Suprema Device Manager
ユーザーガイド

バージョン 1.09

日本語
JA 102.00.DM

suprema
SECURITY & BIOMETRICS

目次

はじめに 4

最小要件 4

デバイスを初期設定する 6

デバイスを選択する 6

アプリを設定する 6

IPデバイスを設定する 8

デバイス設定を変更する 8

デバイスを接続する 11

デバイスのファームウェアをアップグレードする 11

デバイスを再起動する 12

設定を初期化する 13

ネットワーク以外のデバイス設定を初期化する 13

デバイスパスワードを変更する 13

XPass D2 を設定する 15

テンプレートを追加する 15

テンプレートを適用する 22

テンプレートを管理する 24

デバイスの検索と接続 28

デバイスのファームウェアをアップグレードする 29

デバイスを再起動する 12

管理者パスワードを変更する 30

付録 32

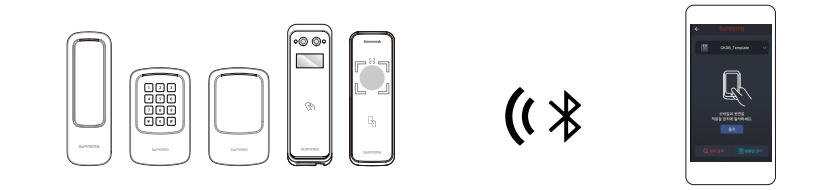
免責事項 32

著作権に関するお知らせ 33

オープンソースライセンス 33

はじめに

Suprema Device Manager は、BLE 通信を使ってシュプリマの XPass D2、XPass 2、XPass 2 V2、BioEntry W3、XPass Q2 を設定できるモバイルアプリケーションです。



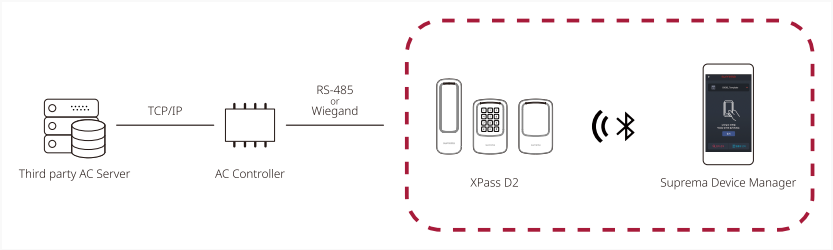
XPass D2 / XPass 2 / XPass 2 V2 / BioEntry W3 / XPass Q2　　Suprema Device Manager

管理者は PC でサーバーに接続したり装置を物理的に取り外したりすることなく、モバイルデバイスから装置のネットワーク、サーバー、RS-485 通信、カード形式、キーパッド設定、PIN、LED、ブザーを設定でき、装置の再起動やファームウェアアップグレード、装置設定の初期化などの機能も利用できます。

また、XPass D2 では、一度設定した値をテンプレートとして保存し、複数の装置に迅速かつ簡単に適用できます。

情報

Suprema Device Manager を使用すると、他社コントローラーと構成された XPass D2 の設定を現場で直接変更できます。



最小要件

モバイルデバイス

モバイルデバイスが BLE 通信に対応しているか確認してください。

- Android 5.0 Lollipop 以上
- iOS 15 以上

装置とファームウェア

互換性のある装置とファームウェアバージョンを確認してください。

- XPass D2 ファームウェア 1.1.0 以上
- XPass 2

  - XP2-MDPB、XP2-GDPB、XP2-GKDPB：ファームウェア 1.0.0 以上
  - XP2-MAPB：ファームウェア 1.4.1 以上
  - XP2-MAPB-H：ファームウェア 1.4.3 以上
- **XPass 2 V2** ファームウェア 1.0.0 以上
- **BioEntry W3** ファームウェア 1.0.1 以上
- **XPass Q2** ファームウェア 1.0.0 以上

情報

- 互換性のある装置とファームウェアは変更される場合があります。
- 装置のファームウェアが上記のバージョンより古い場合は、BioStar X でファームウェアをアップグレードしてください。装置をスレーブ装置として使用している場合、接続されているマスター装置のファームウェアも BioStar 2 2.7.0 以上と互換性のある最新バージョンである必要があります。
- デバイスのファームウェアアップグレードの詳細については、IPデバイス（デバイスのファームウェアをアップグレードする）、XPass D2（デバイスのファームウェアをアップグレードする）、または BioStar X 管理者マニュアルをご参照ください。

デバイスを初期設定する

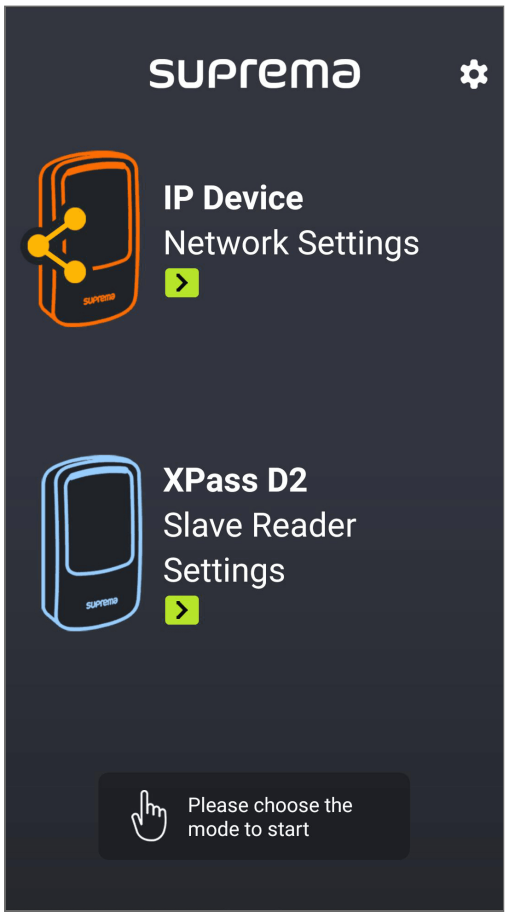
デバイスの選択とアプリ設定の管理方法を案内します。

デバイスを選択する

Suprema Device Manager を使用して設定するデバイスを選択します。

IP デバイスまたは XPass D2 を選択でき、選択したデバイスによって設定できる項目が異なります。

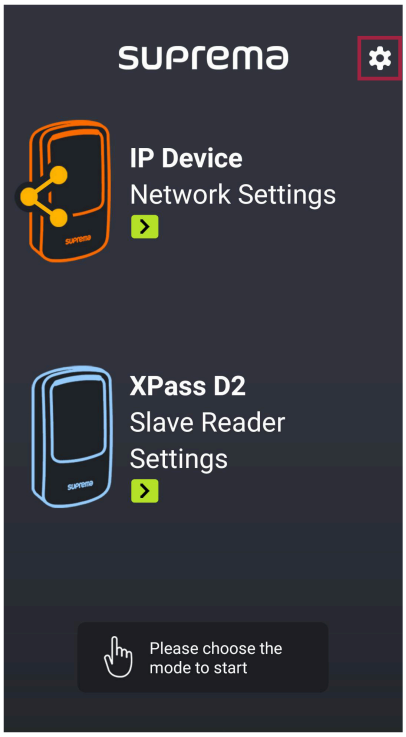
1. デバイス管理者のモバイル端末に **Suprema Device Manager** アプリケーションをインストールします。 **Suprema Device Manager** は **App Store** と **Play ストア** からダウンロードできます。
2. モバイル端末で Suprema Device Manager を起動します。
3. 設定するデバイスを選択します。

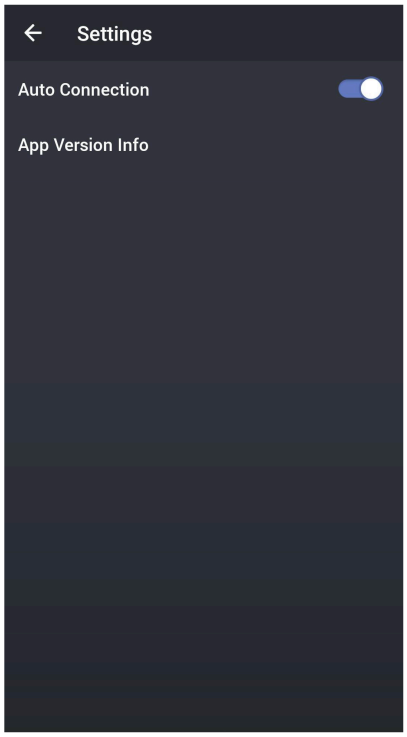


アプリを設定する

デバイス自動接続機能を設定したり、アプリのバージョン情報を確認できます。

1. モバイル端末で Suprema Device Manager を起動します。
2. メイン画面で ⚙ を選択します。





- **Auto Connection**：デバイス自動接続機能を有効化または無効化できます。
- **App Version Info**：アプリの現在のバージョンとライセンス情報を確認できます。

