FaceStation 2

ユーザーガイド

バージョン 1.29

日本語
JA 102.00.FS2

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 10

正しい顔の登録と認証方法 12

インストール 14

ブラケットと製品の固定 14

電源接続 21

ネットワーク接続 22

入力接続 23

リレー接続 24

スタンドアロン接続 26

Secure I/O 2 の接続 27

Wiegand接続 29

使用 30

管理者メニュー 30

ユーザー 30

認証 34

設定 38

イベントログ 47

トラブルシューティング 50

故障報告前の確認事項 50

製品仕様 52

クレデンシャル 52

一般 52

ストレージ 53

インターフェース 53

電気仕様 54

サイズと重量 55

規制認証情報 56

FCC 準拠情報 56

IC 情報 56

欧州連合適合宣言（CE） 57

付録 58

免責事項 58

著作権に関するお知らせ 59

オープンソースライセンス 59

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。

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 °C ~ 50 °C 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。

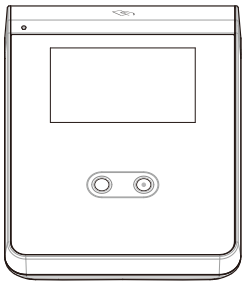
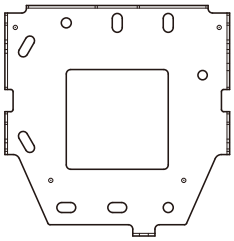
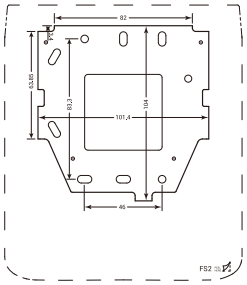
- 故障の原因になります。

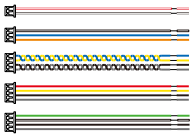
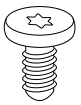
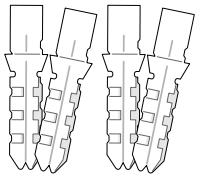
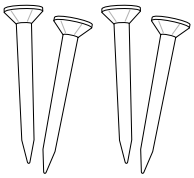
> **RTC バッテリー**
>
> 承認されていない、または不適切な種類のバッテリーに交換すると爆発の危険があります。 バッテリーは居住地域または国際的な廃棄規定に従って廃棄してください。

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

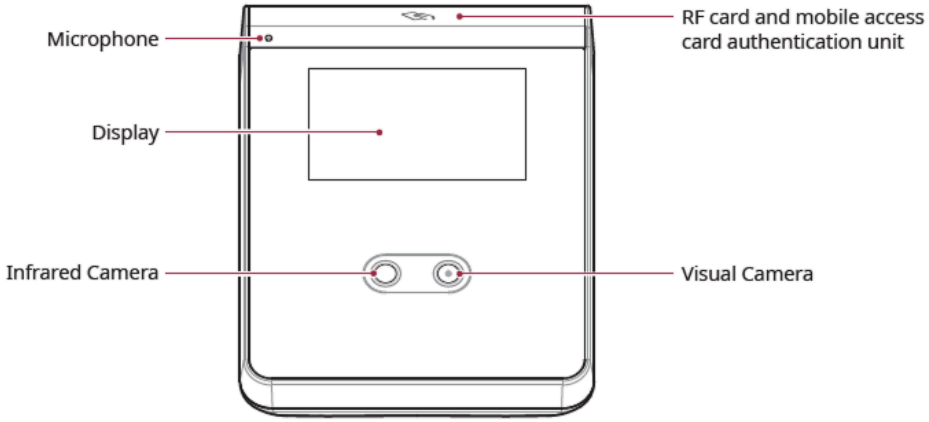
		
FaceStation 2	壁掛けブラケット	ドリルテンプレート

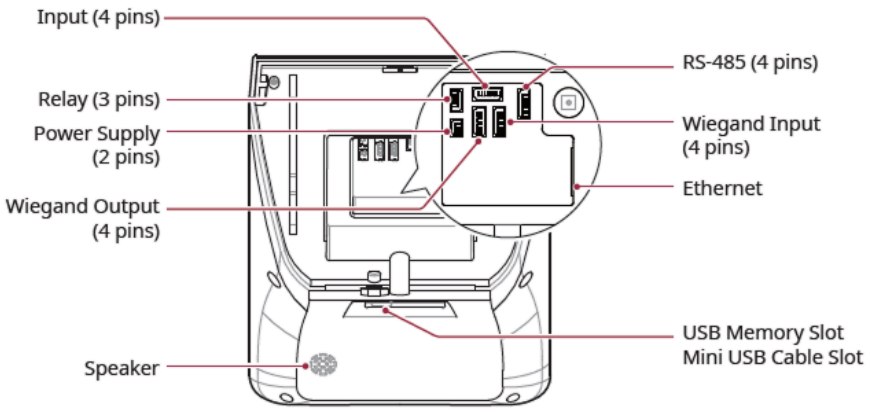
			
接続ケーブル	ダイオード	120 Ω 抵抗	ブラケット固定用ネジ（星形）
			
PVCアンカー ×4	固定用ネジ ×4	クイックガイド	オープンソースライセンスガイド

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





- **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。
- **ディスプレイ**：操作用の UI を提供します。
- **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。
- **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。
- **スピーカー**：音を出力します。
- **USB メモリスロット**：USB メモリを接続します。
  - Supremaサーマルカメラ（TCM10-FS2）と USB メモリは同時に使用できません。
- **Mini USBケーブルスロット**：今後対応予定です。
- **Input（4ピン）**：Input 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。
- **リレー（3ピン）**：リレー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。
- **イーサネット**：イーサネット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。
- **Wiegand 出力（4ピン）**：Wiegand 出力ケーブルを接続します。

ケーブルとコネクタ

電源



ピン	名称	色
1	PWR +VDC	赤(白線)
2	PWR GND	黒(白線)

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	INPUT GND	黒
4	SH GND	灰

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

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40～80 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40~80 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。

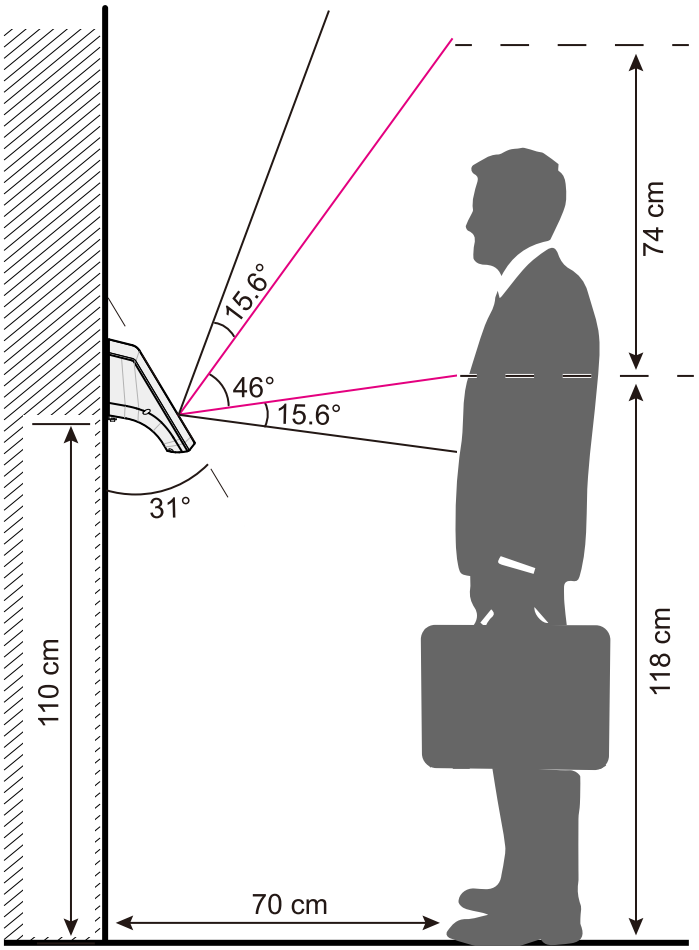
インストール

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

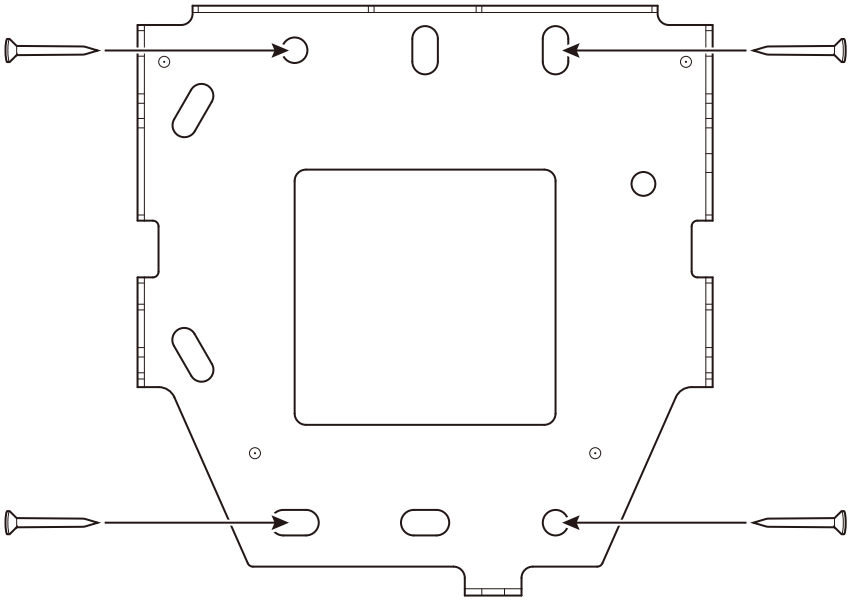
一般ブラケット

1. 付属のドリル用テンプレートを使用して、製品を設置する位置を決めます。



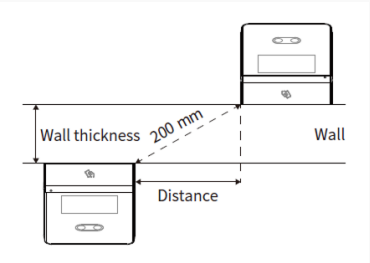
> **情報**
>
> - 装置を設置する最適な高さは 110 cm です。
> - 装置を直射日光や紫外線が直接当たる場所に設置しないでください。
> - 利用者が顔認証を行う際に顔に直射日光が当たらないよう、設置位置を調整してください。

