DS-K1T673 シリーズ 顔認識端末

ユーザーマニュアル

規制情報

FCC 情報

注意：本機器の製造者または販売者による明示的な承認なしに変更または改造を行った場合、ユーザーの機器使用権限が無効になる可能性があります。

FCC準拠：この機器は、FCC規則の第15部に従い、クラスBデジタル機器の制限値に準拠していることが確認されています。これらの制限値は、住宅環境での使用において有害な干渉から合理的な保護を提供するよう設計されています。この機器は無線周波数エネルギーを発生、使用し、放射する可能性があります。指示に従って設置および使用されない場合、無線通信に有害な干渉を引き起こす可能性があります。ただし、特定の設置環境において干渉が発生しないことを保証するものではありません。この機器がラジオまたはテレビの受信に有害な干渉を引き起こす場合（機器の電源をオン/オフすることで確認できます）、ユーザーは次の措置の1つまたは複数を試すよう推奨されます：

—受信アンテナの向きや位置を変更する。

—機器と受信機の間隔を広くしてください。

—機器を、受信機が接続されている回路とは異なる回路のコンセントに接続してください。

—販売店または経験豊富なラジオ/テレビ技術者に相談してください。

この機器は、放射部と身体の間に最低20cmの距離を保って設置し、使用してください。

FCC 条件

この装置はFCC規則の第15部に準拠しています。動作は次の2つの条件に準拠しています：

1. この装置は有害な干渉を引き起こしてはなりません。

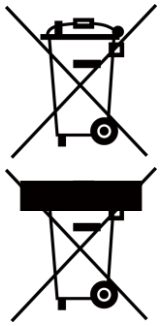
2. この装置は、受信するすべての干渉を許容しなければなりません。これには、正常な動作を妨げる可能性のある干渉も含まれます。

EU適合宣言

CE

この製品および適用される場合、付属品も「CE」マークが付与されており、したがって、以下の調和欧州規格に準拠しています

EMC指令 2014/30/EU、RE指令 2014/53/EU、RoHS指令 2011/65/EU



2012/19/EU（WEEE指令）：このマークが付いた製品は、欧州連合内で未分別一般廃棄物として処分できません。適切なリサイクルのため、同等の新品を購入する際は製品を販売店に返却するか、指定の回収場所に処分してください。詳細情報はwww.recyclethis.infoをご参照ください。

2006/66/EC（電池指令）：この製品には、欧州連合内で一般廃棄物として処分できない電池が含まれています。電池に関する詳細は製品ドキュメントをご確認ください。電池にはこのマークが記載されており、カドミウム（Cd）、鉛（Pb）、または水銀（Hg）を示す文字が含まれる場合があります。適切なリサイクルのため、電池を販売店または指定の回収場所に返却してください。詳細については、www.recyclethis.info をご覧ください。

安全注意事項

これらの指示は、ユーザーが製品を正しく使用し、危険や財産の損失を防止するために作成されています。

安全対策は「危険」と「注意」に分類されています：

危険：警告を無視すると、重大な怪我や死亡事故が発生する可能性があります。

注意：いずれかの注意を無視すると、怪我や機器の損傷を引き起こす可能性があります。

⚠	⚠
危険：重大な怪我や死亡を防止するため、これらの安全対策を必ず遵守してください。	**注意：**これらの注意点を遵守し、潜在的な怪我や材料の損傷を防止してください。

⚠危険:

- すべての電子機器の操作は、ご当地の電気安全基準、防火基準およびその他の関連法規に厳格に従って行う必要があります。
- 電源アダプターは、当社が提供する正規品を使用してください。この機器は、DC 12V、3Aのクラス2過電圧保護機能を備えた電源から供給されることを前提に設計されています。
- 複数の機器を1つの電源アダプターに接続しないでください。アダプターの過負荷により、過熱や火災の危険が生じる可能性があります。
- 装置の配線、設置、または分解を行う前に、必ず電源が切断されていることを確認してください。
- 製品を壁や天井に設置する際は、装置をしっかりと固定してください。
- 装置から煙、臭い、または音が発生した場合は、直ちに電源を切り、電源ケーブルを抜き、その後サービスセンターまでご連絡ください。
- 電池を誤飲しないでください。化学やけどの危険があります。
  この製品にはコイン型/ボタン型電池が含まれています。コイン型/ボタン型電池を誤飲すると、2時間以内に重度の内部やけどを引き起こし、死亡する可能性があります。
  新しい電池と使用済みの電池は、子供の手の届かない場所に保管してください。電池 compartment がしっかり閉まらない場合は、製品の使用を中止し、子供の手の届かない場所に保管してください。電池が飲み込まれたり、体の内部に挿入された可能性がある場合は、直ちに医療機関を受診してください。
- 製品が正常に動作しない場合は、販売店または最寄りのサービスセンターまでご連絡ください。絶対に自分で分解しないでください。（不正な修理やメンテナンスによる問題については、当社は一切の責任を負いません。）

⚠注意:

- 装置を落としたり、物理的な衝撃を与えたりしないでください。また、高電磁波放射にさらさないでください。振動する表面や衝撃を受ける場所への設置を避けてください（無視すると装置が損傷する可能性があります）。
- 極端な高温（製品の仕様書で指定された動作温度範囲内）や低温、塵埃の多い場所、湿気の多い場所には置かず、高電磁波にさらさないでください。
- 室内用機器のカバーは、雨や湿気から保護してください。
- 機器を直射日光、換気不良の場所、またはヒーターやラジエーターなどの熱源にさらすことは禁止されています（無視すると火災の危険があります）。
- 装置を太陽や極端に明るい方向に向けないでください。そうすると、画面のちらつきや汚れが発生する可能性があります（ただし、これは故障ではありません）。同時に、センサーの耐久性に影響を与える可能性があります。
- 装置のカバーを開ける際は、付属の手袋を使用し、カバーに直接触れないようにしてください。指の酸性汗がカバーの表面コーティングを腐食させる可能性があります。
- 装置カバーの内部および外部表面を清掃する際は、柔らかく乾いた布を使用し、アルカリ性洗剤は使用しないでください。
- 開封後は、すべての包装材を保管してください。万一故障が発生した場合は、元の包装材と共に製品を工場へ返送する必要があります。元の包装材なしで輸送した場合、製品に損傷が生じ、追加費用が発生する可能性があります。
- バッテリーの不適切な使用または交換は、爆発の危険を引き起こす可能性があります。交換する場合は、同じまたは同等のタイプのみを使用してください。使用済みのバッテリーは、バッテリー製造元の指示に従って処分してください。
- 生体認証製品は、アンチスプーフィング環境には完全に適用されません。より高いセキュリティレベルが必要な場合は、複数の認証モードを使用してください。
- 動作温度：-30 °C ～ +60 °C
- 室内および屋外での使用が可能です。室内での設置の場合、機器は光源から少なくとも2メートル以上、窓やドアから少なくとも3メートル以上離して設置してください。屋外での設置の場合、ケーブル配線部分にシリコーンシーラントを塗布し、雨滴の侵入を防ぐようにしてください。
- 保護等級：IP65

対応モデル

製品名	モデル
顔認識端末	DS-K1T673DX
	DS-K1T673DWX
	DS-K1T673TDX
	DS-K1T673TDWX
	DS-K1T673TDGX
	DS-K1T673TMW
	DS-K1T673TMG

ユーザーマニュアルに記載されている電源のみを使用してください:

モデル	メーカー	標準
C2000IC12.0-24P-DE	MOSO Power Supply Technology Co., Ltd.	CEE
C2000IC12.0-24P-GB	MOSO パワーサプライテクノロジー株式会社	BS
KPL-040F-VI	チャネルウェルテクノロジー株式会社	CEE

法的情報

この文書について

- このドキュメントには、製品の使用および管理に関する手順が記載されています。本文中に含まれる図、チャート、画像、およびその他の情報は、説明および参考目的のみを目的としています。
- 本ドキュメントに記載されている情報は、ファームウェアの更新またはその他の理由により、事前の通知なしに変更される場合があります。最新のバージョンは、Hikvisionのウェブサイト（***https://www.hikvision.com***）でご確認ください。別途合意がない限り、杭州 Hikvision デジタルテクノロジー株式会社またはその関連会社（以下「Hikvision」といいます）は、明示的または黙示的ないかなる保証もいたしません。
- 本ドキュメントは、製品をサポートする専門家の指導と支援を受けてご使用ください。

本製品について

- この製品は、購入した国または地域でのみアフターサービスサポートを受けることができます。
- 選択された製品がビデオ製品の場合、以下のQRコードをスキャンして「ビデオ製品の利用に関する取り組み」を取得し、必ずお読みください。

知的財産権の承認

- ヒクビジョンは、本文書に記載される製品に組み込まれた技術に関する著作権および/または特許権を保有しています。これには、第三者から取得したライセンスを含む場合があります。
- 本文書の一部（テキスト、画像、グラフィックなど）はすべてヒクビジョンに帰属します。本文書のいかなる部分も、書面による許可なしに、引用、複製、翻訳、または改変を行うことはできません。
- **HIKVISION**およびその他のヒクビジョンの商標およびロゴは、各管轄区域においてヒクビジョンの財産です。
- 本文書で言及されるその他の商標およびロゴは、それぞれの所有者の財産です。

法的免責事項

- 適用される法律で許される最大限の範囲において、本文書および本文書で説明される製品（ハードウェア、ソフトウェア、およびファームウェアを含む）は、「現状有姿」かつ「一切の欠陥およびエラーを含む」状態で提供されます。HIKVISIONは、明示的または

明示的または黙示的ないかなる保証も提供しません。これには、商品性、満足のいく品質、または特定の目的への適合性に関する保証が含まれますが、これらに限定されません。製品の使用は、お客様の責任において行われます。いかなる場合においても、HIKVISIONは、特別損害、間接損害、付随的損害、または派生的損害（事業利益の損失、事業の中断、データの損失、システムの破損、または文書の損失を含む損害について、契約違反、不法行為（過失を含む）、製品責任、またはその他の理由に基づくものであっても、製品の使用に関連して生じた場合、HIKVISIONは一切の責任を負いません。これは、HIKVISIONがそのような損害または損失の可能性について事前に通知を受けていた場合でも同様です。

- あなたは、インターネットの性質上、内在するセキュリティリスクが存在することを承認し、HIKVISIONは、サイバー攻撃、ハッカー攻撃、ウイルス感染、またはその他のインターネットセキュリティリスクに起因する異常な動作、プライバシー漏洩、またはその他の損害について一切の責任を負いません。ただし、必要に応じて適切な技術サポートを提供します。
- あなたは、この製品を適用されるすべての法律に準拠して使用することに同意し、あなたの使用が適用される法律に準拠していることを確保する責任は、あなたのみに帰属します。特に、あなたは、第三者の権利（publicity rights、知的財産権、データ保護その他のプライバシー権を含むがこれらに限定されない）を侵害しない方法で本製品を使用する責任を負います。お客様は、大量破壊兵器の開発または製造、化学兵器または生物兵器の開発または製造、核爆発または安全でない核燃料サイクルに関連するいかなる活動、または人権侵害を支援する目的での使用を含みます。
- 本文書と適用される法律との間に矛盾が生じた場合、後者が優先されます。

データ保護

- データの保護のため、Hikvision製品の開発にはプライバシーバイデザイン原則が組み込まれています。例えば、顔認識機能を備えた製品の場合、生体認証データは暗号化方式で製品内に保存されます。指紋認証製品の場合、指紋テンプレートのみが保存され、指紋画像の復元は不可能です。
- データ管理者/処理者として、個人データの収集、保管、利用、処理、開示、削除などを行う場合があります。個人データの保護に関する適用される法律および規制（セキュリティ対策の実施を含むがこれらに限定されない）に留意し、遵守するようご注意ください。具体的には、個人データを保護するための合理的な管理上および物理的なセキュリティ対策を実施し、セキュリティ対策の有効性を定期的にレビューおよび評価を行うことが含まれます。

記号の規約

本文書において使用される記号は、以下のとおり定義されます。

記号	説明
 危険	危険な状況を示し、回避しない場合、死亡または重大なけがを引き起こす可能性があります。
 注意	回避しない場合、機器の損傷、データ損失、性能の低下、または予期しない結果を引き起こす可能性がある危険な状況を示します。
 注意	本文の重要なポイントを強調したり補足したりするための追加情報を提供します。

目次

第1章 外観

顔認識端末の詳細な情報については、以下の内容をご参照ください:

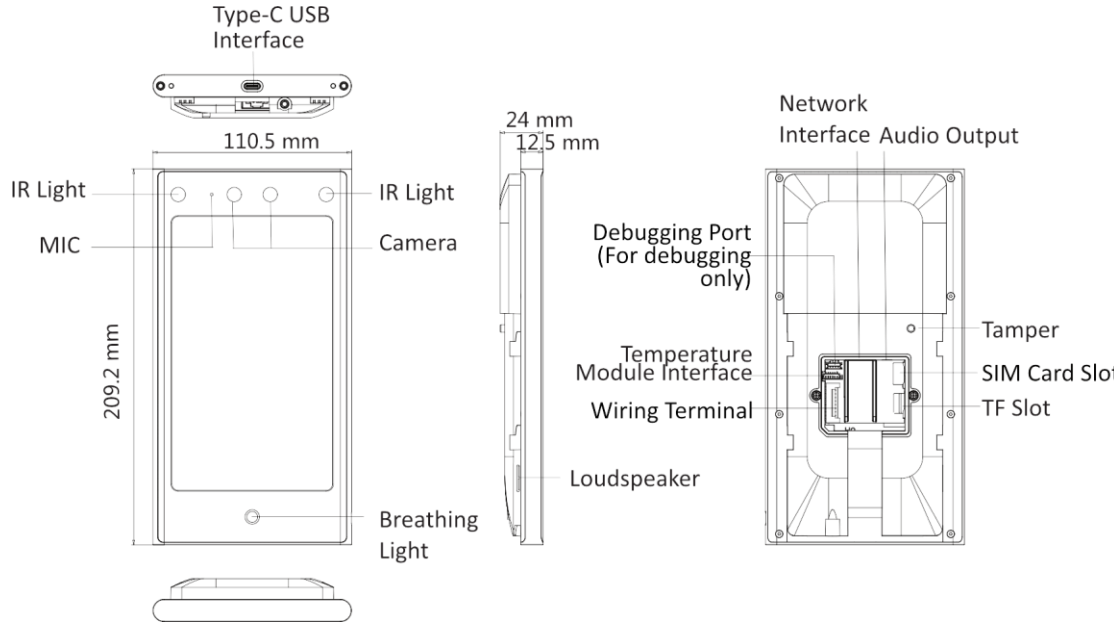


図1-1 顔認識端末

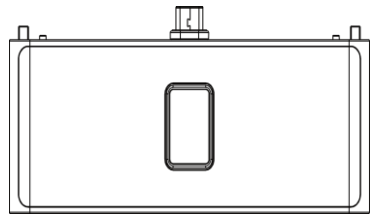


図1-2 指紋+ Bluetooth+ QRコードモジュール

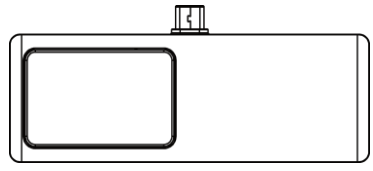


図1-3 無線モジュール（ 433/868 MHz ）

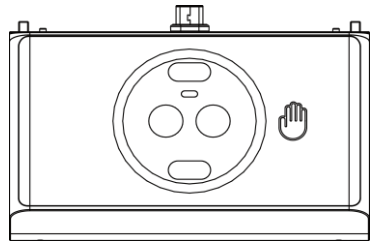


図1-4 手のひら印刷と手のひら静脈モジュール

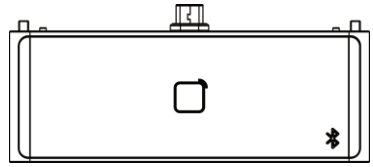


図1-5 2周波数カードモジュール（ 13.56 MHzおよび125 kHz ）

注

- 図は参考用です。
- このデバイスは、実際のニーズに応じてアクセス可能な複数のモジュールに対応しています。
- 手のひら指紋と手のひら静脈モジュールが新しい顔認識端末にアクセスする際、周辺モジュールのデータをクリアし、再発行または収集する必要があります。
- 周辺モジュールの表面は清潔に保つ必要があります。センサーによる誤報を防止するためです。

第2章 インストール

2.1 インストール環境

- バックライト、直射日光、および間接日光を避けてください。
- より良い認識のため、設置環境内またはその近くに光源を設置してください。
- 屋外に設置する必要がある場合は、デバイスに保護カバー（オプション）を取り付けてください。

注意
境の詳細については、*「設置環境のヒント」*を参照してください。

2.2 ギャングボックスを使用した埋め込み取り付け

作業開始前に

デバイスの背面シートを取り外してください。

手順

1. ギャングボックスが壁に正しく取り付けられていることを確認してください。

   注意

   ギャングボックスは付属していません。

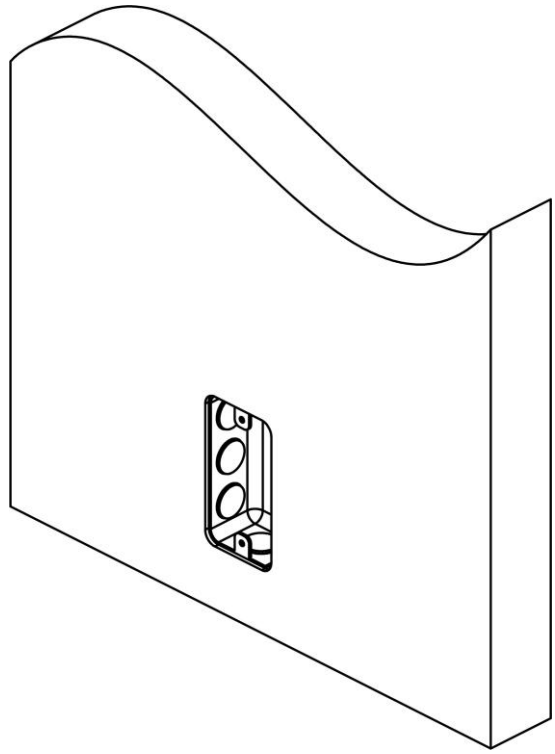


図2-1 ギャングボックスの取り付け

2. 付属の2本のネジ（SC-K1A4X24_5）で、ギャングボックスにマウントプレートを固定してください。

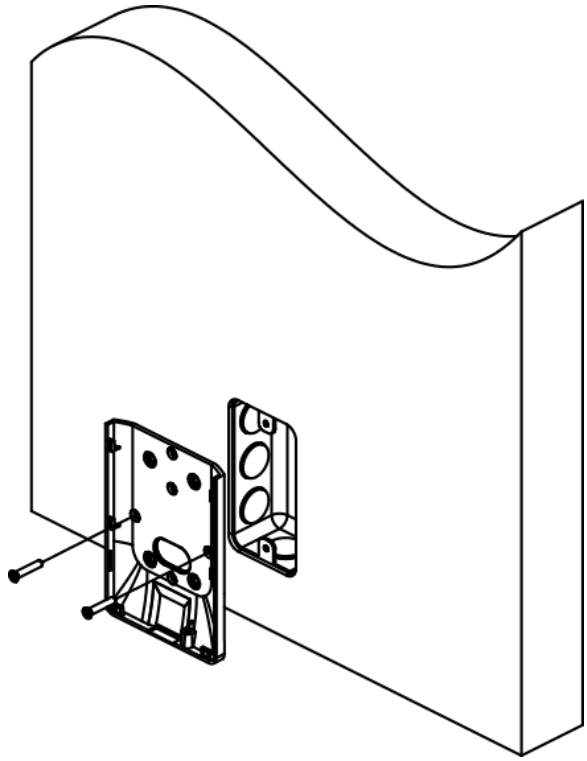


図2-2 マウントプレートの取り付け

3. ケーブルをケーブル穴に通し、ケーブルを配線し、ケーブルをギャングボックスに挿入します。

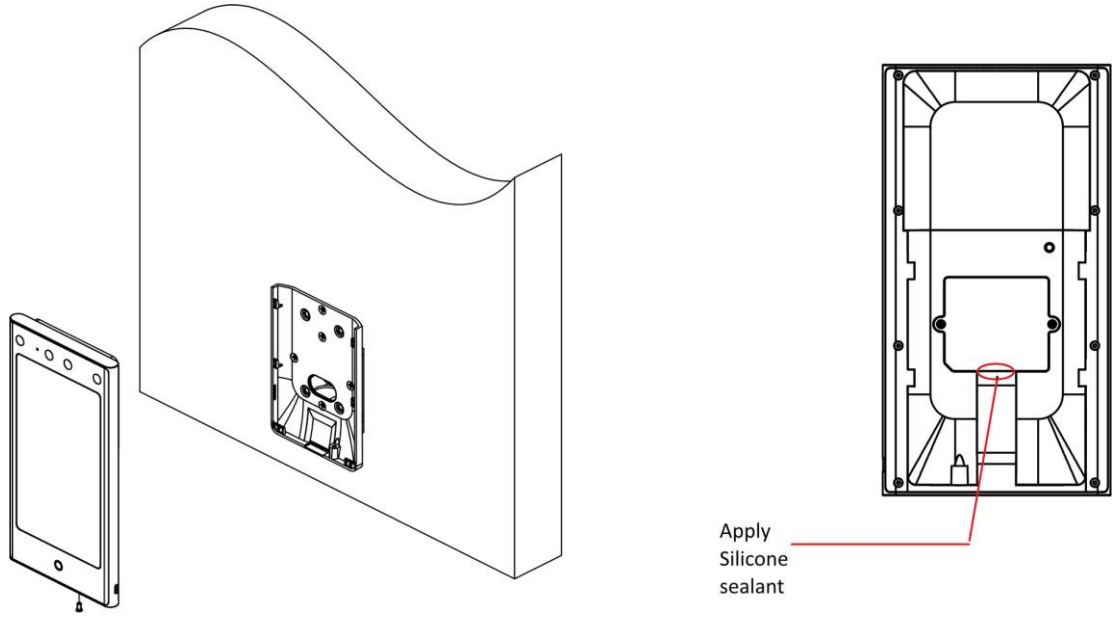


図2-3 デバイスの固定

注意
ケーブル配線部分にシリコーンシーラントを塗布し、雨滴の侵入を防ぎます。

4. デバイスをマウントプレートに合わせ、付属のネジ（SC-KM3X6-H2-SUS）1本でデバイスをマウントプレートに固定してください。

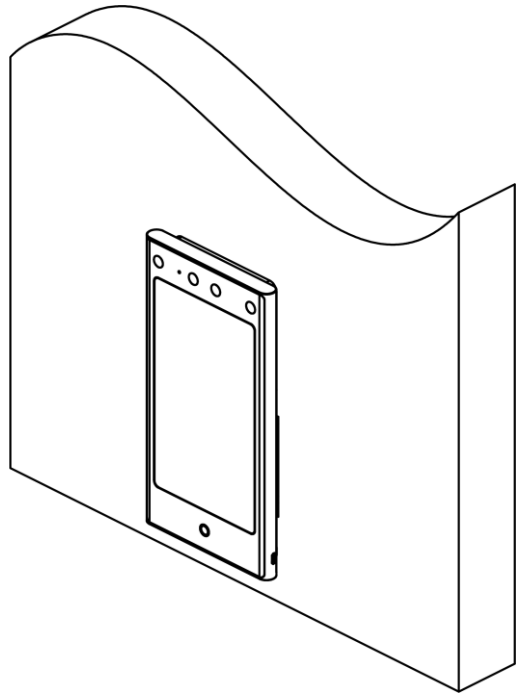


図2-4 デバイスの固定

5. 取り付け後、デバイスの適切な使用（屋外使用）のため、画面に保護フィルム（付属品の部品）を貼り付けてください。

2.3 表面取り付け

手順

注意

追加の力は、機器の重量の3倍に等しいものでなければなりません。機器とその取り付け手段は、取り付け中に確実に固定されている必要があります。取り付け後、機器（関連する取り付けプレートを含む）は損傷を受けてはいけません。

1. 取り付けテンプレートの基準線に従い、取り付けテンプレートを壁または他の表面に貼り付け、地面から1.4メートル高い位置に設置してください。

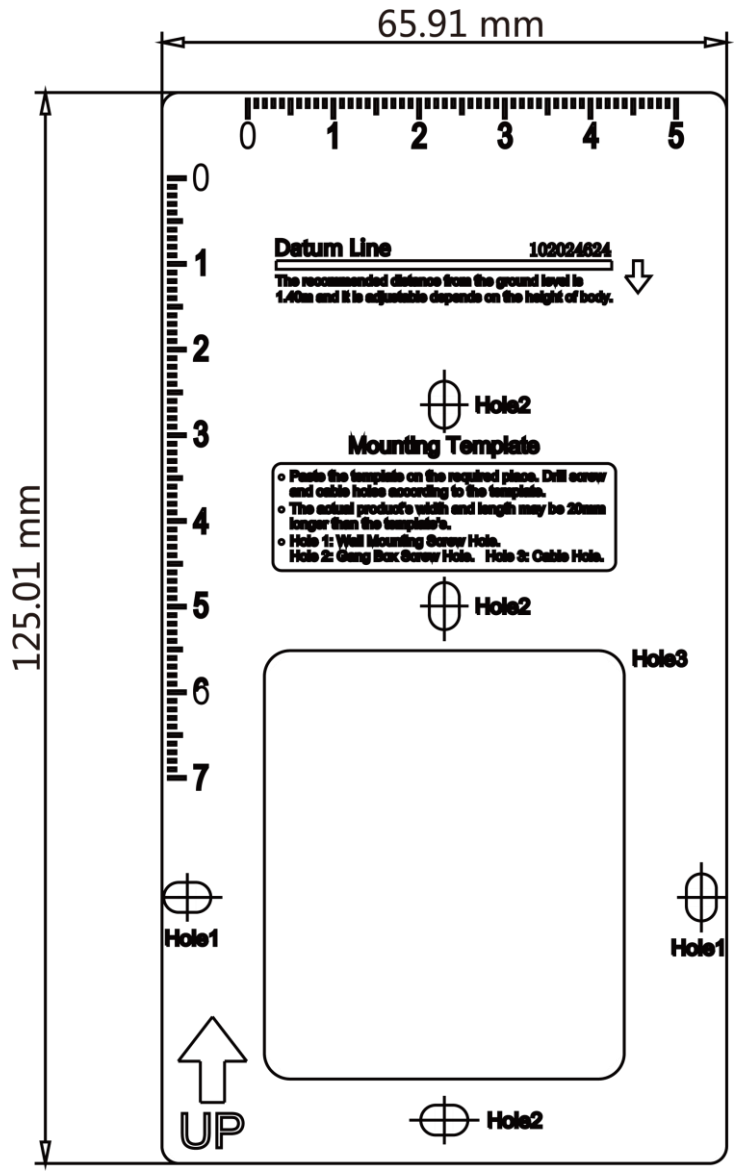


図2-5 取り付けテンプレート

2. 取り付けテンプレートの「穴1」の位置に合わせて、壁または他の表面に穴を開けます。

3. 取り付けプレート上のケーブル穴を工具で取り除きます。

4. 穴をマウントプレートに合わせ、付属の2本のネジ（K1A×24）でマウントプレートを壁に固定します。

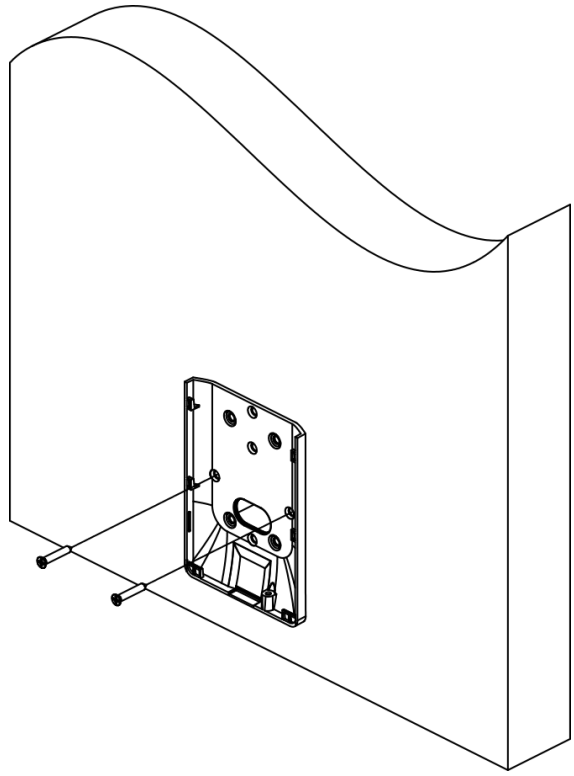


図2-6 取り付けプレートを取り付ける

5. ケーブルをマウントプレートのケーブル穴に通し、対応する周辺機器のケーブルに接続してください。

注意 屋外に設置する場合、配線出口にシリコーンシーラントを塗布し、水の侵入を防ぐ必要があります。

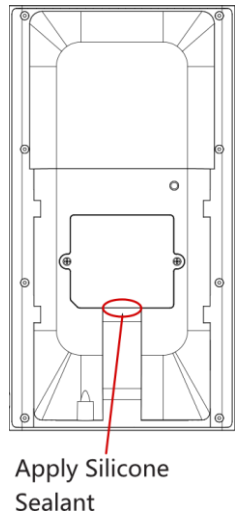


図2-7 シリコーンシーラントの塗布

6. デバイスをマウントプレートと合わせ、デバイスをマウントプレートに吊り下げます。

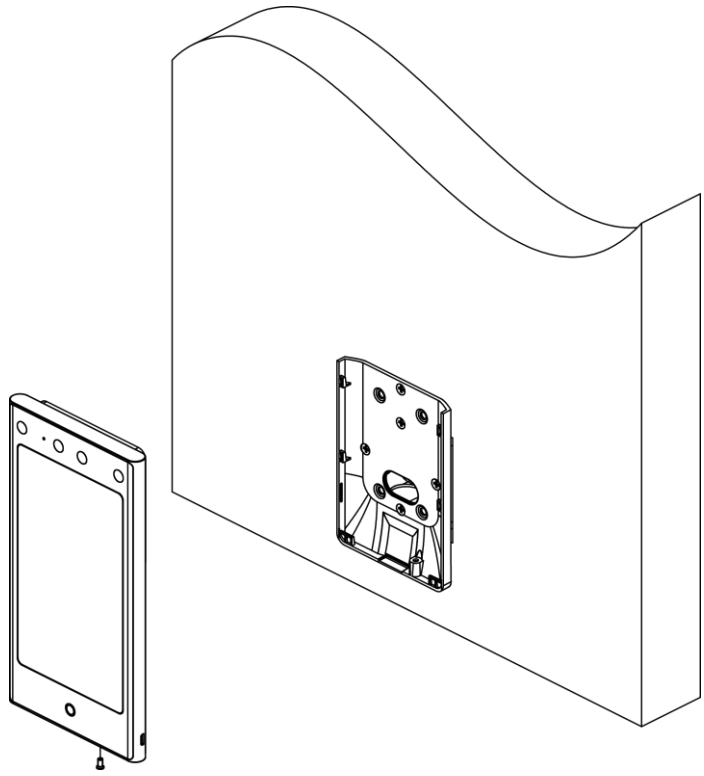


図2-8 デバイスの吊り下げ

7. 付属のネジ（KM3×6）1本を使用して、デバイスと取り付けプレートを固定します。

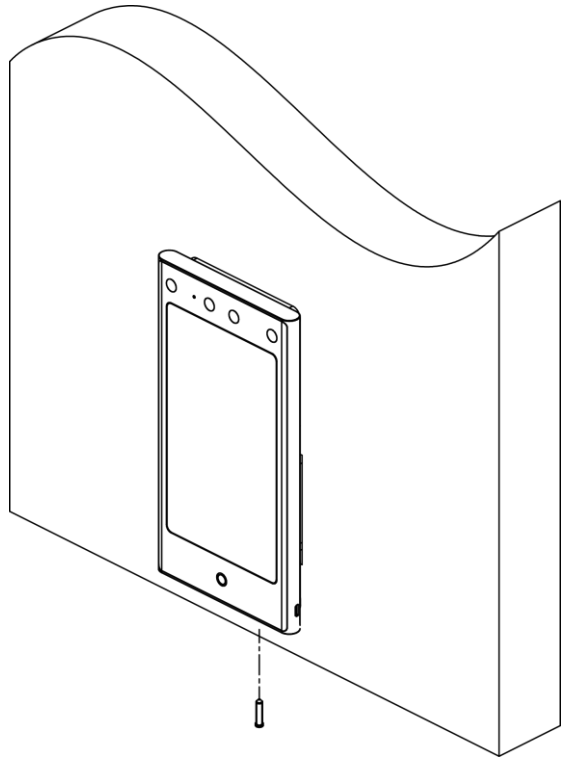


図2-9 セキュアデバイス

8. オプション : 実際の使用状況に応じて周辺モジュールを接続してください。

9. インストール後、デバイスの適切な使用（屋外使用）のため、画面に保護フィルム（モデルによっては付属品）を貼り付けてください。

2.4 ブラケットを使用して取り付け

2.4.1 ブラケットを使用して取り付ける前の準備

手順

1. ターンスタイルの表面に、以下の図に示す位置に穴を開け、防水ナットを取り付けてください。

注意 押し込んだ後、はんだ付けを行い、水が入らないようにします。

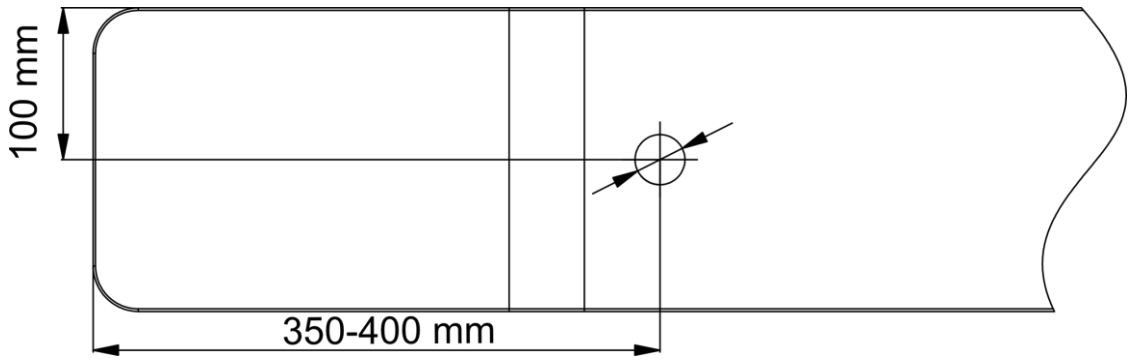


図2-10 ターンスタイルに穴を開ける

2. ターンスタイルの本体に対して取り付け角度を180°直角にする必要がある場合、以下の作業が必要です。

1) 以下の図に示す3本のネジを外します。

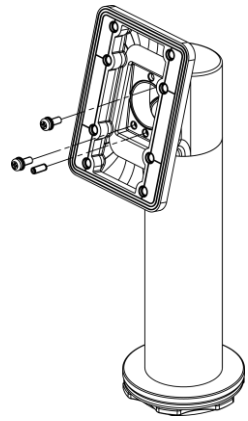


図2-11 ネジの取り外し

2) 固定部を180°回転させ、3本のネジを元に戻して取り付けます。

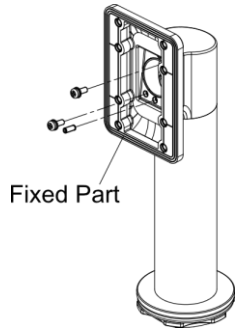


図2-12 固定部を回転させる

2.4.2 ブラケットの取り付け

手順

1. ブラケットの底部をターンスタイルに通し、内蔵ナットでターンスタイルに固定します。ブラケットを適切な角度に調整し、レンチでナットをしっかりと締め付けます。

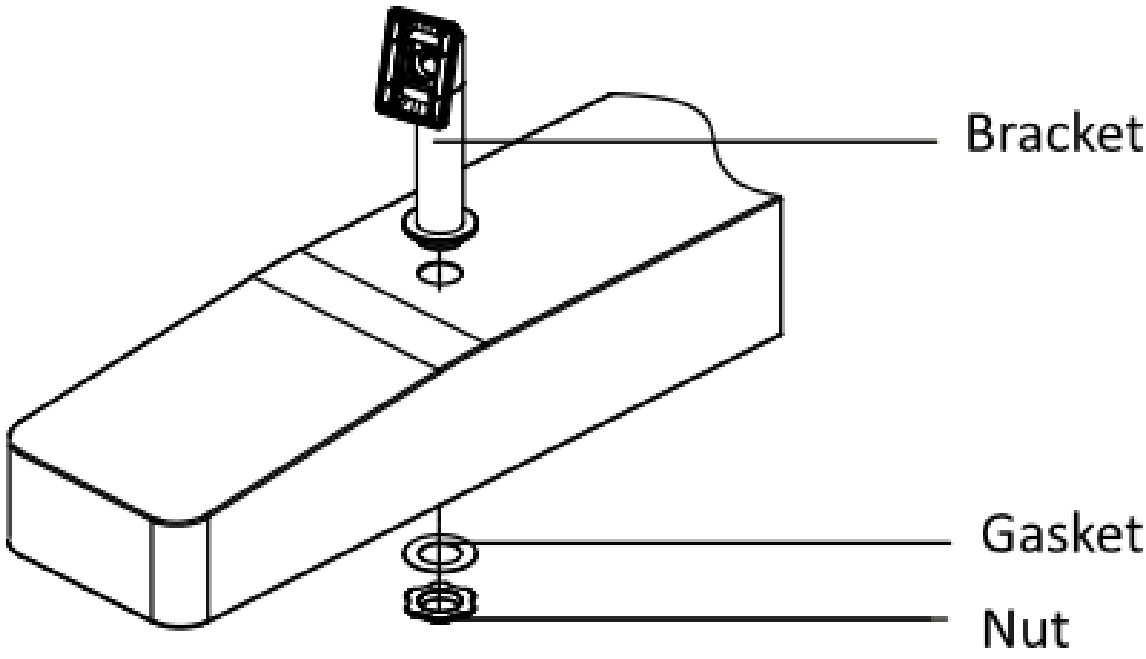


図2-13 ブラケットの固定

2. 4本のK1M4×8-SUSネジを使用して、マウントプレートをブラケットに固定してください。

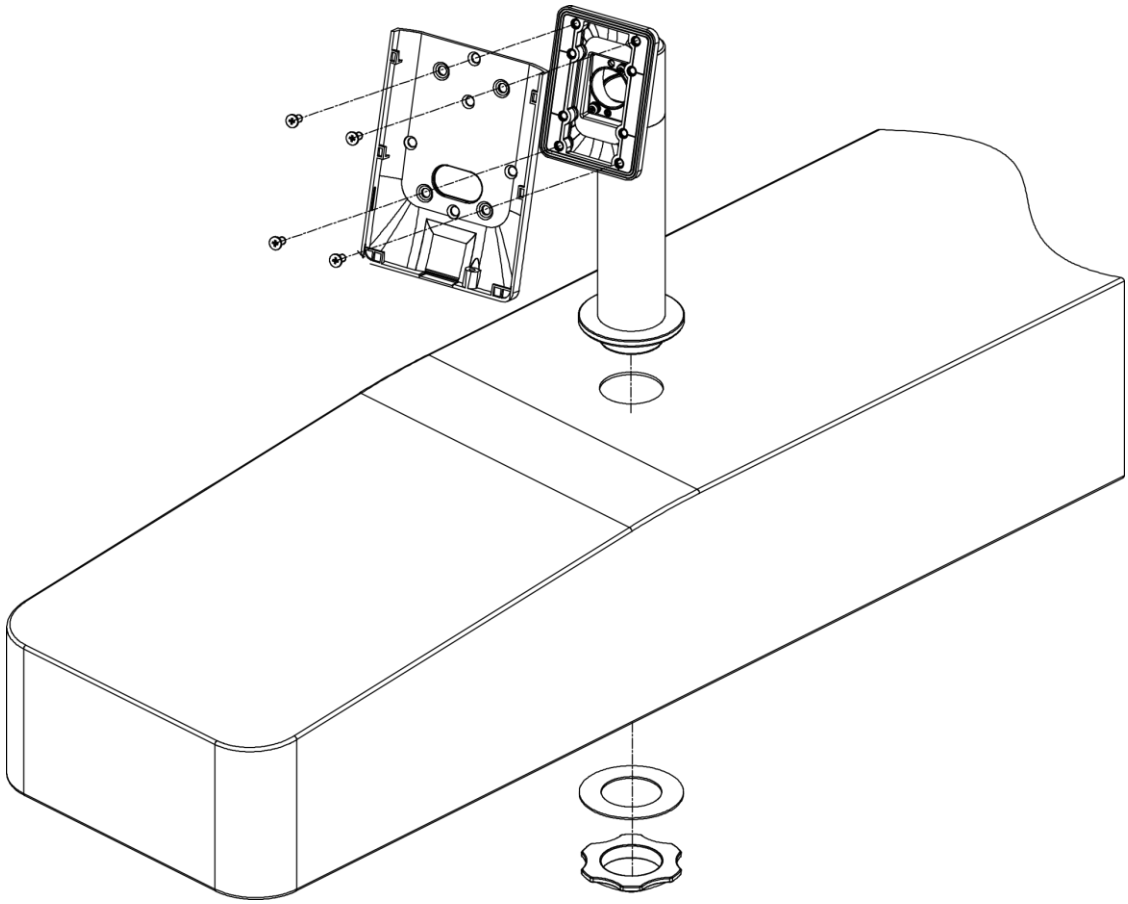


図2-14 取り付けプレートを固定する

3. 顔認識端末のケーブルをケーブル穴に通し、内側の回転ゲートに挿入します。顔認識端末をKM3×6-H2-SUSネジで取り付けプレートに固定します。

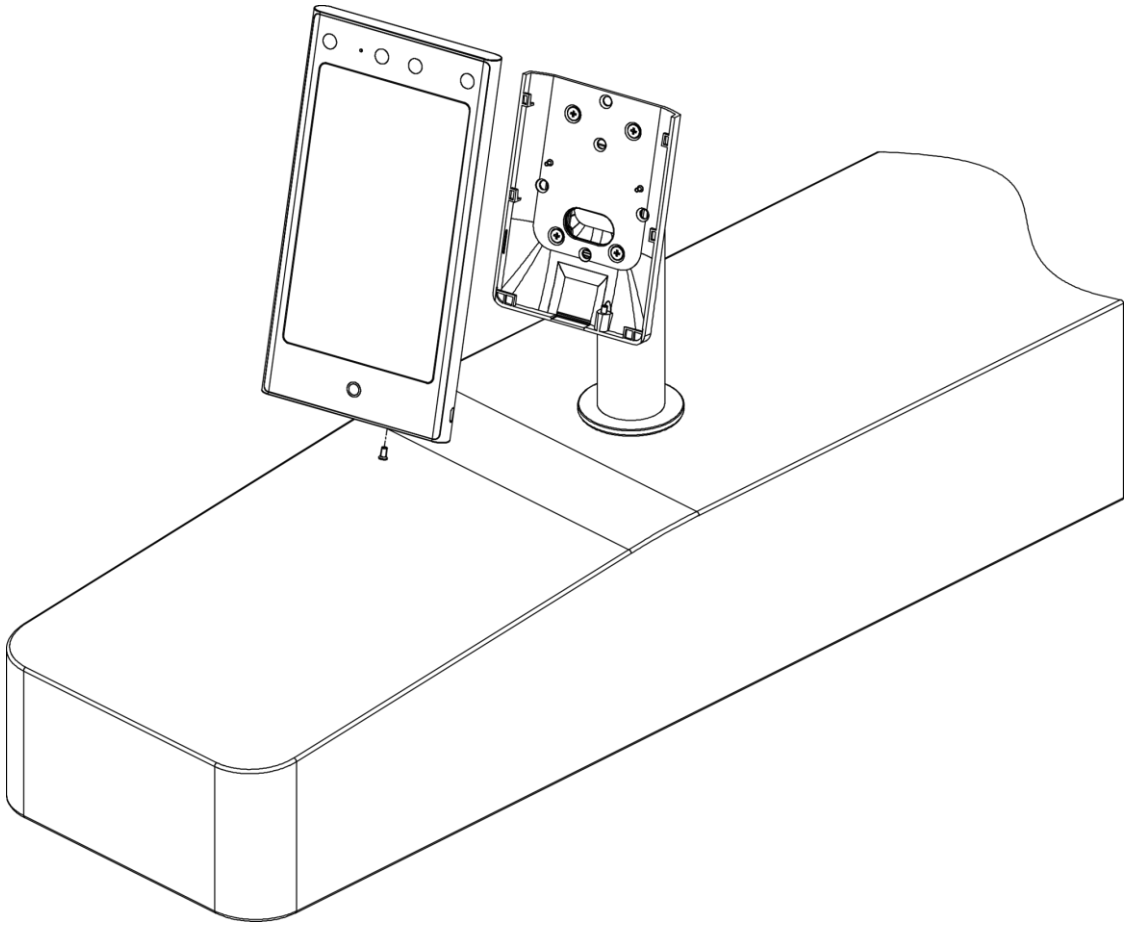


図2-15 顔認識端末の固定

4. 取り付け後、装置の正常な使用（屋外使用）のため、画面に保護フィルム（付属品の一部）を貼り付けます。

第3章 配線

このデバイスは、RS-485ターミナル、ドアロック、出口ボタン、アラーム出力/入力デバイス、Wiegandカードリーダー、アクセスコントローラー、および電源供給装置への接続に対応しています。以下の説明に従って周辺機器を配線してください。

