BioStation 3 Max

ユーザーガイド

バージョン 1.02

日本語
JA 102.00.BS3M

suprema
SECURITY & BIOMETRICS

目次

安全のための注意事項 4

遵守事項 4

はじめに 8

同梱物 8

各部の名称と機能 9

ケーブルとコネクタ 11

正しい顔の登録と認証方法 18

QR/バーコードおよびデバイスライセンスに関する注意事項 21

インストール 22

ブラケットと製品の固定 22

電源接続 25

ネットワーク接続 26

入力接続 27

リレー接続 28

スタンドアロン接続 31

Secure I/O 2 の接続 32

Wiegand接続 33

使用 34

管理者メニュー 34

ユーザー 36

認証 41

設定 49

イベントログ 66

トラブルシューティング 68

故障報告前の確認事項 68

製品仕様 70

クレデンシャル 70

一般 71

ストレージ 72

インターフェース 72

電気仕様 73

サイズと重量 74

規制認証情報 76

規制認証およびライセンス 76

FCC 準拠情報 77

IC 情報 77

付録 79

免責事項 79

著作権に関するお知らせ 80

オープンソースライセンス 80

安全のための注意事項

ユーザーの危険や財産上の損害を防ぐため、製品を使用する前に本書を必ずお読みいただき、製品を安全かつ正しくご使用ください。

本書でいう「製品」とは、本体とともに提供されるすべての構成品を含みます。

遵守事項

警告
これは、製品を使用する際に違反すると重傷や死亡に至るおそれがある警告事項を示すときに使用します。

注意
これは、製品を使用する際に違反すると軽傷や製品の損傷が発生するおそれがある注意事項を示すときに使用します。

情報
これは、製品を使用する際の参考事項や追加情報を提供するときに使用します。

ノート

これは、製品を使用する際の参考事項や追加情報を提供するときに使用します。

⚠ 警告

インストール

大容量の電源装置を使用する場合は、配線ミスに十分ご注意ください。

- 配線を誤ると、重大な火災、感電、製品の損傷が発生するおそれがあります。

ユーザーが製品を任意に設置したり修理したりしないでください。

- 火災、感電、けがの原因となります。
- ユーザーによる任意の設置や修理によって製品が損傷した場合、無償修理サービスは提供されません。

製品を直射日光が当たる場所、湿気・ほこり・すすの多い場所、ガス漏れの可能性がある場所に設置しないでください。

- 火災または感電の原因となります。

製品を屋外に設置する場合は、ひさしがあり通気の良い場所に設置してください。

製品を屋外に設置する場合は、完全に密閉された筐体を使用しないでください。

- 直射日光により筐体内部の温度が上昇し、過熱による火災、感電、製品損傷の原因となります。

製品を電気ヒーターなど熱が発生する場所に設置しないでください。

- 過熱による火災または感電の原因となります。

水気のある場所に設置しないでください。

- 湿気による感電または製品損傷の原因となります。

電磁波障害のある場所に設置しないでください。

- 感電または製品損傷の原因となります。

使用

製品内部に水、飲料、薬品などの液体が入らないように注意してください。

- 火災、感電、製品損傷の原因となります。

破損した電源アダプターやプラグ、緩んだコンセントは使用しないでください。

- 接続が不安定な場合、火災または感電の原因となります。

電源コードを無理に曲げたり破損させたりしないでください。

- 火災または感電の原因となります。

⚠ 注意

インストール

製品を設置する前に本書を必ずお読みいただき、製品を安全かつ正しく設置してください。

電源ケーブルおよびケーブルを配線する際は、必ず接続するすべての装置の電源を切った状態で配線・接続してください。

- 装置が誤作動を起こすおそれがあります。

製品に電源を接続する前に、もう一度マニュアルを確認して配線が正しいことを確認してから電源を接続してください。

製品を直射日光や紫外線が直接当たる場所に設置しないでください。

- 製品の損傷、誤作動、変色、変形の原因となります。

電源ケーブルなどを通行場所に放置しないでください。

- 身体障害または製品損傷の原因となります。

磁石、テレビ、（CRT）モニター、スピーカーなど磁力の強い物体の近くに設置しないでください。

- 故障の原因になります。

複数台の装置を設置する場合は、最小離隔距離を確認してください。

- 他の装置のRFおよびBLE性能に影響を与え、装置が誤作動するおそれがあります。

電源アダプターは IEC/EN 62368-1 の認証を取得し、端末の消費電力以上に対応する製品を使用してください。 Suprema で販売している電源アダプターの使用を推奨します。

- 適切な電源を使用しない場合、装置が誤作動するおそれがあります。
- 最大消費電流の規格は製品仕様の電源を参照してください。

製品と Secure I/O 2、電気錠（電気式ロック装置）は必ず個別の電源を使用してください。

- 装置が誤作動を起こすおそれがあります。

電源装置と PoE+ 電源を同時に接続しないでください。

- 装置が誤作動を起こすおそれがあります。

IP65 等級を満たすために、製品とケーブルを接続した後、必ずケーブルカバーを使用してください。完全に露出した屋外に設置する場合は、筐体の使用を推奨します。

- 防水・防塵性能が低下すると故障の原因となります。

PoE+ 電源を接続する際は、必ず PoE+ または PoE++ 規格で接続してください。

- 標準 PoE を使用すると、デバイスが不安定に動作したり、永久的に損傷したりする可能性があります。

使用

製品を落下させたり衝撃を与えたりしないでください。

- 故障の原因になります。

製品のファームウェアアップグレード中に電源供給が中断されないよう注意してください。

- 故障の原因になります。

パスワードが他人に知られないように管理し、定期的に変更してください。

- 不正侵入の原因となります。

製品のボタン（タッチパッド）を無理に押したり、鋭利な工具で押したりしないでください。

- 故障の原因になります。

製品は -20 ℃～50 ℃ の範囲内で使用し、極端に低温または高温で保管しないでください。

- 故障の原因になります。

製品を清掃する際はご注意ください。

- 製品の表面を清潔な乾いた布でやさしく拭いてください。
- 製品を消毒する場合は、乾いた布に消毒用アルコールを適量含ませ、製品表面をやさしく拭いてください。イソプロピルアルコールを70～75%含む消毒用アルコールと、清潔で糸くずの出ない柔らかい布を使用してください。
- 消毒剤を製品に直接噴霧しないでください。

製品を本来の目的以外で使用しないでください。

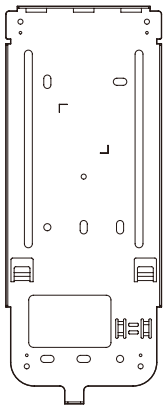
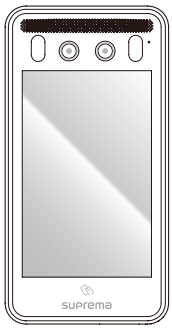
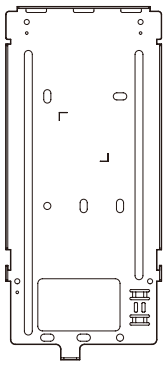
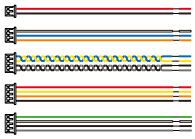
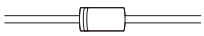
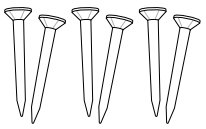
- 故障の原因になります。

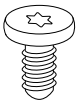
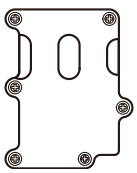
> **RTC バッテリー**
>
> 承認されていない、または不適切な種類のバッテリーに交換すると爆発の危険があります。バッテリーは居住地域または国際的な廃棄規定に従って廃棄してください。

はじめに

デバイスを使用するための初期手順を案内します。

同梱物

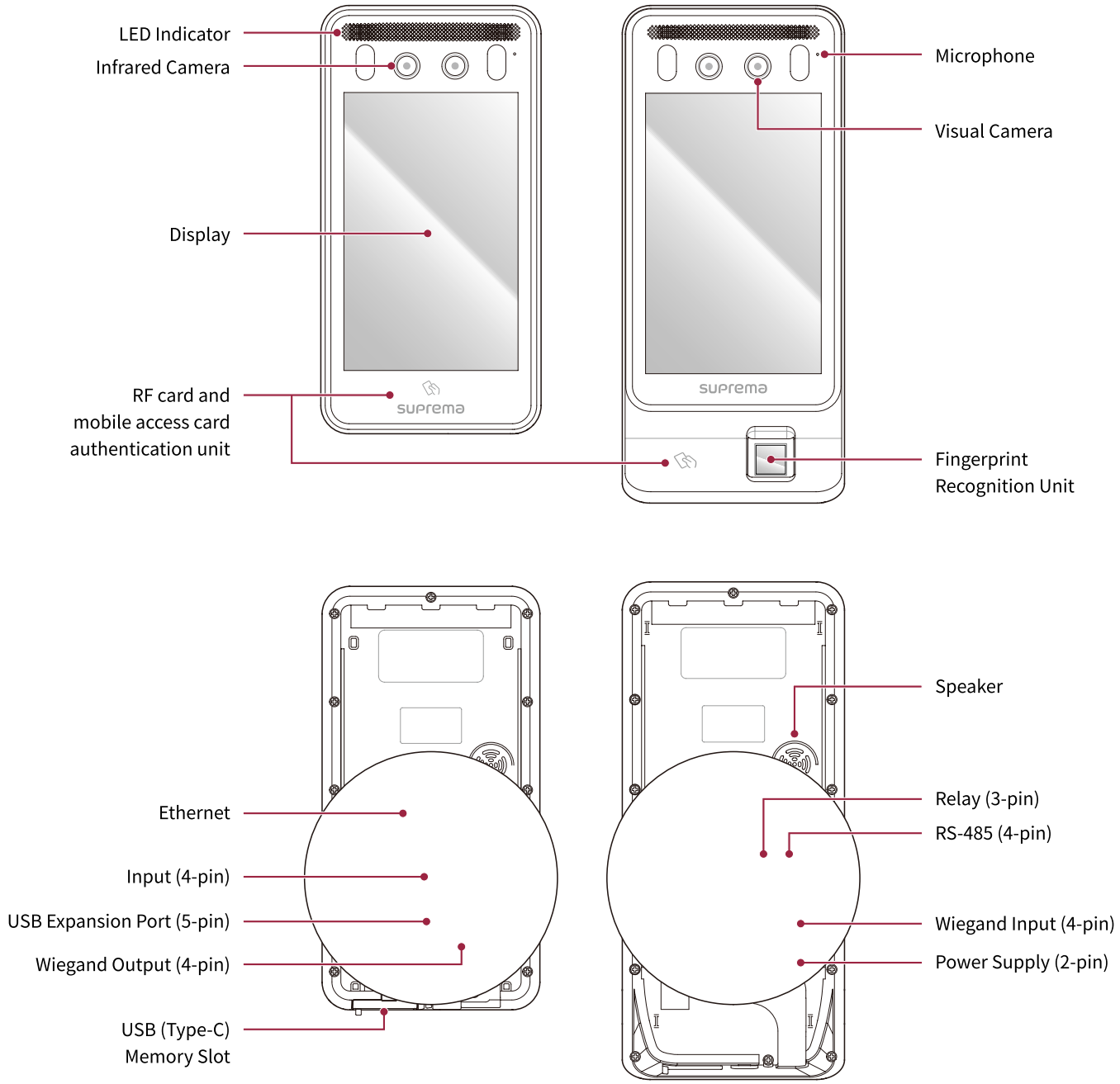
			
BioStation 3 Max (BS3M-ODB, BS3M-OAPB)	壁掛け用ブラケット (BS3M-ODB, BS3M-OAPB)	BioStation 3 Max (BS3M-DB, BS3M-APB)	壁掛け用ブラケット (BS3M-DB, BS3M-APB)
			
接続ケーブル	ダイオード	120 Ω 抵抗	固定用ネジ ×6

		
ブラケット固定用ネジ（星形）	ケーブルカバー	クイックガイド

情報

- 同梱品は設置環境によって異なる場合があります。
- ブラケットと製品を組み立てる際は、セキュリティを向上させるため、製品固定用ネジの代わりに同梱のブラケット固定用ネジ（星形）を使用できます。

各部の名称と機能



- **LED ステータス表示灯**：製品の動作状態を表示します。

  - 緑：認証成功
  - 赤：認証失敗
  - 青：正常動作状態
  - 青／緑点滅：
    - **DHCP** を有効に設定すると、IP アドレスを取得できない状態
    - **Slave** モードのとき、マスター装置との接続が切断された状態
  - 赤／紫点滅：デバイスロック状態
  - 黄点滅：入力待機状態
- **マイク**：インターホン接続時にユーザーの音声を伝えます。
  - マイクを覆ったり塞いだりすると、音声が正常に伝わらない場合があります。
- **赤外線カメラ**：赤外線画像を撮影します。
- **ビジュアルカメラ**：実際の画像を撮影します。
- **ディスプレイ**：操作用の UI を提供します。
- **RF カード・モバイル入退出カードリーダー**：入退出のために RF カードまたはモバイル入退出カードを読み取る部分です。
- **指紋認識部**：**BS3M-ODB, BS3M-OAPB** 入退室のために指紋を読み取る部分です。
- **スピーカー**：音を出力します。
- **イーサネット**：イーサネットケーブルを接続します。
- **Input（4ピン）**：Input ケーブルを接続します。
- **リレー（3ピン）**：リレーケーブルを接続します。
- **RS-485（4ピン）**：RS-485 ケーブルを接続します。
- **USB 拡張ポート（5ピン）**：他のアクセサリ製品を接続できます。
- **Wiegand 出力（4ピン）**：Wiegand 出力ケーブルを接続します。
- **Wiegand 入力（4ピン）**：Wiegand 入力ケーブルを接続します。
- **電源（2ピン）**：電源ケーブルを接続します。
- **USB（Type-C）メモリスロット**：USB メモリを接続します。

ケーブルとコネクタ

電源



ピン	名称	色
1	PWR +VDC	赤
2	PWR GND	黒

リレー



ピン	名称	色
1	RLY NO	白
2	RLY COM	青
3	RLY NC	オレンジ

RS-485



ピン	名称	色
1	485 TRXP	青
2	485 TRXN	黄
3	485 GND	黒
4	SH GND	灰

入力



ピン	名称	色
1	INPUT0	赤
2	INPUT1	黄
3	INPUT2	オレンジ
4	INPUT GND	黒

Wiegand入出力



ピン	名称	色
1	WG D0	緑
2	WG D1	白
3	WG GND	黒
4	SH GND	灰

マスター管理者を設定する CE 向け製品

Master Admin 機能は、デバイスの全面的な管理者権限を強化し、デバイスのセキュリティを向上させ、不正アクセスや設定変更をブロックするための機能です。この機能はEU地域向けの **CE 製品**のみに適用され、**CE 向け製品**では**必ずマスター管理者を登録**する必要があります。登録済みのマスター管理者のみが管理者メニューに入って、デバイス設定を変更できます。

> **情報**
>
> - この機能は EU 地域向けの **CE 向け製品**のセキュリティを強化するために導入された必須ポリシーであり、**グローバル製品**（Non-CE）では対応していません。
> - マスター管理者は直接削除できず、**Factory Default** のときにのみ削除されます。

マスター管理者対応ポリシー CE 製品 vs グローバル製品（Non-CE）

Master Admin 機能は、**CE マークの付いたラベルが貼付された CE 向け製品のみで有効化**されます。

> 製品背面のラベルシールで **CE 製品** / **グローバル製品**（Non-CE）を識別でき、これに応じて機能は次のように区別して動作します。
> - **CE 製品**：CE マークあり
> - **グローバル製品**（Non-CE）：CE マークなし

区分	CE 向け製品	グローバル製品（Non-CE）
Master Admin	有効化（無効化不可）	非対応
Admin 2-step Authentication	必須	非対応
最小 PIN 長	最低 8 桁以上	最低 4 桁以上

> BioStar X（または BioStar 2）と接続すると、デバイスの対応状況に応じてマスター管理者設定の表示が変わり、管理者 2 段階認証メニューの有効化状態も自動で同期されます。

ファームウェアアップグレード時の動作ロジック

既存で使用中の製品のファームウェアをアップグレードする場合、**アップグレード前のバージョンとアップグレード対象バージョン**の組み合わせによって **Master Admin** および **Admin 2-step Authentication** の対応状況が異なる場合があります。

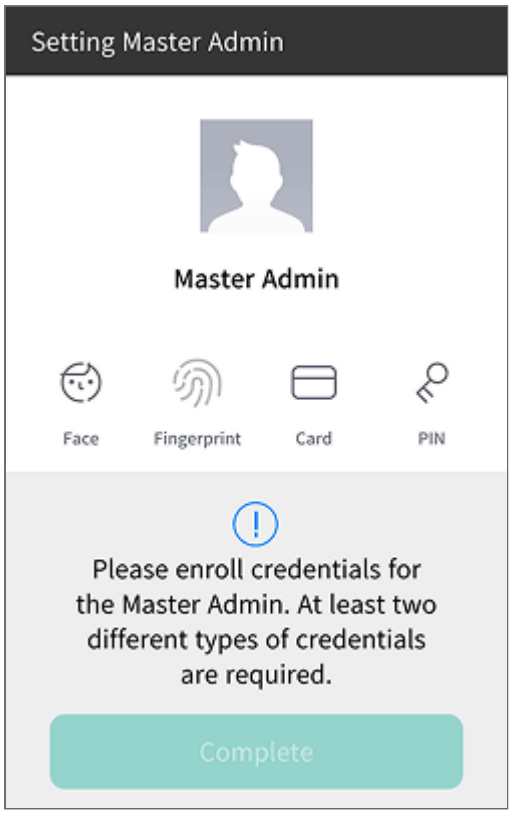
> 詳細なバージョン別の対応状況は Suprema グローバル技術サポートチーム にお問い合わせください。

マスター管理者を登録する

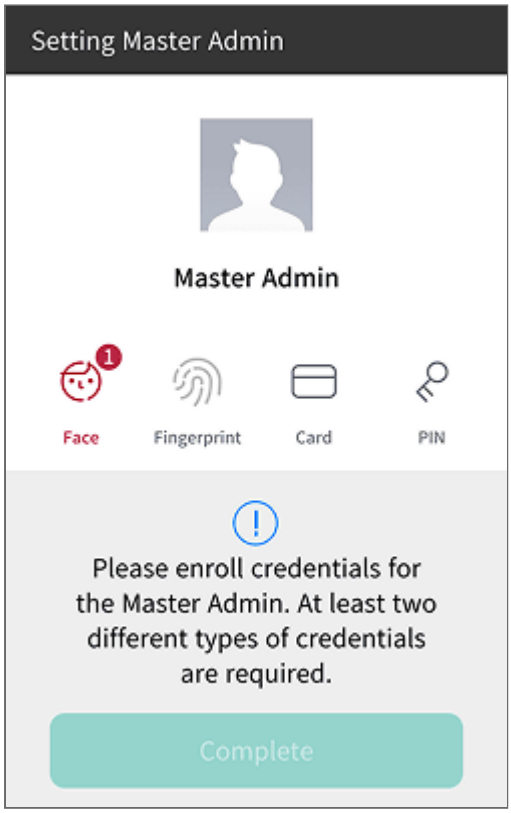
CE 製品の新しいデバイスでは、最初から **Master Admin** の登録が必須であり、登録しない場合はデバイスの使用が制限されます。