IPデバイスを設定する

IPデバイスの設定を変更できます。 PCで管理プログラムに接続して設定を変更したり、コマンドカードを使用する方法よりも、より迅速かつ便利に設定を変更できます。

> **情報**
> デバイスのファームウェアバージョンが低い場合、いくつかの設定が適用されないことがあります。すべての設定を適用するには、デバイスのファームウェアをアップグレードするを参照してファームウェアをアップグレードしてください。

デバイス設定を変更する

デバイスのネットワーク、サーバー、RS-485、LEDおよびブザー、その他の設定を変更できます。

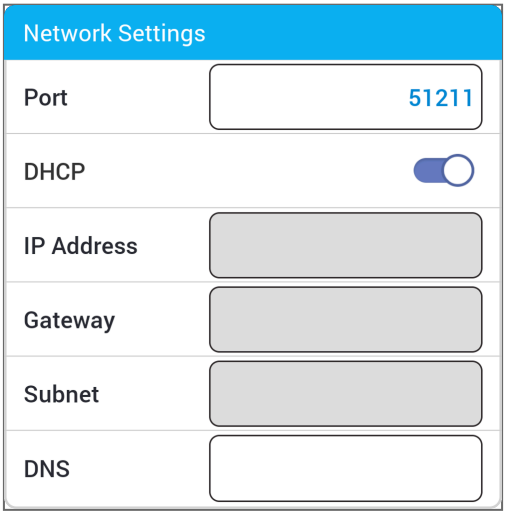
> **情報**
> バイオ認証デバイスはネットワークとサーバー設定のみをサポートします。

1. モバイル機器で Bluetooth 機能を有効にした後、Suprema Device Manager を起動してください。
2. メイン画面で IP デバイスを選択します。
3. 接続可能なデバイス一覧でデバイスIDを確認してデバイスを選択するか、接続するデバイスにモバイル端末を近づけます。
4. デバイスパスワードを設定した後、**OK** をタップします。入力したパスワードを画面に表示するには  を押します。

   > **情報**
   > - デバイスパスワードは 6～32 桁の数字で設定できます。
   > - デバイスパスワードを紛失しないよう注意してください。デバイスパスワードを紛失した場合、デバイスに接続するにはそのデバイスを初期化する必要があります。

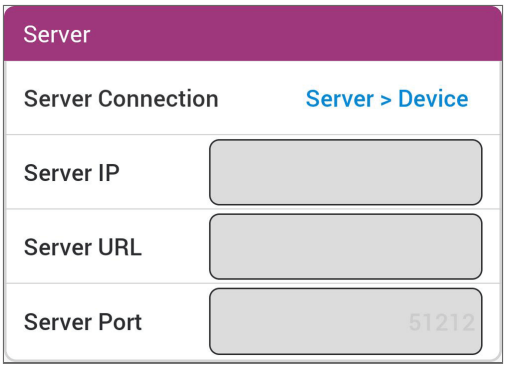
5. 各項目を設定したら、保存するために **Apply Device** をタップします。

ネットワーク設定



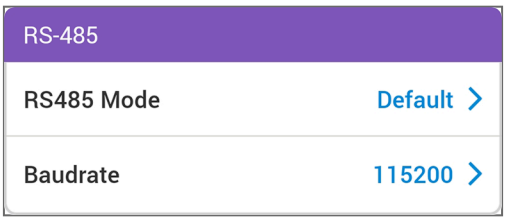
- **Port**：デバイスが使用するポートを入力します。
- **DHCP**：デバイスで DHCP を使用する場合は有効にします。このオプションを有効にすると、ネットワーク情報を直接入力できません。
- **IP Address**、**Gateway**、**Subnet**：デバイスのネットワーク情報を入力します。
- **DNS**：DNS サーバーアドレスを入力します。

サーバー



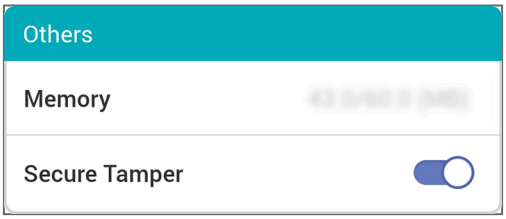
- **Server Connection**：サーバー通信方式を設定できます。サーバーからデバイスを検索して接続する場合は **Server > Device** を選択します。デバイス側で接続先サーバー情報を設定する場合は **Device > Server** を選択します。
- **Server IP**：サーバーの IP アドレスを入力します。
- **Server URL**：サーバーのドメインアドレスを入力します。
- **Server Port**：サーバーのポートを入力します。

RS-485



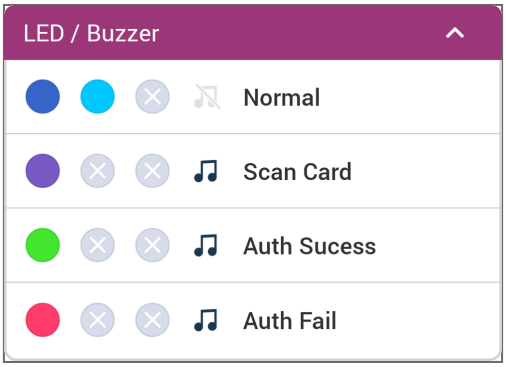
- **RS485 Mode**：RS-485 モードを設定します。
- **Baudrate**：RS-485 の転送速度を設定します。

その他



- **Memory**：メモリ使用状況を確認できます。
- **Secure Tamper**：デバイスでタンパーイベントが発生した場合、保存されている全ユーザー情報、全ログ、セキュリティキーを削除するように設定できます。セキュリティタンパー機能を使用するには有効にしてください。

LED / ブザー



- **Normal**：通常時にデバイスLEDに表示される色を設定できます。
- **Scan Card**：デバイスにカードをスキャンする際にデバイスLEDに表示される色とブザー音の再生回数を設定できます。
- **Auth Sucess**：認証成功時にデバイスLEDに表示される色とブザー音の再生回数を設定できます。
- **Auth Fail**：認証失敗時にデバイスLEDに表示される色とブザー音の再生回数を設定できます。

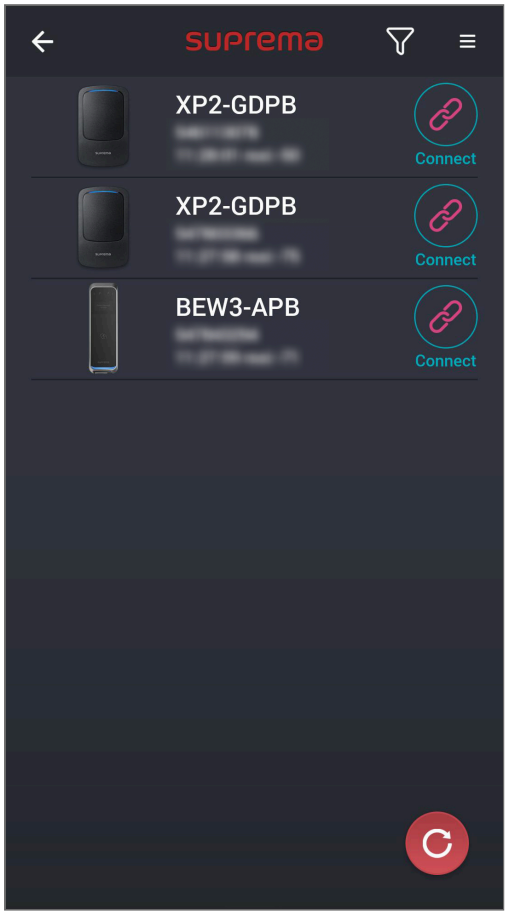
情報

- LED は最大 3 色を交互に繰り返し表示するよう設定できます。スロットを押して色を選択してください。
- を選択すると、該当スロットの色表示順序をスキップし、次の順序のスロットに設定された色が表示されます。

デバイスを接続する

周辺に設置されたIPデバイスを検索して接続できます。 Suprema Device Managerに接続すると、デバイスのファームウェアアップグレード、デバイス再起動、設定初期化、ネットワークを除く設定の初期化、管理者パスワード変更など、さまざまな機能を利用できます。

1. モバイル機器で Bluetooth 機能を有効にした後、Suprema Device Manager を起動してください。
2. メイン画面で IP デバイスを選択します。接続可能なデバイスの一覧が表示されます。



3. デバイス一覧でデバイス ID を確認してデバイスを選択するか、接続するデバイスにモバイル機器を近づけます。
4. 接続パスワードを入力します。入力したパスワードを画面に表示するには を押します。
5. デバイスの接続を完了するには **OK** を押します。

