顔認証 AI サーマルカメラ
取扱説明書

アイリスオーヤマ株式会社
IoT ソリューション事業部

法的情報

このマニュアルについて

このマニュアルには、本製品の使用および管理に関する説明が含まれています。以降の画像、チャート、画像およびその他の情報は、説明および説明のみを目的としています。本書に記載されている情報は、ファームウェアのアップデートなどにより予告なく変更される場合があります。本マニュアルの最新版は、当社ウェブサイトでご確認ください。本マニュアルは、製品のサポートについて訓練を受けた専門家の指導と援助を受けて使用してください。

商標について

記載されている商標およびロゴは、それぞれの所有者の所有物です。

リーガル・ディスクレイマー

適用される法規により許容される最大範囲内で、本マニュアルおよび説明される製品は、そのハードウェア、ソフトウェアおよびファームウェアと共に、「現状のまま」および「すべての故障およびエラーと共に」提供されます。当社は、明示または黙示を問わず、特定の目的に対する商品性、満足できる品質、または適合性を含め、いかなる保証も行いません。お客様による製品の使用は、お客様自身のリスクに基づきます。いかなる場合においても、当社は、契約違反、不法行為（過失を含む）、製品責任、またはその他製品の使用に関連して、事業利益の損失、事業の中断、またはデータの損失、システムの停止、または文書の損失に対する損害など、特別損害、派生的損害、付随的損害、または間接的損害について、たとえ当社会社が当該損害または損失の可能性を通知されていたとしても、貴社に対して一切責任を負いません。
お客様は、インターネットのNATURE OF INTERNETが固有のセキュリティ上のリスクを提供するものであり、当社は、CYBER-ATTACK、HACKER TACK、ウイルス検査、その他のインターネット・セキュリティ上のリスクに起因する異常な操作、プライバシー保護またはその他の損害について一切責任を負わないことを確認するものとしますが、当社は、必要に応じて適時に技術サポートを提供します。
お客様は、適用されるすべての法律に準拠して本製品を使用することに同意し、お客様の使用が適用される法律に準拠していることを確認する責任を単独で負うものとします。特に、お客様は、本製品を、第三者の権利(出版権、知的所有権、データ保護権およびその他のプライバシー権を含みますが、これらに限定されません)を侵害しない方法で、マナーで使用する責任を負います。お客様は、本製品を、禁止された最終用途、たとえば、MASS DESTRUCTION の武器の開発または生産、CHEMICAL または生物学の武器の開発または生産、核のEXPLOSIVE または安全でない核フューエルサイクルに関連する内容、または人権の不正使用のサポートなどには使用しないものとします。 .
本書と適用される法律との間に矛盾がある場合は、法律が優先されます。

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、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、顔認識機能を備えたデバイスの場合、バイオメトリクスデータは暗号化方式でデバイスに保存されます。指紋デバイスの場合、指紋テンプレートのみが保存され、指紋画像を再構築することはできません。
データコントローラとして、適切な管理および物理的セキュリティ制御の実装、定期的なレビューの実施、セキュリティ制御の有効性の評価など、個人データを保護するためのセキュリティ制御の実施を含む(ただしこれに限定されない)、該当す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。

記号の表記規則

本書で使用されている記号は、次のように定義されています。

記号	説明
危険	回避しないと、死亡または重傷につながる可能性がある危険な状況を示します。
注意	回避しないと、装置の損傷、データの損失、性能の劣化、または予期しない結果を招く可能性のある危険な状況を示します。
注意	本文の重要な点を強調または補足するための追加情報を提供します。