Wiegandカードリーダーをアクセスコントローラーに接続した場合、顔認識端末は認証情報をアクセスコントローラーに送信し、アクセスコントローラーはドアを開けるかどうかを判断します。

注意

- ケーブルの太さが18 AWGの場合、12 Vのスイッチング電源を使用する必要があります。また、電源とデバイス間の距離は20 mを超えてはいけません。
- ケーブルの太さが15 AWGの場合、12 Vのスイッチング電源を使用する必要があります。また、電源と機器間の距離は30 mを超えてはなりません。
- ケーブルの太さが12 AWGの場合、12 Vのスイッチング電源を使用する必要があります。また、電源と機器間の距離は40 mを超えてはなりません。

3.1 端子説明

端子には、電源入力、アラーム入力、アラーム出力、RS-485、Wiegand出力、およびドアロックが含まれます。

端子の図は次のとおりです:

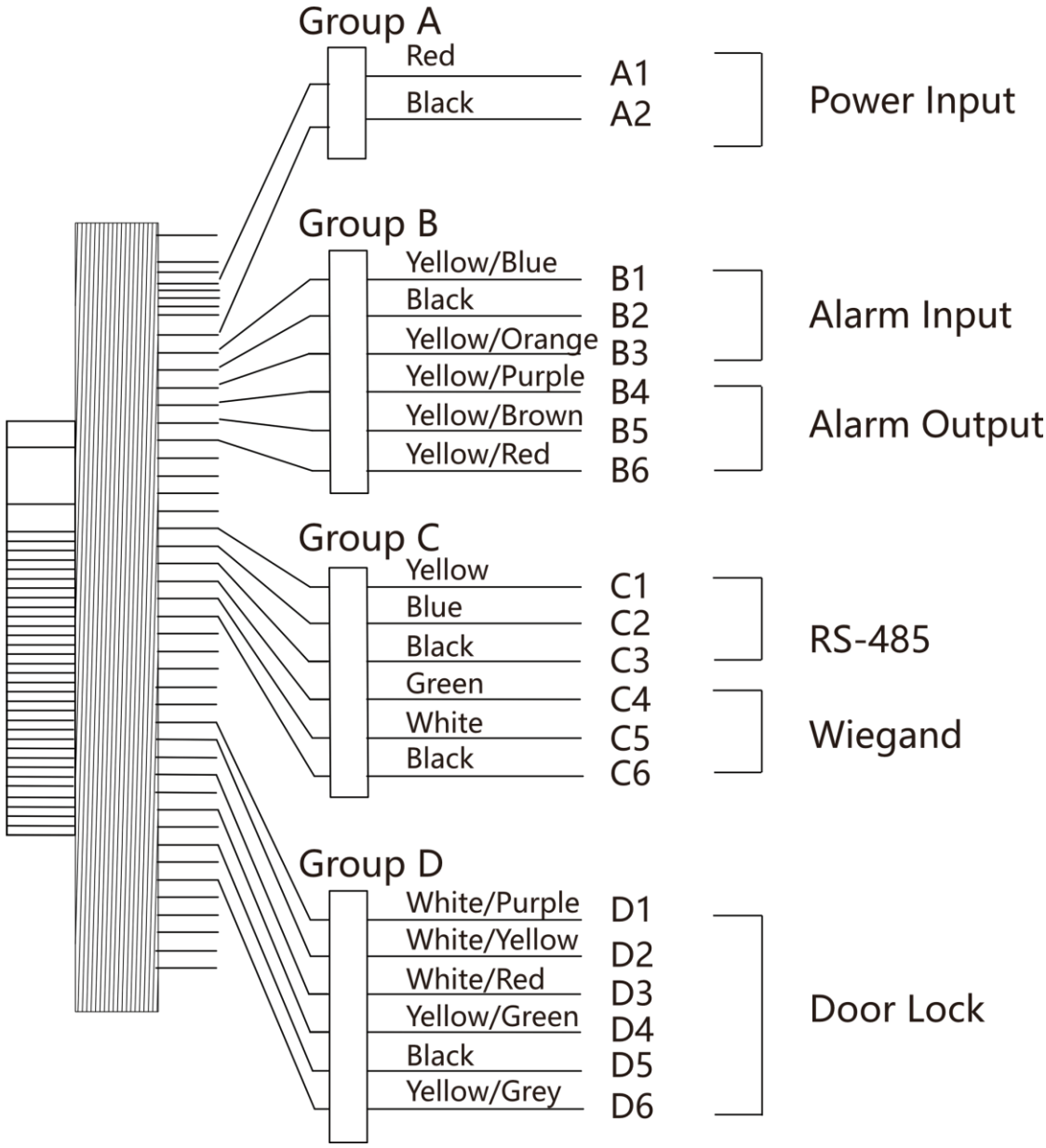


図3-1 端子図

端子の説明は次のとおりです:

表3-1 ターミナルの説明

グループ	番号	機能	色	名前	説明
グループA	A1	入力電力	赤	+12 V	12 VDC電源供給
	A2		黒	GND	接地
グループB	B1	アラーム入力	黄色/青	IN1	アラーム入力1
	B2		黒	GND	接地
	B3		黄色/オレンジ	IN2	アラーム入力2
	B4	アラーム出力	黄色/紫	NC	アラーム出力配線
	B5		黄色/茶色	COM	
	B6		黄色/赤	NO	
グループC	C1	RS-485	黄色	485+	RS-485 配線
	C2		青	485-	
	C3		黒	GND	接地
	C4	ワイガンド	グリーン	W0	ワイガンド配線 0
	C5		ホワイト	W1	ワイガンド配線 1
	C6		黒	GND	接地
グループD	D1	ドアロック	白/紫	NC	ロック配線（NC）
	D2		白/黄	COM	共通
	D3		白/赤	いいえ	ロック配線（NO）
	D4		黄色/緑	センサー	ドアコンタクト
	D5		黒	GND	接地
	D6		黄色/灰色	BTN	出口ドア配線

3.2 通常デバイス用配線

この端子には通常の周辺機器を接続できます。

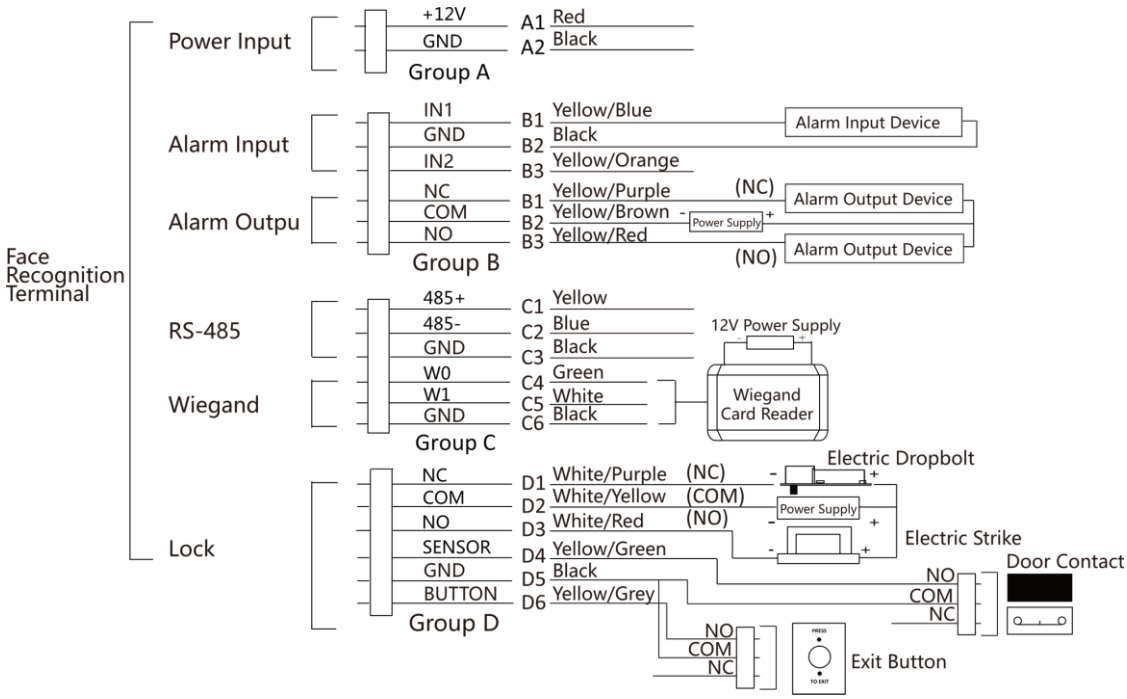


図3-2 デバイス配線

注

- 顔認識端末のWiegand方向を「**入力**」に設定して、Wiegandカードリーダーに接続してください。アクセスコントローラーに接続する場合、Wiegand方向を「**出力**」に設定して、認証情報をアクセスコントローラーに送信してください。
- Wiegand方向の設定の詳細については、「***Wiegandパラメーターの設定***」を参照してください。
- デバイスを直接電源に接続しないでください。

3.3 ワイヤ式セキュアドア制御ユニット

ターミナルをセキュアドア制御ユニットに接続できます。配線図は次のとおりです。

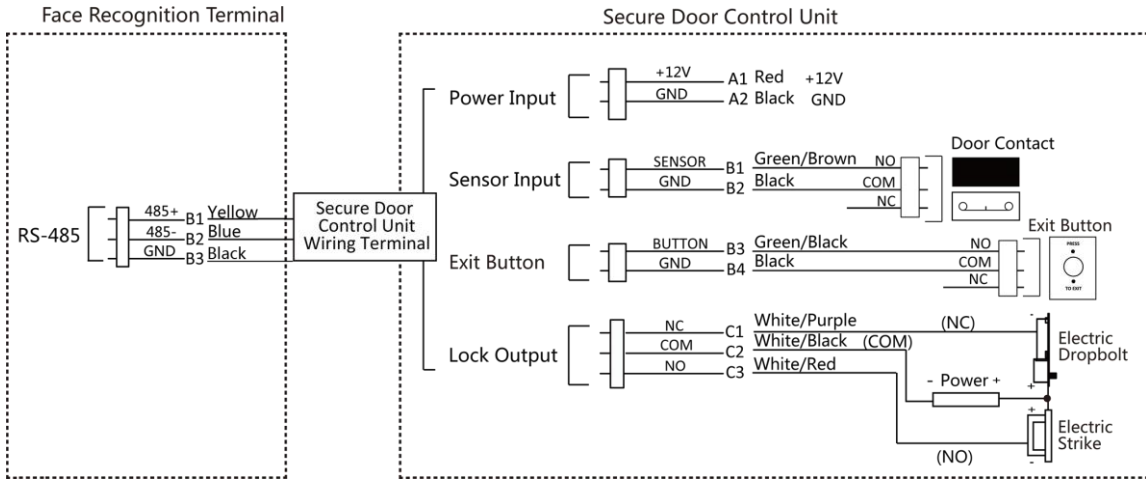


図3-3 セキュアドア制御ユニットの配線

注

セキュアドア制御ユニットは、外部電源に別途接続する必要があります。推奨される外部電源は12V、0.5Aです。

3.4 火災モジュールを配線

3.4.1 電源を切った際にドアが開く配線図

ロックタイプ：陽極ロック、磁気ロック、電気ボルト（NO）セキュリティタイプ：
電源切断時にドアが開く

シナリオ：消防車アクセス用に設置

タイプ1

注

火災システムは、アクセス制御システムの電源供給を制御します。

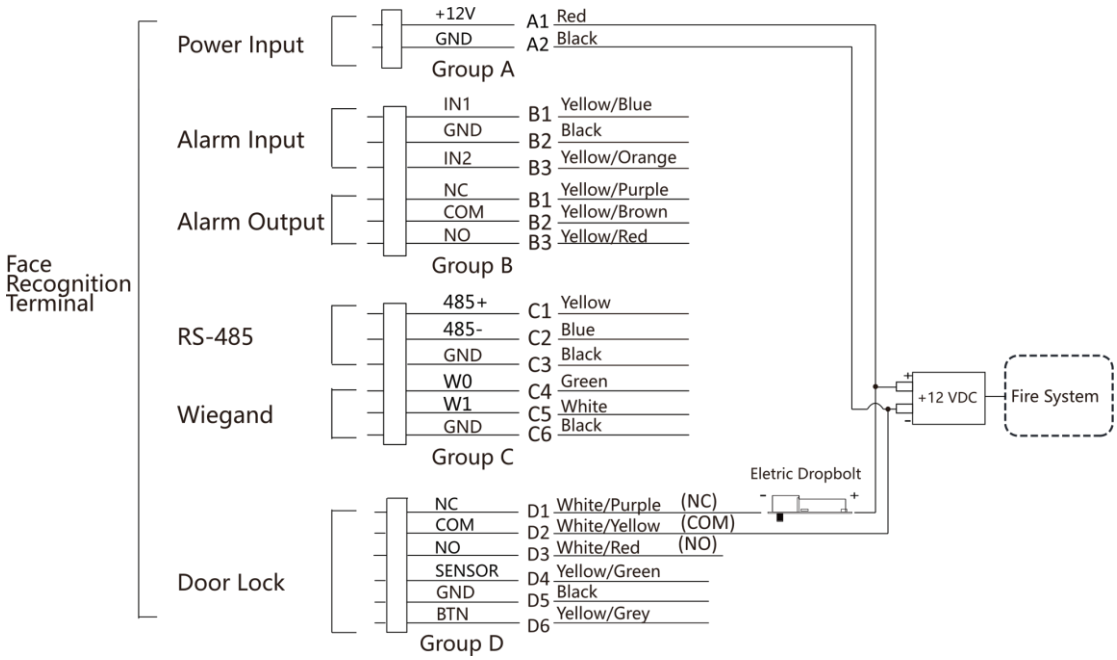


図3-4 ワイヤデバイス

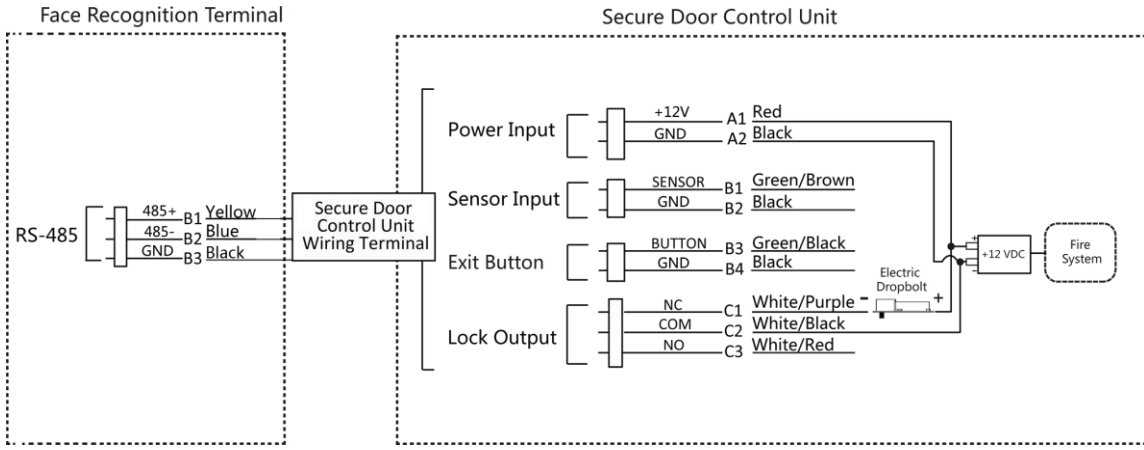


図3-5 配線式セキュアドア制御ユニット

タイプ2

注

火災システム（NOとCOM、電源オフ時に通常開）は、ロックと電源に直列接続されています。火災報知器が作動すると、ドアは開いたままになります。通常時は、NOとCOMは閉じています。

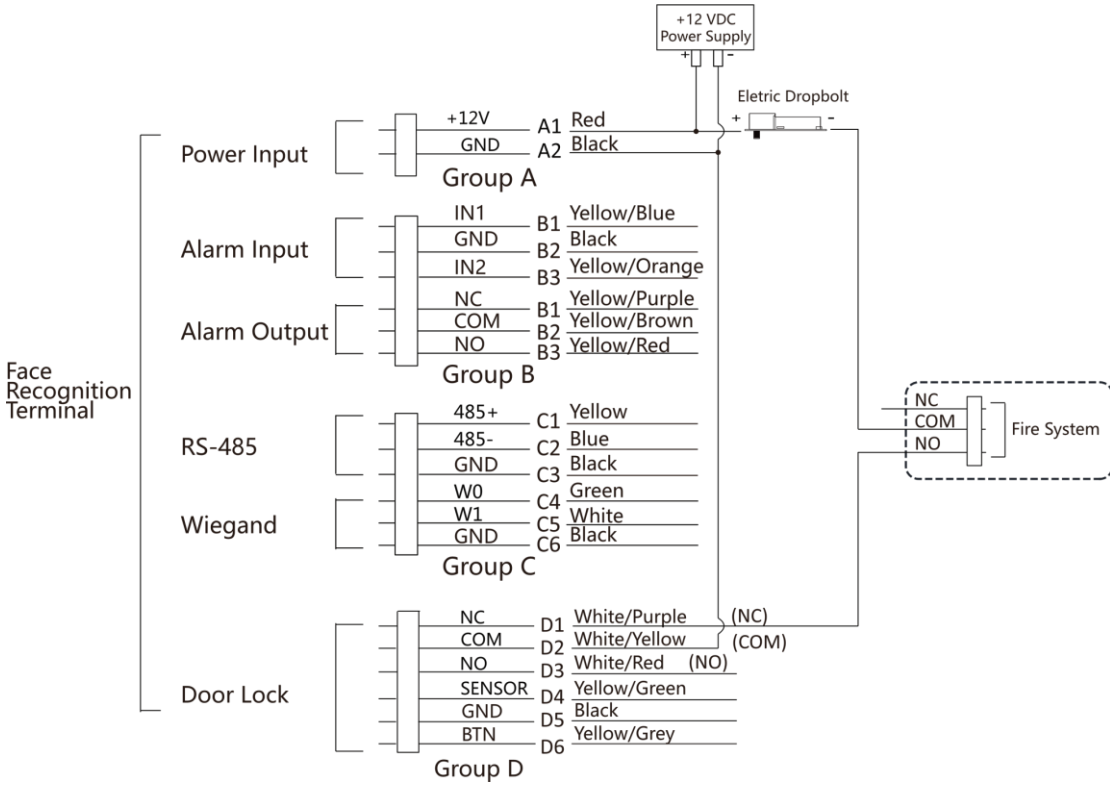


図3-6 配線装置

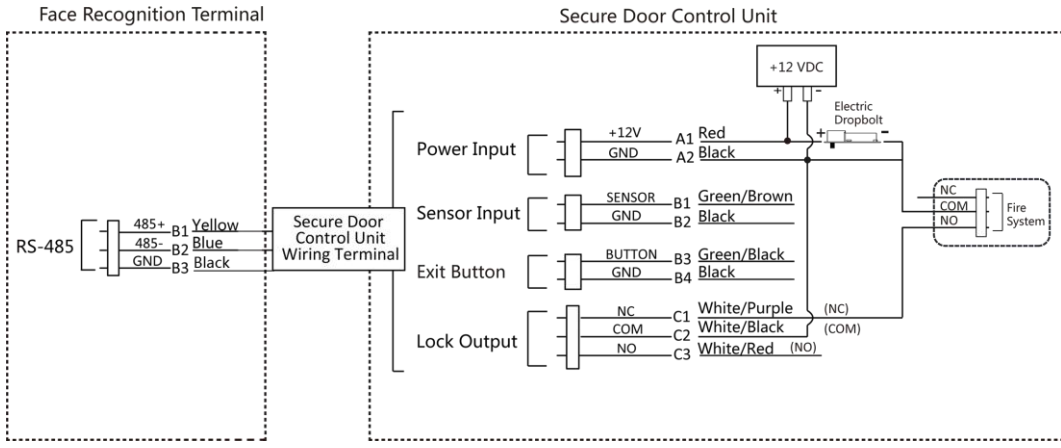


図3-7 配線 セキュアドア制御ユニット

3.4.2 電源切断時のドアロック配線図

ロックタイプ: カソードロック、電気式ロック、および電気式ボルト（NC）セキュリティタイプ: 電源を切断時にドアがロックされる

シナリオ: 火災連動装置と接続された入口/出口に設置

注

- 無停電電源装置（UPS）が必要です。
- 火災システム（NCとCOM、電源オフ時に通常閉）は、ロックと電源に直列接続されています。火災報知器が作動すると、ドアは開いたままになります。通常時は、NCとCOMは開いています。

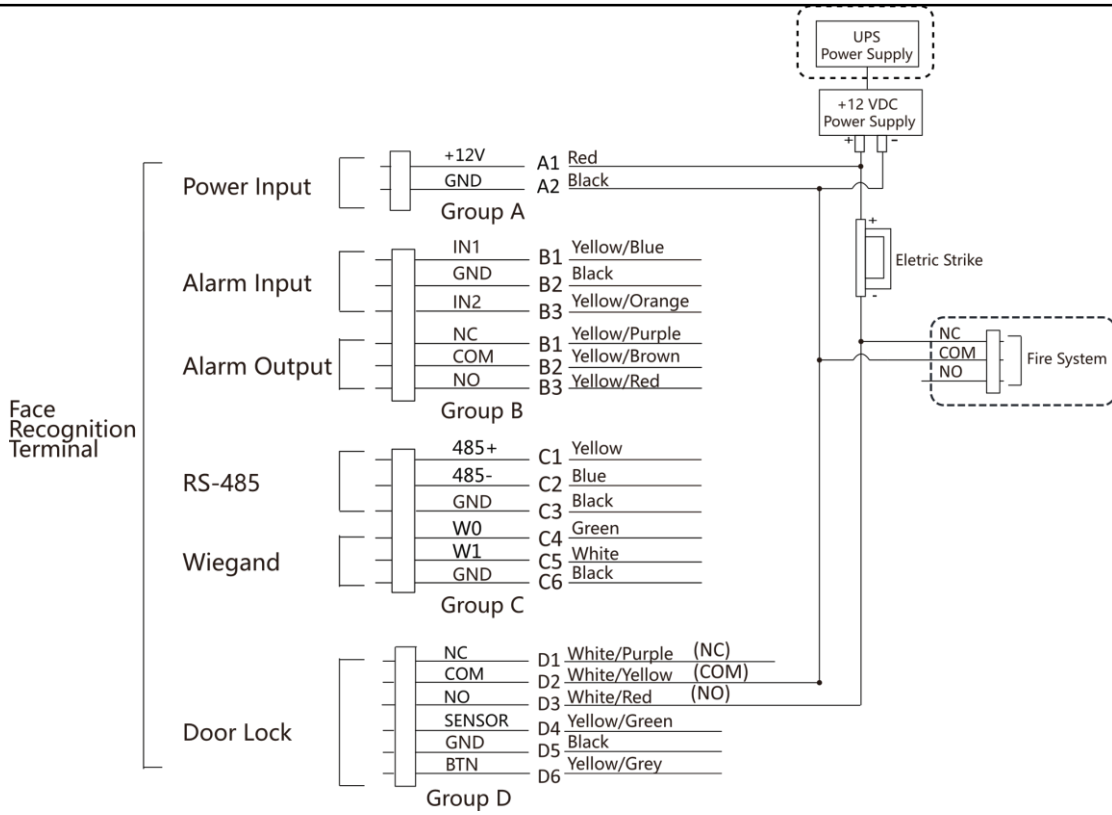


図3-8 機器配線図

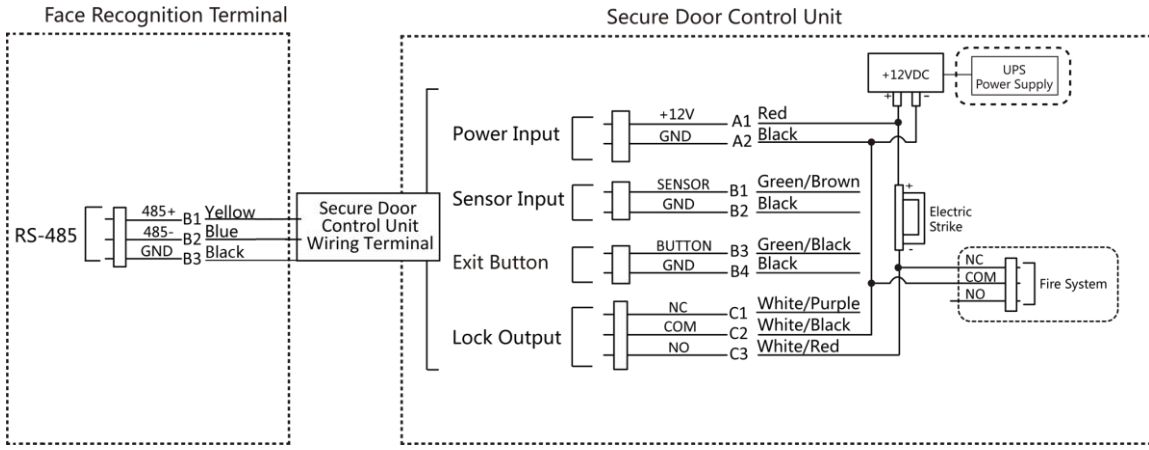

Face Recognition Terminal
Secure Door Control Unit
RS-485
485+
485-
GND
B1
B2
B3
Yellow
Blue
Black
Secure Door Control Unit Wiring Terminal
Power Input
+12V
GND
A1
A2
Red
Black
Sensor Input
SENSOR
GND
B1
B2
Green/Brown
Black
Exit Button
BUTTON
GND
B3
B4
Green/Black
Black
Lock Output
NC
COM
NO
C1
C2
C3
White/Purple
White/Black
White/Red
+12VDC
UPS Power Supply
Electric Strike
NC
COM
NO
Fire System

図3-9 配線図

第4章 パームプリントとパームベインインジケーターの説明

表示器	説明
赤色点灯	デバイスはオフラインです。
高速点滅赤	手のひらがお互いに近すぎます。
赤色点滅（ゆっくり）	認証に失敗しました。
緑のライトが3秒間点灯しています	認証に成功しました。

第5章 アクティベーション

最初のログイン前にデバイスをアクティベーションする必要があります。デバイスを電源投入後、システムはデバイスアクティベーション画面に切り替わります。

デバイス、SADPツール、およびクライアントソフトウェアによるアクティベーションがサポートされています。デバイスのデフォルト値は次のとおりです：

- デフォルトのIPアドレス：192.0.0.64
- デフォルトのポート番号：8000
- デフォルトのユーザー名：admin

5.1 デバイス経由でのアクティベーション

デバイスがアクティベートされていない場合、電源を入れた後にデバイスをアクティベートできます。

「デバイスをアクティベート」ページで、パスワードを作成し、パスワードを確認します。**アクティベートを**タップすると、デバイスがアクティベートされます。

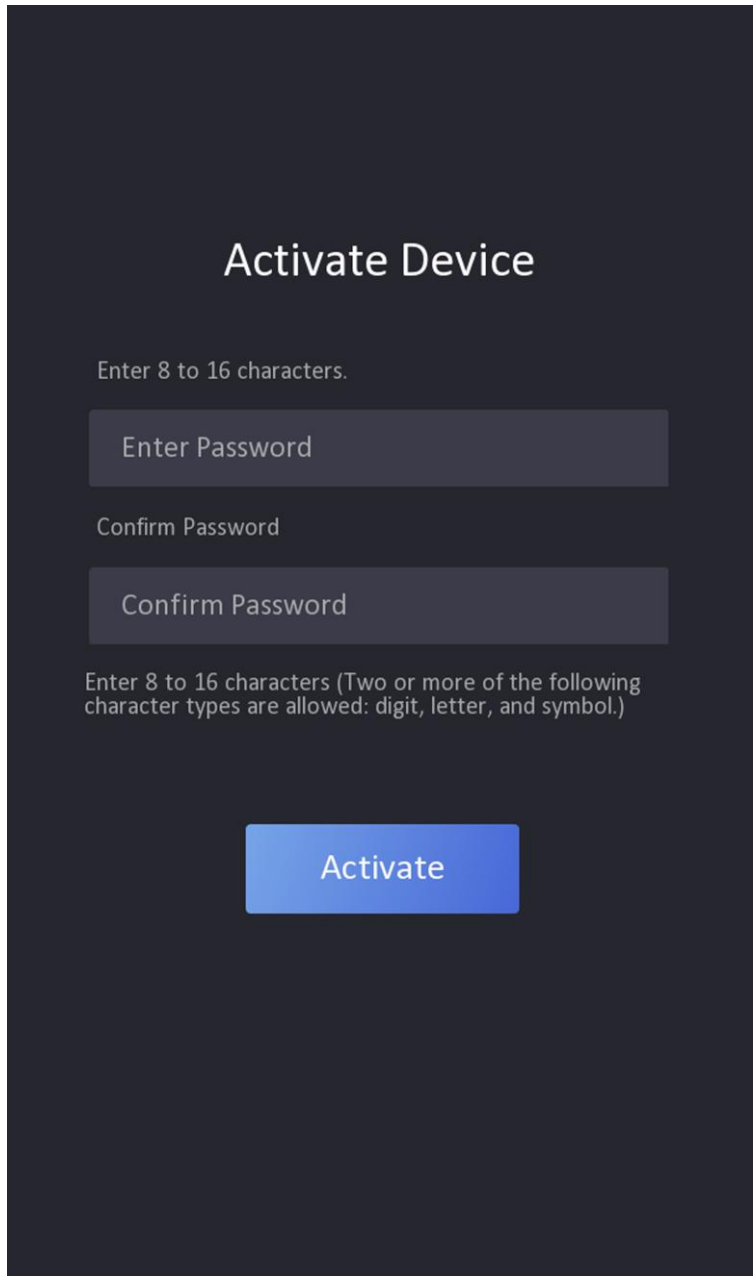


図5-1 アクティベーション画面

注意

- デバイスのパスワードの強度は自動的にチェックされます。最低8文字以上（大文字、小文字、数字、特殊文字の少なくとも3種類を含む）のパスワードに変更することを強くおすすめします。

文字）を使用して、製品のセキュリティを強化してください。また、特に高セキュリティシステムでは、パスワードを定期的に変更することをおすすめします。パスワードを毎月または毎週変更することで、製品のセキュリティをより効果的に保護できます。

- すべてのパスワードおよびその他のセキュリティ設定の適切な設定は、サービスプロバイダーおよび/またはエンドユーザーの責任です。
- パスワードには以下の文字を含めないでください：ユーザー名、123、admin（大文字小文字区別なし）、4つ以上連続して増加または減少する数字、または4つ以上連続して繰り返される文字。
- パスワードには、hik、hkws、hikvision（大文字小文字を区別しません）などの単語を含めないでください。

5.2 ウェブブラウザ経由でアクティベート

デバイスはウェブブラウザ経由でアクティベートできます。

手順

1. ウェブブラウザのアドレスバーにデバイスのデフォルトIPアドレス（192.0.0.64）を入力し、

Enter キーを押します。

注意

デバイスのIPアドレスとコンピュータのIPアドレスが同じIPセグメント内にあることを確認してください。

2. 新しいパスワード（管理者パスワード）を作成し、パスワードを確認してください。

注意

- デバイスのパスワードの強度は自動的に確認できます。製品のセキュリティを強化するため、ご自身で選択したパスワード（8文字以上で、大文字、小文字、数字、特殊文字の少なくとも3種類を含む）に変更することを強くおすすめします。また、特に高セキュリティシステムでは、パスワードを定期的に変更することをおすすめします。月次または週次での変更は、製品の保護をさらに強化します。
- すべてのパスワードおよびその他のセキュリティ設定の適切な設定は、サービスプロバイダーおよび/またはエンドユーザーの責任です。
- パスワードには、以下の文字を含めないでください：ユーザー名、123、admin（大文字小文字区別なし）、4つ以上の連続する増加または減少する数字、または4つ以上の連続する同じ文字。
- パスワードには、hik、hkws、hikvision（大文字小文字を区別しません）などの単語を含めないでください。

3. **「アクティベート」**をクリックしてください。

4. デバイスのIPアドレスを編集します。IPアドレスは、SADPツール、デバイス、およびクライアントソフトウェアから編集できます。

5.3 SADP経由でアクティベート

SADPは、LAN経由でデバイスのIPアドレスを検出、アクティベート、および変更するためのツールです。

開始前に

- 付属のディスクまたは公式ウェブサイト ***http://www.hikvision.com/en/*** からSADPソフトウェアを取得し、表示される指示に従ってSADPをインストールしてください。
- SADP ツールを実行するデバイスと PC は、同じサブネット内に配置する必要があります。

以下の手順は、デバイスのアクティベーションとIPアドレスの変更方法を示します。バッチアクティベーションおよびIPアドレスの変更については、*SADPのユーザーマニュアル*を参照してください。

手順

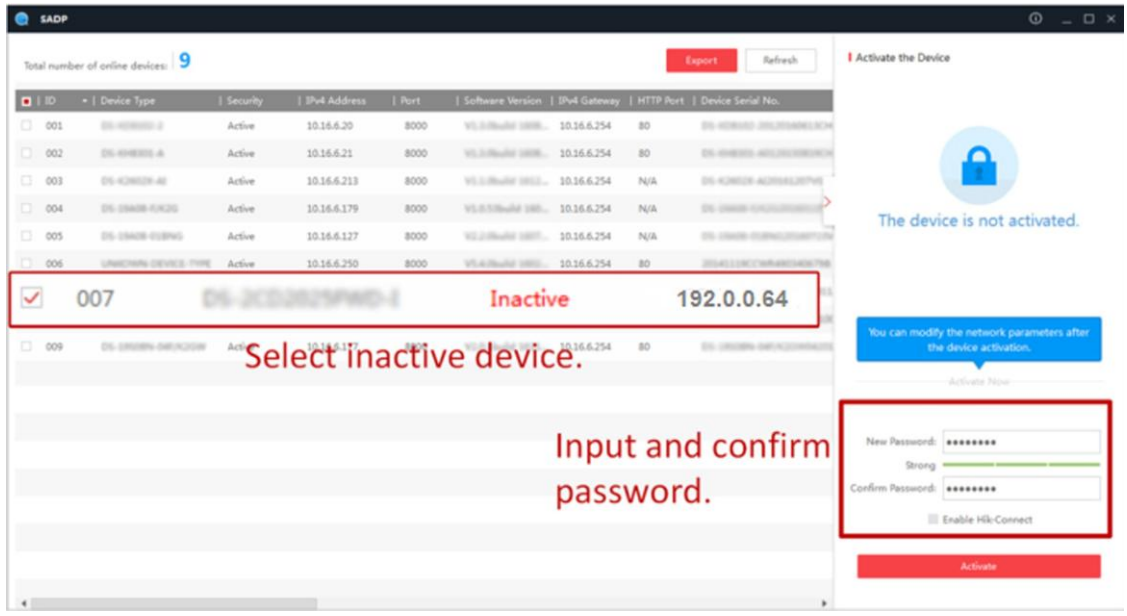
1. SADP ソフトウェアを実行し、オンラインデバイスを検索します。
2. オンラインデバイス一覧から対象のデバイスを検索し、選択します。
3. 新しいパスワード（管理者パスワード）を入力し、パスワードを確認します。

注意

強固なパスワードの使用を推奨します-製品のセキュリティを強化するため、ご自身で選択した強固なパスワード（大文字、小文字、数字、特殊文字をそれぞれ1つ以上含む8文字以上）を設定することを強く推奨します。また、特に高セキュリティシステムでは、パスワードを定期的に変更することを推奨します。月次または週次でのパスワード変更は、製品の保護をさらに強化します。

「admin」および「nimda」を含む文字は、アクティベーションパスワードとして設定できません。

4. **注意 ベート」**をクリックしてアクティベーションを開始してください。



アクティベーションが成功すると、デバイスのステータスが**「アクティブ」**になります。

5. デバイスのIPアドレスを変更します。
   1) デバイスを選択してください。
   2) デバイスのIPアドレスをコンピュータと同じサブネットに変更するには、IPアドレスを手動で変更するか、**DHCPを有効にするオプション**を選択してください。
   3) 管理者のパスワードを入力し、**「変更」**をクリックしてIPアドレスの変更を有効化します。

5.4 iVMS-4200 クライアント ソフトウェアを使用してデバイスを有効化

一部のデバイスでは、iVMS-4200 ソフトウェアに追加して正常に動作させる前に、パスワードを作成してアクティブ化する必要があります。

手順

注意
この機能はデバイスでサポートされている必要があります。

1. デバイス管理ページに移動します。
2. **デバイス管理**の右側にある「 」をクリックし、**デバイス**を選択します。
3. **「オンラインデバイス」**をクリックして、オンラインデバイス領域を表示します。検索されたオンラインデバイスがリストに表示されます。
4. **セキュリティ** レベル列に表示されるデバイス ステータスを確認し、非アクティブなデバイスを選択します。
5. **アクティベート**をクリックしてアクティベーション ダイアログを開きます。
6. パスワードフィールドにパスワードを入力し、パスワードを確認します。

注意

デバイスのパスワードの強度は自動的に確認できます。製品のセキュリティを強化するため、ご自身で選択したパスワード（8文字以上で、大文字、小文字、数字、特殊文字の少なくとも3種類を含む）に変更することを強くおすすめします。また、特に高セキュリティシステムでは、パスワードを定期的に変更することをおすすめします。月次または週次での変更は、製品の保護をさらに強化します。
すべてのパスワードおよびその他のセキュリティ設定の適切な設定は、インストール担当者および/またはエンドユーザーの責任です。

注意

「admin」および「nimda」を含む文字列は、アクティベーションパスワードとして設定できません。

7. **OK**をクリックしてデバイスをアクティベートします。

第6章 クイック操作

6.1 言語を選択

デバイスのシステム言語を選択できます。

デバイスのアクティベーション後、デバイスのシステム言語を選択できます。

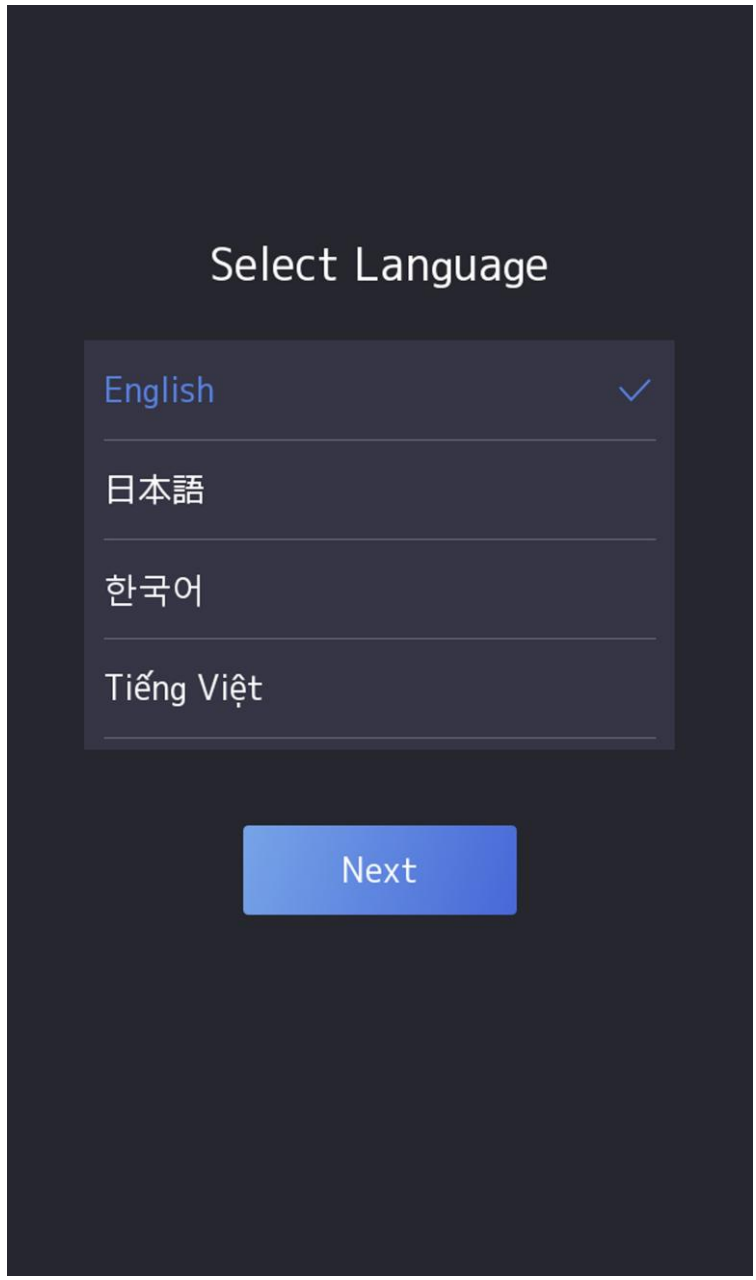


図6-1 システム言語の選択

デフォルトでは、システム言語は英語です。

注意
システム言語を変更すると、デバイスが自動的に再起動します。

6.2 パスワード変更タイプの設定

パスワードの変更タイプを「指定のメールアドレス」または「セキュリティ質問」から選択できます。デバイスパスワードを忘れた場合、選択した変更タイプ経由でパスワードを変更できます。

メールアドレス経由でパスワードを変更する

予約済みのメールアドレスでパスワードを変更する場合は、メールアドレスを入力し、**次へ**をタップしてください。

セキュリティ質問経由で変更

セキュリティ質問を使用してパスワードを変更する必要がある場合は、**画面右上の「セキュリティ質問に変更」**をタップしてください。

をタップしてください。セキュリティ質問を選択し、回答を入力してください。**次に「次へ」**をタップしてください。

注意

パスワードを変更する際は、1つのタイプのみを選択できます。必要に応じて、両方の変更タイプを設定するウェブページにアクセスしてください。

6.3 ネットワークパラメーターの設定

デバイスのネットワークを設定できます。

手順

注意

一部のデバイスモデルではWi-Fi機能が利用可能です。詳細については、実際のデバイスをご確認ください。

1. ネットワーク選択画面が表示されたら、実際のニーズに応じて「**有線ネットワーク**」または「**Wi-Fi**」をタップしてください。

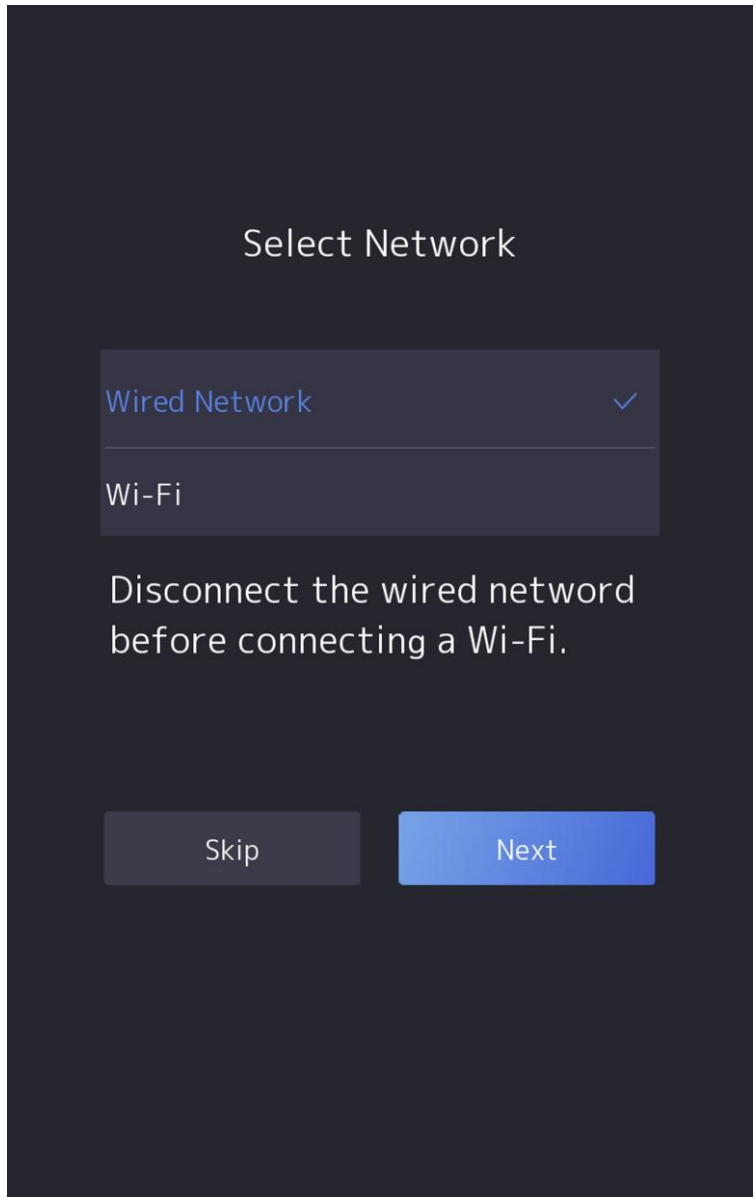


図6-2 ネットワーク選択

注
Wi-Fiに接続する前に、有線ネットワークを解除してください。

2. **「次へ」**をタップし
ます。**有線ネットワ**
ーク

注

デバイスがネットワークに接続されていることを確認してください。

DHCPを有効にすると、システムがIPアドレスその他のパラメーターを自動的に割り当てます。**DHCPを**無効にした場合は、IPアドレス、サブネットマスク、ゲートウェイを設定する必要があります。

