DS-K1T343シリーズ顔認証端末

ユーザーマニュアル

法的情報

本マニュアルについて

本マニュアルには、本製品の使用および管理に関する説明が含まれています。以下に掲載されている写真、図表、画像、その他すべての情報は、説明および解説のみを目的としています。本マニュアルに記載されている情報は、ファームウェアの更新その他の理由により、予告なく変更される場合があります。最新バージョンのマニュアルは、Hikvision ウェブサイト (***https://www.hikvision.com/***) でご確認ください。

本マニュアルは、本製品のサポートに関する訓練を受けた専門家の指導と支援のもとでご使用ください。

商標

HIKVISION およびその他の Hikvision の商標およびロゴは、各管轄区域における Hikvision の所有物です。

記載されているその他の商標およびロゴは、それぞれの所有者に帰属します。

免責事項

適用される法律で認められる最大限の範囲において、本マニュアルおよび記載されている製品（そのハードウェア、ソフトウェア、ファームウェアを含む）は、「現状有姿のまま」かつ「あらゆる欠陥およびエラーを含むまま」提供されます。HIKVISION は、商品性、満足のいく品質、特定目的への適合性を含むがこれらに限定されない、明示的または黙示的な保証を行いません。 本製品の使用は、お客様ご自身の責任において行ってください。いかなる場合においても、HIKVISIONは、特別損害、結果的損害、付随的損害、間接損害（事業利益の損失、事業中断、データの損失、 システムの破損、または文書の損失を含むがこれらに限定されない損害について、契約違反、不法行為（過失を含む）、製造物責任その他のいかなる法的根拠に基づくものであっても、本製品の使用に関連して生じた場合であっても、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されていた場合であっても、一切の責任を負いません。

お客様は、インターネットの性質上、固有のセキュリティリスクが存在することを認識し、サイバー攻撃、ハッカー攻撃、ウイルス感染、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動作、プライバシー漏洩、その他の損害について、HIKVISIONは一切の責任を負わないものとします。ただし、必要に応じてHIKVISIONは適時に技術サポートを提供します。ウイルス感染、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動作、プライバシー漏洩、その他の損害について一切の責任を負わないことを認めるものとします。ただし、必要に応じてHIKVISIONは適時に技術サポートを提供します。

お客様は、適用されるすべての法律を遵守して本製品を使用することに同意し、お客様の使用が適用される法律に準拠していることを確認する責任はお客様のみにあるものとします。 特に、お客様は、パブリシティ権、知的財産権、データ保護および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、第三者の権利を侵害しない方法で本製品を使用することについて責任を負います。 お客様は、本製品を、以下を含む禁止された最終用途に使用してはなりません。

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文脈におけるあらゆる活動、または人権侵害を支援する活動。
本マニュアルと適用法との間に矛盾が生じた場合は、適用法が優先する。

データ保護

デバイス使用中、個人データが収集、保存、処理されます。データ保護のため、Hikvisionデバイス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、顔認識機能付きデバイスでは生体認証データが暗号化方式でデバイス内に保存され、指紋デバイスでは指紋テンプレートのみが保存されるため、指紋画像を再構築することは不可能です。
データ管理者として、適用されるデータ保護法規制に従い、データの収集、保存、処理、転送を行うことが推奨されます。これには、個人データを保護するためのセキュリティ対策の実施（合理的な管理上および物理的なセキュリティ対策の実施、セキュリティ対策の有効性に関する定期的な見直しと評価の実施など）が含まれますが、これらに限定されません。

記号の定義

本書で使用される記号は、以下の通り定義されます。

記号	説明
 危険	回避しなければ死亡または重傷を負う危険な状況があることを示す。
 注意	回避しなければ、機器の損傷、データの損失、性能の低下、または予期しない結果を引き起こす可能性のある潜在的に危険な状況を示します。
 注記	本文の重要な点を強調または補足する追加情報を提供します。

規制情報

FCC 情報

コンプライアンスの責任者が明示的に承認していない変更や改造を行うと、ユーザーが機器を操作する権限が無効になる場合があることにご留意ください。

FCC適合性：本機器は、FCC規則第15部に準拠し、クラスBデジタル機器の制限値に適合することが試験により確認されています。これらの制限値は、住宅環境における有害な干渉から合理的な保護を提供するために設計されています。本機器は無線周波エネルギーを発生•使用し、放射する可能性があります。取扱説明書に従って設置•使用されない場合、無線通信に有害な干渉を引き起こす恐れがあります。 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。本機器がラジオやテレビの受信に有害な干渉を引き起こしている場合（機器の電源をオフにしてからオンにすることで確認可能）、ユーザーは以下の対策のいずれかまたは複数を試み、干渉の解消を図ることを推奨します：

—受信アンテナの方向や設置場所を変更する。

—本機器と受信機の間隔を広げる。

—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本機器を接続する。

—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

本機器は、放射器と身体の間に最低20cmの距離を保って設置•操作してください。

FCC条件

本装置はFCC規則第15部に準拠しています。以下の2条件に従って動作します：

1. 本装置は有害な干渉を引き起こしてはなりません。
2. 本装置は、受信したあらゆる妨害（意図しない動作を引き起こす可能性のある妨害を含む）を受け入れなければなりません。

EU適合宣言

CE

本製品および付属品（該当する場合）には「CE」マークが付与されており、以下の欧州統一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）：この記号が付された製品は、欧州連合において一般廃棄物として廃棄できません。適切なリサイクルのため、同等の新品機器購入時に販売店へ返却するか、指定回収拠点で処分してください。詳細はwww.recyclethis.infoを参照

2006/66/EC（電池指令）：本製品に含まれる電池は、欧州連合（EU）域内で一般廃棄物として廃棄できません。電池の詳細情報は製品説明書をご参照ください。電池にはこのマークが付いており、カドミウム（Cd）、鉛（Pb）、水銀（Hg）を示す文字が併記されている場合があります。 適切なリサイクルのため、電池は販売店または指定回収拠点へ返却してください。詳細は以下を参照：www.recyclethis.info

本装置はカナダ産業省の免許不要RSS規格に準拠しています。動作には以下の2条件を満たす必要があります：

(1) 本機器は干渉を引き起こしてはならないこと、および

(2) この装置は、装置の意図しない動作を引き起こす可能性のある干渉を含む、あらゆる干渉を受け入れなければなりません。

本装置は、免許不要無線機器に適用されるカナダ産業省のCNRに準拠しています。以下の2つの条件を満たす場合に限り、使用が許可されます：

(1) l'appareil ne doit pas produire de brouillage, et

(2) 本装置の使用者は、その動作を妨げる可能性のある電波妨害を含め、あらゆる電波妨害を受け入れること。

安全上の注意

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避けることを目的としています。

注意事項は「危険」と「注意」に分類されます：

危険：警告を無視すると、重傷または死亡の原因となる可能性があります。

注意：いずれかの注意を怠ると、けがや機器の損傷を引き起こす可能性があります。

⚠	⚠
危険：重大な負傷または死亡を防ぐため、これらの安全対策に従ってください。	**注意**：潜在的な負傷や物的損害を防ぐため、これらの予防措置に従ってください。

⚠ 危険：

- 本製品の使用にあたっては、国および地域の電気安全規制を厳守してください。
- 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あります。
- 煙、異臭、または騒音が機器から発生した場合は、直ちに電源を切り、電源ケーブルを抜いてください。その後、サービスセンターまでご連絡ください。
- コンセントは機器の近くに設置し、容易にアクセスできる状態にしてください。
- 1. 電池を飲み込まないでください。化学火傷の危険があります!

2. 本製品にはコイン型電池が含まれています。コイン型電池を飲み込むと、わずか2時間で重度の内部やけどを引き起こし、死に至る可能性があります。
3. 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。
4. 電池ケースが確実に閉まらない場合は、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。
5. 電池を飲み込んだ、または体内に挿入した可能性がある場合は、直ちに医師の診察を受けてください。
6. 注意：誤った種類の電池と交換すると爆発の危険があります。
7. 誤った種類の電池への不適切な交換は、安全装置を無効にする可能性があります（例：一部のリチウム電池タイプの場合）。
8. 電池を火の中や高温のオーブンに廃棄したり、機械的に押しつぶしたり切断したりしないでください。爆発の原因となる可能性があります。
9. 電池を極端に高温の環境に放置しないでください。爆発や可燃性液体•ガスの漏出の原因となる可能性があります。
10. 電池を極端に低い気圧にさらさないでください。爆発や可燃性液体•ガスの漏出の原因となる可能性があります。
11. 使用済み電池は指示に従って廃棄してください。

⚠ 注意事項：

- 本装置を落下させたり物理的衝撃を与えたりせず、高電磁波放射環境に曝さないでください。振動する表面や衝撃を受ける可能性のある場所への設置は避けてください（不注意による装置損傷の原因となります）。
- 本装置を極端に高温（詳細な動作温度は装置の仕様を参照）、低温、ほこりっぽい、または湿気の多い場所に置かないでください。また、強い電磁放射にさらさないでください。
- 直射日光、換気の悪い場所、ヒーターやラジエーターなどの熱源に機器を曝すことは禁止されています（無知は火災の危険を引き起こす可能性があります）。
- 屋内用デバイスカバーは、雨や湿気から保護してください。
- 直射日光、換気の悪い場所、ヒーターやラジエーターなどの熱源に機器を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）。
- デバイスカバーの内側と外側の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。
- 生体認証製品は、完全ななりすまし防止環境には適用されません。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。
- 本装置のシリアルポートはデバッグ専用です。
- 本マニュアルの指示に従って装置を設置してください。怪我を防ぐため、設置指示に従い装置を床/壁に確実に固定してください。
- 電池の不適切な使用または交換は爆発の危険を招く恐れがあります。同種または同等品のみと交換してください。使用済み電池は電池メーカーの指示に従って廃棄してください。
- このブラケットは、付属の機器とのみ使用することを目的としています。他の機器との併用は不安定さを招き、けがの原因となる可能性があります。
- 本装置は専用ブラケットとのみご使用ください。他の台車、スタンド、キャリアなどとの併用は不安定な状態を引き起こし、けがの原因となる可能性があります。

対応モデル

製品名	モデル	ワイヤレス
顔認証端末	DS-K1T343MX	13.56 MHzカード提示周波数
	DS-K1T343MWX	13.56 MHz カード提示周波数、Wi-Fi
	DS-K1T343MFX	13.56 MHz カード提示周波数
	DS-K1T343MFWX	13.56 MHz カード提示周波数、Wi-Fi
	DS-K1T343EX	125 KHz カード提示周波数
	DS-K1T343EWX	125 KHz カード提示周波数、Wi-Fi
	DS-K1T343EFX	125 KHz カード提示周波数
	DS-K1T343EFWX	125 KHz カード提示周波数、Wi-Fi

取扱説明書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
ADS-12FG-12N 12012EPG	深セン•オナー電子有限公司	PG

目次

第1章概要

1.1 概要

顔認識端末は、顔認識のためのアクセス制御デバイスの一種であり、主に物流センター、空港、大学キャンパス、警報センター、住宅などのセキュリティアクセス制御システムに適用されます。

1.2 特徴

- 4.3インチ液晶タッチスクリーン
- 200万画素広角デュアルレンズ
- 顔偽装防止
- 顔認識距離：0.3 m ～ 1.5 m
- 顔認識の推奨高さ：1.4mから1.9mの間
- ディープラーニングアルゴリズム
- 顔登録容量1500件、カード登録容量3000件、イベント記録容量15万件
- 顔認識時間 < 0.2 秒/ユーザー、顔認識精度≥ 99%
- キャプチャ連動とキャプチャ画像保存
- TCP/IPプロトコルを介してクライアントソフトウェアとの間でカードおよびユーザーデータを送受信し、クライアントソフトウェアにデータを保存
- USBフラッシュドライブからデバイスへ画像をインポート、またはデバイスからUSBフラッシュドライブへ画像•イベントをエクスポート
- スタンドアロン動作
- デバイスにローカルでログイン後、デバイスデータの管理、検索、設定が可能
- RS-485プロトコル経由で1台の外部カードリーダーまたはアクセスコントローラーに接続
- RS-485プロトコル経由でセキュアドア制御ユニットに接続し、デバイス破壊時のドア開放を防止
- 双方向音声通信
- 複数クライアントソフトウェアによる武装
- ウォッチドッグ設計と改ざん検知機能
- 英語、スペイン語（南米）、アラビア語、タイ語、インドネシア語、ロシア語、ベトナム語、ポルトガル語（ブラジル）、韓国語、日本語に対応

第2章外観

指紋認証機能付きデバイスの外観は以下の通りです：

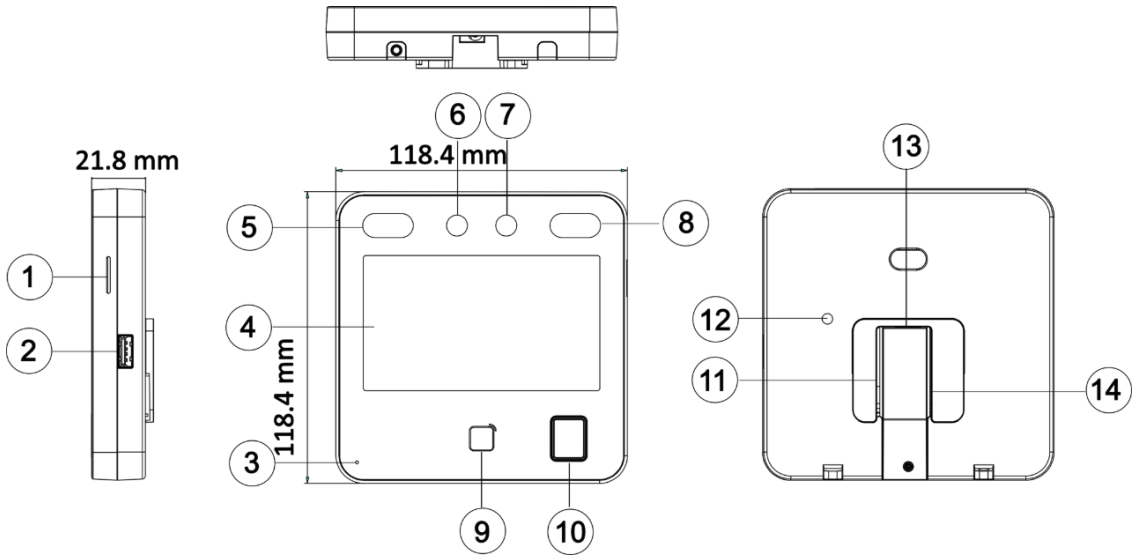


図2-1 外観（指紋認証機能付き）

指紋認証機能なしのデバイスの外観は以下の通りです：

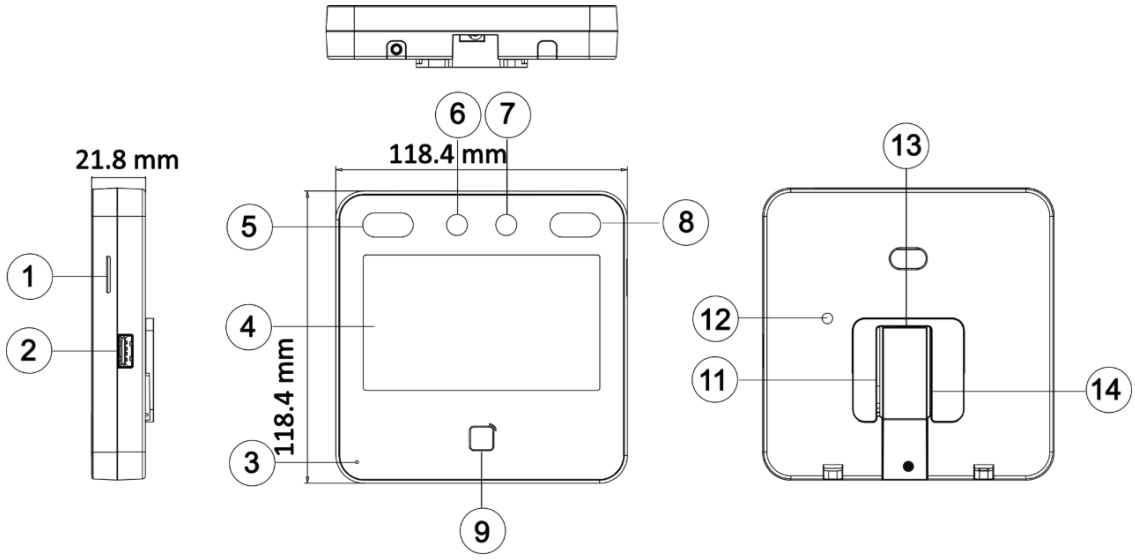


図2-2 外観（指紋認証機能なし）

表 2-1 外観説明

No.	名称
1	スピーカー
2	USBインターフェース
3	マイク
4	タッチスクリーン
5	赤外線ライト
6	カメラ
7	カメラ
8	IRライト
9	カード提示エリア
10	指紋モジュール **注記** 指紋機能をサポートするデバイスにのみ指紋モジュールが搭載されています。
11	配線端子（電源インターフェースを含む）
12	タンパー
13	ネットワークインターフェース
14	デバッグポート（デバッグ専用）

第3章インストール

3.1 設置環境

- バックライト、直射日光、間接日光を避けてください。
- 認識精度を高めるため、設置環境内またはその近くに光源があることが望ましいです。
- 壁などの最小耐荷重は、装置重量の 3 倍以上であること。
- 装置の視野範囲1m以内に、強い反射物（ガラスドア/壁、ステンレス製品、アクリルなどの光沢プラスチック、漆、セラミックタイルなど）があってはいけません。
- デバイスの反射を避けてください。
- 顔認識距離は30cm以上であること。
- カメラを清潔に保ってください。

注意

設置環境の詳細については、「**設置環境に関する注意事項**」を参照してください。

3.2 ジャンボックス付き設置

手順

1. 壁に配線ボックスが設置さ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別途購入してください。

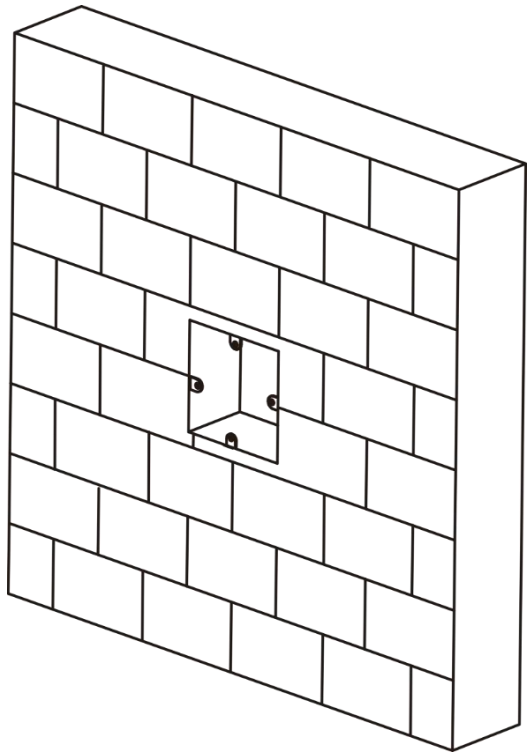


図3-1 ギャングボックスの取り付け

2. 付属のネジ4本（M4）を使用して、取り付けプレートをギャングボックスに固定します。

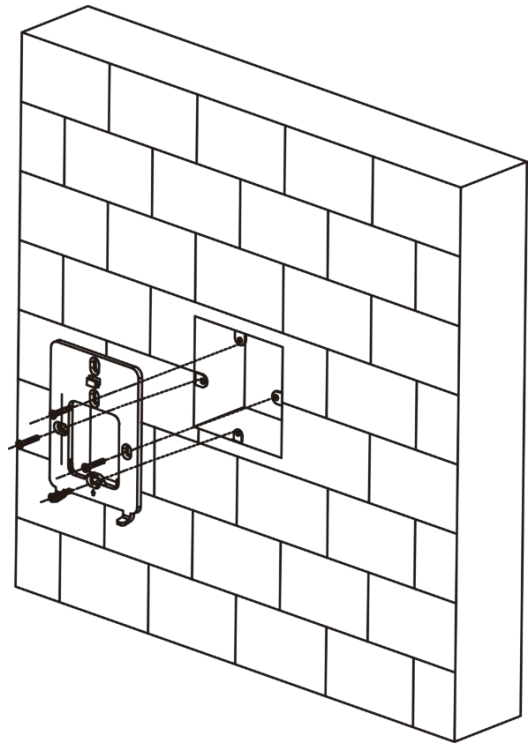


図3-2 取付プレートの取り付け

3. ケーブルをマウントプレートのケーブル穴に通し、対応する周辺機器ケーブルに接続します。
4. デバイスをマウントプレートに合わせたら、マウントプレートに固定します。付属のネジ（M3）1本を使用して、デバイスをマウントプレートに固定します。

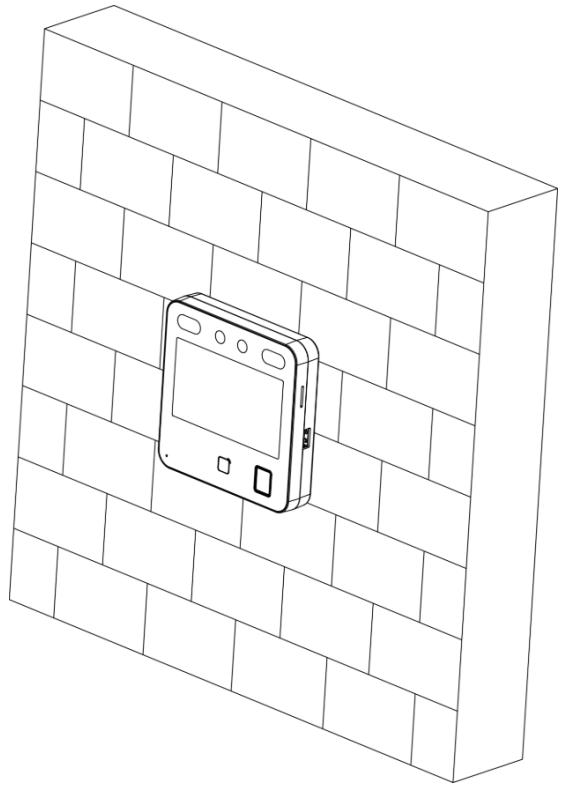


図 3-3 デバイスの固定

3.3 ベース取り付け

手順

1. ケーブルをブラケットのケーブル穴に通し、端子を周辺機器ケーブルに接続します。ブラケットをデバイスの背面近くに配置します。

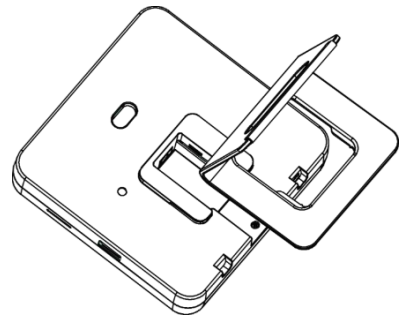


図 3-4 ブラケットをデバイスの背面近くに配置

2. ブラケットを両手で押さえ、ブラケットのバックルがデバイスの裏側に合うことを確認してください。矢印の方向にブラケットを固定してください。

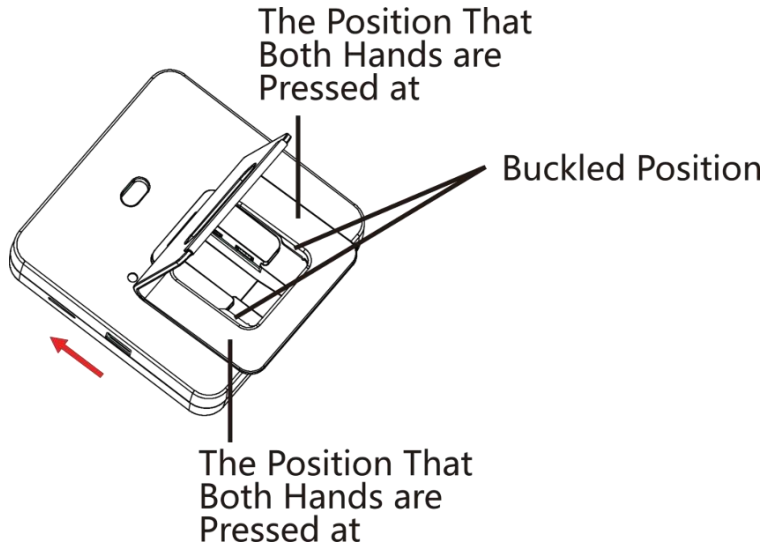


図3-5 ブラケットの固定

3. 取り付けを完了させるため、ブラケットにバックルを最後まで差し込みます。

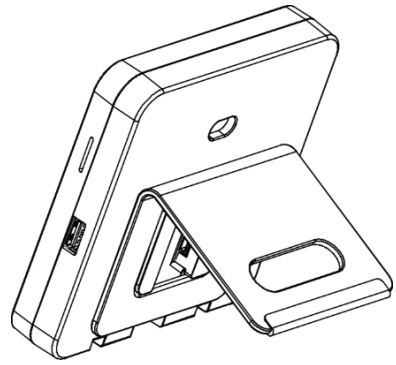


図3-6 取り付け完了

第4章配線

RS-485 端子を RS-485 カードリーダーに接続し、NC/NO 端子と COM 端子をドアロックに接続し、SEN 端子と GND 端子をドアコンタクトに接続し、BTN/GND 端子を退出ボタンに接続し、Wiegand 端子をアクセスコントローラに接続することができます。

WIEGAND端末をアクセスコントローラに接続すると、顔認証端末は認証情報をアクセスコントローラに送信でき、アクセスコントローラはドアを開けるかどうかの判断を行います。

注記

- ケーブルサイズが18AWGの場合、12V電源を使用してください。また、電源と機器間の距離は20m以内にしてください。
- ケーブルサイズが15AWGの場合、12V電源を使用してください。また、電源とデバイス間の距離は30m以内にしてください。
- ケーブルサイズが12AWGの場合、12V電源を使用してください。また、電源と機器間の距離は40m以内にしてください。
- 外部カードリーダー、ドアロック、退出ボタン、ドア磁気センサーにはそれぞれ個別の電源供給が必要です。

4.1 端子説明

端子には電源入力、RS-485、ウィーガンド出力、ドアロックが含まれます。端子の説明は以下の通

りです：

表 4-1 端子説明

グループ	番号	機能	色	名称	説明
グループ A	A1	入力電力	赤	+12 V	12 VDC 電源
	A2		黒	GND	接地
グループ B	B1	RS-485	黄色	485+	RS-485 配線
	B2		青	485-	
	B3		黒	GND	接地
グループ C	C1	ウィーガンド	緑	W0	ウィーガンド配線 0

グループ	番号	機能	色	名称	説明
	C2		白	W1	ウィーガンド配線 1
	C3		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	NO	ロック配線(NO)
	D4		黄/緑	SENSOR	ドアコンタクト
	D5		黒	GND	接地
	D6		黄/灰色	ボタン	出口ドア配線

4.2 ワイヤ通常デバイス

この端子は、通常の周辺機器に接続できます。

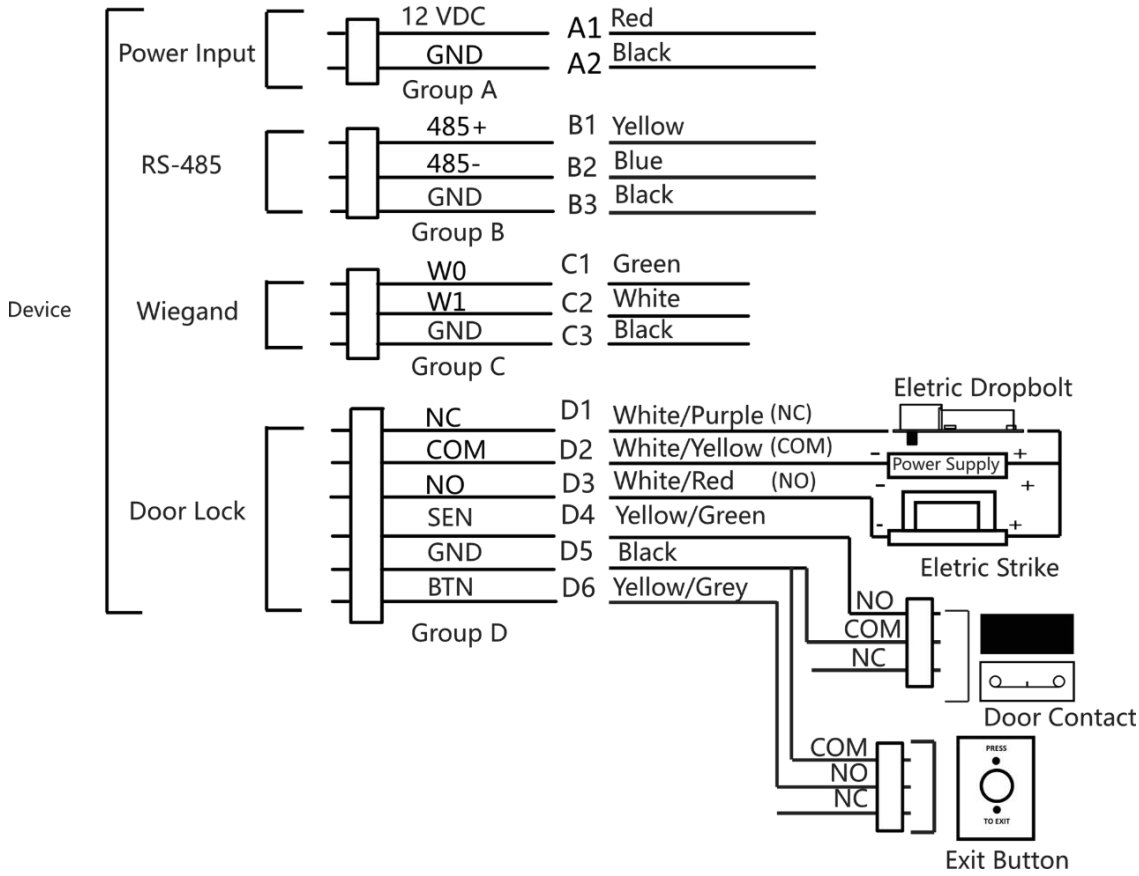


図 4-1 デバイス配線

注記

- アクセスコントローラに接続する場合、認証情報をアクセスコントローラに送信するため、ウィーガンド方向を「**出力**」に設定する必要があります。
- Wiegand方向設定の詳細については、「***Wiegand*パラメータの設定」**を参照してください。
- 本装置を電源に直接配線しないでください。

4.3 セキュアドア制御ユニットの配線

端末をセキュアドア制御ユニットに接続することができます。配線図は次のとおりで

す。

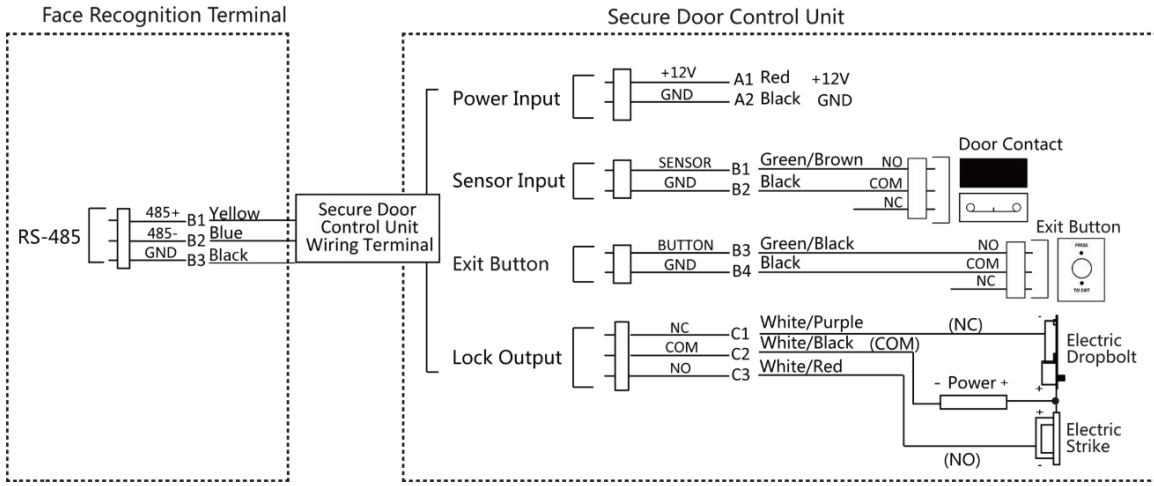


図 4-2 セキュアドア制御ユニットの配線

注記

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。

4.4 ワイヤー火災モジュール

4.4.1 電源オフ時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（常時開放型）セキュリティタ

イプ：電源オフ時にドア開放

シナリオ：消防車アクセス用として設置

タイプ1

注記

消防システムがアクセス制御システムの電源を制御する。

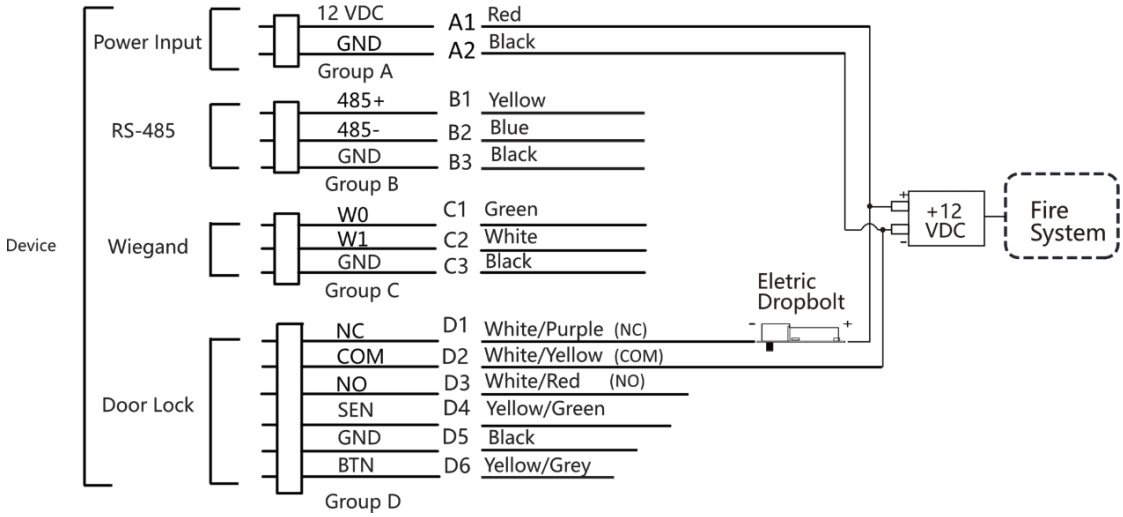


図 4-3 配線装置

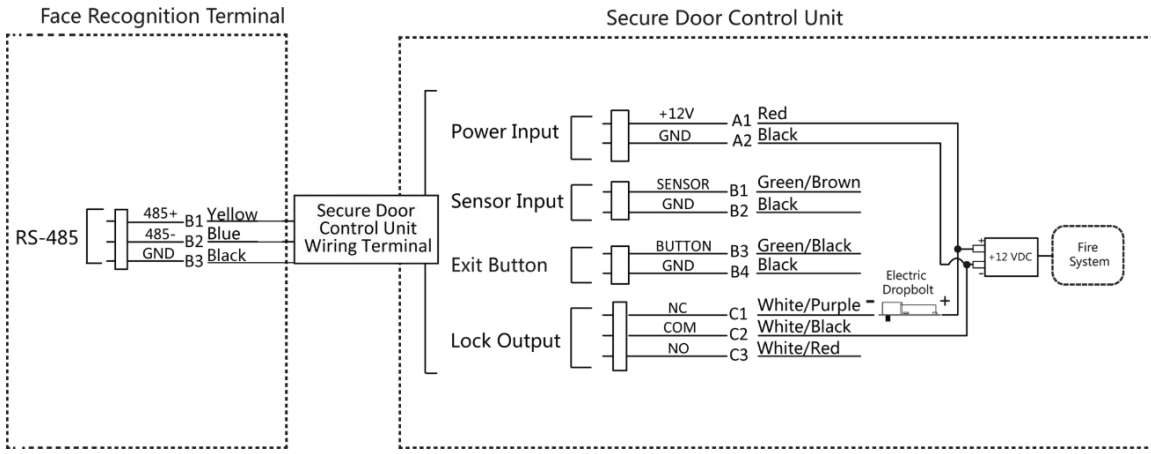


図 4-4 配線式セキュリティドア制御ユニット

タイプ 2

注記

火災システム（NOとCOM、電源オフ時は通常開）は、ロックと電源を直列に接続する。火災警報が作動すると、ドアは開いたままとなる。通常時はNOとCOMは閉状態である。

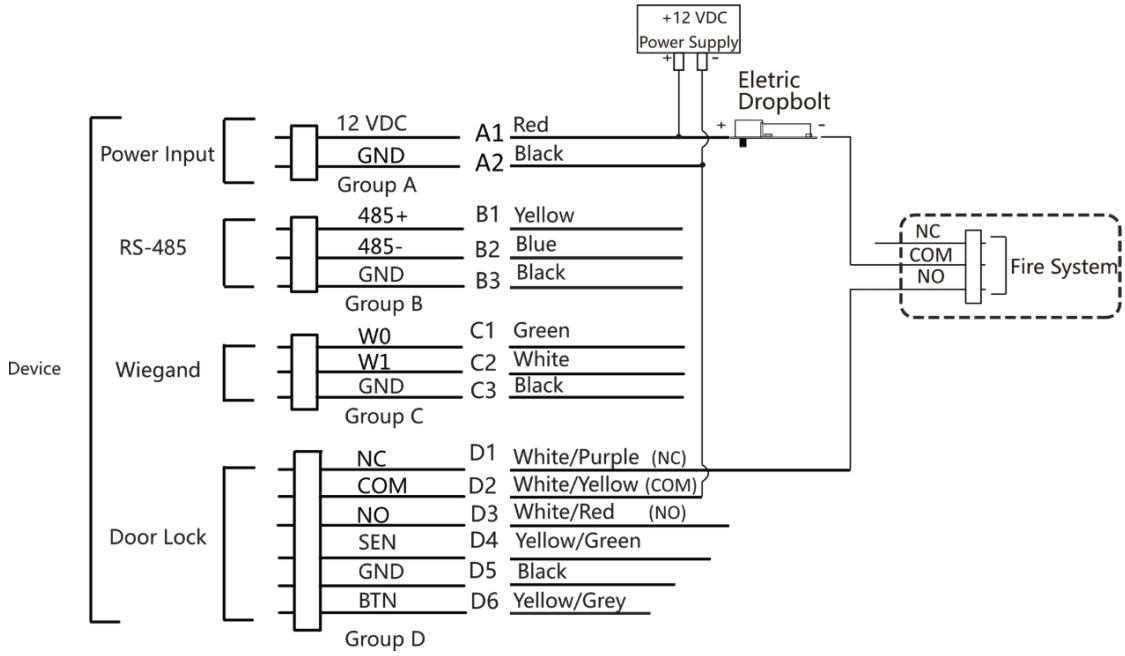


図4-5 配線装置

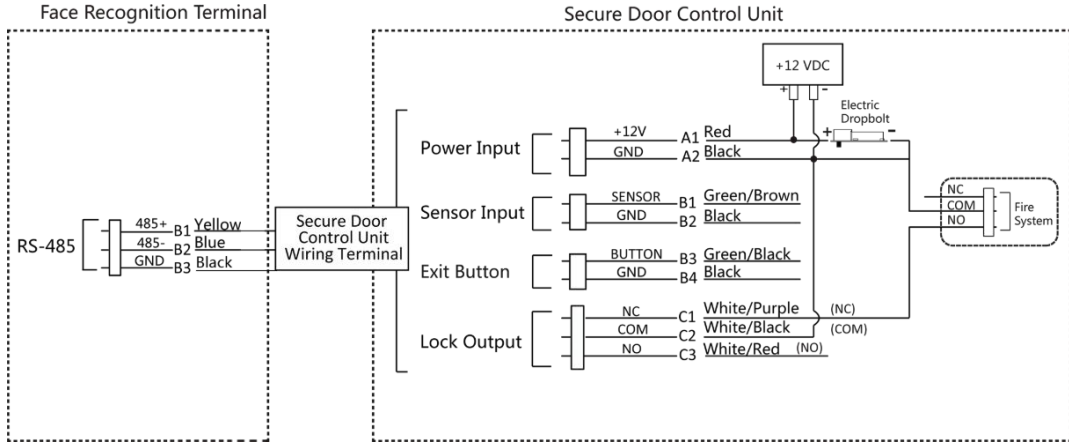


図4-6 セキュアドア制御ユニットの配線

4.4.2 電源オフ時にドアがロックされる配線図

ロックタイプ：カソードロック、電気ロック、電気ボルト（NC）セキュリティタイプ

：電源オフ時にドアロック

シナリオ：火災連動付き出入口への設置

注記

- 無停電電源装置（UPS）が必要です。
- 火災システム（NCとCOM、電源オフ時は通常閉）は、ロックと電源を直列に接続する。火災警報が作動すると、ドアは開いたままとなる。通常時はNCとCOMは開いている。