規制に関する情報

FCC情報

適合規定の当事者が明示的に承認していない変更や改造を行うと、機器を操作するユーザーの権限が無効になる場合がありますのでご注意ください。
FCC 準拠: この装置はテストされ、FCC 規則のパート15 に従ってクラスB デジタル装置の制限に準拠していることが確認されています。これらの限度は、居住地域における設置において、有害な干渉から適度に保護するために設計されています。本製品は無線周波数エネルギーを発生、使用、放出し、指示に従って取り付けられ、使用されなかった場合は、無線通信に有害な干渉を与える可能性があります。しかし、特定の設置条件で障害が発生しないことを保証するものではありません。この機器が無線およびテレビの受信に有害な干渉の原因になったかどうかは、機器をオフにしてオンにすることによって判定できますが、こういったことを引き起こす場合は、以下にある対策のひとつあるいはいくつかを行って干渉を無くすよう試してみることをお勧めします。
受信アンテナの向きを変えるか、場所を変えます。
- 機器と受信機の距離を広げます。
-受信機が接続されている回線とは異なる回線のコンセントに機器を接続します。
-サポートについては、販売店またはラジオ/テレビの専門知識をお持ちの技術者にお問い合わせください。
本装置は、放射体とユーザーの身体の間に最低20cm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
本装置は、FCC規制のパート15に適合しています。運用は、以下の二つの条件に依存します。
1. 本デバイスが有害な干渉を引き起こすことはありません。
2. このデバイスが、望ましくない操作の原因となる妨害を含め、被った妨害を受け入れる必要があること

EU 適合性宣言

この製品および - 該当する場合 - 付属のアクセサリにも ″CE″ の印が付いており、EMC 指令 2014/30/EU、RE 指令 2014/53/EU、RoHS 指令 2011/65/EU に記載されている適用される調和された欧州規格に準拠しています。

2012/19/EU (WEEE指令):この記号が付いている製品は、欧州連合(EU)では未分別の地方自治体廃棄物として処分できません。適切にリサイクルするには、同等の新しい機器を購入したときに、この製品を最寄りの代理店に返品するか、指定の収集場所で廃棄してください。詳細については、www.recyclethis.info を参照してください。

2006/66/EC (バッテリー指令):本製品には、欧州連合で分別されていない一般廃棄物として廃棄できないバッテリーが含まれています。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。電池は、この記号でマークされ、この記号は、カドミウム(Cd)、鉛(Pb)、または水銀(Hg)を示す文字を含むことができる。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収集ポイントに返却してください。詳細については、www.recyclethis.info を参照してください。

安全上の注意

これらの指示は、危険や所有物の損失を防ぐために、ユーザーが製品を正しく使用できることを保証することを目的としています。
予防措置は「危険」と「注意」に分かれています:
危険: 警告を無視すると、重傷または死亡につながる可能性があります。
注意: 注意を省略すると、けがや装置の損傷を招くおそれがあります。

⚠	⚠
危険: 重傷または死亡を防ぐために、以下の安全対策に従ってください。	**注意: ケガや物的損害を防ぐために、次の注意事項に従ってください。**

⚠危険:

- すべての電子操作は、地域の電気安全規則、火災防止規則、およびその他の関連規制に厳密に準拠している必要があります。
- 電源アダプタは、通常の会社が提供しているものを使用してください。本装置は、定格DC 12V、3A のクラス2 サージ保護電源から供給されることを意図しています。
- 1 つの電源アダプタに複数のデバイスを接続しないでください。アダプタが過負荷状態になると、過熱や火災の危険があります。
- デバイスの配線、取り付け、取り外しを行う前に、電源が切断されていることを確認してください。
- 本製品を壁または天壁に設置する場合は、本製品をしっかりと固定する必要があります。
- 本装置から煙、異臭、異音が出たりする場合は、一度電源を切り、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。
- バッテリー、ケミカル・バーン・ハザードを取り込まないでください。
  本機のリモコンにはボタン型電池が使用されています。コイン型電池/ ボタン型電池を入れると、2 時間以内に重大な内部火傷が発生し、死亡する可能性があります。
  新しいバッテリーや使用済みバッテリーは子供の手に近づけないでください。リモコンの電池カバーがしっかり閉まらない場合は、使用を中止し、子どもの手の届かないところに保管してください。電池を飲み込んだり、電池が身体の内部にあると疑われる場合は、ただちに医師の診療を受けてください。
- 製品が正常に動作しない場合は、販売店または最寄りのサービスセンターにお問い合わせください。本装置をご自身で分解しないでください。(不正な修理・メンテナンスによるトラブルについては、一切の責任を負いかねます。

⚠注意:

- デバイスを落としたり衝撃を与えたり、高電磁放射にさらさないでください。振動面や衝撃のある場所への設置は避けてください(無視すると装置破損の原因となります)。
- デバイスを極端に高温の場所(動作温度の詳細については、デバイスの仕様を参照)、低温の