Wi-Fi

Wi-Fiを選択し、Wi-Fiのパスワードを入力して接続します。

または「**Wi-Fiを追加**」をタップし、Wi-Fiの名前とパスワードを入力して接続します。

3. オプション：ネットワーク設定をスキップするには**「スキップ」**をタップします。

6.4 プラットフォームへのアクセス

機能を有効にすると、デバイスはHik-Connect経由で通信可能になります。デバイスをHik-Connectモバイルクライアントに追加するなど、さまざまな操作が可能です。

手順

1. Hik-Connectへのアクセスを有効にし、サーバーのIPアドレスと検証コードを設定します。

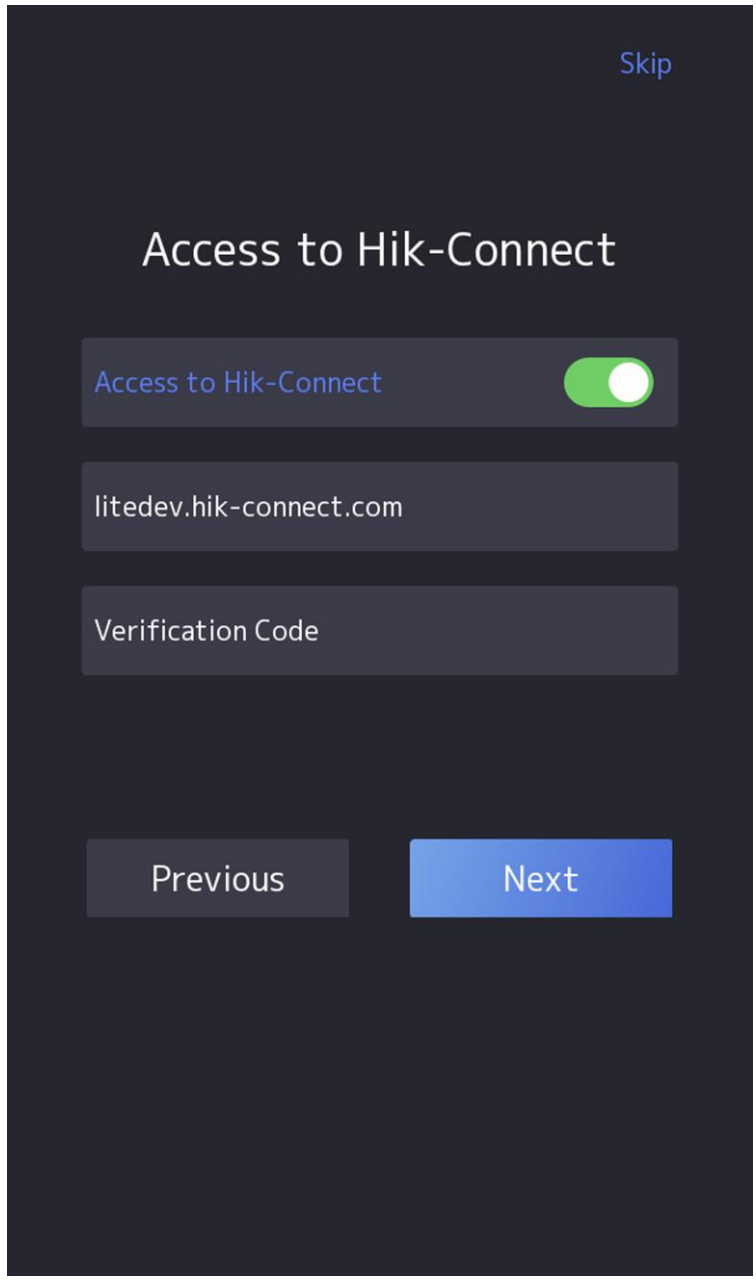


図6-3 Hik-Connectへのアクセス

2. **次へ**をタップします。
3. **オプション：スキップ**をタップしてこのステップをスキップします。
4. **オプション：**前のページに戻るには「前へ」をタップします。

注意

前の画面に戻ってWi-Fi設定画面に戻る場合は、接続済みのWi-Fiをタップするか、別のWi-Fiに接続してプラットフォーム画面に再アクセスする必要があります。

6.5 プライバシー設定

アクティベーション後、アプリケーションモードを選択し、ネットワークを選択した後は、プライバシー設定（画像のアップロードと保存を含む）を設定する必要があります。

実際のニーズに応じてパラメーターを選択してください。

認証時にキャプチャした画像をアップロード（認証時にキャプチャした画像をアップロード）

認証時に撮影した画像をプラットフォームに自動的にアップロードします。

認証時に撮影した画像を保存します。

この機能を有効にすると、デバイスへの認証時に画像を保存できます。

登録した画像を保存（登録した画像を保存）

この機能を有効にすると、登録された顔写真がシステムに保存されます。

画像のアップロード。リンクしたカメラで撮影後（リンクしたカメラで撮影後に画像のアップロード）

リンクされたカメラで撮影した画像をプラットフォームに自動的にアップロードします。

リンクキャプチャ後に画像を保存（リンクキャプチャ後に画像を保存）

この機能を有効にすると、リンクされたカメラで撮影した画像をデバイスに保存できます。

「次へ」をタップして設定を完了します。

6.6 管理者設定

デバイスをアクティベートした後、デバイスのパラメーターを管理するための管理者を追加できます。

開始前に

デバイスを起動し、アプリケーションモードを選択してください。

手順

1. **オプション:** 必要に応じて**「スキップ」**をタップして管理者追加を省略できます。
2. 管理者の名前（オプション）を入力し、**次へ**をタップします。

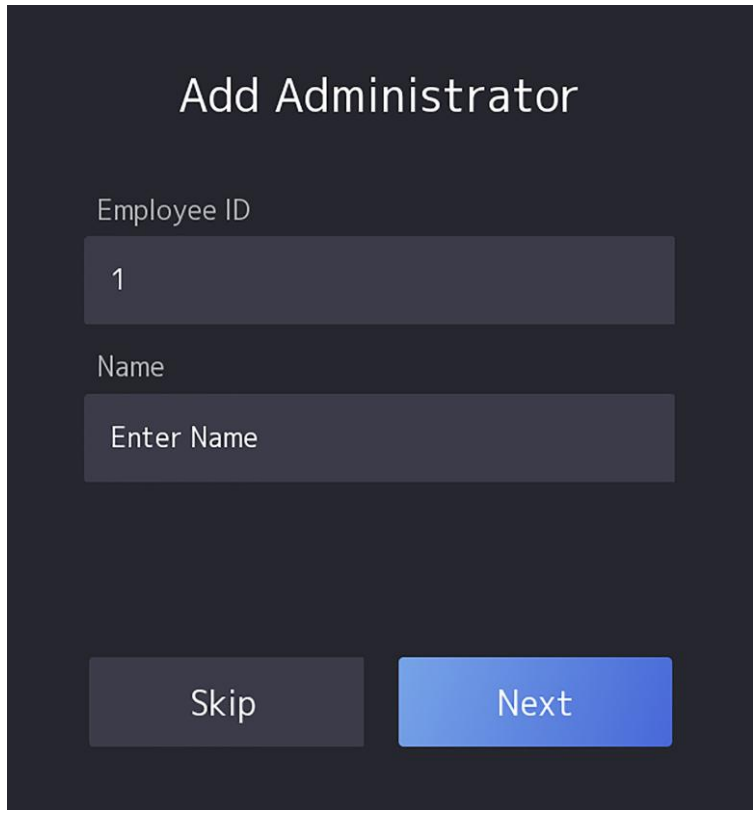


図6-4 管理者追加画面

3. 追加する認証情報を選択します。

注意

1つの認証情報のみを追加してください。

- :カメラに向かって正面を向いてください。顔認識領域内に顔が収まっていることを確認してください。 をクリックして撮影し、 をクリックして確認してください。
- : デバイス画面の指示に従って指を押し当ててください。 をクリックして確認してください。
- : カード番号を入力するか、カード提示エリアにカードをかざしてください。**OK**をクリックしてください。

注意

外部指紋モジュールに接続されたデバイスのみ、指紋機能に対応しています。

4. **OK**をクリックしてください。

認証ページが表示されます。

6.7 認証ページの手順

認証画面を表示します。

ステータスバーの指示

デバイスが武装状態/非武装状態です。

デバイスのWi-Fiは有効になっており、信号は強い/Wi-Fiは有効ですが接続されていません/Wi-FiのIPアドレスが衝突しています。

デバイスの有線ネットワークは接続されています/接続されていません/接続に失敗しました。

デバイスのモバイルネットワークに信号がありません/2Gの強い信号/3Gの強い信号/4Gの強い信号/5Gの強い信号。

デバイスがVoIPに追加されています/VoIPに追加されていません。

デバイスのSIPサーバーは登録済み/登録失敗/ドアステーションには登録済みですがメインステーションには登録されていません。

手のひら紋と手のひら静脈のモジュールはオンラインまたはオフラインです。

デュアル周波数カードモジュールはオンラインです。

認証ページアイコン

認証ページに表示されるアイコンは制御可能です。詳細については、*デバイス経由でショートカットキーを設定する際に*、*ショートカットキー*の設定を参照してください。

カメラにQRコードを表示し、QRコード経由で認証できます。

- 部屋番号を入力し、**OK**をタップして通話します。
- 「  」をタップしてセンターに連絡できます。

デバイスを中央に追加する必要があります。そうしないと、呼び出し操作が失敗します。

PINを入力して認証してください。

第7章 基本操作

7.1 ログイン

デバイスにログインして、デバイスの基本パラメーターを設定します。

7.1.1 管理者としてログイン

デバイスに管理者ユーザーを追加している場合、デバイス操作を行うためには管理者ユーザーのみがログイン可能です。

手順

1. 最初の画面を3秒間長押しし、ジェスチャーに従って左右にスワイプして管理ログイン画面に移動します。

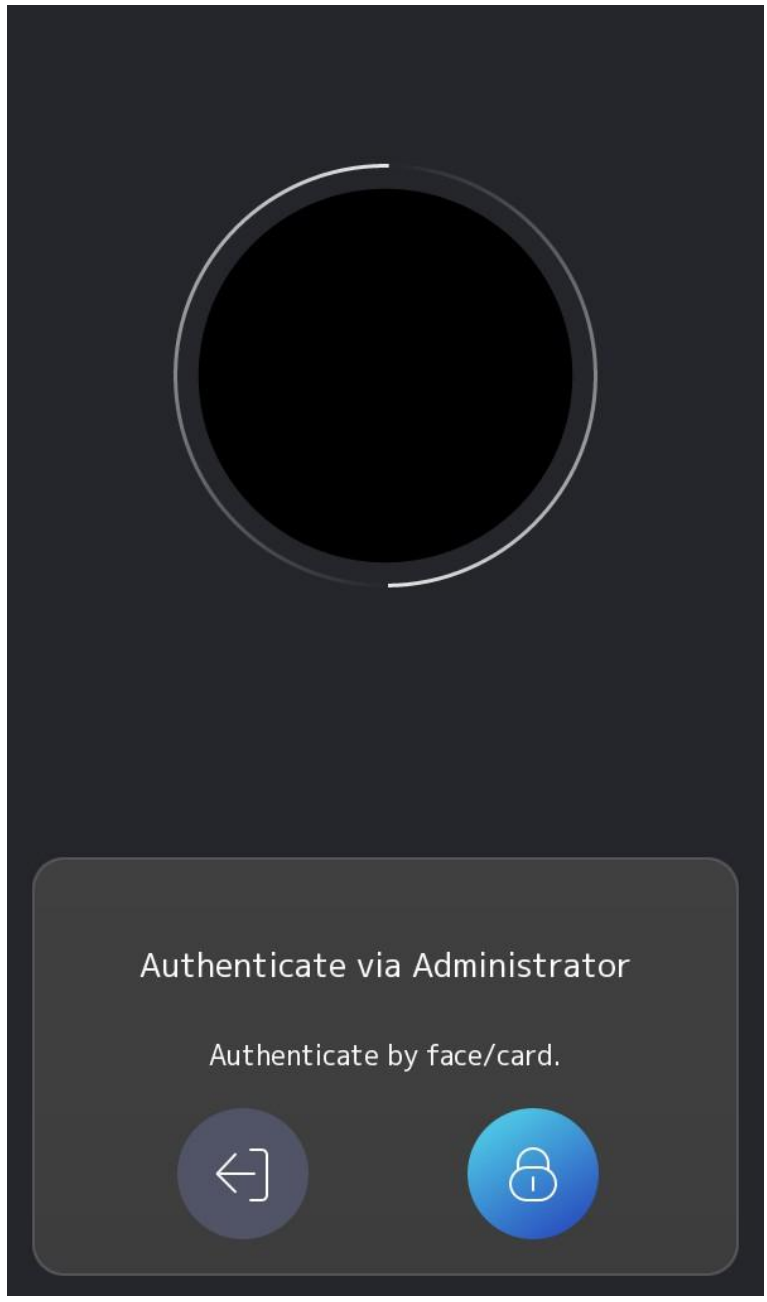


図7-1 管理者ログイン

2. 管理者の顔、指紋、またはカードで認証してホーム画面にアクセスします。

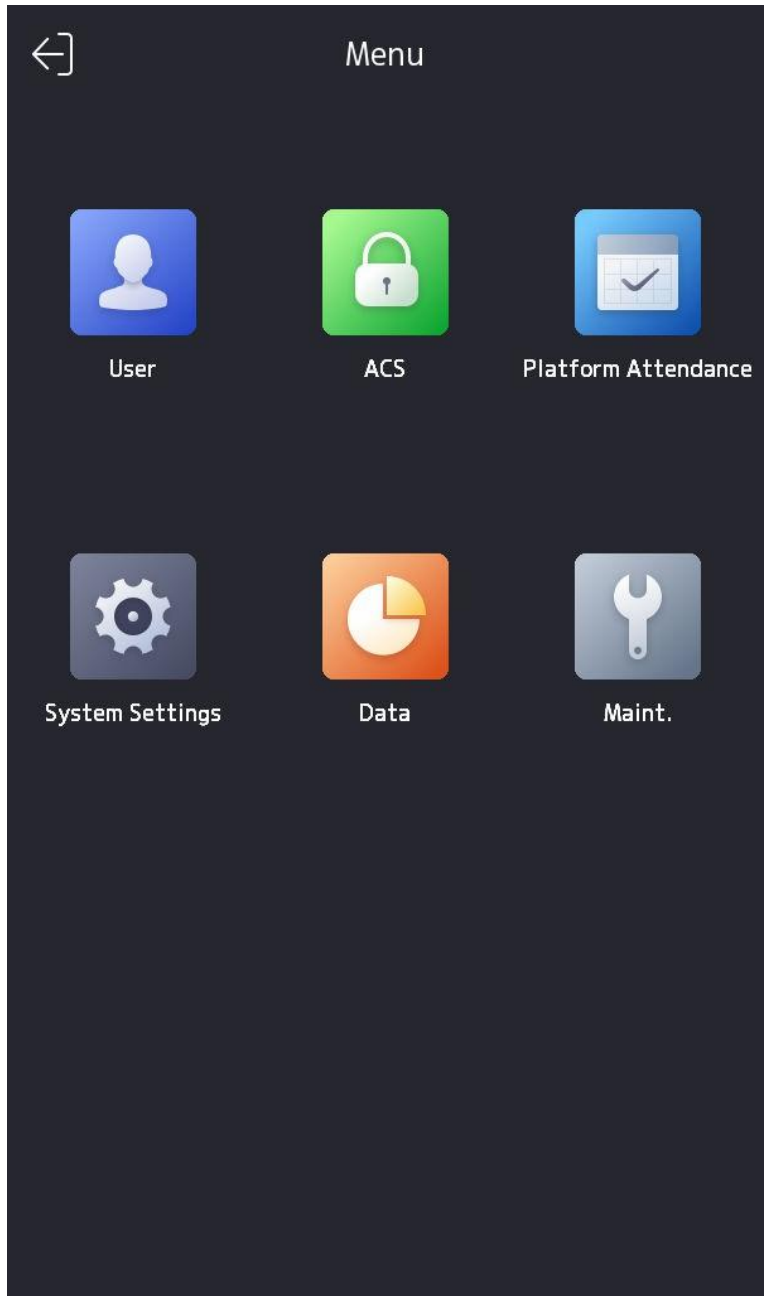


図7-2 ホーム画面

注
指紋またはカード認証に5回失敗すると、デバイスは30分間ロックされます。

3. **オプション:** タップ をタップすると、ログイン用のデバイスアクティベーションパスワードを入力できます。
4. **オプション :** をタップすると、管理ログインページから退出できます。

7.1.2 アクティベーションパスワードでログイン

他のデバイス操作を行う前に、システムにログインする必要があります。管理者アカウントを設定していない場合は、以下の手順に従ってログインしてください。

手順

1. 初期画面を3秒間長押しし、ジェスチャーに従って左右にスワイプしてパスワード入力画面に移動します。
2. パスワードを入力します。
   - デバイスに管理者ユーザーを追加している場合は、「  」をタップし、パスワードを入力してください。
   - デバイスに管理者ユーザーを追加していない場合は、パスワードを入力してください。
3. 「OK」をタップしてホーム画面に移動します。

注意

パスワードの入力が5回失敗すると、デバイスは30分間ロックされます。

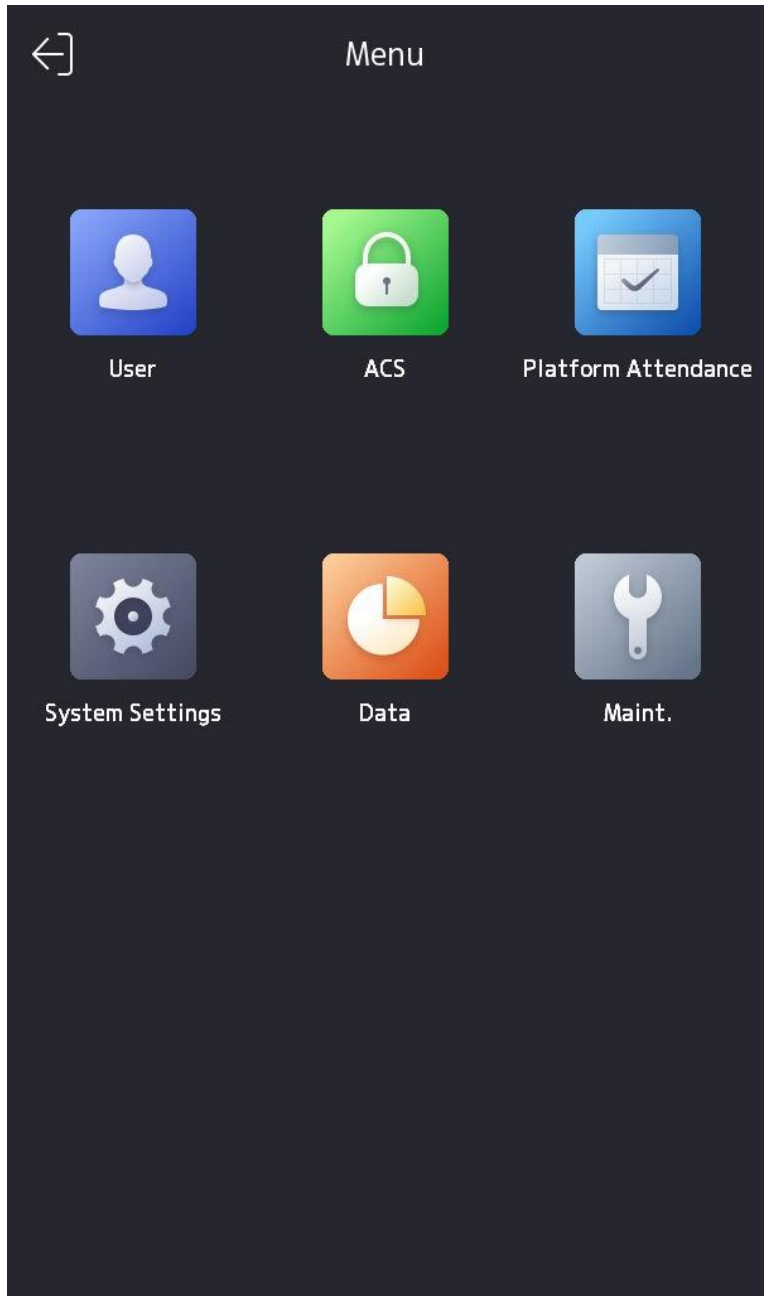


図7-3 ホーム画面

7.1.3 パスワードを忘れた

認証中にパスワードを忘れた場合、パスワードを変更できます。

手順

1. 初期画面を3秒間押し続け、ジェスチャーに従って左右にスワイプし、ログイン画面にアクセスしてください。
2. **オプション:** 管理者を設定している場合、ポップアップの管理者認証画面で「」をタップしてください。
3. **「パスワードを忘れた」**をタップします。
4. リストからパスワード変更の種類を選択してください。

   注意

   パスワード変更タイプを1つしか設定していない場合、対応するパスワード変更ページに移動し、さらに設定を行います。
5. セキュリティ質問に回答するか、メールアドレスに応じてパスワードを変更してください。
   - セキュリティ質問：アクティベーション時に設定したセキュリティ質問に回答してください。
   - メールアドレス

     注意

     デバイスがHik-Connectアカウントに追加されていることを確認してください。

     a. Hik-Connect アプリをダウンロードしてください。
     b. 「設定」→**「→」→「デバイスパスワードのリセット」**を選択してください。
     c. デバイスに表示されているQRコードをスキャンすると、検証コードが表示されます。

        注意

        QRコードをタップして大きな画像を表示します。
     d. デバイス画面に検証コードを入力してください。
6. 新しいパスワードを作成し、確認してください。
7. **OK**をタップしてください。

7.1.4 デバイスパスワードを変更する

デバイスパスワードを変更するには、古いパスワードを入力してください。

手順

1. 最初の画面を3秒間長押しし、ホーム画面にログインします。**「システム」→「→」→「パスワード」**をタップします。
2. **「デバイスパスワードの変更」**をタップします。
3. デバイスの古いパスワードを入力します。

   注意

   パスワードを忘れた場合は、**「パスワードを忘れた」を**タップしてパスワードを変更できます。詳細については、*「パスワードを忘れた」*を参照してください。
4. 新しいパスワードを入力し、パスワードを確認してください。

注意

デバイスのパスワードの強度は自動的に確認できます。製品のセキュリティを強化するため、ご自身で選択したパスワード（8文字以上で、大文字、小文字、数字、特殊文字の少なくとも3種類を含む）に変更することを強くおすすめします。また、特に高セキュリティシステムでは、パスワードを定期的に変更することをおすすめします。月次または週次での変更は、製品の保護をさらに強化します。
すべてのパスワードおよびその他のセキュリティ設定の適切な設定は、インストール担当者および/またはエンドユーザーの責任です。

5. **OK**をタップしてください。

7.2 通信設定

有線ネットワーク、Wi-Fi 設定、RS-485 パラメーター、Wiegand パラメーター、ISUP、および Hik-Connect へのアクセスを、通信設定ページで設定できます。

7.2.1 有線ネットワークパラメーターの設定

デバイスの有線ネットワークパラメーターを設定できます。これには、IPv4/IPv6 IPアドレス、サブネットマスク、ゲートウェイ、およびDNSパラメーターが含まれます。

手順

1. ホーム画面で「**システム**」→「**→**」→「**Comm.**（通信設定）」をタップして、通信設定ページに移動します。
2. 通信設定ページで「**有線ネットワーク**」をタップします。

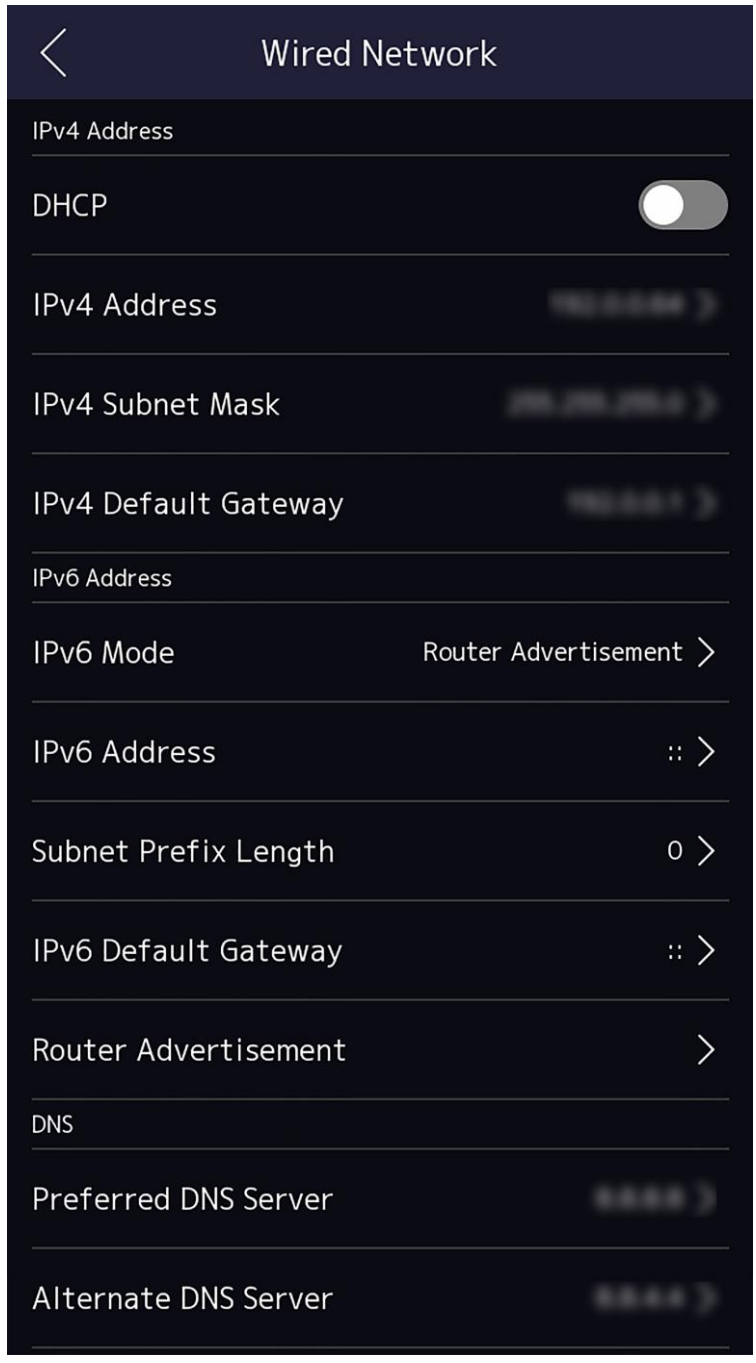


図7-4 有線ネットワーク設定

3. IPv4/IPv6 IPアドレス、サブネットマスク、およびゲートウェイを設定します。

- **DHCPを**有効にすると、システムがIPアドレス、サブネットマスク、およびゲートウェイを自動的に割り当てます。
- **DHCPを**無効にすると、IPアドレス、サブネットマスク、およびゲートウェイを手動で設定する必要があります。

注意

デバイスのIPアドレスとコンピュータのIPアドレスは、同じIPセグメント内に配置する必要があります。

4. DNSパラメーターを設定します。**自動取得DNSを**有効にしたり、優先DNSサーバーと代替DNSサーバーを設定できます。

7.2.2 Wi-Fi パラメーターを設定してください。

Wi-Fi機能を有効にし、Wi-Fi関連のパラメーターを設定できます。

手順

注意

この機能はデバイスでサポートされている必要があります。

1. ホーム画面で**「システム」→「→」→「Comm.**（通信設定）」をタップして、通信設定画面に移動します。
2. 通信設定画面で、をタップします。

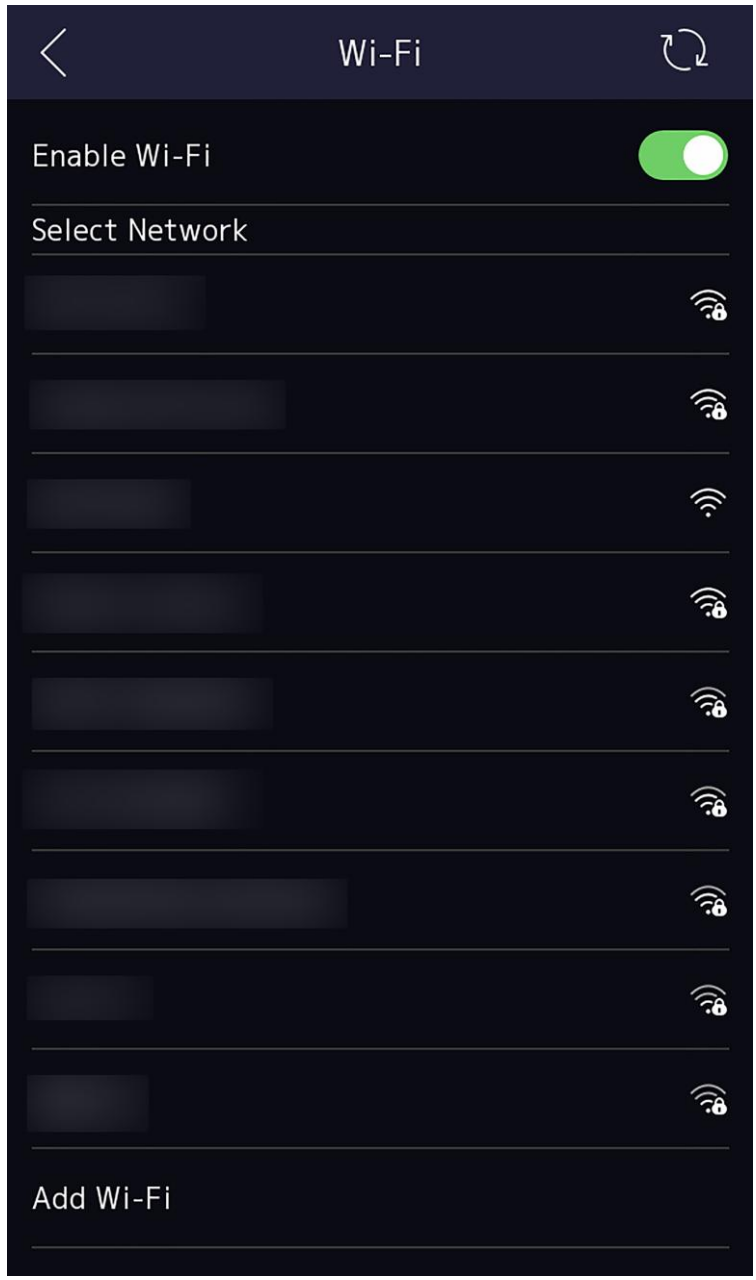


図7-5 Wi-Fi設定

3. Wi-Fi機能を有効にします。

4. Wi-Fi のパラメーターを設定します。

- リストからWi-Fiを選択し、Wi-Fiのパスワードを入力します。**OK**をタップします。
- ターゲットのWi-Fiがリストにない場合は、**「Wi-Fiを追加」**をタップします。Wi-Fiの名前とパスワードを入力し、**OK**をタップします。

注意

パスワードには数字、英字、特殊文字のみ使用可能です。

5. Wi-Fi の設定を指定します。
   - デフォルトではDHCPが有効になっています。システムがIPアドレス、サブネットマスク、ゲートウェイを自動的に割り当てます。
   - DHCPを無効にした場合、IPアドレス、サブネットマスク、およびゲートウェイを手動で入力する必要があります。
6. 「**OK**」をタップして設定を保存し、Wi-Fi タブに戻ります。
7. 「✓」をタップしてネットワークパラメーターを保存します。

7.2.3 RS-485 パラメーターを設定します

顔認識端末は、RS-485 端子経由で外部アクセスコントローラー、セキュアドアコントロールユニット、カードリーダー、または QR コードスキャナーと接続できます。

手順

1. ホーム画面で「**システム**」→「→」→「**Comm.**（通信設定）」をタップして、通信設定画面に移動します。
2. 通信設定画面で「**RS-485**」をタップして、RS-485 タブに移動します。

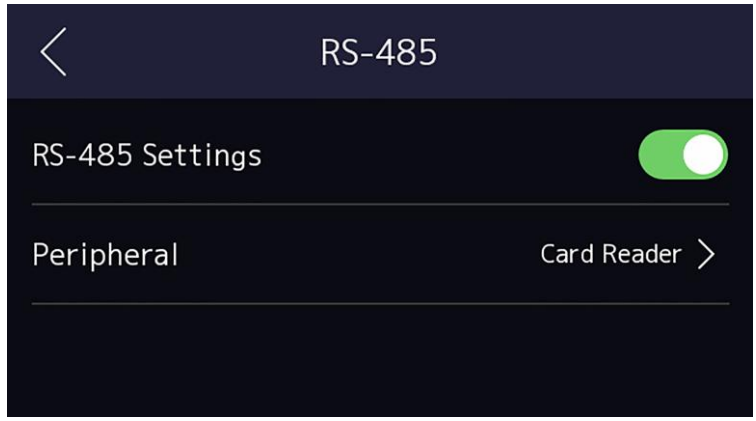


図7-6 RS-485パラメーターの設定

3. 実際のニーズに応じて、適切な周辺機器の種類を選択してください。

注意

アクセスコントローラーを選択した場合：RS-485インターフェース経由でデバイスをターミナルに接続する場合、RS-485アドレスを2に設定してください。コントローラーに接続する場合、ドア番号に応じてRS-485アドレスを設定してください。

4. 左上隅のバックアイコンをタップし、パラメーターを変更した場合はデバイスを再起動してください。

7.2.4 Wiegand パラメーターを設定

Wiegandの送信方向を設定できます。

手順

1. ホーム画面で「**システム→ 通信**（通信設定）」をタップして、通信設定画面に移動します。
2. 通信設定画面で「**Wiegand**」をタップして、Wiegand タブに移動します。
3. Wiegand機能を有効にします。
4. 送信方向を選択します。
   - 出力：顔認識端末は外部アクセスコントローラーに接続できます。2つのデバイスはWiegand 34経由でカード番号を送信します。
   - 入力：顔認識端末はWiegandカードリーダーに接続できます。
5. 「✓」をタップしてネットワークパラメーターを保存します。

注意

外部デバイスを変更した場合、デバイスパラメーターを保存後にデバイスが自動的に再起動します。

7.2.5 ISUPパラメーターを設定します。

ISUPパラメーターを設定すると、デバイスはISUPプロトコル経由でデータをアップロードできます。

開始前に

デバイスがネットワークに接続されていることを確認してください。

手順

1. ホーム画面で「**システム**」→「**→**」→「**Comm.**」→「**→**」→「**ISUP**（通信設定）」をタップして設定画面に移動します。

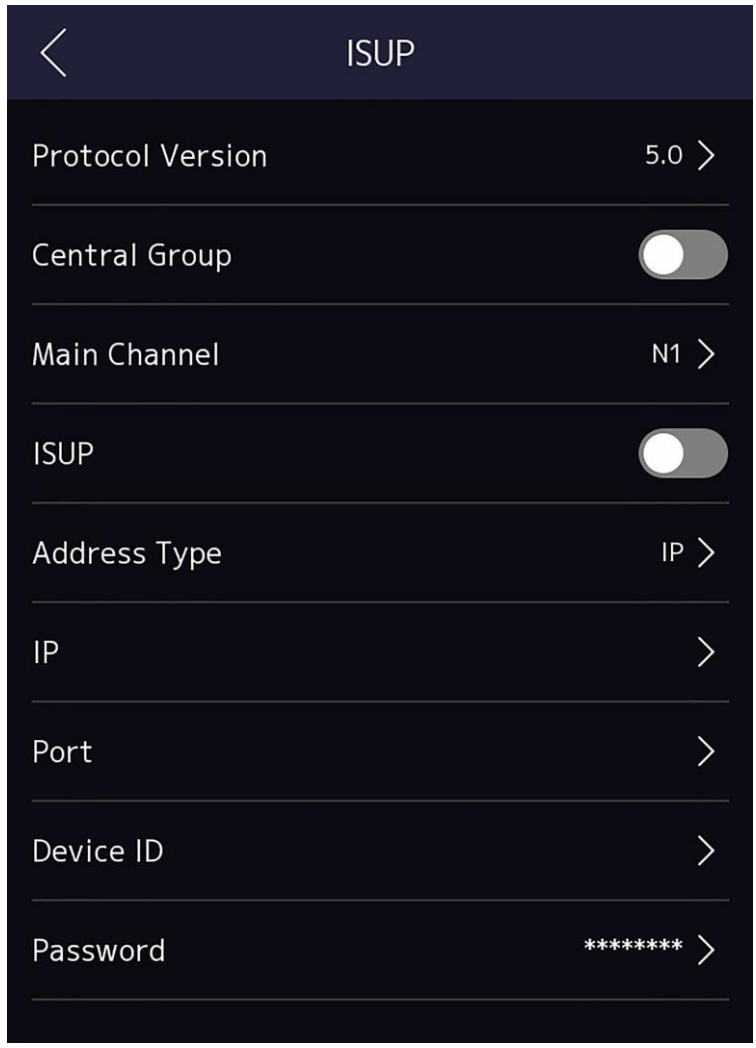


図7-7 ISUP設定

2. ISUP機能を有効にし、ISUPサーバーパラメーターを設定します。

ISUP バージョン

実際の要件に応じてISUPバージョンを設定します。

中央グループ

中央グループを有効にすると、データが中央グループにアップロードされます。

メイン チャネル

N1またはなしをサポートします。

ISUP

ISUP機能を有効にすると、データはISUPプロトコル経由でアップロードされます。

アドレス タイプ

実際の要件に応じてアドレスタイプを選択してください。

IPアドレス

ISUPサーバーのIPアドレスを設定してください。

ポート番号

ISUPサーバーのポート番号を設定してください。

注

ポート番号の範囲: 0 から 65535。

デバイスID

デバイス シリアル番号を設定します。

パスワード

V5.0を選択した場合、アカウントとISUPキーを作成する必要があります。他のバージョンを選択した場合、ISUPアカウントのみを作成する必要があります。

注意

- ISUPアカウントとISUPキーを必ず覚えておいてください。デバイスがISUPプロトコル経由で他のプラットフォームと通信する際は、アカウント名またはキーを入力する必要があります。
- ISUP キーの範囲: 8 文字から 32 文字。

7.2.6 プラットフォームアクセス

デバイスをHik-Connectモバイルクライアントに追加する前に、デバイス検証コードを変更し、サーバーアドレスを設定できます。

開始前に

デバイスがネットワークに接続されていることを確認してください。

手順

1. ホーム画面で**「システム」→「→」→「Comm.**（通信設定）」をタップして、通信設定画面に移動します。
2. 通信設定画面で、**Hik-Connectへのアクセスを**タップします。
3. **Hik-Connectへのアクセスを**有効にします。
4. **サーバーIP**を入力します。
5. **検証コード**を作成し、**Hik-Connect経由で**デバイスを管理する際にはこの検証コードを入力する必要があります。

7.3 ユーザー管理

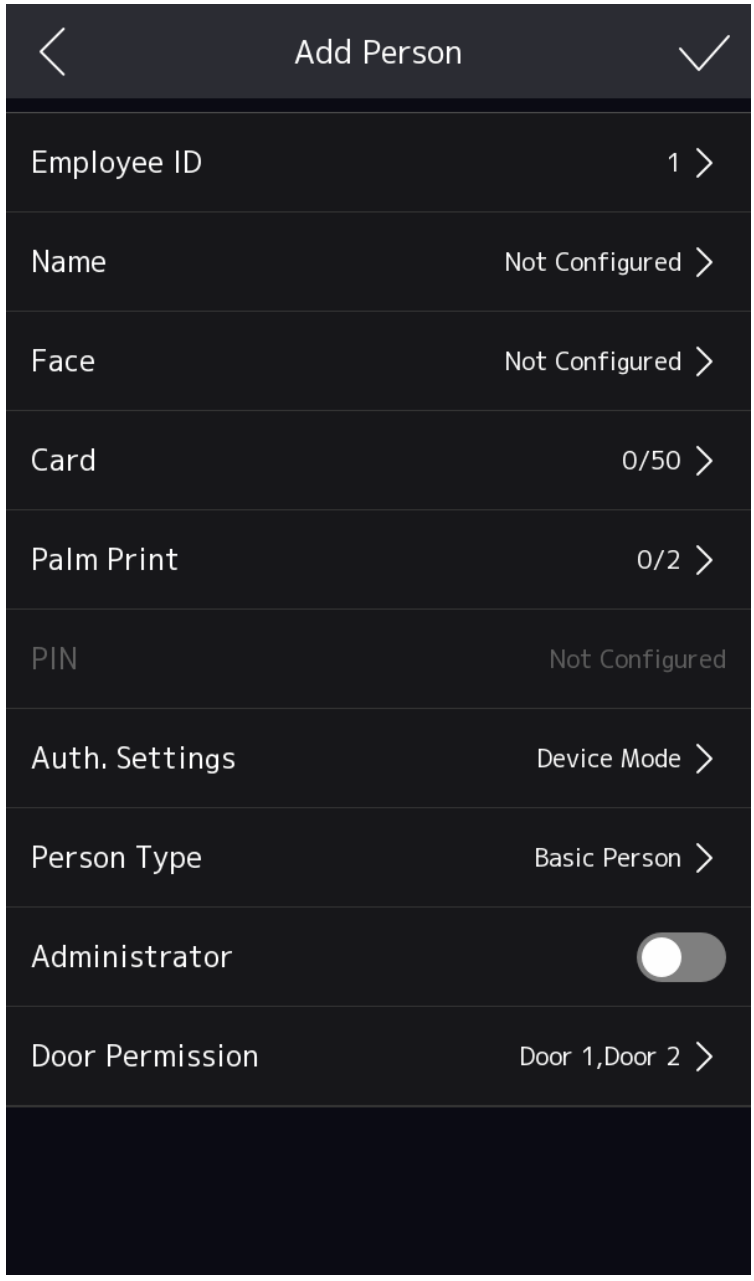
ユーザー管理画面では、ユーザーの追加、編集、削除、検索が可能です。

7.3.1 管理者追加

管理者はデバイスバックエンドにログインし、デバイスのパラメーターを設定できます。

手順

1. 初期画面を3秒間長押しし、ジェスチャーに従って左右にスワイプしてデバイスのバックエンドにアクセスします。
2. **「Person」**をタップします。**「→」をタップします。「+」**をタップして「Add Person」ページに入ります。



3. 従業員IDを編集します。

注意

- 従業員IDは32文字未満でなければなりません。小文字、大文字、数字の組み合わせが可能です。
- 従業員IDは重複してはいけません。

4. 名前フィールドをタップし、ソフトキーボードに人物の名前を入力してください。

注意

- 名前には数字、大文字、小文字、および特殊文字を使用できます。
- 名前には最大32文字まで入力可能です。

5. オプション：管理者用に顔写真、指紋、カード、PIN、手のひら紋、キーフォブを追加できます。

注

- 顔写真の追加方法の詳細については、*「顔写真の追加」*を参照してください。
- 指紋を追加する方法の詳細については、「*指紋の追加」*を参照してください。
- カードを追加する方法については、*「カードを追加」*を参照してください。
- パスワードの追加に関する詳細については、「***PIN コードの表示」***を参照してください。
- キーフォブを追加する方法の詳細については、「*キーフォブを追加」*を参照してください。
- 手のひら認証を追加する方法については、をご覧ください。

6. オプション：管理者の認証タイプを設定します。

注意

認証タイプの設定に関する詳細については、「*認証モードの設定*」を参照してください。

7. 管理者権限機能を有効にします。

管理者権限を有効にする

その人は管理者権限を持っています。通常の出席機能を除き、その人は認証後にホーム画面にアクセスして操作を行うことができます。

8. ドアの権限を設定します。

9. 「✓」をタップして設定を保存します。

7.3.2 デバイス経由で顔と人物データを一括でインポート/エクスポート

USBフラッシュドライブを使用して、デバイスAからデバイスBにデータをインポートできます。

開始前に

- デバイスA（データをエクスポートするデバイス）にログインします。詳細については、*ログイン*を参照してください。
- デバイスAにUSBフラッシュドライブを挿入してください。

注意

- 対応しているUSBフラッシュドライブのファイルシステムはFAT32またはexFATです。
- システムは、1GBから256GBのストレージ容量を持つUSBフラッシュドライブに対応しています。USBフラッシュドライブの空き容量が512MB以上であることを確認してください。