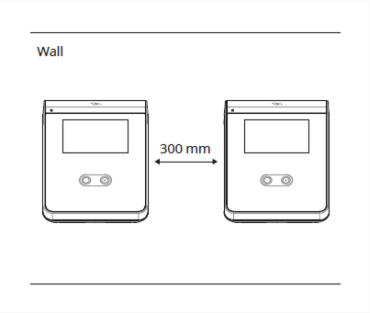
2. 製品を取り付ける位置にブラケットを固定ネジでしっかり固定してください。



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。

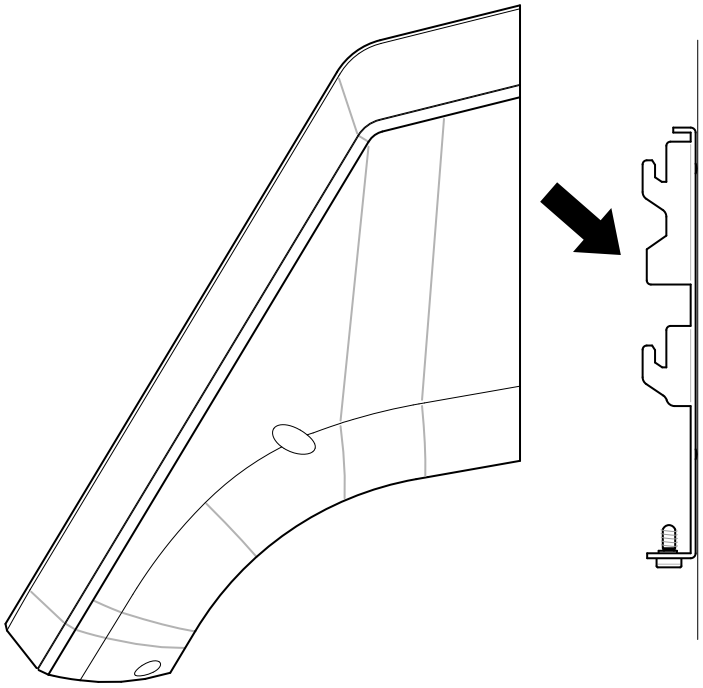




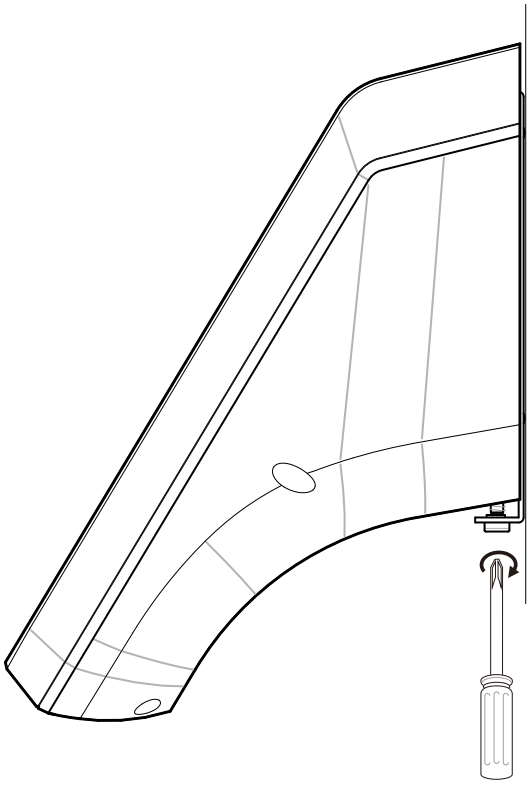
壁の厚さ	距離
100 mm	283 mm
120 mm	275 mm
150 mm	260 mm

- 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. 固定したブラケット上に製品を取り付けます。



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。



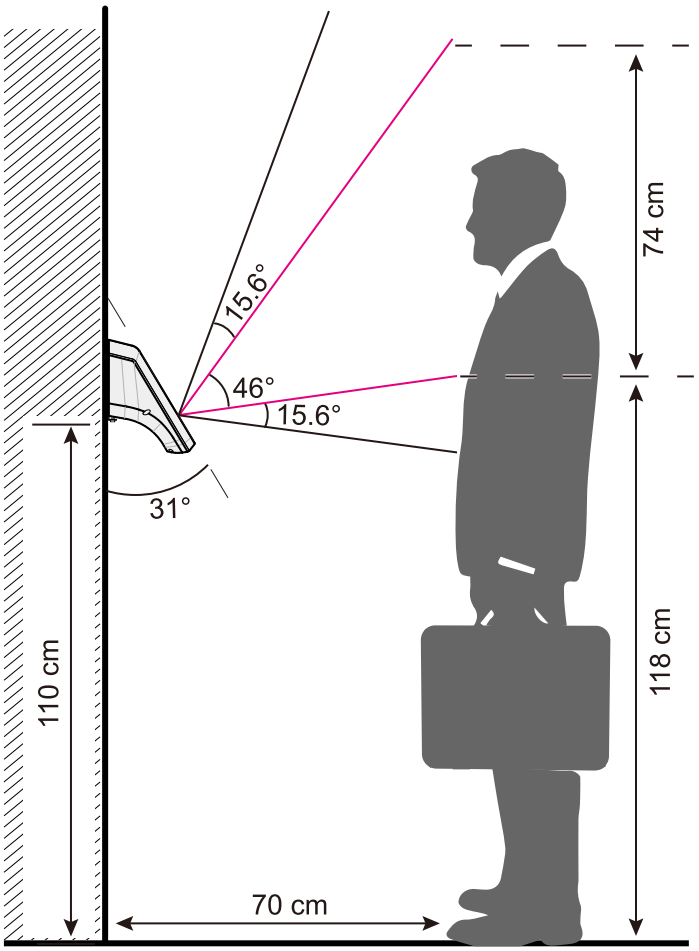
情報

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。

チルトブラケット

専用チルトブラケットを使用すると、設置環境に合わせて認証角度を調整できます。 チルトブラケットは別売です。

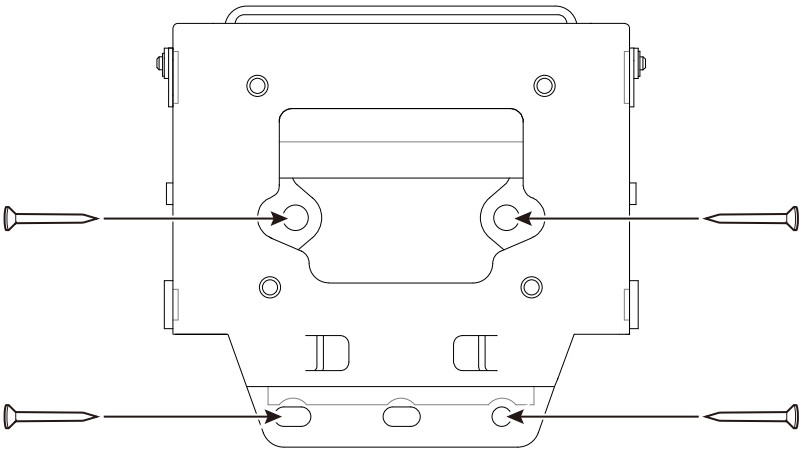
1. 付属のドリル用テンプレートを使用して、製品を設置する位置を決めます。



情報

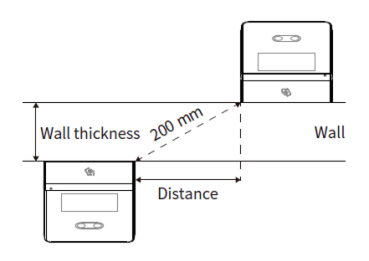
- 装置を設置する最適な高さは 110 cm です。
- 装置を直射日光や紫外線が直接当たる場所に設置しないでください。
- 利用者が顔認証を行う際に顔に直射日光が当たらないよう、設置位置を調整してください。

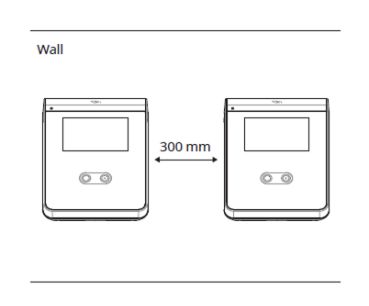
2. 取り付ける位置（壁面）に、チルトブラケットを固定用ネジでしっかりと固定します。



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。

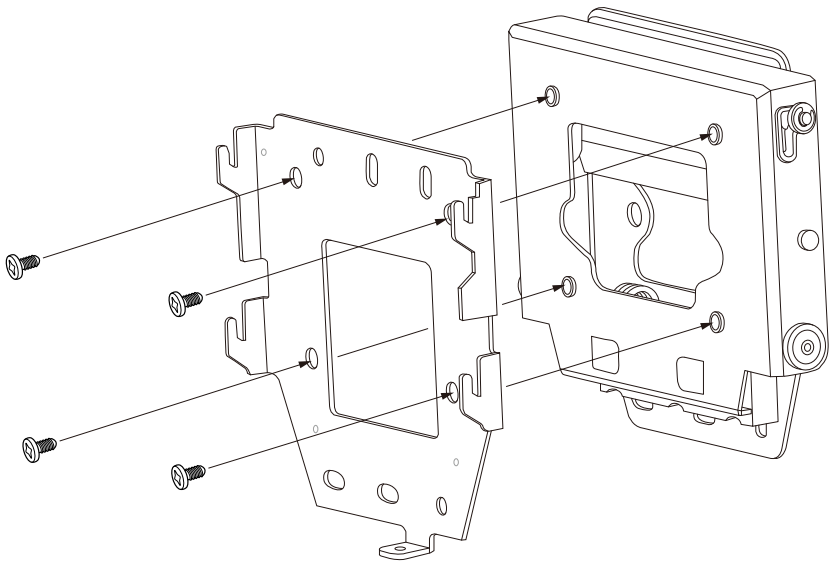




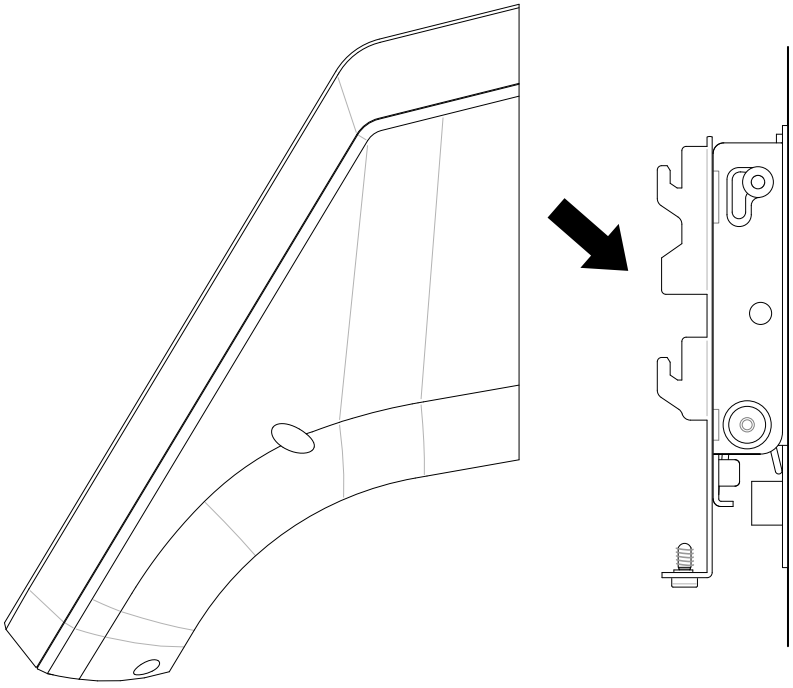
壁の厚さ	距離
100 mm	283 mm
120 mm	275 mm
150 mm	260 mm