場所、ほこりの多い場所、または湿気の多い場所に置かないでください。また、高電磁放射にさらさないでください。

- 屋内用の機器カバーは、レインと水分から守るものとする。
- 装置を直射日光、低換気、またはヒーターやラジエーターなどの熱源に露出することは禁じられています(無視すると火災の危険があります)。
- デバイスを太陽や明るい場所に向けないでください。それ以外の場合は、ブルーミングやしみが発生し(これは故障ではありません)、同時にセンサーの耐久性に影響を及ぼす可能性があります。
- デバイスカバーを開けるときは、付属のグローブを使用してください。指のアシディックスウィートがデバイスカバーの表面コーティングを侵害する可能性があるため、デバイスカバーに直接触れないようにしてください。
- 装置カバーの内外面を清掃する際は、柔らかく乾燥した布を使用し、アルカリ性の洗剤は使用しないでください。
- 開梱後は、後で使用できるように保管してください。障害が発生した場合は、元のラッパーを使用してデバイスを出荷時の状態に戻す必要があります。元のラッパーを使用しないで輸送すると、デバイスが損傷し、追加料金が発生する場合があります。
- バッテリーの不適切な使用または交換は、爆発の危険があります。同等または同等のタイプにのみ置き換えてください。使用済みのバッテリーは、バッテリーメーカーの指示に従って廃棄してください。
- 生体認証製品は、スプーフィング対策環境には100%適用できません。より高いセキュリティレベルが必要な場合は、複数の認証モードを使用します。
- 使用温度: 0 ° C ～50 ° C
- 屋内使用。デバイスは、少なくともライトから2 メートル離れ、ウィンドウから3 メートル離れている必要があります。

使用可能なモデル

製品名:顔認証端子
ユーザーズガイドに記載されている電源装置のみを使用してください:

型式	メーカー	標準
C2000IC12.0-24P-DE	MOSOパワーサプライテクノロジー(株)	CEE
C2000IC12.0-24P-GB	MOSOパワーサプライテクノロジー(株)	BS
KPL-040F-VI	チャネルウェルテクノロジー(株)	CEE

目次

第1章概要

1.1 概要

顔認識端末は、主に物流センター、空港、大学キャンパス、アラームセンター、住宅などのセキュリティアクセス制御システムに適用される顔認識用のアクセス制御装置の一種である。

1.2 機能

- ターゲットの温度を測定するために酸化バナジウム非冷却センサをサポート
- 温度測定範囲: 30 ° C ～45 ° C (86 ° F ～113 ° F)、精度: ± 0.5 ° C 黒体校正なし
- 認識距離:0.5～1.5m
- Fast temperature measurement mode: 顔を検出し、身元認証なしで表面温度を取得します。
- カードと温度、顔と温度、カードと顔と温度など、複数の認証モードを使用できます。
- 顔マスク着信音
  認識している顔がマスクを装着していない場合、デバイスは音声リマインダーを表示します。同時に、認証または参加が有効になります。
- 強制マスク着信音
  認識している顔がマスクを装着していない場合、デバイスは音声リマインダーを表示します。同時に、認証または参加が失敗します。
- 認証ページに温度測定結果を表示します。
- 異常温度検出時に音声プロンプトをトリガします。
- 異常温度検出時の設定可能なドア状態(開閉)
- TCP/IP通信を介してオンラインおよびオフラインの温度情報をクライアントソフトウェアに送信し、クライアントソフトウェアにデータを保存します。
- 顔認識時間<0.2秒/秒;顔認識精度≧99%
- 50,000 顔容量、50,000カード容量、100,000イベント容量
- 推奨される顔認識の高さ: 1.4m ～1.9 m
- チェックイン、チェックアウト、休憩、休憩、時間外労働、時間外労働など6つの出勤状況をサポート
- ウォッチドッグの設計と改ざん機能
- 認証結果のオーディオプロンプト
- NTP、手動時刻同期、および自動同期
- Wiegand プロトコル経由で外部アクセスコントローラまたはWiegand カードリーダーに接続します。
- RS-485 プロトコルを介してセキュアドアコントロールユニットに接続し、端末が破損したときにドアが開かないようにします。

- クライアントソフトウェアからデバイスへのデータのインポートとエクスポート

第2章外観

顔認識端末の詳しい情報については、次の内容を参照してください:

