



DS-K1T342 シリーズ 顔認識端末

ユーザーマニュアル

法的情報

この文書について

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

本製品について

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



知的財産権に関する承認

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

法的免責事項

- 適用される法律で許される最大限の範囲において、本文書および記載された製品（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」かつ「一切の瑕疵およびエラーを含む」状態で提供されます。ヒクビジョンは、明示的または黙示的でないが、保証もいたしません。

明示的または黙示的な一切の保証（商品性、満足のいく品質、または特定の目的への適合性を含むがこれらに限定されない）は、一切提供されません。製品の使用は、お客様の責任において行われます。いかなる場合においても、HIKVISIONは、特別損害、付随的損害、間接損害、または派生損害（事業利益の損失、事業の中断、データの損失を含むがこれらに限定されない）について、契約違反、不法行為（過失を含む）、製品責任、またはその他のいかなる理由に基づくものであっても、一切の責任を負いません。システムの破損、または文書の損失を含む損害について、契約違反、不法行為（過失を含む）、製品責任、またはその他の理由に基づくものであっても、製品の使用に関連して生じた場合、HIKVISIONは一切の責任を負いません。これは、HIKVISIONがそのような損害または損失の可能性について事前に通知を受けていた場合でも同様です。

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

データ保護

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

©杭州海康威視デジタルテクノロジー株式会社。著作権所有。

記号の規約

本文書において使用される記号は、以下のとおり定義されます。

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

規制情報

FCC情報

注意：本機器の製造者または販売者によって明示的に承認されていない変更または改造は、本機器の操作権限を無効にする可能性があります。

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

- 受信アンテナの向きや位置を変更する。
 - 機器と受信機との距離を離す。
 - 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機器を接続してください。
 - 販売店または経験豊富なラジオ/テレビ技術者に相談してください。
- この機器は、放射部と身体の間に最低**20cm**の距離を保って設置し、使用してください。

FCC 条件

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

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

EU適合宣言



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

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

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



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

この装置は、カナダ産業省の免許不要RSS規格に準拠しています。動作は、以下の2つの条件に準拠する必要があります：

- (1) この装置は干渉を引き起こしてはなりません、および
 - (2) この装置は、装置の正常な動作を妨げる可能性のある干渉を含む、いかなる干渉も受け入れる必要があります。
- この装置は、カナダ産業省のライセンス免除無線機器に関するCNRに準拠しています。使用は、以下の2つの条件を満たす場合に限り許可されます：

- (1) この装置は干渉を引き起こしてはなりません、および
- (2) この装置のユーザーは、受けたすべての無線干渉を受け入れる必要があります。この干渉が装置の動作を妨げる可能性があっても同様です。

この機器は、非制御環境におけるFCC/IC RSS-102で定められた放射線被曝限度値に準拠しています。この機器は、放射体と人体との間に最低20cmの距離を保って設置し、使用してください。

この機器は、FCC/CNR-102で定められた放射線の暴露限界値に準拠しています。この機器は、放射源と人体との間に20cm以上の距離を保って設置し、使用してください。

安全注意事項

これらの指示は、ユーザーが製品を正しく使用し、危険や財産損失を回避するために用意されています。

安全対策は「危険」と「注意」に分類されています：

危険：警告を無視すると、重大な怪我や死亡事故を引き起こす可能性があります。

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

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

危険：

- 製品の使用時には、当該国および地域の電気安全規格に厳格に従ってください。
- 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。
- 装置から煙、臭い、または音が発生した場合は、直ちに電源を切り、電源ケーブルを抜き、その後サービスセンターまでご連絡ください。
- 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場所に設置してください。
- 1. 電池を飲み込まないでください。化学やけどの危険があります！
- 2. この製品にはコイン型/ボタン型電池が含まれています。コイン型/ボタン型電池を誤飲した場合、2時間以内に重度の内部やけどを引き起こし、死亡する可能性があります。
- 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 compartment がしっかり閉まらない場合は、製品の使用を中止し、子供の手の届かない場所に保管してください。
- 5. 電池が飲み込まれた可能性や、体のどの部分にも挿入された可能性がある場合は、直ちに医療機関を受診してください。
- 6. 注意：誤った種類の電池を交換すると、爆発の危険があります。
- 7. 誤った種類の電池を交換すると、安全装置が機能しなくな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. バッテリーを火の中や熱いオープンに捨てたり、機械的に潰したり切断したりしないでください。これにより爆発の危険があります。
- 9. バッテリーを極端に高温の環境下に放置しないでください。爆発や可燃性液体またはガスの漏洩を引き起こす可能性があります。
- 10. 電池を極端に低い気圧にさらさないでください。爆発や可燃性液体またはガスの漏洩を引き起こす可能性があります。
- 11. 使用済みのバッテリーは、指示に従って処分してください。

⚠注意:

- デバイスを落としたり、物理的な衝撃を与えたりしないでください。また、高電磁波放射にさらさないでください。振動する表面や衝撃を受ける場所への機器の設置を避けてください（無視すると機器の損傷を引き起こす可能性があります）。
- 装置を極端に高温（装置の仕様書で指定された動作温度範囲内を確認してください）、低温、粉塵の多い、または湿気の多い場所に置かないでください。また、高レベルの電磁波にさらさないでください。
- 装置を直射日光、換気不良の場所、またはヒーターやラジエーターなどの熱源にさらすことは禁止されています（無視すると火災の危険があります）。
- 室内用装置のカバーは、雨や湿気から保護してください。
- 機器を直射日光、換気不良、またはヒーターやラジエーターなどの熱源にさらすことは禁止されています（無視すると火災の危険があります）。
- デバイスカバーの内部および外部表面を清掃する際は、柔らかく乾いた布を使用し、アルカリ性洗剤は使用しないでください。
- 生体認証製品は、アンチスプーフィング環境には完全に適用できません。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。
- 機器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機器をインストールしてください。怪我を防ぐため、本機器はインストール指示に従って床/壁に確実に固定してください。
- バッテリーの不適切な使用または交換は、爆発の危険を引き起こす可能性があります。同じまたは同等のタイプのみ交換してください。使用済みのバッテリーは、バッテリー製造元の指示に従って処分してください。
- このブラケットは、対応した機器とのみ使用することを目的としています。他の機器との使用は、不安定さを引き起こし、けがの原因となる可能性があります。
- この機器は、対応したブラケットとのみ使用してください。他の機器（カート、スタンド、またはキャリアなど）との使用は、不安定さを引き起こし、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
顔認識端末	DS-K1T342MX DS-K1T342MX-E1	13.56 MHz カード読み取り周波数
	DS-K1T342MWX DS-K1T342MWX-E1	13.56 MHz カード読み取り周波数、Wi-Fi (2.4 GHz)
	DS-K1T342MFX DS-K1T342MFX-E1	13.56 MHz カード提示周波数
	DS-K1T342MFWX DS-K1T342MFWX-E1	13.56 MHz カード提示周波数、Wi-Fi (2.4 GHz)
	DS-K1T342EX DS-K1T342EX-E1	125 KHz カード提示周波数
	DS-K1T342EWX DS-K1T342EWX-E1	125 KHz カード提示周波数、Wi-Fi (2.4 GHz)
	DS-K1T342EFWX DS-K1T342EFWX-E1	125 kHz カード提示周波数、Wi-Fi (2.4 GHz)
	DS-K1T342DX DS-K1T342DX-E1	13.56 MHz カード提示周波数
	DS-K1T342DWX DS-K1T342DWX-E1	13.56 MHz カード提示周波数、Wi-Fi (2.4 GHz)

ユーザーマニュアルに記載されている電源のみを使用してください:

モデル	製造元	標準
ADS-12FG-12N 12012EPG	深セン・ホノル・エレクトロニクス株式会社	PG

内容

第1章 概要	1
1.1 概要	1
1.2 機能	1
第2章 外観	2
第3章 インストール	5
3.1 インストール環境	5
3.2 Gang Box を使用してインストール	5
3.3 表面取り付け	8
3.4 ブラケットを使用して取り付け	14
3.4.1 ブラケットを使用した取り付け前の準備	14
3.4.2 ブラケットの取り付け	15
3.5 シリンダーブラケットで取り付け	16
3.5.1 ブラケットを使用した取り付け前の準備	16
3.5.2 シリンダーブラケットの取り付け	18
第4章 配線	2
4.1 端子説明	2
4.2 配線 標準デバイス	2
4.3 セキュアドア制御ユニット用配線	22
4.4 火災モジュール配線	23
4.4.1 電源を切った際のドア開閉配線図	23
4.4.2 電源を切った際のドアロック配線図	2
第5章 アクティベーション	27
5.1 デバイス経由でアクティベーション	27
5.2 ウェブブラウザ経由でアクティベート	29
5.3 SADP経由でアクティベート	30
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	31
第6章 簡易操作	33
6.1 言語を選択	3

6.2	パスワード変更タイプを設定	35
6.3	ネットワークパラメーターを設定	35
6.4	プラットフォームへのアクセス	37
6.5	プライバシー設定	39
6.6	管理者設定	39
第7章	基本操作	42
7.1	ログイン	42
7.1.1	管理者によるログイン	42
7.1.2	アクティベーションパスワードでログイン	45
7.1.3	パスワードを忘れた場合	46
7.2	通信設定	47
7.2.1	有線ネットワークパラメーターの設定	47
7.2.2	Wi-Fi パラメーターを設定	49
7.2.3	RS-485 パラメーターを設定	51
7.2.4	Wiegand パラメーターを設定	53
7.2.5	ISUP パラメーターを設定	55
7.2.6	プラットフォームアクセス	57
7.2.7	SNMP設定	58
7.3	ユーザー管理	58
7.3.1	管理者追加	58
7.3.2	顔写真を追加	60
7.3.3	指紋を追加	63
7.3.4	カードを追加	64
7.3.5	PINを追加	65
7.3.6	認証モードを設定	66
7.3.7	ユーザーを検索して編集する	67
7.4	勤怠状況の設定	67
7.4.1	デバイス経由で出席モードを無効化	67
7.4.2	デバイス経由で手動出席を設定する	69

7.4.3	デバイス経由で自動出席を設定する	71
7.4.4	デバイス経由で手動と自動の出席設定を行う	73
7.5	データ管理.....	75
7.5.1	データの削除	75
7.5.2	データのインポート	75
7.5.3	データをエクスポート	76
7.6	身分認証.....	76
7.6.1	単一認証情報による認証.....	77
7.6.2	複数の認証情報による認証.....	77
7.7	基本設定.....	78
7.8	生体認証パラメーターの設定	79
7.9	設定オプション	82
7.10	デバイスパスワードの変更.....	85
7.11	認証設定	85
7.12	システムメンテナンス	88
第8章	モバイルWeb経由でデバイスを設定する.....	92
8.1	ログイン	92
8.2	概要	92
8.3	パスワードを忘れた場合	92
8.4	設定	93
8.4.1	デバイス情報表示	93
8.4.2	時間設定	93
8.4.3	夏時間設定	94
8.4.4	ユーザー管理	95
8.4.5	ネットワーク設定	95
8.4.6	ユーザー管理	100
8.4.7	イベント検索	101
8.4.8	アクセス制御設定	101
8.4.9	ビデオインターホン設定	105

8.4.10 オーディオ設定	107
8.4.11 顔パラメーター設定	107
8.4.12 プライバシーパラメーターの設定	109
8.4.13 パスワードモード	109
8.4.14 アップグレードとメンテナンス	110
8.4.15 オンラインドキュメントを表示	110
8.4.16 オープンソースソフトウェアライセンスを表示	110
第9章 ウェブブラウザを使用したクイック操作	11
9.1 パスワードを変更	111
9.2 言語を選択	111
9.3 時間設定	111
9.4 プライバシー設定	112
9.5 管理者設定	112
9.6 番号とシステムネットワーク	113
第10章 ウェブブラウザ経由での操作	115
10.1 ログイン	11
10.2 パスワードを忘れた場合	115
10.3 ヘルプ	115
10.3.1 オープンソースソフトウェアライセンス	115
10.3.2 オンラインヘルプドキュメントを表示	116
10.4 ログアウト	116
10.5 ウェブブラウザからのクイック操作	116
10.5.1 パスワードの変更	116
10.5.2 言語選択	116
10.5.3 時間設定	116
10.5.4 プライバシー設定	117
10.5.5 管理者設定	117
10.5.6 番号とシステムネットワーク	118
10.6 ユーザー管理	119

10.7 概要.....	121
10.8 アクセス制御アプリケーション.....	123
10.8.1 パスバック防止設定.....	123
10.8.2 マルチドア・インターロッキング設定.....	123
10.9 アクセス制御管理.....	124
10.9.1 イベント検索.....	124
10.9.2 ドアパラメーター設定.....	124
10.9.3 認証設定.....	127
10.9.4 認証連携設定.....	130
10.9.5 認証プランの設定.....	131
10.9.6 顔パラメーターの設定.....	131
10.9.7 カード設定.....	135
10.9.8 リモート検証の設定.....	137
10.9.9 プライバシー設定.....	138
10.9.10 通話設定.....	140
10.10 デバイス管理.....	145
10.11 システム設定.....	145
10.11.1 PC ウェブ経由でデバイス情報を表示.....	145
10.11.2 時刻設定.....	14
10.11.3 管理者のパスワードを変更する.....	146
10.11.4 PCウェブ経由でのアカウントセキュリティ設定.....	147
10.11.5 PCウェブ経由でデバイスの武装/解除状態を確認する.....	147
10.11.6 PCウェブ経由で作業モードを設定.....	147
10.11.7 ネットワーク設定.....	148
10.11.8 PCウェブ経由でビデオとオーディオのパラメーターを設定.....	153
10.11.9 設定にアクセス.....	154
10.11.10 画像パラメーター設定.....	156
10.11.11 リンク設定.....	157
10.11.12 勤怠設定.....	158

10.12 設定	160
10.12.1 PCウェブ経由で待機画面を設定する	160
10.12.2 PCウェブ経由でスリープ時間を設定	161
10.12.3 PCウェブ経由で認証デスクをカスタマイズ	161
10.12.4 PCウェブ経由で通知の公開を設定する	162
10.12.5 PCウェブ経由でプロンプトスケジュールを設定する	163
10.12.6 PCウェブ経由で通知音声のカスタマイズ	164
10.12.7 PCウェブ経由で認証結果テキストを設定する	165
10.13 システムとメンテナンス	165
10.13.1 再起動	165
10.13.2 アップグレード	165
10.13.3 復元	166
10.13.4 PCウェブ経由でデバイスパラメーターをエクスポート	167
10.13.5 PCウェブ経由でデバイスパラメーターをインポート	167
10.13.6 デバイスのデバッグ	167
10.13.7 PCウェブ経由でログを表示	170
10.13.8 PCウェブ経由での詳細設定	170
10.13.9 セキュリティ管理	170
10.13.10 証明書管理	171
第11章 その他のプラットフォームの設定	17
付録A. 指紋スキャンに関するヒント	17
付録B. 顔写真の収集/比較時のヒント	17
付録C. インストール環境に関する注意事項	178
付録D. 次元	179

第1章 概要

1.1 概要

顔認識端末は、顔認識機能を備えたアクセス制御装置の一種で、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、セキュリティアクセス制御システムに主に適用されます。

1.2 特徴

- 4.3インチLCDタッチスクリーン、272×480の画面解像度、最大顔枠のリアルタイム検出と表示。
- 2メガピクセル広角デュアルレンズ
- 複数の認証モードに対応：顔認証、指紋認証、カード認証、PINコード認証、および複数の認証モードの組み合わせ。
- アクセス制御の時間帯制御（ブランテンプレート）に対応し、必要に応じてドアの開錠を許可します。
- プラットフォーム経由でネットワークの運用および人員権限情報の発行をサポートします。
- データネットワークアップロード機能をサポートし、デバイス比較結果や連携キャプチャ画像をリアルタイムでプラットフォームにアップロードできます。
- デバイスがオフラインの場合、デバイスがプラットフォームに接続された際に生成されたイベントは、再度アップロードされます。
- NTP、手動、および自動の時間校正に対応しています。
- デバイス間のビデオインターコムをサポートします。
- RTSPプロトコル経由でリモート動画プレビューと動画コードストリームの出力に対応しています。
- ウォッチドッグ監視機構と改ざん防止設計を採用し、デバイスの正常な動作を保証します。
- マスク検出モードに対応し、マスクの着用状態の通知やマスクの着用が必須のモードをサポートしています。
- IP65規格に準拠しています。
- 標準のPoEで電源供給を行い、同時にドアロック用の電源供給（12 VDC/1 A）も可能です。



注意

PoE対応のデバイスでのみ機能します。

第2章 外観

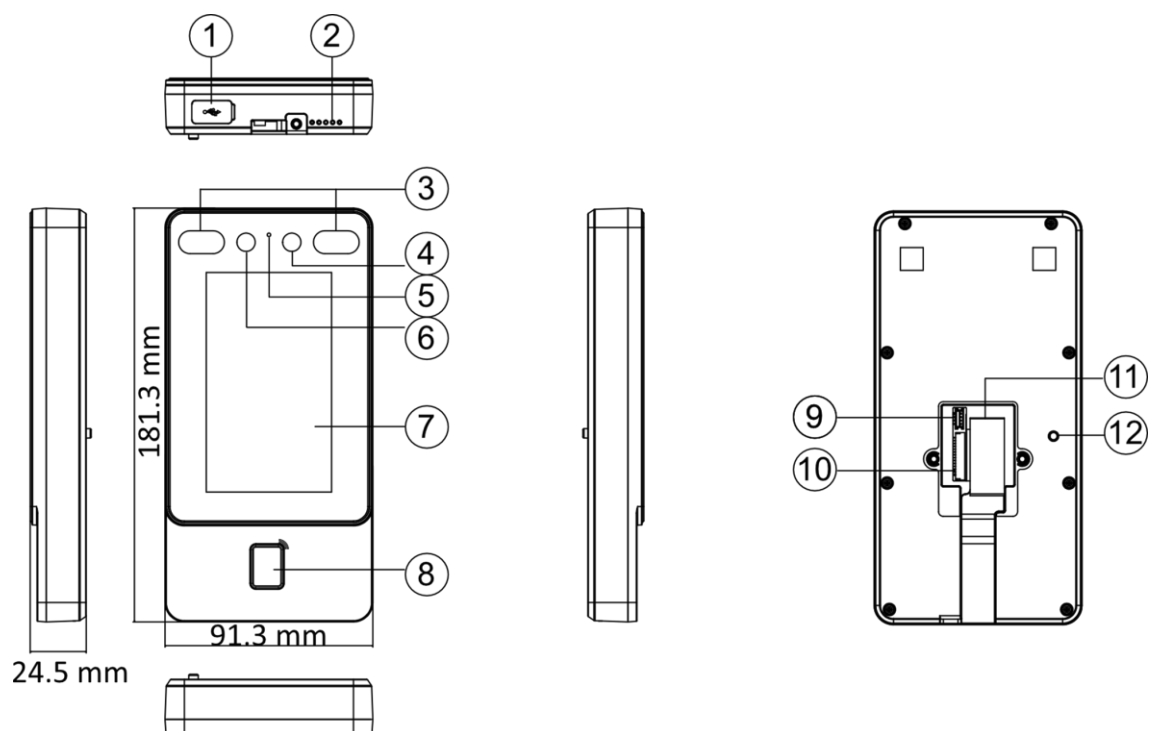


図2-1 指紋モジュール付き表2-1 外観説明

番号	名称
1	USB インターフェース
2	スピーカー
3	赤外線ライト
4	カメラ
5	マイク
6	カメラ
7	タッチスクリーン
8	指紋認証エリア/カード読み取りエリア
9	デバッグ用ポート（デバッグ専用）

番号	名前
10	配線端子
1	ネットワーク インター フェース
12	不正操作検知

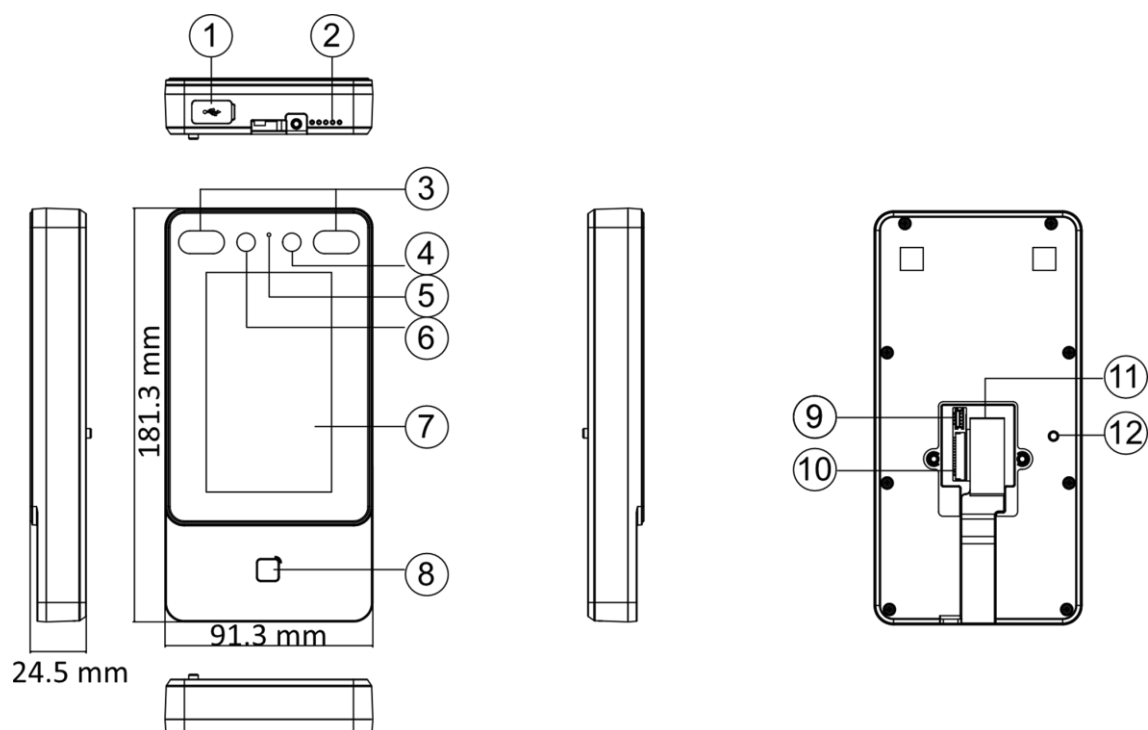


図2-2 指紋モジュールなし表2-2 外観説明

番号	名称
1	USB インターフェース
2	スピーカー
3	赤外線ライト
4	カメラ
5	マイク
6	カメラ

番号	名前
7	タッチスクリーン
8	カード挿入部
9	デバッグポート（デバッグ専用）
10	配線端子
11	ネットワーク インター フェース
12	不正操作検知

第3章 インストール

3.1 インストール環境

- バックライト、直射日光、および間接日光を避けてください。
- より良い認識のため、設置環境内またはその近くに光源を設置してください。
- 壁またはその他の部分の最小支持荷重は、装置の重量の3倍以上である必要があります。
- 装置の視界範囲内1m以内に、強い反射物（ガラスドア/壁、ステンレス鋼製品、アクリルや他の光沢のあるプラスチック、漆、セラミックタイルなど）は設置しないでください。
- 装置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

インストール環境の詳細については、「インストール環境のヒント」を参照してください。

3.2 ギャングボックスを使用してインストールしてください。

手順

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



注意

ギャングボックスは別途購入する必要があります。

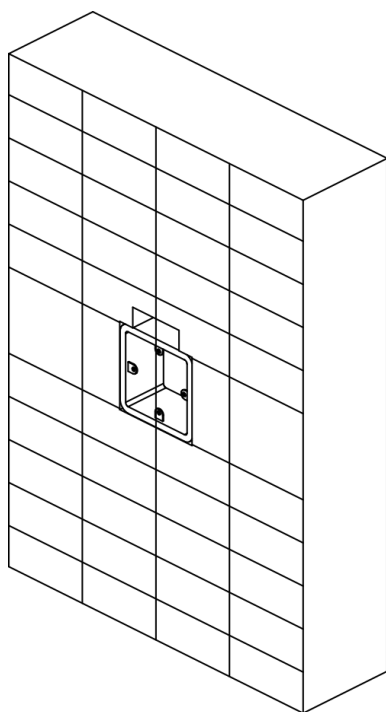


図3-1 ギャングボックスの取り付け

2. 付属の2本のネジ（SC-KA4X22）で、ギャングボックスにマウントプレートを固定してください。

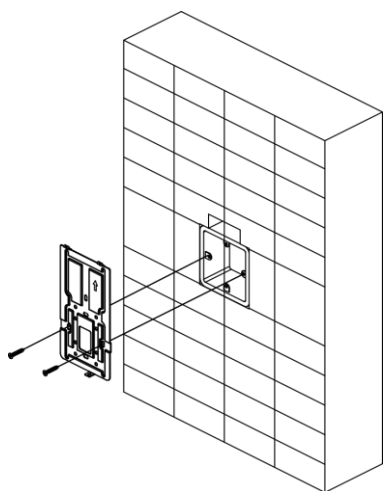


図3-2 マウントプレートの取り付け

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

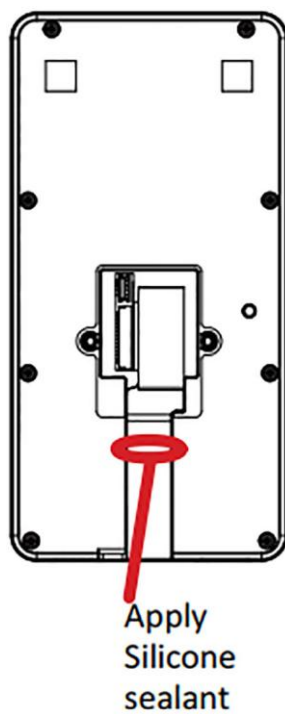


図3-3 シリコンシーラントの塗布

4. デバイスをマウントプレートに合わせ、付属のネジ（SC-KM3X6-T10-SUSS）1本でデバイスをマウントプレートに固定してください。

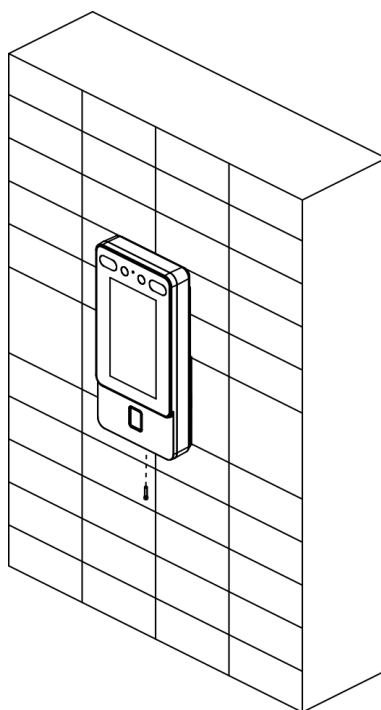


図3-4 デバイスの固定

3.3 表面取り付け

手順

1. 取り付けテンプレートの基準線に従い、取り付けテンプレートを壁または他の表面に貼り付け、地面から1.45メートル高い位置に設置します。

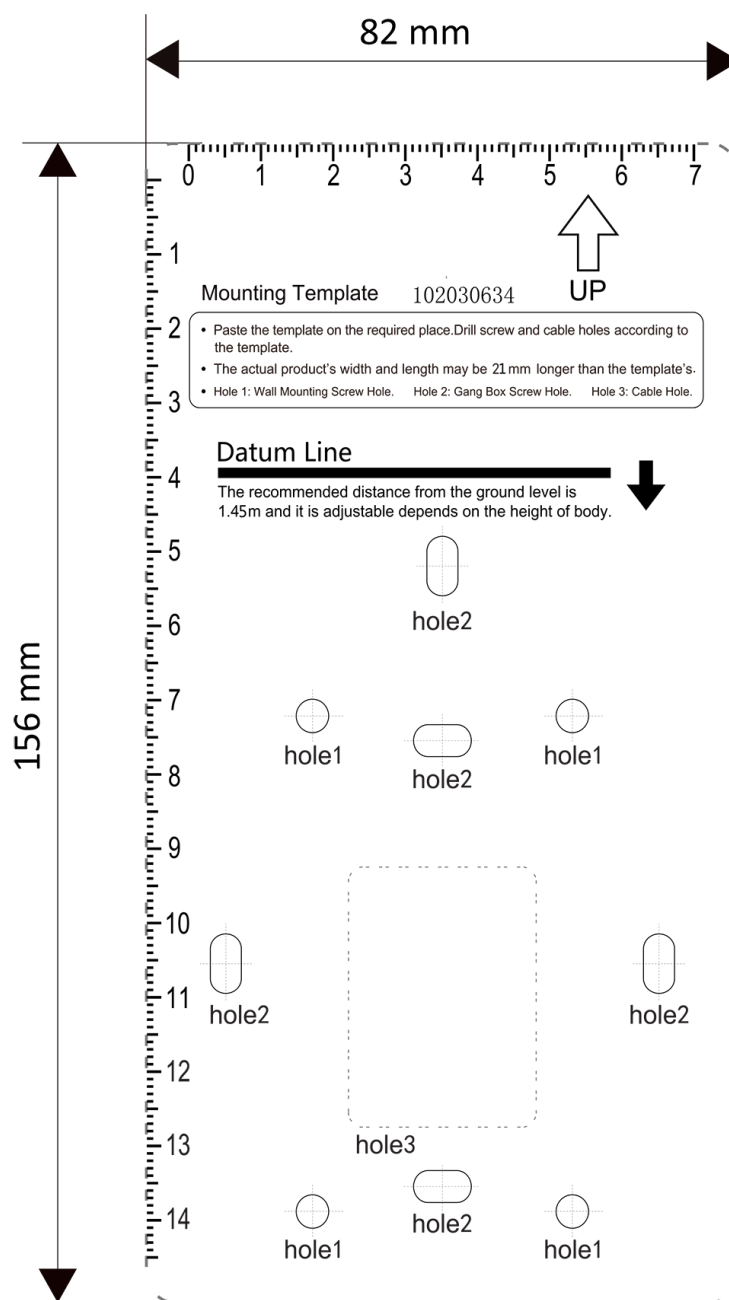


図3-5 取り付けテンプレート

2. 取り付けテンプレートの「Hole 1」の位置に合わせて、壁または他の表面に穴を開けます。
3. 拡張ボルトのプラスチックスリーブを穴に挿入します。
4. 穴をマウントプレートに合わせ、付属の2本のネジ（KA4×22-SUS）でマウントプレートを壁に固定してください。

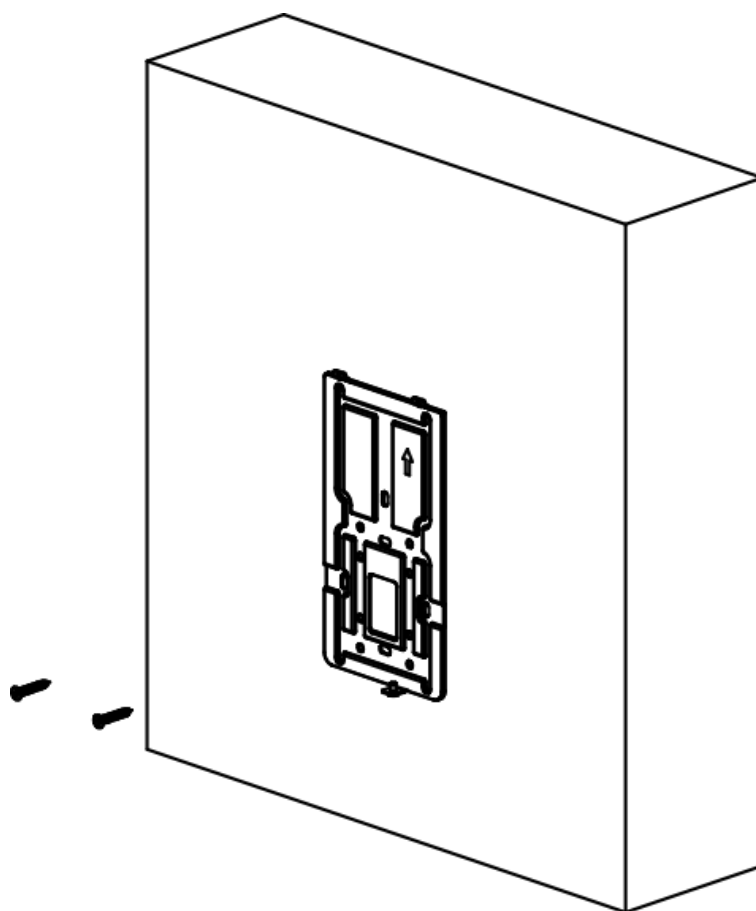


図3-6 取り付けプレートの取り付け

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



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

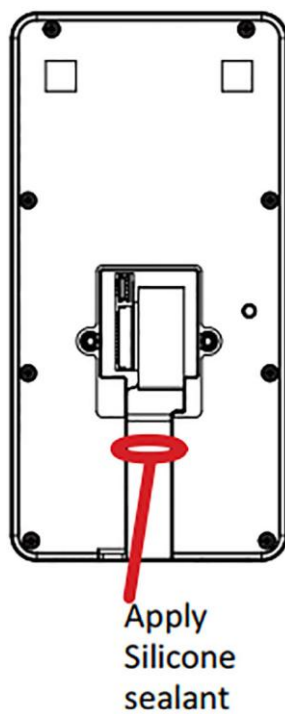


図3-7 シリコンシーラントの塗布

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

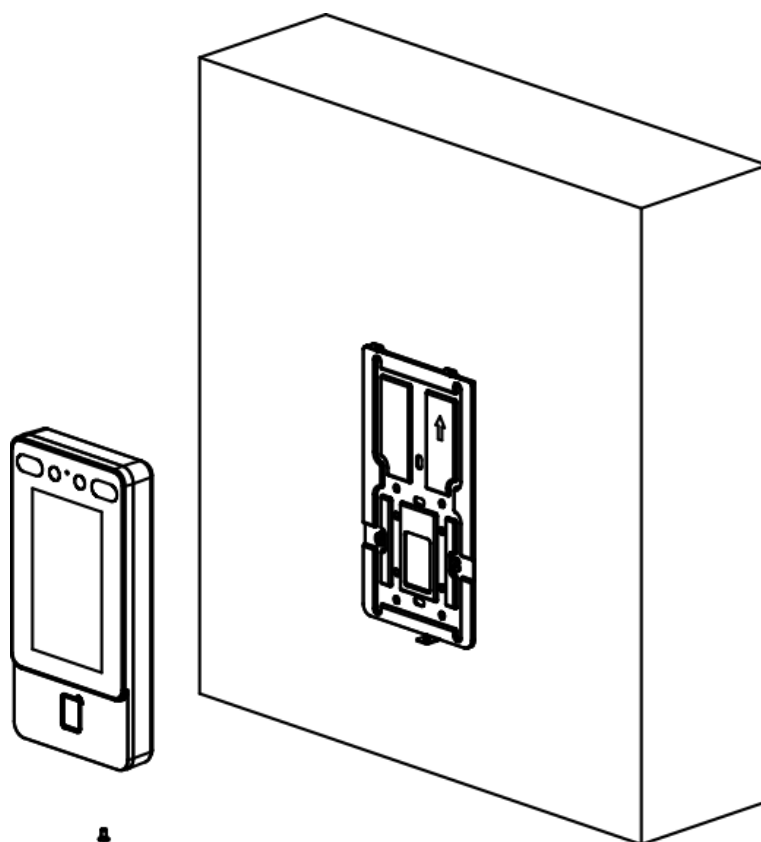


図3-8 デバイスの吊り下げ

7. 付属のネジ（KM3×6-SUS）1本を使用して、デバイスとマウントプレートを固定します。

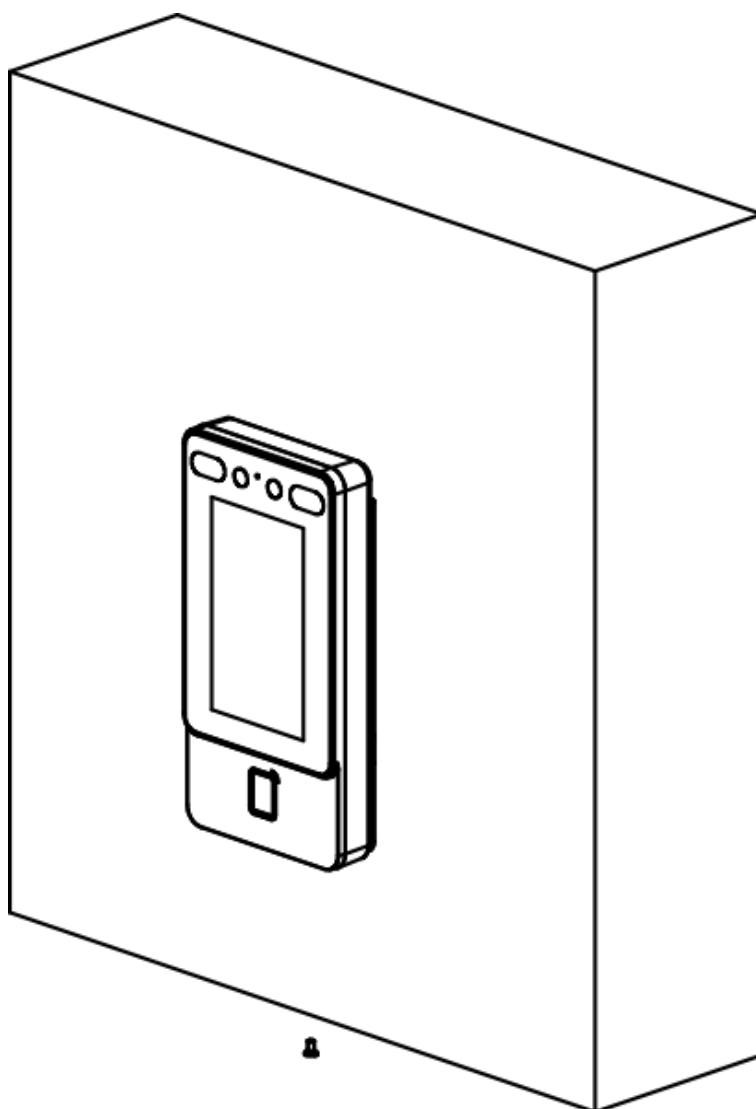


図3-9 デバイスの固定



- 推奨取り付け高さは1.45メートルです。必要に応じて取り付け高さを調整できます。
- 付属の取り付けプレートを使用することをおすすめします。

-
8. インストール後、機器を正しく使用するため（屋外使用时）、画面に保護フィルム（モデルによっては付属品）を貼り付けてください。

3.4 ブラケットを使用して取り付け

3.4.1 ブラケットでの取り付け前の準備

手順

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



注意 押し込んだ後、はんだ付けを行い、水が入らないようにします。

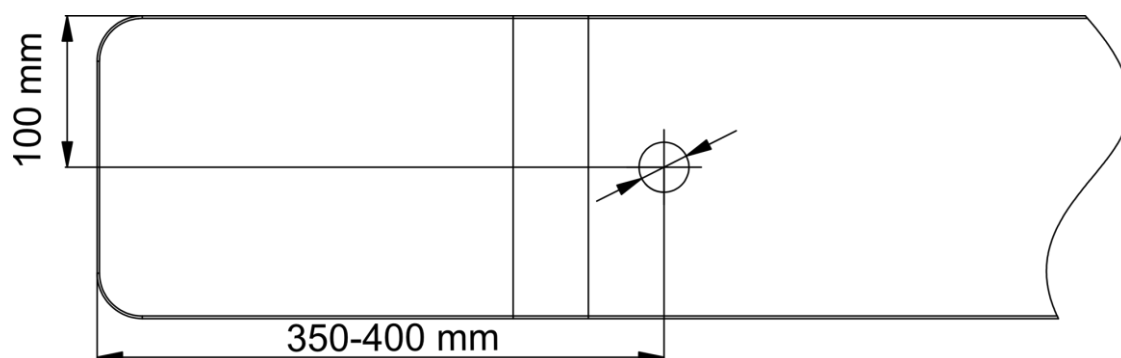


図3-10 ターンスタイルに穴を開ける

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

- 1) 以下の図に示す3本のネジを外します。

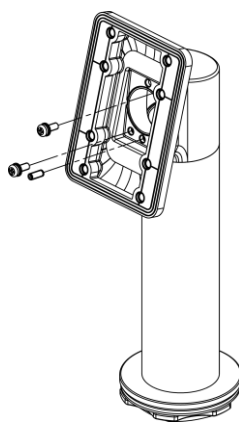


図3-11 ネジの取り外し

- 2) 固定部を180°回転させ、3本のネジを元に戻して取り付けます。

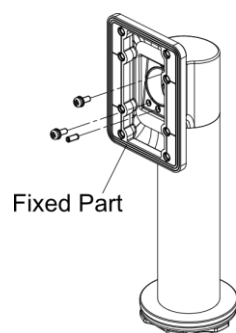


図3-12 固定部の回転

3.4.2 ブラケットの取り付け

手順

1. ベースを回転ゲートに取り付けます。
 - 1) 回転式ゲート穴とベースの穴を合わせ、ベースを回転式ゲートに設置します。
 - 2) ベースを回転させて適切な位置に固定し、デバイスが正しい方向を向いていることを確認してください。
 - 3) レンチを使用してベースを固定します。