> **情報**
>
> - 初回起動時に **Master Admin** の登録画面が表示され、登録を完了しないと次の画面に進めません。
> - BioStar X（または BioStar 2）と接続してデバイス全体の管理者を割り当てても、**Master Admin** をデバイスで直接登録しなければすべての機能を使用できません。
> - 新しいデバイスはファームウェアをダウングレードできません。

1. 新しいデバイスを初回起動すると **Master Admin** 登録画面が表示されます。



2. EU 地域のセキュリティポリシーに従い、**Master Admin** は **最低 2 種類以上** のクレデンシャルを登録する必要があります。必要な 2 種類のクレデンシャルを選択して登録してください。

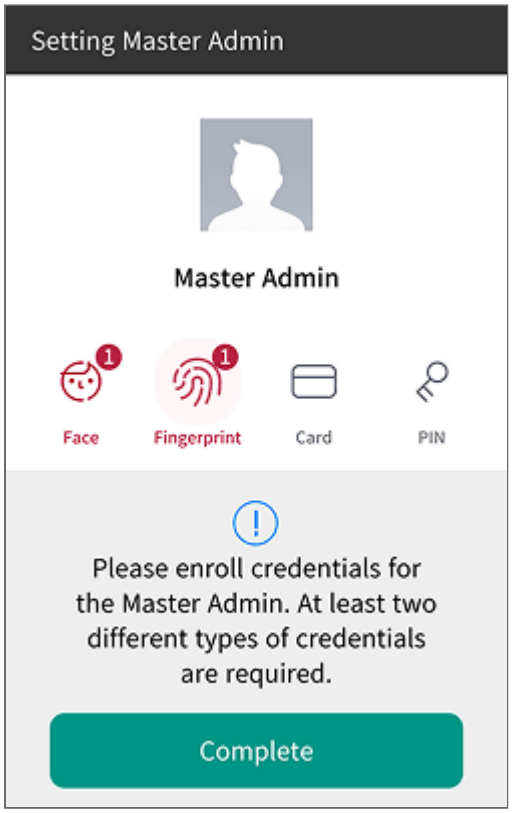


Master Admin に登録できるクレデンシャルは次のとおりです。

クレデンシャルの種類	登録可能数	詳細条件
カード	最大4件	CSN、Wiegand タイプのみ対応 同一タイプ内で重複登録不可
顔	最大2件	同一アルゴリズムを搭載したデバイスでのみ登録可能
指紋	最大2件	-
PIN	1件	8桁以上（CE規制適用）

登録条件
- 少なくとも 2 種類以上のクレデンシャルを登録する必要があります。
- デバイスがサポートするすべてのクレデンシャルを認証手段として使用できます。

3. 2種類以上のクレデンシャルを登録した後、**Complete** ボタンを押すと **Master Admin** の登録が完了します。



ご案内事項

- **BioStarソフトウェアでPINを登録する場合**

  マスター管理者に対応していないグローバル製品（Non-CE）は、4桁以上のPINをデバイスで直接登録できます。ただし、BioStar X（または BioStar 2）を通じてユーザーを登録する場合、下記バージョンでは最低8桁のPINが必要です。

  - BioStar 2 v2.9.11 以上
  - BioStar X v1.0.0 ～ v1.0.2

  上記バージョンで4桁PINとして登録されたユーザーは、デバイス管理者に指定できません。

- **デバイスハッシュキーを手動で変更する場合**

  デバイスハッシュキーを手動で変更する場合、マスター管理者のPINが削除されるという警告メッセージが表示されます。メッセージを確認してから変更してください。

- **RS-485通信区間での顔画像送信制限**

  RS-485通信区間ではバイオメトリッククレデンシャルの画像が送信されないため、スレーブデバイスで登録済みマスター管理者の顔を参照するときは代替画像が表示されます。

正しい顔の登録と認証方法

顔を登録する際の注意事項

- 顔を登録する際は、装置と顔の距離を60〜100 cmに保ってください。
- 表情を変えないように注意してください。
- マスク、帽子、アイマスクを着用しないでください。
- マスクを着用した顔を登録しないでください。マスクを着用した顔と着用していない顔の両方を登録すると、誤認識率が高くなる可能性があります。
- 頭を上げたり下げたりしないでください。
- 濃い化粧をしないでください。
- 目を閉じないでください。
- 画面に両肩が収まるようにしてください。
- 動かず正面を向いて顔を登録してください。
- 2 人の顔が画面に同時に映らないように注意してください。一度に 1 人ずつ登録してください。
- 画面の指示に従わないと、顔登録に時間がかかったり失敗したりすることがあります。

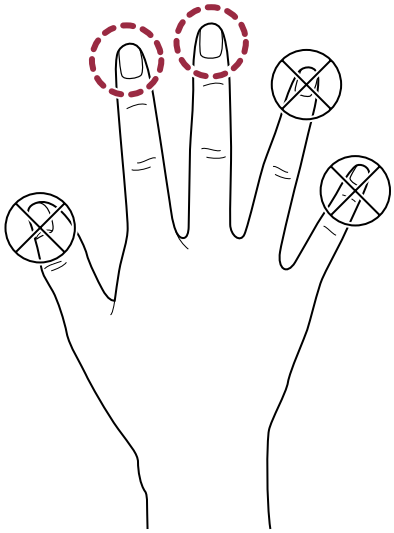
顔を認証する際の注意事項

- デバイスの画面中央に顔が表示されるようにしてください。位置ガイドが表示された場合は、画面の案内に従って顔を認証してください。
- 帽子、マスク、サングラス、アイパッチなどで顔の一部を覆うと、認証に失敗する可能性があります。眉毛と顔全体をデバイスが認識できるように、顔を覆わないでください。
- デバイスから90~100 cmの距離を取って認証してください。
- デバイスの画面に両肩が表示されるようにしてください。左右の肩の位置が対称でない場合、認証に失敗する可能性があります。動かずに正面に立ち、顔を認証してください。

正しい指紋入力方法 BS3M-ODB, BS3M-OAPB

指紋認識率を高めるために、指紋を正しく登録してください。本製品は、ユーザーの指紋入力の角度や位置が変わっても指紋を認識できます。指紋を登録する際に次の点に注意して登録すると、認識率を向上できます。

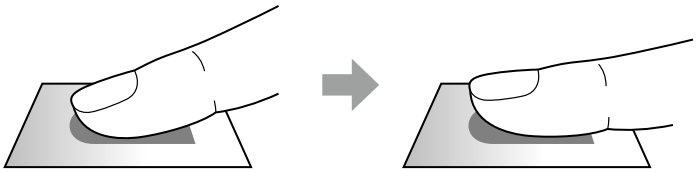
指紋入力用の指の選択



- 片手に荷物を持っている場合や指をけがしている場合など、特定の指の指紋を使用しにくい状況に備え、1人のユーザーにつき最大10個の指紋を登録できます。
- 指紋が認識されにくいユーザーは、同じ指を2回重複登録することで認識率を向上できます。
- 指にけががある場合や指紋が薄い場合は、別の指の指紋を登録してください。
- 指紋入力には人差し指または中指の使用を推奨します。その他の指は指紋センサーの中央に正確に配置しにくく、認識率が低下する可能性があります。

指紋の登録方法

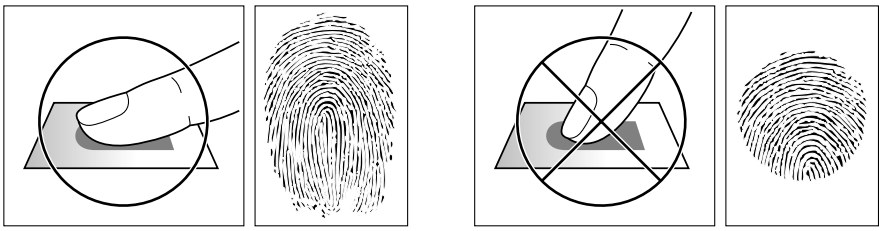
1. 指紋を登録する際、画面に「指紋を入力してください」と表示されたら、登録する指を指紋センサーに載せ、軽く押して指紋が正しく認識されるようにしてください。



2. 「ピッ」という音がして再入力画面が表示されたら、登録した指の指紋を再度スキャンしてください。（登録する指の指紋は2回入力します。）

指紋登録時の注意事項

指紋認識では最初に登録した指紋と比較するため、指紋登録が最も重要です。指紋を登録する際は次の点に注意してください。



- 指がセンサーに完全に接触するよう深く当ててください。
- 指紋の中心がセンサーの中央に来るように配置してください。
- 指にけががある場合や指紋が薄い場合は、別の指の指紋を登録してください。
- 指紋認識時は画面の案内に従い、動かさず正確に入力してください。
- 指を立ててセンサーとの接触面積が小さくなったり、指の角度がずれている場合は、指紋を認識できないことがあります。

指紋が認識されにくい場合

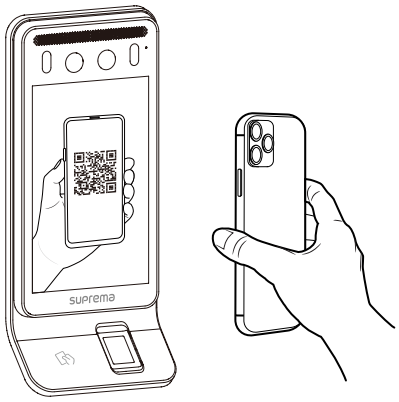
本製品は、季節の変化や指の状態の変化に関係なく指紋を認識できます。ただし、外部環境や指紋の入力方法によって認識率に差が生じる場合があります。指紋がうまく認識されない場合は、次の対策を行うことを推奨します。

- 指に水分や汗がある場合は、拭き取ってから入力してください。
- 指が乾燥し過ぎている場合は、指先に軽く息を吹きかけてから入力してください。
- 指にけがをした場合は、別の指の指紋を再登録してください。
- 最初に登録した指紋は正しく入力されていないことが多いため、指紋登録時の注意事項に従って指紋を再登録してください。

QR/バーコードおよびデバイスライセンスに関する注意事項

正しい QR/バーコード認証方法

ユーザーにQR/バーコードを発行して認証手段として利用できます。認識率を高めるため、案内に従い、正しく QR／バーコードをスキャンしてください。



- 端末のカメラとQR/バーコードの距離を8～25cmに保ってください。
- QR/バーコードをデバイスのスキャン画面中央に位置させます。
- モバイルデバイスでダウンロードした QR/バーコードで認証する場合、画面が見えやすいようにモバイルデバイスの明るさを調整します。
- 画面の指示に従わないと、QR/バーコードの認識に時間がかかるか、失敗する場合があります。

デバイスライセンスに関する注意事項

- より多様な QR/バーコード認証を使用するには、別途デバイスライセンスが必要です。デバイスライセンスを発行するには、購入先にお問い合わせください。
- デバイスライセンスファイルは暗号化されているため、任意に変更できません。
- デバイスライセンスはデバイス ID を基準に発行されます。不正な方法でデバイス ID を変更した場合、ライセンスの保証サービスは提供されません。

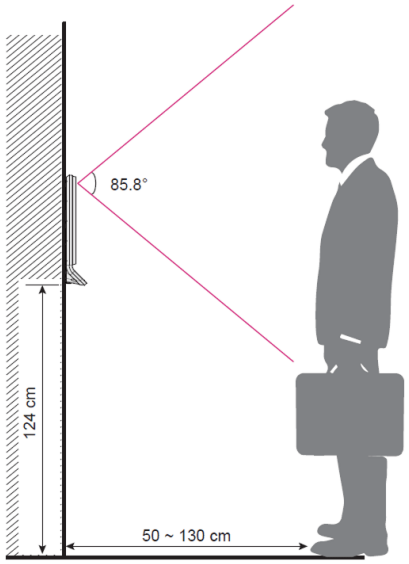
インストール

インストールに必要な全手順と接続例を提供します。

ブラケットと製品の固定

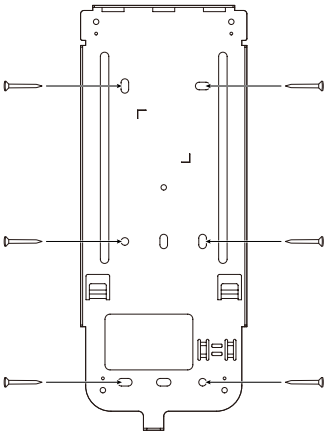
> **情報**
> 本書では、BS3M-ODB、BS3M-OAPBモデルの形状を基準に設置方法を説明します。 BS3M-DB、BS3M-APBモデルも同じ方法で設置してください。

1. 製品を取り付ける位置を決めてください。



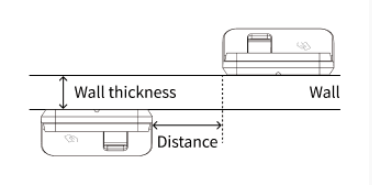
> **情報**
> - 装置を設置する最適な高さは次のとおりです。
> - BS3M-ODB, BS3M-OAPB：124 cm
> - BS3M-DB, BS3M-APB：127 cm
> - 装置を直射日光や紫外線が直接当たる場所に設置しないでください。
> - 利用者が顔認証を行う際に顔に直射日光が当たらないよう、設置位置を調整してください。

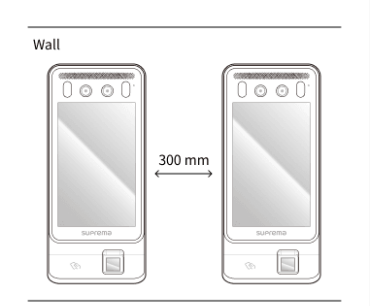
2. 製品を取り付ける位置にブラケットを固定ネジでしっかり固定してください。



情報

- 製品をコンクリート壁に設置する場合は、ドリルで穴を開けてPVCアンカーを挿入し、固定ネジで固定してください。
- RF信号干渉を回避するため、最小離隔距離を確認して設置してください。

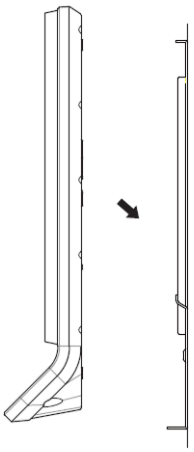




壁の厚さ	距離
100 mm	200 mm
120 mm	180 mm
150 mm	150 mm

- モバイルアクセスカードを使用する場合、BLE信号の干渉を回避するため、デバイス間に1 m以上の距離を空けて設置してください。

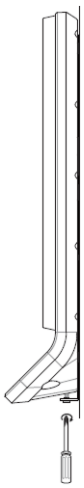
3. ケーブルカバーを取り付けた後、カバーに差し込まれている6本のネジを締めてしっかり固定し、固定されたブラケットの上に製品を取り付けてください。



情報

IP65等級を満たすため、製品とケーブルを接続した後、必ずケーブルカバーを使用してください。

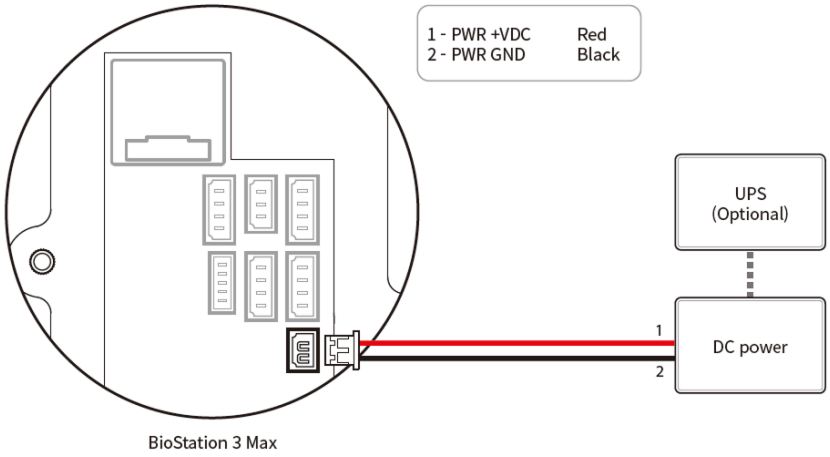
4. 製品固定ネジを締めて、製品とブラケットを組み付けてください。



情報

ブラケットと製品を組み立てる際は、セキュリティを向上させるため、製品固定用ネジの代わりに同梱のブラケット固定用ネジ（星形）を使用できます。

電源接続



注意

- 電源アダプターはIEC/EN 62368-1の認証を受け、端末の消費電力を上回る容量のものを使用してください。電源アダプターに他の機器も接続する場合は、端末の消費電力と他機器の消費電力を合算した電流容量以上のアダプターを使用する必要があります。
  - 最大消費電流の規格は製品仕様の電源を参照してください。
- Secure I/O 2、電気錠（電気式ロック）、製品は必ず個別の電源を使用してください。電源を共用すると装置が誤動作する可能性があります。
- 電源を接続する際は製品と電源装置の距離に注意してください。製品と電源装置はできるだけ近くに設置する必要があります。正しく接続しないと製品が誤動作する恐れがあるため注意してください。製品と電源装置の距離が長い場合は16 AWGまたは18 AWGケーブルの使用を推奨します。使用するケーブルの規格や設置環境によって接続できる距離が異なる場合があります。本製品は DC 24 V と DC 12 Vの両方に対応しているため、ケーブル規格ごとの最大延長長を確認し、適切に電源を接続してください。

ケーブル規格	最大延長長	
	DC 12V	DC 24V
16 AWG	50 m	150 m
18 AWG	30 m	136 m
20 AWG	20 m	90 m

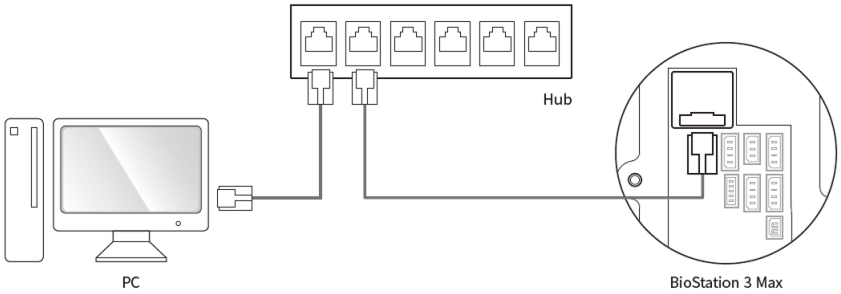
- 電源アダプターを使用する場合、電源ケーブルの長さを任意に延長しないでください。
- CAT5 UTP 2線ケーブルを電源供給用途に使用しないでください。