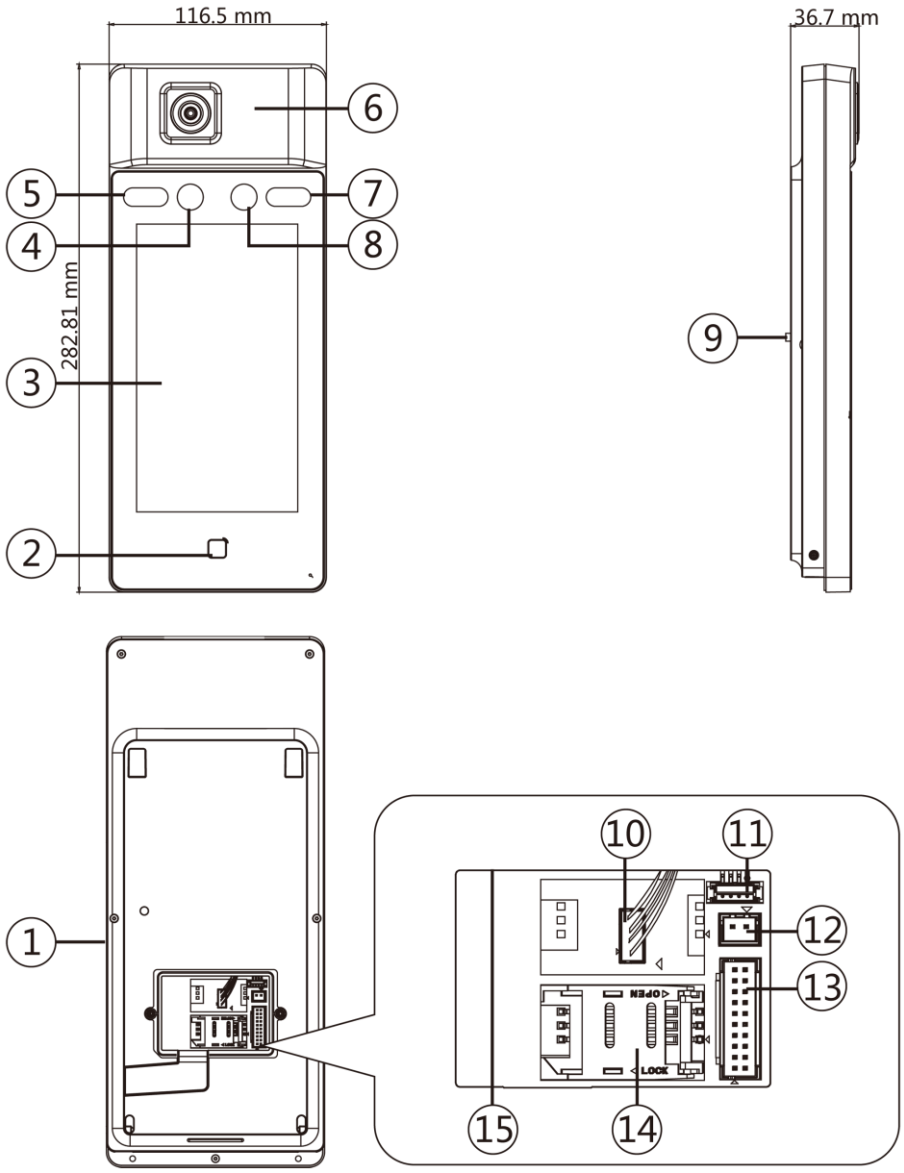


図2-1 顔認識端子図

表2-1 顔認識端子の説明

番号	名前
1	USBインターフェース
2	カードの読み取り範囲

番号	名前
3	タッチスクリーン
4	カメラ
5	IRライト
6	サーモグラフィックモジュール
7	IRライト
8	カメラ
9	タンパー
10	サーモグラフィックモジュールインターフェイス
11	デバッグポート
12	電源インタフェース
13	配線端子
14	PSAM カードスロット(予約済み)
15	ネットワークインタフェース

第3章設置

3.1 設置環境

- バックライト、直射日光、間接日光は避けてください。
- 認識を高めるには、設置環境内またはその近くに光源が必要です。
- 屋内および風のない環境でのみ使用します。