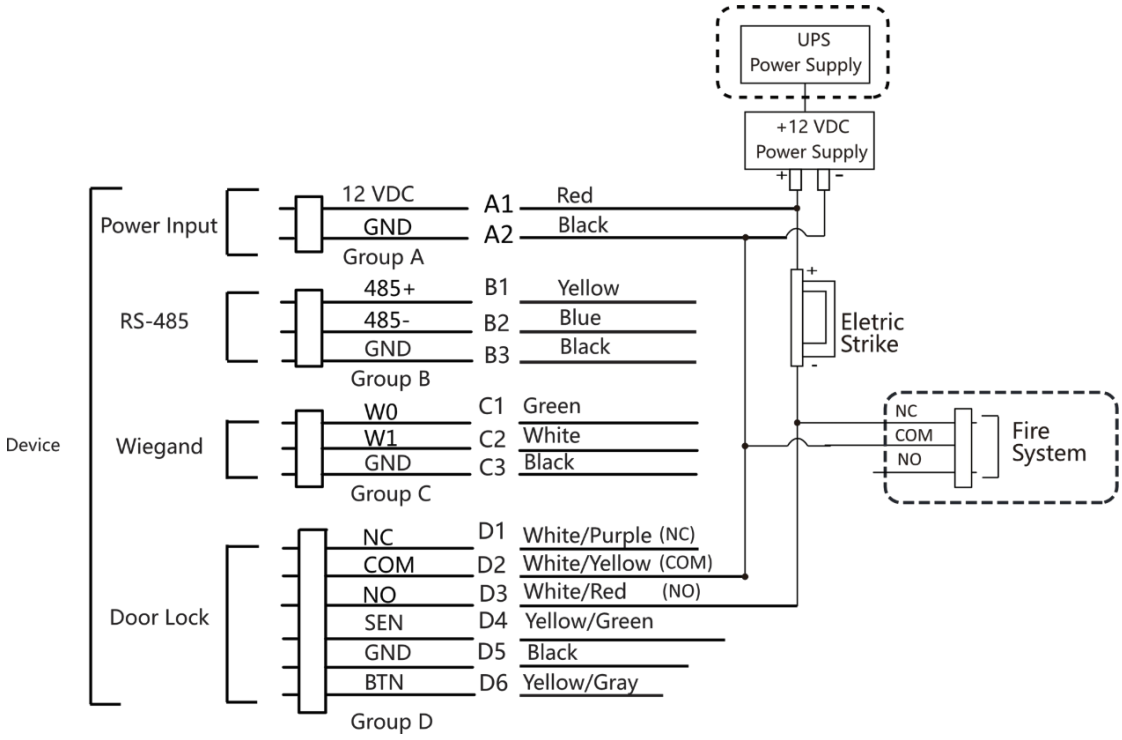


図4-7 装置配線図

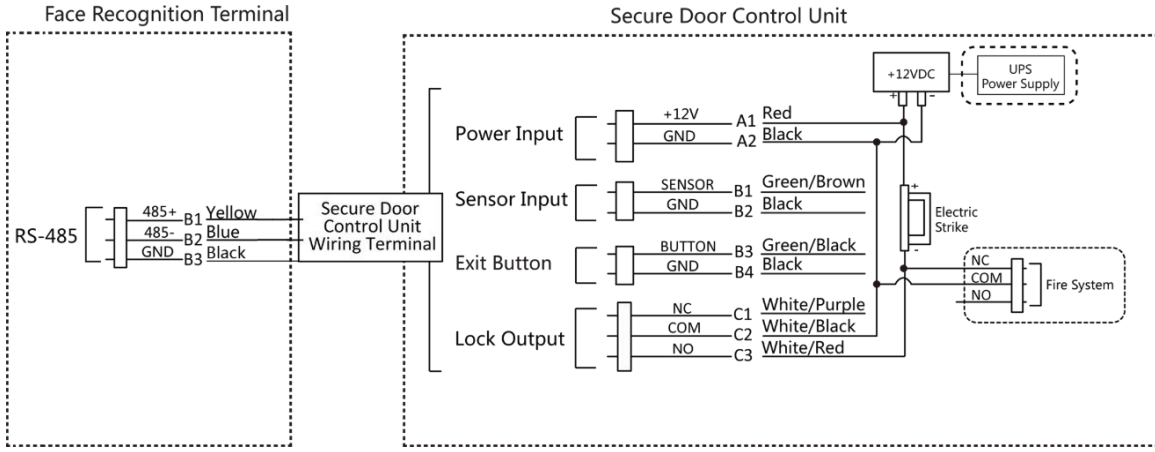


図4-8 配線図

第5章アクティベーション

初回ログイン前にデバイスをアクティベートする必要があります。デバイスの電源投入後、システムはデバイスアクティベーションページに切り替わります。

デバイス本体、SADPツール、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以下の通りです：

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

5.1 デバイス経由でアクティベート

デバイスがアクティベートされていない場合、電源投入後にアクティベートできます。

「デバイスのアクティベート」ページでパスワードを作成し、確認してください。「**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。

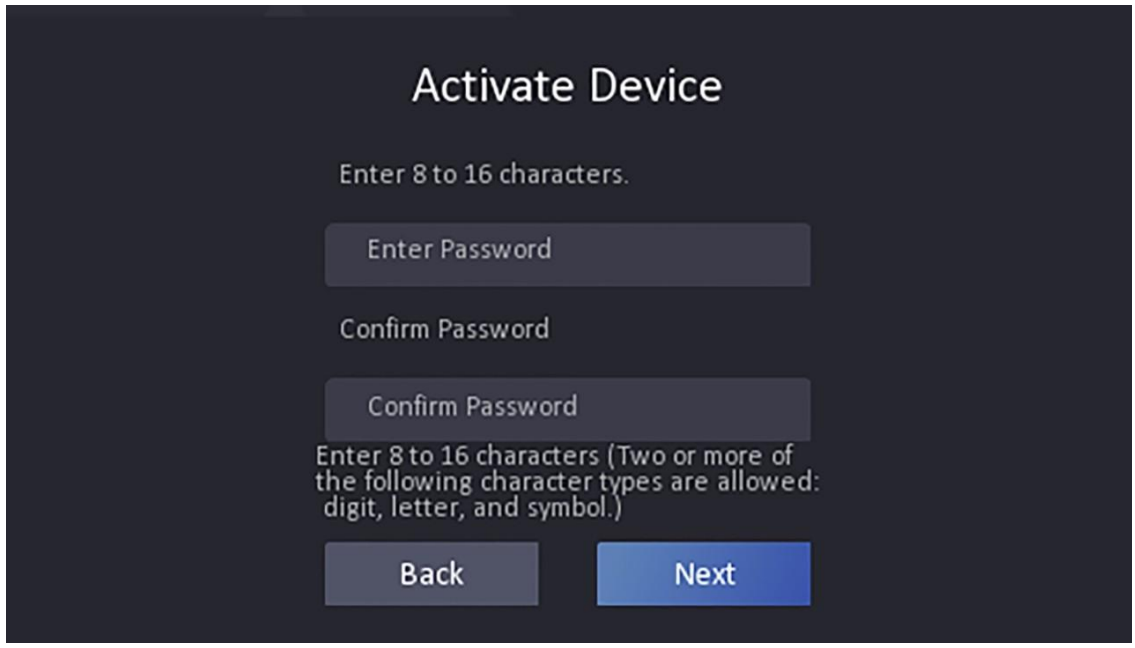


図5-1 アクティベーション画面

注意

デバイスのパスワード強度を自動的に確認できます。ご自身で選択したパスワードに変更することを強く推奨します（最低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）。

製品のセキュリティを強化するため、パスワードには大文字と小文字、数字、記号を含む8文字以上の文字列を使用してください。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推奨します。月次または週次での変更により、製品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構成は、設置業者および / 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。

- アクティベーション後、実際のニーズに応じて言語を選択してください。
- アクティベーション後、アプリケーションモードを選択する必要があります。詳細については、「**アプリケーションモードの設定**」を参照してください。
- アクティベーション後、ネットワークを設定する必要があります。詳細は「**ネットワークパラメータの設定**」を参照してください。
- アクティベーション後、デバイスをプラットフォームに追加できます。詳細は「**プラットフォームへのアクセス**」を参照してください。
- アクティベーション後、プライバシー設定が必要な場合は該当項目を確認してください。詳細は「**プライバシー設定**」を参照してください。
- アクティベーション後、デバイスパラメータを管理する管理者追加が必要な場合は、管理者設定を行ってください。詳細は「**管理者の追加**」を参照してください。

5.2 Webブラウザ経由でアクティベート

ウェブブラウザ経由でデバイスを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。
Enterキーを押します。

注
デバイスの IP アドレスとコンピューターの IP アドレスが同じ IP セグメント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ます。

注意
強力なパスワードの使用を推奨します-製品のセキュリティ強化のため、ご自身で選択した強力なパスワード（大文字、小文字、数字、特殊文字を含む8文字以上）の設定を強く推奨します。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（月次または週次で）リセットすることで製品をより効果的に保護できます。

注意
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。

3. **アクティベート**をクリックします。
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、有効化、変更するためのツールです。

開始前に

- 付属ディスクまたは公式ウェブサイト ***http://www.hikvision.com/en/*** から SADP ソフトウェアを入手し、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 PC とデバイスは、同じサブネット内に存在している必要があります。

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。一括アクティベーションおよびIPアドレス変更の詳細については、***SADP*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デバイスを探して選択します。

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。

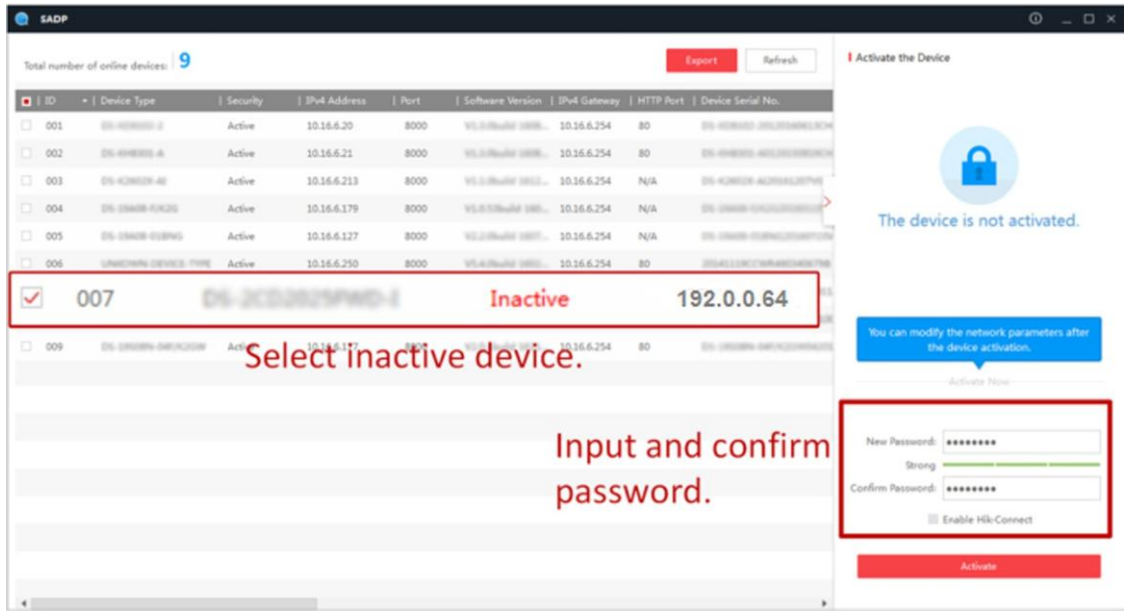
注意

強力なパスワードの使用を推奨します-製品のセキュリティ強化のため、ご自身で選択した強力なパスワード（大文字、小文字、数字、特殊文字を含む8文字以上）の設定を強く推奨します。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（月次または週次で）リセットすることで製品をより効果的に保護できます。

注意

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. **アクティベート**をクリックしてアクティベーションを開始します。



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は「**Active**」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、手動で変更するか「**DHCPを有効にする**」にチェックを入れることで、お使いのコンピューターと同じサブネットに変更してください。

3) 管理者パスワードを入力し、「**変更**」をクリックしてIPアドレス変更を有効化してください。

5.4 iVMS-4200クライアントソフトウェア経由でデバイスをアクティベートする

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、アクティベート用のパスワードを作成する必要があります。

手順

注

この機能はデバイスがサポートしている必要があります。

1. デバイス管理ページに入ります。

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. デバイス状態（セキュリティレベル列に表示）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強度を自動で確認できます。製品のセキュリティ強化のため、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）への変更を強く推奨します。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お勧めします。月次または週次での変更により、製品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構成は、設置業者および/またはエンドユーザーの責任となります。

注記

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。

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 言語の選択

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、デバイスシステムの言語を選択できます。

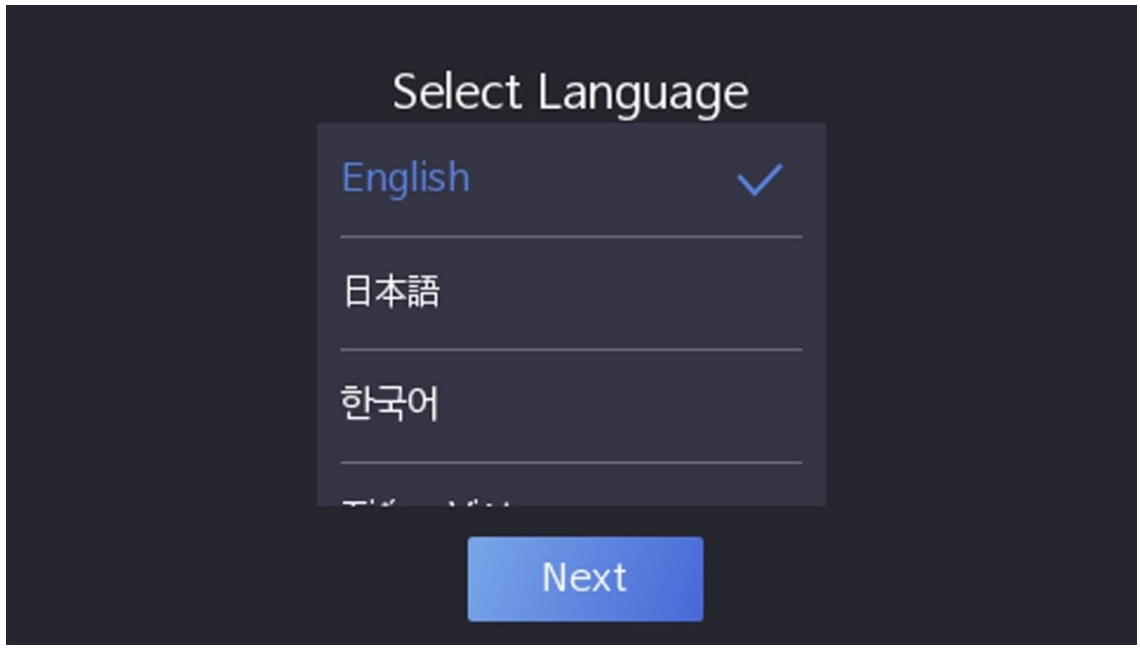


図 6-1 システム言語の選択

デフォルトでは、システム言語は英語です。

注

システム言語を変更すると、デバイスは自動的に再起動します。

6.2 アプリケーションモードの設定

デバイスの起動後、より良いデバイスアプリケーションのためにアプリケーションモードを選択してください。

手順

1. ウェルカムページで、ドロップダウンリストから「**屋内**」または「**その他**」を選択します。

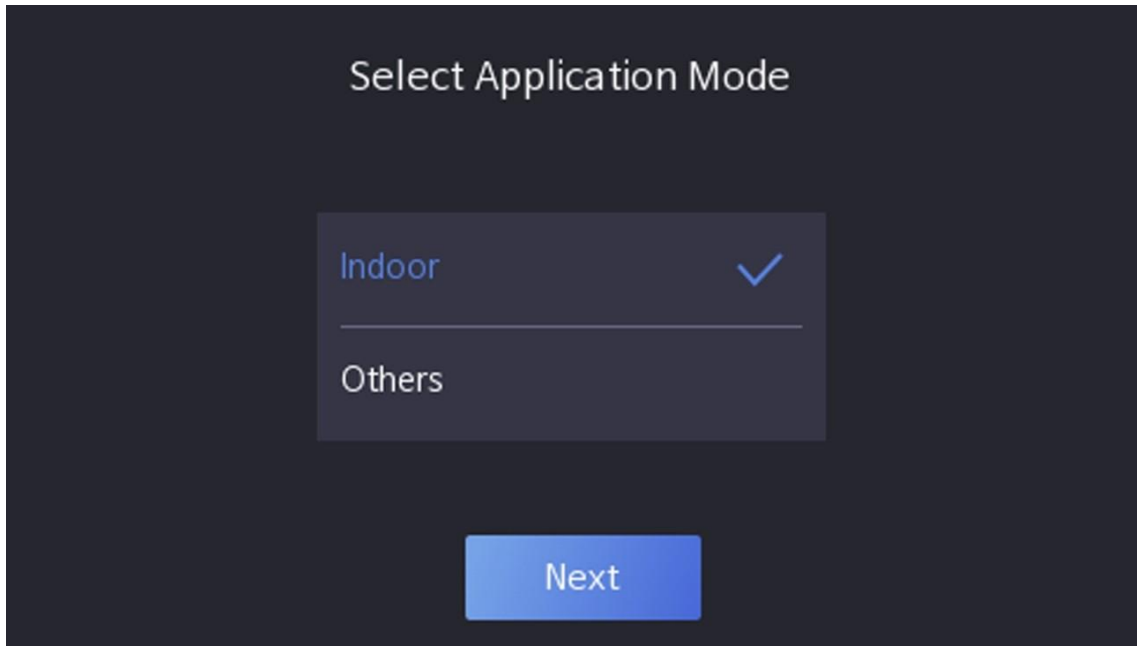


図 6-2 ウェルカムページ

2. **OK** をタップして保存します。

注

- **システム設定でも**設定を変更できます。
- デバイスを屋内の窓の近くに設置する場合、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「**屋内**」を選択します。
- 他のツールでデバイスをリモートで起動する場合、システムはデフォルトでアプリケーションモードとして**屋内**を選択します。

6.3 ネットワークパラメータの設定

起動後、アプリケーションモードを選択すると、デバイスのネットワークを設定できます。

手順

1. ネットワーク選択ページに入ったら、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。

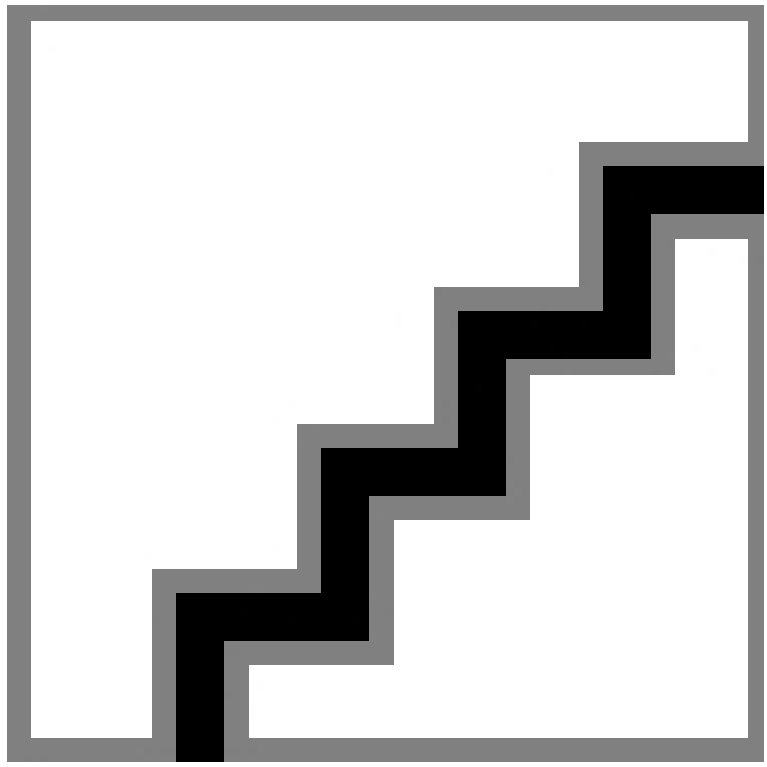


図6-3 ネットワークの選択

注記

Wi-Fi に接続する前に、有線ネットワークを切断してください。

2. [次へ] をタップしま

す。**有線ネットワー**

ク **注**

お使いの端末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アドレスやその他のパラメータを自動的に割り当てます。**DHCPを**無効にする場合は、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てください。

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

この機能を有効にすると、デバイスは Hik-Connect 経由で通信できるようになります。デバイスを Hik-Connect モバイルクライアントなどに追加できます。

手順

1. Hik-Connect へのアクセスを有効にし、サーバー IP および認証コードを設定します。

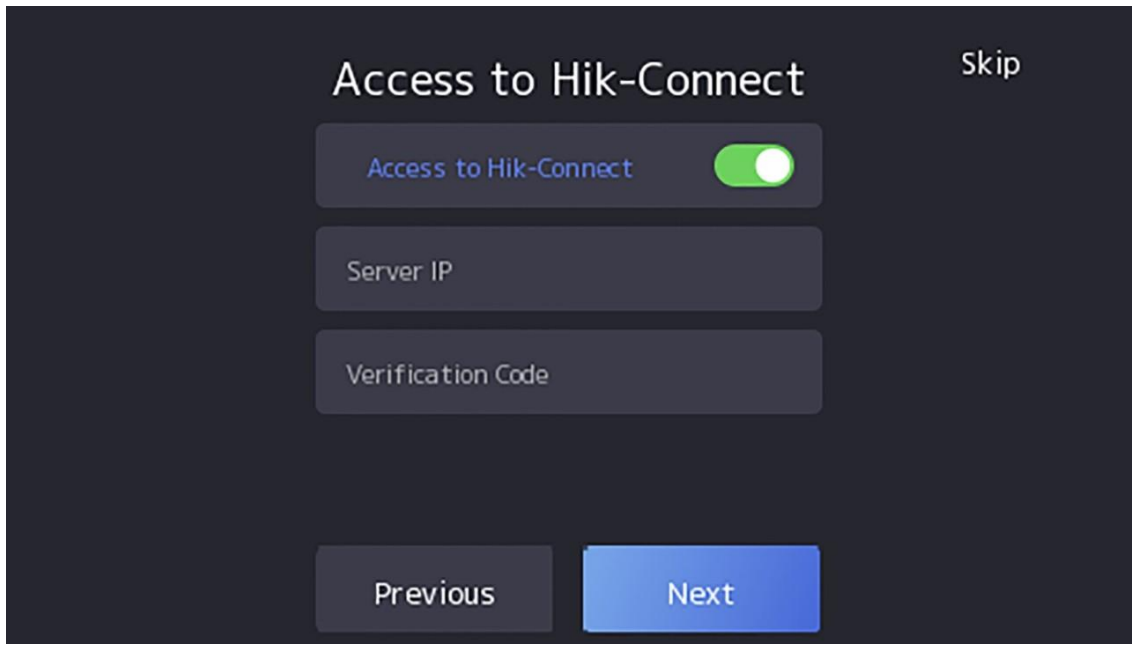


図 6-4 Hik-Connect へのアクセス

2.「次へ」をタップします。

注

前の画面に戻るには**「戻る」を**タップしてください。Wi-Fi設定ページに戻る場合、接続済みのWi-Fiを再度タップするか、別のWi-Fiに接続してプラットフォームページ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

起動後、アプリケーションモードの選択、ネットワークの選択を行った後、画像のアップロードや保存など、プライバシーに関するパラメータを設定してください。

実際のニーズに応じてパラメータを選択してください。

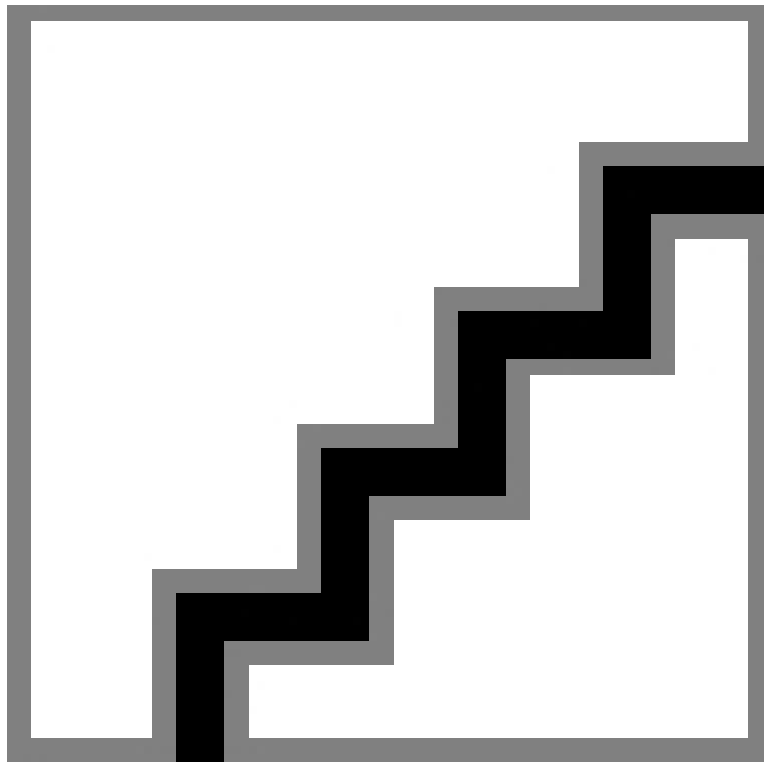


図 6-5 プライバシー

認証時に撮影画像をアップロード

プラットフォームへの認証時に撮影した画像を自動的にアップロードします。

認証時にキャプチャした画像を保存

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。

登録画像を保存 (登録画像を保存)

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。

リンク撮影後の画像アップロード

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

リンク撮影後の画像保存 (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。

設定を完了するには「**次へ**」をタップしてください。

6.6 管理者設定

デバイスのアクティベーション後、デバイスのパラメータを管理する管理者を追加できます。

開始前に

デバイスのアクティベートとアプリケーションモードの選択

手順

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

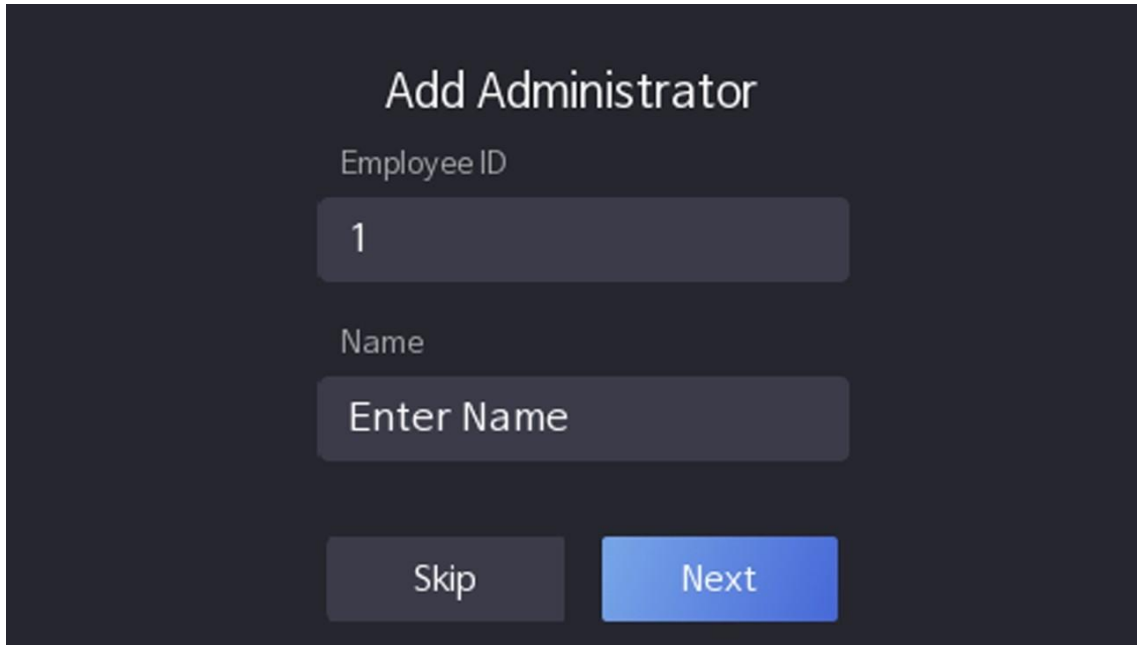


図6-6 管理者追加ページ

3. 追加する認証情報を選択します。

注

認証情報は最大1つまで追加してください。

- : カメラに向かって正面を向いてください。顔が顔認識エリア内にあ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ます。
- : デバイス画面の指示に従って指を押してください。 をクリックして確認します。
- カード番号を入力するか、カードをカード提示エリアに提示してください。**OK**をクリックしてください。

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。

ステータスアイコンの説明

/

装置が武装状態/非武装状態です。

/

Hik-Connectが有効/無効です。

/ /

デバイスの有線ネットワークは接続中/未接続/接続失敗。

デバイスのWi-Fiは有効化され接続済み/未接続/有効化済みだが未接続です。

ショートカットキーの説明

注記

画面に表示されているショートカットキーを設定できます。詳細は**基本設定を**参照してください。

- デバイスルーム番号を入力し、**OK**をタップして呼び出します。
-  をタップしてセンターに呼び出します。

注意

センターにデバイスが追加されていない場合、発信操作は失敗します。

認証用の PIN コードを入力してください。

第7章基本操作

7.1 ログイン

デバイスの基本パラメータを設定するために、デバイスにログインします。

7.1.1 管理者によるログイン

デバイスに管理者を追加した場合、デバイスの操作には管理者だけがログインできます。

手順

1. 初期画面を3秒間長押しし、表示されるジェスチャーに従って左/右にスライドすると、管理者ログイン画面に入ります。

図7-1 管理者ログイン

2. 管理者の顔認証、指紋認証、またはカード認証を行い、ホームページに入ります。

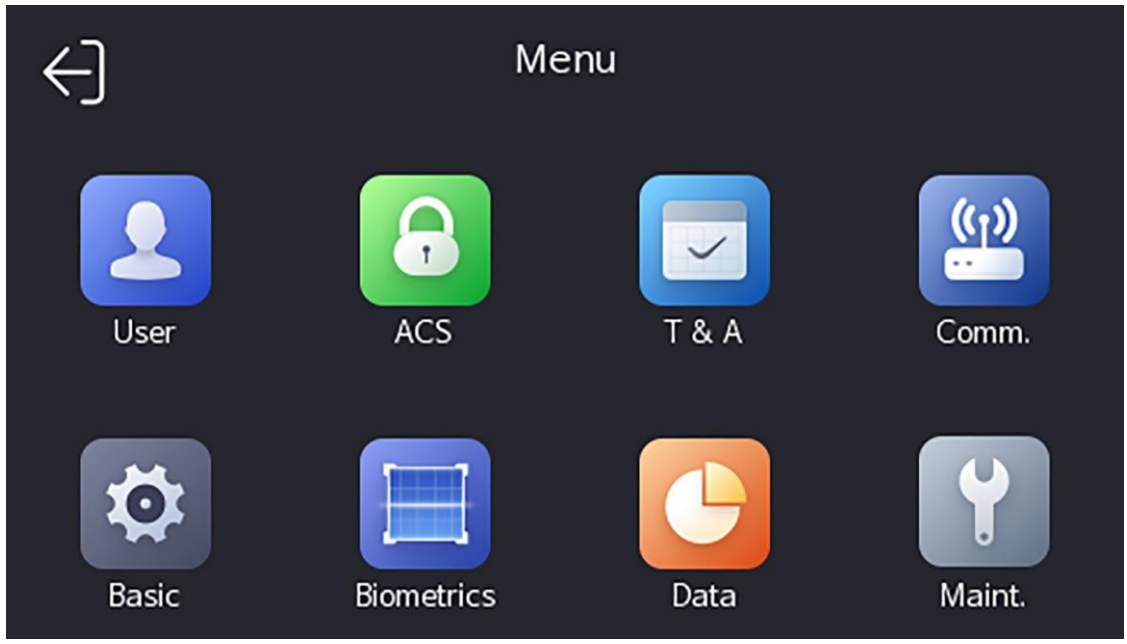


図 7-2 ホームページ

注記

指紋またはカード認証が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起動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、管理者ログインページを終了できます。

7.1.2 アクティベーションパスワードによるログイン

他のデバイス操作の前に、システムにログインする必要があります。管理者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. 最初のページを3秒間長押しし、ジェスチャーに従って左/右にスライドすると、パスワード入力ページに入ります。
2. パスワードを入力してください。
   - デバイスの管理者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。
   - デバイスの管理者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ページに入ります。

注記

パスワードの入力に5回失敗すると、デバイスは30分間ロックされます。

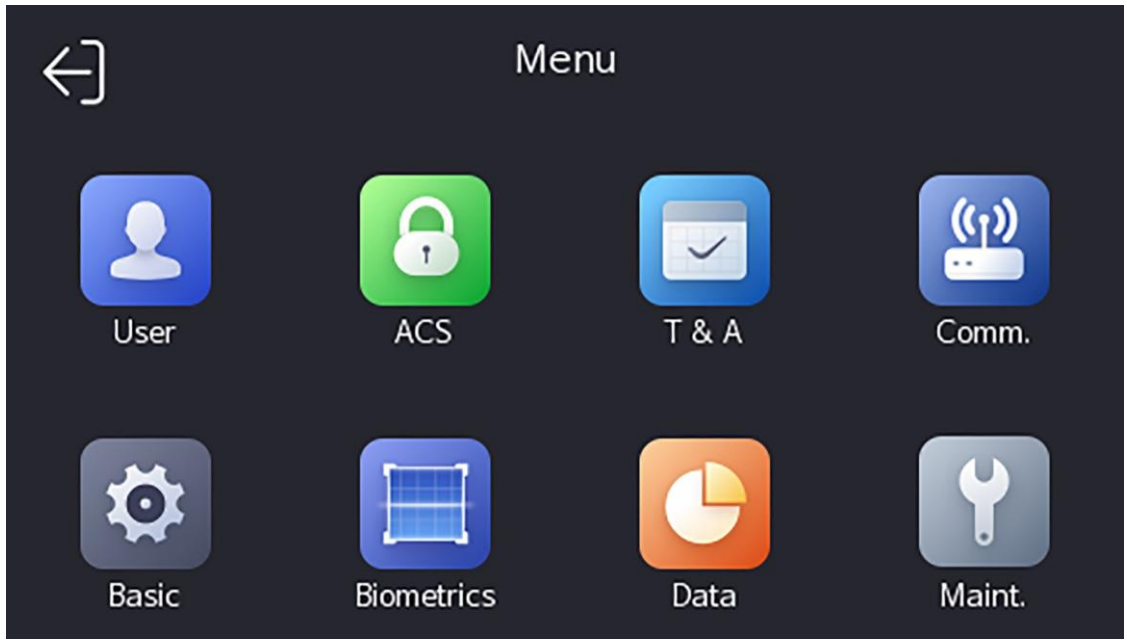


図7-3 ホームページ

7.1.3 パスワードを忘れた場合

認証中にパスワードを忘れた場合、キーをインポートすることでパスワードをリセットできます。

手順

1. 初期ページを 3 秒間長押しし、ジェスチャーに従って左/右にスライドしてログインページに移動します。
2. ポップアップ管理認証ページで「 」をタップします。
3. USBフラッシュドライブをUSBインターフェースに接続します。

注意

- サポートされている USB フラッシュドライブのフォーマットは、FAT32 および exfat です。
- 本デバイスは1GBから32GB（1GBおよび32GBを含む）の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。

4. **「ファイルをエクスポート」**をタップし、技術者に連絡してキーを取得し、エクスポートファイルにキーを入力してください。
5. **「ファイルをインポート」**をタップし、キーを含むファイルをデバイスにインポートします。
6. 指示に従ってパスワードをリセットしてください。

7.2 通信設定

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

7.2.1 有線ネットワークパラメータの設定

デバイスの有線ネットワークパラメータ（IPアドレス、サブネットマスク、ゲートウェイ、DNSパラメータを含む）を設定できます。

手順

1. ホームページで「通信設定」をタップし、通信設定ページに入ります。

2. 通信設定ページで、「**有線ネットワーク**」をタップします。

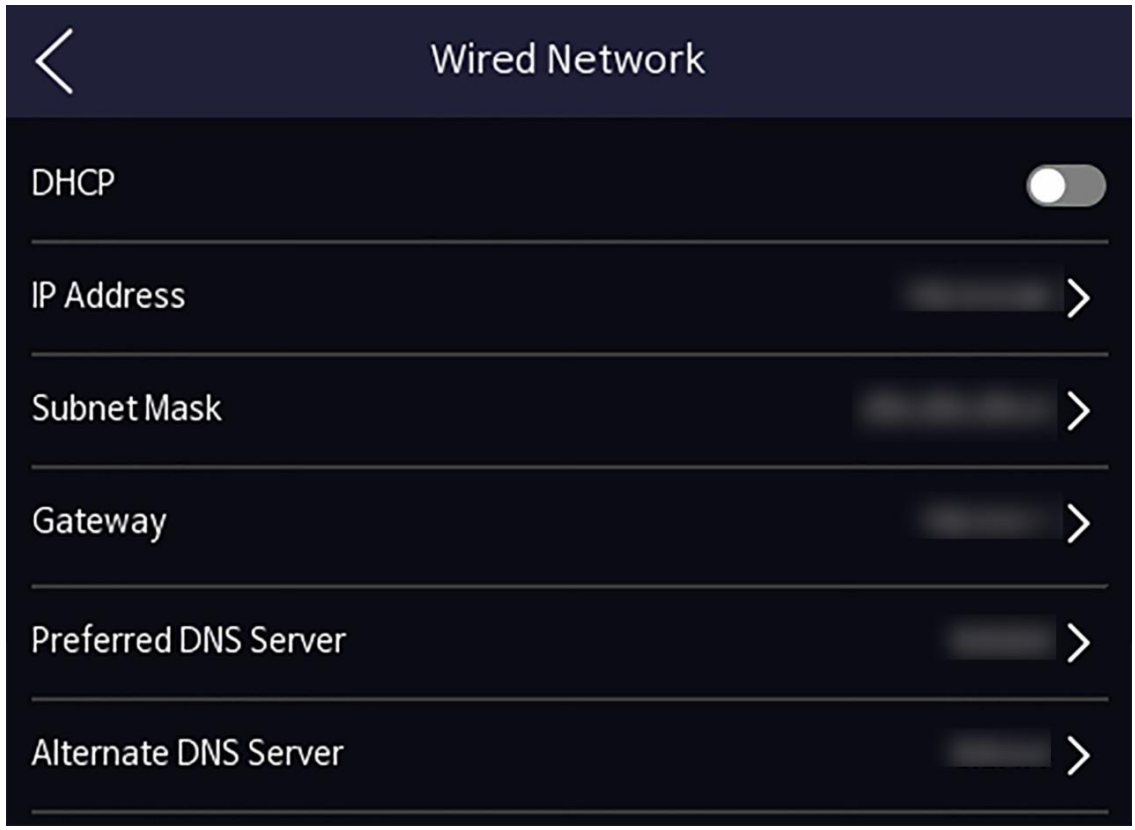


図 7-4 有線ネットワーク設定

3. IP アドレス、サブネットマスク、ゲートウェイを設定します。

- **DHCPを**有効にすると、システムが自動的にIPアドレス、サブネットマスク、ゲートウェイを割り当てます。
- **DHCPを**無効にすると、IPアドレス、サブネットマスク、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 セグメントである必要があります。