ネットワーク接続

TCP/IP

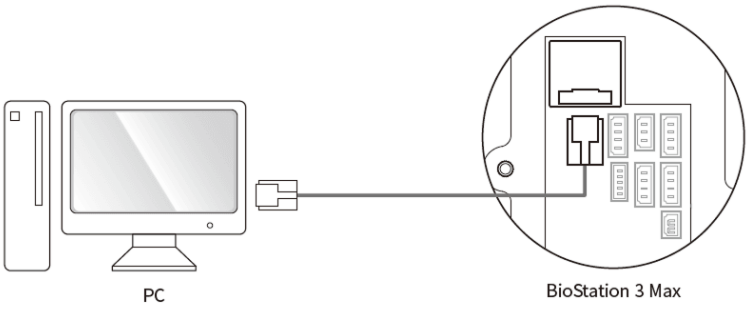
LAN接続（ハブとの接続）

標準タイプの CAT-5e ケーブルを使用してハブに接続できます。



LAN接続（PC と直接接続）

本製品はオート MDI/MDIX 機能をサポートしているため、クロスケーブルまたは標準ストレートタイプの CAT-5e ケーブルで PC に直接接続できます。



情報

ギガビットイーサネットスイッチを使用する際は、以下の情報を確認してください。

- CAT-5e UTP（非シールドツイストペア）ケーブルを使用してください。
- 4 対（8 芯）すべてをネットワーク接続に使用してください。
- ネットワークケーブルの一部の対や線を別用途に使用しないでください。

ネットワークポートおよびサービス

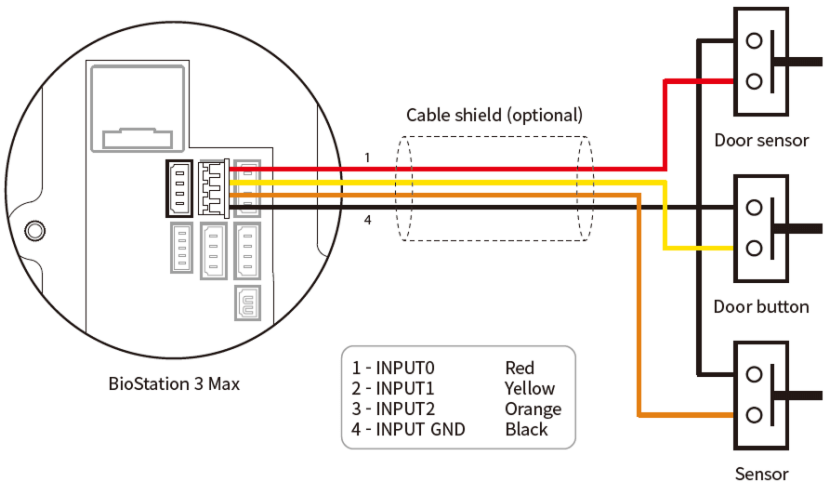
本製品はネットワーク通信および円滑なサービス運用のため、以下のポートを使用します。

プロトコル	サービス
TCP	サーバーとデバイス間の通信サービスおよびデバイスの運用状態切り替えサービスに使用されます。
UDP	ネットワーク上のデバイス検索サービスに使用されます。

情報

上記のポートは製品が正常にネットワーク機能を提供するために使用されます。ファイアウォールやネットワークセキュリティ設定の際には、これらのポートの使用許可が必要です。

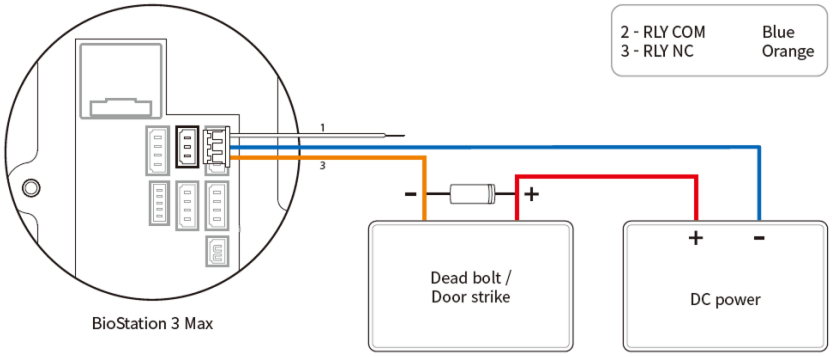
入力接続



リレー接続

Fail Safe Lock

フェイルセーフロックを使用するには、下図のように N/C リレーを接続してください。 Fail Safe Lock は通常、リレー回路に電流が流れており、リレーが動作して電流を一時的に遮断するとドアが開きます。停電や外部要因で装置の電源が切れた場合、ドアが開きます。



注意

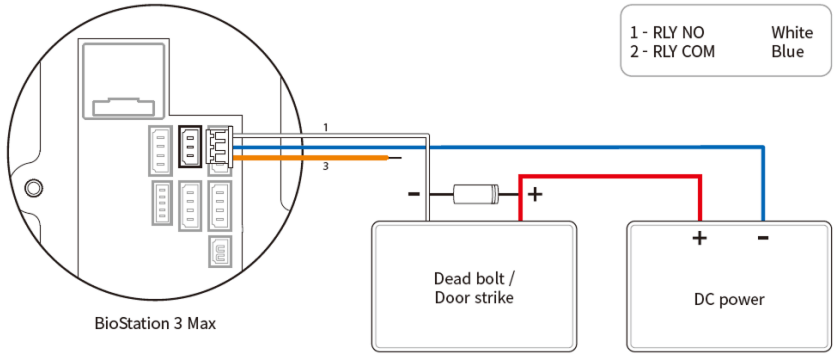
- 扉のロック装置が動作する際に発生する逆電流からリレーを保護するため、図のように扉ロック装置の配線の両側にダイオードを取り付けてください。
- 製品と扉ロック装置には別々の電源を使用してください。
- Suprema のインテリジェントデバイスには、利便性向上のためにコントローラーを介さずスタンドアロンで接続し、扉を直接開閉できるリレーが内蔵されています。しかし、より高いセキュリティが求められる入退室管理アプリケーションでは、扉のロック解除を引き起こす可能性のある改ざん攻撃を防ぐため、デバイス内蔵のリレーを使用しないことを推奨します。このようなアプリケーションでは、ロック制御用に扉内部の安全な位置に設置した Suprema Secure I/O 2、DM-20、CoreStation などの別体リレー装置の使用を推奨します。

情報

ダイオードの取り付け方向に注意してください。ダイオードは扉ロック装置の近くに取り付けてください。

Fail Secure Lock

フェイルセキュアロックを使用するには、下図のように N/O リレーを接続してください。 Fail Secure Lock は通常、リレー回路に電流が流れず、リレーが動作して電流が流れるとドアが開きます。停電や外部要因で装置の電源が切れた場合、ドアが施錠されます。



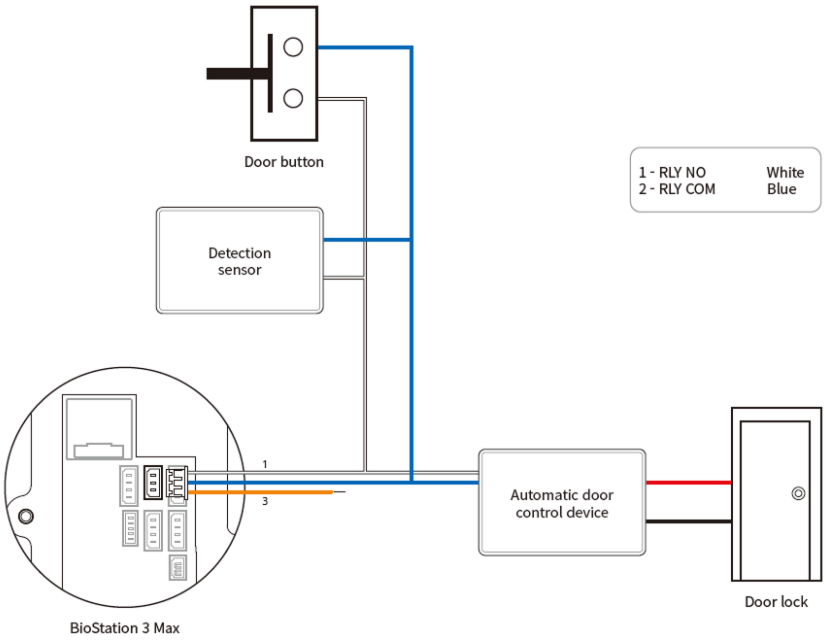
注意

- 扉のロック装置が動作する際に発生する逆電流からリレーを保護するため、図のように扉ロック装置の配線の両側にダイオードを取り付けてください。
- 製品と扉ロック装置には別々の電源を使用してください。
- Suprema のインテリジェントデバイスには、利便性向上のためにコントローラーを介さずスタンドアロンで接続し、扉を直接開閉できるリレーが内蔵されています。しかし、より高いセキュリティが求められる入退室管理アプリケーションでは、扉のロック解除を引き起こす可能性のある改ざん攻撃を防ぐため、デバイス内蔵のリレーを使用しないことを推奨します。このようなアプリケーションでは、ロック制御用に扉内部の安全な位置に設置した Suprema Secure I/O 2、DM-20、CoreStation などの別体リレー装置の使用を推奨します。

情報

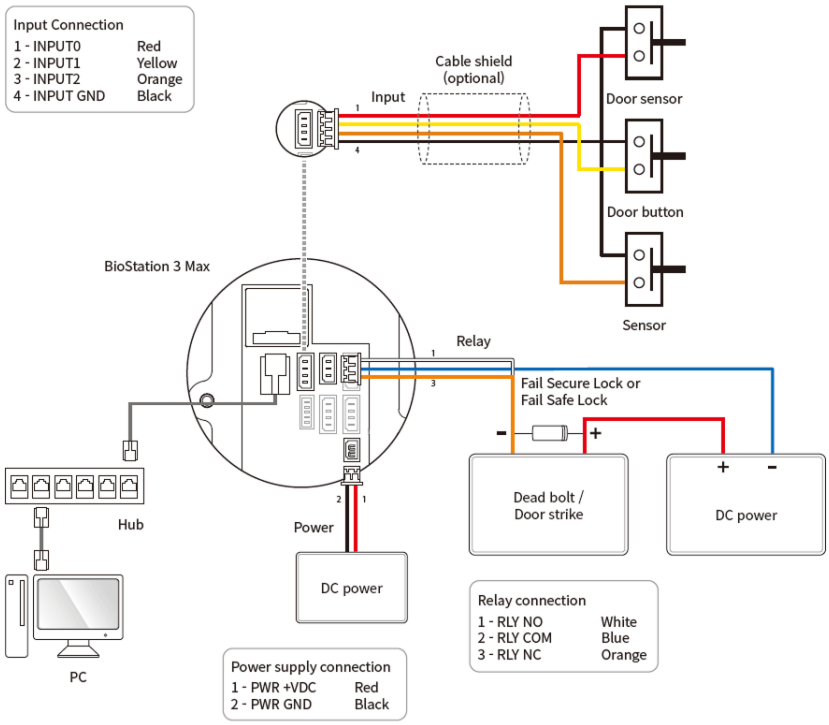
ダイオードの取り付け方向に注意してください。ダイオードは扉ロック装置の近くに取り付けてください。

自動ドア接続


Door button
1 - RLY NO
2 - RLY COM
White
Blue
Detection sensor
1
3
Automatic door control device
Door lock
BioStation 3 Max

スタンドアロン接続

別途I/Oデバイスを接続せずに、製品を直接ドアロック、退出ボタン、ドアセンサーなどに接続します。



注意

Suprema のインテリジェントデバイスには、利便性向上のためにコントローラーを介さずスタンドアロンで接続し、扉を直接開閉できるリレーが内蔵されています。しかし、より高いセキュリティが求められる入退室管理アプリケーションでは、扉のロック解除を引き起こす可能性のある改ざん攻撃を防ぐため、デバイス内蔵のリレーを使用しないことを推奨します。このようなアプリケーションでは、ロック制御用に扉内部の安全な位置に設置した Suprema Secure I/O 2、DM-20、CoreStation などの別体リレー装置の使用を推奨します。

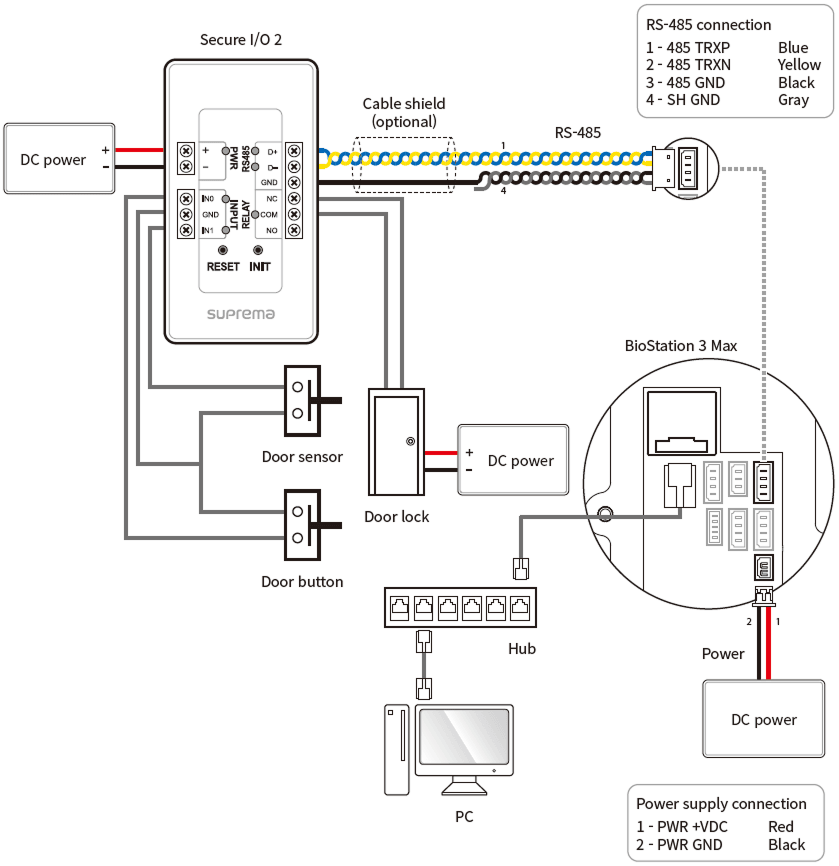
情報

- RS-485 ケーブルでスレーブ装置を接続し、本製品をマルチドアコントローラーとして使用できます。スレーブ装置はダミーリーダーとして使用され、認証はマスター装置で行います。
- FaceStation 2, FaceLiteがマスター装置の場合、BioStation 3 Maxをスレーブ装置として使用できず、その逆も使用できません。
- 接続可能なスレーブ装置の最大数は認証方法、ユーザー数、装置数によって変わり、スレーブ装置の数は認証速度に影響します。
- 1台のマスター装置につき、スレーブ装置は最大31台まで接続できます。 RS-485の帯域幅の制限により、指紋認識装置は最大7台まで接続できます。
- 詳細は Suprema テクニカルサポートまでお問い合わせください。

Secure I/O 2 の接続

製品に I/O デバイスである Secure I/O 2 を RS-485 で接続できます。製品と Secure I/O 2 の接続が切れたり、外部要因により製品の電源が遮断された場合でも、セキュリティを維持できます。

- RS-485 ケーブルには AWG24 のツイストペアケーブルを使用し、最大長は 1.2 km としてください。
- RS-485 ケーブルには特性インピーダンス 120 Ω のケーブルを使用することを推奨します。
- RS-485 をデイジーチェーン接続する場合は、デイジーチェーンの両端に終端抵抗（120 Ω）を取り付けてください。中間ラインに接続すると信号レベルが低下して通信性能が落ちるため、必ずデイジーチェーンの両端に接続してください。

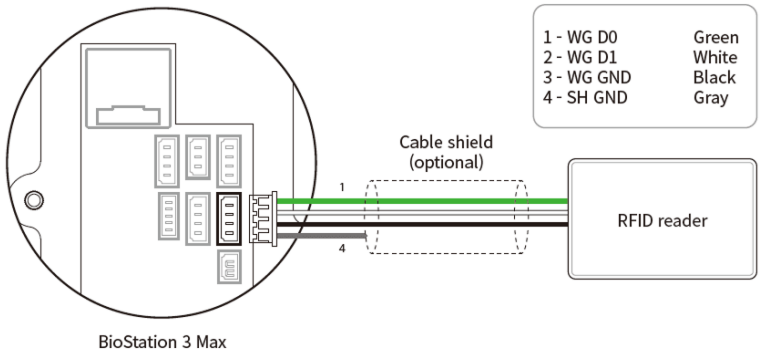


情報

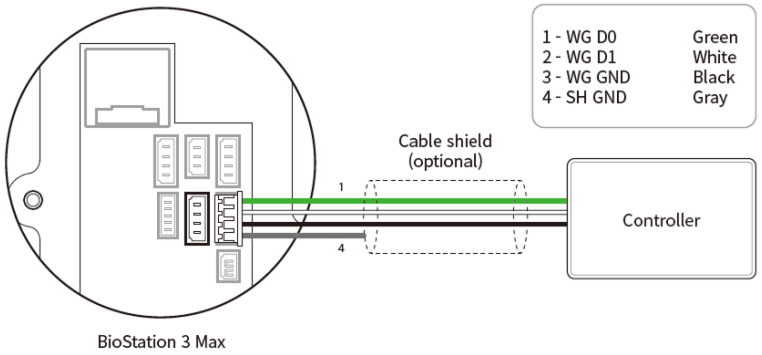
- RS-485 ケーブルでスレーブ装置を接続し、本製品をマルチドアコントローラーとして使用できます。スレーブ装置はダミーリーダーとして使用され、認証はマスター装置で行います。
- FaceStation 2, FaceLiteがマスター装置の場合、BioStation 3 Maxをスレーブ装置として使用できず、その逆も使用できません。
- 接続可能なスレーブ装置の最大数は認証方法、ユーザー数、装置数によって変わり、スレーブ装置の数は認証速度に影響します。
- 1台のマスター装置につき、スレーブ装置は最大31台まで接続できます。 RS-485の帯域幅の制限により、指紋認識装置は最大7台まで接続できます。
- 詳細は Suprema テクニカルサポートまでお問い合わせください。