注意

設置環境については、「設置環境のヒント」を参照してください。

3.2 フラッシュマウント

手順

1. ギャングボックスを取り付けます。
2. 付属のねじ(4_KA4 × 22-SUS)2 本を使用して、ギャングボックスの取り付けプレートを固定します。
3. 背面パネルのネジ(2 本)を外し、シートを外すと配線端子が表示されます。
4. 取り付けプレートのケーブル穴にケーブルを通し、対応する外部機器のケーブルに接続します。
5. 2 本のネジでシートをデバイスに背面に取り付けます。
6. 装置を取り付けプレートに合わせ、装置を取り付けプレートに掛けます。

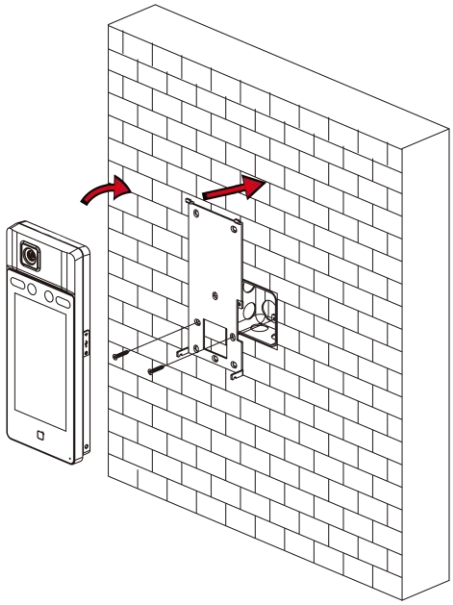


図3-1 デバイスのインストール

7. 付属のねじ(SC-M4×12TP10-SUS)2本で、本体と取付板を固定します。

注意

ネジの頭部がデバイス表面の下にある場合、デバイスは固定されます。

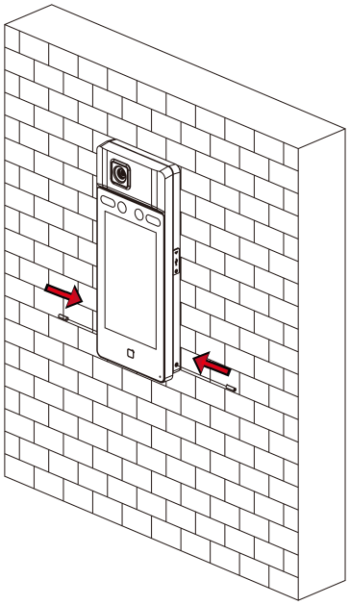


図3-2 セキュアデバイス

3.3 表面実装

手順

1. 取り付けテンプレートの基準線に従って、取り付けテンプレートを壁面または他の面(地面より 1.4 メートル高い場所)に貼り付けます。

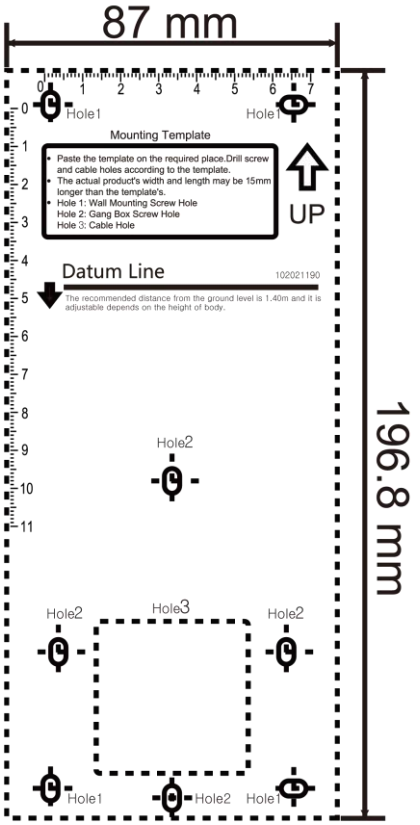


図3-3 取り付けテンプレート

2. 取り付けテンプレートに従って、壁またはその他の表面に4 つの穴を開けます。
3. ドリルで開けた穴に止めねじのねじソケットを挿入します。

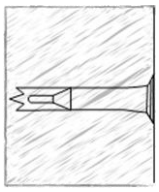


図3-4 挿入ねじソケット

4. 4 つの穴をマウントプレートにドリルで開けた穴に合わせます。
5. フラットトングを使用して、下図に示すシートを取り外します。

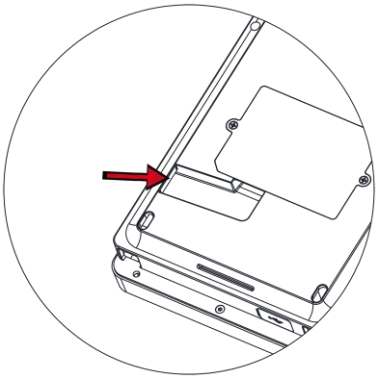


図3-5 シートの削除

6. 背面パネルのネジ(2 本)を外し、シートを外すと配線端子が表示されます。
7. 取り付けプレートのケーブル穴にケーブルを通し、対応する外部機器のケーブルに接続します。