> **情報**
>
> **Device Filter**：デバイス一覧画面の上部で をタップして、目的のデバイスのみが一覧に表示されるように設定できます。

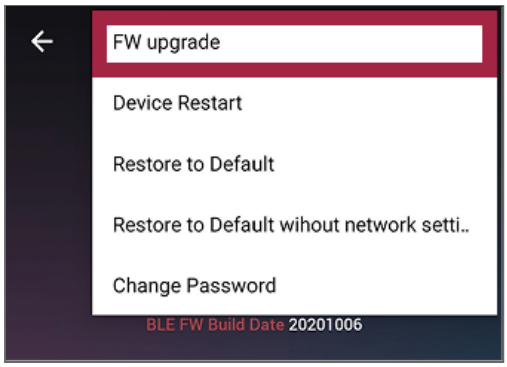
デバイスのファームウェアをアップグレードする

デバイスのファームウェアを簡単にアップグレードできます。

情報

- ファームウェアをアップグレードするには、モバイル機器にファームウェアファイルをダウンロードする必要があります。最新ファームウェアは Suprema ダウンロードセンターからダウンロードできます。
- ファームウェアのアップグレード中は、デバイスとモバイル機器の距離を 1 m 以内に保ってください。
- ファームウェアアップグレード機能は、XPass 2、XPass 2 V2 のみ対応しています。

1. デバイスを接続するを参照して、ファームウェアをアップグレードするデバイスに接続します。
2. ⋮ → **FW upgrade** を押します。

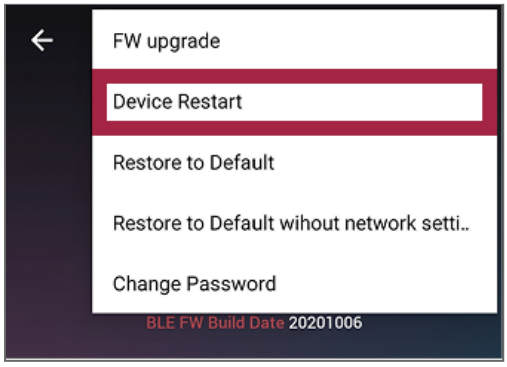


3. ファームウェアファイルが保存されているパスでファームウェアを選択します。ファームウェアのアップグレードが実行されます。
4. ファームウェアのアップグレードを完了するには **OK** を押します。

デバイスを再起動する

デバイスを再起動できます。

1. デバイスを接続するを参照して、再起動するデバイスに接続します。
2. ⋮ → **Device Restart** を押します。

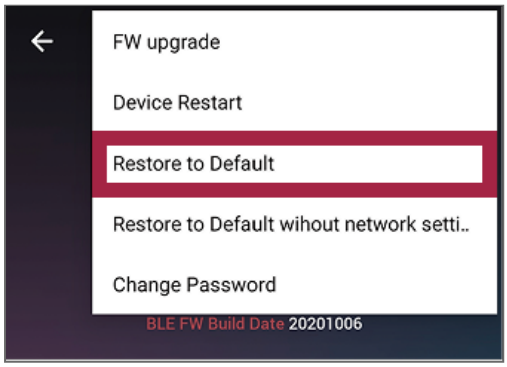


3. デバイスを再起動すると、モバイル機器との BLE 通信が切断されます。自動で再接続するには、**Auto Connection** 機能を有効にします。詳細な設定方法はアプリを設定するを参照してください。

設定を初期化する

デバイス設定を初期化できます。

1. デバイスを接続するを参照して、設定を初期化するデバイスに接続します。
2. ⋮→ **Restore to Default** をタップします。

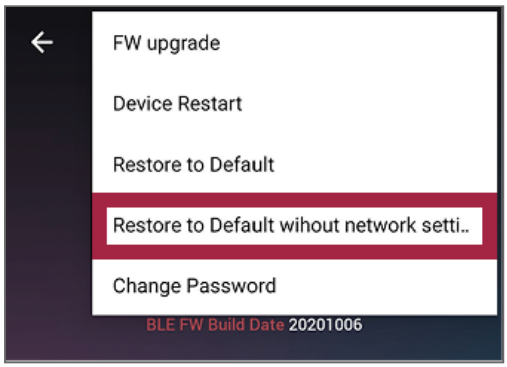


3. 機器を初期化すると、すべての設定がデフォルト値に復元されます。続行するには **OK** をタップします。

ネットワーク以外のデバイス設定を初期化する

ネットワーク設定を除くデバイス設定を初期化できます。

1. デバイスを接続するを参照して、ネットワーク設定を除く設定を初期化するデバイスに接続します。
2. ⋮→ **Restore to Default without network settings** をタップします。

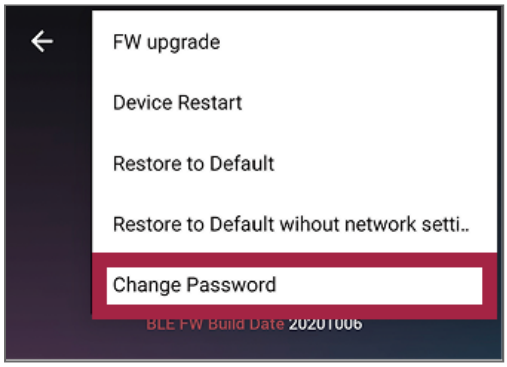


3. ネットワーク以外のデバイス設定を初期化すると、ネットワークを除くその他の設定が初期化されます。続行するには **OK** をタップします。

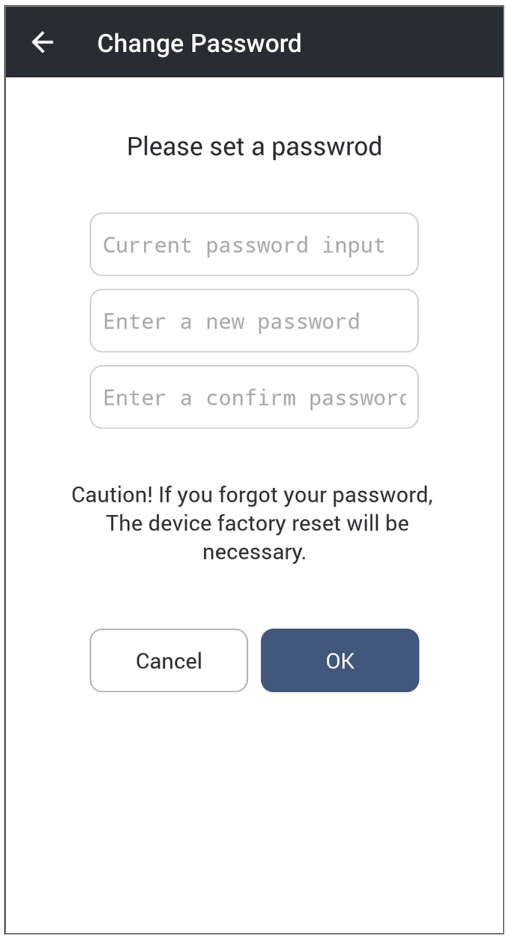
デバイスパスワードを変更する

デバイスのパスワードを変更できます。

1. デバイスを接続するを参照して、パスワードを変更するデバイスに接続します。
2. ⋮→ **Change Password** を押します。



3. 現在のパスワードと新しいパスワードを入力します。



4. パスワードの変更を完了するには **OK** を押します。

情報

- デバイスパスワードは 6〜32 桁の数字で設定できます。
- デバイスパスワードを紛失しないよう注意してください。デバイスパスワードを紛失した場合、デバイスに接続するにはそのデバイスを初期化する必要があります。

XPass D2 を設定する

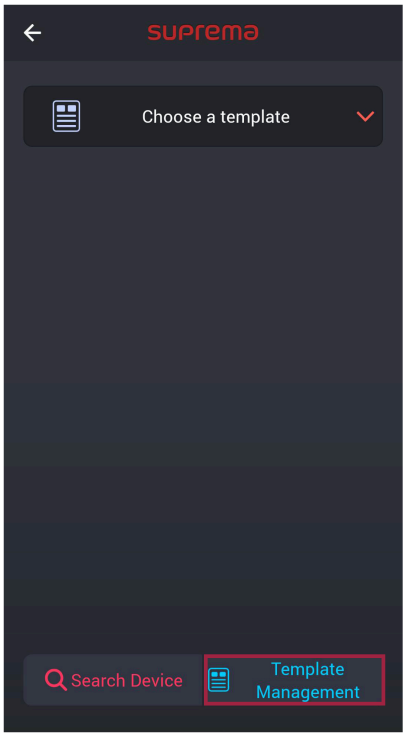
XPass D2 に適用する設定をあらかじめテンプレートとして作成し、個別デバイスに直接適用できます。 PC で管理プログラムに接続して設定を変更したりコマンドカードを使用する方法と比べて、はるかに速く設定を適用できます。

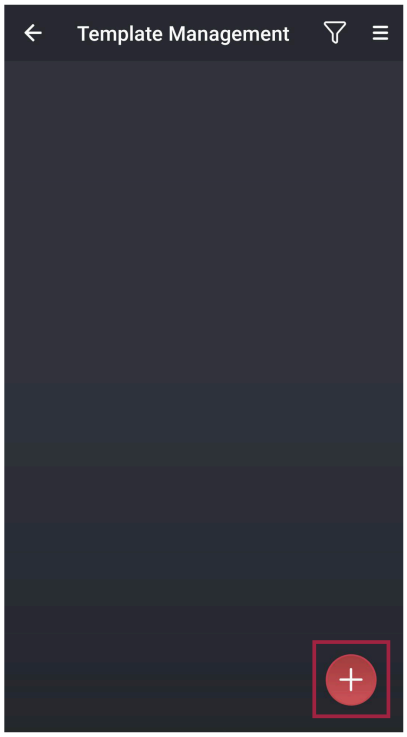
> **情報**
> デバイスのファームウェアバージョンが低い場合、いくつかの設定が適用されないことがあります。すべての設定を適用するには、デバイスのファームウェアをアップグレードするを参照してファームウェアをアップグレードしてください。