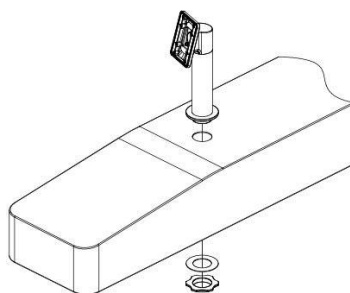


図3-13 ベースの取り付け



注意

ターンスタイルの前後面にシリコンパッドを1枚ずつ取り付けます。

2. 付属の4本のネジ（SC-K1M4×6-SUS）を使用して、ブラケットにマウントテンプレートを取り付けます。

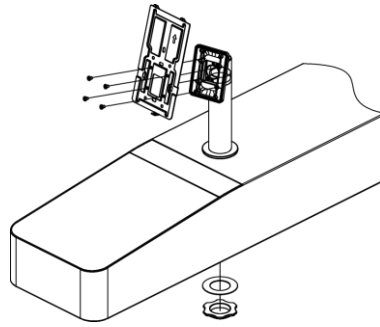


図3-14 取り付けテンプレートの固定

3. ケーブルをターンスタイルのケーブル穴に通し、1本のSC-KM3×6-T10-SUSネジで装置をマウントプレートに固定します。

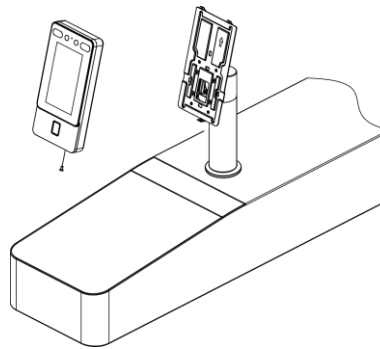


図3-15 デバイスの固定

4. 取り付け後、装置の適切な使用（屋外使用）のため、画面に保護フィルム（付属品の一部）を貼り付けてください。

3.5 シリンダーブラケットを使用して取り付け

3.5.1 ブラケットでの取り付け前の準備

ターンスタイルに穴が空いていることを確認してください。空いていない場合は、以下の手順に従って穴を開けてください。

手順

1. 4本のネジ（M3またはM4）をフランジナットで固定し、回転式ゲートの内側に補強板を取り付けます。



注意 トと端部の間の距離は10mmを超えてはいけません。

2. 図に示すとおり、回転式ゲートの内側に穴を開け、防水ナットを取り付けます。



リベットを押し込んだ後、はんだ付けを行い、水の侵入を防ぐようにしてください。

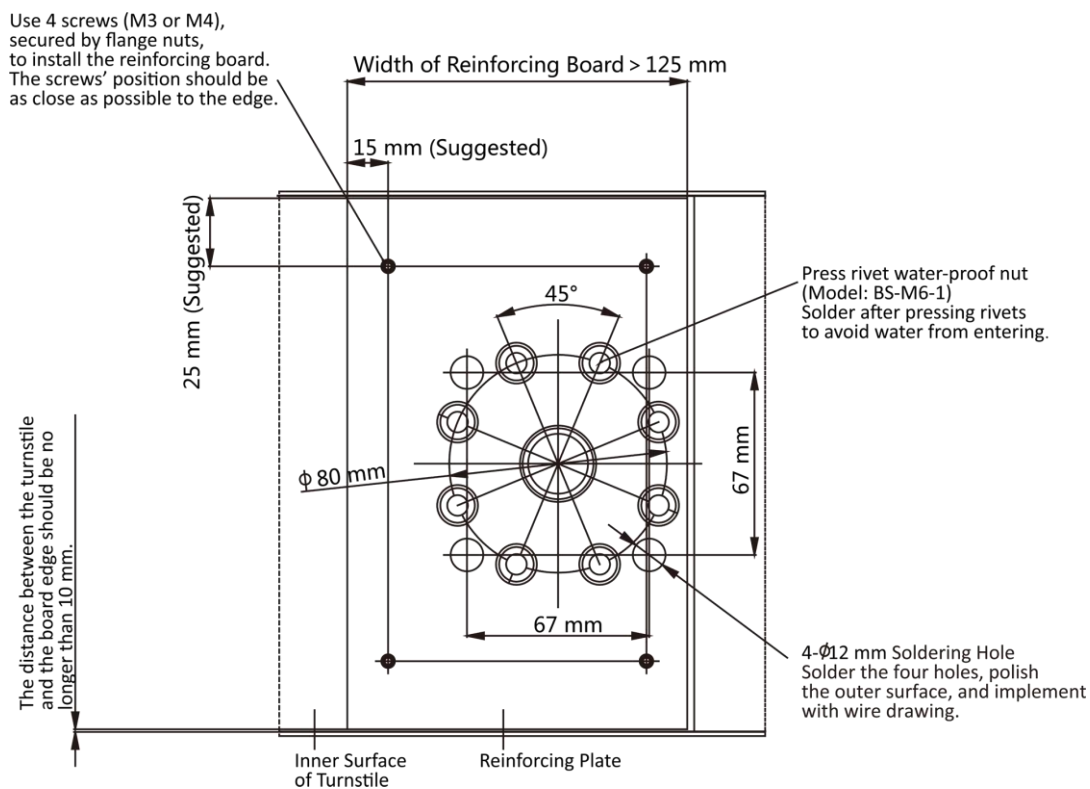


図3-16 回転式ゲートに穴を開ける

3. 残りの4つの穴をハンダ付けし、表面を研磨し、ワイヤー引きを実施します。
4. ターンスタイルの内側に円形チューブをハンダ付けし、水の侵入を防ぐ。

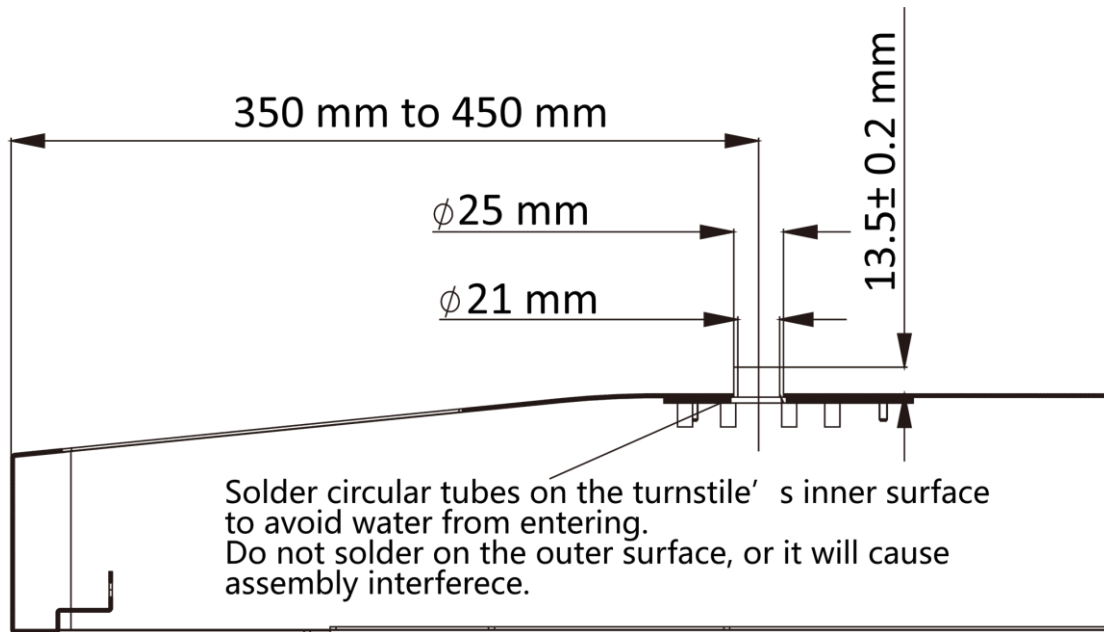


図3-17 管のはんだ付け

3.5.2 シリンダーブラケットの取り付け

手順

1. ベースをターンスタイルに取り付けます。
 - 1) ターンスタイルの穴とベースの穴を合わせ、ベースをターンスタイルに配置します。
 - 2) ベースを適切な位置に回転させ、装置が正しい方向を向いていることを確認します。
 - 3) ベースを4本のSC-OM6×12-H-SUSネジで固定してください。

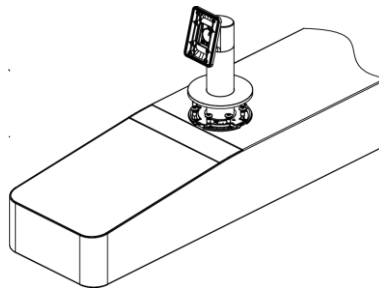


図3-18 ベースの取り付け

2. 4本のSC-K1M4×6-SUSネジを使用して、マウントプレートをブラケットに固定します。

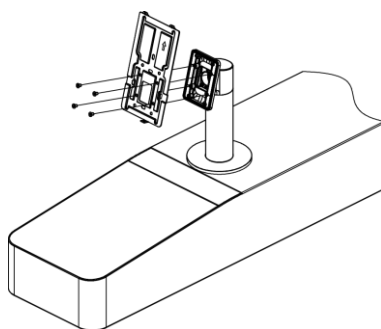


図3-19 取り付けプレートの固定

3. ケーブルをターンスタイルのケーブル穴に通します。
4. 顔認識端末を1本のSC-KM3×6-H2-SUSネジで取り付けプレートに固定します。

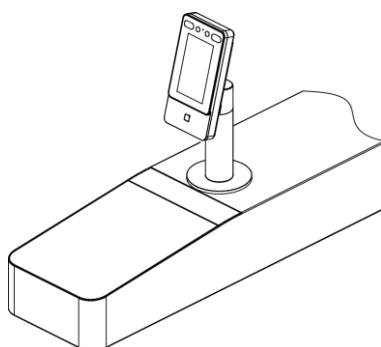


図3-20 取り付けプレートを固定する

5. 取り付け後、装置の正常な使用（屋外使用）のため、画面に保護フィルム（付属品の一部）を貼り付けてください。

第4章 配線

RS-485 ターミナルを RS-485 カードリーダーに接続し、NC/NO ターミナルと COM ターミナルをドアロックに接続します。SEN ターミナルと GND ターミナルをドアコンタクトに接続し、BTN/GND ターミナルを出口ボタンに接続します。さらに、Wiegand ターミナルをアクセスコントローラーに接続します。

WIEGAND端子をアクセスコントローラーに接続すると、顔認識端末は認証情報をアクセスコントローラーに送信し、アクセスコントローラーはドアを開けるかどうかを判断します。



ケーブルの太さが18 AWGの場合、12 Vの電源を使用する必要があります。また、電源とデバイス間の距離は20 mを超えてはいけません。

- ケーブルの太さが15 AWGの場合、12 Vの電源を使用する必要があります。また、電源と機器間の距離は30 mを超えてはいけません。
- ケーブルの太さが12 AWGの場合、12 Vの電源を使用する必要があります。また、電源と機器間の距離は40 mを超えてはいけません。
- 外部カードリーダー、ドアロック、出口ボタン、ドアマグネットはそれぞれ個別に電源供給が必要です。

4.1 端子説明

ターミナルには電源入力、RS-485、Wiegand出力、およびドアロックが含まれます。ターミナルの記述は次のとおりです：

表4-1 端子説明

グループ	番号	機能	色	名前	説明
グループ A	A1	入力電力	赤	+12 V	12 VDC電源供給
	A2		黒	GND	接地
グループ B	B1	RS-485	黄色	485+	RS-485 配線
	B2		青	485-	
	B3		黒	GND	接地
グループ C	C1	ワイガンド	グリーン	W0	ワイガンド配線 0

グループ	番号	機能	色	名前	説明
	C2		白	W1	ワイガンド配線 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		黄色/緑	センサー	ドアコンタクト
	D5		黒	GND	接地
	D6		黄色/灰色	ボタン	出口ドア配線

4.2 通常デバイス用配線

ターミナルは通常の周辺機器と接続できます。

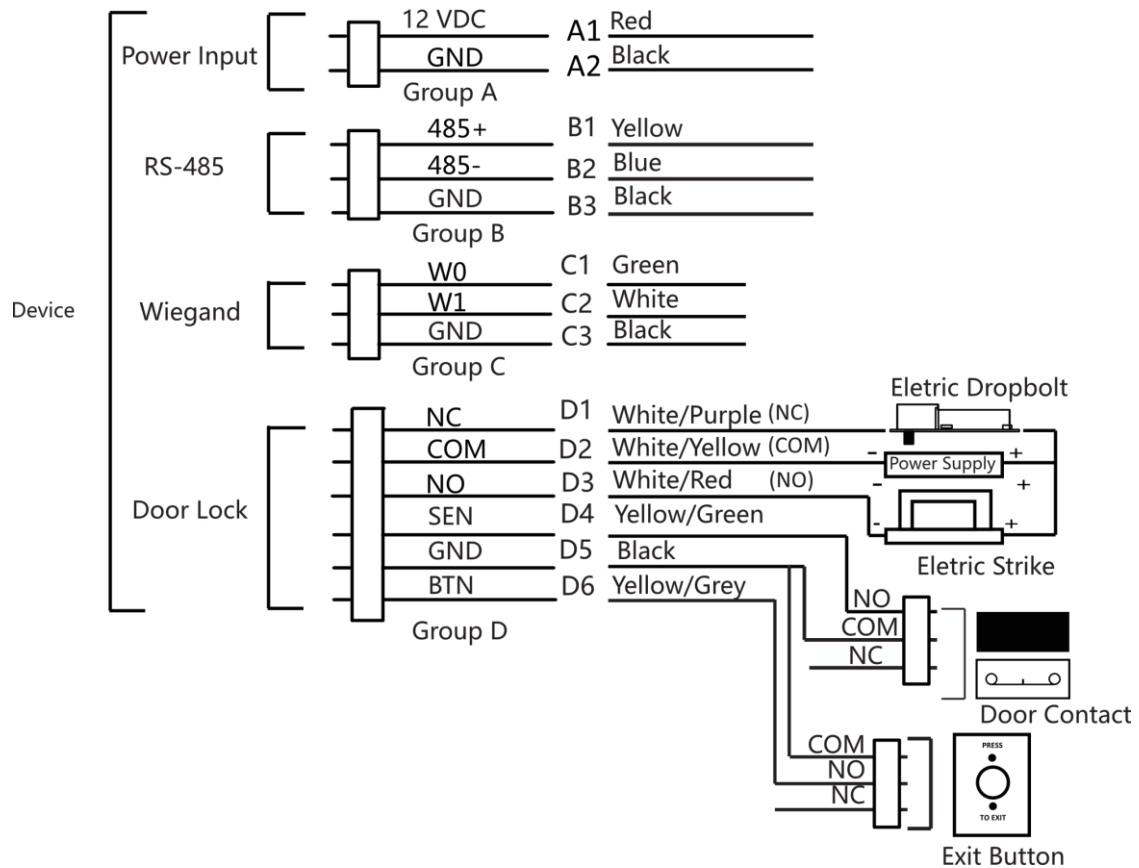


図4-1 デバイス配線



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

4.3 セキュアドアコントロールユニットの配線

端末をセキュアドアコントロールユニットに接続できます。配線図は次のとおりです。

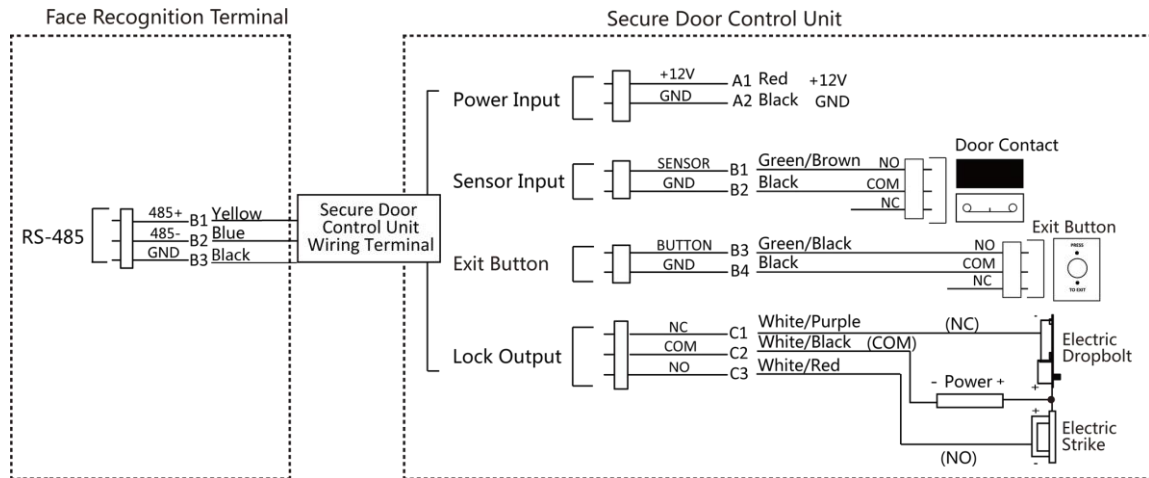


図4-2 セキュアドア制御ユニットの配線



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 火災モジュールを配線

4.4.1 電源を切った際にドアが開く配線図

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

シナリオ：消防車アクセス用に設置

タイプ1



消防システムがアクセス制御システムの電源を制御します。

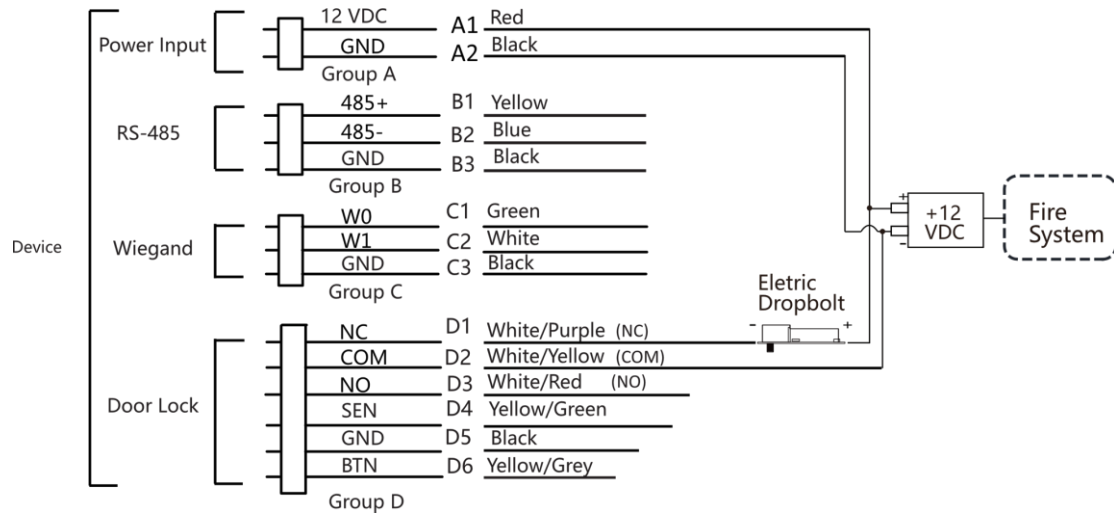


図4-3 配線装置

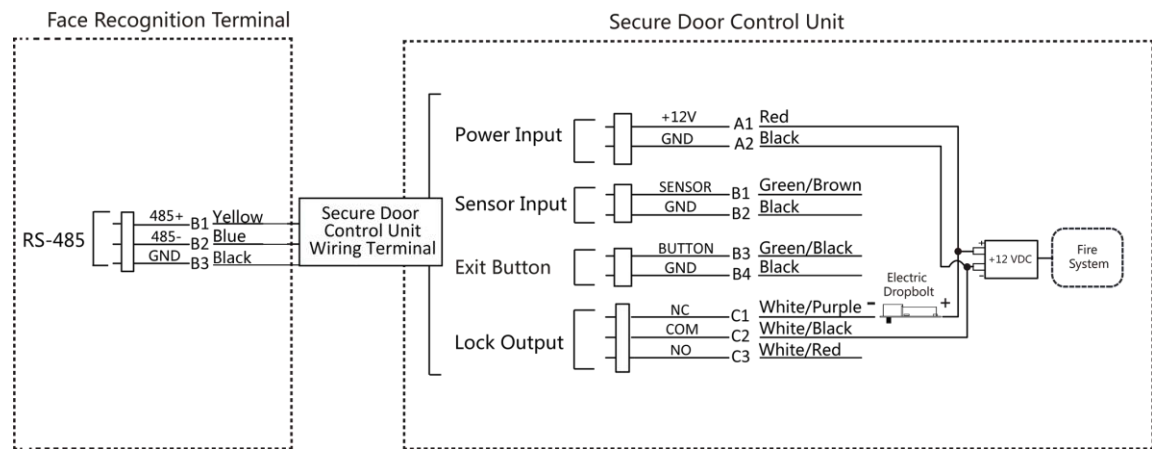
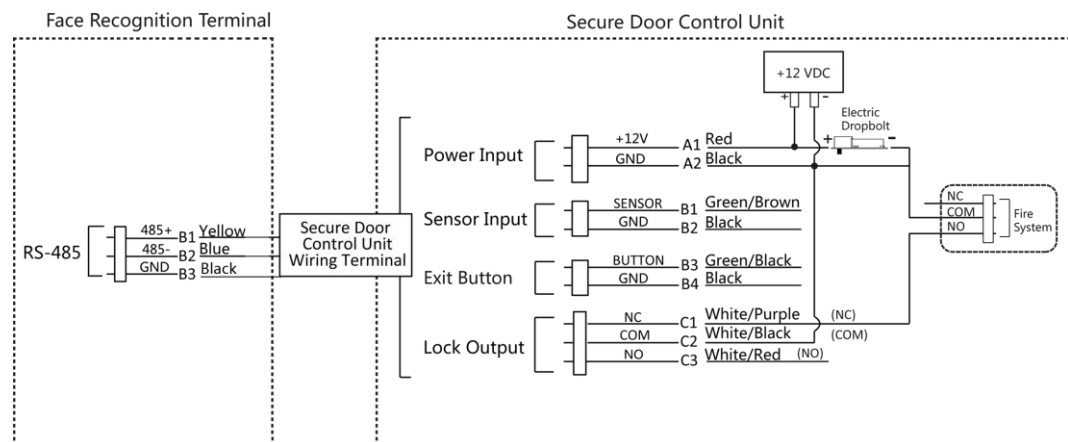
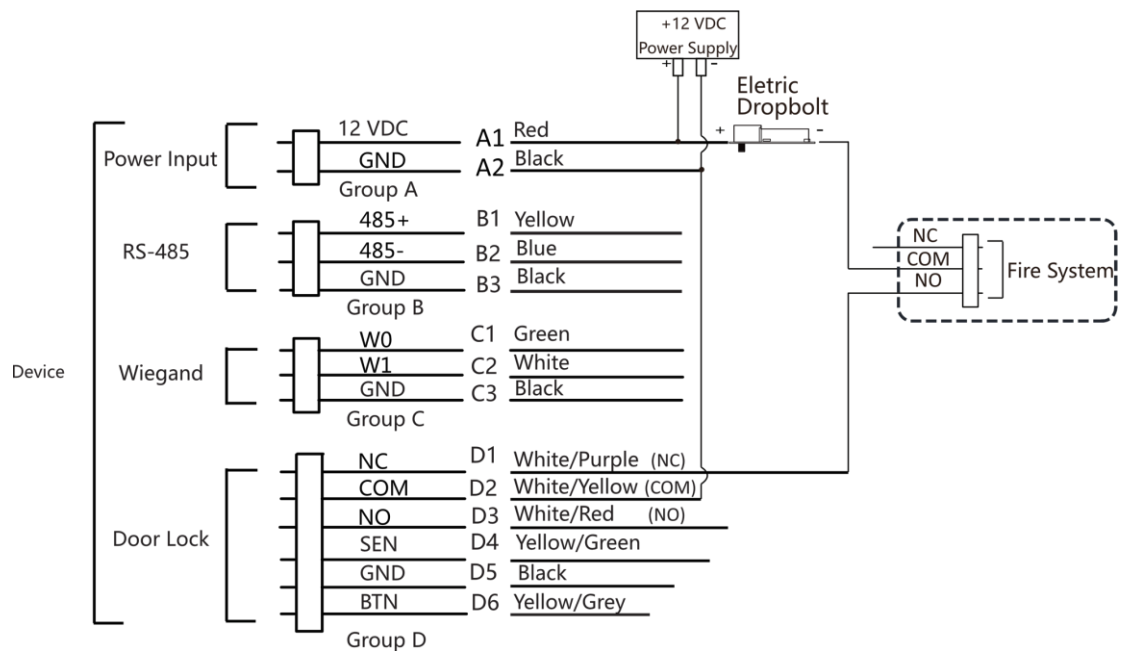


図4-4 ワイヤー固定式ドア制御ユニット

タイプ2



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



4.4.2 電源切断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

プ: 電源切断時にドアがロックされる

シナリオ: 火災連動装置と接続された入口/出口に設置



- 無停電電源装置（UPS）が必要です。
- 火災警報システム（NCとCOM、電源オフ時に通常閉回路）は、ロックと電源供給装置と直列接続されています。火災警報が作動した場合、ドアは開いたままになります。通常時、NCとCOMは開回路です。

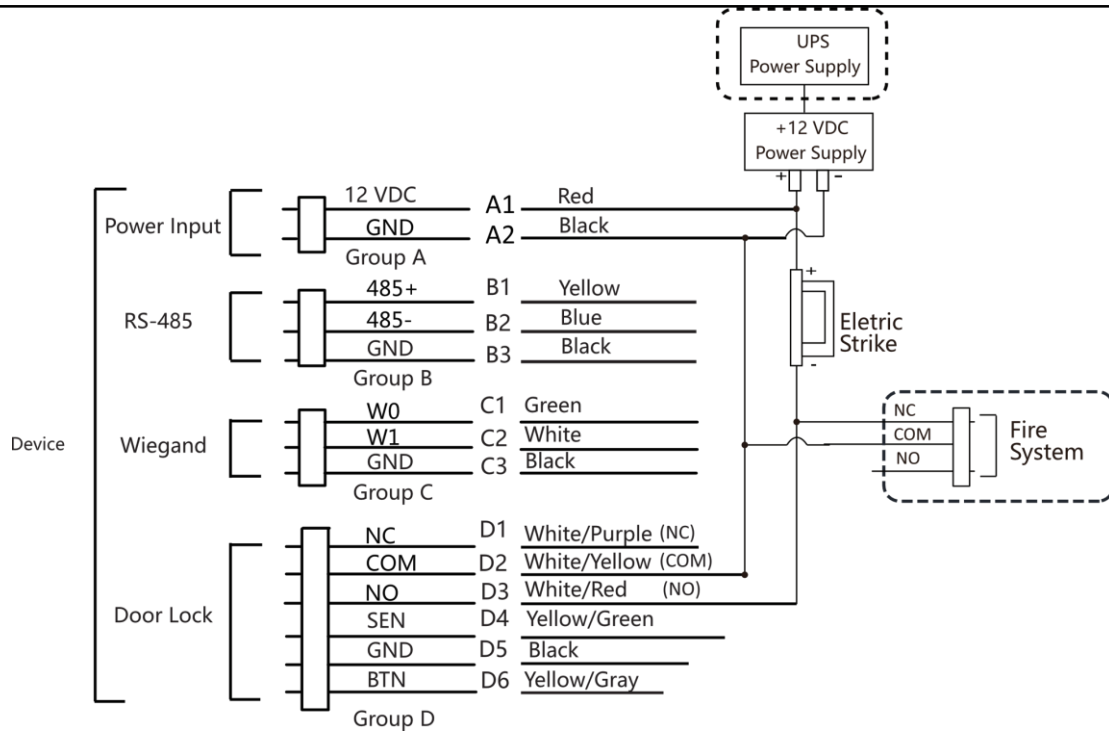


図4-7 装置配線図

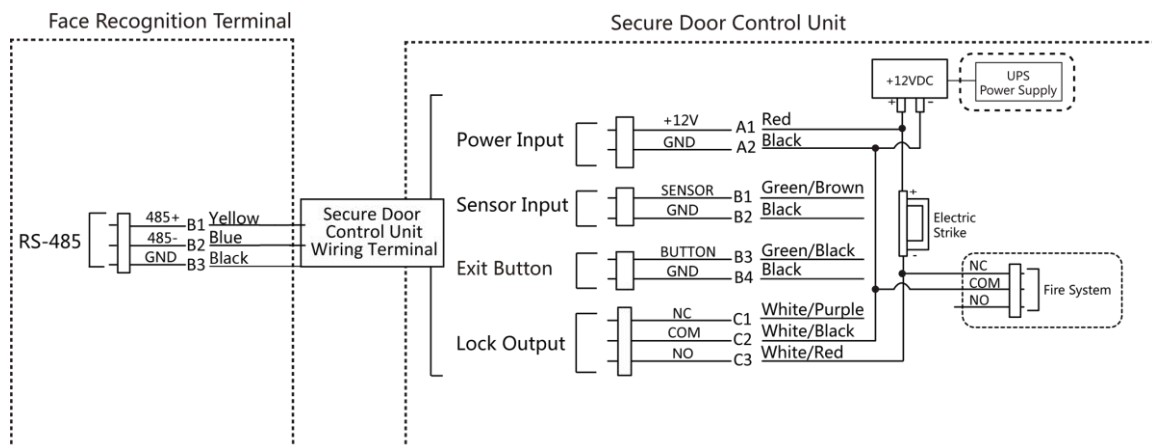


図4-8 配線図

第5章 アクティベーション

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

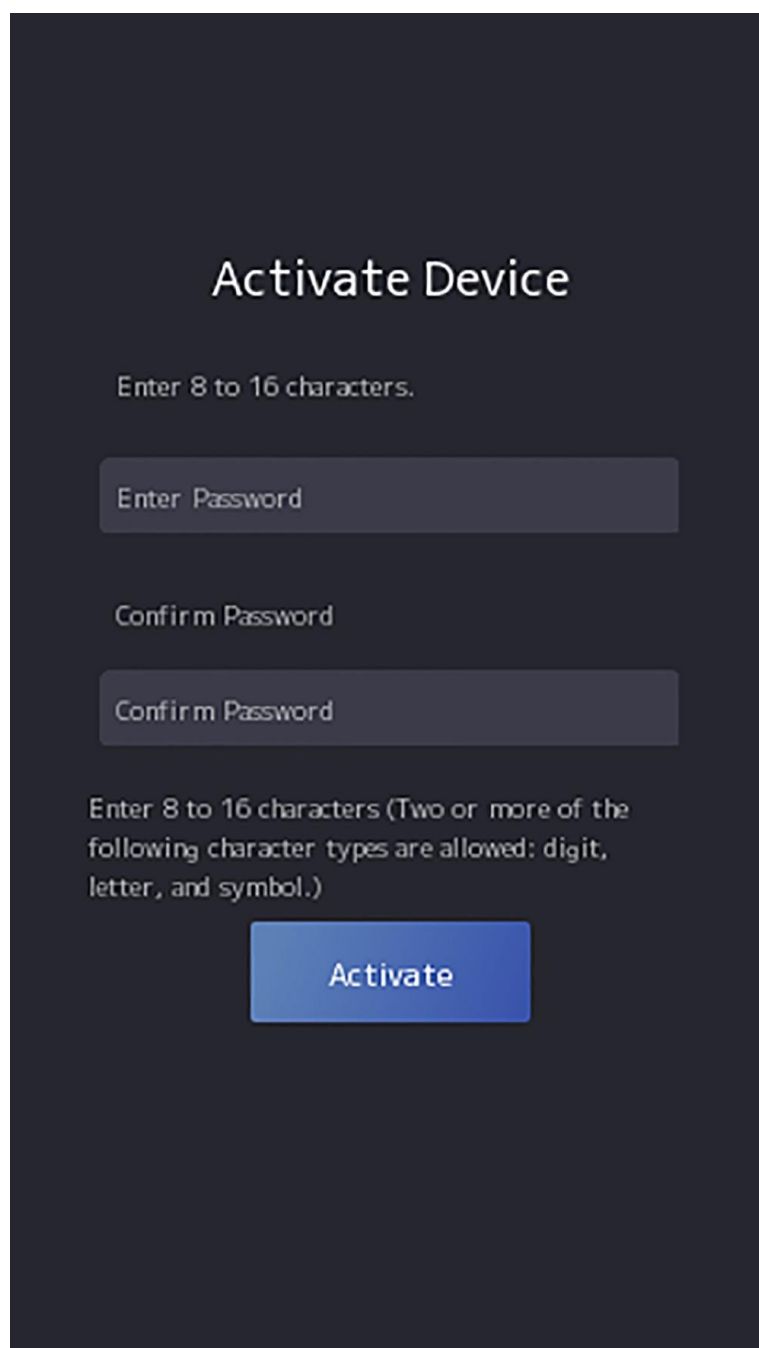
デバイスのアクティベーションは、デバイス本体、SADPツール、およびクライアントソフトウェアから行うことができます。デバイスのデフォルト値は次のとおりです：

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

5.1 デバイス経由でアクティベート

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

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



Activate Device

Enter 8 to 16 characters.