手順

1. デバイスAのメニューで**「データ」**をタップし、データページに移動します。

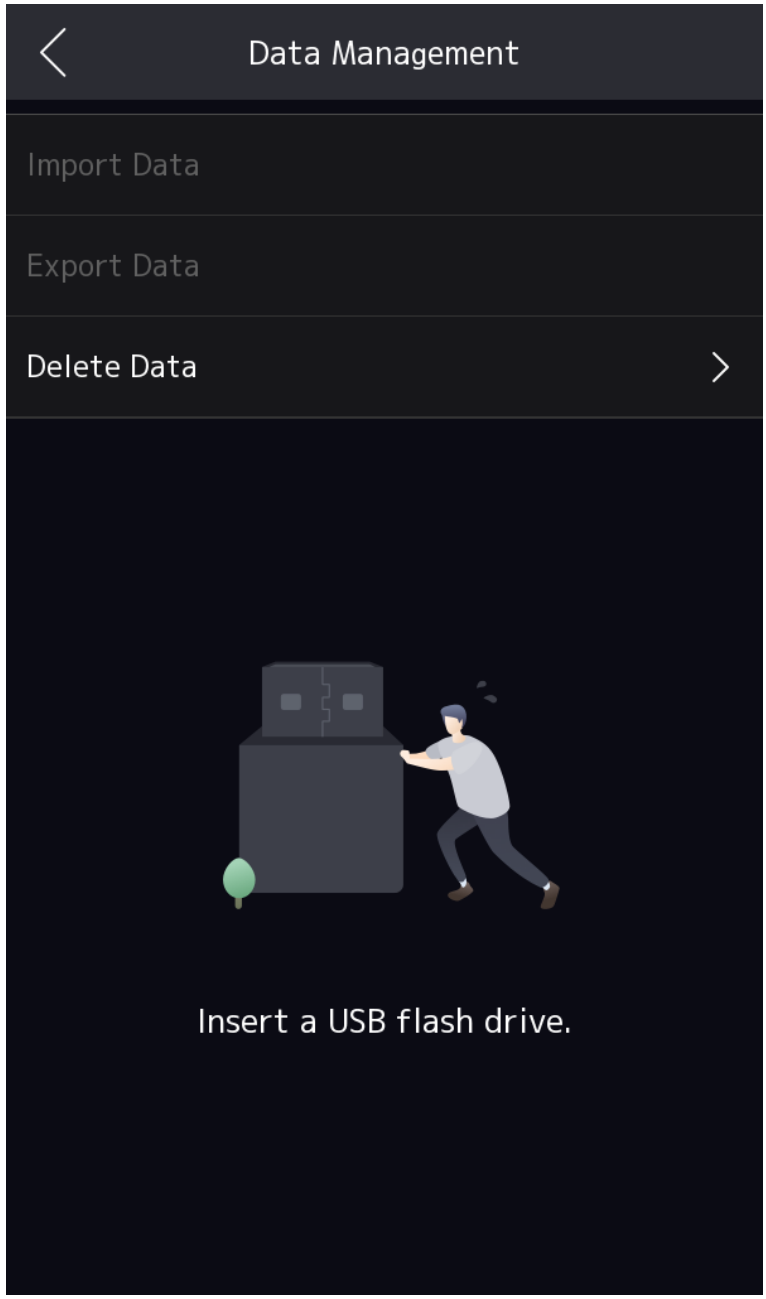


図7-8 データ管理ページ

2. データ管理画面で**「データエクスポート」**をタップします。

3. **「個人データ」**または**「顔データ」**を選択します。

4. **オプション:** データエクスポート用のパスワードを設定します。別のデバイスにデータをインポートする際は、このパスワードを入力する必要があります。

注意
- パスワードは空にできません。パスワードを設定しない場合、エクスポートしたデータをPCで閲覧できます。
- パスワードを設定した場合、PCでエクスポートしたデータを閲覧できません。
- エクスポートされた個人データはDBファイルであり、編集できません。

5. 顔と人物のデータをインポートする必要があるデバイスBにUSBフラッシュドライブを挿入してください。

注意
2つのデバイスが同じデバイスタイプであることを確認してください。

6. デバイスBのメニューで**「データ」**をタップし、データ画面に移動します。

7. **「データインポート」**をタップします。

8. **「個人データ」**または**「顔データ」**を選択します。

9. データをエクスポートした際に作成したパスワードを入力します。データをエクスポートした際にパスワードを作成していない場合は、入力欄を空白のままにし、**OK**をタップします。データはUSBフラッシュドライブからインポートされます。

注意
- 手動で画像をインポートする必要がある場合は、USBフラッシュドライブのルートディレクトリ（enroll_pic）に画像を保存してください。画像のファイル名は以下のルールに従ってください：カード番号_名前_部署_従業員ID_性別.jpg 性別は、3が男性、6が女性、0が不明を表します。従業員IDは32文字未満である必要があります。名前は20文字未満、カード番号は20文字未満である必要があります。
- Enroll_picフォルダーには最大10,000枚の画像を保存できます。Enroll_picフォルダーにすべての画像を保存できない場合は、ルートディレクトリ下にenroll_pic1、enroll_pic2、enroll_pic3、enroll_pic4という名前のフォルダーを最大10個作成できます。画像のファイル名は画像の命名規則に従ってください。
- 顔写真の要件は以下のルールに従う必要があります：顔全体が正面を向いてカメラを直接見ている状態で撮影してください。顔写真撮影時には帽子や頭巾を着用しないでください。形式はJPEGまたはJPGです。解像度は640× 480ピクセル以上でなければなりません。画像サイズは60KBから200KBの間でなければなりません。

7.3.3 顔写真を追加

デバイスの顔写真を追加します。その人は顔写真を使用して認証を行うことができます。

手順

1. 最初の画面を3秒間長押しし、ジェスチャーに従って左右にスワイプし、バックエンドにログインします。

2. 「**Person**」をタップし、「**→**」→「**+**」をタップして「Add Person」ページに移動します。

3. 従業員IDを編集します。

注意

- 従業員IDは32文字未満である必要があります。また、小文字、大文字、および数字の組み合わせで構成できます。
- 従業員IDは重複してはいけません。

4. 名前フィールドをタップし、ソフトキーボードで人物の名前を入力してください。

注意

- 氏名には、数字、大文字、小文字、および特殊文字を使用できます。
- 提案される名前は32文字以内である必要があります。

5. 顔写真フィールドをタップして、顔写真追加ページに移動します。

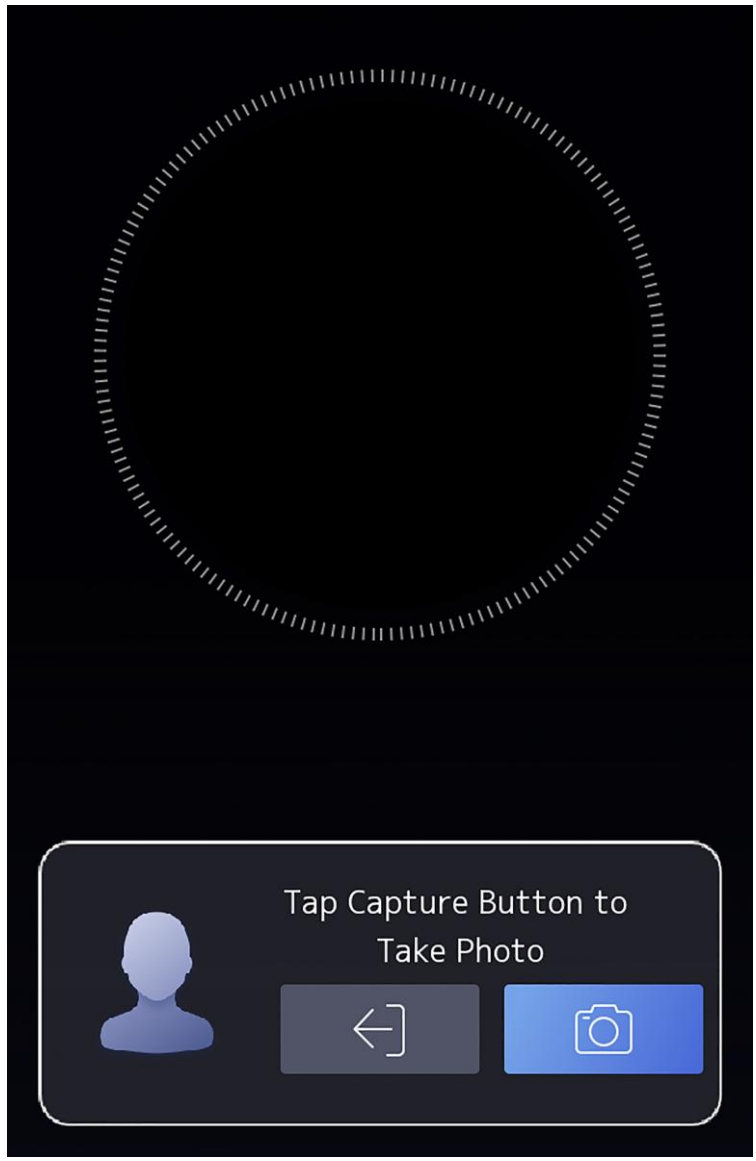


図7-9 顔写真を追加

6. カメラを見てください。

注意

- 顔写真を追加する際は、顔写真が顔写真の枠内に収まっていることを確認してください。
- 撮影した顔写真が良好な品質で正確であることを確認してください。
- 顔写真を追加する際の詳しい手順については、*「顔写真の収集/比較時のヒント」*をご確認ください。

顔写真を完全に追加すると、ページの右上隅に撮影した顔写真が表示されます。

7. **「保存」**をタップして顔写真を保存します。

8. **オプション：[もう一度試す]** をタップし、顔の位置を調整して顔写真を再度追加できます。

9. 人物の種類を設定します。

基本人物

この人物は通常のユーザーです。この人物は初期画面での認証または出席確認のみが可能です。管理者機能を有効にすることで、基本人物を**管理者として設定**することもできます。

訪問者

人物は訪問者です。

ブロックリストの人物

このユーザーはブロックリストに登録されています。ユーザーが認証を開始すると、イベントがアップロードされます。

カスタムタイプ

カスタムのユーザータイプを設定します。

10. 「✓」をタップして設定を保存します。

7.3.4 カードを追加

人物にカードを追加し、その人物は追加されたカードで認証できます。

手順

注意

各ユーザーは最大50枚のカードを追加できます。

1. 最初の画面を3秒間長押しし、ジェスチャーに従って左右にスワイプし、バックエンドにログインします。

2. **「人」**をタップし、**→+** にアクセスして「人追加ページ」に移動します。

3. 外部カードリーダーを配線図に従って接続してください。

4. 従業員IDフィールドをタップし、従業員IDを編集します。

注意

- 従業員IDは32文字未満である必要があります。また、小文字、大文字、数字の組み合わせが可能です。
- 従業員IDは重複してはいけません。

5. 名前フィールドをタップし、ソフトキーボードで人物の名前を入力してください。

注意

- 氏名には、数字、大文字、小文字、および特殊文字を使用できます。
- 提案する名前は32文字以内にしてください。

6. カードフィールドをタップし、**[+]** をタップします。

7. カード番号を設定してください。
- カード番号を手動で入力してください。
- カード提示エリアにカードを提示してカード番号を取得します。

注意
- カード番号は空欄にできません。
- カード番号には最大20文字まで入力可能です。
- カード番号は重複できません。

8. カードの種類を設定してください。
9. 「✓」をタップして設定を保存してください。

7.3.5 指紋を追加してください。

指紋を登録すると、その人は登録された指紋で認証できます。

手順

注意
この機能はデバイスでサポートされている必要があります。

1. 最初の画面を3秒間長押しし、ジェスチャーに従って左右にスワイプし、デバイスのバックエンドにアクセスします。
2. **「Person」**をタップし、次に**「→」をタップし、さらに「+」**をタップして「Add Person」ページに移動します。
3. 「従業員ID」フィールドをタップし、従業員IDを編集します。

注意
- 従業員IDは32文字未満である必要があります。また、小文字、大文字、および数字の組み合わせで構成できます。
- 従業員IDは0で始まってはならず、重複してはなりません。

4. 名前フィールドをタップし、ソフトキーボードに氏名を入力してください。

注意
- 氏名には、数字、大文字、小文字、および特殊文字を使用できます。
- 提案される人物名は32文字以内である必要があります。

5. 指紋フィールドをタップして、指紋を追加する画面を表示します。
6. 指示に従って指紋を追加してください。

注意
- 同じ指紋を繰り返し追加することはできません。
- 1人につき最大10つの指紋を追加できます。
- クライアントソフトウェアまたは指紋レコーダーを使用して指紋を登録することもできます。

指紋のスキャン方法の詳細については、*「指紋スキャンのヒント」*を参照してください。

7. タッチ をタップして設定を保存します。

7.3.6 PINコードを表示

PINコードをユーザーに設定し、ユーザーはPINコードで認証できます。

手順

1. 最初の画面を3秒間長押しし、ジェスチャーに従って左右にスワイプし、バックエンドにログインします。

2. **「Person」**をタップします。**「→」をタップします。「+」**をタップして「Add Person」ページに移動します。

3. 「従業員ID」フィールドをタップし、従業員IDを編集します。

注意

- 従業員IDは32文字未満である必要があります。また、小文字、大文字、および数字の組み合わせで構成できます。
- 従業員IDは重複してはいけません。

4. 名前フィールドをタップし、ソフトキーボードで人物の名前を入力してください。

注意

- 氏名には、数字、大文字、小文字、および特殊文字を使用できます。
- 提案される人物名は32文字以内である必要があります。

5. PINコードをタップしてPINコードを表示します。

注意

PINコードは編集できません。PINコードはプラットフォームによってのみ設定可能です。

6. タッチ をタップして設定を保存してください。

7.3.7 キーフォブを追加

ユーザー用にキーフォブを追加します。

手順

注意

- この機能はデバイスでサポートされている必要があります。
- 各ユーザーは最大1つのキーフォブを追加でき、デバイスは最大5,000個のキーフォブを追加できます。

1. 最初の画面を3秒間長押しし、ジェスチャーに従って左右にスワイプしてデバイスのバックエンドにアクセスします。

2. **「ユーザー」**をタップします。**「→」をタップし、+**にアクセスして「ユーザーを追加」ページに移動します。

3. 「従業員ID」フィールドをタップし、従業員IDを編集します。

注意

- 従業員IDは32文字未満でなければなりません。また、小文字、大文字、数字の組み合わせが可能です。
- 従業員IDは0で始まってはならず、重複してはなりません。

4. 名前フィールドをタップし、ソフトキーボードにユーザー名を入力してください。

注意

- ユーザー名には、数字、大文字、小文字、および特殊文字を使用できます。
- 提案されるユーザー名は32文字以内である必要があります。

5. **キーフォブ**をタップし、**+**をタップし、**キーフォブ** シリアル番号を入力し、**OK を**タップします。キーフォブの左上と右下の角のキーを10秒間長押しして、顔認識端末とペアリングします。

注意
キーフォブのシリアル番号は、QからZまでの文字で始まり、その後8桁の数字が続きます。

6. タップ をタップして設定を保存します。

7.3.8 手のひら紋と手のひら静脈を追加

対象者の手のひらを登録し、登録された手のひらで認証が可能です。

手順

注意

- この機能はデバイスでサポートされている必要があります。
- 最大10,000件の手のひらパターンと手のひら静脈を追加できます。

1. 最初の画面を3秒間長押しし、ジェスチャーに従って左右にスワイプしてデバイスのバックエンドにアクセスします。
2. **「Person」**をタップします。**「→」をタップします。「+」**をタップして「Add Person」ページに移動します。
3. 「従業員ID」フィールドをタップし、従業員IDを編集します。

注意

- 従業員IDは32文字未満でなければなりません。小文字、大文字、数字の組み合わせが可能です。
- 従業員IDは0で始まってはならず、重複してはなりません。

4. 名前フィールドをタップし、ソフトキーボードに人物の名前を入力してください。

注意

- 名前には、数字、大文字、小文字、および特殊文字を使用できます。
- 提案される人物名は32文字以内である必要があります。

5. 「**Palm Print**」をタップし、次に「**+**」をタップして追加ページに移動します。
6. デバイスの周辺モジュールから5~ 12cmの距離に手のひらを置きます。
7. 「✓」をタップして設定を保存します。

7.3.9 デバイスの設定でユーザータイプを設定

人物タイプを「基本人物」「訪問者」「ブロックリストに追加された人物」または「カスタム人物タイプ」から選択します。

開始前に

デバイスにログインします。詳細については、*「ログイン」*を参照してください。

手順

1. 「**Person**」をタップし、→「**+**」をタップします。

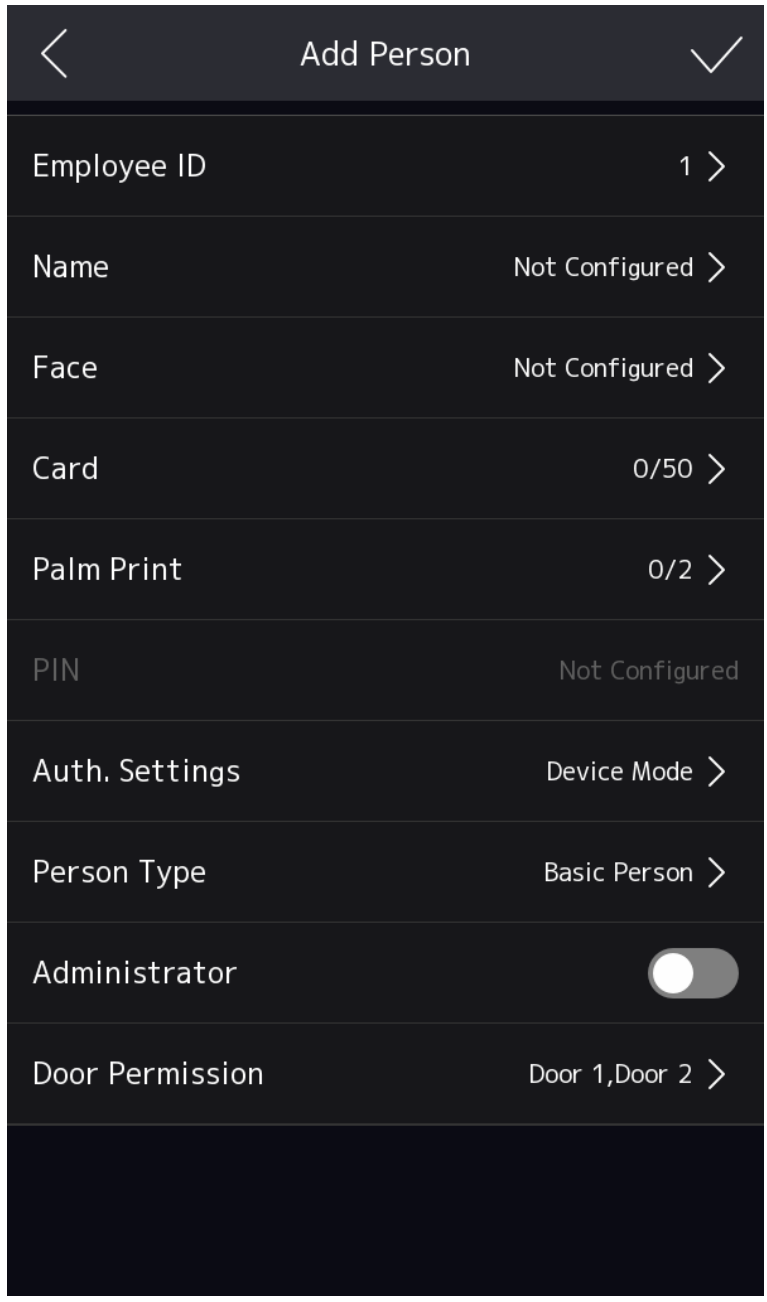


図7-10 人を追加

2. **従業員ID**をタップすると、従業員IDを編集できます。

注意

従業員IDは32文字を超えてはいけません。大文字、小文字、数字の組み合わせが可能です。

3. **名前**をタップし、名前を作成します。ポップアップキーボードに従って、その人の名前を入力します。

注意

- 名前には数字、大文字、小文字、および特殊文字が含まれます。
- 名前は128文字以内にしてください。

4. 顔、カード、指紋、手のひら紋を設定します。

注意

- 「***顔写真を追加***」「***カードを登録***」「***指紋を登録***」を指し、顔、カード、指紋、手のひら紋を追加することを意味します。
- 指紋または手のひらモジュールを搭載したデバイスのみ、指紋または手のひら機能に対応しています。

5. **「人物タイプ」**をタップし、タイプを「**基本人物**」「**訪問者**」「**ブロックリスト内の人物**」または**「カスタムタイプ」**に設定します。

注意

- 「訪問者」に設定した場合、管理者を設定できません。「ブロックリスト内のユーザー」に設定した場合、ドアの権限を設定できません。
- カスタムタイプの名前はPCウェブで設定する必要があります。カスタムタイプに名前を付けた後、デバイス上のカスタムタイプは名前が変更されます。詳細な設定については、***Person Management*** をご参照ください。

6. タップ をタップして設定を保存します。

7.3.10 認証モードを設定する

顔写真、パスワード、またはその他の認証情報を追加した後、認証モードを設定する必要があります。その後、ユーザーは設定された認証モードを通じて自身の身分を認証できます。

手順

1. 最初の画面を3秒間長押しし、ジェスチャーに従って左右にスワイプし、バックエンドにログインします。

2. **「Person」**をタップし、→ **「Add Person/Edit Person」**をタップし、→ **「Authentication Mode」**をタップします。

3. 認証モードとして「デバイス」または「カスタム」を選択します。

デバイス

デバイスモードを選択するには、まずアクセス制御設定ページでターミナル認証モードを設定する必要があります。詳細については「*アクセス制御パラメーターの設定*」を参照してください。

カスタム

実際のニーズに応じて、異なる認証モードを組み合わせて使用できます。

4. 「 」をタップして設定を保存します。

7.3.11 人物の検索と編集

ユーザーを追加した後、ユーザーを検索して編集できます。

人物の検索

「人員管理」ページで、検索領域をタップして「検索対象者」ページに移動します。ページ左側の「**カード**」をタップし、ドロップダウンリストから検索タイプを選択します。検索対象の従業員ID、カード番号、または名前を入力します。検索するには「 」をタップします。

人物の編集

「人物管理」ページで、人物リストから人物を選択して「人物編集」ページに移動します。***人物管理***の手順に従って人物のパラメーターを編集します。設定を保存するには「 」をタップします。

注意
IDは編集できません。

7.3.12 デバイス経由で人物のドアアクセス権限を設定

通常の人または訪問者のドア通過権限を設定します。

開始前に

デバイスにログインしてください。詳細については、***ログイン***を参照してください。

手順

1. 「**Person**」をタップし、→「**+**」を選択します。

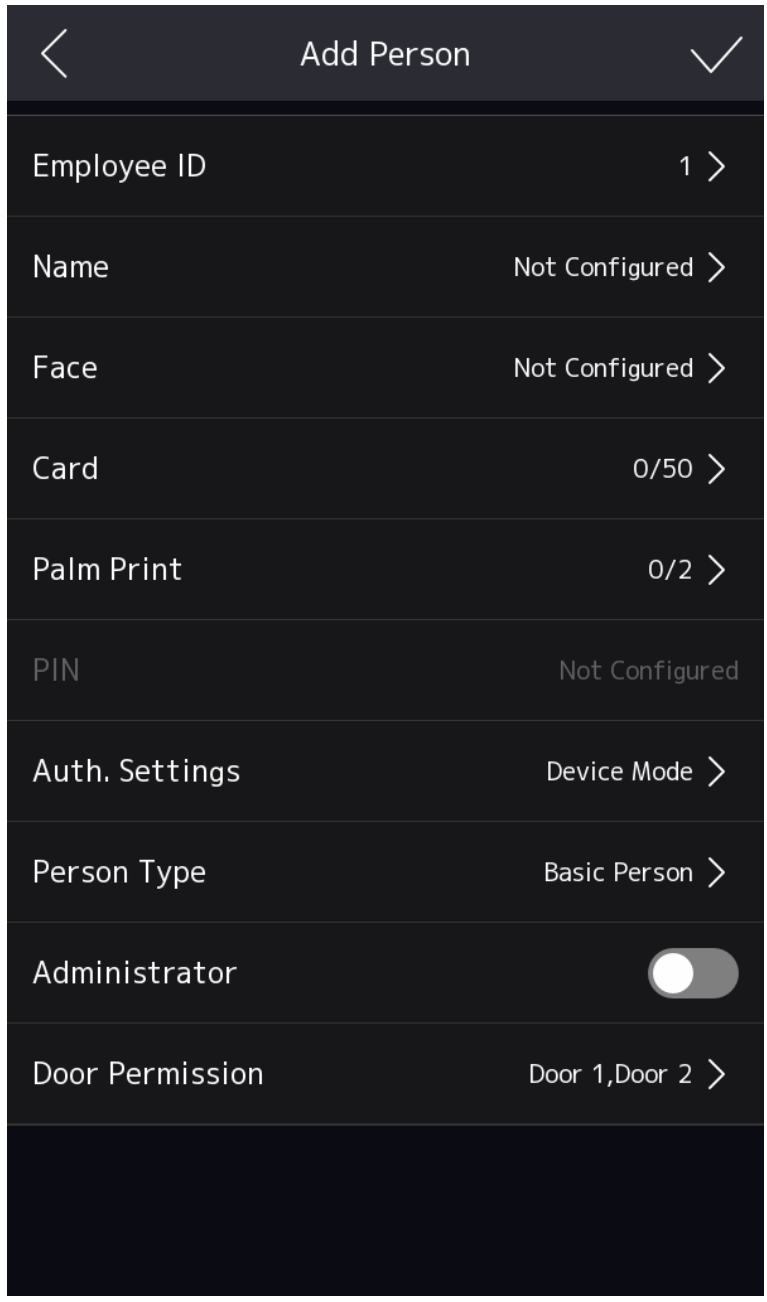


図7-11 「Person」の追加

2. **従業員ID**をタップすると、従業員IDを編集できます。

注

従業員IDは32文字を超えてはいけません。大文字、小文字、数字の組み合わせで構成できます。

3. **名前**をタップし、名前を作成します。ポップアップキーボードに従って、その人の名前を入力します。

注意

- 名前には数字、大文字、小文字、および特殊文字が含まれることができます。
- 名前は128文字以内にしてください。

4. 顔、カード、指紋、手のひら紋を設定します。

注

- 「***顔写真を追加***」「***カードを追加***」「***指紋を追加***」を指し、顔、カード、指紋、および手のひら紋を追加することを意味します。
- 指紋または手のひらモジュールを搭載したデバイスのみ、指紋または手のひら機能に対応しています。

5. **「人物タイプ」**をタップし、タイプを**「基本人物」**または**「訪問者」**に設定します。

注

人物を訪問者に設定した場合、管理者を設定できません。人物をブロックリストの人物に設定した場合、その人物のドア権限を設定できません。

6. **ドアのアクセス権限**をタップし、通過させるドアを選択します。ドア1は、そのドアがデバイスに接続されていることを意味します。ドア2は、そのドアがセキュアドアコントロールユニットに接続されていることを意味します。

注意

リモート認証時、管理者はユーザーのドア権限に基づいてドアの開閉を判断できます。

7. タップ をタップして設定を保存します。

7.4 データ管理

データを削除、インポート、エクスポートできます。

7.4.1 データを削除

個人データを削除します。

ホーム画面で、**[データ]** をタップし、**[→]** をタップし、**[データ削除] を**タップし、**[→] をタップし、[個人データ] をタップします**。デバイスに追加されたすべての個人データが削除されます。

7.4.2 データのインポート

手順

1. USB フラッシュドライブをデバイスに接続します。

2. ホーム画面で、**データ→ データインポート** をタップします。

3. **「個人データ」「顔データ」**または**「アクセス制御パラメーター」**をタップします。

注意

インポートされたアクセス制御パラメーターは、デバイスの設定ファイルです。

4. データをエクスポートした際に設定したパスワードを入力してください。データをエクスポートした際にパスワードを設定していない場合は、入力欄を空白のままにし、すぐに**「OK」を**タップしてください。

注意

- 1つのデバイス（デバイスA）から別のデバイス（デバイスB）にすべての個人情報を転送したい場合は、まずデバイスAからUSBフラッシュドライブに情報をエクスポートし、その後USBフラッシュドライブからデバイスBにインポートする必要があります。この場合、プロフィール写真をインポートする前に、個人データをインポートする必要があります。
- サポートされているUSBフラッシュドライブのファイルシステムはFAT32です。
- インポートした画像は、ルートディレクトリの「enroll_pic」という名前のフォルダーに保存し、画像の名前は次のルールに従って命名してください：

  カード番号_名前_部署_従業員ID_性別.jpg
- フォルダー enroll_pic にすべての画像を保存できない場合は、ルートディレクトリの下に enroll_pic1、enroll_pic2、enroll_pic3、enroll_pic4 という名前のフォルダーを順次作成してください。
- 従業員IDは32文字未満でなければなりません。小文字、大文字、数字の組み合わせが可能です。重複してはならず、0で始まってはいけません。
- 顔写真の要件は以下のルールに従ってください：顔全体が正面を向いてカメラを直接見ている状態で撮影してください。顔写真の撮影時には帽子や頭部覆いを着用しないでください。形式はJPEGまたはJPGです。解像度は640× 480ピクセル以上でなければなりません。画像サイズは60KBから200KBの間でなければなりません。

7.4.3 データエクスポート

手順

1. USBフラッシュドライブをデバイスに接続します。
2. ホーム画面で**「データ」**をタップし、**次に「→ データエクスポート」**をタップします。
3. **「顔データ」**「**イベントデータ**」「**人物データ**」「**アクセス制御パラメーター**」のいずれかをタップします。

注意

エクスポートされたアクセス制御パラメーターは、デバイスの設定ファイルです。

4. **オプション:** データエクスポート用のパスワードを設定します。別のデバイスにデータをインポートする際は、このパスワードを入力する必要があります。

注意

- 対応しているUSBフラッシュドライブのフォーマットはDBです。
- システムは、1GBから256GBのストレージ容量を持つUSBフラッシュドライブに対応しています。USBフラッシュドライブの空き容量が512MB以上であることを確認してください。
- エクスポートされた個人データはDBファイルであり、編集できません。

7.5 ユーザー認証

ネットワーク設定、システムパラメーター設定、ユーザー設定が完了後、認証画面に戻ることができます。システムは設定された認証モードに従ってユーザーを認証します。

7.5.1 シングルクレデンシャルで認証

認証前にユーザー認証の種類を設定します。詳細については、*「認証モードの設定」*を参照してください。

顔

カメラに向かって顔を向け、顔認証を開始します。

指紋

登録済みの指紋を指紋モジュールに置き、指紋認証を開始します。

手のひら

手のひらを手のひら認証モジュールに置き、手のひら認証を開始します。

カード

カードをカード読み取りエリアに提示し、カードによる認証を開始します。

注意

カードは通常のICカードまたは暗号化カードです。

QRコード

デバイスのカメラにQRコードを向けて、QRコードで認証してください。

注意

- QRコードによる認証は、デバイスでサポートされている必要があります。
- *設定画面で*QRコード機能を有効にしてください。

PIN

PINを入力してPINによる認証を行ってください。

キーフォブ

キーフォブのドア開錠ボタンを押して認証してください。

認証が完了すると、「認証完了」というメッセージが表示されます。

7.5.2 複数の認証情報で認証

開始前に

認証前にユーザー認証の種類を設定します。詳細については、*「認証モードの設定」*を参照してください。

手順

1. ライブビューページの手順に従って、任意の資格情報を認証します。

注意

- カードは通常のICカードまたは暗号化カードです。
- QRコードスキャン機能が有効になっている場合、デバイスのカメラにQRコードを向けることで、QRコード経由で認証を行うことができます。

2. 前の認証情報が認証された後、他の認証情報の認証を継続します。

注

- 指紋のスキャンに関する詳細情報は、「*指紋のスキャンに関するヒント*」を参照してください。
- 顔認証に関する詳細情報は、「*顔写真の収集/比較時のヒント*」を参照してください。

認証に成功した場合、プロンプト「認証完了」が表示されます。

7.6 基本設定

最初の画面を3秒間長押しし、ジェスチャーに従って左右にスワイプしてデバイスのホーム画面にログインします。**「システム」→「基本」**をタップします。

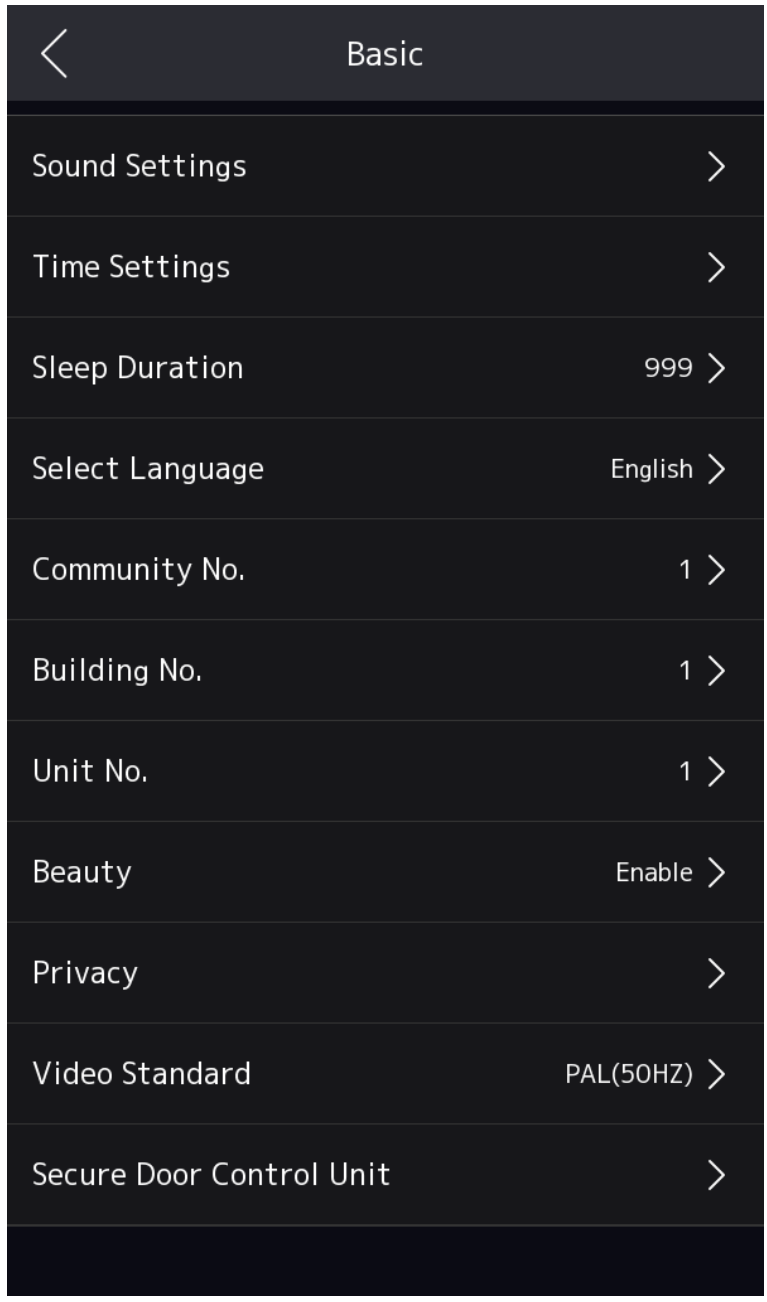


図7-12 基本設定ページ

7.6.1 デバイス経由での音声プロンプトの有効/無効設定

音声プロンプト機能を有効/無効に設定し、音声のボリュームを調整できます。デバイスにログインしてください。詳細については、*「ログイン」を*参照してください。

システム設定をタップし、**→、基本、→、サウンド設定を選択します。**

音声ガイド機能を有効/無効に設定し、音声のボリュームを調整できます。音声ガイド機能を有効にすると、音声のボリュームを設定できます。

7.6.2 デバイス経由でデバイス時間を設定

デバイスの時間を設定します。

デバイスにログインしてください。詳細については、*「ログイン」*を参照してください。

システム設定をタップ → **基本** → **時間設定**。デバイスのタイムゾーン、現在の時刻、および夏時間（DST）を設定します。

7.6.3 デバイス経由でスリープ時間を設定

デバイスのスリープ待機時間を設定します。デバイスにログインします。詳細については、*ログイン*を参照してください。

システム設定をタップし、→ **基本を選択します**。その後、**スリープ時間を**設定します。

初期画面でスリープ時間を30秒に設定した場合、操作がない状態で30秒後にデバイスがスリープ状態になります。

注意

プ時間を0に設定すると、デバイスはスリープモードに入りません。設定可能なスリープ時間は20秒から999秒です。

7.6.4 言語を選択

デバイスにログインしてください。詳細については*「ログイン」*を参照してください。

システム設定をタップし、→ **基本を選択します**。言語を変更するには、**言語を選択**をタップします。言語を変更すると、デバイスが再起動します。

7.6.5 デバイス番号をデバイスから設定

このデバイスは、アクセス制御デバイス、ドアステーション、または外ドアステーションとして使用できます。ビデオインターコム用のデバイス番号を設定できます。

デバイスにログインしてください。詳細については、*「ログイン」*を参照してください。

システム設定をタップし、→ **基本**を設定します。**コミュニティ番号**、**建物番号**、および**ユニット番号**を設定します。

7.6.6 デバイス経由でビューティー機能を設定します

ビューティー機能を有効にし、滑らかさと白さのパラメーターを設定できます。

デバイスにログインします。詳細については、*ログイン*を参照してください。**システム設定**をタップし、
→、Basic、→、Beautyの順に選択します。
美化機能を有効にし、滑らかさと明るさのパラメーターを設定します。**+または-**をタップして効果の強さを調整します。

7.6.7 デバイスの設定からプライバシーパラメーターを設定してください。

画像のアップロードパラメーターを設定します。

注意
異なるデバイスモデルでは異なる機能がサポートされています。実際のモデルをご確認ください。

デバイスにログインします。詳細については「*ログイン*」を参照してください。**「システム設定」**をタップし、**→、Basic、→、Privacy** の順に選択します。

認証設定

名前 / 従業員ID / 顔写真

認証時に名前と従業員IDを表示する/表示しない/非表示にするを選択できます。

画像のアップロードと保存

画像のアップロードと保存の設定を行います。

登録した写真を保存します。

この機能を有効にすると、登録された顔画像がシステムに保存されます。

リンクキャプチャ後の画像保存

この機能を有効にすると、リンクキャプチャ後に画像を保存できます。

リンクキャプチャ後に画像をアップロード

リンクキャプチャ後に撮影した画像をアップロードします。

認証時に画像を保存

この機能を有効にすると、デバイスに認証する際、画像を保存できます。

認証時に画像をアップロード。

この機能を有効にすると、デバイスに認証する際、画像を保存できます。

手のひらプリント画像の保存

この機能を有効にすると、申請時に画像を保存できます。

7.6.8 動画標準設定

ライブビューの動画標準を設定します。デバイスにログインしてください。詳細については、*ログイン*を参照してください。

システム → 基本 → 動画標準 へ移動します。
リモートでライブビューを実行する際の動画フレームレートを設定します。設定を変更後は、変更を反映させるためにデバイスを再起動する必要があります。

PAL (50Hz)

25フレーム/秒。中国本土、香港（中国）、中東諸国、ヨーロッパ諸国などにおすすめです。

NTSC (60Hz)

30フレーム/秒。アメリカ合衆国、カナダ、日本、台湾（中国）、韓国、フィリピンなどに適しています。

7.6.9 セキュアドアコントロールユニットのパラメーターを設定します

セキュアドア制御ユニットに応じて周辺機器を配線できます。セキュアドア制御ユニットを制御するために、ドア1またはドア2を使用するように設定できます。

開始前に

デバイスはRS-485経由でセキュアドア制御ユニットを配線しています。詳細な配線方法については、***配線を***参照してください。

手順

1. デバイスにログインします。詳細については、*「ログイン」*を参照してください。
2. **システム→ 基本→ セキュアドア制御ユニット**に移動します。
3. ドア番号として「**Door 1**」または「**Door 2**」を選択します。

注意

ドア 1 は、セキュア ドア コントロール ユニットで制御されるドアを意味します。ドア 2 の選択についても同様です。

7.7 フェイス パラメーターを設定します。

顔認識の精度を向上させるため、顔のパラメーターをカスタマイズできます。

最初の画面を3秒間長押しし、ホーム画面にログインします。**システム設定**をタップし、**→ Biometrics** を選択します。

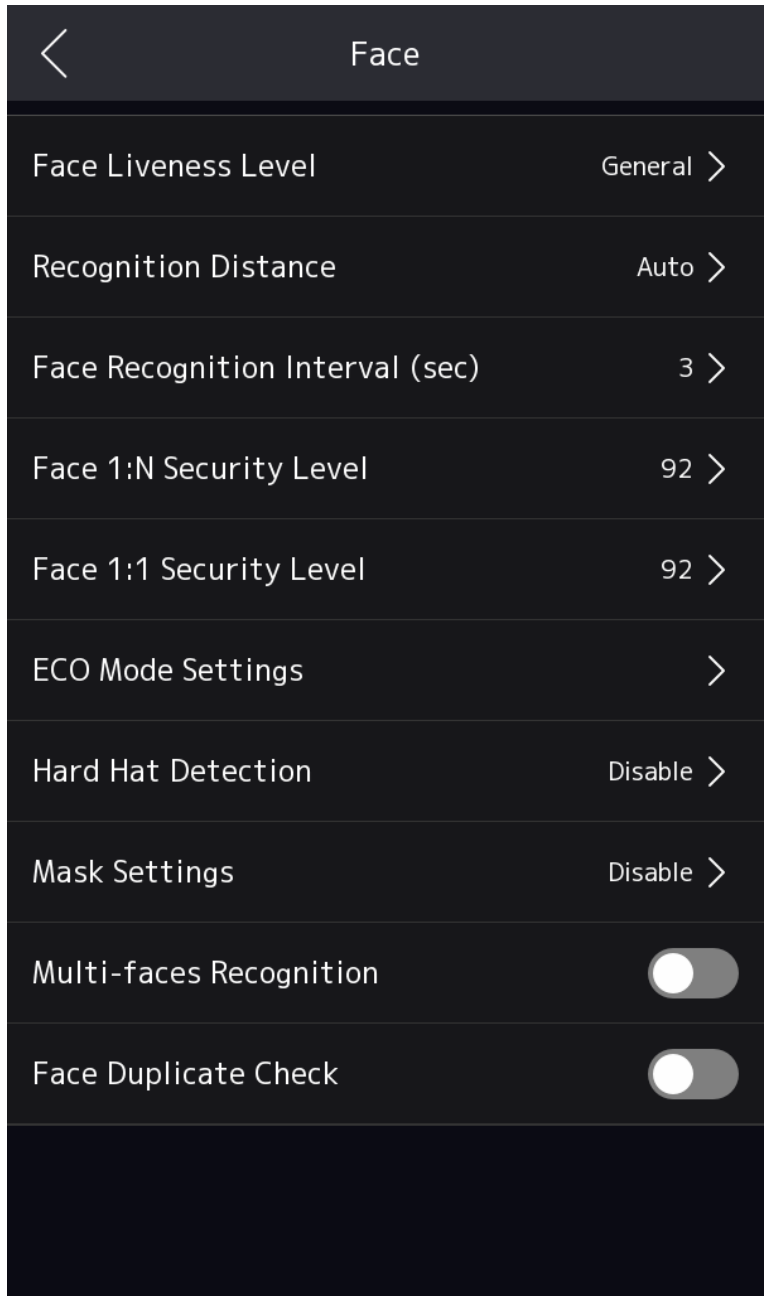


図7-13 顔設定

7.7.1 デバイス経由で顔のライブネスレベルを設定

顔認証の偽装防止機能を有効にした後、ライブ顔認証を行う際の一致セキュリティレベルを設定できます。

デバイスにログインします。詳細については、*「ログイン」*を参照してください。

システム設定をタップし、**→**、**Biometrics**、**→**、**Face** の順に
選択します。顔の活体検出レベルを選択します。
一般、上級、プロフェッショナルから選択できます。レベルが上がるほど、誤検出率は低下し、誤拒否率は上昇します。

7.7.2 デバイス経由で認識距離を設定する

認証時にユーザーとカメラの有効な距離を設定します。デバイスにログインします。詳細について
は*「ログイン」*を参照してください。

システム設定をタップし、**→**、**Biometrics**、**→**、**Face**、**→**、**Recognition Distance** をタップします。
認識距離を設定します。

7.7.3 デバイス経由で顔認識間隔を設定する

認証時に連続する2回の顔認識の間隔を設定します。デバイスにログインします。詳細については、*「ログ
イン」*を参照してください。

システム設定をタップし、**→**、**Biometrics**、**→**、**Face**、**→**、**Face Recognition Interval (sec)** をタップします。
顔認識の間隔を設定します。

注意
1から10までの数値を入力してください。

7.7.4 デバイス経由で顔 1:N セキュリティレベルを設定

1:N一致モードで認証する際の一致閾値を設定します。デバイスにログインします。詳細につい
ては「*ログイン*」を参照してください。

システム設定をタップし、**→**、**Biometrics**、**→**、**Face**、**→**、**Face 1:N Security Level** を順に選択します。
1:N マッチングモードで認証する際の一致閾値を設定します。
しきい値の値が大きいほど、顔認証時の誤認率（FA）は低くなり、誤拒否率（FRR）は高くなります。最大値は100です。