- 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。

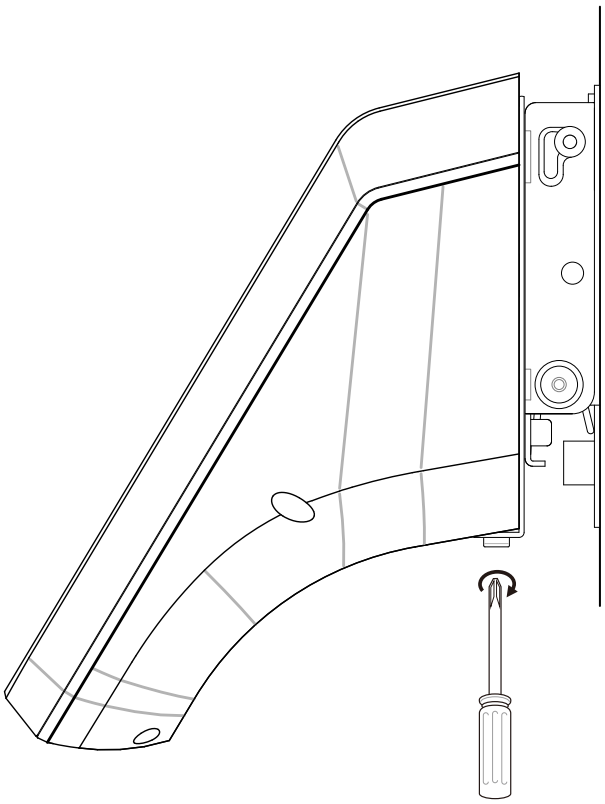
3. チルトブラケットの上に壁掛け用ブラケットをしっかり固定します。



4. 固定した壁掛け用ブラケットの上に製品を取り付けます。



5. 製品固定用ネジを回して、製品と壁掛け用ブラケットを組み立てます。

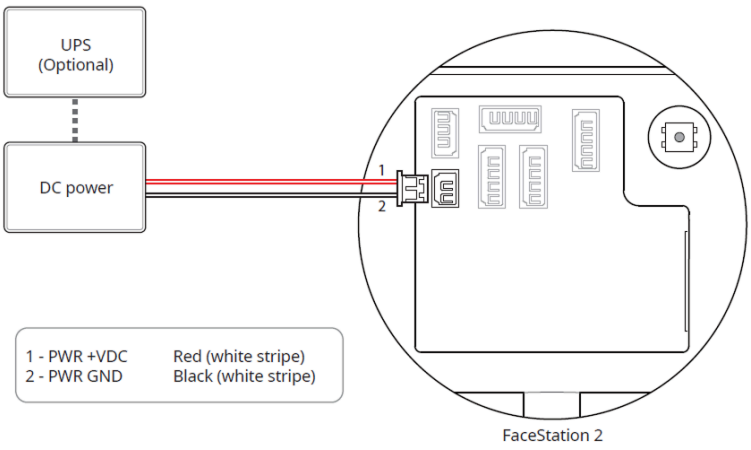


情報

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。

6. チルトブラケットを希望の角度に調整します。

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。

ケーブル規格	最大延長長
16 AWG	150 m
18 AWG	136 m
20 AWG	90 m

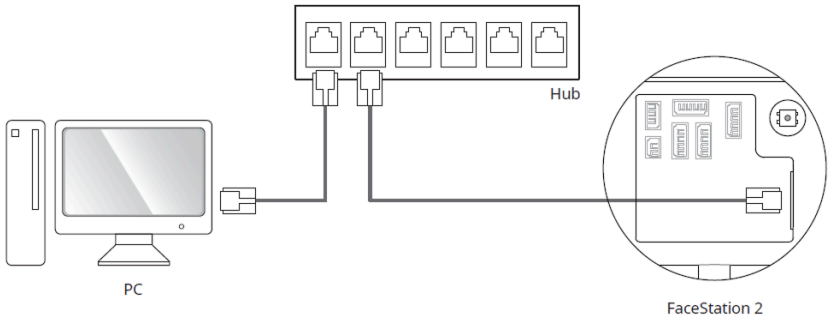
- 電源アダプターを使用する場合、電源ケーブルの長さを任意に延長しないでください。
- CAT5 UTP 2線ケーブルを電源供給用途に使用しないでください。

ネットワーク接続

TCP/IP

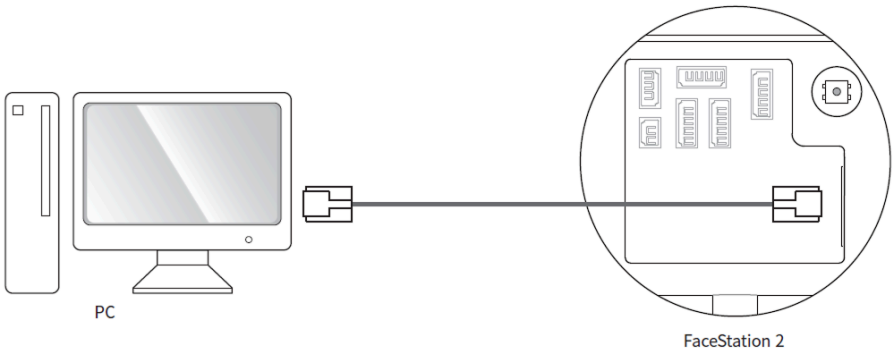
LAN接続（ハブとの接続）

標準タイプのCAT-5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機能を備えているため、クロスケーブルまたは標準ストレートタイプのCAT-5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。

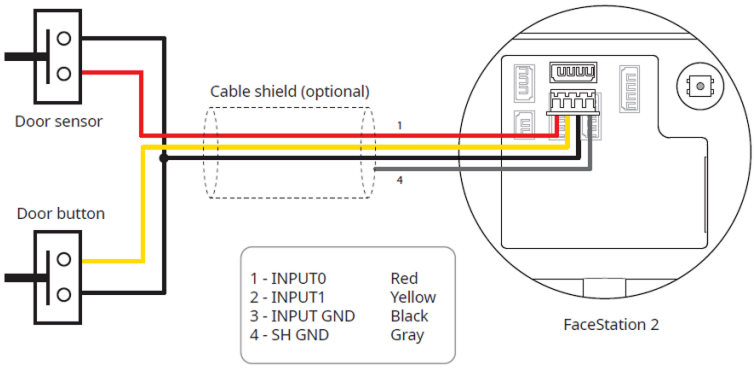
ネットワークポートおよびサービス

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。

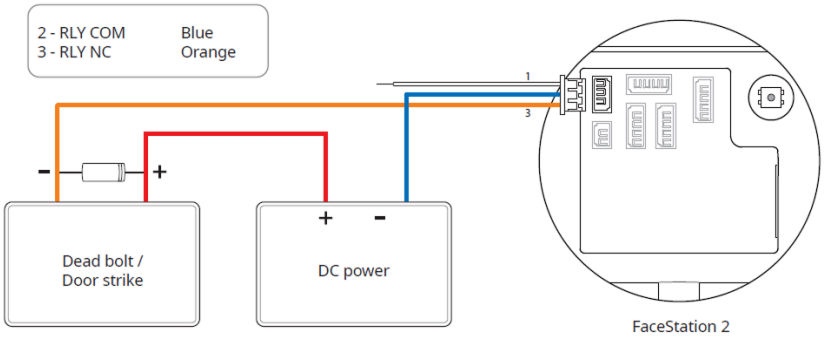
入力接続



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

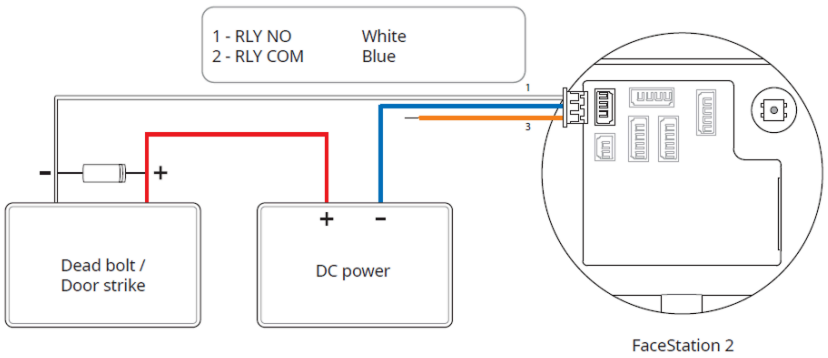
- 扉のロック装置が動作する際に発生する逆電流からリレーを保護するため、図のように扉ロック装置の配線の両側にダイオードを取り付けてください。
- 製品と扉ロック装置には別々の電源を使用してください。
- Suprema のインテリジェントデバイスには、利便性向上のためにコントローラーを介さずスタンドアロンで接続し、扉を直接開閉できるリレーが内蔵されています。 しかし、より高いセキュリティが求められる入退室管理アプリケーションでは、扉のロック解除を引き起こす可能性のある改ざん攻撃を防ぐため、デバイス内蔵のリレーを使用しないことを推奨します。 このようなアプリケーションでは、ロック制御用に扉内部の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



