



ST-DW XK1T342 顔認証端末ユーザーマニュアル

法的情報


© 2013～2024 SeaTech Co., Ltd. All Rights Reserved.

本マニュアルについて

本マニュアルには、製品の使用および管理に関する説明が含まれています。画像、図表、その他の情報は説明のみを目的としており、ファームウェアの更新やその他の理由により、予告なく変更される場合があります。

最新のマニュアルはシーテクのウェブサイト (<https://sea-tech.info/>) でご確認ください。

商標

 商標およびロゴは、各国の法律に基づき保護されています。他の商標やロゴは、それぞれの所有者に帰属します。

免責事項

適用法で許可される最大限の範囲で、このマニュアルおよび製品記載されているハードウェア、ソフトウェア、ファームウェアは、「現状のまま」および「すべての障害とエラーを含む」状態で提供されます。シーテクは、明示的または黙示的を問わず、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保証を行いません。お客様による製品の使用は、お客様ご自身の責任で行ってください。いかなる場合も、シーテクは、特別損害、結果的損害、偶発的損害、または間接損害について、お客様に対して責任を負いません。とりわけ、事業利益の損失に対する損害賠償を含みます。

データの中断、損失、システムの破損、またはドキュメントの損失、契約違反、不法行為(過失を含む)、製造物責任、またはその他に基づくかどうにかかわらず、製品の使用に関連して、シーテクがそのような損害または損失の可能性について助言された。

お客様は、インターネットの性質が固有のセキュリティを提供することを認めます。リスク、およびシーテクは異常な操作について一切の責任を負わないものとします。

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プライバシーの漏洩またはその他の損害。しかし、シーテクはタイムリーに提供します。必要に応じてテクニカルサポート。

お客様は、適用されるすべての法律に準拠して本製品を使用することに同意し、使用が適用法に準拠していることを確認する責任を単独で負うものとします。

特に、第三者の権利を侵害しない方法でこの製品を使用することについて、以下の権利を含むがこれに限定されない責任を負うものとします。

パブリシティ権、知的財産権、またはデータ保護およびその他のプライバシー権。この製品を、以下を含む禁止されている最終用途に使用しないでください。

大量破壊兵器の開発または製造、開発または化学兵器または生物兵器の製造、関連する文脈でのあらゆる活動核爆発性または安全でない核燃料サイクル、または人権侵害を支援するもの。

このマニュアルと適用法との間に矛盾がある場合は、後者が優先されます。

データ保護




デバイスの使用中、個人データは収集、保存、処理されます。データを保護するために、シーテックデバイスの開発には、設計原則によるプライバシーが組み込まれています。たとえば、顔認証機能を備えたデバイスの場合、生体認証データは暗号化方式でデバイスに保存されます。

データ管理者として、適用されるデータ保護法および規制に従ってデータを収集、保存、処理、および転送することをお勧めします。

セキュリティ管理 合理的な管理上および物理的なセキュリティ管理を実施するなど、個人データを保護するため、セキュリティ管理の有効性について定期的なレビューと評価を実施します。

シンボルの表記規則

この文書に記載されている記号の定義は以下の通りです。

記号	説明
 危険	無視すると死亡または重傷を引き起こす可能性があります。
 注意	無視すると機器の損傷やデータ損失の原因となる可能性があります。
 メモ	重要なポイントの補足情報を提供します。

規制情報

FCC情報

コンプライアンスの責任者によって明示的に承認されていない変更または修正を行うと、機器を操作するユーザーの権限が無効になる可能性があることに注意してください。

FCCコンプライアンス:この機器はテスト済みであり、FCC規則のパート15に準拠したクラスBデジタルデバイスの制限に準拠していることが確認されています。これらの制限は、次のものを提供するように設計されています

住宅地での有害な干渉に対する合理的な保護。この機器は無線周波数エネルギーを生成、使用、および放射する可能性があり、指示に従って設置および使用しない場合、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、特定のインストールで干渉が発生しないという保証はありません。この機器がそうする場合はラジオやテレビの受信に有害な干渉を引き起こすこと、これは回すことで判断できます。

この機器では、ユーザーは、次の手段の1つ以上によって干渉を修正しようとするをお勧めします。

- 受信アンテナの向きを変えるか、位置を変えます。
- 機器と受信機との距離を広げます。
- 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ます。
- 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。

この装置は、ラジエーターと身体との間に20cm以上の距離を置いて設置および操作する必要があります。

FCC条件

このデバイスは、FCC規則のパート15に準拠しています。操作には、次の2条件が適用されます。

- 1.このデバイスは、有害な干渉を引き起こさない可能性があります。
- 2.このデバイスは、望ましくない動作を引き起こす可能性のある干渉を含め、受信した干渉を受け入れる必要があります。

EU適合宣言



この製品および(該当する場合は)付属のアクセサリも「CE」マークが付いており、記載されている適用可能な欧州統一規格に準拠しています。



EMC指令2014/30 / EU、RE指令2014/53 / EU、RoHS指令2011/65 / EUに基づく2012/19/EU(WEEE指令):この記号が付いている製品は、欧州連合では未分別都市ごみとして処分することはできません。適切なリサイクルのために、同等の新しい機器を購入したら、この製品を最寄りのサプライヤーに返送するか、指定された場所に廃棄してください。詳細については、以下を参照してください。

www.recyclethis.info



2006/66/EC(電池指令):本製品には、欧州連合では未分別都市ごみとして処分されています。特定のバッテリー情報については、製品のマニュアルを参照してください。バッテリーにはこのマークが付いています。記号には、カドミウム (Cd)、鉛 (Pb)、または水銀 (Hg) を示すレタリングが含まれる場合があります。適切にリサイクルするには、バッテリーをサプライヤーまたは指定された場所に返送してください。詳細はwww.recyclethis.infoをご覧ください。

このデバイスは、カナダ産業省のライセンス免除RSS標準に準拠しています。操作には、次の2条件が適用されます。

(1)このデバイスは干渉を引き起こさないこと。

(2)このデバイスは、デバイスの望ましくない動作を引き起こす可能性のある干渉を含む、あらゆる干渉を受け入れる必要があります。

この装置は、ライセンス免除無線装置に適用されるカナダ産業省のRSSに準拠しています。この操作は、次の2条件で許可されます。

(1)デバイスは干渉を引き起こさないです。

(2)装置のユーザーは、干渉が装置の動作に干渉する可能性がある場合でも、発生した無線周波数干渉を受け入れるものとします。

この装置は、FCC / IC RSS-102放射線被曝制限に準拠しています。

制御されていない環境。この装置は、ラジエーターと身体の間に20cm以上の距離を置いて設置および操作する必要があります。

この装置は、別の環境に記載されているFCC/RSS-102の放射線被ばく線量制限に準拠しています。この装置は、ヒーターと身体との間に20°C以上の距離を置いて設置および操作する必要があります。

安全指導

これらの手順は、ユーザーが危険や財産の損失を避けるために製品を正しく使用できるようにすることを目的としています。

予防措置は、危険と注意に分けられます。

危険: 無視すると死亡または重傷を引き起こす可能性があります。

注意: 無視すると怪我や機器の損傷を引き起こす可能性があります。

⚠	⚠
危険: 重傷や死亡を防ぐために、これらの安全対策に従ってください。	注意: 潜在的な損傷や物的損傷を防ぐために、これらの注意事項に従ってください。

⚠ 危険:

- 製品の使用にあたっては、国や地域の電気安全規制を厳守する必要があります。
- アダプターの過負荷により過熱や火災の危険が発生する可能性があるため、複数のデバイスを1つの電源アダプターに接続しないでください。
- 機器から煙、臭い、騒音が発生した場合は、すぐに電源を切り、電源ケーブルを抜いてから、サービスセンターにご連絡ください。
- コンセントは機器の近くに設置し、簡単にアクセスできるようにしてください。
 1. 電池を摂取しないでください。化学火傷の危険
 2. この製品には、コイン/ボタン電池が含まれています。コイン電池やボタン電池を飲み込むと、わずか2時間で内部に重度の火傷を負い、死に至る可能性があります。
 3. 新品および使用済みのバッテリーを子供から遠ざけてください。
 4. バッテリーコンパートメントがしっかりと閉まらない場合は、製品の使用を中止し、子供から遠ざけてください。
 5. 電池を飲み込んだり、体の中に入れられた可能性があると思われる場合は、すぐに医師の診察を受けてください。
 6. 注意: バッテリーを間違ったタイプに交換すると、爆発の危険があります。
 7. バッテリーを間違ったタイプに不適切に交換すると、セーフガードが無効になる可能性があります(例: ample、一部のリチウム電池タイプの場合)。
 8. バッテリーを火や高温のオーブンに廃棄したり、バッテリーを機械的に押しつぶしたり切断したりしないでください。
 9. バッテリーを周囲の非常に高温の環境に放置しないでください。爆発や可燃性の液体またはガスの漏れを引き起こす可能性があります。
 10. バッテリーを極端に低い空気圧にさらさないでください。爆発や可燃性の液体やガスの漏れ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、指示に従って廃棄してください。

⚠ 注意:

- デバイスを落としたり、物理的な衝撃を与えたり、高いところにさらしたりしないでください。電磁気放射。振動面や衝撃を受ける場所に機器を設置しないでください(無知は機器の損傷を引き起こす可能性があります)。
- 本機器を極端に高温(詳細な動作温度については仕様を参照)、低温、ほこりの多い場所、または湿気の多い場所に設置しないでください。また、強い電磁放射を受ける場所にさらさないでください。
- 本機器を直射日光、低換気、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(無知は火災の危険を引き起こす可能性があります)。
- 屋内用のデバイスカバーは、雨や湿気から守ってください。
- 本機器を直射日光、低換気、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(無知は火災の危険を引き起こす可能性があります)。
- デバイスカバーの内側と外側の表面を掃除するときは、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、なりすまし防止環境に完全に適用できるわけではありません。より高いセキュリティレベルが必要な場合は、複数の認証モードを使用してください。
- 本機器のシリアルポートはデバッグ専用です。
- このマニュアルの指示に従って機器を設置してください。けがを防ぐために、本機器は設置手順に従い、床や壁にしっかりと固定する必要があります。
- バッテリーの不適切な使用や交換は、爆発の危険をもたらす可能性があります。同じタイプまたは同等のタイプのみと交換してください。使用済みのバッテリーは、バッテリーの製造元の指示に従って廃棄してください。
- このブラケットは、装備されたデバイスでのみ使用することを目的としています。他の機器と一緒に使用すると、不安定になり、怪我をする可能性があります。
- 本機器は装備金具のみ使用してください。他のもの(カート、スタンド、キャリア)と一緒に使用すると、不安定になり、怪我をする可能性があります。

利用可能なモデル

商品名	モデル	ワイヤレス
顔認証端末	ST-DWXXK1T342	周波数、Wi-Fi(2.4 GHz)を表示する 13.56 MHzカード

ユーザーの指示に従っている電源のみを使用してください。

モデル	生産者	標準
ADS-12FG-12N 12012EPG	Shenzhen Honor Electronic Co., Ltd	PG

内容

第1章 概要	1
1.1 概要.....	1
1.2 特徴.....	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 ギャングボックスでインストール.....	5
3.3 表面実装.....	8
3.4 ブラケットで取り付け.....	14
3.4.1 ブラケットで取り付ける前の準備.....	14
3.4.2 マウントブラケット.....	15
3.5 シリンダーブラケット付きマウント.....	16
3.5.1 ブラケットで取り付ける前の準備.....	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	20
4.1 ターミナルの説明.....	20
4.2 通常のデバイスを配線する.....	21
4.3 ワイヤセキアドアコントロールユニット.....	22
4.4 ワイヤファイアモジュール.....	23
4.4.1 電源投入時にドアが開いている配線図.....	23
4.4.2 電源投入時にロックされるドアの配線図.....	25
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ブ化する.....	27
5.2 経由でアクティブ化する Web ブラウザ.....	29
5.3 SADPによる有効化.....	30
5.4 iVMS-4200クライアントソフトウェアを介したデバイスのアクティブ化.....	31

第6章クイック操作	33
6.1 言語の選択	33
6.2 アプリモードを設定する	35
6.3 ネットワークパラメータの設定	36
6.4 プラットフォームへのアクセス	38
6.5 モバイルクライアントへのリンク	40
6.6 プライバシー設定	41
6.7 管理者の設定	43
第7章 基本操作	46
7.1 ログイン	46
7.1.1 管理者によるログイン	46
7.1.2 アクティベーションパスワードによるログイン	49
7.2 通信設定	50
7.2.1 有線ネットワークパラメータの設定	51
7.2.2 Wi-Fiパラメータを設定する	53
7.2.3 RS-485パラメータの設定	55
7.2.4 ウィーガンドパラメータの設定	57
7.2.5 ISUPパラメータの設定	59
7.2.6 プラットフォームアクセス	61
7.3 ユーザー管理	62
7.3.1 管理者の追加	62
7.3.2 顔写真を追加	64
7.3.3 カードを追加	67
7.3.5 PINコードの表示	68
7.3.6 認証モードの設定	69
7.3.7 ユーザーの検索と編集	69
7.4 データ管理	70

7.4.1 データの削除	70
7.4.2 データのインポート	70
7.4.3 データのエクスポート	71
7.5 ID認証	71
7.5.1 単一の資格情報で認証する	71
7.5.2 複数認証情報による認証	72
7.6 基本的な設定	72
7.7 生体認証パラメータの設定	74
7.8 アクセス制御パラメータの設定	77
7.9 時間と出席状況の設定	79
7.9.1 デバイスを介して出席モードを無効にする	80
7.9.2 デバイスによる手動出席の設定	81
7.9.3 デバイスによる自動出席の設定	83
7.9.4 デバイスによる手動および自動出席の設定	85
7.10 設定	87
7.11 システムメンテナンス	89
第8章モバイルブラウザを使用したデバイスの構成	92
8.1 ログイン	92
8.2 検索イベント	92
8.3 ユーザー管理	92
8.4 設定	94
8.4.1 ビュー デバイス情報	94
8.4.2 時間設定	94
8.4.3 オープンソースソフトウェアライセンスの表示	95
8.4.4 ネットワーク設定	95
8.4.5 一般的な設定	98
8.4.6 面パラメータの設定	104
8.4.7 ビデオインターホンの設定	108

8.4.8 アクセス制御の設定	110
第9章 Webブラウザによる操作	116
9.1 ログイン	116
9.2 ライブビュー	116
9.3 人の管理	118
9.4 検索イベント	119
9.5 設定	119
9.5.1 ローカルパラメータの設定	119
9.5.2 ビュー デバイス情報	120
9.5.3 設定時間	120
9.5.4 DSTの設定	121
9.5.5 オープンソースソフトウェアライセンスの表示	122
9.5.6 アップグレードとメンテナンス	122
9.5.7 ログクエリ	123
9.5.8 セキュリティモードの設定	123
9.5.9 証明書管理	124
9.5.10 管理者パスワードの変更	125
9.5.11 デバイスの武装/武装解除情報の表示	126
9.5.12 ネットワーク設定	126
9.5.13 ビデオとオーディオのパラメータを設定する	129
9.5.14 オーディオコンテンツのカスタマイズ	131
9.5.15 イメージパラメータの設定	132
9.5.16 サプリメントライトの明るさを設定する	133
9.5.17 時間と出席のセッティング	133
9.5.18 一般的な設定	136
9.5.19 ビデオインターホンの設定	142
9.5.20 アクセス制御の設定	144
9.5.21 生体認証パラメータの設定	147

9.5.22 予告公開の設定	151
第10章 クライアントソフトウェアの構成	154
10.1 クライアントソフトウェアの設定フロー	154
10.2 デバイス管理	154
10.2.1 デバイスの追加	155
10.2.2 デバイスパスワードのリセット	157
10.2.3 追加されたデバイスの管理	158
10.3 グループ管理	159
10.3.1 グループの追加	159
10.3.2 グループへのリソースのインポート	159
10.4 人の管理	160
10.4.1 組織の追加	160
10.4.2 個人識別情報のインポートとエクスポート	160
10.4.3 アクセス制御デバイスからの個人情報の取得	163
10.4.4 バッチで人にカードを発行する	163
10.4.5 通知表の紛失	164
10.4.6 カード発行パラメータの設定	164
10.5 スケジュールとテンプレートの設定	165
10.5.1 休日を追加	166
10.5.2 テンプレートの追加	166
10.6 アクセス権限を人に割り当てるためのアクセスグループの設定	168
10.7 高度な機能の設定	170
10.7.1 デバイスパラメータの設定	170
10.7.2 デバイスパラメータの設定	176
10.8 ドアコントロール	179
10.8.1 コントロールドアのステータス	179
10.8.2 リアルタイムアクセスレコードの確認	180

付録A.顔写真を収集する/比較する際のヒント	184
付録B.設置環境のヒント	186
付録C.寸法	187
付録D.通信マトリックスとデバイスコマンド	188

第1章 概要

1.1 概要

顔認証端末は、顔認証用のアクセス制御デバイス的一种であり、主にアイオジスティックセンター、空港、大学キャンパス、アラームセンター、ホテル、住居などのセキュリティアクセス制御システムに適用されます。

1.2 特徴

- 4.3インチLCDタッチスクリーン、272×480の画面解像度、最大顔フレームのリアルタイム検出と表示します。
- 2 MP 広角デュアルレンズ
- 複数認証モードをサポートします:顔認証、カード、PINコード、複数組み合わせ認証します。
- アクセス制御の期間制御(プランテンプレート)をサポートし、オンデマンドでドアを開けることを許可します。
- プラットフォームを介したネットワーク操作と人事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ており、デバイスの比較結果とリンケージ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ているときに生成されたイベントが再度アップロードされます。
- NTP、手動、および自動の時間計算をサポートします。
- デバイス間のビデオインターホンをサポートします。
- リモートビデオプレビューとRTSPプロトコル経由のビデオコードストリームの出力をサポートします。
- ウォッチドッグガードメカニズム、タンパー設計をサポートして、デバイスが正常に動作することを確認します。
- 着用モードのリマインダーを含むマスク検出モードをサポートし、マスクモードを着用する必要があります。
- IP65をサポートします。

第2章 外観

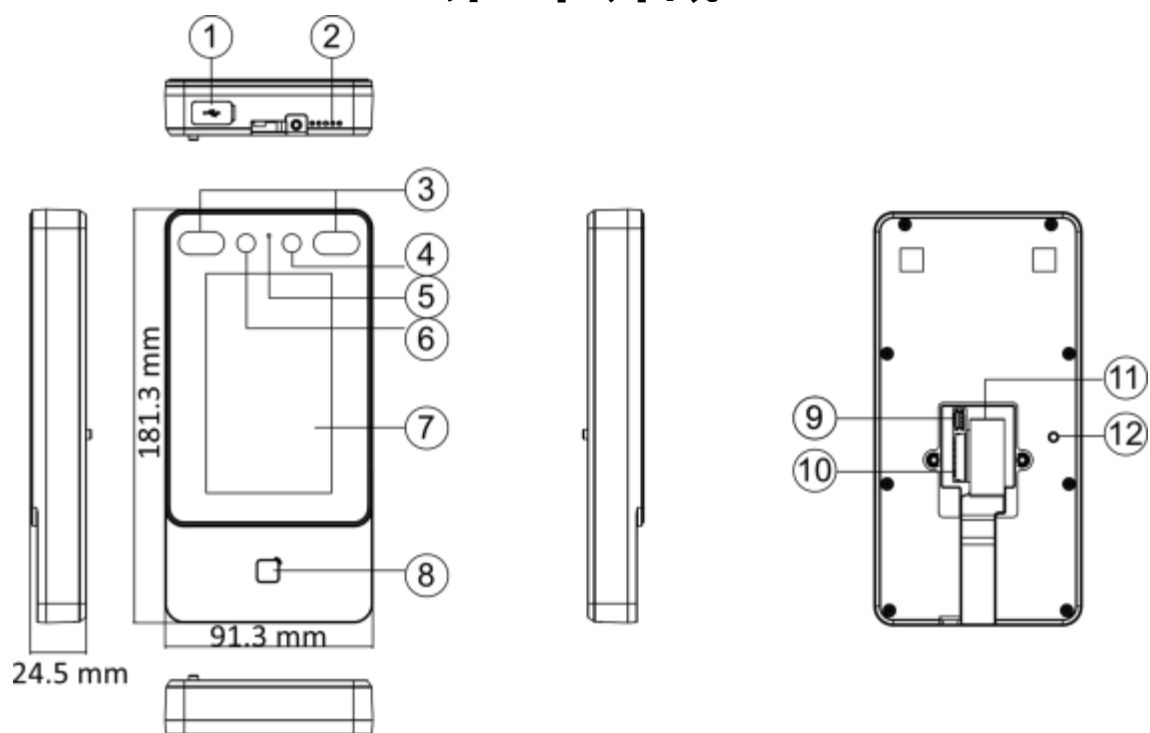


図 2-1 外観の説明

No.	名前
1	USB接続 インター顔
2	スピーカー
3	IRライト
4	カメラ
5	マイク
6	カメラ

No.	名前
7	タッチスクリーン
8	カード提示エリア
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	改ざん

第3章 インスタレーション

3.1 インフラ環境

- 逆光、直射日光、間接光を避けてください。
- 認識を向上させるためには、インストール環境内または近くに光源が必要です。
- 壁やその他の場所の最小支持重量は、デバイスの重量の3倍重くする必要があります。
- 強力な選択物(ガラスのドア/壁、ステンレス鋼の物体、アクリルおよびその他の光沢のあるプラスチック、ラッカー、セラミックタイルなど)のビューのフィールドから1m以内になります。
- デバイスの再選択は避けてください。
- 顔認証距離は30cm以上でなければなりません。
- カメラを清潔に保ちます。



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 ギャングボックスでインストール

手順

1. ギャングボックスが壁に取り付けられていることを確認します。



ギャングボックスは別途購入する必要があります。

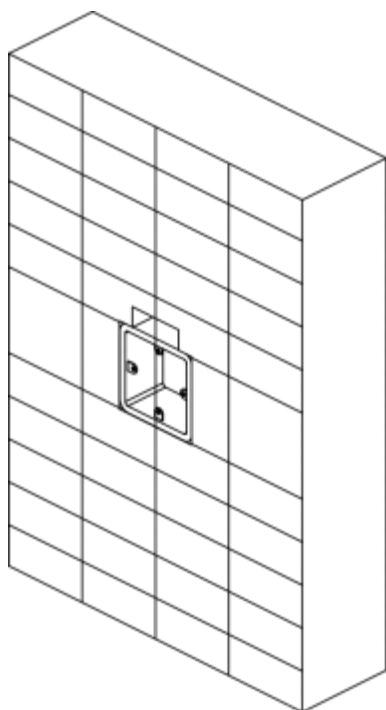


図3-1 ギャングボックスの取り付け

2. 付属の2本のネジ(SC-KA4X22)で取り付けプレートをギャングボックスに固定します。

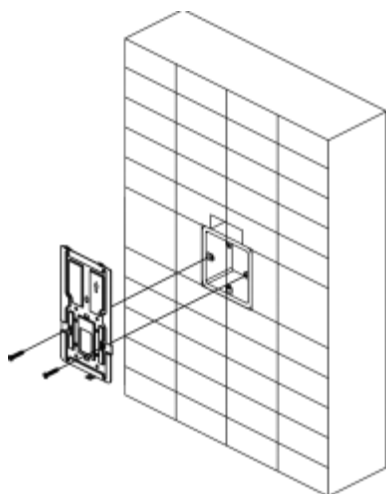


図3-2 取り付けプレートの取り付け

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

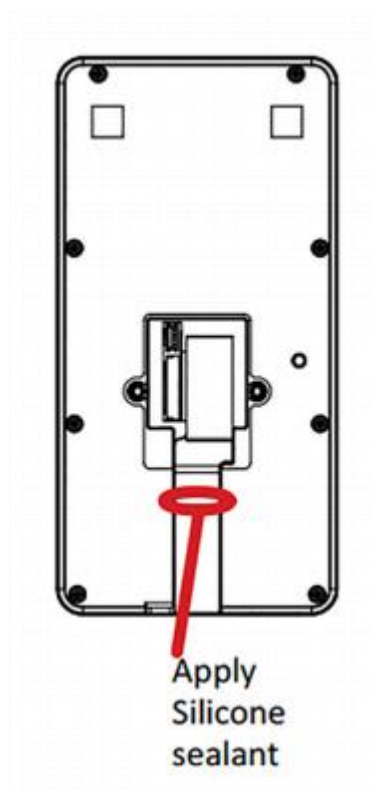


図3-3 シリコンシーラントの塗布

4. デバイスを取り付けプレートに合わせ、付属のネジ1本(SC-KM3X6-T10-SUSS)でデバイスを取り付けプレートに固定します。

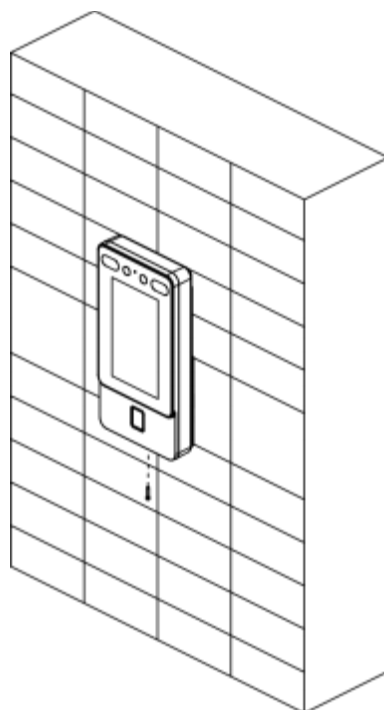


図 3-4 セキュア デバイス

3.3 表面実装

手順

1. 取り付けテンプレートのデータムラインに従って、取り付けテンプレートを地面より1.45メートル高い壁またはその他の表面に貼り付けます。

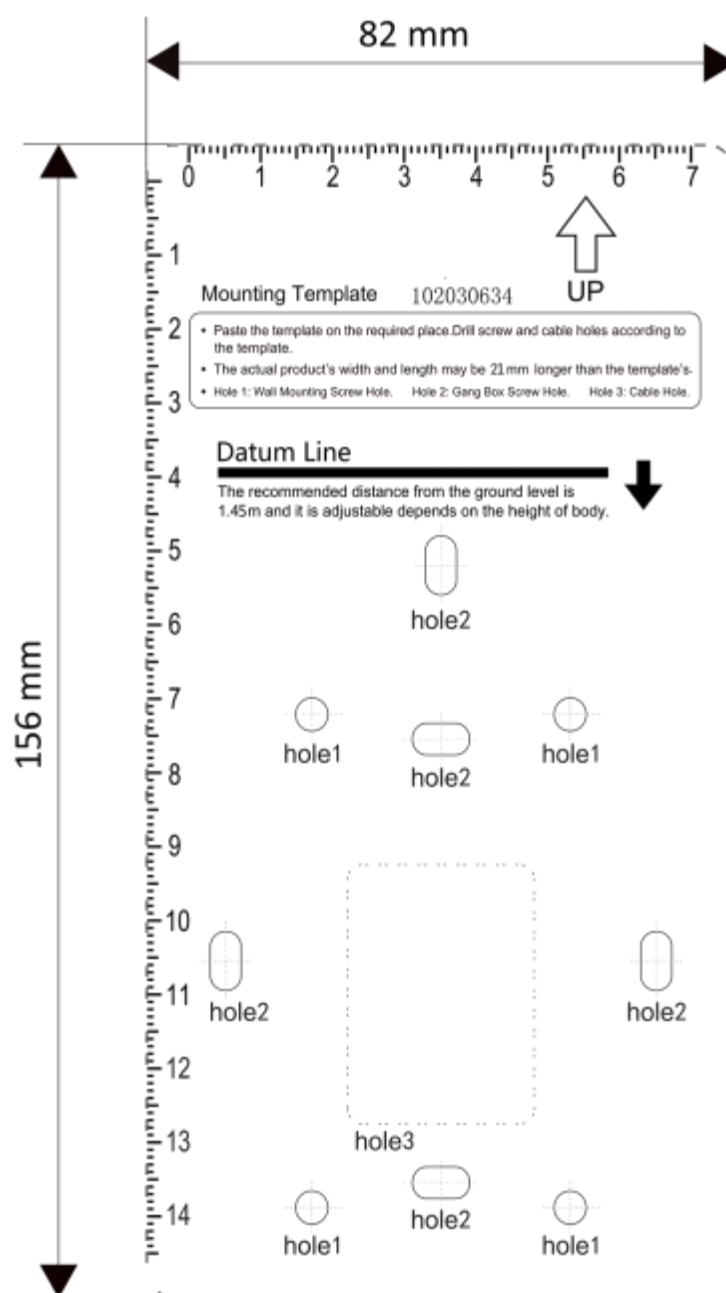


図 3-5 取り付けテンプレート

2. 取り付けテンプレートの穴1に従って、壁またはその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. 穴を取り付けプレートに合わせ、付属の2本のネジ(KA4×22-SUS)で取り付けプレートを壁に固定します。

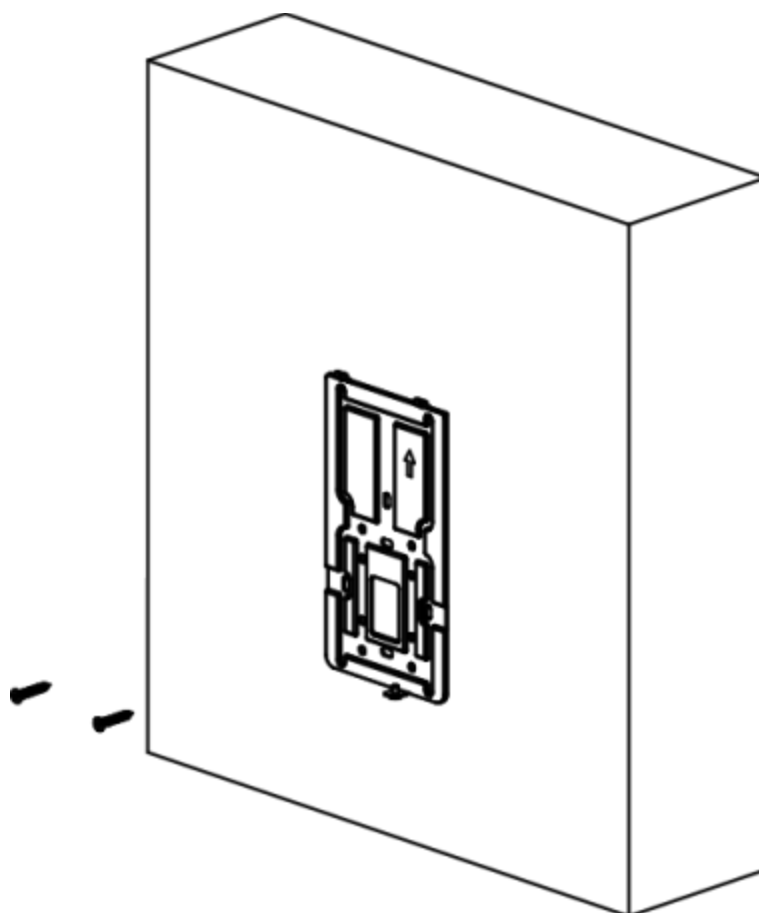



図 3-6 取り付けプレートの取り付け

5. ケーブルを取り付けプレートのケーブル穴に通し、対応する周辺機器ケーブルに接続します。

 **メモ**

デバイスが屋外に設置されている場合は、水が入らないように、配線出口にシリコンシーラントを塗布する必要があります。

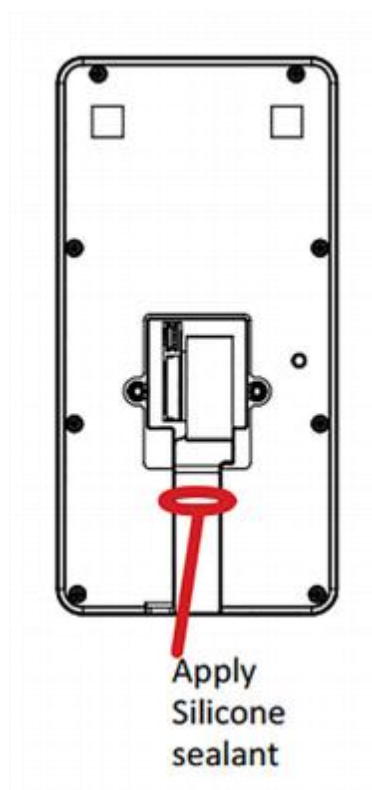


図3-7 シリコンシーラントを塗布する

6. デバイスを取り付けプレートに合わせ、デバイスを取り付けプレートに掛けます。

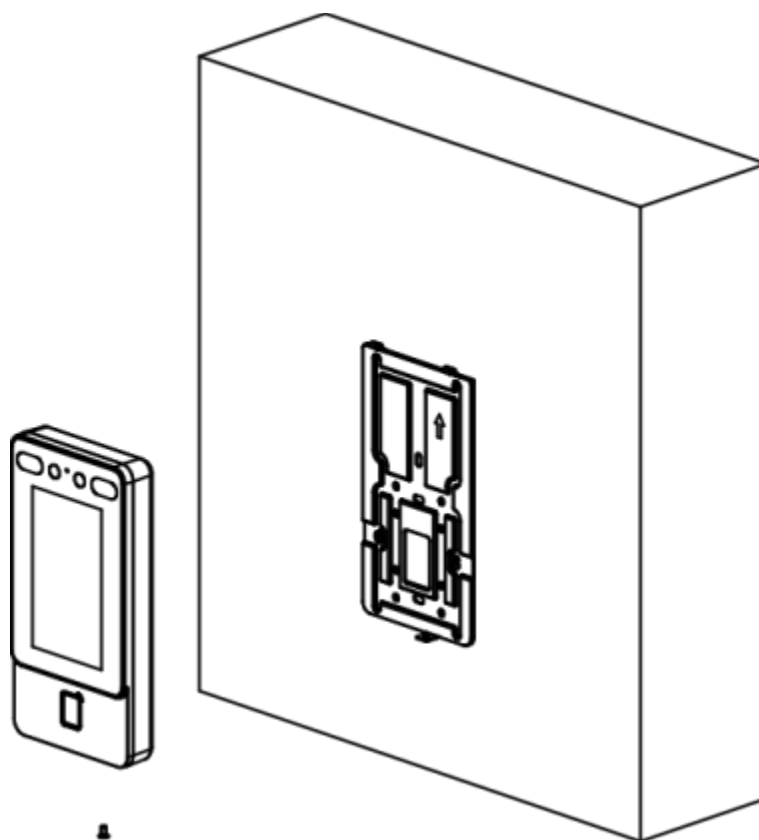


図 3-8 ハング デバイス

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

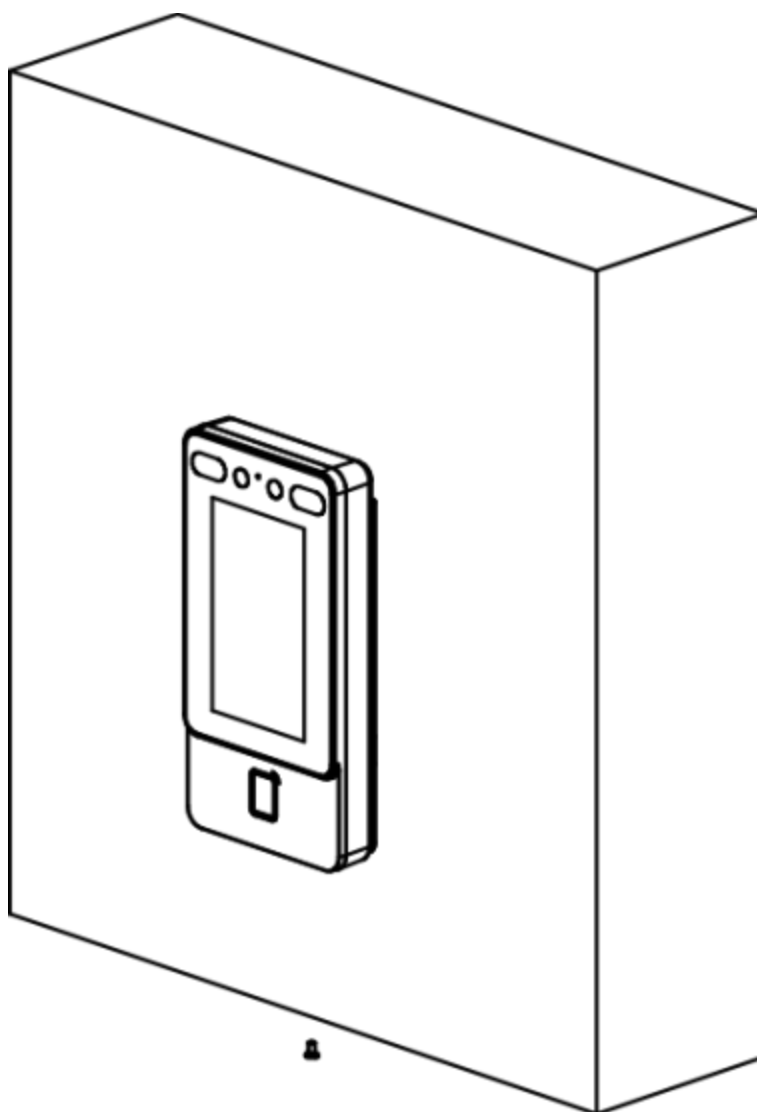


図 3-9 セキュア デバイス

 メモ

- 推奨される高さは1.45メートルで、必要に応じて高さを設定できます。
 - 付属の取り付けプレートを使用することをお勧めします。
-
8. 設置後、デバイスを適切に使用(屋外使用)するために、保護フィルム(付属のモデルの一部)を画面に貼り付けます。

3.4 ブラケットで取り付け

3.4.1 ブラケットで取り付ける前の準備

手順

1. 改札機の表面に穴をあけて、以下に示す図に従って穴を開けます。そして防水ナットを取付けて下さい。



リベットを押してからはんだ付けし、水の侵入を防ぎます。

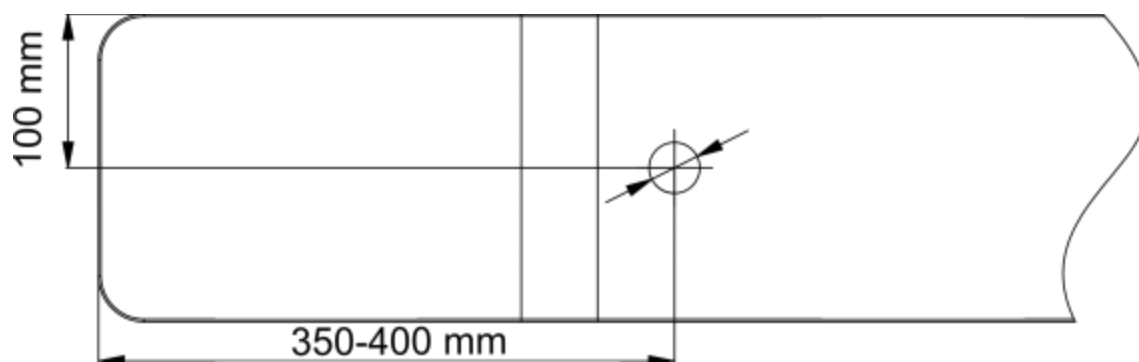


図3-10 改札機のドリル穴

2. インストール角度がターンスティエの本体に対して垂直に180°である必要がある場合は、次の操作が必要です。
 - 1) 下図の3本のネジを外します。



図 3-11 ネジの取り方

- 2) 固定部品を180°回転させ、3本のネジを取り付け直します。

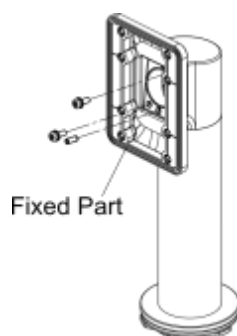


図3-12 固定部品の回転

3.4.2 マウントブラケット

手順

1. ベースを改札機に取り付けます。
 - 1)改札機の穴を合わせ、ベースを改札機に置きます。
 - 2)ベースを取得した場所に回転させ、デバイスが正しい方向を向くことを確認します。
 - 3)ベースをレンチで固定します。