7.7.5 デバイス経由で顔認証のセキュリティレベルを設定する

1:1一致モードで認証する際の一致閾値を設定します。デバイスにログインします。詳細につい
ては、*ログイン*を参照してください。

システム設定をタップし、**→**、**Biometrics**、**→**、**Face**、**→**、**Face 1:1 Security Level** をタップします。
1:1 マッチングモードで認証する際の一致閾値を設定します。

しきい値の値が大きいほど、顔認証時の誤認率（FA）は低くなり、誤拒否率（FRR）は高くなります。最大値は100です。

7.7.6 デバイス経由でECOモードの有効/無効を切り替える

ECOモードを有効にすると、赤外線カメラを使用して低照度または暗い環境で顔認証を行うことができます。

デバイスにログインします。詳細については、*ログイン*を参照してください。

システム設定をタップし、**→**、**Biometrics**、**→**、**Face**、**→**、**ECO Mode Settings** の順に選択します。

ECOモードが有効になっている場合、赤外線カメラを使用して低照度または暗い環境で顔認証を行うことができます。ECOモードの閾値、ECOモード（1:N）、およびECOモード（1:1）を設定できます。

ECOモードの閾値

ECOモードを有効にした場合、ECOモードの閾値を設定できます。値が大きいほど、デバイスがECOモードに入りやすくなります。閾値は照度と関連しています。

ECOモード（1:1）

ECOモードの1:1マッチングモードで認証を行う際の照合閾値を設定します。値が大きいほど、誤認率（FA）が低く、誤拒否率（FRR）が高くなります。最大値は100です。

ECOモード (1:N)

ECO モードの 1:N マッチングモードで認証を行う際の照合閾値を設定します。値が大きいほど、誤認率（false accept rate）が低く、誤拒否率（false rejection rate）が高くなります。最大値は 100 です。

7.7.7 デバイス経由でのヘルメット検出の有効/無効設定

ハードハット検出を有効にした後、デバイスが顔認証を開始すると、システムは被写体がハードハットを着用しているかどうかを検出します。

デバイスにログインします。詳細については、*ログイン*を参照してください。

システム設定をタップし、**→**、**Biometrics**、**→**、**Face**、**→**、**Hard Hat Detection** を順に選択します。

ヘルメット検出

ヘルメット検出機能を有効にした後、ドアの開閉戦略を設定できます。

なし

認証時にマスクを着用していない場合、デバイスは通知を表示しません。

着用リマインダー

認証時にヘルメットを着用していない場合、デバイスは通知を表示し、ドアが開きます。

着用必須

認証時にヘルメットを着用していない場合、デバイスは警告メッセージを表示し、ドアは開かなくなります。

7.7.8 マスク検出の有効/無効設定（デバイス経由）

マスク着用時の顔検出を有効にすると、システムはマスクを着用した顔の画像を認識します。

デバイスにログインします。詳細については、*ログイン*を参照してください。

システム設定をタップし、**→**、**Biometrics**、**→**、**Face**、**→**、**Mask Settingsの順に選択します**。

マスク着用顔検出を有効にすると、システムはマスクを着用した顔の写真を認識します。**マスク着用顔と顔（1:1）**、**マスク着用顔と顔（1:N）**、**ECOモード（1:1）の閾値**、**ECOモード（1:N）の閾値**、**およびプロンプト方法を**設定できます。

マスク着用顔と顔（1:1）

マスク付き顔とマスクなし顔の1:1一致閾値を設定します。値が大きいほど、誤認識率が低く、誤拒否率が大きくなります。最大値は100です。

マスク着用顔と顔 (1:N)

マスク1:N一致閾値を設定します。値が大きいほど、誤認率（FA）は低く、誤拒否率（FR）は高くなります。最大値は100です。

ECOモード（1:1）しきい値

ECOモードを有効にした後、マスク装着時の顔認識機能を設定できます。しきい値を設定できます。

ECOモードの1:1マッチングモードで認証する際のマッチング閾値を設定します。閾値の値が大きいほど、顔認証時の誤認率が低下し、誤拒否率が上昇します。最大値は100です。

ECOモード（1:N）しきい値

ECOモードを有効にした後、マスク着用時の顔認識機能を設定できます。しきい値を設定できます。

ECOモードの1:Nマッチングモードで認証を行う際の照合閾値を設定します。閾値の値が大きいほど、顔認証時の誤認率（誤認率）が低く、誤拒否率（誤拒否率）が高くなります。最大値は100です。

戦略

「**なし**」「**マスク着用リマインダー**」「**マスク着用必須**」を設定します。**なし**

認証時にマスクを着用していない場合、デバイスは通知を表示しません。

着用リマインダー

マスクを着用せずに認証を行った場合、デバイスが通知を表示し、ドアが開きます。

マスクの着用必須

認証時にマスクを着用していない場合、デバイスは通知を表示し、ドアは閉じたままになります。

7.7.9 マルチ顔認識の有効/無効設定

複数顔認証を有効にすると、複数顔認証がサポートされます。デバイスにログインしてください。詳細については、*ログイン*を参照してください。

システム設定をタップし、**→、Biometrics、→ Faceを選択します。**

マルチ顔認識を有効にします。機能が有効になると、複数の顔が同時に認証可能です。

注意まで同時に認証可能です。

- 機能有効化後は、カードリーダー認証モード、カスタム認証、出席状態、顔認証による手動認証は使用できません。

7.7.10 デバイスによる顔の重複チェック

顔重複チェック機能を有効にした後、人物の顔を追加する際、システムは重複をチェックします。システムに重複した顔画像が検出された場合、ポップアップ通知が表示されます。

注意

リモートでの顔写真の追加または一括適用では、この機能はサポートされていません。

デバイスにログインしてください。詳細については「*ログイン*」を参照してください。**システム設定**をタップし、**→、Biometrics、→ Face** の順に選択します。

顔の重複チェックを有効にします。機能を有効にした後、顔を追加する際、システムは重複をチェックします。システムに重複した顔画像が検出された場合、ポップアップ通知が表示されます。

7.7.11 手のひら認証を設定します。

手のひら認証のタイムアウト閾値と手のひら認証の間隔を設定できます。デバイスにログインします。詳細については、*「ログイン」*を参照してください。

システム設定をタップし、**→、Biometrics、→、Palm Print を順にタップします。**

手のひら認証のタイムアウト閾値と**手のひら認証の間隔**を設定します。

7.8 アクセス制御設定

アクセス制御の権限を設定できます。

ホーム画面**でACS**をタップして設定画面に入ります。

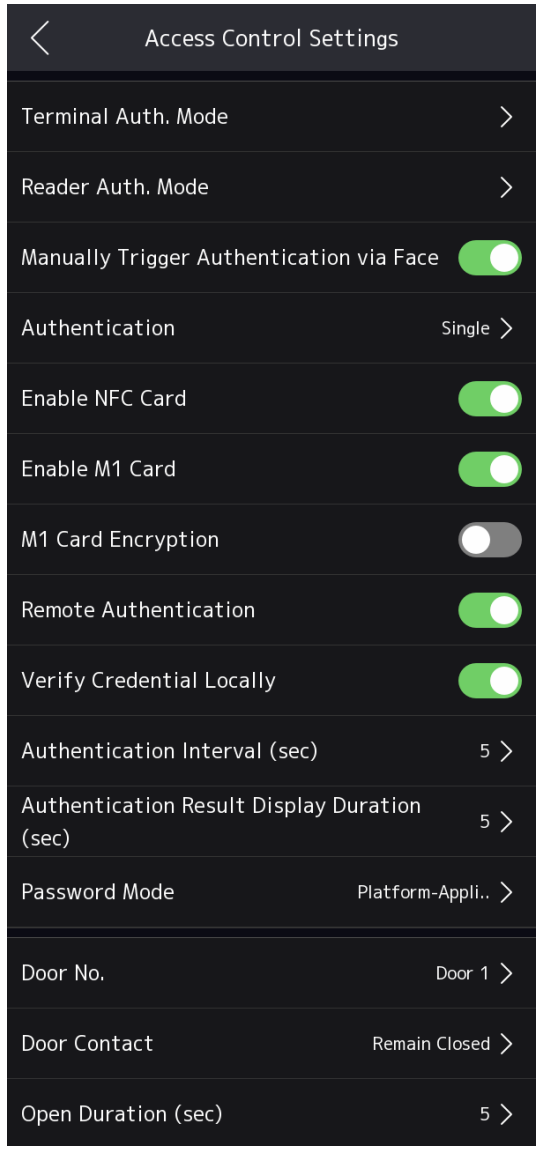


図7-14 アクセス制御設定

7.8.1 デバイス経由でターミナル認証モードを設定します。

顔認識端末の認証モードを選択します。異なる組み合わせを選択して認証を行うことができます。

デバイスにログインします。詳細については、*「ログイン」*を参照してください。**ACS → 端末認証モードを**タップします。

人物認証の種類と方法を選択し、設定を保存します。

デバイスの認証モードがすべて「**デバイスモード**」の場合、デバイス上のすべてのユーザーはデバイス認証モードを使用します。ユーザー認証モードの設定の詳細については、*「認証モードの設定」を*参照してください。

注意

ジュールを搭載したデバイスは指紋認証機能に対応しています。

注意

生体認証製品は、アンチスプーフィング環境において完全に適用可能ではありません。より高いセキュリティレベルが必要な場合は、複数の認証モードを使用してください。

7.8.2 デバイス経由でリーダー認証モードを設定する

有線外部リーダーで人物認証の種類を設定します。異なる組み合わせを選択して認証を行うことができます。

デバイスにログインします。詳細については、*「ログイン」*を参照してください。**ACS → リーダー認証モードを**タップします。

人物認証の種類を選択し、設定を保存します。

人物認証の種類と方法を選択し、設定を保存します。

デバイスの認証モードがすべてのユーザーで「**デバイスモード**」に設定されている場合、そのデバイス上のすべてのユーザーはデバイスの認証モードを使用します。ユーザー認証モードの設定の詳細については、*「認証モードの設定」を*参照してください。

注

指紋モジュールを搭載したデバイスは、指紋機能に対応しています。

注意

生体認証製品は、偽装防止環境において完全に適用できません。より高いセキュリティレベルが必要な場合は、複数の認証モードを使用してください。

7.8.3 PCウェブ経由で手動で顔認証をトリガーする

顔認証を手動でトリガーする機能を有効にした後、顔認識のためにはデバイスの画面を手動でタッチする必要があります。

デバイスにログインします。詳細については、*ログイン*を参照してください。**ACS を**タップします。

「顔認証による手動認証を有効にする」をオンにし、**認証**方法を「**単一認証**」または「**連続単一認証**」に設定します。

認証ページで、各顔認識の前に**認証**をタップして認識をトリガーする必要があります。

継続

認識をトリガーした後、デバイスがスリープモードに入るまで顔で認識できます。

7.8.4 NFC カード機能を有効/無効にする

NFCカード機能を有効/無効にします。ログイ

ン後、**ACS**をタップします。

「NFCを有効にする」をタップします。有効化後、デバイスはNFCカードを読み取ることができます。

注意

デュアル周波数カードモジュールが顔認識端末にアクセスする際、デバイス上でカードをスワイプしても無効です。

7.8.5 M1カード機能を有効/無効にする

M1カード機能を有効または無効にします。

デバイスにログインします。詳細については*「ログ*

イン」を参照してください。ログイン後、**ACS**をタッ

プします。

「M1カード有効化」をタップすると、デバイスがM1カードを読み取ることができます。

M1カード有効化

有効化後、デバイスはM1カードを読み取ることができます。

M1カード暗号化

M1カード暗号化を有効にすると、デバイスはM1カードのセクターを検証します。プラットフォームに移動し、M1カードの暗号化セクターを設定してください。

注意

デュアル周波数カードモジュールが顔認識端末にアクセスする際、デバイス上でカードをスワイプしても無効です。

7.8.6 リモート認証

リモートプラットフォームで認証の可否を判断します。デバイスにログインします。

詳細については「*ログイン」を*参照してください。

ACS をタップします。

リモート認証を有効にします。認証中のユーザーがいる場合、リモートプラットフォームが認証の可否を判断します。

デバイス上で資格情報を認証し、プラットフォームで確認してください。

「**ローカルで資格情報を検証**」を有効にすると、検証はデバイス上で実行されます。

7.8.7 デバイス経由で認証間隔を設定します。

デバイスにログインします。詳細については、*「ログイン」*を参照してください。

ACS をタップし、**認証間隔**を設定して保存します。

同じユーザーが認証する際の認証間隔を設定できます。同じユーザーは設定された間隔内で1回のみ認証可能です。2回目の認証は失敗します。

利用可能な認証間隔の範囲：0から65535。

7.8.8 デバイス経由で認証結果の表示時間を設定する

認証時に認証結果の表示時間を設定します。デバイスにログインします。詳細については、

*「ログイン」を*参照してください。

ACS をタップし、**認証結果の表示時間を**設定して保存します。

7.8.9 パスワードモードを設定する

パスワードモードを設定し、デバイス/PCウェブまたはプラットフォームでパスワードを編集するかどうかを選択できます。

手順

1. デバイスにログインします。詳細については、*ログイン*を参照してください。
2. **ACS** をタップします。
3. **パスワードモード**をタップし、モードを設定します。

   プラットフォーム適用個人PIN

   PINは、デバイスがプラットフォームにアクセスした後、プラットフォームによって管理および配布されます。

   デバイス設定の個人用PIN

   PINはデバイスまたはPC Web上で設定されます。
4. 設定を保存するには、前のページに戻ってください。

7.8.10 ドアパラメーター設定

ドアの解錠パラメーターを設定します。

デバイス経由でドア番号を設定

デバイスに割り当てるドア番号を選択します。

デバイスにログインします。詳細については*「ログイン」*を参照してください。ログイン後、**ACS**をタップします。

ドア番号をタップしてください。**ドア1**または**ドア2**を選択してください。
ドア1は入口に設置されたデバイスを指します。ドア2は出口に設置されたデバイスを指します。

ドアコンタクトをデバイス経由で設定

ドアコンタクトの配線方法に応じて、ドアコンタクトの状態を選択してください。デバイスにログインしてください。詳細については、*ログイン*を参照してください。

ACS をタップしてください。
実際のニーズに応じて「開いたまま」または「閉じたまま」を選択できます。デフォルトは「閉じたまま」です。

デバイス経由で開く時間を設定する

ドアの解錠時間を設定します。

デバイスにログインします。詳細については*「ログイン」*を参照してください。**ACS**をタップします。
ドアの解錠時間を設定します。設定した時間内にドアが開かれない場合、ドアがロックされます。利用可能なドアロック時間範囲：1～255秒。

7.9 プラットフォーム出席管理

実際の状況に応じて、出席モードを「チェックイン」「チェックアウト」「休憩開始」「休憩終了」「残業開始」「残業終了」から選択できます。

注意
この機能は、クライアントソフトウェアの勤怠機能と組み合わせて使用してください。

7.9.1 デバイス経由で出席モードを無効にする

出席モードを無効にすると、システムは初期画面に出席ステータスを表示しなくなります。

「プラットフォーム出席」をタップして、T&A ステータスページに移動します。

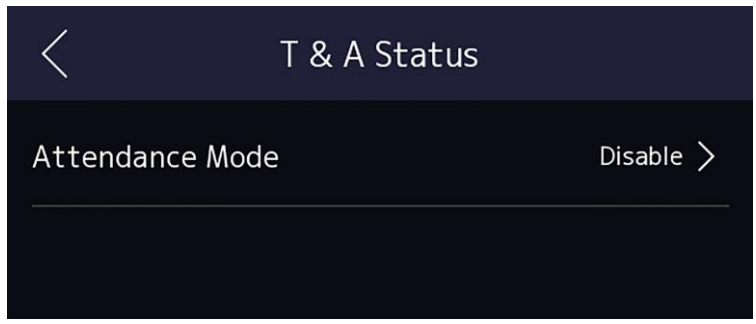


図7-15 出席モードを無効にする

出席モードを**「無効」**に設定します。

初期画面で出席ステータスを表示したり設定したりできなくなります。システムはプラットフォームで設定された出席ルールに従います。

7.9.2 デバイス経由で手動出席を設定する

出席モードを手動に設定し、出席を確認する際は手動でステータスを選択する必要があります。

開始前に

少なくとも1つのユーザーを追加し、ユーザーの認証モードを設定してください。詳細については、*「ユーザー管理」を*参照してください。

手順

1. **「プラットフォーム出席」**をタップして、T&A ステータスページに移動します。
2. **出席モード**を**「手動」**に設定します。

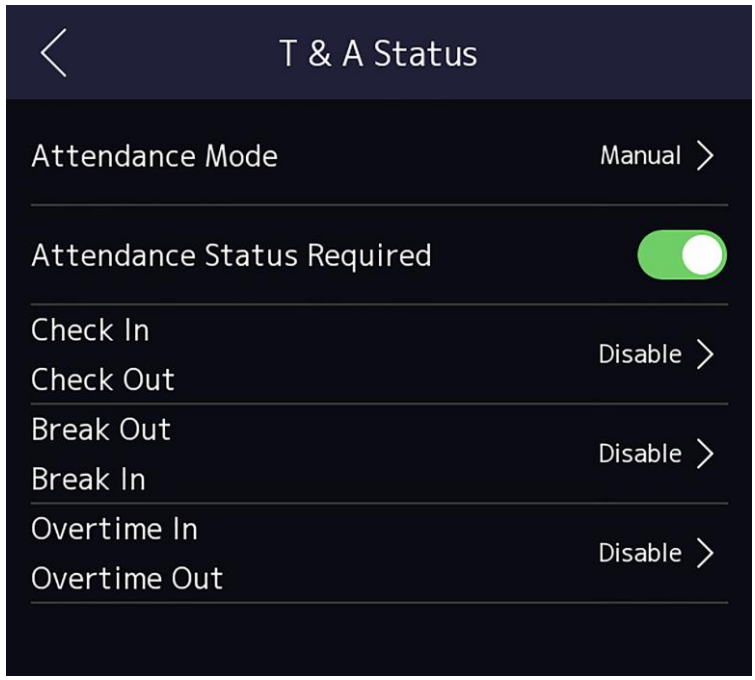


図7-16 手動出席モード

3. 「**出席ステータス必須**」を有効にします。
4. 出席ステータスのグループを有効にします。

注

出席プロパティは変更されません。

5. **オプション：**必要に応じてステータスを選択し、その名前を変更してください。
   名前は「T & A ステータス」ページと認証結果ページに表示されます。

結果

認証後、出席ステータスを手動で選択する必要があります。

注意

ステータスを選択しない場合、認証は失敗し、有効な出席として記録されません。

7.9.3 デバイス経由で自動出席を設定する

出席モードを「自動」に設定すると、出席ステータスとその利用可能なスケジュールを設定できます。システムは、設定されたスケジュールに従って出席ステータスを自動的に変更します。

開始前に

少なくとも1つのユーザーを追加し、ユーザーの認証モードを設定してください。詳細については、*ユーザー管理*を参照してください。

手順

1. **「プラットフォーム出席」**をタップして、T&A ステータスページに移動します。
2. **出席モード**を**「自動」**に設定します。

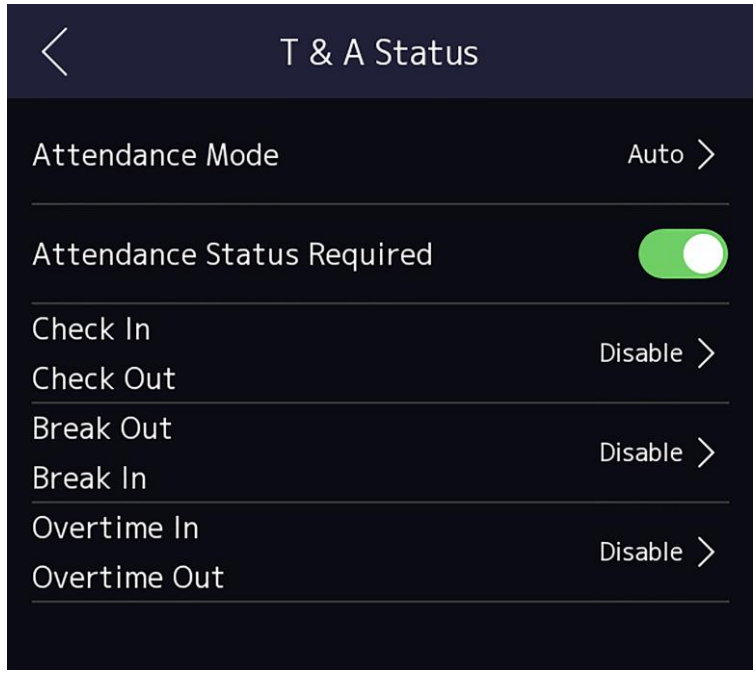


図7-17 自動出席モード

3. **出席ステータス**機能を有効にします。
4. 出席ステータスのグループを有効にします。

注

出席プロパティは変更されません。

5. **オプション：**必要に応じてステータスを選択し、その名前を変更してください。

   名前は「T & A ステータス」ページと認証結果ページに表示されます。
6. ステータスのスケジュールを設定します。
   1) **「出席スケジュール」**をタップします。
   2) **月曜日**、**火曜日**、**水曜日**、**木曜日**、**金曜日**、**土曜日**、または**日曜日**を選択します。
   3) 選択した出席ステータスの1日の開始時間を設定します。
   4) **「確認」**をタップします。
   5) ステップ1から4を、実際の必要に応じて繰り返し実行してください。

注

出席状況は、設定されたスケジュール内で有効です。

結果

初期ページで認証を行った場合、設定されたスケジュールに従って、認証が設定された出席ステータスとしてマークされます。

例
ブレイクアウトを月曜日の11:00に、**ブレイク**インを月曜日の12:00に設定した場合、月曜日の11:00から12:00までの有効なユーザーの認証は「休憩中」としてマークされます。

7.9.4 デバイス経由で手動と自動出席を設定する

出席モードを**「手動」と「自動」**に設定すると、システムは設定されたスケジュールに従って出席ステータスを自動的に変更します。同時に、認証後に手動で出席ステータスを変更することも可能です。

開始前に
少なくとも1つのユーザーを追加し、ユーザーの認証モードを設定します。詳細については、*ユーザー管理*を参照してください。

手順
1. **「プラットフォーム出席」**をタップして、T&A ステータスページに移動します。
2. **出席モード**を**「手動」と「自動」**に設定します。

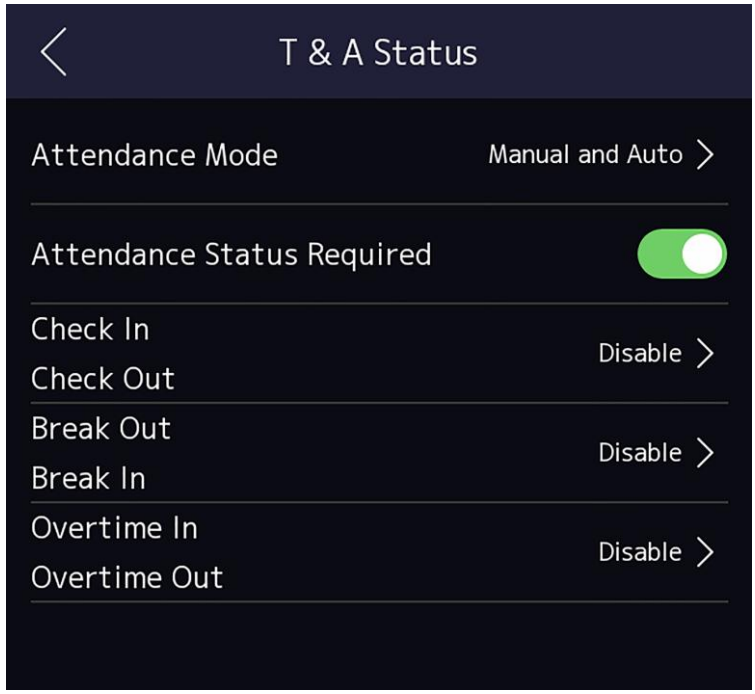


図7-18 手動と自動モード

3. **出席ステータス**機能を有効にします。
4. 出席状況のグループを有効にします。

注
出席プロパティは変更されません。

5. **オプション：**必要に応じてステータスを選択し、名前を変更できます。
名前は「T & A ステータス」ページと認証結果ページに表示されます。

6. ステータスのスケジュールを設定します。

1) **「出席スケジュール」**をタップします。

2) **月曜日**、**火曜日**、**水曜日**、**木曜日**、**金曜日**、**土曜日**、または**日曜日**を選択します。

3) 選択した出席状況のその日の開始時間を設定します。

4) **OK**をタップします。

5) 実際の必要に応じて、手順1から4を繰り返し実行します。

注意

出席ステータスは設定されたスケジュール内で有効になります。

結果

最初のページで認証を行います。認証結果は、スケジュールに従って設定された出席状況としてマークされます。結果タブの編集アイコンをタップすると、手動で出席状況を選択できます。その場合、認証結果は編集された出席状況としてマークされます。

例

ブレイクアウトを月曜日の11:00、**ブレイク**インを月曜日の12:00に設定した場合、月曜日の11:00から12:00までの有効なユーザーの認証は「休憩中」としてマークされます。

7.10 設定

設定パラメーターを構成できます。

手順

1. システム→ 設定をタップして、設定画面に移動します。

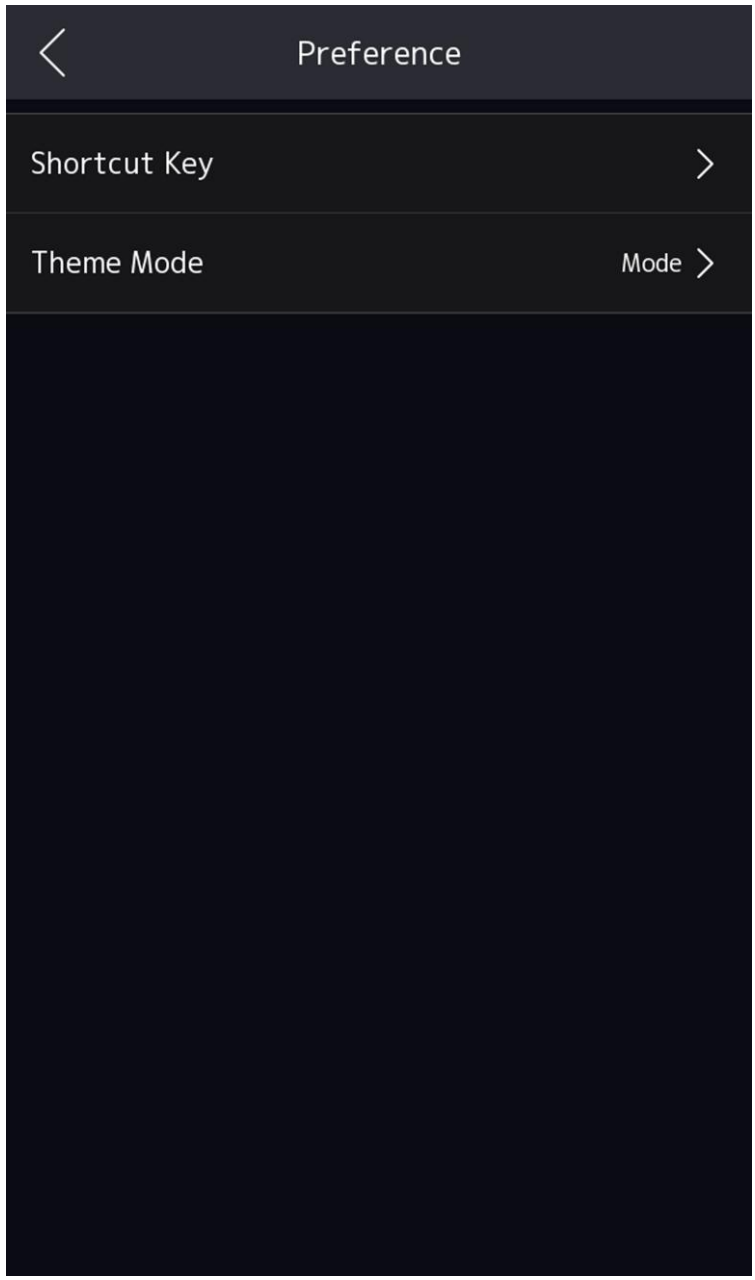


図7-19 設定

7.10.1 デバイス経由でショートカットキーを設定

認証画面に表示されるショートカットキーを選択します。これにはQRコード機能、通話機能、通話タイプ、パスワード入力機能が含まれます。

デバイスにログインします。詳細については、*ログイン*を参照してください。

システム設定→ 設定をタップします。

認証画面に表示されるショートカットキーを選択します。QRコード機能、通話機能、通話タイプ、パスワード入力機能を含みます。

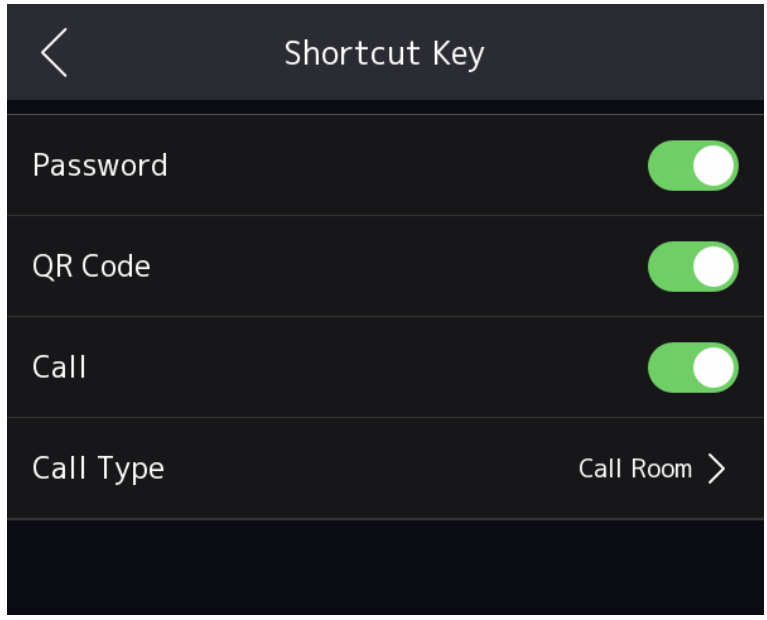


図7-20 ショートカットキーの設定

パスワード

この機能を有効にすると、パスワードで認証を行うことができます。認証画面で「」をタップして確認してください。

QRコード

認証画面でQRコードスキャン機能を使用できます。デバイスは取得したQRコードに関連する情報をプラットフォームにアップロードします。認証画面で「」をタップして確認してください。

通話

「Call Room」「Call Center」「Call Specified Room」「Call APP」から通話タイプを選択できます。**「Call Specified Room」**を選択した場合、部屋番号を入力する必要があります。

認証ページで「」をタップして通話してください。

7.10.2 テーマ

テーマを変更すると、認証画面に異なるコンテンツが表示されます。デバイスにログインしてください。

詳細については、*ログイン*を参照してください。

システム設定→ 設定。

テーマモードを選択してください。

認証

認証中にライブビューが表示され、同時にその人の名前、従業員ID、顔写真も表示されます。

広告

デバイスの広告表示領域と認証領域は別画面に表示されます。広告表示領域には動画、テキスト、ウェルカムメッセージが表示されます。

7.11 システムメンテナンス

最初の画面を3秒間長押しし、ジェスチャーに従って左右にスワイプしてホーム画面にログインします。**「メンテナンス」**をタップします。

7.11.1 システム情報を表示

デバイスのシステム情報を表示します。

最初の画面を3秒間長押しし、ジェスチャーに従って左右にスワイプし、ホーム画面にログインします。**「メンテナンス」**をタップします。**→「システム情報」**をタップします。

デバイスのモデル、シリアル番号、バージョン、アドレス、製造データ、QRコード、およびオープンソースコードのライセンスを確認できます。

注意

ページはデバイスモデルによって異なる場合があります。詳細については実際のページをご確認ください。

画面右下の「」を長押しして、詳細設定画面を開きます。生体認証パラメーターを設定したり、デバイスバージョン情報を確認できます。

生体認証パラメーター

カスタムアンチスプーフィング検出顔認

識精度レベル

顔認証のアンチスプーフィング機能を有効にした後、ライブ顔認証時のマッチングセキュリティレベルを設定できます。

アンチスプーフィング検出閾値

値が大きいほど、誤認率（偽陽性率）が低く、拒否率（偽陰性率）が高くなります。値が小さいほど、誤認率（偽陽性率）が高く、拒否率（偽陰性率）が低くなります。

アンチスプーフィング保護のためのロック画面

この機能を有効にすると、アンチスプーフィング検出に失敗した場合、デバイスが自動的にロックされます。

ロック時間

アンチスプーフィング保護のための顔認証ロックを有効にした後、アンチスプーフィング検出に失敗した際のロック時間。

バージョン情報

デバイスの情報を確認できます。

7.11.2 デバイス経由でデバイス容量を表示

デバイスの容量を確認できます。

初期画面で3秒間長押しし、ジェスチャーに従って左右にスワイプしてホーム画面にログインします。**「メンテナンス」**をタップ **→ 「容量」をタップ**。

ユーザー数、ユーザー名、顔写真、カード、指紋、手のひら紋、およびイベントを確認できます。

注

指紋モジュールが搭載されたデバイスのみ、指紋の表示機能に対応しています。

7.11.3 アップグレード

オンラインアップグレード

デバイスをオンラインでアップグレードできます。

初期画面を3秒間長押しし、ジェスチャーに従って左右にスワイプし、ホーム画面にログインします。**「メンテナンス」**をタップし、**次に「デバイスアップグレード」を選択します**。

デバイスがネットワークに接続されており、Hik-Connect アプリに追加されている場合、Hik-Connect アプリに新しいバージョンが利用可能になった際に、デバイス上で「**デバイス アップグレード」→「→ オンライン** アップグレード」をタップしてアップグレードを行うことができます。

ローカルアップグレード

デバイスをローカルでアップグレードできます。

初期画面を3秒間長押しし、ジェスチャーに従って左右にスワイプしてホーム画面にログインします。**「メンテナンス」→「デバイスアップグレード」**をタップします。

USBフラッシュドライブを挿入します。**デバイスアップグレード**をタップし、**→ USB経由で更新**を選択すると、デバイスがUSBフラッシュドライブ内のdigicap.davファイルを読み込み、アップグレードを開始します。

7.11.4 設定の復元

デバイス経由で工場設定に復元

すべての設定が工場出荷時設定に復元されます。

初期画面を3秒間長押しし、ジェスチャーに従って左右にスワイプしてホーム画面にログインします。**メンテナンス → 工場出荷時設定への復元**をタップします。システムが再起動して設定が適用されます。

デバイス経由でデフォルト設定に復元

通信設定を除くすべてのパラメーターおよびリモートでインポートされたユーザー情報は、デフォルト設定に復元されます。

初期画面を3秒間長押しし、ジェスチャーに従って左右にスワイプし、ホーム画面にログインします。**「メンテナンス」**をタップ **→ 「デフォルト設定に復元」を**タップ。システムが再起動して設定が適用されます。

通信設定を除くすべてのパラメーターおよびリモートでインポートされたユーザー情報は、システムデフォルト設定に復元されます。デフォルト設定の復元後、システムが再起動します。

デバイス再起動

デバイスを手動で再起動できます。

最初の画面を3秒間長押しし、ジェスチャーに従って左右にスワイプしてホーム画面にログインします。**「メンテナンス」**をタップ **→ 「再起動」**をタップ。

7.12 ビデオインターコム

クライアントソフトウェアにデバイスを追加した後、クライアントソフトウェアからデバイスに呼び出す、デバイスからメインステーションに呼び出す、デバイスからクライアントソフトウェアに呼び出す、デバイスから室内ステーションに呼び出す、またはデバイスから特定の部屋に呼び出すことができます。

7.12.1 デバイスからクライアントソフトウェアに呼び出す

手順

1. 付属のディスクまたは公式ウェブサイトからクライアントソフトウェアを取得し、画面の指示に従ってソフトウェアをインストールします。
2. クライアントソフトウェアを実行すると、ソフトウェアのコントロールパネルが表示されます。
3. **「デバイス管理」**をクリックして、デバイス管理画面に移動します。
4. クライアントソフトウェアにデバイスを追加します。

注意

デバイスの追加方法の詳細については、*「デバイスを追加」*を参照してください。

5. クライアントソフトウェアを起動します。
   1) デバイスの初期画面で「」をタップします。
   2) ポップアップ ウィンドウに ***0*** を入力します。
   3) をタップしてクライアントソフトウェアを起動します。
6. クライアントソフトウェアのポップアップ画面で**「応答」**をタップすると、デバイスとクライアントソフトウェアの間で双方向音声通話を開始できます。

注意

デバイスが複数のクライアントソフトウェアに追加されている場合、デバイスがクライアントソフトウェアに呼び出しを行った際、デバイスを最初に追加したクライアントソフトウェアのみが着信ウィンドウを表示します。

7.12.2 デバイスからのコールセンター

手順

1. 付属のディスクまたは公式ウェブサイトからクライアントソフトウェアを取得し、画面の指示に従ってインストールしてください。
2. クライアントソフトウェアを実行すると、ソフトウェアのコントロールパネルが表示されます。
3. **「デバイス管理」**をクリックして、デバイス管理画面に移動します。
4. クライアントソフトウェアにメインステーションとデバイスを追加します。

注意

デバイスの追加に関する詳細については、*「デバイスを追加」*を参照してください。

5. リモート設定ページで、メインステーションのIPアドレスとSIPアドレスを設定します。

注意

操作の詳細については、メインステーションのユーザーマニュアルを参照してください。

6. センターに連絡してください。
   - ***基本設定で***コールセンターを設定している場合、をタップしてセンターに電話をかけることができます。
   - ***基本設定で***コールセンターを設定していない場合、をタップし、→をタップしてセンターに電話をかけることができます。
7. メインステーション経由で通話に応答し、双方向音声通話を開始します。

注意

デバイスはメインステーションを優先して呼び出します。

7.12.3 クライアントソフトウェアからデバイスに電話をかける

手順

1. クライアントソフトウェアを付属のディスクまたは公式ウェブサイトから入手し、画面の指示に従ってソフトウェアをインストールしてください。
2. クライアントソフトウェアを実行すると、ソフトウェアのコントロールパネルが表示されます。
3. **「デバイス管理」**をクリックして、デバイス管理ページに移動します。
4. クライアントソフトウェアにデバイスを追加します。

注意

デバイスの追加方法の詳細については、*「デバイスを追加」*を参照してください。

5. ライブビューページに移動し、追加したデバイスをダブルクリックしてライブビューを開始します。

注

ライブビューページでの操作の詳細については、クライアントソフトウェアのユーザーマニュアルの*「ライブビュー」*を参照してください。

6. ライブビュー画像上で右クリックして、右クリックメニューを開きます。
7. **「Start Two-Way Audio」**をクリックして、デバイスとクライアントソフトウェア間の双方向オーディオを開始します。

7.12.4 デバイスからルームを呼び出す

手順

1. 付属のディスクまたは公式ウェブサイトからクライアントソフトウェアを取得し、表示される指示に従ってソフトウェアをインストールしてください。
2. クライアントソフトウェアを実行すると、ソフトウェアのコントロールパネルが表示されます。
3. **「デバイス管理」**をクリックして、デバイス管理画面に移動します。
4. クライアントソフトウェアに室内ユニットとデバイスを追加します。

注意

デバイスの追加方法の詳細については、*「デバイスを追加」*を参照してください。

5. ユーザーを室内ステーションにリンクし、室内ステーションの部屋番号を設定します。
6. 部屋を呼び出します。
   - ***基本設定で***指定の部屋番号を設定している場合、をタップしてその部屋を呼び出すことができます。
   - ***基本設定で***指定の部屋番号を設定していない場合、タップしてください。ダイヤル画面で部屋番号を入力し、をタップして部屋を呼び出します。
7. 室内端末が通話に応答すると、室内端末との双方向音声通話を開始できます。

7.12.5 デバイスからモバイルクライアントを呼び出す

手順

1. 付属のディスクまたは公式ウェブサイトからモバイルクライアントを取得し、表示される指示に従ってソフトウェアをインストールします。
2. モバイルクライアントを実行し、デバイスをモバイルクライアントに追加します。

注意

詳細については、モバイルクライアントのユーザーマニュアルを参照してください。

3. **基本設定**を入力→**のショートカットキー**を選択し、**Call APP**を有効にします。
4. 最初の画面に戻り、モバイルクライアントを起動します。
   1) タッ をタップします。
   2) タッ をタップしてモバイルクライアントを呼び出します。

第8章 ウェブブラウザ経由での操作

8.1 ログイン

ウェブブラウザまたはクライアントソフトウェアのリモート設定からログインできます。

注意
デバイスがアクティベートされていることを確認してください。アクティベーションに関する詳細情報は、*アクティベーション*をご覧ください。

ウェブブラウザ経由でのログイン

ウェブブラウザのアドレスバーにデバイスのIPアドレスを入力し、**Enterキー**を押してログインページに移動します。
デバイスのユーザー名とパスワードを入力し、**[ログイン]** をクリックします。

クライアントソフトウェアのリモート設定経由でログイン

クライアントソフトウェアをダウンロードして開きます。デバイスを追加した後、[ ] をクリックして設定画面に移動します。

8.2 パスワードを忘れた場合

ログイン時にパスワードを忘れた場合、メールアドレスまたはセキュリティ質問を使用してパスワードを変更できます。

ログイン画面で「**パスワードを忘れた**」をクリックします。
検証モードを選択します。

セキュリティ質問による確認

セキュリティ質問に回答してください。

メール認証

1. QRコードをエクスポートし、***pw_recovery@hikvision.com*** 宛てに添付ファイルとして送信してください。
2. 5分以内に、ご登録のメールアドレスに検証コードが送信されます。
3. 確認コードを「確認コード」欄に入力し、ご本人確認を行ってください。**次に「次へ」**をクリックし、新しいパスワードを作成し、確認してください。

8.3 Webプラグインのダウンロード

プラグイン非対応のライブビューと、プラグインをダウンロード後のライブビューの両方が利用可能です。より良いライブビューをご利用いただくためには、ライブビュー用のプラグインのダウンロードを推奨します。

「 」をクリックしてください。→「**Download Web Pug-In**」をクリックして、プラグインをローカルにダウンロードしてください。

8.4 ヘルプ

8.4.1 オープンソースソフトウェアライセンス

オープンソースソフトウェアのライセンスを確認できます。

画面右上にある「」をクリックし、→ **Open Source Software Statement** を選択してライセンスを確認してください。

8.4.2 オンラインヘルプドキュメントを表示

Web 設定のヘルプドキュメントを表示できます。

Webページの右上にある「」をクリックし、次に**「→ Online Document」**をクリックしてドキュメントを表示します。

8.5 ログアウト

アカウントからログアウトします。

「admin」をクリックし、→ の**「Logout」**をクリックし、→ の**「OK」**をクリックしてログアウトします。

8.6 Web ブラウザからのクイック操作

8.6.1 パスワードを変更

デバイスパスワードを変更できます。

ウェブページの右上にある「」をクリックして、**パスワード変更**ページに移動します。ドロップダウンリストからセキュリティ質問を選択し、回答を入力してください。

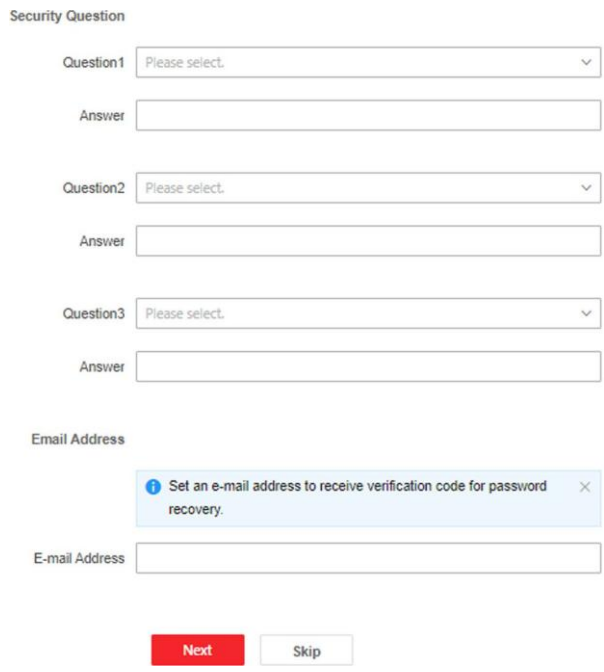


図8-1 パスワードの変更

「**次へ**」をクリックして設定を完了します。または「**スキップ**」をクリックしてこのステップをスキップします。

8.6.2 言語を選択

デバイスのシステム言語を選択できます。

ウェブページの右上にある「」をクリックして、**デバイス**言語設定ページに移動します。ドロップダウンリストからデバイスシステムの言語を選択できます。

デフォルトでは、システム言語は英語です。

注意

システム言語を変更すると、デバイスが自動的に再起動します。

8.6.3 時間設定

ウェブページの右上にある「」をクリックしてウィザード画面に移動します。デバイス言語を設定後、「**次へ**」をクリックして「**時間設定**」画面に移動できます。