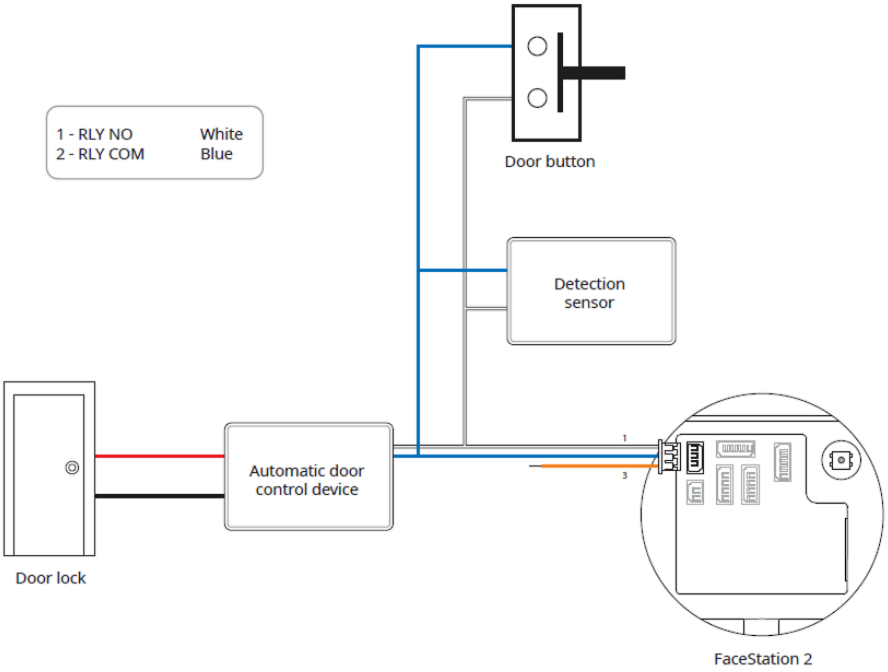
注意

- 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

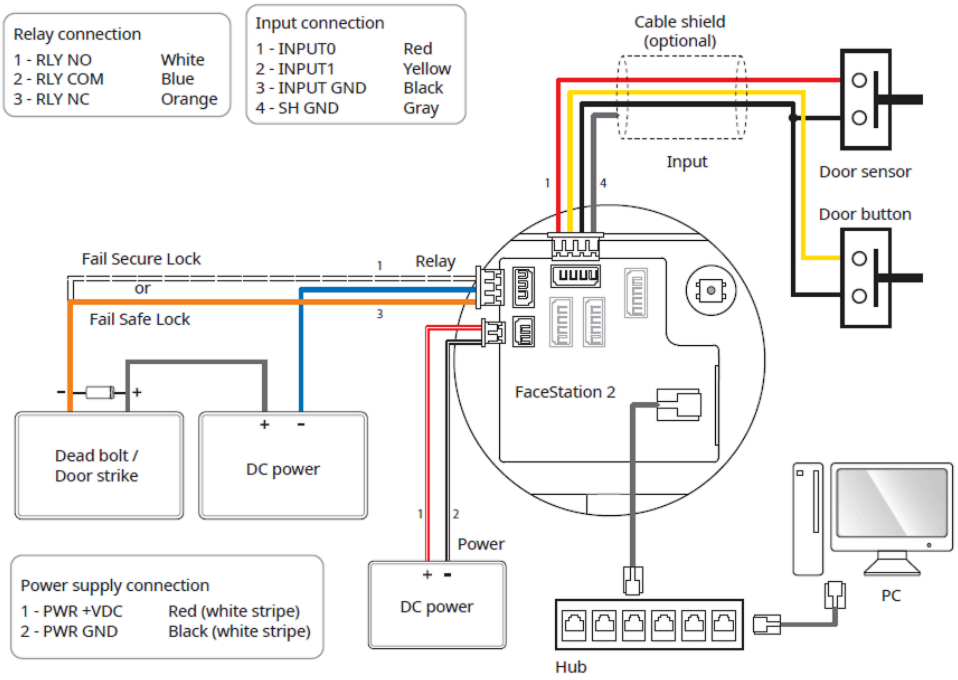
ダイオードの取り付け方向に注意してください。 ダイオードは扉ロック装置の近くに取り付けてください。

自動ドア接続



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。

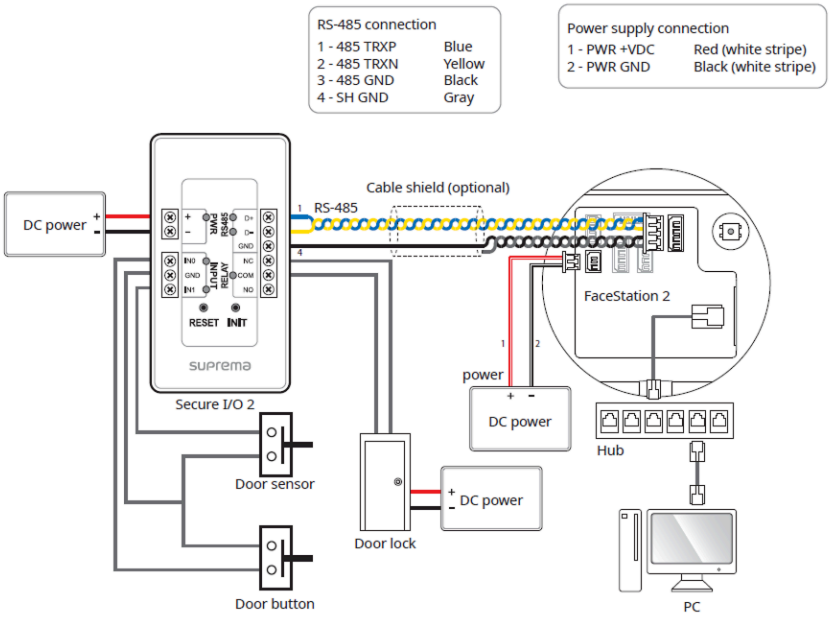
情報

- 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。
- 指紋認識装置がFaceStation 2のスレーブ装置として構成されている場合、別のFaceStation 2をスレーブ装置として追加することはできません。
- 指紋認識装置がマスター装置の場合、FaceStation 2をスレーブ装置として追加することはできません。
- FaceStation 2がマスター装置であり、FaceStation 2をスレーブ装置として接続する場合、スレーブ装置として追加できるFaceStation 2は1台のみです。
- FaceStation 2がマスター装置であり、FaceStation 2をスレーブ装置として接続する場合、Secure I/O 2とDM-20をそれぞれ1台ずつ追加接続できます。
- FaceStation 2がマスター装置であり、FaceStation 2をスレーブ装置として接続する場合、OM-120を追加接続することはできません。
- 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。

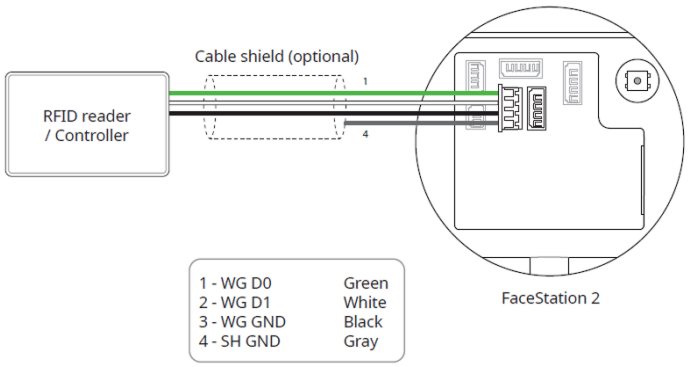


情報

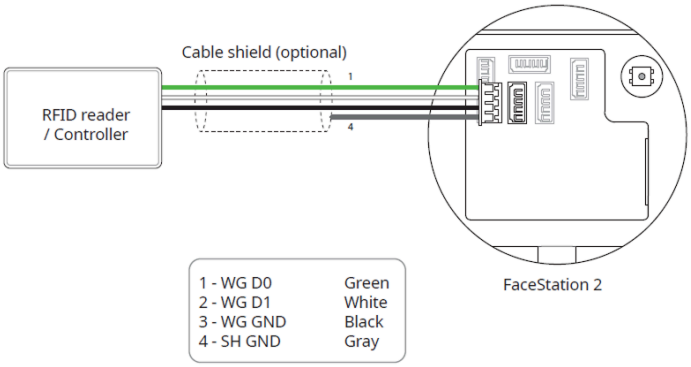
- RS-485 ケーブルでスレーブ装置を接続し、本製品をマルチドアコントローラーとして使用できます。 スレーブ装置はダミーリーダーとして使用され、認証はマスター装置で行います。
- 指紋認識装置がFaceStation 2のスレーブ装置として構成されている場合、別のFaceStation 2をスレーブ装置として追加することはできません。
- 指紋認識装置がマスター装置の場合、FaceStation 2をスレーブ装置として追加することはできません。
- FaceStation 2がマスター装置であり、FaceStation 2をスレーブ装置として接続する場合、スレーブ装置として追加できるFaceStation 2は1台のみです。
- FaceStation 2がマスター装置であり、FaceStation 2をスレーブ装置として接続する場合、Secure I/O 2とDM-20をそれぞれ1台ずつ追加接続できます。
- FaceStation 2がマスター装置であり、FaceStation 2をスレーブ装置として接続する場合、OM-120を追加接続することはできません。
- 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

