **Template Import**.
5. Select the template you want to import from the folder where the templates are stored.

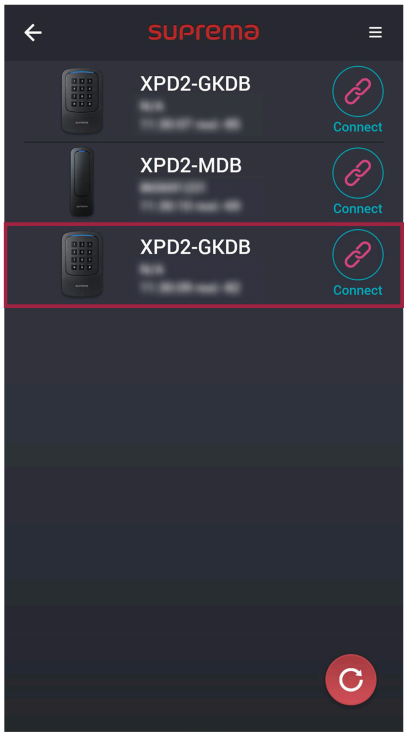
> **Info**
> Template files are saved to the following folder on your mobile device.
> - **Android**: Download → DeviceManager_TemplateFiles
> - **iOS**: Device

Search and connect device

You can search for and connect to XPass D2 installed nearby. By connecting to Suprema Device Manager, you can upgrade the firmware of the device or use features such as restarting the device or changing the template password.

1. Enable Bluetooth on your mobile device and run Suprema Device Manager.
2. Select XPass D2 on the main screen.
3. Click **Search Device**. A list of connectable devices will appear.





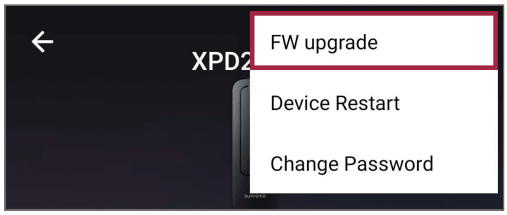
4. Select a device by checking the device ID in the device list or bring your mobile device close to the device to connect.
5. Enter the connection password. Tap to display the entered password.
6. Press **OK** to complete the device connection.

Upgrade device firmware

You can easily upgrade the device's firmware.

> **Info**
>
> - To upgrade the firmware, you need to download the firmware file to your mobile device. The latest firmware can be downloaded from the Suprema Download Center.
> - During the firmware upgrade, keep the distance between the device and mobile device within 1m.

1. Refer to Search and connect device to connect to the device you want to upgrade the firmware.
2. Tap → **FW upgrade**.

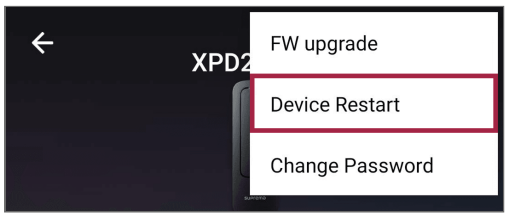


3. Select the firmware from the path where the firmware file is saved. The firmware upgrade is in progress.
4. Press **OK** to complete the firmware upgrade.

Restart device

You can restart the device.

1. Refer to Search and connect device to connect to the device you want to restart.
2. Tap ⋮ → **Device Restart**.

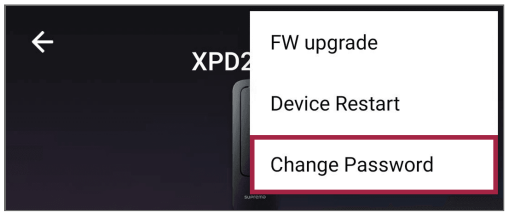


3. When you restart the device, the BLE communication connection with the mobile device will be disconnected. To reconnect automatically, enable the **Auto Connection** feature. For detailed configuration instructions, refer to Configuring app settings.

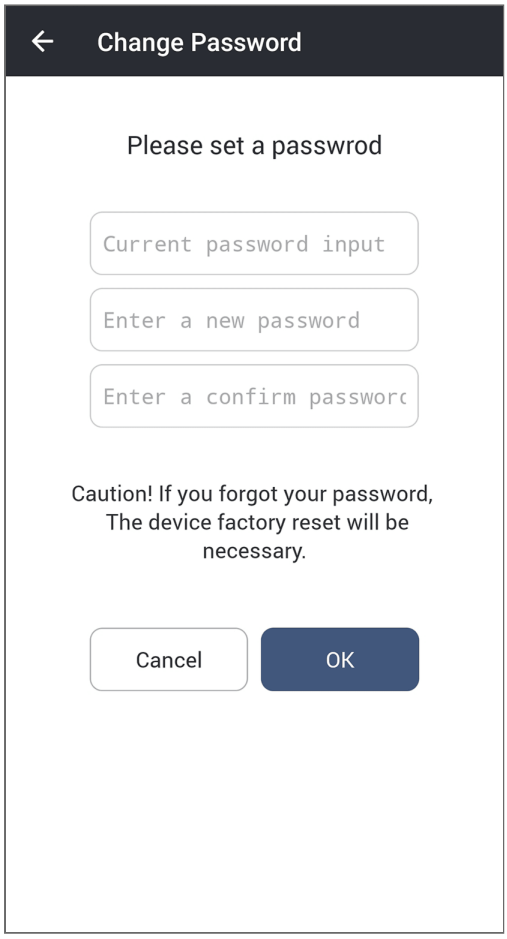
Change admin password

You can change the admin password of the template.

1. Refer to Search and connect device to connect to the device with the template where you want to change the password.
2. Tap ⋮ → **Change Password**.



3. Enter the current password and the new password you will use.



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

Info

- The administrator password can be set to 6-32 digits.
- Be careful not to lose the administrator password. If you lose the administrator password, you will need to initialize the device to connect to the device with the applied template.

Appendices

Includes legal notices contained in the product.

Disclaimers

- Information in this web site 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 web site.
- 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 for this website is owned by Suprema. Rights to other product names, trademarks, and registered trademarks belong to the respective individuals or organizations that own them.

Open Source License

- This product contains open-source software. Source code subject to GPL, LGPL, MPL, and other open source licenses requiring source code distribution can be requested from the Suprema Technical Support Team.
- The source code of this product can be requested from the Suprema Technical Support Team for 3 years from the final delivery date of the product.
- 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.
- For more information about the Android and iOS licenses included in this product, please see Android and 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

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

© 2026 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.