タイムゾーン

ドロップダウンリストから、デバイスが所在するタイムゾーンを選択してください。

タイムシンクロナイズ。

NTP

NTPサーバーのIPアドレス、ポート番号、および間隔を設定する必要があります。

手動

デフォルトでは、デバイスの時間は手動で同期されます。デバイスの時間を手動で設定するか、または**「コンピュータの時間と同期」にチェック**を付けて、デバイスの時間をコンピュータの時間と同期させることができます。

サーバーアドレス/NTPポート/間隔

サーバーアドレス、NTP ポート、および間隔を設定できます。

DST

DSTの開始時間、終了時間、およびバイアス時間を表示できます。

「次へ」をクリックして設定を保存し、次のパラメーターに移動します。または**「スキップ」**をクリックして時間設定をスキップします。

8.6.4 環境設定

デバイスを起動した後、より適切なデバイス動作のため、アプリケーションモードを選択してください。

手順

1. ウェブページの右上にある「」をクリックしてウィザードページに移動します。デバイス言語と時間を設定後、**「次へ」**をクリックして**環境**設定ページに移動します。
2. **「室内」**または**「その他」**を選択します。

注意

- デバイスを室内の窓の近くなどに設置した場合、または顔認識機能が正常に動作しない場合は、**「その他」**を選択してください。
- アプリケーションモードを設定せずに**「次へ」**をタップすると、システムはデフォルトで**「室内」**を選択します。
- 他のツールを使用してリモートでデバイスをアクティブ化した場合、システムはデフォルトで**「室内」**をアプリケーションモードとして選択します。

設定を保存して次のパラメーターに進むには**「次へ」**をクリックしてください。または、環境設定をスキップするには**「スキップ」**をクリックしてください。

8.6.5 プライバシー設定

画像のアップロードと保存の設定を行います。

ウェブページの右上にある「」をクリックして、ウィザードページに移動します。

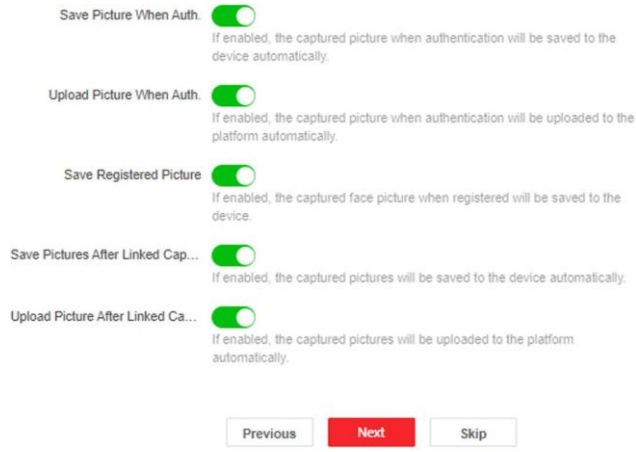


図8-2 プライバシー設定

画像のアップロードと保存

認証時に画像を保存する

認証時に画像を自動的に保存します。

認証時に画像をアップロード

プラットフォームへの認証時に画像を自動的にアップロードします。

登録済み画像の保存

この機能を有効にすると、登録された顔画像がシステムに保存されます。

リンクしたキャプチャ後に画像をアップロードする

リンクされたカメラで撮影した写真をプラットフォームに自動的にアップロードします。

リンクしたカメラで撮影した写真を保存する

この機能を有効にすると、リンクされたカメラで撮影した写真をデバイスに保存できます。設定を保存して次のパラメーターに進むには**「次へ」**をクリックしてください。または、プライバシー設定をスキップするには**「スキップ」**をクリックしてください。

8.6.6 管理者設定

手順

1. ウェブページの右上にある「 」をクリックしてウィザードページに移動します。

2. 管理者の従業員IDと名前を入力します。

3. 追加する認証情報を選択します。

注

少なくとも1つの資格情報を選択してください。

1) **「顔を追加」**をクリックして、ローカルストレージから顔写真をアップロードしてください。

注意

アップロードする画像は200KB以内であり、JPG、JPEG、PNG形式である必要があります。

2) **「カードを追加」**をクリックして、カード番号を入力し、カードの属性を選択してください。

注意

最大5枚のカードがサポートされます。

3) **「指紋を追加」**をクリックして指紋を追加してください。

注意

最大10つの指紋が登録可能です。

「完了」をクリックして設定を完了してください。

8.6.7 番号とシステムネットワーク

手順

1. ウェブページの右上にある「 」をクリックしてウィザードページに移動します。以前の設定が完了したら、**「次へ」**をクリックして**「番号とネットワーク システム ネットワーク」**の設定ページに移動します。
2. デバイスタイプを設定します。

注意

- デバイスタイプを「**ドアステーション**」に設定した場合、**フロア番号**、**ドアステーション番号**、**コミュニティ番号**、**ビル番号**、**ユニット番号**、**フロア番号**、および**ドアステーション番号**を設定できます。
- デバイスタイプを「**外ドアステーション**」に設定すると、**外ドアステーション番号**を設定できます。

コミュニティ番号

デバイスタイプ

このデバイスはドアステーションまたは外ドアステーションとして使用できます。ドロップダウンリストからデバイス タイプを選択してください。

コミュニティ番号

デバイスのコミュニティ番号を設定します。

建物番号

デバイスの建物番号を設定してください。

ユニット番号

デバイスのユニット番号を設定します。

階番号

デバイスが設置されている階番号を設定してください。

ドアステーション番号

インストールされたドアステーションの番号を設定してください。

注意
メインドアステーションの番号は0で、サブドアステーションの番号は1から16までです。

外ドアステーション番号

デバイスにインストールされた外ドアステーションの番号を設定してください。

注
番号は1から99までです。

3. ビデオインターコムのネットワークパラメーターを設定します。

登録パスワード

メインステーションの通信用登録パスワードを設定します。メインステーションの通信用登録パスワードを設定します。

メインステーションのIPアドレス

通信に使用するメインサーバーのIPアドレスを入力してください。

プライベートサーバーIP

SIPサーバーのIPアドレスを指します。通信に使用するメインステーションのIPアドレスを入力してください。この時点では、メインステーションがSIPサーバーとして機能します。他のインターコムデバイスはこのサーバーアドレスに登録する必要があります。

プロトコル1.0を有効にする

有効にすると、ドアステーションは古いプロトコルバージョンでメインステーションに登録できます。無効にすると、ドアステーションは新しいプロトコルバージョンでメインステーションに登録できます。

4. 設定を保存するには、設定完了後**「完了」**をクリックしてください。

8.7 ユーザー管理

「追加」をクリックして、その人の情報を追加します。基本情報、証明書、認証、設定を含むすべての情報を入力してください。

基本情報を追加

「Person Management」をクリックし、**「→」をクリックして**「Add Person」ページに移動します。
従業員ID、氏名、性別、人物の種類を含む、人物の基本情報を入力します。

人物タイプに**「訪問者」**を選択した場合、訪問時間を設定できます。
カスタムタイプを選択すると、名前を編集できます。変更した名前はデバイスに適用されます。設定を保存するには、**[保存]**をクリックしてください。

権限時間の設定

「Person Management」をクリックし、**「→」をクリックして**「Add」を選択し、追加ページに移動します。

「**長期有効ユーザーを有効にする**」または「**長期有効ユーザー**を設定する」を選択すると、ユーザーは設定した時間期間内のみ権限を取得できます。

ドアの権限を設定します。

保存をクリックして設定を保存します。

デバイス番号を設定します。

→「Person Management」をクリックします。**「→」をクリックします。「Add Person」をクリックして**「Add Person」ページに移動します。

「階番号」と**「部屋番号」**のテキストボックスをクリックし、1から999までの数値を入力して階番号と部屋番号を設定します。

「保存」をクリックして設定を保存します。

認証設定

「Person Management」をクリックし、**→「Add」**をクリックして「Add Person」ページに移動します。認証タイプを設定します。

保存をクリックして設定を保存します。

カードを追加

「Person Management」をクリックし、**「→」を選択し、**「Add」をクリックして「Add Person」ページに移動します。

「カードを追加」をクリックし、**カード番号**を入力し、**プロパティ**を選択し、OKをクリックしてカードを追加します。設定を保存するには**「保存」**をクリックします。

顔写真を追加

「Person Management」をクリックし、**「→」をクリックして**「Add」を選択し、顔写真を追加するページに移動します。**「+ Upload」**をクリックして、ローカルPCから顔写真をアップロードします。

注意

画像形式はJPG、JPEG、またはPNGで、サイズは200 KB未満である必要があります。

「保存」をクリックして設定を保存します。

指紋を追加

注意

指紋機能に対応したデバイスのみ、指紋を追加できます。

「Person Management」をクリックし、**→「Add」**を選択して「Add Person」ページに移動します。

「指紋を追加」をクリックし、デバイスの指紋認証モジュールに指を置いて指紋を追加します。

「保存」をクリックして設定を保存します。

手のひら指紋を追加

注意

- 手のひら認証機能に対応したデバイスのみ、手のひら認証を追加できます。
- 最大10,000件の手のひらプリントと手のひら静脈を追加できます。

「Person Management」をクリックし、**→「Palm Printを追加」**を選択して「Add Person」ページに移動します。
デバイスの周辺モジュールから5~ 12 cmの距離に手のひらを置きます。設定を保存するには**「保存」**をクリックします。

キーフォブを追加

「Person Management」をクリックし、**→「Add」**をクリックして「Add Person」ページに移動します。
「+」をクリックし、**「キーフォブを追加」**を選択し、シリアル番号を入力し、**「OK」**をクリックします。キーフォブの左上と右下の角のキーを10秒間長押しして、顔認識端末とペアリングします。

注意

各ユーザーは最大1つのキーフォブを追加でき、デバイスは最大5,000個のキーフォブを追加できます。キーフォブのシリアル番号は「Q-Z」で始まり、その後8桁のアラビア数字が続きます。

デバイス番号の設定

「Person Management」をクリックし、**「→」をクリックして**「Add」を選択し、追加ページに移動します。
ユーザーの基礎情報を入力します。デバイス番号モジュールに移動します。**追加**をクリックし、ユーザーが所属する部屋番号と階番号を入力します。**追加**または**保存して続行**をクリックします。

人物の削除

ユーザー管理ページで削除するユーザーを選択し、**「削除」**をクリックします。すべてのユーザーを削除するには**「すべてクリア」**をクリックします。

人物の編集

人物管理ページで、編集が必要な人物を選択します。人物情報を編集するには、[✎]をクリックします。

フィルタ

人物管理ページで、**従業員ID/名前/カード番号**を入力します。**資格ステータス**を選択し、**フィルター**をクリックして人物をフィルターします。**リセット**をクリックしてすべての条件をクリアします。

8.8 アクセス制御管理

8.8.1 概要

デバイスのライブ動画、リンクされたデバイス、人物情報、ネットワーク状態、基本情報、およびデバイス容量を確認できます。

機能説明:

ドア状態

動画内の「 」をクリックすると、デバイスのライブ動画を表示できます。

ライブビューを開始する際に音量を設定してください。

注意

双方向オーディオを開始時に音量を調整すると、繰り返し音が聞こえる場合があります。

ライブビューを開始時に画像を撮影できます。

/ / /

ドアの状態は「開いている」「閉まっている」「開いたまま」「閉まったまま」です。

ライブビューを開始時に録画できます。

ライブビューを開始する際にストリーミングタイプを選択できます。メインストリーム、サブストリーム、またはサードストリームから選択できます。

フルスクリーン表示。

制御状態

ドアの開閉状態（開く、閉じる、開いたまま、閉じたまま）を、実際のニーズに応じて制御できます。

リアルタイムイベント

従業員ID、名前、カード番号、イベントタイプ、時間、操作内容を確認できます。また、**「詳細を表示」**をクリックすると、イベント検索ページに移動できます。イベントタイプを選択し、従業員ID、名前、カード番号、開始時間、終了時間を入力し、**「検索」**をクリックすると、結果が右側のパネルに表示されます。

デバイスリンク

リンクされたデバイスの数量とステータスを確認できます。

注

「詳細を表示」をクリックすると、該当するページに移動します。

ユーザー情報

追加された情報と追加されていない情報の両方を確認できます。

ネットワーク状態

有線ネットワーク、無線ネットワーク、Hik-Connect、ISUP、OTAP、およびVoIPの接続状態と登録状態を確認できます。

基本情報

モデル、シリアル番号、およびファームウェアバージョンを確認できます。

デバイス容量

人物、顔、指紋、カード、手のひら認証、およびイベントの容量を確認できます。

注意

指紋または手のひら印刷モジュールがインストールされているデバイスのみ、指紋または手のひら印刷の容量を表示できます。

8.8.2 イベント検索

「イベント検索」をクリックして検索画面に移動します。

検索条件を入力してください。イベントの種類、従業員ID、名前、カード番号、開始時間、終了時間を入力し、**[検索]**をクリックしてください。

検索結果は右側のパネルに表示されます。

8.8.3 ドアパラメーター設定

ドアの解錠パラメーターを設定します。

ドア番号を選択してください。

設定するドアを選択します。

「アクセス制御」→「→パラメーター設定」→「→ドアパラメーター」をクリックして設定画面に移動します。

ドア番号を選択してください。通常、ドア1はデバイスと接続されたドアであり、ドア2はセキュアドア制御ユニットと接続されたドアです。

その他のドアパラメーターを設定し、**[保存]**をクリックしてください。

デバイスのオンライン状態を表示

デバイスのステータスを表示し、更新します。

アクセス制御 → パラメーター設定 → ドアパラメーターをクリックして設定画面に入ります。デバイスのオンラインステータスを確認できます。**リフレッシュ**をクリックしてデバイスのステータスを更新します。

ドア名を設定

ドア名を作成します。

アクセス制御をクリックし、**→パラメーター設定、→ ドアパラメーター**を選択して設定画面を開きます。**ドア名**を入力し、**保存**をクリックします。

PC ウェブ経由でドアの開錠時間を設定

カードをかざした後にドアロックが開く時間を設定できます。

アクセス制御をクリックし、**→パラメーター設定→ ドアパラメーター**を選択して設定ページに移動します。
開錠後の動作時間（開錠後、ドアが開いたままの時間を設定します）を設定します。設定時間内にドアが開かれない場合、ドアは自動的にロックされます。設定可能な時間：1～255秒。
「保存」をクリックします。

PCウェブ経由でドアの開錠タイムアウトアラームを設定する

ドアがロック動作時間内に閉まらない場合、アクセス制御ポイントがアラームを鳴らします。

アクセス制御をクリック**→パラメーター設定→ ドアパラメーター**をクリックして設定画面に移動します。
ドア開時間切れアラームを設定します。ドアがロック動作時間に達しても閉まらない場合、アクセス制御ポイントがアラームを鳴らします。0に設定すると、アラームは有効になりません。
「保存」をクリックします。

PCウェブ経由でドア磁気センサータイプを設定します。

ドアの接触タイプは配線方法に応じて選択できます。

アクセス制御 → パラメーター設定 → ドアパラメーターを選択して設定画面を開きます。磁気センサーの種類を「常時閉」または「常時開」から選択します。デフォルトでは「**常時閉**」に設定されています。
（特殊な要件を除く）。
保存をクリックします。

PCウェブ経由で退出ボタンを設定

実際の配線方法に応じて、退出ボタンを「常時開」または「常時閉」に設定します。

アクセス制御 →→ パラメーター設定 →→ ドアパラメーターをクリックして設定画面を開きます。**退出ボタンタイプ**を設定します。デフォルトは「開いたまま」です（特別な要件を除く）。

保存をクリックします。

PCウェブ経由でドアロックの電源オフ状態を設定する

ドアロックの電源が切れる際のドアロックの状態を設定できます。

「アクセス制御」→「→パラメーター設定」→「→ ドアパラメーター」をクリックして設定画面を開きます。**ドアロックの電源オフ状態**を設定します。デフォルトでは「閉じたまま」に設定されています。

「保存」をクリックします。

PCウェブ経由で延長開錠時間を設定

拡張アクセス権限を持つユーザーがカードをかざした後、適切な遅延後にドアコンタクトを有効にできます。

アクセス制御をクリックし、**→パラメーター設定、→ ドアパラメーター**を選択して設定画面を開きます。

拡張開錠時間を設定します。拡張アクセス権限を持つユーザーがカードをかざした後、適切な遅延後にドアの接触センサーを有効にできます。

保存をクリックします。

PC ウェブ経由で最初のユーザーによるドアの開いたまま保持時間を設定します。

最初の人が認証されると、複数の人物がドアへのアクセスまたは他の認証アクションを実行できます。

「アクセス制御」をクリックし、**「→パラメーター設定」→「→ ドアパラメーター」**を選択して設定画面を開きます。

最初の人がドア内にいる際のドアの開状態持続時間を設定し、**「保存」**をクリックします。

PCウェブ経由で緊急コードを設定

緊急コードを設定後、緊急事態が発生した際にコードを入力してドアを開錠します。同時に、アクセス制御システムは緊急事態を報告します。

「アクセス制御」→「→」→「パラメーター設定」→「→」→「ドアパラメーター」をクリックして設定画面を開きます。緊急コードを設定し、**「保存」**をクリックします。

注意

緊急コードとスーパーパスワードは重複できません。通常、4から8桁の数字で構成されます。

PCウェブ経由でスーパーパスワードを設定

管理者または指定されたユーザーがスーパーパスワードを入力してドアを開錠できます。

アクセス制御 → パラメーター設定 → ドアパラメーターをクリックして設定画面を開きます。**スーパーパスワード**を設定し、指定されたユーザーがスーパーパスワードを入力してドアを開錠できます。**保存**をクリックします。

緊急コードとスーパーパスワードは重複できません。通常、4から8桁の数字で構成されます。

注意

8.8.4 認証設定

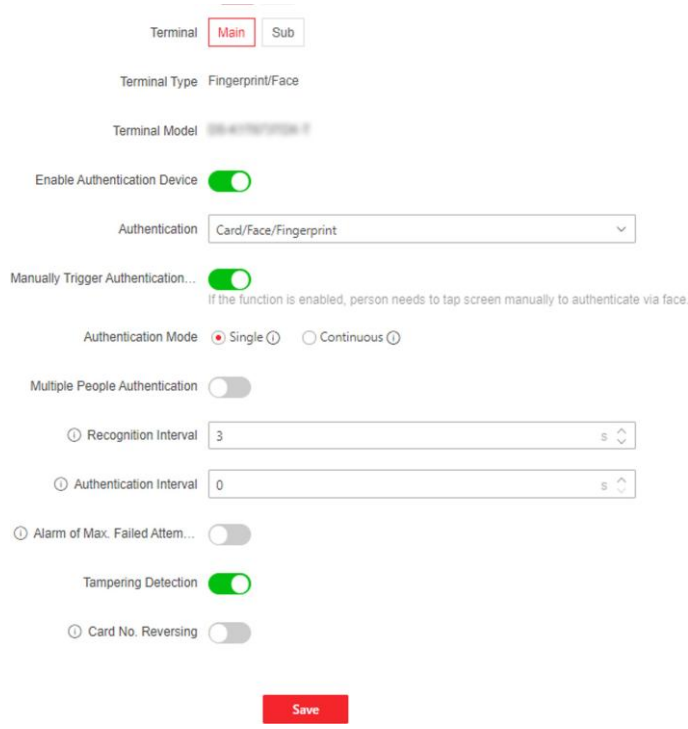


図8-3 認証設定

PCウェブ経由でメインまたはサブカードリーダーを選択

個人認証用の端末を設定します。

アクセス制御の「→パラメーター設定」をクリックし、**→認証設定**を選択して設定画面に入ります。端末をメインまたはサブカードリーダーとして選択します。

その他のパラメーターを設定し、**[保存]** をクリックします。

PCウェブ経由でターミナルの種類とモデルを確認する

ターミナルの種類とモデルを確認できます。

アクセス制御をクリックします。**→ パラメーター設定をクリックします。→ 認証設定**をクリックして設定ページに移動します。**ターミナルタイプ**と**ターミナルモデル**を確認します。

PC Web経由で認証デバイスを有効化

有効化後、認証端末でカード読み取りが可能になります。

手順

1. **アクセス制御**をクリックし、**→パラメーター設定、→認証設定**を選択して設定ページに移動します。
2. **認証デバイスを**有効にします。有効化後、端末は通常通りカード読み取りに使用できます。
3. **保存**をクリックします。

PCウェブ経由での認証を設定します。

証明書を設定します。

アクセス制御をクリックします。**→パラメーター設定→認証設定**をクリックして設定画面に移動します。

メインのカードリーダーを端末として選択した場合、ドロップダウンリストから「認証」を選択できます。認証方法が複数ある場合は、**「シングルクレデンシャル認証タイムアウト」**と「**初期認証タイプの制御**」を設定する必要があります。

シングルクレデンシャル認証タイムアウト

各認証の有効期間を設定できます。

注意

パスワード認証のタイムアウト時間はデフォルトで20秒です。この設定は上記の設定によって制限されません。

初期認証タイプの制御

有効にすると、選択されたすべてのタイプが初回認証に使用可能です。

ターミナルとしてサブカードリーダーを選択した場合、ドロップダウンリストから「認証」を選択できます。
保存をクリックします。

PCウェブ経由で顔認証を手動でトリガー

「顔認証による手動認証のトリガー」を有効にした後、顔認識のため、デバイスの画面に手動でタッチする必要があります。

アクセス制御をクリックし、**→パラメーター設定、→認証設定**を選択して設定画面に移動します。
メインのカードリーダーをターミナルとして選択した場合、**顔認証による手動認証を**有効にするをクリックし、認証モードを選択します。

単一認識

前の顔認識が完了した後（成功または失敗に関わらず）、次の認識をトリガーするために画面をタップする必要があります。

連続

認識をトリガーした後、デバイスがスリープモードに入るまで顔認証が可能です。

「保存」をクリックします。

PCウェブ経由で複数人認証を有効にする

有効にすると、複数のユーザーが同時に顔認証を行うことができます。

「アクセス制御」→「→パラメーター設定」→「→認証設定」をクリックして設定画面に移動します。
端末をメインのカードリーダーとして選択し、**複数人認証を**有効にし、**保存**をクリックします。

PC Web経由で認識間隔を設定

認証時に連続する2回の顔認識の間隔を設定します。

アクセス制御をクリックし、**→パラメーター設定、→認証設定**を選択して設定画面に移動します。端末をメインまたはサブカードリーダーとして選択し、認識間隔を設定した後、**保存**をクリックします。

注意
1から10までの数値を入力してください。

PC Web 経由で認証間隔を設定

同じ人物の認証時の認証間隔を設定できます。設定された間隔内では、同じ人物は1回のみ認証可能です。2回目の認証は失敗します。設定された間隔内に他の人が認証した場合、その人物は再度認証可能です。

アクセス制御をクリックし、**→パラメーター設定、→認証設定**を選択して設定画面に移動します。メインのカードリーダーとして端末を選択し、**認証間隔**を設定し、**保存**をクリックします。

PC ウェブ経由で最大失敗試行回数のアラームを有効にする

設定値に達した際にアラームを報告するように有効にします。

アクセス制御をクリックし、**→パラメーター設定、→認証設定**を選択して設定ページに移動します。

端末をメインまたはサブカードリーダーとして選択し、**最大失敗試行回数アラームを**有効にし、**最大認証失敗試行回数を**設定します。

保存をクリックしてください。

PC ウェブ経由でパームプリント認識タイムアウト閾値と認識間隔を設定する

認証時に連続したパームプリント認識の間隔とタイムアウト閾値を設定します。

アクセス制御の「→パラメーター設定」をクリックします。**→認証設定をクリック**して設定画面に移動します。

端末をメインまたはサブカードリーダーとして選択した場合、**パームプリント認識タイムアウト閾値**と**パームプリント認識間隔**を設定し、**保存**をクリックします。

PC Web経由で改ざん検出の有効/無効を設定します。

改ざん検出機能を有効にすると、カードリーダーが取り外されたり持ち去られたりした際に、デバイスが自動的に改ざんイベントを生成します。

「アクセス制御」→「→パラメーター設定」→「→認証設定」をクリックして設定画面に移動します。

実際のニーズに応じて、**改ざん検出を**有効または無効に設定します。機能を有効にした場合、カードリーダーが取り外されたり持ち去られたりすると、デバイスは自動的に改ざんイベントを生成します。機能を無効にした場合、アラームイベントは生成されません。

「保存」をクリックします。

PC Web経由でのカード番号反転の有効/無効設定

カード番号の逆表示機能を有効または無効にできます。

アクセス制御 →→ パラメーター設定 →→ 認証設定をクリックして設定画面に移動します。

カード番号反転を有効にすると、読み取ったカード番号が逆順で表示されます。**保存**をクリックします。

サブカードリーダーの位置を設定します

サブカードリーダーの位置を選択できます。

アクセス制御 →→ パラメーター設定 →→ 認証設定をクリックして設定画面に入ります。
サブカードリーダーをターミナルとして選択した場合、サブカードリーダーの位置を「**メインカードリーダーと異なる側**」**または「メインカードリーダーと同じ側」から**選択できます。**保存をクリックします。**

コントローラーとの通信をPCウェブ経由で設定

各サブカードリーダーのコントローラーとの通信を設定できます。設定した時間内にカードリーダーがアクセスコントローラーと接続できない場合、カードリーダーはオフライン状態になります。

「アクセス制御」→「→パラメーター設定」→「→認証設定」をクリックして設定画面に入ります。
ターミナルをサブカードリーダーとして選択し、**[コントローラーとの通信間隔] を [毎回]** に設定し、**[保存]** をクリックします。

Webクライアント経由でのパスワード入力のタイムアウト期間を設定します

パスワードの2文字を入力する最大間隔を設定します。1文字を入力した後、設定された間隔内に次の文字が入力されない場合、入力された文字はすべて自動的にクリアされます。

「アクセス制御」→「→パラメーター設定」→「→認証設定」をクリックして設定画面に移動します。
サブカードリーダーをターミナルとして選択した場合、**パスワード入力時の最大間隔**を設定し、**[保存]をクリックします。**

PC Web経由でOK LEDの極性とエラー LEDの極性を設定します。

OKとERRインターフェースのダイオードの極性を実際の配線に合わせて設定します。デフォルトは正極性です。

「アクセス制御」→「→パラメーター設定」→「→認証設定」をクリックして設定画面に入ります。
ターミナルをサブカードリーダーとして選択した場合、**OK LEDの**極性と**エラーLEDの極性を**設定し、**[保存]**をクリックします。

8.8.5 顔パラメーターの設定

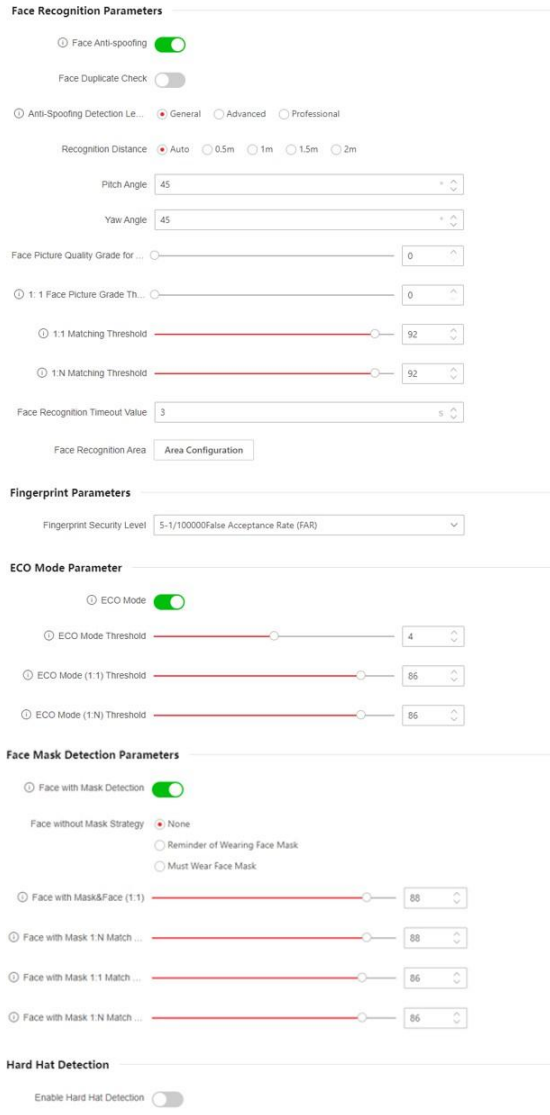


図8-4 顔パラメーターの設定

Webブラウザ経由で顔認証の偽装防止機能を有効/無効にする

有効にすると、デバイスは人物が本物かどうかを認識できます。

アクセス制御をクリックし、→**パラメーター設定**→ Smartを選択して設定画面に移動します。**顔認証偽装防止を**有効にし、**保存**をクリックします。

ライブ顔検出機能を有効または無効にします。有効にすると、デバイスは人物が生きているかどうかを認識できます。顔が生きているものでない場合、認証は失敗します。

顔重複チェックの有効/無効設定

顔重複チェックを有効にした後、顔を追加するたびにシステムは顔の重複をチェックします。重複した顔が検出された場合、通知が表示されます。

注意
リモートで顔を追加する場合や、一括で顔を適用する場合、この機能はサポートされていません。

アクセス制御をクリックし、→**パラメーター設定をクリックし、→ Smart** をクリックして設定ページに移動します。**顔重複チェックを**有効にします。

保存をクリックします。

PC ウェブ経由でアンチスプーフィング検出レベルを設定

顔認証の偽装防止機能を有効にした後、ライブ顔認証時に使用するマッチングのセキュリティレベルを設定できます。

アクセス制御をクリックし、→**パラメーター設定→ Smart** を選択して設定ページに移動します。アンチスプーフィング検出レベルを選択し、**保存**をクリックします。
一般、詳細、プロフェッショナルから選択できます。レベルが高いほど、偽認識率が低く、拒否率が高くなります。

PCウェブ経由で認識距離を設定する

認証ユーザーとデバイスカメラの間の距離を設定できます。**アクセス制御 → パラメーター設定 → スマート**をクリックして設定画面に移動します。

認識距離を選択し、**保存**をクリックします。

PCウェブ経由でピッチ角度を設定

顔認識および認証時のレンズのピッチ角度を設定できます。**アクセス制御 → パラメーター設定 → スマート**をクリックして設定画面に移動します。

注意
異なるモデルではサポートされるパラメーターが異なる場合があります。実際のページをご確認ください。

ピッチ角度を設定し、**保存**をクリックします。

PCウェブ経由でヨー角を設定

顔認識および認証時にレンズのヨー角を設定できます。**アクセス制御 → パラメーター設定 → スマート**をクリックして設定画面に移動します。

注意
モデルによってサポートされるパラメーターが異なる場合があります。実際のページをご確認ください。

ヨー角を設定し、**保存**をクリックします。

PCウェブ経由での適用時の顔画像品質グレードを設定します

顔認証のグレードは、閾値よりも高い必要があります。**アクセス制御 → パラメーター設定 → スマート**をクリックして設定画面に移動します。

注意
異なるモデルでは異なるパラメーターがサポートされる場合があります。詳細は実際のページをご確認ください。

顔認証**に適用する顔画像の品質グレード**を設定します。顔認証のグレードは、閾値よりも高い必要があります。
保存をクリックしてください。

PCウェブ経由で1:1顔グレード閾値を設定

1:1顔グレード閾値を設定します。

アクセス制御→ パラメーター設定→ Smart に移動します。**1:1 顔画像グレード閾値**を設定し、**保存**をクリックします。
閾値が高いほど、フロントカメラで撮影された画像の品質要件が厳しくなり、認証失敗の通知がより容易になります。

PCウェブ経由でセットフェイス1:1一致閾値を設定

顔認識の1対1一致閾値を設定します。

アクセス制御をクリックし、**→ パラメーター設定→** Smartを選択して設定画面に移動します。顔認証の1対1一致閾値を設定し、**保存**をクリックします。
しきい値の値が大きいほど、顔認証時の誤認率（誤通過率）が低く、誤拒否率（誤拒否率）が高くなります。最大値は100です。

PCウェブ経由で1:N一致閾値を設定

顔の1:Nマッチングの閾値を設定できます。

アクセス制御をクリックし、→**パラメーター設定をクリックし、→Smart** をクリックして設定ページに移動します。1:N マッチング閾値を設定し、**保存**をクリックします。
値が大きいほど、誤認率（FA）が低く、誤拒否率（FRR）が高くなります。最大値は100です。

ウェブブラウザ経由で顔認識領域を設定

顔認識と認証時にレンズの認識領域を設定できます。

アクセス制御→ パラメーター設定→ エリア設定をクリックして設定画面に入ります。
プレビュー画面の黄色いボックスをドラッグして、顔認識の有効領域を左右上下に調整します。
または、ブロックをドラッグするか、数値を入力して有効領域を設定します。**保存**を
クリックします。
「 」「 」「 」をクリックして、キャプチャ、記録、またはフルスクリーン表示に移動します。

PC ウェブ経由で指紋パラメーターを設定する

デバイスの指紋パラメーターを設定できます。

アクセス制御をクリックし、→**パラメーター設定を選択し、→Smart** をクリックして設定画面に移動します。
指紋セキュリティレベルを選択します。レベルが高いほど、偽認識率が低く、拒否率が上昇します。
保存をクリックします。

PC ウェブ経由でパームプリント認識パラメーターを設定

デバイスのパームプリントパラメーターを設定できます。

アクセス制御→ パラメーター設定→ Smart をクリックして設定画面に移動します。
手のひら認証の偽装防止検出を有効にします。**手のひら認証 1:1** の閾値と**手のひら認証 1:N の閾値**を設定します。

注意
きいほど、誤認識率が低く、誤拒否率が大きくなります。最大値は100です。

保存をクリックします。

PC ウェブ経由で ECO モードを有効/無効にする

ECOモードが有効になっている場合、赤外線カメラを使用して低照度または暗い環境での顔認証が可能です。

アクセス制御をクリックし、→ **パラメーター設定をクリックし、→** Smartを選択して設定ページに移動します。

ECO モードが有効になっている場合、赤外線カメラを使用して低照度または暗い環境で顔認証を行うことができます。ECO モード (1:N) と ECO モード (1:1) を設定できます。

マスク検出が有効になっている場合、マスク検出パラメーターも設定できます。

ECOモード（1:1）しきい値

ECOモードの1:1マッチングモードで認証する際の一致閾値を設定します。値が大きいほど、誤認率が低く、誤拒否率が大きくなります。最大値は100です。

ECOモード（1:N）しきい値

ECOモードの1:Nマッチングモードで認証を行う際の照合閾値を設定します。値が大きいほど、誤認率（false accept rate）が低く、誤拒否率（false rejection rate）が高くなります。最大値は100です。

マスク着用時の顔認証 1:1 マッチング閾値 (ECO)

マスク着用時の認証において、ECOモードの1:1マッチングモードで認証を行う際の一致閾値を設定します。値が大きいほど、誤認率が低下し、誤拒否率が上昇します。最大値は100です。

マスク着用時の顔認証 1:N マッチング閾値 (ECO)

ECOモードの1:Nマッチングモードでマスクを着用した顔認証を行う際のマッチング閾値を設定します。値が大きいほど、誤認率が低く、誤拒否率が大きくなります。最大値は100です。

保存をクリックします。

PCウェブ経由でマスク着用時の顔検出の有効化/無効化

マスク着用時の顔検出を有効にすると、システムはマスクを着用した顔の写真を認識するか否かを判断します。

アクセス制御をクリックし、→ **パラメーター設定、→** Smartを選択して設定画面に移動します。

マスク着用時の顔検出を有効にすると、**以下の**設定が可能です：**マスクなし顔戦略、マスク着用顔とマスクなし顔（1:1）**、**マスク着用顔 1:N 一致閾値（ECO）**、**マスク着用顔 1:1 一致閾値**、および**マスク着用顔 1:N 一致閾値（ECO）**。

マスクなし顔の戦略

「**なし**」「**マスク着用リマインダー**」「**マスク着用必須**」から選択できます。**マスク着用リマインダー**

認証時にマスクを着用していない場合、デバイスが通知を表示し、ドアが開きます。

マスク着用必須

認証時にマスクを着用していない場合、デバイスが通知を表示し、ドアは閉じたままになります。

マスク着用時の顔とマスクなしの顔（1:1）

顔マスクを使用した1対1マッチングモードでの認証時に、一致値を設定します。値が大きいほど、誤認率（FA）は低く、誤拒否率（FRR）は高くなります。最大値は100です。

マスク着用顔&顔（1:N）

マスクを着用した顔認証時の1:Nマッチングモードで、マッチング閾値を設定します。値が大きいほど、誤認率が低下し、誤拒否率が上昇します。最大値は100です。

マスク着用顔 1:1 マッチング閾値 (ECO)

ECOモードの1:1マッチングモードでマスクを着用した顔認証を行う際の照合値を設定します。しきい値が大きいほど、顔認証時の認識誤り率が低下し、拒否率が上昇します。最大値は100です。

マスク着用時の顔認証 1:N マッチングしきい値 (ECO)

ECOモードの1:Nマッチングモードでマスクを着用した顔認証を行う際の一致閾値を設定します。閾値が大きいほど、顔認証時の認識誤り率が低下し、拒否率が上昇します。最大値は100です。

保存をクリックします。

PCウェブ経由でヘルメット検出の有効/無効を切り替えます。

ハードヘルメット検出を有効にすると、システムは顔認証時に安全ヘルメットの着用を認識します。

アクセス制御をクリックし、**→パラメーター設定、→**Smartを選択して設定画面に移動します。**ヘルメット検出を**有効にし、**保存**をクリックします。

ヘルメット検出を有効にする

リマインダー戦略を設定できます。

着用リマインダー

認証時にヘルメットを着用していない場合、デバイスに通知が表示され、ドアが開きます。

着用必須

ヘルメットを着用していない状態で認証を行った場合、デバイスは警告メッセージを表示し、ドアは開いたままになります。

8.8.6 カード設定

PCウェブ経由でNFC保護の有効/無効を切り替える

有効化後、デバイスはNFCカードを読み取ることができます。

「アクセス制御」→「→パラメーター設定」→「→カード設定」をクリックして設定画面に入ります。

「NFCカード」を有効にし、「保存」をクリックします。有効化後、デバイスはNFCカードを読み取ることができます。アクセス制御デバイスのデータがモバイルデバイスで取得された場合、認証されていないアクセスが発生する可能性があります。この状況を防止するため、NFC機能を無効にすることができます。

M1カードの設定をWebクライアントで有効/無効にする

有効化後、デバイスはM1カードを認識し、ユーザーはデバイス経由でM1カードをスワイプできます。**アクセス制御 → パラメーター設定 → カード設定をクリック**して設定画面に移動します。

M1 カードを有効にするをクリックします。

M1カード暗号化

M1カード暗号化を有効にすると、入口カードのセキュリティレベルが向上します。これにより、入口カードがコピーされにくくなります。

セクター

M1カード暗号化を有効にした後、暗号化セクターを設定する必要があります。

注意

セクター13を暗号化することをおすすめします。

保存をクリックしてください。

EMカードの設定をWebクライアントで有効/無効にする

有効化後、デバイスはEMカードを認識し、ユーザーはデバイス経由でEMカードをスワイプできるようになります。**アクセス制御 → パラメーター設定 → カード設定をクリックして**設定画面に移動します。

EMカード有効化をクリックし、**保存**をクリックします。

注意

- EMカードを読み取れる周辺カードリーダーが接続されている場合、この機能を有効にすると、このカードリーダー経由でもEMカードをスワイプできます。
- デュアル周波数カードモジュールが接続されている場合、EMカードとDESfireカードを同時にスワイプできます。ただし、デバイス上でカードをスワイプすることは無効です。

CPUカードの設定をWebクライアントから有効/無効にする

有効化後、デバイスはCPUカードを認識し、ユーザーはデバイス経由でCPUカードをスワイプできるようになります。**アクセス制御 → パラメーター設定 → カード設定をクリックして**設定画面に移動します。

CPU カードを有効にするをクリックします。

「**CPU カードの内容を読み取る**」をクリックして**有効化します**。有効化後、デバイスは CPU カードから内容を読み取ることができます。

「保存」をクリックします。

DESFire カードの設定

DESFire カードと DESFire カードの内容を読み取る機能を有効にできます。

パラメーター設定 → カード設定をクリックして設定画面を開きます。**DESFire** カードと **DESFire カード**の内容**を読み取りを有効にし、保存**をクリックします。

注意

デュアル周波数カードモジュールが接続されている場合、EMカードとDESFireカードを同時にスワイプできます。ただし、デバイス上でカードをスワイプすることは無効です。

FeliCa カードの設定

FeliCa カードを有効にできます。

パラメーター設定をクリックし、**→ カード設定**を選択して設定画面に入ります。**FeliCaカード有効化**を選択します。

Web経由でカード番号認証パラメーターを設定

デバイス上でカード認証時に読み取るカードの内容を設定します。**アクセス制御 → パラメーター設定 → カード設定** へ移動します。

カード認証モードを選択し、**[保存]** をクリックしてください。

全カード番号

すべてのカード番号が読み込まれます。

3 バイト

デバイスは3バイトを読み込んでカードを読み込みます。

4 バイト

デバイスは4バイトでカードを読み取ります。

8.8.7 エレベーター制御をWeb経由で

手順

1. **アクセス制御**をクリック→**パラメーター設定**→**エレベーター制御パラメーター**。

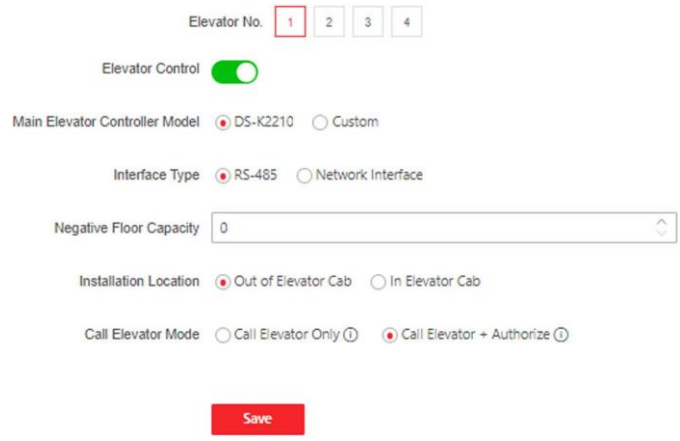


図8-5 エレベーター制御

2. **エレベーター制御を**有効にします。

3. エレベーターのパラメーターを設定します。

メインエレベーターコントローラーモデル

設定対象のエレベーター番号を選択します。

インターフェースタイプ

エレベーター通信の通信方式をドロップダウンリストから選択してください。

RS-485を選択した場合、デバイスを**RS-485**ケーブルでエレベーターコントローラーに接続していることを確認してください。

ネットワークインターフェースを選択した場合、通信用にエレベーターコントローラーのIPアドレス、ポート番号、ユーザー名、パスワードを入力してください。

負の階数容量

負の階数を設定してください。

設置場所

設置場所を「**エレベーターキャビン外**」または「**エレベーターキャビン内**」から選択してください。

エレベーター呼び出しモード

エレベーター呼び出しモードを選択します。

エレベーター呼び出しのみ

認証が完了すると、デバイスはエレベーターを指定の階に呼び出します。

エレベーターを呼び出す+許可

ユーザーが認証に成功すると、デバイスはエレベーターをその階に呼び出し、ユーザーの部屋とリンクされた階のアクセス権限を認証します。ユーザーは対応する階番号を押すことで、目的の階に移動できます。

注意

- このデバイスに最大4つのエレベーターコントローラーを接続できます。
- 最大10つの負階を追加できます。
- 同じデバイスに接続されているエレベーターコントローラーのインターフェースタイプが一致していることを確認してください。

8.8.8 リンク設定

設定されたイベントがトリガーされた場合、設定された方法に従ってイベント情報を中央プラットフォームにアップロードします。

手順

1. **アクセス制御**をクリックし、→**パラメーター設定**、→**リンク設定**を選択して設定画面に移動します。

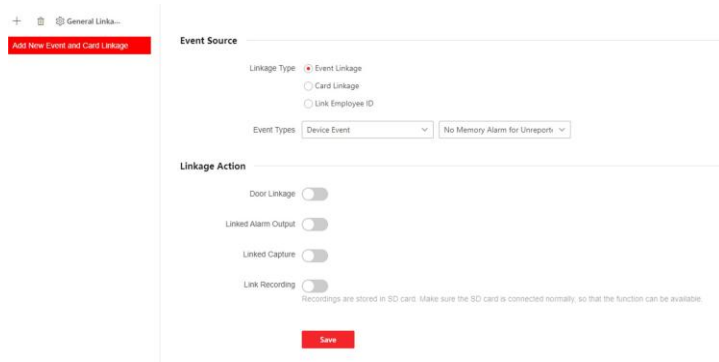


図8-6 連携設定

2. **+**「**」**をクリックします。
3. イベントソースを設定します。連携タイプを「**イベント連携**」「**カード連携**」または「**従業員ID連携**」から選択します。
   - **リンクタイプを**「**イベントリンク**」に選択した場合、実際のニーズに応じてイベントタイプを選択できます。
   - **リンクタイプ**を「**カードリンク**」を選択し、**カード番号**を入力し、**カードリーダー**を選択します。
   - **リンクタイプを**「**従業員IDリンク**」に選択し、**従業員ID**を入力し、**カードリーダー**を選択します。
4. リンク動作を設定します。
   1) **ドアリンクを**有効にし、ドアアクションを選択します。
   2) **リンクアラーム出力を**有効にし、アラーム出力アクションを選択します。
   3) **リンクキャプチャを**有効にします。
   4) **リンク記録を**有効にし、**一般リンク設定**をクリックして事前記録時間と記録遅延を設定し、動画記録時に音声記録を有効にします。**保存**をクリックします。