Wiegand接続

Wiegand入力装置として使用



Wiegand出力装置として使用



使用

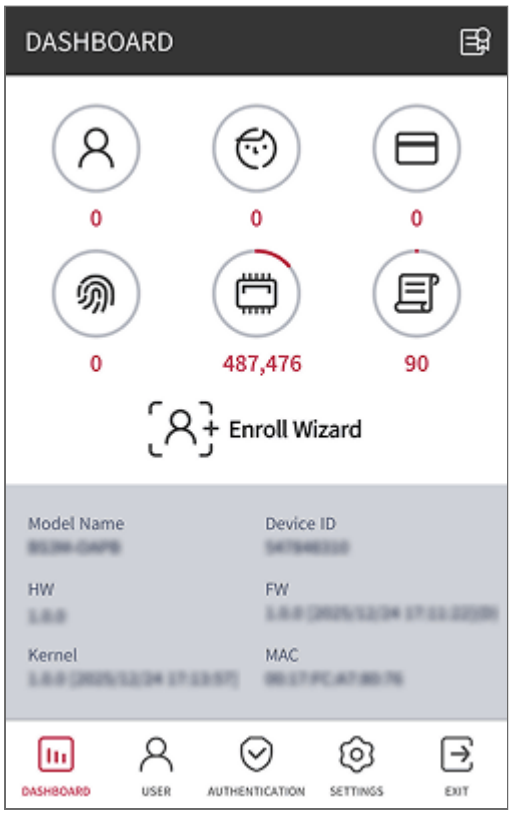
デバイスの主要機能を効果的に使用する方法を案内します。

管理者メニュー

管理者権限でアクセスできる主なメニューと機能を案内します。

ダッシュボード

1. を押した後、管理者権限の認証方法で認証してください。
   デバイスの使用状況と情報は **DASHBOARD** で確認できます。また、**Enroll Wizard** を押してすぐにユーザーを登録することもできます。
2. ユーザーを登録するかデバイスを設定するには、ダッシュボード下部で目的のメニューを選択します。

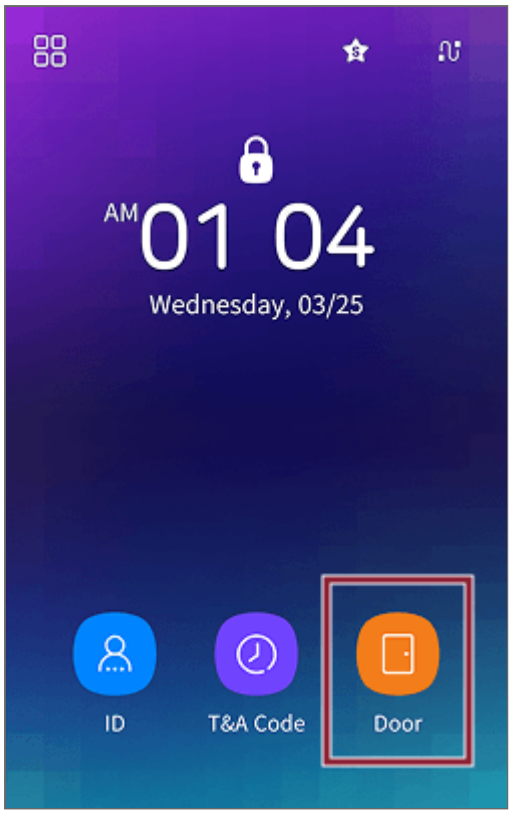


出入口ドア制御

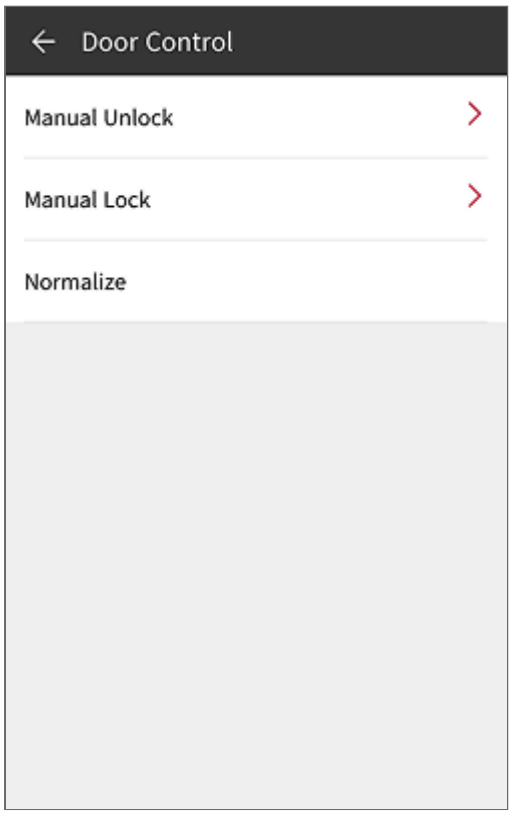
接続された出入口ドアを手動で開けたり、施錠・解錠したりできます。

> **情報**
>
> - デバイスをマスターとして構成している場合のみ、出入口ドアを制御できます。
> - **Administrator** または **Configuration** で出入口ドアを制御できます。

1. ホーム画面で **Door** を選択してください。



2. 管理者権限の認証手段で認証してください。
3. 希望する出入口ドアの制御方法を選択してください。



- **Manual Unlock**：出入口ドアをすぐに開けるか、開放状態を維持する時間を設定できます。
- **Manual Lock**：出入口ドアをすぐに施錠するか、施錠状態を維持する時間を設定できます。

- **Normalize**：手動で開放または解錠を行います。

> **情報**
> 手動開放および施錠の保持時間は1～86,400秒に設定できます。

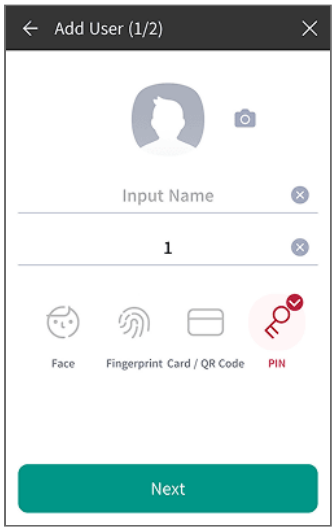
ユーザー

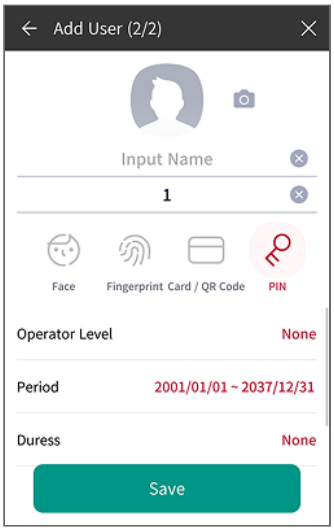
ユーザーの登録、編集、削除および管理方法について説明します。

ユーザー情報の登録

生体認証情報を含むユーザー情報を登録できます。

1. を選択し、管理者権限の認証手段で認証します。
2. **USER** → を選択し、必要な項目を設定します。ユーザー情報の登録は 2 段階で行われ、いくつかのオプションは認証手段を登録した後に有効になります。





- ：ユーザー写真を登録できます。
- **名前**: ユーザー名は、特殊記号（`~` `!` `@` `#` `$` `%` `^` `&` `(` `)` `-` `_` `=` `+` `[` `]` `{` `}` `;` `.` `'`）を含めて最大 48 文字まで入力できます。ただし、`&` `@` `~` で始まる名前は入力できません。
- **ID**：1～4294967295 の数字を入力してユーザー ID を登録します。 **User ID Type** を **Alphanumeric** に設定した場合、英数字と一部の特殊記号（`_` `-` `.`）を組み合わせて最大 32 文字まで入力できます。 ID は空白を含めることはできず、ピリオド(`.`)は含められますが、ピリオド一つ(`.`)またはピリオド二つ(`..`)だけでは入力できません。
- **Face**：ユーザー認証用の顔を登録します。 **Face** → **Next** をタップし、画面の指示に従って顔を登録します。顔を追加登録するには をタップします。顔の登録の詳細はユーザー顔登録を参照してください。
- **Fingerprint**：**BS3M-ODB, BS3M-OAPB** ユーザー認証用の指紋を登録できます。 **Fingerprint** → **Next** を押し、画面の指示に従って指紋を登録します。指紋をさらに登録するには、 をクリックします。指紋登録の詳細はユーザー指紋登録を参照してください。
- **Card / QR Code**：ユーザー認証用のカードを登録できます。 **Card / QR Code** → **Next** をタップし、ユーザーに割り当て

るカードをRFカード認証部にスキャンします。カードを追加登録するには **Card / QR Code** → ＋ をタップします。

> **情報**
> **QR Code** 認証を使用するには、**AUTHENTICATION** → **Operation** で **QR Authentication** が有効になっている必要があり、別途デバイスライセンスが必要です。詳細はライセンスを参照してください。

- **PIN**：使用する PIN を入力できます。 **PIN** → **Next** をタップし、使用する PIN を入力します。確認のため再度 PIN を入力し、**OK** をタップします。 PIN は漏えい防止のため 4〜16 桁の数字を入力してください。

> **情報**
> **Master Admin** 機能を使用する場合は、少なくとも 8 桁の数字を入力してください。

- **Operator Level**：ユーザーに割り当てる権限を選択できます。

> **情報**
> 設定されているユーザー権限によって使用できるメニューが異なります。
> - **None**：一般ユーザーレベルで、メニューは使用できません。
> - **Administrator**：すべてのメニューを利用できます。
> - **Configuration**：**AUTHENTICATION**、**DISPLAY & SOUND**、**DEVICE**、**NETWORK**、**EVENT LOG** メニューを利用できます。
> - **User Management**：**USER**、**EVENT LOG** メニューを利用できます。

- **Period**：ユーザーアカウントの利用期間を設定できます。
- **Duress**：**BS3M-ODB, BS3M-OAPB** デュレス指紋として使用する指紋番号を選択できます。脅迫されたり、強制的に扉を開けなければならない場合、この指紋で認証すると BioStar X にアラーム信号を送ることができます。指紋が 2 個以上登録されている必要があります。
- **Extended Private Auth Mode**：拡張個別認証モードを設定できます。拡張個別認証モードを使用すると、ユーザーごとに顔を含む認証方式を組み合わせることができます。使用しない場合は、デバイスの基本認証モードが適用されます。

3. ユーザー情報の登録を完了するには **Save** をタップします。

ユーザー顔登録

1. ☰ を選択し、管理者権限の認証手段で認証します。
2. **USER** → ＋ を選択します。
3. **Face** → **Next** をタップします。
4. 顔が画面に表示されるように距離を調整し、デバイスのカメラを正面から見てください。
5. 撮影が完了したら **OK** → **Save** をタップします。顔を再撮影するには **Re-Shot** をタップします。

情報

- 本製品の顔情報は、FaceStation 2 および FaceLite の顔情報と互換性がありません。
- 本製品の顔情報は、デバイスだけでなく、BioStar X で写真をアップロードしたり、CSV インポートを通じて一括登録することもできます。ユーザーに顔登録リンクを送信し、ユーザー自身のモバイルデバイスからも顔を登録できます。それぞれの登録方法の詳細については、BioStar X 管理者マニュアルをご参照ください。
- 顔を登録する際は次の事項に注意してください。
  - 顔を登録する際は、装置と顔の距離を60～100 cmに保ってください。
  - 表情を変えないように注意してください。
  - マスク、帽子、アイマスクを着用しないでください。
  - マスクを着用した顔を登録しないでください。マスクを着用した顔と着用していない顔の両方を登録すると、誤認識率が高くなる可能性があります。
  - 頭を上げたり下げたりしないでください。
  - 濃い化粧をしないでください。
  - 目を閉じないでください。
  - 画面に両肩が収まるようにしてください。
  - 動かず正面を向いて顔を登録してください。
  - 2 人の顔が画面に同時に映らないように注意してください。一度に 1 人ずつ登録してください。
  - 画面の指示に従わないと、顔登録に時間がかかったり失敗したりすることがあります。

ユーザー指紋登録 BS3M-ODB, BS3M-OAPB

1. を選択し、管理者権限の認証手段で認証します。
2. **USER** → を選択します。
3. **Fingerprint** → **Next** をクリックします。
4. 登録する指の指紋をスキャンした後、同じ指の指紋をもう一度スキャンします。

> **情報**
>
> - 指紋登録は BS3M-ODB、BS3M-OAPB 製品でのみ利用できます。
> - 指がセンサーに完全に接触するよう深く当ててください。
> - 指紋の中心がセンサーの中央に来るように配置してください。
> - 指にけががある場合や指紋が薄い場合は、別の指の指紋を登録してください。
> - 指紋認証時は画面の案内に従って正確に入力します。
> - 指を立ててセンサーとの接触面積が小さくなったり、指の角度がずれている場合は、指紋を認識できないことがあります。

ユーザー情報の編集

ユーザー管理者または全体管理者が登録済みのユーザー情報を編集できます。ユーザーの顔、指紋、カードを追加することや、PIN および権限を修正することができます。

1. を選択し、管理者権限の認証手段で認証します。
2. **USER** → をクリックします。
3. 使用する検索条件を選択します。**All**、**User ID**、**Name**、**Face**、**Fingerprint**、**Card** でユーザーを検索できます。
4. 編集するユーザーを選択します。
5. ユーザー情報の登録を参照して情報を編集し、**OK** をクリックします。
   - を選択して **OK** をクリックし、ユーザーを削除します。

> **情報**
>
> - 指紋検索は BS3M-ODB、BS3M-OAPB 製品でのみ使用できます。
> - **Access Group** は BioStar X で登録できます。出入グループ登録の詳細については、BioStar X 管理者説明書をご参照ください。

ユーザーの一括削除

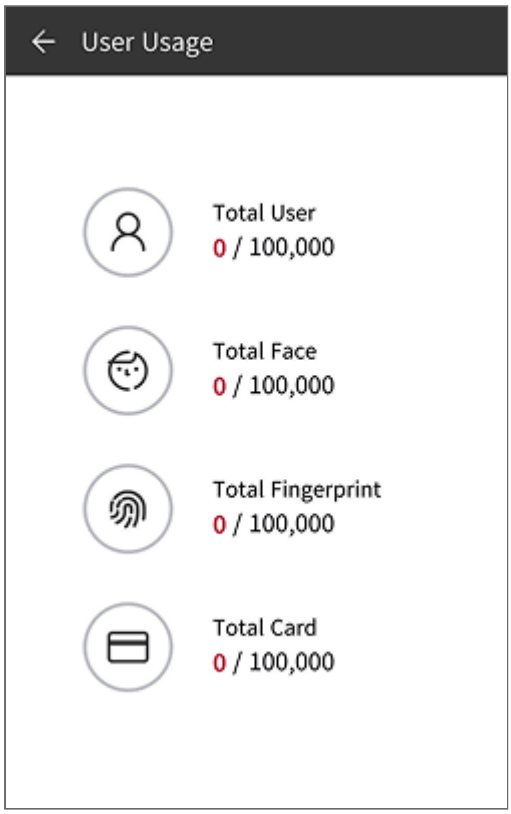
登録済みのすべてのユーザーを一度に削除できます。

1. を選択し、管理者権限の認証手段で認証します。
2. **USER** → を選択します。
3. **Delete All** を選択してチェックし、**OK** をクリックします。
4. すべてのユーザーを削除するには **OK** をクリックします。

ユーザー登録状況の確認

登録済みのユーザー、顔、カード、指紋の数を一目で確認できます。

1. を選択し、管理者権限の認証手段で認証します。
2. **USER** → をタップします。ユーザー登録状況を確認できます。



情報
指紋数は BS3M-ODB、BS3M-OAPB 製品でのみ確認できます。

認証

サポートする認証方式と認証手順について説明します。

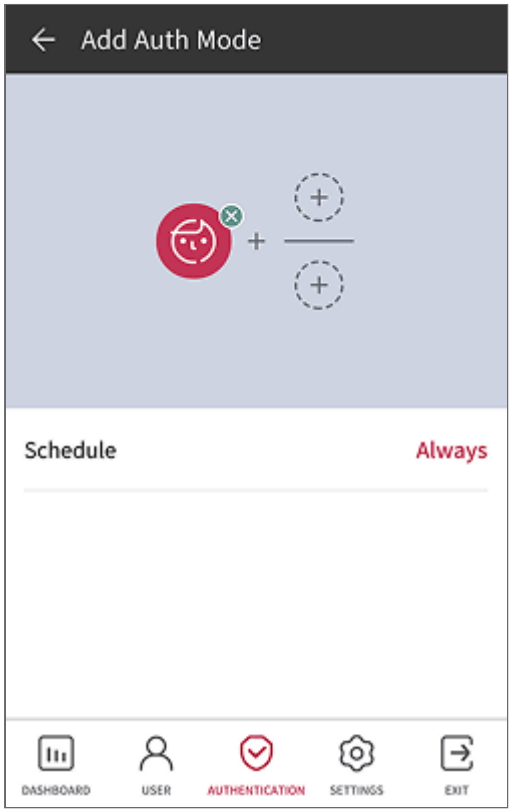
認証モード

デバイスの認証モードを設定できます。**Face**、**Fingerprint**、**PIN**、**Card / QR Code**、**ID** を組み合わせて認証モードとして使用でき、各認証モードごとに使用するスケジュールも設定できます。

> **情報**
> 指紋認証は BS3M-ODB、BS3M-OAPB 製品でのみ使用できます。

認証モードの登録

1. を選択し、管理者権限の認証手段で認証します。
2. **AUTHENTICATION** → **Auth Mode** を押します。
3. を選択します。
4. を押すと、追加できるクレデンシャルが画面に表示されます。必要なクレデンシャルを追加します。クレデンシャルが追加された状態で を押すと、追加したクレデンシャルを削除できます。



- : 顔、: 指紋、: カード / QRコード、: ID、: PIN
- 選択した認証方法を順番にすべて認証するように組み合わせることも、一部のみを選択して認証するように組み合わせることもできます。選択した認証方法を順番にすべて認証するように組み合わせることも、一部のみを選択して認証するよ

うに組み合わせることもできます。例えば、を組み合わせる場合は、カード / QR コード、顔、PIN のすべてで認証する必要があります。を組み合わせる場合は、カード / QR コードで認証した後、顔または PIN を入力する必要があります。

5. 目的の認証モードを設定した後、**Schedule** を設定します。

> **情報**
>
> - **Schedule** は BioStar X で設定できます。設定したスケジュールがない場合は、**Always** だけを選択できます。
> - **Schedule** の設定については、BioStar X 管理者マニュアルをご参照ください。
> - **QR Code** 認証を使用するには、**AUTHENTICATION** → **Operation** で **QR Authentication** が有効になっている必要があり、別途デバイスライセンスが必要です。詳細はライセンスを参照してください。

6. 設定を保存するには **OK** を押します。

認証モードの編集

1. を選択し、管理者権限の認証手段で認証します。
2. **AUTHENTICATION** → **Auth Mode** を押します。
3. 編集する認証モードを選択します。
4. 認証モードの登録を参照して認証モードを修正した後、**OK** を押します。