Enter Password

Confirm Password

Confirm Password

Enter 8 to 16 characters (Two or more of the following character types are allowed: digit, letter, and symbol.)

Activate

図5-1 アクティベーション画面



注意

デバイスのパスワードの強度は自動的にチェックされます。最低8文字以上（少なくとも1文字は英大文字、1文字は小文字、1文字は数字、1文字は特殊文字を含む）のパスワードに変更することを強くおすすめします。

以下の3種類のカテゴリ（大文字、小文字、数字、特殊文字）を使用することで、製品のセキュリティを強化します。また、特に高セキュリティシステムでは、パスワードを定期的に変更することをおすすめします。月次または週次でのパスワード変更は、製品の保護をさらに強化します。

すべてのパスワードおよびその他のセキュリティ設定の適切な設定は、インストール担当者および/またはエンドユーザーの責任です。

**注意**

- デバイスのパスワードの強度は自動的に確認できます。製品のセキュリティを強化するため、ご自身で選択したパスワード（8文字以上で、大文字、小文字、数字、特殊文字の少なくとも3種類を含む）に変更することを強くおすすめします。また、特に高セキュリティシステムでは、パスワードを定期的に変更することをおすすめします。月次または週次での変更は、製品の保護をさらに強化します。
 - すべてのパスワードおよびその他のセキュリティ設定の適切な設定は、サービスプロバイダーおよび/またはエンドユーザーの責任です。
 - パスワードには以下の文字を含めないでください：ユーザー名、123、admin（大文字小文字区別なし）、4つ以上の連続する増加または減少する数字、または4つ以上の連続する同じ文字。
 - パスワードには「hik」「hkws」「hikvision」などの単語を含めることはできません（大文字小文字は区別されません）。
-
- 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、[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。詳細については、「[ネットワークパラメーターの設定](#)」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。詳細については、「[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、該当の項目を確認してください。詳細については、[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、デバイスのパラメーターを管理するための管理者ユーザーを追加する必要がある場合は、管理者ユーザーを設定してください。詳細については、「[管理者ユーザーの追加](#)」を参照してください。

5.2 ウェブブラウザ経由でアクティベート

デバイスはウェブブラウザ経由でアクティベートできます。

手順

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

**メモ**

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

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

**注意**

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

3. 「アクティベート」をクリックしてください。

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

5.3 SADP経由でアクティベート

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

開始前に

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

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

手順

1. SADP ソフトウェアを実行し、オンラインデバイスを検索します。
 2. オンラインのデバイス一覧からデバイスを選択してください。
 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てください。
-

**注意**

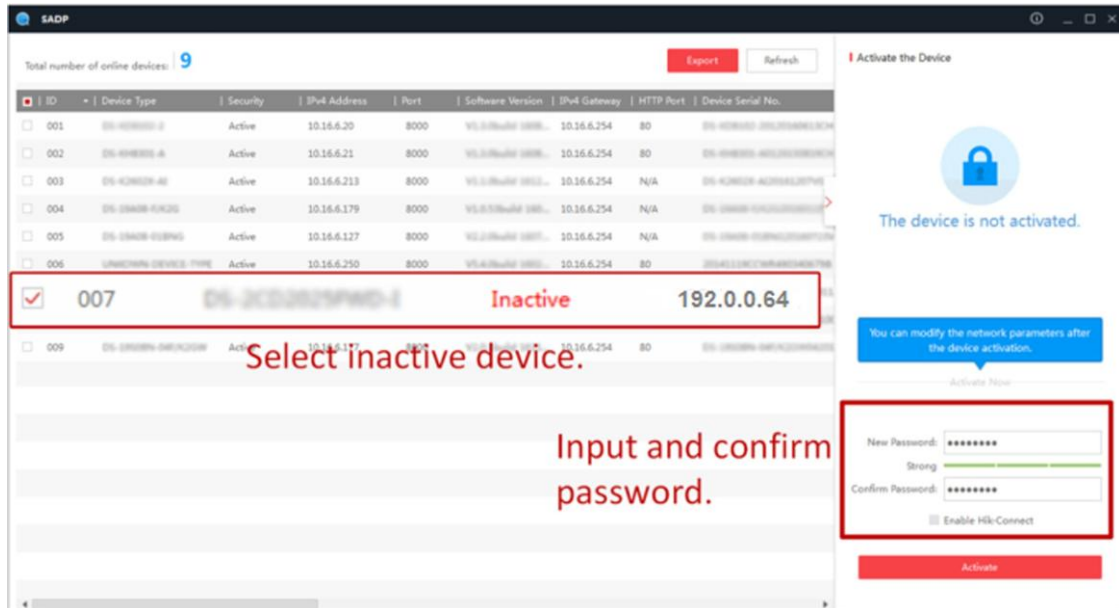
強固なパスワードの使用を推奨します-製品のセキュリティを強化するため、ご自身で選択した強固なパスワード（大文字、小文字、数字、特殊文字を組み合わせた8文字以上）を設定することを強く推奨します。また、特に高セキュリティシステムでは、パスワードを定期的に変更することを推奨します。月次または週次でのパスワード変更は、製品の保護をさらに強化します。



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てください。



デバイスの状態は、アクティベーションが正常に完了すると「アクティブ」になります。

5. デバイスのIPアドレスを変更します。

- 1) デバイスを選択します。
- 2) デバイスのIPアドレスを、コンピュータと同じサブネットに設定します。これには、IPアドレスを手動で変更するか、**DHCPを有効にするか**を選択します。
- 3) 管理パスワードを入力し、**[変更]**をクリックしてIPアドレスの変更を有効化します。

5.4 iVMS-4200クライアントソフトウェアを使用してデバイスをアクティベートします。

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

手順



注意

この機能はデバイスでサポートされている必要があります。

1. デバイス管理ページを開きます。
2. デバイス管理の右側にある「」をクリックし、デバイスを選択します。
3. 「オンラインデバイス」をクリックして、オンラインデバイス領域を表示します。検索されたオンラインデバイスがリストに表示されます。
4. セキュリティ レベル列に表示されるデバイス ステータスを確認し、非アクティブなデバイスを選択します。

5. 「アクティベート」をクリックしてアクティベーションダイアログを開きます。
6. パスワードフィールドにパスワードを入力し、パスワードを確認します。



注意

デバイスのパスワードの強度は自動的に確認できます。製品のセキュリティを強化するため、ご自身で選択したパスワード（8文字以上で、大文字、小文字、数字、特殊文字の少なくとも3種類を含む）に変更することを強くおすすめします。また、特に高セキュリティシステムでは、パスワードを定期的に変更することをおすすめします。月次または週次での変更は、製品の保護をさらに強化します。

すべてのパスワードおよびその他のセキュリティ設定の適切な設定は、インストール担当者および/またはエンドユーザーの責任です。



注意

「admin」および「nimda」を含む文字は、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有効化します。

第6章 快速操作

6.1 言語を選択

デバイスのシステム言語を選択できます。

デバイスのアクティベーション後、デバイスのシステム言語を選択できます。

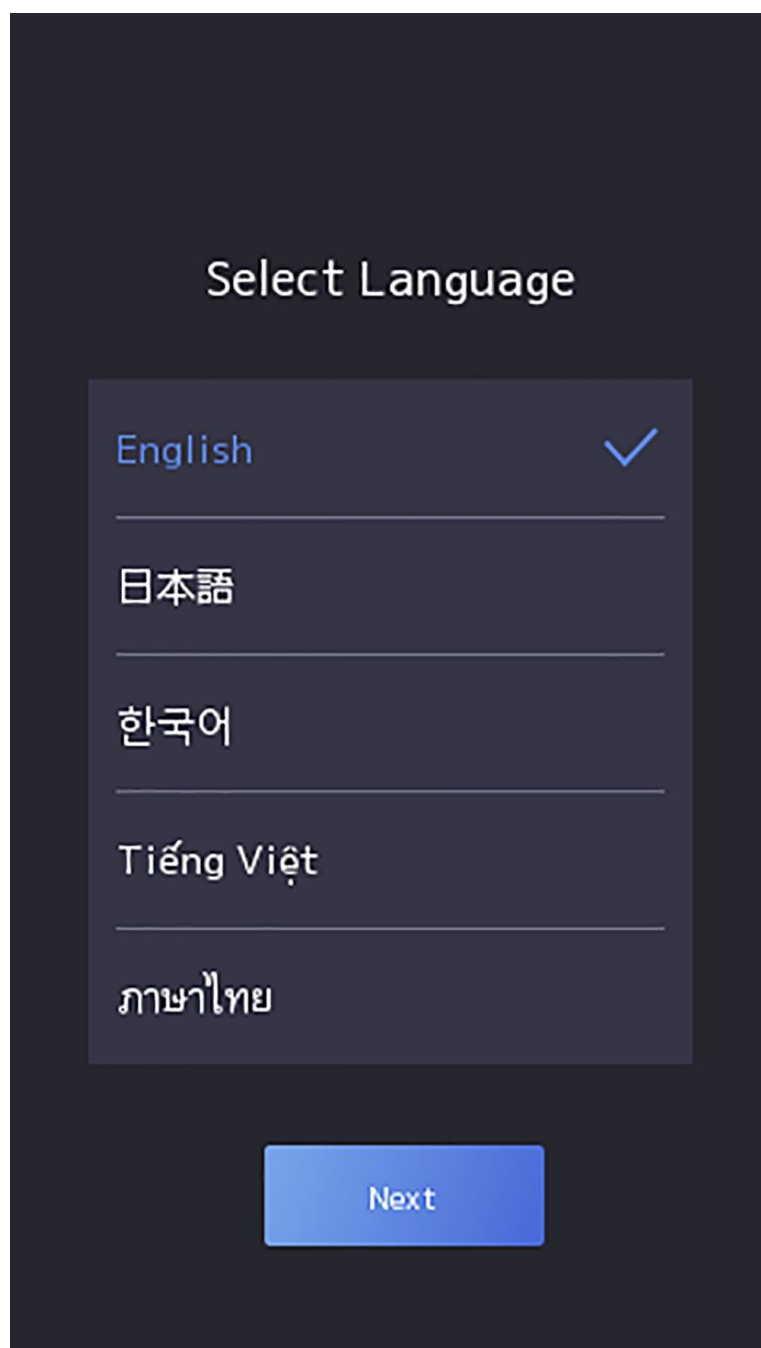


図6-1 システム言語の選択

デフォルトでは、システム言語は英語です。



注意

システム言語を変更すると、デバイスが自動的に再起動します。

6.2 パスワード変更タイプの設定

デバイスをアクティベートした後、パスワードの変更方法を「予約済みメールアドレス」または「セキュリティ質問」から選択できます。デバイスパスワードを忘れた場合、選択した変更方法を使用してパスワードを変更できます。

メールアドレス経由でパスワードを変更する

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

セキュリティ質問経由での変更

セキュリティ質問でパスワードを変更する必要がある場合は、「**セキュリティ質問に変更**」をタップします。

右上隅をクリックします。セキュリティ質問を選択し、回答を入力します。**次**に進みます。



注意

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

6.3 ネットワークパラメーターの設定

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

手順



注意

一部のデバイスモデルではWi-Fi機能がサポートされています。詳細は実際のデバイスをご確認ください。

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

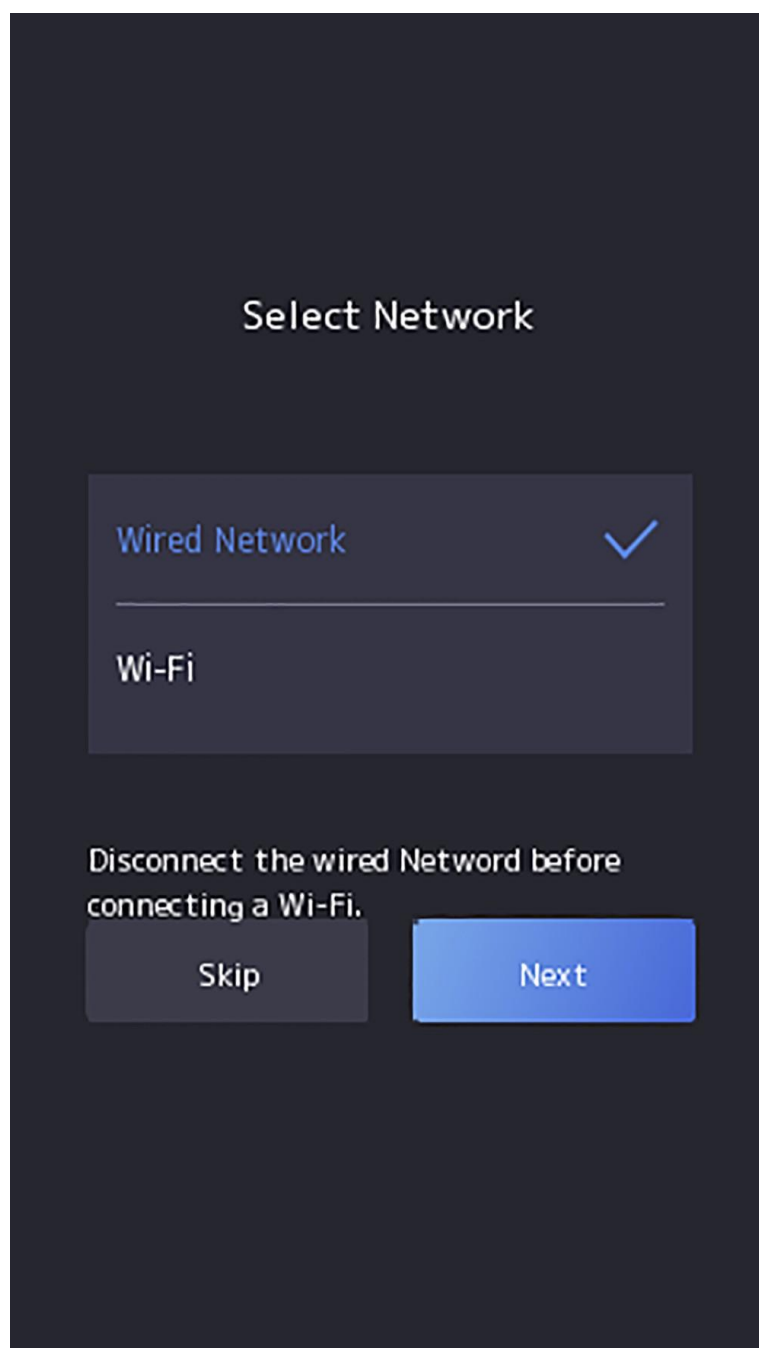


図6-2 ネットワーク選択



注 Wi-Fiに接続する前に、有線ネットワークを解除してください。

-
2. 「次へ」をタップします。有線ネットワーク



注意

デバイスがネットワークに接続されていることを確認してください。

DHCPを有効にしている場合、システムがIPアドレスその他のパラメーターを自動的に割り当てます。**DHCP**を無効にしている場合、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

機能を有効にすると、デバイスはHik-Connect経由で通信可能になります。デバイスをHik-Connectモバイルクライアント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と検証コードを設定します。

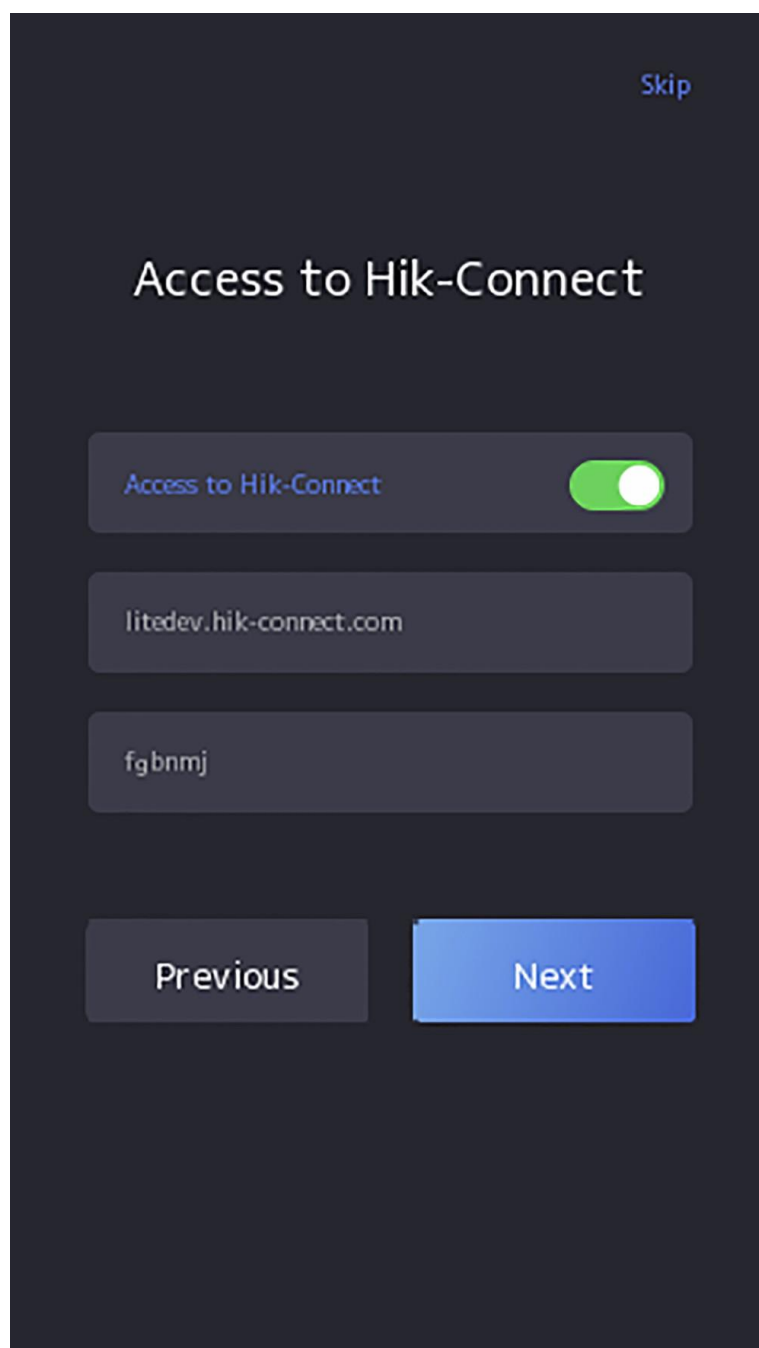


図6-3 Hik-Connectへのアクセス

2. 次へをタップします。



「前の画面に戻る」をタップしてWi-Fi設定画面に戻った場合、接続中のWi-Fiをタップするか、別のWi-Fiに接続する必要があります。これにより、プラットフォーム画面に再びアクセスできます。

6.5 プライバシー設定

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

実際のニーズに応じてパラメーターを選択してください。

認証時に撮影した写真をアップロード（認証時に撮影した写真をアップロード）

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。

認証時に撮影した写真を保存（認証時に撮影した写真を保存）

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。

登録した画像を保存（登録した画像の保存）

この機能を有効にすると、登録された顔画像がシステムに保存されます。

リンクキャプチャ後に画像をアップロード（リンクキャプチャ後に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。

リンクキャプチャ後に画像を保存（リンクキャプチャ後に画像を保存）

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

通話中に撮影した写真をアップロード

通話中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。

「次へ」をタップして設定を完了します。

6.6 管理者設定

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

開始前に

デバイスをアクティベートし、アプリケーションモードを選択します。

手順

1. オプション: 必要に応じて「スキップ」をタップして管理者の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。

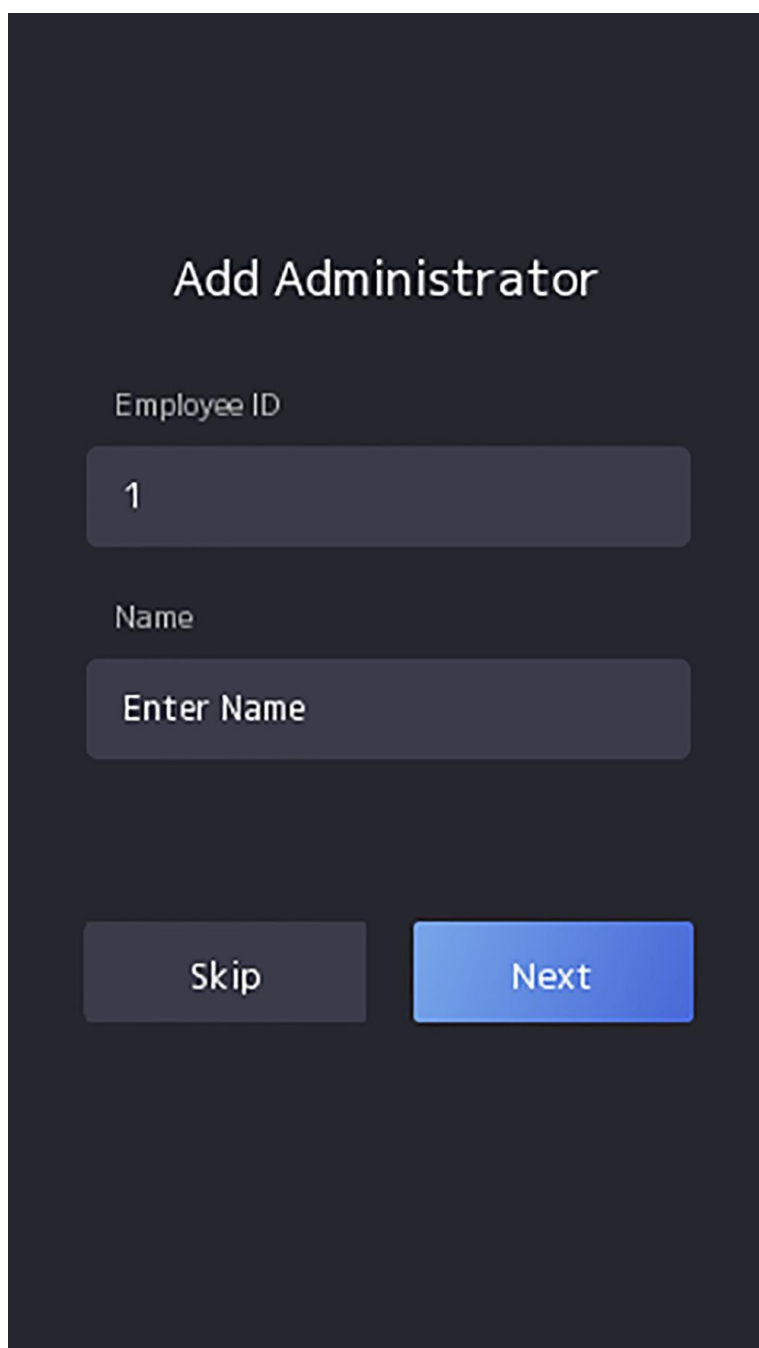


図6-4 管理者追加画面

3. 追加する認証情報を選択します。



1つの認証情報のみを追加してください。

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

認証画面が表示されます。

ステータスアイコンの説明



デバイスが武装状態/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/接続されていない/接続に失敗しました。



デバイスのWi-Fiは有効で接続中/接続されていません/有効ですが接続されていません。

ショートカットキーの説明



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。詳細については、**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連絡します。



デバイスがセンターに追加されていない場合、呼び出し操作は失敗します。



PINコードを入力して認証してください。

第7章 基本操作

7.1 ログイン

デバイスにログインして、デバイスの基本パラメーターを設定します。

7.1.1 管理者によるログイン

デバイスに管理者ユーザーを追加した場合、デバイスの操作を行うためには、その管理者ユーザーのみがログイン可能です。

手順

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

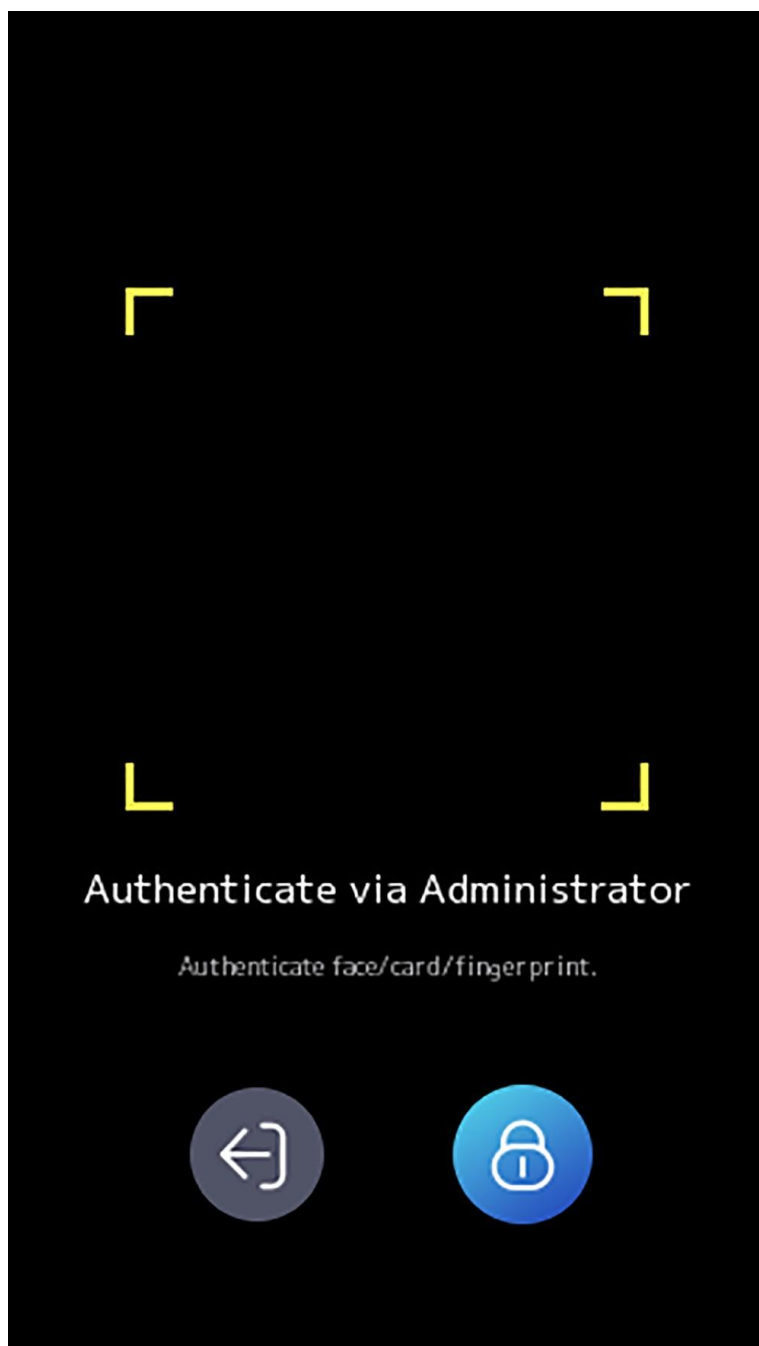


図7-1 管理者ログイン

2. 管理者の顔、指紋、またはカードで認証し、ホーム画面にアクセスします。

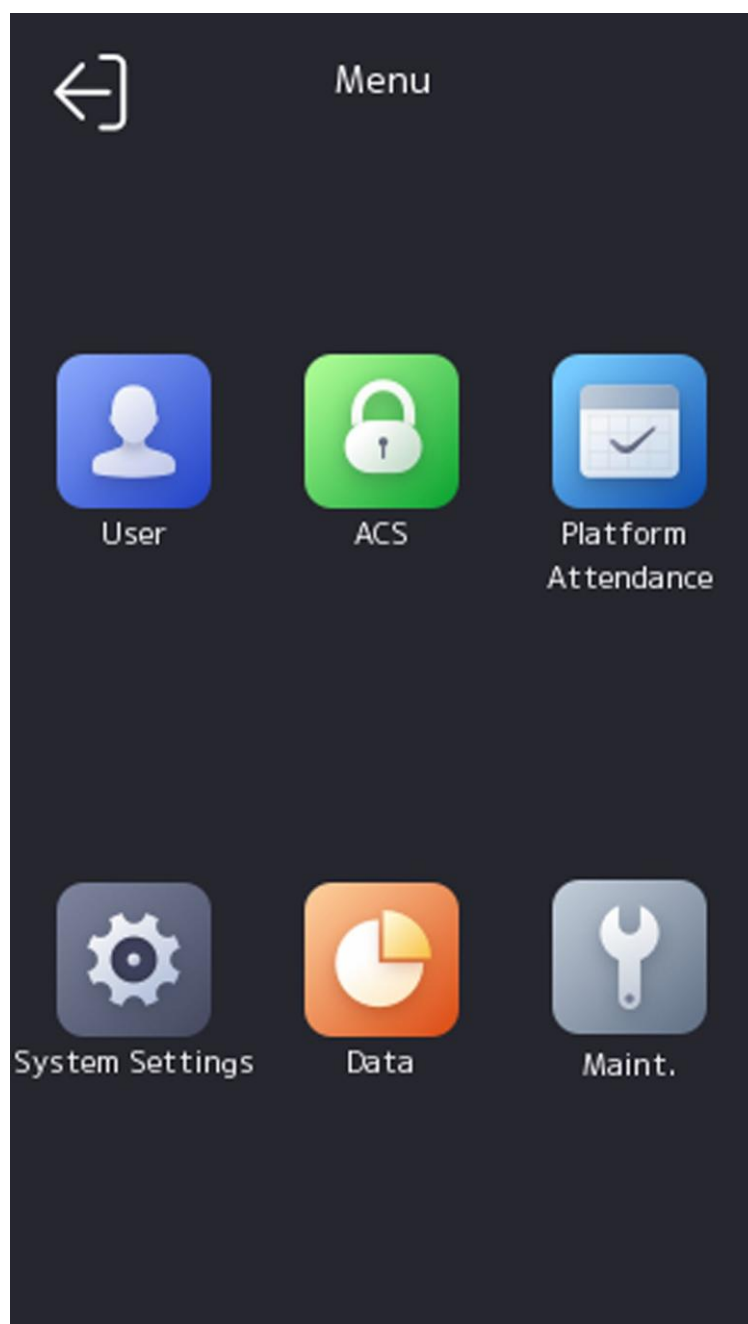


図7-2 ホーム画面



デバイスは、指紋またはカードによる認証が5回連続で失敗した場合、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、ログイン用にデバイスのアクティベーションパスワードを入力できます。
4. オプション: タップ  を選択すると、管理ログイン画面から退出できます。

7.1.2 アクティベーションパスワードでログイン

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

手順

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



注意

パスワードの入力が5回失敗すると、デバイスは30分間ロックされます。

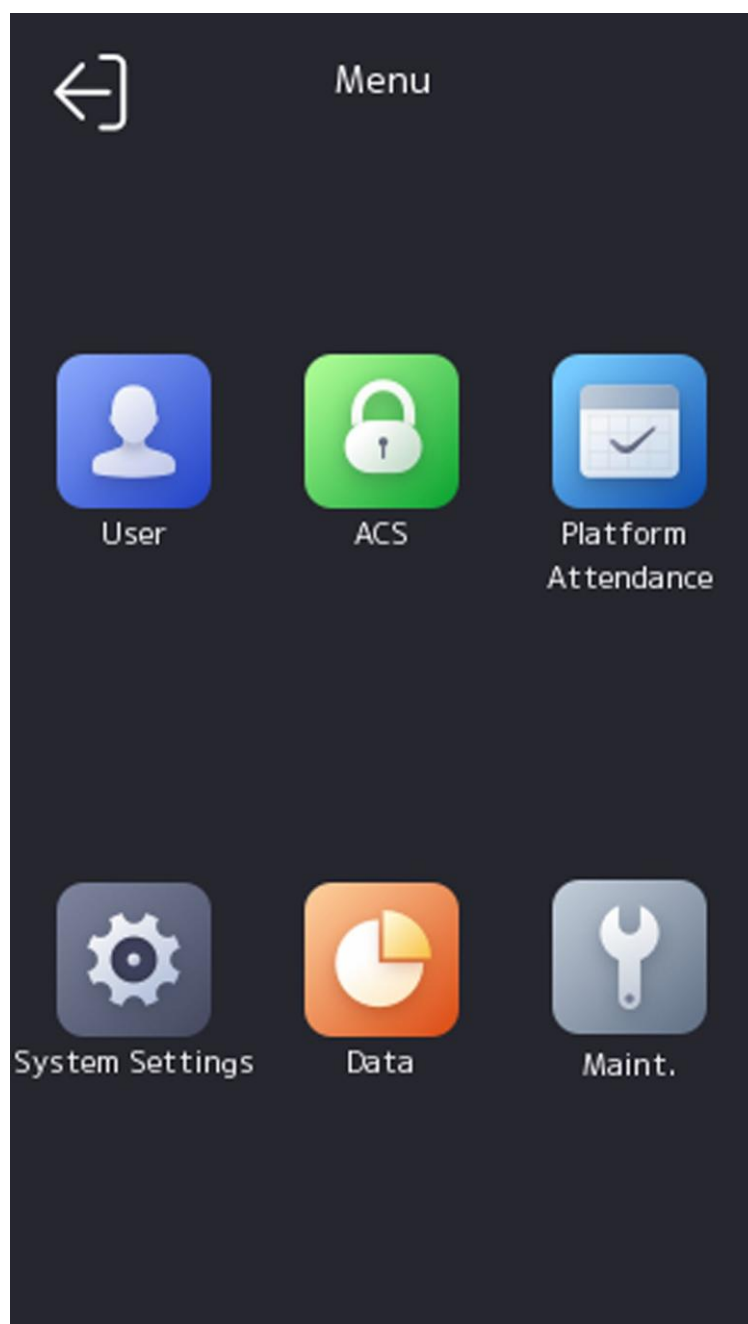


図7-3 ホームページ

7.1.3 パスワードを忘れた

認証時にパスワードを忘れた場合、パスワードを変更できます。

手順

1. 最初の画面を3秒間長押しし、ジェスチャーに従って左右にスワイプしてログイン画面に移動します。
2. **オプション:** 管理者設定がされている場合、ポップアップの管理者認証画面で「」をタップします。
3. 「パスワードを忘れた」をタップします。
4. リストからパスワード変更の種類を選択します。



パスワードの変更タイプを1つだけ設定した場合、対応するパスワード変更ページに移動し、さらに設定を続行します。

5. セキュリティ質問に回答するか、メールアドレスに応じてパスワードを変更してください。
 - セキュリティ質問: アクティベーション時に設定したセキュリティ質問に回答してください。
 - メールアドレス



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

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



QRコードをタップして、より大きな画像を表示します。

- d. デバイス画面に表示された検証コードを入力してください。
6. 新しいパスワードを作成し、確認してください。
 7. **OK**をタップしてください。

7.2 通信設定

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

7.2.1 有線ネットワークパラメーターを設定する

デバイスの有線ネットワーク設定（IPアドレス、サブネットマスク、ゲートウェイ、DNS設定など）を設定できます。

手順

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

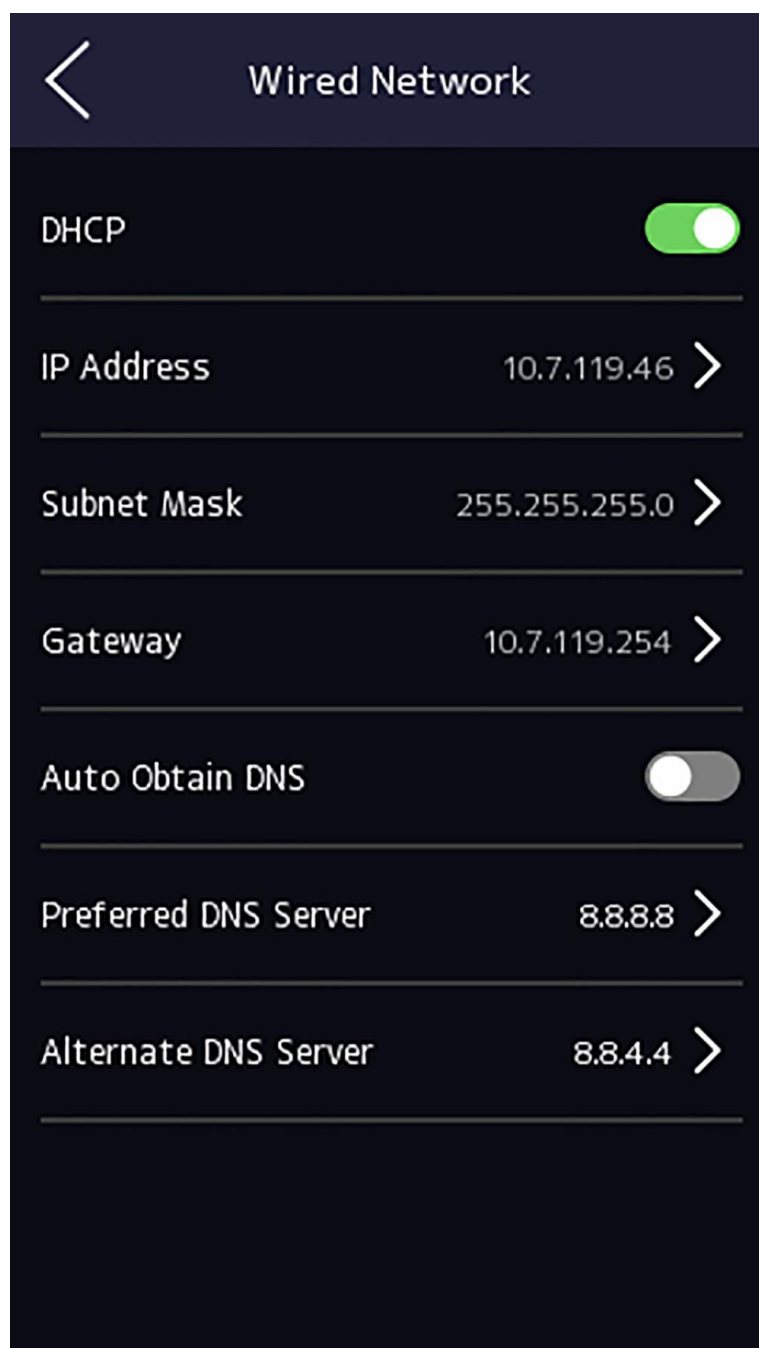


図7-4 有線ネットワーク設定

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**を無効にし、IPアドレス、サブネットマスク、およびゲートウェイを手動で設定する必要があります。