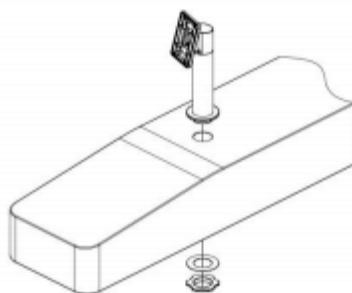


図3-13 インストールベース

メモ

改札機の前面と背面にシリコンパッドを取り付けます。

2. 付属のネジ4本(SC-K1M4×6-SUS)で取り付けテンプレートをブラケットに取り付けます。

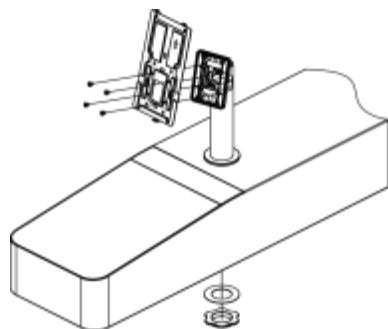


図 3-14 セキュアマウントテンプレート

3. ケーブルをターンスティのケーブル穴に通し、1本のSC-KM3×6-T10-SUSネジでデバイスを取り付けプレートに固定します。

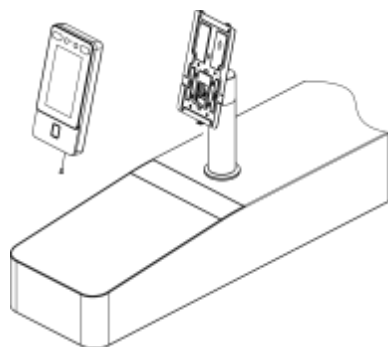


図 3-15 デバイスの修正

4. インスタレーション後、デバイスを適切に使用(屋外での使用)するために、保護(付属モデルの一部)を画面に貼り付けます。

3.5 シリンダーブラケット付きマウント

3.5.1 ブラケットで取り付ける前の準備

改札機に穴が開けられていることを確認してください。そうでない場合は、以下の手順に従って穴を開けます。

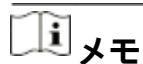
手順

1. 長いナットによって固定される4本のねじ(M3かM4)を使用して、改札機の内面に補強板を取付けて下さい。



改札機と端末の間の間隔は10 mm以下でなければなりません。

2. 改札機の内面に下記の図に従って穴をあけて下さい。そして防水ナットを取付けて下さい。



メモ

リベットを押してからはんだ付けし、水の侵入を防ぎます。

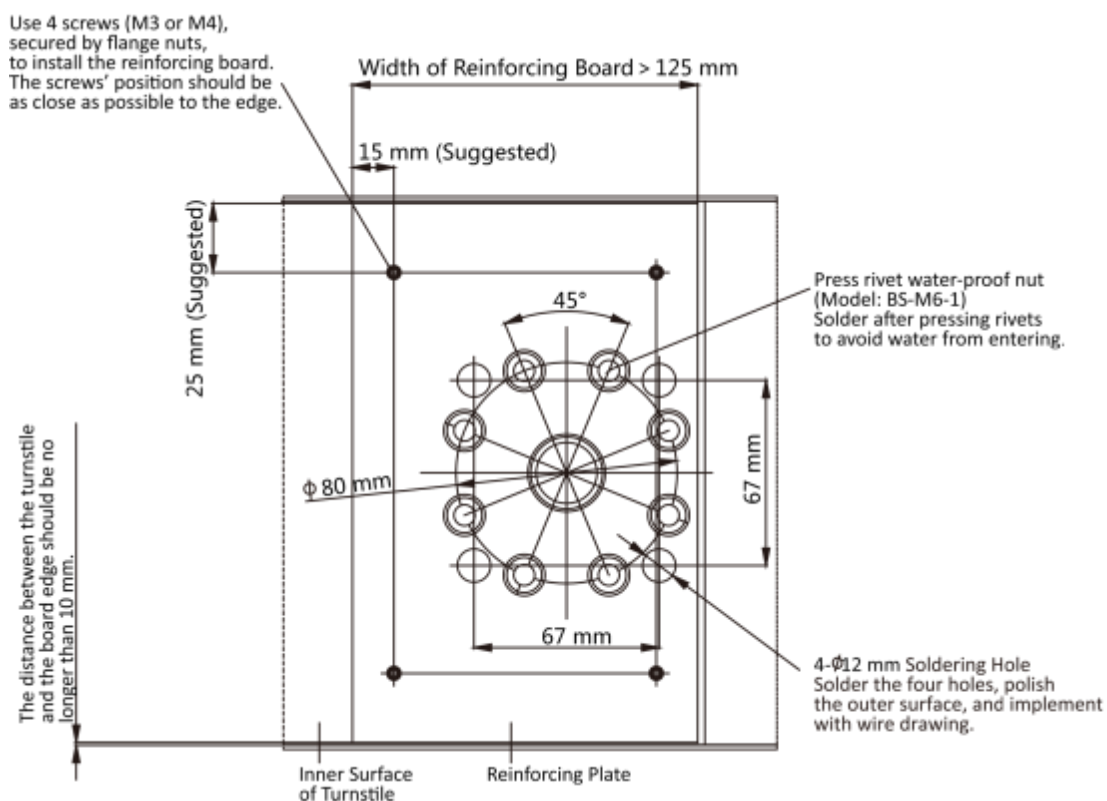


図3-16 改札機のドリル穴

3. 他の4つの穴をはんだ付けし、表面を研磨し、伸線を実装します。
4. 改札機の内部表面のはんだ円形の管は水が入ることを避けます。

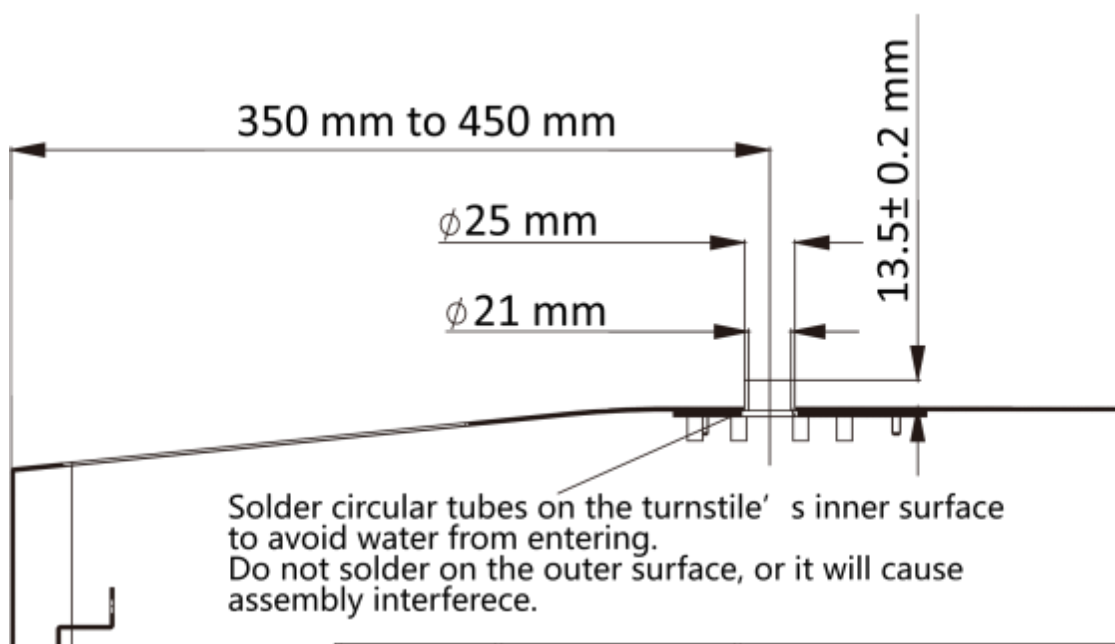


図 3-17 はんだチューブ

3.5.2 シリンダーブラケットの取り付け

手順

1. ベースを改札機に取り付けます。
 - 1)改札機の穴を合わせ、ベースを改札機に置きます。
 - 2)ベースを取得した場所に回転させ、デバイスが正しい方向を向くことを確認します。
 - 3)ベースを4本のSC-OM6×12-H-SUSネジで固定します。

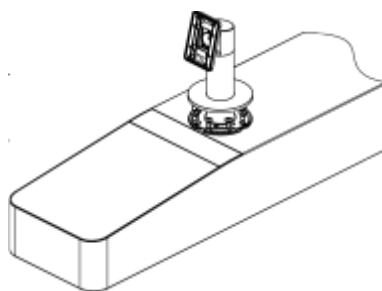


図3-18 インストールベース

2. 取り付けプレートを4本のSC-K1M4×6-SUSネジでブラケットに固定します。

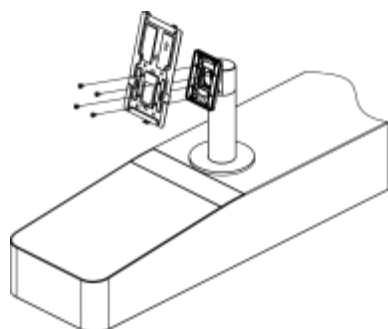


図 3-19 固定取り付けプレート

3. ターンステイエのケーブル穴にケーブルを通します。
4. 顔認証端子をSC-KM3×6-H2-SUSネジ1本で取り付けプレートに固定します。

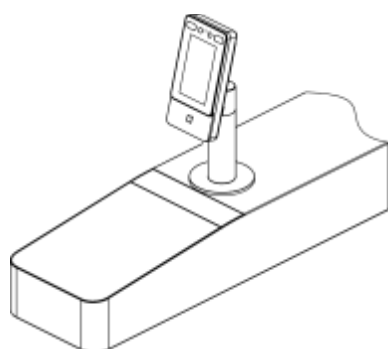


図 3-20 固定取り付けプレート

5. インスタレーション後、デバイスを適切に使用(屋外での使用)するために、保護(付属のモデルの一部)を画面に貼り付けます。

第4章 配線

RS-485端子とRS-485カードリーダーを接続し、NC/NOとCOMを接続できます。

ドアロック付きの端子、SENおよびGND端子をドア接点、BTN / GND端子を出口ボタン、ウィーガンド端子をアクセスコントローラーに接続します。

ウィーガンド端子をアクセスコントローラーに接続すると、顔認証端末は認証情報をアクセスコントローラーに送信し、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できます。



メモ

- ケーブルサイズが18AWGの場合は、12V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20m以下である必要があります。
- ケーブルサイズが15AWGの場合は、12V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30m以下である必要があります。
- ケーブルサイズが12AWGの場合は、12V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40m以下である必要があります。
- 外部カードリーダー、ドアロック、出口ボタン、およびドアマグネティックには個別の電源が必要です。

4.1 ターミナルの説明

端子には、電源入力、RS-485、ウィーガンド出力、ドアロックが含まれています。端末の説明は次のとおりです。

表 4-1 端末の説明

群	No.	機能	色	名前	詳細
グループA	A1	電源入力	赤	+12V	12V DC電源
	A2		黒	GND	地面
グループB	B1	RS-485	黄色	485+	RS-485配線
	B2		青	485-	
	B3		黒	GND	地面
グループC	C1	ウィーガンド	緑	W0	ウィーガンド配線0

群	No.	機能	色	名前	詳細
	C2		白	W1	ウィーガンド配線1
	C3		黒	GND	地面
グループD	D1	ドアロック	ホワイト/パープル	NC	ロック配線(NC)
	D2		ホワイト/黄色	COM	コモン
	D3		ホワイト/レッド	NO	ロック配線(NO)
	D4		黄色/グリーン	センサー	ドアコンタクト
	D5		黒	GND	地面
	D6		黄色/グレー	ボタン	出口ドアの配線

4.2 通常のデバイスを配線する

端末を通常の周辺機器と接続できます。

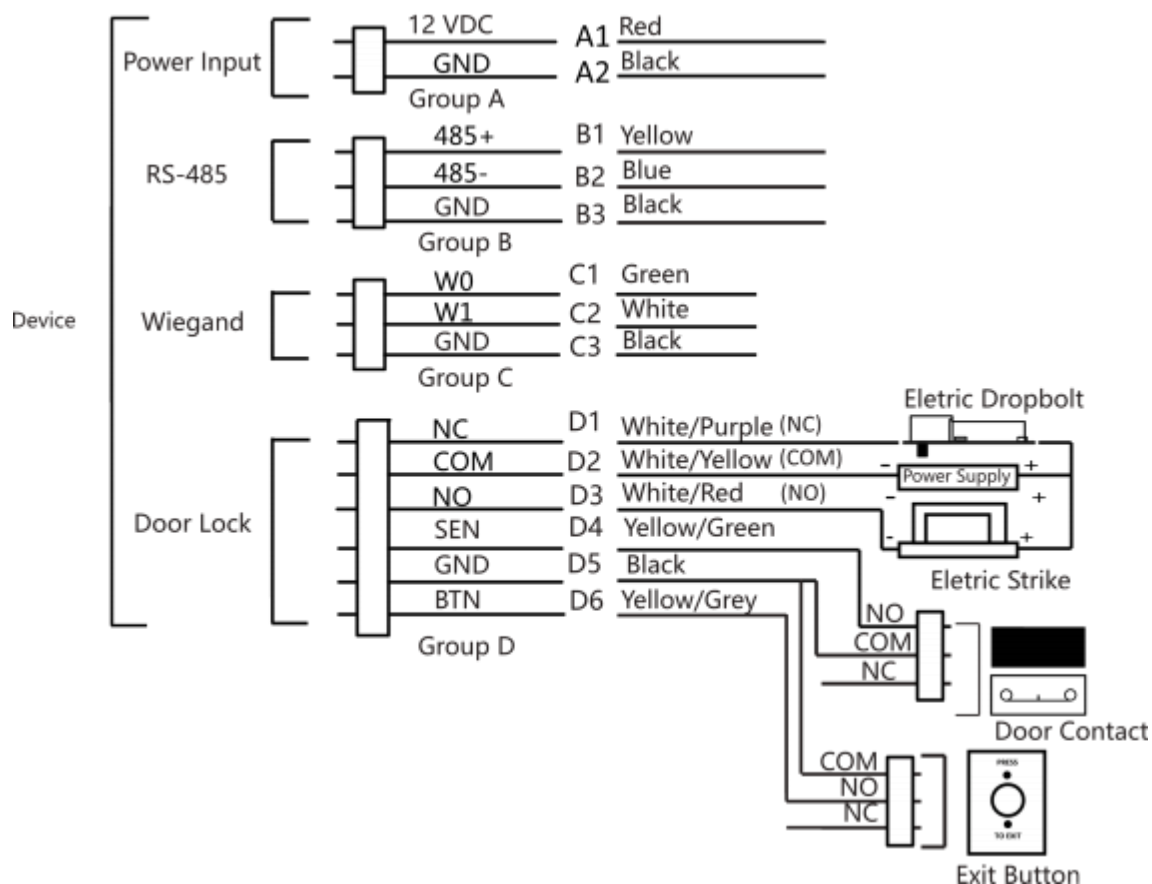


図 4-1 デバイスの配線

メモ

- 顔認証端末のウィーガンド方向を**入力に設定**して接続する必要があります
ウィーガンドカードリーダー。アクセスコントローラーに接続する場合は、ウィーガンド方向を**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必要があります。
- ウィーガンド方向設定の詳細については、ウィーガンドパラメータの設定を参照してください
- デバイスを電源に直接配線しないでください。

4.3ワイヤーセキュアドアコントロールユニット

端子をセキュアドアコントロールユニットと接続できます。

配線図は以下の通りです。

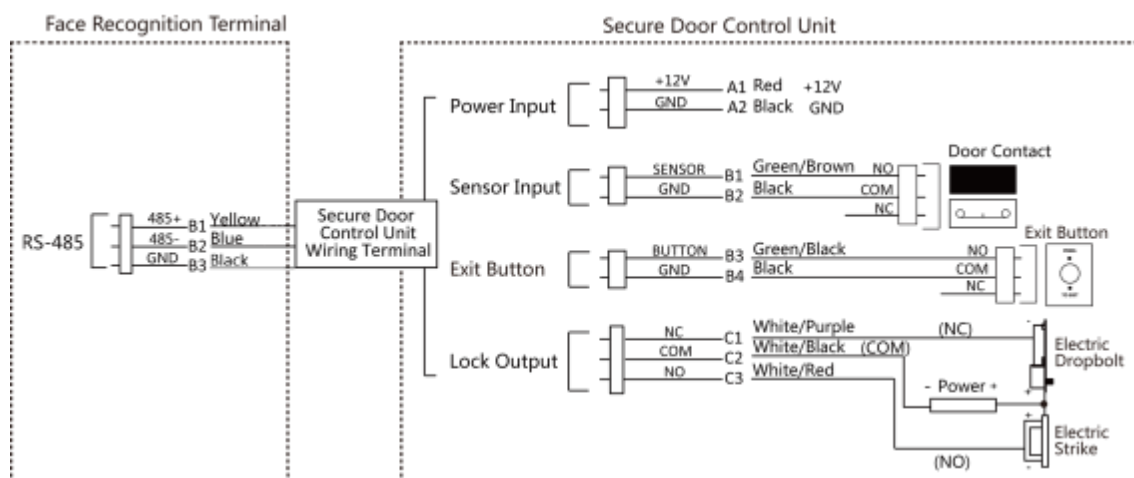


図4-2 セキュアドアコントロールユニットの配線



メモ

セキュアドアコントロールユニットは、外部電源に別途接続する必要があります。推奨される外部電源は12V、0.5Aです。

4.4 ワイヤファイアモジュール

4.4.1 電源投入時にドアが開いている配線図

ロックタイプ:アノードロック、磁気ロック、電気ボルト(NO)

セキュリティタイプ:電源投入時にドアが開いています。

シナリオ:消防車のアクセスに設置

タイプ1



メモ

消防システムは、アクセス制御システムの電源を制御します。

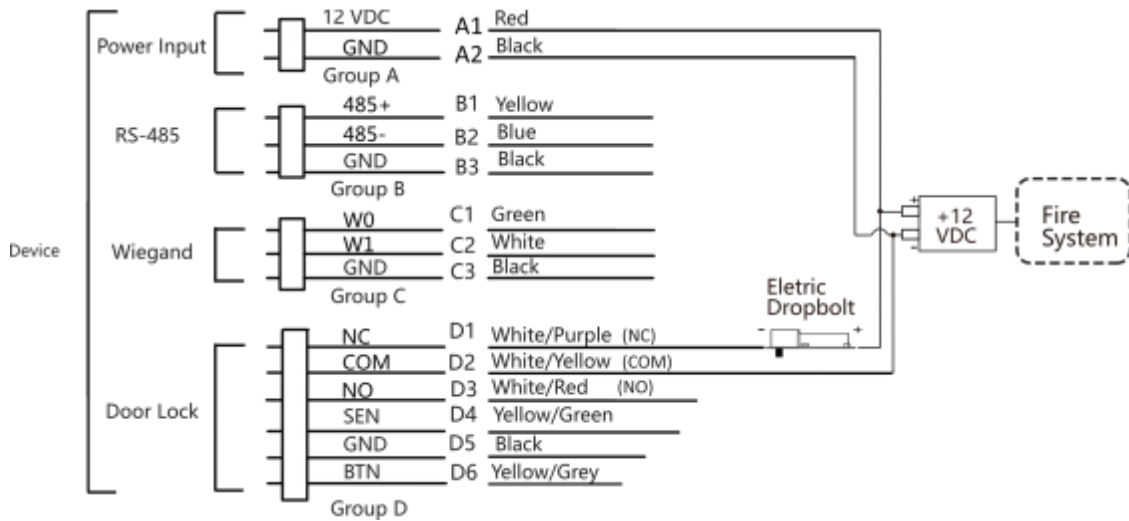


図 4-3 ワイヤデバイス

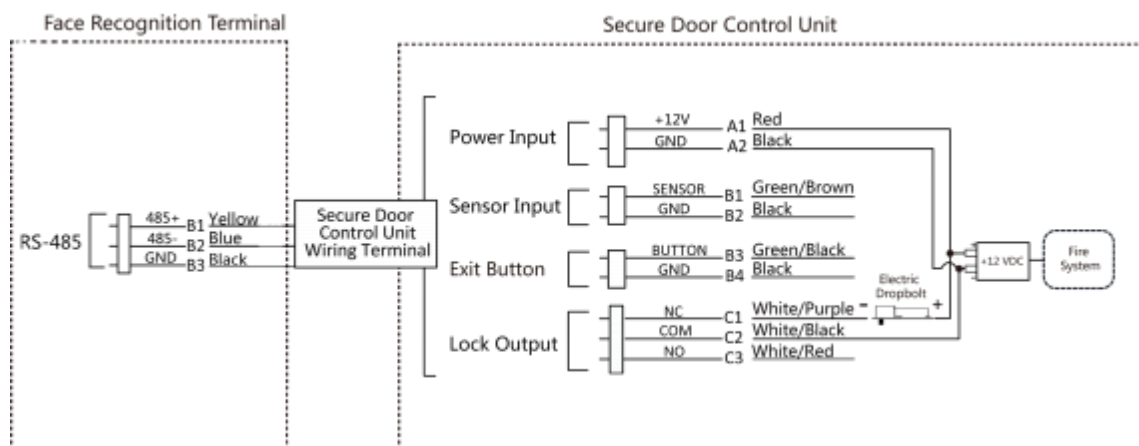


図4-4 ワイヤセキュアドアコントロールユニット

タイプ2

メモ

火災システム (NOとCOM、電源オフ時には通常開放) は、ロックと電源供給装置と直列に接続されています。火災警報が作動すると、ドアは開放されたままになります。平常時には、NOとCOMは閉じています。

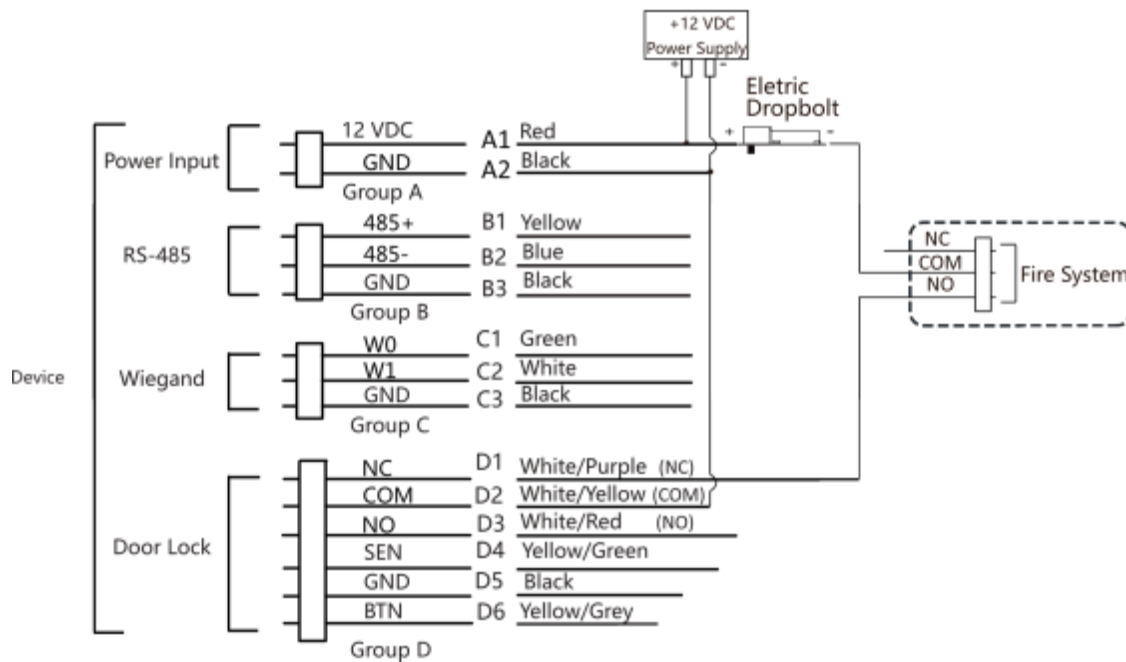


図4-5 配線装置

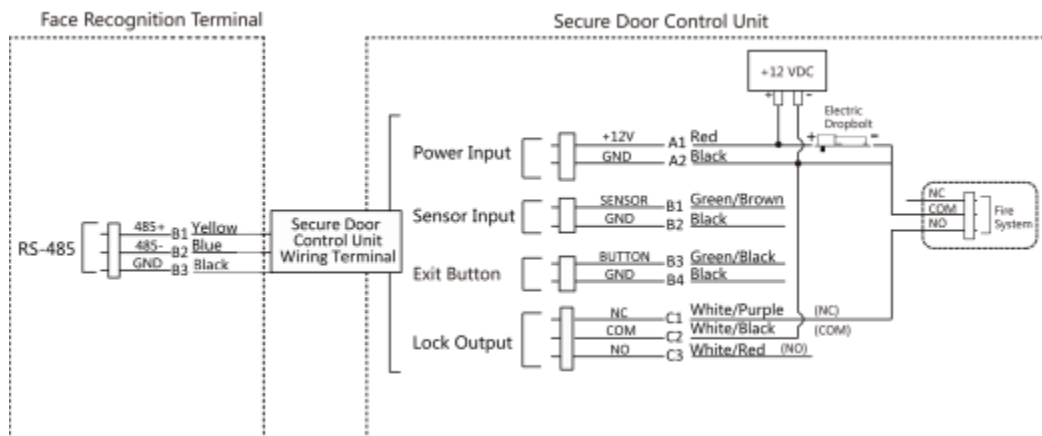


図4-6 配線固定ドアコントロールユニット

4.4.2 電源投入時にロックされたドアの配線図

ロックタイプ:カソードロック、エレクトリックロック、エレクトリックボルト(NC)

セキュリティタイプ:電源投入時にドアがロックされます。

シナリオ:ファイヤーリンケージを備えた入口/出口に設置されます。

 **メモ**

- 無停電電源装置 (UPS) が必要です。
- 火災システム (NOとCOM、電源オフ時には通常開放) は、ロックと電源供給装置と直列に接続されています。火災警報が作動すると、ドアは開放されたままになります。平常時には、NOとCOMは閉じています。

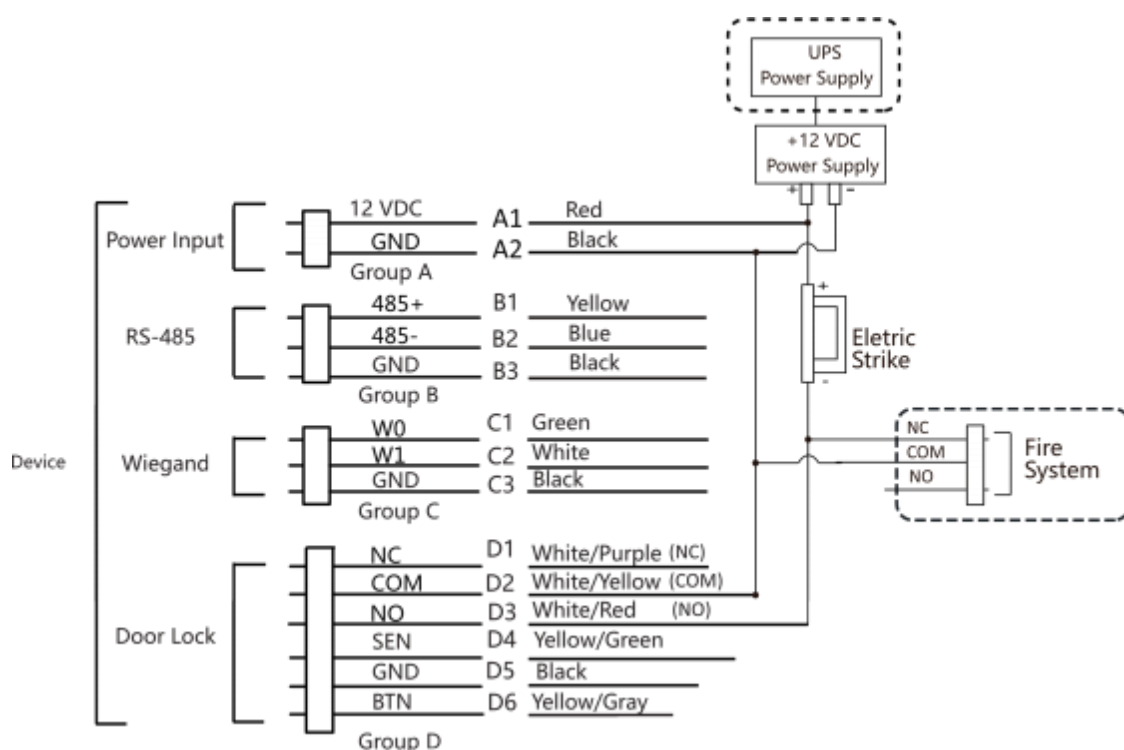


図 4-7 デバイスの配線

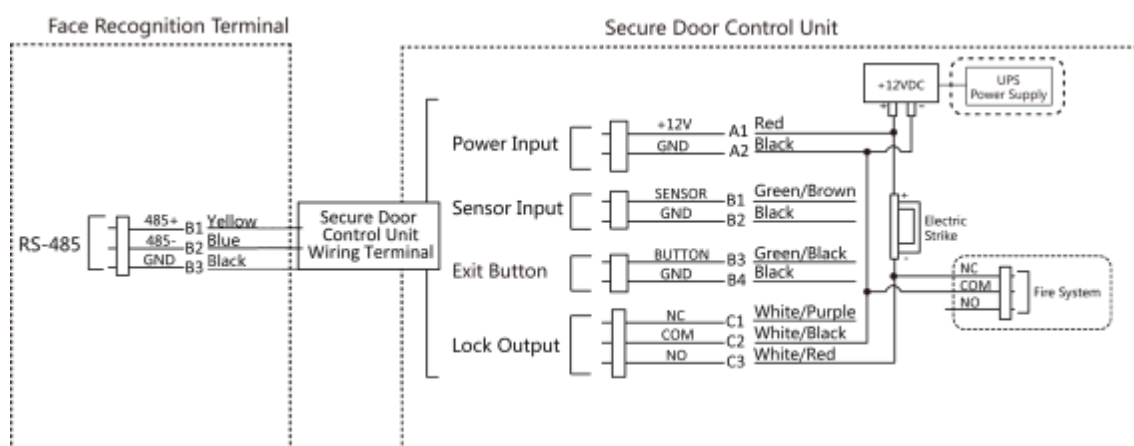


図4-8配線図

第5章 アクティベーション

最初のログインの前に、デバイスをアクティブ化する必要があります。デバイスの電源を入れると、システムはデバイスのアクティベーションページに切り替わります。

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

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

5.1 デバイス経由でアクティブ化する

デバイスがアクティブ化されていない場合は、デバイスの電源をオンにした後にアクティブ化できます。

デバイスの[アクティブ化] 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ブになります。

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 「アクティブ化」 ページ

 **注意**

デバイスのパスワードの強度は、自動的にチェックできます。パスワードは、ご自身で選択して変更することを強くお勧めします(少なくとも8文字以上を使用してください)。

大文字の文字、小文字の文字、数字、特殊の3種類のカテゴリキャラクターを使用して、製品のセキュリティを強化します。そして、私たちはあなたを変更することをお勧めします。

パスワードを定期的に、特に高セキュリティシステムでは、パスワードを毎月または毎週変更すると、製品の保護が向上します。

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、インストーラーおよび/またはエンドユーザーの責任です。

メモ

admin と 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することはサポートされていません。

- 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する必要があります。
- アクティベーション後、アプリケーションモードを選択する必要があります。詳細については、「[アプリケーションモードの設定](#)」を参照してください。
- アクティベーション後、ネットワークを設定する必要があります。詳細については、「[ネットワークパラメータの設定](#)」を参照してください。
- アクティベーション後、デバイスをプラットフォームに追加できます。詳細については、「[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、プライバシーを設定する必要がある場合は、アイテムを確認する必要があります。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、デバイスパラメータを管理するために管理者を追加する必要がある場合は、次のことを行う必要があります
管理者を設定します。詳細については、「[管理者の追加](#)」を参照してください。

5.2 経由でアクティブ化する Web ブラウザ

Webブラウザからデバイスをアクティブ化できます。

手順

1. デバイスのデフォルトのIPアドレス(192.0.0.64)をWebブラウザのアドレスバーに入力し、**Enter**キーを押します。
-

メモ

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

2. 新しいパスワード(管理者パスワード)を作成し、パスワードを確認します。
-

注意

強力なパスワードを推奨-製品のセキュリティを強化するために、自分で選択した強力なパスワードを作成することを強くお勧めします(大文字の文字、小文字の文字、数字、特殊文字を含む最低8文字を使用)。

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リセットすることをお勧めします。パスワードを毎月または毎週リセットすると、製品の保護が向上します。



メモ

admin と 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することはサポートされていません。

3. 「アクティブ化」をクリックします。
4. デバイスのIPアドレスを編集します。IPアドレスは、SADPツール、デバイス、およびクライアントソフトウェアを使用して編集できます。

5.3 SADPによる有効化

SADPは、LAN上のデバイスのIPアドレスを検出、アクティブ化、および変更するためのツールです。

始める前に

- 付属のディスクまたは公式からSADPソフトウェアを入手します webサイト (<https://seatech.info/>) をクリックし、プロンプトに従ってSADPをインストールします。

次の手順は、デバイスをアクティブ化し、そのIPアドレスを変更する方法を示しています。バ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で詳細を確認してください。

手順

1. SADPソフトウェアを実行し、オンラインデバイスを検索します。
 2. オンラインデバイスリストでデバイスを見つけて選択します。
 3. 新しいパスワード(管理者パスワード)を入力し、パスワードを確認します。
-



注意

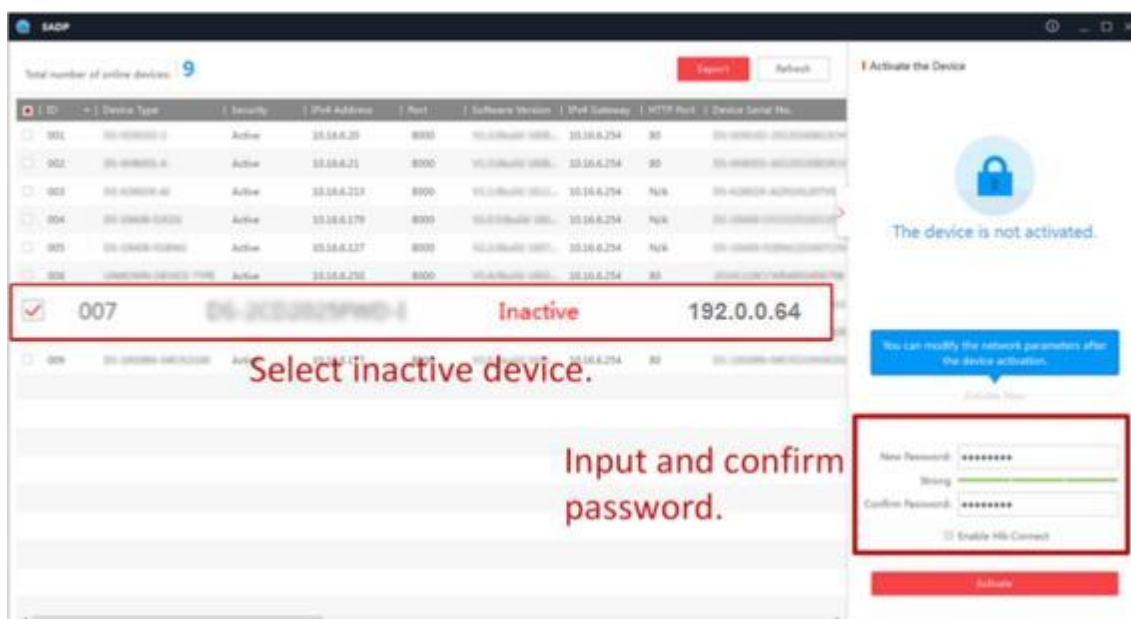
強力なパスワードを推奨、製品のセキュリティを強化するために、自分で選択した強力なパスワードを作成することを強くお勧めします(大文字の文字、小文字の文字、数字、特殊文字を含む最低8文字を使用)。特に高セキュリティシステムでは、パスワードを定期的リセットすることをお勧めします。パスワードを毎月または毎週再設定することで、製品をより適切に保護できます。



メモ

admin と 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することはサポートされていません。

4. 「アクティブ化」をクリックして、アクティブ化を開始します。



アクティベーションが成功すると、デバイスのステータスは[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) IPアドレスを手動で変更するか、[DHCPを有効にする]をオンにして、デバイスのIPアドレスをコンピューターと同じサブネットに変更します。
- 3) 管理者パスワードを入力し、[変更]をクリックして IPアドレスの変更を有効にします。

5.4 クライアントソフトウェアを介してデバイスをアクティブ化する

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

手順



メモ

この機能は、デバイスでサポートされている必要があります。

1. [デバイス管理]ページに入ります。
2. ■ 「デバイス管理」の右側をクリックし、「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。 検索したオンラインデバイスがリストに表示されます。
4. デバイスのステータス([セキュリティレベル]列に表示)を確認し、非アクティブなデバイスを選択します。
5. 「アクティブ化」をクリックして、「アクティブ化」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作成し、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lyチェックできます。製品のセキュリティを強化するために、自分で選択したパスワードを変更することを強くお勧めします(少なくとも3種類のカテゴリを含む、8文字以上、大文字の文字、小文字の文字、数字、特殊文字を含む)。そして、変更することをお勧めします。

パスワードを定期的に、特に高度なセキュリティシステムでは、パスワードを毎月または毎週変更することで、製品の保護を強化することができます。

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



メモ

admin と 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することはサポートされていません。

7. [OK]をクリックして、デバイスをアクティブにします。

第6章 クイック操作

6.1 言語の選択

デバイスシステムの言語を選択できます。

デバイスのアクティベーション後、デバイスシステムの言語を選択できます。

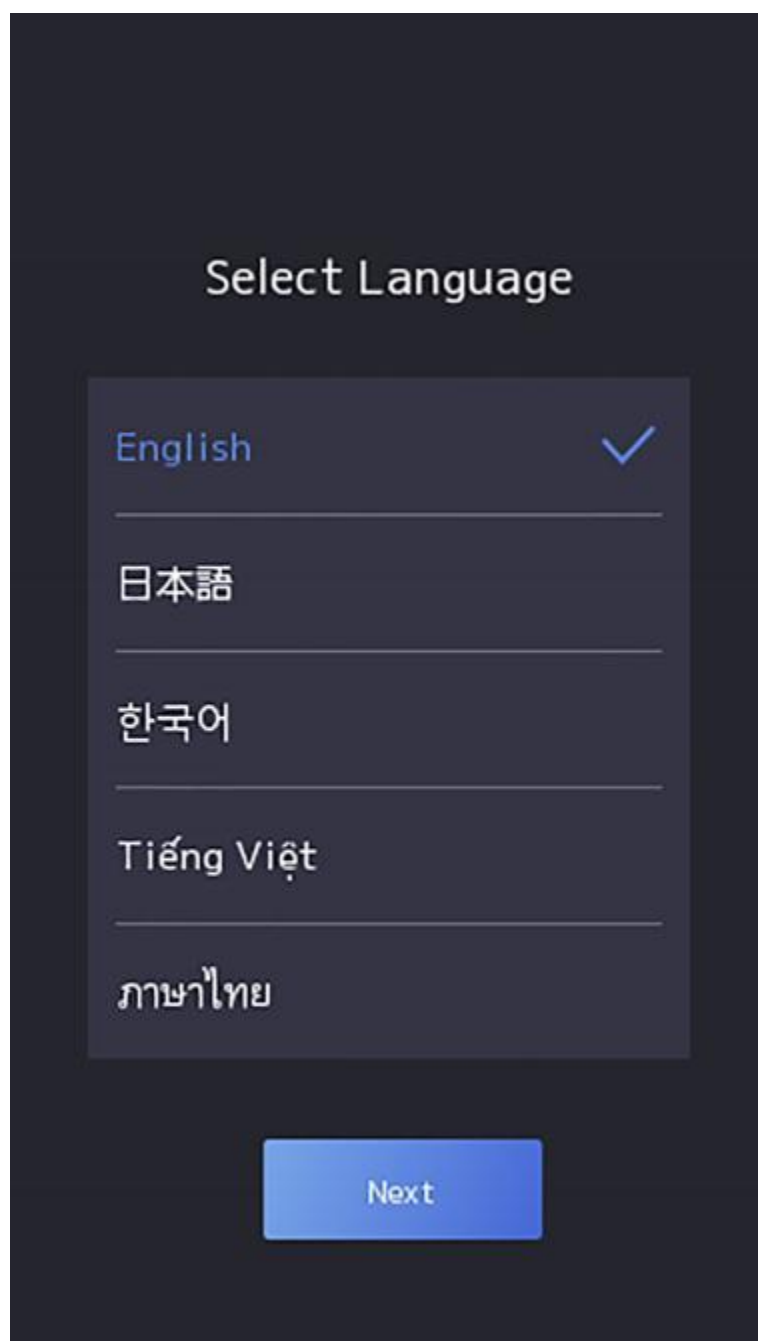


図6-1 システム言語の選択

システムのデフォルト言語は英語です。

 **メモ**

システム言語を変更すると、デバイスは自動的に再起動します。

6.2 アプリモードを設定する

デバイスをアクティブ化した後、デバイスをより適切に利用するために、アプリケーションモードを選択する必要があります。

手順

1. 「ようこそ」ページで、**ドロップダウンリストから「屋内」または「その他」**を選択します。

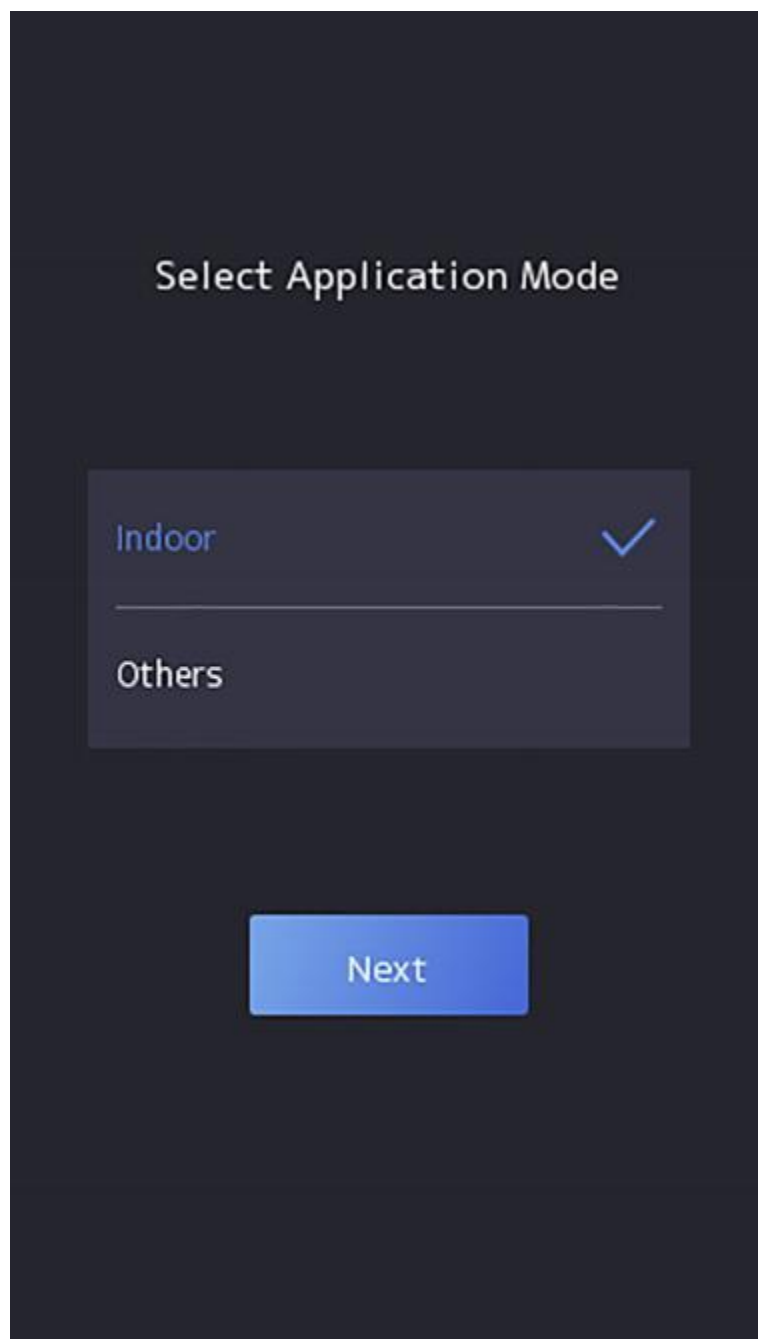


図6-2 「ようこそ」ページ

2)[OK]をタップ



- ・システム設定の変更も可能です。
 - ・屋内の窓際に設置する場合や、顔認証機能がうまく動作しない場合は、「その他」を選択してください。
 - ・アプリケーションモードを構成せずに[次へ]をタップすると、システムはデフォルトで**屋内**を選択します。
 - ・他のツールを使用してデバイスをリモートでアクティブ化すると、システムは**デフォルトでアプリケーションモードとして屋内**を選択します。
-