Note

録音機能を使用するには、SDカードを準備する必要があります。録音後、クリックできます
イベント**検索**をクリックして録画を確認できます。詳細については、*イベント検索*

5. をクリックして設定を有効にします。

8.8.9 PC Web経由で作業モードを設定

デバイスの端末パラメーターを設定できます。

注
この機能は一部のモデルのみ対応しています。詳細については、該当するデバイスをご確認ください。

アクセス制御をクリックし、**→パラメーター設定、→ターミナルパラメーター**を選択して設定ページに移動します。

動作モード

動作モードをアクセス制御モードまたは許可フリーモードに設定できます。

アクセス制御モード

アクセス制御モードはデバイスの通常モードです。アクセスするには、資格情報を認証する必要があります。

8.8.10 リモート認証を設定

デバイスは、ユーザーの認証情報をプラットフォームに送信します。プラットフォームがドアを開けるかどうかを判断します。

アクセス制御に移動し、**→パラメーター設定→ ターミナルパラメーターを選択します**。パラメータ
ーを設定後、**[保存] をクリックします**。

リモート検証

リモート検証を有効にした後、認証時にデバイスは認証情報をプラットフォームにアップロードし、プラットフォームがドアを開けるかどうかを確認します。

ローカルでの認証情報の確認

機能を有効にすると、デバイスは権限を確認しますが、プランテンプレートを推定しません。

8.8.11 プライバシー設定

PCウェブブラウザ経由でイベントの保存タイプを設定

イベントの保存タイプを設定できます。

アクセス制御をクリックし、**→パラメーター設定、→プライバシー設定**を選択して設定画面に移動します。

イベントの保存タイプとして「**古いイベントを定期的に削除**」「**指定した時間に古いイベントを削除**」または「**上書き**」を選択できます。

古いイベントを定期的に削除

ブロックをドラッグするか、数値を入力してイベント削除の期間を設定します。設定された時間経過後に、すべてのイベントが削除されます。

指定した時間に古いイベントを削除

時間を設定し、設定した時間にすべてのイベントが削除されます。

上書き

システムが保存されたイベントが全体の95%を超えたことを検出すると、最も古い5%のイベントが削除されます。

保存をクリックしてください。

PCウェブ経由で認証結果を設定

認証結果の内容（画像、名前、従業員ID、体温など）を設定します。**アクセス制御 → アクセス制御 → パラメータ一設定 → プライバシー設定** を選択します。

認証結果に表示される内容（画像、名前、従業員IDなど）を確認します。

実際の必要に応じて、**名前**非識別化と**ID非識別化を選択します**。非識別化後、名前とIDは内容の一部のみ表示されます。

認証結果の表示期間を設定すると、認証結果は設定された時間期間だけ表示されます。

保存をクリックします。

PC ウェブ経由での画像アップロードと保存の設定

画像のアップロードと保存のパラメーターを設定できます。

アクセス制御をクリックします**。→パラメーター設定をクリックします。→プライバシー設定**をクリックして設定ページに移動します。

認証時に画像を保存。

認証時に画像を自動的に保存します。

認証時に画像をアップロード

プラットフォームへの認証時に画像を自動的にアップロードします。

画像モード

デフォルトとして選択した場合、デバイスはパノラマビューを撮影します。最大画像サイズと画像解像度を設定できます。

マット画像モードを選択した場合、デバイスは顔のみを撮影します。最大画像サイズを設定できます。

登録した画像を保存

この機能を有効にすると、登録された顔画像はシステムに保存されます。

リンク撮影後の画像保存

この機能を有効にすると、リンクされたカメラで撮影した画像をデバイスに保存できます。

リンクしたカメラで撮影した画像をアップロード

リンクされたカメラで撮影した画像をプラットフォームに自動的にアップロードします

登録された手のひらプリント画像を保存

この機能を無効にすると、パームプリントデータのみが保存され、登録された画像は保存されません。

保存をクリック。

PCウェブ経由でデバイス内の画像を削除

登録済み、認証済み、または撮影した顔写真や画像をすべて削除できます。

アクセス制御 → パラメーター設定 → プライバシー設定をクリックして設定画面に移動します。**クリア**をクリックすると、登録済み、認証済み、またはキャプチャされた顔画像または手のひら画像がすべて削除されます。

PC ウェブ経由で PIN モードを設定

設定前に、PINがプラットフォーム適用型個人PINかデバイス設定型個人PINかを確認してください。PINがデバイス設定型個人PINの場合、デバイスまたはPC WebでPINを編集できますが、プラットフォームで設定できません。PINがプラットフォーム適用型個人PINの場合、プラットフォームでPINを設定し、デバイスまたはPC Webでは設定できません。

アクセス制御→ パラメーター設定→ プライバシー設定に移動します。

PIN モードモジュールで、以下のパラメーターを設定できます。パラメーター設定後、**保存**をクリックしてください。

プラットフォーム適用型個人用PIN

プラットフォーム上で個人用PINを作成できます。PINはデバイスに設定する必要があります。デバイスやPC Web上でPINを作成または編集することはできません。

デバイス設定の個人用PIN

デバイスまたはPC WebでPINを作成または編集できます。プラットフォーム上でPINを設定することはできません。

保存をクリックしてください。

8.8.12 設定

Web経由でデバイス番号を設定する

このデバイスはドアステーションまたは外ドアステーションとして使用できます。使用前にデバイス番号を設定してください。

アクセスコントロールをクリックし、**→**、**コール設定**、**→**、**デバイス番号を選択します**。

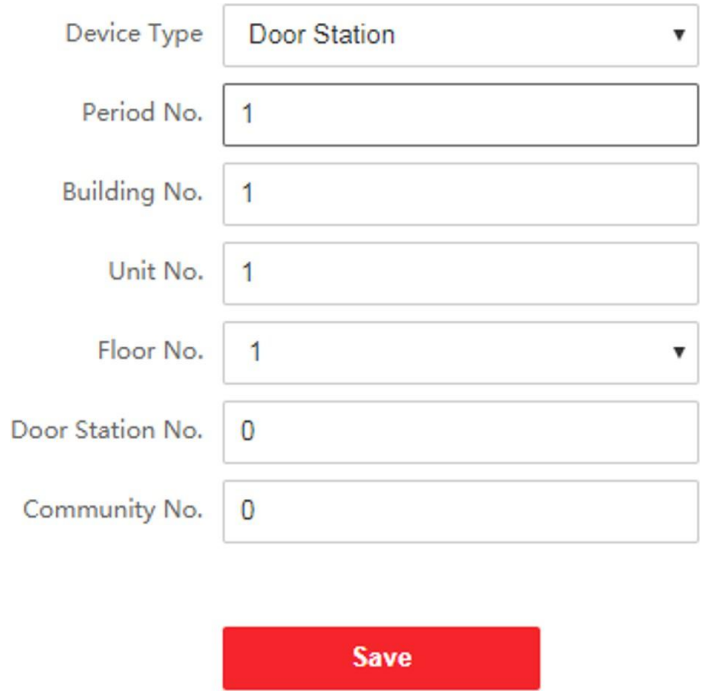


図8-7 デバイス番号設定

デバイスタイプを「**ドアステーション**」に設定した場合、**フロア番号**、**ドアステーション番号**、**コミュニティ番号**、**ビル番号**、**ユニット番号**を設定できます。

デバイスタイプ

このデバイスはドアステーションまたは外ドアステーションとして使用できます。ドロップダウンリストからデバイスタイプを選択してください。

注意
デバイスタイプを変更した場合は、デバイスを再起動する必要があります。

階数

デバイスが設置されている階番号を設定してください。

ドアステーション番号

デバイスが設置されている階番号を設定してください。

注意

- 番号を変更した場合、デバイスを再起動する必要があります。
- メインドアステーションの番号は0です。サブドアステーションの番号は1から16までです。

コミュニティ番号

デバイスのコミュニティ番号を設定してください。

建物番号

デバイスの建物番号を設定してください。

ユニット番号

デバイスのユニット番号を設定します。

注

番号を変更した場合、デバイスを再起動する必要があります。設定を

保存するには、設定完了後に**「保存」**をクリックしてください。

デバイスタイプを「**外ドアステーション**」に設定した場合、外ドアステーション番号とコミュニティ番号を設定できます。

外ドアステーション番号

外ドアステーションをデバイスタイプとして選択した場合、1から

99の間の数値を入力する必要があります。

注意

番号を変更した場合、デバイスを再起動する必要があります。

コミュニティ番号

デバイスのコミュニティ番号を設定します。

ウェブブラウザ経由でビデオインターコムネットワークパラメーターを設定

登録パスワード、メインステーションのIPアドレス、プライベートサーバーのIPアドレスを設定でき、実際のニーズに応じてプロトコル1.0を有効にできます。

「設定」をクリックし、**→ ビデオインターコム ネットワーク**を選択して設定画面に移動します。

登録パスワード

メインステーションの通信用登録パスワードを設定します。メインステーションの通信用登録パスワードを設定します。

メインステーションのIPアドレス

通信に使用するメインステーションのIPアドレスを入力します。

プライベートサーバーIP

SIPサーバーのIPアドレスを指します。通信に使用するメインステーションのIPアドレスを入力してください。この時点では、メインステーションがSIPサーバーとして機能します。他のインターコムデバイスはこのサーバーアドレスに登録する必要があります。

プロトコル 1.0 を有効にする

有効に設定されている場合、ドアステーションは古いプロトコルバージョンでメインステーションに登録できます。無効に設定されている場合、ドアステーションは新しいプロトコルバージョンでメインステーションに登録できます。

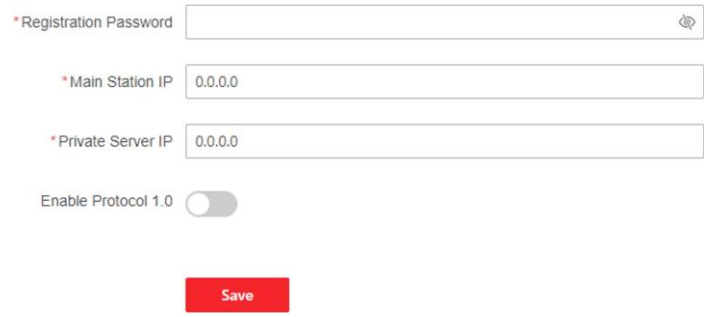


図8-8 ビデオインターコムネットワーク

設定完了後、アクセス制御装置とビデオインターコムドアステーション、室内ステーション、メインステーション、プラットフォームなどとの間で通信が可能になります。

保存をクリックします。

PCウェブ経由で通信時間を設定

最大通信時間を設定します。

アクセス制御の「→」→「Call Settings」→「→」→「Call Settings」に移動します。**最大通信時間**を入力し、**保存**をクリックします。

注意
最大通信時間範囲は90秒から120秒です。

PCウェブ経由で呼び出すにはボタンを押してください

手順

1. **アクセス制御**をクリックし、**→ コール設定をクリックし、→ ボタンを押してコール**設定ページに入ります。

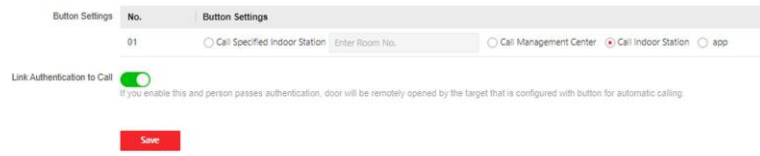


図8-9 ボタンを押して呼び出す

2. 必要に応じて「**指定した室内ステーションへの通話**」「**管理センターへの通話**」「**室内ステーションへの通話**」または「**アプリ**」を選択します。

注意
「**指定の室内ステーションを呼び出す**」を選択した場合、室内ステーションの**部屋番号**を入力する必要があります。

3. 必要に応じて「**リンク認証を有効にする**」を選択してください。有効にした後、認証を通過した人がボタンで自動呼び出しが設定された対象にアクセスすると、ドアが遠隔で解錠されます。
4. 「**保存**」をクリックしてください。

PCウェブ経由での番号設定

部屋のSIP番号を設定します。部屋はSIP番号経由で相互に通信できます。

手順

1. **アクセス制御→ コール設定→ 番号設定**。

図8-10 番号設定

2. 「**追加**」をクリックし、**部屋番号**と**SIP1**の電話番号を入力します。
3. **オプション：**SIP番号を追加するには「**Add**」をクリックし、番号を削除するには「 」をクリックします。
4. **[保存]をクリックします。**
5. **オプション：[削除]** をクリックして、部屋番号とその SIP 番号を削除できます。

8.9 システム設定

8.9.1 PC ウェブ経由でデバイス情報を表示

デバイス名、デバイス番号、言語、モデル、シリアル番号、バージョン、チャンネル数、IO入力、IO出力、ロック、ローカルRS-485番号、レジスタ番号、アラーム入力、アラーム出力、デバイス容量など、詳細情報を表示します。

システムとメンテナンスをクリックします。**→システム構成をクリックします。→システムをクリックします。→システム設定をクリックします。→基本情報**を入力して設定ページに移動します。

デバイス名、デバイス番号、言語、モデル、シリアル番号、バージョン、チャンネル数、IO入力、IO出力、ロック、ローカルRS-485番号、レジスタ番号、アラーム入力、アラーム出力、デバイス容量など、各種情報を確認できます。

ファームウェアバージョンで**「アップグレード」**をクリックすると、アップグレードページに移動してデバイスをアップグレードできます。

8.9.2 時間設定

デバイスのタイムゾーン、同期モード、サーバーアドレス、NTPポート、および間隔を設定します。

システムとメンテナンスをクリックします。**→システム構成をクリックします。→システムをクリックします。→システム設定をクリックします。→タイム設定をクリックします。**

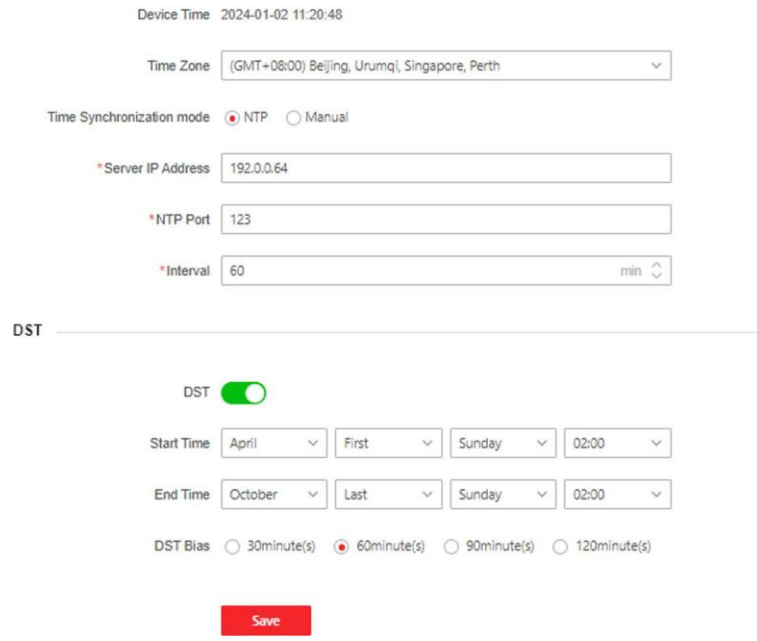


図8-11 タイム設定

設定を保存するには、設定後**「保存」**をクリックします。

タイムゾーン

ドロップダウンリストからデバイスの所在するタイムゾーンを選択します。

時間同期。

NTP

NTPサーバーのIPアドレス、ポート番号、および間隔を設定してください。

手動

デフォルトでは、デバイスの時間は手動で同期されます。デバイスの時間を手動で設定するか、または**「コンピュータの時間と同期」にチェック**を付けて、デバイスの時間をコンピュータの時間と同期させることができます。

サーバー アドレス タイプ/サーバー アドレス/NTP ポート/間隔

サーバーのアドレス タイプ、サーバー アドレス、NTP ポート、および間隔を設定できます。

8.9.3 管理者のパスワードを変更する

手順

1. **システムとメンテナンス**をクリックし、**→ システム構成→ システム→ ユーザー管理 → ユーザー管理を選択します**。

2. 「 」 をクリックします。

3. 古いパスワードを入力し、新しいパスワードを作成します。

4. 新しいパスワードを確認します。

5. **「保存」**をクリックします。

注意

デバイスのパスワードの強度は自動的に確認できます。製品のセキュリティを強化するため、ご自身で選択したパスワード（8文字以上で、大文字、小文字、数字、特殊文字の少なくとも3種類を含む）に変更することを強くおすすめします。また、特に高セキュリティシステムでは、パスワードを定期的に変更することをおすすめします。月次または週次での変更は、製品の保護をさらに強化します。
すべてのパスワードおよびその他のセキュリティ設定の適切な設定は、インストール担当者および/またはエンドユーザーの責任です。

8.9.4 PCウェブ経由のアカウントセキュリティ設定

セキュリティ質問と回答、またはデバイスのメールアドレスを変更できます。設定を変更した後、デバイスのパスワードを忘れた場合は、新しい質問に回答するか、新しいメールアドレスを使用してデバイスのパスワードをリセットする必要があります。

手順

1. **システムとメンテナンス**をクリックし、**→ システム構成→ システム→ユーザー管理 → ユーザー管理 → アカウントセキュリティ設定を選択します**。
2. 実際の必要に応じて、セキュリティ質問またはメールアドレスを変更します。
3. デバイスのパスワードを入力し、**OK**をクリックして変更を確認します。

8.9.5 PC ウェブ経由でデバイスの武装/解除情報を表示

デバイスの武装タイプと武装IPアドレスを確認します。

システムとメンテナンスに移動し、**→ システム構成→ システム→ ユーザー管理 → 警報設定/解除情報 を選択します**。
デバイスの武装/解除情報を表示できます。ページを更新するには**「リフレッシュ」**をクリックしてください。

8.9.6 ネットワーク設定

PC ウェブ経由で基本ネットワークパラメーターを設定

システムとメンテナンスをクリックし、**→ システム構成→ ネットワーク→ ネットワーク設定 → TCP/IP** を選択します。

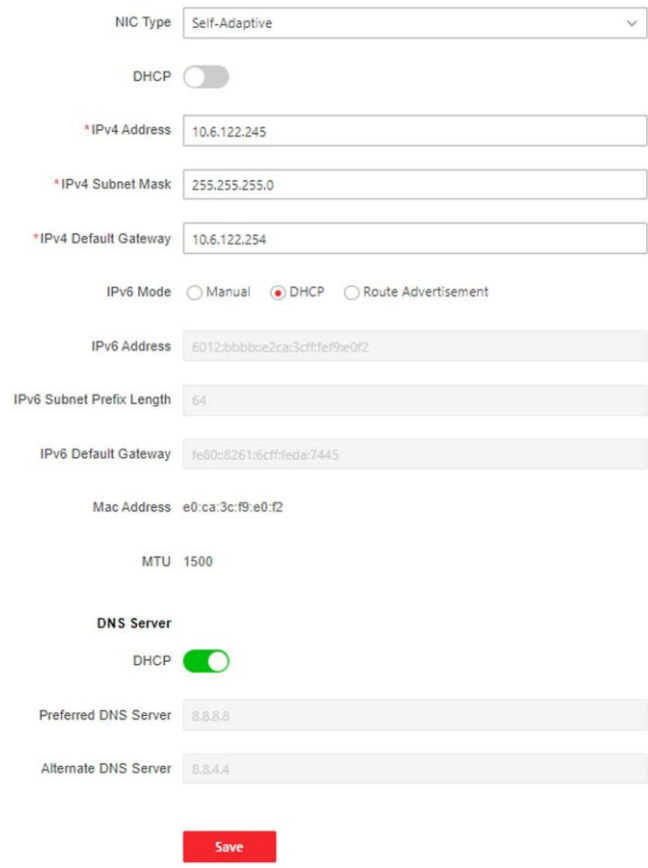


図8-12 TCP/IP設定ページ

パラメーターを設定し、**保存**をクリックして設定を保存します。

NIC タイプ

ドロップダウンリストからNICの種類を選択してください。デフォルトでは「**Auto**」が選択されています。

DHCP

この機能をオフにすると、IPv4アドレス、IPv4サブネットマスク、IPv4デフォルトゲートウェイ、MACアドレス、およびMTUを設定する必要があります。

この機能にチェックを付けると、システムがIPv4アドレス、IPv4サブネットマスク、IPv4デフォルトゲートウェイを自動的に割り当てます。

DNSサーバー

実際の必要に応じて、優先DNSサーバーと代替DNSサーバーを設定してください。

Wi-Fi パラメーターを設定してください。

デバイスのワイヤレス接続用のWi-Fi設定を指定します。

手順

注意
この機能はデバイスでサポートされている必要があります。

1. **システムとメンテナンス**をクリックし、→、**システム構成**、→、**ネットワーク**、→、**ネットワーク設定**、→、**Wi-Fi** をクリックします。

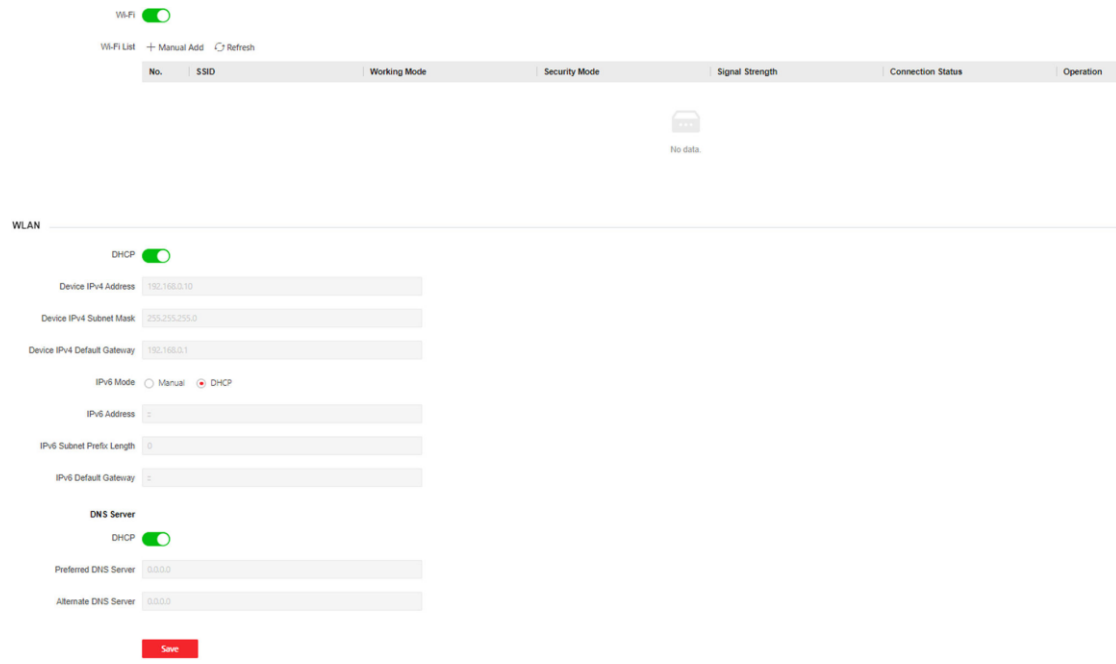


図8-13 Wi-Fi設定画面

2. **Wi-Fi** を確認します。
3. Wi-Fi を選択します。
   - リストからWi-Fiを選択し、Wi-Fiの をクリックし、Wi-Fiのパスワードを入力します。
   - **「追加」**をクリックし、Wi-Fi の名前、パスワード、および暗号化タイプを入力します。**「接続」**をクリックします。Wi-Fi が接続されたら、**「OK」**をクリックします。
4. **オプション:** WLAN パラメーターを設定します。
   1) IPアドレス、サブネットマスク、およびデフォルトゲートウェイを設定します。または**DHCPを**有効にすると、システムがIPアドレス、サブネットマスク、およびデフォルトゲートウェイを自動的に割り当てます。
5. **保存**をクリックします。

PC Web経由でBluetoothを有効/無効にする

Bluetoothを有効にして、Bluetooth対応のサウンドデバイスを接続できます。

手順

1. **「アクセス制御」→「→」→「システム構成」→「→」→「Network」→「→」→「Network Settings」→「→」→「Bluetooth」**をクリックして設定画面を開きます。
2. Bluetooth のパラメーター設定セクションで、**[Open]** を有効にします。
3. 外部音源を「**デバイス名**」に入力してください。Bluetoothが接続された後、**[保存]**をクリックしてください。

PCのウェブ経由でポートを設定

システムとメンテナンス→ システム構成→ ネットワーク→ ネットワークサービス。

HTTPの有効/無効を切り替えます

HTTP機能を有効にすると、ブラウザのセキュリティが向上します。

システムとメンテナンス →→ → システム構成 →→ → ネットワーク →→ → ネットワークサービス → HTTP(S) を選択します。

パラメーターを設定後、**[保存] をクリックします**。

HTTP ポート

ブラウザでログインする際は、アドレスの後に変更されたポート番号を追加する必要があります。例えば、HTTPポート番号が81に変更された場合、ブラウザでログインする際はhttp://

192.0.0.65:81と入力する必要があります。

HTTPS ポート

ブラウザでアクセスするためのHTTPSポートを設定します。ただし、証明書が必要です。

HTTP リスニング

デバイスはHTTPプロトコルを使用して、アラーム情報を目的のIPアドレスまたはドメイン名に送信します。目的のIPアドレスまたはドメイン名はHTTPプロトコルに対応している必要があります。目的のIPアドレスまたはドメイン名、URL、ポートを入力し、プロトコルタイプを選択してください。

PC ウェブ経由で RTSP ポートを表示

RTSPポートは、リアルタイムストリーミングプロトコルのポートです。

システムとメンテナンスに移動し、**→ システム構成→ ネットワーク→ ネットワークサービス→ RTSP** を選択し、ポートを確認します。

PC Web経由でWebSocketを設定します。

WebSocket と WebSockets ポートを表示します。

システムとメンテナンス →→ → システム構成 →→ → ネットワーク →→ → ネットワークサービス → WebSocket(s) を選択します。

WebSocket と WebSockets のポートを表示します。

SDK サービスを有効にする

SDKサービスを有効にすると、デバイスはSDKサーバーに接続できます。

システムとメンテナンスをクリックします。→ **システム構成をクリックします。→ ネットワークをクリックします。→ デバイスアクセスをクリックします。→ SDK サーバー**をクリックして設定ページに移動します。

サーバーポートを入力します。

保存をクリックして設定を有効にします。

PC ウェブ経由で ISUP パラメーターを設定

ISUPプロトコルでデバイスにアクセスするためのISUPパラメーターを設定します。

手順

注意
この機能はデバイスでサポートされている必要があります。

1. **システムとメンテナンス**をクリックし、→、**システム構成、→、ネットワーク、→、デバイスアクセス、→、ISUP** を選択します。
2. **「有効」**を選択します。
3. ISUPバージョン、サーバーアドレス、デバイスID、およびISUPステータスを設定します。

   注意
   バージョンに5.0を選択した場合、暗号化キーも設定する必要があります。
4. ISUP リスニングパラメーターを設定します。これには、ISUP アラームセンター IP アドレス/ドメイン名、ISUP アラームセンター URL、および ISUP アラームセンター ポートが含まれます。
5. **保存**をクリックします。

PC Web経由でOTAPを設定

OTAPプロトコルを使用してデバイスをプラットフォームに接続し、デバイス情報取得、操作状態およびアラーム情報のアップロード、デバイスの再起動およびアップグレードを行います。

手順

1. **システムとメンテナンス**をクリックします。→ **システム構成をクリックします。→ ネットワークをクリックします。→ デバイスアクセスをクリックします。→ OTAP** をクリックします。

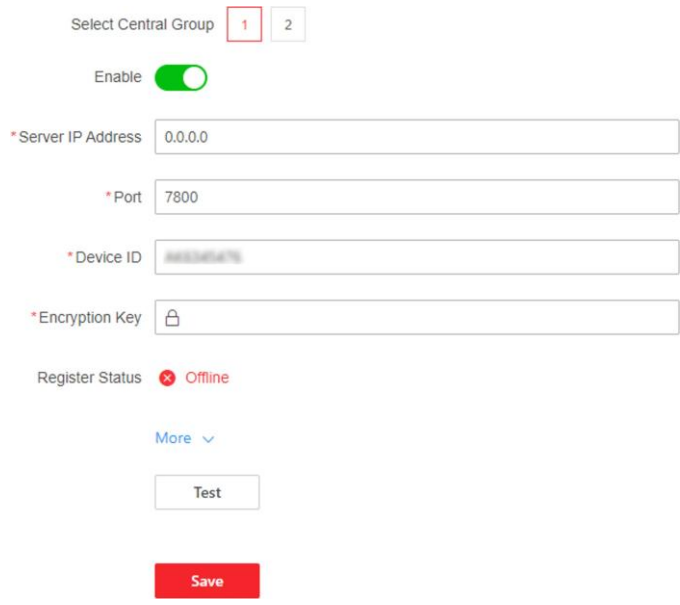


図8-14 OTAPを設定

2. OTAP を**有効にする**をクリックします。
3. **サーバーのIPアドレス**、**ポート**、**デバイスID**、および**暗号化キー**を設定します。
4. **テスト**をクリックして、デバイスがサーバーに接続でき、正常に登録されることを確認します。ページを再読み込みするか、デバイスを再起動して**登録状態**を確認します。
5. **「詳細」**をクリックしてネットワークタイプとアクセス優先度を表示します。操作アイコンを上下にドラッグしてネットワーク優先度を調整します。
6. **保存**をクリックします。

PCウェブ経由でのプラットフォームアクセス

プラットフォームアクセスは、プラットフォーム経由でデバイスを管理するオプションを提供します。

手順

1. **システムとメンテナンス**をクリックします。→ **システム構成をクリックします。→ ネットワークをクリックします。→ デバイスアクセスをクリックします。→ Hik-Connect** をクリックして設定ページに移動します。

注意
Hik-Connectはモバイルデバイス用のアプリケーションです。このアプリを使用すると、デバイスのライブ映像を確認したり、アラーム通知を受け取ったりできます。

---

2. **「有効」**にチェックを入れて機能を有効にします。
3. **オプション:「カスタム」**のチェックボックスをオンにすると、サーバーアドレスを自分で設定できます。
4. 検証コードを入力してください。
5. **「表示」**をクリックしてデバイスのQRコードを表示します。QRコードをスキャンしてアカウントを連携します。

注意

8文字から32文字（aからz、AからZ）または数字（0から9）、大文字と小文字を区別します。8文字以上の文字または数字の組み合わせを使用することをおすすめします。

6. **「保存」**をクリックして設定を有効化してください。

VoIP アカウント設定

ネットワーク経由で音声通話を実現できます。

手順

1. **システムとメンテナンス**に移動し、**→ システム構成→ ネットワーク→ デバイスアクセス→ VoIP**。
2. **VoIP ゲートウェイを**有効にします。
3. **ユーザー名、登録パスワード、サーバーIPアドレス、サーバーポート、有効期限、登録状態、番号、表示ユーザー名を設定**します。

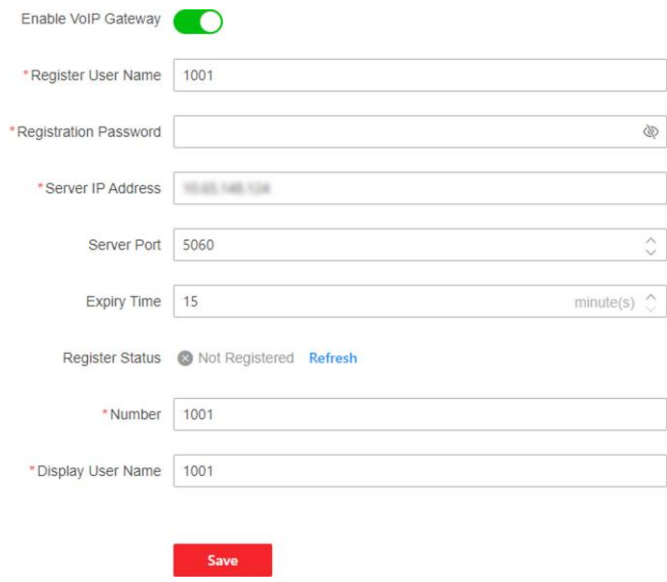


図8-15 VoIP アカウント設定

登録パスワード

SIPサーバー経由の通信用の登録パスワードを入力します。SIPサーバーの登録パスワードは、通常、メインステーションのSIP設定で設定されます。

サーバーIPアドレス

VoIP通信に使用するメインステーションのIPアドレスを入力します。この時点では、メインステーションがSIPサーバーとして機能します。他のインターコムデバイスはこのサーバーアドレスに登録する必要があります。

番号 / ユーザー名表示

デバイスは、通話番号とユーザー名を表示しました。

4. **保存**をクリックします。

8.9.7 PCウェブ経由でビデオとオーディオのパラメーターを設定

ウェブブラウザ経由でビデオパラメーターを設定

デバイスのカメラの画質、解像度、その他のパラメーターを設定できます。

システムとメンテナンスをクリックします。**→ システム構成をクリックします。→ ビデオ/オーディオ→ ビデオ**をクリックして設定画面に移動します。

カメラ名、ストリームタイプ、ビデオタイプ、解像度、ビットレートタイプ、ビデオ品質、フレームレート、最大ビットレート、ビデオエンコード、およびIフレーム間隔を設定します。

「保存」をクリックします。

ウェブブラウザ経由でオーディオ設定を構成する

デバイスの音量を設定できます。

「システムとメンテナンス」をクリックし、次に「**→**」**→**「**システム構成**」**→**「**→**」**→**「**Video/Audio**」**→**「**→**」**→**「**Audio**」を選択して設定画面を開きます。

実際のニーズに応じてストリームタイプとオーディオエンコードを設定します。スライダーを操作して入力と出力の音量を設定します。

スライダーを動かして音声ガイド機能を有効にします。

オーディオミキシングを有効にし、**出力サブボリューム**を設定できます。**「保存」**をクリックします。

8.9.8 画像パラメーター設定

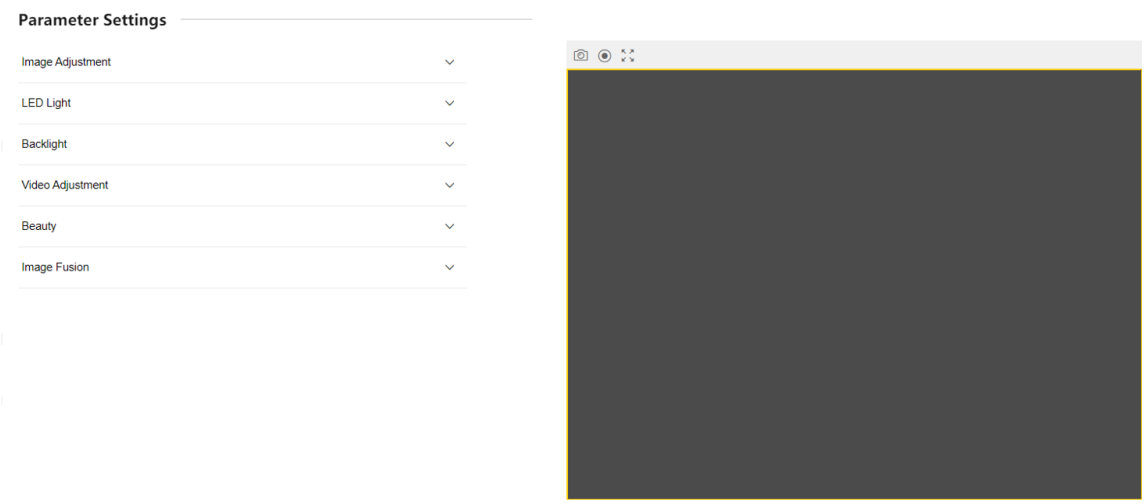


図8-16 ディスプレイ設定

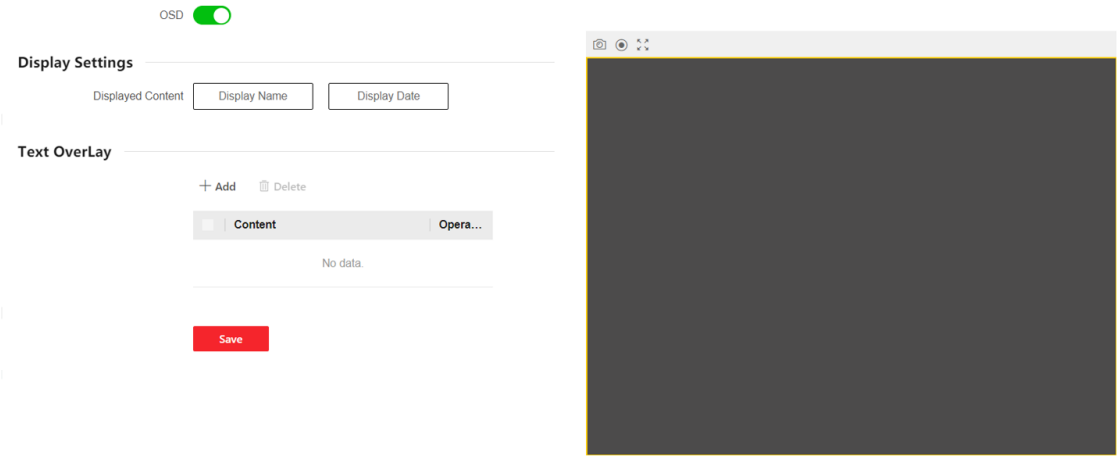


図8-17 OSD設定

PCウェブ経由で明るさ/コントラスト/彩度/シャープネスを設定

ライブビュー画面の明るさ、コントラスト、彩度、シャープネスなどの画像設定を変更できます。

「システムとメンテナンス」→「→」→「システム構成」→「→」→「Image」→「→」→「Display Settings」をクリックして設定画面に移動します。

画像調整

ブロックをドラッグするか、数値を入力して明るさ、コントラスト、彩度、シャープネスを設定します。**デフォルト設定**に戻すには「デフォルト設定に戻す」をクリックします。

PC Web経由でLEDライトを設定

補助ライトの明るさを調整できます。

手順

1. **システムとメンテナンス**をクリックします。→**システム構成をクリックします。→イメージをクリックします。→ディスプレイ設定**をクリックして設定画面に入ります。
2. 補助照明のタイプ、モード、明るさを設定します。
3. **オプション：デフォルト設定に戻す**をクリックして、デフォルト設定に戻します。

PC Web経由でWDRを設定します。

システムとメンテナンスをクリックし、→、**システム構成**、→、**Image**、→、**ディスプレイ設定**をクリックして設定ページに入ります。

ワイドダイナミックレンジを有効または無効にします。有効にすると、シーンの明るい部分と暗い部分が同時にクリアに表示されます。

「デフォルト設定に戻す」をクリックして、デフォルト設定に戻します。

PC ウェブ経由でビデオ標準を設定

ライブビューページのビデオ標準を設定できます。

「システムとメンテナンス」→「→」→「システム構成」→「→」→「Image」→「→」→「Display Settings」をクリックして設定画面を開きます。

ビデオ調整

リモートプレビュー中のビデオフレームレートを設定します。新しい設定を有効にするには、デバイスを再起動する必要があります。

PAL

25フレーム/秒。中国本土、香港（中国）、中東諸国、ヨーロッパ諸国などに対応しています。

NTSC

30フレーム/秒。アメリカ合衆国、カナダ、日本、台湾（中国）、韓国、フィリピンなどに適しています。

「デフォルト設定に戻す」をクリックして、デフォルト設定に戻します。

PCウェブ経由でビューティーパラメーターを設定

有効化後、認証済みの画像を白くしたり滑らかにしたりできます。

「システムとメンテナンス」→「→」→「システム構成」→「→」→「Image」→「→」→「Display Settings」をクリックして設定画面に入ります。

美しさを引き出すには、ブロックをドラッグするか数値を入力して、明るさと滑らかさのレベルを設定します。

デフォルト設定に戻すには、「デフォルト設定に戻す」をクリックします。

PCウェブ経由で画像融合を設定

画像融合機能を有効にすると、画像の品質を向上させることができます。

システムとメンテナンスをクリックし、**→**、**システム構成**、**→**、**Image**、**→**、**Display Settings**の順にクリックして設定画面に移動します。

画像融合

画像融合を「自動」または「**無効**」に設定します。ブロックをドラッグするか、数値を入力して感度を設定します。

「デフォルト設定に戻す」をクリックして、デフォルト設定に戻します。

PC Web経由でOSDパラメーターを設定

ライブビューに表示されるカメラ名、日時形式、表示モード、およびOSDのサイズをカスタマイズできます。

手順

1. **システムとメンテナンス**をクリックし、**→**、**システム構成**、**→**、**Image**、**→**、**OSD** Configurationの順にクリックして設定画面に入ります。
2. **OSDを**有効にします。
3. 必要に応じて、カメラ名、日付、または週の表示を選択するために、対応するチェックボックスにチェックを入れます。
4. **カメラ名**を入力します。
5. ドロップダウンリストから選択して、**時間**形式と**日付形式**を設定します。
6. **「追加」**をクリックしてテキストボックスに文字を入力し、OSDの位置と揃え方を調整します。

8.9.9 PC ウェブ経由のアラーム設定

アラーム出力パラメーターを設定します。

手順

1. **システムとメンテナンス**をクリックし、**→**、**システム構成**、**→**、**イベント**、**→**、**アラーム設定**、**→**、**アラーム出力を選択します**。
2. **アラーム名**と**アラーム持続時間を**設定します。

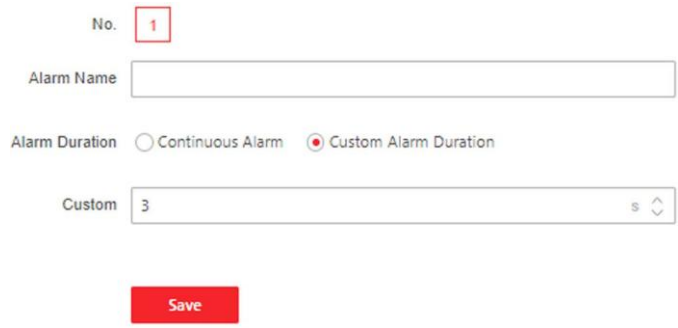


図8-18 アラーム設定

連続アラーム

アラームがトリガーされると、アラームが継続的に鳴動します。

カスタムアラーム持続時間

アラームがトリガーされた際に、デバイスの**アラーム持続時間を**設定できます。

8.9.10 アクセス設定

PCウェブ経由でRS-485パラメーターを設定

周辺機器、アドレス、ボーレートなど、RS-485パラメーターを設定できます。

システムとメンテナンスをクリックし、**→ システム設定→ アクセス設定→ RS-485を選択します。RS-485を有効にし**、パラメーターを設定します。

設定後、**保存**をクリックして設定を保存します。

No.