注意

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

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

7.2.2 Wi-Fi パラメーターを設定します

Wi-Fi機能を有効にし、Wi-Fi関連のパラメーターを設定できます。

手順



注意

この機能はデバイスでサポートされている必要があります。

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

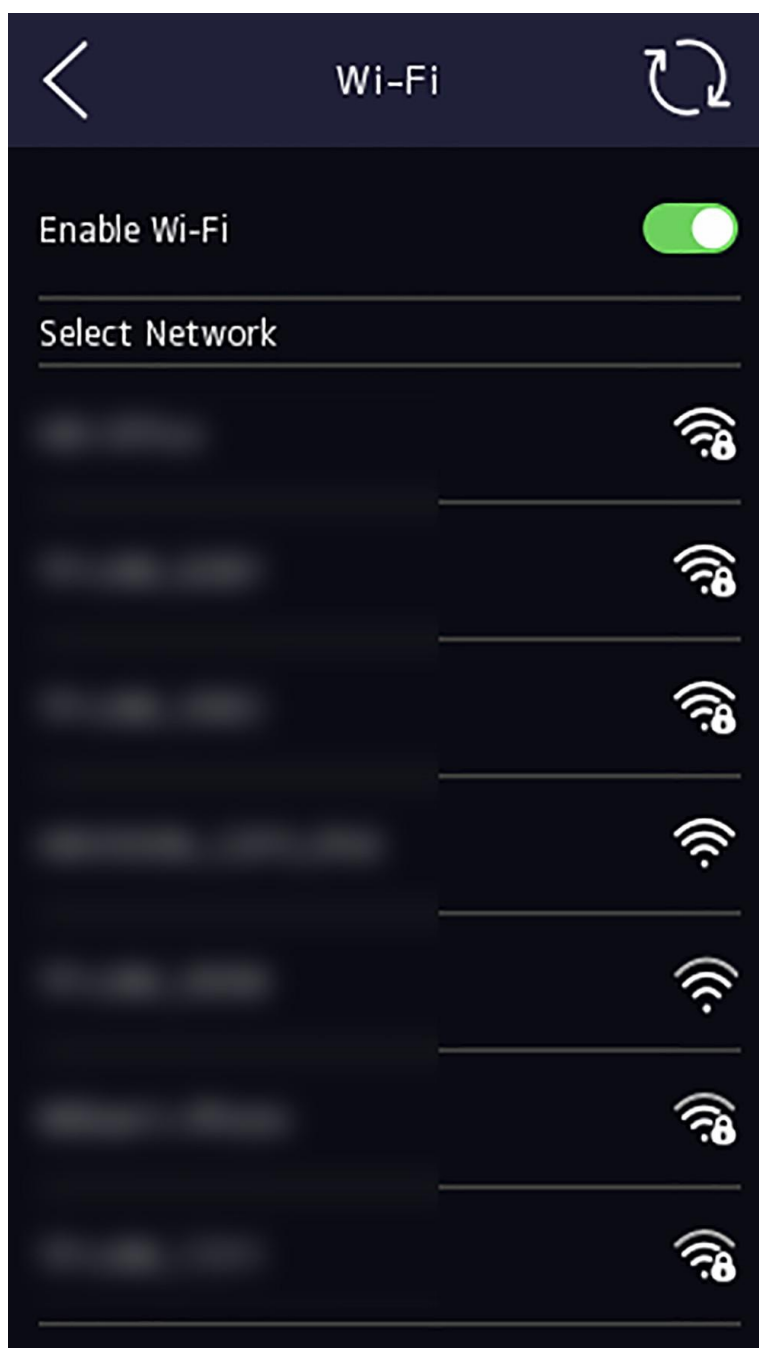


図7-5 Wi-Fi設定

3. Wi-Fi機能を有効にします。

4. Wi-Fiのパラメーターを設定します。

- リストからWi-Fiを選択し、Wi-Fiのパスワードを入力します。**OK**をタップします。
- 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、および特殊文字のみが使用可能です。

5. Wi-Fi の設定を行います。

- デフォルトではDHCPが有効になっています。システムがIPアドレス、サブネットマスク、ゲートウェイを自動的に割り当てます。
- DHCPを無効にする場合、IPアドレス、サブネットマスク、およびゲートウェイを手動で入力する必要があります。

6. OKをタップして設定を保存し、Wi-Fi タブに戻ります。

**7. **をタップしてネットワークパラメーターを保存します。

7.2.3 RS-485パラメーターを設定します。

顔認識端末は、RS-485端子経由で外部アクセスコントローラー、セキュアドア制御ユニット、またはカードリーダーと接続可能です。

手順

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

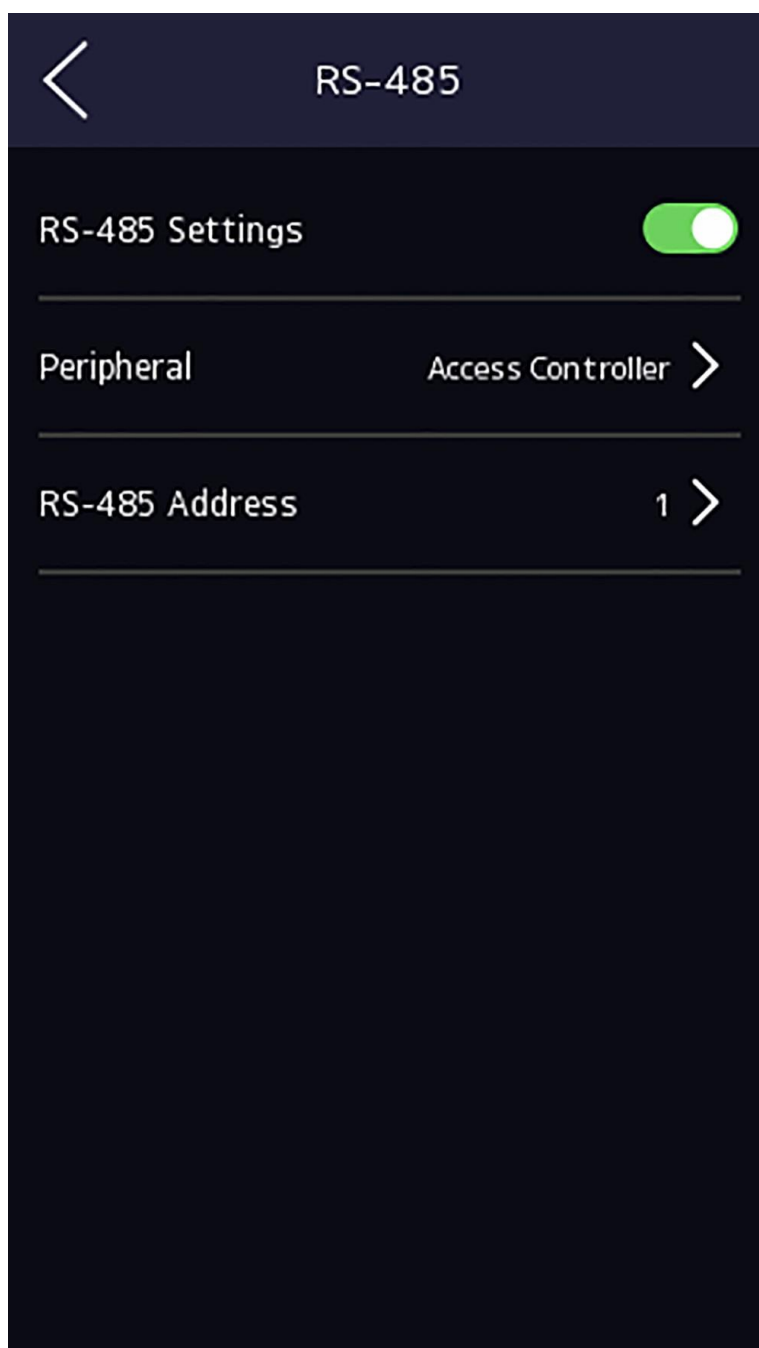


図7-6 RS-485パラメーターの設定

3. 実際の要件に応じて周辺機器の種類を選択します。



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

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

7.2.4 Wiegand パラメーターの設定

Wiegandの送信方向を設定できます。

手順

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

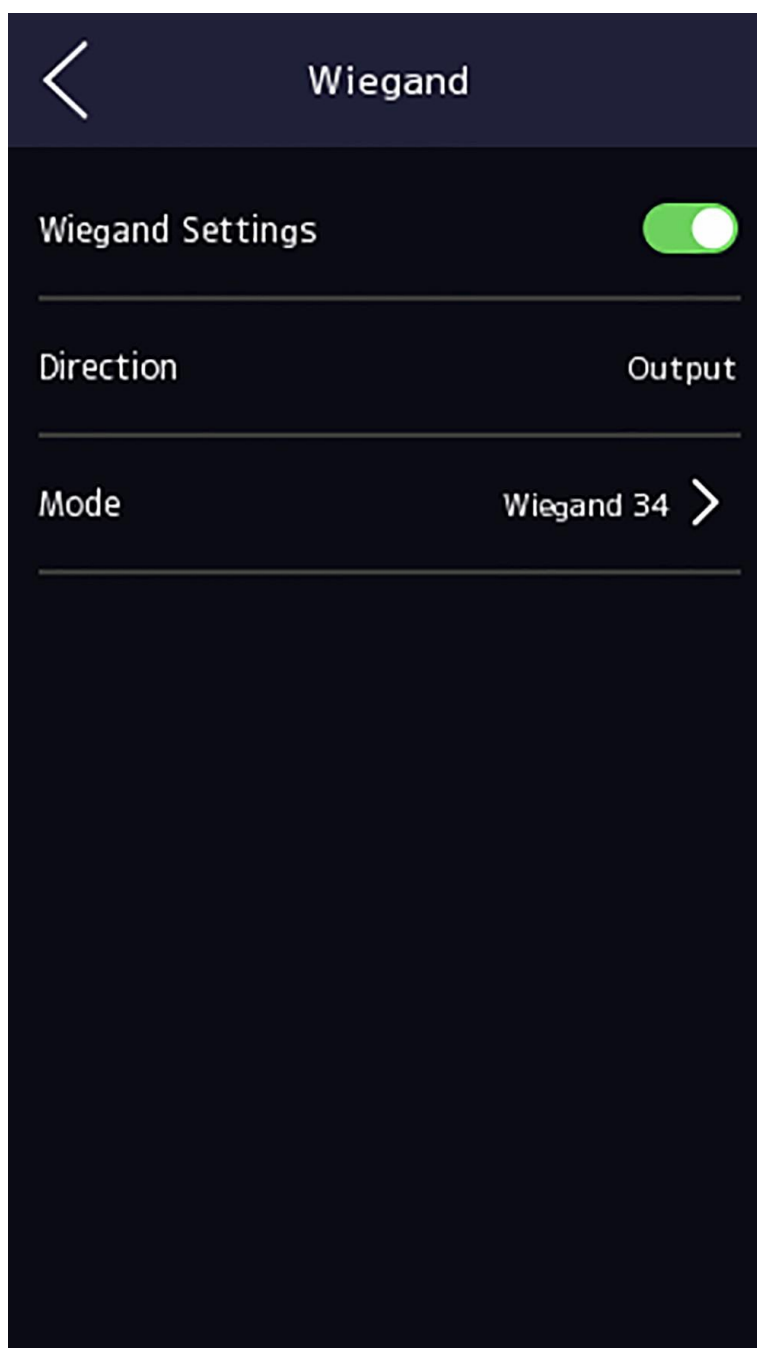


図7-7 Wiegand設定

3. Wiegand機能を有効にします。
4. Wiegand モードを選択します。
 - 出力: 顔認識端末は外部アクセスコントローラーと接続可能です。両デバイスはWiegand 26またはWiegand 34経由で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ーを保存します。



注意

外部デバイスを変更した場合、デバイスパラメーターを保存した後、デバイスは自動的に再起動します。

7.2.5 ISUPパラメーターの設定

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

開始前に

デバイスがネットワークに接続されていることを確認してください。

手順

1. ホーム画面で「システム設定」→「→通信」→「→ISUP（通信設定）」をタップして設定画面に入ります。

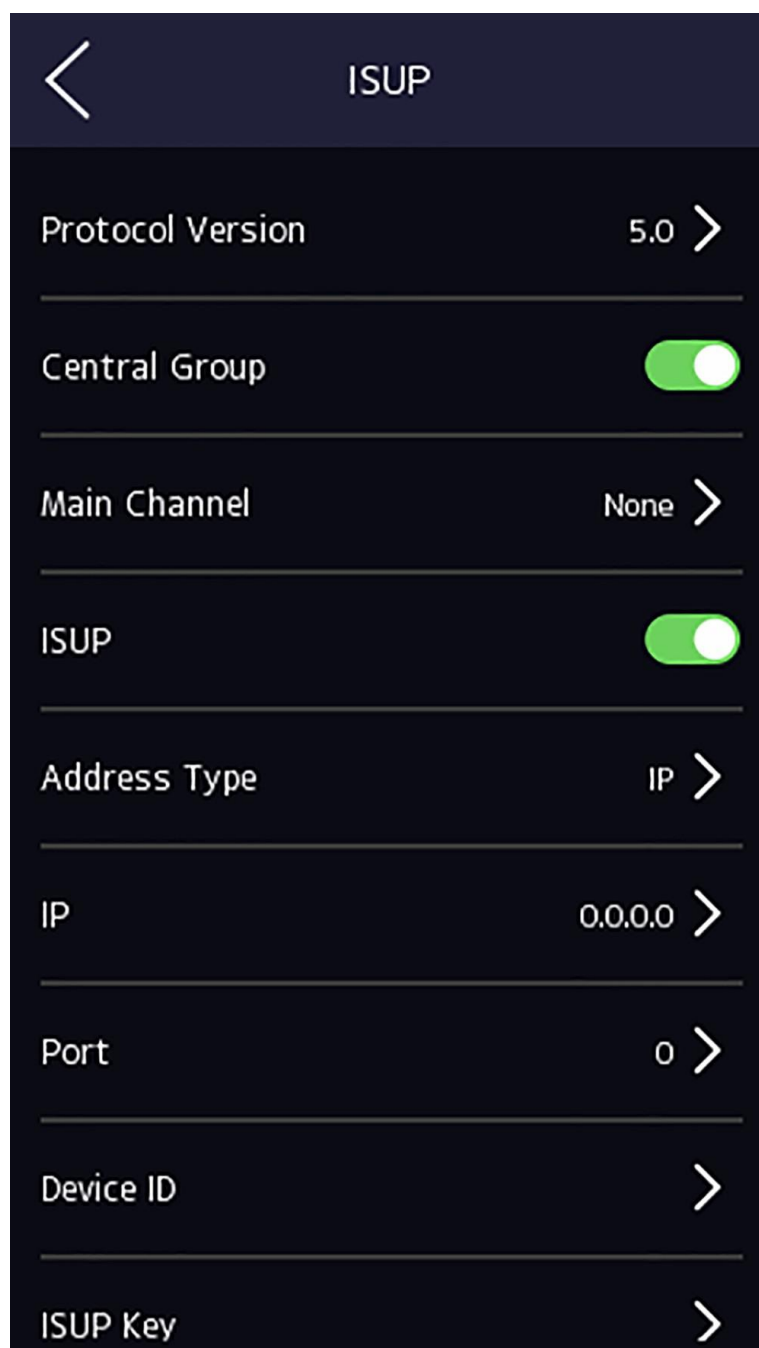


図7-8 ISUP設定

2. ISUP機能を有効にし、ISUPサーバーパラメーターを設定します。

ISUPバージョン

実際の要件に応じてISUPバージョンを設定します。

中央グループ

中央グループを有効にすると、データが中央グループにアップロードされます。

メインチャネル

N1またはNoneを選択できます。

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、適切なアドレスの種類を選択してください。

IPアドレス

ISUPサーバーのIPアドレスを設定してください。

ポート番号

ISUP サーバーのポート番号を設定してください。



注

ポート番号の範囲: 0 から 65535。

デバイスID

デバイス シリアル番号を設定します。

パスワード

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



注意

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

7.2.6 プラットフォームアクセス

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

開始前に

デバイスがネットワークに接続されていることを確認してください。

手順

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

7.2.7 SNMP設定

SNMPパラメーターを設定できます。

手順

1. ホーム画面で「システム設定」→「→」→「Comm.（通信設定）」をタップして、通信設定画面に移動します。
2. 通信設定画面で、**SNMP**をタップします。
3. **SNMP**を有効にします。
4. トラップコミュニティ文字列を設定します。
5. **NMS IP アドレス**と**NMS ポート**を設定します。

7.3 ユーザー管理

ユーザー管理画面では、ユーザーを追加、編集、削除、検索することができます。

7.3.1 管理者追加

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

手順

1. 初期画面を長押しし、バックエンドにログインします。
2. +「ユーザー」をタップします。「→」をタップして「ユーザーを追加」ページに移動します。

Add Person	
Employee ID	3
Name	Not Configured
Face	Not Configured
Card	0/50
Fingerprint	0/10
PIN	Not Configured
Auth. Settings	Device Mode
Person Type	Basic Person

3. 従業員IDを編集します。



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

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



注意

- ユーザー名には、数字、大文字、小文字、および特殊文字を使用できます。
- ユーザー名には最大32文字まで使用可能です。

5. オプション: 管理者用に顔写真、指紋、カード、またはPINを追加できます。



注意

- 顔写真を追加する方法の詳細については、「顔写真を追加する」を参照してください。



注意

指紋を追加する方法については、「指紋を追加」を参照してください。

- カードを追加する方法については、「カードを追加」を参照してください。
- パスワードの追加方法については、「PIN の追加」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

認証タイプの設定方法については、「認証モードの設定」を参照してください。

7. ユーザーの種類と役割を設定します。

8. 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

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

9. 「出席確認のみ」を有効にできます。有効化後、このユーザーにはアクセス制御権限が与えられません。

10. 「」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追加します。ユーザーは顔写真で認証できます。

手順



注意

最大1,500枚の顔写真を追加できます。

1. 最初の画面を3秒間長押しし、ジェスチャーに従って左右にスワイプし、バックエンドにログインしてください。
2. 「ユーザー」をタップし、ユーザーID（例: →）とパスワードを入力して「+」をタップし、ユーザー追加ページに移動します。
3. 従業員IDを編集します。



注意

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

-
4. 名前フィールドをタップし、ソフトキーボードにユーザー名を入力し、部門を選択します。
-



注

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

-
5. 顔写真フィールドをタップして、顔写真追加ページに移動します。
-

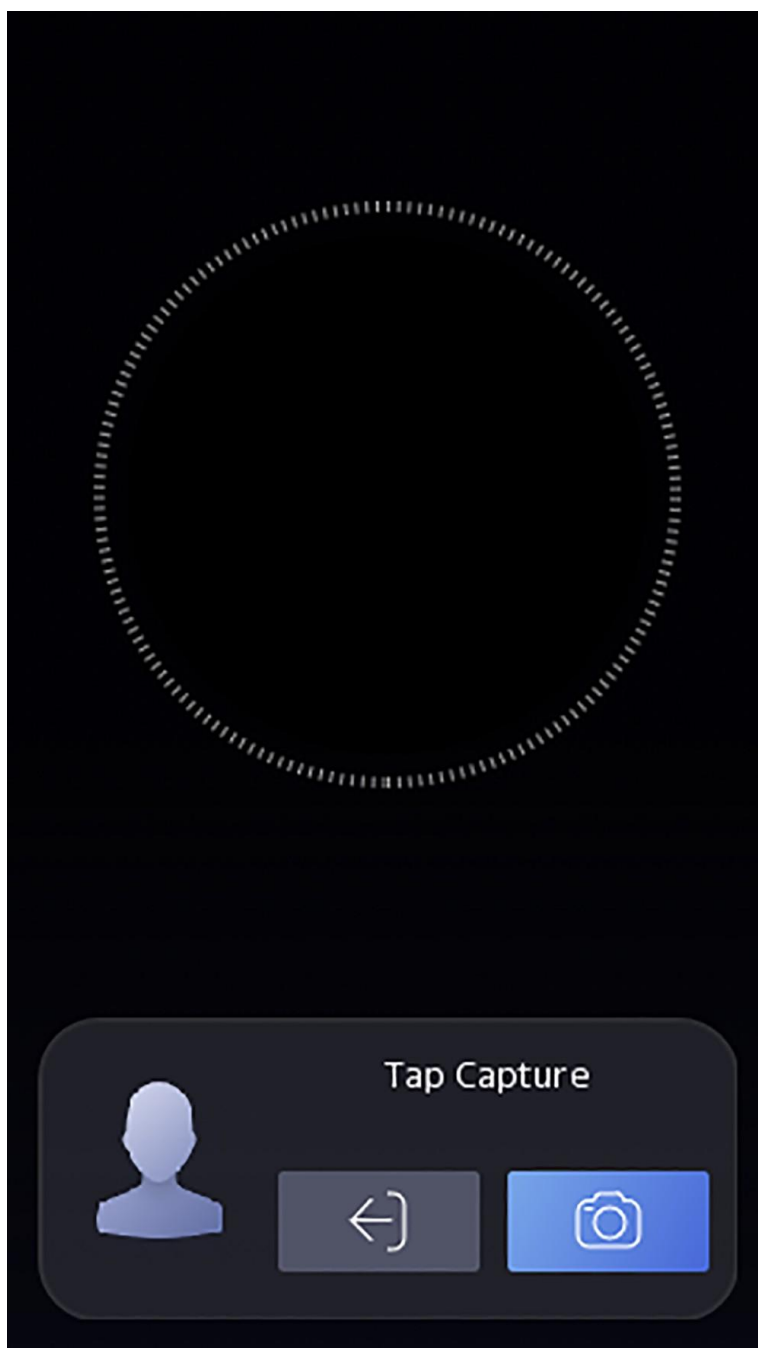


図7-9 顔画像の追加

6. カメラを見ます。



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

顔写真を完全に追加すると、ページの右上隅に撮影した顔写真が表示されます。

7. 「保存」をタップして顔写真を保存してください。
8. オプション: 「もう一度試す」をタップし、顔の位置を調整して顔写真を再度追加してください。
9. ユーザー役割を設定します。

管理者

この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画面にアクセスして操作を行うことができます。

通常ユーザー

ユーザーは通常のユーザーです。ユーザーは初期画面での認証または出席記録のみが可能です。

10. 「」をタップして設定を保存します。

7.3.3 指紋を追加

ユーザーに指紋を追加し、ユーザーは追加された指紋で認証できるようになります。

手順



- この機能はデバイスでサポートされている必要があります。
- 最大3000件の指紋を追加できます。

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



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

4. 名前フィールドをタップし、ソフトキーボードでユーザー名を入力し、部門を選択してください。

**注意**

- ユーザー名には、数字、大文字、小文字、および特殊文字を使用できます。
 - 推奨されるユーザー名は32文字以内にしてください。
-

5. 指紋フィールドをタップして、指紋を追加する画面を表示します。

6. 指示に従って指紋を追加してください。

**注意**

- 同じ指紋を繰り返し追加することはできません。
 - 1ユーザーにつき最大10つの指紋を追加できます。
 - クライアントソフトウェアまたは指紋リーダーを使用して指紋を登録することもできます。
- 指紋のスキャン方法の詳細については、[「指紋スキャンのヒント」](#)を参照してください。
-

7. ユーザー役割を設定します。

管理者

ユーザーは管理者です。通常の出席機能を除き、ユーザーは権限認証後にホーム画面にアクセスして操作を行うことができます。

通常ユーザー

ユーザーは通常のユーザーです。ユーザーは初期画面での認証または出席記録のみが可能です。

8. 「」をタップして設定を保存します。

7.3.4 カードを追加

ユーザーにカードを追加し、追加したカードで認証が可能です。

手順

**注意**

最大3,000枚のカードを追加できます。

1. 最初の画面を3秒間長押しし、ジェスチャーに従って左右にスワイプし、バックエンドにログインしてください。
 2. 「ユーザー」をタップし、→+にアクセスして「ユーザー追加ページ」を開きます。
 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を編集します。
-

**注意**

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

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



- ユーザー名には、数字、大文字、小文字、および特殊文字を使用できます。
- 推奨されるユーザー名は32文字以内にしてください。

6. カードフィールドをタップし、+をタップします。
7. カード番号を設定します。
 - 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てください。



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

8. カードの種類を設定してください。
9. ユーザー役割を設定してください。

管理者

このユーザーは管理者です。通常の出席機能を除き、権限認証後にホーム画面にアクセスして操作が可能です。

一般ユーザー

ユーザーは通常のユーザーです。ユーザーは初期画面でのみ認証または出席確認を行うことができます。

10. 「」をタップして設定を保存します。

7.3.5 PINを追加

ユーザーにPINを追加すると、ユーザーはPINを使用して認証できます。

開始前に



パスワードモードが「ローカルパスワード」または「プラットフォームパスワード」であることを確認してください。ローカルパスワードを選択した場合、デバイスまたはWeb上でPINを追加できます。プラットフォームパスワードを選択した場合、デバイスまたはWeb上でPINを追加できません。代わりに、プラットフォーム上でPINを追加する必要があります。パスワードモードの設定の詳細については、[***Authentication SeFngs***](#) を参照してください。

手順

1. 最初の画面を3秒間長押しし、ジェスチャーに従って左右にスワイプし、バックエンドにログインします。
2. 「ユーザー」をタップします。「→」をタップし、+にアクセスして「ユーザーを追加」ページに移動します。
3. 「従業員ID」フィールドをタップし、従業員IDを編集します。

**注意**

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

- 名前フィールドをタップし、ソフトキーボードにユーザー名を入力し、部門を選択します。

**注**

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

- PINコードをタップし、ユーザー用のPINを作成します。

**注意**

パスワードモードが「ローカルパスワード」に設定されていない場合、PIN領域を編集できません。

- ユーザー役割を設定します。

管理者

このユーザーは管理者です。通常の出席機能を除き、ユーザーは権限認証後にホーム画面にアクセスして操作を行うことができます。

一般ユーザー

ユーザーは通常のユーザーです。ユーザーは初期画面での認証または出席記録のみが可能です。

- 「」をタップして設定を保存します。

7.3.6 認証モードの設定

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

手順

- 最初の画面を3秒間長押しし、ジェスチャーに従って左右にスワイプし、バックエンドにログインします。
- 「ユーザー」をタップします。→「ユーザーを追加/編集」をタップします。→「認証モード」を選択します。
- 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。詳細については「アクセス制御パラメーターの設定」を参照してください。

カスタム

実際のニーズに応じて、異なる認証モードを組み合わせで使用できます。

- 「」をタップして設定を保存します。

7.3.7 ユーザーを検索して編集

ユーザーを追加した後、ユーザーを検索して編集できます。

ユーザーを検索

ユーザー管理ページで、検索領域をタップして「ユーザー検索ページ」に移動します。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。従業員ID、カード番号、またはユーザー名を入力して検索します。をタップして検索します。

ユーザーを編集

ユーザー管理ページで、ユーザー一覧からユーザーを選択し、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ーを編集します。設定を保存するには、をタップします。

 **注意**
従業員IDは編集できません。

7.4 勤怠ステータス設定

実際の状況に応じて、出勤モードを「出勤」「退勤」「休憩開始」「休憩終了」「残業開始」「残業終了」から選択できます。

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

7.4.1 デバイスによる出勤モードの無効化

出勤モードを無効にすると、システムは最初のページに出勤ステータスを表示しません。

プラットフォームの出席をタップして、T&A ステータスページに入ります。

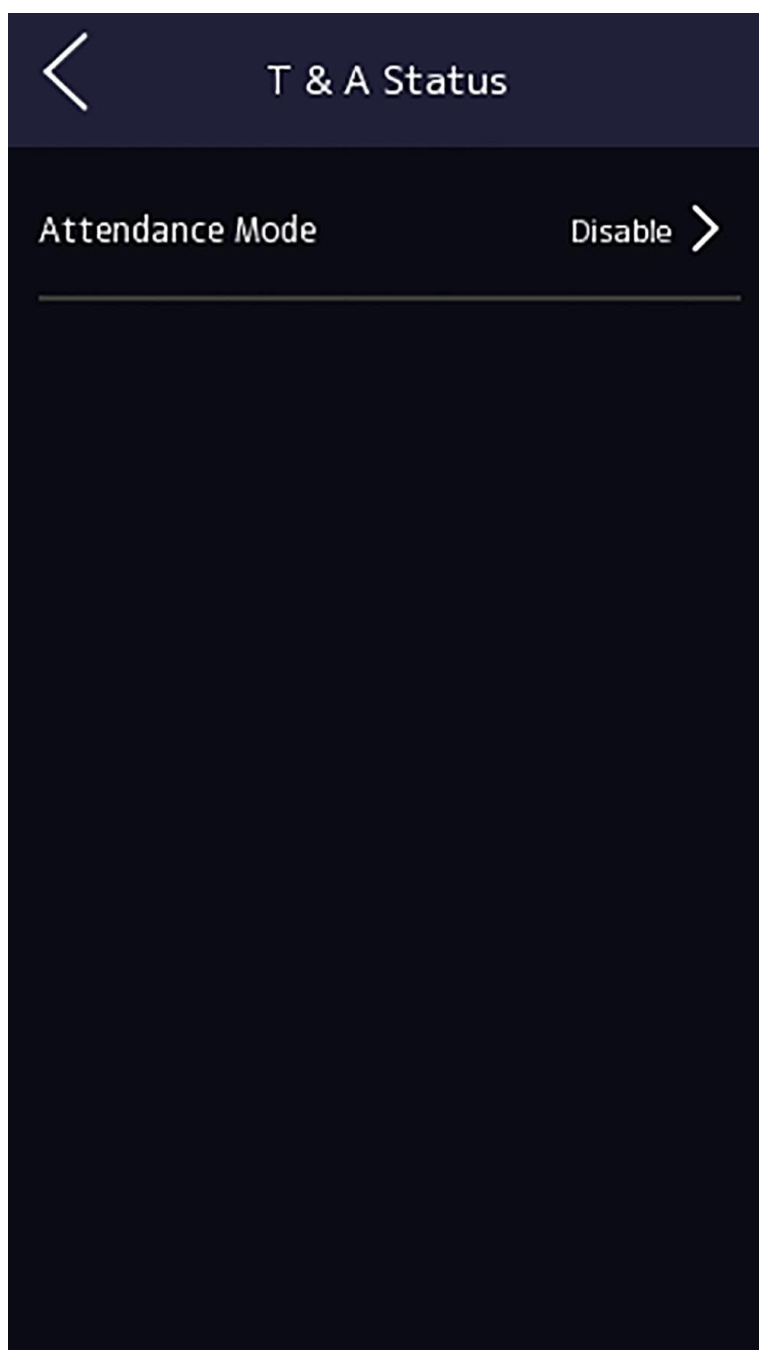


図 7-10 出勤モードを無効にする

出席モードを「無効」に設定します。

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

7.4.2 デバイス経由で手動出席を設定する

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

開始前に

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

手順

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

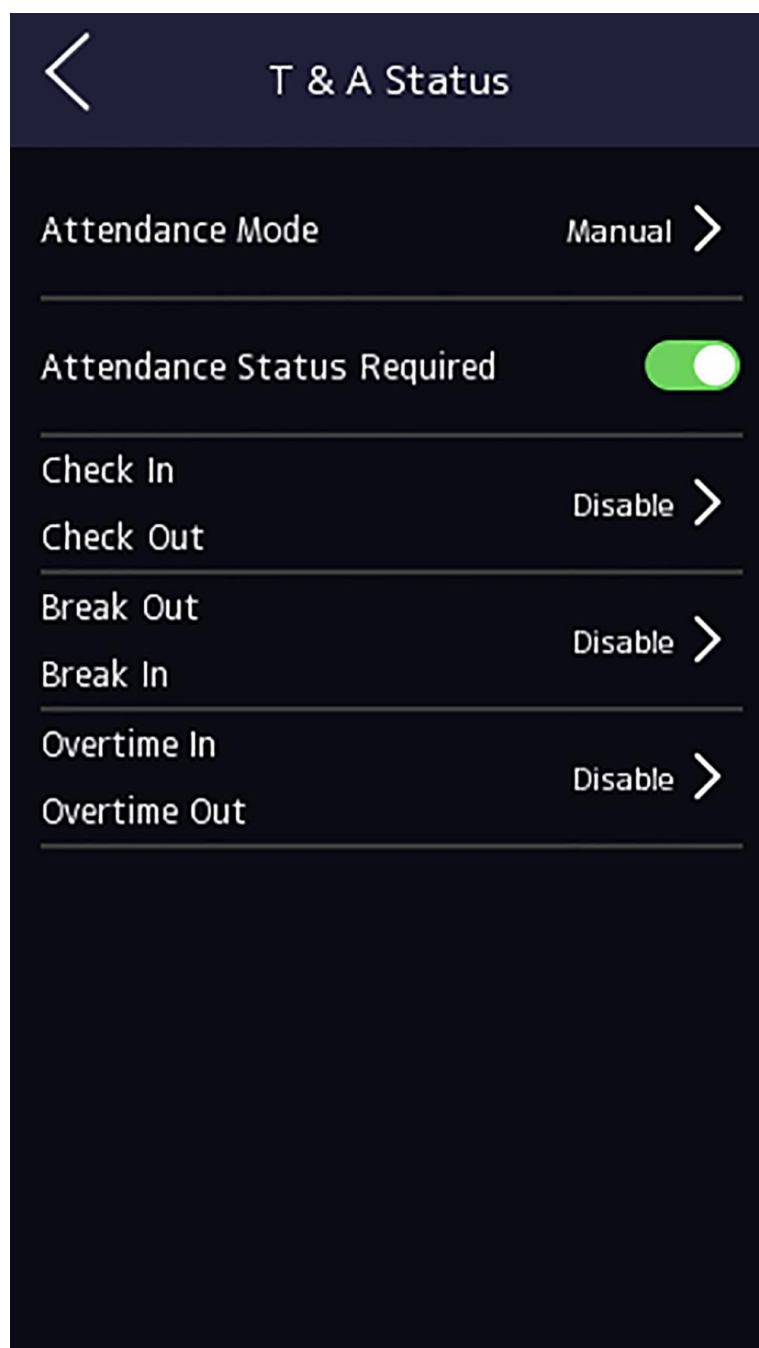


図7-11 手動出席モード

3. 出席ステータスの必須設定を有効にします。
4. 出席ステータスのグループを有効にします。



出席プロパティは変更されません。

5. オプション: 必要に応じてステータスを選択し、名前を変更できます。

名前は「T & A ステータス」ページと認証結果ページに表示されます。

結果

認証後、出席ステータスを手動で選択する必要があります。



注意

ステータスを選択しない場合、認証は失敗し、有効な出席として記録されません。

7.4.3 デバイス経由で自動出席を設定する

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

開始前に

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

手順

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

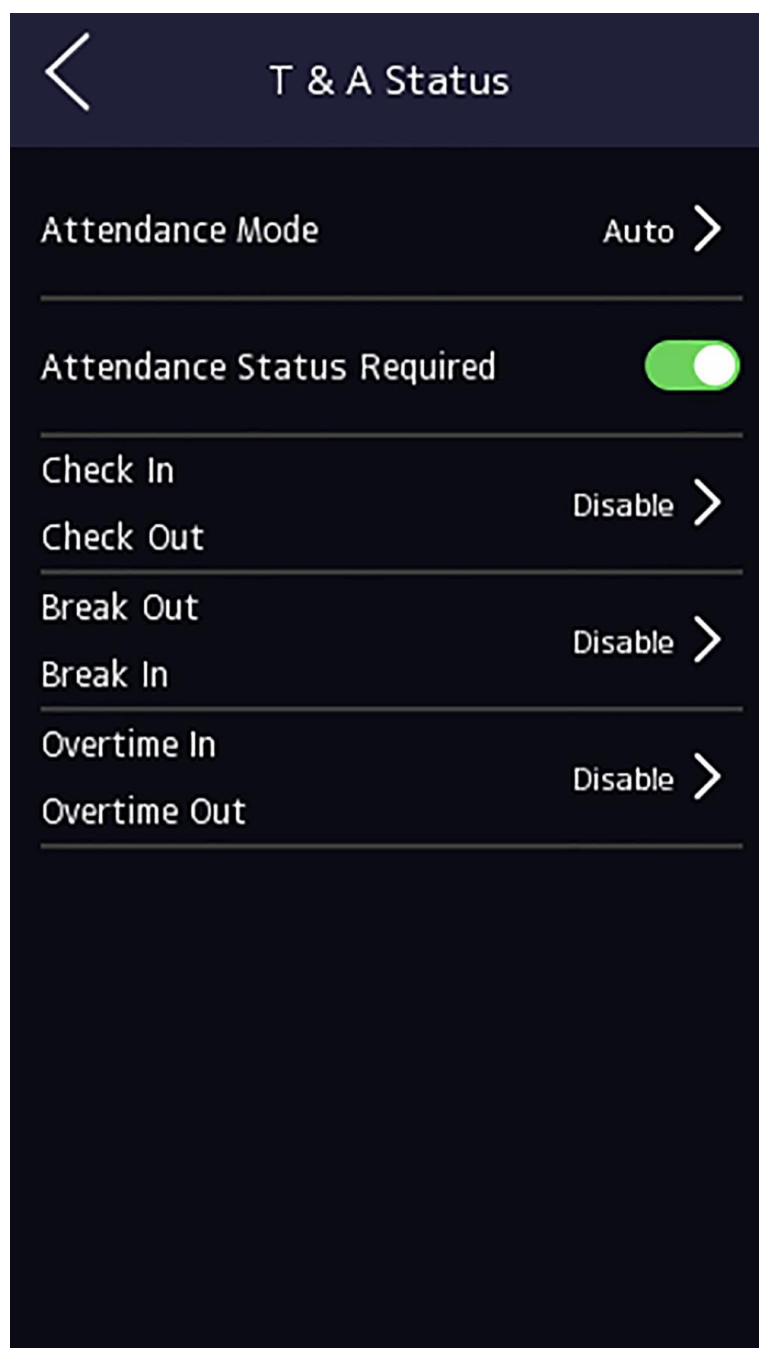


図7-12 自動出席モード

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



出席プロパティは変更されません。

5. オプション: 必要に応じてステータスを選択し、名前を変更できます。

名前は「T & A ステータス」ページと認証結果ページに表示されます。

6. ステータスのスケジュールを設定します。

- 1) 「出席スケジュール」をタップします。
- 2) 月曜日、火曜日、水曜日、木曜日、金曜日、土曜日、または日曜日を選択してください。
- 3) 選択した出席ステータスのその日の開始時間を設定してください。
- 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を繰り返してください。