6.3 ネットワークパラメータの設定

アクティベーションしてアプリケーションモードを選択したら、デバイスのネットワークを設定できます。

手順

- 1.[ネットワークの選択]ページに入ったら、**実際のニーズに合わせて[有線ネットワーク]または[Wi-Fi]をタップ**します。

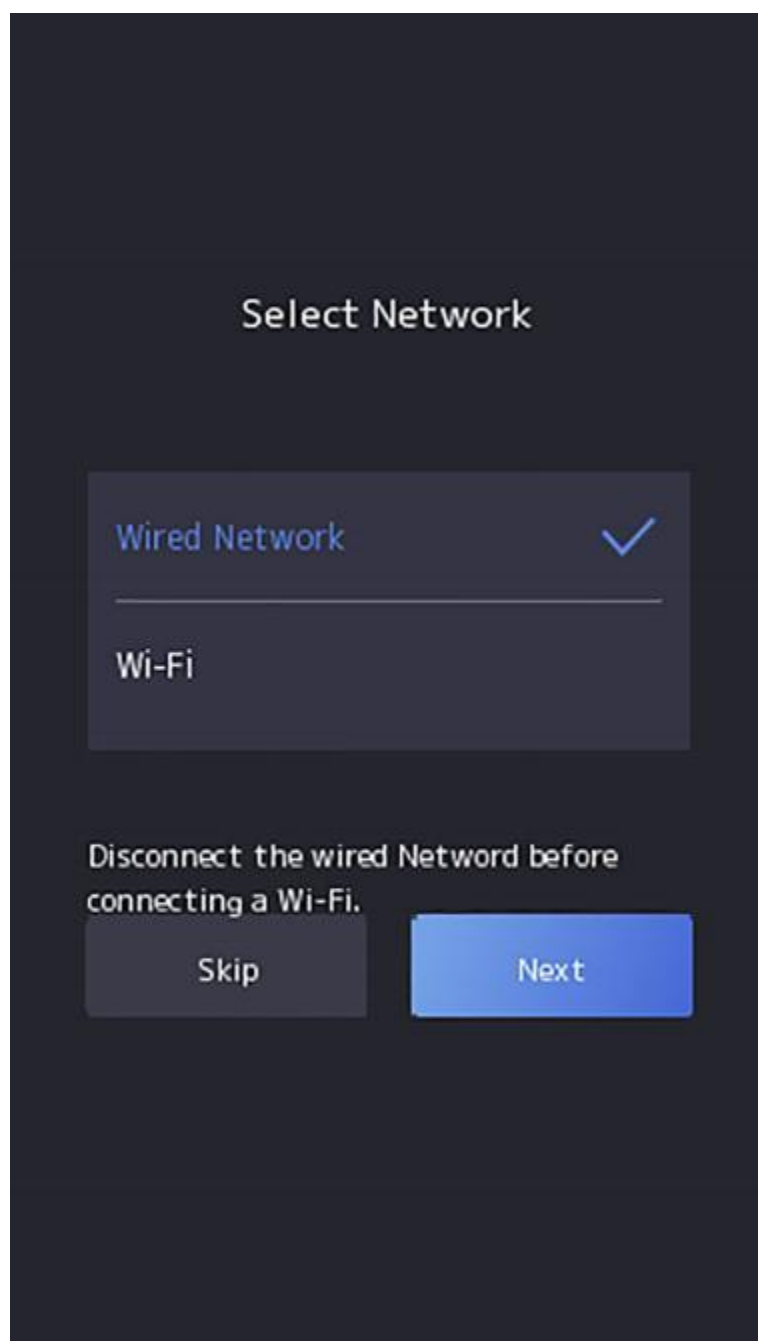


図6-3 ネットワークの選択

 **メモ**

Wi-Fiを接続する前に、有線ネットワークを切断してください。

2.[次へ]をタップ

有線ネットワーク



メモ

デバイスがネットワークに接続されていることを確認してください。

DHCPを有効にすると、システムはIPアドレスとその他のパラメータを自動的に割り当てます。DHCPを無効にする場合は、IPアドレス、サブネットマスク、およびゲートウェイを設定する必要があります。

Wi-Fi接続

Wi-Fiを選択し、Wi-Fiのパスワードを入力して接続します。

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

3. オプション: [スキップ]をタップして ネットワーク設定をスキップします。

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Connectを介して通信できます。デバイスをConnectモードクライアントなどに追加できます。

手順

1. Connectへのアクセスを有効にし、サーバーIPと確認コードを設定します。

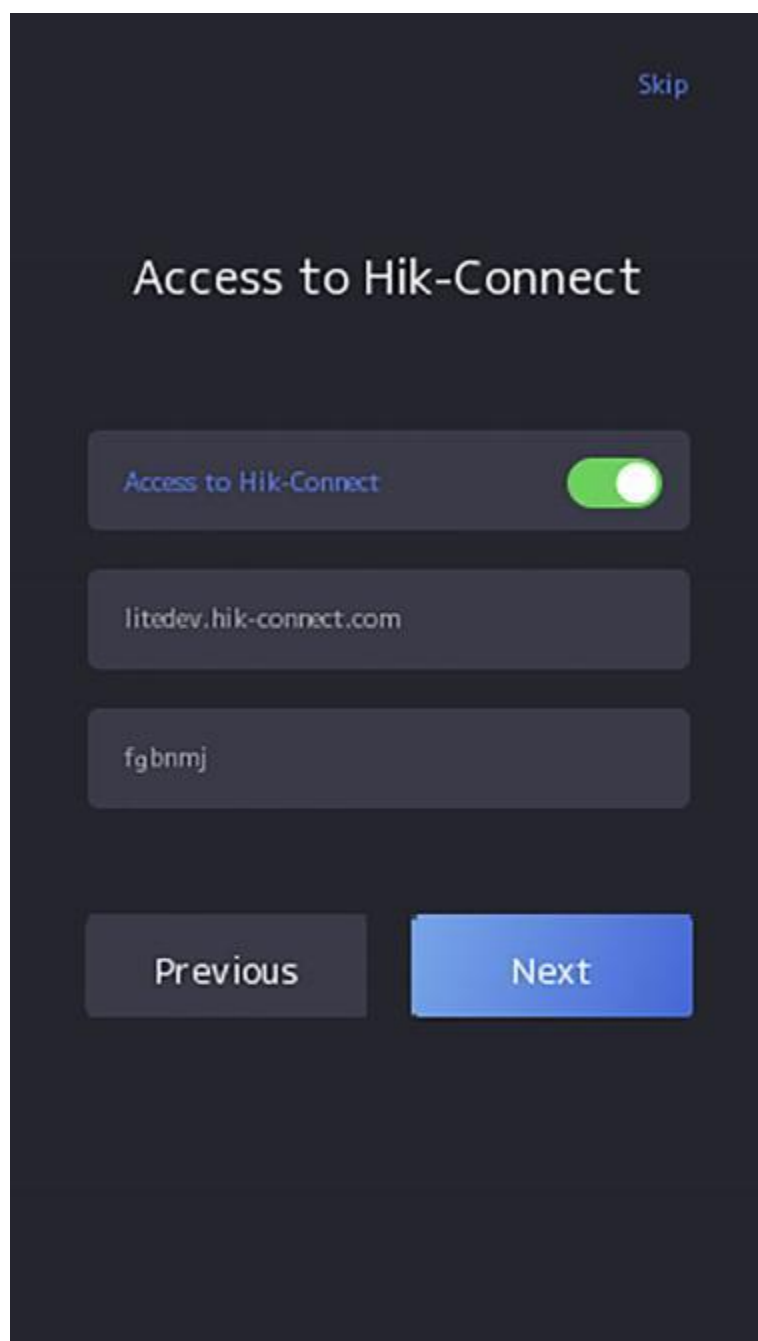


図 6-4 Connect へのアクセス

2)[次へ]をタップ



メモ

[前へ]をタップしてWi-Fi構成ページに戻った場合、接続されているWi-Fiをタップするか、別のWi-Fiを接続してプラットフォームページに再度入る必要があります。

6.5 モバイルクライアントへのリンク

アクティベーション、アプリケーションモードの設定、ネットワーキングの設定後、デバイスをモバイルクライアントに追加できます。

モバイルクライアントをダウンロードしてインストールします。モバイルクライアントのQRコードスキャン機能を使用して、デバイスに表示されているQRコードをスキャンして、デバイスをモバイルクライアントにリンクします。

指示に従って、デバイスをモバイルクライアントにリンクします。

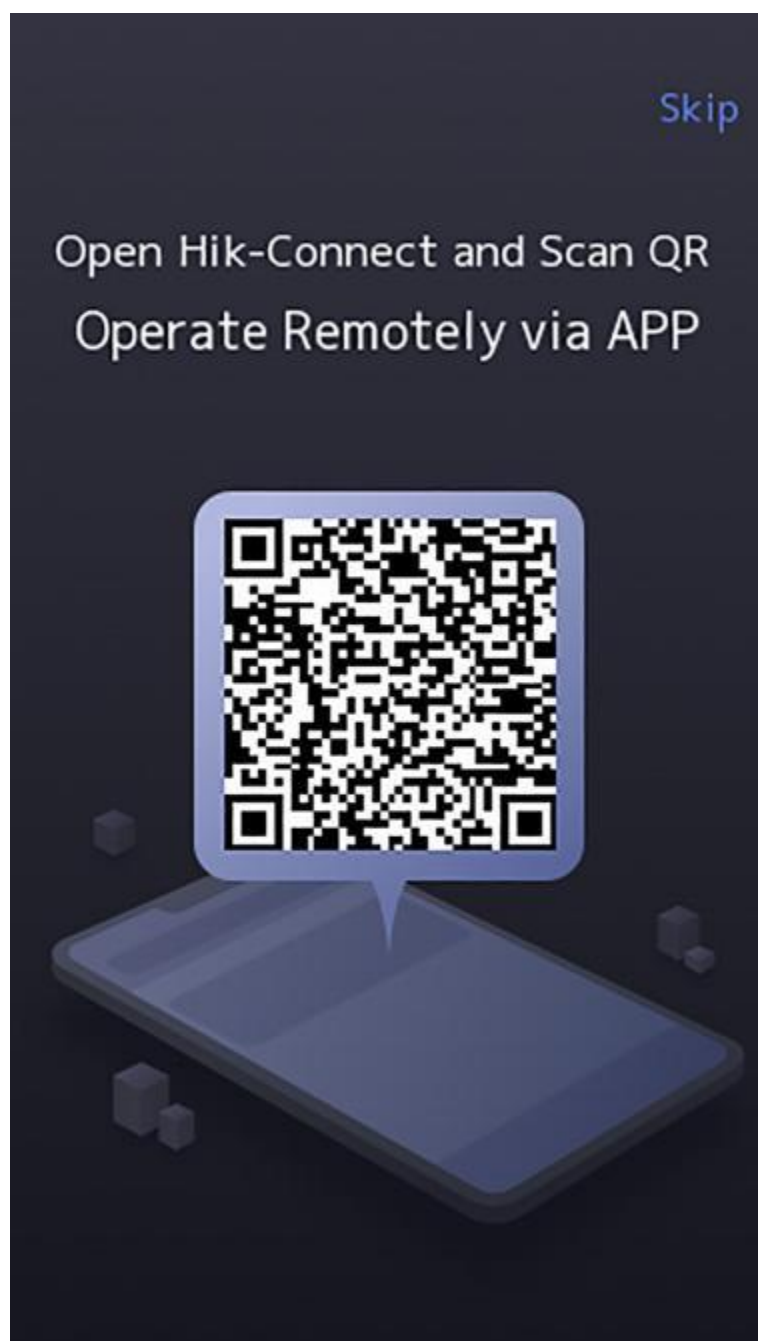


図6-5 モバイル・クライアントへのリンク

6.6 プライバシー設定

アクティベーション、アプリケーションモードの設定、およびネットワークの設定後、画像のアップロードや保存などのプライバシーパラメータ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を選択してください。

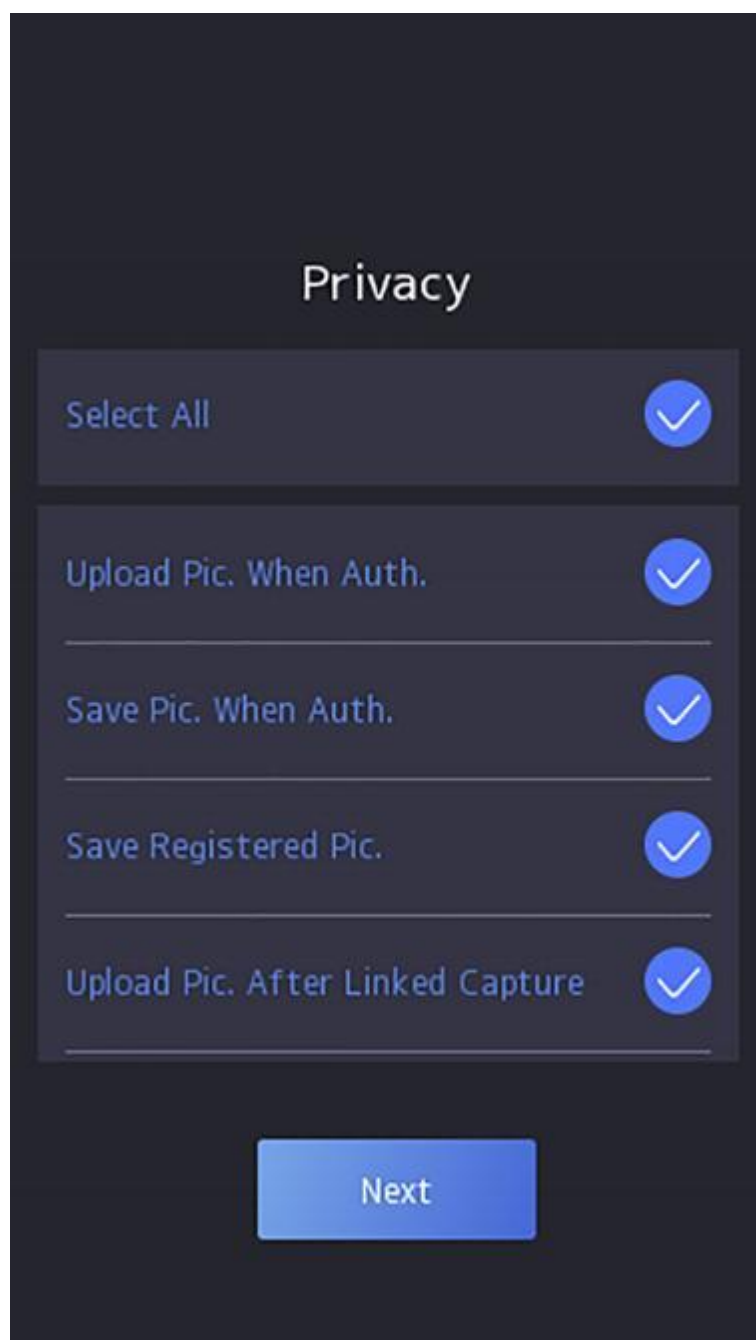


図6-6 プライバシー

キャプチャした写真をアップロードします。認証時(認証時にキャプチャした画像をアップロードする)

認証時に撮影した写真をプラットフォーム自動的にアップロードします。

キャプチャした写真を保存します。認証時(認証時にキャプチャした画像を保存する)

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。

登録した写真を保存します。(登録した画像を保存)

登録した顔写真は、機能を有効にするとシステムに保存されます。

写真をアップロードする

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自動的にアップロードします。

写真を保存します。

この機能を有効にすると、連携したカメラで撮影した画像をデバイスに保存できます。[次へ]をタップして設定を完了します。

6.7 管理者の設定

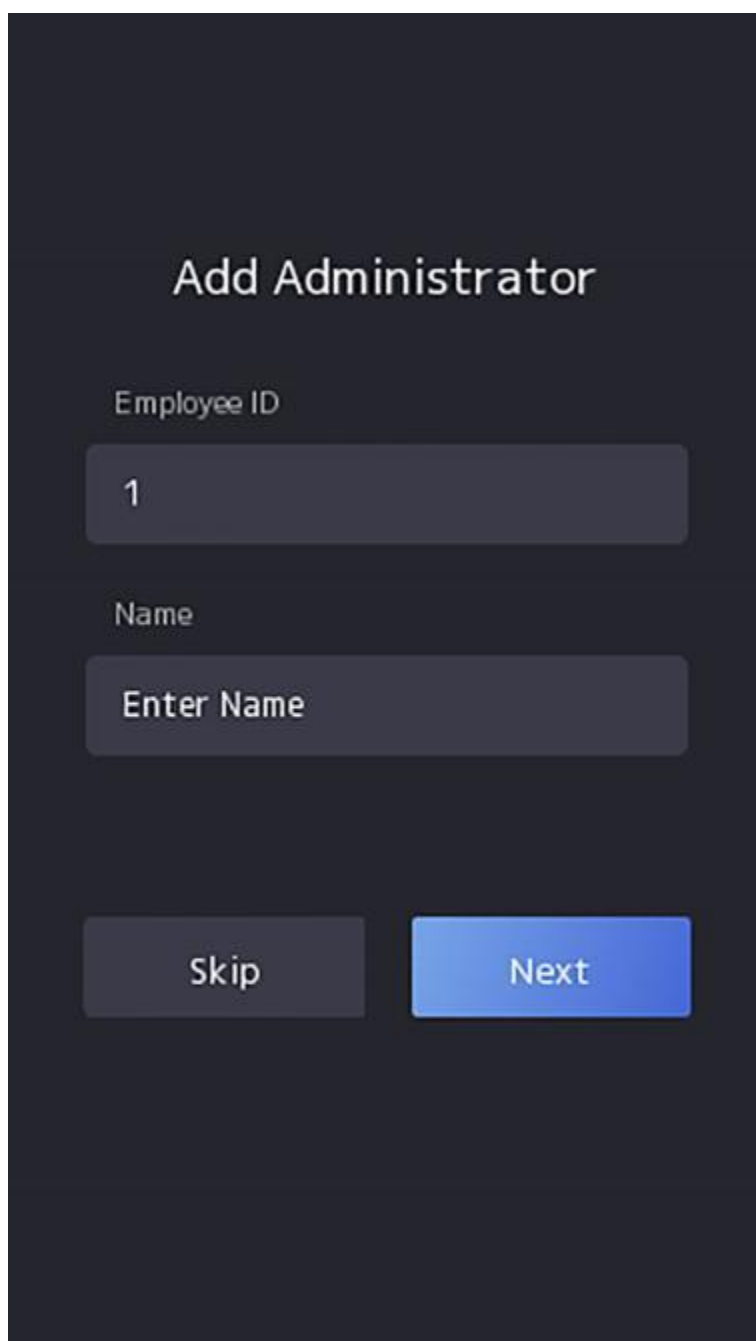
デバイスのアクティベーション後、デバイスパラメータを管理する管理者を追加できます。

始める前に

デバイスをアクティブにして、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スキップします。
2. 管理者名(オプション)を入力し、[次へ]をタップ



Add Administrator

Employee ID

1

Name

Enter Name







Skip Next

図6-7 「管理者の追加」ページ

3. 追加する認証情報を選択します。



最大1つの認証情報を追加する必要があります。

-  :カメラに向かって正面を向いています。顔が顔認証エリアにあることを確認します。
。クリックして  キャプチャし、クリックして  確認します。
-  :デバイス画面の指示に従って指を押します。クリックして  確定します。
-  :カード提示エリアにカード番号または提示カードを入力します。[OK]をクリックします。

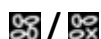
4. [OK]をクリックします。

認証ページに入ります。

ステータスアイコンの説明



デバイスは武装している/武装していない。



Connectは有効/無効です。



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




デバイスのWi-Fiは有効で接続されています/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



画面に表示されるショートカットキーを設定できます。詳しくは、**基本設定をご覧ください**



- ・ デバイスの部屋番号を入力し、[OK]をタップして 電話をかけます。
- ・ タップ  してセンターに電話します。



デバイスをセンターに追加するか、呼び出し操作が失敗します。



PINコードを入力して認証します。

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を設定します。

7.1.1 管理者によるログイン

デバイスの管理者を追加した場合、デバイス操作のためにデバイスにログインできるのは管理者のみです。

手順

1. 初期ページで3秒間長押しし、ジェスチャーに従って左または右にスライドすると、管理者ログインページに入ります。

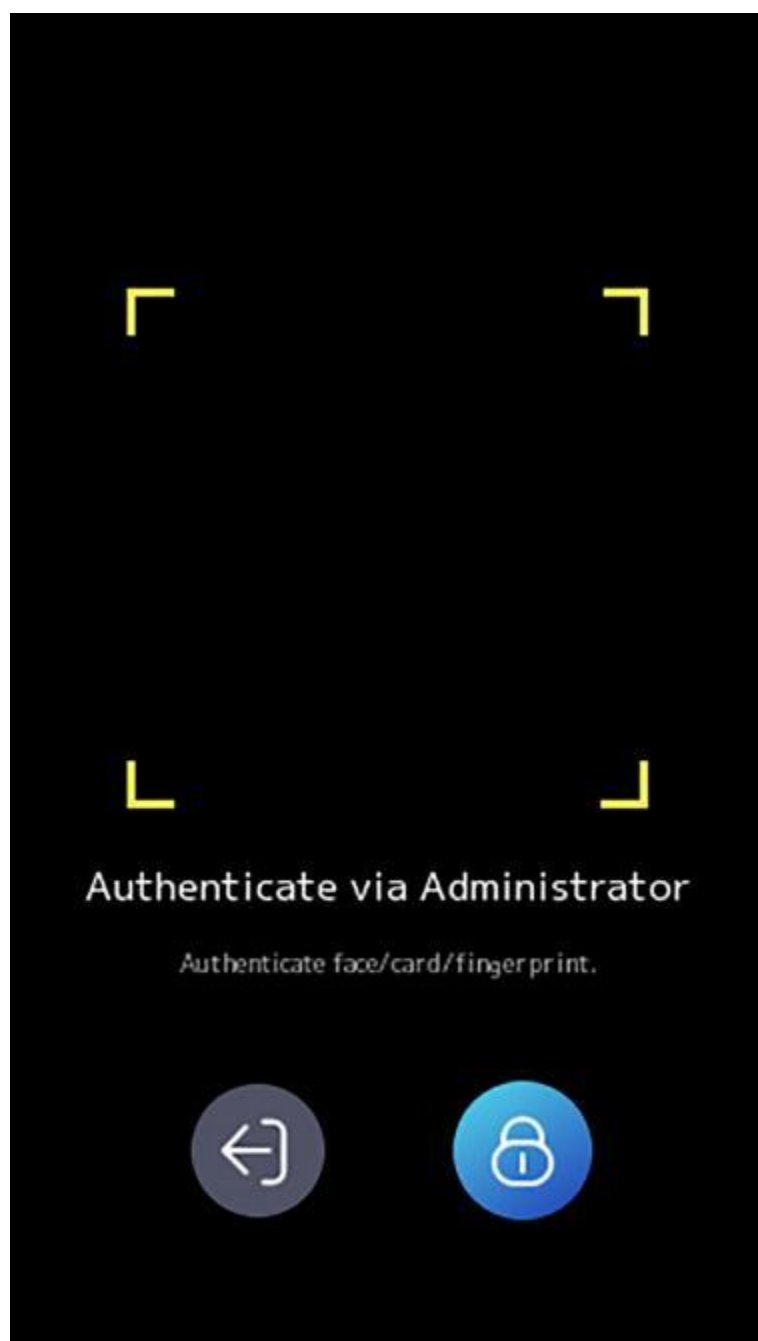


図7-1 管理者ログイン

2. 管理者の顔、またはカードを認証して、ホームページに入ります。

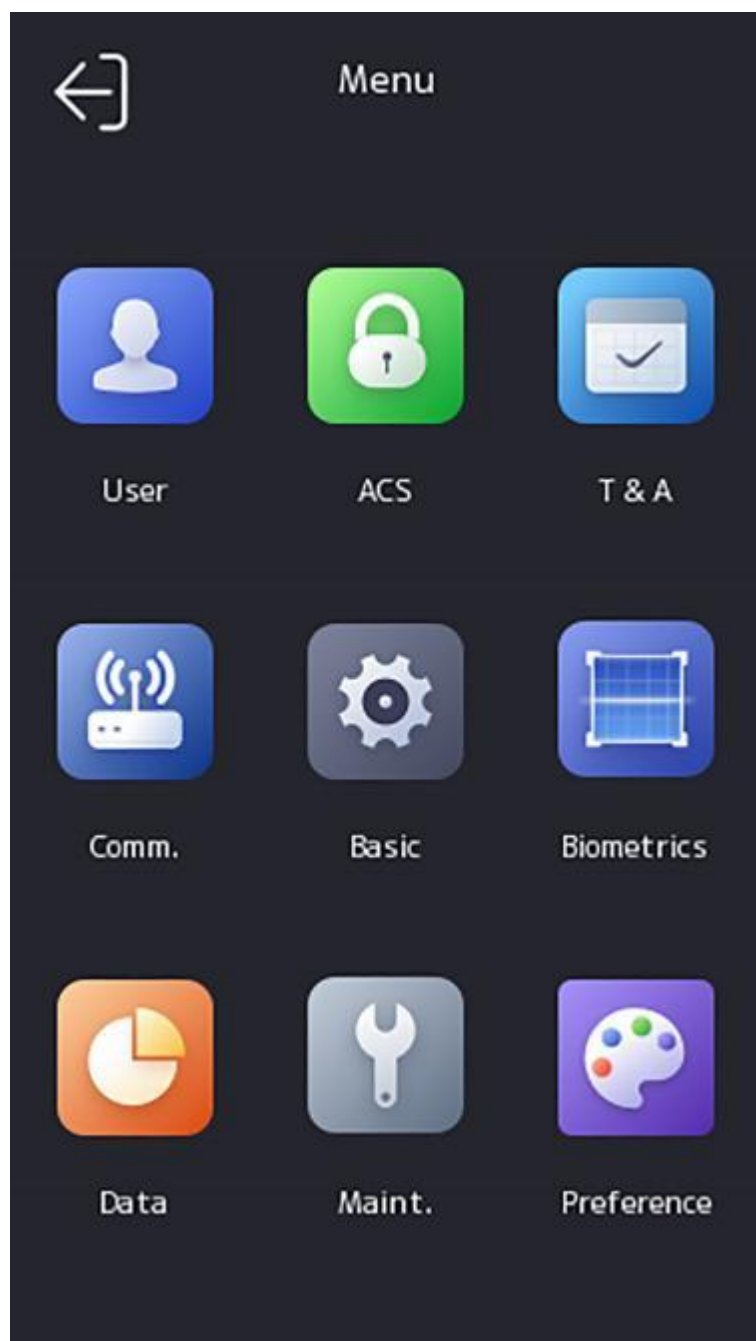




図7-2 ホームページ

 **メモ**

カードの試行が5回失敗すると、デバイスは30分間ロックされます。


3. オプション: タップ  すると、ログイン用のデバイスアクティベーションパスワードを入力できます。

4. オプション: タップ  すると、管理者ログインページを終了できます。

7.1.2 アクティベーションパスワードによるログイン

他のデバイス操作の前にシステムにログインする必要があります。管理者を設定しない場合は、以下の手順に従ってログインしてください。

手順

1. 初期ページを3秒間長押しし、ジェスチャーに従って左/右にスライドしてパスワード入力ページを入力します。
2. パスワードを入力します。
 - デバイスの管理者を追加した場合は、 をタップしてパスワードを入力します。
 - デバイスの管理者を追加していない場合は、パスワードを入力します。
- 3) **[OK]**をタップしてホームページに入ります。



メモ

パスワードの試行が5回失敗すると、デバイスは30分間ロックされます。

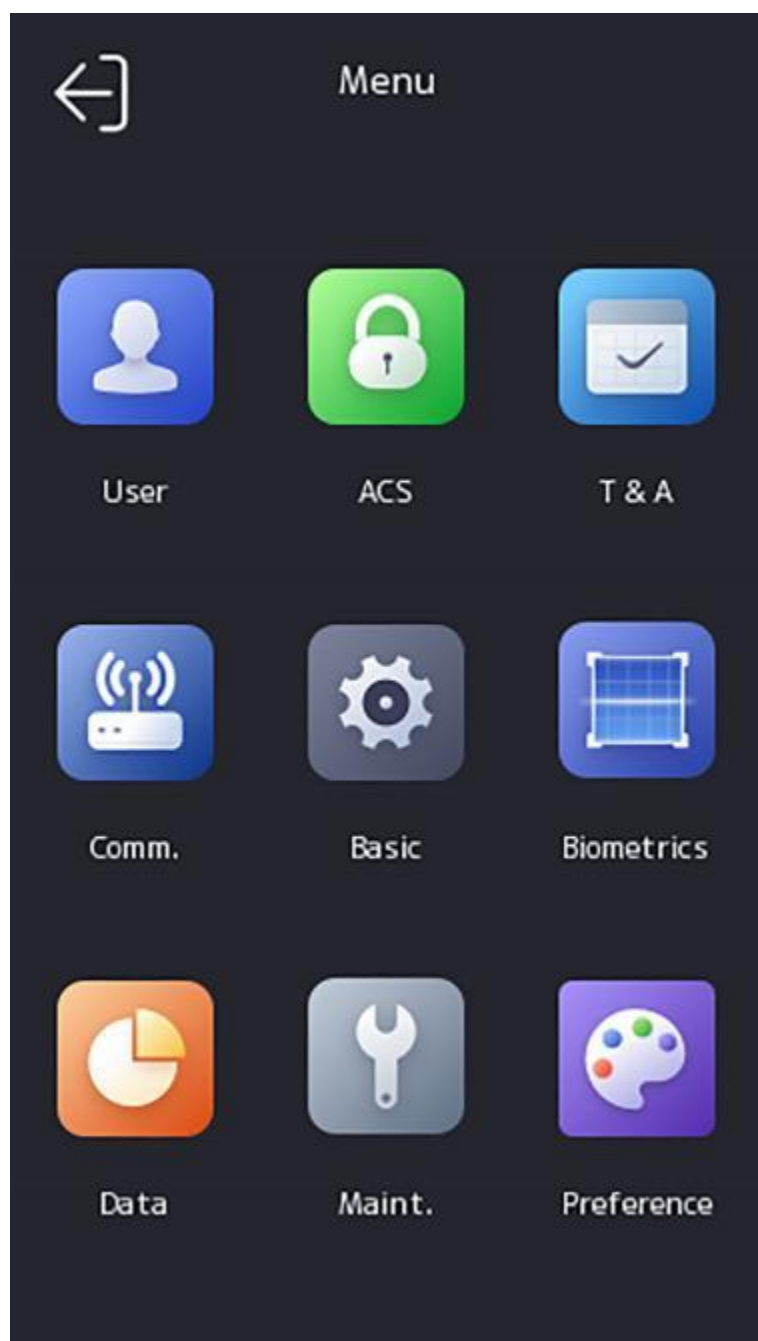


図7-3 ホームページ

7.2 通信設定

有線ネットワーク、Wi-Fiパラメータ、RS-485パラメータ、ウィーガンドパラメータ、ISUP、およびConnectへのアクセスは、通信設定ページで設定できます。

7.2.1 有線ネットワークパラメータの設定

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

手順

1. ホームページで「**Comm. (通信設定)**」をタップすると、通信設定ページに入ります。
2. 通信設定ページで、**[有線ネットワーク]**をタップします。

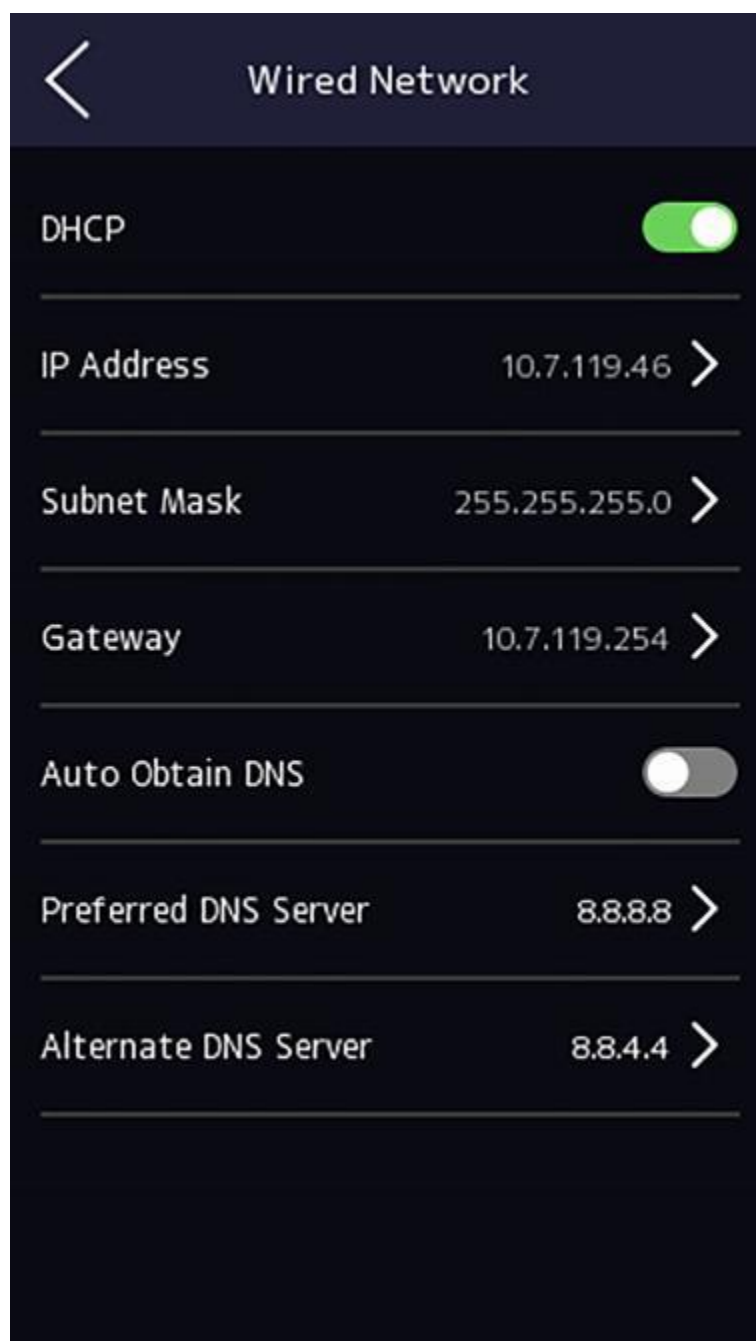


図7-4有線ネットワークの設定

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、ゲートウェイを手動で設定する必要があります。



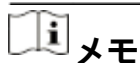
デバイスのIPアドレスとコンピューターのIPアドレスは、同じIPセグメント内にある必要があります。

4. DNSパラメータを設定します。**自動取得DNS**を有効にし、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パラメータを設定する

Wi-Fi機能を有効にし、Wi-Fi関連のパラメータを設定できます。

手順



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. ホームページで「**Comm. (通信設定)**」をタップすると、通信設定ページに入ります。
2. 通信設定ページで、**[有線ネットワーク]**をタップします。

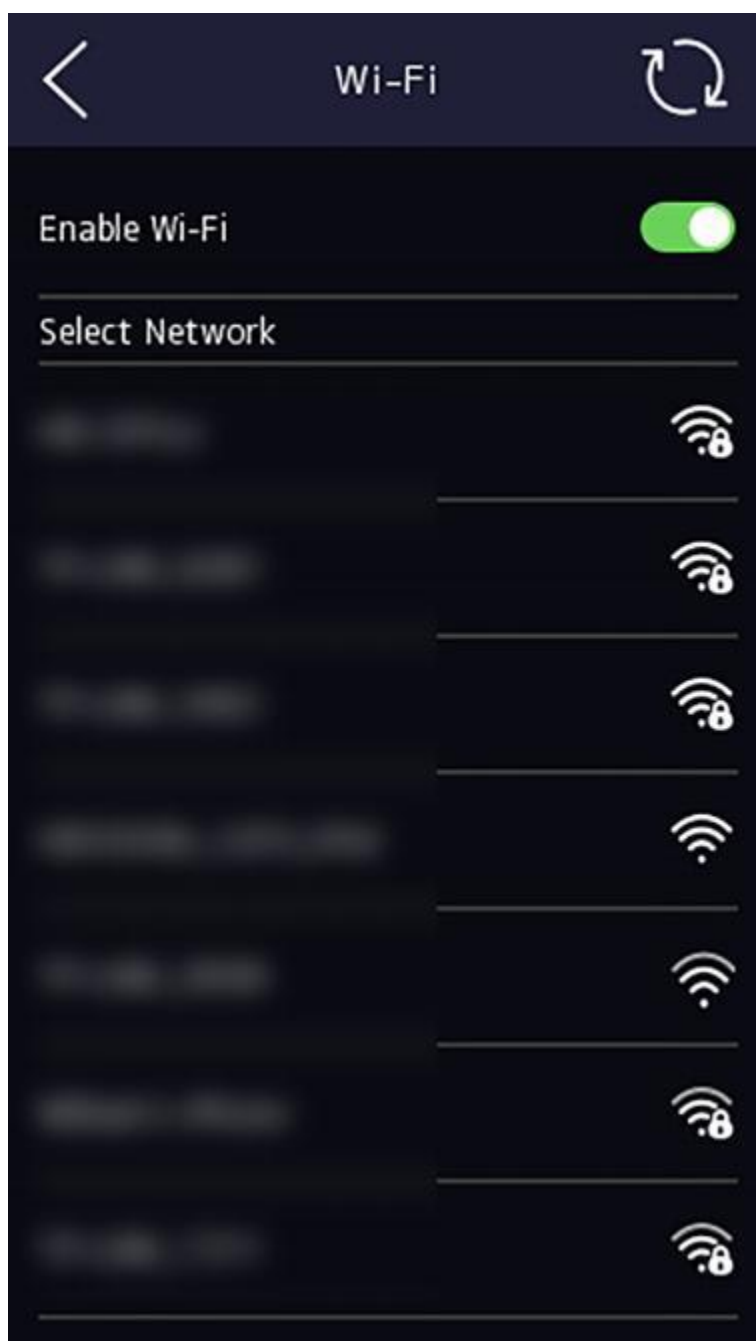


図7-5 Wi-Fi設定

3. Wi-Fi機能を有効にします。
4. Wi-Fiパラメータを設定します。
 - リストからWi-Fiを選択し、Wi-Fiのパスワードを入力します。[OK]をタップします。
 - 対象のWi-Fiがリストにない場合は、[Wi-Fiを追加]をタップします。Wi-Fiの名前とパスワードを入力します。そして、[OK]をタップします。




メモ

パスワードに使用できるのは、数字、文字、および特殊文字のみです。

5. Wi-Fiのパラメータを設定します。

- デフォルトでは、DHCPは有効になっています。システムは、IPアドレス、サブネットマスク、およびゲートウェイを自動的に割り当てます。
- DHCPを無効にする場合は、IPアドレス、サブネットマスク、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. タップ  してネットワークパラメータを保存します。

7.2.3 RS-485パラメータの設定

顔認証端末は、RS-485端子を介して外部アクセスコントローラー、セキュアドアコントロールユニット、またはカードリーダーを接続できます。

手順

1. ホームページで「Comm. (通信設定)」をタップすると、通信設定ページに入ります。
2. 通信設定ページで、[有線ネットワーク]をタップします。



図 7-6 RS-485 パラメータの設定

3. 実際のニーズに応じて周辺機器のタイプを選択します。



[アクセス制御]を選択した場合:RS-485インターフェースを介してデバイスを端末に接続する場合は、RS-485アドレスを2に設定します。デバイスをコントローラーに接続する場合は、ドア番号によるRS-485アドレスを設定します。