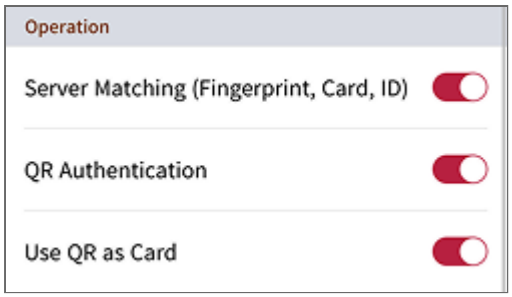
認証モードの削除

1. を選択し、管理者権限の認証手段で認証します。
2. **AUTHENTICATION** → **Auth Mode** を押します。
3. をクリックして削除する項目を選択します。複数選択することもできます。
4. 選択した項目を削除するには **OK** を押します。

認証オプション

認証オプションを設定できます。

1. を選択し、管理者権限の認証手段で認証します。
2. **AUTHENTICATION** を押してから **Operation** で必要なオプションを有効にしてください。



- **Server Matching (Fingerprint, Card, ID)**: サーバーマッチングを使用すると、デバイスではなく BioStar X でユーザー認証を実行します。デバイスに保存されたユーザー情報が多い場合や、クレデンシャル情報が保存されているデバイスを外部にさらしたくない場合に有用です。

  情報

  - **Server Matching** では、指紋・カード・ID だけを使用できます。
  - **Server Matching** を使用する場合は、デバイスと BioStar X の両方でサーバーマッチングを有効にする必要があります。 BioStar X サーバーマッチング設定については、BioStar X 管理者マニュアルをご参照ください。

- **QR Authentication**：デバイスのカメラによる QR コード認証の使用可否を設定できます。

  情報

  QR Authentication を使用するには、別途デバイスライセンスが必要です。詳細はライセンスを参照してください。

- **Use QR as Card**：付与した CSN カードまたは Wiegand カードと同じデータを持つ QR コードで認証できるように設定します。 **QR Authentication** が有効な場合にのみ設定できます。

PIN

パスワード入力時にスクランブルキーパッドを使用するかどうかを設定できます。

1. を選択し、管理者権限の認証手段で認証します。
2. **AUTHENTICATION** を選択し、**PIN** で **Scramble Keypad** の使用有無を設定します。

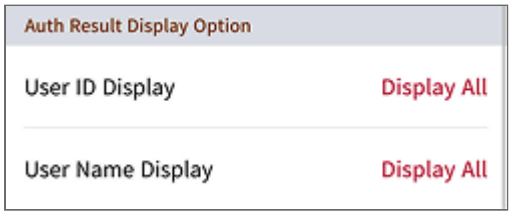


- **Scramble Keypad**：パスワード入力時に数字キーの位置をランダム化して、パスワード流出を防止できます。

認証結果表示オプション

認証結果表示オプションを設定できます。

1. を選択し、管理者権限の認証手段で認証します。
2. **AUTHENTICATION** を選択し、**Auth Result Display Option** で必要な項目を変更します。



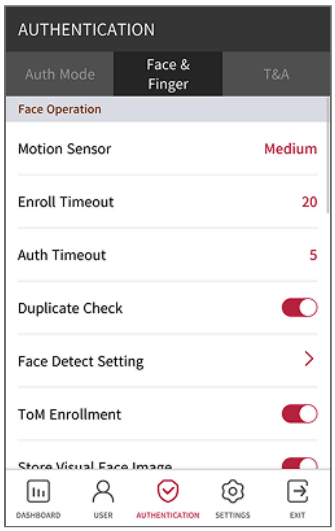
- **User ID Display**：デバイスの認証結果画面でユーザー ID の表示方法を選択できます。
  - **Display All**：ユーザー ID をすべて表示します。
  - **Mask All but First Letter**：ユーザー ID の先頭文字のみ表示します。
  - **Hide All**：ユーザー ID を表示しません。
- **User Name Display**：デバイスの認証結果画面でユーザー名の表示方法を選択できます。
  - **Display All**：ユーザー名をすべて表示します。
  - **Mask All but First Letter**：ユーザー名の先頭文字のみ表示します。
  - **Hide All**：ユーザー名を表示しません。

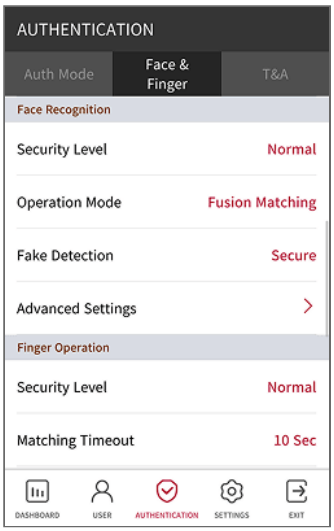
顔 & 指紋

顔

顔認証に関する設定を変更できます。

1. を選択し、管理者権限の認証手段で認証します。
2. **AUTHENTICATION** → **Face & Finger** を選択します。
3. **Face Operation** または **Face Recognition** の設定で必要な項目を変更します。





- **Motion Sensor**：デバイス周辺の動きを検知する感度を設定します。 **Motion Sensor** を **Off** に設定した場合、顔認証を行うには画面をタッチしてから認証を進めてください。
- **Enroll Timeout**：設定した時間内に顔を登録できないと、顔登録がキャンセルされます。
- **Auth Timeout**：設定した時間内に認証を完了できないと、認証失敗となります。
- **Duplicate Check**：顔登録時に重複顔をチェックできます。
- **Face Detect Setting**：顔認証時にデバイスが顔を検出する領域の位置とサイズを設定できます。

> **情報**
> 最適な性能を得るために、**Face Detect Setting** のサブオプションはデフォルト設定のまま使用することを推奨します。各オプションのデフォルト値は次のとおりです。
>
> - 最大顔回転角度：15
> - 顔認識距離：最小 30 cm、最大 100 cm
> - 顔認識領域拡張：無効

- **ToM Enrollment**：**ToM Enrollment** を有効にすると、BioStar X で発行された **Template on Mobile** を登録できます。**Template on Mobile** は、ユーザーのバイオメトリックテンプレートをモバイル端末に保存するモバイルアクセスカードであり、BioStar X サーバー、Airfob Portal、デバイスにユーザーデータを保存せずにバイオメトリック認証を行えます。

> **情報**
> **Template on Mobile** については、BioStar X 管理者マニュアルをご参照ください。

- **Store Visual Face Image**：ビジュアルフェイスに実際の画像とテンプレートの両方を保存するか、画像を保存せずテンプレートのみを保存するかを設定できます。無効にすると、保存されているビジュアルフェイスの画像はすべて削除され、今後登録されるビジュアルフェイスも画像を除いたテンプレートのみ保存されます。

> **情報**
> この設定を無効にした後は、BioStar 2 v2.9.7 以降または BioStar X に接続して使用してください。

- **Security Level**：1:N 認証のセキュリティレベルを設定できます。
- **Operation Mode**：顔認証時のデバイス動作モードを設定できます。
  - **Fusion Matching**：ビジュアルと赤外線の両方でマッチングを行い、顔認証の精度を向上させます。
  - **Fast Matching**：ユーザーはデバイスの認証範囲内を歩きながらでも顔認証を行うなど、高速に認証を実施できます。
- **Fake Detection**：写真などの偽造顔を用いたユーザー認証を防止できます。 **Operation Mode** を **Fusion Matching** に設定すると有効になります。

> **情報**
> 日差しが強い環境では、**Fake Detection** 機能を **Normal** に設定することを推奨します。

- **Advanced Settings**：マスク検出など顔認証に関する高度な設定を変更できます。
  - **Mask Detection**：マスク検出の使用有無を設定できます。
  - **Detection Mode**：マスク着用の確認方法を設定できます。 **Mask Detection** を **Enabled** に設定すると有効になります。

    > **情報**
    > - **Require Mask (Hard)**：マスク未着用のユーザーは認証が拒否され、マスク未着用イベントがログに記録されます。
    > - **Require Mask (Soft)**：マスク未着用のユーザーも認証できますが、マスク未着用イベントがログに記録されます。
    > - **Require No Mask**：マスク未着用のユーザーのみ認証でき、このモードを使用する場合、マスク確認モードは **Check Before Authentication** に固定されます。

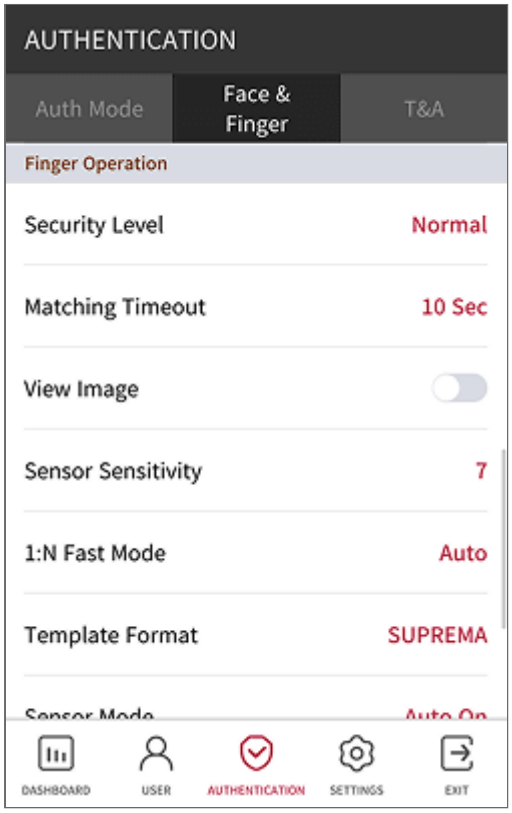
  - **Mask Detection Level**：マスク着用を検知する感度を設定できます。 **Mask Detection** を **Enabled** に設定すると有効になります。
  - **Check Mode**：デバイスの用途に応じて確認モードを設定できます。

> **情報**
>
> - **Check After Authentication**：認証を実行した後にユーザーのマスク着用を確認します。
> - **Check Before Authentication**：ユーザーのマスク着用を確認した後に認証を実行します。
> - **Check Only**：デバイスをマスク着用確認専用として使用できます。このモードを使用すると、認証に関係なくマスクを着用したユーザーはすべて入退室できます。

指紋 BS3M-ODB, BS3M-OAPB

指紋認証に関する設定を変更できます。

1. を選択し、管理者権限の認証手段で認証します。
2. **AUTHENTICATION** → **Face & Finger** を選択します。
3. **Finger Operation** の設定で必要な項目を変更します。



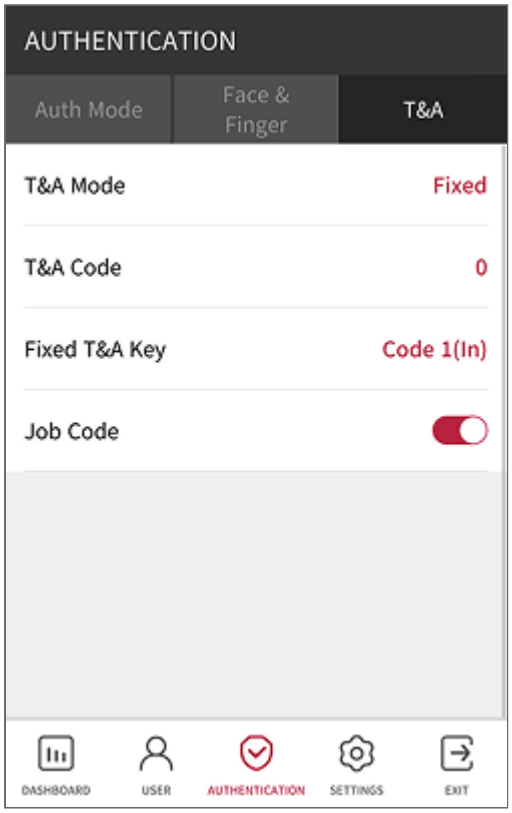
- **Security Level**：1:N 認証のセキュリティレベルを設定できます。
- **Matching Timeout**：指紋マッチング時の待機時間を設定できます。設定した時間内に認証を完了できないと、認証失敗となります。
- **View Image**：指紋をスキャンしたときに元画像を表示できます。
- **Sensor Sensitivity**：指紋センサーの感度を設定できます。より精密な指紋情報を取得するには、センサー感度を高く設定してください。
- **1:N Fast Mode**：指紋認証速度を設定できます。 **Auto** を選択すると、端末に登録されている指紋テンプレートの総数に応じて認証パフォーマンスが設定されます。

- **Template Format**：指紋テンプレート形式を設定できます。 **SUPREMA** が既定で設定されており、テンプレート形式を変更すると以前に保存されたすべての指紋が使用できなくなるため、変更する際は注意してください。
- **Sensor Mode**：**Auto On** に設定すると、指紋センサーがユーザーの指を検知して起動します。 **Always On** に設定すると、指紋をスキャンしていないときでもセンサーが常にオンになります。
- **Live Finger Detection**：偽造指紋検出レベルを設定できます。偽造指紋検出レベルを高く設定すると、実際の指紋に対する拒否率も高くなる場合があります。
- **Advanced Enrollment**：高品質な指紋情報を保存するために、スキャンした指紋の品質を検査できます。有効にすると、指紋の品質が低い場合にユーザーに通知して、指紋を正しくスキャンするのを支援します。
- **Duplicate Check**：指紋登録時に重複指紋かどうかを検査できます。

勤怠

勤怠モードの登録方法を設定できます。

1. を選択し、管理者権限の認証手段で認証します。
2. **AUTHENTICATION** → **T&A** を選択します。
3. 必要な項目を設定してください。



- **T&A Mode**：勤怠モードの使用方法を設定できます。
- **T&A Code**：勤怠イベントを登録できます。勤怠イベントを登録するには、**T&A Code** → を選択し、画面に表示するアイコン、**T&A Event Name**、**Schedule** を設定します。
- **T&A Required**：ユーザーが認証する際に必ず勤怠イベントを選択するよう設定できます。 **T&A Mode** を **By User** に設定したときに使用できます。
- **Fixed T&A Key**：管理者が選択した勤怠イベントのみ使用するよう設定できます。 **T&A Mode** を **Fixed** に設定したとき

に使用できます。

- **Job Code**：作業コードの使用有無を選択できます。

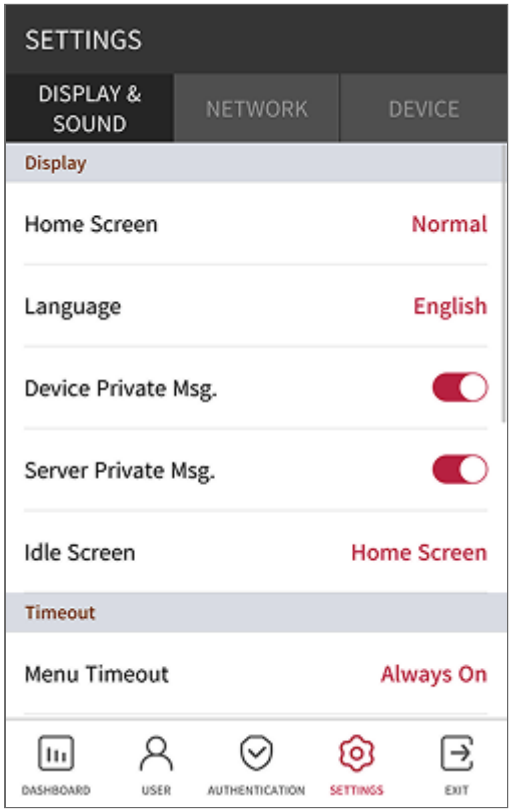
設定

システムおよびデバイスの設定方法について案内します。

画面とサウンド

デバイスの画面とサウンドの設定を変更できます。

1. を選択し、管理者権限の認証手段で認証します。
2. **SETTINGS** → **DISPLAY & SOUND** を押してください。
3. 必要な項目を変更してください。



- **Home Screen**：ホーム画面の背景に表示する項目を選択できます。
- **Language**：画面に表示される言語を選択できます。
- **Device Private Msg.**：ユーザーが認証する際に画面に表示する個人メッセージの使用有無を設定できます。 **Device Private Msg.** は BioStar Device SDK を使用して設定できます。設定していない場合、デバイスで **Device Private Msg.** を有効にしても、認証成功時にメッセージは表示されません。
- **Server Private Msg.**：ユーザーが認証する際に画面に表示する個人メッセージの使用有無を設定できます。 **Server Private Msg.** は BioStar X API を使用して設定できます。設定していない場合、デバイスで **Server Private Msg.** を有効にしても、認証成功時にメッセージは表示されません。
- **Idle Screen**: デバイスを使用しないときに画面に表示する待機画面を選択できます。

  - **Home Screen**: ほかの待機画面を表示せず、設定したホーム画面を表示します。
  - **Screen Saver**: スクリーンセーバーを表示します。デバイスを使用していないときに画面の明るさを下げて電力消費を削減できます。
  - **Video**: BioStar X に登録した動画を再生します。**Video Schedule**を設定すると、指定した時間は動画を繰り返し再生し、それ以外の時間は**Home Screen**または**Screen Saver**で表示する画面を選択できます。動画再生の詳細はBioStar X 管理者説明書を参照してください。

    > **情報**
    > 動画は最大 3 件まで登録できます。

- **Menu Timeout**：メニュー画面が自動的に消えるまでの時間（秒）を設定できます。設定した時間内にボタン入力がない場合は、ホーム画面に戻ります。
- **Message Timeout**：設定完了メッセージや通知メッセージなどが自動的に消えるまでの時間（秒）を設定できます。
- **Backlight Timeout**：画面のバックライトが消灯するまでの時間（秒）を設定できます。
- **Voice Instruction**：通知音の代わりに音声ガイダンスを使用できます。
- **Volume**：音量を設定できます。
- **Video Volume**: 待機画面で再生する動画の音量を調整できます。
- **Intercom Speaker Volume**：IPインターホン使用時にスピーカーから出力される音量を調整できます。
- **Intercom Microphone Volume**：IPインターホン使用時にマイクに入力される音量を調整できます。

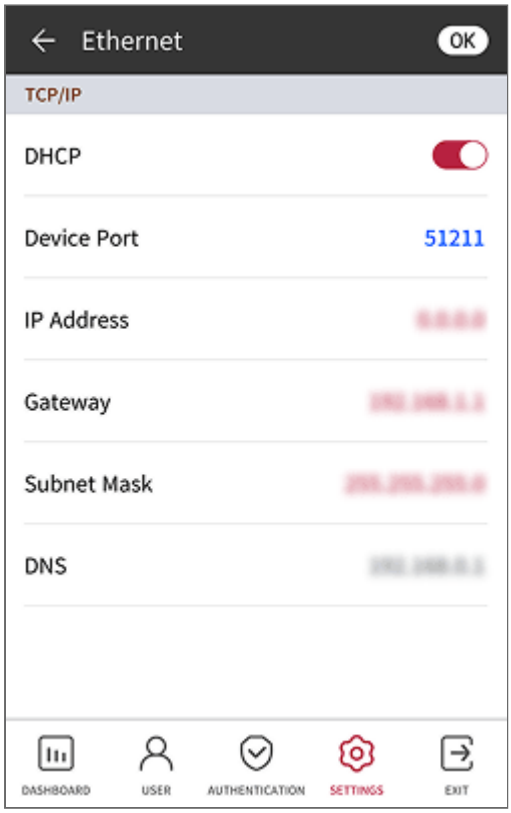
> **情報**
> BioStar Device SDK の詳細については、Suprema ナレッジベースの BioStar Device SDK ページ を参照してください。