4. DNS パラメータを設定します。**DNS の自動取得を**有効にし、優先 DNS サーバーと代替 DNS サーバーを設定することができます。

7.2.2 Wi-Fi パラメータの設定

Wi-Fi機能を有効にし、Wi-Fi関連のパラメータを設定できます。

手順

注意

お使いの端末がこの機能をサポートしている必要があります。

1. ホーム画面で「通信設定」をタップし、「通信設定」ページに入ります。
2. 通信設定ページで、をタップします。

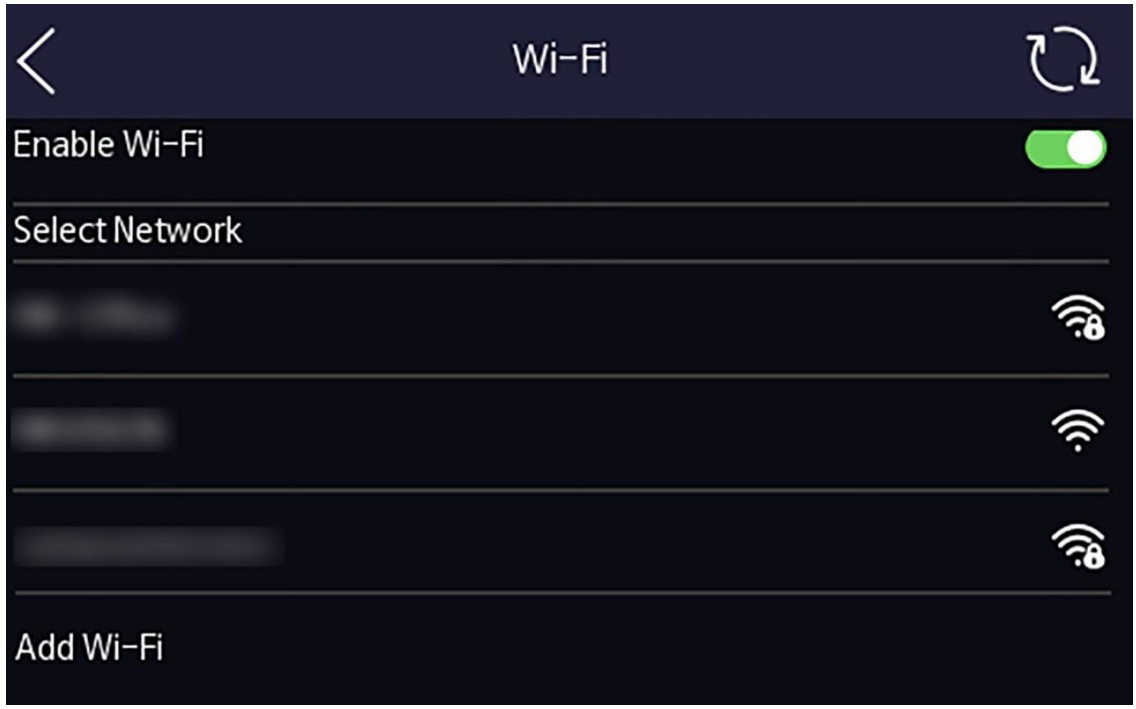


図 7-5 Wi-Fi 設定

3. Wi-Fi 機能を有効にします。
4. Wi-Fi パラメータを設定します。
   - 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。
   - 対象の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のパラメータを設定します。

- デフォルトでは、DHCPが有効になっています。システムは、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を無効にする場合は、IPアドレス、サブネットマスク、ゲートウェイを手動で入力する必要があります。

6. 設定を保存してWi-Fiタブに戻るには、**[OK]**をタップしてください。

7. をタップしてネットワークパラメータを保存します。

7.2.3 RS-485パラメータの設定

顔認識端末は、RS-485 端末を介して、外部アクセスコントローラ、セキュリティドア制御ユニット、またはカードリーダーに接続できます。

手順

1. ホームページで「**Comm.** (通信設定)」をタップし、通信設定ページに入ります。

2. 通信設定ページで、**[RS-485]** をタップして RS-485 タブに入ります。

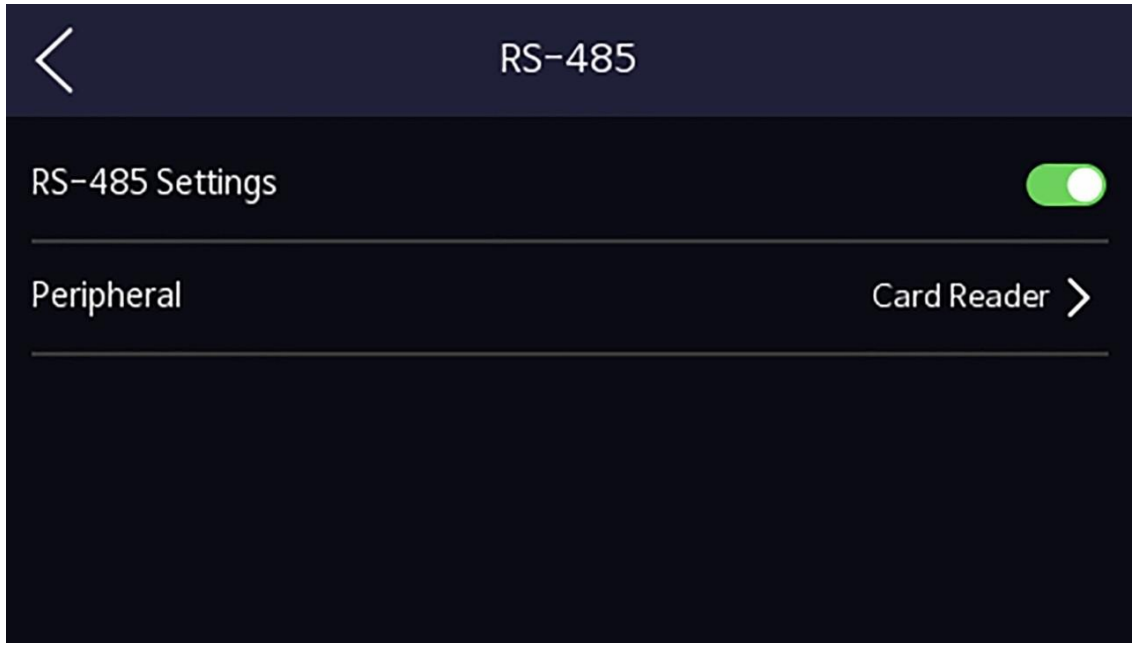


図 7-6 RS-485 パラメータの設定

3. 実際のニーズに応じて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を選択した場合：RS-485 インターフェースを介してデバイスを端末に接続する場合は、RS-485 アドレスを 2 に設定してください。デバイスをコントローラに接続する場合は、ドア番号に応じて RS-485 アドレスを設定してください。

4. 左上の戻るアイコンをタップし、パラメータ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 パラメータの設定

Wiegand 伝送方向を設定できます。

手順

1. ホームページで「**Comm.** (通信設定)」をタップし、通信設定ページに入ります。
2. 通信設定ページで、**ウィーガンド**をタップしてウィーガンドタブに入ります。

図 7-7 ウィーガンド設定

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に接続することができます。そして、2 つのデバイスは、Wiegand 26 または Wiegand 34 を通じてカード番号を送信します。
5. をタップしてネットワークパラメータを保存します。

注記

外部デバイスを変更し、デバイスパラメータを保存すると、デバイスは自動的に再起動します。

7.2.5 ISUP パラメータの設定

ISUPパラメータを設定すると、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

お使いの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. **[通信]** → **[ISUP]** をタップします。

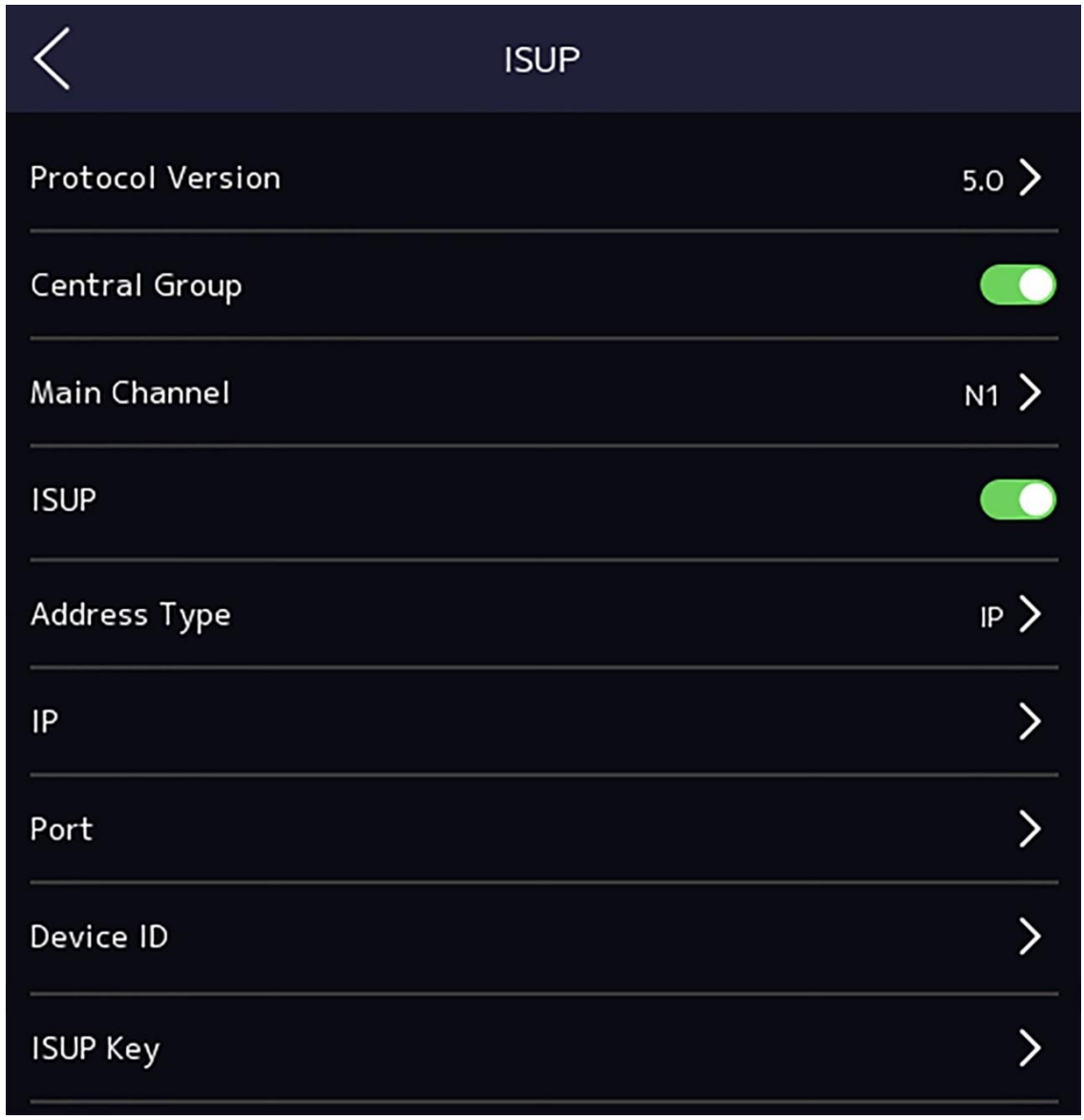


図 7-8 ISUP 設定

2. ISUP 機能を有効にし、ISUP サーバーのパラメータを設定します。

ISUP バージョン

実際のニーズに応じて ISUP バージョンを設定します。

中央グループ

セントラルグループを有効にすると、データはセントラル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EHome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

実際のニーズに応じて、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 アドレスを設定します。

ポート番号

ISUP サーバーのポート番号を設定します。

注

ポート番号の範囲：0～65535。

デバイス ID

デバイスのシリアル番号を設定します。

パスワード

V5.0 を選択した場合は、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は、ISUP アカウントのみを作成する必要があります。

注

- ISUPアカウントとISUPキーを覚えておいてください。デバイスがISUPプロトコルを介して他のプラットフォームと通信する際には、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：8～32文字。

7.2.6 プラットフォームアクセス

Hik-Connectモバイルクライアントにデバイスを追加する前に、デバイス認証コードの変更やサーバーアドレスの設定が可能です。

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「通信設定」をタップし、通信設定ページに入ります。
2. 通信設定ページで、**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**有効にする
4. **サーバーIP**を入力してください。
5. **認証コード**を作成します。**Hik-Connect経由で**デバイスを管理する際には、この認証コードの入力が必要です。

7.3 ユーザー管理

ユーザー管理インターフェースでは、ユーザーの追加、編集、削除、検索が可能です。

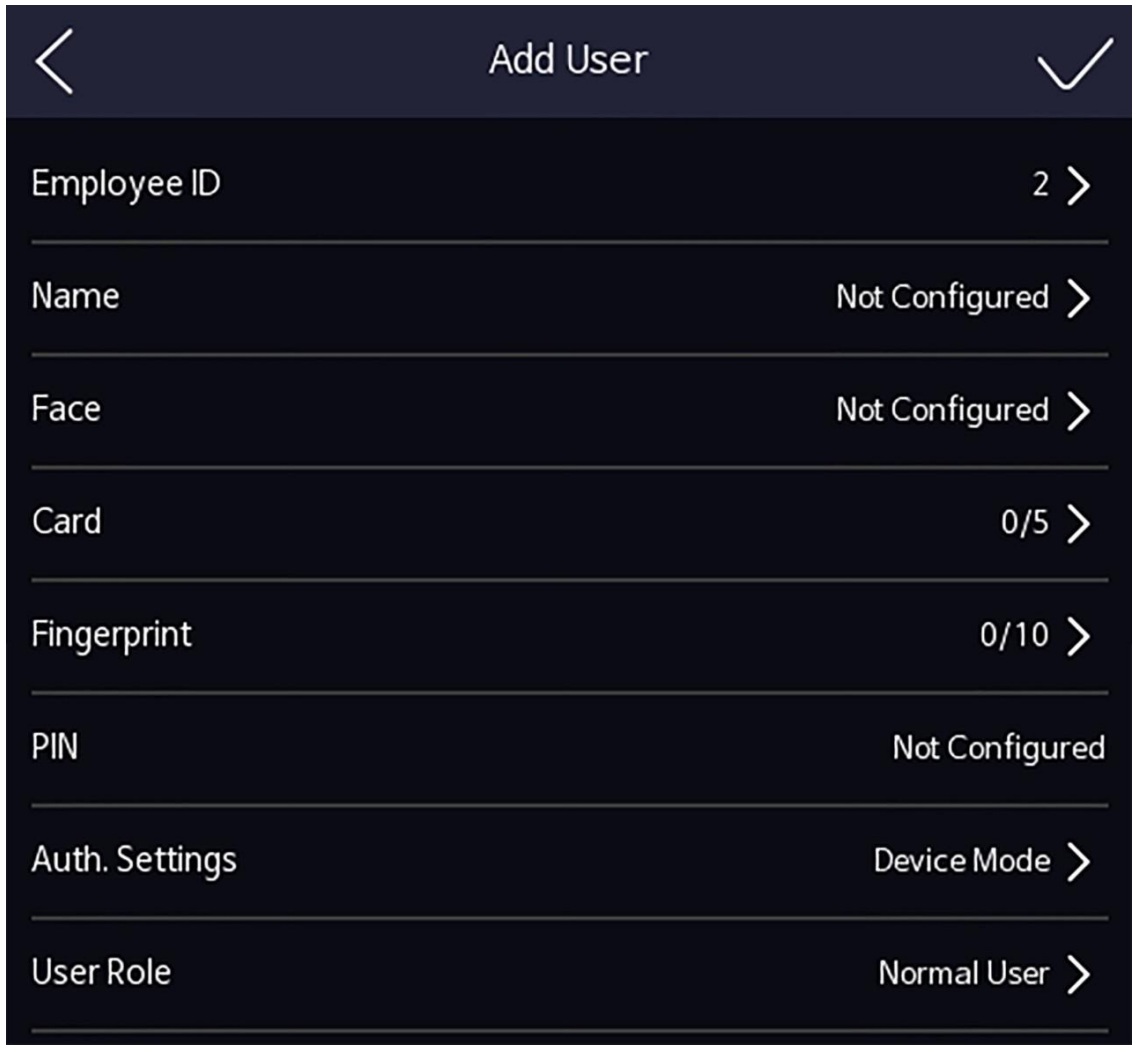
7.3.1 管理者の追加

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

手順

1. 最初のページを長押しし、バックエンドにログインしてください。

2. **ユーザー→+** をタップしてユーザー追加ページに入ります。



3. 従業員IDを編集します。

注意

- 従業員IDは32文字未満である必要があります。小文字、大文字、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ユーザー名を入力します。

注記

- ユーザー名には数字、大文字、小文字、特殊文字を使用できます。
- ユーザー名には最大32文字まで使用できます。

5. **オプション：**管理者の顔写真、指紋、カード、または PIN を追加します。

注記

- 顔写真の追加の詳細**については**、「顔写真の**追加」を**参照してください。
- **注**

  指紋の追加については、「**指紋の追加」**を参照してください。
- カード追加の詳細については、「**カードを追加する」**を参照してください。
- パスワードの追加方法の詳細については、「***PIN*コードの表示」**を参照してください。

6. **オプション：**管理者の認証タイプを設定します。

注記

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。

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

ユーザーは管理者です。通常の勤怠機能に加え、権限認証後にホームページにアクセスして操作することもできます。

8. ✓ をタップして設定を保存します。

7.3.2 顔写真を追加

ユーザーの顔写真をデバイスに登録します。ユーザーは顔写真を使用して認証できます。

手順

注意

最大1500枚の顔写真を追加できます。

1. 初期画面を3秒間長押しし、表示されるジェスチャーに従って左右にスライドし、バックエンドにログインします。

2. **ユーザー→+ を**タップしてユーザー追加ページに入ります。

3. 社員IDを編集します。

注記

- 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ユーザー名を入力します。

注意

- ユーザー名には、数字、大文字、小文字、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. 顔写真フィールドをタップして、顔写真を追加するページに入ります。

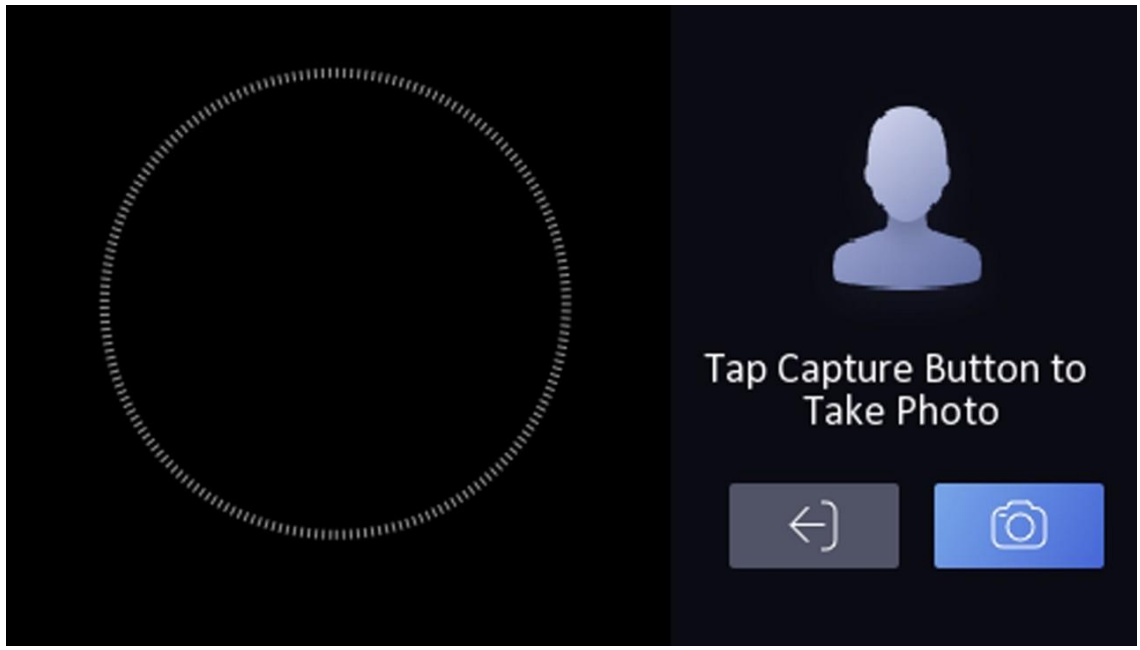


図7-9 顔写真を追加

6. カメラを見てください。

注記

- 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。
- 撮影した顔写真は、画質が良く正確であることを確認してください。
- 顔写真の追加手順の詳細については、「**顔写真の収集・比較時の注意点」を**参照してください。

顔写真を完全に追加すると、ページ右上に撮影され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：「再試行」**をタップし、顔の位置を調整して顔写真を再度追加します。

9. ユーザーロールを設定

します。

管理者

ユーザーは管理者です。通常の出席機能に加え、権限認証後にホームページにアクセスして操作することもできます。

一般ユーザー

ユーザーは通常のユーザーです。ユーザーは初期ページでのみ認証または出席確認が可能です。

10. 設定を保存するには、 をタップしてください。

7.3.3 指紋を追加

ユーザーに指紋を追加すると、追加した指紋で認証できるようになります。

手順

注意

- この機能はデバイスがサポートしている必要があります。
- 最大3000個の指紋を追加できます。

1. 最初のページを3秒間長押しし、表示されるジェスチャーに従って左右にスライドすると、デバイスのバックエンドに入ります。

2. **ユーザー→+ を**タップしてユーザー追加ページに入ります。

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。

注記

- 従業員IDは32文字未満である必要があります。小文字、大文字、数字の組み合わせで構成できます。
- 従業員IDは0で始まってはいけません。また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、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. 指紋フィールドをタップして、指紋追加ページに入ります。

6. 指示に従って指紋を追加してください。

注記

- 同じ指紋を繰り返し追加することはできません。
- 1 人のユーザーにつき、最大 10 個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リーダーを使用して指紋を記録することもできます。

指紋スキャンの手順の詳細については、「**指紋スキャンのヒント」を**参照してください。

7. ユーザーロールを設定
します。

管理者

ユーザーは管理者です。通常の勤怠機能に加え、権限認証後にホームページにアクセスして操作することもできます。

一般ユーザー

ユーザーは一般ユーザーです。ユーザーは初期ページでの認証または勤怠管理のみ可能です。

8. をタップして設定を保存します。

7.3.4 カード追加

ユーザーにカードを追加すると、ユーザーは追加されたカードで認証できます。

手順

注意

最大3000枚のカードを追加できます。

1. 初期ページを3秒間長押しし、表示されるジェスチャーに従って左右にスライドし、バックエンドにログインします。
2. **ユーザー→+ を**タップしてユーザー追加ページに入ります。
3. 配線図に従って外部カードリーダーを接続してください。
4. 従業員IDフィールドをタップし、従業員IDを編集してください。

注記

- 従業員IDは32文字未満である必要があります。小文字、大文字、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。

5. 名前フィールドをタップし、ソフトキーボードでユーザー名を入力します。

注記

- ユーザー名には数字、大文字、小文字、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。

6. カードフィールドをタップし、+をタップします。
7. カード番号を設定する
- 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. カードタイプを設定します。

9. ユーザーロールを設定します。

管理者

ユーザーは管理者です。通常の勤怠機能に加え、権限認証後にホームページにアクセスして操作することもできます。

通常ユーザー

ユーザーは通常のユーザーです。ユーザーは初期ページでの認証または出席確認のみ可能です。

10. 設定を保存するには、 をタップしてください。

7.3.5 PINコードを表示

ユーザーに PIN コードを追加すると、ユーザーは PIN コードで認証できます。

手順

1. 初期画面を3秒間長押しし、表示されるジェスチャーに従って左右にスライドし、バックエンドにログインします。

2. **ユーザー**をタップ →+ をタップしてユーザー追加ページに入ります。

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

- 従業員IDは32文字未満である必要があります。小文字、大文字、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ユーザー名を入力します。

注記

- ユーザー名には数字、大文字、小文字、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. PIN コードをタップすると、PIN コードが表示されます。

注記

PINコードは編集できません。プラットフォームによってのみ適用されます。

6. ユーザーロールを設定

します。

管理者

ユーザーは管理者です。通常の出席機能に加え、権限認証後にホームページにアクセスして操作することもできます。

一般ユーザー

ユーザーは通常のユーザーです。ユーザーは初期ページでのみ認証または出席確認が可能です。

7. 設定を保存するには、[✓] をタップしてください。

7.3.6 認証モードの設定

ユーザーの顔写真、パスワード、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。ユーザーは設定された認証モードを通じて自身の身元を認証できます。

手順

1. 初期ページを3秒間長押しし、表示されるジェスチャーに従って左右にスライドしてバックエンドにログインしてください。

2. **ユーザー**をタップ → **ユーザー追加/ユーザー編集→ 認証モード**。

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場合は、まずアクセス制御設定ページで端末認証モードを設定する必要があります。詳細は**アクセス制御パラメータの設定を**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。

7.3.7 ユーザーの検索と編集

ユーザーを追加した後、そのユーザーを検索して編集できます。

ユーザー検索

ユーザー管理ページで、検索エリアをタップしてユーザー検索ページに入ります。ページの左側にある「**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。検索には従業員ID、カード番号、またはユーザー名を入力します。「 🔍 」をタップして検索します。

ユーザーの編集

ユーザー管理ページで、ユーザーリストからユーザーを選択すると、ユーザー編集ページに移動します。**ユーザー管理**の手順に従ってユーザーパラメータを編集してください。設定を保存するには、[✓]をタップします。

注記

従業員IDは編集できません。

7.4 データ管理

データの削除、データのインポート、データのエクスポートが可能です。

7.4.1 データの削除

ユーザーデータを削除します。

ホーム画面で、**データ→データの削除→ユーザーデータを**タップします。デバイスに追加されたすべてのユーザー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→データのインポート** をタップします。
3. **ユーザーデータ**、**顔データ**、または**アクセス制御パラメータ**をタップします。

注

インポートされたアクセス制御パラメータは、デバイスの設定ファイルです。

4. データエクスポート時に作成したパスワードを入力してください。エクスポート時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、すぐに**「OK」を**タップしてください。

注意

- あるデバイス（デバイスA）から別のデバイス（デバイスB）へ全てのユーザー情報を転送したい場合は、デバイスAからUSBフラッシュドライブへ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へ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ユーザーデータをインポートしてください。
- 対応するUSBフラッシュドライブのフォーマットはFAT32です。
- インポートした画像はルートディレクトリのフォルダ（enroll_pic）に保存し、画像名は以下の規則に従うこと：カード番号_氏名_部署名_社員ID_性別.jpg
- enroll_picフォルダにすべての画像を保存できない場合、ルートディレクトリ下にenroll_pic1、enroll_pic2、enroll_pic3、enroll_pic4といった名前のフォルダを追加作成できます。
- 従業員IDは32文字未満であること。小文字、大文字、数字の組み合わせで構成され、重複せず、0で始まってはいけません。
- 顔写真の要件は以下の規則に従うこと：正面をカメラに向けて撮影すること。帽子や頭部覆いを着用しないこと。形式はJPEGまたはJPGであること。解像度は640×480ピクセル以上であること。画像サイズは60KBから200KBの間であること。

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. ホームページで、**[データ]→[データのエクスポート]**をタップします。
3. **「顔データ」**、**「イベントデータ」**、**「ユーザーデータ」**、または**「アクセス制御パラメータ」**をタップします。

注

エクスポートされたアクセス制御パラメータは、デバイスの設定ファイルです。

4. **オプション：**エクスポート用のパスワードを作成します。これらのデータを別のデバイスにインポートする際には、パスワードを入力する必要があります。

注

- サポートされているUSBフラッシュドライブのフォーマットはDBです。
- 本システムは1GBから32GBの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ユーザーデータはDBファイルであり、編集できません。

7.5 本人認証

ネットワーク設定、システムパラメータ設定、ユーザー設定の後、初期ページに戻って本人認証を行うことができます。システムは設定された認証モードに従って本人認証を行います。

7.5.1 シングルクレデンシャルによる認証

認証前にユーザー認証タイプを設定してください。詳細は「**認証モードの設定**」を参照してください。顔認証、指紋認証、またはカード認証を行います。

顔認証

カメラに向かって正面を向き、顔認証を開始してください。

指紋認証

登録済みの指紋を指紋モジュールに置き、指紋による認証を開始します。

カード

カードをカード提示エリアに提示し、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を使用できます。

PINコード

PIN コードによる認証を行うには、PIN コードを入力してください。

認証が完了すると、「認証済み」というプロンプトが表示されます。

7.5.2 複数の認証情報による認証

開始前に

認証前にユーザー認証タイプを設定してください。詳細は「**認証モードの設定**」を参照してください。

手順

1. 認証モードが「カードと顔認証」「パスワードと顔認証」「カードとパスワード」「カードと顔認証」「カードと指紋認証」の場合、ライブビュー画面の指示に従いいずれかの認証手段で認証を行ってください。

注

- カードは通常のICカード、または暗号化カードを使用できます。

2. 前の認証手段が認証された後、他の認証手段の認証を続行します。

注

- 指紋スキャンに関する詳細情報は、「**指紋スキャンのヒント」**を参照してください。
- 顔認証の詳細については、「**顔画像収集・比較時の注意事項」**を参照してください。

認証が成功した場合、「認証済み」というプロンプトが表示されます。

7.6 基本設定

ショートカットキー、テーマ、音声、時間、スリープ（秒）、ログアウトまでの待機時間（秒）、言語、コミュニティ番号、建物番号、ユニット番号を設定できます。

初期ページを3秒間長押しし、表示されるジェスチャーに従って左右にスライドしてデバイスのホームページにログインします。「**基本設定」を**タップします。

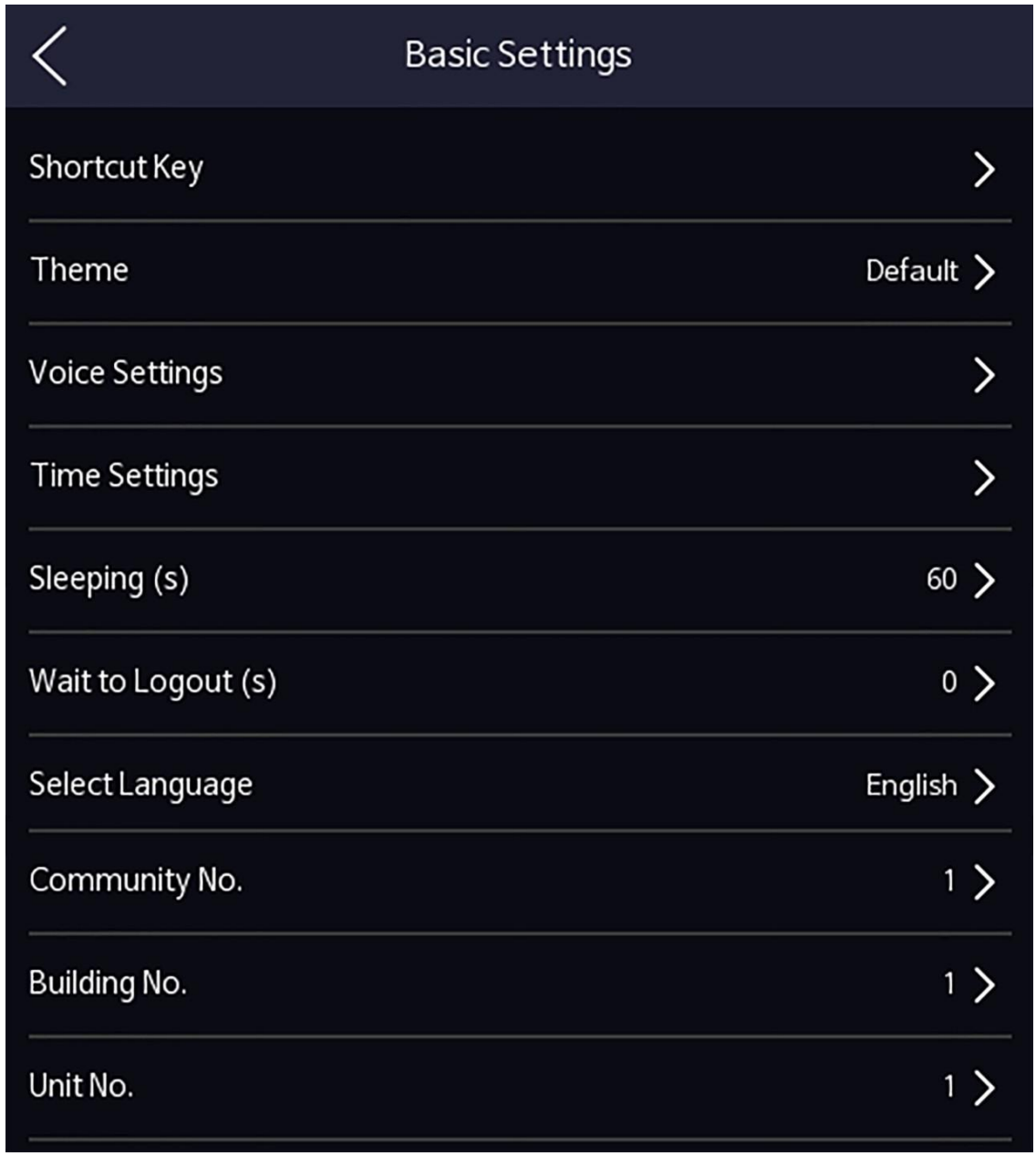


図7-10 基本設定ページ

ショートカット

キー

認証ページに表示されるショートカットキー（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む）を選択します。

注

- 顔とQRコードの組み合わせ認証がサポートされており、QRコードショートカットキーが無効になっている場合（認証ページにQRコードショートカットキーアイコンがない場合）、認証ページ中央のQRコードをスキャンして認証できます。
- 通話タイプは「**通話ルーム**」「**コールセンター**」「**指定ルーム番号への通話**」から選択できます。**通話ルーム**

  認証ページで通話ボタンをタップすると、通話する部屋番号をダイヤルする必要があります。

  コールセンター

  認証ページで呼び出しボタンをタップすると、センターに直接呼び出すことができます。

  指定部屋番号への通話

  認証ページで呼び出しボタンをタップすると、設定済みの部屋番号にダイヤルせずに直接呼び出すことができます。

テーマ

認証ページのプロンプトウィンドウのテーマを設定できます。**テーマは「デフォルト」または「シンプル」**から選択可能です。**「シンプル」**を選択すると、認証ページのライブビューが無効化され、同時に氏名、社員ID、顔写真がすべて非表示になります。

音声設定

音声プロンプト機能の有効化/無効化および音声音量の調整が可能です。

注記

音声の音量は0から10の間で設定できます。

時刻設定

タイムゾーン、デバイスの時刻、夏時間を設定します。

スリープ時間 (秒)

デバイスのスリープ待機時間（分）を設定します。初期画面でスリープ時間を30分に設定した場合、操作がない状態で30分経過するとデバイスはスリープ状態になります。

注意

スリープ時間を0に設定した場合、デバイスはスリープモードに入りません。

ログアウト待機時間 (秒)

設定時間内に操作がない場合、システムはログアウトします。

言語の選択

実際のニーズに応じて言語を選択してください。

コミュニティ番号

設置された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

デバイスが設置されている建物の番号を設定してください。

ユニット番号

設置されたデバイスのユニット番号を設定する

7.7 生体認証パラメータの設定

顔認識性能を向上させるため、顔パラメータをカスタマイズできます。設定可能なパラメータには、アプリケーションモードの選択、顔生体検知レベル、顔認識距離、顔認識間隔、顔1:Nセキュリティレベル、顔1:1セキュリティレベル、ECO設定、マスク着用顔検出が含まれます。

初期ページを3秒間長押ししてホームページにログインします。「**生体認証」を**タップします。

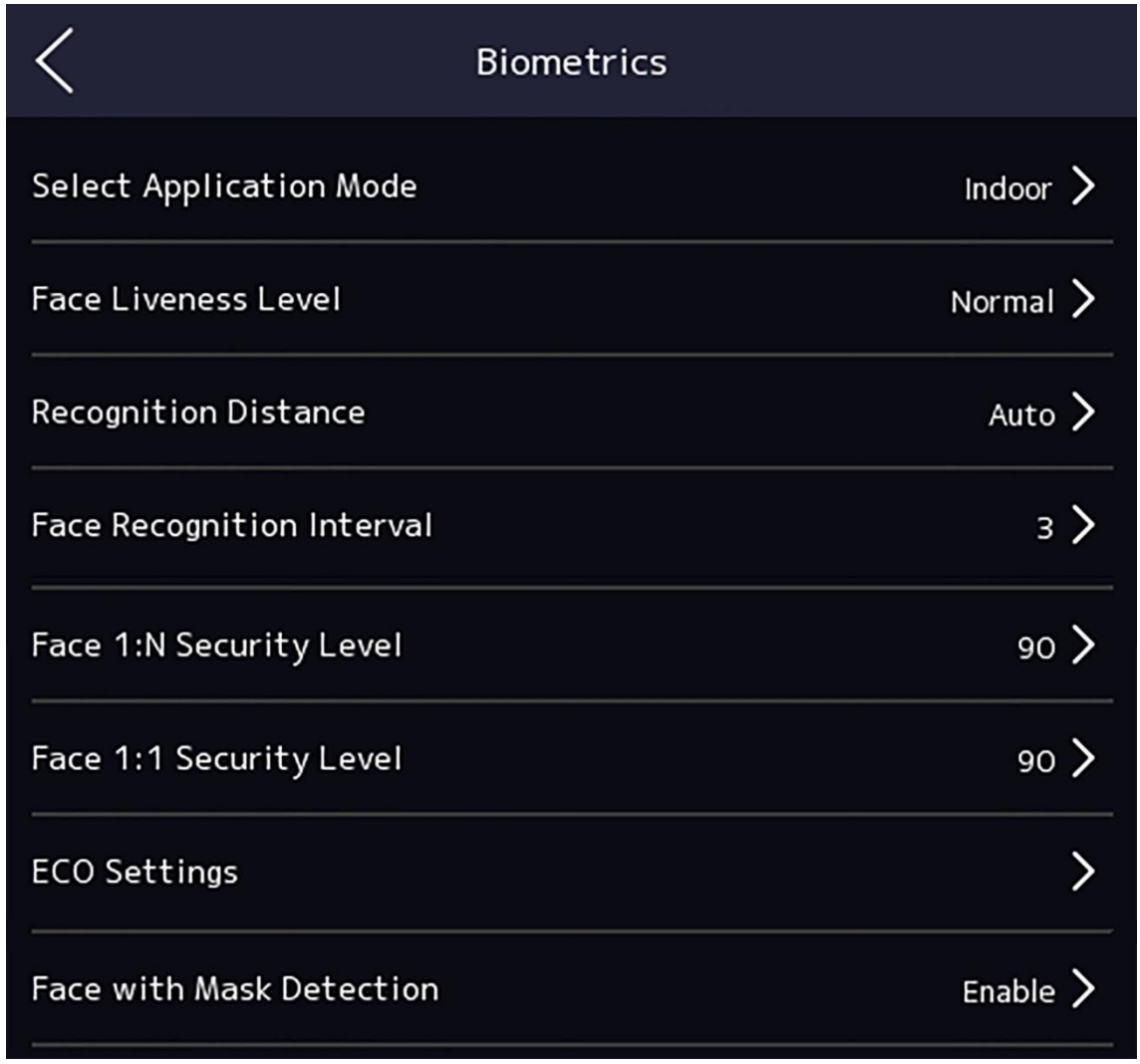


図 7-11 生体認証パラメータページ表 7-1 顔写真パラメータ

パラメータ	説明
アプリケーションモードの選択	実際の環境に応じて「その他」または「屋内」を選択してください。
顔の鮮明度レベル	顔偽装防止機能を有効にした後、生体認証時に照合のセキュリティレベルを設定できます。
顔認識距離	認証時にユーザーとカメラの有効な距離を設定します。