4. 上部の左コーナーにある背面アイコンをタップし、パラメータを変更した場合はデバイスを再起動する必要があります。

7.2.4 ウィーガンドパラメータの設定

ウィーガンドの伝達方向を設定できます。

手順

1. ホームページで「Comm. (通信設定)」をタップすると、通信設定ページに入ります。
2. 通信設定ページで、[有線ネットワーク]をタップします。

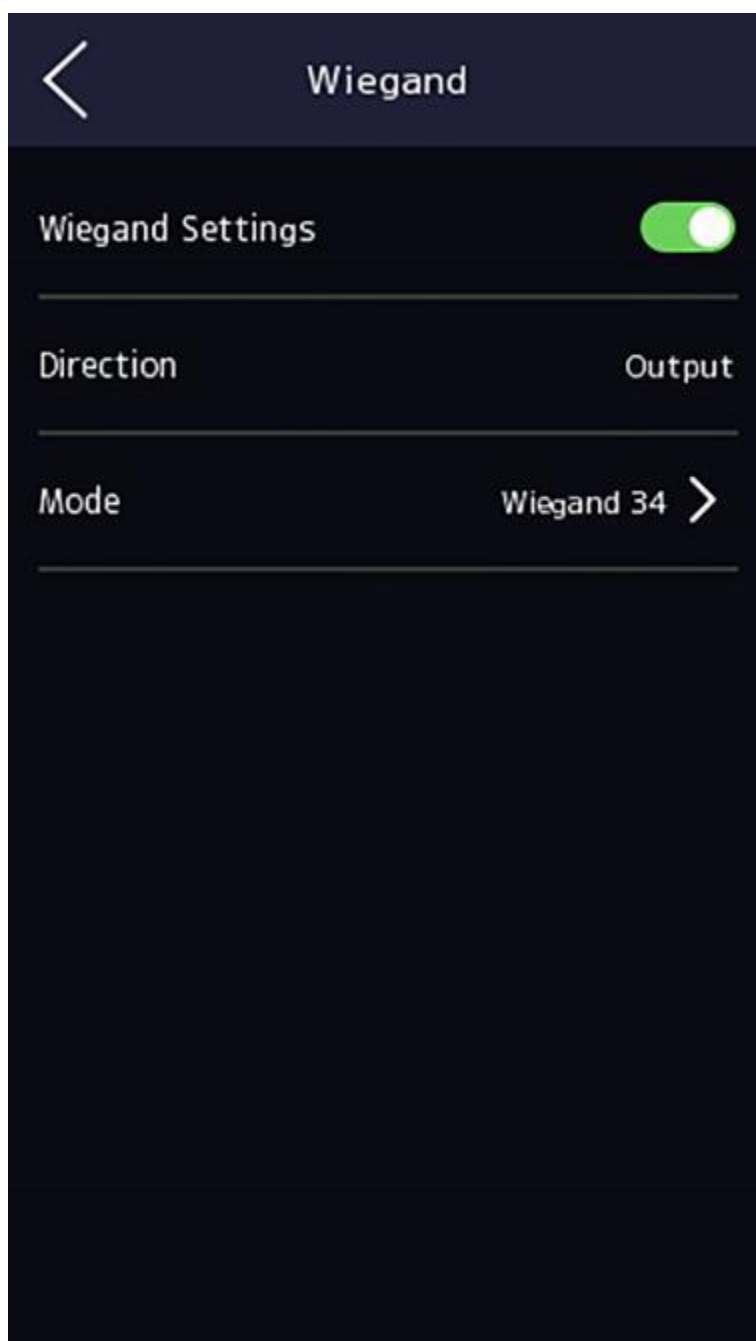


図7-7 ウィーガンドの設定

3. ウィーガンド機能を有効にします。
4. 送信方向を選択します。

出力:顔認証端末は、外部アクセスコントローラを接続できます。そして、2つのデバイスはカード番号を送信します。ウィーガンド26またはウィーガンド34経由します。

5. タップ してネットワークパラメータを保存します。



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

7.2.5 ISUPパラメータの設定

ISUPパラメータを設定すると、デバイスはISUPプロトコルを介してデータをアップロードできます。

始める前に

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. 「Communication. → ISUP」をタップします。

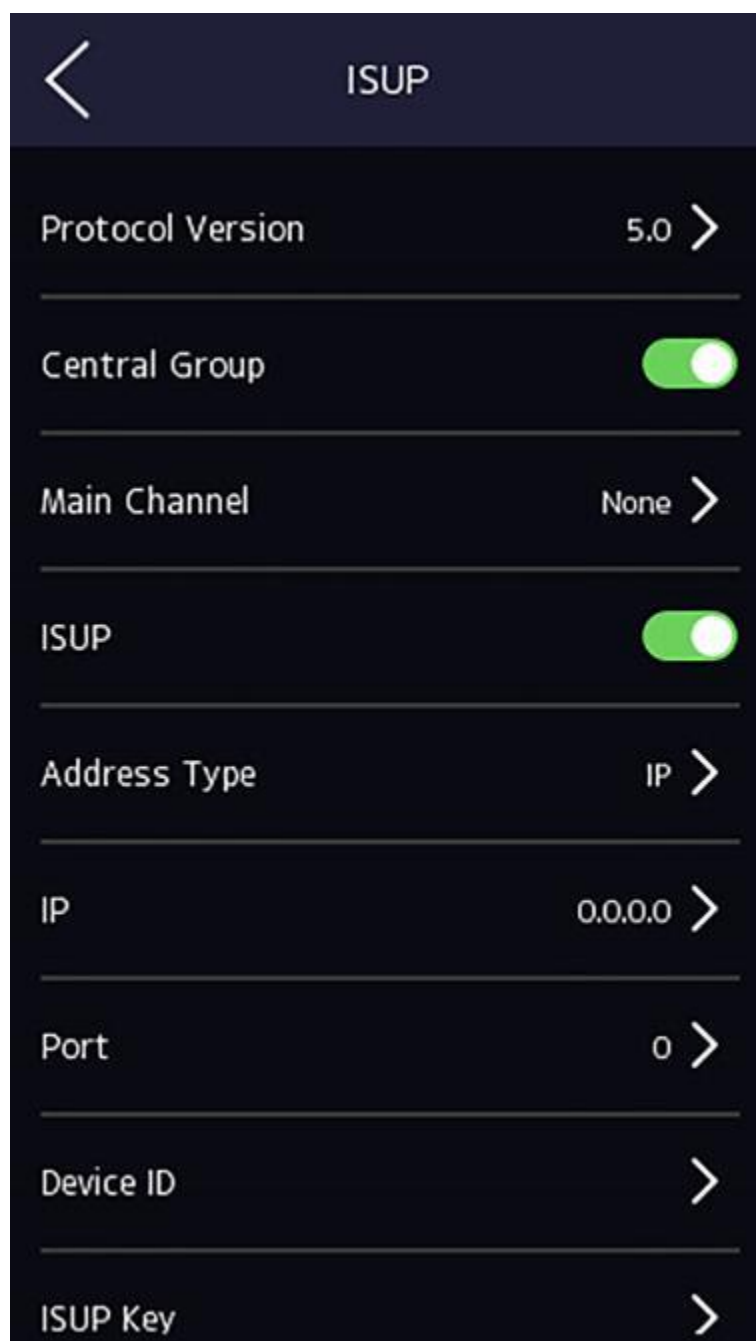


図7-8 ISUP設定

- ISUP機能を有効にし、ISUPサーバーパラメータを設定します。ISUPバージョン実際のニーズに応じてISUPバージョンを設定します。

セントラルグループ

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。

メインチャンネル

N1 または None をサポートします。

ISUPの

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

アドレスタイプ

実際のニーズに応じてアドレスタイプを選択してください。

IPアドレス

ISUP サーバーの IP アドレスを設定します。

ポート番号

ISUP サーバーのポート番号を設定します。



メモ

ポート番号範囲:0 ~ 65535。

デバイスID

デバイスのシリアル番号を設定します。

パスワード

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



メモ

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

7.2.6 プラットフォームアクセス

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

始める前に

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. ホームページで「Comm. (通信設定)」をタップすると、通信設定ページに入ります。
 2. 通信設定ページで、[Connectへのアクセス]をタップします。
 3. 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. 確認コードを作成し、Connectを介してデバイスを管理するときに確認コードを入力する必要があります。
-

7.3 ユーザー管理

ユーザー管理インターフェースでは、ユーザーを追加、編集、削除、検索できます。

7.3.1 管理者の追加

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

手順

1. 初期ページを長押しして、バックエンドにログインします。
2. 「ユーザー→+」をタップして、「ユーザーの追加」ページに入ります。

Add User	
Employee ID	2
Name	Not Configured
Face	Not Configured
Card	0/5
Fingerprint	0/10
PIN	Not Configured
Auth. Settings	Device Mode
User Role	Normal User

3. 従業員IDを編集します。



メモ

- 従業員IDは32文字以内にしてください。また、下位の文字、上位の文字、および数値の組み合わせにすることができます。
- 従業員IDは重複してはいけません。

4. 「名前」フィールドをタップし、ソフトキーボードでユーザー名を入力します。



メモ

- ユーザー名には、数字、大文字の文字、小文字の文字、および特殊文字を使用できます。
- ユーザー名には最大32文字を使用できます。

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



メモ

- 顔写真の追加の詳細については、**顔写真の追加を参照してください。**



メモ

- カードの追加の詳細については、「**カードの追加**」を参照してください。
- パスワードの追加の詳細については、「**PINコードの表示**」を参照してください。

6. **オプション:** 管理者の認証タイプを設定します。



メモ

- 認証タイプの設定の詳細については、「**認証モードの設定**」を参照してください。

7. 管理者権限機能を有効にします。 **管理者権**

限の有効化

ユーザーが管理者である。通常の出席機能を除き、ユーザーは権限を認証した後、ホームページにアクセスして操作することもできます。

8. 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。また、ユーザーは顔写真を使用して認証できます。

手順



メモ

顔写真は最大1500枚まで追加できます。

1. 初期ページを3秒間長押しし、ジェスチャーに従って左/右にスライドし、バックエンドにログインします。
2. 「ユーザー→+」をタップして、「ユーザーの追加」ページに入ります。
3. 従業員IDを編集します。



メモ

- 従業員IDは32文字以内にしてください。また、下位の文字、上位の文字、および数値の組み合わせにすることができます。
- 従業員IDは重複してはいけません。

4. 「名前」フィールドをタップし、ソフトキーボードでユーザー名を入力します。

メモ

- ユーザー名には、数字、大文字の文字、小文字の文字、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、顔写真の追加ページに入ります。



図7-9 顔画像の追加

6. カメラを見てください。



メモ

- 顔写真を追加するときは、顔写真が顔写真のアウトラインにあることを確認してください。
 - キャプチャした顔写真が高品質で正確であることを確認してください。
 - 顔写真の追加方法については、**顔写真を収集/比較する際のヒントをご覧ください。**
-

顔写真を完全に追加すると、キャプチャした顔写真がページの右上隅に表示されます。

7) [保存] をタップして顔写真を保存します。

8. オプション: [再試行] をタップし、顔の位置を調整して顔の写真を再度追加します。


9. ユーザーロールを設定します。

管理者

ユーザーが管理者である。通常の出席機能を除き、ユーザーは権限を認証した後、ホームページにアクセスして操作することもできます。

通常の利用者

ユーザーは通常の利用者です。ユーザーは、初期ページでのみ認証または出席を行うことができます。

10. タップ  して設定を保存します。

7.3.4 カードを追加

ユーザーのカードを追加すると、ユーザーは追加されたカードを介して認証できます。

手順



メモ

最大3000枚のカードを追加できます。

1. 初期ページを3秒間長押しし、ジェスチャーに従って左/右にスライドし、バックエンドにログインします。
2. 「ユーザー→+」をタップして、「ユーザーの追加」ページに入ります。
3. 配線図に従って外部カードリーダーを接続します。
4. [社員ID.フィールド]をタップし、社員IDを編集



メモ

- 従業員IDは32文字以内にしてください。また、下位の文字、上位の文字、および数値の組み合わせにすることができます。
- 従業員IDは重複してはいけません。

5. 「名前フィールド」をタップし、ソフトキーボードでユーザー名を入力します。



メモ

- ユーザー名には、数字、大文字の文字、小文字の文字、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文字以内である必要があります。
-

6. カードフィールドをタップし、[+]をタップします。
 7. カード番号を設定します。
 - カード番号を手動で入力します。
 - カード提示エリアにカードを提示すると、カード番号が発行されます。
-



メモ

- カード番号は空欄にすることはできません。
 - カードNo.には20文字まで入力できます。
 - カード番号は重複できません。
-

8. カードの種類を設定します。
9. ユーザーロール
を設定します。

管理者

ユーザーが管理者である。通常の出席機能を除き、ユーザーは権限を認証した後、ホームページにアクセスして操作することもできます。

通常の利用者

ユーザーは通常の利用者です。ユーザーは、初期ページでのみ認証または出席を行うことができます。

10. タップ して設定を保存します。

7.3.5 PINコードの表示

ユーザーのPINコードを追加すると、ユーザーはPINコードを使用して認証できます。

手順

1. 初期ページを3秒間長押しし、ジェスチャーに従って左/右にスライドしてログインします
バックエンド。
 2. 「ユーザー→+」をタップして、「ユーザーの追加」ページに入ります。
 3. [社員IDフィールド]をタップし、社員IDを編集
-



メモ

- 従業員IDは32文字以内にしてください。また、下位の文字、上位の文字、および数値の組み合わせにすることができます。
 - 従業員IDは重複してはいけません。
-

4. 「名前」フィールドをタップし、ソフトウェアキーボードでユーザー名を入力します。
-



メモ

- ユーザー名には、数字、大文字の文字、小文字の文字、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文字以内である必要があります。

5. PINコードをタップしてビューPINコード。



メモ

PINコードは編集できません。プラットフォームによってのみ適用できます。

6. ユーザーロール

を設定します。

管理者

ユーザーが管理者である。通常の出席機能を除き、ユーザーは権限を認証した後、ホームページにアクセスして操作することもできます。

通常の利用者

ユーザーは通常の利用者です。ユーザーは、初期ページでのみ認証または出席を行うことができます。

7. 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、またはその他の信頼性を追加した後、認証モードとユーザーは、構成された認証モード。

手順

1. 初期ページを3秒間長押しし、ジェスチャーに従って左/右にスライドしてログインします。
2. [認証モード]→[ユーザーの追加]→[ユーザー編集]をタップします。
3. 認証モードとして[デバイス]または[カスタム]を選択します。

デバイス

デバイスモードを選択する場合は、最初に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の設定を参照してください。

習慣

実際のニーズに応じて、異なる認証モードを組み合わせることができます。

4. タップ して設定を保存します。

7.3.7 ユーザーの検索と編集

ユーザーを追加した後、ユーザーを検索して編集できます。

ユーザーの検索

[ユーザー管理]ページで、検索領域をタップして[ユーザーの検索]ページに入ります。ページのIEで[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。🔍 タップして検索します。

ユーザーの編集

[ユーザー管理]ページで、ユーザーリストからユーザーを選択して[ユーザーの編集]ページに入ります。**「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。✅ をタップして設定保存します。



メモ

従業員IDは編集できません。

7.4 データ管理

データの削除、データのインポート、およびデータのエクスポートを行うことができます。

7.4.1 データの削除

ユーザーデータを削除します。

ホームページで、「**データ**」→「**データの削除**」→「**ユーザーデータ**」をタップします。デバイスに追加されたすべてのユーザーデータが削除されます。

7.4.2 データのインポート

手順

- 1.USB ラッシュドライブをデバイスに接続します。
2. ホームページで、「**データ**」→「**データのインポート**」をタップします。
- 3.「**ユーザーデータ**」、「**顔データ**」、または「**アクセス制御パラメータ**」をタップします。



メモ

インポートされたアクセス制御パラメータは、デバイスの設定要件です。

4. データをエクスポートしたときに作成したパスワードを入力します。データのエクスポート時にパスワードを作成しなかった場合は、入力ボックスに空白を残して、すぐに「OK」をタップします。



メモ

- すべてのユーザー情報を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)に転送する場合は、デバイスAからUSBラッシュドライブに情報をエクスポートしてから、USB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、プロフィールの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。

- サポートされているUSBラッシュドライブのフォーマットはFAT32です。

- インポートされた画像は、ルートディレクトリのフォルダー(enroll_picという名前)に保存する必要があり、画像の名前は以下のルールに従う必要があります。

カードNo_Name_Department_Employee ID_Gender.jpg

- フォルダ[enroll_pic]インポートされたすべての画像を保存できない場合は、ルートディレクトリの下にenroll_pic1、enroll_pic2、enroll_pic3、enroll_pic4という名前の別のフォルダを作成できます。
- 従業員IDは32文字以内にしてください。これは、下位の文字、上位の文字、および数値の組み合わせにすることができます。重複したり、0で開始したりしないでください。
- 顔写真の要件は、以下のルールに従う必要があります。顔全体を撮影する必要があります。カメラに直接向いているビュー。顔を撮るときは帽子や頭を覆わないでください。

画像形式はJPEGまたはJPGである必要があります。解像度は640×480ピクセル、または640ピクセル×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の間である必要があります。

7.4.3 データのエクスポート

手順

- 1.USB ラッシュドライブをデバイスに接続します。
2. ホームページで、「**データ → データのエクスポート**」をタップします。
3. **[顔データ]**、**[イベントデータ]**、**[ユーザーデータ]**、**または****[アクセス制御パラメータ]**をタップします。



メモ

エクスポートされたアクセス制御パラメータは、デバイスの設定要件です。

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



メモ

- サポートされているUSBラッシュドライブのフォーマットはDBです。
 - システムは、1G〜32Gのストレージを備えたUSBラッシュドライブをサポートしています。USBラッシュドライブの空き容量が512Mを超えてい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、編集することはできません。
-

7.5 識別情報認証

ネットワーク設定、システムパラメータ設定、およびユーザー設定が完了したら、ID認証のために初期ページ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人物を認証します。

7.5.1 シングル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、またはカードを認証します。

顔

カメラに向かって前方を向き、顔認証を開始します。

カード

カード提示エリアでカードを提示し、カードによる認証を開始します。



メモ

カードは、通常のICカード、または暗号化されたカードにすることができます。

PINコード

PINコードを入力して、PINコードで認証します。

認証が完了すると、「認証済み」というプロンプトがポップアップ表示されます。

7.5.2複数の認証情報を使用して認証

始める前に

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。

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、カードと顔の場合は、ライブビューページの指示に従って任意の資格情報を認証します。
-



メモ

- ・カードは通常のICカードでも暗号化カードでもかまいません。
-

2. 前回の認証後、他の認証を継続して認証します。
-



メモ

- ・顔認証の詳細については、[顔写真を収集/比較する際のヒント](#)を参照してください。
-

認証が成功すると、「認証済み」というプロンプトがポップアップ表示されます。

7.6基本設定

音声、時間、睡眠(秒)、言語、コミュニティ番号、建物番号、ユニット番号を設定できます。

初期ページを3秒間長押しし、ジェスチャーに従って左/右にスライドし、デバイスのホームページにログインします。[基本]をタップします。

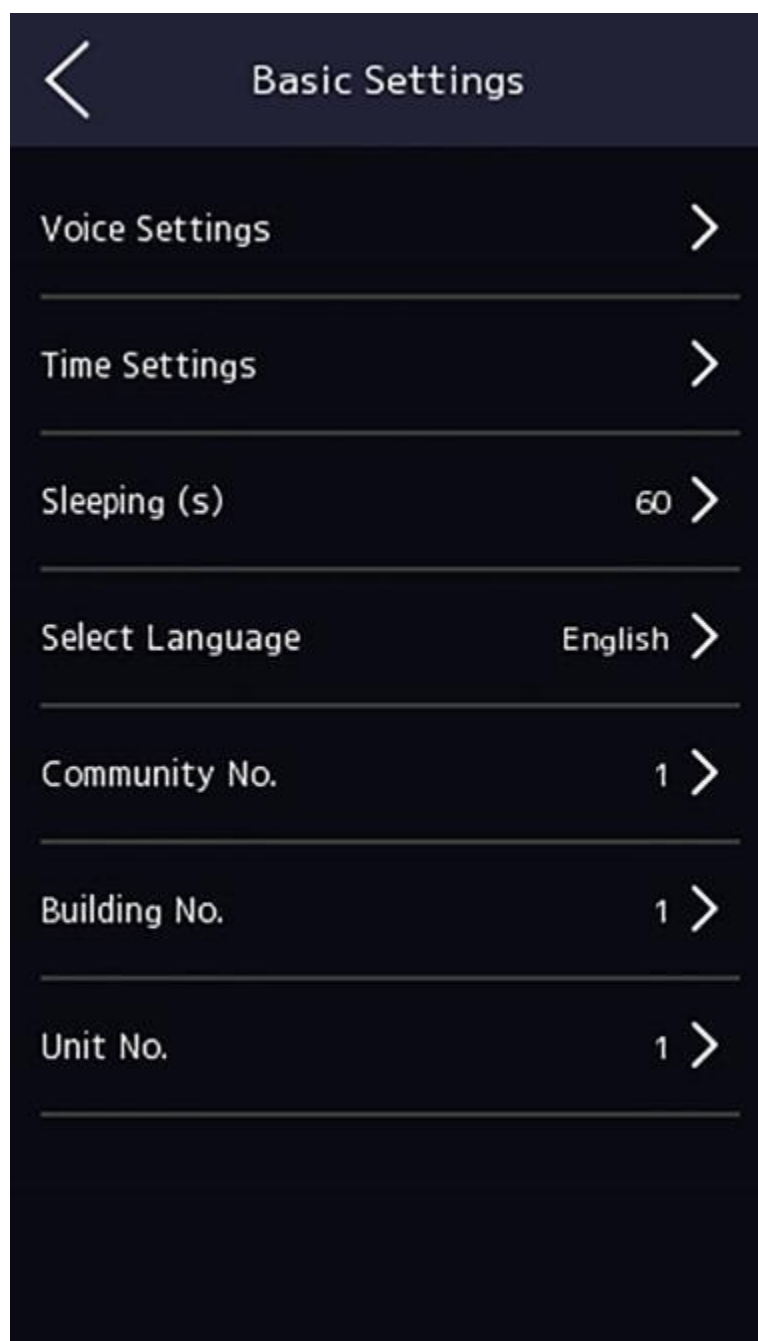


図7-10「基本設定」ページ

音声設定

音声プロンプト機能を有効/無効にしたり、音声の音量を調整したりできます。



メモ

音声の音量は0～10に設定できます。

時間設定

タイムゾーン、デバイス時刻、およびDSTを設定します。

スリーピング(秒)

デバイスのスリープ待機時間を設定します(秒)。たとえば、初期ページを表示しているときにスリープ時間を30秒に設定すると、デバイスは30秒後にスリープ状態になり、操作は行われません。



メモ

20秒から999秒まで構成できます。

言語の選択

実際のニーズに応じて言語を選択してください。

コミュニティ番号

インストールされているデバイスを設定するコミュニティ番号。

建物番号

デバイスを設置した建物番号を設定します。

ユニット番号

デバイス搭載ユニットNo.を設定します。

7.7 生体認証パラメータの設定

顔パラメータをカスタマイズして、顔認証のパフォーマンスを向上させることができます。設置可能なパラメータには、アプリケーションモード、顔の生体レベル、顔認証の選択が含まれます。

距離、顔認証間隔、顔1:Nセキュリティレベル、顔1:1セキュリティレベル、ECO 設置、マスク検出付き顔。

初期ページを3秒間長押しし、ホームページにログインします。[生体認証]をタップします。

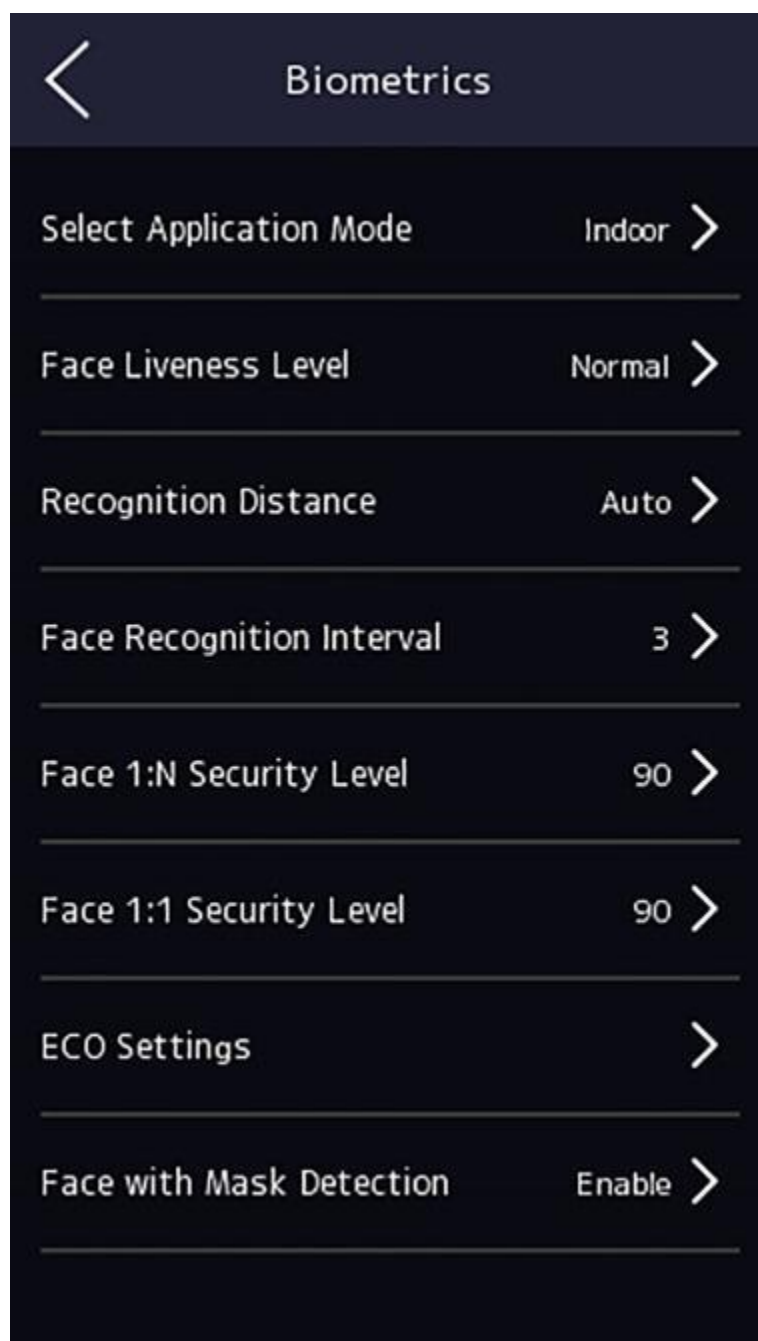



図7-11 [Biometric Parameters] ページ

表 7-1 顔画像パラメータ

パラメーター	形容
アプリモード選択	実際の環境に応じて、その他または屋内のいずれかを選択します。
顔の活性レベル	顔反スプーフィング機能を有効にした後、ライブ顔認証を実行するときに一致するセキュリティレベルを設定できます。
顔認証距離	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。
顔認証インターバル	認証時の2つの連続した顔認証の時間間隔。  メモ 1から10までの数値を入力できます。
Face 1:Nセキュリティレベル	1:N マッチングモードで認証する場合、マッチングしきい値を設定します。値が大きいほど、偽の受け入れ率は小さくなり、偽の拒否率は大きくなります。
Face 1:1セキュリティレベル	1:1 マッチングモードで認証する場合、マッチングしきい値を設定します。値が大きいほど、偽の受け入れ率は小さくなり、偽の拒否率は大きくなります。
ECO設定	ECOモードを有効にすると、デバイスはIRカメラを使用して次のことを行います。 暗い環境または暗い環境で顔を認証します。また、ECOモードのしきい値、ECOモード(1:N)、ECOモード(1:1)、Face with マスク&顔(1:1 ECO)とマスク&顔付き顔(1:N ECO)です。 ECOしきい値 ECOモードを有効にする場合は、ECOモードのしきい値を設定できます。値が大きいほど、デバイスはECOモードに入りやすくなります。 ECOモード(1:1) ECOモードで認証する際のマッチングしきい値を1:1で設定します。マッチングモード。値が大きいほど、偽の受け入れ率は小さくなり、偽の拒否率は大きくなります。 ECOモード(1:N) ECOモード1:Nで認証する場合の一致しきい値を設定します。マッチングモード。値が大きいほど、誤受理率は小さくなり、誤受理率は大きくなります。 マスク付き顔&顔(1:1 ECO)

パラメーター	形容
	<p>ECOモード1:1マッチングモード顔マスクで認証する場合のマッチング値を設定します。値が大きいほど、偽の受け入れ率は小さくなり、偽の拒否率は大きくなります。</p> <p>マスク付き顔&顔(1:N ECO)</p> <p>ECOモード1:Nマッチングモードで顔マスクで認証する場合のマッチング値を設定します。値が大きいほど、偽の受け入れ率は小さくなり、偽の拒否率は大きくなります。</p>
マスク付き顔検出	<p>マスク検出で顔を有効にすると、システムはマスク画像でキャプチャされた顔を認識します。マスクと顔1:Nレベルと戦略で顔を設定できます。</p> <p>戦略</p> <p>なし、着用のリマインダー、および着用する必要があります。戦略を設定します。</p> <p>着用のリマインダー</p> <p>認証時に顔マスクを着用していない場合、デバイスから通知が促され、ドアが開きます。</p> <p>必着</p> <p>認証時に顔マスクを着用していない場合、デバイスは通知を促し、ドアは閉じたままになります。</p> <p>なし</p> <p>認証時に顔マスクを着用していない場合、デバイスは通知を求めません。</p> <p>マスクと顔(1:1)</p> <p>顔マスク1:1で認証する際のマッチング値を設定します。 マッチングモード。値が大きいほど、偽の受け入れ率は小さくなり、偽の拒否率は大きくなります。</p> <p>マスクと顔(1:N)</p> <p>顔マスクで認証する際に1:Nで照合値を設定します。 マッチングモード。値が大きいほど、偽の受け入れ率は小さくなり、偽の拒否率は大きくなります。</p>

7.8 アクセス制御パラメータの設定

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

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

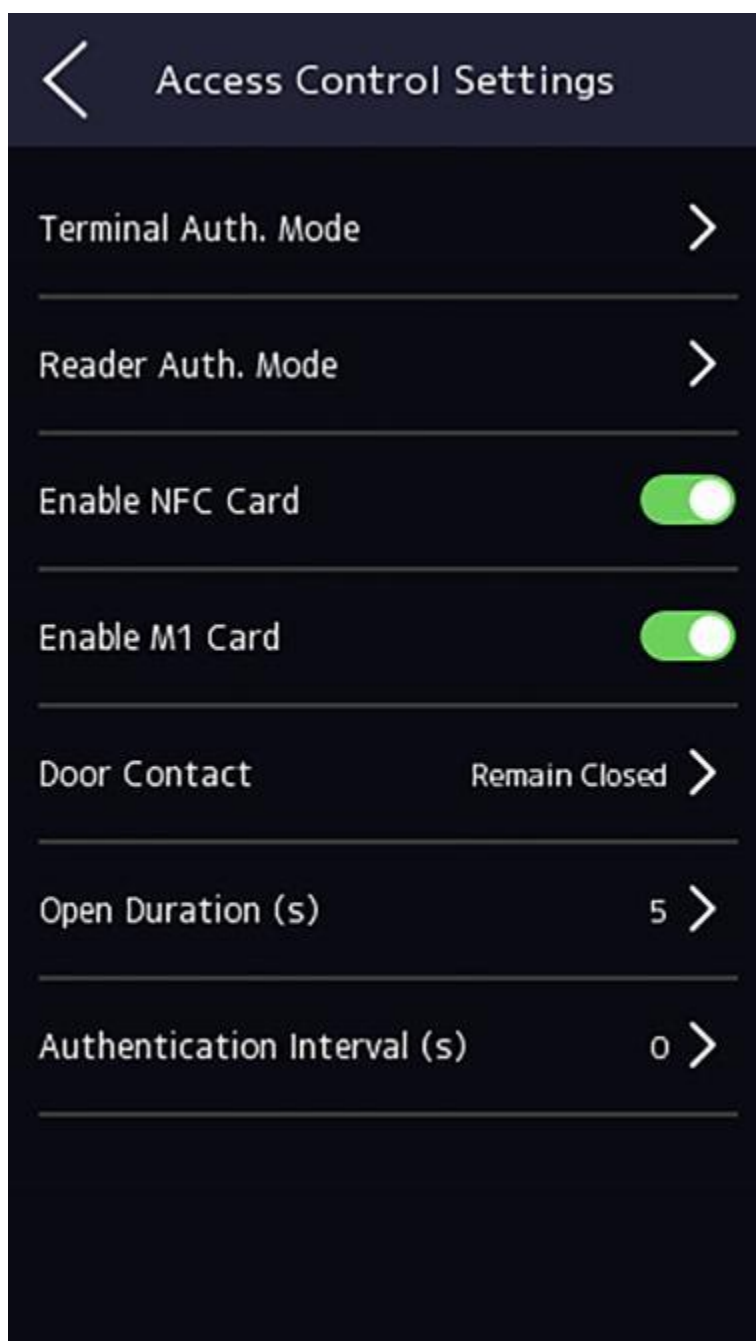



図 7-12 アクセス制御パラメータ

使用可能なパラメータ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の説明

パラメーター	形容
Terminal Auth. Mode(端末認証モード)	顔認証端末の認証モードを選択します。認証モードをカスタマイズすることもできます。  メモ <ul style="list-style-type: none"> 生体認証製品は、なりすまし防止環境に完全に適用できるわけではありません。より高いセキュリティレベルでは、複数認証モードを使用します。 複数認証モードを採用する場合は、顔認証の前に他の方法を認証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カードを有効にする	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カードを有効にする	この機能を有効にすると、M1カードを提示して認証できます。
ドアコンタクト	「オープン(開いたまま)」または「クローズ(レミアン)」を選択できます Closed)」をあなたの実際のニーズに応じて。デフォルトはClose (Remian Closed) です。
開館期間	ドアの解錠時間を設定します。ドアが開いていない場合設定された時間になると、ドアはロックされます。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。使用可能な認証間隔の範囲:0 ~ 65535。

7.9 時刻と出勤ステータスの設定

実際の状況に応じて、チェックイン、チェックアウト、ブレイクアウト、ブレイクイン、残業、残業などの勤怠モードを設定できます。



メモ

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

7.9.1 デバイスを介して出席モードを無効にする

出席モードを無効にすると、初期ページに出席ステータスが表示されなくなります。
「T&A Status」をタップして、「T&A Status」ページに入ります。

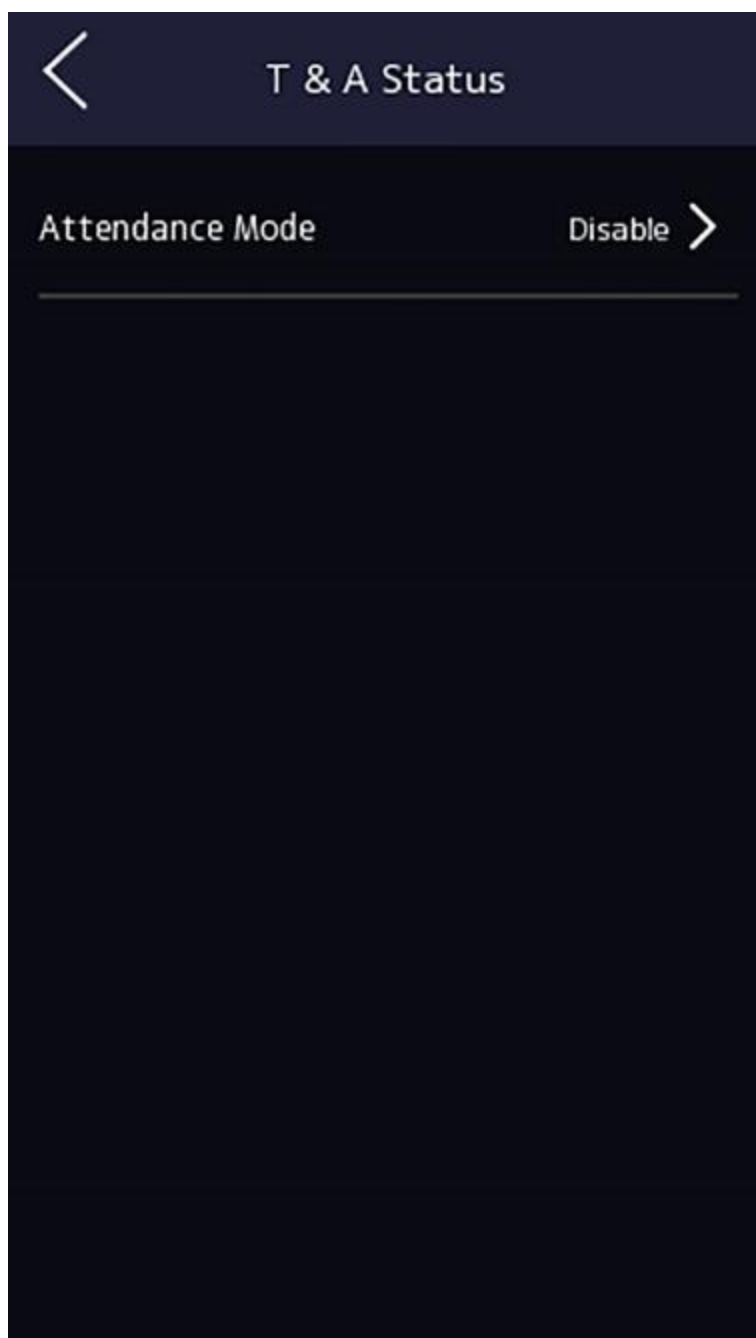


図7-13 出席モードの無効化

[出席モード]を[無効]に設定します。

初期ページで出席ステータスを表示または構成することはできません。また、システムはプラットフォームで設定された出席ルールに従います。

7.9.2 デバイスによる手動出席の設定

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

始める前に

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. 「T&Aステータス」をタップして、「T&Aステータス」ページに入ります。
2. 出席モードを手動に設定します。

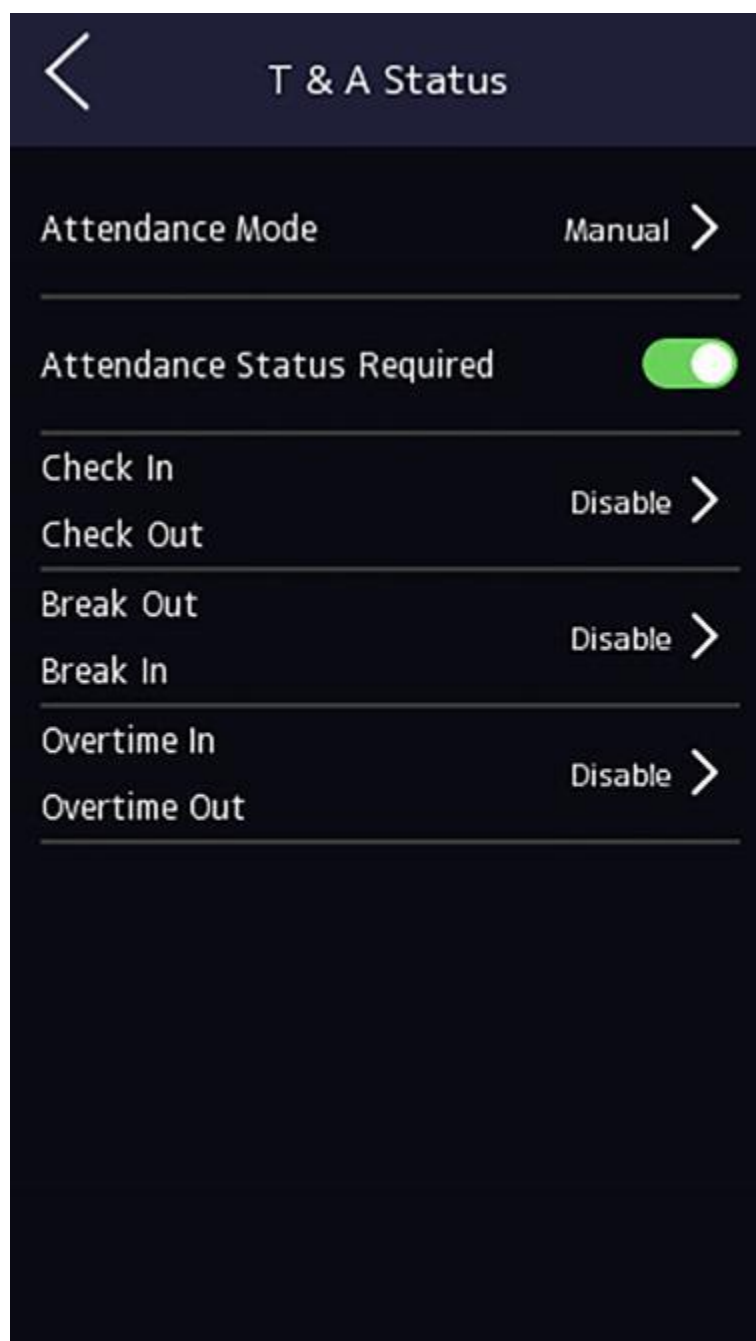


図7-14 手動出席モード

3. 「必要な出席ステータス」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。



メモ

アテンダントプロパティは変更されません。

5. オプション: ステータスを選択し、必要に応じて名前を変更します。
-

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、出席状況を手動で選択する必要があります。



メモ

ステータスを選択しない場合、認証は失敗し、有効な出席としてマークされません。

7.9.3 デバイスによる自動出席の設定

勤怠モードを自動に設定すると、勤怠状況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状況を自動的に変更します。