通信

イーサネット、サーバー、OSDP 通信など、デバイスの通信設定を変更できます。

イーサネット

1. を選択し、管理者権限の認証手段で認証します。
2. **SETTINGS** → **NETWORK** → **Ethernet** を選択します。
3. 必要な項目を設定してください。

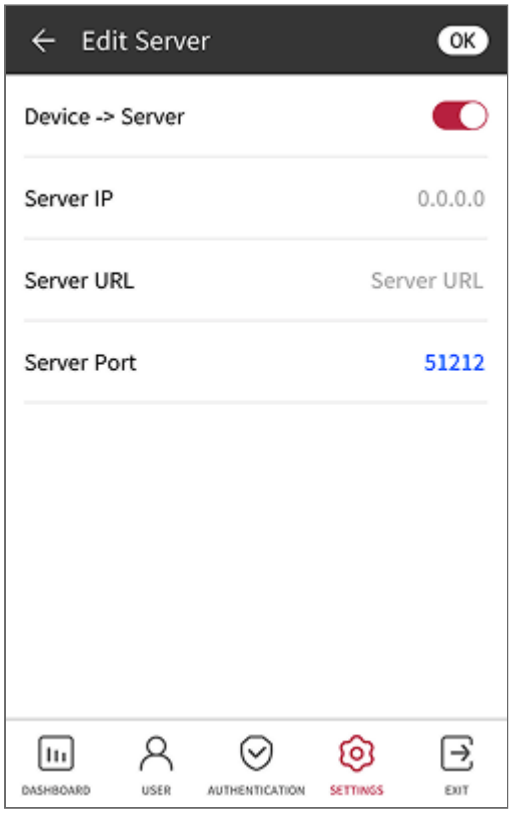


- **DHCP**：DHCP の使用有無を設定します。 DHCP 設定をオフにすると、**IP Address**、**Gateway**、**Subnet Mask** をユーザーが編集できます。
- **Device Port**：デバイスのポートを設定できます。
- **IP Address**：デバイスの IP アドレスを確認できます。 DHCP 設定をオフにして変更する。
- **Gateway**：デバイスのゲートウェイを確認できます。 DHCP 設定をオフにして変更する。
- **Subnet Mask**：デバイスのサブネットマスクを確認できます。 DHCP 設定をオフにして変更する。
- **DNS**：ドメインネームサーバーのアドレスを設定できます。

4. 設定を保存するには **OK** を押します。

サーバー

1. を選択し、管理者権限の認証手段で認証します。
2. **SETTINGS** → **NETWORK** → **Server** を選択します。
3. 必要な項目を設定してください。

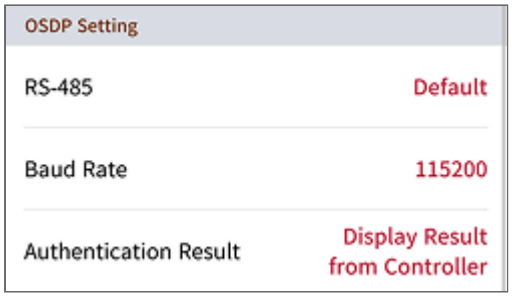


- **Device → Server**：デバイスから入力した情報を持つサーバーに直接接続信号を送信できます。 **Device → Server** 設定をオンにすると、**Server IP**、**Server URL**、**Server Port** をユーザーが入力できます。
- **Server IP**：BioStar XがインストールされたPCのIPを入力します。
- **Server URL**：**Server IP** の代わりに **Server URL** を入力できます。
- **Server Port**：BioStar XがインストールされたPCのポートを入力します。

4. 設定を保存するには **OK** を押します。

OSDP 通信設定

1. を選択し、管理者権限の認証手段で認証します。
2. **SETTINGS** → **NETWORK** を選択します。
3. **OSDP Setting** で必要な項目を設定します。



- **RS-485**：RS-485 の動作モードを選択できます。
- **Baud Rate**：必要な通信速度を選択できます。
- **Authentication Result**：**Intelligent Slave** を使用する場合、他社コントローラーまたはデバイスの認証結果を画面に表示するかどうかを選択できます。 **RS-485** モードを **Default** または **Slave** に設定したときに使用できます。

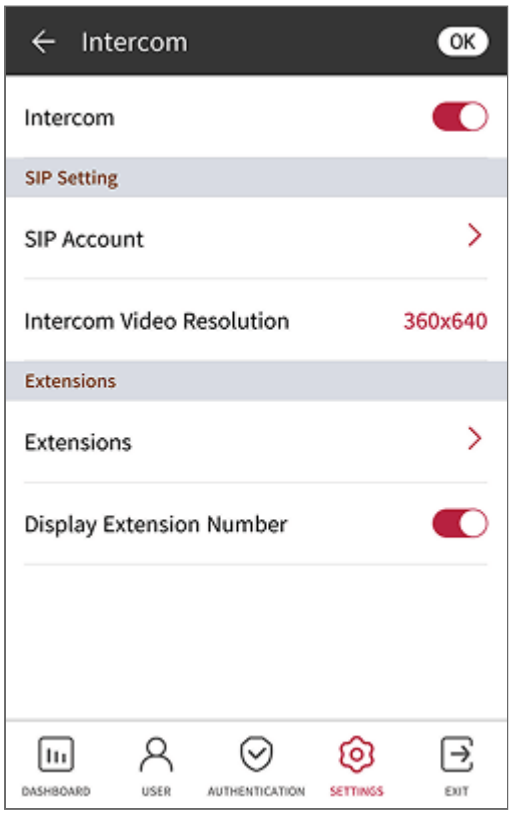
デバイス

IPインターホン

IP インターホンのアカウントと内線を設定できます。

> **情報**
> エコーキャンセリング（AEC）機能を利用するには、SIP クライアント（例：MicroSIP、Linphone）のオーディオコーデックを G.722 に設定する必要があります。 G.721 コーデックに設定されている場合、通話は可能ですが、エコーキャンセリング機能は利用できません。

1. を選択し、管理者権限の認証手段で認証します。
2. **SETTINGS** → **DEVICE** → **Intercom** を押します。



- **Intercom**：IPインターホンの有効化を設定できます。 IPインターホン設定をオンにすると、**SIP Account** と **Extensions** を設定できます。
- **SIP Account**：SIPサーバーにデバイスを登録できるよう、各項目を正しく入力してください。
- **Intercom Video Resolution**：デバイスから送出されるIPインターホン映像の解像度を選択できます。
- **Extensions**：内線番号を追加および削除できます。
- **Display Extension Number**：内線番号の表示可否を設定できます。

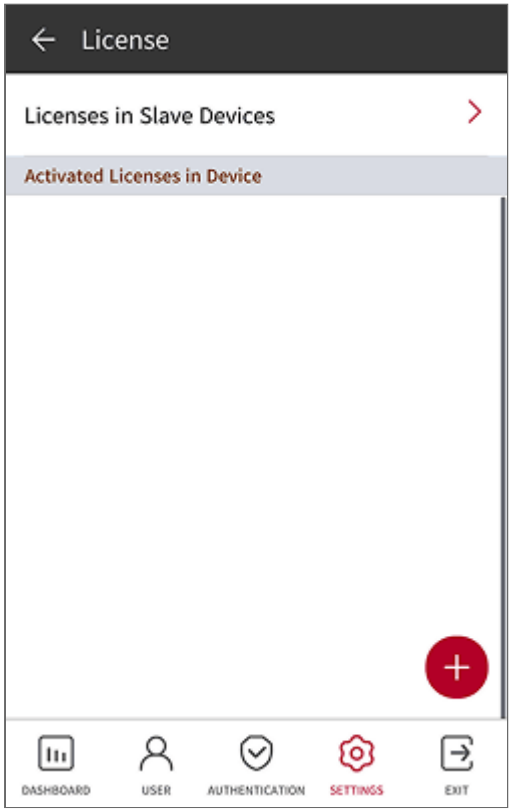
> **情報**
>
> - 内線番号に **Display Name** を設定していない場合、発信画面で受信者を識別できなくなります。
> - 内線番号には英字（大文字・小文字）、数字、特殊記号 `+` `-` `@` `.` のみ入力できます。

3. 設定を保存するには **OK** を押します。

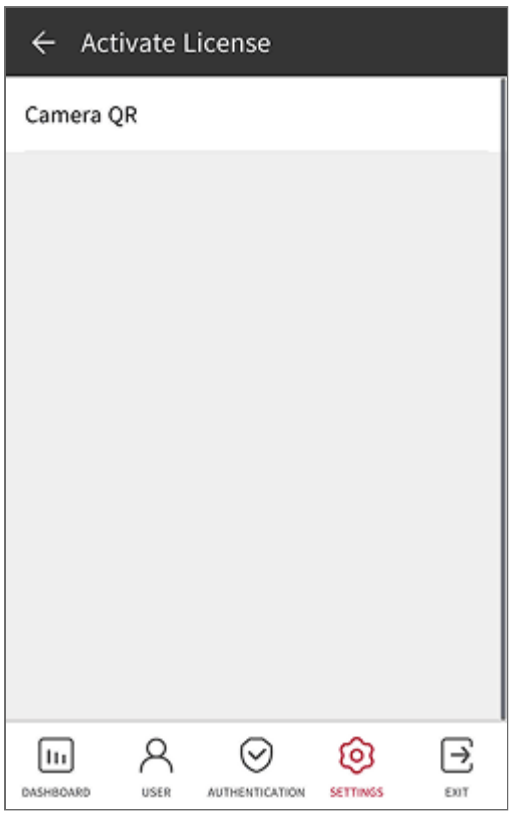
ライセンス

デバイスライセンスを有効化したり、**Licenses in Slave Devices** と **Activated Licenses in Device** を確認できます。

1. を選択し、管理者権限の認証手段で認証します。
2. **SETTINGS** → **DEVICE** → **License** をタップします。
3. デバイスライセンスを有効化するには、ライセンスが保存された USB をデバイスに接続し、を選択してください。



4. 有効化できるライセンスが画面に表示されます。必要なライセンスを有効化してください。



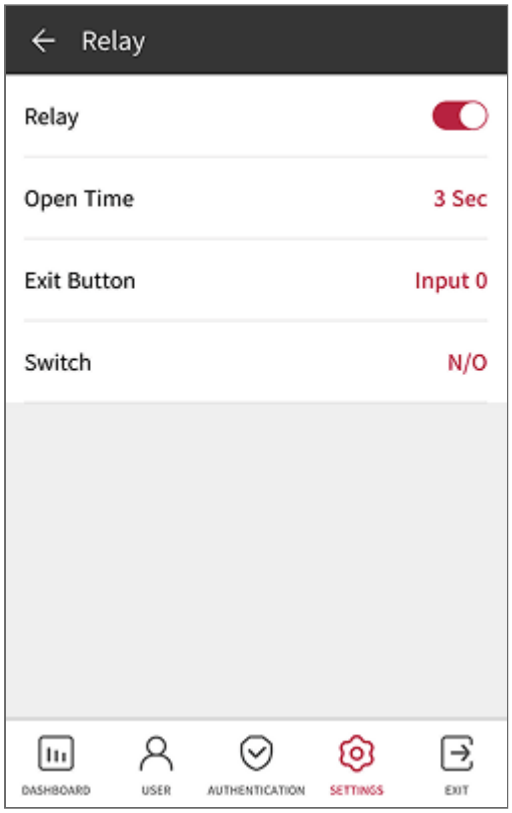
情報

- デバイスライセンスを発行するには、購入先にお問い合わせください。
- デバイスライセンス 1 つにつき、1 つの機能を使用できます。
- 1 つのデバイスライセンスファイルに複数のデバイスライセンスを含めることができます。（最大 100 個まで対応）
- デバイスライセンスファイルは暗号化されているため、任意に変更できません。
- デバイスライセンスはデバイス ID を基準に発行されます。不正な方法でデバイス ID を変更した場合、ライセンスの保証サービスは提供されません。

リレー

デバイスで **Open Time** と **Exit Button** の入力ポートを設定できます。

1. を選択し、管理者権限の認証手段で認証します。
2. **SETTINGS** → **DEVICE** → **Relay** をタップします。

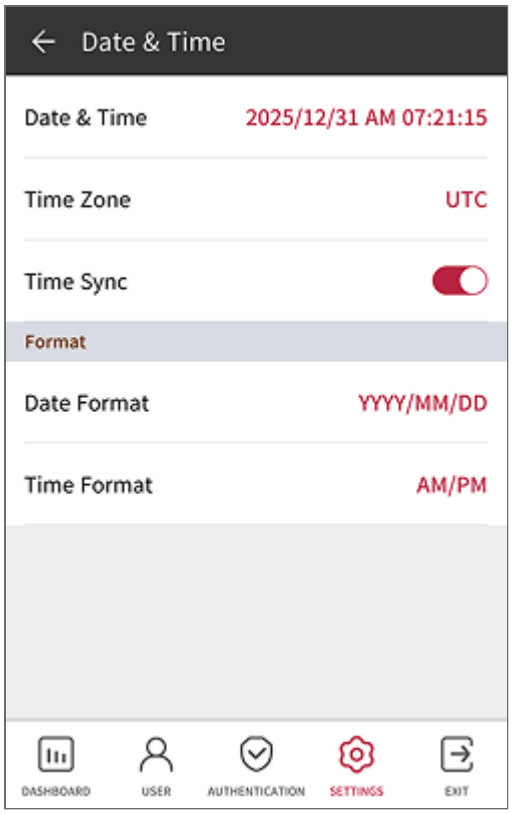


- **Relay**：リレーの有効化を設定できます。リレー設定をオンにすると、**Open Time**、**Exit Button** を設定できます。
- **Open Time**：正しくユーザー認証が行われたときにドアを開けておく時間を設定できます。
- **Exit Button**：退室ボタンが接続されている入力ポートを選択してください。
- **Switch**：退室ボタン入力ポートのスイッチ（**N/O** または **N/C**）の種類を選択できます。

日付と時刻

日付と時刻を設定できます。正確なログデータを収集するために適切に設定してください。

1. を選択し、管理者権限の認証手段で認証します。
2. **SETTINGS** → **DEVICE** → **Date & Time** をタップします。
3. 必要な項目を変更してください。

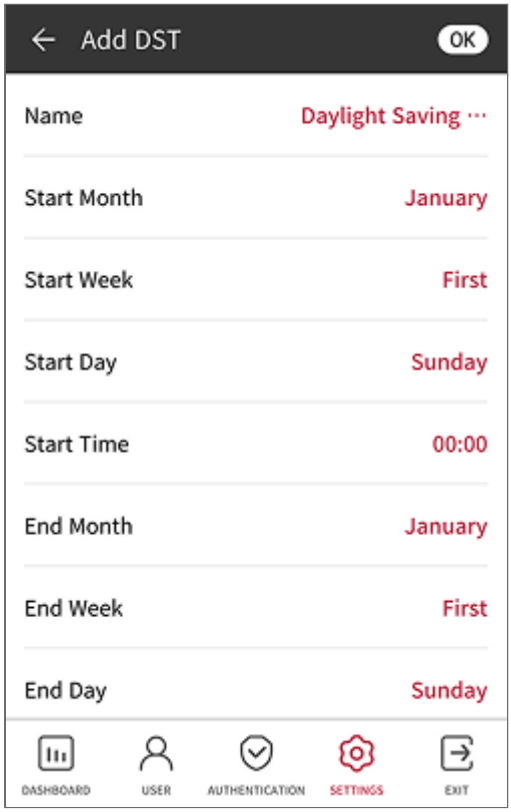


- **Date & Time**：現在の日付と時刻を確認できます。直接修正するには、**Time Sync** をオフにしてください。
- **Time Zone**：現在の地域の時間基準を設定できます。
- **Time Sync**：サーバーと時刻を同期できます。サーバーと時刻を同期するには、**Time Sync** をオンにしてください。
- **Date Format**：日付形式を設定できます。**YYYY/MM/DD**、**MM/DD/YYYY**、**DD/MM/YYYY** を選択できます。
- **Time Format**：時刻形式を設定できます。**AM/PM**、**24-Hour** を選択できます。

サマータイム

デバイスで夏時間（DST）を適用できます。開始日時と終了日時を適切に設定してください。

1. を選択し、管理者権限の認証手段で認証します。
2. **SETTINGS** → **DEVICE** → **Daylight Saving Time** を選択してから、をタップしてサマータイムを追加します。
3. 必要な項目を変更してください。



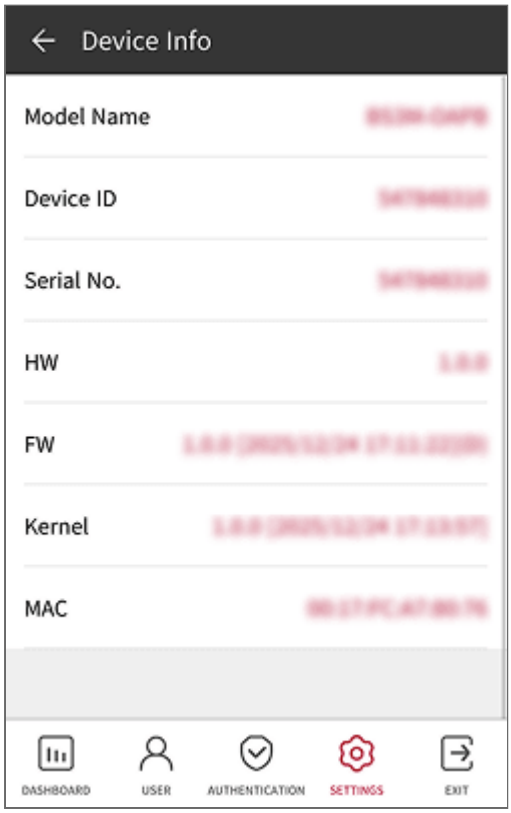
- **Name**：サマータイムの名前を入力してください。
- **Start Month** / **Start Week** / **Start Day** / **Start Time**：サマータイム適用を開始する月、週、曜日、時刻を設定してください。
- **End Month** / **End Week** / **End Day** / **End Time**：サマータイム適用を終了する月、週、曜日、時刻を設定してください。