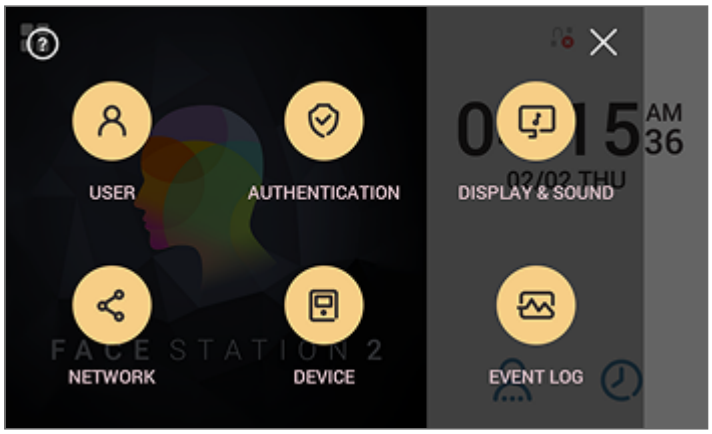
デバイスの主要機能を効果的に使用する方法を案内します。

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。

すべてのメニュー

1. を押して、管理者権限の認証手段で認証してください。
2. 目的のメニューを選択してください。



> **情報**
>
> 管理者が指定されていない場合、 を押すとメニュー画面が表示されます。

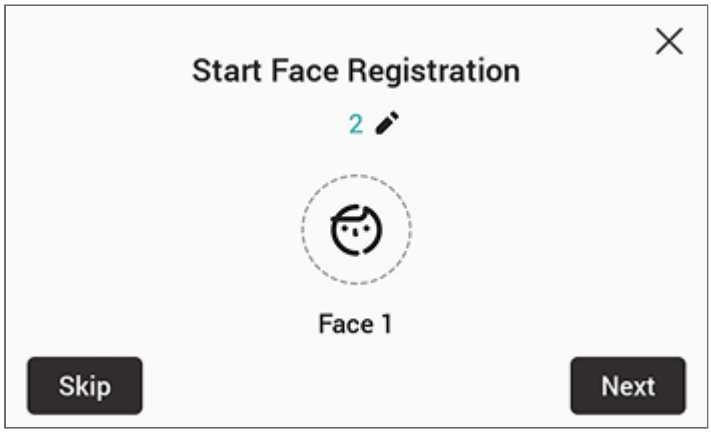
ユーザー

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。

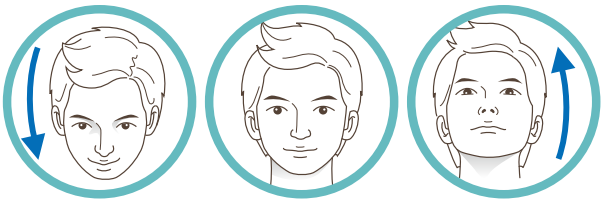
1. を押して、管理者権限の認証手段で認証してください。
2. **USER** → をクリックします。 顔登録ウィザードが開始されます。



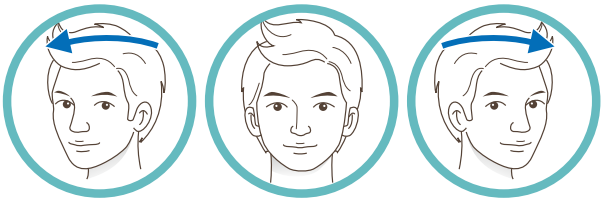
3. **Next** をクリックして顔登録ウィザードを続行します。 **Skip** をクリックしてスキップし、手順 **5** を確認します。
4. **Next** をクリックしたら、画面の指示に従って顔を登録します。 顔登録は全3段階で行います。
    1. 正面の顔登録



    2. 顔を上下に動かす



    3. 顔を左右に動かす

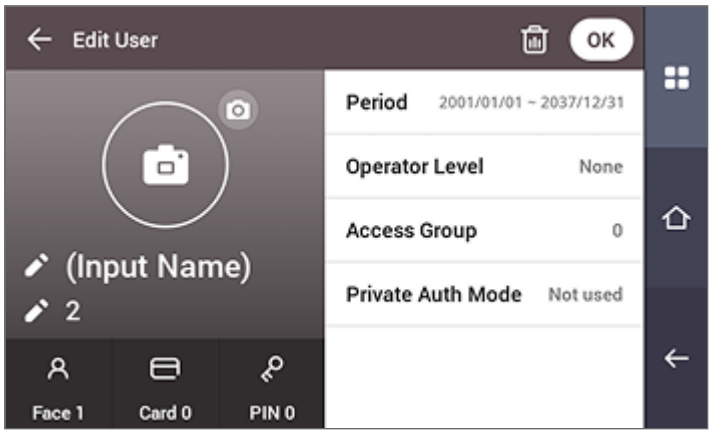


顔登録ウィザードでは、ユーザーの顔のみを登録します。 顔登録が完了したら、そのユーザーを選択して追加情報を設定します。

顔を登録するときは次の点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40～80 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。

5. **Skip** をクリックしたら、必要な項目を選択して設定します。



- : ユーザーの写真を登録します。
- **名前**：ユーザー名を入力できます。
- **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、英数字と記号 _ - の組み合わせをIDとして使用でき、最大32文字まで入力できます。
- **Face**：ユーザー認証用の顔を登録します。 をクリックして、画面の指示に従い顔を登録します。 をクリックして顔を追加登録します。
- **Card**：ユーザー認証用のカードを登録できます。 をクリックしてから、ユーザーに割り当てるカードをRFカードリーダーにスキャンします。 をクリックしてカードを追加登録します。
- **PIN**：使用する PIN を入力できます。 使用する PIN を入力した後、確認のためもう一度 PIN を入力し、**OK** をクリックします。 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。
- **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。

- **Face Group**：ユーザーの顔グループを選択します。 顔グループは **Group Matching** がオンの場合にのみ利用でき、BioStar X でのみ登録します。
- **Access Group**：ユーザーの入退室グループを確認します。 入退室グループはBioStar Xでのみ登録します。
- **Private Auth Mode**：個人認証モードを設定します。 個人認証モードでは、ユーザーごとに顔を含む認証方式を組み合わせます。 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。

6. **OK** をクリックしてユーザー情報登録を完了します。

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。 ユーザーの顔やカードを追加したり、PINおよび権限を修正したりできます。

1. を押して、管理者権限の認証手段で認証してください。
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**、**Card** でユーザーを検索します。
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**
> **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。

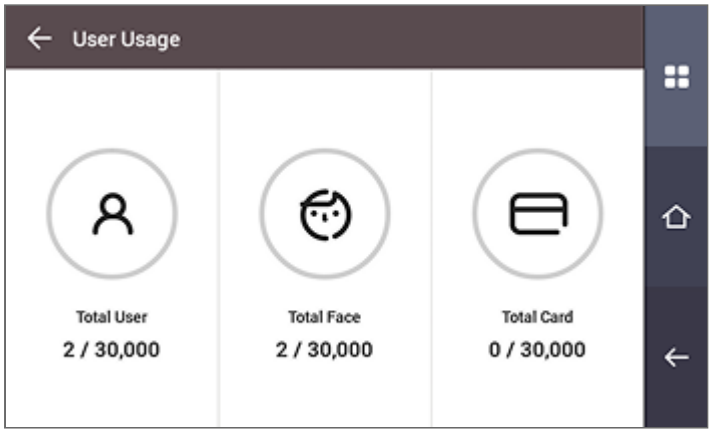
1. を押して、管理者権限の認証手段で認証してください。
2. **USER** → を選択します。
3. **Delete All** を選択してチェックし、**OK** をクリックします。

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数、顔数、カード数を一目で確認できます。

1. を押して、管理者権限の認証手段で認証してください。
2. **USER** → をクリックします。 ユーザー登録状況を確認できます。



認証

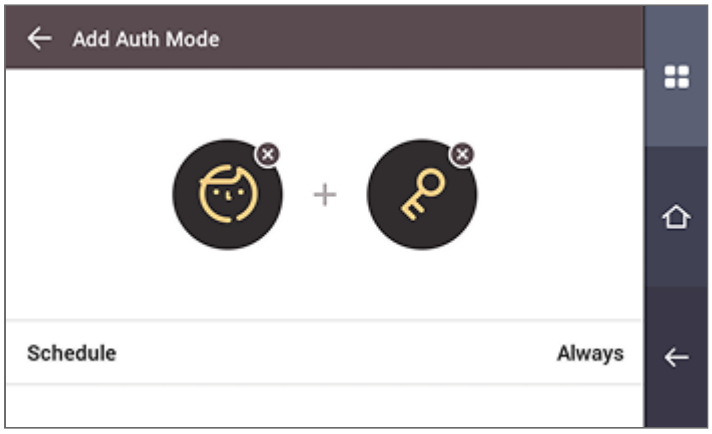
サポートする認証方式と認証手順について説明します。

認証モード

デバイスの認証モードを設定できます。 **Face**、**PIN**、**Card**、**ID** を組み合わせて認証モードとして利用でき、各認証モードごとに使用するスケジュールを設定することも可能です。

認証モードの登録

1. を押して、管理者権限の認証手段で認証してください。
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。



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

区分	説明
顔	- : 顔だけを使用するモードです。 - + : 顔で認証した後に PIN を入力するモードです。
カード	- : カードのみを使用するモードです。 - + : カードで認証した後に顔で認証するモードです。 - + : カードで認証した後に PIN を入力するモードです。 - + / : カードで認証した後に顔で認証するか、PIN を入力するモードです。 - + + : カードで認証した後に顔認証と PIN 入力を両方使用するモードです。
ID	- + : ID を入力した後に顔で認証するモードです。 - + : ID を入力した後に PIN を入力するモードです。 - + / : ID を入力した後に顔で認証するか、PIN を入力するモードです。 - : 顔だけを使用するモードです。 - + : 顔で認証した後に PIN を入力するモードです。

> **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。

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. を押して、管理者権限の認証手段で認証してください。
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。

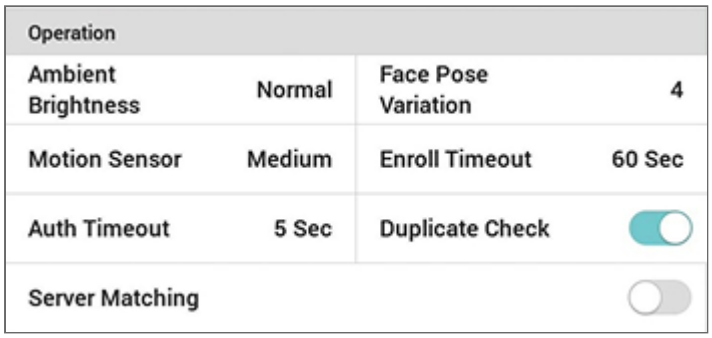
4. 認証モードの登録を参照して認証モードを修正した後、**OK** を押します。

認証モードの削除

1. を押して、管理者権限の認証手段で認証してください。
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

1. を押して、管理者権限の認証手段で認証してください。
2. **AUTHENTICATION** を押してから **Operation** で目的の項目を変更します。