始める前に

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. 「T&Aステータス」をタップして、「T&Aステータス」ページに入ります。
2. 出席モード を自動に設定します。

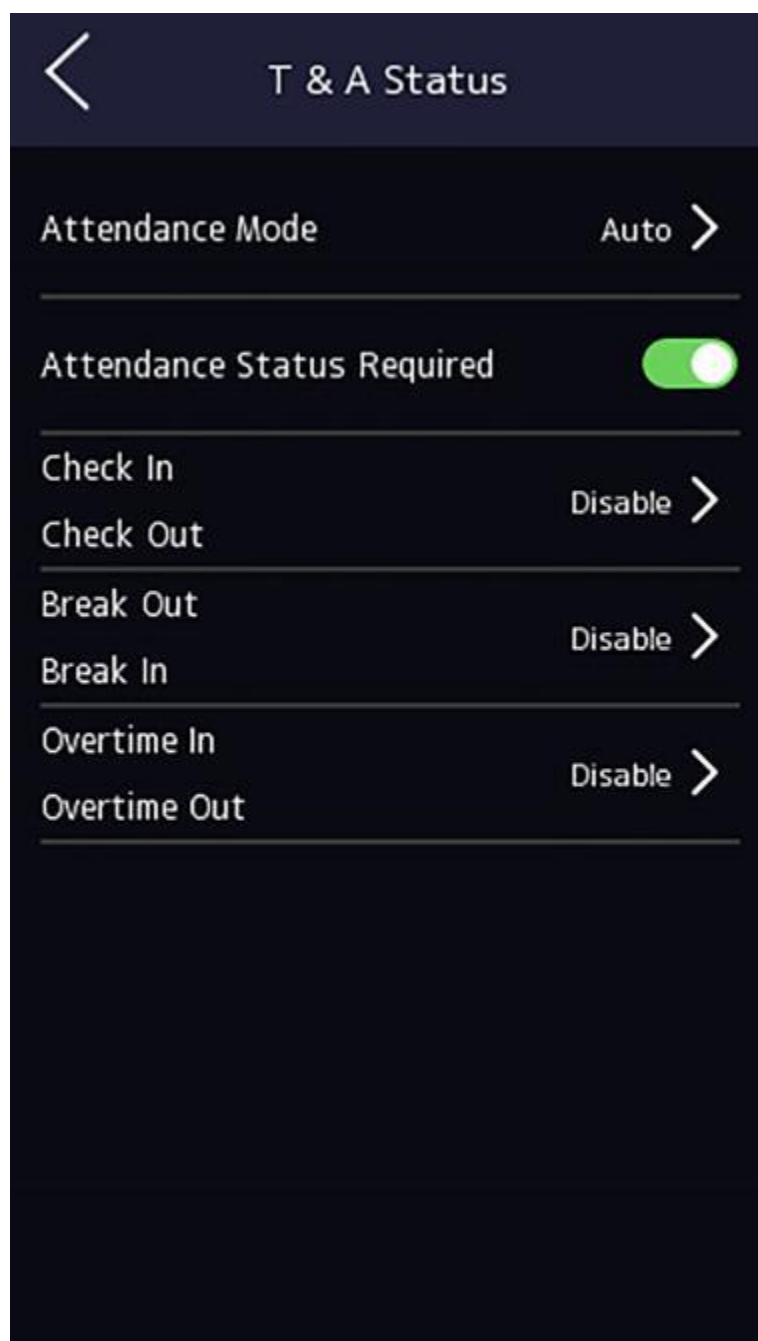


図7-15 自動出席モード

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



メモ

アテンダントプロパティは変更されません。

5. オプション: ステータスを選択し、必要に応じて名前を変更します。

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]をタップする
 - 2)月曜日、火曜日、水曜日、木曜日、金曜日、土曜日、または日曜日を選択します。
 - 3)選択した出席状況のその日の開始時間を設定します。
 - 4)[確認]をタップ
 - 5)実際のニーズに応じて、手順1〜4を繰り返します。
-



メモ

出席状況は、設定されたスケジュール内で有効になります。

結果

初期ページで認証すると、認証は設定された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。

例

[ブレイクアウト]を[月曜日 11:00]に設定し、[ブレイクイン]を[月曜日 12:00]に設定すると、月曜日の11:00から12:00までの有効なユーザーの認証がブレイクとしてマークされます。

7.9.4 デバイスによる手動および自動出席の設定

出席モードを手動および自動に設定すると、システムは設定されたスケジュールに従って自動的に出席ステータスを変更します。同時に、認証後に出席ステータスを手動で変更できます。

始める前に

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. 「T&Aステータス」をタップして、「T&Aステータス」ページに入ります。
2. 出席モードを手動と自動に設定します。

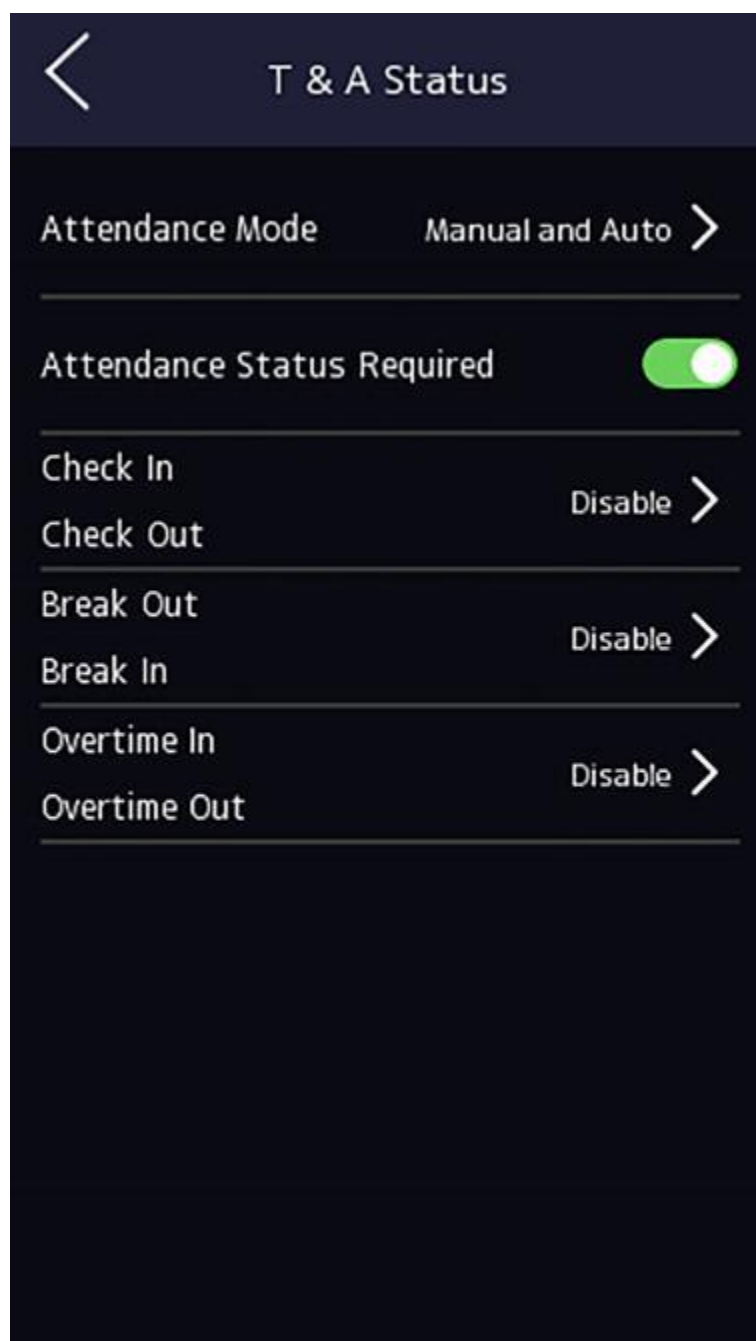


図7-16 手動モードと自動モード

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



メモ

アテンダントプロパティは変更されません。

5. オプション: ステータスを選択し、必要に応じて名前を変更します。

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]をタップする
 - 2)月曜日、火曜日、水曜日、木曜日、金曜日、土曜日、または日曜日を選択します。
 - 3)選択した出席状況のその日の開始時間を設定します。
 - 4)[OK]をタップする
 - 5)実際のニーズに応じて、手順1〜4を繰り返します。
-



メモ

出席状況は、設定されたスケジュール内で有効になります。

結果

初期ページで認証します。認証は、構成されたものとしてマークされます。

スケジュールに応じた出席状況。結果タブの編集アイコンをタップすると、手動で出席を取るステータスを選択でき、認証は編集済みとしてマークされます。

出席ステータス。

例

[ブレイクアウト] を [月曜日 11:00] に設定し、[ブレイクイン] を [月曜日 12:00] に設定すると、月曜日の 11:00 から 12:00 までの有効なユーザーの認証がブレイクとしてマークされます。

7.10 設定

プリファレンス設定パラメータを設定できます。

手順

- 1.[基本設定]→[設定]をタップして、設定ページに入ります。

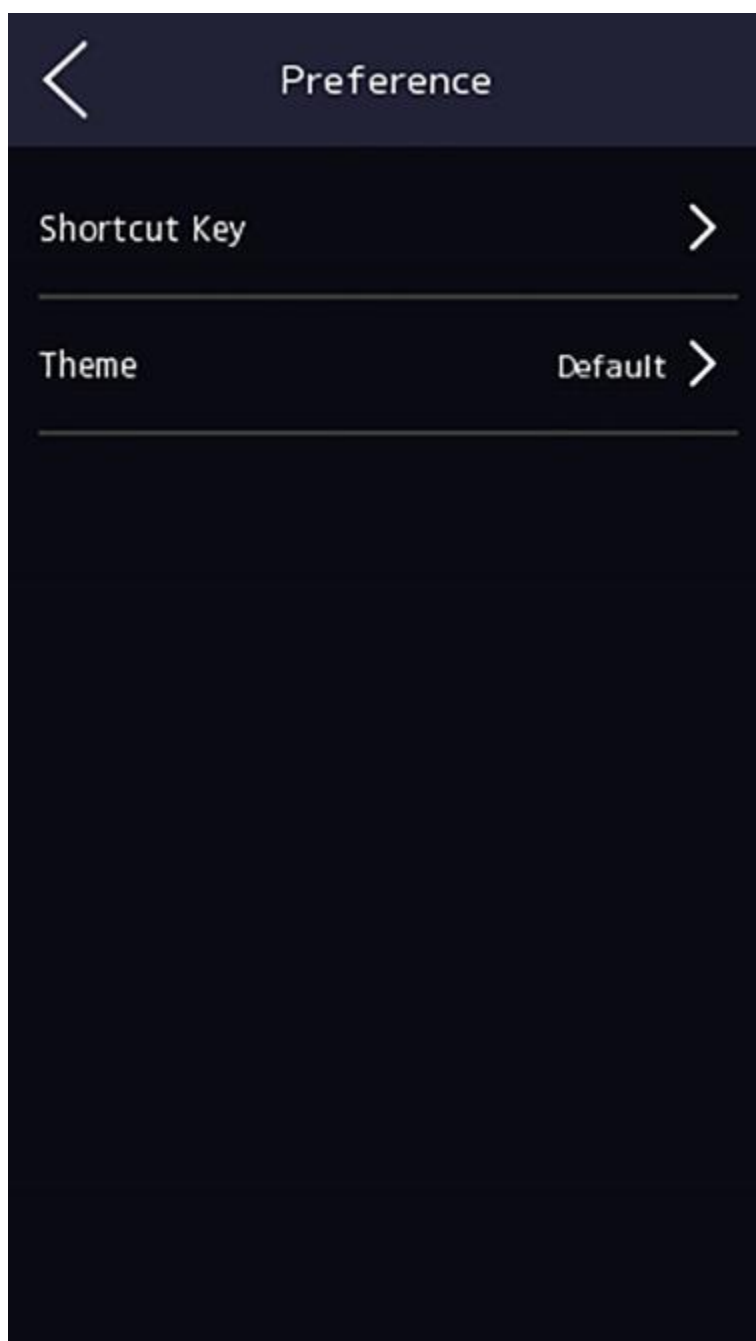


図7-17 プリファレンス設定

ショートカットキー

認証ページに表示されるショートカットキー(QRコード機能、通話機能、通話タイプ、パスワード入力機能など)を選択します。

メモ

コールタイプは、**コールルーム**、**コールセンター**、**コール指定ルーム番号**から選択できます。と [APPの呼び出し] をクリックします。

コールルーム

認証ページの通話ボタンをタップしたら、部屋番号をダイヤルする必要があります。電話します。

コールセンター

認証ページの通話ボタンをタップすると、センターに直接電話をかけることができます。

指定の部屋番号に電話してください

部屋番号を設定する必要があります。認証ページの通話ボタンをタップすると、ダイヤルせずに設定したルームに直接通話できます。

APPを呼び出す

認証ページの通話ボタンをタップすると、デバイスが追加されたモバイルクライアントに電話がかかります。

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パスワードで認証できます。

QRコード

認証インターフェースのQRコードスキャン機能を使用できます。デバイスは、取得したQRコードに関連付けられた情報をプラットフォームにアップロードします。

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。**テーマをデフォルト/シンプルとして**選択できます。「**シンプル**」を選択すると、認証ページのライブビューが無効になり、その間、本人の名前、従業員ID、顔写真はすべて非表示になります。

7.11 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表示できます。また、システムを工場出荷時の設定、デフォルトの設定に復元し、APPアカウントのリンクを解除して、システムを再起動することもできます。

初期ページを3秒間長押しし、ホームページにログインします。[メンテナンス]をタップします。

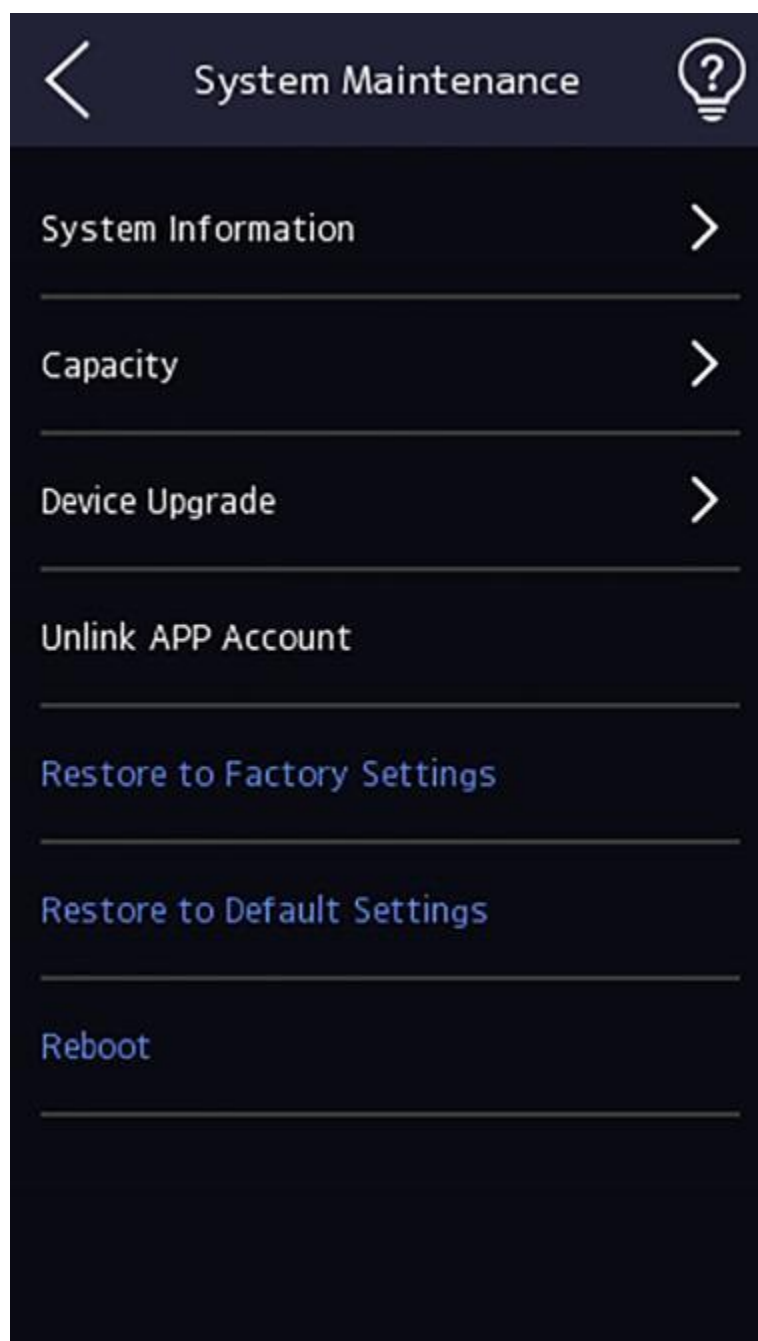


図7-18 メンテナンス・ページ

システム情報

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



ページは、デバイスのモデルによって異なる場合があります。詳細は実際のページを参照しています。

能力

管理者、ユーザー、顔写真、カード、およびイベントの数を表示できます。



詳細は実際のページを参照しています。

アップグレード

USBラッシュドライブをデバイスのUSBインターフェースに接続します。**[アップグレード]→[OK]**をタップすると、デバイスはUSBラッシュドライブの *digicap.dav* ファイルを読み取り、アップグレードを開始します。

APPアカウントのリンクを解除します

Connectアカウントをプラットフォームからリンク解除します。

ファクトリへの復元



すべてのパラメータは工場出荷時の設定に復元されます。システムが再起動して効果を発揮します。

デフォルトに復元

通信設定を除くすべてのパラメータ、リモートでインポートされたユーザー情報は、デフォルトの設定に復元されます。システムが再起動して効果を発揮します。

リブート

確認後、デバイスが再起動します。

 を長押し  し、管理者パスワードを入力してビューデバイスのバージョン情報を表示します。

第8章 モバイルブラウザを使用したデバイスの構成

8.1 ログイン

モバイルブラウザからログインできます。



- モデルの一部はWi-Fi設定をサポートしています。
- デバイスがアクティブ化されていることを確認してください。

Wi-Fiを有効にした後、デバイスからIPアドレスを取得します。デバイスとコンピューターのIPセグメントが同じであることを確認してください。詳細については、[Wi-Fiパラメータの設定を参照してください](#)。

モバイルブラウザのアドレスバーにデバイスのIPアドレスを入力し、**Enter**キーを押してログインページに入ります。

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

8.2 検索イベント

[検索]をクリックして**[検索]**ページに入ります。

社員ID、氏名、カード番号、開始時刻、終了時刻などの検索条件を入力し、**[検索]**をクリックします。



32桁以内の名前の検索をサポートします。

結果がリストに表示されます。

8.3 ユーザー管理

モバイルWebブラウザからユーザーを追加、編集、削除、検索できます。

手順

- 1) **[ユーザー]**をタップして設定ページに入ります。
2. ユーザーを追加します。

- 1) 「+」をタップします。

Add Person		
Basic Information		
* Employee ID		
Name		
Gender	none >	
User Role	Normal User >	
Face	0 >	
Fingerprint	0 >	
Start Date		2021-06-28 >
End Date		2031-06-28 >
Administrator	<input type="checkbox"/>	
Authentication Settings		
Authentication Type	The Same Device >	
Save		

図8-1 ユーザーの追加

2) 以下のパラメータを設定します。

従業員 ID

従業員IDを入力します。従業員IDは0または32文字を超えることはできません。これは、大文字、小文字の文字、および数字の組み合わせにすることができます。

名前

名前を入力します。名前は、数字、大文字と小文字の英語、および文字をサポートします。名前は32文字以内にするをお勧めします。

ユーザーロール

ユーザーロールを選択します。

階番号/部屋番号

部屋番号/部屋番号を入力してください。

顔

顔写真を追加します。「顔」をタップし、「読み込み」をタップして、顔を読み込むモードを選択します。

開始日/終了日

ユーザー権限の開始日と終了日を設定します。

管理者

ユーザーを管理者として設定する必要がある場合は、管理者を有効にすることができます。

認証の種類

認証タイプを設定します。

3)[保存]をタップ

- 3.ユーザー一覧で編集が必要なユーザーをタップし、情報を編集
- 4.ユーザー一覧で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
- 5.検索バーに従業員IDまたは名前を入力して、ユーザーを検索できます。

8.4 設定

8.4.1 ビューデバイス情報

ビューデバイス名、言語、モデル、シリアル番号、QRコード、バージョンなど。

[設定]→[システム]→[システム設定]→[基本情報]をタップして、設定ページに入ります。デバイス名、言語、モデル、シリアル番号、QRコード、バージョンなどを表示できます。

8.4.2 時間設定

タイムゾーン、時刻同期を設定します。モード、および表示時間。

[システム]→[設定]→[時間設定]をタップして、設定ページに入ります。

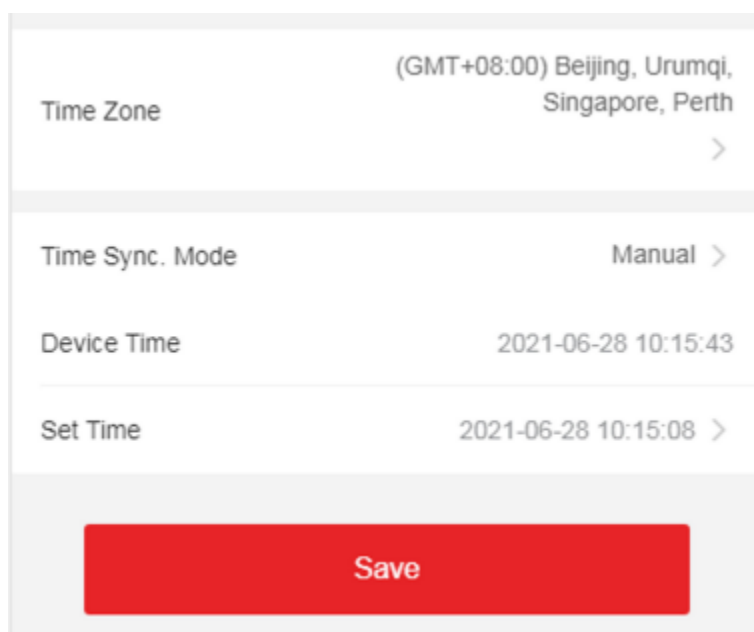


図8-2 時間設定

[保存]をタップして 設定を保存します。

時間帯

ドロップダウンリストから、デバイスが配置されているタイムゾーンを選択します。

タイムシンクモード

手動

デフォルトでは、デバイスの時刻は手動で同期する必要があります。デバイスの時刻は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 ビュー オープンソースソフトウェアライセンス

「システム設定」→「システム設定」→「バージョン情報」→タップし、「ライセンスの表示」をタップしてデバイスのライセンスを表示します。

8.4.4 ネットワーク設定

ポートとWi-Fiのパラメータを設定できます。

ポートパラメータの設定

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

[構成]→[ネットワーク]→[基本設定]→[ポート]の順にタップして、設定ページに入ります。

HTTP

これは、ブラウザがデバイスにアクセスするときに使用するポートを指します。たとえば、HTTPポートが81に変更された場合、ログインするにはブラウザにhttp://192.0.0.65:81と入力する必要があります。

RTSP

これは、リアルタイムストリーミングプロトコルのポートを指します。

HTTPS

ブラウザにアクセスするためのHTTPSを設定します。アクセス時には証明書が必要です。

サーバー

これは、クライアントがデバイスを追加するときに使用するポートを指します。

Wi-Fiパラメータの設定

デバイスのワイヤレス接続のWi-Fiパラメータを設定します。

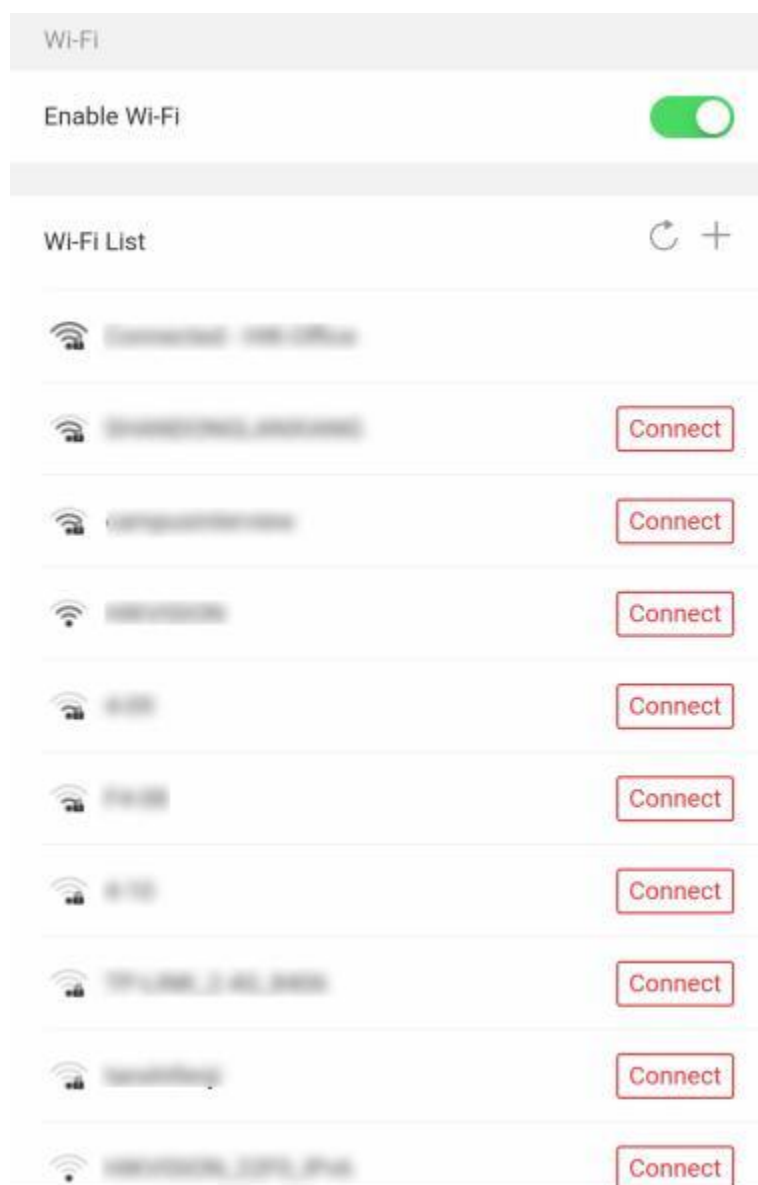
手順



メモ

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. [ネットワーク]→[基本設定]→[Wi-Fi]の順にタップして、設定ページに入ります。
2. [Wi-Fiを有効にする]をオンにします。



☒ 8-3 Wi-Fi

3.Wi-Fiを追加します。

1. [+]をタップ

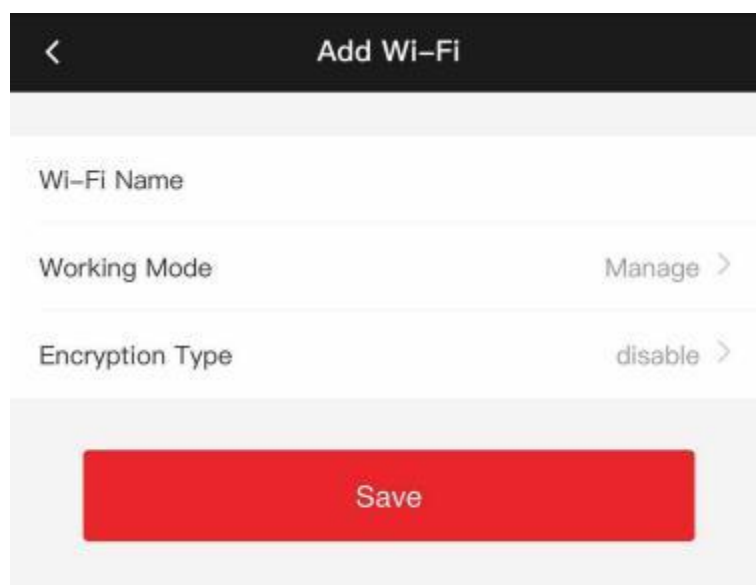


図84 Wi-Fiの追加

2. Wi-Fi名と Wi-Fiパスワードを入力し、[作業モード]と[暗号化タイプ]を選択します。
3. [保存]をタップ
4. Wi-Fi名を選択し、[接続]をタップ
5. パスワードを入力し、[保存]をタップ
6. WLANパラメータを設定します。
 - 1) IPアドレス、サブネットマスク、ゲートウェイを設定します。または、DHCPを有効にすると、システムはIPアドレス、サブネットマスク、およびゲートウェイを自動的に割り当てます。
 - 2) [保存]をタップ

8.4.5 一般設定

認証パラメータの設定

認証パラメータを設定します。

手順

1. [設定]→[基本設定]→[認証設定]をタップします。

Device Type	Main Card Reader >
Card Reader Type	fingerPrint/Face
Card Reader Description	
Enable Card Reader	<input checked="" type="checkbox"/>
Authentication	Card or Face or Fingerprint >
Recognition Interval(s)	1
Minimum Card Swiping Interval(s)	22
Alarm of Max. Failed Attempts	<input type="checkbox"/>
Max. Authentication Failed Attempts	5
Enable Tampering Detection	<input checked="" type="checkbox"/>
Enable Card No. Reversing	<input type="checkbox"/>
Enable Tampering Detection	<input checked="" type="checkbox"/>
Enable Card No. Reversing	<input type="checkbox"/>
<input type="button" value="Save"/>	

図8-5 認証設定

2. [保存]をタップ

デバイスタイプ

メインカードリーダー

デバイスカードリーダーのパラメータを設定できます。メインカードリーダーを選択した場合は、次のパラメータを設定する必要があります: **カードリーダータイプ**、**カードリーダーの説明**、**カードリーダーを有効にする**、**認証**、**認識間隔(秒)**、**最小カードスワイプ間隔(秒)**、**最大認証失敗試行アラーム/最大失敗試行のアラーム**、**改ざん検出を有効にする**、**カード番号を有効にする逆転**

サブカードリーダー

接続された周辺機器のカードリーダーのパラメータを設定できます。

サブカードリーダーを選択する場合は、以下のパラメータを設定する必要があります。**カードリーダータイプ**、**カードリーダーの説明**、**カードリーダーの有効化**、**認証**、**認識間隔(秒)**、**認証失敗試行アラーム/最大失敗試行のアラーム**、**改ざん検出を有効にする**、**コントローラーとの通信ごと(s)**、および**パスワード入力時の最大間隔**

カードリーダーの種類

カードリーダータイプを取得します。

カードリーダーの説明

カードリーダーの説明を取得します。読み取り専用です。

カードリーダーを有効にする

カードリーダーの機能を有効にします。

認証

ドロップダウンリストから実際のニーズに応じて認証モードを選択します。

認識間隔

同じカードのカード提示間隔が設定値より短い場合、カード提示は無効です。間隔の時間範囲は0秒から255秒です(0に設定すると、認識間隔は無効ではなく、同じ認証を無制限に使用できます)。

認証間隔

認証時に同一人物の認証間隔を設定できます。同じ人物は、設定された間隔で1回だけ認証できます。2回目の認証は失敗します。

最大認証失敗試行アラーム/最大失敗試行数のアラーム

カードの読み取り試行が設定値に達したときにアラームを報告するように有効にします。

改ざん検出を有効にする

カードリーダーの改ざん防止検出を有効にします。

カード番号を有効にする反転

読み込んだカード番号機能を有効にすると、逆の順序でなります。

コントローラーとの通信間隔(秒)

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

パスワード入力の最大間隔(秒)

カードリーダーでパスワードを入力するとき、2つ押す間隔が番号が設定値より長い場合、前に押した番号は自動的にクリアされます。

プライバシーパラメータの設定

イベントのストレージタイプ、画像のアップロードと保存のパラメータ、および画像のクリアパラメータを設定します。

「設定」→「一般設定」→「プライバシー」をタップします。

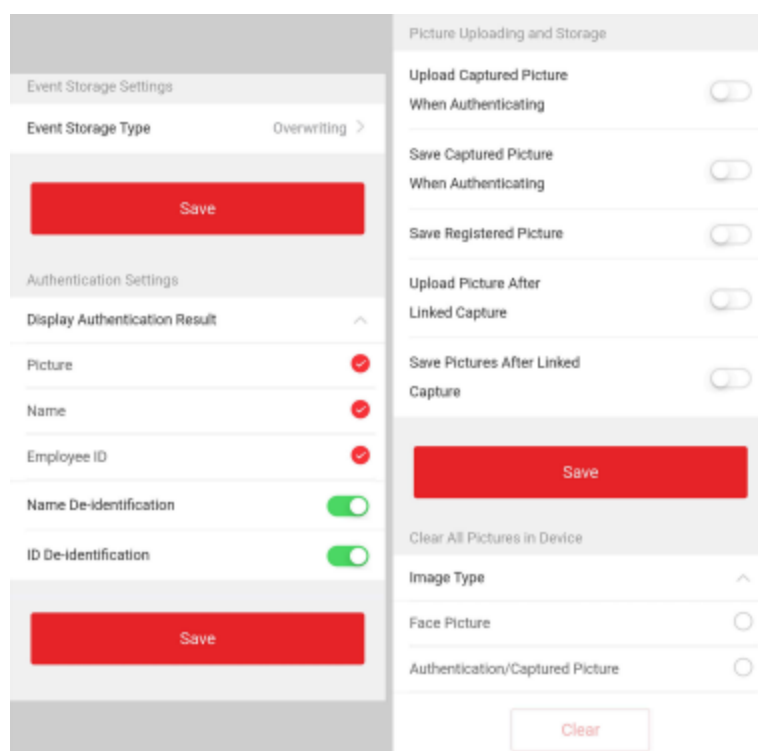


図8-6 プライバシー設定

イベントストレージ設定

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

古いイベントを定期的に削除

イベントデイティングの期間を設定するための数値を入力します。すべてのイベントは、設定された期間に従って削除されます。

指定した時間で古いイベントを削除

時間を設定すると、設定された時間にすべてのイベントが削除されます。

上書き

保存されたイベントが全スペースの 95% を超えたことをシステムが検出すると、最も古い 5% のイベントが削除されます。

認証設定

認証結果の表示

顔写真、名前、または従業員IDを確認してください。認証が完了すると、選択した内容が結果に表示されます。

名前の匿名化

名前情報はアスタリスクで鈍感化されます。

IDの匿名化

ID情報は、アスタリスクで感度が鈍化されます。

画像のアップロードと保存

写真をアップロードして保存できます。

認証時にキャプチャした画像をアップロードする

認証時に撮影した写真をプラットフォーム自動的にアップロードします。

認証時にキャプチャした画像を保存する

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する

登録した顔写真は、機能を有効にするとシステムに保存されます。

写真のアップロード After Linked Capture

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自動的にアップロードします。

写真を保存する After リンクされたキャプチャ

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

デバイス内のすべての画像をクリアする

デバイスに登録した顔写真やキャプチャした画像を消去できます。

登録された顔写真をクリア

「顔の画像」を選択し、「消去」をタップします。デバイスに登録されている。

認証/キャプチャされた画像をクリア

「認証/キャプチャー画像」を選択し、「クリア」をタップします。デバイス内のすべての認証/キャップ画像が削除されます。

セットカードセキュリティ

[設定]→[一般設定]→[カードセキュリティ]をタップして、設定ページに入ります。

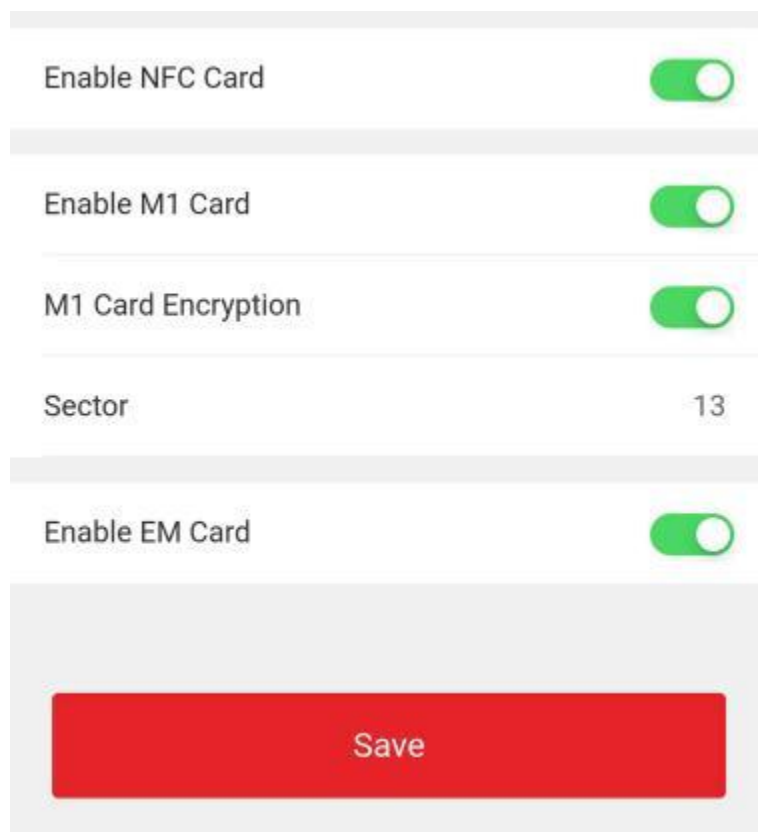


図8-7 カードのセキュリティ

パラメータを設定し、[保存]をクリックします。

NFCカードを有効にする

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

M1カードを有効にする

M1カードを有効にし、M1カードを提示して認証することができます。

M1カードの暗号化

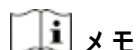
M1カードの暗号化により、認証のセキュリティレベルを向上させることができます。

セクター

機能を有効にし、暗号化セクタを設定します。デフォルトでは、セクター13は暗号化されています。セクター13を暗号化することをお勧めします。

EMカードを有効にする

EMカードを有効にし、EMカードを提示して認証することができます。



メモ

周辺機器カードリーダーがEMカードの表示をサポートしている場合、この機能は次のものもサポートされています。
EMカード機能を有効/無効にします。

CPUカードを有効にする

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

CPUカードの読み取り内容

CPUカードコンテンツ読み取り機能を有効にすると、デバイスはCPUカードコンテンツを読み取ることができます。

IDカードを有効にする

IDカードを有効にし、IDカードを提示して認証することができます。

カード認証パラメータの設定

デバイス上でカードによる認証を行う際のカード読み取り内容を設定します。 [設定]→[基本設定]→[カード認証設定]をタップします。

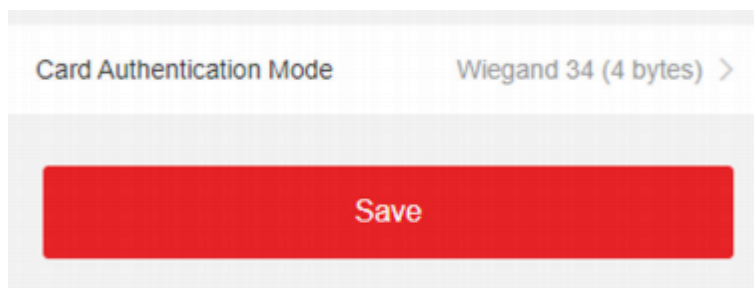


図8-8 [Card Authentication] ページ

カード認証モードを選択し、[保存]をタップします。

フルカード番号

すべてのカード番号が読まれます。

ウィーガンド 26(3 バイト)

デバイスは、ウィーガンド26プロトコル(3バイトの読み取り)を介してカードを読み取ります。

ウィーガンド 34(4 バイト)

デバイスは、ウィーガンド34プロトコル(4バイトの読み取り)を介してカードを読み取ります。

8.4.6 面パラメータ設定

面パラメータを設定します。

Face Parameters 設定

[Smart → Intelligent Parameter] → [Configuration] をタップします。

Face Anti-spoofing	<input checked="" type="checkbox"/>	Face with Mask Detection	<input checked="" type="checkbox"/>
Live Face Detection Security Level	Normal >	Face without Mask Strategy	None >
Recognition Distance	Auto >	Face with Mask&Face (1:1)	68
Application Mode	Indoor >	Face with Mask 1:N Matching Threshold	80
Face Recognition Mode	Normal Mode >	Face with Mask&Face (1:1 ECO)	78
Continuous Face Recognition Interval(s)	3	Face with Mask 1:N Matching Threshold (ECO Mode)	70
1:1 Matching Threshold	90	ECO Mode	<input checked="" type="checkbox"/>
1:N Matching Threshold	90	ECO Mode Threshold	4
Face Recognition Timeout Value(s)	3	1:1 Matching Threshold	80
		1:N Matching Threshold	80

Save

図8-9 面パラメータ

メモ

機能は、異なるモデルによって異なります。詳細については、実際のデバイスを参照してください。

顔認証のなりすまし防止

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

ライブ顔検出のセキュリティレベル

顔スプーフィング対策機能を有効にした後、ライブ顔認証を実行する際の照合セキュリティレベルを設定できます。

認識距離

認証するユーザーとデバイスのカメラとの距離を選択します。

アプリモード

実際の環境に応じて、屋内またはその他を選択します。屋外のシーン、窓際の屋内のシーン、または環境が悪い場合は、その他を選択できます。



メモ

デバイスが他のツールによってアクティブ化されていない場合、デバイスはデフォルトで環境モードとして屋内を使用します。

顔認証モード:ノーマ

ルモード

このデバイスは、カメラを使用して顔認証を行います。

ディープモード

より複雑な環境に適用でき、認識される人の範囲が広がります。



メモ

- 2モードを相互に互換性を持つことはできません。モードを選択したら変更しないでください。モードを変更すると、前のモードのすべての顔写真がクリアされます。
 - ディープモードでは、デバイスまたは登録ステーションのユーザー追加機能を介してのみ顔写真を追加できます。写真による顔写真の追加はサポートされていません。
-

このデバイスは、カメラを使用して顔認証を行います。

連続顔認証間隔 (秒)

認証時に2回連続した顔認証の時間間隔を設定します。



メモ

値の範囲:1 ~ 10

1:1マッチングしきい値

1:1マッチングモードで認証する場合、マッチングしきい値を設定します。値が大きいほど、偽の受け入れ率は小さくなり、偽の拒否率は大きくなります。

1:N マッチングしきい値

1:N マッチング モードで認証する場合、マッチングしきい値を設定します。値が大きいほど、偽の受け入れ率は小さくなり、偽の拒否率は大きくなります。最大値は 100 です。

。

顔認証タイムアウト値 (秒)

顔認証のタイムアウト期間を設定します。顔認証時間が設定値を超えると、デバイスは顔認証タイムアウトを促します。

マスク付き顔検出

マスク検出で顔を有効にすると、システムはマスク画像でキャプチャされた顔を認識します。mask1:N一致しきい値、そのECOモード、および戦略

なし

認証時に顔マスクを着用していない場合、デバイスは通知を求めません。

着用のリマインダー

認証時に顔マスクを着用していない場合、デバイスから通知が促され、ドアが開きます。

必着

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

マスクと顔(1:1)

顔マスクで1:1マッチングモードで認証する場合、マッチング値を設定します。値が大きいくほど、偽の受け入れ率は小さくなり、偽の拒否率は大きくなります。

マスク付き顔 1:N マッチングしきい値

1:Nマッチングモードを介して顔マスクで認証する場合のマッチングしきい値を設定します。値が大きいくほど、偽の受け入れ率は小さくなり、偽の拒否率は大きくなります。

マスク付き顔&顔(1:1 ECO)

ECOモード1:1マッチングモードで顔マスクで認証する場合のマッチング値を設定します。値が大きいくほど、偽の受け入れ率は小さくなり、偽の拒否率は大きくなります。

マスク付き顔 1:N マッチングしきい値 (ECO モード)

ECOモード1:Nマッチングモードを介して顔マスクで認証する場合のマッチングしきい値を設定します。値が大きいくほど、偽の受け入れ率は小さくなり、偽の拒否率は大きくなります。

ECOモード

ECOモードを有効にすると、デバイスはIRカメラを使用して、暗い環境または暗い環境で顔を認証します。また、ECOモードしきい値、ECOモード(1:1マッチングしきい値)、およびECOモード(1:Nマッチングしきい値)を設定できます。

ECOモードしきい値

ECOモード、1:1マッチングモード、およびECOで認証する際のマッチングしきい値の設定モード1:Nマッチングモード。

1:1マッチングしきい値

ECOモード1:1マッチングモードで認証する場合、マッチングしきい値を設定します。値が大きいほど、偽の受け入れ率は小さくなり、偽の拒否率は大きくなります。

1:N マッチングしきい値

ECOモード1:Nマッチングモードで認証する場合、マッチングしきい値を設定します。値が大きいほど、偽の受け入れ率は小さくなり、偽の拒否率は大きくなります。最大値は100です。

認識領域の設定

[設定]→[スマート→エリア設定]をタップしてページに入ります。

ライブ動画の青い枠をドラッグして、認識領域を調整します。エリア内の顔のみがシステムで認識できます。

スライダーをドラッグして、顔認証の有効領域を構成します。[保存]をタップして設定を保存します。

8.4.7 ビデオインターホン設定

デバイスIDの設定

このデバイスは、ドアステーション、アウトードアステーション、またはアクセス制御デバイスとして使用できます。デバイスIDは、使用前に設定してください。

デバイスID設定

[設定]→[インターコム]→[デバイスID設定]をタップします。

デバイスタイプを[ドアステーション]または[アクセス制御デバイス]に設定した場合、ドアNo.とドアステーションNo.を設定できます。

[保存]をタップして、設定後の設定を保存します。

Device Type	Access Control Device >
Floor No.	1 >
Door Station No.	0

Save

図8-10 デバイスID設定(ドアステーション)

デバイスタイプ

ST-DW XK1T342顔認証端末ユーザーマニュアル

このデバイスは、ドアステーション、アウトードアステーション、またはアクセス制御デバイスとして使用できます。ドロップダウンリストからデバイスタイプを選択します。



メモ

デバイスの種類を変更した場合は、デバイスを再起動する必要があります。

フロア番号

デバイスの取り付け場所を設定します 階No.