テンプレートを追加する

RS-485 通信、カード形式、キーパッド設定、PIN、LED、ブザーなどを設定した後、テンプレートとして追加できます。テンプレートを追加すると、複数の個別デバイスを毎回設定せずに、迅速かつ簡単に設定を適用できます。

1. モバイル端末で Suprema Device Manager を起動します。
2. メイン画面で XPass D2 を選択します。
3. **Template Management** → ⊕ を押します。





4. テンプレートを作成するデバイスモデルを選択します。
5. 各項目を設定した後、テンプレートを保存するには **Save** を押します。

> **情報**
> テンプレートは最大 100 個まで追加できます。

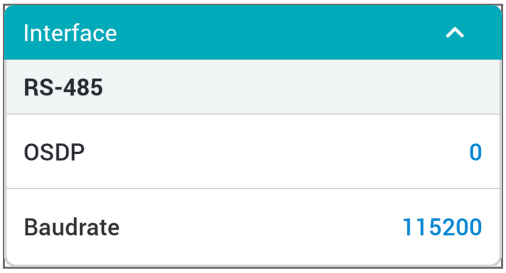
テンプレート名および管理者パスワードの設定



- **Template Name**：希望するテンプレート名を入力します。
- **Admin Password**：管理者パスワードを入力します。

> **情報**
>
> - 管理者パスワードは 6〜32 桁の数字で設定できます。
> - 管理者パスワードを紛失しないよう注意してください。管理者パスワードを紛失した場合、テンプレートを適用したデバイスに接続するにはそのデバイスを初期化する必要があります。
> - 管理者パスワードの変更について詳しくは、管理者パスワードを変更するを参照してください。

インターフェース



- **OSDP**：デバイスとマスターデバイスの通信で使用する OSDP アドレスを設定します。 0〜126 の数値で設定できます。
- **Baudrate**：RS-485 の転送速度を設定します。

認証

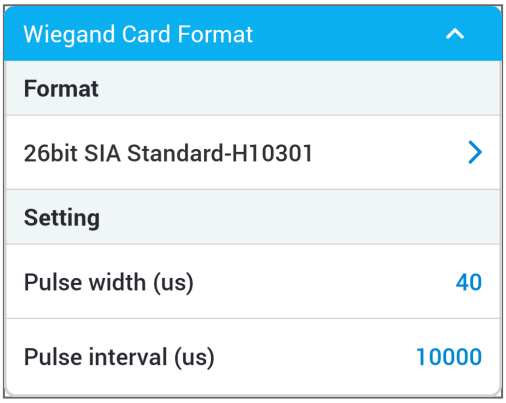


- **Card Type**：デバイスで使用するカードタイプを設定できます。
  - **CSN Card**：CSN カードタイプを選択し、バイト順序を設定できます。
  - **Suprema Smart Card**：Suprema が発行したスマートカードタイプを選択できます。
  - **Custom Smart Card**：他社が発行したスマートカードタイプを選択できます。
  - **Mobile**：モバイルカードタイプを設定できます。

情報

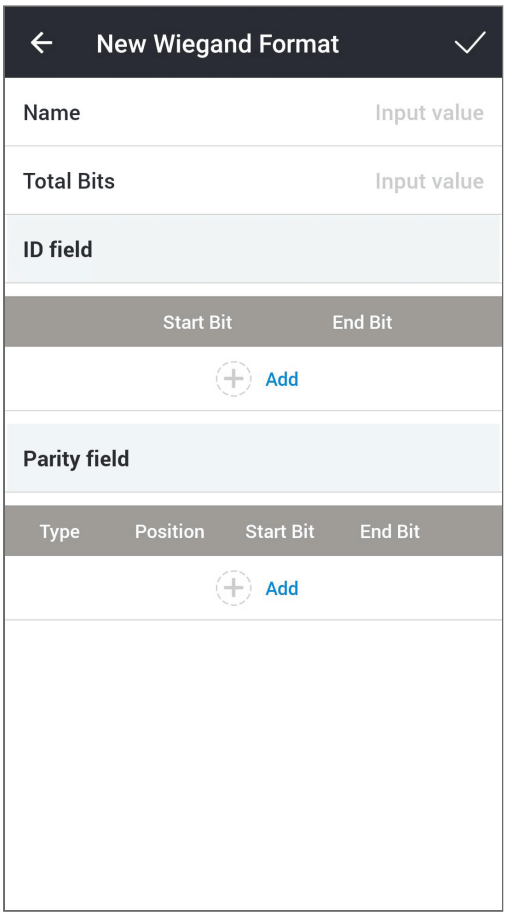
バイト順序を **MSB** に設定すると、カードデータを処理する際に上位バイトから下位バイトの順に処理し、カードのシリアル番号（CSN）を保存するときに左から右へ順に処理します。 **LSB** は下位バイトから上位バイトの順に処理し、カードのシリアル番号（CSN）を保存します。

ウィーガンドカードフォーマット



- **Format**：デバイスに指定する Wiegand カード形式を設定できます。設定した形式でカードデータが処理されます。

- **New Wiegand Format**：希望するフォーマットがない場合、＋ を押して新しい Wiegand フォーマットを追加できます。

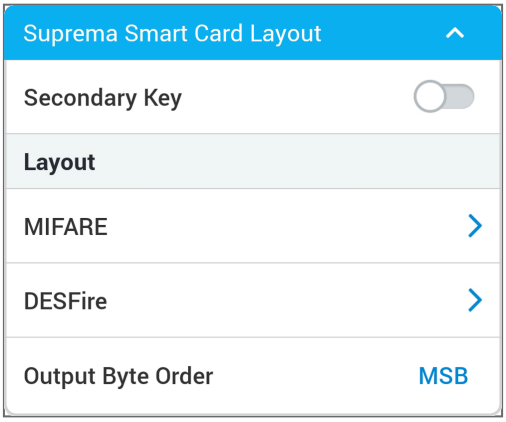


  - **Name**：希望する Wiegand フォーマットの名前を入力します。
  - **Total Bits**：合計ビット数を入力します。
  - **ID field**：使用する ID の開始ビットと終了ビットを入力します。 **Add** を押すと、ID フィールドを追加できます。
  - **Parity field**：使用するパリティフィールドの位置と開始ビット、終了ビットを入力します。 **Add** を押すと、パリティフィールドを追加できます。

> **情報**
> パリティフィールドを追加するには、合計ビット数を入力します。

- **Pulse width (µs)**：Wiegand 信号のパルス幅を設定できます。
- **Pulse interval (µs)**：Wiegand 信号のパルス間隔を設定できます。

Suprema スマートカードレイアウト

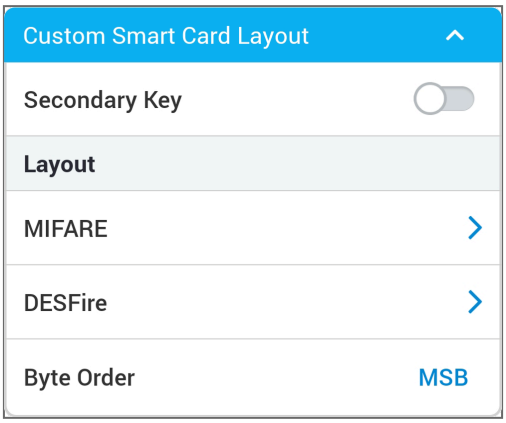


- **Secondary Key**：補助サイトキーの使用有無を設定できます。補助サイトキーを設定すると、カードの基本キーが一致しない場合に補助サイトキーを使用して認証を実行できます。
- **MIFARE**：MIFARE カードを設定できます。
  - **Security Level**：セキュリティレベルを SL1 または SL3 に設定できます。
  - **Primary Key**：スマートカードとデバイス間の通信を暗号化するキーです。
  - **Secondary Key**：カードの基本サイトキーが一致しない場合に使用して認証を実行できます。補助サイトキーの項目は、前レベルの **Secondary Key** を有効にしたときのみ表示されます。
  - **Start Block Index**：各テンプレートを保存する開始ブロックを選択します。このブロックはユーザー情報を保存するブロックのインデックスです。既にスマートカードを使用している場合は、保存可能なブロックを設定します。 MIFARE のみ設定できます。
- **DESFire**：DESFire カードを設定できます。
  - **DESFire Advanced**：他社が発行した DESFire カードを使用できます。 DESFire のみ設定します。
  - **Primary Key**：スマートカードとデバイス間の通信を暗号化するキーです。
  - **Secondary Key**：カードの基本サイトキーが一致しない場合に使用して認証を実行できます。補助サイトキーの項目は、前レベルの **Secondary Key** を有効にしたときのみ表示されます。
  - **App ID**：アプリケーションIDを設定してください。ファイルIDを含む一種のディレクトリとして機能します。 DESFire のみ設定します。
  - **File ID**：ファイルIDを設定してください。 DESFire のみ設定します。
  - **Encryption Type**：暗号化方式を DES/3DES または AES に設定できます。
  - **Enforce EV2/EV3 Secure Messaging**：このオプションを有効にすると、DESFire EV2、EV3 カードでデバイスに認証する際にセキュアメッセージングの使用を強制できます。 **Encryption Type** を AES に設定している場合のみ有効化できます。
- **Output Byte Order**：スマートカード出力のバイト順序を設定できます。