注意

出席ステータスは設定されたスケジュール内で有効になります。

結果

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

例

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

7.4.4 デバイス経由での手動と自動の出席設定

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

開始前に

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

手順

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

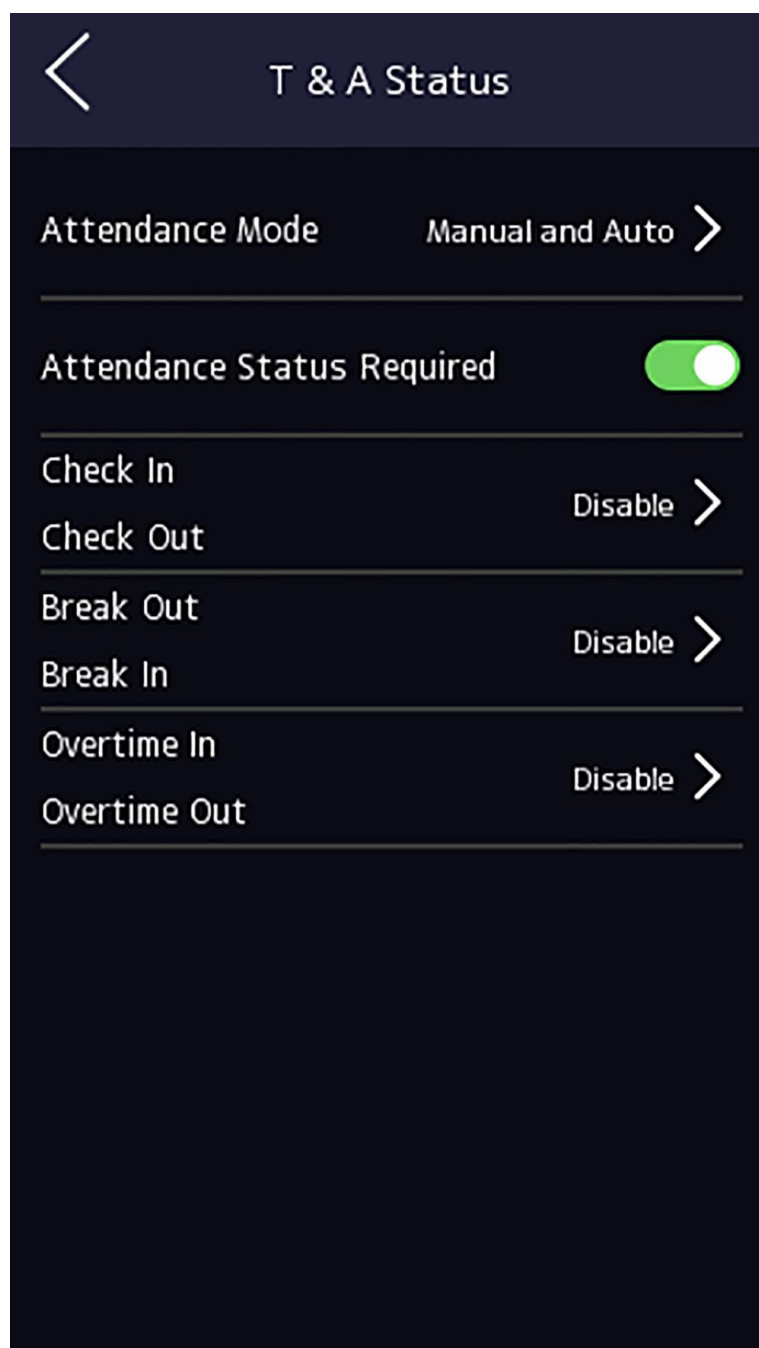


図7-13 手動モードと自動モード

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



出席プロパティは変更されません。

5. オプション: 必要に応じてステータスを選択し、名前を変更できます。
-

名前は「T & A ステータス」ページと認証結果ページに表示されます。

6. ステータスのスケジュールを設定します。

- 1) 出席スケジュールをタップしてください。
 - 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) 選択した出席ステータスのその日の開始時間を設定します。
 - 4) **OK**をタップします。
 - 5) 実際の必要に応じて、手順1から4を繰り返し実行してください。
-



注意

出席ステータスは設定されたスケジュール内で有効になります。

結果

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

例

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

7.5 データ管理

データを削除、インポート、エクスポートできます。

7.5.1 データ削除

ユーザーデータを削除します。

ホーム画面で、**[データ]**をタップし、**[→]**をタップし、**[データ削除]**をタップし、**[→]**をタップし、**[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。

7.5.2 データのインポート

手順

1. デバイスにUSBフラッシュドライブを接続します。
 2. ホーム画面で、**[データ]**をタップし、**[→]**をタップし、**[データインポート]**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ー」をタップします。
-



注意

インポートしたアクセス制御パラメーターは、デバイスの設定ファイルです。

4. データをエクスポートした際に作成したパスワードを入力してください。データをエクスポートした際にパスワードを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。



- ユーザー情報を1つのデバイス（デバイスA）から別のデバイス（デバイスB）に移行したい場合は、まずデバイスAからUSBフラッシュドライブに情報をエクスポートし、その後USBフラッシュドライブからデバイスBにインポートする必要があります。この場合、プロフィール写真をインポートする前にユーザーデータをインポートする必要があります。
- 対応している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内の「enroll_pic」という名前のフォルダーに保存し、画像の名前は次のルールに従って命名する必要があります：
カード番号_名前_部署_従業員ID_性別.jpg
- フォルダー「enroll_pic」にすべてのインポートした画像を保存できない場合は、ルートディレクトリの下に「enroll_pic1」「enroll_pic2」「enroll_pic3」「enroll_pic4」という名前のフォルダーを新たに作成してください。
- 従業員IDは32文字未満でなければなりません。小文字、大文字、数字の組み合わせが可能です。重複してはならず、0で始まってはいけません。
- 顔写真の要件は以下のルールに従ってください：顔全体が正面を向いてカメラを直接見ている状態で撮影してください。顔写真の撮影時には帽子や頭巾を着用しないでください。形式はJPEGまたはJPGです。解像度は640×480ピクセル以上で、640×480ピクセル以上である必要があります。画像サイズは60KBから200KBの間でなければなりません。

7.5.3 データエクスポート

手順

1. USBフラッシュドライブをデバイスに接続します。
2. →ホーム画面で「データ」をタップし、次に「データエクスポート」をタップします。
3. 顔データ、イベントデータ、ユーザーデータ、またはアクセス制御パラメーターをタップします。



エクスポートされたアクセス制御パラメーターは、デバイスの設定ファイルです。

4. オプション: 輸出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は、パスワードを入力する必要があります。



- 対応するUSBフラッシュドライブの形式はDBです。
 - システムは、1GBから32GBのストレージ容量を持つUSBフラッシュドライブに対応しています。USBフラッシュドライブの空き容量が512MB以上であることを確認してください。
 - エクスポートされたユーザーデータはDBファイルであり、編集できません。
-

7.6 身分認証

ネットワーク設定、システムパラメーター設定、およびユーザー設定が完了した後、アイデンティティ認証の初期画面に戻ることができます。システムは、設定された認証モードに従ってユーザーを認証します。

7.6.1 単一認証情報による認証

認証前にユーザー認証タイプを設定します。詳細については、[「認証モードの設定」](#)を参照してください。顔、指紋、またはカードで認証します。

顔

カメラに向かって顔を向け、顔認証を開始します。

指紋

登録した指紋を指紋認証モジュールに置き、指紋認証を開始してください。

カード

カードをカード読み取りエリアに提示し、カードによる認証を開始してください。



注意

カードは通常のICカードまたは暗号化カードのいずれかです。

PIN

PINコードを入力してPINによる認証を行ってください。

認証が完了すると、「認証完了」というメッセージが表示されます。

7.6.2 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の種類を設定します。詳細については、[「認証モードの設定」](#)を参照してください。

手順

1. 認証モードが「カードと顔」「パスワードと顔」「カードとパスワード」「カードと顔と指紋」の場合、ライブビューページに表示される指示に従って、いずれかの認証情報を認証してください。



注意

カードは通常のICカードまたは暗号化カードです。

2. 前の認証情報が認証された後、他の認証情報を認証し続けます。
-



注意

- 指紋のスキャンに関する詳細な情報は、「[指紋のスキャンに関するヒント](#)」を参照してください。
- 顔認証に関する詳細な情報は、「[顔写真の収集/比較時の注意点](#)」をご確認ください。

認証が成功した場合、プロンプト「認証完了」が表示されます。

7.7 基本設定

音量、時間、スリープ時間（秒）、言語、コミュニティ番号、建物番号、ユニット番号、プライバシー設定、動画規格を設定できます。

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

サウンド設定

音声ガイド機能をオン/オフに切り替えたり、音声のボリュームを調整できます。



注意

音声のボリュームを0から10の間で設定できます。0は消音を表します。

時間設定

タイムゾーン、デバイスの時刻、および夏時間（DST）を設定します。

スリープ（秒）

デバイスのスリープ待機時間を設定（分）。初期画面にいる状態でスリープ時間を30分に設定した場合、操作がないまま30分経過するとデバイスがスリープ状態になります。



注意

スリープ時間を0に設定すると、デバイスはスリープモードに入りません。

言語を選択

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

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てください。

建物番号

デバイスがインストールされているビル番号を設定してください。

ユニット番号

デバイスがインストールされているユニット番号を設定します。

通話設定

ダイヤル後自動発信

自動発信機能を有効にし、タイムアウト期間を設定できます。

コールセンターボタンの通話先

通話先を選択します。

VoIPサーバー

VoIPサーバーを選択します。

プライバシー

名前/従業員ID

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

顔写真

認証時に顔写真を表示する/表示しないを選択できます。

登録した画像の保存

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。

認証時に写真を保存する

この機能を有効にすると、デバイスに認証する際、画像を保存できます。

認証時に画像をアップロード

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。

通話中に撮影した画像をアップロード

通話中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。

動画規格

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。標準を変更後は、変更を反映させるためにデバイスを再起動する必要があります。

PAL (50Hz)

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

NTSC (60Hz)

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

7.8 生体認証パラメーターの設定

顔認識性能を向上させるため、顔パラメーターをカスタマイズできます。設定可能なパラメーターには、顔の活体検出レベル、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モード設定、マスク検出が含まれます。

初期画面で3秒間長押しし、ホーム画面にログインします。システム設定をタップし、→生体認証を選択します。

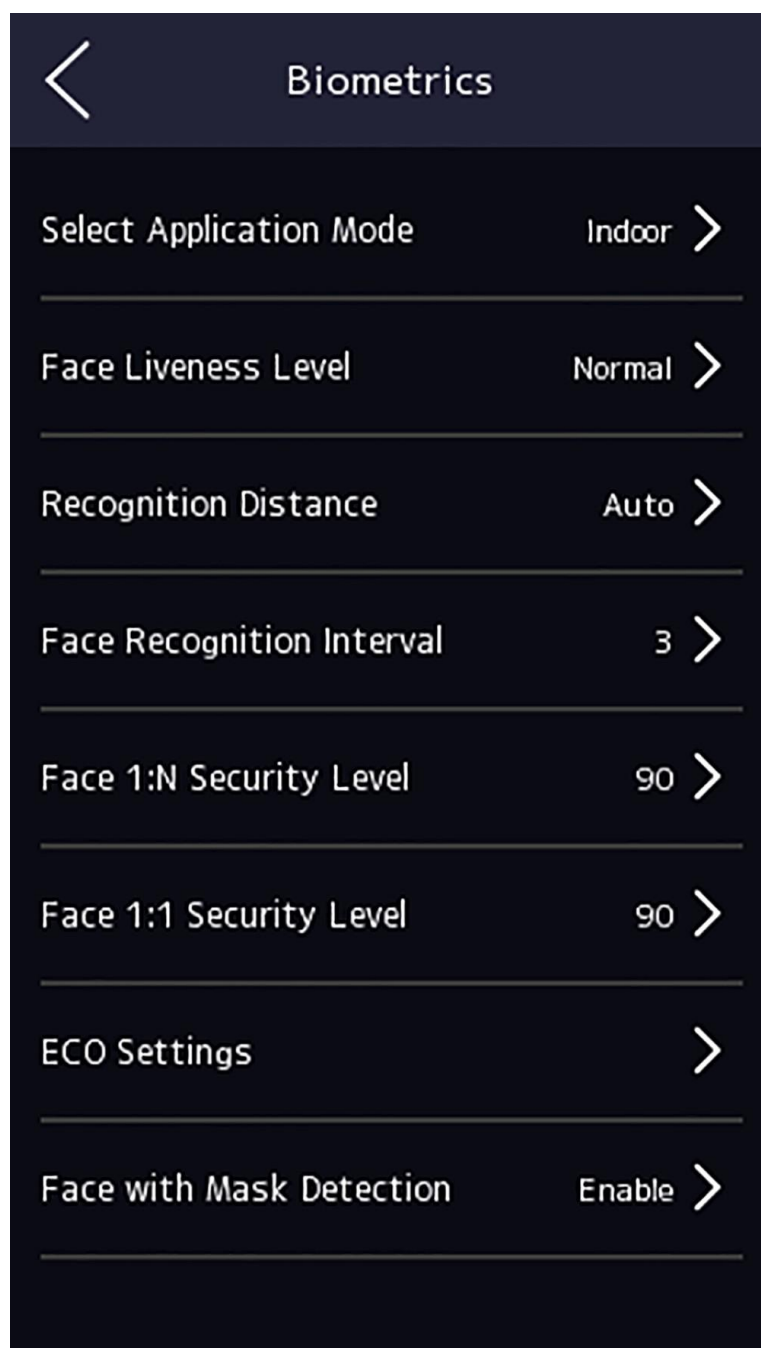


図7-14 生体認証パラメーターページ

表7-1 顔画像パラメーター

パラメーター	説明
顔の鮮明度レベル	顔認証の偽装防止機能を有効にした後、ライブ顔認証を行う際の認証セキュリティレベルを設定できます。
認識距離	認証時にユーザーとカメラの間の有効な距離を設定します。
顔認識間隔	認証時に連続する2回の顔認識の間隔を設定します。  注意 1から10までの数値を入力できます。
顔1対Nセキュリティレベル	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（FA）は低く、誤拒否率（FRR）は高くなります。
顔1:1 セキュリティレベル	1対1一致モードで認証を行う際の照合閾値を設定します。値が大きいほど、誤認率（false accept rate）が低く、誤拒否率（false rejection rate）が高くなります。
ECOモード設定	ECOモードを有効にすると、デバイスは低照度または暗い環境で顔認証を行う際に赤外線カメラを使用します。また、ECOモードの閾値、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モードの1:1マッチングモードで認証する際の一致閾値を設定します。値が大きいほど、誤認率が低く、誤拒否率が大きくなります。 ECOモード（1:N） ECOモード1:Nマッチングモードで認証を行う際の照合閾値を設定します。値が大きいほど、誤認率（false accept rate）が低く、誤拒否率（false rejection rate）が高くなります。
マスク設定	マスク検出機能を有効にすると、システムはマスクを着用した顔の画像を認識します。マスク着用顔と顔（1:1）、マスク着用顔と顔（1:N）、ECO（1:1）閾値、ECOモード（1:N）閾値、およびプロンプト方法を設定できます。 マスク付き顔と顔（1:1）

パラメーター	説明
	マスクを着用した顔で1:1マッチングモードで認証する際の一致値を設定します。値が大きいほど、誤認率が低く、誤拒否率が大きくなります。 マスク着用時の顔認識 & 顔認識 (1:N) マスクを着用した顔認証時の1:Nマッチングモードでの一致閾値を設定します。値が大きいほど、誤認率が低く、誤拒否率が大きくなります。 ECOモード (1:1) しきい値 ECOモードの1:1マッチングモードでマスク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（FA）が低く、誤拒否率（FRR）が高くなります。 ECOモード (1:N) しきい値 ECOモードの1:Nマッチングモードでマスク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。 プロンプト方法 「なし」「着用リマインダー」「着用必須」の戦略を設定します。 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 顔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。

7.9 設定オプション

設定パラメーターを構成できます。

手順

1. システム設定をタップし、→設定をタップして、設定画面に移動します。

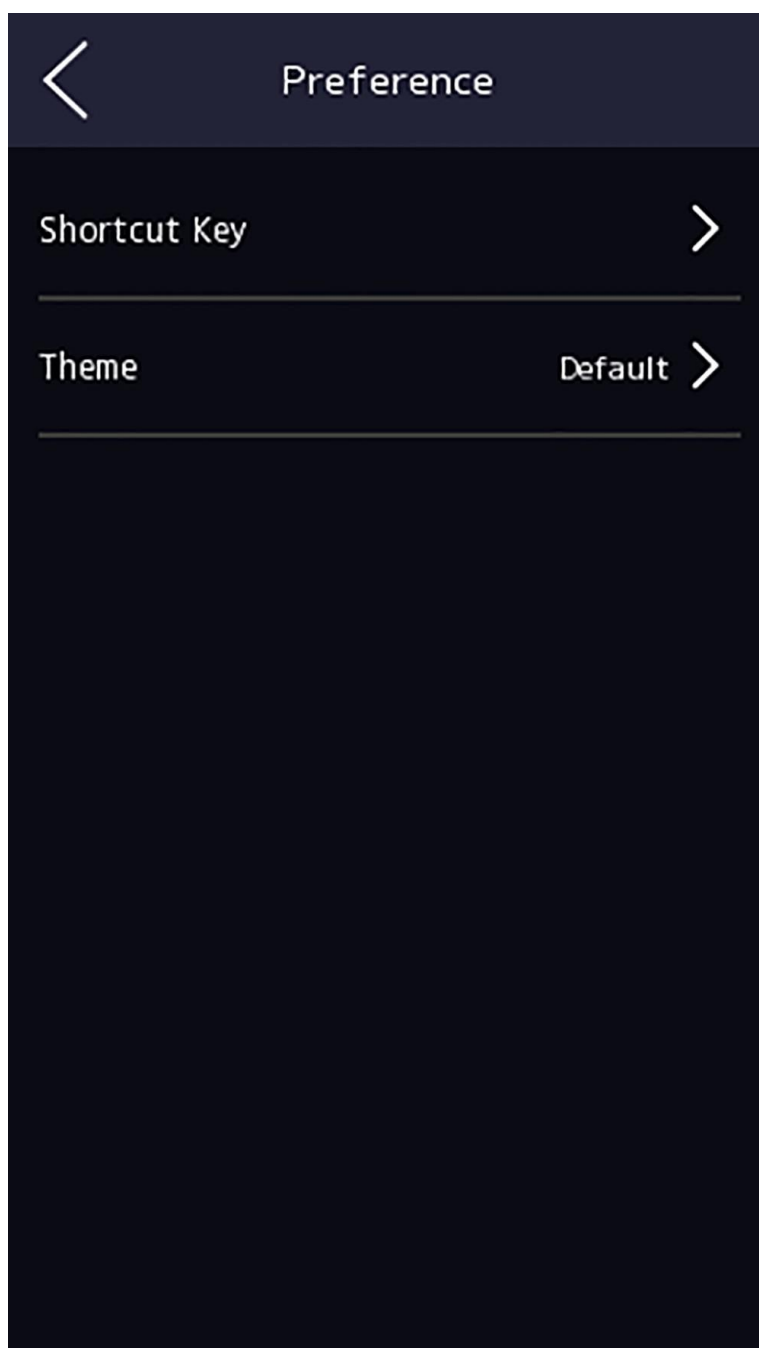


図7-15 設定

ショートカットキー

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



注意

通話タイプは、コールルーム、コールセンター、指定した部屋番号への通話、およびアプリへの通話から選択できます。
パスワード

この機能を有効にすると、パスワードを入力して認証を行うことができます。

QRコード

認証画面でQRコードの読み取り機能をご利用いただけます。デバイスは取得したQRコードに関連する情報をプラットフォームに送信します。

コールルーム

認証ページでコールボタンをタップすると、コールする部屋番号を入力する必要があります。

コールセンター

認証ページでコールボタンをタップすると、センターに直接通話できます。

指定の部屋番号にコール

部屋番号を設定してください。認証画面の通話ボタンをタップすると、ダイヤルせずに設定した部屋に直接通話できます。

通話アプリ

認証画面の呼び出しボタンをタップすると、デバイスが追加されているモバイルクライアントに呼び出しがかかります。

室内ステーション番号を呼び出す

有効化後、認証画面に室内ステーション番号が表示されます。

管理センター/VoIPセンターへの通話

有効化後、認証画面から管理センターまたはVoIPセンターに呼び出すことができます。

テーマ

認証ページでプロンプトウィンドウのテーマを設定できます。テーマとして

テーマを「認証/シンプル」から選択できます。**認証**

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

シンプル

このモードを選択すると、認証ページのライブビューが無効になり、その間、人物の名前、従業員ID、顔写真がすべて非表示になります。

インターコムモード

このモードを選択すると、認証ページの最下部にショートカットが表示されます。

チェック時に出席記録を表示する

「チェック時に出席記録を表示」を有効にすると、有効化後、チェック時に出席記録が表示されます。

7.10 デバイスパスワードの変更

古いパスワードを入力することで、デバイスのパスワードを変更できます。

手順

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



注意

パスワードを忘れた場合は、「パスワードを忘れた」をタップし、パスワードを変更できます。詳細については、「[パスワードを忘れた](#)」を参照してください。

-
4. 新しいパスワードを入力し、パスワードを確認してください。



注意

デバイスのパスワードの強度は自動的にチェックされます。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おすすめします。また、特に高セキュリティシステムでは、パスワードを定期的に変更することをおすすめします。月次または週次での変更が、製品の保護をより強化します。

すべてのパスワードおよびその他のセキュリティ設定の適切な設定は、インストール担当者および/またはエンドユーザーの責任です。

-
5. OKをタップします。

7.11 認証設定

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、開錠時間（秒）、認証間隔（秒）、認証結果表示時間（秒）、パスワードモードなどのアクセス制御権限を設定できます。

ホーム画面で「認証設定」をタップして設定画面に移動します。

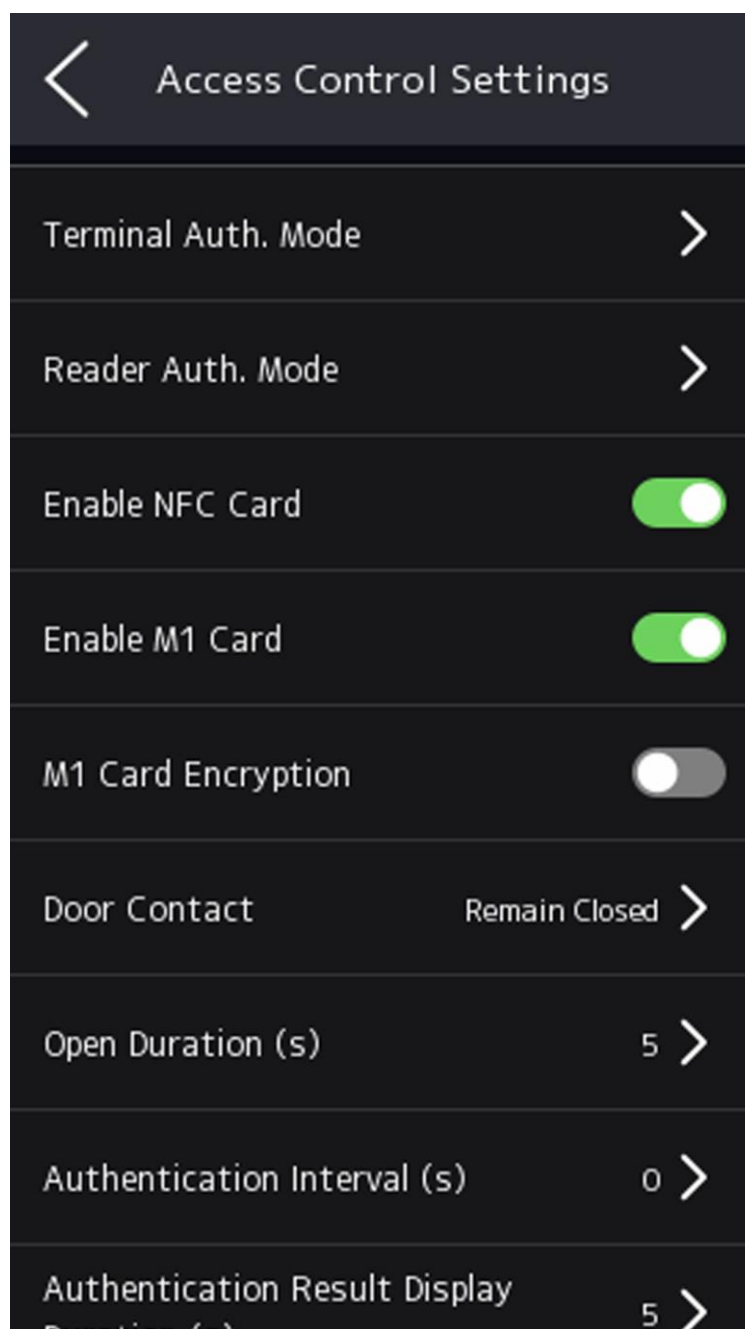


図7-16 認証設定

利用可能なパラメーターの説明は次のとおりです：

表7-2 アクセス制御パラメーター説明

パラメーター	説明
端末認証モード (Terminal Authentication Mode)	顔認識端末の認証モードを選択してください。認証モードをカスタマイズすることも可能です。  注意 - 指紋モジュールを搭載したデバイスのみが、指紋関連機能に対応しています。 - 生体認証製品は、偽装防止環境において完全に適用できません。より高いセキュリティレベルが必要な場合は、複数の認証モードを使用してください。 - 複数の認証モードを採用する場合、顔認証を行う前に他の認証方法での認証を実行する必要があります。
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	機能を有効にすると、NFCカードを提示して認証できます。
M1カード有効化	機能を有効にすると、M1カードを提示して認証を行うことができます。
M1カード暗号化	M1カード暗号化機能を有効にすると、カードのセキュリティレベルが向上します。カードは容易にコピーされなくなります。
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。
開錠時間	ドアの解錠時間を設定します。設定した時間内にドアが開かれない場合、ドアがロックされます。利用可能なドアロック時間範囲：1～255秒。
認証間隔	デバイスの認証間隔を設定します。認証間隔の範囲：0～65535。
認証結果表示時間（秒）	認証結果の表示時間を設定します。
パスワードモード	プラットフォーム適用型個人用PIN PINはプラットフォームによって管理および配布されます。Webのデバイス上でPINを設定することはできません。 デバイス設定型個人用PIN

パラメーター	説明
	PINはデバイスまたはWeb上で設定されます。他のプラットフォームでPINを設定することはできません。

7.12 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。デバイスのアップグレード、ユーザーマニュアルの閲覧、システムを工場出荷時設定またはデフォルト設定に復元、システムの再起動を行うこともできます。

初期画面を3秒間長押しし、ホーム画面にログインします。「メンテナンス」をタップします。

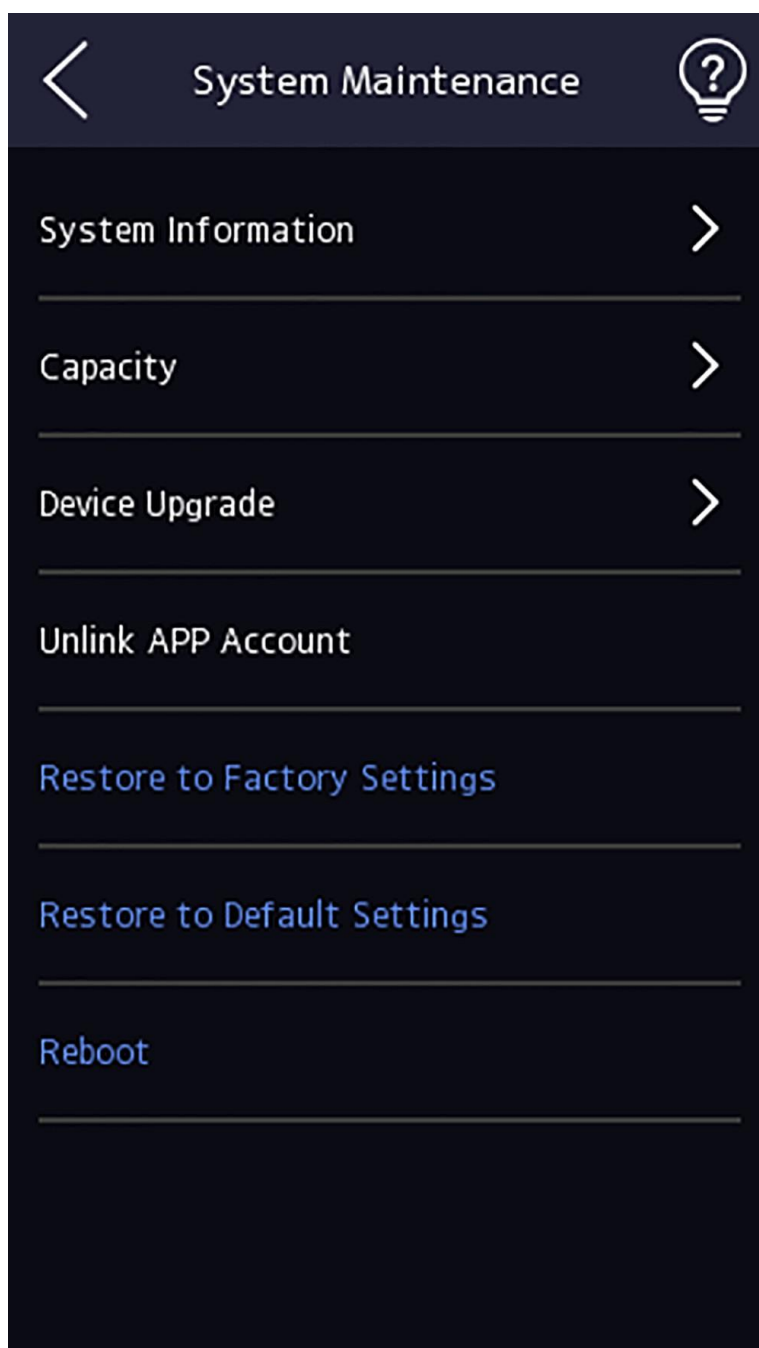


図7-17 メンテナンスページ

システム情報

デバイス情報（デバイスモデル、シリアル番号、ファームウェアバージョン、MACアドレス、製造データ、ライセンスなど）を確認できます。



注意

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



を長押しし、管理パスワードを入力してデバイスバージョン情報を表示します。

顔パラメーター

カスタム顔認証偽装防止検出顔の鮮明度

レベル

顔アンチスプーフィング機能を有効にした後、ライブ顔認証時に使用するマッチングのセキュリティレベルを設定できます。

アンチスプーフィング検出閾値

値が大きいほど、誤検出率（偽陽性率）は低く、誤拒否率（偽陰性率）は高くなります。値が小さいほど、誤検出率（偽陽性率）は高く、誤拒否率（偽陰性率）は低くなります。

顔認証ロック機能（なりすまし防止）

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

ロック時間

アンチスプーフィング保護のためのロックフェイスを有効化した後、アンチスプーフィング検出に失敗した際のロック時間。

バージョン情報

デバイスの情報を確認できます。

容量

人物数、顔画像、カード、指紋、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、指紋認証機能の表示が可能です。詳細については、実際のページをご確認ください。

デバイス アップグレ

ード オンライン更

新

デバイスがHik-Connectとネットワークに接続されている場合、Hik-Connectに新しいインストールパッケージが存在する際に、**デバイスアップグレード→オンラインアップデート**をタップして、デバイスのシステムをアップグレードできます。

USB経由での更新

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。**デバイスアップグレード→USB経由で更新**をタップすると、デバイスは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。

ユーザーマニュアル

QRコードをスキャンして、デバイスのユーザーマニュアルを表示します。

工場出荷時設定への復元

すべての設定が工場出荷時設定に復元されます。システムが再起動して設定が適用されます。

デフォルト設定への復元

通信設定を除くすべてのパラメーター、およびリモートでインポートされたユーザー情報は、デフォルト設定に復元されます。システムは再起動して設定が有効になります。

再起動

確認後、デバイスが再起動します。

第8章 モバイルウェブ経由でのデバイスの設定

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

- 一部のモデルではWi-Fi設定がサポートされています。
 - デバイスがアクティブになっていることを確認してください。
 - デバイスとスマートフォンが同じWi-Fi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。
-

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画面に移動します。
デバイスのユーザー名とパスワードを入力し、**ログイン**をタップします。

8.2 概要

ショートカットから、ドアの状態、ネットワークの状態、基本情報を確認し、ユーザー管理、スマート設定、認証設定、ドアのパラメーターを設定できます。

機能説明:

ドアの状態



ドアの状態は「開いている」「閉まっている」「開いたまま」「閉まったまま」です。実際の状況に応じて、タップして「開いている」「閉まっている」「開いたまま」「閉まったまま」の状態を選択できます。

ショートカット入力

ショートカット入力経由で、ユーザー管理、スマート設定、認証設定、およびドアパラメーターを設定できます。

ネットワーク状態

接続済みおよび登録済みのネットワークの状態を確認できます。

基本情報

モデル、シリアル番号、およびファームウェアバージョンを確認できます。

8.3 パスワードを忘れた場合

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

ログイン画面で「パスワードを忘れた場合」をタップします。

検証モードを選択してください。セキュリティ質問による検証

セキュリティ質問による検証

セキュリティ質問に回答してください。

メール認証

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

8.4 設定

8.4.1 デバイス情報を表示

デバイス名、言語、モデル、シリアル番号、バージョン、IO入力番号、IO出力番号、ローカルRS-485番号、アラーム入力番号、アラーム出力番号、レジスタ番号、工場情報、デバイス容量など、各種情報を表示します。