- **Ambient Brightness**：周囲の明るさを検出して IR LED の強度を調整します。 設置環境に応じて設定を変更します。
- **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。
- **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。
- **Server Matching**：サーバーマッチングを設定すると、デバイスではユーザー認証を行わず、BioStar X でユーザー認証を実行します。 サーバーマッチングは、デバイスにユーザー情報が多すぎる場合や、ユーザー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

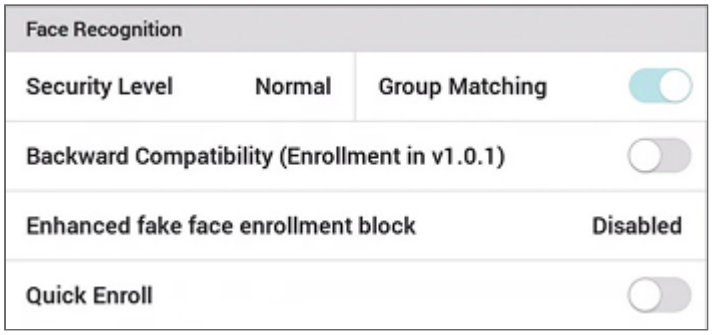
  - **Server Matching** ではカードと ID のみ使用できます。
  - **Server Matching** を使用する場合は、デバイスと BioStar X の両方でサーバーマッチングを有効にする必要があります。 BioStar Xサーバーマッチング設定については、BioStar X管理者マニュアルをご参照ください。

- **Face Pose Variation**：顔を登録する際に顔の位置、角度、距離に対する感度を設定します。 高精度の顔テンプレートを取得するには高く設定します。
- **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。
- **Duplicate Check**：顔登録時に重複顔をチェックできます。

顔認証

顔認証に関する設定を変更できます。

1. を押して、管理者権限の認証手段で認証してください。
2. **AUTHENTICATION** を押してから **Face Recognition** で目的の項目を変更します。



- **Security Level**：1:N: 認証のセキュリティレベルを設定できます。
- **Group Matching**：グループマッチングの使用有無を確認できます。 グループマッチングを使用すると、複数ユーザーの顔をグループ化して認証速度を向上できます。
- **Backward Compatibility (Enrollment in v1.0.1)**：顔テンプレートを登録したデバイスのファームウェアが v1.0.1 以前の場合はこのオプションを有効にします。
- **Enhanced fake face enrollment block**：写真などの偽造顔を使用したユーザー登録を防止できます。 **Level 1** から **Level 3** まで強度を設定でき、段階が上がるほど検査強度が強化されます。
- **Quick Enroll**：高速顔登録の使用有無を設定できます。 高速顔登録を有効にすると登録手順は 1 段階になり、無効にすると 3 段階になります。

> **情報**
>
> - **Group Matching** は BioStar X で設定できます。
> - **Enhanced fake face enrollment block** を高い段階に設定すると、実際の顔の登録が拒否される可能性があります。 登録に失敗した場合は再試行するか、検査強度を下げます。
> - 高品質の顔テンプレートを登録するには **Quick Enroll** を無効にします。

勤怠モード

勤怠モードの登録方法を設定できます。

1. を押して、管理者権限の認証手段で認証してください。
2. **AUTHENTICATION** を押してから **T&A Mode** で目的の項目を変更します。



- **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。
- **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。

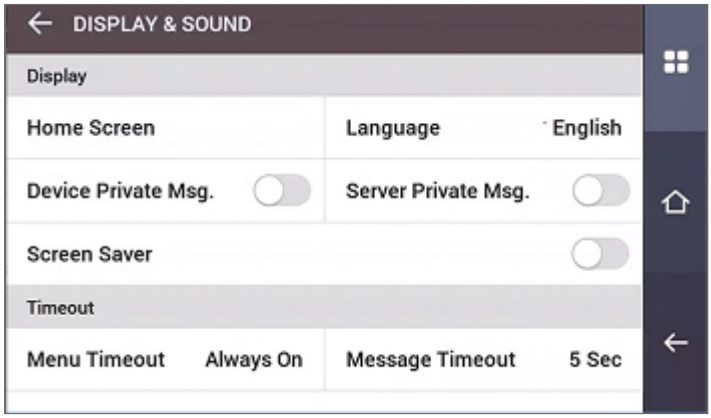
設定

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。

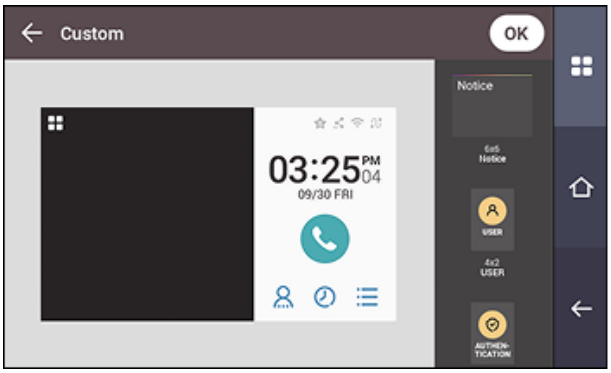
画面とサウンド

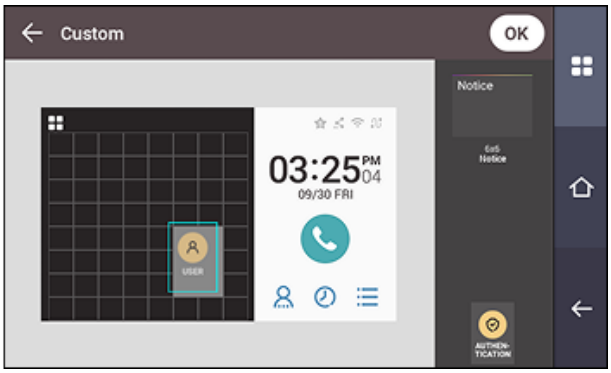
デバイスの画面とサウンドの設定を変更できます。

1. を押して、管理者権限の認証手段で認証してください。
2. **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。 スタイルで「ユーザー定義」を選択すると、ホーム画面をユーザーが直接編集できます。 編集したいオブジェクトを長押ししてドラッグ＆ドロップし、ホーム画面を編集してください。





- **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。
- **Screen Saver**：スクリーンセーバーの使用有無を設定できます。 スクリーンセーバーを使用すると、デバイスを使用していないときに画面の明るさを下げ、不要な電力消費を抑えることができます。
- **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。

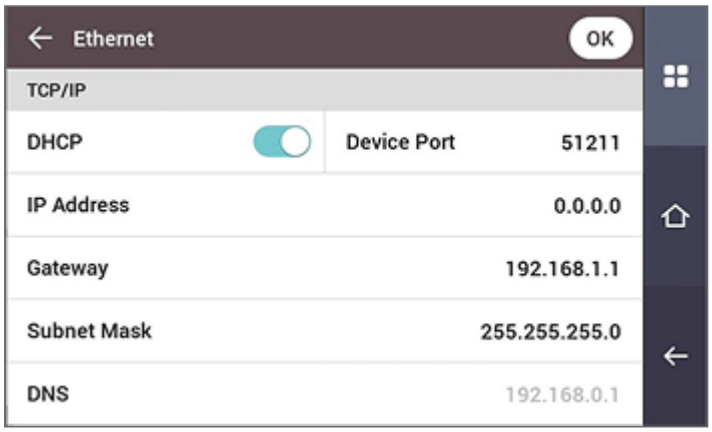
> **情報**
> BioStar Device SDK の詳細については、Suprema ナレッジベースの BioStar Device SDK ページ を参照してください。

通信

Ethernet、サーバー、シリアル通信など、デバイスの通信設定を変更できます。

イーサネット

1. を押して、管理者権限の認証手段で認証してください。
2. **NETWORK** → **Ethernet** を選択してください。
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。

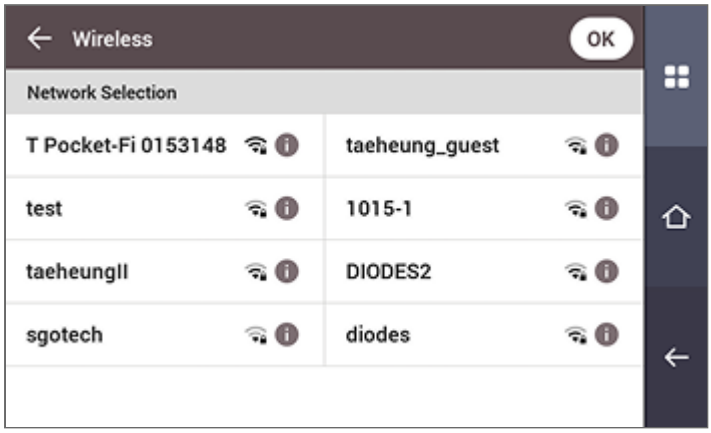
- **IP Address**：デバイスのIPアドレスを確認できます。 DHCP設定をオフにして変更する。
- **Gateway**：デバイスのゲートウェイを確認できます。 DHCP設定をオフにして変更する。
- **Subnet Mask**：デバイスのサブネットマスクを確認できます。 DHCP設定をオフにして変更する。
- **DNS**：ドメインネームサーバーのアドレスを設定できます。

4. 設定を保存するには **OK** を押します。

> **情報**
> **Ethernet** は **Wireless** と同時には使用できません。

無線 LAN

1. を押して、管理者権限の認証手段で認証してください。
2. **NETWORK** → **Wireless** を選択してください。
3. 接続可能なネットワークの一覧が表示されます。



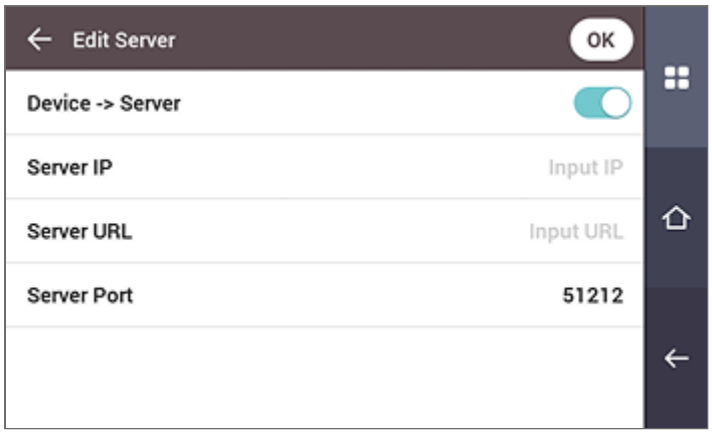
4. 接続したいネットワークを選択し、パスワードを入力します。 **OK**を押すと無線ネットワークに接続されます。
5. 使用する無線ネットワークの をタップして DHCP 設定をオフにすると、**IP Address**、**Gateway**、**Subnet Mask** をユーザーが編集できます。