情報

- **DESFire Advanced** を使用するには、**App Master Key**、**App Master Key Index**、**File Read Access Key**、**File Read Access Key Index**、**App ID**、**File ID**、**Encryption Type** の情報を正確に入力してください。
- **App Master Key**、**File Read Access Key** は最大 32 バイトの 16 進数のみ入力できます。
- バイト順序を **MSB** に設定すると、カードデータを処理する際に上位バイトから下位バイトの順に処理し、カードのシリアル番号（CSN）を保存するときに左から右へ順に処理します。 **LSB** は下位バイトから上位バイトの順に処理し、カードのシリアル番号（CSN）を保存します。

カスタムスマートカードレイアウト



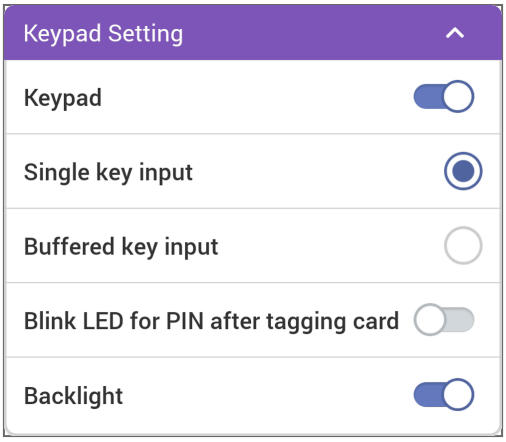
- **Secondary Key**：補助サイトキーの使用有無を設定できます。補助サイトキーを設定すると、カードの基本キーが一致しない場合に補助サイトキーを使用して認証を実行できます。
- **MIFARE**：MIFARE カードを設定できます。
  - **Security Level**：セキュリティレベルを SL1 または SL3 に設定できます。
  - **Primary Key**：スマートカードとデバイス間の通信を暗号化するキーです。
  - **Secondary Key**：カードの基本サイトキーが一致しない場合に使用して認証を実行できます。補助サイトキーの項目は、前レベルの **Secondary Key** を有効にしたときのみ表示されます。
  - **Block Index**：各テンプレートが保存される開始ブロックを選択してください。このブロックはユーザー情報を保存するブロックのインデックスです。既にスマートカードを使用している場合は、保存可能なブロックを設定します。 MIFARE のみ設定できます。
  - **Skip Bytes**：カード番号を読み取る開始位置を設定できます。
  - **Data Size**：（設定した **Primary Key** と **Secondary Key** がカードの設定値と同じ場合）読み取るカードのデータサイズを設定できます。
- **DESFire**：DESFire カードを設定できます。
  - **DESFire Advanced**：他社が発行した DESFire カードを使用できます。 DESFire のみ設定します。
  - **Primary Key**：スマートカードとデバイス間の通信を暗号化するキーです。
  - **Secondary Key**：カードの基本サイトキーが一致しない場合に使用して認証を実行できます。補助サイトキーの項目は、前レベルの **Secondary Key** を有効にしたときのみ表示されます。

  - **App ID**：アプリケーションIDを設定してください。ファイルIDを含む一種のディレクトリとして機能します。 DESFire のみ設定します。
  - **File ID**：ファイルIDを設定してください。 DESFire のみ設定します。
  - **Encryption Type**：暗号化方式を DES/3DES または AES に設定できます。
  - **Skip Bytes**：カード番号を読み取る開始位置を設定できます。
  - **Data Size**：（設定した **Primary Key** と **Secondary Key** がカードの設定値と同じ場合）読み取るカードのデータサイズを設定できます。
  - **Enforce EV2/EV3 Secure Messaging**：このオプションを有効にすると、DESFire EV2、EV3 カードでデバイスに認証する際にセキュアメッセージングの使用を強制できます。 **Encryption Type** を AES に設定している場合のみ有効化できます。

- **Byte Order**：スマートカード出力のバイト順序を設定できます。

> **情報**
>
> - **DESFire Advanced** を使用するには、**App Master Key**、**App Master Key Index**、**File Read Access Key**、**File Read Access Key Index**、**App ID**、**File ID**、**Encryption Type** の情報を正確に入力してください。
> - **App Master Key**、**File Read Access Key** は最大 32 バイトの 16 進数のみ入力できます。
> - バイト順序を **MSB** に設定すると、カードデータを処理する際に上位バイトから下位バイトの順に処理し、カードのシリアル番号（CSN）を保存するときに左から右へ順に処理します。 **LSB** は下位バイトから上位バイトの順に処理し、カードのシリアル番号（CSN）を保存します。

キーパッド設定

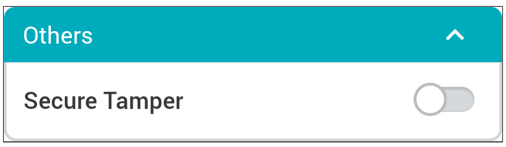


- **Keypad**：キーパッドの使用可否を設定できます。キーパッドを有効にすると、キーパッドでカードIDを入力して認証できます。
- **Single key input**：キーパッドでカードIDを入力する際、キーを押すたびに値を送信します。
- **Buffered key input**：キーパッドでカードIDを入力する際、すべてのキーを押した後に「#」キーを押すと、全値を一括で送信します。
- **Blink LED for PIN after tagging card**：デバイスの認証モードをカード＋PINに設定した場合、ユーザーがカードを提示するとLEDを動作させてPIN入力を促すことができます。
- **Backlight**：キーパッドのバックライトをオンまたはオフにできます。

情報

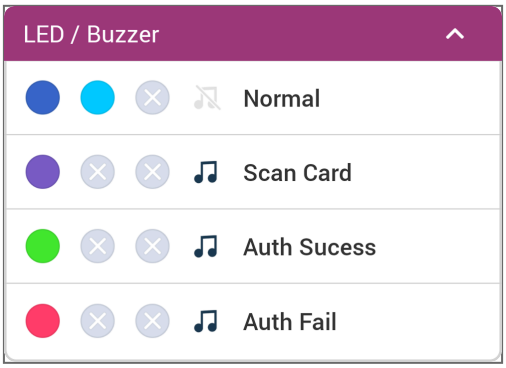
- **Keypad Setting** は XPD2-GKDB デバイスのテンプレート設定画面にのみ表示されます。
- **Backlight** は XPD2-GKDB ハードウェアV02M、ファームウェアv1.7.1以上でのみサポートされます。
- デバイスでキーパッドを通じて入力された値は、基本的に4ビット単位で送信されます。キーパッドで入力したカードIDは、Wiegandカード形式に従ってカードIDと同じ形式で送信されます。

その他



- **Secure Tamper**：デバイスでタンパーイベントが発生した場合、デバイスに保存されたセキュリティキーを削除するよう設定できます。セキュリティタンパー機能を使用するには有効にしてください。

LED / ブザー



- **Normal**：通常時にデバイスLEDに表示される色を設定できます。
- **Scan Card**：デバイスにカードをスキャンする際にデバイスLEDに表示される色とブザー音の再生回数を設定できます。
- **Auth Sucess**：認証成功時にデバイスLEDに表示される色とブザー音の再生回数を設定できます。
- **Auth Fail**：認証失敗時にデバイスLEDに表示される色とブザー音の再生回数を設定できます。

情報

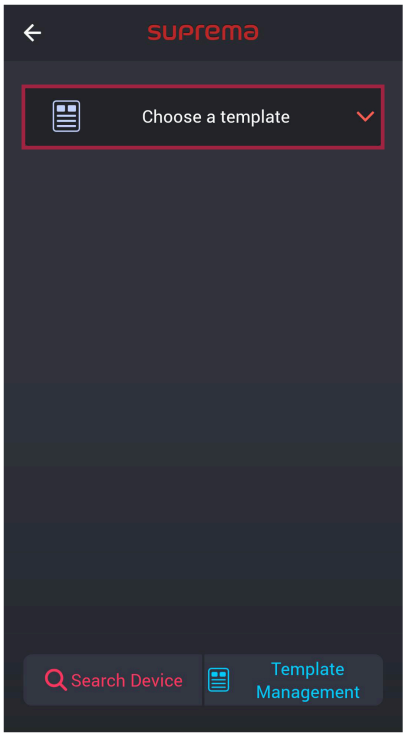
- LED は最大 3 色を交互に繰り返し表示するよう設定できます。スロットを押して色を選択してください。
- を選択すると、該当スロットの色表示順序をスキップし、次の順序のスロットに設定された色が表示されます。