パラメータ	説明
顔認識間隔	認証時に連続する2回の顔認識の間隔。  1 から 10 までの数値を入力できます。
顔認証1:Nセキュリティレベル	1:N照合モードによる認証時の照合閾値を設定します。値が大きいほど誤認率は低くなりますが、誤拒否率は高くなります。
顔1:1セキュリティレベル	1対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は低くなりますが、誤拒否率は高くなります。
ECO設定	ECOモードを有効にすると、デバイスは低照度または暗所環境においてIRカメラを使用して顔認証を行います。ECOモードしきい値、ECOモード（1:N）、ECOモード（1:1）、マスク着用顔＆顔（1:1 ECO）、マスク着用顔＆顔（1:N ECO）を設定できます。 **ECOしきい値** ECOモードを有効にした場合、ECOモードのしきい値を設定できます。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。 **ECOモード（1:1）** ECOモード1:1照合モードによる認証時の照合閾値を設定します。値が大きいほど誤認率が低くなり、誤拒否率が高くなります。 **ECOモード（1:N）** ECOモード1:Nマッチングモードによる認証時の一致閾値を設定します。値が大きいほど誤認率は低くなり、誤拒否率は高くなります **マスク着用時の顔認証 & 顔認証 (1:1 ECO)** ECOモード1:1マッチングモードでマスク着用時の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（偽陽性率）は低くなり、誤拒率（偽陰性率）は高くなります。 **マスク着用顔と顔（1:N ECO）**

パラメータ	説明
	ECOモード1:Nマッチングモードでマスク着用時の顔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くなり、誤拒否率が高くなります。
マスク着用顔検出	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画像を認識します。マスク着用顔と顔1:Nレベルおよび戦略を設定できます。 **戦略** **「なし」、「着用リマインダー」、「着用必須」**の戦略を設定してください。 **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。 **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。 **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。 **マスク着用時の顔認証と顔認証（1:1）** 1:1照合モードでマスク着用時の顔認証を行う場合、照合精度値を設定します。値が大きいほど誤認率は低くなりますが、誤拒否率が高くなります。 **マスク着用時の顔認証 & 顔認証 (1:N)** 1:Nマッチングモードでマスク着用時の顔認証を行う際の照合値を設定します。値が大きいほど誤認率は低くなりますが、誤拒否率は高くなります。

7.8 アクセス制御パラメータの設定

認証モードの機能、NFCカード有効化、M1カード有効化、ドアコンタクト、開放時間（秒）、認証間隔（秒）などのアクセス制御権限を設定できます。

ホーム画面で**「ACS**（アクセス制御設定）」をタップし、アクセス制御設定ページに入ります。このページでアクセス制御パラメータを編集します。

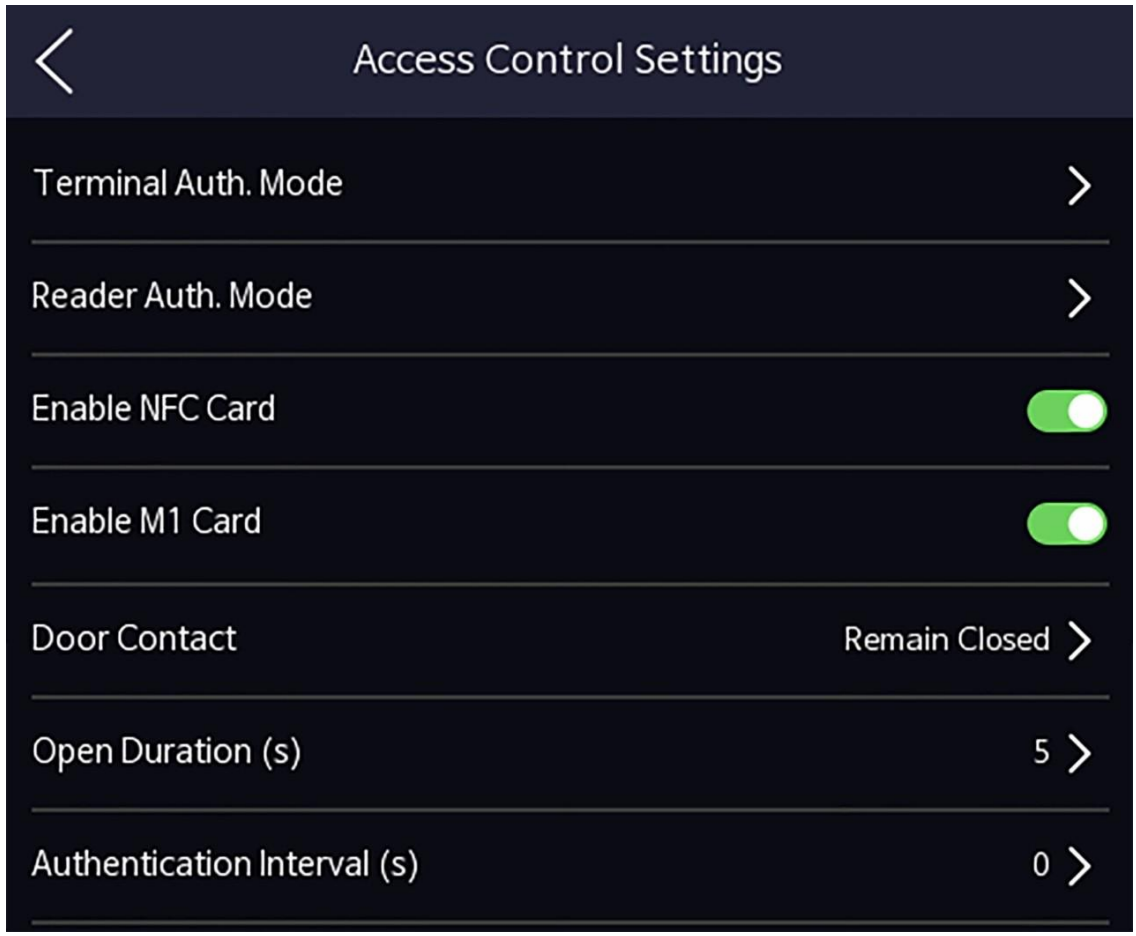


図7-12 アクセス制御パラメータ

利用可能なパラメータの説明は以下の通りです：

表 7-2 アクセス制御パラメータの説明

パラメータ	説明
端末認証モード（Terminal Authentication Mode）	顔認証端末の認証モードを選択します。認証モードをカスタマイズすることも可能です。

パラメータ	説明
	注 • 指紋モジュールを搭載したデバイスのみが指紋関連機能をサポートします。 • 生体認証製品は、偽装防止環境に対して完全には適用できません。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。 • 複数の認証モードを採用する場合、顔認証の前に他の認証方法による認証を行う必要があります。
リーダー認証モード（カードリーダー認証モード）	カードリーダーの認証モードを選択します。
NFC カード有効化	この機能を有効にすると、NFC カードを提示して認証を行うことができます。
M1 カードの有効化	機能を有効にすると、M1カードを提示して認証できます。
ドアコンタクト	実際のニーズに応じて「開く（開いたまま）」または「閉じる（閉じたまま）」を選択できます。デフォルトは「閉じる（閉じたまま）」です。
開扉時間	ドアの解錠時間を設定します。設定時間内にドアが開かない場合、ドアはロックされます。設定可能なドアロック時間範囲：1～255秒。
認証間隔	デバイスの認証間隔を設定します。設定可能な認証間隔の範囲：0～65535。

7.9 勤怠ステータス設定

実際の状況に応じて、出勤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、残業終了に設定できます。

注記

この機能は、クライアントソフトウェア上の勤怠管理機能と連携して使用する必要があります。

7.9.1 デバイス経由での出勤モード無効化

勤怠モードを無効にすると、システムは初期ページに勤怠ステータスを表示しません。

T&A Status をタップして T&A Status ページに入ります。

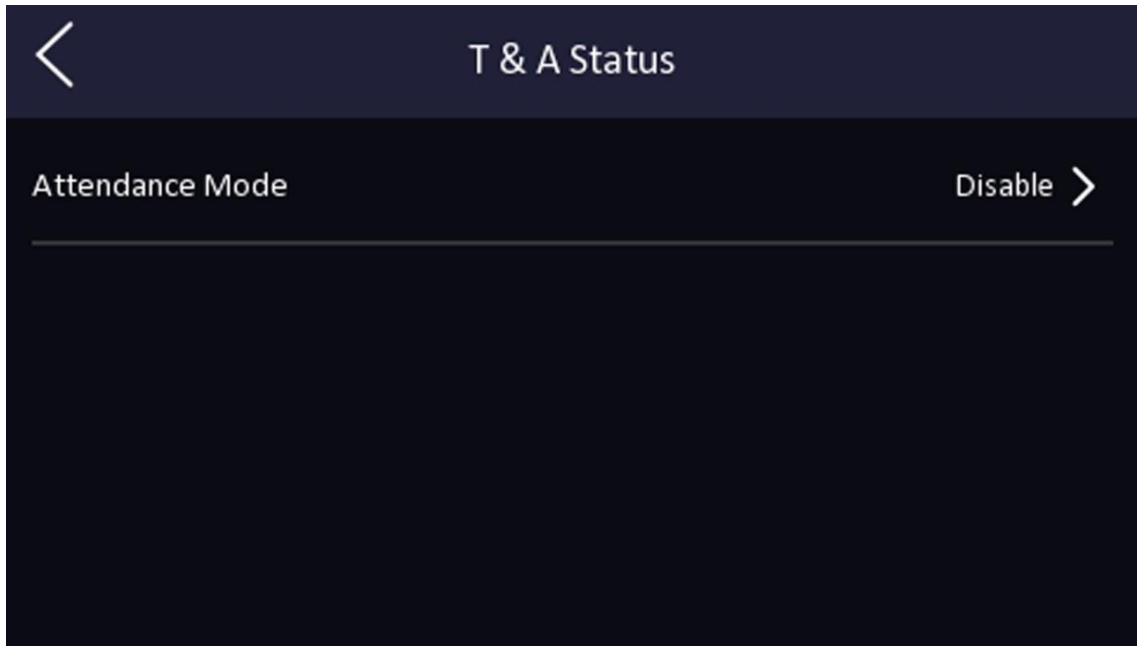


図 7-13 出退モードを無効にする

出勤モードを「**無効**」に設定します。

初期画面では出席状況を確認または設定できません。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。

7.9.2 デバイス経由での手動出席設定

出席モードを手動に設定し、出席を取る際に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人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。詳細は「**ユーザー管理**」を参照してください。

手順

1. 「**T&Aステータス**」をタップして、T&Aステータスページに入ります。
2. **出席モード**を手**動**に設定してください。

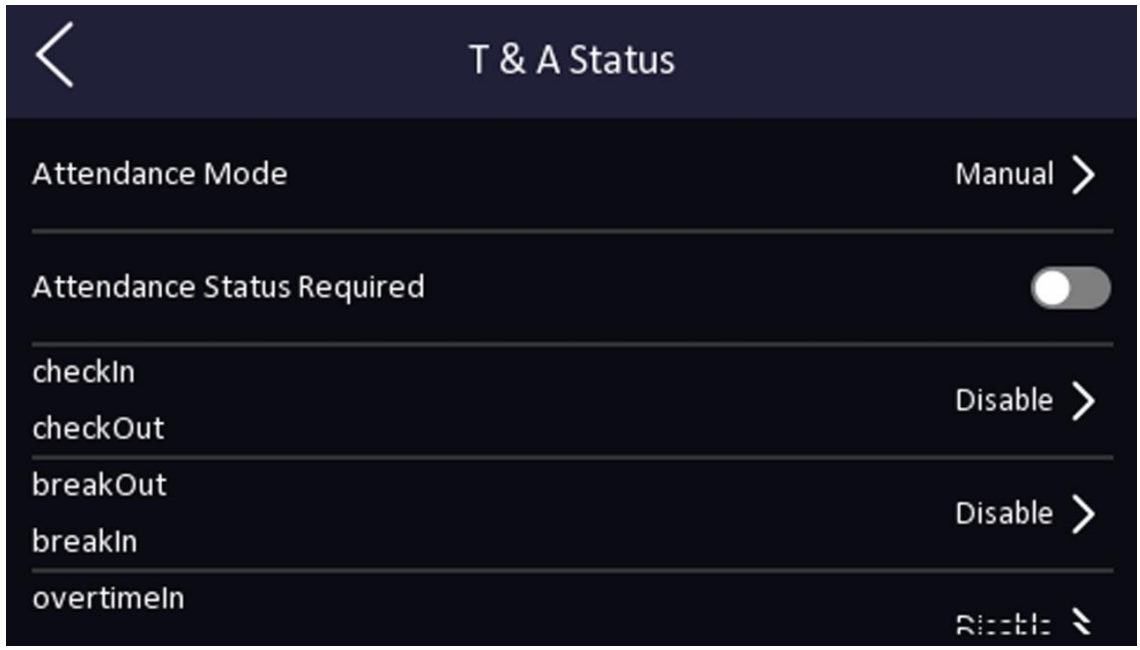


図7-14 手動出席モード

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。

注記

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。

この名前は、勤怠状況ページおよび認証結果ページに表示されます。

結果

認証後、手動で出勤ステータスを選択する必要があります。

注

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 デバイス経由での自動出席設定

出席モードを自動に設定すると、出席ステータスとその有効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人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。詳細は「**ユーザー管理**」を参照してください。

手順

1. **T&Aステータスをタップして**、T&Aステータスページに入ります。
2. **出勤モード**を**自動**に設定します。

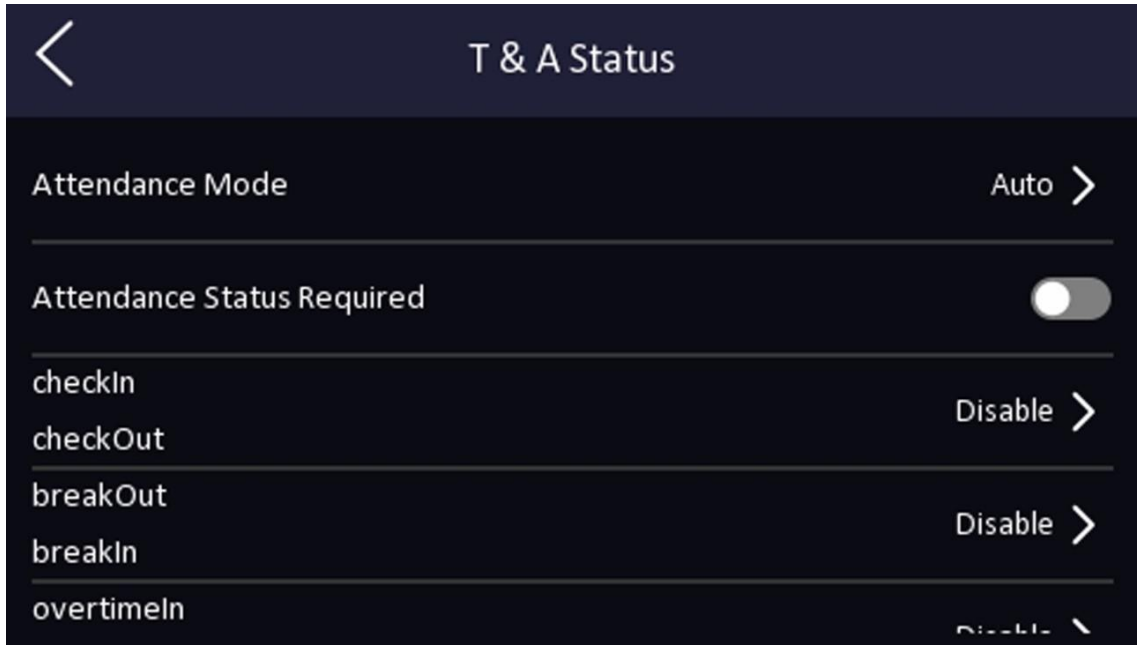


図 7-15 自動勤怠モード

3. **出勤**ステータス機能を有効にします。
4. グループ単位で勤怠ステータスを有効化します。

注記

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、その名前を変更します。

   この名前は、勤怠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) **「出勤スケジュール」**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**を選択してください。
   3) 選択した出勤ステータスの当日の開始時刻を設定します。
   4) **確認**をタップしてください。
   5) 実際の必要に応じて、手順1から4を繰り返します。

注意

設定されたスケジュール内で出席ステータスが有効になります。

結果

初期ページで認証を行うと、設定されたスケジュールに基づき、設定された出席ステータスとして認証がマークされます。

例

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

7.9.4 デバイス経由での手動・自動勤怠設定

出勤モード**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勤ステータスを自動的に変更します。同時に、認証後に手動で出勤ステータスを変更することも可能です。

開始前に

ユーザーを少なくとも1人追加し、そのユーザーの認証モードを設定してください。詳細は「**ユーザー管理」**を参照してください。

手順

1. **T&Aステータスをタップして**、T&Aステータスページに入ります。
2. **出勤モードを手動と自動**に設定します。

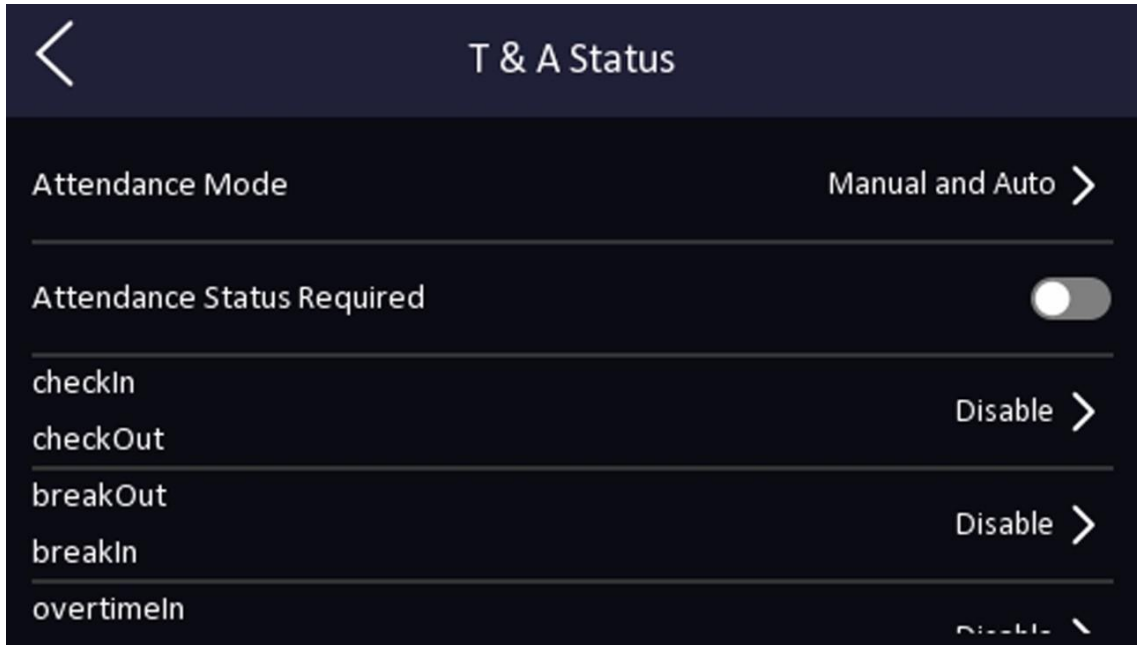


図7-16 手動モードと自動モード

3. **出勤**ステータス機能を有効にします。
4. グループ単位で勤怠ステータスを有効化します。

注記

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、その名前を変更します。

   この名前は、勤怠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**タップしてください。
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**を選択してください。
3) 選択した出勤ステータスのその日の開始時刻を設定します。
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 を繰り返します。

注記

設定されたスケジュール内で出席ステータスが有効になります。

結果

初期ページで認証を行います。スケジュールに基づき、設定された出席ステータスとして認証が記録されます。結果タブの編集アイコンをタップすると、手動で出席ステータスを選択できます。編集した出席ステータスとして認証が記録されます。

例

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

7.10 システムメンテナンス

デバイスのシステム情報と容量を確認できます。また、システムを工場出荷時設定に復元、デフォルト設定に戻す、APPアカウントのリンク解除、システムの再起動を行うこともできます。

初期ページを 3 秒間長押ししてホームページにログインします。

図 7-17 メンテナンスページ

システム情報

シリアル番号、ファームウェアバージョン、MCUバージョン、MACアドレス、製造データ、デバイスQRコード、オープンソースコードライセンスなどのデバイス情報を確認できます。

注

ページは端末モデルによって異なる場合があります。詳細は実際のページをご参照ください。

容量

管理者、ユーザー、顔写真、カード、イベントの数を表示できます。

注意

一部のデバイスモデルでは指紋登録数の表示に対応しています。詳細は実際の画面をご確認ください。

アップグレード

USBフラッシュドライブをデバイスのUSBインターフェースに接続します。**アップグレード→OK**をタップすると、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。

APPアカウントのリンク解除

プラットフォームからHik-Connectアカウントのリンクを解除します。

工場出荷時設定に復元

すべてのパラメータが工場出荷時の設定に復元されます。システムは再起動して設定を有効にします。

デフォルト設定への復元

通信設定、リモートでインポートされたユーザー情報を除くすべてのパラメータがデフォルト設定に復元されます。システムは再起動して設定を有効にします。

再起動

確認後、デバイスが再起動します。

を長押しし、管理者パスワードを入力すると、デバイスのバージョン情報を確認できます。

第8章モバイルブラウザによるデバイスの設定

8.1 ログイン

モバイルブラウザからログインできます。

注意

- モデルの一部はWi-Fi設定に対応しています。
- デバイスの電源が入っていることを確認してください。

Wi-Fiを有効にした後、デバイスからIPアドレスを取得してください。デバイスとコンピューターのIPセグメントが同じであることを確認してください。詳細は「***Wi-Fiパラメータの設定***」を参照してください。

モバイル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アクセスしてください。

デバイスのユーザー名とパスワードを入力してください。**ログイン**をクリックしてください。

8.2 イベントを検索

検索をクリックして検索ページに入ります。

検索条件（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**」をクリックします。

注記

32桁以内の名前検索に対応しています。

検索結果が一覧で表示されます。

8.3 ユーザー管理

モバイルWebブラウザからユーザーの追加、編集、削除、検索が可能です。

手順

1. **ユーザー**をタップして設定ページに入ります。

2. ユーザーを追加。

1) + をタップします。

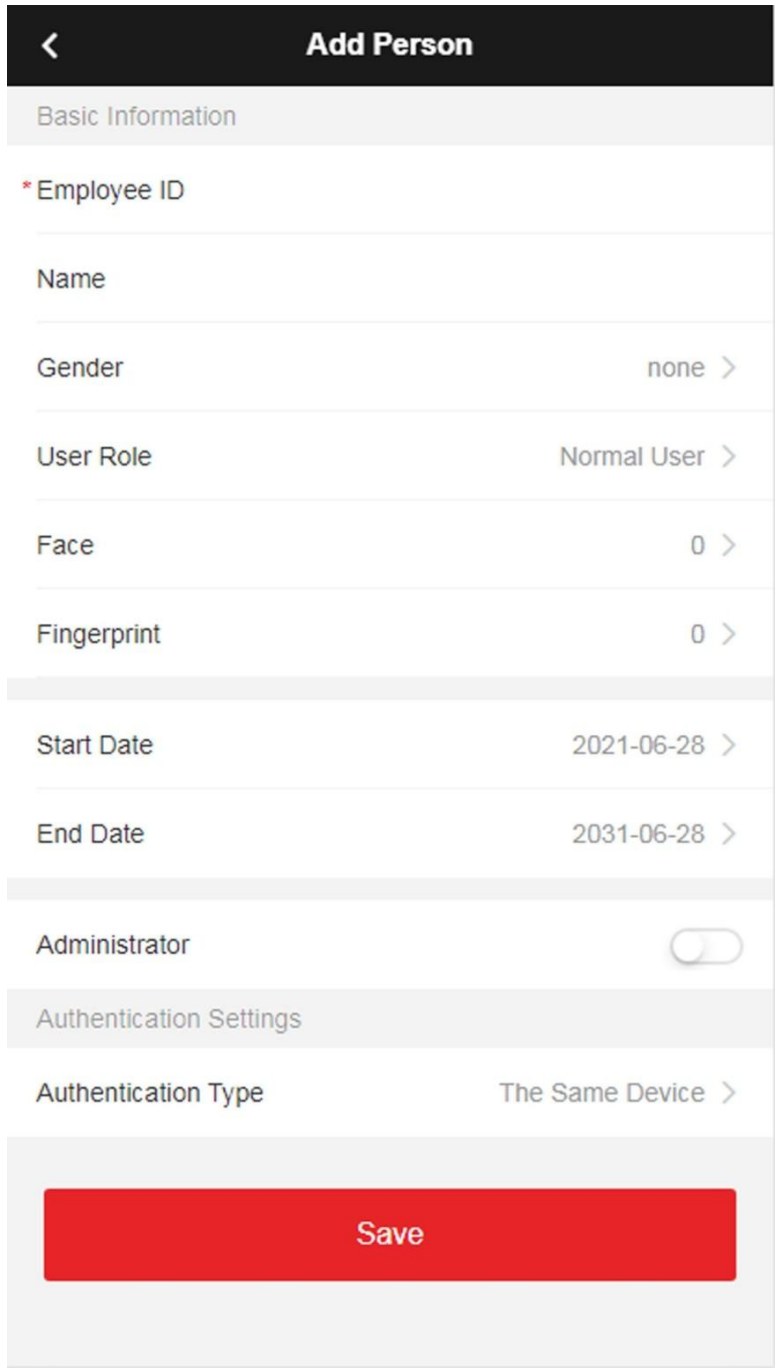


図 8-1 ユーザーの追加

2) 以下のパラメータを設定します。

従業員 ID

従業員 ID を入力します。従業員 ID は 0 または 32 文字を超えることはできません。大文字、小文字、数字の組み合わせで構成できます。

名前

名前を入力してください。名前には数字、英字の大文字•小文字、記号を使用できます。名前は32文字以内が推奨されます。

ユーザーロール

ユーザーロールを選択してください。

フロア番号/部屋番号

階数/部屋番号を入力してください。

顔

顔写真を追加します。**顔写真を**タップし、次に「**インポート」をタップして**、顔写真をインポートするモードを選択します。

指紋

指紋を追加します。「**指紋」**をタップし、**「+」**をタップして、指紋モジュールから指紋を追加します。

開始日/終了日

ユーザー権限の**開始日**と**終了日を**設定します。

管理者

ユーザーを管理者として設定する必要がある場合は、**[管理者]を**有効にできます。

認証タイプ

認証タイプを設定します。

3) **保存**をタップします。

3. 編集が必要なユーザーをユーザーリストでタップして情報を編集します。
4. ユーザーリストで削除が必要なユーザーをタップし、「 」をタップしてユーザーを削除します。
5. 検索バーに従業員IDまたは名前を入力してユーザーを検索できます。

8.4 設定

8.4.1 デバイス情報の表示

デバイス名、言語、モデル、シリアル番号、QRコード、バージョンなどを表示します。

設定→システム→システム設定→基本情報 をタップして設定ページに入ります。

デバイス名、言語、モデル、シリアル番号、QRコード、バージョンなどを確認できます。

8.4.2 時刻設定

タイムゾーン、時刻同期モード、表示時刻を設定します。

設定→システム→システム設定→時刻設定 をタップして設定ページに入ります。

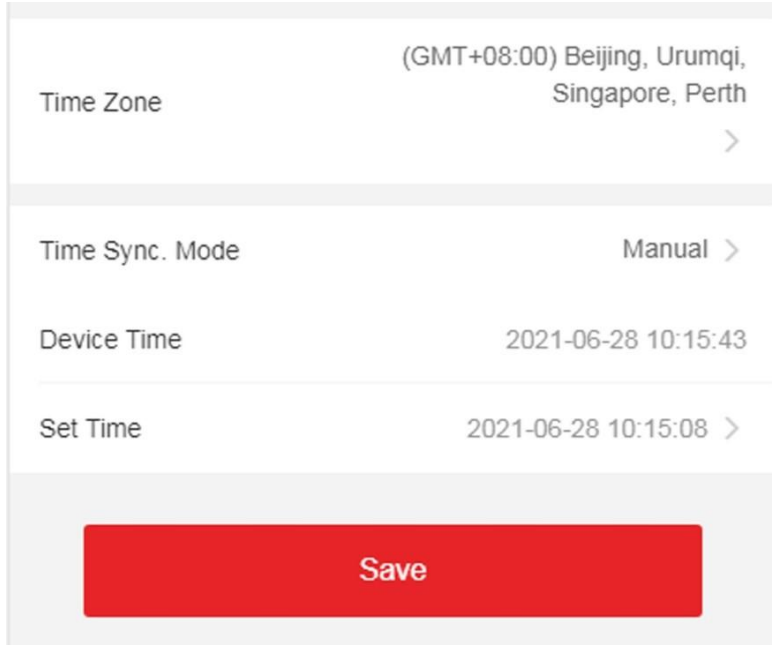


図 8-2 時刻設定

設定を保存するには、**保存**をタップします。

タイムゾーン

ドロップダウンリストから、デバイスが設置されているタイムゾーンを選択してください。

時刻同期モード手動

デフォルトでは、デバイスの時刻は手動で同期する必要があります。デバイスの時刻を手動で設定できます。

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ます。

8.4.3 オープンソースソフトウェアライセンスを表示

設定→システム→システム設定→バージョン情報 をタップし、**ライセンスを表示** をタップすると、デバイスのライセンスを確認できます。

8.4.4 ネットワーク設定

ポートとWi-Fiのパラメータを設定できます。

ポートパラメータの設定

ネットワーク経由でデバイスにアクセスする際、実際のニーズに応じてHTTP、RTSP、HTTPS、サーバーを設定できます。

設定→ネットワーク→基本設定→ポート をタップして設定ページに入ります。

HTTP

ブラウザがデバイスにアクセスする際に使用するポートを指します。例えば、HTTPポートを81に変更した場合、ブラウザでログインするにはhttp://192.0.0.65:81を入力する必要があります。

RTSP

リアルタイムストリーミングプロトコルのポートを指します。

HTTPS

ブラウザへのアクセスにHTTPSを設定してください。アクセス時には証明書が必要です。

サーバー

クライアントがデバイスを追加する際に使用するポートを指します。

Wi-Fiパラメータの設定

デバイスの無線接続用Wi-Fiパラメータを設定します。

手順

注

この機能はデバイスがサポートしている必要があります。

1. **設定→ネットワーク→基本設定→Wi-Fi** をタップして設定ページに入ります。
2. **Wi-Fiを有効にする**にチェックを入れます。

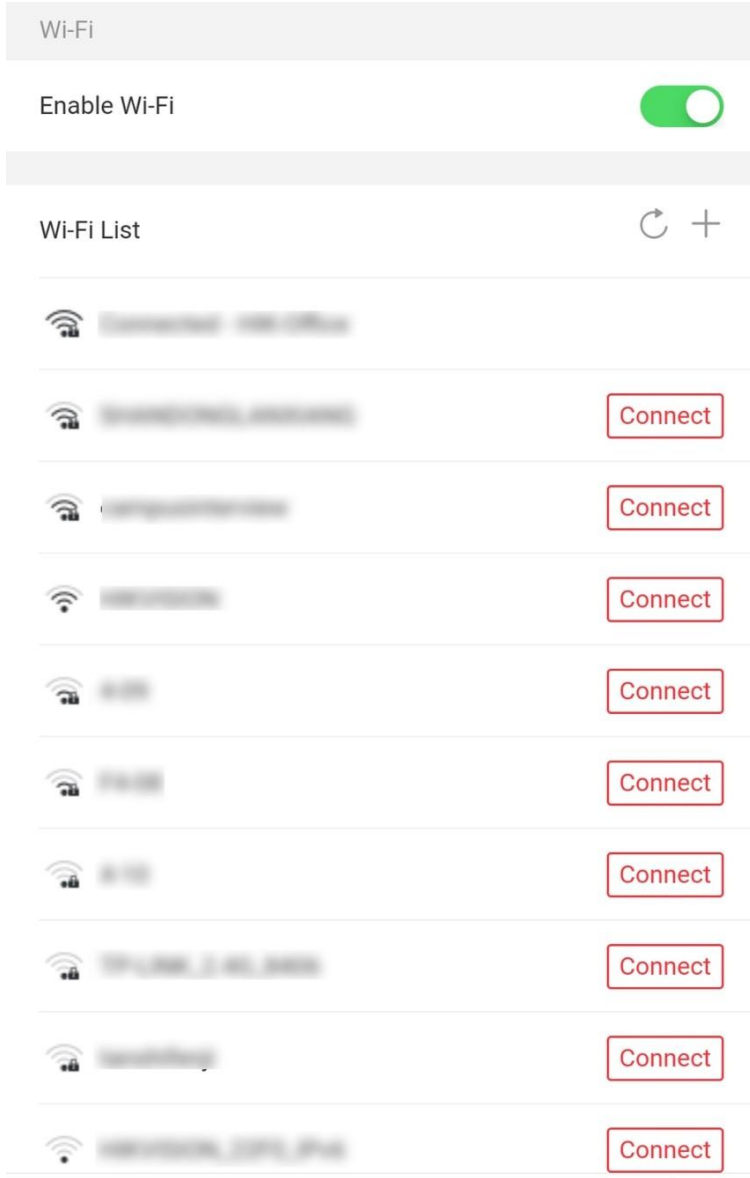


図 8-3 Wi-Fi

3. Wi-Fi を追加します。

1)「**+**」をタップします。

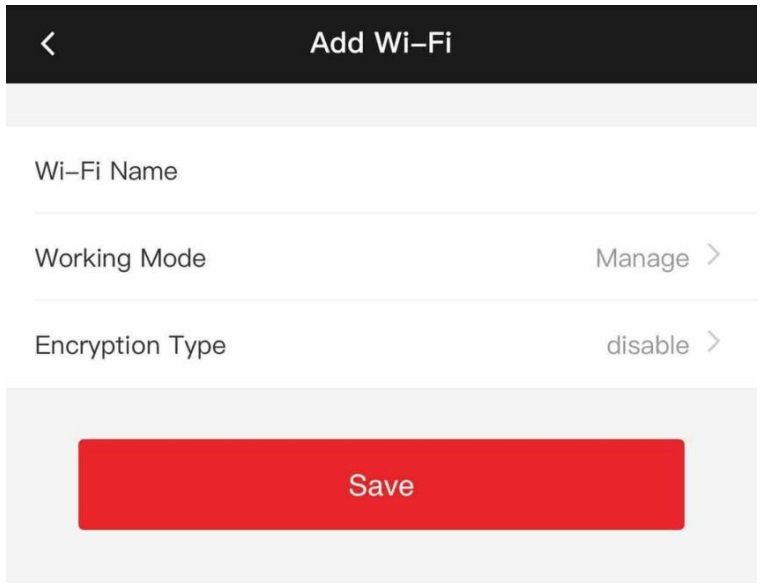


図8-4 Wi-Fiの追加

2) **Wi-Fi** 名と **Wi-Fi パスワード**を入力し、**動作モード**と**暗号化方式**を選択します。
3) **保存**をタップします。

4. Wi-Fi 名を選択し、「**接続**」をタップします。

5. パスワードを入力し、「**保存**」をタップします。

6. WLAN パラメータを設定します。
1) IP アドレス、サブネットマスク、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、ゲートウェイを自動的に割り当てます。
2) **保存**をタップします。

8.4.5 一般設定

認証パラメータの設定

認証パラメータを設定します。

手順

1. **設定→一般設定→認証設定** をタップします。

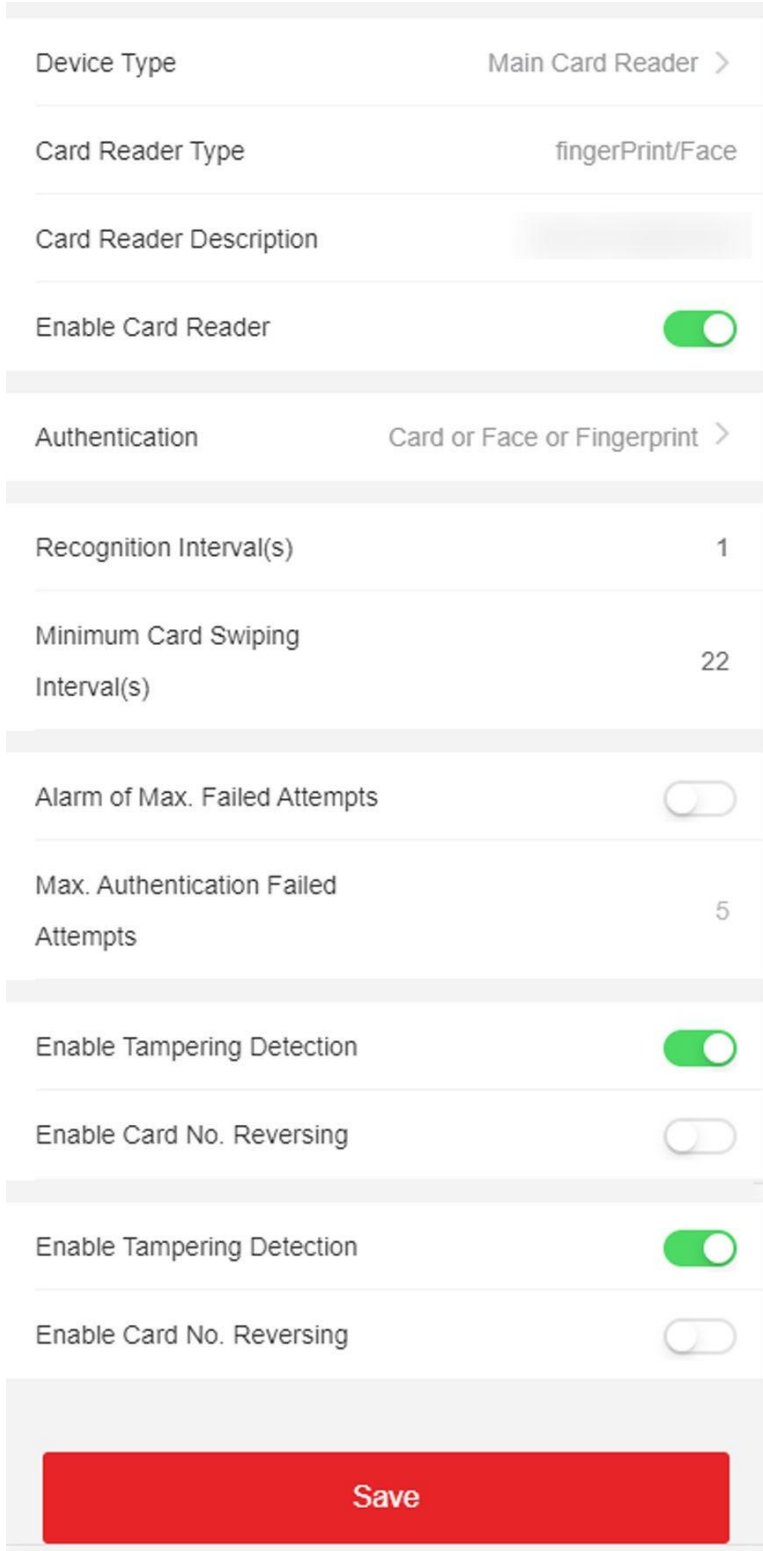


図8-5 認証設定

2. **保存**をタップします。

デバイスタイプ

メインカードリーダー

デバイスのカードリーダーのパラメータを設定できます。 メインカードリーダーを選択した場合は、次のパラメータを設定する必要があります：**カードリーダータイプ、カードリーダーの説明、カードリーダーの有効化、認証、認識間隔（秒）、最小カードスワイプ間隔（秒）、最大認証失敗回数アラーム/最大失敗回数アラーム、改ざん検出の有効化、カード番号反転の有効化**。

サブカードリーダー

接続された周辺機器カードリーダーのパラメータを設定できます。 サブカードリーダーを選択した場合、以下のパラメータを設定する必要があります：**カードリーダータイプ、カードリーダーの説明、カードリーダーの有効化、認証、認識間隔（秒）、最大認証失敗試行回数アラーム/最大失敗試行回数アラーム、改ざん検出の有効化、コントローラーとの通信間隔（秒）、パスワード入力時の最大間隔（秒）**。