> **情報**
>
> - **Wireless** は FS2-AWB モデルでのみ使用できます。
> - **Wireless** は **Ethernet** と同時には使用できません。
> - **Wireless**で接続するには無線ルーターが必要です。 無線ルーターの設置および設定については、無線ルーターのユーザーガイドを参照してください。

サーバー

1. を押して、管理者権限の認証手段で認証してください。
2. **NETWORK** → **Server** を選択してください。

3. 必要な項目を設定してください。

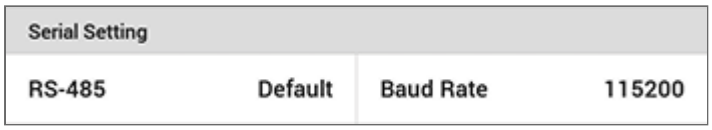


- **Device → Server**：デバイスから入力した情報を持つサーバーに直接接続信号を送信できます。 **Device → Server** 設定をオンにすると、**Server IP**、**Server URL**、**Server Port** をユーザーが入力できます。
- **Server IP**：BioStar XがインストールされたPCのIPを入力します。
- **Server URL**：**Server IP** の代わりに **Server URL** を入力できます。
- **Server Port**：BioStar XがインストールされたPCのポートを入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

4. 設定を保存するには **OK** を押します。

シリアル通信設定

1. を押して、管理者権限の認証手段で認証してください。
2. **NETWORK** を押してから、**Serial Setting** で必要な項目を変更してください。



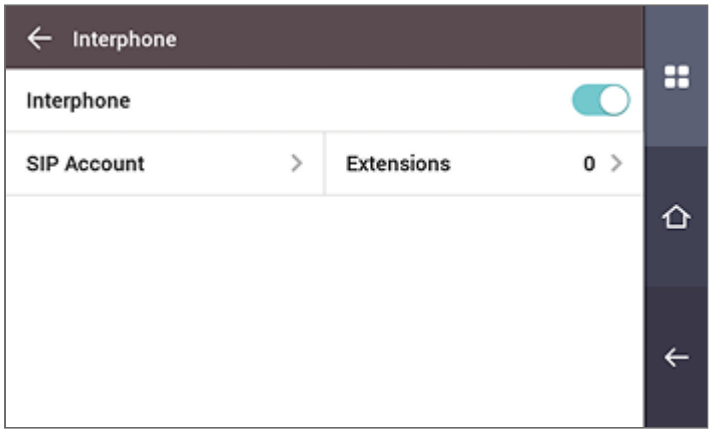
- **RS-485**：RS-485の動作モードを選択できます。
- **Baud Rate**：必要な通信速度を選択できます。

デバイス

インターホン

SIPインターホンのアカウントと内線を設定できます。

1. を押して、管理者権限の認証手段で認証してください。
2. **DEVICE** → **Interphone** を押してください。



- **Interphone**：インターホンの有効／無効を設定できます。 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。
- **Extensions**：内線番号を追加および削除できます。

リレー

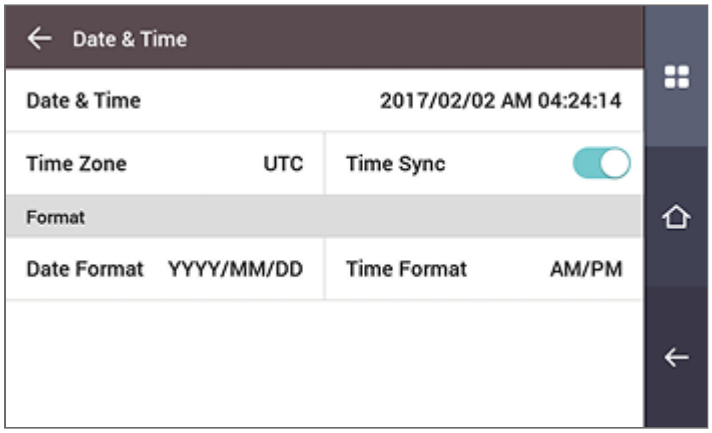
デバイスで **Open Time** と **Exit Button** の入力ポートを設定できます。

1. を押して、管理者権限の認証手段で認証してください。
2. **DEVICE** → **Relay** を押してください。
   - **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** と **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**：退出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. を押して、管理者権限の認証手段で認証してください。
2. **DEVICE** → **Date & Time** を押してください。
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. を押して、管理者権限の認証手段で認証してください。
2. **DEVICE** → **Daylight Saving Time** を選択し、 を押してサマータイムを追加してください。
3. 必要な項目を変更してください。
   - **Name**：サマータイム名を確認できます。
   - **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. を押して、管理者権限の認証手段で認証してください。
2. **DEVICE** → **Device Info** を選択してください。 **Model Name**、**Device ID**、**Serial No.**、**HW**、**FW**、**Kernel**、**MAC**、**WiFi MAC** の情報を確認できます。

> **情報**
> **WiFi MAC** 項目は FS2-AWB モデルでのみ確認できます。

メモリ情報

メモリ使用情報を確認できます。

1. を押して、管理者権限の認証手段で認証してください。
2. **DEVICE** → **Memory Info** を選択してください。 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. を押して、管理者権限の認証手段で認証してください。
2. **DEVICE** → **USB Memory** 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。
   - **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。

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. を押して、管理者権限の認証手段で認証してください。
2. **DEVICE** を選択してください。
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。

デバイスの再起動

デバイスを再起動できます。

1. を押して、管理者権限の認証手段で認証してください。

2. **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。

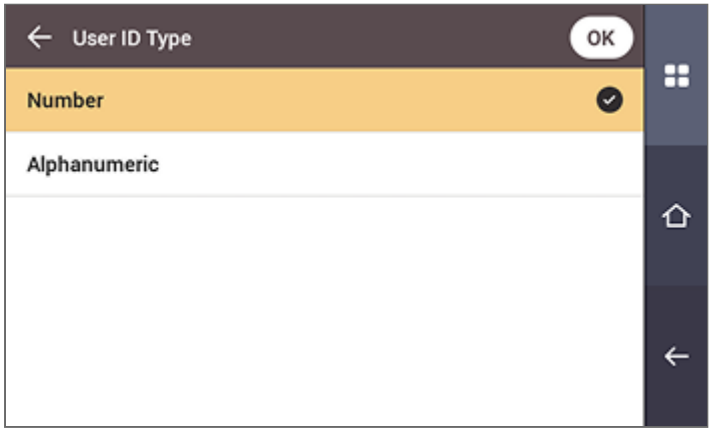
1. を押して、管理者権限の認証手段で認証してください。
2. **DEVICE** → **Restore Default** を選択してください。
   - **All settings**：デバイスに保存されているすべての設定を初期化します。 デバイス設定をすべて初期化するには、**OK** → **OK** を押してください。 前の画面に戻るには **Cancel** を押してください。
   - **Keep Network Settings**：ネットワーク設定を除くすべての設定を初期化します。 ネットワーク設定を除くすべての設定を初期化するには、**OK** → **OK** を押してください。 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. を押して、管理者権限の認証手段で認証してください。
2. **DEVICE** → **User ID Type** を選択してください。



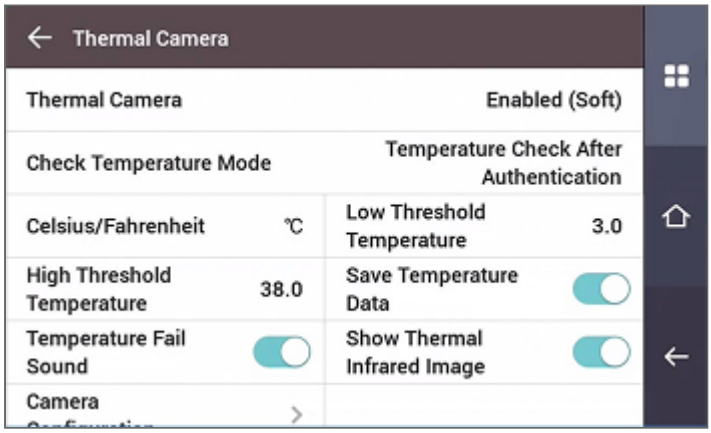
- **Number**：ユーザー ID は数字のみ入力できます。
- **Alphanumeric**：ユーザー ID は英字、数字、一部記号 _ - を組み合わせて入力できます。

3. 必要な項目に変更した後、**OK** を押してください。

熱画像カメラ

デバイスとサーマルカメラを連携させ、出入口を通過するユーザーの温度を測定し、基準温度を超えたユーザーのアクセスを制限できます。

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



- **Thermal Camera**：サーマルカメラの使用可否を設定できます。 **Enabled (Hard)** に設定すると、基準温度を超えたユーザーは認証が拒否され、温度超過イベントがログに記録されます。 **Enabled (Soft)** に設定すると、基準温度を超えたユーザーでも認証できますが、温度超過イベントがログに記録されます。
- **Check Temperature Mode**：用途に応じて温度確認モードを設定できます。
  - **Temperature Check After Authentication**：認証を実施した後、ユーザーの温度を測定します。
  - **Temperature Check Before Authentication**：ユーザーの温度を測定してから認証を実施します。 このモードを使用すると、基準温度を超えるユーザーは認証できません。
  - **Check Temperature Only**：デバイスを温度測定専用として使用できます。 このモードを使用すると、認証に関係なく基準温度以下のユーザーはすべて通行できます。
- **Celsius/Fahrenheit**：温度表示単位を設定できます。
- **Low Threshold Temperature**：入場を制限する最低基準温度を設定できます。 表面温度が最低基準温度より低いユーザーは認証が拒否されます。
  低基準温度は 1 °C～45 °C の範囲で設定でき、高基準温度より高く設定することはできません。
- **High Threshold Temperature**：入室を制限するための最高基準温度を設定します。 表面温度が高基準温度を上回るユーザーは認証を拒否されます。
  高基準温度は 1 °C～45 °C の範囲で設定でき、低基準温度より低く設定することはできません。
- **Save Temperature Data**：ユーザーの温度ログを保存するかどうかを設定します。 このオプションを有効にすると、認証の成否とユーザーの温度値の両方がログに保存され、無効にすると認証の成否のみがログに保存されます。
- **Show Thermal Infrared Image**：デバイス画面にサーマル画像を表示するかどうかを設定します。