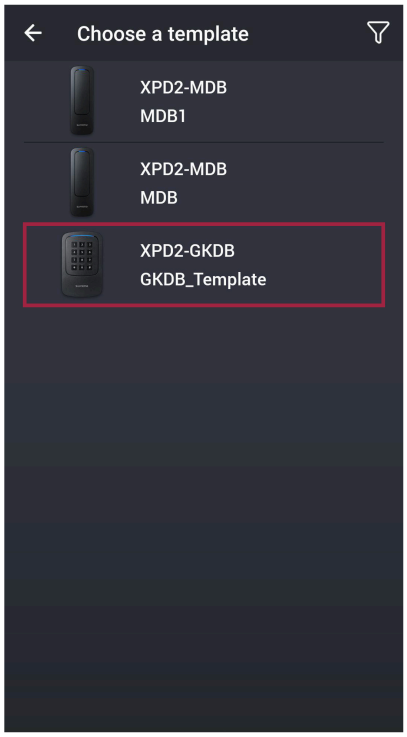
テンプレートを適用する

追加したテンプレートはBLE通信を利用して複数台のデバイスに同一に適用できます。

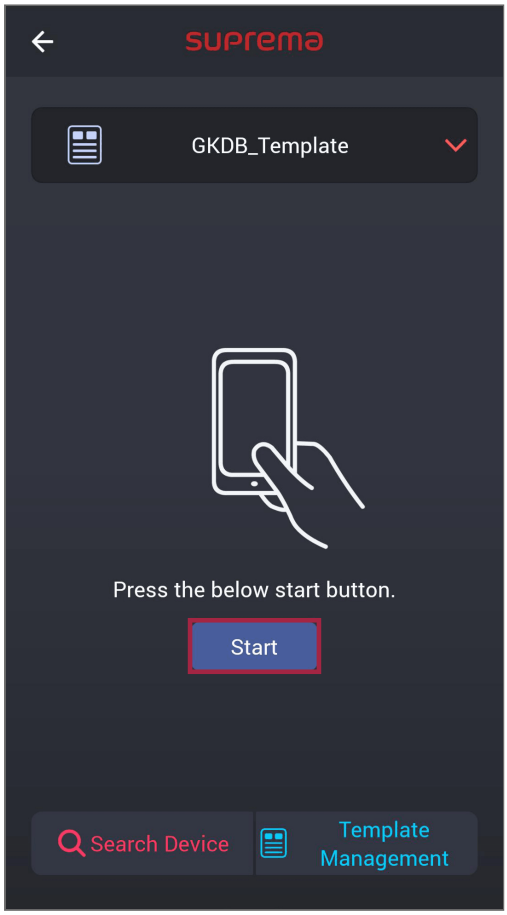
> **情報**
> デバイスのファームウェアバージョンが低い場合、いくつかの設定が適用されないことがあります。すべての設定を適用するには、デバイスのファームウェアをアップグレードするを参照してファームウェアをアップグレードしてください。

1. モバイル機器で Bluetooth 機能を有効にした後、Suprema Device Manager を起動してください。
2. メイン画面で XPass D2 を選択します。
3. **Choose a template** を押してください。選択可能なテンプレートの一覧が表示されます。





4. テンプレート一覧から目的のテンプレートを選択してください。
5. **Start** を押してください。



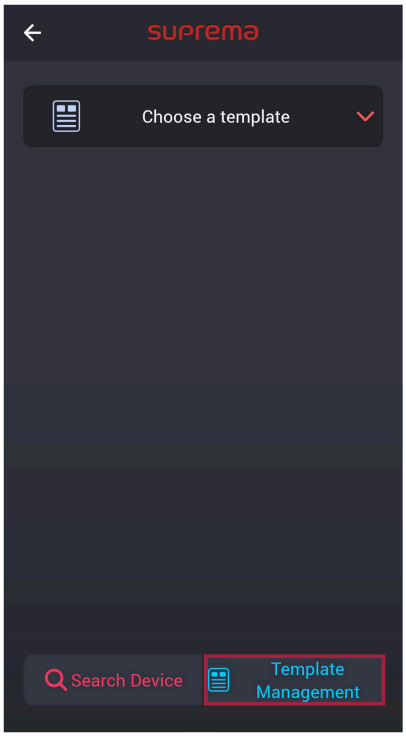
6. テンプレートを適用するデバイスにモバイル機器の背面を完全に接触させてください。
7. テンプレート適用が完了したら、**OK** を押してください。

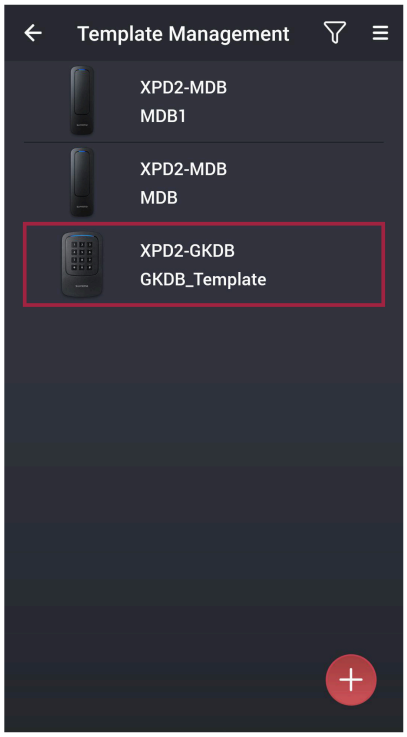
> **情報**
>
> - Suprema Device Managerで変更した設定はデバイスにのみ適用され、サーバーには同期されません。
> - デバイスがマスターデバイスと接続されているか、Wiegand出力設定が変更されている場合、Suprema Device Managerにデフォルトキーで接続できません。 Suprema Device Managerに接続するにはデバイスを初期化してください。

テンプレートを管理する

テンプレートを編集する

1. モバイル端末で Suprema Device Manager を起動します。
2. メイン画面で XPass D2 を選択します。
3. **Template Management** を押してください。

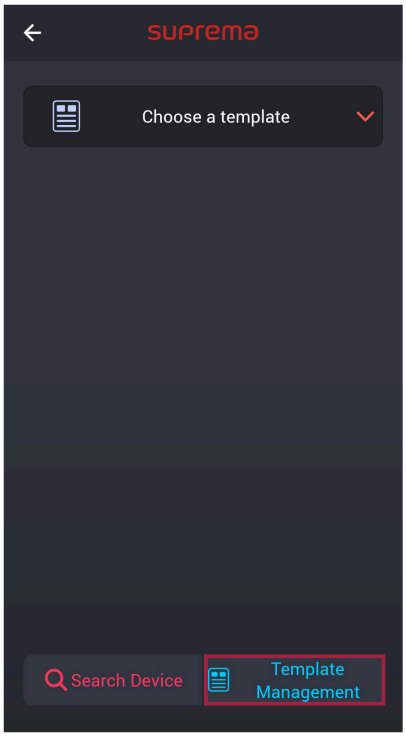


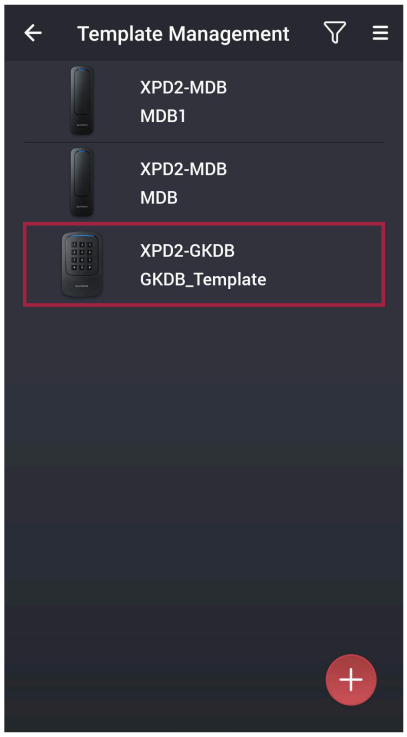


4. テンプレート一覧から編集するテンプレートを選択します。
5. テンプレートを追加するを参照してテンプレートを編集します。
6. 変更した設定を保存するには **Save** を、新しいテンプレートとして保存するには **Save as new template** を押します。