カードリーダータイプ

カードリーダーのタイプを取得します。

カードリーダーの説明

カードリーダーの説明を取得します。読み取り専用です。

カードリーダーを有効化

カードリーダーの機能を有効にします。

認証

実際のニーズに応じて、ドロップダウンリストから認証モードを選択してください。

認識間隔

同一カードの提示間隔が設定値未満の場合、カード提示は無効となります。間隔時間の範囲は0～255秒です（0に設定した場合、認識間隔は無効となり、同一認証を無制限に使用できます）。

認証間隔

認証時に同一人物の認証間隔を設定できます。設定された間隔内で同一人物は1回のみ認証可能です。2回目の認証は失敗します。

最大認証失敗回数アラーム/最大失敗回数アラーム

設定値に達した際に警報を通知する機能を有効化します。

改ざん検知を有効にする

カードリーダーの改ざん検知を有効にします。

カード番号反転を有効にする

機能有効化後、読み取りカード番号は逆順で表示されます。

コントローラとの通信毎秒

アクセス制御装置が設定時間以上カードリーダーと接続できない場合、カードリーダーは自動的にオフラインになります。

パスワード入力時の最大間隔 (秒)

カードリーダーでパスワードを入力する場合、2桁の数字を押す間隔が設定値より長いと、前に押した数字は自動的にクリアされます。

プライバシーパラメータの設定

イベントの保存タイプ、画像アップロードと保存のパラメータ、および画像消去のパラメータを設定します。

設定→一般設定→プライバシー をタップします。

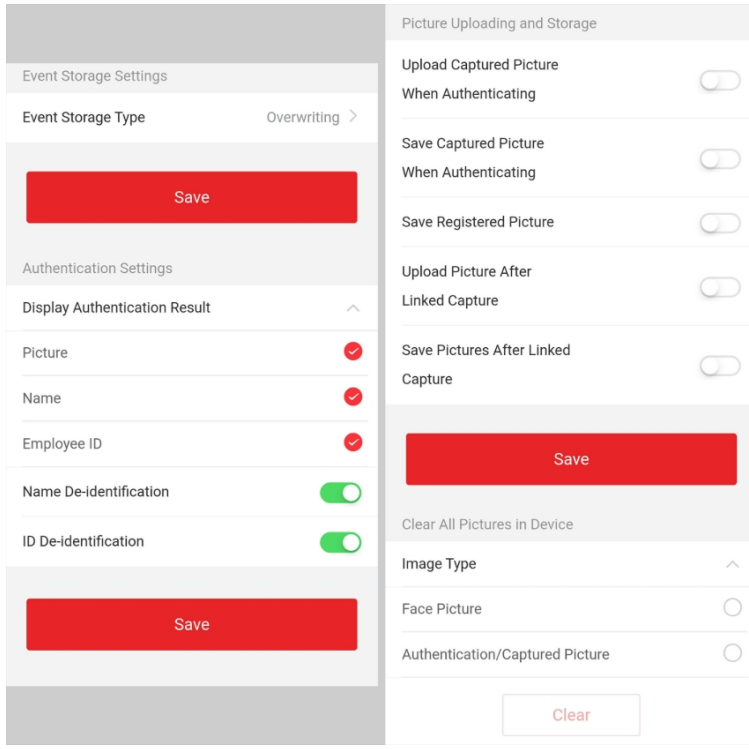


図 8-6 プライバシー設定

イベント保存設定

イベントを削除する方法を選択します。**古いイベントを定期的に削除、指定した時間で古いイベントを削除、上書きから**選択できます。

古いイベントを定期的に削除

イベント削除の期間を設定する数値を入力します。設定された期間に基づき、すべてのイベントが削除されます。

指定した時刻で古いイベントを削除

指定した時刻を設定すると、設定時刻にすべてのイベントが削除されます。

上書き

保存されたイベントが全容量の95%を超えたとシステムが検知した場合、最も古い5%のイベントが削除されます。

認証設定

認証結果の表示

顔写真、氏名、社員IDを確認します。認証が完了すると、システムは結果に選択した内容を表示します。

名前の匿名化

名前情報はアスタリスクで非表示化されます。

IDの匿名化

ID情報はアスタリスクで非表示化されています。

画像のアップロードと保存

画像をアップロードして保存できます。

認証時に撮影した画像をアップロード

プラットフォーム認証時に撮影された画像を自動的にアップロードします。

認証時の撮影画像保存

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。

登録済み画像の保存

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。

リンクされ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自動的にプラットフォームにアップロードします。

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。

デバイス内の全画像を消去

登録済みの顔写真とデバイス内の撮影済み写真を消去できます。

登録済み顔写真を消去

顔写真を選択し、「**削除**」をタップします。デバイス内の登録済み写真がすべて削除されます。

認証/撮影済み画像を消去

認証/撮影済み画像を選択し、**クリア**をタップしてください。端末内のすべての認証/撮影済み画像が削除されます。

カードセキュリティの設定

設定→一般設定→カードセキュリティをタップして設定ページに入ります。

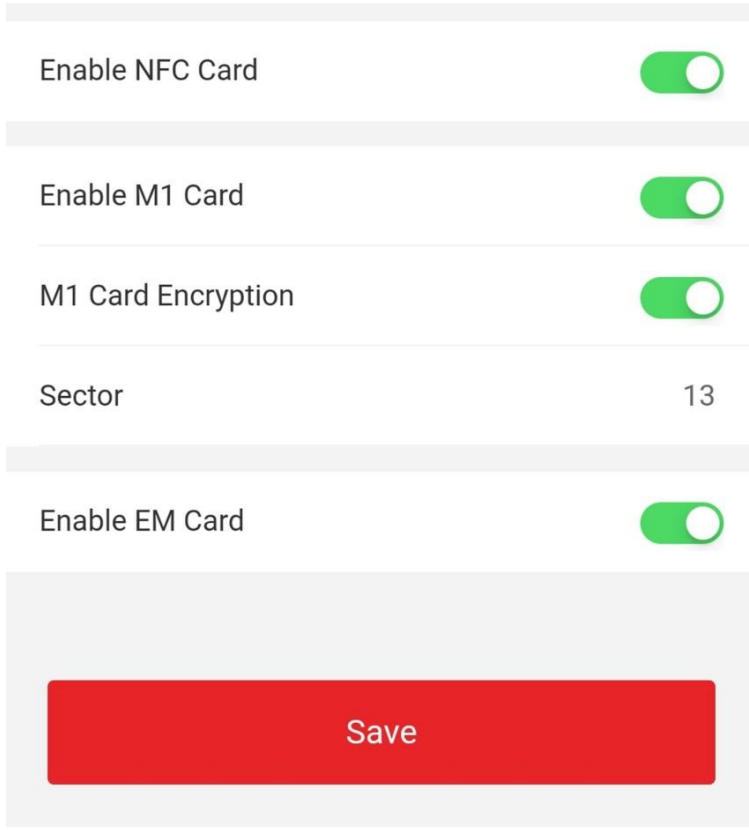


図8-7 カードセキュリティ

パラメータを設定し、「**保存**」をクリックします。

NFC カードを有効にする

携帯電話がアクセス制御のデータを取得するのを防ぐため、NFC カードを有効にしてデータのセキュリティレベルを高めることができます。

M1カードの有効化

M1カードを有効にすると、M1カードを提示して認証を行うことが可能になります。

M1カード暗号化

M1カードの暗号化は、認証のセキュリティレベルを向上させることができます。

セクター

機能を有効化し、暗号化セクターを設定します。デフォルトではセクター13が暗号化されます。セクター13の暗号化を推奨します。

EMカード有効化

EMカードを有効化し、EMカードの提示による認証が可能になります。

注記

周辺機器カードリーダーがEMカードの提示をサポートしている場合、EMカード機能の有効化/無効化機能もサポートされます。

CPUカードの有効化

CPUカード機能を有効にすると、デバイスはCPUカードからデータを読み取ることができます。

CPUカード読み取り内容

CPUカード内容読み取り機能を有効にした後、本装置はCPUカードの内容を読み取ることができます。

IDカードの有効化

ID カードを有効にし、ID カードを提示して認証を行うことができます。

カード認証パラメータの設定

デバイス上でカードによる認証を行う際のカード読み取り内容を設定します。**設定→一般設定**

→カード認証設定をタップします。

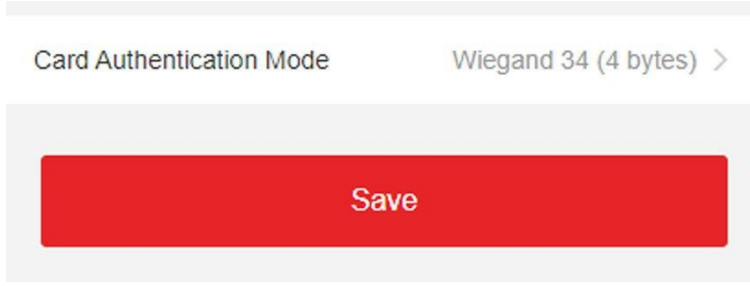


図 8-8 カード認証ページ

カード認証モードを選択し、「**保存**」をタップしてください。

すべてのカード番号が読み取られます。

Wiegand 26 (3 バイト)

デバイスはウィーガンド26プロトコルでカードを読み取ります（3バイト読み取り）。

Wiegand 34 (4 バイト)

デバイスはウィーガンド34プロトコルでカードを読み取ります（4バイト読み取り）。

8.4.6 顔パラメータ設定

顔パラメータを設定します。

顔パラメータ設定

設定→スマート→インテリジェントパラメータ をタップします。

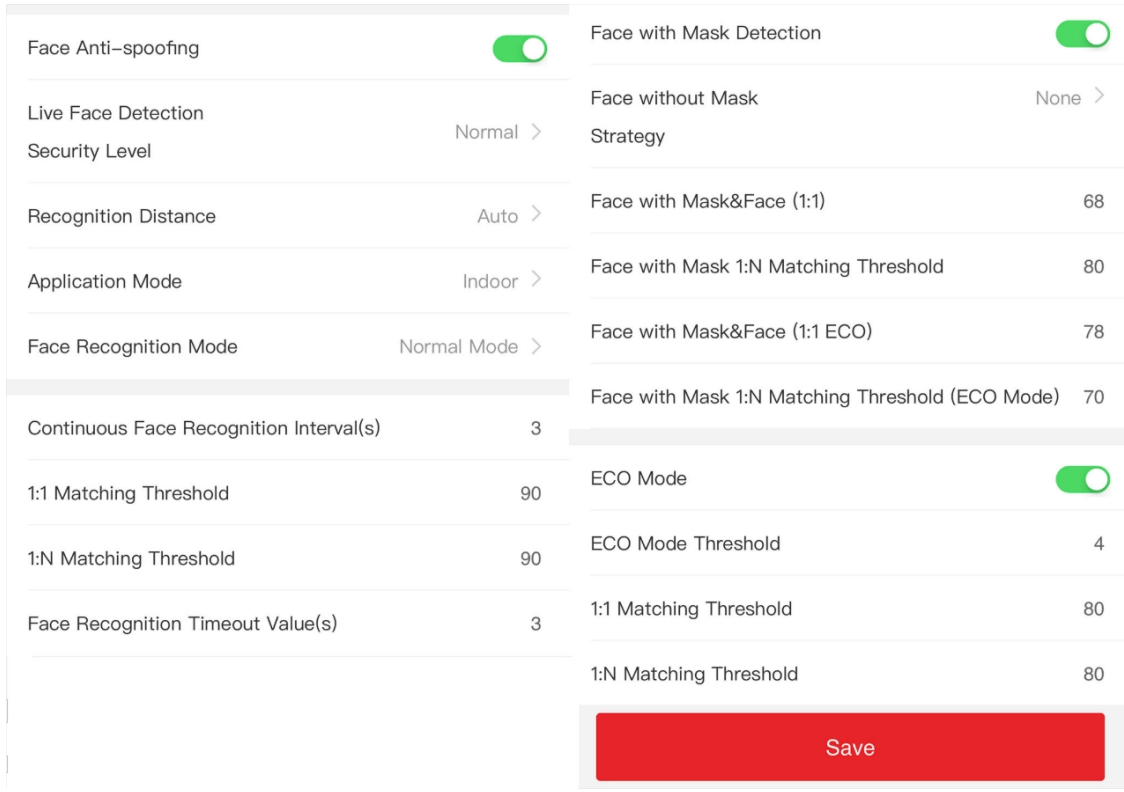


図 8-9 顔パラメータ

注意

機能は機種によって異なります。詳細は実際のデバイスをご確認ください。

顔認証パラメータの設定

顔認証偽装防止

生体顔検出機能を有効または無効にします。機能を有効にすると、デバイスは人物が生体かどうかを認識できます。

生体顔検出セキュリティレベル

顔偽装防止機能を有効にした後、生体顔認証を行う際の照合セキュリティレベルを設定できます。

認識距離

認証ユーザーとデバイスカメラ間の距離を選択します。

アプリケーションモード

実際の環境に応じて「**屋内**」または「**その他**」を選択してください。屋外シーン、窓際の屋内シーン、または環境が悪い場合は「**その他**」を選択できます。

注意

他のツールでデバイスが起動されていない場合、デフォルトで室内環境モードが使用されます。

顔認識モード通常モード

デバイスはカメラを使用して顔認識を行います。

ディープモード

より複雑な環境に適用でき、認識される人物の範囲が広くなります。

注

- 両モードは互いに互換性がありません。モード選択後は変更しないでください。モードを変更すると、以前のモードで登録された顔写真はすべて消去されます。
- ディープモードでは、端末または登録ステーションのユーザー追加機能を通じてのみ顔写真を追加できます。写真インポートによる顔写真の追加はサポートされていません。

本装置はカメラを使用して顔認識を行います。

連続顔認証間隔（秒）

認証時に連続する2回の顔認証の間隔を設定します。

注

値の範囲：1～10。

1:1 マッチングのしきい値

1対1マッチングモードによる認証時のマッチング閾値を設定します。値が大きいほど誤認率は低くなりますが、誤拒否率は高くなります。

1:N マッチングしきい値

1:Nマッチングモードによる認証時のマッチング閾値を設定します。値が大きいほど誤認率は低くなりますが、誤拒否率は高くなります。最大値は100です。

顔認識タイムアウト値 (秒)

顔認識のタイムアウト期間を設定します。顔認識時間が設定値を超えると、デバイスは顔認識タイムアウトを通知します。

マスク着用顔検出

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画像を認識します。マスク着用顔の1対N照合閾値、ECOモード、および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、ドアは開きます。

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。

マスク着用時の顔と顔（1:1）

マスク着用時の顔認証において、1対1照合モードでの一致判定閾値を設定します。値が大きいほど誤認率は低くなりますが、誤拒否率は高くなります。

マスク着用時の顔認証 1:N マッチング閾値

マスク着用時の顔認証において、1:N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は低くなりますが、誤拒否率は高くなります。

マスク着用顔と顔（1:1 ECO）

ECOモード1:1マッチングモードでマスク着用時の顔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は低くなり、誤拒否率は高くなります。

マスク着用時の顔 1:N マッチングしきい値（ECO モード）

ECOモードの1:Nマッチングモードでマスク着用時の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は低くなりますが、誤拒否率は高くなります。

ECOモード

ECOモードを有効にすると、デバイスは低照度または暗所環境においてIRカメラを使用して顔認証を行います。ECOモードしきい値、ECOモード（1:1マッチングしきい値）、ECOモード（1:Nマッチングしきい値）を設定できます。

ECOモードしきい値

ECOモード1:1マッチングモードおよびECOモード1:Nマッチングモードによる認証時のマッチングしきい値を設定します。

1:1照合しきい値

ECOモード1:1照合モードによる認証時の照合閾値を設定します。値が大きいほど誤認率は低くなりますが、誤拒否率は高くなります。

1:N マッチングしきい値

ECOモード1:Nマッチングモードによる認証時の一致閾値を設定します。値が大きいほど誤認率は低くなりますが、誤拒否率は高くなります。最大値は100です。

認識エリアの設定

設定→スマート→エリア設定をタップしてページに入ります。
ライブ映像内の青い枠をドラッグして認識領域を調整します。領域内の顔のみがシステムによって認識されます。
スライダーをドラッグして顔認識の有効領域を設定します。**保存**をタップして設定を
保存します。

8.4.7 ビデオインターホン設定

デバイスIDの設定

本装置はドアステーション、外部ドアステーション、またはアクセス制御装置として使用できます。使用前にデバイスIDを設定してください。

デバイスID設定

設定→インターコム→デバイスID設定 をタップします。
デバイスタイプを「**ドアステーション**」または「**アクセス制御デバイス**」に設定した場合、階番号とドアステーション番号を設定できます。
設定後、**保存**をタップして設定を保存します。

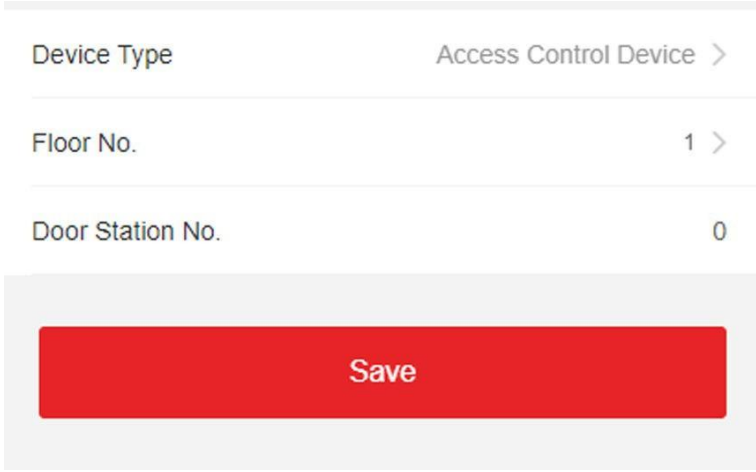


図 8-10 デバイス ID 設定 (ドアステーション)

デバイスタイプ

このデバイスは、ドアステーション、外部ドアステーション、またはアクセス制御デバイス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、デバイスを再起動してください。

階数

設置階を設定してください。

ドアステーション番号

設置されたデバイスの階数を設定

注記

番号を変更した場合は、デバイスを再起動してください。

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を設定できます。

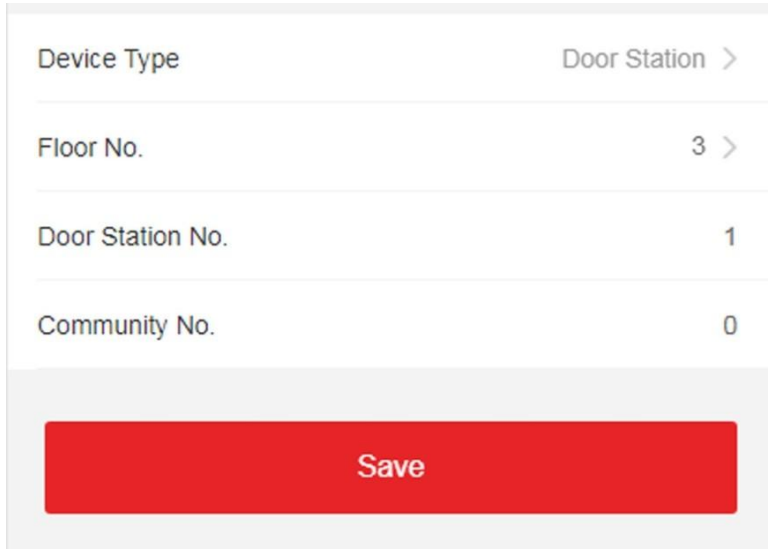


図8-11 デバイスID設定 (外部ドアステーション)

外部ドアステーション番号

デバイスタイプとして外部ドアステーションを選択した場合、**1** から 99 の間の番号を入力してください。
99 の間の番号を入力してください。

注記

番号を変更した場合は、デバイスを再起動してください。

SIP パラメータの設定

デバイスのIPアドレスとSIPサーバーのIPアドレスを設定します。パラメータ設定後、アクセス制御デバイス、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、プラットフォーム間で通信が可能になります。

注意

アクセス制御装置とその他のデバイスまたはシステム（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）が同一のIPセグメントにある場合のみ、双方向音声通信が可能です。

設定→インターコム→リンクネットワーク設定をタップします。

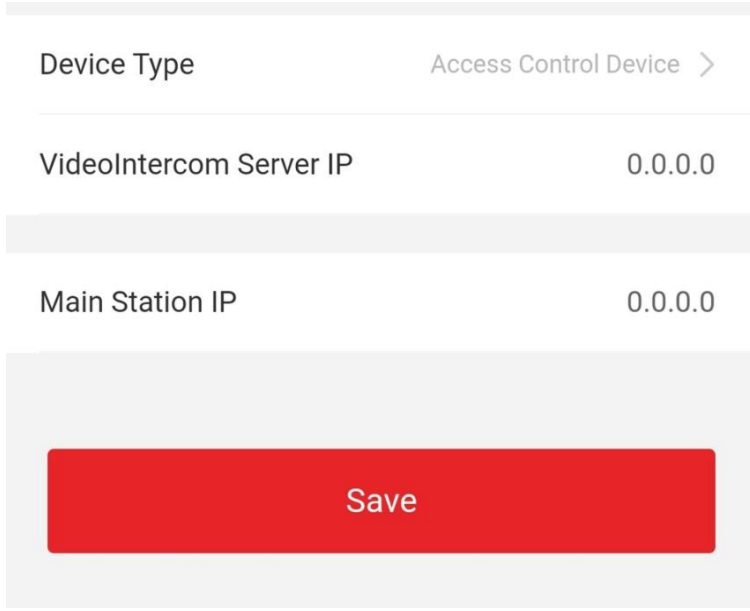


図 8-12 リンクネットワーク設定

ビデオインターホンサーバーの IP アドレスとメインステーションの IP アドレスを設定します。**保存** をタップします。

ボタンを押して呼び出す

手順

1. **設定→インターコム→ボタンを押して呼び出しを**タップして設定ページに入ります。
2. 呼び出しボタンを設定します。
   - **室内機呼び出し**にチェックを入れ、室内機番号を設定すると、ボタンで室内機を呼び出せます。
   - **管理センター呼び出し**にチェックを入れ、ボタンを管理センター呼び出しに設定します。

8.4.8 アクセス制御設定

ドアパラメータの設定

設定→アクセス制御→ドアパラメータ をタップします。

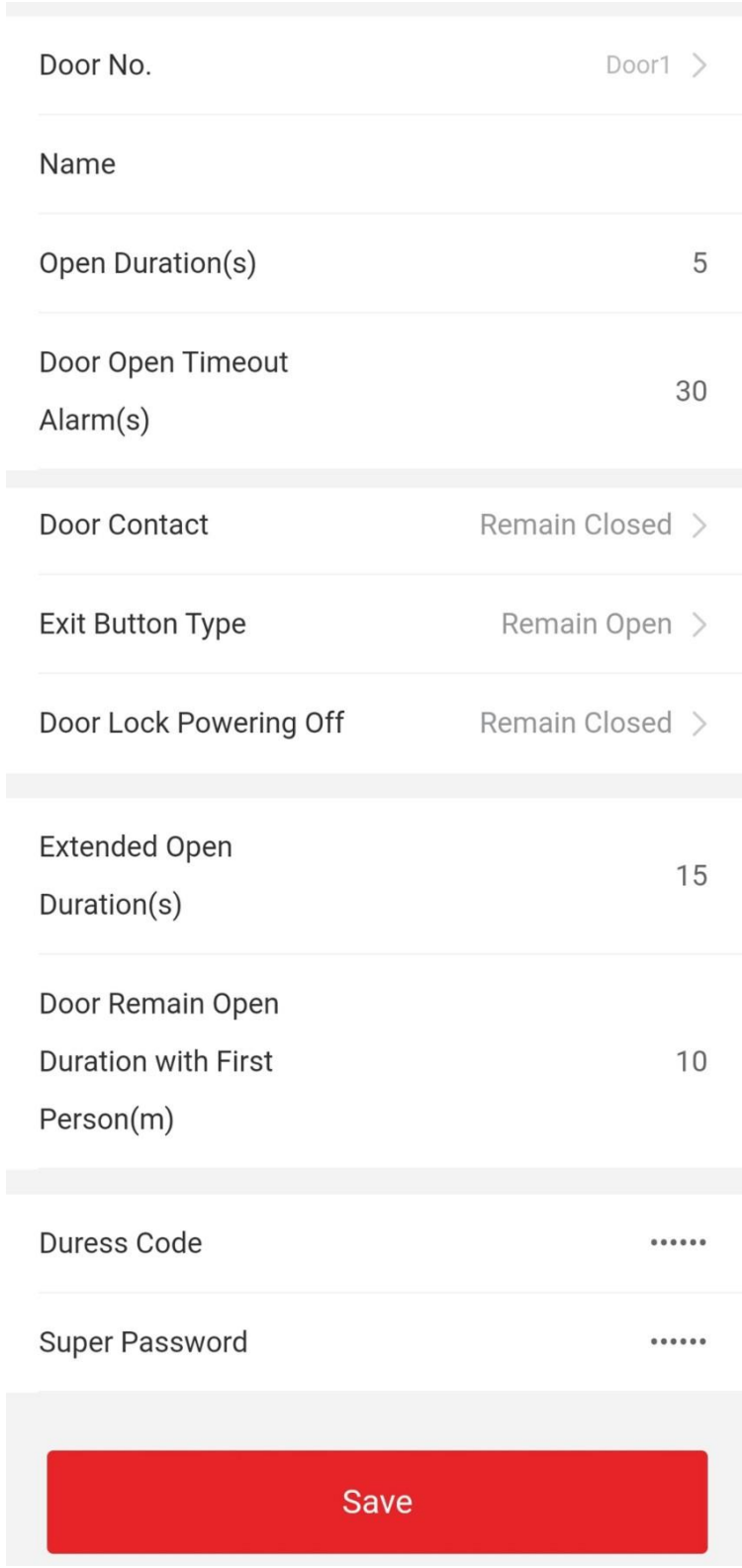


図 8-13 ドアパラメータ設定ページ

設定後、**保存**をクリックして設定を保存してください。

ドア番号

対応するドア番号のデバイスを選択してください。

名称

ドアの名前を作成できます。

開錠時間

ドアのロック解除時間を設定します。設定時間内にドアが開かない場合、ドアはロックされます。

ドア開放タイムアウトアラーム

設定時間内にドアが閉じられなかった場合、アラームが作動します。

ドアコンタクト

ドアコンタクトは、実際のニーズに応じて「**開いたまま**」または「**閉じたまま**」に設定できます。デフォルトでは「**閉じたまま**」です。

退出ボタンタイプ

実際のニーズに応じて、退出ボタンを「**開いたまま**」または「**閉じたまま**」に設定できます。デフォルトは「**開いたまま**」です。

ドアロック電源オフ時の状態

ドアロックの電源オフ時の状態を設定できます。デフォルトは「**閉じたまま**」です。

延長開放時間

延長アクセス権限を持つ人物がカードをスワイプした後、適切な遅延を経てドアコンタクトを有効化できます。

最初の入室者によるドア開放時間設定

最初の人が入室した際のドア開放時間を設定します。最初の人の認証後、複数人の入室やその他の認証操作を許可します。

緊急コード

緊急事態発生時、緊急コード入力によりドアを開錠可能。同時にクライアントは緊急事態を報告できる。

スーパーパスワード

特定の者がスーパーパスワードを入力することでドアを開錠できます。

注記

緊急コードとスーパーコードは異なるものにする必要があります。また、桁数は4から8までです。

RS-485 パラメータの設定

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

設定→ アクセス制御→ RS-485 をタップします。

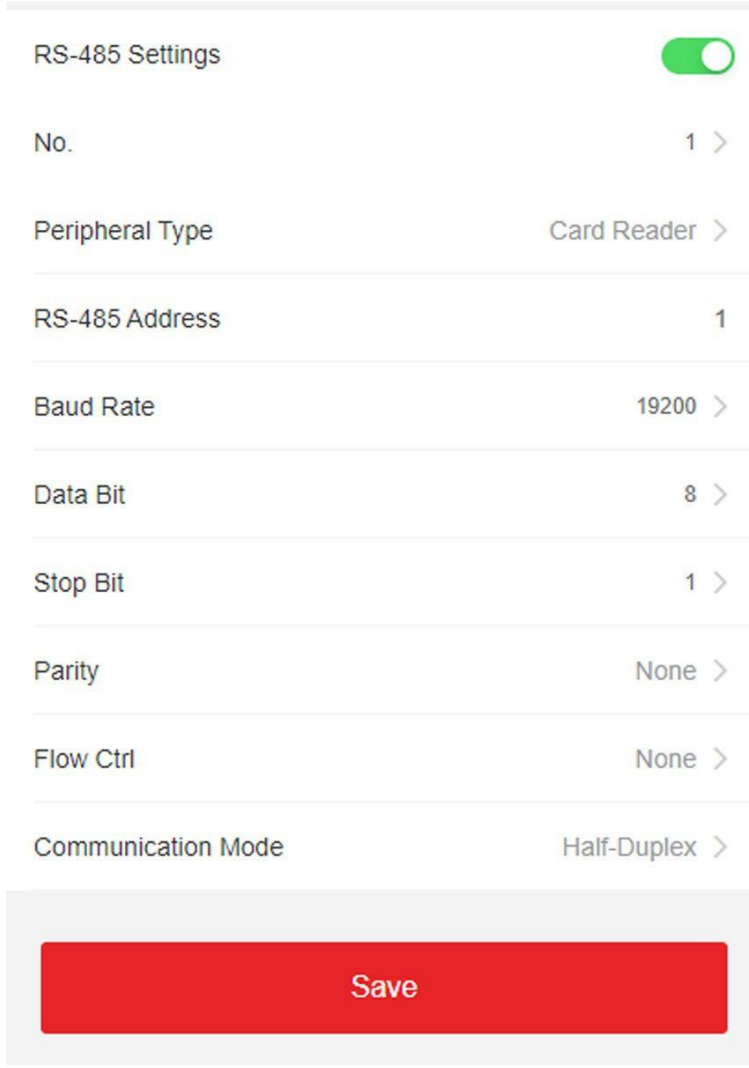


図 8-14 RS-485 ページ

設定後、**保存**をタップして設定を保存します。

周辺機器タイプ

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。以下の選択肢から選択できます。**カードリーダー**、**拡張モジュール**、または**アクセスコントローラー**。

注記

周辺機器を変更して保存すると、デバイスは自動的に再起動します。

RS-485 アドレス

実際のニーズに応じて RS-485 アドレスを設定してください。

注記

アクセスコントローラを選択した場合：RS-485 インターフェースを介してデバイスを端末に接続する場合は、RS-485 アドレスを 2 に設定してください。デバイスをコントローラに接続する場合は、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

デバイスが RS-485 プロトコルを介して通信する場合のボーレート。

データビット

デバイスがRS-485プロトコルで通信している際のデータビット。

ストップビット

デバイスが RS-485 プロトコルで通信する場合のストップビット。

デフォルトで有効。

デフォルトで有効。

Wiegand パラメータの設定

Wiegand 伝送方向を設定できます。

手順

1. **設定→ アクセス制御→ ウィーガンド設定** をタップします。

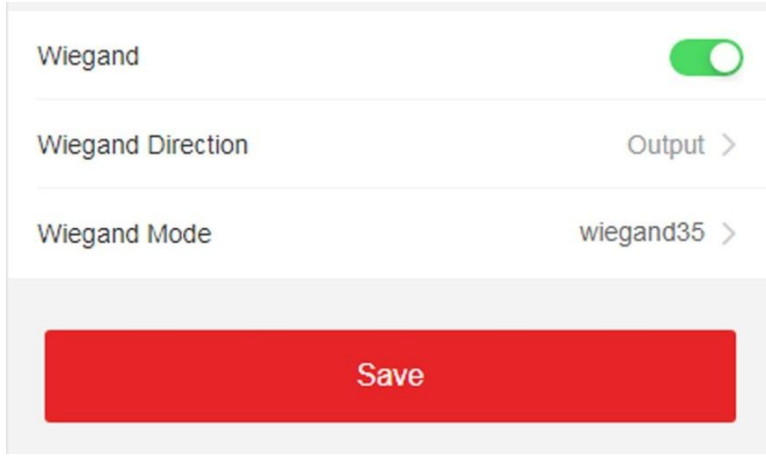


図 8-15 ウィーガンドページ

2. **Wiegand** を有効にして、Wiegand 機能を有効にします。

3. 送信方向を設定します。

出力

外部アクセスコントローラーを接続できます。両デバイスは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、デバイスパラメータを保存すると、デバイスは自動的に再起動します。

第9章 Webブラウザによる操作

9.1 ログイン

Web 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。

注記

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の詳細については、「アクティベーション」を参照してください。

Web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アクセスします。

注

IP アドレスが「Https:」で始まっていることを確認してください。

デバイスのユーザー名とパスワードを入力します。**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によるログイン

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ページに入ります。

9.2 ライブビュー

デバイスのライブ映像を視聴できます。

ログイン後、ライブビューページが表示されます。ライブビュー、キャプチャ、録画などの操作が可能です。

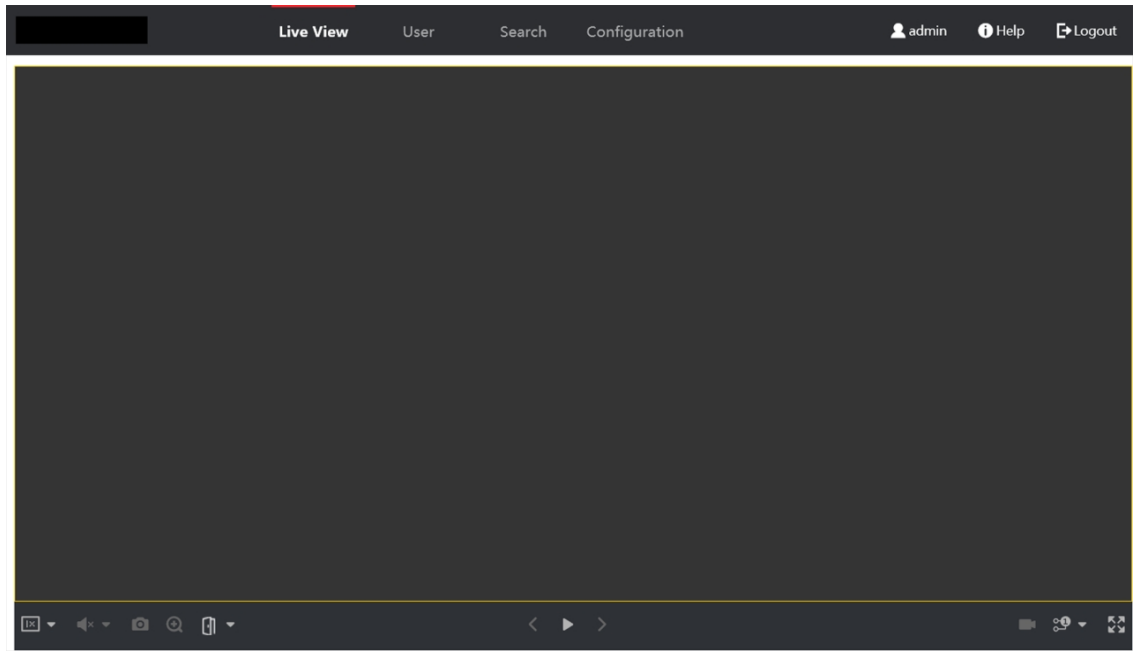


図9-1 ライブビュー画面

機能説明:

ライブビュー開始時の画像サイズを選択します。ライブビ

ュー開始時の音量を設定します。

注意

双方向オーディオを開始する際に音量を調整すると、音が繰り返し聞こえる場合があります。

ライブビュー開始時に画像をキャプチャできます。予約済み機能です。

ライブビュー画像を拡大できます。ライブビューを開始または停止しま

す。

ビデオ録画を開始または停止します。

ライブビュー開始時にストリーミングタイプを選択します。メインストリームとサブストリームから選択できます。

全画面表示。

9.3 人物管理

基本情報、カード、認証モード、写真などの人物情報をクリックして追加します。

OKをクリックして人物を保存します。

基本情報を追加

ユーザー→追加をクリックして、人物追加ページに入ります。
従業員ID、氏名、ユーザーレベル、フロア番号、部屋番号などの基本情報を追加します。
設定を保存するには、**[OK]**をクリックします。

カードを追加

ユーザー→追加をクリックして、人物追加ページに入ります
。**カード追加**をクリックし、カード番号を入力します。
設定を保存するには、**[OK]** をクリックします。

顔写真を追加

ユーザー→追加をクリックして、人物追加ページに入ります。
右側の**「+」**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てください。

注意

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

設定を保存するには**「OK」**をクリックしてください。

許可時間の設定

ユーザー→追加をクリックして、人物追加ページに入ります
。**開始**時間と**終了時間を**設定します。
設定を保存するには、**[OK]**をクリックしてください。

アクセス制御の設定

ユーザー→追加をクリックして、ユーザー追加ページに入ります。
アクセス制御で管理者を確認後、追加された人物は顔認証でログインできます。 **[Add]** をクリックしてアクセス制御の**フロア番号**と**部屋番号**を入力し、［ ］をクリックして削除できます。 **[OK]** をクリックして設定を保存します。

認証モードの追加

ユーザー→追加をクリックして「人物追加」ページに入りま
す。認証タイプを設定します。

設定を保存するには「**OK**」をクリックします。

9.4 イベント検索

検索をクリックすると、検索ページに入ります。

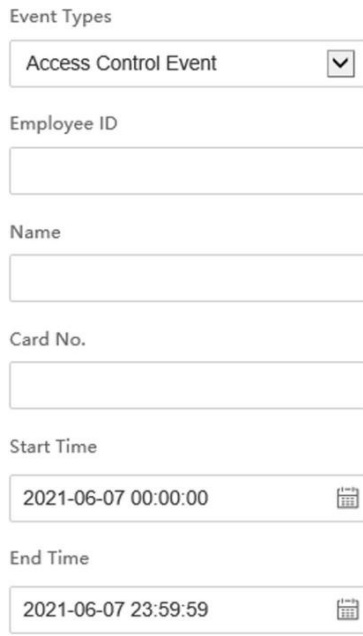


図 9-2 検索ページ

検索条件（従業員ID、氏名、カード番号、開始時刻、終了時刻）を入力し、「**検索**」をクリックしてください。

検索結果は右パネルに表示されます。

9.5 設定

9.5.1 ローカルパラメータの設定

ライブビューのパラメータ、録画ファイルの保存先、キャプチャ画像の保存先を設定します。

ライブビューパラメータの設定

設定→ローカルをクリックしてローカルページに入ります。ストリームタイプ、再生パフォーマンス、ライブビューの自動開始、画像フォーマットを設定し、**保存**をクリックします。

録画ファイル保存パス設定

設定→ローカルをクリックしてローカルページに入ります。レコードファイルサイズを選択し、ローカルコンピュータから保存先パスを選択して**保存**をクリックします。
[開く]をクリックするとファイルフォルダが開き、詳細を確認できます。

キャプチャ画像の保存パス設定

設定→ローカルをクリックしてローカルページに入ります。ローカルコンピュータから保存パスを選択し、**保存**をクリックします。
詳細を確認するには、**[開く]**をクリックしてファイルフォルダを開くこともできます。

9.5.2 デバイス情報の表示

デバイス名、言語、モデル、シリアル番号、QRコード、バージョン、チャンネル数、アラーム入力、アラーム出力、ロックとRS-485、デバイス容量などを表示します。

設定→システム→システム設定→基本情報 をクリックして設定ページに入ります。

デバイス名、言語、モデル、シリアル番号、QRコード、バージョン、チャンネル数、アラーム入力、アラーム出力、ロックとRS-485、デバイス容量などを表示できます。

9.5.3 時刻設定

デバイスのタイムゾーン、同期モード、およびデバイスの時刻を設定します。**設定→システム→システム設定→時刻設定** をクリックします。

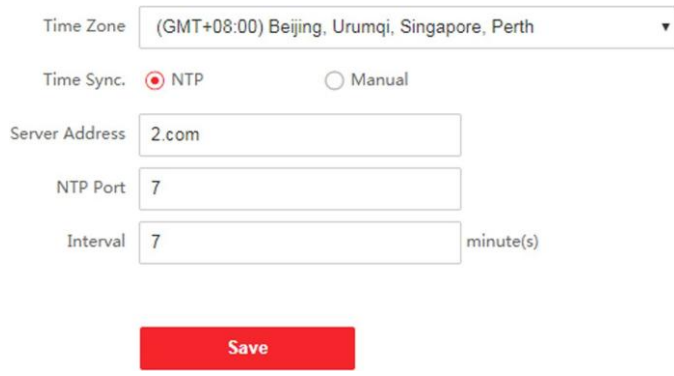


図 9-3 時刻設定

設定後、**保存**をクリックして設定を保存してください。

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。

時刻同期

NTP

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

手動

デフォルトでは、デバイスの時刻は手動で同期する必要があります。デバイスの時刻を手動で設定するか、**[コンピュータの時刻と同期]** をチェックしてデバイスの時刻をコンピュータの時刻と同期させることができます。