4. 設定を保存するには **OK** を押します。

デバイス情報

モデル名、デバイス ID、シリアル番号、デバイスおよびファームウェアのバージョン、カーネル、MAC アドレスを確認できます。

1. を選択し、管理者権限の認証手段で認証します。
2. **SETTINGS** → **DEVICE** → **Device Info** を選択します。**Model Name**、**Device ID**、**Serial No.**、**HW**、**FW**、**Kernel**、**MAC** の情報を確認できます。



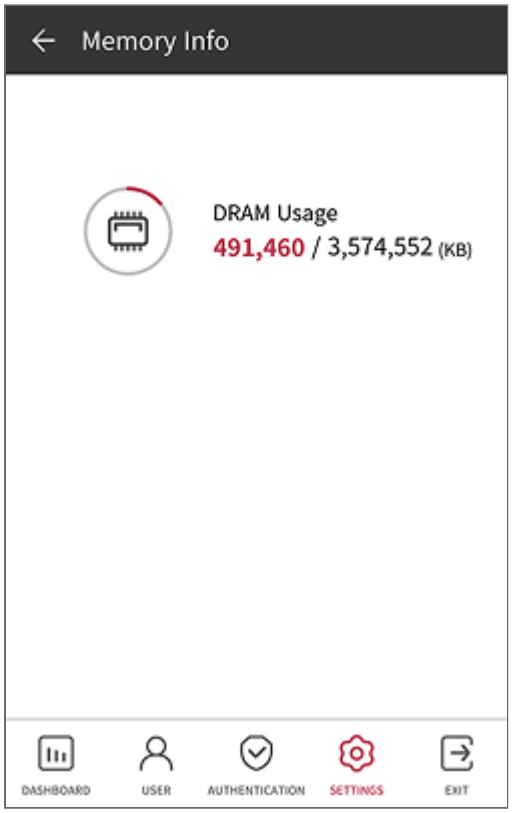
情報

MAC 項目を長押しすると、偽顔検出のアルゴリズムバージョンを確認できる **FAS_IR_SP** 情報が表示されます。
FAS_IR_SP 項目をタップすると、全体ハッシュ値をポップアップメッセージで確認できます。

メモリ情報

メモリ使用情報を確認できます。

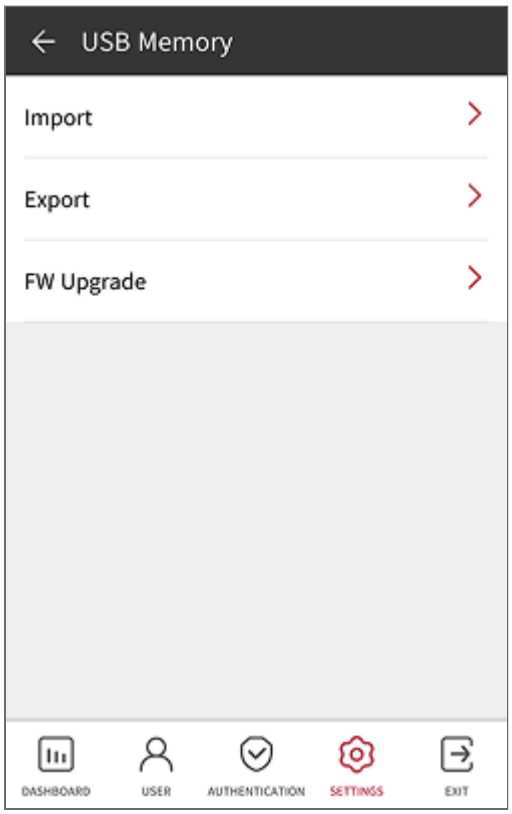
1. を選択し、管理者権限の認証手段で認証します。
2. **SETTINGS** → **DEVICE** → **Memory Info** を選択します。デバイスのメモリ使用状況を確認できます。



USB メモリ

デバイスに USB メモリを接続してユーザー情報をインポートしたり、ログとユーザー情報をエクスポートしたりできます。ファームウェアをアップグレードすることもできます。

1. を選択し、管理者権限の認証手段で認証します。
2. **SETTINGS** → **DEVICE** → **USB Memory** を選択します。
3. 必要な項目を選択して設定を変更してください。



- **Import**：接続された USB メモリからユーザー情報をインポートできます。
- **Export**：接続された USB メモリにエクスポートする情報を選択できます。
- **FW Upgrade**：接続された USB メモリにファームウェアファイルが保存されている場合、ファームウェアをアップグレードできます。

注意

ファームウェアのアップグレード中に電源が切れないよう注意してください。故障の原因になります。

情報

- USB メモリはファイルシステムが exFAT 形式の製品を使用することを推奨します。 FAT32 形式の USB メモリを使用すると、保存されている顔データが 50,000 件を超える場合にデバイスが誤動作する可能性があります。
- USB メモリの空き容量を確認してください。顔データ 100,000 件の場合、15 GB 以上の空き容量が必要です。

セキュリティタンパー

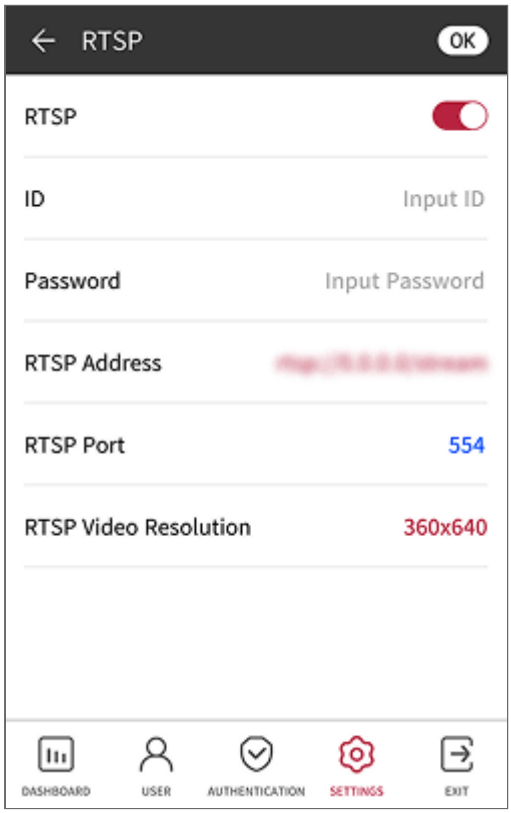
セキュリティタンパーの使用可否を設定できます。セキュリティタンパーが発生した場合、すべてのユーザー、すべてのログ、セキュリティキーが削除されます。

1. を選択し、管理者権限の認証手段で認証します。
2. **SETTINGS** → **DEVICE** を選択します。
3. タンパー発生時にすべてのユーザー、すべてのログ、セキュリティキーが削除されるように設定するには、**Secure Tamper** 設定をオンにしてください。

RTSP

サードパーティ製ビデオ管理システム (VMS) と接続して、製品のビジュアルカメラで撮影した映像をモニタリングします。

1. を選択し、管理者権限の認証手段で認証します。
2. **SETTINGS** → **DEVICE** → **RTSP** を選択してください。
3. 必要な項目を選択して設定を変更してください。



- **RTSP**：RTSP の有効化を設定できます。 RTSP 設定を有効にすると、**ID**、**Password**、**RTSP Address**、**RTSP Port**、**RTSP Video Resolution** を設定できます。
- **ID**：ID を入力してください。 ID には英字（大文字と小文字を区別）、数字、一部の記号 - _ を組み合わせて最大 32 文字まで入力できます。
- **Password**：パスワードを入力します。パスワードには英字（大文字または小文字）と数字を組み合わせて 8～32 文字を入力できます。
- **RTSP Address**：RTSP アドレスを入力してください。

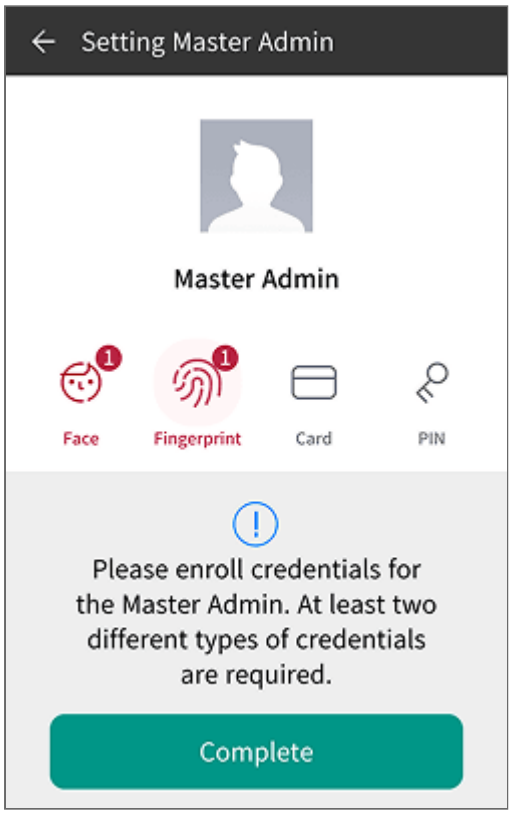
- **RTSP Port**：RTSP ポート番号を入力してください。
- **RTSP Video Resolution**：デバイスから出力される RTSP 映像の解像度を選択できます。

> **情報**
> デバイスをスレーブデバイスとして構成した場合、RTSP 機能は使用できません。

マスター管理者 CE 向け製品

マスター管理者の認証手段を変更できます。

1. を選択し、管理者権限の認証手段で認証します。
2. **SETTINGS** → **DEVICE** → **Master Admin** を選択してください。
3. **Complete** を押して、希望する認証手段を設定した後に保存します。



> **情報**
> 少なくとも 2 種類以上のクレデンシャルを登録する必要があります。

デバイスの再起動

デバイスを再起動できます。

1. を選択し、管理者権限の認証手段で認証します。
2. **SETTINGS** → **DEVICE** → **Restart Device** を選択してください。
3. デバイスを再起動するには **OK** を押してください。前の画面に戻るには **Cancel** を押してください。

デフォルト値に戻す

デバイス設定、ネットワーク設定、ユーザー権限などが初期化されます。

1. を選択し、管理者権限の認証手段で認証します。
2. **SETTINGS** → **DEVICE** → **Restore Default** を選択してください。
   - **All settings**：デバイスに保存されているすべての設定を初期化します。デバイス設定をすべて初期化するには **OK** を押してください。前の画面に戻るには **Cancel** を押してください。
   - **Keep Network Settings**：ネットワーク設定を除くすべての設定を初期化します。ネットワーク設定を除くすべての設定を初期化するには **OK** を押してください。前の画面に戻るには **Cancel** を押してください。
   - **Factory Default**：デバイスに保存されているすべての情報とルート証明書を削除し、設定を初期化します。
   - **Delete the Root Certificate**：デバイスに保存されているルート証明書を削除します。
3. **Restore Default** を実行すると、デバイスが再起動します。

> **情報**
>
> - 初期化を実行すると、ユーザー権限も同時に初期化されます。初期化を実行した後、必ずユーザー権限を再設定してください。
> - 初期化を実行しても言語設定は変更されません。
> - **Factory Default** メニューは、デバイスにルート証明書が保存されている場合に使用できます。
> - **Delete the Root Certificate** メニューは、デバイスにルート証明書が保存され、全管理者が設定されている場合に使用できます。

ユーザー ID の種類

デバイスに登録するユーザー ID の形式を選択できます。

1. を選択し、管理者権限の認証手段で認証します。
2. **SETTINGS** → **DEVICE** → **User ID Type** を選択してください。
   - **Number**：ユーザー ID は数字のみ入力できます。
   - **Alphanumeric**：ユーザー ID は英数字と一部の特殊記号（`_` `-` `.`）を組み合わせて入力できます。
3. 必要な項目を選択してください。

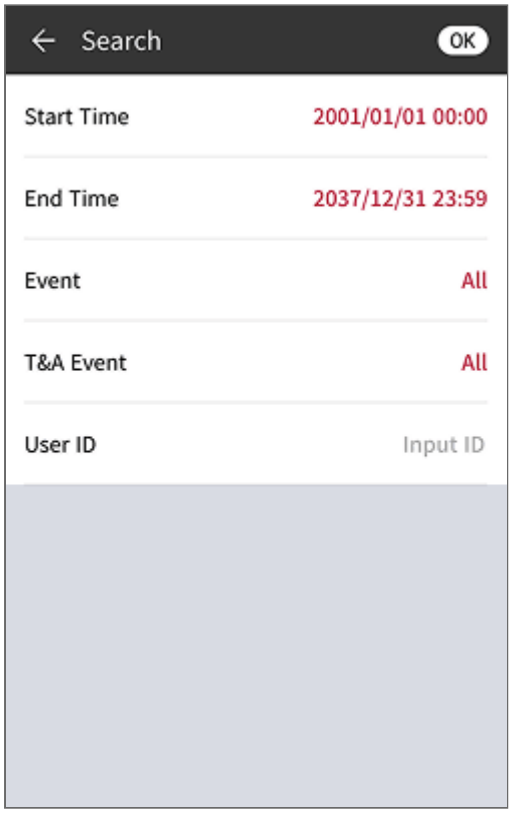
イベントログ

デバイスで発生したイベントの履歴を確認する方法を説明します。

イベントログを検索する

条件を設定してログを検索できます。

1. を選択し、管理者権限の認証手段で認証します。
2. **DASHBOARD** で を選択します。すべてのイベントログの一覧が表示されます。
3. 特定のイベントを検索するには を押し、必要な項目を変更します。



4. 検索条件を設定して **OK** を押すと、条件に一致するログが画面に表示されます。

すべてのログを削除

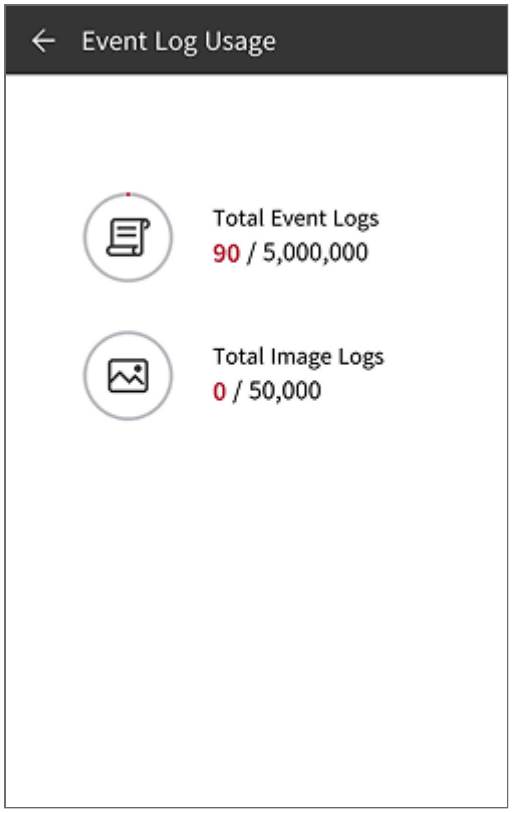
保存されているログをすべて削除できます。

1. を選択し、管理者権限の認証手段で認証します。
2. **DASHBOARD** で を選択します。すべてのイベントログの一覧が表示されます。
3. を選択してから **OK** を押して、すべてのログを削除します。前の画面に戻るには **Cancel** を押してください。

ログの使用量を確認する

ログの使用状況を確認できます。

1. を選択し、管理者権限の認証手段で認証します。
2. **DASHBOARD** で → を押します。デバイスのイベントログとイメージログの使用量を確認できます。



トラブルシューティング

デバイス使用中に発生する可能性のある問題のチェック項目と基本的な解決方法を提供します。

故障報告前の確認事項

デバイスを使用中に発生する可能性のある予期しない問題の解決に役立つ情報を提供します。

電源

Q. 電源が供給されていますが、動作しません。

- 端末とブラケットが離れている場合、タンパースイッチによって動作しないことがあります。
- アダプターまたは電源接続ケーブルを確認してください。

PIN

Q. PIN を紛失しました。

- 一般ユーザーの PIN は管理者に依頼してから再入力してください。
- 管理者 PIN を紛失した場合は、設置業者にお問い合わせください。

Q. PIN を入力してから OK ボタンを押しても、施錠されたドアを開けられません。

- 登録した PIN を正しく入力したか確認してください。
- 最近 PIN を変更していないか確認してください。
- PIN が分からない場合は管理者に依頼してから再入力してください。

QR/バーコード

Q. QR/バーコードがうまく読み取れません。

- 正しいQR/バーコード認証方法を確認してから再度お試しください。
- モバイル端末で受け取ったQR/バーコードの場合は、画面が見やすいようにモバイル端末の明るさを調整するか、画面を拭いてから再度お試しください。
- 問題が解決しない場合は、QR/バーコードを発行した管理者にお問い合わせください。

顔

Q. 登録はされたものの顔認証がうまくいかず、エラーが多発します。

- 顔を登録する際の注意事項を確認してから顔を再登録してください。
- 登録されている顔の数が多い場合は、**Matching Timeout** を変更してから再度お試しください。

Q. 突然顔認証ができなくなりました。

- 顔を認証する際の注意事項を確認してから再度お試しください。

Q. Mask Detection 機能を Enabled に設定しましたが、マスク着用時に顔認証がうまくいかずエラーが多発します。

- マスクを鼻先まで下げてから顔を2回認証し、その後鼻を覆って再度顔認証を試してください。問題が続く場合は設置業者にお問い合わせください。

指紋

Q. 登録はされたものの指紋認証がうまくいかず、エラーが多発します。

- 正しい指紋入力方法を確認してから指紋を再登録してください。
- 指紋に傷がある場合、機器が他人の指紋として誤認識することがあります。
- 登録されている指紋の数が多い場合は、**Matching Timeout** を変更してから再度お試しください。
- 指紋ごとの特徴の違いにより認識率が異なるため、別の指の指紋を登録してください。

Q. 突然指紋認証ができなくなりました。

- 指や指紋センサーに汗、水分、ほこりなどが付着していないか確認し、きれいに拭いてください。
- 乾いたタオルなどで指と指紋センサーを拭いてから再度お試しください。
- 指の指紋が非常に乾燥している場合は、息を吹きかけてから再度お試しください。

Q. 指紋センサーが起動しません。

- **Sensor Mode** が **Auto On** に設定されている場合、指紋センサーに指を置いたときのみセンサーがオンになります。常に指紋センサーをオンにしたい場合は、**Sensor Mode** を **Always On** に設定してください。

ドアロック

Q. ドアを閉めてもロック装置が施錠されません。

- 電気ロック装置の異常の可能性があります。設置業者による点検を受けてください。

時間

Q. 突然時刻が合わなくなりました。

- 装置には内蔵バッテリーがありますが、長時間電源が供給されないと内蔵バッテリーが放電し、時刻がずれることがあります。日付と時刻メニューを参照して時刻を修正できます。