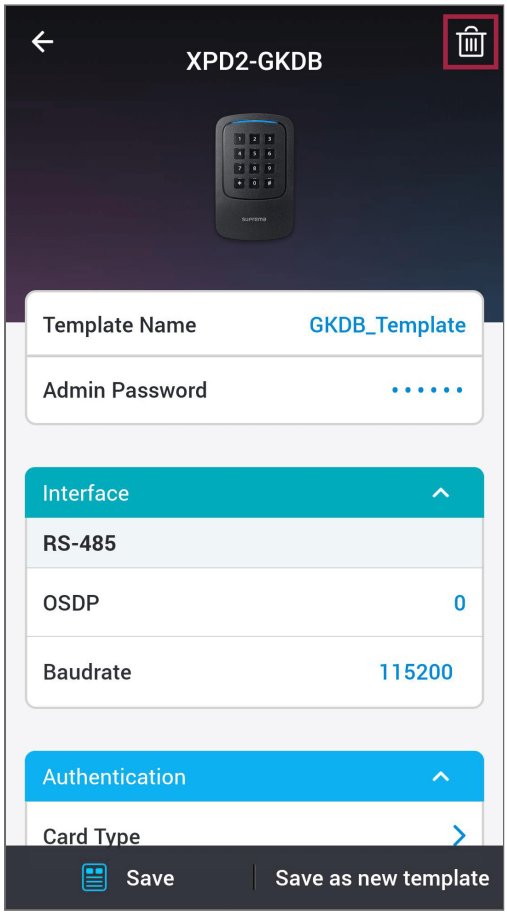
テンプレートを削除する

1. モバイル端末で Suprema Device Manager を起動します。
2. メイン画面で XPass D2 を選択します。
3. **Template Management** を押してください。





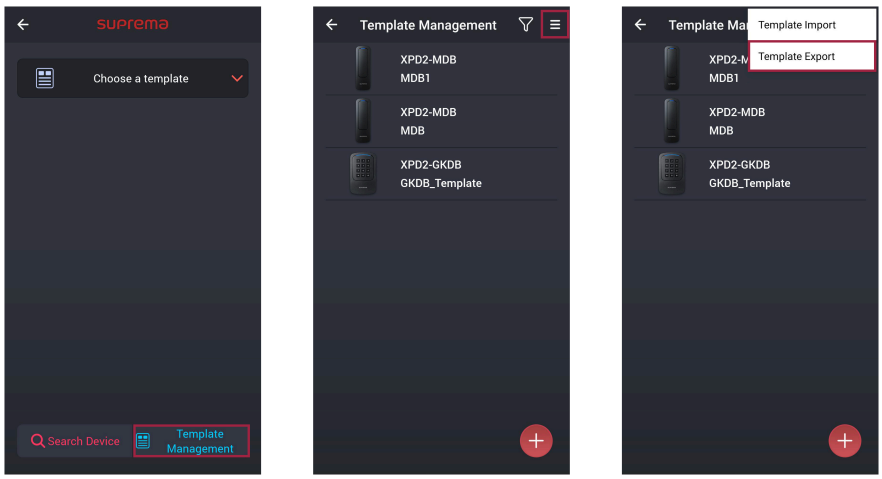
4. テンプレート一覧で削除するテンプレートを選択します。
5. テンプレートを削除するには → **OK** を押します。



テンプレートをエクスポートする

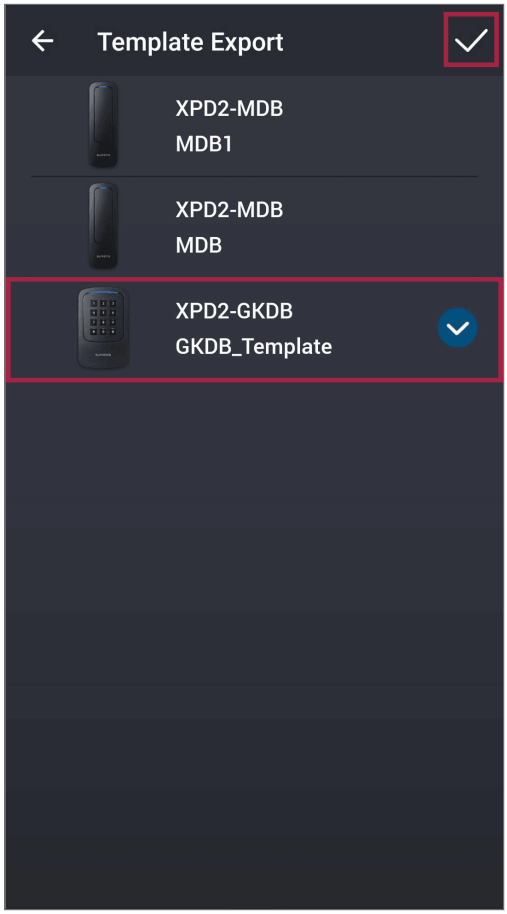
XPass D2 設定のテンプレートをアプリからエクスポートできます。

1. モバイル端末で Suprema Device Manager を起動します。
2. メイン画面で XPass D2 を選択します。
3. **Template Management** を押してください。



4. テンプレート一覧画面の上部で ☰ を押してから **Template Export** を選択します。

5. エクスポートするテンプレートを選択した後、✓ を押します。

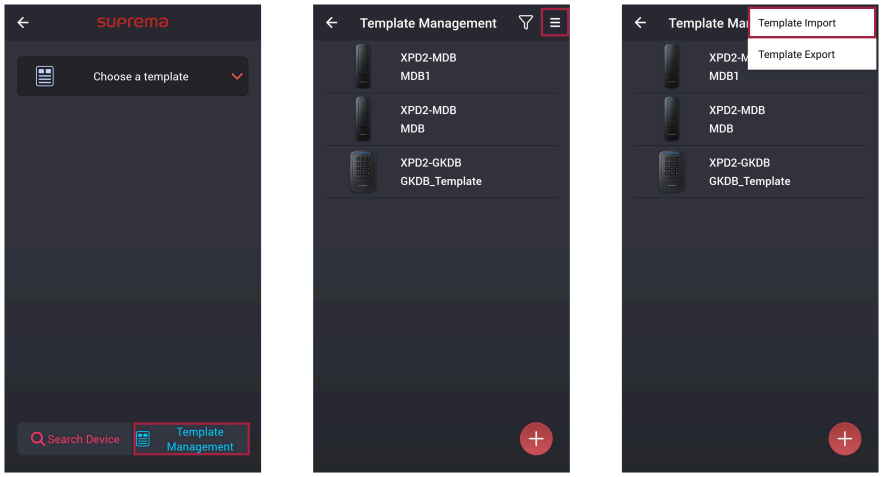


> **情報**
> テンプレートファイルはモバイル端末の以下のフォルダに保存されます。
> - **Android**: Download → DeviceManager_TemplateFiles
> - **iOS**: Device

テンプレートをインポートする

XPass D2 設定のテンプレートをアプリにインポートできます。

1. モバイル端末で Suprema Device Manager を起動します。
2. メイン画面で XPass D2 を選択します。
3. **Template Management** を押してください。



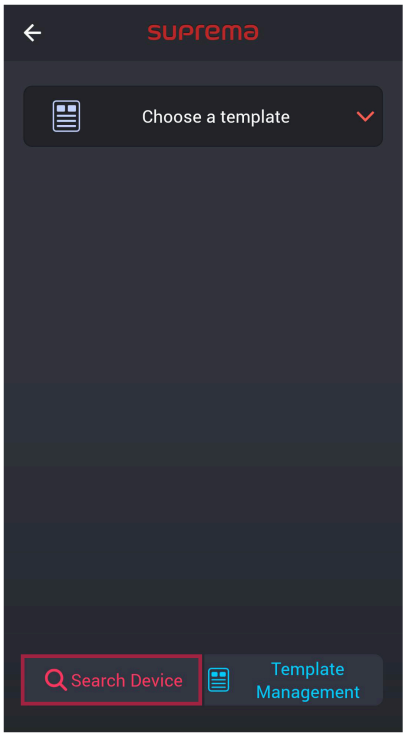
4. テンプレート一覧画面の上部で ☰ を押してから **Template Import** を選択します。
5. テンプレートが保存されているフォルダーでインポートするテンプレートを選択します。

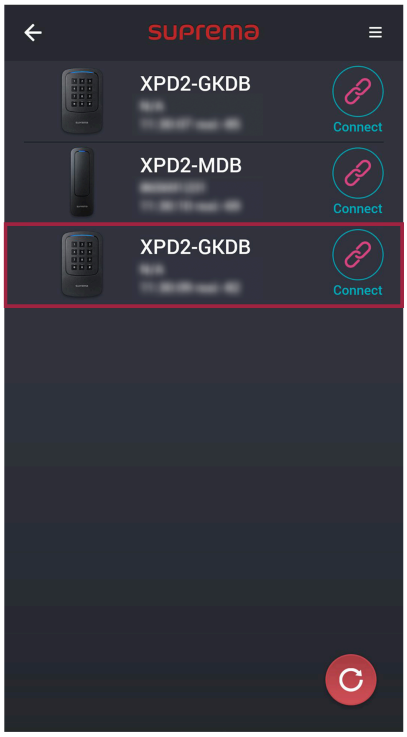
> **情報**
> テンプレートファイルはモバイル端末の以下のフォルダに保存されます。
> - **Android**: Download → DeviceManager_TemplateFiles
> - **iOS**: Device

デバイスの検索と接続

周辺に設置された XPass D2 を検索して接続できます。 Suprema Device Manager と接続すると、デバイスのファームウェアのアップグレードやデバイスの再起動、テンプレートのパスワード変更など、さまざまな機能を利用できます。