ドアステーションNo.

デバイスの取り付け場所を設定します 階No.



メモ

No.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。

デバイスタイプを[アウトードアステーション]に設定すると、アウトードアステーションNoを設定できます。

Device Type	Door Station >
Floor No.	3 >
Door Station No.	1
Community No.	0

Save

図8-11 デバイスID設定(アウトードアステーション)

アウトードアステーションNo.

デバイスタイプとしてアウトードアステーションを選択した場合は、1~99の番号を入力する必要があります。



メモ

No.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。

SIPパラメータの設定

デバイスのIPアドレスとSIPサーバーのIPアドレスを設定します。パラメータを設定した後、次のことができます

アクセス制御デバイス、ドアステーション、屋内ステーション、メインステーション、およびプラットフォーム間で通信します。



メモ

アクセス制御デバイスとその他のデバイスまたはシステム(ドアステーション、屋内ステーション、メインステーション、プラットフォーム)が同じIPセグメントにある場合、双方向オーディオを実行できます。

[設定]→[インターコム]→[リンク ネットワーク設定]をタップします。

Device Type	Access Control Device >
VideoIntercom Server IP	0.0.0.0
Main Station IP	0.0.0.0

Save

図8-12 リンク ネットワークの設定

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

ボタンを押して電話をかける

手順

- 1.[設定]→[インターコム]をタップし→ボタンを押して電話して設定ページに入ります。
2. ボタンを通話に設定します。
 - 「屋内ステーションに電話する」にチェックを入れ、「インドアステーションNo」に設定して、ボタンを「インドアステーションに電話する」に設定します。
 - [Call Management Center] をオンにして、ボタンを [Call Management Center] 設定します。

8.4.8 アクセス制御設定

ドアパラメータの設定

「設定」→「アクセス制御」→「ドアパラメータ」をタップします。

Door No.	Door1 >
Name	
Open Duration(s)	5
Door Open Timeout Alarm(s)	30
Door Contact	Remain Closed >
Exit Button Type	Remain Open >
Door Lock Powering Off	Remain Closed >
Extended Open Duration(s)	15
Door Remain Open Duration with First Person(m)	10
Duress Code
Super Password
<div style="text-align: center;"><input type="button" value="Save"/></div>	

図8-13 ドア・パラメータ設定ページ

[保存]をクリックして、設定後の設定を保存します。

ドア番号

対応ドアNo.に対応したデバイスを選択します。

名前

ドアの名前を作成できます。

開館期間

ドアの解錠時間を設定します。設定した時間内にドアを開けないと、ドアは施錠されます。

オープンタイムアウトアラームによる

設定された時間内にドアが閉じられなかった場合、アラームがトリガーされます。

ドアコンタクト

ドアの接点は、**実際のニーズに応じて開いたまままたは閉じたままに設定**できます。デフォルトでは、**閉じたまま**です。

終了ボタンの種類

実際のニーズに応じて、終了ボタンを**開いたままにするか、閉じたままにするか**を設定できます。デフォルトでは、**開いたまま**になっています。

ステータスのドアロック電源

ドアロックの電源がオンのときに、ドアロックのステータスを設定できます。デフォルトでは、**閉じたまま**です。

オープン期間の延長

ドアの接触は、アクセスが延長された人の後に適切な遅延で有効にすることができます。彼女/彼のカードをスワイプする必要があります。

ドアは開いたままの時間、一人称

一人称が入るときにドアを開ける時間を設定します。最初のユーザーが承認されると、複数ユーザーはドアまたはその他の認証アクションにアクセスできるようになります。

強要コード

ドアは、強要があるときに強要コードを入力することで開くことができます。同時に、クライアントは強要イベントを報告できます。

スーパーパスワード

特定の人には、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。



メモ

強要コードとスーパーコードは異なるはずです。また、桁の範囲は4から8です。

RS-485 パラメータの設定

RS-485パラメータには、ペリフェラル、アドレス、ボーレートなどを設定できます。

[設定] → [アクセス制御] → [RS-485] をタップします。

RS-485 Settings	<input checked="" type="checkbox"/>
No.	1 >
Peripheral Type	Card Reader >
RS-485 Address	1
Baud Rate	19200 >
Data Bit	8 >
Stop Bit	1 >
Parity	None >
Flow Ctrl	None >
Communication Mode	Half-Duplex >

Save

図 8-14 RS-485 ページ

[保存] をタップして、設定後の設定を保存します。

ペリフェラルタイプ

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

メモ

周辺機器を変更して保存すると、デバイスは自動的に再起動します。

RS-485アドレス

実際のニーズに応じてRS-485アドレスを設定します。



メモ

[アクセス制御]を選択した場合:RS-485インターフェースを介してデバイスを端末に接続する場合は、RS-485アドレスを2に設定します。デバイスをコントローラーに接続する場合は、ドア番号によるRS-485アドレスを設定します。

ボーレート

デバイスがRS-485プロトコルを介して通信しているときのボーレート。

データビット

デバイスがRS-485プロトコルを介して通信しているときのデータビット。

ストップビット

デバイスがRS-485プロトコルを介して通信しているときのストップビット。

パリティ/フローCtrl/通信モード

デフォルトでは有効になっています。

ウィーガンドパラメータの設定

ウィーガンドの伝達方向を設定できます。

手順

1. 「設定」 → 「アクセス制御」 → 「ウィーガンド設定」をタップします。

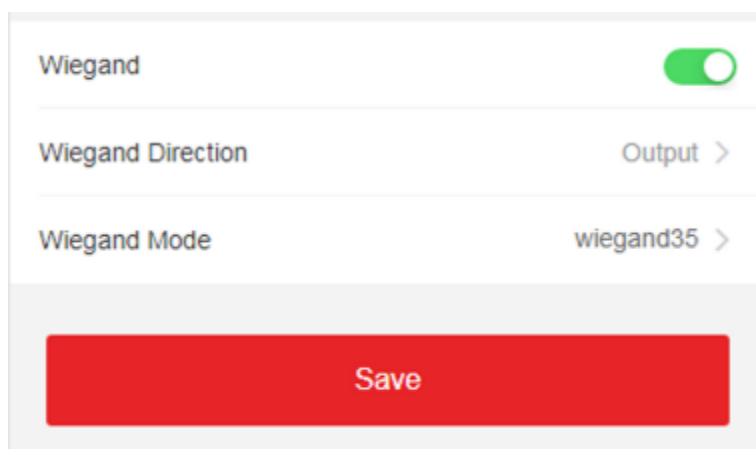


図8-15 ウィーガンド・ページ

2. ウィーガンドを有効にして、ウィーガンド機能を有効にします。
3. 送信方向を設定します。

インプット

デバイスはウィーガンドカードリーダーを接続できます。

アウトプット

外部アクセスコントローラを接続できます。そして、2つのデバイスはカード番号を送信します。ウィーガンド26または34経由。

4. [保存]をクリックして、設定を保存します。
-



メモ

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

第9章 Webブラウザによる操作

9.1 ログイン

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



メモ

デバイスがアクティブ化されていることを確認します。アクティベーションの詳細については、「アクティベーション」を参照してください。

Webブラウザ経由でログイン

のアドレスバーにデバイスのIPアドレスを入力し、web ブラウザをクリックし、**Enter**キーを押してログインページに入ります。




メモ

IPアドレスが「**Https:**」で始まることを確認してください。

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

クライアントソフトウェアのリモート設定によるログイン

クライアントソフトウェアをダウンロードして開きます。デバイスを追加したら、クリックして  設定ページに入ります。

9.2 ライブビュー

あなたはすることができます ビュー デバイスのライブビデオ。

ログイン後、ライブビューページに入ります。ライブビュー、キャプチャ、ビデオ録画、およびその他の操作を実行できます。

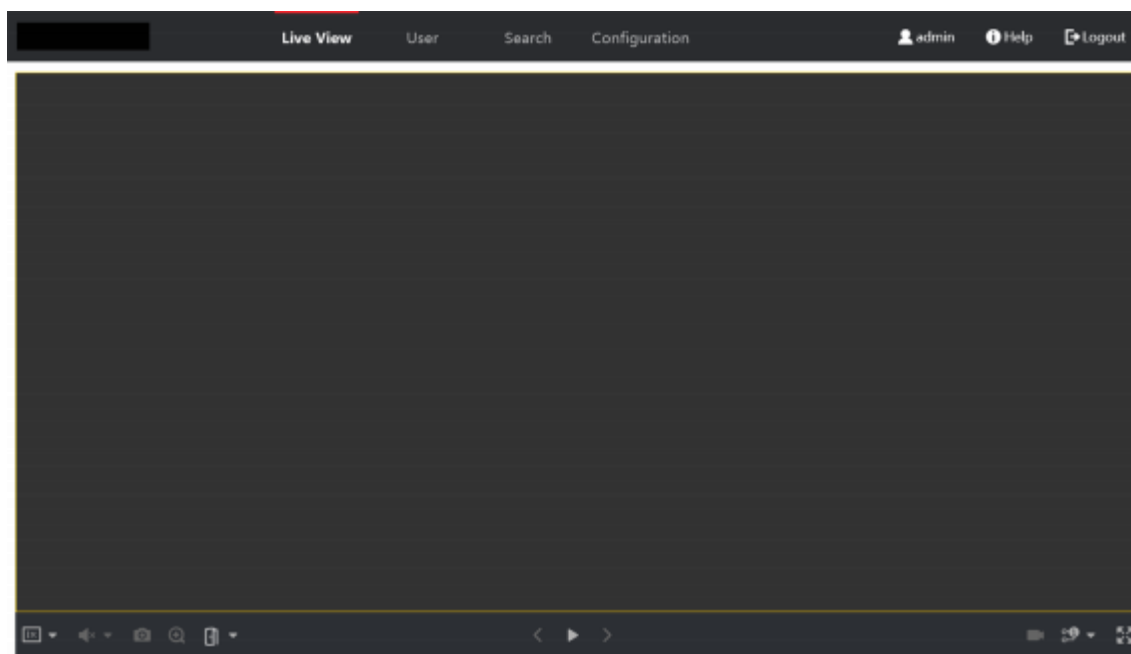


図9-1 「ライブ・ビュー」ページ

機能の説明:



ライブビュー開始時の画像サイズを選択します。



ライブビュー開始時の音量を設定します。

メモ

双方向音声の開始時に音量を調整すると、音が繰り返し聞こえる場合があります。



ライブビュー開始時に画像をキャプチャできます。



予約済み機能。ライブビューの画像を拡大することができます。



ライブビューを開始または停止します。



ビデオ録画を開始または停止します。



ライブビューを開始するときにストリーミングタイプを選択します。メインストリームとサブストリームから選択できます。



全画面表示。

9.3 人の管理

クリックして、基本情報、認証モード、カードなどのユーザーの情報を追加します。また、ユーザー情報の編集、ユーザーの写真の表示、ユーザーの検索もできます。

ユーザーリスト内の情報。[OK]をクリックして、ユーザーを保存します。

基本的な情報を追加

[ユーザー]→[追加]をクリックして、[ユーザーの追加]ページに入ります。

従業員ID、名前、ユーザーレベル、階 No.、room No.などの基本情報を追加します。

[OK]をクリックして、設定を保存します。

カードを追加

[ユーザー]→[追加]をクリックして、[ユーザーの追加]ページに入ります。

[カードの追加]をクリックし、[カード番号]を入力します。をクリックし、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。[OK]をクリックして、設定を保存します。

顔写真を追加

[ユーザー]→[追加]をクリックして、[ユーザーの追加]ページに入ります。

右側の[+]をクリックして、ローカルPCから顔写真をアップロードします。

メモ

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

[OK]をクリックして、設定を保存します。

許可時間の設定

[ユーザー]→[追加]をクリックして、[ユーザーの追加]ページに入ります。開始時刻と終了時刻を設定します。

[OK]をクリックして、設定を保存します。

アクセス制御の設定

[ユーザー]→[追加]をクリックして、[ユーザーの追加]ページに入ります。

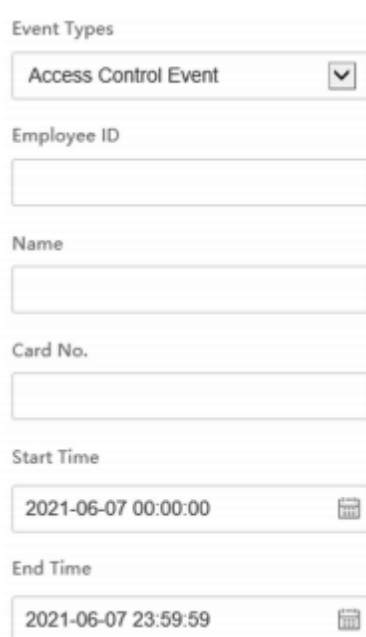
アクセスコントロールで管理者をチェックした後、追加された人は顔認証でログインできます。「追加」をクリックしてアクセスコントロールの階数と部屋番号を入力し、削除するには をクリックします。「OK」をクリックして設定を保存します。

認証モードの追加

[ユーザー]→[追加]をクリックして、[ユーザーの追加] ページに入ります。
認証タイプを設定します。[OK]をクリックして、設定を保存します。

9.4 検索イベント

[検索]をクリックして [検索] ページに入ります。



The screenshot shows a search event page with the following fields:

- Event Types:** A dropdown menu with "Access Control Event" selected.
- Employee ID:** An empty text input field.
- Name:** An empty text input field.
- Card No.:** An empty text input field.
- Start Time:** A date and time picker showing "2021-06-07 00:00:00".
- End Time:** A date and time picker showing "2021-06-07 23:59:59".

図9-2 「検索」 ページ

社員ID、氏名、カード番号、開始時刻、終了時刻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。

9.5 設定

9.5.1 ローカルパラメータの設定

ライブを設定します ビュー パラメータ、ファイルの保存パスの記録、およびキャプチャした画像の保存パス。

ライブビューパラメータの設定

[設定]→[ローカル]をクリックして[ローカル]ページに入ります。ストリームタイプ、再生パフォーマンス、ライブビューの自動開始、およびイメージフォーマットを設定し、[保存]をクリックします。

レコードファイルの保存パスの設定

[ローカル→設定]をクリックして、[ローカル]ページに入ります。レコードのファイルサイズを選択し、ローカルコンピューターから保存パスを選択して、[保存]をクリックします。

[開く]をクリックしてファイルフォルダを開き、詳細を表示することもできます。

キャプチャした画像の保存パスを設定する

[ローカル→設定]をクリックして、[ローカル]ページに入ります。ローカルコンピューターから保存パスを選択し、[保存]をクリックします。

[開く]をクリックしてファイルフォルダを開き、詳細を表示することもできます。

9.5.2 ビュー デバイス情報

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

[Configuration]→[System]→[System settings]→[Basic 情報]をクリックして、設定ページに入ります。

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

9.5.3 設定時間

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

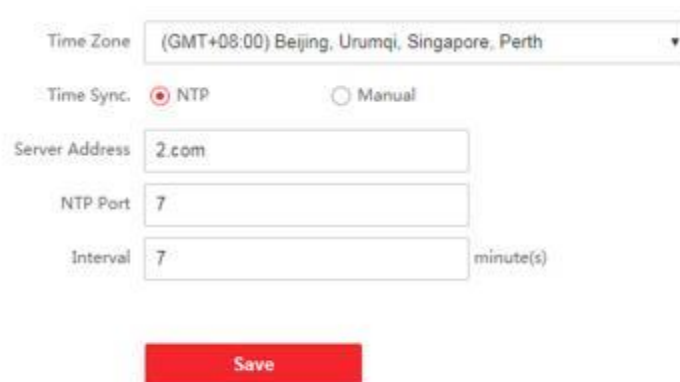


図9-3 時間設定

[保存] をクリックして、設定後の設定を保存します。

時間帯

ドロップダウンリストから、タイムゾーンが位置するデバイスを選択します。

タイムシンク

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、[Sync. with Computer Time] をオンにして、デバイスの時刻をコンピュータします。

9.5.4 DST設定

手順

1. [Configuration] → [System] → [System settings] → DST をクリックします。

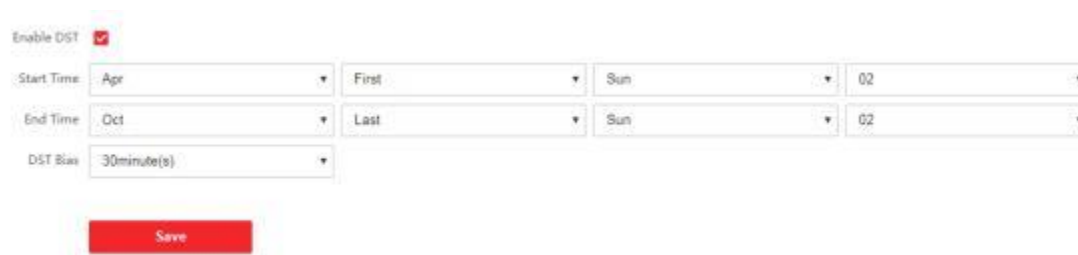


図9-4 DSTページ

2. [Enable DST] をオンにします。

3. DSTの開始時間、終了時間、バイアス時間を設定します。

4. [保存] をクリックして、設定を保存します。

9.5.5 ビュー オープンソースソフトウェアライセンス

[Configuration] → [System] → [System Settings] → [About] に移動し、[ビューライセンス] をクリックして、デバイスのライセンスを表示します。

9.5.6 アップグレードとメンテナンス

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

デバイスの再起動

[Configuration (設定)] → [System → Mntenance (システムメンテナンス)] → [Upgrade & Mntenance (アップグレードとメンテナンス)] をクリックします。

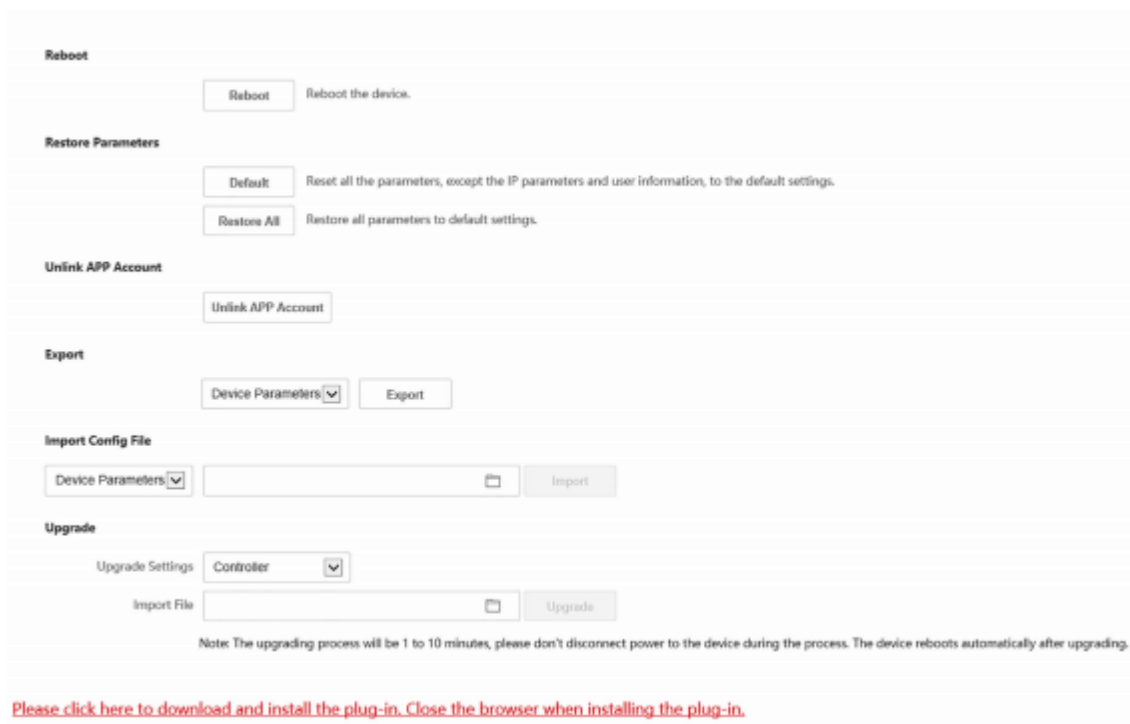


図9-5 [アップグレードとメンテナンス] ページ

[再起動] をクリックして、デバイスの再起動を開始します。

リストアパラメータ

[Configuration → System → Mntenance → Upgrade & Mntenance] をクリックします。

すべて復元

すべてのパラメータは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ブ化する必要があります。

デフォルト

デバイスは、デバイスのIPアドレスとユーザー情報を除いて、デフォルトの設定に復元されます。

APPアカウントのリンクを解除

Connectアカウントをプラットフォームからリンク解除します。

インポートおよびエクスポートパラメータ

[Configuration → System → Mntenance → Upgrade & Mntenance] をクリックします。

輸出


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



メモ


エクスポートしたデバイスパラメータを別のデバイスにインポートできます。

輸入

インポート  するファイルをクリックして選択します。「Import」をクリックして、インポート構成ファイルを開始します。

アップグレード

[Configuration (設定)] → [System → Mntenance (システムメンテナンス)] → [Upgrade & Mntenance (アップグレードとメンテナンス)] をクリックします。

ドロップダウンリストからアップグレードタイプを選択します。クリックして 、ローカルPCからアップグレードファームウェアを選択します。[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。



メモ

アップグレード中は電源を入れしないでください。

9.5.7 ログクエリ

デバイスのログを検索して表示できます。

[Configuration (設定)] → [System → Mntenance (メンテナンス)] → [Log Query (ログクエリ)] に移動します。

ログ・タイプのメジャー・タイプとマイナー・タイプを設定します。検索の開始時刻と終了時刻を設定し、[検索] をクリックします。

結果は、番号、時間、メジャータイプ、マイナータイプ、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などを含む下に表示されます。

9.5.8 セキュリティモードの設定

クライアントソフトウェアにログインするためのセキュリティモードを設定します。

[Device for Management] ページで、[Configuration] → [System] → [Security] → [Security Service] をクリックします。

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

セキュリティモード

クライアントソフトウェアにログインする際のユーザー情報検証のための高いセキュリティレベル。

ファッションの互換性

ユーザー情報の確認は、ログイン時の旧クライアントソフトウェア版と互換性があります。

SSHを有効にする

ネットワークセキュリティを強化するには、SSHサービスを無効にします。この設定は、専門家向けのデバイスのデバッグにのみ使用されます。

HTTPを有効にする

Webサイトにアクセスする際のネットワークセキュリティレベルを向上させるために、HTTPを有効にして、より安全で暗号化されたネットワーク通信環境を取得できます。通信は、HTTPを有効にした後、IDと暗号化パスワードで認証する必要があります。

9.5.9 証明書管理

サーバー/クライアント証明書とCA証明書の管理に役立ちます。



この機能は、特定のデバイスモデルでのみサポートされています。

自己署名証明書の作成とインストール

手順

1. [設定] → [システム] → [セキュリティ] → [証明書の管理] に移動します。
2. [証明書ファイル]領域で、ドロップダウンリストから「証明書タイプ」を選択します。
3. [作成]をクリックします。
4. 証明書情報を入力します。
5. [OK] をクリックして、証明書を保存してインストールします。

作成された証明書が [証明書の詳細] 領域に表示されます。

証明書は自動的に保存されます。

6. 証明書をダウンロードし、ローカルコンピューターのドアコンタクト先に保存します。
 7. 署名のために、求めている証明書を認証局に送信します。
 8. 署名付き証明書をインポートします。
 - 1) [Import Passwords] 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て [Install] をクリックします。
-

- 2) [Import Communication Certificate]領域で**証明書タイプ**を選択し、ローカルから証明書を
選択して [Install] をクリックします。

その他の認定証明書のインストール

認証された証明書(デバイスによって作成されていない証明書)がすでにある場合は、デバイスに直接インポートできます。

手順

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

CA 証明書のインストール

始める前に

事前にCA証明書を準備してください。

手順

1. [設定] → [システム] → [セキュリティ] → [証明書の管理] に移動します。
2. [Import CA Certificate] で ID を作成します。




メモ

入力された証明書IDを既存のものと同じにすることはできません。

-
3. ローカルから証明書ファイルをアップロードします。
 4. 「インストール」 をクリックします。

9.5.10 管理者パスワードの変更

手順

1. 「Configuration → User Management」 をクリックします。
2. をクリックします .
3. 古いパスワードを入力し、新しいパスワードを作成します。
4. 新しいパスワードを確認します。
5. [OK] をクリックします。



注意

デバイスのパスワードの強度は、自動的にlyチェックできます。製品のセキュリティを強化するために、自分で選択したパスワードを変更することを強くお勧めします(少なくとも3種類のカテゴリを含む、8文字以上、大文字の文字、小文字の文字、数字、特殊文字を含む)。そして、変更することをお勧めします。

パスワードを定期的に、特に高度なセキュリティシステムでは、パスワードを毎月または毎週変更することで、製品の保護を強化することができます。

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

9.5.11 ビュー デバイスの武装/武装解除情報

デバイスのアーミングタイプとアーミングIPアドレスを表示します。

[Configuration] → [Arming/Disarming] 情報に移動します。

デバイスの武装/武装解除情報を表示できます。「リフレッシュ」をクリックして、ページを再表示します。

9.5.12 ネットワーク設定

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



メモ

一部のデバイスモデルはWi-Fi設定をサポートしていません。設定の際は、実際の製品を参照してください。

基本的なネットワークパラメータの設定

[ネットワーク] → [設定] → [基本設定] → [TCP/IP] をクリックします。パラメータを設定し、[保存] をクリックして設定を保存します。

DHCP

この機能のチェックを外す場合は、IPv4 アドレス、IPv4 サブネットマスク、IPv4 デフォルトゲートウェイ、MTU、およびデバイスポートを設定する必要があります。

この機能にチェックを入れると、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が自動的に割り当てられます。

NICタイプ

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

DNSサーバー

実際のニーズに応じて、優先DNSサーバーと代替DNSサーバーを設定します。

ポートパラメータの設定

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

[Configuration] → [Network] → [Basic settings] → [Port] をクリックします。

HTTP

これは、ブラウザがデバイスにアクセスするときに使用するポートを指します。たとえば、HTTPポートが81に変更された場合、**ログインするにはブラウザにhttp://192.0.0.65:81**と入力する必要があります。

RTSP

これは、リアルタイムストリーミングプロトコルのポートを指します。

HTTPS

ブラウザにアクセスするためのHTTPSを設定します。アクセス時には証明書が必要です。

サーバー

これは、クライアントがデバイスを追加するときに使用するポートを指します。

Wi-Fiパラメータの設定

デバイスのワイヤレス接続のWi-Fiパラメータを設定します。

手順



メモ

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. [Wi-Fi]→[Wi-Fi]→[ネットワーク]→[設定] [設定] をクリックします。



図9-6 Wi-Fi設定ページ

2. Wi-Fiを確認します。

3. Wi-Fiを選択します

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

1)[ネットワーク設定]をクリックします。

2) IPアドレス、サブネットマスク、デフォルトゲートウェイを設定します。または、**[DHCPを有効にする]**をオンにすると、システムは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. **[OK]**をクリックします。

レポート戦略の設定

ISUP プロトコルを使用してログをアップロードするためのセンターグループを設定できます。**[Configuration] → [Network] → [Basic settings] → [Report Strategy]**に移動します。

センターグループを設定すると、システムはISUPプロトコルを介してログを転送します。**[保存]**をクリックして、設定を保存します。

センターグループ

ドロップダウンリストからセンターグループを選択します。

メインチャンネル

デバイスは、メインチャンネルを介してセンターと通信します。



メモ

N1は有線ネットワークを指します。

プラットフォームアクセス

プラットフォームアクセスは、プラットフォームを介してデバイスを管理するオプションを提供します。

手順

1. **[Configuration → Network → Advanced] → [プラットフォーム Access]**をクリックして、設定ページに入ります。
2. **プラットフォームアクセスモード**を選択します。



メモ

Connectは、モバイルデバイス用のアプリです。このアプリを使用すると、デバイスのライブ画像を表示したり、アラーム通知を受け取ったりすることができます。

3. **[有効にする]**のチェックボックスをオンにして、機能を有効にします。
4. **オプション:カスタムのチェックボックス**をオンにすると、サーバーアドレスを自分で設定できます。
5. **デバイスのストリーム暗号化/暗号化キー**を作成します。



メモ

6~12個のアイター(a~z、A~Z)または数字(0~9)、大文字と小文字が区別されます。8つ以上のアルファベットまたは数字の組み合わせを使用することをお勧めします。

6. **[保存]**をクリックして、設定を有効にします。
-

ISUP パラメータの設定

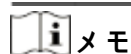
ISUPプロトコルを介してデバイスにアクセスするためのISUPパラメータを設定します。

手順



機能は、デバイスでサポートされている必要があります。

1. 「設定」→「ネットワーク」→「詳細設定」→「プラットフォーム」をクリックします。
 2. プラットフォームアクセスモードドロップダウンリストから**ISUP**を選択します。
 3. [Enable] をオンにします。
 4. ISUPバージョンを設定し、アラームレシーバーのタイプ、サーバーアドレス、ポート、デバイスID、レジスタステータスを表示します。
-



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

5. ISUPアラームセンターのIPアドレス/ドメイン名、ISUPアラームセンターURL、ISUPアラームセンターポートなどのISUPリスニングパラメータを設定します。
6. 「保存」をクリックします。

HTTP リスニングの設定

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

始める前に

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



機能は、デバイスでサポートされている必要があります。

手順

1. [Configuration→Network→Advanced→HTTP Listening] をクリックします。
2. イベントアラームのIPアドレスまたはドメイン名、URL、ポート、およびプロトコルを編集します。
3. オプション:[デフォルト] をクリックして、イベントアラームのIPアドレスまたはドメイン名をリセットします。
4. [保存] をクリックします。

9.5.13 ビデオとオーディオのパラメータを設定

画質、解像度、およびデバイスの音量を設定します。

ビデオパラメータの設定

[設定]→[ビデオ/オーディオ]→[ビデオ]をクリックします。

Stream Type	Main Stream	▼
Video Type	Video&Audio	▼
Resolution	1280*720	▼
Bitrate Type	Constant	▼
Video Quality	Lowest	▼
Frame Rate	25	▼ fps
Max. Bitrate	2048	Kbps
Video Encoding	H.264	▼
I Frame Interval	25	

Save

図9-7「ビデオ設定」ページ

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

[保存]をクリックして、設定後の設定を保存します。

オーディオパラメータの設定

[設定]→[ビデオ/オーディオ]→[オーディオ]をクリックします。オーディオストリームの種類とオーディオエンコードを設定します。

スライダーをドラッグして、デバイスの入力と出力の音量を調整します。音声プロンプトを有効にすることもできます。

[保存]をクリックして、設定後の設定を保存します。

メモ

機能は、異なるモデルによって異なります。詳細については、実際のデバイスを参照してください。

9.5.14 オーディオコンテンツのカスタマイズ

認証が成功したときと失敗したとき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. 「Configuration → Video/Audio → Prompt」 をクリックします。

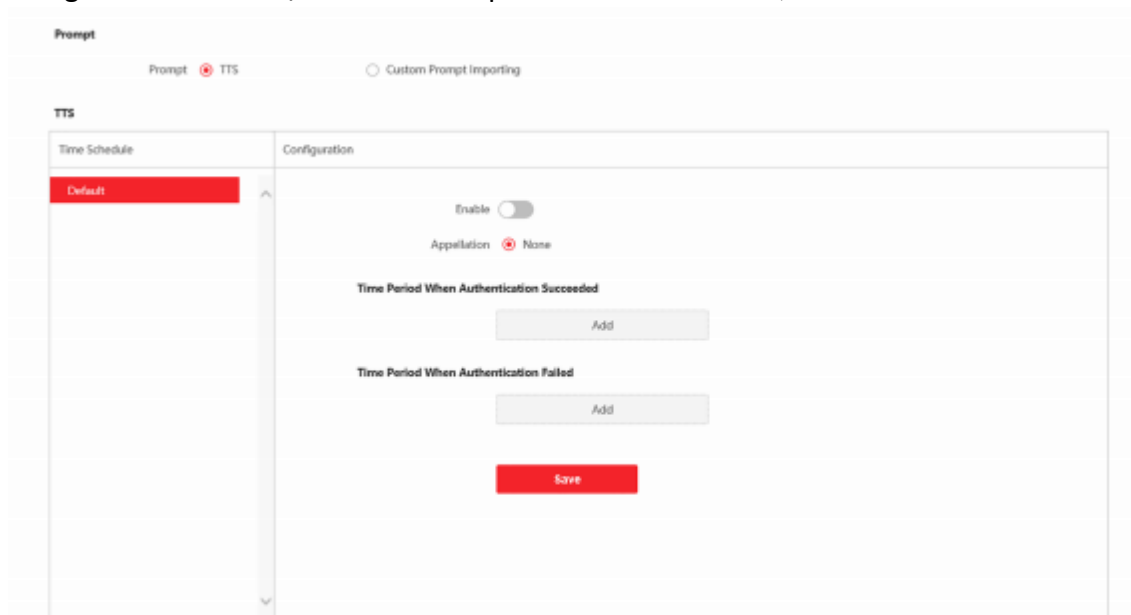


図9-8 オーディオ・コンテンツのカスタマイズ

2. 「プロンプトをTTS(Text to Speech)」として選択し、テキストを音声コンテンツに変換します。
3. または、カスタムプロンプトImportingとしてプロンプトを選択することもできます。
 - 1) カスタムタイプを選択するか、ローカルPCからカスタムプロンプトをインポートできます。
 - 2) カスタムプロンプトのインポートステータスをリストで確認できます。




メモ

音声ファイルはWAV形式でモノラルである必要があり、サンプリングレートは8Kまたは16Kでなければなりません。音声ファイルの振幅は-3dBを超えてはならず、ファイルサイズは512Kを超えてはいけません。

4. タイムスケジュールを選択します。
5. 機能を有効にします。
6. アプリを設定します。
7. 認証が成功する時間を設定します。
 - 1) 「追加」をクリックします。
 - 2) 期間と言語を設定します。


 **メモ**

設定された時間内に認証が成功すると、デバイスは設定されたコンテンツをブロードキャストします。

- 3) オーディオコンテンツを入力します。
 - 4) **オプション**: サブステップ1~3を繰り返します。
 - 5) **オプション**: クリックして 、設定された期間を削除します。
8. 認証に失敗した時間を設定します。
- 1) 「追加」をクリックします。
 - 2) 期間と言語を設定します。

 **メモ**

設定され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ブロードキャストします。

- 3) オーディオコンテンツを入力します。
 - 4) **オプション**: サブステップ1~3を繰り返します。
 - 5) **オプション**: クリックして 、設定された期間を削除します。
9. **オプション**: 休日のスケジュールを追加します。
- 1) 「追加」をクリックして、休日のスケジュールを追加します。
 - 2) 手順3から6を繰り返します。
10. **[保存]**をクリックして、設定を保存します。

9.5.15 イメージパラメータの設定

ビデオの標準、明るさ、コントラスト、彩度を設定します。

手順

1. 「設定」→「画像調整」をクリックします。
2. パラメータを設定して画像を調整します。

ビデオスタンダード

ライブビューをリモートで実行するときのビデオフレームレートを設定します。規格を変更した後は、デバイスを再起動して有効にする必要があります。

PAL

毎秒25フレーム。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

毎秒30フレーム。米国、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。

明るさ/コントラスト/彩度

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



ビデオの録画を開始/終了します。



画像をキャプチャします。

3. 「デフォルト」をクリックして、パラメータをデフォルトの設定に戻します。

9.5.16 サプリメントライトの明るさを設定する

デバイスの補助光の明るさを設定します。

手順

1. 「設定」→「イメージ」→「ライトパラメータを追加」をクリックします。

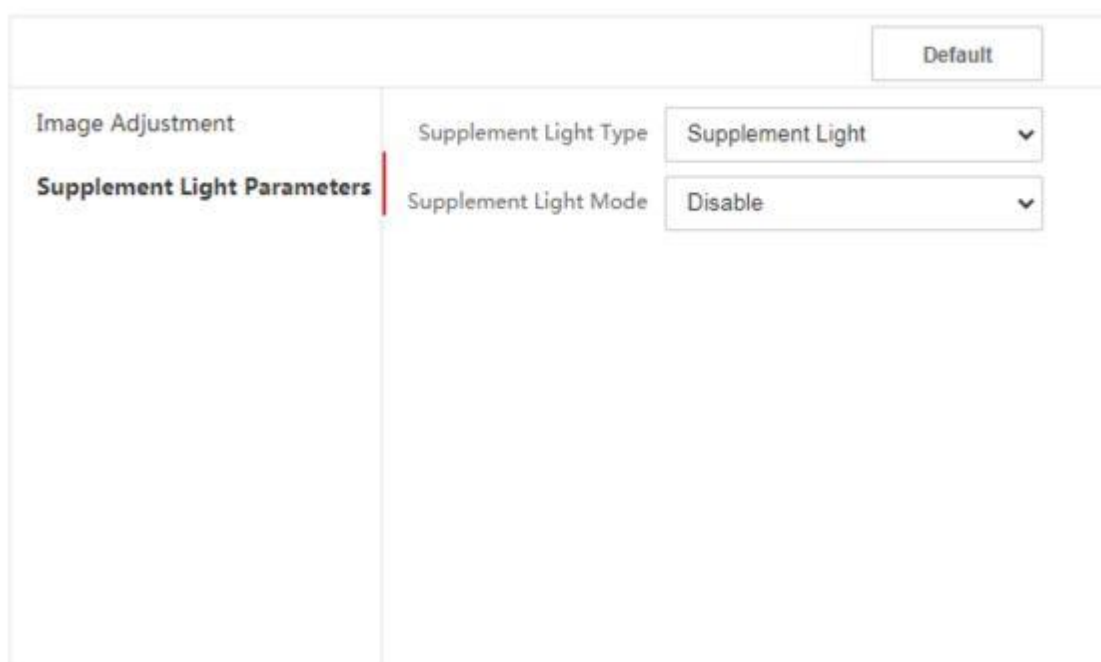


図9-9 「Supplement Light」設定ページ

2. ドロップダウンリストから補助ライトの種類とモードを選択します。モードをONにする場合は、明るさを設定する必要があります。

9.5.17 時間と出勤の設定

その人がいつ仕事を開始/停止するかを追跡し、監視し、彼らの仕事を監視する場合、時間と遅刻、早退、休憩時間にかかった時間、欠勤の場合は、その人をシフトグループに追加し、シフトスケジュールを割り当てることができます(出席のルールで、スケジュールの繰り返し)