9.5.4 夏時間設定

手順

1. **設定→システム→システム設定→DST** をクリックします。

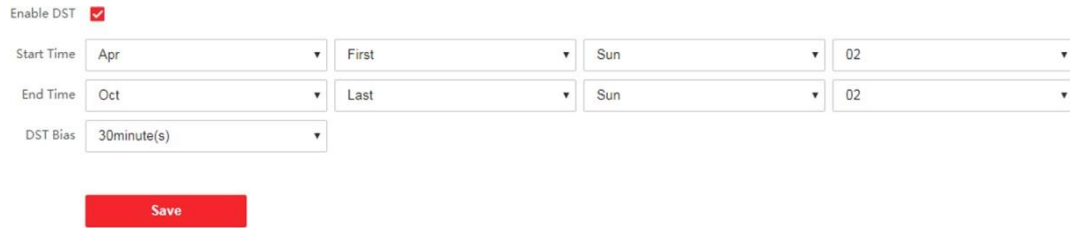


図 9-4 DST ページ

2. **夏時間有効化**にチェックを入れます。

3. 夏時間の開始時刻、終了時刻、およびバイアス時間を設定します。

4. 設定を保存するには「**保存**」をクリックしてください。

9.5.5 オープンソースソフトウェアライセンスを表示

設定→システム→システム設定→バージョン情報 に移動し、「**ライセンスを表示**」をクリックしてデバイスのライセンスを確認します。

9.5.6 アップグレードとメンテナンス

デバイスの再起動、デバイスパラメータの復元、デバイスバージョンのアップグレードを行います。

デバイスの再起動

設定→システム→メンテナンス→アップグレードとメンテナンス をクリックします。

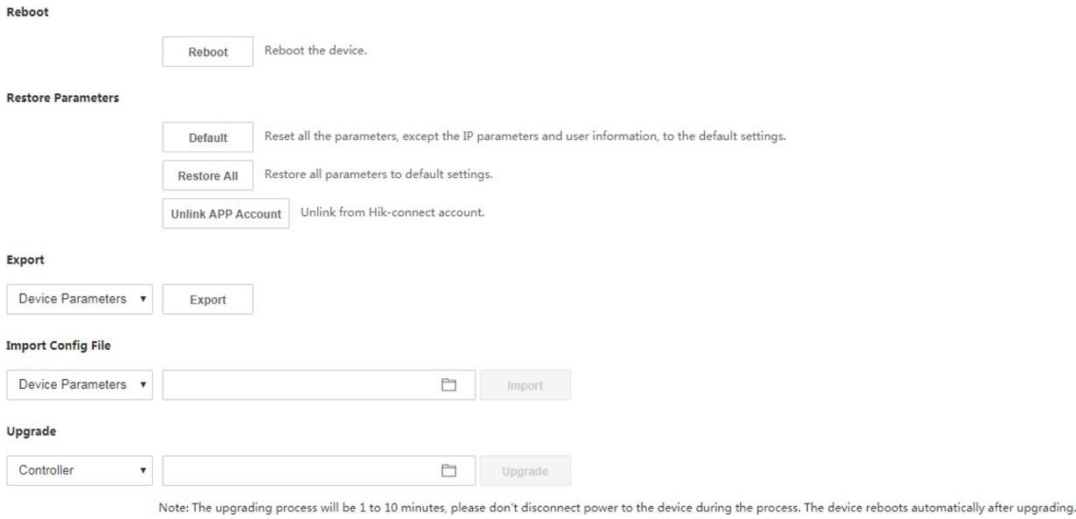


図9-5 アップグレードとメンテナンスページ

再起動をクリックしてデバイスの再起動を開始します。

パラメータの復元

設定→システム→メンテナンス→アップグレードとメンテナンス をクリックします。

すべて復元

すべてのパラメータが工場出荷時の設定に復元されます。使用前にデバイスをアクティベートする必要があります。

デフォルト

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。

APPアカウントのリンク解除

プラットフォームからHik-Connectアカウントのリンクを解除します。

パラメータのインポートとエクスポート

設定→システム→メンテナンス→アップグレードとメンテナンス をクリックします。

エクスポート

エクスポートをクリックして、ログまたはデバイスパラメータをエクスポートします。

注

エクスポートしたデバイスパラメータを別のデバイスにインポートできます。

インポート

をクリックし、インポートするファイルを選択します。**Import**をクリックして設定ファイルのインポートを開始します。

アップグレード

設定→ システム→ メンテナンス→ アップグレードとメンテナンス をクリックします。
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てください。［ ］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てください。 **[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。

注意

アップグレード中は電源を切らないでください。

9.5.7 ログクエリ

デバイスのログを検索および表示できます。

設定→ システム→ メンテナンス→ ログクエリ に移動します。

ログタイプのメジャーおよびマイナー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ます。これには、番号、時刻、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。

9.5.8 セキュリティモード設定

クライアントソフトウェアのログイン用セキュリティモードを設定します。

[管理対象デバイス] ページで、**[設定]→[システム]→[セキュリティ]→[セキュリティサービス]** をクリックします。

ドロップダウンリストからセキュリティモードを選択し、[**保存**] をクリックします。

セキュリティモード

クライアントソフトウェアへのログイン時に、ユーザー情報の検証を行うセキュリティレベルを高く設定します。

互換モード

ユーザー情報の検証は、ログイン時に旧クライアントソフトウェアバージョンと互換性があります。

SSHを有効にする

ネットワークセキュリティを強化するため、SSHサービスを無効化してください。この設定は、専門家によるデバイスのデバッグにのみ使用されます。

HTTPSを有効にする

ウェブサイトを訪問する際のネットワークセキュリティレベルを高めるため、HTTPSを有効にして、より安全で暗号化されたネットワーク通信環境を取得することができます。HTTPSを有効にした後、通信はIDと暗号化パスワードによって認証されるべきであり、それは安全です。

9.5.9 証明書管理

サーバー/クライアント証明書およびCA証明書の管理を支援します。

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。

自己署名証明書の作成とインストール

手順

1. **設定→ システム→ セキュリティ→ 証明書管理** に移動します。
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およびインストールします。
   作成された証明書は「**証明書の詳細**」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任意のファイルに保存します。
7. 要求ファイルを認証機関に送信して署名を受け取ります。
8. 署名済み証明書をインポートします。
   1) **[パスワードのインポート]** 領域で証明書の種類を選択し、ローカルから証明書を選択して **[インストール]** をクリックします。
   2) **通信**証明書のインポート領域で証明書の種類を選択し、ローカルから証明書を選択して「**インストール**」をクリックします。

その他の認可済み証明書のインストール

認証済み証明書（デバイスで作成されたものではない）を既に所有している場合は、それをデバイスに直接インポートすることができます。

手順

1. **設定→ システム→ セキュリティ→ 証明書管理** に移動します。
2. **「パスワードのインポート」**および「**通信証明書のインポート」**領域で、証明書の種類を選択し、証明書をアップロードします。
3. **インストールを**クリックします。

CA証明書のインストール

開始前に

CA 証明書を事前に準備してください。

手順

1. **設定→ システム→ セキュリティ→ 証明書管理** に移動します。
2. **インポートCA証明書**領域でIDを作成します。

> **注**
>
> 入力する証明書IDは既存のものと同じにできません。

3. ローカルから証明書ファイルをアップロードしてください。
4. **インストールを**クリックします。

9.5.10 管理者のパスワードを変更する

手順

1. **設定→ ユーザー管理** をクリックします。
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. **[OK]** をクリックします。

> **注意**
>
> デバイスのパスワード強度を自動的に確認できます。製品のセキュリティ強化のため、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）への変更を強く推奨します。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お勧めします。月次または週次での変更により、製品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構成は、設置業者および / またはエンドユーザーの責任となります。

9.5.11 デバイスの武装/解除状態を確認する

デバイスの武装タイプと武装IPアドレスを表示します。

設定→ 警備/解除情報 に移動してください。

デバイスの武装/解除情報を確認できます。「**更新**」をクリックするとページが更新されます。

9.5.12 ネットワーク設定

TCP/IP、ポート、Wi-Fiパラメータ、レポート戦略、プラットフォームアクセス、HTTPリスニングを設定します。

注意

一部のデバイスモデルはWi-Fi設定に対応していません。設定時は実際の製品を参照してください。

基本ネットワークパラメータの設定

設定→ネットワーク→基本設定→TCP/IPをクリックします。パラメータを設

定し、**保存**をクリックして設定を保存します。

DHCP

この機能をオフにした場合、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、MTU、およびデバイスのポートを設定する必要があります。

この機能をチェックすると、システムは IPv4 アドレス、IPv4 サブネットマスク、および IPv4 デフォルトゲートウェイを自動的に割り当てます。

NIC タイプ

ドロップダウンリストから NIC タイプを選択します。デフォルトは「**自動**」です。

DNS サーバー

実際のニーズに応じて、優先 DNS サーバーと代替 DNS サーバーを設定してください。

ポートパラメータの設定

HTTP、RTSP、HTTPS、およびサーバーポートのパラメータを設定します。**設**

定→ネットワーク→基本設定→ポートをクリックします。

HTTP

ブラウザがデバイスにアクセスする際に使用するポートを指します。例えば、HTTPポートを81に変更した場合、ログインにはブラウザで***http://192.0.0.65:81***を入力する必要があります。

RTSP

リアルタイムストリーミングプロトコルのポートを指します。

HTTPS

ブラウザアクセス用にHTTPSを設定します。アクセス時には証明書が必要です。

サーバー

クライアントがデバイスを追加する際に使用するポートを指します。

Wi-Fiパラメータの設定

デバイスの無線接続用Wi-Fiパラメータを設定します。

手順

注記

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. **設定→ ネットワーク→ 基本設定→ Wi-Fi** をクリックします。

図 9-6 Wi-Fi 設定ページ

2. **Wi-Fi** をチェックします。

3. Wi-Fi を選択

- リスト内の Wi-Fi の [🔗] をクリックし、Wi-Fi パスワードを入力します。
- **[追加]** をクリックし、SSID、動作モード、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 パラメータを設定します。

1) **ネットワーク設定**をクリックします。

2) 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**」をチェックすると、システムが自動的に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割り当てます。

5. **[OK]**をクリックします。

レポート戦略設定

ISUPプロトコル経由でログをアップロードするためのセンターグループを設定できます。**設定**

→ ネットワーク→ 基本設定→ レポート戦略 に移動します。

センターグループを設定すると、システムはISUPプロトコル経由でログを転送します。設定を保存するには **[保存]** をクリックします。

設定を保存します。

センターグループ

ドロップダウンリストからセンターグループを選択してください。

メインチャネル

本装置はメインチャネルを介してセンターと通信します。

注記

N1 は有線ネットワークを指します。

プラットフォームアクセス

プラットフォームアクセスにより、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が提供されます。

手順

1. **設定→ネットワーク→詳細設定→**プラットフォームアクセスをクリックして設定ページに入ります。
2. **プラットフォームアクセスモード**を選択**します**。

注記

Hik-Connectはモバイル端末用アプリケーションです。本アプリでは、デバイスのライブ映像の閲覧やアラーム通知の受信などが可能です。

3. **「有効にする」**のチェックボックスをオンにして機能を有効にします。
4. **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。
5. デバイス用の**ストリーム暗号化/暗号化キー**を作成します。

注記

6～12 文字（a～z、A～Z）または数字（0～9）で、大文字と小文字が区別されます。8 文字以上の英数字の組み合わせを使用することをお勧めします。

6. **保存**をクリックして設定を有効にします。

ISUP パラメータを設定する

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

手順

注記

デバイスがこの機能をサポートしている必要があります。

1. **設定→ネットワーク→詳細設定→ プラットフォーム** をクリックします。
2. プラットフォームアクセスモードのドロップダウンリストから**ISUP**を選択します。
3. **有効化**をチェックします。
4. ISUP バージョンを設定し、アラーム受信機タイプ、サーバーアドレス、ポート、デバイス ID、登録ステータスを確認します。

注記

バージョンとして 5.0 を選択した場合は、ISUP キーも設定する必要があります。

5. ISUP監視パラメータを設定します。これには、ISUPアラームセンターのIPアドレス/ドメイン名、ISUPアラームセンターのURL、およびISUPアラームセンターのポートが含まれます。
6. **保存**をクリックします。

HTTP リスニングの設定

デバイスは、HTTPプロトコル/HTTPSプロトコルを介して、イベントアラームの IP アドレスまたはドメイン名にアラーム情報を送信できます。

開始前に

イベントアラームの IP アドレスまたはドメイン名は、アラーム情報を受信するために HTTPプロトコル/HTTPSプロトコルをサポートしている必要があります。

注

この機能は、デバイスがサポートしている必要があります。

手順

1. **設定→ ネットワーク→ 詳細設定→ HTTP リスニング** をクリックします。
2. イベントアラームのIPアドレスまたはドメイン名、URL、ポート、プロトコルを編集します。
3. **オプション：[デフォルト]**をクリックして、イベントアラームのIPアドレスまたはドメイン名をリセットします。
4. **[保存]** をクリックします。

9.5.13 ビデオとオーディオのパラメータを設定

画質、解像度、デバイスの音量を設定します。

ビデオパラメータの設定

設定→ ビデオ/オーディオ→ ビデオ をクリックします。

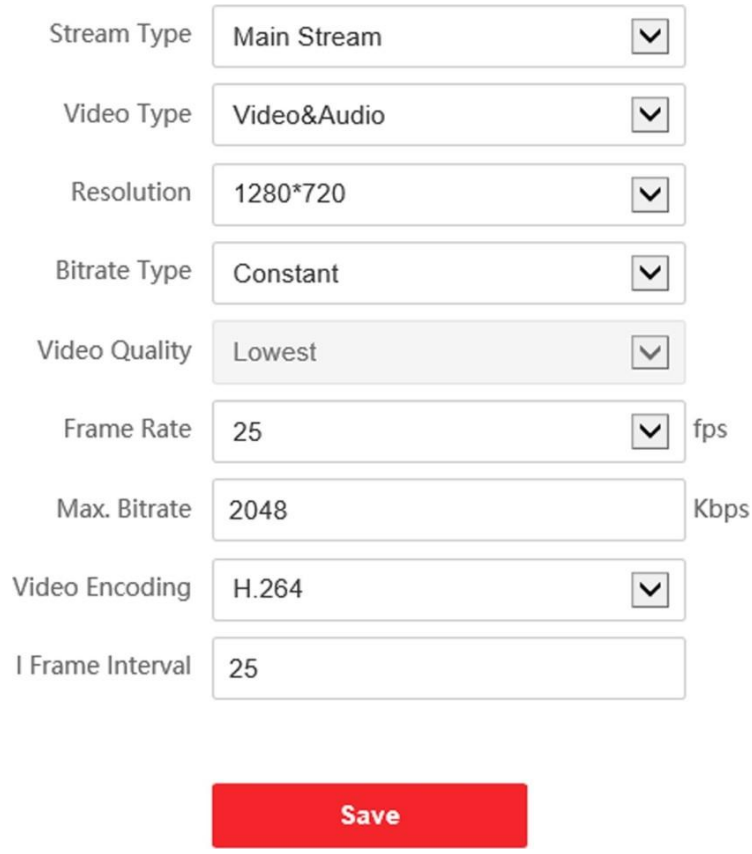


図 9-7 ビデオ設定ページ

ストリームタイプ、ビデオタイプ、ビットレートタイプ、フレームレート、最大ビットレート、ビデオエンコーディング、およびIフレーム間隔を設定します。

設定後、**保存**をクリックして設定を保存します。

オーディオパラメータの設定

設定→ビデオ/オーディオ→オーディオ をクリックします。

オーディオストリームタイプとオーディオエンコーディングを

設定します。

ブロックをドラッグしてデバイスの入力/出力音量を調整することもできます。設定後、**保存**をクリックして設定を保存します。

注記

機能は機種によって異なります。詳細は実際のデバイスを参照してください。

9.5.14 オーディオコンテンツのカスタマイズ

認証成功時と失敗時の出力オーディオコンテンツをカスタマイズします。

手順

1. **設定→ ビデオ/オーディオ→ プロンプト** をクリックします。

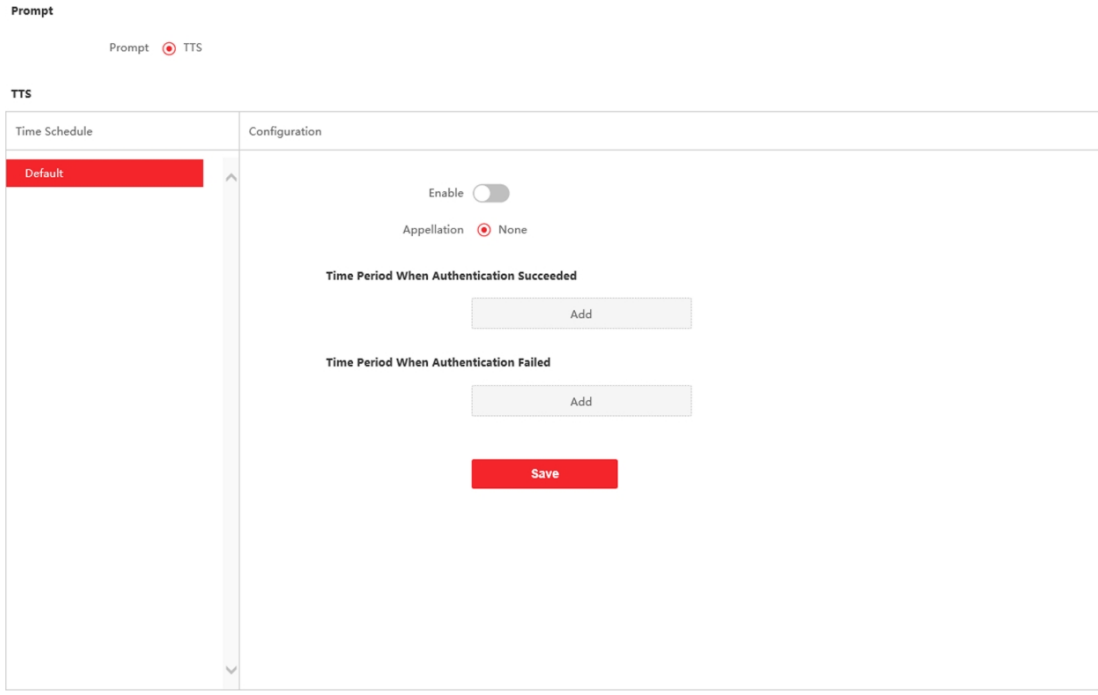


図 9-8 音声コンテンツのカスタマイズ

2. **プロンプトを TTS**（テキスト読み上げ）として選択し、テキストを音声コンテンツに変換します。

3. タイムスケジュールを選択します。

4. 機能を有効にします。

5. 呼び出し名を設定します。

6. 認証成功時の期間を設定します。

1) **追加**をクリックします。

2) 時間枠と言語を設定します。

注記

設定された時間内に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ブロードキャストします。

3) 音声コンテンツを入力してください。

4) **オプション**：サブステップ1～3を繰り返します。

5) **オプション**：設定した時間制限を削除するには、[🗑] をクリックします。

7. 認証が失敗した場合の時間設定を行います。

1) **[追加]** をクリックします。

2) 時間と言語を設定します。

注記

設定した時間内に認証が失敗した場合、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) 音声コンテンツを入力してください。

4) **オプション:** サブステップ1から3を繰り返します。

5) **オプション：** 設定した時間枠を削除するには、[ ]をクリックします。

8. オプション： 休日スケジュールを追加します。

1) **「追加」**をクリックして休日スケジュールを追加します。

2) ステップ3から6を繰り返します。

9. 設定を保存するには、**[保存]**をクリックします。

9.5.15 画像パラメータの設定

ビデオ規格、WDR、明るさ、コントラスト、彩度、シャープネスを設定します。

手順

1. 設定→ 画像調整 をクリックします。

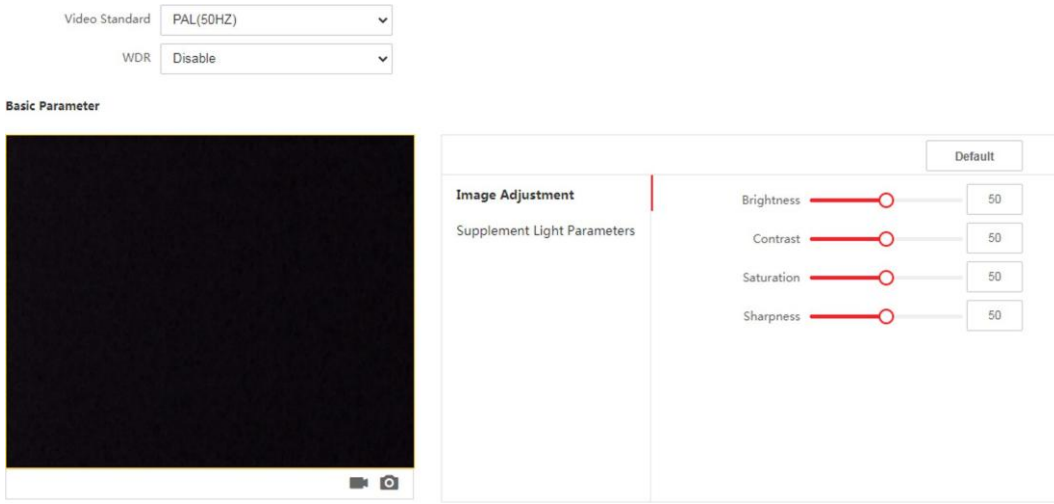


図 9-9 画像設定ページ

2. 画像調整を行うパラメータを設定します。

ビデオ規格

リモートでライブビューを行う際の動画フレームレートを設定します。設定変更後は、変更を有効にするためにデバイスを再起動してください。

PAL

毎秒25フレーム。中国本土、香港（中国）、中東諸国、欧州諸国などに適しています。

NTSC

30フレーム/秒。アメリカ、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。

WDR

WDR 機能を有効または無効にします。

視野内に非常に明るい部分と非常に暗い部分が同時に存在する場合、WDR は画像全体の明るさのレベルをバランスさせ、細部まで鮮明な画像を提供します。

明るさ/コントラスト/彩度/シャープネス

ブロックをドラッグするか値を入力して、ライブ動画の明るさ、コントラスト、彩度、シャープネスを調整します。

動画の録画開始/終了。画像をキ

ャプチャ。

3. **デフォルト**をクリックすると、パラメータがデフォルト設定に復元されます。

9.5.16 補助ライトの明るさを設定

デバイスの補助光輝度を設定します。

手順

1. **設定→ 画像→ 補助光パラメータ** をクリックします。

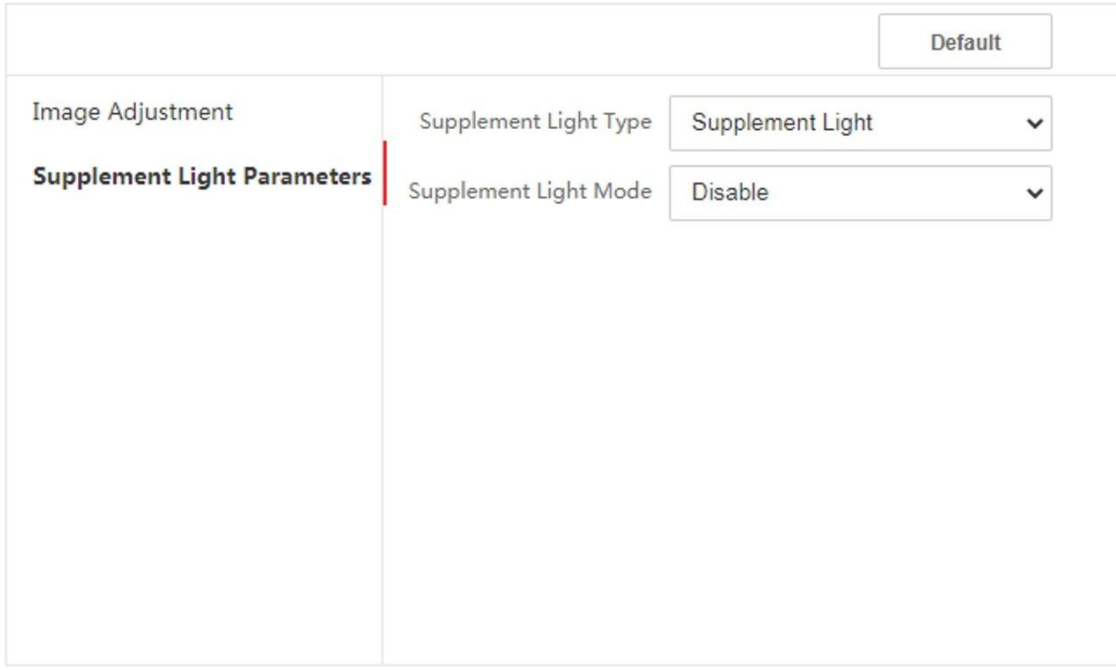


図 9-10 補助光設定ページ

2. ドロップダウンリストから補助照明のタイプとモードを選択してください。モードを**ON**に設定する場合は、明るさを設定する必要があります。

9.5.17 勤怠管理設定

従業員の出勤•退勤時刻の追跡•監視、勤務時間、遅刻•早退、休憩時間、欠勤を管理したい場合、従業員をシフトグループに追加し、シフトスケジュール（出勤定義ルール：スケジュールの繰り返し方法、シフトタイプ、休憩設定、カード打刻ルール）を割り当てて、シフトグループ内の従業員の出勤パラメータを定義できます。

Web経由での勤怠モード無効化

勤怠モードを無効にすると、システムは初期画面で勤怠ステータスを表示しなくなります。

手順

1. **設定→勤怠**をクリックして設定ページに入ります。
2. **出席モード**を**無効**に設定してください。

結果

初期ページでは出席ステータスを表示または設定しません。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。

時間設定

手順

1. **設定→時間設定**をクリックして設定ページに入ります。
2. **ステータスタイプ**を選択します。
3. **オプション：**実際のニーズに応じて**スケジュール名を**編集します。
4. マウスをドラッグしてスケジュールを設定します。

   注意

   実際のニーズに応じて、月曜日から日曜日までのスケジュールを設定してください。

5. **オプション：**タイムラインを選択し、「**削除」**をクリックします。または「**すべて削除」**をクリックして設定をクリアします。
6. **保存**をクリックします。

Web経由での手動出席設定

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

開始前に

ユーザーを少なくとも1人追加し、そのユーザーの認証モードを設定してください。詳細は「**ユーザー管理」**を参照してください。

手順

1. **設定→出席**をクリックして設定ページに入ります。
2. **出席モード**を手**動**に設定します。
3. **出席ステータス必須**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。

   注記

   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、その名前を変更します。

結果

認証後、手動で出席ステータスを選択する必要があります。

注記

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経由での自動出席設定

出席モードを自動に設定すると、出席ステータスとその有効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人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。詳細は「**ユーザー管理」**を参照してください。

手順

1. **設定→出席**をクリックして設定ページに入ります。
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。

注記

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、その名前を変更します。
6. ステータスのスケジュールを設定します。詳細は「**時間設定」**を参照してください。

Web経由での手動および自動出席設定

出勤モードを「**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勤ステータスを自動的に変更します。同時に、認証後に出勤ステータスを手動で変更することも可能です。

開始前に

少なくとも1人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。詳細は「**ユーザー管理」**を参照してください。

手順

1. **設定→出席**をクリックして設定ページに入ります。
2. **出席モード**を「**手動」と「自動」**に設定します。
3. **「出席状況」**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する。

注記

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、その名前を変更します。
6. ステータスのスケジュールを設定します。詳細は「***Time SeFngs」***を参照してください。

結果

初期ページで認証を行います。スケジュールに従い、設定された出席ステータスで認証がマークされます。結果タブの編集アイコンをタップすると、手動で出席を取るステータスを選択でき、認証は編集された出席ステータスでマークされます。

例

休憩開始を月曜11:00、**休憩終了**を月曜12:00に設定した場合、月曜11:00～12:00の有効なユーザー認証は休憩として記録されます。

9.5.18 一般設定

認証パラメータの設定

設定→一般→認証設定 をクリックします。

注意

機能はモデルによって異なります。詳細は実際のデバイスを参照してください。

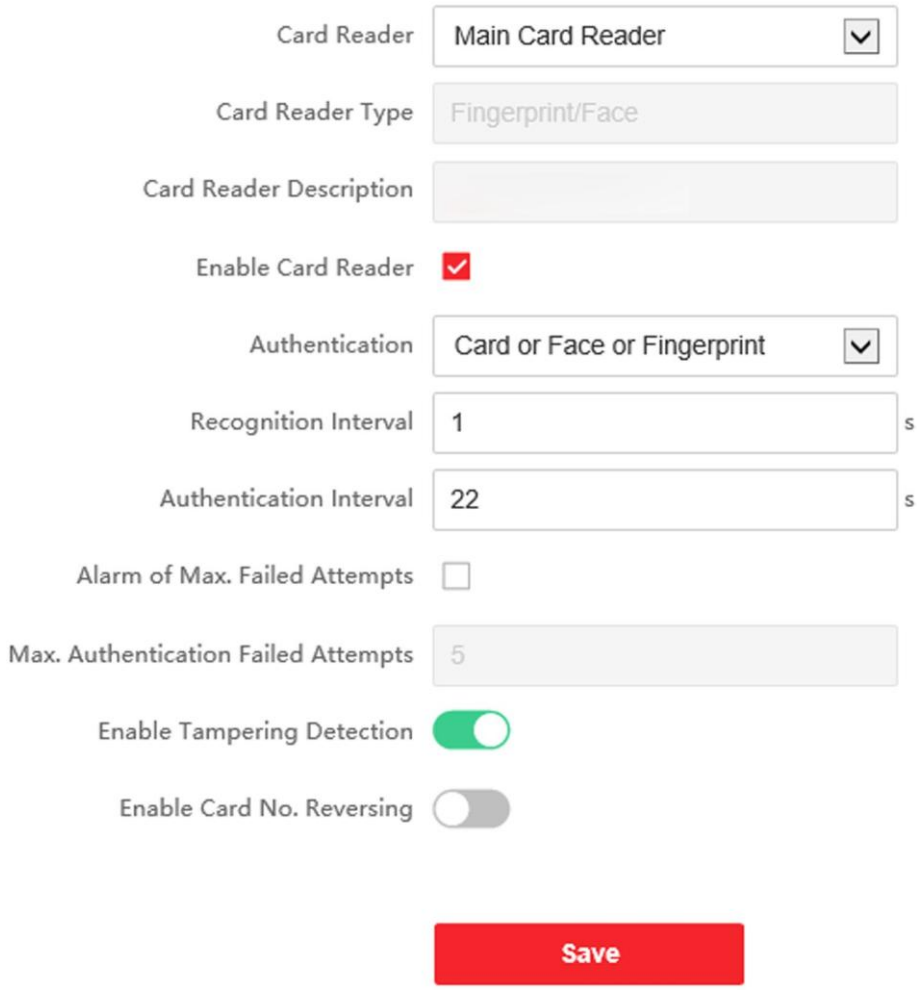


図 9-11 認証パラメータの設定

設定後、**保存**をクリックして設定を保存します。

デバイスタイプ

ドロップダウンリストから**メインカードリーダー**または**サブカードリーダー**を選択します。

メインカードリーダー

デバイスのカードリーダーのパラメータを設定できます。

サブカードリーダー

接続された周辺機器カードリーダーのパラメータを設定できます。

メインカードリーダーを選択した場合:

カードリーダーの種類/カードリーダーの説明

カードリーダーのタイプと説明を取得します。これらは読み取り専用です。

カードリーダーを有効化

カードリーダーの機能を有効にします。

認証

実際のニーズに応じて、ドロップダウンリストから認証モードを選択します。

認識間隔

認証中に同一人物が連続して認識される間隔を設定できます。設定された間隔内では、人物Aは1回のみ認識されます。その間隔中に別の人物（人物B）が認識された場合、人物Aは再度認識可能になります。

認証間隔

認証時に同一ユーザーの本認証間隔を設定できます。設定された間隔内で同一ユーザーは1回のみ認証可能です。2回目の認証は失敗します。

最大失敗試行回数アラーム

カード読み取り試行回数が設定値に達した際にアラームを通知する機能を有効にします。

最大認証失敗回数

設定値に達した際にアラームを通知します。

改ざん検知を有効にする

カードリーダーの改ざん検知を有効にします。

カード番号反転を有効にする

機能有効化後、読み取りカード番号は逆順になります。

サブカードリーダーを選択した場合:

カードリーダータイプ/カードリーダー説明

カードリーダーのタイプと説明を取得します。これらは読み取り専用です。

カードリーダーを有効化

カードリーダーの機能を有効にします。

認証

実際のニーズに応じて、ドロップダウンリストから認証モードを選択します。

認識間隔

同一カードの提示間隔が設定値未満の場合、カード提示は無効となります。

認証間隔

認証時に同一ユーザーが認証できる間隔を設定できます。設定された間隔内で同一ユーザーは1回のみ認証可能です。2回目の認証は失敗します。

最大失敗試行回数アラーム

カード読み取り試行回数が設定値に達した際にアラームを通知する機能を有効にします。

最大認証失敗回数

設定値に達した際にアラームを通知します。

コントローラとの通信間隔

設定時間以上、アクセス制御デバイスがカードリーダーに接続できない場合、カードリーダーは自動的にオフラインになります。

パスワード入力時の最大間隔

カードリーダーでパスワードを入力する際、2桁の数字を押す間隔が設定値より長いと、以前に押した数字は自動的にクリアされます。

OK LED極性/エラーLED極性

カードリーダーのパラメータに基づき、アクセス制御装置の OK LED 極性/エラー LED 極性を設定します。通常はデフォルト設定を採用します。

改ざん検知を有効にする

カードリーダーの改ざん検知を有効にします。

プライバシーパラメータの設定

イベント保存タイプ、画像アップロードおよび保存パラメータ、画像消去パラメータを設定します。

設定→一般→プライバシー に移動してください。

イベント保存設定

イベントを削除する方法を選択します。「**古いイベントを定期的に削除**」「**指定した時間で古いイベントを削除**」「**上書き**」から選択できます。

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、イベント削除の期間を設定します。設定した期間に基づき全てのイベントが削除されます。

指定時間による古いイベント削除

指定時刻を設定すると、設定時刻にすべてのイベントが削除されます。

上書き

システムが保存済みイベントが全容量の95%を超えたことを検知すると、最も古い5%のイベントが削除されます。

認証設定

認証結果の表示

顔写真、**氏名**、**社員ID**、**体温**を確認し、認証結果を表示することができます。

名前の匿名化

名前の匿名化を確認でき、名前全体は表示されません。

画像アップロードと保存

認証時の撮影画像アップロード

認証時に撮影した画像を自動的にプラットフォームにアップロードします。

認証時にキャプチャした画像を保存

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。

登録済み画像の保存

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。

リンク撮影後の画像アップロード

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

リンク撮影後の画像保存

この機能を有効にすると、接続されたカメラで撮影した画像を端末に保存できます。

デバイス内の全画像を消去

注意

一度削除した画像は復元できません。

登録済み顔写真を消去

登録されているすべての画像が削除されます。

撮影した写真を消去

デバイス内の撮影済み画像をすべて削除します。

顔認識パラメータの設定

アクセス用の顔認識パラメータを設定できます。

設定→アクセス制御→顔認識パラメータ をクリックします。

動作モードを「**アクセス制御モード**」に設定できます。アクセス制御モードはデバイスの通常動作モードです。アクセスには認証情報の認証が必要です。

カードセキュリティの設定

設定→一般→カードセキュリティをクリックして設定ページに入ります。パラメータを設定し、

保存をクリックします。

NFCカード有効化

携帯電話がアクセス制御データを取得するのを防ぐため、NFCカードを有効化してデータのセキュリティレベルを高めることができます。

M1カードの有効化

M1カードの有効化と、M1カードの提示による認証が利用可能です。

M1カードの暗号化

M1カードの暗号化により、認証のセキュリティレベルを向上させることができます。

セクター

機能を有効化し、暗号化セクターを設定します。デフォルトではセクター13が暗号化されます。セクター13の暗号化を推奨します。

EMカード有効化

EMカードを有効化し、EMカードの提示による認証が可能になります。

注記

周辺機器のカードリーダーがEMカードの提示をサポートしている場合、EMカード機能の有効化/無効化機能もサポートされます。

DESFireカードの有効化

DESFireカード機能を有効にすると、デバイスはDESFireカードからデータを読み取ることができます。

DESFireカード内容読み取り

DESFireカード内容読み取り機能を有効にした後、デバイスはDESFireカードの内容を読み取ることができます。

カード認証パラメータの設定

デバイス上でカードによる認証を行う際のカード読み取り内容を設定します。

設定→アクセス制御→カード認証設定に移動します。カード認証モードを選択し、**保存**をクリックします。

全カード番号

すべてのカード番号が読み取られます。

ウィーガンド26（3バイト）

本デバイスはウィーガンド26プロトコル（3バイト読み取り）でカードを読み取ります。

ウィーガンド34（4バイト）

本デバイスはウィーガンド34プロトコルでカードを読み取ります（4バイト読み取り）。

9.5.19 ビデオインターホン設定

ビデオインターコムパラメータの設定

本装置は、ドアステーション、外部ドアステーション、またはアクセス制御装置として使用できます。使用前にデバイス番号を設定する必要があります。

設定→ビデオインターホン→デバイス番号をクリック

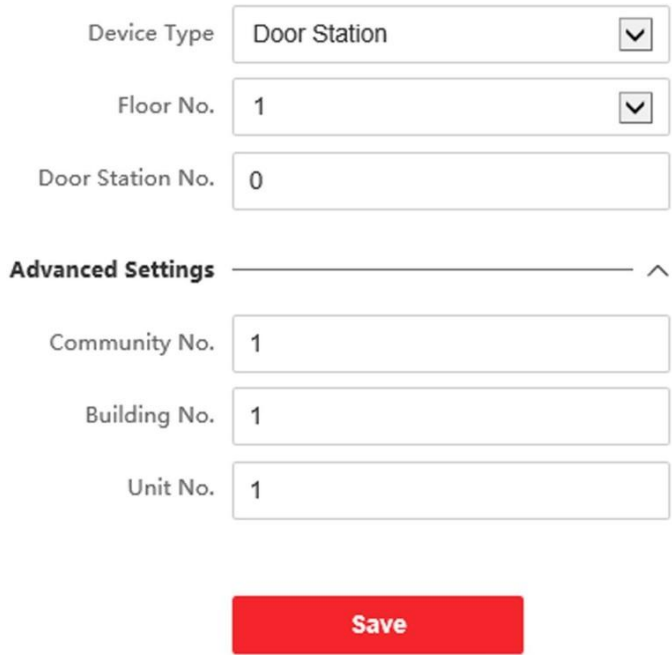


図 9-12 ビデオインターコムパラメータの設定

デバイスタイプを「**ドアステーション**」および「**アクセス制御デバイス**」に設定した場合、階番号、ドアステーション番号を設定でき、「**詳細設定**」をクリックするとコミュニティ番号、建物番号、ユニット番号を設定できます。

設定後、「**保存**」をクリックして設定を保存します。

デバイスタイプ

このデバイスは、ドアステーション、外部ドアステーション、またはアクセス制御デバイス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

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

設置階を設定してください。

ドアステーション番号

設置された装置の階数を設定してください

注記

番号を変更した場合は、デバイスを再起動してください。

コミュニティ番号

設置された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

デバイスが設置されている建物の番号を設定してください。

ユニット番号

設置ユニット番号を設定

デバイスタイプを「**屋外ドアステーション**」に設定した場合、屋外ドアステーション番号を設定し、「詳細設定」をクリックしてコミュニティ番号を設定できます。

詳細設定をクリックすると、コミュニティ番号を設定できます

外部ドアステーション番号

デバイスタイプとして「外ドアステーション」を選択した場合、1から99までの数字を入力してください。

99の間の数字を入力してください。

注意

番号を変更した場合は、デバイスを再起動してください。

コミュニティ番号

デバイスにインストールされているコミュニティ番号を設定します。

SIP パラメータの設定

デバイスの IP アドレスと SIP サーバーの IP アドレスを設定します。パラメータを設定すると、アクセス制御デバイス、ドアステーション、屋内ステーション、メインステーション、およびプラットフォーム間で通信できるようになります。

注

アクセス制御装置とその他の装置またはシステム（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）が同一のIPセグメントにある場合のみ、双方向音声通信が可能です。

設定→ビデオインターホン→リンクネットワーク設定 に移動します。メインステーションのIPアドレスとSIPサーバーのIPアドレスを設定します。

保存をクリックします。

ボタンを押して呼び出し

手順

1. **インターコム→ボタンを押して呼び出し** をクリックして設定ページに入ります。
2. パラメータを設定します。
   - 各ボタンの呼び出し番号を編集します。
   - **通話管理センター**をチェックして、ボタン通話センターを設定します。

注意

コール管理センターにチェックを入れ、さらにコール番号も設定した場合、コール管理センターはコール番号よりも優先度が高くなります。

9.5.20 アクセス制御設定

ドアパラメータの設定

設定→アクセス制御→ドアパラメータ をクリックします。

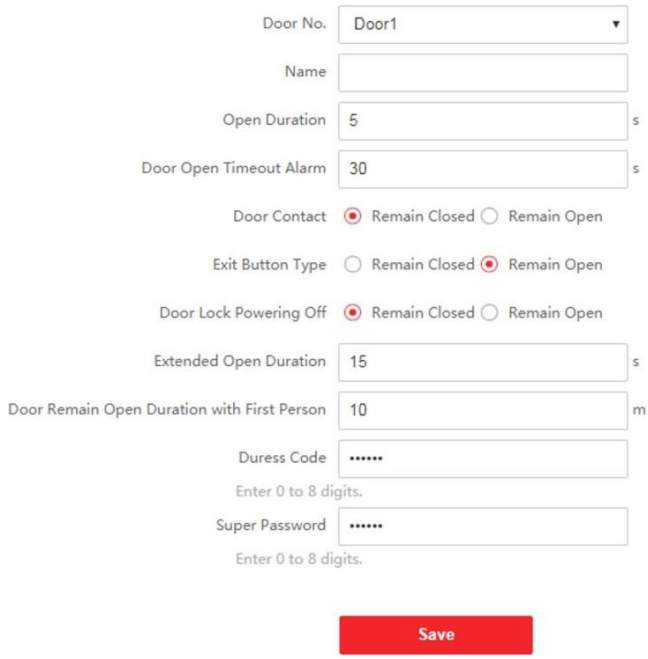


図 9-13 ドアパラメータ設定ページ

設定後、**保存**をクリックして設定を保存します。

ドア番号

対応するドア番号のデバイスを選択します。

名前

ドアに名前を付けることができます。

開放時間

ドアの解錠時間を設定します。設定時間内にドアが開かれない場合、ドアはロックされます。

ドア開放タイムアウト警報

設定時間内にドアが閉じられない場合、アラームが作動します。

ドアコンタクト

実際のニーズに応じて、ドアコンタクトを「**開いたまま**」または「**閉じたまま**」に設定できます。デフォルトは「**閉じたまま**」です。

退出ボタンタイプ

実際のニーズに応じて、出口ボタンを「**開いたままにする**」または「**閉じたままにする**」に設定できます。デフォルトでは「**開いたままにする**」です。

ドアロック電源オフ時の状態

ドアロックの電源オフ時の状態を設定できます。デフォルトは「**閉じたまま**」です。

延長開放時間

延長アクセス権限を持つ人物がカードをスワイプした後、適切な遅延を経てドアコンタクトを有効化できます。

最初の利用者のドア開放持続時間

最初の人が入室した際のドア開放時間を設定します。最初の人が認証されると、複数人の入室やその他の認証操作が可能になります。

緊急コード

脅迫状態発生時、脅迫コード入力によりドアを開錠可能。同時にクライアントは脅迫事象を報告できる。

スーパーパスワード

特定の者はスーパーパスワードを入力することでドアを開錠できます。

注記

緊急コードとスーパーコードは異なるものにする必要があります。

RS-485 パラメータの設定

RS-485パラメータ（周辺機器、アドレス、ボーレートなど）を設定できます。**設定→アクセス制御→RS-485設定**をクリックしてください。

「**RS-485を有効にする**」にチェックを入れ、パラメータを設定します。

設定後、**保存**をクリックして設定を保存します。

No.