1. モバイル機器で Bluetooth 機能を有効にした後、Suprema Device Manager を起動してください。
2. メイン画面で XPass D2 を選択します。
3. **Search Device** を押してください。接続可能なデバイスの一覧が表示されます。





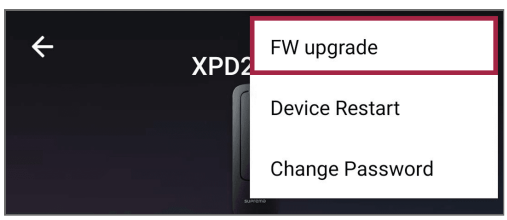
4. デバイス一覧でデバイス ID を確認してデバイスを選択するか、接続するデバイスにモバイル機器を近づけます。
5. 接続パスワードを入力します。入力したパスワードを画面に表示するには を押します。
6. デバイスの接続を完了するには **OK** を押します。

デバイスのファームウェアをアップグレードする

デバイスのファームウェアを簡単にアップグレードできます。

> **情報**
>
> - ファームウェアをアップグレードするには、モバイル機器にファームウェアファイルをダウンロードする必要があります。最新ファームウェアは Suprema ダウンロードセンターからダウンロードできます。
> - ファームウェアのアップグレード中は、デバイスとモバイル機器の距離を 1 m 以内に保ってください。

1. デバイスの検索と接続を参照して、ファームウェアをアップグレードするデバイスと接続します。
2. → **FW upgrade** を押します。

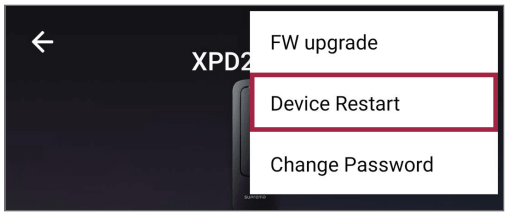


3. ファームウェアファイルが保存されているパスでファームウェアを選択します。ファームウェアのアップグレードが実行されます。
4. ファームウェアのアップグレードを完了するには **OK** を押します。

デバイスを再起動する

デバイスを再起動できます。

1. デバイスの検索と接続を参照して、再起動するデバイスと接続します。
2. ⋮ → **Device Restart** を押します。

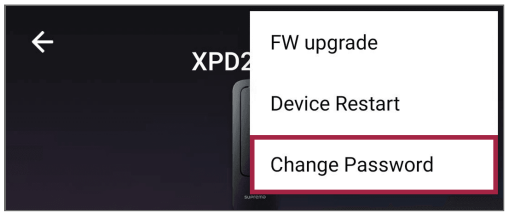


3. デバイスを再起動すると、モバイル機器との BLE 通信が切断されます。自動で再接続するには、**Auto Connection** 機能を有効にします。詳細な設定方法はアプリを設定するを参照してください。

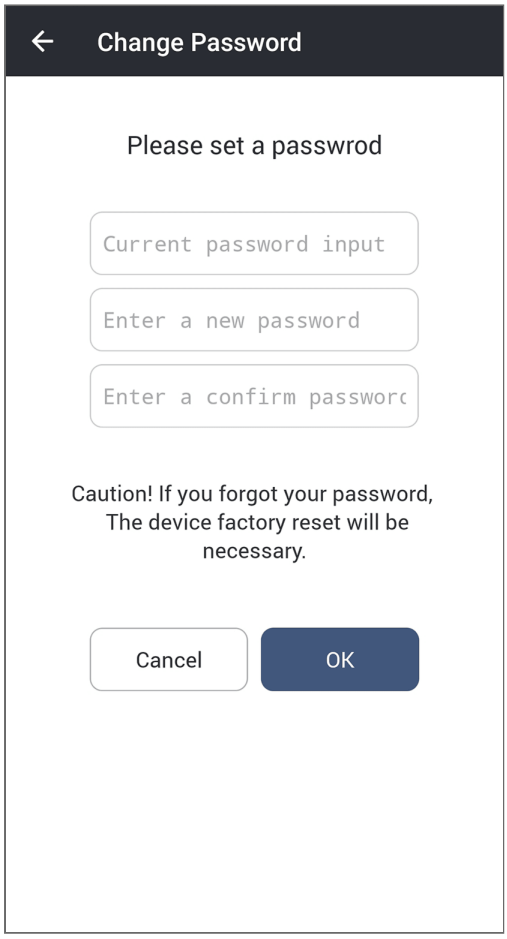
管理者パスワードを変更する

テンプレートの管理者パスワードを変更できます。

1. デバイスの検索と接続を参照し、パスワードを変更するテンプレートが適用されたデバイスと接続します。
2. ⋮ → **Change Password** を押します。



3. 現在のパスワードと新しいパスワードを入力します。



4. パスワードの変更を完了するには **OK** を押します。

> **情報**
>
> - 管理者パスワードは 6〜32 桁の数字で設定できます。
> - 管理者パスワードを紛失しないよう注意してください。管理者パスワードを紛失した場合、テンプレートを適用したデバイスに接続するにはそのデバイスを初期化する必要があります。

付録

製品に含まれる法的通知事項を掲載しています。

免責事項

- このウェブサイトは、Suprema製品に関する情報を提供します。
- このウェブサイトは、Supremaの製品使用および販売契約に含まれるSuprema製品にのみ使用できます。 このウェブサイトは、明示的、黙示的、禁反言の原則、またはその他いかなる方法によっても、知的財産権に対するライセンスを付与しません。
- お客様とSupremaとの契約に明示されている場合を除き、Supremaは一切の責任を負わず、特定目的への適合性、商品性、非侵害に関するあらゆる明示的または黙示的保証を否認します。
- 保証が無効となるのは、次の場合です。Suprema製品が 1) 誤って設置される、またはハードウェアのシリアル番号、保証情報、品質保証ステッカーが変更または除去された場合、2) Supremaが許可した方法以外で使用された場合、3) SupremaまたはSupremaが承認した以外の者によって変更、改造、修理された場合、4) 不適切な環境で運用または保守された場合。
- Suprema製品は、製品の故障が負傷や死亡事故につながる可能性のある医療、救命、生命維持などの用途向けに設計されていません。 お客様がこのような用途でSuprema製品を購入または使用する場合、これに起因する負傷または死亡によって発生するすべての請求、費用、損失、支出および合理的な弁護士費用から、SupremaおよびそのメンバーⅠ、子会社、関連会社、供給業者を免責するものとします。 製品の設計または製造にSupremaの過失があると主張される場合でも同様です。
- Supremaは、信頼性、機能または設計を向上させるため、予告なくいつでも仕様および製品説明を変更する権利を有します。
- 個人情報は、製品使用時に認証メッセージおよびその他の関連情報の形でSuprema製品に保存されることがあります。 Supremaは、Supremaが直接制御できない、または関連契約に明示されたSuprema製品に保存される個人情報を含むいかなる情報についても責任を負いません。 個人情報を含む保存された情報を使用する場合、製品ユーザーは関連法（例：GDPR）を遵守し、適切に取り扱いおよび処理する責任があります。
- お客様は、いかなる機能の欠如や特性、または"reserved"や"undefined"と表示された説明に依存してはなりません。 Supremaは後日これを定義することができ、後日行われた変更が現行内容と矛盾した場合でも、Supremaは責任を負いません。
- 本サイトに明示的に記載されている場合を除き、Supremaは法律で許容される最大範囲で"現状のまま"販売されます。
- 製品を注文する前に、最寄りのSuprema営業所または代理店に問い合わせ、最新の仕様を確認してください。

著作権に関するお知らせ

本ウェブサイトの著作権は Suprema に帰属します。 その他の製品名、商標、登録商標に関する権利は、それぞれの所有者である個人または団体に帰属します。

オープンソースライセンス

- 本製品にはオープンソースソフトウェアが含まれています。 GPL、LGPL、MPL およびソースコードの配布が必要なその他のオープンソースライセンスが適用されるソースコードは、Suprema サポートチームへご依頼いただくことで入手可能です。
- 本製品のソースコードは、製品最終出荷日から 3 年間、Suprema サポートチームへご依頼いただくことで入手可能です。
- ソースコードをその他の物理媒体で受け取る場合、料金が発生することがあります。 本提案は、この情報を受け取ったすべての方に有効です。
- 本製品に含まれる Android および iOS のライセンスの詳細は、Android と iOS でご確認いただけます。

Suprema Inc.

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

電話: +82 31 783 4502 | Fax: +82 31 783 4503 | お問い合わせ: sales_sys@supremainc.com

Supremaのグローバル支社の詳細については、
QRコードをスキャンして以下のWebページにアクセスしてください。
https://www.supremainc.com/en/about/contact-us.asp

© 2026 Suprema, Inc. 本書に記載されている Suprema および Suprema 社の製品名および番号は、Suprema, Inc. の登録商標です。Suprema 社以外のすべてのブランドおよび製品名は、それぞれの企業の商標または登録商標です。製品の外観、ビルドステータスおよび/または仕様は、予告なく変更されることがあります。