、シフトタイプ、休憩設定、およびカードスワイプルール。シフトグループに対して、シフトグループ内の個人の出席パラメーターを定義します。

Web経由で出席モードを無効にする

出席モードを無効にすると、初期ページに出席ステータスが表示されなくなります。

手順

1. [Configuration → Attendance]をクリックして、設定ページに入ります。
2. 出席モード を無効に設定します。

結果

初期ページで出席ステータスを表示または構成することはできません。また、システムはプラットフォームで設定された出席ルールに従います。

時間設定

手順

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



メモ

実際のニーズに応じて、月曜日から日曜日までのスケジュールを設定します。

5. オプション: 時間を選択し、[削除] をクリックします。または、[すべて削除] をクリックして設定をクリアします。
6. 「保存」をクリックします。

Web経由で手動の出席を設定する

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

始める前に

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. [Configuration → Attendance]をクリックして、設定ページに入ります。
2. 出席モード を手動に設定します。
3. 「Attendance Status Required」を有効にし、出席ステータスの持続時間を設定します。
4. 出席ステータスのグループを有効にします。



メモ

アテンダントプロパティは変更されません。

5. オプション: ステータスを選択し、必要に応じて名前を

変更します。結果

認証後、出席状況を手動で選択する必要があります。



メモ

ステータスを選択しない場合、認証は失敗し、有効な出席としてマークされません。

Web経由でAuto Aテンダンスを設定する

勤怠モードを自動に設定すると、勤怠状況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状況を自動的に変更します。

始める前に

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. [Configuration → Attendance]をクリックして、設定ページに入ります。
 2. 出席モード を自動に設定します。
 3. 出席状況機能を有効にします。
 4. 出席ステータスのグループを有効にします。
-



メモ

アテンダントプロパティは変更されません。

5. オプション: ステータスを選択し、必要に応じて名前を変更します。

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、[Timesettings](#)を参照してください**。

Webによる手動および自動出席の設定

出席モードを手動および自動に設定すると、システムは設定されたスケジュールに従って自動的に出席ステータスを変更します。同時に、認証後に出席ステータスを手動で変更できます。

始める前に

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. [Configuration → Attendance]をクリックして、設定ページに入ります。
 2. 出席モード を手動と自動に設定します。
 3. 出席状況機能を有効にします。
-

4. 出席ステータスのグループを有効にします。
-



メモ

アテンダントプロパティは変更されません。

5. オプション: ステータスを選択し、必要に応じて名前を変更します。

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、Timesettingsを参照してください。結果

初期ページで認証します。認証は、構成されたものとしてマークされます
スケジュールに応じた出席状況。結果タブの編集アイコンをタップすると、手動で出席を取る
ステータスを選択でき、認証は編集済みとしてマークされます
出席ステータス。

例

[ブレイクアウト] を [月曜日 11:00] に設定し、[ブレイクイン] を [月曜日 12:00] に設定すると、月曜日の 11:00 から 12:00 までの有効なユーザーの認証がブレイクとしてマークされます。

9.5.18 一般設定

認証パラメータの設定

「Configuration」→「General」→「Authentication settings」をクリックします。



メモ

機能は、異なるモデルによって異なります。詳細については、実際のデバイスを参照してください。

Card Reader: Main Card Reader

Card Reader Type: Fingerprint/Face

Card Reader Description:

Enable Card Reader:

Authentication: Card or Face or Fingerprint

Recognition Interval: 1 s

Authentication Interval: 22 s

Alarm of Max. Failed Attempts:

Max. Authentication Failed Attempts: 5

Enable Tampering Detection:

Enable Card No. Reversing:

Save

図9-10 認証パラメータの設定

[保存]をクリックして、設定後の設定を保存します。

デバイスタイプ

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

メインカードリーダー

デバイスカードリーダーのパラメータを設定できます。

サブカードリーダー

接続されている周辺機器カードリーダーのパラメータを設定できます。

メインカードリーダーを選択した場合:

カードリーダータイプ/カードリーダーの説明

カードリーダーの種類と説明を取得します。これらは読み取り専用です。

カードリーダーを有効にする

カードリーダーの機能を有効にします。

認証

ドロップダウンリストから実際のニーズに応じて認証モードを選択します。

認識間隔

同じ人物を2回連続して認識する間隔を設定できます。

認証。設定された間隔では、人物Aは1回だけ認識できます。インターバル中に別の人(Bさん)が認識した場合、Aさんは再度認識できます。

認証間隔

認証時に同一人物の認証間隔を設定できます。同じ人物は、設定された間隔で1回だけ認証できます。2回目の認証は失敗します。

最大失敗試行数のアラーム

カードの読み取り試行が設定値に達したときにアラームを報告するように有効にします。

認証失敗の最大試行回数

カードの読み取り試行が設定値に達したときにアラームを報告するように有効にします。

改ざん検出を有効にする

カードリーダーの改ざん防止検出を有効にします。

カード番号を有効にする反転

読み取られたカード番号は、機能を有効にすると逆の順序でなります。

サブカードリーダーを選択した場合:

カードリーダータイプ/カードリーダーの説明

カードリーダーの種類と説明を取得します。これらは読み取り専用です。

カードリーダーを有効にする

カードリーダーの機能を有効にします。

認証

ドロップダウンリストから実際のニーズに応じて認証モードを選択します。

認識間隔

同じカードのカード提示間隔が設定値より短い場合、カード提示は無効です。

認証間隔

認証時に同一人物の認証間隔を設定できます。同じ

人物は、設定された間隔で1回だけ認証できます。2回目の認証は失敗します。

最大失敗試行数のアラーム

カードの読み取り試行が設定値に達したときにアラームを報告するように有効にします。

認証失敗の最大試行回数

カードの読み取り試行が設定値に達したときにアラームを報告するように有効にします。

コントローラーとの通信間隔

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

パスワード入力の最大間隔

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

OKLED極性/エラーLED極性

カードリーダーのパラメータに従って、アクセス制御デバイスのOKLED極性/エラーLED極性を設定します。通常、デフォルトの設定を採用しています。

改ざん検出を有効にする

カードリーダーの改ざん防止検出を有効にします。

プライバシーパラメータの設定

イベントのストレージタイプ、画像のアップロードと保存のパラメータ、および画像のクリアパラメータを設定します。

[設定]→[一般]→[プライバシー]に移動します。

イベントストレージ設定

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

古いイベントを定期的に削除する

ブロックをドラッグするか、数値を入力して、イベントダイエティングの期間を設定します。すべてのイベントは、設定された期間に従って削除されます。

指定した時間で古いイベントを削除

時間を設定すると、設定された時間にすべてのイベントが削除されます。

上書き

保存されたイベントが全スペースの95%を超えたことをシステムが検出すると、最も古い5%のイベントが削除されます。

認証設定

認証結果の表示

顔写真、名前、従業員IDを確認して、認証結果を表示できます。名前の匿名化名前の識別解除を確認すると、名前全体は表示されません。

画像のアップロードと保存

認証時にキャプチャした画像をアップロードする

認証時に撮影した写真をプラットフォーム自動的にアップロードします。

認証時にキャプチャした画像を保存する

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する

登録した顔写真は、機能を有効にするとシステムに保存されます。

写真のアップロード After Linked Capture

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自動的にアップロードします。

写真を保存する After リンクされたキャプチャ

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

デバイス内のすべての画像をクリアする



メモ

一度削除した画像は復元できません。

登録された顔写真をクリア

デバイスに登録されているすべての画像が削除されます。

キャプチャした写真をクリア

デバイス内でキャプチャされたすべての画像が削除されます。

顔認証パラメータの設定

アクセス用の顔認証パラメータを設定できます。

「一般」→「顔認証パラメータ」→「設定」をクリックします。

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

ブロックリスト認証を有効にします。

[保存]をクリックして、設定後の設定を保存します。

セットカードセキュリティ

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

NFCカードを有効にする

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

M1カードを有効にする

M1カードを有効にし、M1カードを提示して認証することができます。

M1カード暗号化セクター

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

機能を有効にし、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 は暗号化されています。セクター 13 を暗号化することをお勧めします。

EMカードを有効にする

EMカードを有効にし、EMカードを提示して認証することができます。



メモ

周辺カードリーダーがEMカードの提示をサポートしている場合、EMカード機能を有効/無効にする機能もサポートされます。

DESFireカードを有効にする

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

DESFireカード読み取りコンテンツ

DESFireカードコンテンツ読み取り機能を有効にすると、デバイスはDESFireカードコンテンツを読み取ることができます。

FeliCaカードを有効にする

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

カード認証パラメータの設定

デバイス上でカードによる認証を行う際のカード読み取り内容を設定します。[Configuration] → [General → Card Authentication settings] に移動します。

カード認証モードを選択し、[保存] をクリックします。

フルカード番号

すべてのカード番号が読めます。

ウィーガンド 26(3 バイト)

デバイスは、ウィーガンド26プロトコル(3バイトの読み取り)を介してカードを読み取ります。

ウィーガンド 34(4 バイト)

デバイスは、ウィーガンド34プロトコル(4バイトの読み取り)を介してカードを読み取ります。

認証結果テキストの設定

手順

1. [Configuration] → [General (一般)] → [Authentication Result Text (認証結果テキスト)] に移動します。

Text	Content	Custom
Stranger		
Authenticated		
Authentication Failed		

Save

図9-11 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。

9.5.19 ビデオインターホン設定

ビデオインターコムパラメータの設定

このデバイスは、ドアステーション、アウトードアステーション、またはアクセス制御デバイスとして使用できます。デバイス番号を設定する必要があります。使用する前に。

[Configuration](設定)→[Intercom](インターコム)→[Device No](デバイス番号) をクリックします。で囲まれています。

デバイスタイプをドアステーションまたはアクセス制御デバイスとして設定する場合は、ドア番号、ドアステーション番号を設定し、[詳細設定]をクリックしてフェーズ番号を設定できます。、建物番号、およびユニット番号[保存]をクリックして、設定後の設定を保存します。

デバイスタイプ

このデバイスは、ドアステーションまたはアウトー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ます。



メモ

デバイスの種類を変更した場合は、デバイスを再起動する必要があります。

フロア番号

デバイスの取り付け場所を設定します 階 No.

ドアステーションNo.

デバイスの取り付け場所階No.を設定します



メモ

No.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。

フェーズ番号

デバイスのフェーズNo.を設定します。

建物番号

デバイスの建物番号を設定します。

ユニット番号

デバイスユニットNo.を設定します。



メモ

No.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。

デバイスタイプを[アウトードアステーション]に設定した場合、[期間番号]、[アウトードアステーション番号]、および[コミュニティ番号]を設定できます。

アウトードアステーションNo.

デバイスタイプとしてアウトードアステーションを選択した場合は、**1～99の番号を入力する必要があります。**



メモ

No.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。

フェーズ番号

デバイスのフェーズNo.を設定します。

SIPパラメータの設定

デバイスのIPアドレスとSIPサーバーのIPアドレスを設定します。パラメータを設定した後、次のことができます。

アクセス制御デバイス、ドアステーション、屋内ステーション、メインステーション、およびプラットフォーム間で通信します。



メモ

アクセス制御デバイスとその他のデバイスまたはシステム(ドアステーション、屋内ステーション、メインステーション、プラットフォーム)が同じIPセグメントにある場合、**双方向オーディオを実行できます。**

[構成]→[インターコム]→[リンクネットワークの設定]に移動します。メインステーションのIPアドレスとSIPサーバーのIPアドレスを設定します。

「保存」をクリックします。

ボタンを押して電話をかける

手順

- 1.[設定]→[インターコム]をクリックし→ボタンを押して電話をかけます。
2. パラメータを設定します。
 - すべてのボタンのコール番号を編集します。
 - 「コール管理センター」にチェックを入れ、ボタンのコールセンターを設定します。



メモ

Call Management Centerにチェックを入れ、Call No.も設定すると、Call Management CenterはCall Noよりも権限が高くなります。

9.5.20 アクセス制御設定

ドアパラメータの設定

[設定]→[アクセス制御]→[ドアパラメータ]をクリックします。

Door No. Door1

Name

Open Duration 5 s

Door Open Timeout Alarm 30 s

Door Contact Remain Closed Remain Open

Exit Button Type Remain Closed Remain Open

Door Lock Powering Off Remain Closed Remain Open

Extended Open Duration 15 s

Door Remain Open Duration with First Person 10 m

Duress Code *****
Enter 0 to 8 digits.

Super Password *****
Enter 0 to 8 digits.

Save

図9-12 ドア・パラメータ設定ページ

[保存]をクリックして、設定後の設定を保存します。

ドア番号

対応ドアNo.に対応したデバイスを選択します。

名前

ドアの名前を作成できます。

開館期間

ドアの解錠時間を設定します。設定した時間内にドアを開けないと、ドアは施錠されます。

オープンタイムアウトアラームによる

設定された時間内にドアが開じられなかった場合、アラームがトリガーされます。

Byおドアコンタクト

ドアの接点は、**実際のニーズに応じて開いたまままたは閉じたままに設定**できます。デフォルトでは、**Remn Closed**です。

終了ボタンの種類

実際のニーズに応じて、終了ボタンを**開いたままにするか、閉じたままにするか**を設定できます。デフォルトでは、**開いたままになっています**。

ステータスのドアロック電源

ドアロックの電源がオンのときに、ドアロックのステータスを設定できます。デフォルトでは、**Remn Closed**です。

オープン期間の延長

ドアの接触は、アクセスが延長された人の後に適切な遅延で有効にすることができます。彼女/彼のカードをスワイプする必要があります。

ドアは開いたままの時間、一人称

一人称が入るときにドアを開ける時間を設定します。最初のユーザーが承認されると、複数ユーザーはドアまたはその他の認証アクションにアクセスできるようになります。

強要コード

ドアは、強要があるときに強要コードを入力することで開くことができます。同時に、クライアントは強要イベントを報告できます。

スーパーパスワード

特定の人、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。



メモ

強要コードとスーパーコードは異なるはずです。

RS-485 パラメータの設定

RS-485パラメータには、ペリフェラル、アドレス、ボーレートなどを設定できます。

[設定]→[アクセス制御]→[RS-485 設定]をクリックします。[RS-485を有効にする]をオンにし、パラメータを設定します。

[保存]をクリックして、設定後の設定を保存します。

No.

Set the RS-485 No.

ペリフェラルタイプ

実際の状況に応じて、ドロップダウンリストから周辺機器を選択します。カードリーダー、拡張モジュール、アクセスコントローラー、または無効化から選択できます。



メモ

周辺機器を変更して保存すると、デバイスは自動的に再起動します。

RS-485アドレス

実際のニーズに応じてRS-485アドレスを設定します。



メモ

[アクセス制御ler]を選択した場合:RS-485インターフェースを介してデバイスを端末に接続する場合は、RS-485アドレスを2に設定します。デバイスをコントローラーに接続する場合は、RS-485アドレスを設定します
ドア番号によると。

ボーレート

デバイスがRS-485プロトコルを介して通信しているときのボーレート。

ウィーガンドパラメータの設定

ウィーガンドの伝達方向を設定できます。

手順



メモ

一部のデバイスモデルはこの機能をサポートしていません。設定の際は、実際の製品を参照してください。

1. 「コンフィギュレーション」→「アクセス制御」→「ウィーガンド設定」をクリックします。

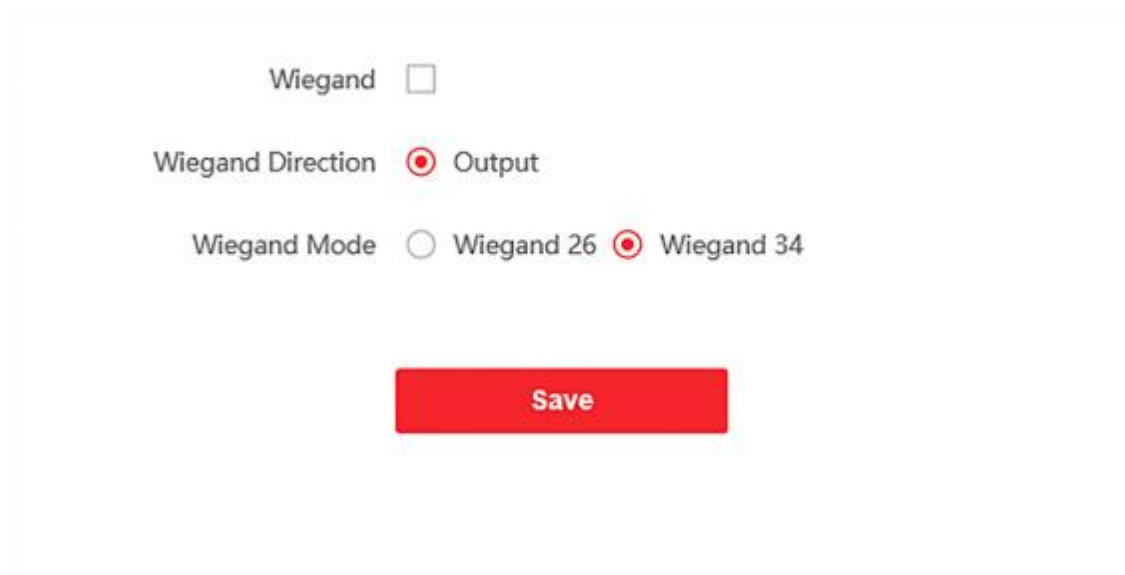


図9-13 ウィーガンド

2. ウィーガンドを**チェック**して、ウィーガンド機能を有効にします。
3. 送信方向を設定します。

アウトプット

外部アクセスコントローラを接続できます。そして、2つのデバイスはカード番号を送信します。ウィーガンド26または34経由。

4. **[保存]**をクリックして、設定を保存します。



メモ

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

9.5.21 生体認証パラメータの設定

基本パラメータの設定

[設定] → [スマート] → [スマート] をクリックします。

Face Parameters

Face Anti-spoofing

Live Face Detection Security Level Normal High Profile Highest

Recognition Distance Automatic 0.5m 1m 1.5m 2m

Application Mode Indoor Other

Face Recognition Mode **Normal Mode**

Continuous Face Recognition Interval 3 s

Pitch Angle 45 °

Yaw Angle 45 °

Face Grading 50

1:1 Matching Threshold 90

1:N Matching Threshold 90

Face Recognition Timeout Value 3 s

Face with Mask Detection

Face without Mask Strategy **None**

Face with Mask&Face (1:1) 68

Face with Mask 1:N Matching Threshold 80

ECO Mode

ECO Mode Threshold 4

ECO Mode (1:1) 80

ECO Mode (1:N) 80

Face with Mask&Face (1:1 ECO) 78

Face with Mask 1:N Matching Threshold (ECO Mode) 70

Fingerprint Parameters

Fingerprint Security Level **5-1/100000False Acceptance Rat**

Save

図9-14 面パラメータの設定

メモ

機能は、異なるモデルによって異なります。詳細については、実際のデバイスを参照してください。

[保存]をクリックして、設定を保存します。

顔アンチSpoofing

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、デバイスはその人が生きているかどうかを認識できます。

メモ

生体認証製品は、なりすまし防止環境に完全に適用できるわけではありません。より高いセキュリティ・レベルが必要な場合は、複数認証モードを使用してください。

ライブ顔検出のセキュリティレベル

顔スプーフィング対策機能を有効にした後、ライブ顔認証を実行する際の照合セキュリティレベルを設定できます。

認識距離

認証するユーザーとデバイスのカメラとの距離を選択します。

アプリモード

実際の環境に応じて、その他または屋内のいずれかを選択します。

顔認証モード:ノーマ

ルモード

通常どおりカメラで顔を認識します。

ディープモード

ディープモードでは、デバイスのユーザー追加機能または登録ステーションを通じてのみ顔写真を追加できます。写真のインポートによる顔写真の追加はサポートされていません。

メモ

ディープモードでは、デバイスまたは登録ステーションを介してのみ顔写真を追加できます。写真のインポートによる顔写真の追加はサポートされていません。

Continuous 顔認証インターバル

認証時に2つ連続した顔認証の時間間隔を設定します。

ピッチ角

顔認証を開始するときの最大ピッチ角。

ヨー角

顔認証を開始するときの最大ヨー角。

顔グレーディング

必要に応じて顔グレーディングを設定します。

1:1マッチングしきい値

1:1マッチングモードで認証する場合、マッチングしきい値を設定します。値が大きいほど、偽の受け入れ率は小さくなり、偽の拒否率は大きくなります。

1:N マッチングしきい値

1:N マッチングモードで認証する場合、マッチングしきい値を設定します。値が大きいほど、偽の受け入れ率は小さくなり、偽の拒否率は大きくなります。

顔認証タイムアウト値

顔認証時のタイムアウト値を設定します。顔認証時間が設定値よりも長い場合、システムはプロンプトをポップアップ表示します。

マスク付き顔検出

マスク検出で顔を有効にすると、システムはマスク画像でキャプチャされた顔を認識します。mask1:N一致しきい値、そのECOモード、および戦略。

なし

認証時に顔マスクを着用していない場合、デバイスは通知を求めません。

着用のリマインダー

認証時に顔マスクを着用していない場合、デバイスから通知が促され、ドアが開きます。

必着

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

マスクと顔(1:1)

顔マスク1:1マッチングモードで認証する場合、マッチング値を設定します。値が大きいほど、偽の受け入れ率は小さくなり、偽の拒否率は大きくなります。

マスク付き顔 1:N マッチングしきい値

1:Nマッチングモードを介して顔マスクで認証する場合のマッチングしきい値を設定します。値が大きいほど、偽の受け入れ率は小さくなり、偽の拒否率は大きくなります。

ECOモード

ECOモードを有効にすると、デバイスはIRカメラを使用して、暗い環境または暗い環境で顔を認証します。また、ECOモードのしきい値、ECOモード(1:N)、およびECOモード(1:1)を設定できます。

ECOモードしきい値

ECOモードのしきい値を設定します。値が大きいほど、デバイスはECOモードに入りやすくなります。

ECOモード(1:1)

ECOモード1:1マッチングモードで認証する場合、マッチングしきい値を設定します。値が大きいほど、偽の受け入れ率は小さくなり、偽の拒否率は大きくなります。

ECOモード(1:N)

ECOモード1:Nマッチングモードで認証する場合、マッチングしきい値を設定します。値が大きいほど、誤受理率は小さくなり、誤受理率は大きくなります。

マスク付き顔&顔(1:1ECO)

ECOモード1:1マッチングモードで顔マスクで認証する場合のマッチング値を設定します。値が大きいほど、偽の受け入れ率は小さくなり、偽の拒否率は大きくなります。

マスク付き顔1:N マッチングしきい値(ECOモード)

ECOモード1:Nマッチングモードを介して顔マスクで認証する場合のマッチングしきい値を設定します。値が大きいほど、偽の受け入れ率は小さくなり、偽の拒否率は大きくなります。

認識領域の設定

[設定(Configuration)] → [スマート → エリアの設定(Smart Area Configuration)] をクリックします。

ライブビデオの黄色のフレームをドラッグして、認識領域を調整します。エリア内の顔のみがシステムで認識できます。

必要に応じて、エリア構成、マージン(左)、マージン(右)、マージン(上)、マージン(下)を設定します。

[保存] をクリックして、設定を保存します。

またはをクリックして  、ビデオを録画したり、写真をキャプチャしたりします。

9.5.22 予告公開の設定

デバイスのテーマを設定できます。

「設定」→「テーマ」→メディアデータベース、「+追加」の順にクリックし、「アップロード」をクリックして、素材をメディアライブラリにアップロードします。

「設定」→「テーマ」→「テーマ」をクリックします。

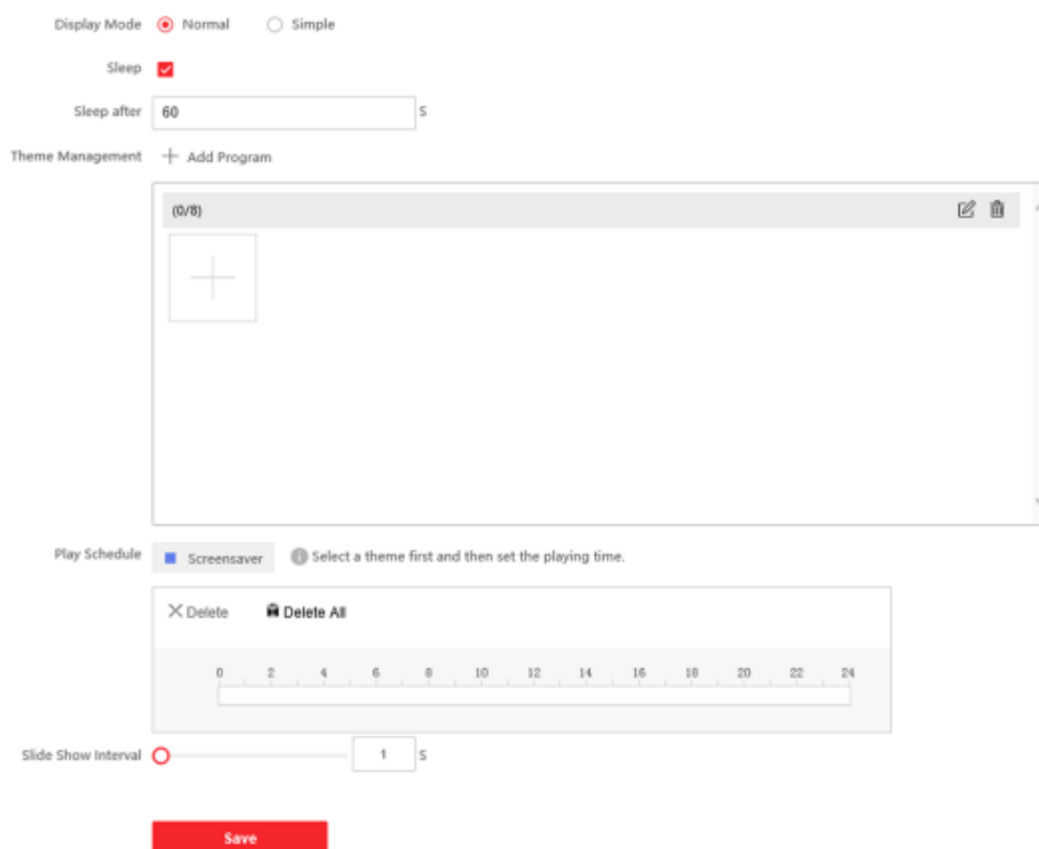


図9-15 「テーマ」 ページ

表示モード

デバイス認証の表示テーマを選択できます。**表示モード** は、**シンプル**または**ノーマル**から**選択**できます。**シンプル**を選択すると、名前、ID、顔写真の情報は表示されなくなります。

寝る

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

テーマ管理

フレーム内の[+プログラムの追加]をクリックして、ローカルPCからスクリーンセーバーの画像をアップロードできます。

メモ

現在、追加できるテーマは1つだけです。

プレイスケジュール

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

描画されたスケジュールを選択すると、正確な開始時刻と終了時刻を編集できます。

描画されたスケジュールを選択し、[削除]または[すべて削除]をクリックしてスケジュールを削除できます。

スライドショーのインターバル

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。間隔に応じて写真が切り替わります。

第10章 クライアントソフトウェアの構成

10.1 クライアントソフトウェアの設定フロー

次の図に従って、クライアントソフトウェアで構成します。

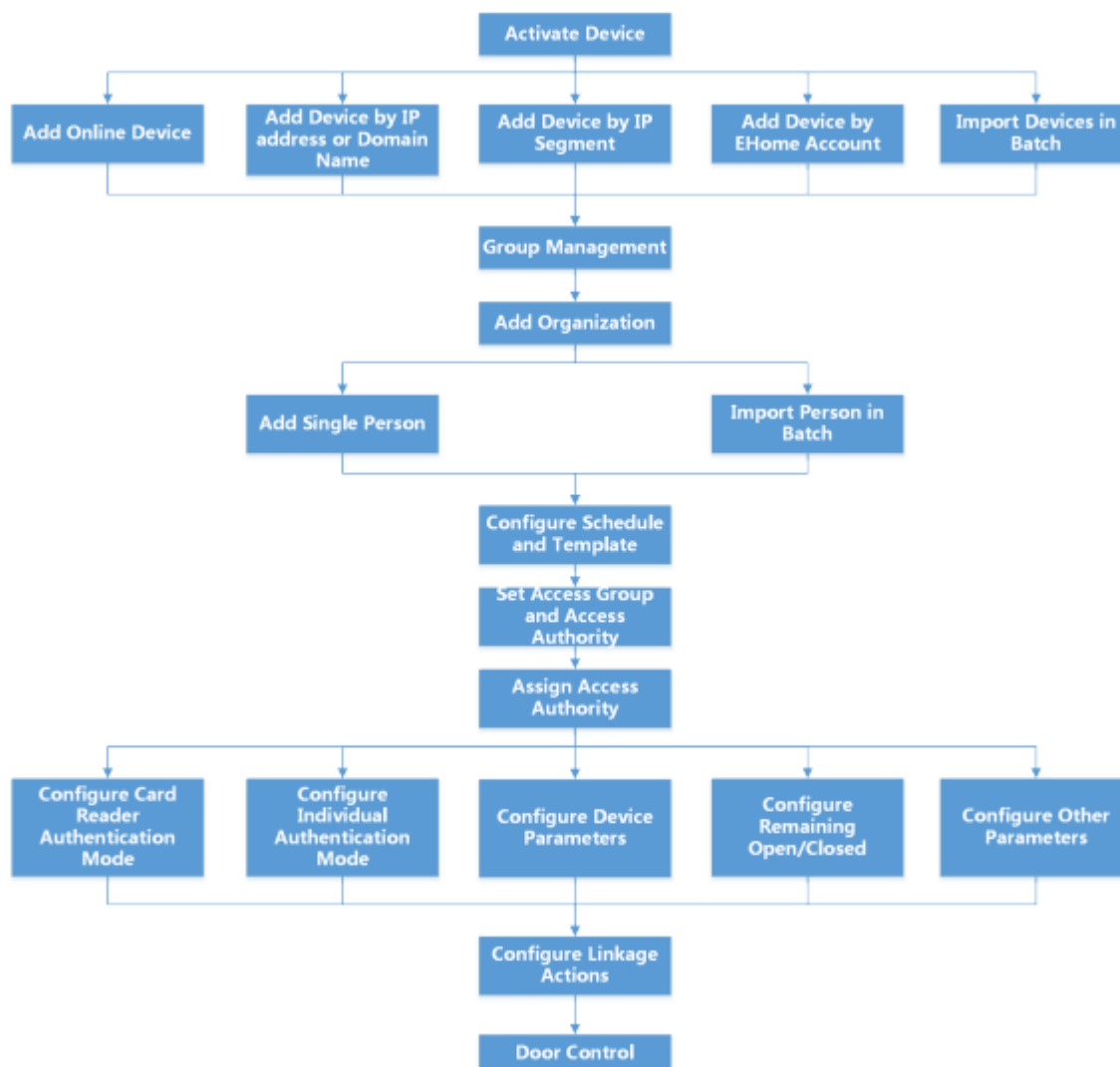


図10-1 クライアントソフトウェアでの構成のフロー図

10.2 デバイス管理

クライアントは、アクセス制御デバイスとビデオインターコムデバイスの管理をサポートしています。

例

入退室を制御し、アクセスコントロールデバイスをクライアントに追加した後で出席を管理できます。屋内ステーションとドアステーションでビデオインターホンを実行できます。

10.2.1 デバイスの追加

クライアントには、IP/ドメイン、IPセグメント、EHome プロトコルの3つのデバイス追加モードが用意されています。クライアントは、大規模なデバイスの数を追加します。

IPアドレスまたはドメイン名によるデバイスの追加

追加するデバイスのIPアドレスまたはドメイン名がわかっている場合は、IPアドレス(またはドメイン名)、ユーザー名、パスワードなどを指定して、クライアントにデバイスを追加できます。

手順

1. デバイス管理モジュールに入ります。
2. **右側のパネルの上部にある[デバイス]タブをクリックします。**
追加されたデバイスが右側のパネルに表示されます。
3. **[追加]**をクリックして[追加]ウィンドウを開き、**追加モードとして[IP/ドメイン]**を選択します。
4. 必要な情報を入力します。 **名**

前

デバイスを説明する名前を作成します。たとえば、デバイスの location や機能を示すニックネームを使用できます。

住所

デバイスの IP アドレスまたはドメイン名。

港

追加するデバイスは、同じポート番号を共有します。デフォルト値は**8000**です。

ユーザー名

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

パスワード

デバイスのパスワードを入力します。



注意

デバイスのパスワードの強度は、自動的にlyチェックできます。強くお勧めします。

自分で選択したパスワードを変更します(少なくとも3種類の大文字の文字、小文字の文字、数字、および特殊文字)を使用して、製品のセキュリティを強化します。そして、私たちはお勧めします。

パスワードは定期的に変更しますが、特に高度なセキュリティシステムでは、パスワードを毎月または毎週変更することで、製品の保護を強化できます。

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

- 5.オプション:**セキュリティ目的でTLS(Transport Layer Security)プロトコルを使用した伝送暗号化を有効にするには、**伝送暗号化(TLS)**をオンにします。
-



- 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。
 - 証明書の検証を有効にしている場合は、**[証明書ディレクトリを開く]**をクリックして、デフォルトフォルダを開き、デバイスからエクスポートされた証明書ファイルをこのデフォルトディレクトリにコピーして、セキュリティを強化します。証明書の検証の有効化の詳細については、「」を参照してください。
 - デバイスにログインして、Webブラウザで証明書を取得できます。
-

- 6. [Synchronize Time]をオンにして**、デバイスをクライアントに追加した後、クライアントを実行しているPCとデバイスの時刻を同期します。

- 7.オプション:[グループにインポート]**をオンにして、デバイス名でグループを作成し、デバイスのすべてのチャンネルをこのグループにインポートします。

例

アクセス制御デバイスの場合、そのアクセスポイント、アラーム入力/出力、およびエンコーディングチャンネル(存在する場合)がこのグループにインポートされます。

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

バッチでのデバイスのインポート

複数デバイスをクライアントにバッチで追加するには、事前定義されたCSVファイルでデバイスパラメータを入力します。

手順

1. デバイス管理モジュールに入ります。
 2. **右側のパネルの上部にある[デバイス]タブをクリックします。**
 3. **[追加]をクリックして**「追加」ウィンドウを開き、**追加モードとして**「バッチインポート」を選択します。
 4. **[テンプレートのエクスポート]**をクリックし、事前定義されたテンプレート(CSVファイル)をPCに保存します。
 5. エクスポートされたテンプレートファイルを開き、対応する列に追加するデバイスの必要な情報を入力します。
-



必要なフィールドの詳細については、テンプレートの紹介を参照してください。

モードの追加

0または1または2を入力します。

住所

デバイスのアドレスを編集します。

港

デバイスのポート番号を入力します。デフォルトのポート番号は **8000** です。

ユーザー名

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

パスワード

デバイスのパスワードを入力します。



注意

デバイスのパスワードの強度は、自動的にチェックできます。お勧めします。
自分で選択したパスワードを変更します(少なくとも3種類の大文字の文字、小文字の文字、数字、および特殊文字)を使用して、製品のセキュリティを強化します。そして、私たちはお勧めします

パスワードは定期的に変更しますが、特に高度なセキュリティシステムでは、パスワードを毎月または毎週変更することで、製品の保護を強化できます。
すべてのパスワードおよびその他のセキュリティ設定の適切な設定は、インストーラーおよび/またはエンドユーザー。

グループへのインポート

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

6. テンプレートファイルをクリックして選択します。
7. [追加]をクリックして、デバイスをインポートします。

10.2.2 デバイスパスワードのリセット

検出されたオンラインデバイスのパスワードを忘れた場合は、クライアントを介してデバイスのパスワードをリセットできます。

手順

1. デバイス管理ページに入ります。
2. [オンラインデバイス]をクリックして、オンラインデバイス領域を表示します。
同じサブネットを共有しているすべてのオンラインデバイスがリストに表示されます。
3. リストからデバイスを選択し、 操作列をクリックします。
4. デバイスのパスワードをリセットします。
-[生成]をクリックしてQRコードウィンドウをポップアップし、[ダウンロード]をクリックしてQRコードをPCに保存します。QRコードの写真を撮って携帯電話に保存することもできます。写真をテクニカルサポートに送信してください。

**メモ**

パスワードをリセットするための次の操作については、テクニカルサポートにおドアコンタクトください。

**注意**

デバイスのパスワードの強度は、自動的にlyチェックできます。製品のセキュリティを強化するために、自分で選択したパスワードを変更することを強くお勧めします(少なくとも3種類のカテゴリを含む、8文字以上、大文字の文字、小文字の文字、数字、特殊文字を含む)そして、変更することをお勧めします。

パスワードを定期的に、特に高度なセキュリティシステムでは、パスワードを毎月または毎週変更することで、製品の保護を強化することができます。

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

10.2.3 追加されたデバイスの管理

デバイスをデバイスリストに追加すると、デバイスパラメータの編集、リモート設定、デバイスステータスの表示など、追加したデバイスを管理できます。

表 10-1 追加されたデバイスの管理

デバイス編集	クリック すると、デバイス名、アドレス、ユーザー名、パスワードなどのデバイス情報を変更できます。
デバイス削除	1つ以上のデバイスをオンにし、 [削除] をクリックして選択したデバイスを削除します。
リモート設定	クリックして 、対応するデバイスのリモート構成を設定します。詳細については、デバイスのユーザーマニュアルを参照してください。
デバイスステータス表示	<p>クリック するとビュードア番号、ドアステータスなどのデバイスステータス。</p> <p> メモ</p> <p>異なるデバイスの場合、デバイスのステータスに関する異なる情報が表示されます。</p>
オンラインユーザー表示	クリック すると、ユーザー名、ユーザータイプ、IPアドレス、ログイン時間など、デバイスにアクセスするオンラインユーザーの詳細が表示されます。
デバイス情報の更新	クリックして 更新し、最新のデバイス情報を取得します。

10.3 グループ管理

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

例

たとえば、1番目のローアには、16ドア、64アラーム入力、および16アラーム出力が取り付けられています。これらのリソースを1つグループ(1st F階)に整理して、管理を便利に行うことができます。ドアのステータスを制御したり、グループごとにリソースを管理した後、デバイスの他の操作を行うことができます。

10.3.1 グループの追加

グループを追加して、追加したデバイスを整理し、管理を便利にすることができます。

手順

1. デバイス管理モジュールに入ります。
2. [デバイス管理] → [グループ] をクリックして、グループ管理ページに入ります。
3. グループを作成します。
 - [グループの追加] をクリックし、必要に応じてグループ名を入力します。
 - [デバイス名によるグループの作成] をクリックし、追加したデバイスを選択して、選択したデバイスの名前新しいグループを作成します。



メモ

このデバイスのリソース(アラーム入力/出力、アクセスポイントなど)は次のようになります。

デフォルトでグループにインポートされます。

10.3.2 グループへのリソースのインポート

デバイスリソース(アラームの入力/出力、アクセスポイントなど)を、追加したグループにバッチでインポートできます。

始める前に

デバイスを管理するためのグループを追加します。 [「グループの追加」を参照してください](#)

手順

1. デバイス管理モジュールに入ります。
2. [デバイス管理] → [グループ] をクリックして、グループ管理ページに入ります。
3. グループリストからグループを選択し、リソースタイプとして **アクセスポイント、アラーム入力、アラーム出力**などを選択します。
4. 「インポート」をクリックします。
5. サムネイル/リストビューでリソースのサムネイル/名前を選択します。



メモ

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

6. 「インポート」をクリックして、選択したリソースをグループにインポートします。

10.4 人の管理

アクセス制御、ビデオインターホン、時間と出勤などのさらなる操作のために、システムに個人情報を追加できます。にカードを発行するなど追加された人物を管理できます。それらをバッチで、個人情報をバッチでインポートおよびエクスポートするなど。

10.4.1 組織の追加

組織を追加し、その組織に個人情報をインポートして、個人の効率的な管理を行うことができます。追加した組織に対して、代理組織を追加することもできます。

手順

1. 人物モジュールに入ります。
2. 「左」列で親組織を選択し、**左上部の隅にある「追加」**をクリックして組織を追加します。
3. 追加した組織の名前を作成します。