RS-485 No. を設定

周辺機器タイプ

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。
カード**リーダー**、**拡張モジュール**、**アクセスコントローラ**、または**無効**

注

周辺機器を変更して保存すると、デバイスは自動的に再起動します。

RS-485 アドレス

実際のニーズに応じて RS-485 アドレスを設定してください。

注記

アクセスコントローラを選択した場合：RS-485 インターフェースを介してデバイスを端末に接続する場合は、RS-485 アドレスを 2 に設定してください。デバイスをコントローラに接続する場合は、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

デバイスが RS-485 プロトコルを介して通信する場合のボーレート。

ウィーガンドパラメータの設定

Wiegand 伝送方向を設定できます。

手順

注記

一部のデバイスモデルではこの機能をサポートしていません。設定時は実際の製品を参照してください。

1. **設定→ アクセス制御→ ウィーガンド設定** をクリックします。

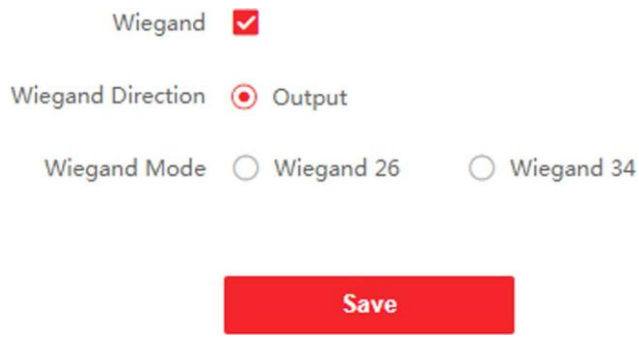


図 9-14 ウィーガンド設定ページ

2. **Wiegand** チェックボックスをオンにして Wiegand 機能を有効にします。
3. 送信方向を設定します。

   出力

   外部アクセスコントローラを接続できます。2台のデバイスは、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**」をクリックします。

注記

周辺機器を変更し、デバイスパラメータを保存すると、デバイスは自動的に再起動します。

9.5.21 生体認証パラメータの設定基本

パラメータの設定

設定→スマート→スマート をクリックします。

図 9-15 顔パラメータの設定

注

機能はモデルによって異なります。詳細は実際のデバイスを参照してください。

設定後、**[保存]**をクリックして設定を保存します。

顔認証のなりすまし防止

ライブ顔検出機能を有効または無効にします。機能を有効にすると、デバイスは人物が生きているかどうかを認識できます。

注意

生体認証製品は、偽装防止環境に対して完全には適用できません。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。

生体顔検出セキュリティレベル

顔偽装防止機能を有効にした後、生体顔認証時の照合セキュリティレベルを設定できます。

認識距離

認証ユーザーとデバイスカメラ間の距離を選択します。

適用モード

実際の環境に応じて「その他」または「屋内」を選択してください。

顔認識モード通常モード

カメラで通常通り顔を認識します。

ディープモード

ディープモードでは、顔写真を追加するには、デバイスのユーザー追加機能または登録ステーション経由でのみ可能です。写真インポートによる顔写真の追加はサポートされていません。

注意

ディープモードでは、顔写真はデバイスまたは登録ステーションからのみ追加できます。写真インポートによる顔写真の追加はサポートされていません。

連続顔認証間隔

認証時に連続する2回の顔認識の間隔を設定します。

ピッチ角

顔認証を開始する際の最大ピッチ角を設定します。

ヨー角

顔認証開始時の最大ヨー角。

顔評価

必要に応じて顔評価を設定してください。

1:1マッチング閾値

1対1照合モードでの認証時の照合閾値を設定します。値が大きいほど誤認率は低くなりますが、誤拒否率は高くなります。

1:Nマッチング閾値

1:Nマッチングモードによる認証時のマッチング閾値を設定します。値が大きいほど誤認率は低くなりますが、誤拒否率は高くなります。

顔認識タイムアウト値

顔認識時のタイムアウト値を設定します。顔認識時間が設定値を超えると、システムが警告を表示します。

マスク着用顔検出

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画像を認識します。マスク着用顔の1対N照合閾値、ECOモード、および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、ドアは開きます。

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。

マスク着用時の顔と顔（1:1）

マスク着用時の顔認証において、1対1照合モードでの一致判定閾値を設定します。値が大きいほど誤認率は低くなりますが、誤拒否率は高くなります。

マスク着用時の顔認証 1:N マッチング閾値

マスク着用時の顔認証において、1:N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は低くなりますが、誤拒否率は高くなります。

ECOモード

ECOモードを有効にすると、デバイスは低照度または暗所環境において赤外線カメラを使用して顔認証を行います。ECOモードしきい値、ECOモード（1:N）、ECOモード（1:1）を設定できます。

ECOモードしきい値

ECOモードのしきい値を設定します。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。

ECOモード（1:1）

ECOモード1:1照合モードによる認証時の照合しきい値を設定します。値が大きいほど誤認率が低くなり、誤拒否率が高くなります。

ECOモード（1:N）

ECOモード1:Nマッチングモードによる認証時のマッチングしきい値を設定します。値が大きいほど誤認率が低くなり、誤拒否率が大きくなります。

マスク着用時顔認証＆顔認証（1:1 ECO）

ECOモード1:1照合モードでマスク着用時の顔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。

マスク着用時の顔認証 1対Nマッチングしきい値（ECOモード）

ECOモードの1:N照合モードでマスク着用時の顔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は低くなりますが、誤拒否率は高くなります。

指紋セキュリティレベル

指紋セキュリティレベルを選択します。

セキュリティレベルが高いほど、誤認率（FAR）は低くなります。

認識エリアの設定

設定→スマート→エリア設定 をクリックします。
ライブ映像内の黄色い枠をドラッグして認識領域を調整してください。領域内の顔のみがシステムによって認識されます。
領域設定、**マージン（左）**、**マージン（右）**、**マージン（上）**、**マージン（下）**を任意に設定してください。
設定を保存するには「**保存**」をクリックしてください。
「  」または「  」をクリックして、動画を録画または静止画を撮影します。

9.5.22 通知の公開設定

デバイスのテーマを設定できます。

設定→テーマ→メディアデータベース をクリックし、**[+追加]** をクリックして、メディアライブラリに素材をアップロードします。

設定→テーマ→テーマ をクリックします。

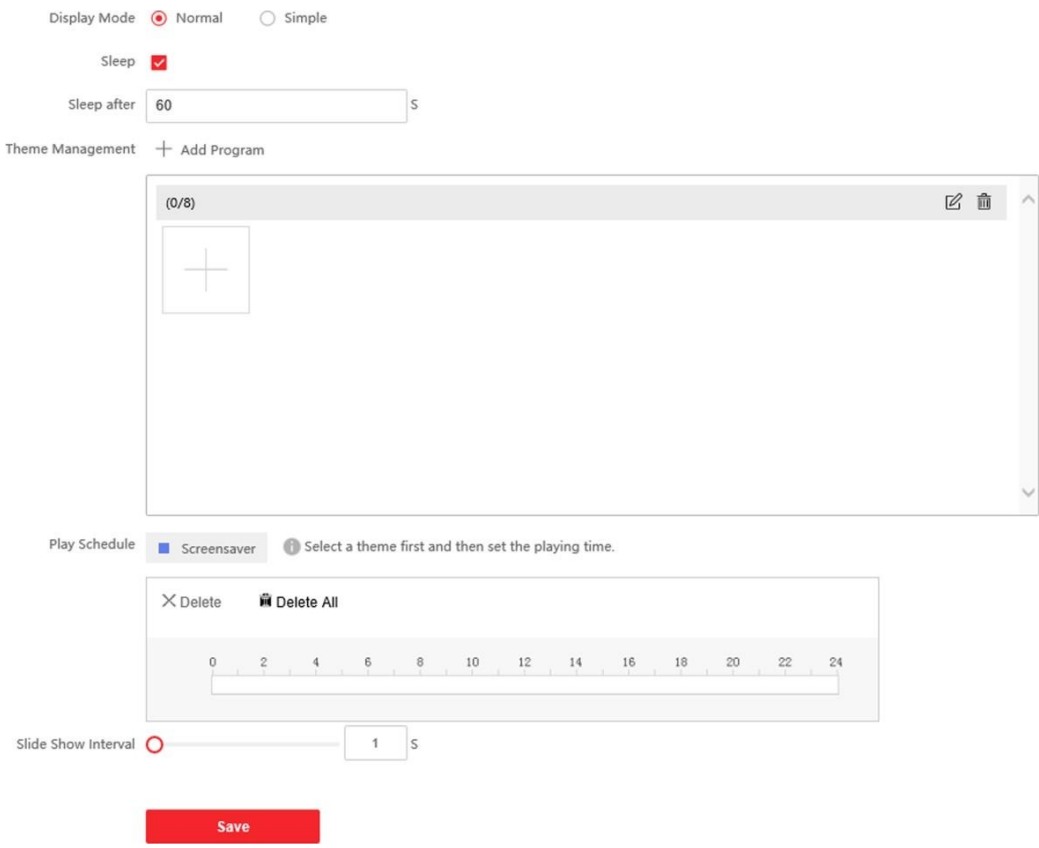


図 9-16 テーマページ

表示モード

デバイス認証の表示テーマを選択できます。**表示モード**は「**シンプル**」または「**通常**」から選択できます。**「シンプル」**を選択すると、名前、ID、顔写真の情報は表示されません。

スリープ

スリープを有効にすると、設定されたスリープ時間内に操作がない場合、デバイスはスリープモードに入ります。

テーマ管理

フレーム内の**「+ プログラムを追加」**をクリックし、ローカルPCからスクリーンセーバー画像をアップロードできます。

注意

現時点では、追加できるテーマは1つだけです。

プレイスケジュール

テーマを作成したら、そのテーマを選択し、タイムライン上にスケジュールを描いてテーマの再生スケジュールを設定できます。

描画したスケジュールを選択すると、正確な開始時間と終了時間を編集できます。

描画されたスケジュールを選択し、「**削除**」または「**すべて削除**」をクリックすると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間隔を設定します。設定した間隔で画像が切り替わります。

第10章クライアントソフトウェアの設定

10.1 クライアントソフトウェアの設定フロー

以下のフロー図に従ってクライアントソフトウェアを設定してください。

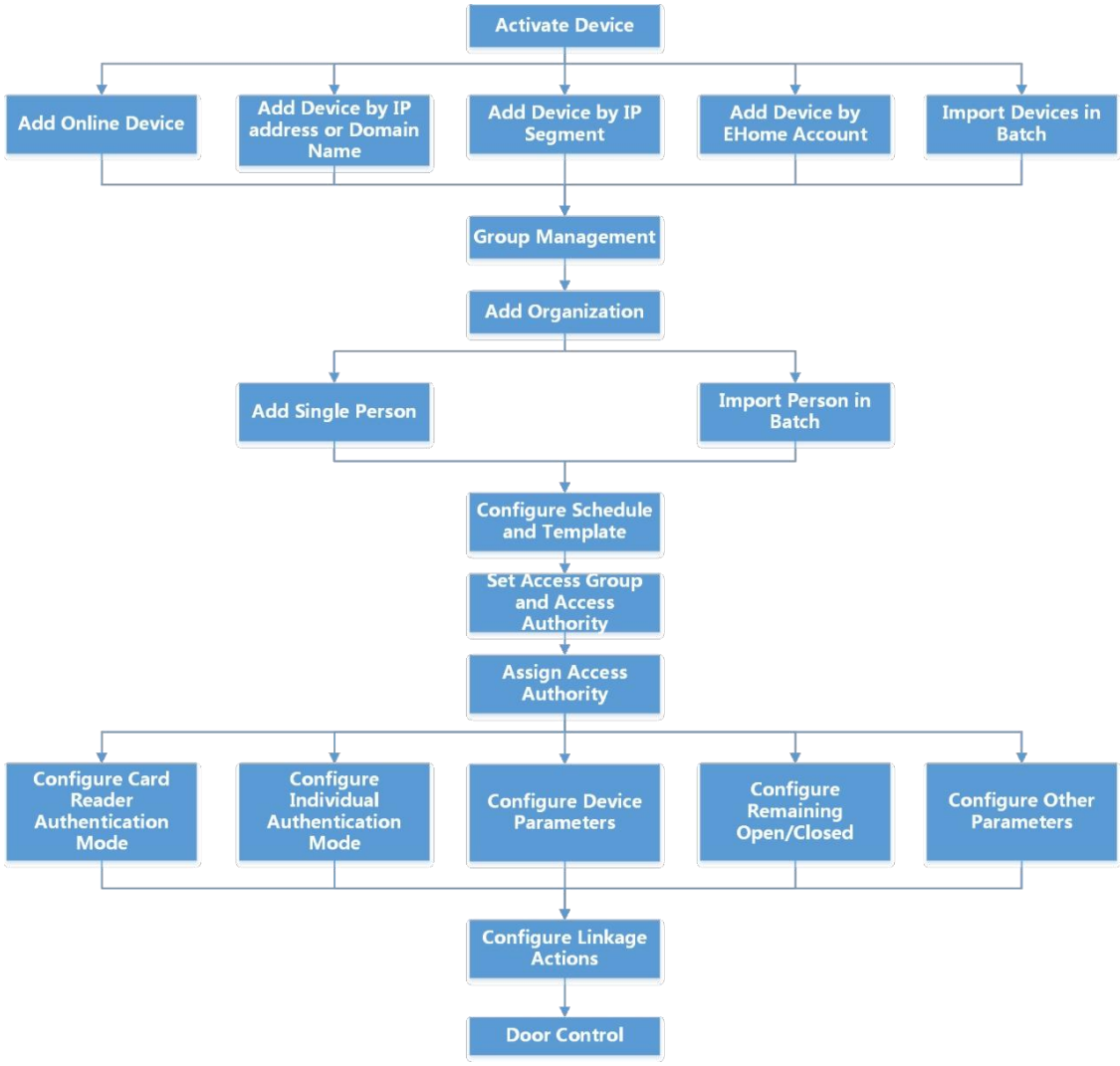


図10-1 クライアントソフトウェア設定フロー図

10.2 デバイス管理

クライアントは、アクセス制御装置およびビデオインターホン装置の管理をサポートします。

例

クライアントにアクセス制御デバイスを追加すると、入退室管理や勤怠管理が可能になります。また、室内機やドアステーションとのビデオインターホン機能も利用できます。

10.2.1 デバイスの追加

クライアントは、IP/ドメイン、IPセグメント、EHomeプロトコルによる3つのデバイス追加モードを提供します。また、追加するデバイスが大量にある場合、複数のデバイスを一括でインポートすることもサポートしています。

IPアドレスまたはドメイン名によるデバイス追加

追加するデバイスのIPアドレスまたはドメイン名をご存知の場合は、IPアドレス（またはドメイン名）、ユーザー名、パスワードなどを指定してクライアントにデバイスを追加できます。

手順

1. デバイス管理モジュールに入ります。
2. 右パネル上部の**「デバイス」**タブをクリックします。
   追加されたデバイスは右パネルに表示されます。
3. **[追加]** をクリックして追加ウィンドウを開き、追加モードとして **[IP/ドメイン]** を選択します。
4. 必要な情報を入力します。

   名前

   デバイスにわかりやすい名前を付けます。例えば、デバイスの場所や特徴を示す愛称を使用できます。

   アドレス

   デバイスのIPアドレスまたはドメイン名。

   ポート

   追加するデバイスは同じポート番号を共有します。デフォルト値は***80***00です。

   ユーザー名

   デバイスのユーザー名を入力します。デフォルトのユーザー名は ***admin*** です。

   パスワード

   デバイスのパスワードを入力してください。

   注意

   デバイスのパスワード強度を自動的に確認できます。製品のセキュリティ強化のため、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）への変更を強く推奨します。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お勧めします。月次または週次での変更により、製品の保護がより強化されます。

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勧めします。月次または週次での変更により、製品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構成は、設置業者および / またはエンドユーザーの責任となります。

5. **オプション：**セキュリティ保護のため、TLS（Transport Layer Security）プロトコルを使用した伝送暗号化を有効にするには、**「伝送暗号化（TLS）」**にチェックを入れてください。

注記

- この機能は、デバイスがサポートしている必要があります。
- 証明書検証を有効にしている場合は、セキュリティ強化のため、**[証明書ディレクトリを開く]**をクリックしてデフォルトフォルダを開き、デバイスからエクスポートした証明書ファイルをこのデフォルトディレクトリにコピーしてください。証明書検証の有効化に関する詳細は、を参照してください。
- ウェブブラウザを使用してデバイスにログインし、証明書ファイルを取得できます。

6. デバイスをクライアントに追加後、**[時刻を同期]**にチェックを入れると、クライアントを実行しているPCとデバイスの時刻を同期できます。

7. **オプション：「グループにインポート」**をチェックすると、デバイス名でグループが作成され、デバイスの全チャンネルがこのグループにインポートされます。

例

アクセス制御デバイスについては、そのアクセスポイント、警報入力/出力、およびエンコーディングチャネル（存在する場合）がこのグループにインポートされます。

8. デバイスの追加を完了します。

- **[追加]**をクリックしてデバイスを追加し、デバイス一覧ページに戻ります。
- **[追加] および [新規]** をクリックして設定を保存し、他のデバイスの追加を続行します。

デバイスの一括インポート

あらかじめ定義された CSV ファイルにデバイスパラメータを入力することで、複数のデバイスをクライアントに一括で追加することができます。

手順

1. デバイス管理モジュールに入ります。

2. 右パネル上部の**「デバイス」**タブをクリックします。

3. **「追加」**をクリックして追加ウィンドウを開き、追加モードとして「**一括インポート」**を選択します。

4. **エクスポートテンプレート**をクリックし、事前定義されたテンプレート（CSVファイル）をPCに保存します。

5. エクスポートしたテンプレートファイルを開き、追加するデバイスの必要な情報を対応する列に入力します。

注記

必須フィールドの詳細については、テンプレートの説明を参照してください。

追加モード

0、***1***、または***2***を入力してください。

アドレス

デバイスのアドレスを編集します。

ポート

デバイスのポート番号を入力してください。デフォルトのポート番号は ***8000*** です。

ユーザー名

デバイスのユーザー名を入力します。デフォルトのユーザー名は ***admin*** です。

パスワード

デバイスのパスワードを入力してください。

注意

デバイスのパスワード強度を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（大文字、小文字、数字、特殊文字の少なくとも3種類を含む8文字以上）に変更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変更により、製品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構成は、設置者および / またはエンドユーザーの責任です。

グループへのインポート

デバイス名でグループを作成するには***1***を入力してください。デフォルトでは、デバイスの全チャンネルが対応するグループにインポートされます。この機能を無効にするには***0***を入力してください。

6. 「 」をクリックし、テンプレートファイルを選択します。
7. **「Add」**をクリックしてデバイスをインポートします。

10.2.2 デバイスのパスワードをリセット

検出されたオンラインデバイスのパスワードを忘れた場合、クライアント経由でデバイスパスワードをリセットできます。

手順

1. デバイス管理ページを開く。
2. **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。

   同じサブネットを共有するすべてのオンラインデバイスがリストに表示されます。
3. リストからデバイスを選択し、操作列の「 」をクリックします。
4. デバイスのパスワードをリセットします。

   - **「生成」**をクリックしてQRコードウィンドウを表示し、**「ダウンロード」**をクリックしてQRコードをPCに保存します。

     QRコードを撮影してスマートフォンに保存することも可能です。撮影した画像を技術サポートまでお送りください。

注意

パスワードをリセットする以下の操作については、テクニカルサポートまでお問い合わせください。

注意

デバイスのパスワード強度を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（大文字、小文字、数字、特殊文字の少なくとも3種類を含む8文字以上）に変更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変更により、製品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構成は、設置者および / またはエンドユーザーの責任です。

10.2.3 追加デバイスの管理

デバイスリストにデバイスを追加した後、デバイスパラメータの編集、リモート設定、デバイスステータスの表示など、追加されたデバイスを管理できます。

表 10-1 追加されたデバイスの管理

デバイスの編集	をクリックすると、デバイス名、アドレス、ユーザー名、パスワードなどのデバイス情報を編集できます。
デバイスの削除	1 つ以上のデバイスをチェックし、**[Delete]** をクリックして選択したデバイスを削除します。
リモート設定	対応するデバイスのリモート設定を行うには、をクリックしてください。詳細はデバイスのユーザーマニュアルを参照してください。
デバイス状態の表示	をクリックすると、ドア番号やドア状態などのデバイス状態を確認できます。 **注意** デバイスによって、表示されるデバイス状態の情報が異なります。
オンラインユーザーを表示	をクリックすると、デバイスにアクセスしているオンラインユーザーの詳細（ユーザー名、ユーザータイプ、IP アドレス、ログイン時間など）を表示できます。
デバイス情報の更新	をクリックすると、最新のデバイス情報を取得できます。

10.3 グループ管理

クライアントは、追加されたリソースを異なるグループで管理するためのグループ機能を提供します。リソースの場所に応じて、リソースを異なるグループに分類できます。

例

例えば、1階には16個のドア、64個の警報入力、16個の警報出力が設置されています。これらのリソースを1つのグループ（名前：1階）に整理することで、管理を容易にできます。リソースをグループ単位で管理した後、ドアの状態を制御したり、デバイスのその他の操作を行ったりできます。

10.3.1 グループ追加

追加したデバイスを整理し、管理を容易にするためにグループを追加できます。

手順

1. デバイス管理モジュールに入ります。
2. **デバイス管理→グループ**をクリックして、グループ管理ページに入ります。
3. グループを作成します。
   - **グループ追加**をクリックし、任意のグループ名を入力します。
   - 「**デバイス名でグループを作成**」をクリックし、追加済みのデバイスを選択すると、選択したデバイス名で新しいグループが作成されます。

   注

   このデバイスのリソース（アラーム入力/出力、アクセスポイントなど）は、デフォルトでグループにインポートされます。

10.3.2 リソースをグループにインポート

デバイスリソース（アラーム入力/出力、アクセスポイントなど）を追加したグループに一括でインポートできます。

開始前に

デバイス管理用のグループを追加してください。詳細は「**グループの追加**」を参照してください。

手順

1. デバイス管理モジュールに入ります。
2. **デバイス管理→グループ**をクリックし、グループ管理ページに入ります。
3. グループ一覧からグループを選択し、リソースタイプを**アクセスポイント**、**アラーム入力**、**アラーム出力**などから選択します。
4. **インポート**をクリックします。
5. サムネイル/リスト表示でリソースのサムネイル/名前を選択してください。

注

クリックできます または をクリックすると、リソースの表示モードをサムネイル表示またはリスト表示に切り替えることができます。

6. **インポート**をクリックすると、選択したリソースをグループにインポートします。

10.4 人物管理

アクセス制御、ビデオインターホン、勤怠管理などの操作のために、システムに人物情報を追加できます。追加した人物の管理（一括でのカード発行、人物情報の一括インポート/エクスポートなど）が可能です。

10.4.1 組織の追加

組織を追加し、その組織に個人情報をインポートすることで、効果的な個人管理が可能です。追加した組織に対して上位組織を追加することもできます。

手順

1. **「人物」**モジュールを開きます。

2. 左側の列で親組織を選択し、左上隅の「**追加」**をクリックして組織を追加します。

3. 追加した組織の名前を作成します。

注記

最大10階層の組織を追加できます。

4. **オプション：**以下の操作を実行します。

組織の編集	追加された組織にマウスを合わせ、[ ]をクリックして名前を編集します。
組織の削除	追加された組織にマウスを合わせ、「 」をクリックして削除します。 **注記** • 組織を削除すると、下位組織も削除されます。 • 組織の下に追加された人物がいないことを確認してください。いない場合のみ、組織を削除できます。
サブ組織の人員を表示	「**サブ組織のメンバーを表示」**にチェックを入れ、組織を選択すると、その組織のサブ組織のメンバーが表示されます。

10.4.2 個人識別情報のインポートとエクスポート

複数人の情報と写真を一括でクライアントソフトウェアにインポートできます。同時に、個人情報や写真をエクスポートしてPCに保存することも可能です。

個人情報のインポート

あらかじめ定義されたテンプレート（CSV/Excelファイル）に複数人の情報を入力することで、クライアントへの情報を一括でインポートできます。

手順

1. 「人物」モジュールに入ります。
2. リストから追加済みの組織を選択するか、左上の**「追加」**をクリックして組織を追加し、選択します。
3. **「インポート」**をクリックしてインポートパネルを開きます。
4. インポートモードとして「**個人情報の選択」**を選択してください。
5. **「人物インポート用テンプレートをダウンロード」**をクリックしてテンプレートをダウンロードします。
6. ダウンロードしたテンプレートに個人情報を入力してください。

注意

- 人物が複数のカードを持っている場合は、カード番号をセミコロンで区切ってください。
- アスタリスクが付いている項目は必須です。
- デフォルトでは、採用日は現在の日付です。

7. ローカルPCから　　をクリックして、ローカルPCから人物情報のCSV/Excelファイルを選択してください。
8. **インポート**をクリックしてインポートを開始します。

注

- クライアントのデータベースに既に人物番号が存在する場合、インポート前に既存の情報を削除してください。
- 最大2,000人分の情報をインポートできます。

顔写真のインポート

追加した人物の顔写真をクライアントにインポートした後、追加した顔認識端末で写真内の人物を識別できます。必要に応じて、人物写真を1枚ずつインポートすることも、一度に複数の写真をインポートすることもできます。

開始前に

事前にクライアントに人物情報をインポートしておく必要があります。

手順

1. 人物モジュールに入ります。
2. リストから追加済みの組織を選択するか、左上の **[追加]** をクリックして組織を追加し、その後選択してください。
3. **「インポート」**をクリックしてインポートパネルを開き、「**顔」**にチェックを入れます。
4. **オプション：「デバイスによる検証」**を有効にして、クライアントで管理されている顔認識デバイスが写真内の顔を認識できるかどうかを確認します。
5. 「 ··· 」をクリックして顔写真ファイルを選択します。

注記

- 顔写真（のフォルダ）は ZIP 形式である必要があります。
- 各画像ファイルはJPG形式で、200KB以下である必要があります。
- 各画像ファイルは「人物ID_名前」という名前で命名してください。人物IDは、インポートする人物情報と同一である必要があります。

6. **インポート**をクリックしてインポートを開始します。

インポートの進捗状況と結果が表示されます。

人物情報のエクスポート

追加した人物の情報を CSV/Excel ファイルとしてローカル PC にエクスポートできます。

開始前に

組織に人物が追加されていることを確認してください。

手順

1. 人物モジュールに入ります。
2. **オプション**：リストから組織を選択します。

注記

組織を選択しない場合、すべての人の情報がエクスポートされます。

3. **エクスポート**をクリックしてエクスポートパネルを開きます。
4. エクスポートする内容として「**個人**」にチェックを入れます。
5. エクスポートしたい項目にチェックを入れてください。
6. **エクスポート**をクリックすると、エクスポートされたファイルが CSV/Excel ファイルとして PC に保存されます。

人物写真をエクスポート

追加した人物の顔写真ファイルをエクスポートし、PCに保存できます。

開始前に

組織に人物とその顔写真を追加済みであることを確認してください。

手順

1. 人物モジュールに入ります。
2. **オプション**：リストから組織を選択します。

注

組織を選択しない場合、全人物の顔写真がエクスポートされます。

3. **エクスポート**をクリックしてエクスポートパネルを開き、エクスポートするコンテンツとして「**顔**」を選択します。
4. **エクスポート**をクリックしてエクスポートを開始します。

注意

- エクスポートされたファイルはZIP形式です。
- エクスポートされた顔写真は「Person ID_Name_0」（「0」は正面顔）という名前で保存されます。

10.4.3 アクセス制御デバイスから人物情報を取得

追加したアクセス制御デバイスに人物情報（人物の詳細、指紋、発行済みカード情報など）が設定されている場合、そのデバイスから人物情報を取得し、クライアントにインポートしてさらに操作することができます。

手順

注

- デバイスに保存されている人物名が空の場合、クライアントへのインポート後、人物名は発行済みカード番号で埋まります。
- デバイスに保存されているカード番号または人物ID（従業員ID）がクライアントデータベースに既に存在する場合、このカード番号または人物IDを持つ人物はクライアントにインポートされません。

1. **人物**モジュールに入ります。
2. 個人をインポートする組織を選択します。
3. **デバイスから取得**をクリックします。
4. 追加されたアクセス制御デバイスまたは登録ステーションをドロップダウンリストから選択します。

   注記

   登録ステーションを選択する場合は、**[ログイン]**をクリックし、デバイスのIPアドレス、ポート番号、ユーザー名、パスワードを設定する必要があります。
5. **「インポート」**をクリックして、クライアントへの人物情報のインポートを開始します。

   注意

   最大2,000人の人物と5,000枚のカードをインポートできます。

   個人詳細、指紋情報（設定されている場合）、および関連付けられたカード（設定されている場合）を含む個人情報が、選択した組織にインポートされます。

10.4.4 個人へのカードの一括発行

クライアントは、複数の個人に一括でカードを発行する便利な方法を提供します。

手順

1. **「人物」**モジュールに入ります。
2. **「カードの一括発行」**をクリックします。

   カードが発行されていない追加された人物はすべて右パネルに表示されます。

3. **オプション：**入力ボックスにキーワード（名前または人物ID）を入力し、カード発行が必要な人物を絞り込みます。
4. **オプション：設定**をクリックしてカード発行パラメータを設定します。詳細は**ローカルモードによるカード発行**を参照してください。
5. **初期化**をクリックすると、カード登録ステーションまたはカードリーダーが初期化され、カード発行の準備が整います。
6. **カード番号の**欄をクリックし、カード番号を入力してください。
   - カードをカード登録ステーションに置きます。
   - カードリーダーでカードをスワイプしてください。
   - カード番号を手動で入力し、**Enter**キーを押します。リストに記載されている人物にカードが発行されます。

10.4.5 カード紛失の報告

カード紛失の場合、カード紛失を報告すると、そのカードに関連するアクセス権限が無効になります。

手順

1. **「担当者」**モジュールに入ります。
2. カード紛失を報告したい人物を選択し、「**編集」**をクリックして「人物編集」ウィンドウを開きます。
3. **Credential → Card** パネルで、追加されたカード上の「  」をクリックし、このカードを紛失カードとして設定します。
   カード紛失を報告すると、このカードのアクセス権限は無効化され、使用できなくなります。紛失カードを所持している他の人が、このカードをスワイプしてもドアにアクセスできなくなります。
4. **オプション：**紛失したカードが見つかった場合、「  」をクリックして紛失処理を解除できます。
   カード紛失をキャンセルした後、当該人物のアクセス権限は有効かつ有効な状態となります。
5. 紛失したカードが1つのアクセスグループに追加されており、そのアクセスグループが既にデバイスに適用されている場合、カード紛失の報告または紛失登録解除後、変更をデバイスに適用するよう通知するウィンドウが表示されます。デバイスへの適用後、これらの変更はデバイス上で有効になります。

10.4.6 カード発行パラメータの設定

クライアントは、カード番号を読み取るために2つのモードを提供します：カード登録ステーション経由、またはアクセス制御装置のカードリーダー経由です。 カード登録ステーションが利用可能な場合は、USBインターフェースまたはCOMポートでクライアントを実行しているPCに接続し、カードをカード登録ステーションに置いてカード番号を読み取ります。利用できない場合は、追加したアクセス制御装置のカードリーダーでカードをスワイプしてカード番号を取得することもできます。結果として、1人にカードを発行する前に、発行モードや関連パラメータを含むカード発行パラメータを設定する必要があります。

1人にカードを追加する場合、「**設定」**をクリックしてカード発行設定ウィンドウを開きます。

ローカルモード：カード登録ステーションによるカード発行

カード登録ステーションをクライアントを実行しているPCに接続します。カードをカード登録ステーションに置くことでカード番号を取得できます。

カード登録ステーション

接続したカード登録ステーションのモデルを選択してください

注記

現在、サポートされているカード登録ステーションのモデルは、DS-K1F100-D8、DS-K1F100-M、DS-K1F100-D8E、および DS-K1F180-D8E です。

カードタイプ

このフィールドは、モデルが DS-K1F100-D8E または DS-K1F180-D8E の場合にのみ使用できます。実際のカードタイプに応じて、カードタイプを EM カードまたは IC カードとして選択してください。

シリアルポート

この項目は、モデルが DS-K1F100-M の場合にのみ使用できます。カード登録ステーションが接続する COM を選択してください。

ブザー

カード番号が正常に読み取られた際のブザー音のオン/オフ設定

カード番号タイプ

実際のニーズに応じてカード番号のタイプを選択してください。

M1 カード暗号化

このフィールドは、モデルが DS-K1F100-D8、DS-K1F100-D8E、または DS-K1F180-D8E の場合にのみ使用できます。

カードが M1 カードの場合、M1 カード暗号化機能を有効にする必要がある場合は、この機能を有効にして、暗号化するカードのセクターを選択してください。

リモートモード：カードリーダーによるカード発行

クライアントに追加されたアクセス制御デバイスを選択し、そのカードリーダーでカードをスワイプしてカード番号を読み取ります。

10.5 スケジュールとテンプレートの設定

休日や週単位のスケジュールを含むテンプレートを設定できます。テンプレート設定後、アクセスグループ設定時にこの設定済みテンプレートを適用することで、アクセスグループがテンプレートの有効時間枠内で機能するようになります。

注意

アクセスグループの設定については、「**アクセス権限を人に割り当てるためのアクセスグループの設定**」を参照してください。

10.5.1 休日を追加

休日を作成し、開始日、終了日、および休日の期間（1日単位）を設定できます。

手順

注意

ソフトウェアシステムでは最大64件の休日を追加できます。

1. **アクセス制御→ スケジュール→ 休日**をクリックして休日ページに入ります。
2. 左パネルの「**追加**」をクリックします。
3. 休日の名前を作成します。
4. **任意**：備考欄にこの休日の説明や通知事項を入力します。
5. 休暇リストに休暇期間を追加し、休暇期間を設定します。

   注記

   1 つの休暇に最大 16 個の休暇期間を追加できます。

   1) 休暇リストフィールドの［**追加** ］をクリックします。
   2) カーソルをドラッグして期間を描画します。これにより、設定されたアクセスグループがその期間中に有効になります。

      注記

      1 つの休日期間に最大 8 つの時間枠を設定できます。

   3) **オプション**：以下の操作で時間範囲を編集できます。
      - カーソルを時間範囲に移動し、カーソルが に変わったら、タイムラインバー上の時間範囲を希望の位置までドラッグします。
      - 時間範囲をクリックし、表示されるダイアログで開始/終了時間を直接編集します。
      - カーソルを時間範囲の開始点または終了点に移動し、カーソルが に変わったらドラッグして時間範囲を延長または短縮します。
   4) **オプション**：削除する時間範囲を選択し、操作列の「 」をクリックして選択した時間範囲を削除します。
   5) **オプション: [**操作] 列の 操作列のをクリックして、タイムバー上のすべての時間範囲をクリアします。
   6) **オプション: [**操作] 列 操作列のをクリックして、休日リストから追加した休日期間を削除します。
6. **[保存]** をクリックします。

10.5.2 テンプレートの追加

テンプレートには週スケジュールと休日が含まれます。週スケジュールを設定し、異なる個人またはグループに対してアクセス権限の時間範囲を割り当てることができます。また、テンプレートに追加した休日を選択することもできます。