ホーム画面で、、、**[System Settings]**、、**[Basic Information]** をタップします。

デバイス名、言語、モデル、シリアル番号、バージョン、IO入力番号、IO出力番号、ローカルRS-485番号、アラーム入力番号、アラーム出力番号、レジスタ番号、工場情報、デバイス容量など、各項目を確認します。

「保存」をタップします。

8.4.2 時間設定

タイムゾーン、時間同期モード、表示時間を設定します。

 をタップします。→ **システム設定** → **時間設定** をタップして設定画面に入ります。

Time Zone	(GMT+08:00) Beijing, Urumqi, Singapore, Perth >
Time Sync. Mode	Manual >
Device Time	2021-06-28 10:15:43
Set Time	2021-06-28 10:15:08 >

Save

図8-1 タイム設定

「保存」をタップして設定を保存します。

タイムゾーン

デバイスの所在地に対応するタイムゾーンをドロップダウンリストから選択します。

時間同期モード手動

デフォルトでは、デバイスの時間は手動で同期されます。デバイスの時間を手動で設定できます。

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 夏時間設定

手順

1. 「」をタップします。「→」→「System Settings」→「→」→「Time Settings」をタップして、設定画面に移動します。

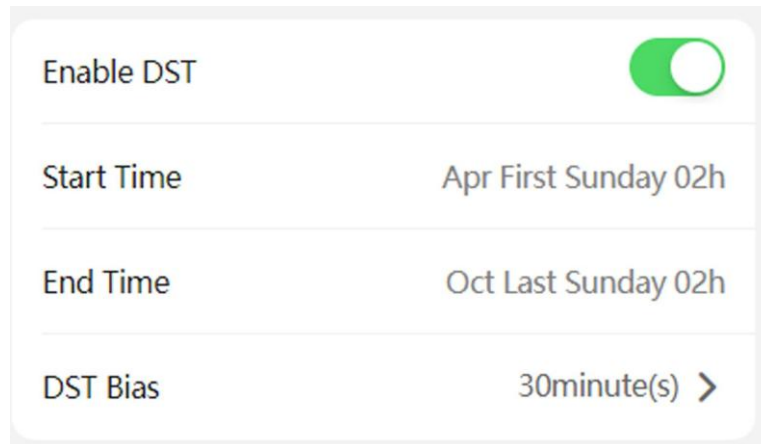


図8-2 DST

2. 「DSTを有効にする」をタップします。
3. 開始時間、終了時間、およびDSTのオフセットを設定します。
4. 「保存」をタップします。

8.4.4 ユーザー管理

手順

1. 「」をタップします。→ User Management→ User Management→ admin にアクセスして設定画面を開きます。
2. 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。
3. 新しいパスワードを確認します。
4. 「保存」をタップします。



注意

デバイスのパスワードの強度は自動的にチェックされます。製品のセキュリティを強化するため、ご自身で選択したパスワード（8～16文字で、大文字、小文字、数字、特殊文字の少なくとも2種類を含む）に変更することを強くおすすめします。また、特に高セキュリティシステムでは、パスワードを定期的に変更することをおすすめします。月次または週次での変更が、製品の保護をより強化します。

8.4.5 ネットワーク設定

有線ネットワーク、Wi-Fiの設定、およびデバイスポートを設定できます。

有線ネットワーク

有線ネットワークを設定します。

「」をタップします。「**→通信設定**」をタップします。「**→有線ネットワーク**」をタップして設定画面に移動します。

DHCP

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

機能を有効にした場合、システムがIPv4アドレス、IPv4サブネットマスク、IPv4デフォルトゲートウェイを自動的に割り当てます。

DNSサーバー

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

Wi-Fi パラメーターを設定

デバイスの無線接続用のWi-Fiパラメーターを設定します。

手順



注意

この機能はデバイスでサポートされている必要があります。

1. 「」をタップします。「**→ Communication Settings**」をタップし、次に「**→ Wi-Fi**」をタップして設定画面に移動します。
2. **Wi-Fi** を有効にします。

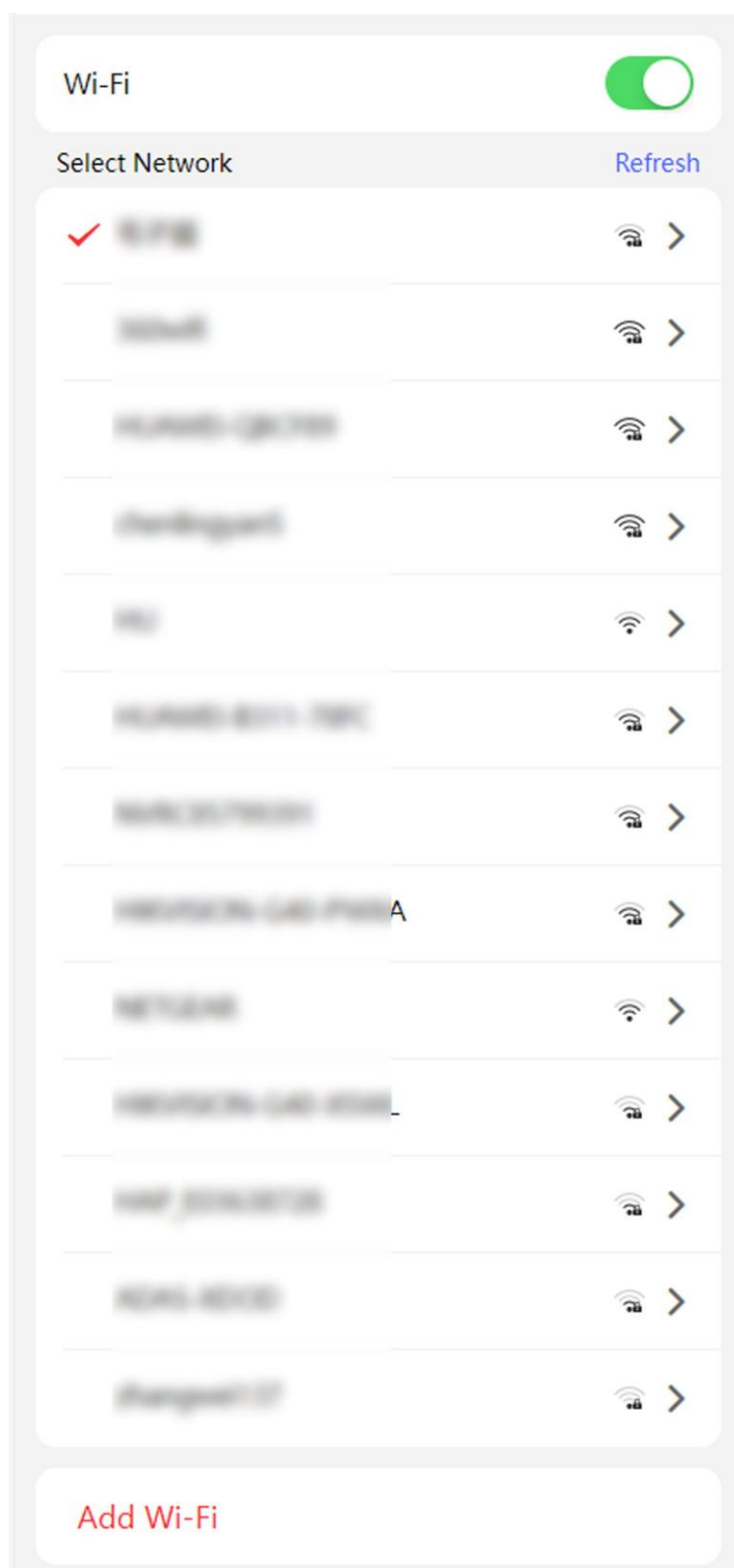


図8-3 Wi-Fi

3. Wi-Fiを追加します。
 - 1) 「**Wi-Fiを追加**」をタップします。
 - 2) **Wi-Fi** 名と **Wi-Fi** パスワードを入力し、**暗号化タイプ**を選択します。
 - 3) 「**保存**」をタップします。
4. Wi-Fiの名前を選択し、**[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。

ポートパラメーターを設定します

ネットワーク経由でデバイスにアクセスする際、実際の必要に応じてHTTPとHTTPSを設定できます。「」→「**Network Service**」→「**HTTP(S)**」をタップして、設定画面を開きます。

HTTP

ブラウザがデバイスにアクセス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に**http://192.0.0.65:81**を入力する必要があります。

HTTPS

ブラウザでアクセスする際のHTTPSを設定します。アクセスには証明書が必要です。

プラットフォームアクセス

プラットフォームへのアクセスにより、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利用可能です。

手順

1. 「」をタップします。「→ **デバイスアクセス**」をタップします。「→ **Hik-Connect**」をタップして設定画面に移動します。



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

2. 「**有効**」をタップして機能を有効にします。
3. 「**カスタム**」を有効にすると、サーバーアドレスを入力できます。



- 6文字から12文字（aからz、AからZ）または数字（0から9）、大文字と小文字を区別します。8文字以上の文字または数字の組み合わせを使用することをおすすめします。
- 検証コードは「**123456/**」または「**abcdef**」（大文字小文字を区別しない）に設定できません。

4. **登録状態**と**バインディング状態**を確認できます。
5. **ビデオ暗号化**を有効にし、パスワードを作成して確認してください。



デバイスをアプリに追加した後、ライブビューでデバイスを表示するには、動画暗号化パスワードを入力する必要があります。

6. 「**アカウントを連携**」をタップし、→の**QRコードを表示**し、QRコードをスキャンしてアカウントを連携します。

7. 「保存」をタップして設定を有効にします。

ISUPパラメーターを設定します

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

手順



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. 「」をタップします。「→」→「Device Access」→「→」→「ISUP」を選択して設定画面に移動します。
2. ISUPを有効にします。
3. ISUPバージョン、サーバーアドレス、ポート、デバイスID、および暗号化キーを設定します。



バージョンに5.0を選択した場合、暗号化キーも設定する必要があります。

4. 「保存」をタップして設定を保存します。

OTAPを設定

OTAPプロトコルを使用してデバイスをプラットフォームに接続し、デバイス情報、操作状態、アラーム情報を取得し、デバイスの再起動とアップグレードを行います。

手順

1. 「」をタップします。「→」→「Device Access」→「→」→「OTAP」をタップして設定画面に移動します。
2. 「OTAPを有効にする」をタップします。
3. サーバーアドレス、ポート、デバイスID、および暗号化キーを設定します。
4. 「テスト」をタップして、デバイスがサーバーに接続でき、正常に登録されることを確認します。ページを再読み込みするか、デバイスを再起動して、登録状態を確認します。
5. 「保存」をタップします。

ネットワークペネトレーションサービスを設定します。

デバイスがLANに展開された場合、ペネトレーションサービスを有効にすることで、デバイスのリモート管理を実現できます。

手順

1. 「」をタップします。「→ Device Access」をタップします。「→ Network Penetration Service」をタップして設定画面に移動します。
2. 「Enable Penetration Service」をタップします。
3. サーバーのIPアドレスとポート番号を設定します。ユーザー名とパスワードを作成します。
4. オプション：ハートビートタイムアウトを設定できます。値の範囲は1から6000です。
5. オプション：ペネトレーションサービスの状態を確認できます。状態を更新するには「リフレッシュ」をクリックします。

6. 保存をタップします。



注意

ペネトレーションサービスは48時間後に自動的に無効化されます。

8.4.6 ユーザー管理

モバイルウェブブラウザ経由でユーザーを追加、編集、削除、検索できます。

手順

1. 「」をタップし、→の「ユーザー管理」をタップして設定画面に移動します。

2. ユーザーを追加します。

1) 「+」をタップします。

2) 以下のパラメーターを設定します。

従業員ID

従業員IDを入力します。従業員IDは0または32文字を超えてはいけません。大文字、小文字、数字の組み合わせが可能です。

名前

名前を入力してください。名前には数字、大文字と小文字の英字、および文字が含まれます。名前は32文字以内が推奨されます。

長期有効ユーザー

ユーザー権限を長期有効に設定します。

開始日/終了日

ユーザー権限の開始日と終了日を設定してください。

ユーザーロール

ユーザー役割を選択してください。

個人ユーザー

個人役割を選択してください。

出席確認のみ

有効化後、このユーザーにはアクセス制御権限が与えられません。

顔

顔写真を追加します。顔を選択し、カメラをタップして顔を追加するか、アルバムから選択をタップして顔をインポートします。

指紋

指紋を追加します。指紋をタップし、次に「+」をタップし、指紋モジュール経由で指紋を追加します。

カード

カードを追加します。カードをタップし、次に「+」をタップし、カード番号を入力してカードの種類を選択します。

3) 「保存」をタップします。

3. ユーザーリストから編集が必要なユーザーをタップして、情報を編集します。
4. ユーザーリストから削除したい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。

8.4.7 イベントを検索

「検索」をタップして検索画面に移動します。

検索条件を入力してください。従業員ID、氏名、カード番号、開始時間、終了時間を入力し、**[検索]**をタップしてください。



以下の名前検索に対応しています。

8.4.8 アクセス制御設定 認証パラメー

ターの設定

認証パラメーターを設定します。

手順

1. 「」をタップします。「→」→「Access Control」→「→」→「Authentication Settings」を選択します。

2. 保存をタップします。

ターミナル

設定対象の端末を選択します。

ターミナルタイプ/ターミナルモデル

ターミナルの説明を取得します。これらは読み取り専用です。

認証デバイスを有効にする

認証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。

連続顔認識間隔（秒）

認証中に同じ人物の連続した認識の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。間隔内に別の人物（人物B）が認識された場合、人物Aは再び認識可能です。

認証間隔

同じ人物の認証時の認証間隔を設定できます。設定された間隔内では、同じ人物は1回のみ認証可能です。2回目の認証は失敗します。

最大失敗試行回数アラーム

設定値に達した際にアラームを通知するように有効にします。

メインインターフェースモード

メインインターフェースモードを**認証モード**または**シンプル**に設定できます。

改ざん検出を有効にする

カードリーダーの改ざん検出を有効にします。

カード番号の逆転を有効にする

この機能を有効にすると、カード番号が逆順になります。

ドアパラメーターを設定

 をタップします。→ **Access Control**→ **Door Parameters** をタップします。

設定を保存するには「**保存**」をタップします。

ドア名

ドアの名前を作成できます。

開錠時間

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

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。デフォルトでは「**開いたまま**」です。

最初の人が入室した際のドアの開いたままの持続時間（分）

最初の人が入室した際のドアの開錠時間を設定します。最初の人認証されると、複数の人物がドアにアクセスしたり、他の認証アクションを実行したりできるようになります。

ドア開錠タイムアウトアラーム

設定された時間内にドアが閉められていない場合、アラームが鳴動します。

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。デフォルトでは「**閉じたまま**」に設定されています。

ドアロックの電源オフ

ドアロックの電源オフを、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。

延長開状態時間

ドアの接触センサーは、拡張アクセス権限を持つユーザーがカードをかざした後、適切な遅延後に有効化されます。

緊急コード

緊急事態が発生した場合、緊急コードを入力することでドアを開けることができます。同時に、クライアントは緊急事態を報告することができます。

スーパーパスワード

特定のユーザーは、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ます。



注意

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

ターミナルパラメーター

ターミナルパラメーターを設定できます。

「」をタップします。「」→「Access Control」→「」→「Terminal Parameters」を選択します。

アクセス制御モードとして作業モードを設定できます。アクセス制御モードはデバイスの通常モードです。アクセスするには、資格情報を認証する必要があります。

リモート認証

リモート認証を有効にした後、認証時にデバイスは認証情報をプラットフォームに送信し、プラットフォームがドアを開けるかどうかを確認します。

資格情報をローカルで検証

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

タイムアウト期間

リモート認証のタイムアウト期間を設定できます。

設定を保存するには、設定完了後に「保存」をタップしてください。

カードセキュリティを設定する

「」をタップします。「」→「Access Control」→「」→「Card Security」をタップして設定画面に移動します。パラメーターを設定し、「保存」をタップします。

NFC カード有効化

モバイル端末がアクセス制御のデータにアクセスできないようにするため、NFCカードを有効化してデータのセキュリティレベルを向上させることができます。

M1 カード有効化

M1カードを有効にすると、M1カードを提示して認証が可能になります。

M1 カード暗号化

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。

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が暗号化されています。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カードを提示して認証を行う機能が利用可能になります。



注意

EMカードは、EMカードを読み取る機能を備えた周辺機器のカードリーダーを接続した際にサポートされます。

DESFire カードの有効化

デバイスは、DESFireカード機能有効時にDESFireカードからデータを読み取ることができます。

FeliCaカード機能を有効にする

デバイスは、FeliCaカード機能を有効にした際に、FeliCaカードからデータを読み取ることができます。

RS-485 パラメーターの設定

周辺機器、アドレス、ボーレートなど、RS-485パラメーターを設定できます。「」→「Access Control」→「RS-485」をタップします。

設定を保存するには、設定完了後に「保存」をタップします。

周辺機器の種類

実際の状況に応じて、ドロップダウンリストから周辺機器を選択してください。選択可能な周辺機器はカードリーダー、拡張モジュール、またはアクセスコントローラーから選択できます。



注意

周辺機器を変更して保存すると、デバイスが自動的に再起動します。

RS-485 プロトコル プラ

イペート

このデバイスはRS-485経由で第三者デバイスと接続可能です。

OSDP

標準のRS-485プロトコル。

RS-485 アドレス

実際の要件に応じてRS-485アドレスを設定してください。



注意

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

ボーレート

RS-485プロトコルでデバイスが通信する際のボーレートです。

データビット

RS-485プロトコルでデバイスが通信する際のデータビット数。

ストップビット

RS-485プロトコルでデバイスが通信する際のストップビット。

パリティ/フロー制御/通信モード

デフォルトで有効です。

8.4.9 ビデオインターコム設定

デバイスID設定

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

手順

1.  をタップします。→ **Intercom** → **デバイスID設定**。
2. 以下のパラメーターを設定してください。

デバイス タイプ

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



注意

デバイス タイプを変更した場合、デバイスを再起動する必要があります。

期間番号

デバイスの期間番号を設定してください。

建物番号

装置の番号を設定してください

ユニット番号

デバイスユニット番号を設定してください。



注

番号を変更した場合、デバイスを再起動する必要があります。

階番号

デバイスが設置されている階番号を設定してください。

ドアステーション番号

デバイスが設置されている階の番号を設定してください。



注意

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

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

外ドアステーション番号

外ドアステーションをデバイスタイプとして選択した場合、1から

99の数字を入力する必要があります。



注意

番号を変更した場合、デバイスを再起動する必要があります。

期間番号

デバイスの期間番号を設定します。

セッション設定

ドアステーション、メインステーション、およびビデオインターコムサーバー間の通信を有効にします。

手順

1. をタップします。→ **Intercom**→ **Session Settings** をタップします。
2. 登録パスワード、メインステーションのIPアドレス、プライベートサーバーのIPアドレスを設定し、プロトコル1.0を有効にします。

登録パスワード

メインステーションのアクティベーションパスワード。

メインステーションのIPアドレス

メインステーションのIPアドレス。

プライベートサーバーIP

プライベートサーバーのIPアドレス。

プロトコル1.0を有効にする

有効化後、デバイスは以前のプロトコルを通じてメインステーションに登録されます。無効化すると、デバイスは新しいプロトコルを通じてメインステーションに登録されます。

3. **保存**をタップします。

時間設定

最大通話時間を設定します。

をタップします。→ **インターコム**→ **コール設定** をタップします。

最大通信時間を設定します。「**保存**」をタップします。



注意

最大通話時間範囲は90秒から120秒です。

ボタンを押して通話する

手順

1. 「」をタップします。→ **Intercom** → 「ボタンを押して通話」を押します。
2. 必要に応じて「通話」または「コールセンター」をタップしてください。

番号設定

SIP番号で部屋に電話をかけることができます。

手順

1. 「」をタップし、→ 「インターコム」をタップし、→ 「番号設定」をタップします。
2. 「+」をタップし、部屋番号とSIP番号を入力します。
3. 「保存」をタップします。

8.4.10 オーディオ設定

手順

1. タップ  → オーディオ。
2. オプション：入力と出力の音量を設定します。

8.4.11 顔パラメーター設定

顔パラメーターを設定します。

顔パラメーター設定

「」をタップし、→ **Smart** → **Face Recognition Parameters** を選択します。

顔偽装防止

ライブ顔検出機能を有効または無効にします。この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。

ライブ顔検出セキュリティレベル

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

1:1一致閾値

1:1マッチングモードで認証を行う際の一致閾値を設定します。値が大きいほど、誤認率（FA）が低く、誤拒否率（FRR）が高くなります。

1対N一致閾値

1:N一致モードで認証を行う際の照合閾値を設定します。値が大きいほど、誤認率（false accept rate）が低く、誤拒否率（false rejection rate）が高くなります。最大値は100です。

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。

指紋パラメーター

「」をタップします。「」をタップします。「Smart→ Fingerprint Parameters」をタップします。

指紋セキュリティレベル

指紋のセキュリティレベルを設定できます。セキュリティレベルを高く設定するほど、誤認識率（FAR）は低くなります。セキュリティレベルを高く設定するほど、誤拒否率（FRR）は低くなります。

フェイスマスク検出パラメーター

マスク着用時の顔検出

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の画像を認識します。マスク着用顔の1対N一致閾値、その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。

マスク着用リマインダー

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

マスクの着用必須

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

マスク着用時と顔（1:1）

マスクを着用した状態で1:1マッチングモードで認証する際のマッチング値を設定します。値が大きいほど、誤認率（FA）は低く、誤拒否率（FRR）は高くなります。

マスク着用時の顔 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照合閾値を設定します。値が大きいほど、誤認率（偽陽性率）が低く、誤拒否率（偽陰性率）が高くなります。



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ご確認ください。

「保存」をタップして設定を保存します。

8.4.12 プライバシーパラメーターを設定

表示設定、画像のアップロードおよび保存パラメーターを設定します。「」→

「設定」→「セキュリティ」→「プライバシー設定」をタップします。

認証設定

画像表示/名前表示/従業員ID

画像、名前、または従業員IDの表示を有効にするには、タップしてください。認証が完了すると、システムは選択した内容を結果に表示します。

名前/IDの匿名化

名前/ID情報はアスタリスクで非識別化されます。

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。**登録した画像の保存**

機能有効化時に、登録された顔画像がシステムに保存されます。

認証時に画像を保存

この機能を有効にすると、デバイスへの認証時に画像を保存できます。

認証時に撮影した画像のアップロード

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。

リンクキャプチャ後に画像を保存

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

リンクしたカメラで撮影した画像をアップロード

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

8.4.13 パスワードモード

パスワードを設定する前に、パスワードがデバイス設定の個人用PINかプラットフォーム適用個人用PINかを明確にする必要があります。デバイスで設定された個人用PINの場合、デバイスまたはウェブ上で作成または編集でき、他のプラットフォームでは設定できません；プラットフォームで適用された個人用PINの場合、プラットフォーム上で作成または編集でき、使用前にデバイスに発行する必要があります。デバイスまたはウェブ上で設定できません。

手順

1. 「」をタップします。「→」をタップします。「→」をタップします。
「PIN Mode」をタップします。
「Device-Set Personal PIN」をタップします。

デバイス上またはウェブ上で作成または編集でき、他のプラットフォームでは設定できません。

プラットフォーム適用型個人PIN

プラットフォーム上で作成または編集でき、使用可能になる前にデバイスに発行されます。デバイスやウェブ上で設定することはできません。

2. 「保存」をタップします。

8.4.14 アップグレードとメンテナンス

デバイスを再起動し、デバイスのパラメーターを復元し、デバイスのバージョンをアップグレードします。

デバイスを再起動

☰ 「」をタップします。→ **Restart Device** をタップします。

「再起動」をタップしてデバイスを再起動します。

アップグレード

☰ 「」をタップし、→ をタップしてアップグレードします。

「アップグレード」をタップしてデバイスをアップグレードします。



注意

アップグレード中は電源を切らないでください。

パラメーターの復元

☰ 「」をタップします。「→」をタップします。「Default」をタップします。

デフォルト設定に復元

デバイスはデフォルト設定に復元されます。ただし、デバイスのIPアドレスとユーザー情報は除きます。

工場出荷時設定に復元

すべてのパラメーター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。

8.4.15 オンラインドキュメントを表示

☰ をタップしてください。→ **オンラインドキュメントを表示**。オンラインドキュメントを表示をタップすると、スマートフォンでQRコードをスキャンして詳細を確認できます。

8.4.16 オープンソースソフトウェアライセンスを表示

設定をタップし、→ **システム** → **システム設定** → **について** をタップし、**ライセンスを表示** をタップしてデバイスのライセンスを表示します。

第9章 ウェブブラウザを使用したクイック操作

9.1 パスワードの変更

デバイスのパスワードを変更できます。

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

「次へ」をクリックして設定を完了します。または「スキップ」をクリックしてこのステップを飛ばすことができます。

9.2 言語を選択

デバイスのシステム言語を選択できます。

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

デフォルトでは、システム言語は英語です。



注意

システム言語を変更すると、デバイスが自動的に再起動します。

9.3 時間設定

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

タイムゾーン

ドロップダウンリストからデバイスの所在するタイムゾーンを選択します。

時間同期

NTP

NTP サーバーの IP アドレス、ポート番号、および間隔を設定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。

サーバーアドレス/NTPポート/間隔

サーバーアドレス、NTP ポート、および間隔を設定できます。

DST

DSTの開始時間、終了時間、およびバイアス時間を表示できます。

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

9.4 プライバシー設定

画像のアップロードと保存に関するパラメーターを設定できます。

ウェブページの右上にある「」をクリックして、ウィザードページに移動します。

画像のアップロードと保存

認証時に画像を保存

認証時に画像を自動的に保存します。

認証時に画像をアップロード

認証時に画像をプラットフォームに自動的にアップロードします。

登録済み画像の保存

この機能を有効にすると、登録された顔画像がシステムに保存されます。

リンクした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。

リンクしたカメラで撮影した画像を保存

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

9.5 管理者設定

手順

1. ウェブページの右上にある「」をクリックしてウィザードページに移動します。
2. 管理者の従業員IDと名前を入力します。
3. 追加する認証情報を選択します。



少なくとも1つの資格情報を選択する必要があります。

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



アップロードする画像は200KB以内であり、JPG、JPEG、PNG形式でなければなりません。

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



最大50枚のカードに対応しています。

-
- 3) 「指紋を追加」をクリックして指紋を追加してください。
-



最大10つの指紋が登録可能です。

9.6 番号とシステムネットワーク

手順

1. ウェブページの右上にある「」をクリックして、ウィザードページに移動します。以前の設定が完了したら、「次へ」をクリックして「No. とネットワークシステム設定」ページに移動します。
2. デバイスタイプを設定します。



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

デバイス タイプ

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

コミュニティ番号

デバイスのコミュニティ番号を設定してください。

建物番号

デバイスの建物番号を設定してください。

ユニット番号

デバイスのユニット番号を設定します。

階番号

デバイスが設置されている階番号を設定してください。

ドアステーション番号

デバイスが設置されているドアステーション番号を設定します。



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

外ドアステーション番号

設置された外ドアステーションの番号を設定してください。



番号は1から99までの範囲です。

3. ビデオインターコムのネットワークパラメーターを設定します。

登録パスワード

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

メインステーションのIPアドレス

通信に使用するメインステーションのIPアドレスを入力してください。

プライベートサーバーIP

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

プロトコル 1.0 を有効にする

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

4. 設定を保存するには、設定完了後「完了」をクリックしてください。

第10章 ウェブブラウザ経由の操作

10.1 ログイン

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



注意

デバイスがアクティベートされていることを確認してください。

ウェブブラウザからログインしてください

ウェブブラウザのアドレスバーにデバイスのIPアドレスを入力し、**Enter**キーを押してログインページに移動します。

デバイスのユーザー名とパスワードを入力し、**ログイン**をクリックします。

クライアントソフトウェアのリモート設定経由でログイン

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

10.2 パスワードを忘れた場合

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

ログインページで「**パスワードを忘れた場合**」をクリック

し、**検証モード**を選択してください。

セキュリティ質問の確認

セキュリティ質問に回答してください。

メール認証

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

10.3 ヘルプ

10.3.1 オープンソースソフトウェアのライセンス

オープンソースソフトウェアのライセンスを確認できます。

画面右上にある「」をクリックし、→ **Open Source Software Statement** を選択してライセンスを確認できます。

10.3.2 オンラインヘルプドキュメントを表示

Web 設定のヘルプドキュメントを確認できます。

 → の右上にある「**オンラインドキュメント**」をクリックしてドキュメントを表示できます。

10.4 ログアウト

アカウントからログアウトします。

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

10.5 Web ブラウザからのクイック操作

10.5.1 パスワードを変更

デバイスのパスワードを変更できます。

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

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

10.5.2 言語を選択

デバイスのシステム言語を選択できます。

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

デフォルトでは、システム言語は英語です。



注意

システム言語を変更すると、デバイスが自動的に再起動します。

10.5.3 時間設定

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

タイムゾーン

ドロップダウンリストからデバイスの所在するタイムゾーンを選択します。

時間同期

NTP

NTP サーバーの IP アドレス、ポート番号、および間隔を設定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。

サーバーアドレス/NTPポート/間隔

サーバーアドレス、NTP ポート、および間隔を設定できます。

DST

DSTの開始時間、終了時間、およびバイアス時間を表示できます。

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

10.5.4 プライバシー設定

画像のアップロードと保存に関するパラメーターを設定できます。

ウェブページの右上にある「」をクリックして、ウィザードページに移動します。

画像のアップロードと保存

認証時に画像を保存

認証時に画像を自動的に保存します。

認証時に画像をアップロード

認証時に画像をプラットフォームに自動的にアップロードします。

登録済み画像の保存

この機能を有効にすると、登録された顔画像がシステムに保存されます。

リンクした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。

リンクしたカメラで撮影した画像を保存

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

10.5.5 管理者設定

手順

1. ウェブページの右上にある「」をクリックしてウィザードページに移動します。
2. 管理者の従業員IDと名前を入力します。
3. 追加する資格情報を選択します。

**注意**

少なくとも1つの資格情報を選択する必要があります。

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

**注意**

アップロードする画像は200KB以内であり、JPG、JPEG、PNG形式でなければなりません。

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

**注意**

最大50枚のカードに対応しています。

- 3) 「指紋を追加」をクリックして指紋を追加してください。

**注意**

最大10件の指紋を登録できます。

10.5.6 番号とシステムネットワーク

手順

1. ウェブページの右上にある「」をクリックして、ウィザードページに移動します。以前の設定が完了したら、「次へ」をクリックして「No. とネットワークシステム設定」ページに移動します。
2. デバイスタイプを設定します。

**注意**

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

デバイスタイプ

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

コミュニティ番号

デバイスのコミュニティ番号を設定してください。

建物番号

デバイスの建物番号を設定してください。

ユニット番号

デバイスのユニット番号を設定します。

階番号

デバイスが設置されている階番号を設定してください。

ドアステーション番号

デバイスが設置されているドアステーション番号を設定します。



注

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

外ドアステーション番号

設置された外ドアステーションの番号を設定してください。



注意

番号は1から99までの範囲です。

3. ビデオインターCOMのネットワークパラメーターを設定します。

登録パスワード

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

メインステーションのIPアドレス

通信に使用するメインステーションのIPアドレスを入力してください。

プライベートサーバーIP

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

プロトコル1.0を有効にする

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

4. 設定を保存するには、設定完了後「完了」をクリックしてください。

10.6 ユーザー管理

「追加」をクリックして、基本情報、証明書、認証設定を含むユーザーの情報を追加します。

基本情報を追加

「Person Management」をクリックし、→をクリックして「Add Person」ページに移動します。
従業員のID、氏名、性別、従業員の種類などの基本情報を入力します。

人物タイプに「訪問者」を選択した場合、訪問時間を設定できます。

「カスタムタイプ」を選択した場合、名前を編集できます。変更した名前はデバイスに適用されます。「人物の役割」を選択します。

「保存」をクリックして設定を保存します。

権限時間を設定します。

「Person Management」をクリックし、→をクリックして「Add Person」ページに移動します。
「長期有効ユーザーを有効にする」を選択するか、または「長期有効ユーザー」を設定すると、そのユーザーは設定した期間内のみ権限が有効になります。
「出席確認のみ」を有効にできます。有効化後、このユーザーにはアクセス制御権限が与えられません。
「保存」をクリックして設定を保存します。

デバイス番号を設定します。

「Person Management」をクリックし、「→」を選択し、「Add Person」をクリックし、「→」を選択して「Add」をクリックして「Add Person」ページに移動します。
「階数」と「部屋番号」のテキストボックスをクリックし、1から999までの数値を入力して階数と部屋番号を設定してください。
「保存」をクリックして設定を保存します。

認証設定

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

カードを追加

「Person Management」をクリックし、「→」を選択し、「Add」をクリックして「Add Person」ページに移動します。
「カードを追加」をクリックし、カード番号を入力し、プロパティを選択し、OKをクリックしてカードを追加します。
設定を保存するには「保存」をクリックします。

顔写真を追加

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



注意

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

「保存」をクリックして設定を保存します。

指紋を追加



注意

指紋機能に対応したデバイスのみ、指紋を追加できます。

「Person Management」をクリックし、→「Add」を選択して「Add Person」ページに移動します。
「指紋を追加」をクリックし、デバイスの指紋認証モジュールに指を置いて指紋を追加します。
「保存」をクリックして設定を保存します。

PINを追加

PINを設定する前に、PINがデバイス設定の個人用PINかプラットフォーム適用型個人用PINかを確認する必要があります。デバイス設定の個人用PINの場合、デバイスまたはウェブ上で作成または編集でき、他のプラットフォームでは設定できません。プラットフォーム適用型個人用PINの場合、プラットフォーム上で作成または編集でき、使用可能になる前にデバイスに発行する必要があります。デバイスまたはウェブ上で設定することはできません。

PINモードが「**デバイス設定の個人用PIN**」に設定されていることを確認してください。ページ上の「**PINモード**」をクリックして設定画面に移動します。

「**ユーザー管理**」→「**追加**」をクリックして「ユーザー追加」ページに移動します。

PINを設定します。または「**自動生成**」をクリックしてPINを自動的に生成します。設定を保存するには「**追加**」をクリックします。

「**保存して次へ**」をクリックして設定を保存し、次の人の追加を続行します。

デバイス番号の設定

「**人物管理**」をクリックし、「**→**」をクリックして「人物を追加」ページに移動します。

人物の基本情報を入力します。デバイス番号モジュールに移動します。**追加**をクリックし、該当する人物の部屋番号と階番号を入力します。**追加**または**保存して次へ**をクリックします。

人物の削除

人管理ページで削除する必要がある人物を選択し、**削除**をクリックします。**すべて削除**をクリックして、すべてのユーザーを削除します。

人物の編集

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

フィルタ

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

10.7 概要

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

 「」をクリックします。

機能説明:

ドア状態

動画画面のをクリックして、デバイスのライブ動画を表示します。



ライブビューを開始する際に音量を設定してください。



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



像を撮影できます。



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



ライブビューを開始時に録画できます。



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



フルスクリーン表示。

制御状態

ドアの開閉、開いたまま、閉じたままの状態を、実際のニーズに応じて制御できます。

リアルタイムイベント

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

デバイスリンク

リンクされたデバイスの数量とステータスを確認できます。



「**詳細を表示**」をクリックすると、に移動します。

人物情報

追加された情報と追加されていない情報の両方を確認できます。

ネットワーク状態

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

基本情報

モデル、シリアル番号、およびファームウェアバージョンを確認できます。

デバイス容量

人物、顔、指紋、カード、およびイベントの容量を確認できます。

**注意**

指紋モジュールが搭載されているデバイスのみ、指紋容量を表示できます。

10.8 アクセス制御アプリケーション

10.8.1 アンチパスバック設定

デバイス間のアンチパスバック機能は、設定されたルートに従って人員が順次認証を行う必要があります。この機能はサブデバイスでのみサポートされており、認証を伴う一方通行の通過のみがサポートされています。

手順

1. **アクセス制御**をクリックします。→ **アクセス制御アプリケーション**をクリックします。→ **クロスデバイス アンチパスバック**。
2. 機能を有効にします。
3. アクセスコントローラーのパラメーターを設定します（メインデバイス IP アドレス、メインデバイス ポート番号、メインデバイス パスワードを含む）。
4. デバイス登録コードを設定し、**登録状態**を確認できます。
5. カードリーダーを確認します。チェックされていないカードリーダーは、アンチパスバック機能で相互接続できません。