管理者アクセス

Q. 管理者PINを紛失して管理者モードに入れません。

- 装置は管理者が入出許可権限を付与するため、メニューに入れるのは管理者のみです。
- 管理者 PIN を紛失した場合は、設置業者にお問い合わせください。

製品仕様

製品のサイズ、機能、性能などの主要な仕様情報を提供します。

クレデンシャル

生体認証	**顔** • **認証距離[1]:0.3 ~ 1.3 m** • **認証高さ:1.4 ~ 1.9 m** • **マッチング速度:0.2 秒以内** • **偽顔検出:対応** **指紋** BS3M-ODB, BS3M-OAPB • **画像サイズ:300 x 400 画素** • **解像度:500 dpi** • **テンプレート:SUPREMA / ISO19794-2 / ANSI-378** • **抽出／照合:MINEX 認証取得および準拠** • **センサー認証:FBI PIV および FBI モバイル ID FAP20** • **偽造指紋検出:サポート対象（SW ベース）**	
RFカード	**BS3M-DB, BS3M-ODB**	**125kHz EM および 13.56MHz MIFARE、MIFARE Plus、DESFire、DESFire EV1/EV2/EV3、FeliCa**
	BS3M-APB, BS3M-OAPB	**125kHz EM、HID Prox および 13.56MHz MIFARE、MIFARE Plus、DESFire、DESFire EV1/EV2/EV3、FeliCa、iCLASS SE/SR/Seos**
RF認証距離[2]	**EM/MIFARE/DESFire/HID iCLASS：50 mm、HID Prox/FeliCa：30 mm**	
モバイル	**NFC、BLE**	
スクランブルキーパッド（PIN）	**対応**	
QR/バーコード[3]	**対応[4]**	
QR/バーコード認証距離[5]	**8 ~ 25 cm**	

一般

モデル名	**BS3M-DB, BS3M-APB, BS3M-ODB, BS3M-OAPB**	
CPU	**1.4 GHz クアッドコア**	
メモリ	**32 GB Flash + 4 GB RAM**	
暗号チップ	**対応**	
ディスプレイ	**7 インチ IPS カラー LCD**	
画面解像度	**800 x 1280 画素**	
サウンド	**16 bit**	
動作温度	**-20 °C ~ 50 °C**	
保管温度	**-40 °C ~ 70 °C**	
動作湿度	**0 % ~ 80 %（結露なきこと）**	
保管湿度	**0 % ~ 90 %（結露なきこと）**	
カメラ	• **IR：200 万画素** • **ビジュアル：200 万画素**	
寸法 (W x H x D)	**機器**	• **BS3M-DB, BS3M-APB: 119.8 x 233 x 23.5 (mm)** • **BS3M-ODB, BS3M-OAPB: 119.8 x 268.3 x 23.5 (上部) / 49.6 (下部) (mm)**
	ブラケット	• **BS3M-DB, BS3M-APB: 98.4 x 223.3 (mm)** • **BS3M-ODB, BS3M-OAPB: 98.4 x 251.4 (mm)**
重量	**機器**	• **BS3M-DB, BS3M-APB: 565 g** • **BS3M-ODB, BS3M-OAPB: 640 g**
	ブラケット	• **BS3M-DB, BS3M-APB: 187 g (ワッシャーおよびボルトを含む)** • **BS3M-ODB, BS3M-OAPB: 206 g (ワッシャーおよびボルトを含む)**

IP等級	**IP65**
IK等級	**IK06**
認証	**CE** CE モデルのみ、**UKCA、KC、FCC、IC、RCM、RoHS、REACH、WEEE、SIG、MIC、TELEC、ETL Listed to UL 294**

ストレージ

最大ユーザー数	**100,000**[6)]	
最大クレデンシャル数（1:N）	**BS3M-DB, BS3M-APB**	• **顔：50,000** • **カード：100,000**
	BS3M-ODB, BS3M-OAPB	• **顔：50,000** • **指紋：100,000** • **カード：100,000**
最大クレデンシャル数（1:1）	**BS3M-DB, BS3M-APB**	• **顔：100,000** • **カード：100,000** • **PIN：100,000**
	BS3M-ODB, BS3M-OAPB	• **顔：100,000** • **指紋：100,000** • **カード：100,000** • **PIN：100,000**
最大テキストログ数	**5,000,000**	
最大イメージログ数	**50,000**	

インターフェース

イーサネット	**サポート対象（10/100/1000 Mbps、自動 MDI/MDI-X）**
ネットワークプロトコル	**TCP、UDP**
RS-485	**1 チャンネルホスト/スレーブ（選択可能）**

RS-485通信プロトコル	**OSDP V2 準拠**
Wiegand	**1 チャンネル入力、1 チャンネル出力**
入力	**3 チャンネル入力**
リレー	**1 リレー**
PoE+[7)]	**BS3M-DB, BS3M-ODB　非対応** **BS3M-APB, BS3M-OAPB　対応（IEEE 802.3at 互換）**
インターホン	**対応**
RTSP	**対応**
USB	**USB 2.0 (Type C)**
USB拡張ポート	**対応**
タンパー	**対応**

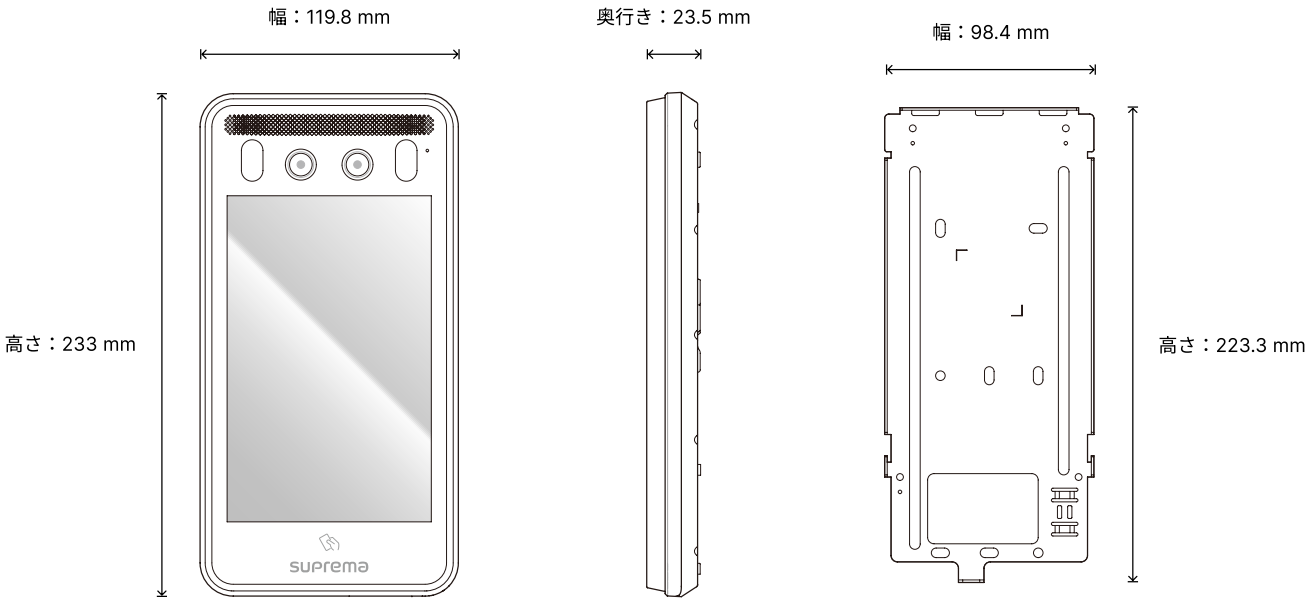
電気仕様

電源	**12 Vdc**	**電流：最大 2.1 A**
	24 Vdc	**電流：最大 1 A**
スイッチ入力 VIH	• **最小：3 V** • **最大：5 V**	
スイッチ入力 VIL	**最大：1 V**	
スイッチプルアップ抵抗	**4.7 kΩ（入力ポートは 4.7 KΩ でプルアップされる）**	
Wiegand出力VOH	**4.8 V 以上**	
Wiegand出力VOL	**0.2 V 未満**	

Wiegand出力プルアップ抵抗	**1 kΩ の内部プルアップ**
リレー	• **2 A @ 30 VDC 抵抗負荷** • **1 A @ 30 VDC 誘導負荷**

サイズと重量

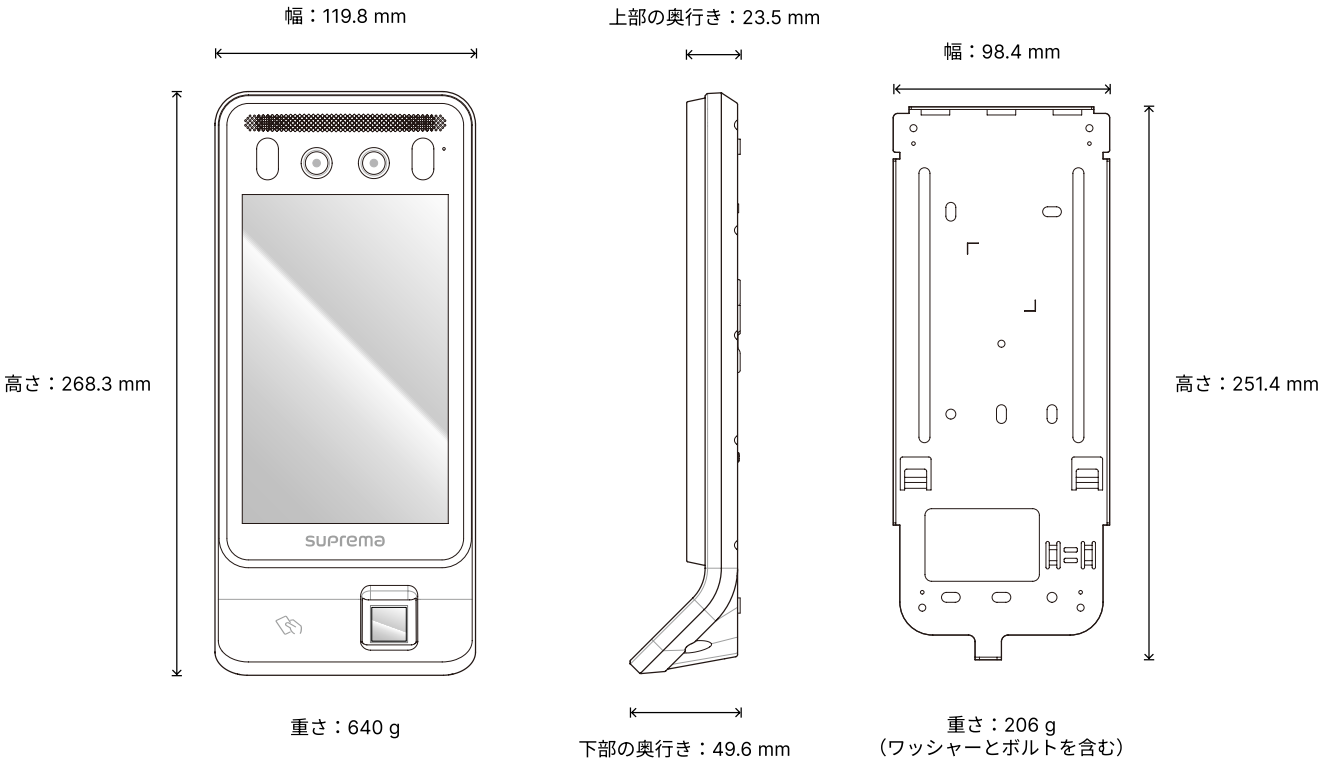
BS3M-DB, BS3M-APB



重さ：565 g

重さ：187 g
（ワッシャーとボルトを含む）

BS3M-ODB, BS3M-OAPB



---

1) 表示されている最小顔認証距離は製品のデフォルト設定であり、推奨顔認証距離は 0.5〜1.3 m です。

2) RF 認識距離は設置環境によって異なる場合があります。

3) 最大 32 文字の ASCII コード文字列で構成された QR/バーコードをサポートします。

4) より多様な QR/バーコード認証を使用するには、Camera QR ライセンスが必要です。デバイスライセンスの詳細については、BioStar X 管理者マニュアルをご参照ください。

5) 記載された QR/バーコードの認識距離は推奨距離であり、実際の認識可能距離は QR/バーコードのサイズおよび設置環境によって異なる場合があります。

6) クレデンシャルなしで登録されたユーザーを基準としています。

7) PoE+（IEEE 802.3at、30 W）または PoE++（IEEE 802.3bt、60〜100 W）の電源が必要です。標準 PoE (IEEE 802.3af、15.4 W) には対応していません。標準 PoE を使用すると、デバイスが不安定に動作したり、永久的に損傷したりする可能性があります。デバイスを接続する前に、ネットワークスイッチまたは PoE インジェクターが PoE+ または PoE++ に対応していることを必ず確認してください。

情報

製品仕様は性能向上のため予告なく変更されることがあります。

規制認証情報

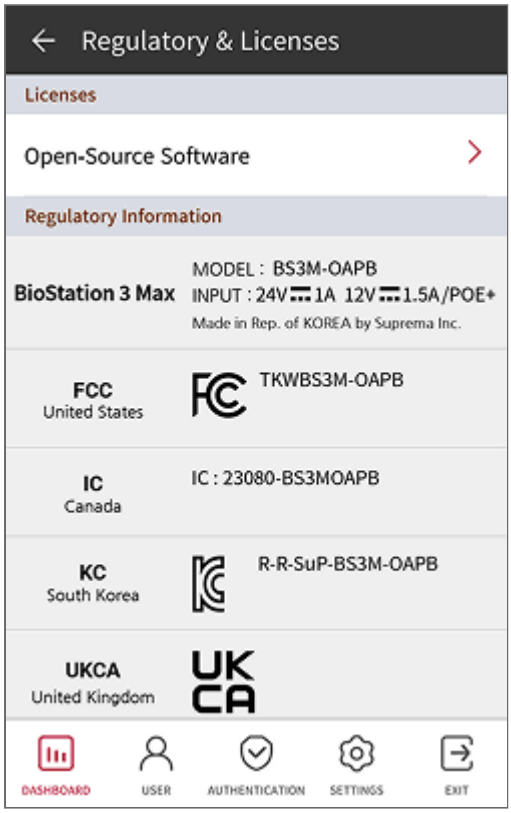
製品が準拠する規制および認証に関する情報を提供します。

規制認証およびライセンス

製品上でライセンス、規制認証、適合マークを確認できます。

- CE CE モデルのみ / FCC / IC / KC / UKCA / RCM

1. を選択し、管理者権限の認証手段で認証します。
2. **DASHBOARD** 右上の をタップすると **Regulatory & Licenses** を確認できます。



FCC 準拠情報

本機器は FCC 規制 Part 15 に準拠しています。

動作は次の 2 つの条件に従います。

1. 本機器は有害な干渉を発生させません。
2. 本機器は、望ましくない動作を引き起こす可能性のある干渉を含む、あらゆる干渉を受け入れなければなりません。

> **情報**
> 本機器は、FCC 規則 Part 15 に基づく Class A デジタル機器の制限に適合することがテストにより確認されています。これらの制限は、機器が商業環境で動作する際に有害な干渉から合理的な保護を提供するために設計されています。本機器は無線周波エネルギーを生成、使用、放射するため、指示に従って設置および使用しないと無線通信に有害な干渉を引き起こす可能性があります。本機器を住宅地域で使用すると有害な干渉が発生する可能性があり、その場合、干渉を解消する費用は使用者が負担しなければなりません。
>
> 適合性責任者が明示的に承認していない製品の変更または改造は、本製品を操作するユーザーの権限を無効にする場合があります。
>
> 本送信機は、他のアンテナまたは送信機と一緒に配置または運用してはいけません。
>
> 本機器は、制御されていない環境に対して規定された FCC の放射曝露制限に準拠しています。ユーザー（または付近の他の人）と本製品のアンテナとの間に少なくとも 20 cm の距離を保ってください。本機器およびそのアンテナを、他のアンテナまたは RF 送信装置と一緒に設置または運用しないでください。

IC 情報

本機は Industry Canada の免許不要 RSS に適合しています。

動作は、次の 2 つの条件に従います。

1. 本機は干渉を発生させてはなりません。また、
2. このデバイスは、望ましくない動作を引き起こす可能性のある電波干渉を含め、受信したあらゆる電波干渉を許容する必要があります。

Le présent appareil est conforme aux CNR d’Industrie Canada applicables aux appareils radio exempts de licence.

L’exploitation est autorisée aux deux conditions suivantes :

1. l’appareil ne doit pas produire de brouillage ;
2. l’appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d’en compromettre le fonctionnement.

欧州連合適合宣言（CE） CE モデルのみ

本製品は無線・通信端末機器指令 (RED) 2014/53/EU の規定に従って CE マークを取得しています。

Suprema Inc. は、本書で説明する装置が欧州連合無線・通信端末機器指令 (RED) 2014/53/EU に準拠した CE マークを有することを宣言します。本装置は指令に従いクラス1の無線機器です。

- Bluetooth 送信電力：-0.1 dBm
- Bluetooth 周波数：2402~2480 MHz
- NFC 周波数：13.56 MHz
- RFID 周波数：13.56 MHz + 125 kHz

詳細については、以下の連絡先までお問い合わせください。

Suprema Inc.

住所： 17F-5, Parkview Office Tower, 248, Jeongjail-ro, Seongnam-si, Gyeonggi-do, 13554, Republic of Korea

電話：+82-31-783-4502/Fax：+82-31-783-4503

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、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

- 本製品のソフトウェアは Linux カーネルを改変して作成されており、ライセンスは GPL に従います。 GPL ライセンスの詳細については GNU General Public License をご覧ください。
- 本製品に含まれる glibc ライブラリは LGPL に従います。 LGPL ライセンスの詳細については GNU Lesser General Public License をご覧ください。
- 本製品に含まれる WebRTC ライブラリは BSD-3-Clause に従います。 BSD-3-Clause ライセンスの詳細は The 3-Clause BSD License でご確認いただけます。
- 本製品に含まれる OpenSSL は OpenSSL ライセンスおよび Original SSLeay ライセンスに従います。 OpenSSL ライセンスおよび Original SSLeay ライセンスの詳細は OpenSSL License と Original SSLeay License でご確認いただけます。
- 本製品に含まれる Open CV 4.8 は Apache ライセンスに従います。 Apache ライセンス 2.0 の詳細は Apache License でご確認いただけます。
- 本製品に含まれる NotoSans フォントは SIL OPEN FONT LICENSE に従います。 SIL オープンフォントライセンスの詳細は SIL Open Font License でご確認いただけます。
- 本製品に含まれる Linux カーネルを基に改変されたソース、glibc ライブラリ、WebRTC ライブラリは、Suprema 技術サポートチームにお問い合わせいただければダウンロードできます。

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。