手順

注記

ソフトウェアシステムでは最大255個のテンプレートを追加できます。

1. **アクセス制御→スケジュール→テンプレート**をクリックして、テンプレートページに入ります。

注記

デフォルトでは「終日許可」と「終日拒否」の 2 つのテンプレートが用意されており、これらは編集も削除もできません。

終日許可

アクセス許可は週の毎日有効であり、休日設定はありません。

終日拒否

アクセス許可は週のすべての日に無効であり、休日設定はありません。

2. 左パネルの「**追加**」をクリックして新しいテンプレートを作成します。

3. テンプレートの名前を作成します。

4. 備考欄にこのテンプレートの説明や通知事項を入力してください。

5. 週スケジュールを編集してテンプレートに適用します。

1) 下部パネルの「**週間スケジュール**」タブをクリックします。

2) 曜日を選択し、タイムラインバー上に時間枠を描画します。

注記

週スケジュールでは、各曜日に最大8つの時間枠を設定できます。

3) **オプション：**時間枠を編集するには、以下の操作を行います。

- カーソルを時間枠に移動し、カーソルが  に変わったタイミングで、タイムラインバー上の時間枠を希望の位置までドラッグします。
- 時間枠をクリックし、表示されるダイアログで開始時間/終了時間を直接編集します。
- カーソルを時間区間の開始点または終了点に移動し、カーソルが  に変わった状態でドラッグすると、時間区間を延長または短縮できます。

4) 上記の2つの手順を繰り返して、他の曜日にさらに時間枠を描画します。

6. 休日を追加してテンプレートに適用します。

注

1 つのテンプレートに最大 4 つの休日を追加できます。

1) **「休日」**タブをクリックします。

2) 左側のリストから休日を選択すると、右側のパネルの選択済みリストに追加されます。

3) **オプション：[追加]**をクリックすると新しい休日を追加できます。

注意

休日の追加に関する詳細は、**「休日の追加」**を参照してください。

4) **オプション：**右リストで選択済みの休日を選択し、「 ✕ 」をクリックすると選択した休日を削除できます。または「**Clear**」をクリックすると右リストの選択済み休日をすべてクリアできます。

7. 設定を保存してテンプレートの追加を完了するには、**[保存]**をクリックします。

10.6 アクセスグループを設定して人物へのアクセス権限を割り当てる

人物を追加し、その認証情報を設定した後、どのドアにどの人がアクセスできるかを定義するアクセスグループを作成できます。その後、アクセスグループをアクセス制御デバイスに適用して有効にします。

開始前に

- クライアントに人物を追加する。
- クライアントにアクセス制御デバイスを追加し、アクセスポイントをグループ化します。詳細は「**グループ管理**」を参照してください。
- テンプレートを追加する。

手順

アクセスグループ設定を変更した場合、変更を有効にするにはデバイスに再度アクセスグループを適用する必要があります。アクセスグループ変更には、テンプレートの変更、アクセスグループ設定、個人のアクセスグループ設定、および関連する個人詳細（カード番号、指紋、顔写真、カード番号と指紋の紐付け、カードパスワード、カード有効期限など）の変更が含まれます。

1. **アクセス制御→権限設定→アクセスグループ**をクリックし、アクセスグループ画面に入ります。

2. **「追加」**をクリックして追加ウィンドウを開きます。

3. **名前**テキストフィールドで、アクセスグループに任意の名前を付けます。

4. アクセスグループ用のテンプレートを選択します。

注記

アクセスグループ設定の前にテンプレートを設定する必要があります。詳細は**「スケジュールとテンプレートの設定」**を参照してください。

5. 「対象者選択」フィールドの左リストから、アクセス権限を割り当てる対象者を選択します。

6. 「アクセスポイントの選択」フィールドの左リストから、選択した人物がアクセスするドア、ドアステーション、またはフロアを選択します。

7. **保存**をクリックします。

インターフェースの右側で、選択した人物とアクセスポイントを確認できます。

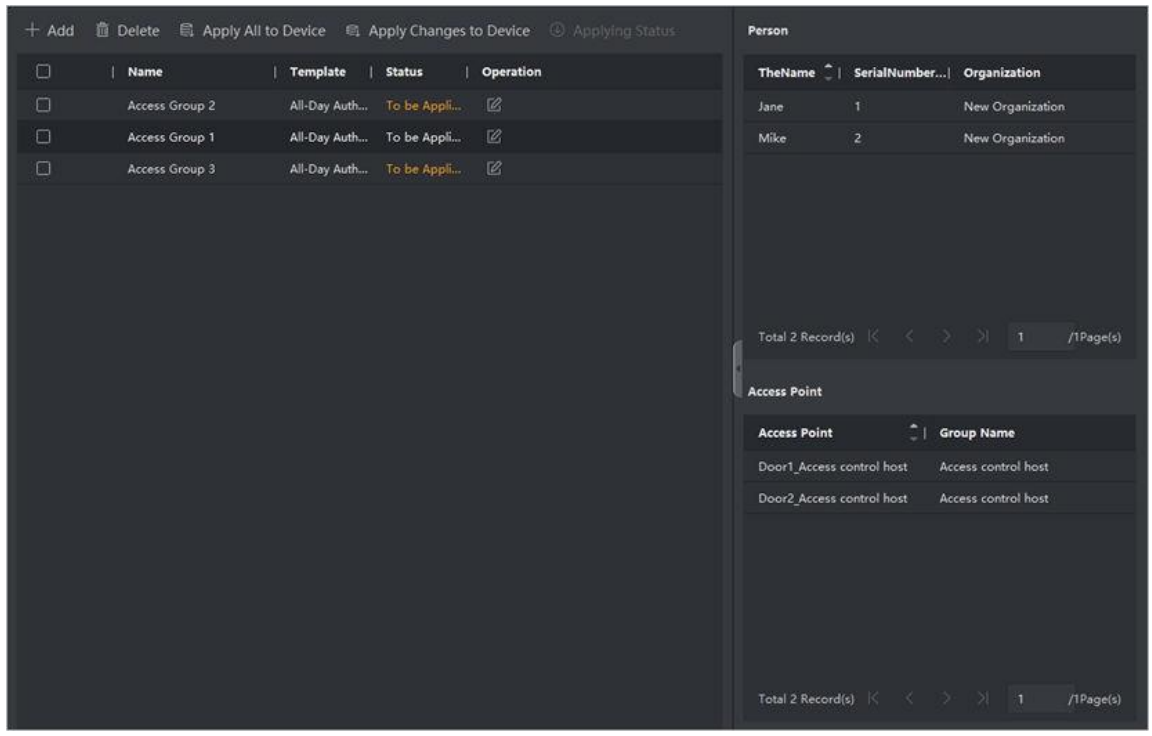


図 10-2 選択した人物とアクセスポイントの表示

8. アクセスグループを追加した後、アクセス制御デバイスに適用して有効にする必要があります。

1) アクセス制御装置に適用するアクセスグループを選択します。

2) **「すべてのデバイスに適用」**をクリックすると、選択したアクセスグループをすべてアクセス制御デバイスまたはドアステーションに適用し始めます。

3) **「デバイスにすべて適用」**または「**デバイスに変更を適用」**をクリックします。**デバイスにすべて適用**

この操作により、選択したデバイスの既存のアクセスグループはすべてクリアされ、新しいアクセスグループがデバイスに適用されます。

デバイスへの変更の適用

この操作では、選択したデバイスの既存のアクセスグループは削除されず、選択したアクセスグループの変更部分のみがデバイスに適用されます。

4) 適用状況は「ステータス」列で確認するか、「**適用状況」**をクリックして適用されたアクセスグループをすべて表示します。

注

適用結果をフィルタリングするには、**[失敗のみ表示]** をチェックしてください。

適用されたアクセスグループで選択された人物は、リンクされたカードまたは指紋を使用して、選択されたドア/ドアステーションに出入りする権限を持ちます。

9. オプション：必要に応じて、 をクリックしてアクセスグループを編集します。

注意

担当者のアクセス情報またはその他の関連情報を変更すると、クライアントの右隅に「**適用されるアクセスグループ」というプロンプト**が表示されます。

プロンプトをクリックすると、変更したデータをデバイスに適用できます。**今すぐ適用または後で適用**を選択できます。

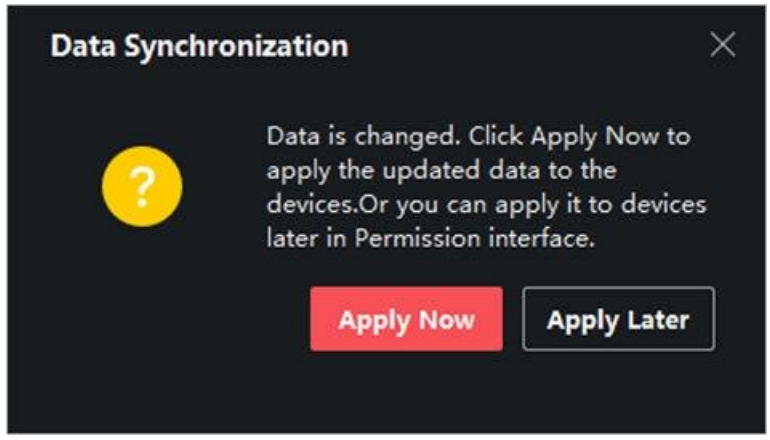


図 10-3 データ同期

10.7 詳細機能の設定

アクセス制御の高度な機能を設定し、様々な状況における特別な要件に対応できます。

注

- カード関連機能（アクセス制御カードの種類）については、カード追加時にアクセスグループが適用されたカードのみが表示されます。
- 高度な機能はデバイスがサポートしている必要があります。
- 高度な機能にカーソルを合わせ、[ ] をクリックして、表示する高度な機能をカスタマイズします。

10.7.1 デバイスパラメータの設定

アクセス制御デバイスを追加した後、アクセス制御デバイスおよびアクセス制御ポイントのパラメータを設定できます。

アクセス制御デバイスのパラメータ設定

アクセス制御デバイスを追加した後、そのパラメータを設定できます。これには、画像へのユーザー情報の重ね書き、撮影後の画像アップロード、撮影済み画像の保存などが含まれます。

手順

1. **アクセス制御→ 高度な機能→ デバイスパラメータ** をクリックします。

注意

詳細機能リストに「デバイスパラメータ」がある場合は、その詳細機能にカーソルを合わせ、 をクリックして表示するデバイスパラメータを選択します。

2. 右ページにパラメータを表示するアクセスデバイスを選択します。
3. 対応する機能を有効にするには、スイッチをONに切り替えてください。

注記

- 表示されるパラメータは、アクセス制御デバイスによって異なる場合があります。
- 以下のパラメータの一部は基本情報ページに表示されません。編集するには「**詳細**」をクリックしてください。

音声プロンプト

この機能を有効にすると、デバイスで音声プロンプトが有効になります。デバイス操作時に音声プロンプトが聞こえます。

リンク後、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自動的にシステムにアップロードします。

リンク撮影後の画像保存

この機能を有効にすると、接続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。

顔認識モード通常モード

カメラで通常通り顔を認識します。

ディープモード

通常モードよりも広い範囲の人物を認識できます。より複雑な環境に適しています。

NFCカード対応

この機能を有効にすると、デバイスはNFCカードを認識できます。デバイスにNFCカードを提示できます。

M1カード有効化

この機能を有効にすると、デバイスはM1カードを認識できます。デバイスにM1カードを提示できます。

EMカード有効化

この機能を有効にすると、デバイスはEMカードを認識できます。デバイスにEMカードを提示できます。

注意

周辺機器のカードリーダーがEMカードの提示をサポートしている場合、EMカード機能の有効化/無効化もサポートされます。

4. **[OK]**をクリックします。
5. **オプション: [コピー先]**をクリックし、ページ内のパラメータを選択したアクセス制御デバイスにコピーします。

ドア/エレベーターのパラメータ設定

アクセス制御デバイスを追加した後、そのアクセスポイント（ドアまたはフロア）のパラメータを設定できます。

開始前に

クライアントにアクセス制御デバイスを追加する。

手順

1. **アクセス制御→ 高度な機能→ デバイスパラメータ** をクリックします。
2. 左パネルでアクセス制御デバイスを選択し、 をクリックすると、選択したデバイスのドアまたはフロアが表示されます。
3. ドアまたはフロアを選択すると、右ページにそのパラメータが表示されます。
4. ドアまたはフロアのパラメータを編集します。

注記

- 表示されるパラメータは、アクセス制御デバイスによって異なる場合があります。
- 以下のパラメータの一部は、基本情報ページには表示されません。「**詳細**」をクリックしてパラメータを編集してください。

カードリーダー名

カードリーダーの名前を任意に編集してください。

ドアコンタクト

ドアセンサーは「閉状態を維持」または「開状態を維持」に設定できます。通常は「閉状態を維持」です。

退出ボタンタイプ

退出ボタンは閉状態継続または開状態継続に設定できます。通常は開状態継続です。

ドアロック時間

通常カードのスワイプとリレー動作後、ドアロックのタイマーが作動します。

延長開放時間

延長アクセス権限を持つ者がカードをスワイプした後、適切な遅延を経てドアコンタクトを有効化できます。

ドア開放時間超過アラーム

設定された時間内にドアが閉じられなかった場合にアラームが作動します。設定値が0の場合、アラームは作動しません。

ドア閉時ロック

ドアロック時間未満でも閉めた時点でドアをロックできます。

緊急コード

緊急事態発生時、緊急コードを入力することでドアを開錠できます。同時にクライアントは緊急事態を報告できます。

スーパーパスワード

特定の人物はスーパーパスワードを入力することでドアを開けることができる。

解除コード

カードリーダーのブザーを停止するために使用できる解除コードを作成します（キーパッドで解除コードを入力）。

注記

- 脅迫コード、スーパーコード、解除コードは異なるものにする必要があります。
- 脅迫コード、スーパーパスワード、および解除コードは、認証パスワードとは異なるものにする必要があります。
- 緊急コード、スーパーパスワード、および解除コードの長さはデバイスによって異なりますが、通常は4桁から8桁で構成される必要があります。

5. **OK**をクリックしてください。

6. **オプション：** **[コピー先]** をクリックし、ページ内のパラメータを選択したドア / フロアにコピーします。

注記

ドアまたはフロアのステータス継続時間設定も、選択したドア/フロアにコピーされます。

カードリーダーのパラメータ設定

アクセス制御デバイスを追加した後、そのカードリーダーのパラメータを設定できます。

開始前に

クライアントにアクセス制御デバイスを追加する。

手順

1. **アクセス制御→ 高度な機能→ デバイスパラメータ** をクリックします。

2. 左側のデバイス一覧で「 」をクリックしてドアを展開し、カードリーダーを選択すると、右側でカードリーダーのパラメータを編集できます。

3. 基本情報ページでカードリーダーの基本パラメータを編集します。

注意

- 表示されるパラメータはアクセス制御デバイスによって異なる場合があります。以下に一部パラメータを列挙します。詳細はデバイスのユーザーマニュアルを参照してください。
- 以下のパラメータの一部は基本情報ページに表示されていません。編集するには「**詳細**」をクリックしてください。

名前

カードリーダー名を任意に編集してください。

OK LED 極性/エラー LED 極性/ブザー極性

カードリーダーのパラメータに応じて、メインボードの OK LED 極性/エラー LED 極性/ブザー LED 極性を設定します。通常、デフォルト設定を採用します。

最小カードスワイプ間隔

同一カードのカードスワイプ間隔が設定値未満の場合、カードスワイプは無効となります。0～255の範囲で設定可能です。

パスワード入力時の最大間隔

カードリーダーでパスワードを入力する際、2桁の数字を押す間隔が設定値より長い場合、以前に押した数字は自動的にクリアされます。

最大失敗試行回数アラーム

カード読み取り試行回数が設定値に達した際にアラームを通知する機能を有効にします。

カード読み取り失敗の最大回数

カード読み取りの最大失敗回数を設定します。

改ざん検知

カードリーダーの改ざん検知を有効にします。

コントローラとの通信間隔

アクセス制御装置が設定時間を超えてカードリーダーと接続できない場合、カードリーダーは自動的にオフライン状態になります。

ブザー鳴動時間

カードリーダーのブザー音を鳴らす時間を設定します。設定可能な時間は0～5,999秒です。0は連続ブザーを意味します。

カードリーダータイプ/カードリーダー説明

カードリーダーのタイプと説明を取得します。これらは読み取り専用です。

指紋認証レベル

ドロップダウンリストから指紋認証レベルを選択します。

デフォルトカードリーダー認証モード

デフォルトのカードリーダー認証モードを表示します。

指紋容量

利用可能な指紋の最大数を確認する。

既存の指紋数

デバイス内に存在する指紋の数を表示します。

スコア

デバイスは、ヨー角、ピッチ角、瞳孔間距離に基づいて撮影された画像にスコアを付けます。スコアが設定値未満の場合、顔認識は失敗します。

顔認識タイムアウト値

認識時間が設定時間を超えた場合、デバイスが通知します。

顔認証間隔

認証時の連続した2回の顔認識の間隔。デフォルトは2秒です。

顔1対1照合のしきい値

1対1マッチングモードによる認証時の一致閾値を設定します。値が大きいほど、認証時の誤認率は低くなりますが、誤拒否率は高くなります。

1:N セキュリティレベル

1:Nマッチングモードによる認証時のセキュリティレベルを設定します。値が大きいほど、認証時の誤認率が低くなり、誤拒否率が大きくなります。

生体顔検出

生体顔検出機能を有効または無効にします。機能を有効にすると、デバイスは人物が生体であるかどうかを認識できます。

生体顔検出セキュリティレベル

ライブ顔検出機能を有効にした後、ライブ顔認証時に使用する照合セキュリティレベルを設定できます。

顔認証の最大失敗回数

生体顔検出の最大失敗回数を設定します。設定回数を超えて生体顔検出に失敗した場合、システムはユーザーの顔を5分間ロックします。同じユーザーは5分以内に偽の顔による認証を行うことはできません。5分以内に、ユーザーは本物の顔で連続して2回認証を行うことでロックを解除できます。

認証失敗時の顔ロック

生体顔検出機能を有効にした後、設定回数を超えて生体顔検出が失敗した場合、システムはユーザーの顔を5分間ロックします。同一ユーザーは5分以内に偽の顔による認証を行うことはできません。5分以内に、ユーザーは本物の顔で連続して2回認証を行うことでロックを解除できます。

アプリケーションモード

実際の環境に応じて、屋内モードまたはその他モードを選択できます。

4. **OK**をクリックします。

5. オプション：「コピー先」をクリックし、選択したカードリーダーにページ内のパラメータをコピーします。

警報出力のパラメータ設定

アクセス制御デバイスを追加した後、そのデバイスがアラーム出力にリンクしている場合は、パラメータを設定できます。

開始前に

クライアントにアクセス制御デバイスを追加し、そのデバイスがアラーム出力をサポートしていることを確認してください。

手順

1. アクセス制御→高度な機能→デバイスパラメータをクリックし、アクセス制御パラメータ設定ページに入ります。

2. 左側のデバイスリストで「 」をクリックしてドアを展開し、アラーム入力を選択すると、右側でアラーム入力のパラメータを編集できます。

3. 警報出力パラメータを設定します。

名前

カードリーダー名を任意に編集します。

アラーム出力アクティブ時間

アラーム出力は、トリガー後どのくらいの時間持続するか。

4. [OK]をクリックします。

5. オプション：右上隅のスイッチを**ON**に設定すると、警報出力が作動します。

10.7.2 デバイスパラメータの設定

アクセス制御デバイスを追加後、ネットワークパラメータなどの設定が可能です。

顔認証端末のパラメータ設定

顔認証端末については、顔画像データベース、QRコード認証などのパラメータを設定できます。

手順

注意事項

この機能はデバイスがサポートしている必要があります。

1. アクセス制御モジュールに入ります。

2. 左側のナビゲーションバーで、**[高度な機能] → [その他のパラメータ]** を選択します。

3. デバイスリストからアクセス制御デバイスを選択し、「**顔認証端末**」をクリックします。

4. パラメータを設定します。

注

表示されるこれらのパラメータは、デバイスモデルによって異なります。

COM

設定用の COM ポートを選択します。COM1 は RS-485 インターフェース、COM2 は RS-232 インターフェースを指します。

顔画像データベース

顔画像データベースとしてディープラーニングを選択してください。

QRコードによる認証

有効にすると、デバイスのカメラでQRコードをスキャンして認証できます。デフォルトではこの機能は無効です。

ブロックリスト認証

有効にすると、デバイスはアクセスを要求する人物をブロックリストに登録されている人物と比較します。

一致した場合（人物がブロックリストに登録されている場合）、アクセスは拒否され、デバイスはクライアントにアラームをアップロードします。

一致しない場合（人物がブロックリストにない場合）、アクセスが許可されます。

認証用顔写真の保存

有効にすると、認証時に撮影された顔写真が端末に保存されます。

MCUバージョン

デバイスのMCUバージョンを表示します。

5. **保存**をクリックします。

RS-485 パラメータの設定

ボーレート、データビット、ストップビット、パリティタイプ、フロー制御タイプ、通信モード、動作モード、接続モードなど、アクセス制御デバイスの RS-485 パラメータを設定できます。

手順

注

RS-485設定はデバイスがサポートしている必要があります。

1. アクセス制御モジュールに入ります。
2. 左側のナビゲーションバーで、**[詳細機能] → [その他のパラメータ]** を選択します。
3. デバイスリストからアクセス制御デバイスを選択し、**RS-485**をクリックしてRS-485設定ページに入ります。
4. RS-485パラメータを設定するには、ドロップダウンリストからシリアルポート番号を選択します。
5. シリアル番号、外部デバイス、認証センター、ボーレート、データビット、ストップビット、パリティタイプ、フロー制御タイプ、通信モード、動作モードをドロップダウンリストで設定します。

6. **保存**をクリックします。

- 設定したパラメータは自動的にデバイスに適用されます。
- 動作モードまたは接続モードを変更すると、デバイスは自動的に再起動します。

ウィーガンドパラメータの設定

アクセス制御デバイスのウィーガンドチャネルと通信モードを設定できます。

手順

注記

この機能はデバイスがサポートしている必要があります。

1. アクセス制御モジュールに入ります。

2. 左側のナビゲーションバーで、**[詳細機能] → [その他のパラメータ]** に移動します。

3. デバイスリストからアクセス制御デバイスを選択し、「**Wiegand**」をクリックして「Wiegand設定」ページに入ります。

4. スイッチをオンに設定して、デバイスのウィーガンド機能を有効にします。

5. ドロップダウンリストからウィーガンドチャンネル番号と通信モードを選択してください。

注意

通信方向を送信に設定した場合、**Wiegandモード**は**Wiegand** 26またはWiegand 34に設定する必要があります。

Wiegand 26 または **Wiegand 34** に設定する必要があります。

6. Wiegand機能を有効にするには、**[Wiegand 有効化]** をチェックします。

7. **保存**をクリックします。

- 設定したパラメータは自動的にデバイスに適用されます。
- 通信方向を変更した後、デバイスは自動的に再起動します。

M1カード暗号化を有効にする

M1カード暗号化は、認証のセキュリティレベルを向上させます。

手順

注記

この機能は、アクセス制御デバイスとカードリーダーの両方でサポートされている必要があります。

1. アクセス制御モジュールに入ります。

2. 左側のナビゲーションバーで、**[詳細機能] → [その他のパラメータ]** を選択します。

3. デバイスリストからアクセス制御デバイスを選択し、「**M1カード暗号化検証**」をクリックしてM1カード暗号化検証ページに入ります。

4. スイッチをオンに設定してM1カード暗号化機能を有効にします。

5. セクターIDを設定します。

注記

- セクター ID は 1 から 100 までの範囲です。
- デフォルトではセクター13が暗号化されています。セクター13の暗号化を推奨します。

6. 設定を保存するには、**[保存]**をクリックしてください。

10.8 ドア制御

監視モジュールでは、追加されたアクセス制御デバイスで管理されるドアのリアルタイム状態を確認できます。また、クライアントから遠隔でドアの開閉操作や、ドアを開いた状態 / 閉じた状態に維持するなどの制御が可能です。リアルタイムのアクセスイベントがこのモジュールに表示されます。アクセス詳細と人物詳細を確認できます。

注記

ドア制御権限を持つユーザーは、監視モジュールにアクセスしてドアを制御できます。権限のないユーザーには制御用アイコンが表示されません。ユーザー権限の設定については、**人物管理**を参照してください。

10.8.1 ドア状態の制御

ドアの状態を制御できます。具体的には、ドアのロック解除、ドアのロック、ドアのロック解除状態の維持、ドアのロック状態の維持、すべてのドアのロック解除状態の維持などです。

操作前に

- 人物を追加し、指定した人物にアクセス権限を割り当てると、その人物はアクセスポイント（ドア）へのアクセス権限を取得します。詳細は「**人物管理**」および「**人物へのアクセス権限割り当てのためのアクセスグループ設定**」を参照してください。
- 操作ユーザーがアクセスポイント（ドア）の権限を持っていることを確認してください。詳細はを参照してください。

手順

1. **「監視」**をクリックして状態監視ページに入ります。

2. 右上隅でアクセスポイントグループを選択します。

注記

アクセスポイントグループの管理については、**グループ管理**を参照してください。選択した

アクセス制御グループのドアが表示されます。

3. ドアアイコンをクリックしてドアを選択するか、**Ctrlキー**を押しながら複数のドアを選択します。

注記

「すべてロック解除状態を維持」および「**すべてロック状態を維持」**の場合、この手順は無視してください。

4. ドアを制御するには、以下のボタンをクリックします。

開錠

ドアがロックされている場合、アンロックすると一度だけ開きます。開いている時間が経過すると、ドアは自動的に閉まりロックされます。

ロック

ドアがロックされていない場合は、ロックすると閉まります。アクセス権限を持つ者は認証情報でドアにアクセスできます。

開錠状態を維持

ドアは解錠状態（閉まっているか開いているかを問わず）になります。認証情報なしで全ての人がドアにアクセスできます。

常に施錠状態

ドアは閉まり、ロックされます。スーパーユーザーを除き、認証情報を持つ者であってもアクセスできません。

すべて開錠状態を維持

グループ内の全てのドアはロック解除されます（閉まっているか開いているかを問わず）。全ての人が認証情報なしでドアにアクセスできます。

すべて施錠状態を維持

グループ内の全てのドアは閉められ、ロックされます。スーパーユーザーを除き、認証情報を持つ者であってもドアにアクセスできません。

キャプチャ

手動で写真を撮影します。

注記

キャプチャボタンは、デバイスがキャプチャ機能をサポートしている場合に利用可能です。画像はクライアントを実行しているPCに保存されます。保存パスの設定については、クライアントソフトウェアのユーザーマニュアルの**「ファイル保存パスの設定」**を参照してください。

結果

操作が成功した場合、ドアのアイコンは操作に応じてリアルタイムで変化します。

10.8.2 リアルタイムアクセス記録の確認

カードスワイプ記録、顔認識記録、指紋照合記録などのアクセス記録がリアルタイムで表示されます。アクセス時に撮影された写真とともに、人物情報を閲覧することができます。

手順

1. **監視**をクリックし、右上のドロップダウンリストからグループを選択します。

   選択したグループのドアで発生したアクセス記録がリアルタイムで表示されます。カード番号、人物名、所属組織、イベント時間などの記録詳細を確認できます。

2. **オプション:** イベントの種類とステータスをチェックすると、該当するイベントが検出された場合にリストに表示されます。チェックされていない種類またはステータスのイベントはリストに表示されません。

3. **オプション:** [**最新のイベントを表示**] にチェックを入れると、最新のアクセス記録が選択され、記録リストの上部に表示されます。

4. **オプション：**イベントをクリックすると、アクセスされた人物の詳細（人物写真（撮影画像とプロフィール）、人物番号、人物名、組織、電話番号、連絡先住所など）を表示できます。

   注記
   キャプチャされた画像をダブルクリックすると、拡大して詳細を確認できます。

5. **オプション：**アクセスイベントテーブルの列名を右クリックし、実際の必要に応じて列を表示または非表示にします。

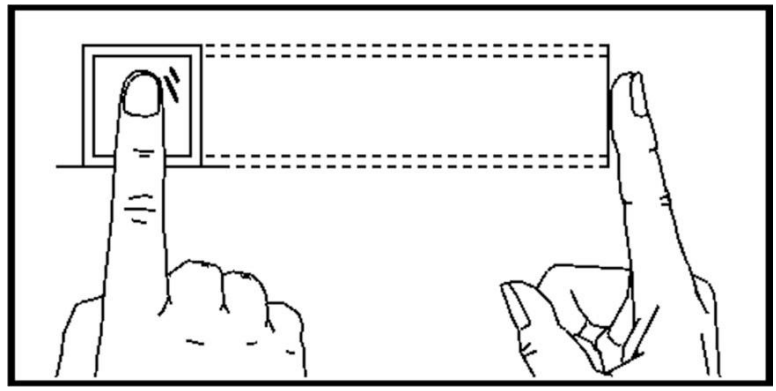
付録A. 指紋スキャンのコツ

推奨指

人差し指、中指、または第三指。

正しいスキャン方法

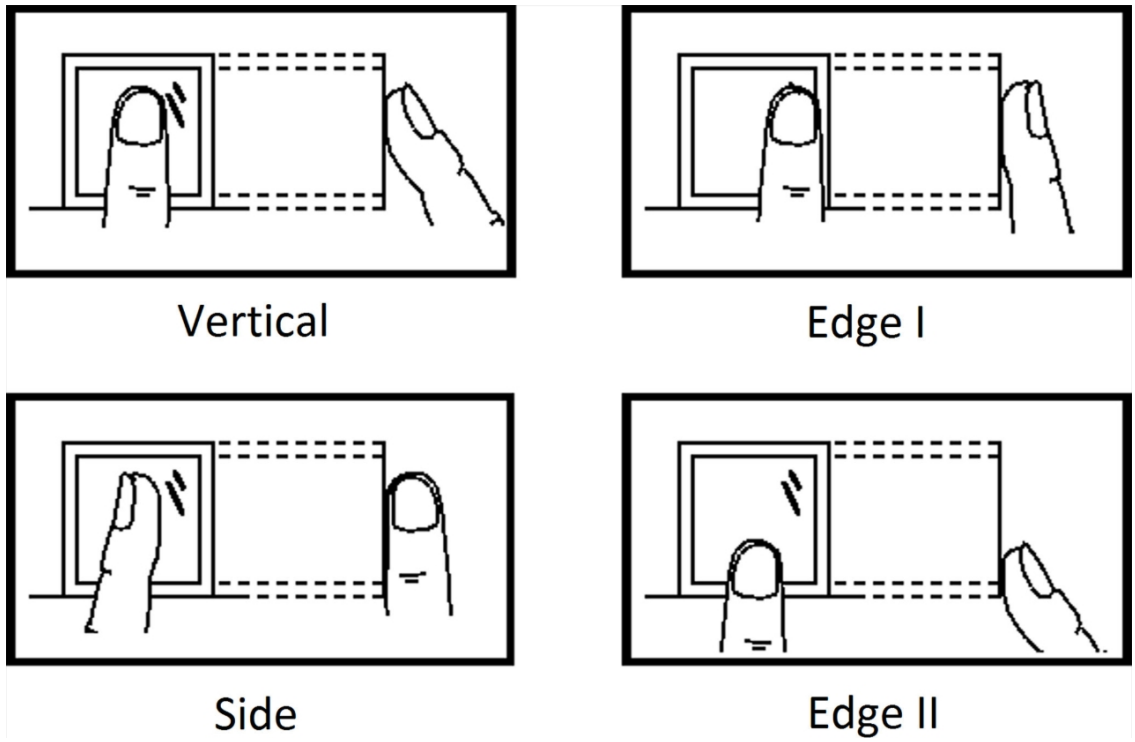
下図は指をスキャンする正しい方法です：



指をスキャナーに水平に押し当ててください。スキャンする指の中心がスキャナーの中心と一致している必要があります。

不正解のスキャン方法

以下に表示されているスキャン指紋の図は誤っています：



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。乾燥状態では指紋が正常に認識されない場合があります。
指を軽く吹きかけ、再度スキャンしてください。

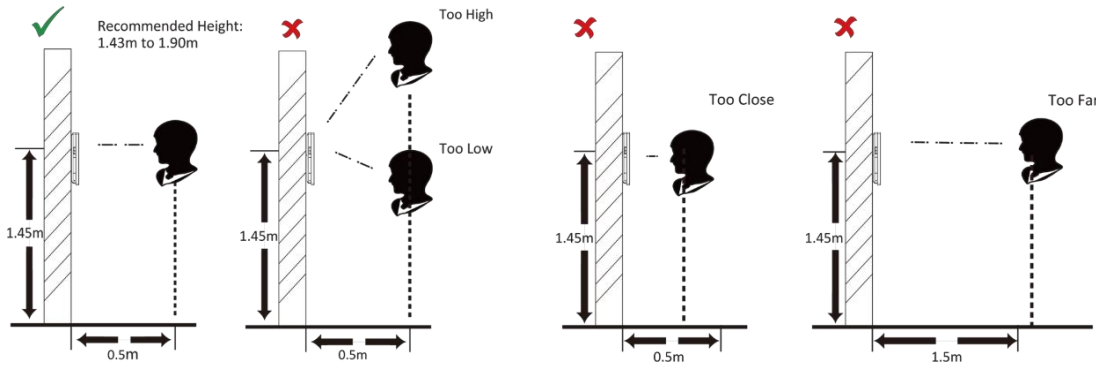
その他

指紋が浅い場合や指紋のスキャンが困難な場合は、他の認証方法の使用をお勧めします。
スキャンする指に怪我がある場合、スキャナーが認識できないことがあります。別の指に変更して再度お試しください。

付録B. 顔画像収集/比較時のヒント

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：0.5 m）



表情

- 顔写真の収集または比較時には、下の写真のような自然な表情を保ってください。

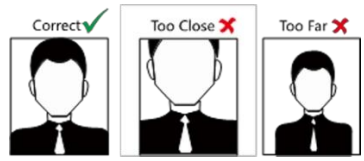
- 帽子、サングラス、その他顔認識機能に影響を与える可能性のあるアクセサリーは着用しないでください。
- 髪が目や耳などを覆わないようにし、濃いメイクは避けてください。

姿勢

高品質で正確な顔写真を得るためには、顔写真を収集または比較する際、カメラに向かって顔を向けてください。

サイズ

顔は収集ウィンドウの中央に収まるようにしてください。



付録 C. 設置環境に関するヒント

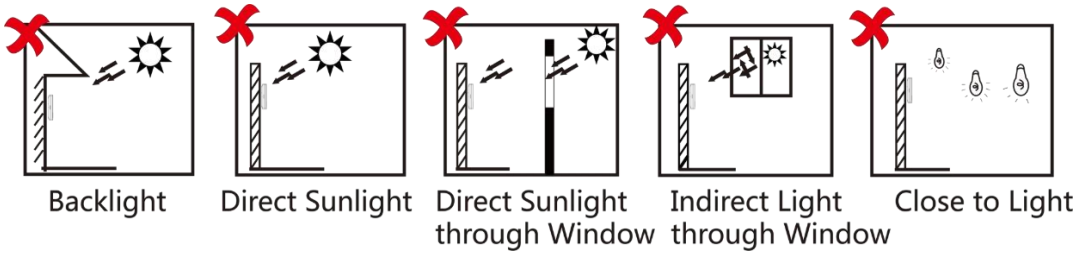
1. 光源の照度基準値

ろうそく：10ルクス

電球：100～850ルクス

太陽光：1200ルクス以上

2. 逆光、直射日光、間接日光を避けてください。



付録D. 寸法

指紋認証機能付きデバイスの寸法は以下の通りです：

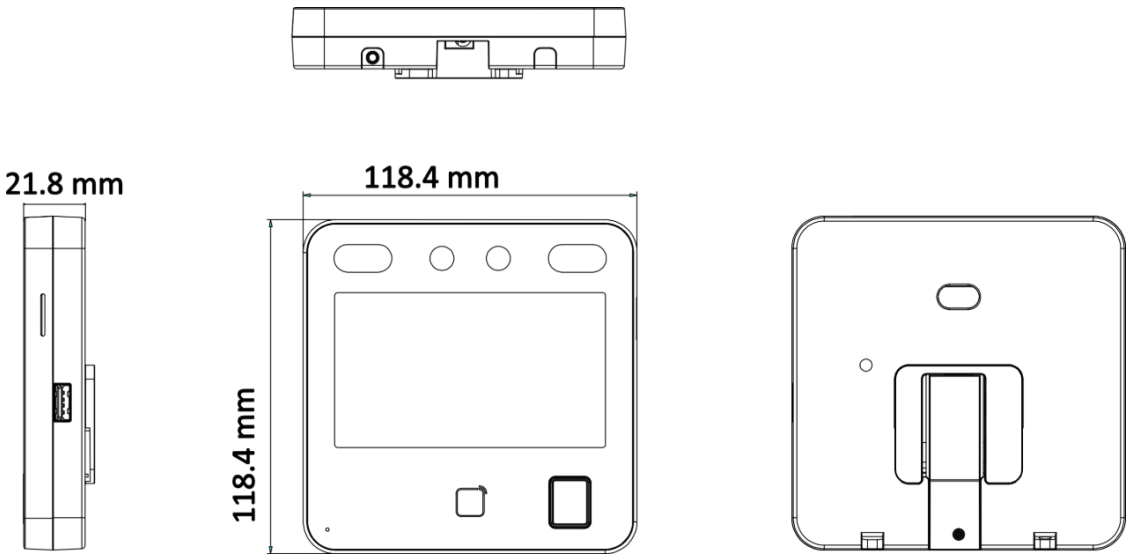


図 D-1 寸法（指紋認証機能付き）

指紋認証機能なしのデバイスの寸法は以下の通りです：

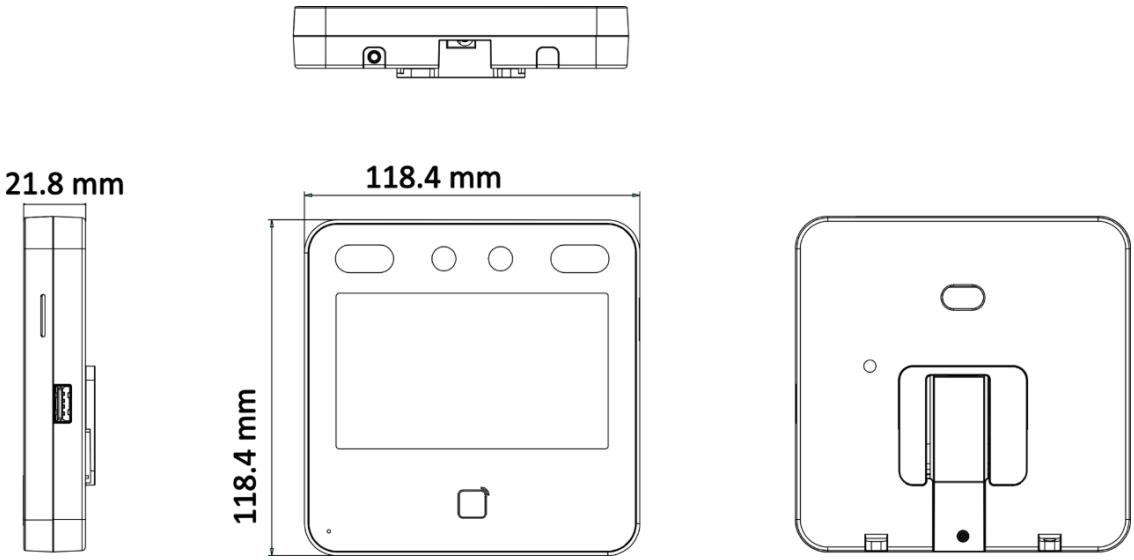


図 D-2 寸法（指紋なし）

付録E. 通信マトリクスとデバイスコマンド

通信マトリックス

以下のQRコードをスキャンして、デバイスの通信マトリックスを取得してください。
本マトリックスには、Hikvisionアクセス制御装置およびビデオインターホン装置の全通信ポートが含まれています。

図 E-1 通信マトリックスの QR コード

デバイスコマンド

以下のQRコードをスキャンして、デバイスの共通シリアルポートコマンドを取得してください。
注：このコマンド一覧には、Hikvisionの全アクセス制御装置およびビデオインターホン装置で一般的に使用されるシリアルポートコマンドがすべて含まれています。

図 E-2 デバイスコマンド


See Far, Go Further