10.8.2 マルチドアインターロッキング設定

同じアクセス制御デバイスに接続された複数のドア間のマルチドアインターロッキングを設定します。1つのドアを開けるには、他のドアは閉じたままにする必要があります。

手順

1. **アクセス制御**をクリック→**アクセス制御アプリケーション**→**クロスデバイス・マルチドア・インターロッキング**。
2. 機能を有効にします。
3. **デバイスタイプ**を選択
 - メインデバイスとして設定されたデバイスには、**ポート番号**を設定し、**[追加]**をクリックしてアクセスポイントを追加します。**サブデバイス管理**をクリックすると、デバイスの状態を確認したり、デバイスを削除したりできます。
 - サブデバイスとして設定されたデバイスには、アクセスコントローラーパラメーター（**メインデバイスIPアドレス**、**メインデバイスポート番号**、**メインデバイスパスワード**）を設定する必要があります。デバイス登録コードを設定し、**登録ステータス**を確認できます。**カードリーダー**を確認してください。チェックされていないカードリーダーは、アンチパスバック機能で相互接続できません。
4. **アンチパスバックルール**を設定します。**認証ステータス**により
 - カードによる認証結果に基づいてアンチパスバックルーチンが判断されます。

実際の交通状況に応じて

実際のカード開錠状況に基づいて判断されるアンチパスバックルーチン。
5. **OK**をクリックしてください。

10.9 アクセス制御管理

10.9.1 イベント検索

イベント**検索**をクリックして検索画面に移動します。

イベントの種類、従業員ID、名前、カード番号、開始時間、終了時間などの検索条件を入力し、**検索**をクリックします。
結果は右側のパネルに表示されます。

10.9.2 ドアパラメーター設定

ドアの解錠パラメーターを設定します。

ドア番号を選択します。

ドアを選択して相対パラメーターを設定します。

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

ドア番号を選択します。通常、ドア1はデバイスとリンクされたドアであり、ドア2はセキュアドア制御ユニットとリンクされたドアです。

その他のドアパラメーターを設定し、**保存**をクリックします。

デバイスオンラインステータスを表示

デバイスのステータスを表示し、更新します。

アクセス制御→**パラメーター設定**→**ドアパラメーター**をクリックして設定画面を開きます。デバイスのオンライン状態を確認できます。リフレッシュをクリックしてデバイスの状態を更新します。

ドア名を設定

ドア名を作成します。

アクセス制御→**パラメーター設定**→**ドアパラメーター**をクリックして設定画面に入ります。**ドア名**を設定し、**保存**をクリックします。

PCウェブ経由でドアの開錠時間を設定

カードをかざした後にドアロックが開く時間を設定できます。

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

開錠後の動作時間（ドアが開錠された後の動作時間）を設定します。設定した時間内にドアが開られない場合、ドアは自動的にロックされます。設定可能な時間：1秒から255秒。

「保存」をクリックします。

PC Web 経由でドア開時間切れアラームを設定

ロック動作時間が経過してもドアが閉まらない場合、アクセス制御ポイントがアラームを鳴らします。

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

ドアの開錠タイムアウトアラームを設定します。ドアがロック動作時間内に閉まらない場合、アクセス制御ポイントでアラームが鳴ります。0に設定すると、アラームは有効になりません。

保存をクリックします。

ドアが閉まった際にドアをロックする

ドアが閉まった際にドアをロックするように設定できます。

アクセス制御の「→パラメーター設定」をクリックし、→の「ドアパラメーター」を選択して設定画面に入ります。

「ドアが閉まった際にドアをロックする」を有効にできます。

保存をクリックします。

PCウェブ経由でドア磁気センサーの種類を設定

配線方法に応じてドアの接触タイプを選択できます。

アクセスコントロール→パラメーター設定→ドアパラメーターを選択し、設定画面に移動します。磁気センサーの種類を「常時閉」または「常時開」から選択します。デフォルトでは「常時閉」に設定されています。

（特別な要件を除く）。

保存をクリックします。

PCウェブ経由で退出ボタンを設定

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

アクセス制御をクリックし、→パラメーター設定、→ドアパラメーターを選択して設定画面を開きます。退出ボタンタイプを設定します。デフォルトでは「常時開」です（特別な要件を除く）。

保存をクリックします。

PC ウェブ経由でドアロックの電源オフ状態を設定

ドアロックの電源オフ時のドアロック状態を設定できます。

アクセス制御をクリックし、**→パラメーター設定→ドアパラメーター**を選択して設定ページを開きます。**ドアロックの電源オフ状態**を設定します。デフォルトでは「閉じたまま」です。

保存をクリックします。

PCウェブ経由で拡張オープン時間を設定します。

ドアの接触センサーは、拡張アクセス権限を持つユーザーがカードをかざした後、適切な遅延時間を経て有効化できます。

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

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

「**保存**」をクリックします。

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

最初の人が認証されると、複数の人がドアにアクセスしたり、他の認証アクションを実行したりできます。

アクセス制御をクリックし、**→パラメーター設定→→ドアパラメーター**を選択して設定画面を開きます。最初の人が入室した際のドアの開錠時間を設定し、**保存**をクリックします。

PC ウェブ経由で緊急コードを設定

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

アクセス制御をクリックし、**→パラメーター設定→ドアパラメーター**を選択して設定ページに入ります。緊急コードを設定し、**保存**をクリックします。



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

PCウェブ経由でスーパーパスワードを設定する

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

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

保存をクリックします。



注意

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

10.9.3 認証設定

PC Web経由でメインまたはサブカードリーダーを選択してください。

端末を個人認証用に設定します。

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

その他のパラメーターを設定し、**保存**をクリックします。

PC ウェブ経由で端末タイプとモデルを確認

ターミナルタイプとモデルを確認できます。

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

PC Web経由で認証デバイスを有効化

有効化後、認証端末でカード読み取りが可能になります。

手順

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

PC ウェブ経由での認証を設定

証明書を設定します。

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

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

シングルクレデンシャル認証タイムアウト

各認証の有効期間を設定できます。



注

パスワード認証のタイムアウトはデフォルトで20秒であり、上記の設定によって制限されません。

初期認証タイプの制御

有効にすると、選択されたすべてのタイプが初回認証に使用可能です。

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

保存をクリックします。

PCウェブ経由で顔認証を手動でトリガーする

「手動で顔認証をトリガーする」を有効にした後、顔認証を行うには、デバイスの画面を手動でタッチする必要があります。

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

メインのカードリーダーをターミナルとして選択した場合、**顔認証による手動認証**を有効にし、認証モードを選択します。

単一認識

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

連続

認識をトリガーした後、デバイスがスリープモードに入るまで顔認識を継続できます。

保存をクリックします。

PCウェブ経由で認識間隔を設定

認証時に連続する2回の顔認識の間隔を設定します。

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



注意

1から10までの数字を入力してください。

PCウェブ経由で認証間隔を設定する

同じユーザーが認証を行う際の認証間隔を設定できます。同じユーザーは、設定された間隔内に1回のみ認証可能です。2回目の認証は失敗します。設定された間隔内に他のユーザーが認証を行った場合、そのユーザーは再度認証可能です。

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

PC Web経由で最大失敗試行回数のアラームを有効にする

設定値に達した際にアラームを報告するように有効にします。

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

端末をメインまたはサブカードリーダーとして選択した場合、**最大失敗試行回数アラーム**を有効にするためにスライダーを移動し、**最大認証失敗試行回数**を設定します。

保存をクリックします。

PC ウェブ経由での不正操作検出の有効/無効設定

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

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

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

保存をクリックしてください。

PC Web経由でカード番号反転機能を有効/無効にする

カード番号の反転機能を有効または無効にできます。

アクセス制御をクリックします。**→パラメーター設定**をクリックします。**→認証設定**をクリックして設定画面に入ります。**カード番号の逆転**を有効にすると、読み取ったカード番号が逆順で表示されます。

保存をクリックします。

サブカードリーダーの位置を設定します。

サブカードリーダーの位置を選択できます。

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

サブカードリーダーをターミナルとして選択した場合、サブカードリーダーの位置を「メインカードリーダーと異なる側」または「メインカードリーダーと同じ側」から選択できます。**保存**をクリックします。

PC Web経由でコントローラーとの通信を毎回設定

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

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

サブカードリーダーとして端末を選択した場合、**[コントローラーとの通信間隔]**を設定し、**[保存]**をクリックします。

Webクライアント経由でのパスワード入力タイムアウト期間を設定します。

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

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

サブカードリーダーをターミナルとして選択した場合、パスワード入力時の**最大間隔**を設定し、**[保存]**をクリックします。

PC Web経由でOK LEDの極性とエラー LEDの極性を設定します。

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

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

ターミナルをサブカードリーダーとして選択した場合、**OK LEDの極性**と**エラーLEDの極性**を設定し、**[保存]**をクリックします。

10.9.4 認証リンク設定

認証連携設定を設定できます。

手順

1. アクセス制御→パラメーター設定→認証設定をクリックして設定画面に入ります。

2. 連携機能を設定します。

認証時にリンクを呼び出す

この設定を有効にし、ユーザーが認証に成功した場合、ボタン設定の呼び出し先を自動的に呼び出し、ドアを遠隔操作で開きます。

認証に失敗した場合に呼び出しをリンク

有効化後、認証失敗の試行回数が設定数に達した場合、自動的にボタン設定の呼び出し先を呼び出し、ドアを遠隔操作で開錠します。

3. 保存をクリックします。

10.9.5 認証プランを設定

認証プランを設定できます。

アクセス制御の「→パラメーター設定」→「→認証設定」をクリックして設定画面に移動します。認証タイプを選択し、タイムバーで時間範囲をドラッグします。

保存をクリックします。

10.9.6 顔パラメーターを設定

ウェブブラウザ経由での顔認証の偽装防止を有効/無効にする

有効にすると、デバイスは人物が本物かどうかを認識できます。

アクセス制御をクリックし、→パラメーター設定をクリックし、→Smart をクリックして設定ページに移動します。顔認証の偽装防止を有効にし、保存をクリックします。

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

顔重複チェックの有効/無効

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



注意

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

アクセス制御をクリックし、→パラメーター設定、→Smart の順に選択して設定画面を開きます。顔の重複チェックを有効にします。

「保存」をクリックします。

PCウェブ経由でアンチスプーフィング検出レベルを設定します。

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

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

PCウェブ経由で認識距離を設定

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

PCウェブ経由でピッチ角度を設定

顔認識と認証時のレンズのピッチ角度を設定できます。**アクセスコントロール→パラメーター設定→スマート** をクリックして設定画面に入ります。



注意

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

ピッチ角度を設定し、**[保存]** をクリックします。

PCウェブ経由でヨー角を設定

顔認識と認証時にレンズのヨー角を設定できます。**アクセスコントロール→パラメーター設定→スマート** をクリックして設定画面に移動します。



注意

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

ヨー角を設定し、**保存** をクリックします。

PCウェブ経由での適用時に使用する顔画像の品質グレードを設定します。

顔認証のグレードは、成功するためには閾値よりも高くなければなりません。**アクセス制御→パラメーター設定→スマート** をクリックして設定画面に移動します。



注意

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

顔画像の品質等級を設定します適用する顔認証の等級は、閾値よりも高い必要があります。
保存をクリックします。

PCウェブ経由で1:1顔グレード閾値を設定

1:1顔グレード閾値を設定します。

アクセス制御に移動し、→パラメーター設定→Smartを選択します。1:1

顔画像グレード閾値を設定し、保存をクリックします。

閾値が高いほど、フロントカメラで撮影された画像の品質要件が高くなり、認証失敗の発生しやすさが増します。

PCウェブ経由で顔 1:1 一致閾値を設定

顔 1:1 一致閾値を設定します。

アクセス制御→パラメーター設定→Smartをクリックして設定画面に入ります。顔 1:1 一致閾値を設定し、保存をクリックします。

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

PCウェブ経由で1対N一致のしきい値を設定

顔認証の1:Nマッチング閾値を設定できます。

アクセス制御をクリックし、→パラメーター設定、→Smartを選択して設定画面に移動します。1:Nマッチング閾値を設定し、保存をクリックします。

値が大きいほど、誤認率が低く、誤拒否率が高くなります。最大値は100です。

ウェブブラウザで顔認識領域を設定する

顔認識および認証時にレンズの認識領域を設定できます。

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

プレビュー画面の黄色いボックスをドラッグして、顔認識の有効領域を左右上下に調整します。

または、ブロックをドラッグするか、数値を入力して有効領域を設定します。保存をクリックします。

、、またはをクリックして、キャプチャ、記録、またはフルスクリーン表示に移動します。

PC ウェブ経由で指紋パラメーターを設定

デバイスの指紋パラメーターを設定できます。

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

指紋セキュリティレベルを選択します。レベルが高いほど、偽認識率が低く、拒否率が高くなります。

「**保存**」をクリックします。

PC Web経由でECOモードを有効/無効にする

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

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

ECOモードが有効になっている場合、赤外線カメラを使用して低照度または暗い環境での顔認証が可能です。ECOモード（1:N）とECOモード（1:1）を設定できます。

マスク検出が有効になっている場合、マスク検出パラメーターも設定できます。

ECOモード（1:1）のしきい値

ECOモードの1:1一致モードで認証を行う際の照合閾値を設定します。値が大きいほど、誤認率（false accept rate）が低く、誤拒否率（false rejection rate）が高くなります。最大値は100です。

ECOモード（1:N）しきい値

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

マスク着用時の1:1一致閾値（ECO）

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

マスク着用時の顔認証 1:N マッチング閾値 (ECO)

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

保存をクリックします。

PCウェブ経由でマスク着用顔検出の有効/無効を切り替える

マスク着用顔検出を有効にすると、システムはマスクを着用した顔の画像を認識するか否かを判定します。

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

マスク着用顔の検出を有効にした後、以下の設定が可能です：マスクなし顔の戦略、マスク着用顔とマスクなし顔（1:1）、マスク着用顔 1:N 一致閾値（ECO）、マスク着用顔 1:1 一致閾値、およびマスク着用顔 1:N 一致閾値（ECO）。

マスクなし顔戦略

「なし」、「マスク着用リマインダー」および「マスク着用必須」から選択できます。マスク着用リマインダー
認証時にマスクを着用していない場合、デバイスが通知を表示し、ドアが開きます。

マスク着用必須

マスクを着用せずに認証を行った場合、デバイスは警告メッセージを表示し、ドアは閉じたままになります。

マスク着用時の顔認証（1:1）

マスクを着用した状態で顔認証を行う際の1:1マッチングモードでの一致値を設定します。値が大きいほど、誤認率（偽陽性率）が低く、誤拒否率（偽陰性率）が高くなります。最大値は100です。

マスク着用時の顔と顔（1:N）

マスクを着用した状態で認証を行う際の1:Nマッチングモードでの一致閾値を設定します。値が大きいほど、誤認率が低く、誤拒否率が大きくなります。最大値は100です。

マスク着用顔 1:1 マッチングしきい値 (ECO)

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

マスク着用時の顔認証 1:N マッチングしきい値 (ECO)

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

保存をクリックします。

10.9.7 カード設定

PC ウェブ経由で NFC 保護の有効/無効を設定します。

有効化後、デバイスはNFCカードを読み取ることができます。

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

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

Webクライアント経由でM1カード機能を有効/無効にする

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

M1 カードを有効にするをクリックします。

M1カード暗号化

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

セクター

M1カード暗号化を有効にした後、暗号化セクターを設定する必要があります。



注意

セクター13を暗号化することをおすすめします。

保存をクリックします。

Webクライアント経由でEMカードの有効/無効を切り替える

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

EMカードを有効にするをクリックし、**保存**をクリックしてください。



注

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

Webクライアント経由でCPUカード有効/無効化

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

CPUカードを有効にするをクリックします。

CPUカードの内容を読み込むを有効にするをクリックしてください。有効にすると、デバイスはCPUカードからコンテンツを読み込むことができます。

保存をクリックしてください。

DESFire カードの設定

DESFire カードと DESFire カードの内容を読み込む機能を有効にできます。

パラメーター設定 → **カード設定** をクリックして設定画面に入ります。**DESFire カード**と **DESFire カードの内容を読み取るを有効にし、保存** をクリックします。



注意

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

FeliCa カードの設定

FeliCa カードを有効にできます。

「**パラメーター設定**」をクリックし、**→ カード設定** を選択して設定画面に移動します。

FeliCa カード有効化 を選択します。

Web経由でカード番号認証パラメーターを設定

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

カード認証モードを選択し、**保存** をクリックします。

全カード番号

すべてのカード番号が読み込まれます。

3 バイト

デバイスは3バイトを読み取り、カードを読み込みます。

4 バイト

デバイスは4バイトでカードを読み取ります。

10.9.8 リモート検証を設定します。

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

アクセス制御 に移動してください。**→ パラメーター設定** → **端末パラメーター**。パラメーターを設定後、**保存** をクリックしてください。

リモート検証

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

リモートでの認証対象者タイプの選択

「リモートで認証対象者タイプを確認」を選択します。

資格情報をローカルで検証

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

リモート検証のタイムアウト期間

リモート検証のタイムアウト期間を設定します。

オフラインリモート検証によるロック解除

オフラインリモート検証によるロック解除を有効にできます。

結果返却モード

結果の返却モードを設定します。

10.9.9 プライバシー設定

PCウェブブラウザ経由でイベントの保存タイプを設定します。

イベントの保存タイプを設定できます。

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

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

古いイベントを定期的に削除

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

指定した時間に古いイベントを削除

時間を設定すると、設定した時間にすべてのイベントが削除されます。

上書き

システムが保存されたイベントが総容量の95%を超えたことを検出した場合、最も古い5%のイベントが削除されます。

保存をクリックします。

PCウェブ経由で認証結果を設定します。

認証結果の内容（画像、名前、従業員ID、体温など）を設定します。

アクセス制御をクリックし、→**アクセス制御**をクリックし、→**パラメーター設定**をクリックし、→**プライバシー設定**をクリックします。

認証結果に表示される内容（画像、名前、従業員IDなど）を確認します。

必要に応じて、**名前非識別化**と**ID非識別化**を設定します。非識別化後、名前とIDは内容の一部のみ表示されます。

認証結果の表示期間を設定すると、認証結果が設定した時間だけ表示されます。

保存をクリックします。

PC ウェブ経由での画像のアップロードと保存を設定します。

画像のアップロードと保存に関する設定を行うことができます。

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

認証時に画像を保存する。

認証時に画像を自動的に保存します。

認証時に画像をアップロード

プラットフォームへの認証時に画像を自動的にアップロードします。

画像モード

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

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

登録した画像を保存

この機能を有効にすると、登録された顔の写真はシステムに保存されます。

リンク撮影後の画像保存

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

リンク撮影後の画像のアップロード

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

通話中に撮影した写真をアップロード

この機能を有効にすると、通話中に写真が自動的に撮影され、自動的にアップロードされます。

保存をクリックします。

PCウェブ経由でデバイス内の画像を削除

登録済み、認証済み、またはキャプチャされた顔写真や画像をすべて削除できます。

アクセス制御 → **パラメーター設定** → **プライバシー設定**をクリックして設定画面に移動します。**クリア**をクリックして、登録済み、認証済み、または撮影した顔写真や手のひら写真をすべて削除します。

PC ウェブ経由で PIN モードを設定する

設定を行う前に、PINがプラットフォームで設定された個人用PINか、デバイスで設定された個人用PINかを確認してください。PINがデバイスで設定された個人用PINの場合、デバイスまたはPC WebでPINを編集できますが、プラットフォームで設定することはできません。PINがプラットフォームで設定された個人用PINの場合、プラットフォームでPINを設定する必要があります。デバイスまたはPC Webで設定することはできません。

アクセス制御→パラメーター設定→プライバシー設定に移動します。

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

プラットフォーム適用個人用PIN

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

デバイス設定の個人用PIN

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

保存をクリックします。

10.9.10 設定

Web経由でデバイス番号を設定

このデバイスはドアステーションまたは外ドアステーションとして使用できます。使用前にデバイス番号を設定する必要があります。

「ビデオインターコム」をクリックし、「→」→「Call Settings」→「→」→「Device No.」を選択します。

Device Type	Door Station ▼
Period No.	1
Building No.	1
Unit No.	1
Floor No.	1 ▼
Door Station No.	0
Community No.	0

Save

図10-1 デバイス番号の設定

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

デバイスタイプ

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

**注意**

デバイスタイプを変更した場合、デバイスを再起動する必要があります。

階番号

デバイスが設置されている階番号を設定してください。

ドアステーション番号

デバイスが設置されている階番号を設定してください。

**注意**

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

コミュニティ番号

デバイスのコミュニティ番号を設定してください。

建物番号

デバイスのビル番号を設定してください。

ユニット番号

デバイスのユニット番号を設定します。



注

番号を変更した場合、デバイスを再起動する必要があります。設定を

保存するには、設定後「保存」をクリックしてください。

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

外ドアステーション番号

外ドアステーションをデバイスタイプとして選択した場合、1から

99の数字を入力する必要があります。



注意

番号を変更した場合、デバイスを再起動する必要があります。

コミュニティ番号

デバイスのコミュニティ番号を設定します。

ウェブブラウザ経由でビデオインターCOMのネットワークパラメーターを設定します。

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

「ビデオインターCOM」をクリックし、→「コール設定」をクリックし、→「ビデオインターCOMネットワーク」をクリックして設定画面に入ります。

登録パスワード

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

メインステーションIP

通信に使用するメインステーションのIPアドレスを入力します。

プライベートサーバーIP

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

プロトコル1.0を有効にする

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

*Registration Password

*Main Station IP

*Private Server IP

Enable Protocol 1.0 ☐

Save

図10-2 ビデオインターコムネットワーク

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

保存をクリックします。

PC ウェブ経由で通信時間を設定

最大通信時間を設定します。

ビデオインターコムに移動し、→ コール設定→ コール設定 を選択します。

最大通信時間を入力してください。自動応答を有効にできます。



注意

最大通信時間の範囲は90秒から120秒です。保存をクリックします。

PC ウェブから通話するにはボタンを押してください

手順

1. アクセス制御をクリック→ コール設定→ ボタンを押してコールをクリックして設定ページに移動します。

No.	Button Settings
01	☐ Call Specified Indoor Station Enter Room No. ☐ Call Management Center ☒ Call Indoor Station ☐ app

Link Authentication to Call ☒

If you enable this and person passes authentication, door will be remotely opened by the target that is configured with button for automatic calling.

Save

図10-3 ボタンを押して通話

2. 必要に応じて、指定の室内ステーションへの通話、コール管理センターへの通話、室内ステーションへの通話、またはアプリを選択してください。



指定の室内端末を呼び出すを選択した場合、室内端末の**部屋番号**を入力する必要があります。

- 必要に応じて**リンク認証を有効にしてください**。有効にした後、認証を通過した人がボタンで自動呼び出しが設定されたターゲットに近づくと、ドアがリモートで開きます。
- 保存**をクリックしてください。

呼び出し優先度

通話の優先順位を設定できます。

手順

- ビデオインターコム**をクリックし、→ **コール設定**→ **コール優先度**を選択して設定画面に移動します。
- コールタイプ**を確認し、各3つの優先順位ごとに**リング持続時間**を設定します。
- 保存**をクリックして設定を有効にします。



レベルが高いほど、呼び出しやすいデバイスになります。呼び出し時間が経過すると、次のレベルの呼び出しがトリガーされます。

PCウェブ経由での番号設定

部屋のSIP番号を設定します。部屋同士はSIP番号を介して通信可能です。

手順

- アクセス制御**→ **コール設定**→ **番号設定**。

+ Add Delete				
☐	No. ↕	Room No. ↕	SIP Number ↕	Operation
☐	1	4	SIP1 : 114	⚡ 🗑
☐	2	5	SIP1 : 115	⚡ 🗑
☐	3	2	SIP1 : 116 SIP2 : 114	⚡ 🗑
☐	4	6	SIP1 : 116	⚡ 🗑
☐	5	1	SIP1 : 2002	⚡ 🗑

図10-4 番号設定

- 「**追加**」をクリックし、**部屋番号**と**SIP1**電話番号を入力します。
- オプション**: **[追加]**をクリックして SIP 番号を追加するか、**[🗑]**をクリックして番号を削除します。
- 保存**をクリックします。
- オプション**: **削除**をクリックして、部屋番号とそのSIP番号を削除できます。

10.10 デバイス管理

デバイス番号、タイプ、IPアドレス、シリアル番号、モデル、バージョン、階数、部屋番号、番号、武装状態、ユーザー名、ネットワーク状態、および操作を確認できます。デバイス管理ページでは、室内ステーションとサブドアステーションを追加し、デバイスを管理、アップグレード、または削除することもできます。

手順

1. 「デバイス管理」をクリックします。
2. 「追加」をクリックします。
3. デバイスタイプを選択し、デバイスパスワード、登録パスワード、シリアル番号、IP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、ポート、フロア番号（室内ステーションの場合はフロア番号と番号の入力は不要）を入力します。
4. 「保存」をクリックします。
5. オプション: 以下の操作も行うことができます。

デバイスを削除 削除するデバイスを選択し、**削除**をクリックします。

デバイスをインポート USBフラッシュドライブ（デバイス情報を含む）をデバイスに接続し、インポートをクリックしてデバイス情報をインポートします。

デバイスをエクスポート 「エクスポート」をクリックして、デバイス情報ファイルをUSBフラッシュドライブにエクスポートします。

10.11 システム構成

10.11.1 PC ウェブ経由でデバイス情報を表示

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

「システムとメンテナンス」をクリックし、「→」→「System Configuration」→「→」→「System」→「→」→「System Settings」→「→」→「Basic Information」をクリックして設定ページに入力します。

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

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

10.11.2 時間設定

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

「システムとメンテナンス」→「→」→「System Configuration」→「→」→「System」→「→」→「System Settings」→「→」→「Time Settings」をクリックします。

Device Time 2024-01-02 11:20:48

Time Zone (GMT+08:00) Beijing, Urumqi, Singapore, Perth

Time Synchronization mode ☒ NTP ☐ Manual

* Server IP Address 192.0.0.64

* NTP Port 123

* Interval 60 min

DST

DST ☒

Start Time April First Sunday 02:00

End Time October Last Sunday 02:00

DST Bias ☐ 30minute(s) ☒ 60minute(s) ☐ 90minute(s) ☐ 120minute(s)

Save

図10-5 時刻設定

設定を保存するには、設定完了後に「保存」をクリックしてください。

タイムゾーン

ドロップダウンリストからデバイスが所在するタイムゾーンを選択してください。

タイムシンクロナイズ

NTP

NTPサーバーのIPアドレス、ポート番号、および間隔を設定してください。

手動

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

サーバー アドレス タイプ/サーバー アドレス/NTP ポート/間隔

サーバーアドレスの種類、サーバーアドレス、NTP ポート、および間隔を設定できます。

10.11.3 管理者のパスワードを変更する

手順

1. システムとメンテナンスをクリックします。→システム構成をクリックします。→システムをクリックします。→ユーザー管理→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. 「保存」をクリックします。



注意

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

10.11.4 PCウェブ経由のアカウントセキュリティ設定

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

手順

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

10.11.5 PC ウェブ経由でデバイスの武装/解除情報を確認する

デバイスの武装タイプと武装IPアドレスを確認します。

システムとメンテナンスに移動し、→システム構成→システム→ユーザー管理→警報設定/解除情報を選択します。

デバイスの武装/解除情報を表示できます。ページを更新するには「リフレッシュ」をクリックしてください。

10.11.6 PC Web経由で動作モードを設定

デバイスのターミナルパラメーターを設定できます。



注意

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

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

動作モード

作業モードをアクセス制御モードまたは許可不要モードに設定できます。

アクセス制御モード

アクセス制御モードはデバイスの標準モードです。アクセスするには、認証情報を入力する必要があります。

10.11.7 ネットワーク設定

PCのウェブブラウザから基本ネットワークパラメーターを設定します

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

NIC Type: Self-Adaptive

DHCP: ☐

*IPv4 Address: 10.6.122.245

*IPv4 Subnet Mask: 255.255.255.0

*IPv4 Default Gateway: 10.6.122.254

IPv6 Mode: ☐ Manual ☒ DHCP ☐ Route Advertisement

IPv6 Address: 6012:bbbb:2ca3:cf:fe:f9:e0:f2

IPv6 Subnet Prefix Length: 64

IPv6 Default Gateway: fe80::8261:6cff:fe:da7445

Mac Address: e0:ca:3c:f9:e0:f2

MTU: 1500

DNS Server

DHCP: ☒

Preferred DNS Server: 8.8.8.8

Alternate DNS Server: 8.8.4.4

Save

図10-6 TCP/IP設定ページ

パラメーターを設定し、[保存] をクリックして設定を保存します。

NIC タイプ

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

DHCP

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

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

DNSサーバー

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

Wi-Fi パラメーターを設定してください。

デバイスのワイヤレス接続用のWi-Fi設定を指定します。

手順



注意

この機能はデバイスでサポートされている必要があります。

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

図10-7 Wi-Fi設定画面

2. Wi-Fiを確認します。
3. Wi-Fiを選択します。

-  リストからWi-Fiを選択し、Wi-Fiのパスワードを入力します。
- 「追加」をクリックし、Wi-Fiの名前、パスワード、および暗号化タイプを入力します。「接続」をクリックします。Wi-Fiが接続されたら、「OK」をクリックします。

4. オプション: WLAN パラメーターを設定します。

- 1) IPアドレス、サブネットマスク、およびデフォルトゲートウェイを設定します。またはDHCPを有効にすると、システムがIPアドレス、サブネットマスク、およびデフォルトゲートウェイを自動的に割り当てます。

5. 保存をクリックします。

PC Web経由でポートを設定

システムとメンテナンスに移動し、→、システム構成、→、ネットワーク、→、ネットワークサービスを選択します。

HTTPの有効/無効を切り替えます

HTTP機能を有効にすると、ブラウザのアクセスセキュリティが向上します。

システムとメンテナンス →→→ システム構成 →→→ ネットワーク →→→ ネットワークサービス → HTTP(S) を選択します。
パラメーターを設定した後、[ClickSave] をクリックしてください。

HTTP ポート

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

192.0.0.65:81 と入力する必要があります。

HTTPS ポート

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

HTTP リスニング

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

PC ウェブ経由で RTSP ポートを表示

RTSPポートは、リアルタイムストリーミングプロトコルのポートです。

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

PC Web経由でWebSocketを設定します。

WebSocket と WebSockets ポートを表示します。

システムとメンテナンス →→→ システム構成 →→→ ネットワーク →→→ ネットワークサービス → **WebSocket(s)** を選択します。
WebSocket と WebSockets のポートを表示します。

SDK サービスを有効にする

SDKサービスを有効にすると、デバイスはSDKサーバーに接続できます。

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

サーバーポートを入力します。

保存をクリックして設定を有効にします。

PC ウェブ経由で ISUP パラメーターを設定

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

手順



注意

この機能はデバイスでサポートされている必要があります。

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



注意

バージョンに5.0を選択した場合、暗号化キーも設定する必要があります。

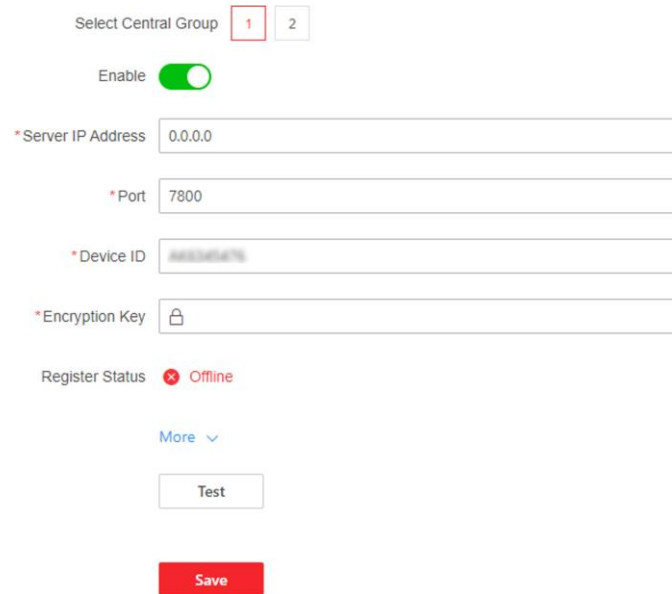
4. ISUP リスニングパラメーターを設定します。これには、ISUP アラームセンター IP アドレス/ドメイン名、ISUP アラームセンター URL、および ISUP アラームセンター ポートが含まれます。
5. 保存をクリックします。

PC Web経由でOTAPを設定

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

手順

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



Select Central Group 1 2

Enable ☒

* Server IP Address

* Port

* Device ID

* Encryption Key

Register Status ❌ Offline

[More](#) ▼

図10-8 OTAPを設定

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

PCウェブ経由でのプラットフォームアクセス

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

手順

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



注意

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

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



注意

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

-
6. 「保存」をクリックして設定を有効にします。

VoIP アカウント設定

ネットワーク経由で音声通話を実現できます。

手順

1. システムとメンテナンスに移動し、→システム構成→ネットワーク→デバイスアクセス→VoIP。
2. コールタイプを選択し、VoIPを選択します。
3. VoIPゲートウェイを有効にします。
4. ユーザー名、登録パスワード、サーバーIPアドレス、サーバーポート、有効期限、登録状態、番号、表示ユーザー名、およびセンター番号を設定します。
5. 保存をクリックします。

10.11.8 PC ウェブ経由でビデオとオーディオパラメーターを設定

ウェブブラウザ経由でビデオパラメーターを設定します。

デバイスカメラの品質、解像度、その他のパラメーターを設定できます。

システムとメンテナンスをクリックし、→システム構成→ビデオ/オーディオ→ビデオを選択して設定ページに移動します。カメラ名、ストリームタイプ、ビデオタイプ、解像度、ビットレートタイプ、ビデオ品質、フレームレート、最大ビットレート、ビデオエンコード、およびフレーム間隔を設定します。
「保存」をクリックします。

ウェブブラウザ経由でオーディオパラメーターを設定

デバイスの音量を設定できます。

システムとメンテナンスをクリックし、→システム設定→ビデオ/オーディオ→オーディオをクリックして設定画面に入ります。ストリームの種類とオーディオエンコードを実際のニーズに合わせて設定してください。スライダーを動かして入力音量と出力音量を調整してください。

スライダーを動かして音声ガイド機能を有効にします。

オーディオミキシングを有効にし、出力サブボリュームを設定できます。SIPオーディオエンコードを選択してください。

保存をクリックしてください。

10.11.9 設定にアクセス

PCウェブ経由でRS-485パラメーターを設定

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

システムとメンテナンスをクリックします。→システム構成をクリックします。→アクセス構成をクリックします。→RS-485をクリックします。RS-485プロトコルを選択します。

RS-485を有効にし、パラメーターを設定してください。

設定完了後、[保存]をクリックして設定を保存します。

No.