- **Camera Configuration**：正確な測定のためにカメラの詳細オプションを設定します。
  - **Distance(cm)**：ユーザーとサーマルカメラの距離を設定します。
  - **Emissivity**：赤外線放射率を設定します。
  - **ROI X(%)**、**ROI Y(%)**、**ROI Width(%)**、**ROI Height(%)**：近くに他の照明が設置されている場合でも、サーマルカメラがその照明ではなくユーザーの温度を自動で測定するように設定できます。 ROI（関心領域）の位置とサイズを調整して、サーマルカメラが温度を測定する領域を手動で設定します。
  - **Skin Temperature Compensation**：使用環境と周囲温度を考慮してサーマルカメラが自動で温度を補正するように設定します。
  - **Skin Temperature Correction**：使用環境に応じて温度を一定値だけ高くまたは低く測定するように補正できます。 例えば、常に温度が 0.1 °C 高く測定される環境では、補正値を -0.1 に設定してください。

情報

- 最適な性能を得るために、カメラ設定のサブオプションはデフォルト値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。
  - **Distance(cm)**：100
  - **Emissivity**：0.98
  - **ROI X(%)**：47
  - **ROI Y(%)**：45
  - **ROI Width(%)**：15
  - **ROI Height(%)**：10
- サーマルカメラは TCM10-FS2 をサポートしています。

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. を押して、管理者権限の認証手段で認証してください。
2. **EVENT LOG** 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。

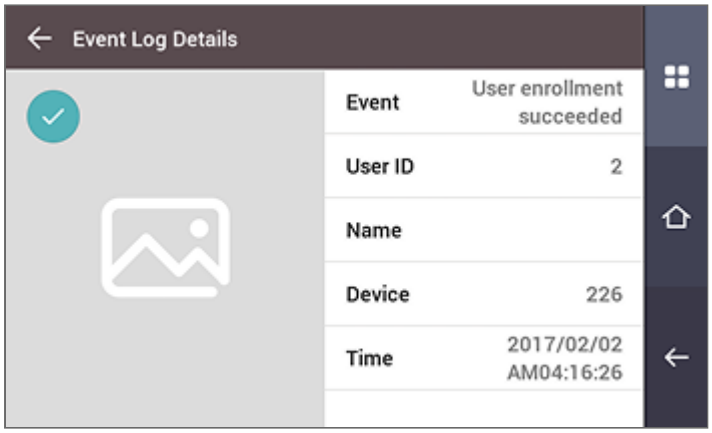


4. 検索条件を設定して **OK** を押すと、条件に一致するログが画面に表示されます。

イベントログの詳細

ログの詳細を確認します。

1. を押して、管理者権限の認証手段で認証してください。
2. **EVENT LOG** 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. 詳細を確認したいログをクリックします。



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。

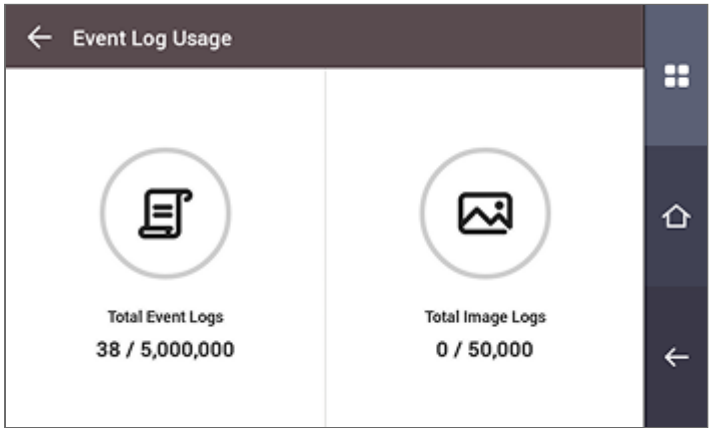
1. を押して、管理者権限の認証手段で認証してください。
2. **EVENT LOG** を選択します。 すべてのイベントログの一覧が表示されます。
3. を選択してから **OK** を押して、すべてのログを削除します。 前の画面に戻るには **Cancel** を押してください。

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. を押して、管理者権限の認証手段で認証してください。

2. **EVENT LOG** → 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。

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. サーマルカメラ使用時に温度が正常に測定されません。

- 端末にサーマルカメラが正常に接続されているか確認してください。
- 額が隠れていない状態で再度温度測定を試してください。問題が続く場合は設置業者にお問い合わせください。

Q. サーマルカメラ使用時に温度が低すぎて測定されます。

- 冬季にユーザーが長時間屋外の低温にさらされた状態で温度を測定すると、体温より低く測定されることがあります。屋内で1〜2分待機してから再度お試しください。問題が続く場合は設置業者にお問い合わせください。

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** • **偽顔検出:対応**	
RFカード	**FS2-D**	**125kHz EM および 13.56MHz MIFARE、MIFARE Plus、DESFire、DESFire EV1/EV2/EV3[1)]、FeliCa**
	FS2-AWB	**125kHz EM、HID Prox および 13.56MHz MIFARE、MIFARE Plus、DESFire、DESFire EV1/EV2/EV3[1)]、FeliCa、iCLASS SE/SR/Seos**
RF認証距離[2)]	**EM/HID Prox/MIFARE/DESFire/HID iCLASS/FeliCa：30 mm**	
モバイル	**FS2-D**	**NFC**
	FS2-AWB	**NFC、BLE**

一般

CPU	**1.4 GHz クアッドコア**
メモリ	**8 GB Flash + 1 GB RAM**
暗号チップ	**対応**
ディスプレイ	**4 インチカラー TFT タッチ**
画面解像度	**800 x 480 画素**
サウンド	**24 ビット/音声 DSP（エコーキャンセル）**
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）**
カメラタイプ	**CMOS**
カメラ解像度	**720 x 480 画素**
カメラ角度	• **視覚レンズ：対角 92.7°** • **IR レンズ：対角 58°**
認証	**CE、UKCA、KC、FCC、IC、RCM、BIS、SIG、RoHS、REACH、WEEE**

ストレージ

最大ユーザー数	**30,000**[3)]
最大クレデンシャル数（1:N）	**顔：4,000**
最大クレデンシャル数（1:1）	• **顔：30,000** • **カード：30,000** • **PIN：30,000**
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）**	
Wi-Fi	**FS2-D**	**非対応**
	FS2-AWB	**サポート対象（内蔵、IEEE 802.11 b/g）**

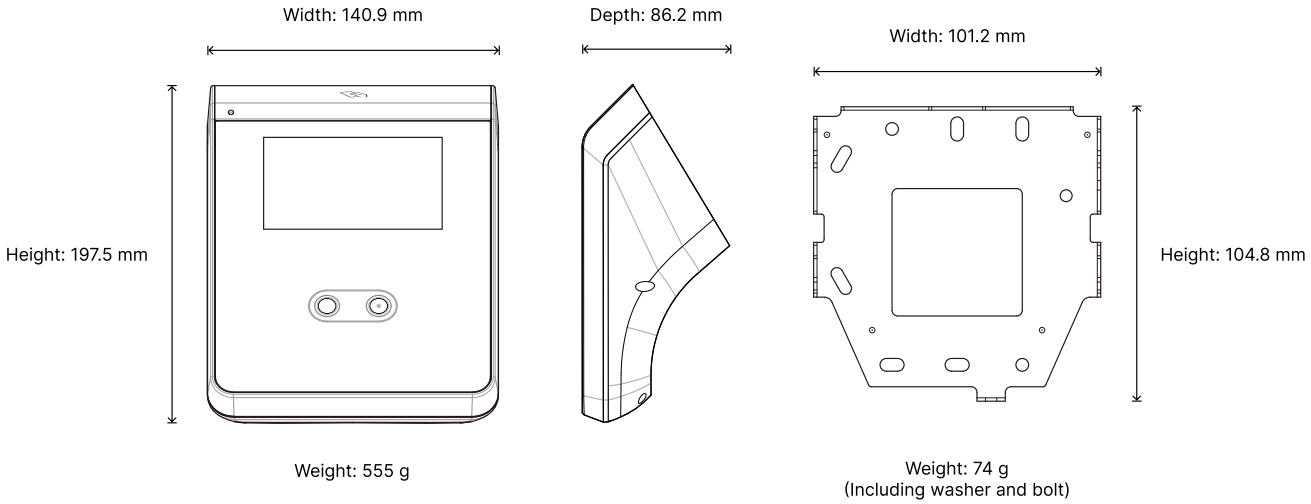
ネットワークプロトコル	**TCP、UDP**
RS-485	**1 チャンネルホスト/スレーブ（選択可能）**
RS-485通信プロトコル	**OSDP V2 準拠**
Wiegand	**1 チャンネル入力、1 チャンネル出力**
入力	**2 チャンネル入力**
リレー	**1 リレー**
インターホン	**対応**
USB	**USB 2.0（ホスト）**
タンパー	**対応**

電気仕様

電源	**24 Vdc**	**電流：最大 1.2 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



1) DESFire EV2/EV3 カードは DESFire EV1 カードとの下位互換性があるため、DESFire EV1 カードの機能を含む CSN およびスマートカード機能がサポートされます。

2) RF 読取距離は設置環境によって変動する可能性があります。

3) 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。

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。
- 本製品をマスター装置として使用する場合、指紋センサーを搭載した装置をスレーブとして接続すると、スレーブ装置で指紋認証が行えます。
  - 最大指紋クレデンシャル数（1:N:）：10,000
  - 指紋クレデンシャル最大数 (1:1:)：100,000

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。

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）

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：FS2-AWB 0.049 mW
- Bluetooth 周波数：FS2-AWB 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

- 本製品のソフトウェアは Linux カーネル 3.x を改変して作成されており、Linux カーネルのライセンスは GPL に従っています。 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 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 AOSP は Apache ライセンス 2.0 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 Linux カーネル 3.x ベースで改変されたソースおよび AOSP ソースコードは、Suprema サポートチームへお問い合わせいただくことで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。