RS-485番号を設定します。

周辺機器の種類

実際の状況に応じて、ドロップダウンリストから周辺機器を選択してください。選択可能なオプションは**カードリーダー**、**拡張モジュール**、**アクセスコントローラー**、または**無効化**。

注

周辺機器を変更して保存すると、デバイスが自動的に再起動します。

RS-485 アドレス

実際の要件に応じてRS-485アドレスを設定してください。

注意

アクセスコントローラーを選択した場合：RS-485 インターフェース経由でデバイスをターミナルに接続する場合、RS-485 アドレスを 2 に設定してください。コントローラーに接続する場合、ドア番号に応じて RS-485 アドレスを設定してください。

ボーレート

RS-485プロトコルでデバイスが通信する際のボーレート。

PC Web経由でWiegandパラメーターを設定する

Wiegandの送信方向を設定できます。

手順

注意

一部のデバイスモデルではこの機能に対応していません。設定時は実際の製品をご確認ください。

1. **システムとメンテナンス**をクリックし、**→**、**システム構成**、**→**、**アクセス構成**、**→**、**Wiegand設定を選択します**。

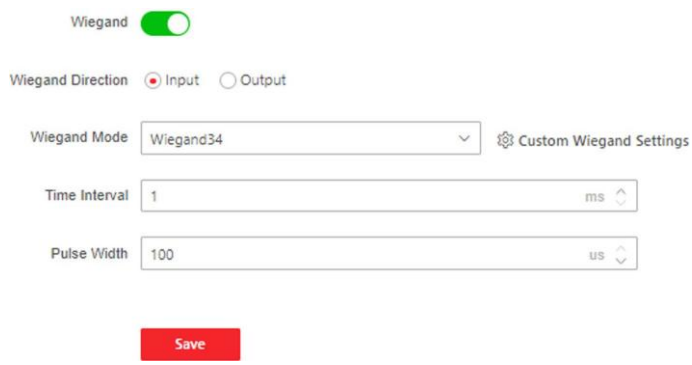


図8-19 Wiegand ページ

2. **Wiegand** をチェックして、Wiegand 機能を有効にします。
3. 送信方向を設定します。

   入力

   このデバイスは、ワイガンドカードリーダーを接続できます。

   出力

   外部アクセスコントローラーに接続できます。そして、2つのデバイスはWiegand 26または34経由でカード番号を送信します。
4. 設定を保存するには**「保存」**をクリックしてください。

注意

周辺機器を変更し、デバイスのパラメーターを保存した後、デバイスは自動的に再起動します。

PC Web経由でセキュアドアコントロールユニットのパラメーターを設定する

セキュアドアコントロールユニットのパラメーターを設定できます。

手順

1. **システムとメンテナンス**をクリックします。**→ アクセス構成をクリックします。→ セキュアドアコントロールユニットをクリックします**。
2. ドアを選択します。

注

ドア 1 を選択すると、そのドアはセキュア ドア コントロール ユニットで制御されます。ドア 2 の選択についても同様です。

3. セキュア ドア コントロール ユニットのステータスを表示します。
4. **2ドアインターロックを**有効にできます。

注意

この機能が有効になっている場合、2つのドアを同時に開けることはできません。

8.9.11 勤怠設定

従業員の勤務時間、遅刻、早退、休憩、欠勤などを記録したい場合は、従業員をシフトグループに追加し、シフトグループにシフトスケジュール（出席を定義するルールで、スケジュールの繰り返し方法、シフトの種類、休憩設定、カードスワイプルールを含む）を割り当てることで、シフトグループ内の従業員の出席パラメーターを定義できます。

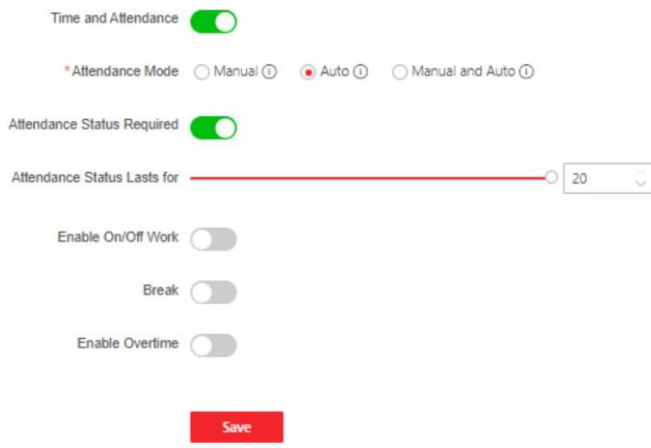


図8-20 勤怠管理

ウェブ経由で出席モードを無効化

出席モードを無効にすると、システムは初期画面に出席ステータスを表示しなくなります。

手順

1. **システムとメンテナンス**をクリックし、**→**、**システム構成**、**→**、**プラットフォーム出席**を選択して設定ページに移動します。
2. **「時間と出席」**を無効にします。**結果**

初期画面では、出席状況を確認したり設定したりすることはできません。システムはプラットフォームで設定された出席ルールに従います。

ウェブ経由で手動出席を設定する

出席モードを手動に設定し、出席を確認する際には手動でステータスを選択する必要があります。

開始前に

少なくとも1つのユーザーを追加し、ユーザーの認証モードを設定してください。詳細については、*ユーザー管理*を参照してください。

手順

1. **システムとメンテナンス**をクリックし、**→**、**システム構成**、**→**、**プラットフォーム出席**を選択して設定画面に移動します。
2. **出席モード**を「**手動**」に設定してください。
3. **出席ステータスの必須設定を**有効にし、出席ステータスの有効期間を設定します。

4. 出席ステータスのグループを有効にします。

注意
出席プロパティは変更されません。

5. オプション：必要に応じてステータスを選択し、名前を変更できます。

結果

認証後、出席ステータスを手動で選択する必要があります。

注意
ステータスを選択しない場合、認証は失敗し、有効な出席として記録されません。

Web経由で自動出席を設定する

出席モードを「自動」に設定すると、出席ステータスとその利用可能なスケジュールを設定できます。システムは、設定されたスケジュールに従って出席ステータスを自動的に変更します。

開始前に

少なくとも1つのユーザーを追加し、ユーザーの認証モードを設定してください。詳細については、*ユーザー管理*を参照してください。

手順

1. **システムとメンテナンス**をクリックし、**→ システム構成→ プラットフォーム出席**を選択して設定画面を開きます。

2. **出席モード**を「**自動**」に設定します。

3. 「**出席ステータス必須**」機能を有効にします。

4. 出席ステータスのグループを有効にします。

注
出席プロパティは変更されません。

5. オプション：必要に応じてステータスを選択し、名前を変更します。

6. ステータスのスケジュールを設定します。詳細については、該当するセクションを参照してください。

Web経由で手動と自動の出席を設定します。

出席モードを**「手動」と「自動」**に設定すると、システムは設定されたスケジュールに従って出席ステータスを自動的に変更します。同時に、認証後に手動で出席ステータスを変更することも可能です。

開始前に

少なくとも1つのユーザーを追加し、ユーザーの認証モードを設定します。詳細については、*ユーザー管理*を参照してください。

手順

1. **システムとメンテナンス**をクリックし、**→**、**システム構成**、**→**、**Platform Attendance**の順に選択して設定画面に移動します。
2. **出席モード**を「**手動**」と「**自動**」に設定します。
3. **出席状況の必須**設定を有効にします。
4. 出席ステータスのグループを有効にします。

注

出席プロパティは変更されません。

5. **オプション**：必要に応じてステータスを選択し、名前を変更します。
6. ステータスのスケジュールを設定します。詳細については、を参照してください。

結果

最初のページで認証を行います。認証結果は、スケジュールに従って設定された出席ステータスとしてマークされます。結果タブの編集アイコンをタップすると、手動で出席を記録するためのステータスを選択でき、認証結果は編集された出席ステータスとしてマークされます。

例

ブレイクアウトを月曜日の11:00に設定し、**ブレイクイン**を月曜日の12:00に設定した場合、月曜日の11:00から12:00までの有効なユーザーの認証は「ブレイク」としてマークされます。

8.10 設定オプション

8.10.1 PCウェブ経由で起動画像を設定

起動画像を設定します。

システムとメンテナンスに移動し、**→ 設定→ 画面表示 を選択します**。

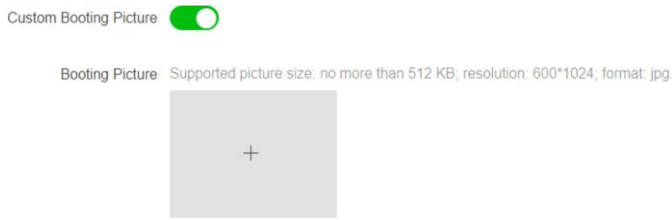


図8-21 起動画像

カスタム起動画像の有効化をクリックし、**[+]** をクリックしてローカルブラウザから起動画像を選択します。

注意

サポートされる画像サイズ：512 KB以下；解像度：600×1024；形式：JPG。

保存をクリックしてください。

8.10.2 PC ウェブ経由でスタンバイ画像を設定

スタンバイ画像のパラメーターを設定します。これには、スタンバイ状態に移行する時間、スクリーンセーバーの画像、表示効果、スライドショーの間隔が含まれます。

システムとメンテナンスに移動し、**→**、**Preference**、**→**、**Screen Display** の順に選択します。

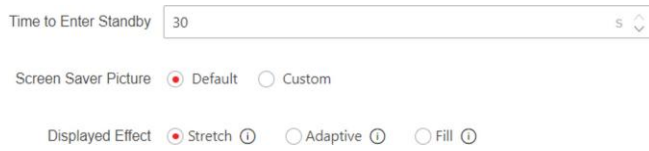


図8-22 スタンバイ画像設定

スタンバイ画像のパラメーターを設定し、**保存**をクリックします。**ス**

タンバイに入るまでの時間

設定した時間経過後に、デバイスにスタンバイ画像が表示されます。

スクリーンセーバー画像

スタンバイ画像をデフォルト画像またはカスタム画像に設定します。**Customを選択し**、**+** をクリックして、ローカルブラウザからスタンバイ画像を選択してアップロードします。

注意

画像の数は3枚までです。1枚あたりの画像サイズ：1024 KB以下；形式：JPG。

表示効果

スタンバイ画像の表示効果を「**Stretch**」「**Adaptive**」「**Fill**」から選択します。

スライドショー間隔

複数の画像を追加した場合、画像の切り替え時間を設定できます。

8.10.3 PCウェブ経由でスリープ時間を設定します。

デバイスは、設定された時間経過後にスリープモードに移行します。この機能は電力消費を削減します。

システムとメンテナンスに移動し、**→ 設定、→ 画面表示を選択します。**

図8-23 スリープ設定

スリープをスライドしてスリープ時間を設定します。**保存**をクリックします。

8.10.4 PC ウェブ経由で認証デスクをカスタマイズ

認証ページ/デスクのモジュールをカスタマイズします。

手順

1. **システムとメンテナンス**に移動します。→**設定**→**カスタムホームページ**。
2. **アプリケーションモード**を選択します。

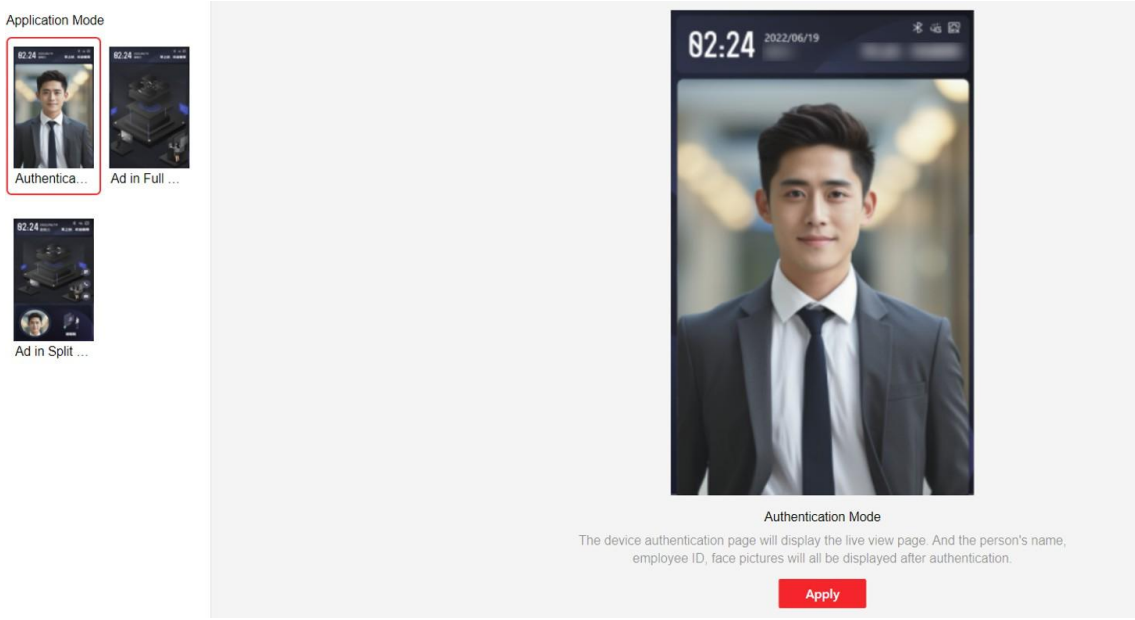


図8-24 アプリケーションモードの選択

認証モード

デバイス認証ページにはライブビューページが表示されます。認証後、ユーザーの氏名、従業員ID、顔写真が表示されます。

フルスクリーン広告

広告は認証ページの画面全体を占有します。スクリーンセーバーやウェルカムメッセージを広告内で再生できます。

分割画面広告

認証ページには広告領域と認証領域が含まれます。広告内でスクリーンセーバーやウェルカムメッセージを再生できます。

3. **「適用」**をクリックしてください。

8.10.5 PCウェブ経由で通知の公開を設定

デバイスの通知の公開を設定できます。

システムとメンテナンスに移動し、**→ 設定→ 通知の公開 を選択します。**

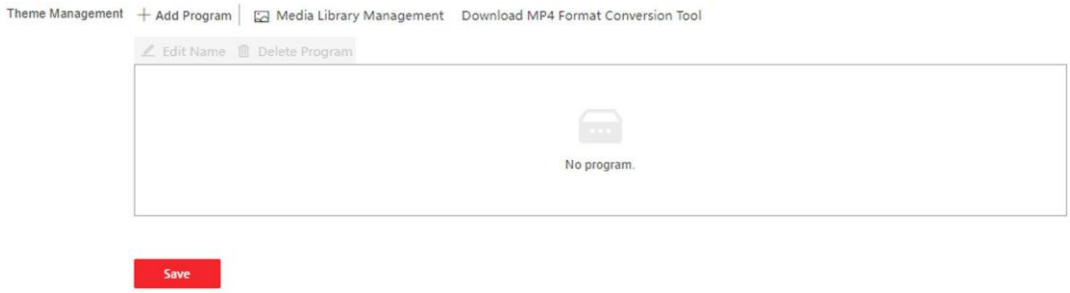


図8-25 通知の公開 MP4形式変換ツール

のダウンロード

MP4 形式変換ツールをダウンロードするには、[**ダウンロード**] をクリックしてください。

素材管理

「+」をクリックし、**「Add Theme」**を選択し、**テーマ**名と**テーマタイプ**を設定します。

「アップロード」をクリックし、ローカルPCから画像または動画をアップロードするには**「+」**をクリックしてください。

注意

現在、追加できるテーマは1つだけです。

プログラムの追加

プログラム名を設定し、プログラムの種類を選択できます。

画像

画像を選択した場合、画像を追加するには**「+」**をクリックしてください。

ウェルカムメッセージ

ウェルカムメッセージを選択すると、メインタイトルとサブタイトルのテンプレート、コンテンツ、フォントサイズ、色を設定できます。背景画像もカスタマイズ可能です。

標準

標準を選択すると、背景色と画像を設定できます。

プレイスケジュール

テーマを作成した後、テーマを選択し、タイムライン上にスケジュールを配置できます。配置したスケジュールを選択すると、開始時間と終了時間を詳細に編集できます。

選択したスケジュールを選択し、**削除**または**すべて削除**をクリックしてスケジュールを削除できます。

スライドショー間隔

ブロックをドラッグするか、数値を入力してスライドショーの間隔を設定します。画像と動画は設定した間隔に従って切り替わります。

8.10.6 PCウェブ経由でプロンプトスケジュールを設定

認証に成功した場合と失敗した場合の出力オーディオコンテンツをカスタマイズできます。

手順

1. **システムとメンテナンス**に移動し、**→ 設定→ プロンプトスケジュール** を選択します。

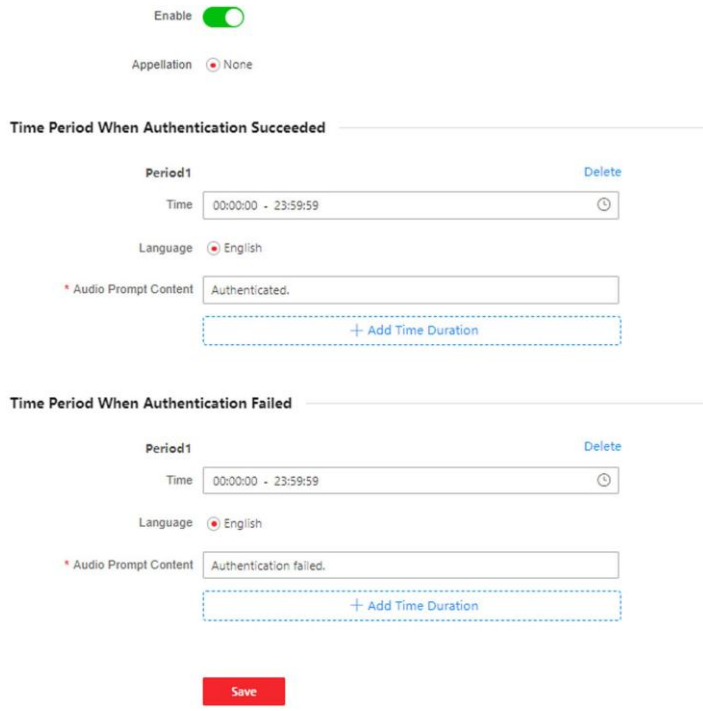


図8-26 プロンプトスケジュール

2. 機能を有効にします。

3. 名称を設定します。

4. 認証スケジュールを選択します。
5. 認証が成功した時間帯を設定します。
   1) **「時間期間を追加」**をクリックします。
   2) 時間期間を設定します。

   注
   設定した時間範囲内で認証が成功した場合、デバイスは設定されたコンテンツを放送します。
   3) 音声プロンプトの内容を設定します。
   4) **オプション:** サブステップ1から3を繰り返し実行します。
   5) **オプション：** をクリックして、設定された時間範囲を削除します。
6. 認証に失敗した際の時間設定を設定します。
   1) **「Add Time Duration」**をクリックします。
   2) 時間設定を設定します。

   注
   認証が設定された時間内に失敗した場合、デバイスは設定されたコンテンツをブロードキャストします。
   3) オーディオコンテンツを設定します。
   4) **オプション：** サブステップ1から3を繰り返し実行します。
   5) **オプション：** 設定した時間範囲を削除するには、[ ]をクリックします。
7. **「Save」**をクリックして設定を保存します。

8.10.7 PC ウェブ経由でプロンプト音声のカスタマイズ

デバイスのプロンプトボイスをカスタマイズできます。

手順

1. **システムとメンテナンス**に移動し、**→ 設定→ カスタムプロンプト を選択します**。

Custom Type	Importing Status	Operation
Call Center	Not Imported	
Nobody Answered	Not Imported	
Thanks	Not Imported	
Authenticating Failed	Not Imported	
The Door Is Open	Not Imported	
Please Wear the Safety Helmet	Not Imported	
Please Wear the Mask	Not Imported	

図8-27 カスタムプロンプト

2. 、→、 にアクセスし、実際のニーズに応じてローカルPCからオーディオファイルをインポートしてください。

注意
アップロードするオーディオファイルは512 KB未満で、WAV形式である必要があります。

8.10.8 PCのウェブブラウザで認証結果テキストを設定

手順

1. システムとメンテナンスに移動し、→**設定**→**認証結果テキスト** を選択します。

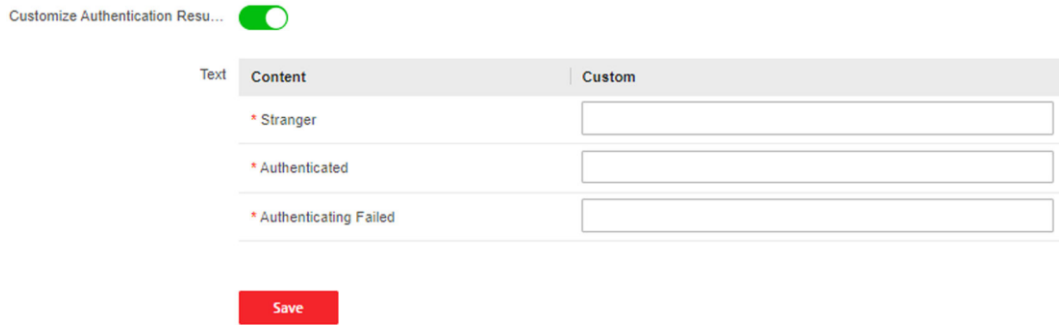


図8-28 認証結果テキスト

2. **「認証結果テキストのカスタマイズ」**を有効にします。

3. カスタムテキストを入力します。

4. **保存**をクリックします。

8.11 システムとメンテナンス

8.11.1 再起動

デバイスを再起動できます。

→**「システムとメンテナンス」**をクリックし、次に**「→メンテナンス」**をクリックし、さらに**「再起動」**をクリックして設定画面に移動します。**「再起動」**をクリックしてデバイスを再起動します。

8.11.2 アップグレード

PC ウェブ経由でローカルにアップグレード

デバイスをローカルでアップグレードできます。

システムとメンテナンスをクリックし、→**Maintenance**→**Upgrade** を選択して設定画面に移動します。

ドロップダウンリストからアップグレードの種類を選択します。をクリックし、ローカルPCからアップグレードファイルを選択します。**アップグレード**をクリックしてアップグレードを開始します。

PCウェブ経由でのオンラインアップグレード

デバイスをオンラインでアップグレードできます。

システムとメンテナンスをクリックし、**→ Maintenance→ Upgrade** をクリックして設定画面に移動します。更新を確認**をクリックして**、更新されたバージョンがあるかどうかを確認します。

デバイスがネットワークに接続されており、Hik-Connect アプリに追加されている場合、Hik-Connect アプリに更新バージョンがある場合に、デバイス上で「**デバイス アップグレード」→「→ オンライン アップグレード」**をタップしてアップグレードできます。

8.11.3 復元

ウェブブラウザ経由で工場設定に復元

デバイスを工場出荷時設定に復元できます。

システムとメンテナンス→ Maintenance→ Backup and Reset をクリックして設定画面に入ります。

「すべてを復元」をクリックすると、すべての設定が工場出荷時の設定に戻ります。使用前にデバイスをアクティベートしてください。

PC ウェブ経由でデフォルト設定に復元

デバイスをデフォルト設定に復元できます。

「システムとメンテナンス」をクリックし、**「→ メンテナンス」を選択し、「→ バックアップとリセット」**をクリックして設定画面に移動します。

「復元」をクリックすると、デバイスのIPアドレスとユーザー情報を除き、デフォルト設定に復元されます。

8.11.4 PCウェブ経由でデバイスパラメーターをエクスポート

デバイスのパラメーターをエクスポートします。

システムとメンテナンスに移動し、**→ メンテナンス→ バックアップとリセット** を選択します。

バックアップ

「エクスポート」をクリックしてデバイス設定をエクスポートします。

注意

デバイスのパラメーターをエクスポートし、他のデバイスにインポートします。

8.11.5 PC Web経由でデバイスパラメーターをインポート

構成パラメーターをインポートします。

システムとメンテナンスに移動し、**→ メンテナンス、→ バックアップとリセットを選択します。**

設定ファイルのインポート

「 」をクリックし、ローカルPCからファイルを選択します。**「インポート」**をクリックします。

8.11.6 デバイス デバッグ

デバイスのデバッグ設定を指定できます。

Web ブラウザ経由で SSH を有効/無効にします

SSHを有効にしてリモートデバッグを実行できます。

システムとメンテナンスをクリックし、**→ Maintenance、→ Device Debugging、→ Log for Debugging** の順に選択し、**SSH を有効にします。**

SSHはリモートデバッグに使用されます。このサービスを使用しない場合は、セキュリティを向上させるため、SSHを無効にすることをおすすめします。

PCのウェブブラウザからデバイスログを印刷

デバイスログを印刷できます。

システムとメンテナンスをクリックし、**→ Maintenance→** にアクセスして設定ページを開きます。**エクスポート**をクリックしてデバイスログを印刷します。

PC ウェブ経由でネットワーク パケットをキャプチャ

キャプチャ パケットの期間とサイズを設定し、キャプチャを開始します。キャプチャ結果に応じてログを確認し、デバッグを行うことができます。

システムとメンテナンス→ メンテナンス→ デバイスデバッグ→ デバッグ用ログをクリックします。キャプチャパケットの期間、キャプチャパケットのサイズを設定し、[**キャプチャ開始**]をクリックします。

PCのウェブブラウザでプロトコルをテストします。

プロトコルアドレスを選択し、テストするプロトコルを入力します。応答ヘッダーと返却値に基づいてデバイスをデバッグできます。

システムとメンテナンス→ Maintenance→ Device Debugging→ Protocol Testing へ移動します。

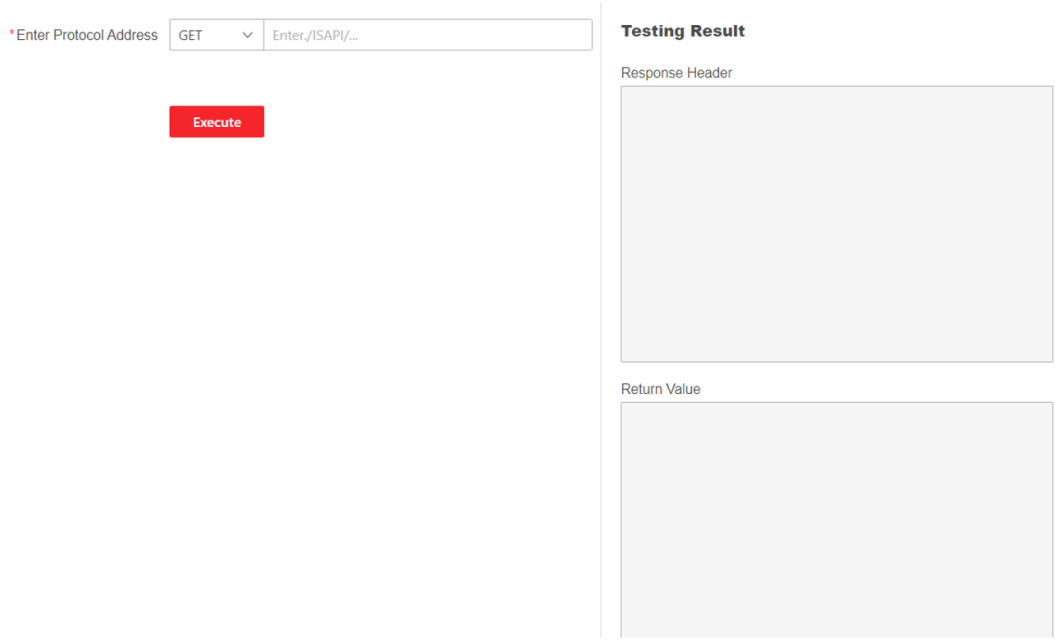


図8-29 プロトコルテスト

プロトコルアドレスを選択し、プロトコルを入力します。**実行**をクリックします。
応答ヘッダーと返却値に基づいてデバイスをデバッグします。

PC ウェブ経由のネットワーク診断

デバイスのIPアドレスまたはドメイン名を入力し、PING設定を行うことができます。PINGの結果に基づいてネットワークをデバッグします。

システムとメンテナンス→ Maintenance→ Device Debugging→ Network Diagnosis へ移動します。

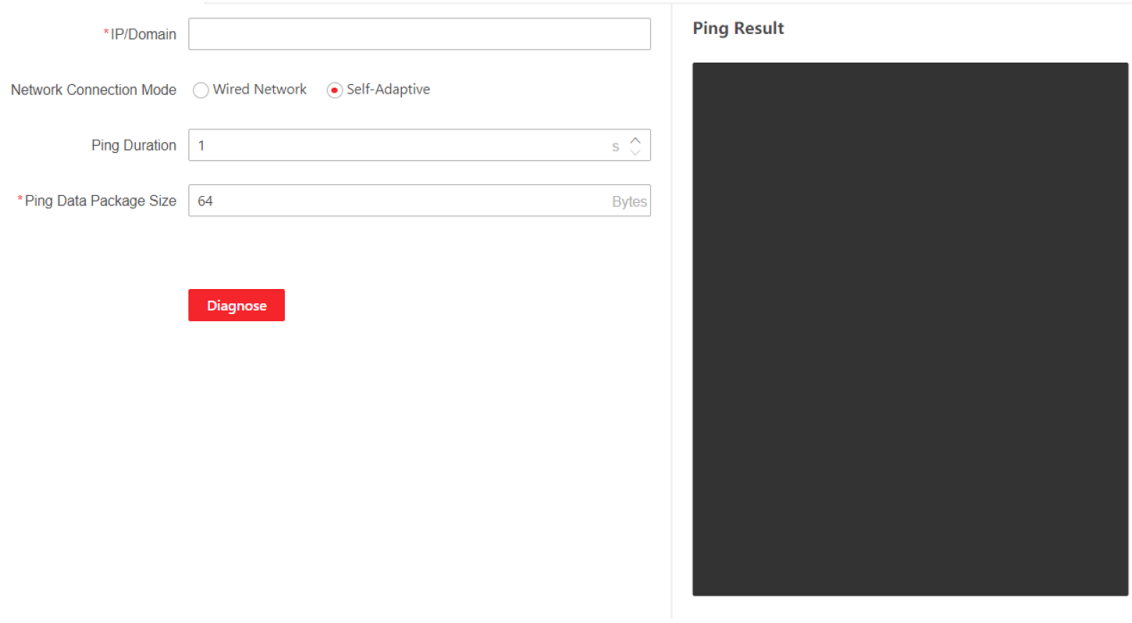


図8-30 ネットワーク診断

PING操作用のデバイスIPを入力し、ネットワーク接続モード、PING持続時間、およびPingデータパケットサイズを選択します（デフォルトパラメーターが推奨されます）。**「診断」**をクリックします。結果は**PING結果**に表示されます。

PC ウェブ経由でネットワークペネトレーションサービスを設定します。

デバイスがLANに展開された場合、ペネトレーションサービスを有効化することで、デバイスのリモート管理を実現できます。

手順

1. **システムとメンテナンス**に移動します。→ **メンテナンス**→ **デバイスデバッグ**→ **ネットワークペネトレーションサービス**。
2. **「ペネトレーション サービスを有効にする」**をスライドします。
3. **サーバーIPアドレス**と**サーバーポート**を設定します。**ユーザー名**と**パスワード**を作成します。
4. **オプション：ハートビートタイムアウト**を設定できます。値の範囲は1から6000です。
5. **オプション:** ペネトレーション サービスの状態を確認できます。状態を更新するには**「リフレッシュ」**をクリックしてください。
6. **「保存」**をクリックしてください。

注

ペネトレーションサービスは48時間後に自動的に無効化されます。

8.11.7 PC ウェブ経由でログを表示

デバイスログを検索して表示できます。

システムとメンテナンスに移動し、**→ メンテナンス、→ ログを選択してください**。

ログタイプの主要タイプと副次タイプを設定します。検索の開始時間と終了時間を設定し、**[検索]** をクリックします。

結果は以下に表示され、番号、時間、主要タイプ、副次タイプ、チャンネル番号、ローカル/リモートユーザー情報、リモートホストIPなどが含まれます。

8.11.8 PC ウェブ経由の高度な設定

顔パラメーター、手のひらパラメーターを設定し、バージョン情報を確認できます。**システムとメンテナンス → メンテナンス → 詳細設定** へ移動します。

デバイスアクティベーションパスワードを入力し、**Enter**をクリックします。

顔パラメーター

カスタムアンチスプーフィング検出を有効にすると、**アンチスプーフィング検出閾値 1:1** および**アンチスプーフィング検出閾値 1:N** を設定できます。

顔認証用の顔ロックを有効にし、**ロック時間を**設定します。アンチスプーフィング検出の失敗回数制限に達すると、設定したロック時間中に顔がロックされます。

保存をクリックします。

パームプリントパラメーター

カスタムアンチスプーフィング検出を有効にすると、**アンチスプーフィング検出閾値**を設定できます。**保存**をクリックします。

バージョン情報

ここで異なるバージョン情報を確認できます。

8.11.9 セキュリティ管理

PCウェブにログインする際のセキュリティレベルを設定します。

システムとメンテナンスに移動し、**→ を選択し、→ セキュリティ サービス** をクリックします。

セキュリティモード

ログイン時とユーザー情報の確認時に高いセキュリティレベルを適用します。

互換性モード

古いユーザー認証方法と互換性があります。

保存をクリックします。

8.11.10 証明書管理

サーバー/クライアント証明書およびCA証明書を管理するのに役立ちます。

注意
この機能は、特定のデバイスモデルでのみサポートされています。

自己署名証明書を作成してインポートする

手順

1. **システムとメンテナンス**に移動し、**→**、**Safe**、**→**、**Certificate Management** の順に選択します。
2. **証明書**ファイル領域で、ドロップダウンリストから**証明書タイプ**を選択します。
3. **「作成」**をクリックします。
4. 証明書情報を入力します。
5. **OK**をクリックして証明書を保存し、インストールします。
   作成された証明書は**証明書詳細**領域に表示されます。証明書は自動的に保存されます。
6. 証明書をダウンロードし、ローカルコンピュータの指定したファイルに保存します。
7. 要求ファイルを認証局に送信して署名を取得します。
8. 署名済みの証明書をインポートします。
   1) 「**キーのインポート**」領域で証明書タイプを選択し、ローカルから証明書を選択し、**[インポート]** をクリックします。
   2) 「**通信証明書をインポート**」領域で証明書タイプを選択し、ローカルから証明書を選択し、**[インポート]** をクリックします。

その他の承認済み証明書をインポート

既に承認済み証明書（デバイスで作成されていないもの）がある場合は、直接デバイスにインポートできます。

手順

1. **システムとメンテナンス**に移動し、**→**、**Safe**、**→**、**Certificate Management** の順に選択します。
2. **「インポートキー」**と**「インポート通信証明書」**の領域で、証明書タイプを選択し、証明書をアップロードします。
3. **インポート**をクリックします。

CA証明書をインポート

開始前に
事前にCA証明書を準備してください。

手順

1. **システムとメンテナンス**に移動します**。→ 安全→ 証明書管理**。
2. 「**CA証明書をインポート**」領域でIDを作成します。

   注意

   入力する証明書 ID は既存のものと同一にしてはいけません。
3. ローカルから証明書ファイルをアップロードします。
4. **インポート**をクリックします。

第9章 その他のプラットフォームの設定

デバイスは、iVMS-4200 クライアント ソフトウェアまたは HikCentral アクセス コントロール 経由でも設定可能です。詳細については、各プラットフォームのユーザー マニュアルを参照してください。

iVMS-4200 クライアントソフトウェア

リンクをクリックまたはタップして、クライアントソフトウェアのユーザーマニュアルを表示します。

http://enpinfodata.hikvision.com/analysisQR/showQR/ca930247

HikCentral Access Control (HCAC)

リンクをクリックまたはタップして、HCACのユーザーマニュアルを表示します。

http://enpinfodata.hikvision.com/analysisQR/showQR/f2f6cf42

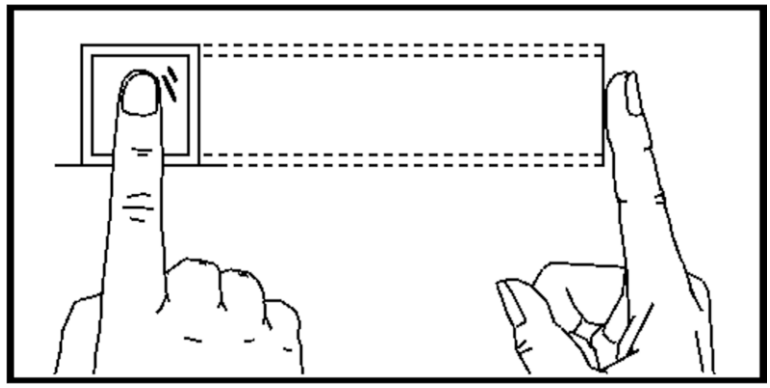
付録A. 指紋スキャン時のヒント

推奨される指

人差し指、中指、または薬指。

正しいスキャン方法

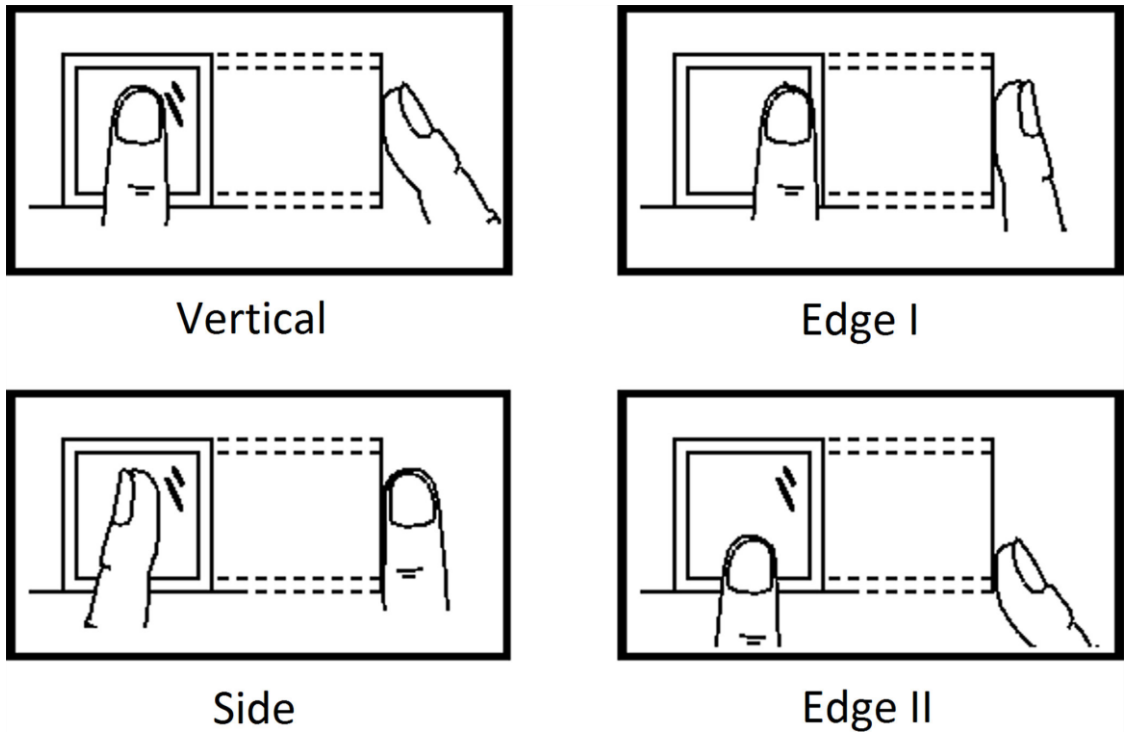
以下の図は、指をスキャンする正しい方法です:



指をスキャナーに水平に押し当ててください。スキャンした指の中心がスキャナーの中心と一致するようにしてください。

不正なスキャン

以下の指紋スキャン図は誤っています:



環境

スキャナーは直射日光、高温、湿気、雨を避けてください。乾燥している場合、スキャナーが指紋を正しく認識できない可能性があります。指に息を吹きかけてから再度スキャンしてください。

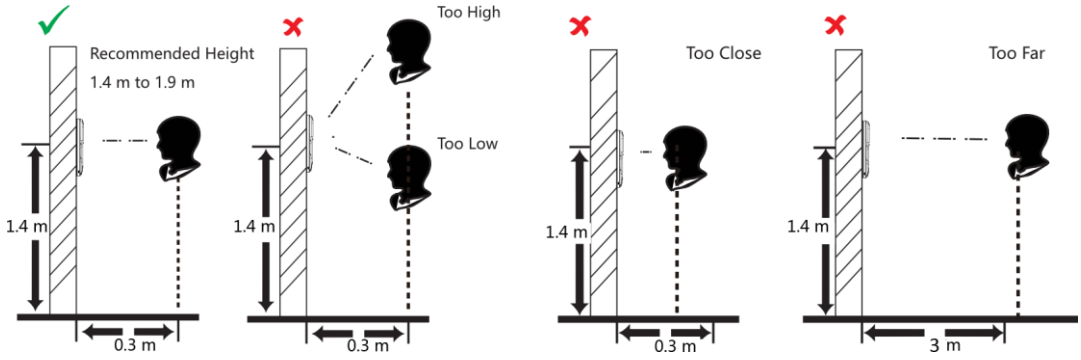
その他

指紋が浅い場合、または指紋の読み取りが難しい場合は、他の認証方法をご利用いただくことをおすすめします。
スキャンする指に傷がある場合、スキャナーが認識しない可能性があります。別の指に変更して再度お試しください。

付録B. 顔写真の収集/比較時の注意点

顔写真の収集または比較時の位置は、以下の通りです：

位置（推奨距離：0.3 m）



表情

- 顔写真を撮影したり比較したりする際は、自然な表情を保ってください。下の写真のような表情を心がけてください。

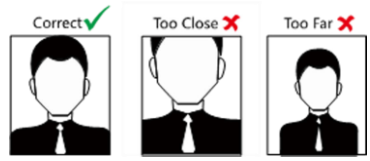
- 帽子、サングラス、または顔認識機能に影響を与える可能性のある他のアクセサリーは着用しないでください。
- 髪が目や耳などを覆わないようにし、濃いメイクは禁止です。

姿勢

顔の写真を収集または比較する際は、カメラに向かって顔を向けてください。これにより、高品質で正確な顔写真が得られます。

サイズ

顔の中心が収集ウィンドウの真ん中に来ていることを確認してください。



付録C. 手のひら紋と手のひら静脈の追加に関するヒント

- 手のひら紋と手のひら静脈を認識する際は、手のひらの中心をデバイスの中央から5～12cmの距離に配置し、周辺モジュールと平行になるように注意してください。
- 周辺モジュールが新しい顔認識端末にアクセスする際は、周辺モジュールのデータをクリアし、再発行または再収集する必要があります。
- 手のひらは汚れが付かないように清潔に保ってください。
- 周辺モジュールの表面は、センサーによる誤報を防止するため、清潔に保つ必要があります。

付録D. 設置環境に関する注意事項

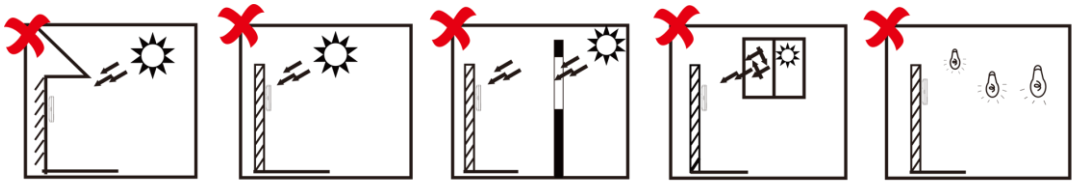
1. 光源の照度基準値

キャンドル: 10ルクス

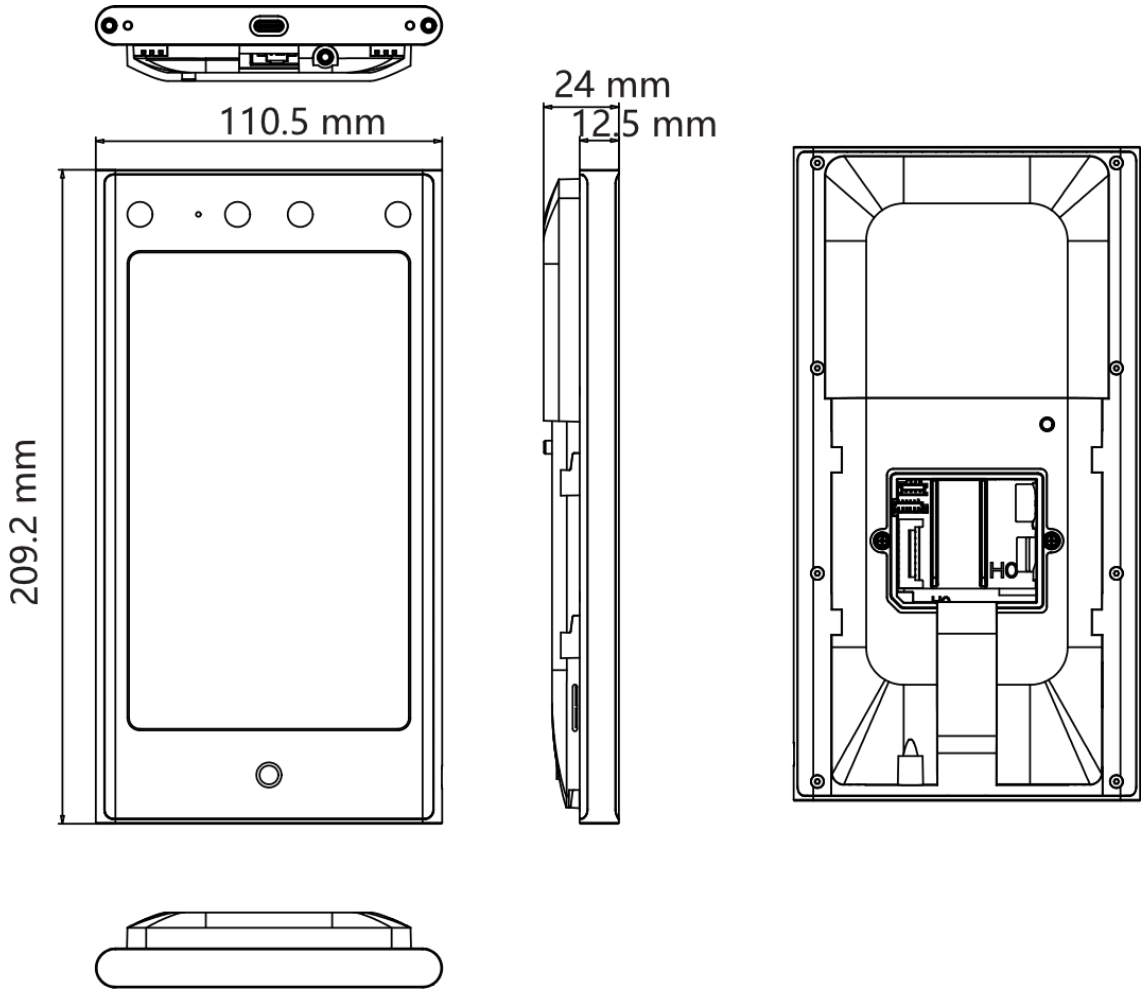
電球：100～850ルクス

日光：1200ルクス以上

2. バックライト、直射日光および間接日光を避けてください



付録E. 寸法



図E-1 寸法


See Far, Go Further