RS-485番号を設定してください。

周辺機器の種類

実際の状況に応じて、ドロップダウンリストから周辺機器を選択してください。



注意

周辺機器を変更して保存すると、デバイスが自動的に再起動します。

RS-485 アドレス

実際の要件に応じてRS-485アドレスを設定してください。



注意

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

ボーレート

RS-485プロトコルでデバイスが通信する際のボーレートです。

PC Web経由でWiegandパラメーターを設定

Wiegandの送信方向を設定できます。

手順



注意

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

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

Wiegand ☒

Wiegand Direction ☒ Input ☐ Output

Wiegand Mode Wiegand34 Custom Wiegand Settings

Time Interval 1 ms

Pulse Width 100 us

Save

図10-9 Wiegand ページ

2. **Wiegand** をチェックして、Wiegand 機能を有効にします。

3. 送信方向を設定します。

入力

このデバイスはWiegandカードリーダーを接続できます。

出力

外部アクセスコントローラーに接続できます。2つのデバイスは、Wiegand 26または34経由でカード番号を送信します。

4. 設定を保存するには「**保存**」をクリックしてください。



注意

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

10.11.10 画像パラメーター設定

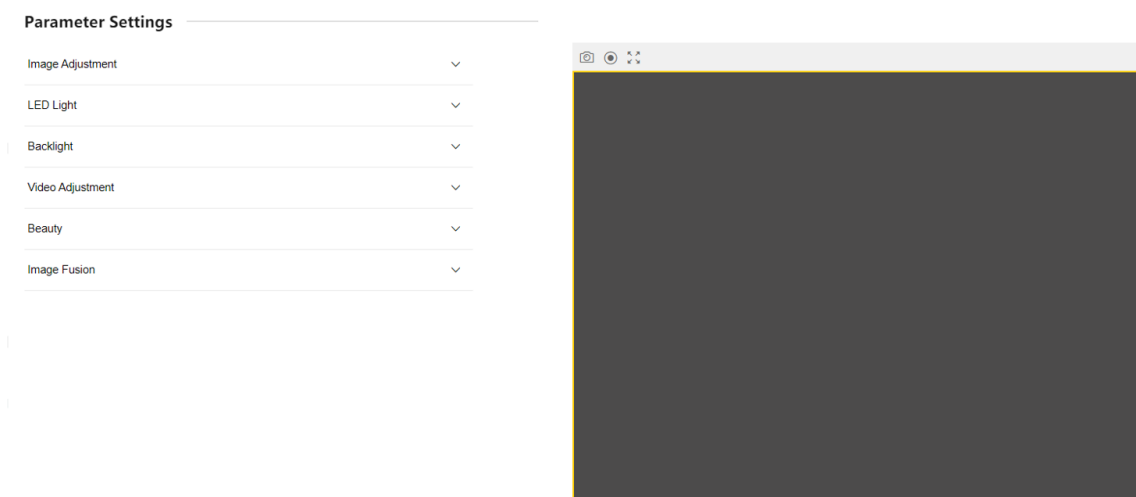


図10-10 表示設定

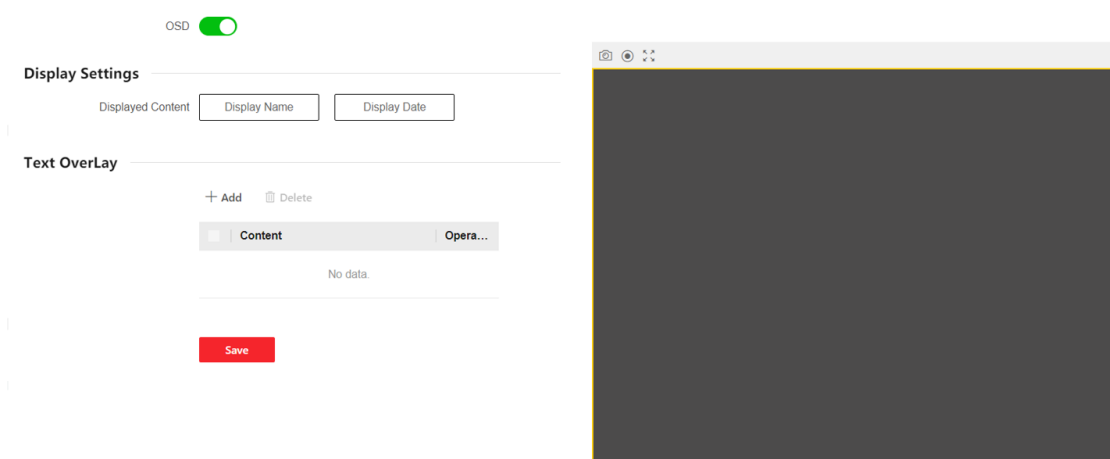


図10-11 OSD設定

PC Web経由で明るさ/コントラスト/彩度/シャープネスを設定

ライブビューページの明るさ、コントラスト、彩度、シャープネスなどの画像情報を設定できます。

システムとメンテナンスをクリックし、→、システム構成、→、画像、→、ディスプレイ設定を選択して設定画面に入ります。
画像調整

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

PCウェブ経由でLEDライトを設定

補助ライトの明るさを調整できます。

手順

1. 「システムとメンテナンス」をクリックし、「→」→「システム構成」→「→」→「Image」→「→」→「Display Settings」をクリックして設定画面を開きます。
2. 補助ライトのタイプ、モード、明るさを設定します。
3. オプション: **デフォルト設定に戻す**をクリックして、デフォルト設定に戻します。

PCのウェブブラウザからビデオ標準を設定します。

ライブビューページの動画設定を変更できます。

システムとメンテナンスをクリックし、→、システム構成、→、画像、→、ディスプレイ設定を選択して設定画面に移動します。

動画調整

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

PAL

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

NTSC

1秒あたり30フレーム。アメリカ合衆国、カナダ、日本、台湾（中国）、韓国、フィリピンなどに適しています。

「**デフォルト設定に戻す**」をクリックして、デフォルト設定に戻します。

10.11.11 リンク設定

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

手順

1. 「システムとメンテナンス」をクリックし、「→」→「システム構成」→「→」→「Event」→「→」→「Linkage Settings」をクリックして設定画面に移動します。
2. +「」をクリックします。
3. イベントソースを設定します。連携タイプとして「**イベント連携**」「**カード連携**」または「**従業員ID連携**」を選択します。

- リンクタイプを「イベントリンク」に設定すると、実際のニーズに応じてイベントの種類を選択できます。
- リンクタイプを「カードリンク」に選択し、カード番号を入力し、カードリーダーを選択します。
- リンクタイプを「従業員IDリンク」に選択し、従業員IDを入力し、カードリーダーを選択します。

4. リンク動作を設定します。

- 1) ドアリンクを有効にし、ドアアクションを選択します。
- 2) リンクキャプチャを有効にします。

5. 保存をクリックして設定を有効にします。

10.11.12 勤怠設定

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

ウェブ経由で出席モードを無効化

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

手順

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

結果

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

ウェブ経由で手動出席を設定する

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

開始前に

少なくとも1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。詳細については、ユーザー管理を参照してください。

手順

1. システムとメンテナンスをクリックし、→、システム構成、→、プラットフォーム出席を選択して設定画面に移動します。
2. 出席モードを「手動」に設定してください。

3. 出席ステータスの必須設定を有効にし、出席ステータスの有効期間を設定します。

4. 出席ステータスのグループを有効にします。



注意

出席プロパティは変更されません。

5. オプション: 必要に応じてステータスを選択し、名前を変更できます。

結果

認証後、出席ステータスを手動で選択する必要があります。



注意

ステータスを選択しない場合、認証は失敗し、有効な出席として記録されません。

Web経由で自動出席を設定する

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

開始前に

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

手順

1. システムとメンテナンスをクリックし、**→システム構成→プラットフォーム出席**を選択して設定画面を開きます。
 2. 出席モードを「自動」に設定します。
 3. 「出席ステータス必須」機能を有効にします。
 4. 出席ステータスのグループを有効にします。
-



注

出席プロパティは変更されません。

5. オプション: 必要に応じてステータスを選択し、名前を変更します。

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

Web経由で手動と自動の出席を設定します。

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

開始前に

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

手順

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



出席プロパティは変更されません。

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

結果

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

例

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

10.12 設定オプション

10.12.1 PCウェブ経由でスタンバイ画像を設定

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

システムとメンテナンスに移動し、→ 設定→ 画面表示 を選択します。

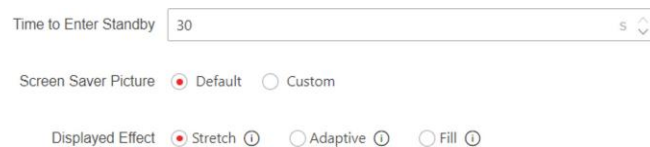


図10-12 スタンバイ画像設定

スタンバイ画像のパラメーターを設定し、[保存]をクリックします。

スタンバイ状態に移行する時間

設定された時間経過後、デバイスは待機画面を表示します。

スクリーンセーバー画像

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



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

表示効果

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

スライドショー間隔

複数の写真を追加した場合、写真の切り替え時間を設定できます。

10.12.2 PCウェブ経由でスリープ時間を設定

設定した時間経過後、デバイスはスリープモードになります。この機能は電力消費を削減します。

システムとメンテナンスに移動し、→設定、→画面表示を選択します。



図10-13 スリープ設定

スリープ時間をスライドして設定し、**保存**をクリックします。

10.12.3 PCウェブ経由で認証デスクをカスタマイズ

認証ページ/デスクのモジュールをカスタマイズします。

手順

1. システムとメンテナンスに移動し、→設定→カスタムホームページを選択します。

2. アプリケーションモードを選択

します。**アクセスモード**

デバイス認証ページが表示され、ライブビューページが表示されます。認証後、人物の名前、従業員ID、顔写真が表示されます。

インターコムモード

認証インターフェースには、クイック操作領域と認証領域が表示されます。クイック操作領域では、機能用のカスタマイズ可能なショートカットキーをサポートしています。

シンプル

このモードを選択すると、認証ページのライブビューが無効になります。認証後、人物の名前、従業員ID、顔写真がすべて非表示になります。

3. 適用をクリック。

10.12.4 PCウェブ経由での通知の公開を設定します。

デバイスの通知の公開設定を変更できます。

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

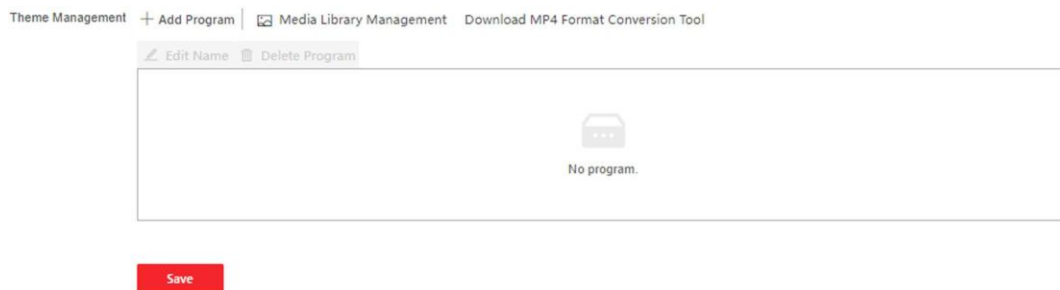


図10-14 通知の公開MP4形式変換ツールのダ

ウンロード

MP4 形式変換ツールをダウンロードするには、必要に応じて「**MP4 形式変換ツールをダウンロード**」をクリックしてください。

素材管理

「+」をクリックし、「**テーマを追加**」を選択し、テーマ名と**テーマの種類**を設定します。

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



注意

現在、追加できるテーマは1つだけです。

プログラムの追加

プログラム名を設定し、プログラムの種類を選択できます。

画像

画像を選択した場合、画像を追加するには「+」をクリックしてください。

ウェルカムメッセージ

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

標準

標準を選択すると、背景色と画像を設定できます。

再生スケジュール

テーマを作成した後、テーマを選択し、タイムライン上にスケジュールを描画できます。描画したスケジュールを選択すると、開始時間と終了時間を正確に編集できます。

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

スライドショー間隔

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

10.12.5 PCウェブ経由でプロンプトスケジュールを設定する

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

手順

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

Enable ☒

Appellation ☒ None

Time Period When Authentication Succeeded

Period1 Delete

Time 00:00:00 - 23:59:59

Language ☒ English

* Audio Prompt Content Authenticated.

+ Add Time Duration

Time Period When Authentication Failed

Period1 Delete

Time 00:00:00 - 23:59:59

Language ☒ English

* Audio Prompt Content Authentication failed.

+ Add Time Duration

Save

図10-15 プロンプトスケジュール

2. 機能を有効にします。
3. 呼び出し名を設定します。
4. 時間スケジュールを選択します。
5. 認証が成功した際の時間範囲を設定します。
 - 1) 「時間期間を追加」をクリックします。

- 2) 時間期間を設定します。



設定した時間範囲内で認証が成功した場合、デバイスは設定されたコンテンツを放送します。

- 3) 音声プロンプトの内容を設定します。
 4) オプション: サブステップ1から3を繰り返し実行します。
 5) オプション: [🗑️] をクリックして、設定された時間期間を削除します。

6. 認証に失敗した際の時間設定を設定します。

- 1) 「時間間隔を追加」をクリックします。
 2) 時間設定を設定します。



設定した時間内に認証に失敗した場合、デバイスは設定されたコンテンツを放送します。

- 3) オーディオコンテンツを設定します。
 4) オプション: サブステップ1から3を繰り返し実行します。
 5) オプション: 設定した時間範囲を削除するには、[🗑️] をクリックします。

7. 「Save」をクリックして設定を保存します。

10.12.6 PC ウェブ経由でプロンプト音声のカスタマイズ

デバイスのプロンプト音声のカスタマイズが可能です。

手順

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

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

図10-16 カスタムプロンプト

2. 「」 をクリックし、「→」を選択し、「」 をクリックし、実際のニーズに応じてローカルPCからオーディオファイルをインポートします。



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

10.12.7 PC ウェブ経由で認証結果テキストを設定

手順

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

Text	Content
* Stranger	
* Authenticated	
* Authenticating Failed	

Save

図10-17 認証結果テキスト

2. 認証結果テキストのカスタマイズを有効にします。
3. カスタムテキストを入力します。
4. 保存をクリックします。

10.13 システムとメンテナンス

10.13.1 再起動

デバイスを再起動できます。

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

10.13.2 アップグレード

PC ウェブ経由でローカルにアップグレード

デバイスをローカルでアップグレードできます。

システムとメンテナンスをクリックし、→ **Maintenance**→ **Upgrade** を選択して設定画面に移動します。

ドロップダウンリストからアップグレードの種類を選択します。📁 をクリックし、ローカルPCからアップグレードファイルを選択します。アップグレードをクリックしてアップグレードを開始します。

PC ウェブ経由のオンラインアップグレード

デバイスをオンラインでアップグレードできます。

システムとメンテナンスをクリックし、**→メンテナンス→アップグレード**を選択して設定画面に移動します。「更新を確認」をクリックして、更新バージョンがあるかどうかを確認します。

デバイスがネットワークに接続されており、Hik-Connect アプリに追加されている場合、Hik-Connect アプリに更新バージョンがある場合に、デバイス上で「**デバイスアップグレード**」→「**→オンラインアップグレード**」をタップしてアップグレードできます。

キーフォブをアップグレード



注意

- 周辺モジュールがオンライン状態であることを確認してください。
- キーフォブをアップグレードする際は、顔認識端末を1台のみ周囲に配置し、キーフォブを移動しないでください。

システムとメンテナンスをクリックし、**→メンテナンス、→アップグレード**を選択します。アップグレード設定のドロップダウンリストから**キーフォブ**を選択します。ローカルPCからアップグレードファイルを選択し、**アップグレード→OK**をクリックします。キーフォブの任意のボタンを押してアップグレードを実行します。

10.13.3 復元

ウェブブラウザ経由で工場設定に復元

デバイスを工場出荷時設定に復元できます。

システムとメンテナンスをクリックし、**→メンテナンス、→バックアップとリセット**を選択して設定画面に移動します。

「**すべて復元**」をクリックすると、すべてのパラメーターが工場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。

PC ウェブ経由でデフォルト設定に復元

デバイスをデフォルト設定に復元できます。

システムとメンテナンスをクリックし、**→Maintenance→Backup and Reset**を選択して設定画面に入ります。

「**復元**」をクリックすると、デバイスはデフォルト設定に復元されます。ただし、デバイスのIPアドレスとユーザー情報は除きます。

10.13.4 PC ウェブ経由でデバイス パラメーターをエクスポート

デバイスパラメーターをエクスポートします。

システムとメンテナンスに移動し、→ メンテナンス、→ バックアップとリセットを選択します。

バックアップ

エクスポートをクリックして、デバイスパラメーターをエクスポートします。



注意

デバイスのパラメーターをエクスポートし、他のデバイスにインポートします。

10.13.5 PC Web経由でデバイスパラメーターをインポート

構成パラメーターをインポートします。

システムとメンテナンスに移動し、→ メンテナンス→ バックアップとリセットを選択します。

設定ファイルのインポート

「」をクリックし、ローカルPCからファイルを選択します。次に「インポート」をクリックします。

10.13.6 デバイス デバッグ

デバイス デバッグ パラメーターを設定できます。

Web ブラウザ経由で SSH を有効/無効にする

SSHを有効にしてリモートデバッグを実行できます。

システムとメンテナンスをクリックし、→ Maintenance、→、Device Debugging、→、Log for Debugging の順に選択し、SSH を有効にします。

SSHはリモートデバッグに使用されます。このサービスを使用する必要がある場合は、セキュリティを向上させるため、SSHを無効にすることをおすすめします。

PCのウェブブラウザからデバイスログを印刷

デバイスログを印刷できます。

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

「エクスポート」をクリックしてデバイスログを印刷します。

PCのウェブブラウザからネットワークパケットをキャプチャ

キャプチャするパケットの期間とサイズを設定し、キャプチャを開始します。キャプチャ結果に基づいてログを確認し、デバッグを行うことができます。

システムとメンテナンスに移動し、→メンテナンス→デバイスデバッグ→デバッグ用ログをクリックします。キャプチャパケット期間、キャプチャパケットサイズを設定し、[キャプチャを開始]をクリックします。

PCウェブ経由でプロトコルをテスト

プロトコルアドレスを選択し、テストするプロトコルを入力します。応答ヘッダーと返却値に基づいてデバイスをデバッグできます。

システムとメンテナンスに移動し、→メンテナンス、→デバイスデバッグ、→プロトコルテストを選択します。

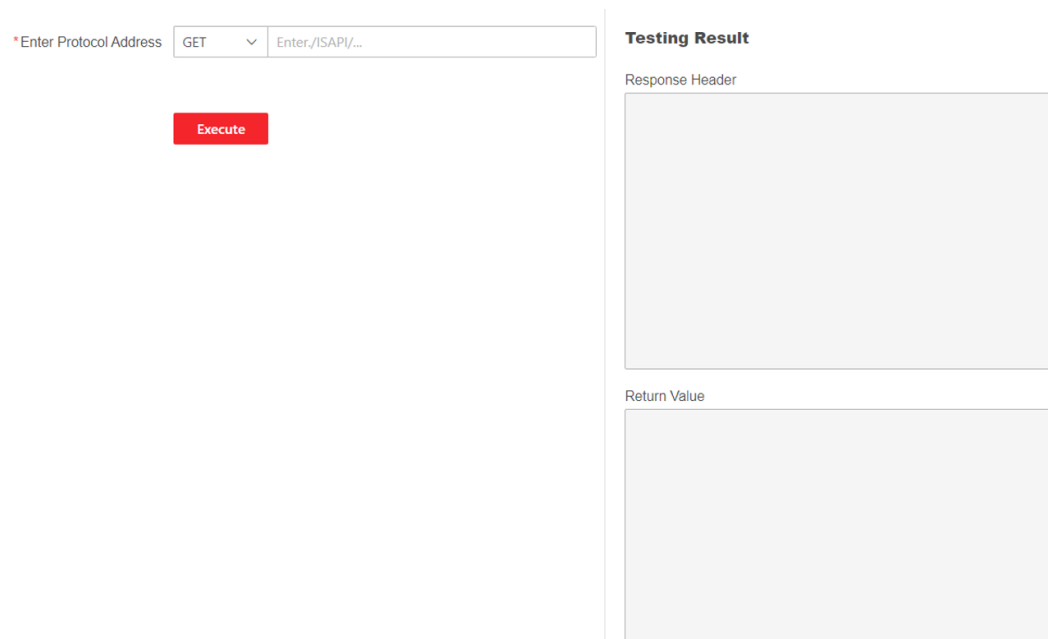


図10-18 プロトコルテスト

プロトコルアドレスを選択し、プロトコルを入力します。**実行**をクリックします。
デバイスの応答ヘッダーと返り値に基づいてデバッグを行います。

PCウェブ経由のネットワーク診断

デバイスのIPアドレスまたはドメイン名を入力し、PING設定を行うことができます。PINGの結果に基づいてネットワークをデバッグします。

システムとメンテナンス→Maintenance→デバイスデバッグ→ネットワーク診断へ移動します。

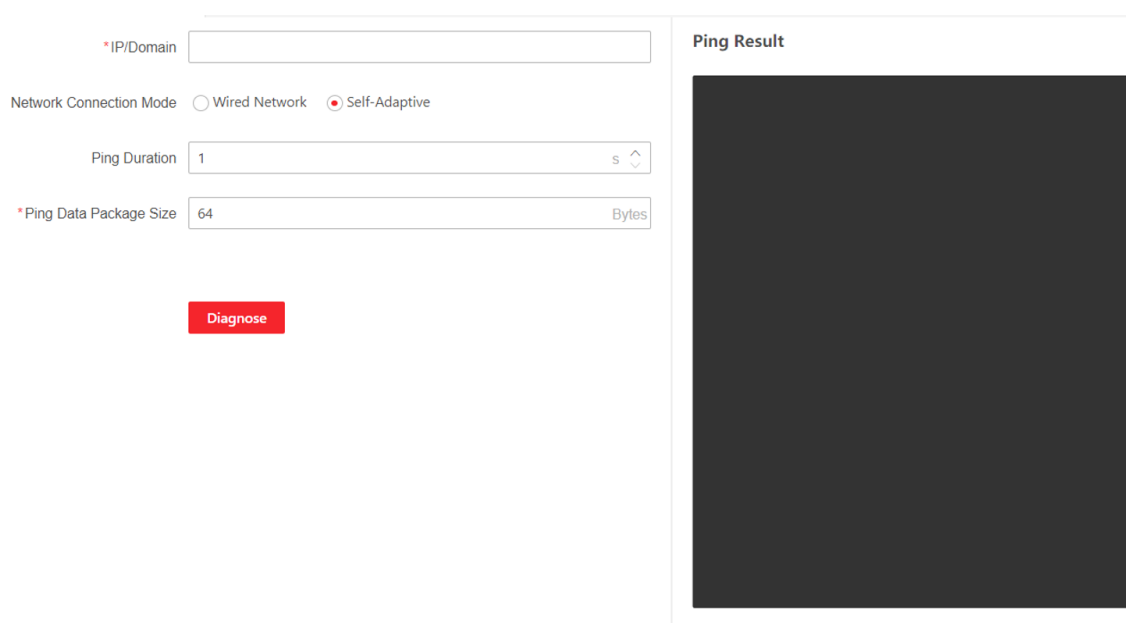


図10-19 ネットワーク診断

PING操作のデバイスIPを入力し、ネットワーク接続モード、PING持続時間、Pingデータパッケージサイズ（デフォルトパラメーターが推奨されます）を選択します。**診断**をクリックします。結果は**PING結果**に表示されます。

PCウェブ経由でネットワークペネトレーションサービスを設定

デバイスがLANに展開された後、ペネトレーションサービスを有効化することで、デバイスのリモート管理を実現できます。

手順

1. システムとメンテナンスに移動し、→ メンテナンス→デバイスデバッグ→ネットワークペネトレーションサービスを選択します。
2. 「ネットワークペネトレーションサービスを有効にする」をオンにします。
3. サーバーIPアドレスとサーバーポートを設定します。ユーザー名とパスワードを作成します。
4. オプション: ハートビートタイムアウトを設定できます。値の範囲は1から6000です。
5. オプション: ペネトレーションサービスの状態を確認できます。状態を更新するには「リフレッシュ」をクリックしてください。
6. 「保存」をクリックしてください。



ペネトレーションサービスは48時間後に自動的に無効化されます。

10.13.7 PC ウェブ経由でログを表示

デバイスログを検索して表示できます。

システムとメンテナンスに移動し、→メンテナンス、→ログを選択してください。

ログタイプの主要タイプと副次タイプを設定します。検索の開始時間と終了時間を設定し、[検索]をクリックします。

結果は以下に表示され、番号、時間、主要タイプ、副次タイプ、チャンネル番号、ローカル/リモートユーザー情報、リモートホストIPなどが含まれます。

10.13.8 PC Web 経由の高度な設定

顔パラメーター、手のひらパラメーターを設定し、バージョン情報を確認できます。システムとメンテナン

ス→メンテナンス→詳細設定へ移動します。

デバイスアクティベーションパスワードを入力し、Enterをクリックします。

顔パラメーター

カスタムアンチスプーフィング検出を有効にすると、アンチスプーフィング検出閾値 1:1 およびアンチスプーフィング検出閾値 1:N を設定できます。

顔認証用の顔ロックを有効にし、ロック時間を設定します。アンチスプーフィング検出の失敗回数制限に達すると、設定したロック時間中に顔がロックされます。

保存をクリックします。

パームプリントパラメーター

カスタムアンチスプーフィング検出を有効にすると、アンチスプーフィング検出閾値を設定できます。保存をクリックします。

バージョン情報

ここで異なるバージョン情報を確認できます。

10.13.9 セキュリティ管理

PCウェブにログインする際のセキュリティレベルを設定します。

システムとメンテナンスに移動し、→を選択し、→セキュリティ サービスをクリックします。

セキュリティモード

ログイン時とユーザー情報の確認時に高いセキュリティレベルを適用します。

互換性モード

古いユーザー認証方法と互換性があります。

保存をクリックします。

10.13.10 証明書管理

サーバー/クライアント証明書およびCA証明書を管理するのに役立ちます。



注意

この機能は、特定のデバイスモデルでのみサポートされています。

自己署名証明書を作成してインポートする

手順

1. システムとメンテナンスに移動し、→、**Safe**、→、**Certificate Management** の順に選択します。
2. 証明書ファイル領域で、ドロップダウンリストから**証明書タイプ**を選択します。
3. 「作成」をクリックします。
4. 証明書情報を入力します。
5. **OK**をクリックして証明書を保存し、インストールします。
作成された証明書は**証明書詳細**領域に表示されます。証明書は自動的に保存されます。
6. 証明書をダウンロードし、ローカルコンピュータの指定したファイルに保存します。
7. 要求ファイルを認証局に送信して署名を取得します。
8. 署名済みの証明書をインポートします。
 - 1) 「キーのインポート」領域で証明書タイプを選択し、ローカルから証明書を選択し、**[インポート]**をクリックします。
 - 2) 「通信証明書をインポート」領域で証明書タイプを選択し、ローカルから証明書を選択し、**[インポート]**をクリックします。

その他の承認済み証明書をインポート

既に承認済み証明書（デバイスで作成されていないもの）がある場合は、直接デバイスにインポートできます。

手順

1. システムとメンテナンスに移動し、→、**Safe**、→、**Certificate Management** の順に選択します。
2. 「インポートキー」と「インポート通信証明書」の領域で、証明書タイプを選択し、証明書をアップロードします。
3. インポートをクリックします。

CA証明書をインポート

開始前に

事前にCA証明書を準備してください。

手順

1. システムとメンテナンスに移動します。→ 安全→証明書管理。
2. 「CA証明書をインポート」領域でIDを作成します。



注意

入力する証明書IDは既存のものと同一にしてはいけません。

3. ローカルから証明書ファイルをアップロードします。
4. インポートをクリックします。

第11章 その他のプラットフォームの設定

デバイスは、iVMS-4200 クライアントソフトウェアまたは HikCentral アクセスコントロール 経由でも設定可能です。詳細については、各プラットフォームのユーザーマニュアルを参照してください。

iVMS-4200 クライアントソフトウェア

リンクをクリックまたはタップして、クライアントソフトウェアのユーザーマニュアルを表示します。

<http://enpinfodata.hikvision.com/analysisQR/showQR/ca930247>

HikCentral Access Control (HCAC)

リンクをクリックまたはタップして、HCACのユーザーマニュアルを表示します。

<http://enpinfodata.hikvision.com/analysisQR/showQR/f2f6cf42>

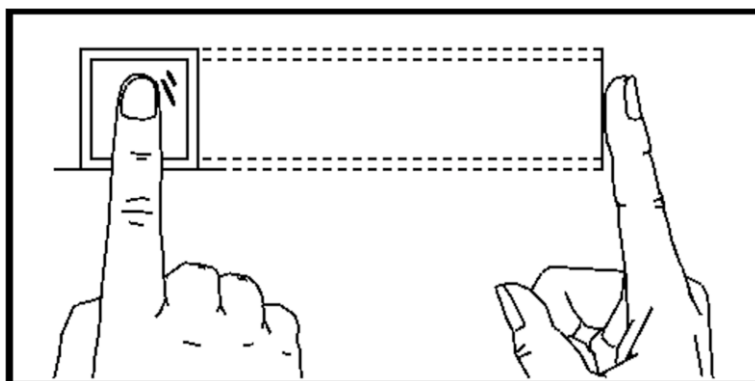
付録A. 指紋スキャン時のヒント

推奨される指

人差し指、中指、または薬指。

正しいスキャン方法

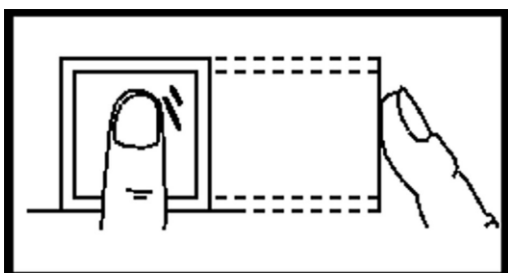
以下の図は、指をスキャンする正しい方法です:



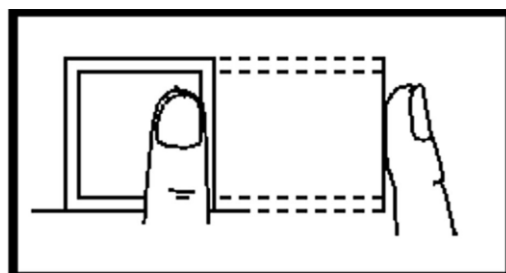
指をスキャナーに水平に押し当ててください。スキャンした指の中心がスキャナーの中心と一致するようにしてください。

不正なスキャン

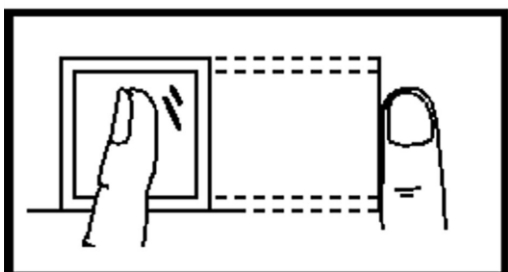
以下の指紋スキャン図は誤っています:



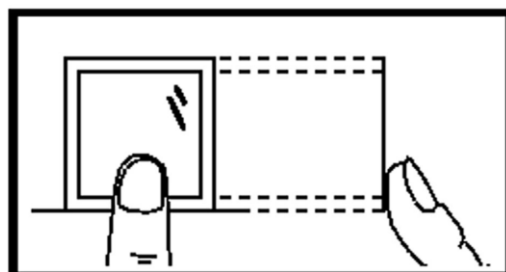
Vertical



Edge I



Side



Edge II

環境

スキャナーは直射日光、高温、湿気、雨を避けてください。乾燥している場合、スキャナーが指紋を正しく認識できない可能性があります。指に息を吹きかけてから再度スキャンしてください。

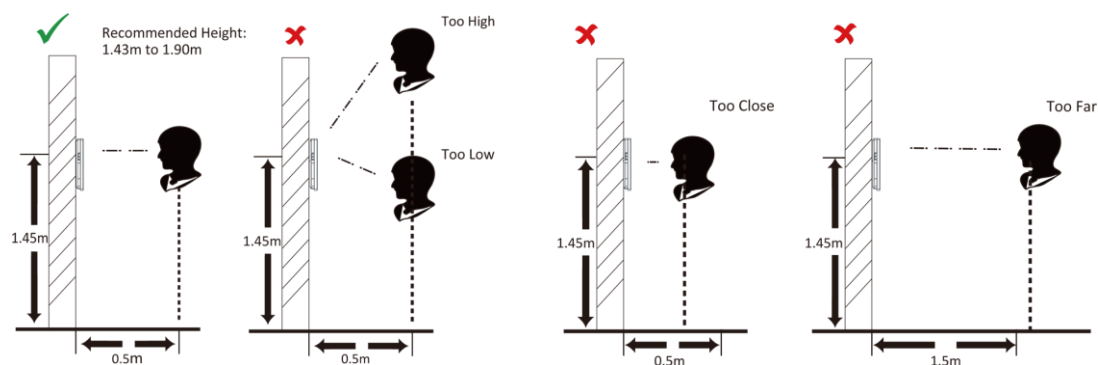
その他

指紋が浅い場合、または指紋の読み取りが難しい場合は、他の認証方法をご利用いただくことをおすすめします。スキャンする指に傷がある場合、スキャナーが認識しない可能性があります。別の指に変更して再度お試しください。

付録B. 顔写真の収集/比較時の注意点

顔写真の収集または比較時の位置は、以下の通りです：

位置（推奨距離：0.5 m）



表情

- 顔写真を撮影したり比較したりする際は、自然な表情を保ってください。下の写真のような表情を心がけてください。



- 帽子、サングラス、または顔認識機能に影響を与える可能性のある他のアクセサリは着用しないでください。
- 髪が目や耳などを覆わないようにし、濃いメイクは禁止です。

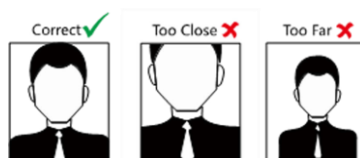
姿勢

顔の写真を収集または比較する際は、カメラに向かって顔を向けてください。これにより、高品質で正確な顔写真が得られます。



サイズ

顔の中心が収集ウィンドウの真ん中に来ていることを確認してください。



付録C. 設置環境のヒント

1. 光源の照度基準値



キャンドル：10ルクス

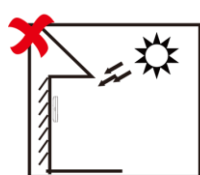


電球：100～850ルクス

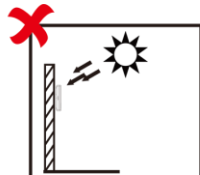


日光：1200ルクス以上

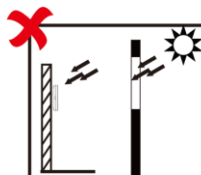
2. バックライト、直射日光、間接日光を避けてください



Backlight



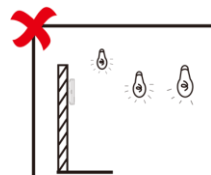
Direct Sunlight



Direct Sunlight
through Window

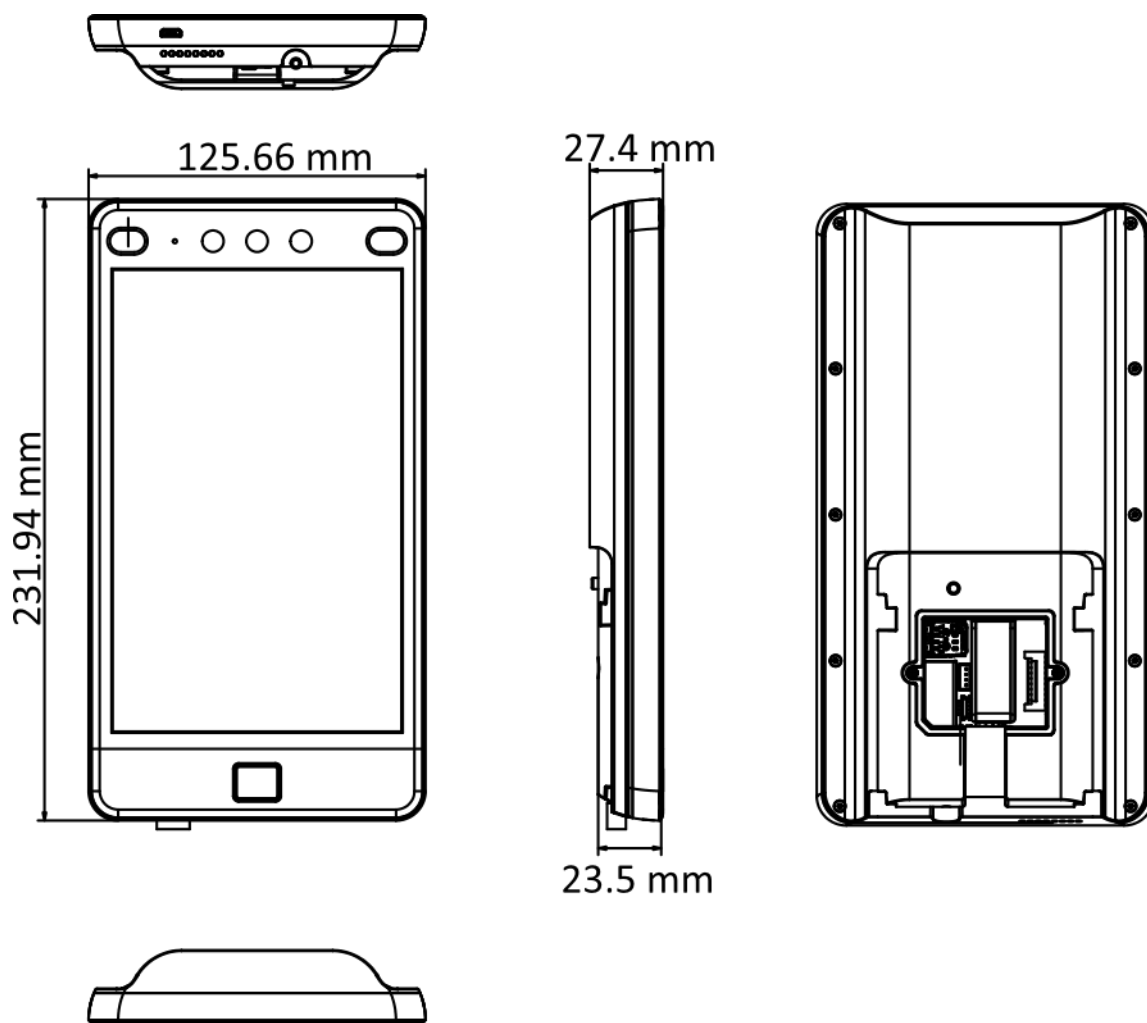


Indirect Light
through Window



Close to Light

付録D. 寸法



図D-1 寸法