メモ

最大10レベルの組織を追加できます。

4. **オプション:** 次の操作を実行します。

組織の編集

追加した組織にマウスを合わせ、クリックして 名前を編集します。

削除

追加した組織にマウスを合わせ、クリックして 削除します。

組織



メモ

- 組織を削除すると、下位の組織も削除されます。
- 組織の下に追加された人物がないか、組織を削除できないことを確認してください。

下位組織の

人物を表示

「サブ組織の個人を表示」を選択し、サブ組織の個人を表示する組織を選択します。

10.4.2 インポートおよびエクスポート担当者は情報を識別

複数の人物の情報と写真を一括してクライアントソフトウェアにインポートできます。また、人物情報や写真をエクスポートしてPCに保存することもできます。

個人情報のインポート

事前定義されたテンプレート(CSV / Excelファイル)に複数人の情報を入力して、情報をバッチでクライアントにインポートできます。


手順

1. 人物 モジュールに入ります。
2. リストに追加された組織を選択するか、**左上部の隅にある [追加] をクリックして組織を追加し、それを選択します。**
3. **「インポート」をクリックして「インポート」** パネルを開きます。
4. インポートモードとして**「人物情報」** を選択します。
5. **「Download Template for Import Person」** をクリックし、テンプレートをダウンロードします。
6. ダウンロードしたテンプレートに個人情報を入力します。



メモ

- ・複数カードをお持ちの方は、カードNo.をセミコロンで区切ってください。
- ・アスタリスクが付いている項目は必須です。
- ・デフォルトでは、採用日は現在の日付です。

7.  クリックして、ローカルPCから個人情報を含むCSV / Excelファイルを選択します。
8. **「インポート」をクリックしてインポートを開始します。**



メモ

- ・クライアントのデータベースにすでに人物番号が存在する場合は、既存の情報を削除してからインポートしてください。
- ・インポートできる情報は2,000人以内です。

人物の写真のインポート

追加された人物の顔写真をクライアントにインポートした後、追加された顔認証端末によって写真の人物を識別できます。人の写真を1つずつインポートできます。またはあなたの必要性に従って一度に複数の写真をインポートします。

始める前に

事前にクライアントへの個人情報をインポートしておいてください。

手順

1. 人物 モジュールに入ります。
2. リストに追加された組織を選択するか、**左上部の隅にある [追加] をクリックして組織を追加し、それを選択します。**
3. **「インポート」をクリックして「インポート」** パネルを開き、「面」をオンにします。
4. **オプション:** デバイスによる確認を**有効にして**、クライアントで管理されている顔認証デバイスが写真の顔を認識できるかどうかを確認します。

5. 顔写真をクリックして  選択します。
-



メモ

- ・ 顔写真(のフォルダ)はZIP形式である必要があります。
 - ・ 各画像ファイルはJPG形式であり、200KB以下である必要があります。
 - ・ 各写真には「Person ID Name」という名前を付けます。ユーザー ID は、インポートされた個人情報と同じである必要があります。
-

6. 「インポート」をクリックしてインポートを開始します。

インポートの進行状況と結果が表示されます。

エクスポート担当者情報

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

始める前に

組織に個人を追加していることを確認します。

手順

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



メモ

組織を選択しない場合、すべての人の情報がエクスポートされます。

3. 「エクスポート」をクリックして「エクスポート」パネルを開きます。

4. エクスポートするコンテンツとして **人物情報** をオンにします。

5. エクスポートするアイテムを確認します。

6. [エクスポート]をクリックして、エクスポートしたファイルをPC上のCSV/Excelファイルに保存します。

人物の写真のエクスポート

追加した人の顔写真をエクスポートして、PCに保存できます。

始める前に

組織に人物とその顔写真を追加したことを確認します。

手順

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



メモ

組織を選択しない場合、すべての人の顔写真がエクスポートされます。

3. 「エクスポート」をクリックして「エクスポート」パネルを開き、**エクスポートするコンテンツ**として「面」をオンにします。

4. 「エクスポート」をクリックしてエクスポートを開始します。
-



メモ

- ・エクスポートされたファイルはZIP形式です。
 - ・エクスポートされた顔写真には「人物 ID_Name_0」という名前が付けられます(「0」は正面顔の場合)。
-

10.4.3 アクセス制御デバイスからの人物情報の取得

追加されたアクセス制御デバイスが個人情報(個人の詳細、発行されたカード情報を含む)で構成されている場合は、から個人情報を取得できます。

デバイスを作成し、クライアントにインポートしてさらに操作します。

手順



メモ

- ・デバイスに保存されている人名が空の場合、クライアントにインポート後、発行されたカード番号で人名が登録されます。
 - ・デバイスに保存されているカード番号または人物ID(従業員ID)がクライアントデータベースにすでに存在する場合、このカード番号または人物IDを持つ人物はクライアントにインポートされません。
-

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



メモ

登録ステーションを選択した場合は、**[ログイン]**をクリックし、デバイスのIPアドレス、ポート番号、ユーザー名、パスワードを設定する必要があります。

5. **「インポート」**をクリックして、クライアントへ個人情報のインポートを開始します。
-



メモ

最大2,000人、5,000枚のカードがインポートできます。

個人情報、個人の詳細を含む、リンクされたカード(設定されている場合)が選択した組織にインポートされます。

10.4.4 バッチで人にカードを発行する

クライアントは、複数の人にバッチでカードを発行する便利な方法を提供します。

手順

1. **人物モジュール**に入ります。
-

2. 「発行カードのバッチ処理」をクリックします。


カードが発行されていないすべての追加された人物は、右側のパネルに表示されます。

3. オプション: 入力ボックスにキーワード(名前または人ID)を入力して、カードを発行する必要がある人を選択します。
4. オプション: 設定をクリックして、カード発行パラメータを設定します。詳細は、ローカルモードでカードを発行するを参照してください。
5. 「Initiize」をクリックして、カード登録ステーションまたはカードリーダーを開始し、カードを発行できる状態にします。
6. カード番号をクリックします。列にカード番号を入力します。
 - カードをカード登録ステーションに置きます。
 - カードリーダーでカードをスワイプします。
 - カード番号を手動で入力し、**Enter** キーを押します。リストに記載されている人物にはカードが発行されます。


10.4.5 通知表の紛失

その人がカードを紛失した場合は、カードの紛失を報告して、カードに関連するアクセス認証が無効になるようにすることができます。

手順

1. 人物モジュールに入ります。
2. カードの紛失を報告する相手を選択し、「編集」をクリックして「人物の編集」ウィンドウを開きます。
3. 「認証情報→カード」パネルで、 追加したカードをクリックして、このカードを紛失カードとして設定します。

カードの紛失を報告した後、このカードのアクセス認証は無効になり、非アクティブになります。このカードを受け取った他の人は、この紛失したカードをスワイプしてもドアにアクセスできません。

4. オプション: 紛失したカードが見つかった場合はクリックして  紛失をキャンセルできます。カードの紛失をキャンセルすると、その人のアクセス認証が有効になり、アクティブになります。
5. 紛失したカードが1つのアクセスグループに追加され、アクセスグループがデバイスに適用されている場合

すでに、カードの紛失を報告したり、カードの紛失をキャンセルしたりすると、デバイスに変更を適用するように通知するウィンドウがポップアップ表示されます。デバイスに適用した後、これらの変更はデバイスに反映される可能性があります。

10.4.6 カード発行パラメータの設定

クライアントには、カードの番号を読み取るための2つのモードがあります: カード登録ステーション経由またはアクセス制御デバイスのカードリーダー経由。カード登録ステーションが利用可能な場合は、USBインター顔またはCOMでクライアントを実行しているPCに接続し、カードをカード登録に置いてカード番号を読み取ります。そうでない場合は、追加されたアクセス制御デバイスのカードリーダーでカードをスワイプして、カード番号を取得することもできます。そのため、1人の人にカードを発行する前に、発行モードや関連パラメータなどのカード発行パラメータを設定する必要があります。

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

ローカルモード:カード登録ステーションでカードを発行

クライアントを実行しているPCにカード登録ステーションを接続します。カードをカード登録ステーションにセットして、カード番号を取得できます。

カード登録ステーション

接続されたカード登録ステーションのモデルを選択します。



現在、サポートされているカード登録ステーションのモデルには、DS-K1F100-D8、DS-K1F100-M、DS-K1F100-D8E、DS-K1F180-D8Eが含まれます。

カードの種類

このフィールドは、モデルがDS-K1F100-D8EまたはDS-K1F180-D8Eの場合にのみ使用できます。実際のカードの種類に合わせて、カードの種類をEMカードまたはICカードからお選びください。

シリアルポート

DS-K1F100-Mのときのみ利用可能です。

カード登録ステーションが接続するCOMを選択します。

振動音

カード番号が正常に読み取られたときのブーンという音を有効または無効にします。

カード番号種類

実際のニーズに応じてカード番号の種類を選択します。

M1カードの暗号化

このフィールドはモデルがDS-K1F100-D8、DS-K1F100-D8E、またはDS-K1F180-D8Eの場合にのみ使用できます。カードがM1カードで、M1カード暗号化機能を有効にする必要がある場合は、次のことを行う必要があります。

この機能を有効にし、暗号化するカードのセクターを選択します。

リモートモード:カードリーダーでカードを発行

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

10.5 スケジュールとテンプレートの構成

休日と週のスケジュールを含むテンプレートを構成できます。テンプレートを設定した後、アクセスグループを設定するときに、設定されたテンプレートをアクセスグループに適用できるため、アクセスグループはテンプレートの期間に影響を及ぼします。



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

10.5.1 休日を追加

休日を作成し、開始日、終了日、1日の休日期間など、休日の日数を設定できます。

手順

メモ

ソフトウェアシステムには、最大64の休日を追加できます。

1. 「アクセス制御」→「休日→スケジュール」をクリックし、休日ページに入ります。
2. 「左」パネルで「追加」をクリックします。
3. 休日の名前を作成します。
4. **オプション:** この休日の説明またはいくつかの通知を[備考]ボックスに入力します。
5. 休日リストに休日の期間を追加し、休日の期間を設定します。







メモ

1つの休日に最大16の休日期間を追加できます。

- 1) **ホリデーリストフィールド**で[追加]をクリックします。
- 2) カーソルをドラッグして期間を描画し、その期間に設定されたアクセスグループがアクティブになります。

メモ

1つの休日期間に最大8つの期間を設定できます。

- 3) **オプション:** 次の操作を実行して、期間を編集します。
 - ・カーソルを期間に移動し、タイムラインバーの期間をカーソルが変わったときの目的の位置 。
 - ・期間をクリックし、表示されたダイアログで開始/終了時間を直接編集します。
 - ・カーソルを期間の開始または終了に移動し、カーソルが  に変わったときにドラッグして期間を長くしたり短くしたりします 。
 - 4) **オプション:** 削除する必要のある期間を選択し、 操作列をクリックして選択した期間を削除します。
 - 5) **オプション:**  操作列をクリックして、タイムバー内のすべての期間をクリアします。
 - 6) **オプション:**  操作列をクリックして、この追加された休日期間を休日リストから削除します。
6. 「保存」をクリックします。

10.5.2 テンプレートの追加

テンプレートには、週のスケジュールと休日が含まれています。週のスケジュールを設定し、異なる個人またはグループのアクセス認証の期間を割り当てることができます。テンプレートに追加された休日を選択することもできます。

手順

メモ

ソフトウェアシステムには、最大255個のテンプレートを追加できます。

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

メモ

デフォルトのテンプレートには、終日認証済みと終日拒否の2つがあり、編集や削除はできません。

終日オーソリゼーション

アクセス認証は各曜日で有効で、休日はありません。


終日拒否

アクセス認証は、曜日ごとに無効であり、休日はありません。

2. 「左」パネルの「追加」をクリックして、新しいテンプレートを作成します。
 3. テンプレートの名前を作成します。
 4. このテンプレートの説明または通知を[備考]ボックスに入力します。
 5. 週のスケジュールを編集して、テンプレートに適用します。
 - 1) 下部パネルの[週スケジュール]タブをクリックします。
 - 2) 曜日を選択し、タイムラインバーに期間を描画します。
-

メモ

週のスケジュールの各日に最大8つの期間を設定できます。

- 3) オプション: 次の操作を実行して、期間を編集します。
 - カーソルを期間に移動し、タイムラインバーの期間をカーソルがに変わったときの目的の位置。 
 - 期間をクリックし、表示されたダイアログで開始/終了時間を直接編集します。
 - カーソルを期間の開始または終了に移動し、カーソルがに変わったときにドラッグして期間を長くしたり短くしたりします。
 - 4) 上記の2つの手順を繰り返して、他の曜日でより多くの期間を描画します。
6. 休日を追加して、テンプレートに適用します。
-

メモ

1つのテンプレートに最大4つの休日を追加できます。

- 1) [休日]タブをクリックします。
 - 2) 左リストで休日を選択すると、右側のパネルの選択リストに追加されます。
-

3) **オプション**: [追加] をクリックして、新しい休日を追加します。



休日の追加については、**休日の追加を参照してください**。

4) **オプション**: 右側のリストで選択した休日を選択し、クリックして 選択した休日を削除するか、クリアをクリックして右側のリストで選択したすべての休日をクリアします。

7. [保存] をクリックして設定を保存し、テンプレートの追加を終了します。

10.6 アクセス権限を人に割り当てるためのアクセスグループの設定

ユーザーを追加し、そのユーザーの認証情報を構成した後、アクセスグループを作成して、どのユーザーがどのドアにアクセスできるかを定義し、アクセスグループをアクセス制御デバイスに適用して有効にすることができます。

始める前に

- ・クライアントに人を追加します。
- ・アクセス制御デバイスをクライアントおよびグループアクセスポイントに追加します。
詳細は、[グループ管理を参照してください](#)。
- ・テンプレートを追加します。

手順

アクセスグループの設定を変更した場合は、アクセスグループをデバイスに再度適用して有効にする必要があります。アクセスグループの変更には、テンプレート、アクセスグループの設定、個人のアクセスグループの設定、および関連する個人の詳細(カード番号、顔など)の変更が含まれます。

写真、カード番号の紐付け、カード番号の紐付け、カードのパスワード、カードの有効期限など)。

1. [Access Group] → [アクセス制御] → [Authorization] をクリックし、アクセスグループインターフェースに入ります。
2. 「追加」 をクリックし、「追加」ウィンドウを開きます。
3. 「名前」テキスト「フィールド」で、必要に応じてアクセスグループの名前を作成します。
4. アクセスグループのテンプレートを選択します。



アクセスグループ設置の前にテンプレートを構成する必要があります。詳細については、[スケジュールとテンプレートの設定を参照してください](#)。

5. 「人物フィールド選択」の「左」リストで、アクセス権限を割り当てる人物を選択します。
6. アクセスポイント選択フィールドの左リストで、選択した人がアクセスするドア、ドアステーション、またはルーターを選択します。
7. [保存] をクリックします。

選択したユーザーと選択したアクセスポイントをインター顔の右側に表示できます。

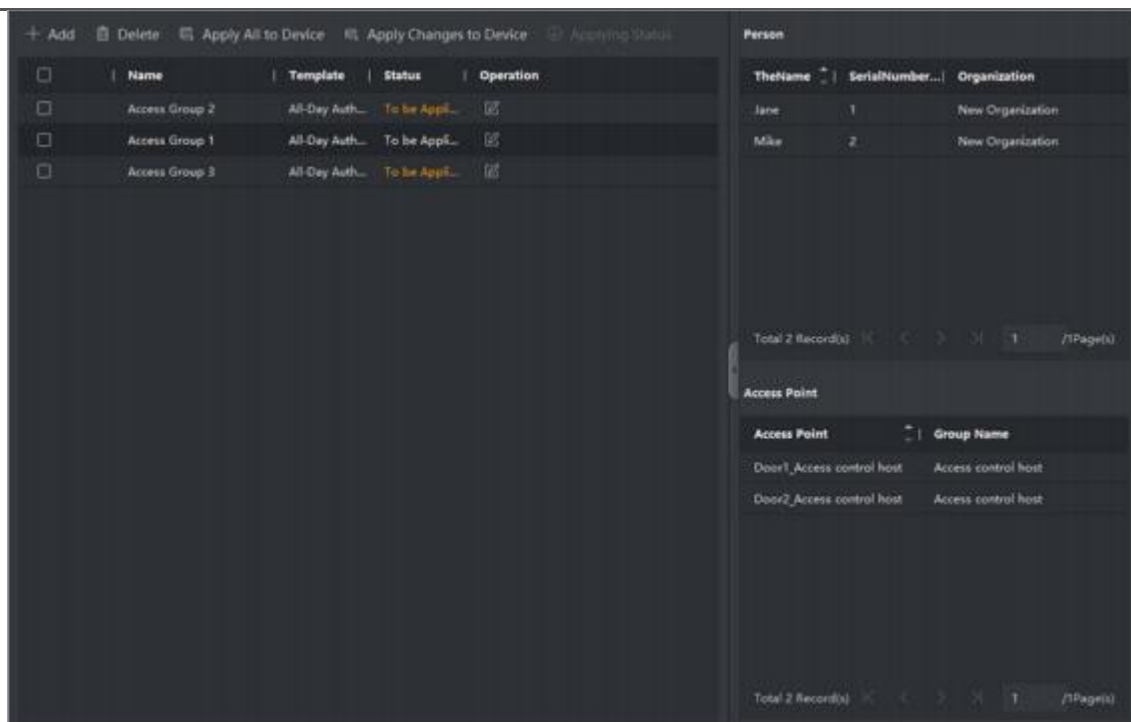


図 10-2 選択した人物とアクセスポイントの表示

8. アクセスグループを追加した後、効果を得るためにそれらをアクセス制御デバイスに適用する必要があります。

- 1) アクセス制御デバイスに適用するアクセスグループを選択します。
- 2) [すべてデバイスに適用]をクリックし、選択したすべてのアクセスグループをアクセス制御デバイスまたはドアステーションに適用し始めます。
- 3) [すべてデバイスに適用]または[変更をデバイスに適用]をクリックします。

すべてデバイスに適用

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

デバイスへの変更の適用


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

- 4) [ステータス]列で適用ステータスを表示するか、[適用ステータス]をクリックして適用されたすべてのアクセスグループを表示します。

メモ

[Display Flure Only]をオンにすると、適用結果を確認できます。

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

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



メモ

ユーザーのアクセス情報またはその他の関連情報を変更すると、クライアントの右隅に「アクセスグループ to Be Apply」というプロンプトが表示されます。

プロンプトをクリックして、変更したデータをデバイスに適用できます。[Apply Now] または [Apply Later] を選択できます。

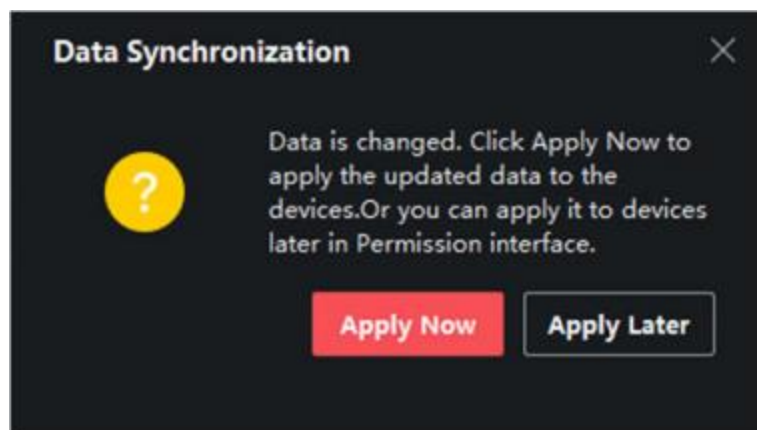



図10-3 データ同期

10.7 高度な機能の設定

アクセス制御の高度な機能を設定して、さまざまなシーンでいくつかの特別な要件を満たすことができます。



メモ

- カード関連機能(アクセス制御カードの種類)については、カードを追加すると、アクセスグループが適用されたカードのみが表示されます。
- 高度な機能は、デバイスでサポートされている必要があります。
- Advanced Functionにカーソルを合わせてから、クリックして、 表示するAdvanced Functionをカスタマイズします。

10.7.1 デバイスパラメータの設定

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

アクセス制御デバイスのパラメータの設定


アクセス制御デバイスを追加した後、画像へのユーザー情報のオーバーレイ、キャプチャ後の画像のアップロード、キャプチャした写真の保存など、パラメーターを構成できます。

手順

1. 「アクセス制御」→「拡張機能」→「デバイスパラメータ」をクリックします。
-



メモ

[Advanced Function] リストに [Device Parameter] がある場合は、カーソルを [Advanced Function] にマウスポインタを置き、 表示するデバイスパラメータをクリックして選択します。

2. アクセスデバイスを選択して、そのパラメータを右側のページに表示します。
 3. スイッチをONにして、対応する機能を有効にします。
-



メモ

表示されるパラメータは、アクセスコントロールデバイスによって異なる場合があります。

- 以下のパラメータの一部が「基本情報」ページにリストされていない場合は、「詳細」をクリックしてパラメータを編集します。
-

音声プロンプト

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

写真をアップロードAfterリンクキャプチャ

リンクされたカメラで撮影した画像をシステムに自動的にアップロードします。

写真を保存します。Afterリンクキャプチャ

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

顔認証モード:ノーマル

モード

通常どおりカメラで顔を認識します。

ディープモード

このデバイスは、通常モードよりもはるかに広い範囲を認識できます。このモードは、より複雑な環境に適用できます。

NFCカードを有効にする

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

M1カードを有効にする

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

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



メモ

周辺機器カードリーダーがEMカードの表示をサポートしている場合、EMカード機能を有効/無効にする機能もサポートされています。

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

ドア/エレベーターのパラメータの設定

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

始める前に

アクセス制御デバイスをクライアントに追加します。

手順

1. 「アクセス制御」→「拡張機能」→「デバイスパラメータ」をクリックします。
 2. 左パネルでアクセス制御デバイスを選択し、クリックして 選択したデバイスのドアまたはドアを表示します。
 3. ドアまたはドアを選択して、そのパラメーターを右側のページに表示します。
 4. ドアまたはドアのパラメータを編集します。
-



メモ

表示されるパラメータは、アクセスコントロールデバイスによって異なる場合があります

- 以下のパラメータの一部が「基本情報」ページにリストされていない場合は、「詳細」をクリックしてパラメータを編集します。
-

名前

必要に応じて、カードリーダーの名前を編集します。

Byおドアコンタクト

ドアセンサーは、閉じたまままたは開いたままに設定できます。通常、閉じたままです。

終了ボタンの種類

終了ボタンは、閉じたまままたは開いたままに設定できます。通常、開いたままです。

ドアロック時間

通常のカードをスワイプしてアクションをリレーすると、ドアをロックするためのタイマーが作動し始めます。

オープン期間の延長

ドアの連絡先は、拡張アクセスが必要な人が自分のカードをスワイプした後、適切な遅延で有効にすることができます。

ドアオープンタイムアウトアラーム

アラームは、設定された時間内にドアが閉じられていない場合にトリガーできます。0に設定すると、アラームはトリガーされません。

ドアが閉じたときにドアロック

ドアが閉まると、**ドアロック時間**に達していなくてもロックできます。

強要コード

ドアは、強要があるときに強要コードを入力することで開くことができます。同時に、クライアントは強要イベントを報告できます。

スーパーパスワード

特定の人は、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。

コード閉じる

カードリーダーのブザーを停止するために使用できる無視コードを作成します(キーパッドに無視コードを入力します)。



メモ

- 強要コード、スーパーコード、および却下コードは異なる必要があります。
- 強要コード、スーパーパスワード、および解除コードは、認証パスワードとは異なる必要があります。
- 強要コード、スーパーパスワード、および却下コードの長さはデバイスに応じており、通常は4〜8桁を含める必要があります。

5. [OK]をクリックします。

6. オプション:[コピー先]をクリックし、ドア/部屋を選択して、ページ内のパラメーターを選択したドア/部屋にコピーします。



メモ

ドアまたはローアのステータス期間の設定は、選択したドア/ローアにもコピーされます。

カードリーダーのパラメータの設定

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

始める前に

アクセス制御デバイスをクライアントに追加します。

手順

1. 「アクセス制御」→「拡張機能」→「デバイスパラメータ」をクリックします。
2. 左のデバイスリストで、ドアをクリックして 展開し、カードリーダーを選択すると、右側でカードリーダーのパラメーターを編集できます。
3. 「基本情報」ページでカードリーダーの基本パラメーターを編集します。



メモ

- 表示されるパラメータは、アクセスコントロールデバイスによって異なる場合があります。パラメータの一部は次のようにリストされています。詳細については、デバイスのユーザーマニュアルを参照してください。
 - 以下のパラメータの一部が「基本情報」ページにリストされていない場合は、「詳細」をクリックしてパラメータを編集します。
-

名前

必要に応じて、カードリーダーの名前を編集します。

OKLED極性/エラーLED極性/ブザー極性

カードリーダーのパラメータに従って、メインボードのOKLED極性/エラーLED極性/ブザーLEDの極性を設定します。通常、デフォルトの設定を採用しています。

最小カードスワイプ間隔

同じカードのカードスワイプの間隔が設定値より短い場合、カードスワイプは無効となります。0から255に設定できます。

PWD入力時の最大インターバル

カードリーダーにパスワードを入力したとき、2つを押す間隔が空いていれば番号が設定値より大きい場合、前に押した番号は自動的にクリアされます。

最大失敗試行数のアラーム

カードの読み取り試行が設定値に達したときにアラームを報告するように有効にします。

カード故障の最大回数

カードの読み取りの最大失敗回数を設定します。

タンパー検出

カードリーダーの改ざん防止検出を有効にします。

コントローラーとの通信間隔

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

ブーンという時間

カードリーダーのブーンという時間を設定します。使用可能な時間の範囲は0から5,999秒です。0は、連続したブーンという音を表します。

カードリーダータイプ/カードリーダーの説明

カードリーダーの種類と説明を取得します。これらは読み取り専用です。

デフォルトのカードリーダー認証モード

デフォルトのカードリーダー認証モードを表示します。

フィンガープリント容量

使用可能なフィンガープリントの最大数を表示します。

スコア

デバイスは、ヨー角、ピッチ角、および瞳孔距離。スコアが設定値より小さい場合、顔認証は失敗します。

顔認証タイムアウト値

認識時間が設定された時間よりも長い場合、デバイスは通知します。

顔認証インターバル

認証時の2つの連続した顔認証の時間間隔。デフォルトでは、2秒です。

Face 1:1 マッチングしきい値

1:1 マッチングモードで認証する場合、マッチングしきい値を設定します。値が大きいほど、認証時の誤受け入れ率が小さくなり、誤拒否率が大きくなります。

1:N セキュリティ・レベル

1:N マッチングモードで認証する場合のマッチングセキュリティレベルを設定します。大きいvalueの場合、認証時の偽の受け入れ率が小さくなり、偽の拒否率が大きくなります。

ライブ顔検出

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、デバイスはその人が生きているかどうかを認識できます。

ライブ顔検出のセキュリティレベル

ライブ顔検出機能を有効にした後、ライブ顔認証を実行する際の照合セキュリティレベルを設定できます。

顔認証のAttemPtsの失敗最大。

ライブ顔検出の失敗試行の最大数を設定します。設定された試行回数を超えてライブ顔検出が失敗した場合、システムはユーザーの顔を5分間ロックします。同じユーザーは5分以内に偽の顔で認証できません。5分以内に、ユーザーは実際の顔を介して2回連続して認証してロックを解除できます。

認証失敗顔のロック

ライブ顔検出機能を有効にすると、システムはユーザーの顔を5秒間ロックします。ライブ顔検出が設定された試行回数を超えて失敗した場合は分。同じユーザーが偽の顔で5分以内に認証できなくなります。5分以内に、ユーザーは実際の顔を介して2回連続して認証してロックを解除できます。

アプリモード

実際の環境に応じて、屋内または他のアプリケーションモードを選択できます。

4. [OK]をクリックします。

5. オプション:[コピー先]をクリックし、カードリーダーを選択して、ページ内のパラメーターを選択したカードリーダーにコピーします。


アラーム出力のパラメータの設定

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

始める前に

アクセス制御デバイスをクライアントに追加し、デバイスがアラーム出力をサポートしていることを確認します。

手順

1. 「アクセス制御」 → 「Advanced Function」 → 「Device Parameter」 をクリックして、アクセス制御パラメータの設定ページに入ります。
2. 左のデバイスリストで、ドアをクリックして  展開し、アラーム入力を選択すると、右側でアラーム入力のパラメータを編集できます。
3. アラーム出力パラメータを設定します。

名前

必要に応じて、カードリーダーの名前を編集します。

アラーム出力アクティブ時間

トリガーされた後、アラーム出力が持続する時間。

4. [OK] をクリックします。
5. オプション: 右上隅のスイッチをONに設定して、アラーム出力をトリガーします。

10.7.2 デバイスパラメータの設定

アクセス制御デバイスを追加した後、ネットワークパラメータなどのパラメータを設定できます。

顔認証端末のパラメータを設定する

顔認証端末の場合、顔画像データベース、QRコード認証などのパラメータを設定できます

手順

メモ

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. アクセス制御モジュールに入ります。
2. 左のナビゲーションバーで、「Advanced Function」 → 「More Parameters」と入力します
3. デバイスリストでアクセス制御デバイスを選択し、[顔認証端末] をクリックします。
4. パラメータを設定します。



メモ

表示されるこれらのパラメータは、異なるデバイスモデルによって異なります。

COM (英語)

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

顔写真データベース

顔画像データベースとして [Deep Learning] を選択します。

QRコードによる認証

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

ブロックリスト認証

有効にすると、デバイスはアクセスするユーザーとブロックリスト内のユーザーを比較します。

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

一致しない場合(ユーザーがブロックリストにない場合)、アクセスは許可されます。

認証用の顔画像保存

有効にすると、認証時にキャプチャされた顔写真がデバイスに保存されます。

MCUバージョン

デバイスのMCUバージョンを表示します。

5. [保存]をクリックします。

RS-485 パラメータの設定

アクセス制御デバイスのRS-485パラメータには、ボーレート、データビット、ストップビット、パリティタイプ、ローコントロールタイプ、通信モード、ワークモード、接続モード。

手順



メモ

RS-485セトリングは、デバイスでサポートされている必要があります。

1. アクセス制御モジュールに入ります。
2. 左のナビゲーションバーで、「**Advanced Function**」 → 「**More Parameters**」と入力します。
3. デバイスリストでアクセス制御デバイスを選択し、**[RS-485]**をクリックしてRS-485設定ページに入ります。
4. ドロップダウンリストからシリアルポート番号を選択して、RS-485パラメータを設定します。
5. シリアル番号、外部デバイス、認証センター、ボーレート、データビット、ストップビット、パリティタイプ、低制御タイプ、通信モード、および動作モードをドロップダウンリストに設定します。

6. 「保存」をクリックします。

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

ウィーガンドパラメータの設定

アクセス制御デバイスのウィーガンドチャンネルと通信モードを設定できます。ウィーガンドパラメータを設定した後、デバイスはウィーガンド通信を介してウィーガンドカードリーダーに接続できます。

手順

メモ

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. アクセス制御モジュールに入ります。
2. 左のナビゲーションバーで、「**Advanced Function**」 → 「**More Parameters**」と入力します。
3. デバイスリストでアクセス制御デバイスを選択し、**[Wiegand]**をクリックしてWiegand設定ページに入ります。
4. スイッチをオンに設定して、デバイスのウィーガンド機能を有効にします。
5. ドロップダウンリストからウィーガンドチャンネル番号と通信モードを選択します。

メモ

[通信方向]を**[送信]**に設定した場合は、**[ウィーガンドモード]**を**[ウィーガンド 26]**または**[ウィーガンド 34]**に設定する必要があります。

6. **[ウィーガンドを有効にする]**を**オン**にして、ウィーガンド機能を有効にします。
7. **[保存]**をクリックします。

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

M1カードの暗号化を有効にする

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

手順

メモ

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

1. アクセス制御モジュールに入ります。
2. 左のナビゲーションバーで、「**Advanced Function**」 → 「**More Parameters**」と入力します。

3. デバイスリストでアクセス制御デバイスを選択し、**[M1カード暗号化の検証]**をクリックして、M1カード暗号化の検証ページに入ります。

4. スイッチをオンに設定して、M1カードの暗号化機能を有効にします。
5. セクターIDを設定します。



メモ

- ・セクタIDの範囲は1～100です。
- ・デフォルトでは、セクター13は暗号化されています。セクター13を暗号化することをお勧めします。

6. 「保存」をクリックして、設定を保存します。

10.8 ドアコントロール

モニタリングモジュールでは、追加されたドアの管理下にあるドアのリアルタイムステータスを表示できます。

アクセス制御デバイス。ドアの開閉などのドアを制御したり、そのままにしたりすることもできます。

ドアはクライアントを介してリモートで開閉します。このモジュールでは、リアルタイムアクセスイベントが表示されます。アクセスの詳細と人物の詳細を表示できます。



メモ

ドア制御権限を持つユーザーは、監視モジュールに入り、ドアを制御できます。または、制御に使用されるアイコンが表示されなくなります。ユーザー権限の設定については、以下を参照してください。

パーソンマネジメント。

10.8.1 コントロールドアのステータス

ドアのロック解除、ドアのロック、ドアのロック解除のまま、ドアのロックのまま、すべてのロック解除のままなど、ドアのステータスを制御できます。

始める前に

- ・人を追加し、設計された人にアクセス権限を割り当てると、人はアクセスポイント(ドア)へのアクセス権限を持つこととなります。詳細は、**人物管理**と**設定を参照してくださいアクセス権限を人に割り当てるためのアクセスグループ**。
- ・操作ユーザーがアクセスポイント(ドア)の許可を得ていることを確認してください。詳細については、「」を参照してください。

手順

1. **[監視]**をクリックして、ステータス監視ページに入ります。
2. 右上隅でアクセスポイントグループを選択します。



メモ

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

選択したアクセス制御グループのドアが表示されます。

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



メモ

[Remn All Unlocked] と [Remn All Locked] では、この手順を無視します。

4. 次のボタンをクリックして、ドアを制御します。

アンロック

ドアがロックされたら、ロックを解除すると、一度だけ開きます。開室時間が経過すると、ドアは自動的に閉じられ、再びロックされます。

錠

ドアのロックが解除されたら、ドアをロックすると閉じられます。アクセス権限を持っている人は、資格情報でドアにアクセスできます。

アンロックされたまま

ドアはロックが解除されます(閉じていても開いていても)。すべての人がドアにアクセスできるのは、何の信用も必要ありません。

ロックされたまま

ドアは閉められ、施錠されます。スーパーユーザーを除いて、許可された資格情報を持っていても、誰もドアにアクセスすることはできません。

すべてアンロックされたまま

グループ内のすべてのドアのロックが解除されます(閉じていても開いていても関係ありません)。すべての人がドアにアクセスできるのは、無理である。

すべてロックされたまま

グループ内のすべてのドアは閉じられ、ロックされます。

スーパーユーザーを除いて、認定された資格情報を持っています。

キャプチャ

写真を手動でキャプチャします。



メモ

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

結果

操作が成功すると、操作に応じてドアのアイコンがリアルタイムで変化します。

10.8.2 リアルタイムアクセスレコードの確認

アクセスレコードは、カードスワイプレコード、顔認証など、リアルタイムで表示されます。記録などアクセス時に撮影した画像や人物情報を閲覧することができます。

手順

1. 「**モニタリング**」をクリックし、右上隅のドロップダウンリストからグループを選択します。

選択したグループのドアでトリガーされたアクセスレコードは、リアルタイムで表示されます。カード番号、人名、組織、イベント時間など、レコードの詳細を表示できます。

2. **オプション**: イベントタイプとイベントステータスを確認して、イベントが検出された場合にこれらのイベントがリストに表示されるようにします。チェックされていないタイプまたはステータスのイベントはリストに表示されません。

3. **オプション**: 「Show Latest Event」に**チェックを入れる**と、最新のアクセスレコードが選択され、レコードリストの上部に表示されます。

4. **オプション**: イベントをクリックして、人の写真を含むアクセスした人の詳細を表示します。

(キャプチャー写真と添付)、人番号、人名、所属、電話番号、連絡先など



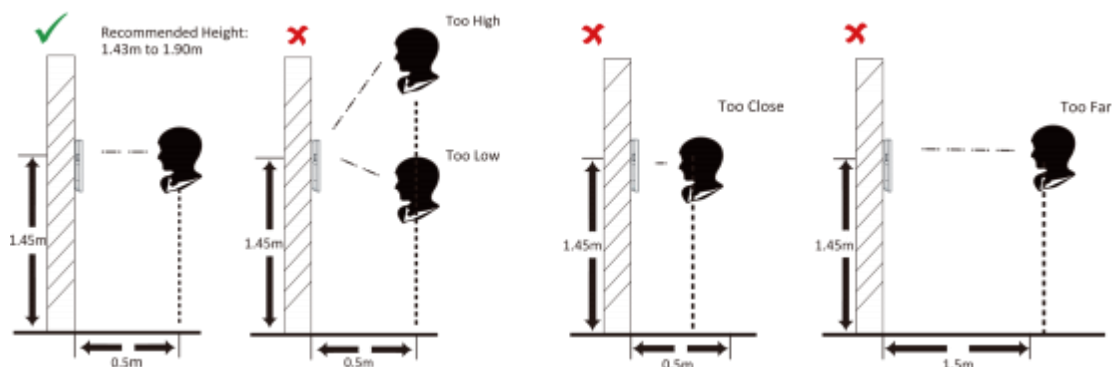
キャプチャした画像をダブルクリックして拡大し、詳細を表示できます。

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

付録A.顔を収集する/比較する際のヒント画像

顔写真を収集するまたは比較するときの位置は次のとおりです。

位置(推奨距離:0.5 m)



表現

- 下の写真の表情のように、顔写真を組み合わせたり比較したりするときは、自然な表情を保ちます。



- 帽子、サングラス、または顔認証機能に影響を与える可能性のあるその他のアクセサリを着用しないでください。
- 髪の毛に目や耳などを隠したり、濃い化粧は禁止です。

姿勢

高品質で正確な顔写真を撮るには、顔写真を写真と比較するときに、カメラに向かって顔を配置します。



大きさ

顔が収集するウィンドウの中央にあることを確認してください。



付録B. Installation環境のヒント

1. 光源照度基準値



キャンドル:10ルクス



電球:100~850Lux

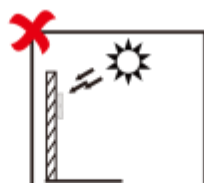


日光:1200ルクス以上

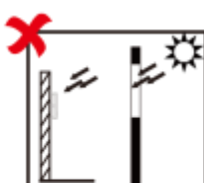
2. 逆光、直射日光、間接光を避けてください。



Backlight



Direct Sunlight



Direct Sunlight
through Window

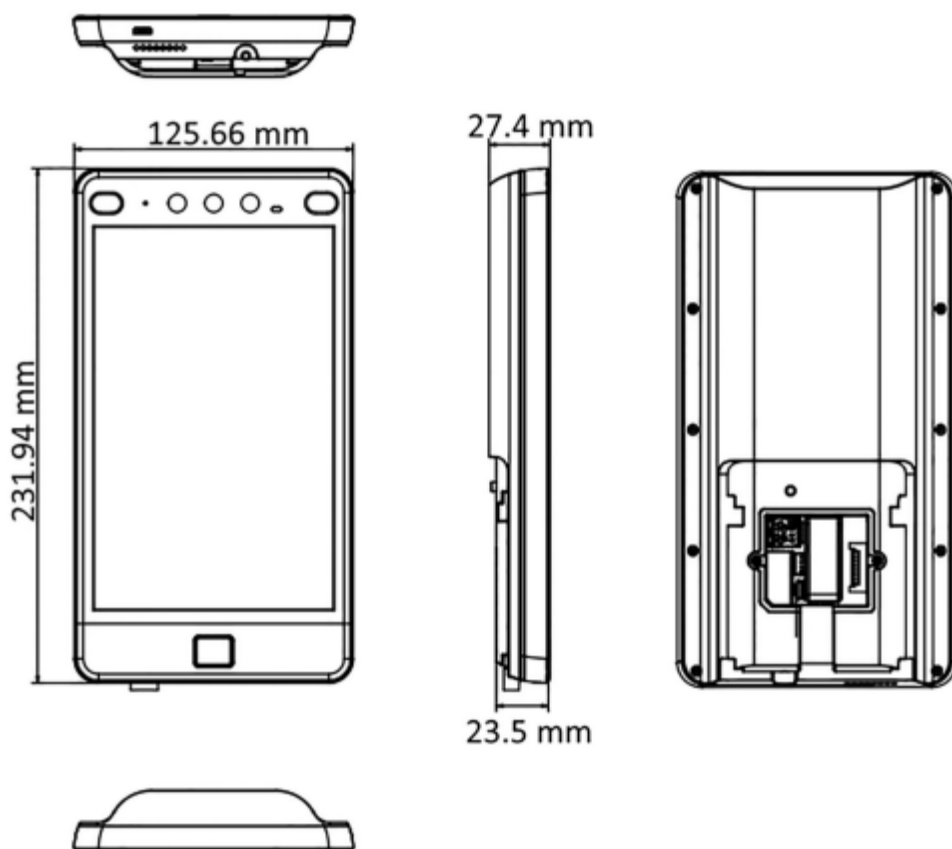


Indirect Light
through Window



Close to Light

付録C.寸法



図D-1 寸法

付録D.通信マトリックスとデバイスコマンド

コミュニケーションマトリックス

次のQRコードをスキャンして、デバイスの通信マトリックスを取得します。

マトリックスには、シーテクのアクセス制御およびビデオインターコムデバイスのすべての通信ポートが含まれていることに注意してください。



図E-1 通信マトリックスのQRコード

デバイスコマンド

次のQRコードをスキャンして、デバイスの一般的なシリアルポートコマンドを取得します。

コマンドリストには、すべてのシーテクアクセス制御およびビデオインターコムデバイスで一般的に使用されるすべてのシリアルポートコマンドが含まれていることに注意してください。



図 E-2 デバイスコマンド