8. 2 本のネジでシートをデバイスに背面に取り付けます。
9. 装置を取り付けプレートに合わせ、装置を取り付けプレートに掛けます。

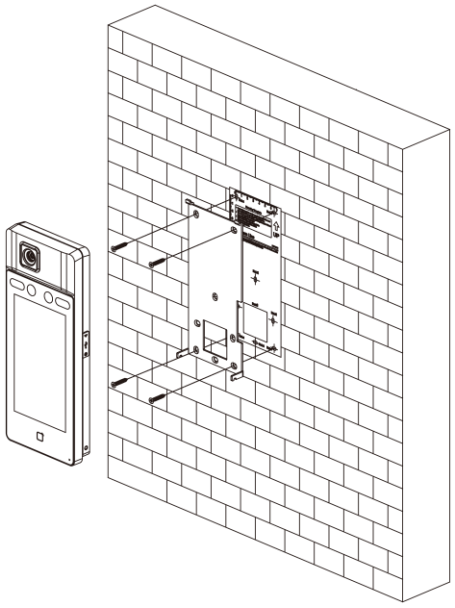


図3-6 デバイスのインストール

10. 付属のねじ(SC-M4×12TP10-SUS)2本で、本体と取付板を固定します。

注意

ネジの頭部がデバイス表面の下にある場合、デバイスは固定されます。

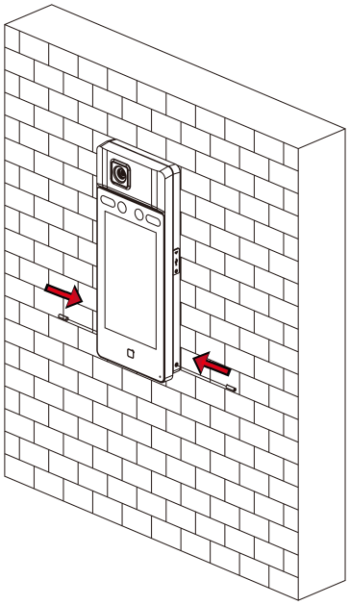


図3-7 セキュアデバイス

注意

- ここでの取り付け高さは推奨される高さです。実際のニーズに合わせて変更できます。
- 取り付けを容易にするために、付属の取り付けテンプレートに従って取り付け面に穴を開けてください。

第4章配線

RS-485ターミナルとRS-485カードリーダーを接続し、NC、COMターミナルとドアロックを接続し、SENSORターミナルとドア接点を接続し、BTN/GNDターミナルとExitボタンを接続し、アラーム出力/アラーム入出力機器を接続し、Wiegandターミナルと Wiegandカードリーダーまたはアクセスコントローラを接続することができます。
WIEGAND端末をアクセスコントローラに接続すると、顔認識端末は認証情報をアクセスコントローラに送信することができ、アクセスコントローラはドアを開けるか否かを判断することができる。

注意

- ケーブルサイズが18 AWG の場合、12 V 電源を使用する必要があります。また、電源装置とデバイスの距離は 20m 以下にしてください。
- ケーブルサイズが15 AWG の場合、12 V 電源を使用する必要があります。また、本機と本機の距離は30m 以内にしてください。
- ケーブルサイズが12 AWG の場合は、12 V 電源を使用する必要があります。また、電源装置とデバイスの距離は40m 以下にしてください。

4.1 ターミナルの説明

端子には、電源入力、アラーム入力、アラーム出力、RS-485、Wiegand出力、ドアロックがあります。
ターミナルの図は次の通りです:

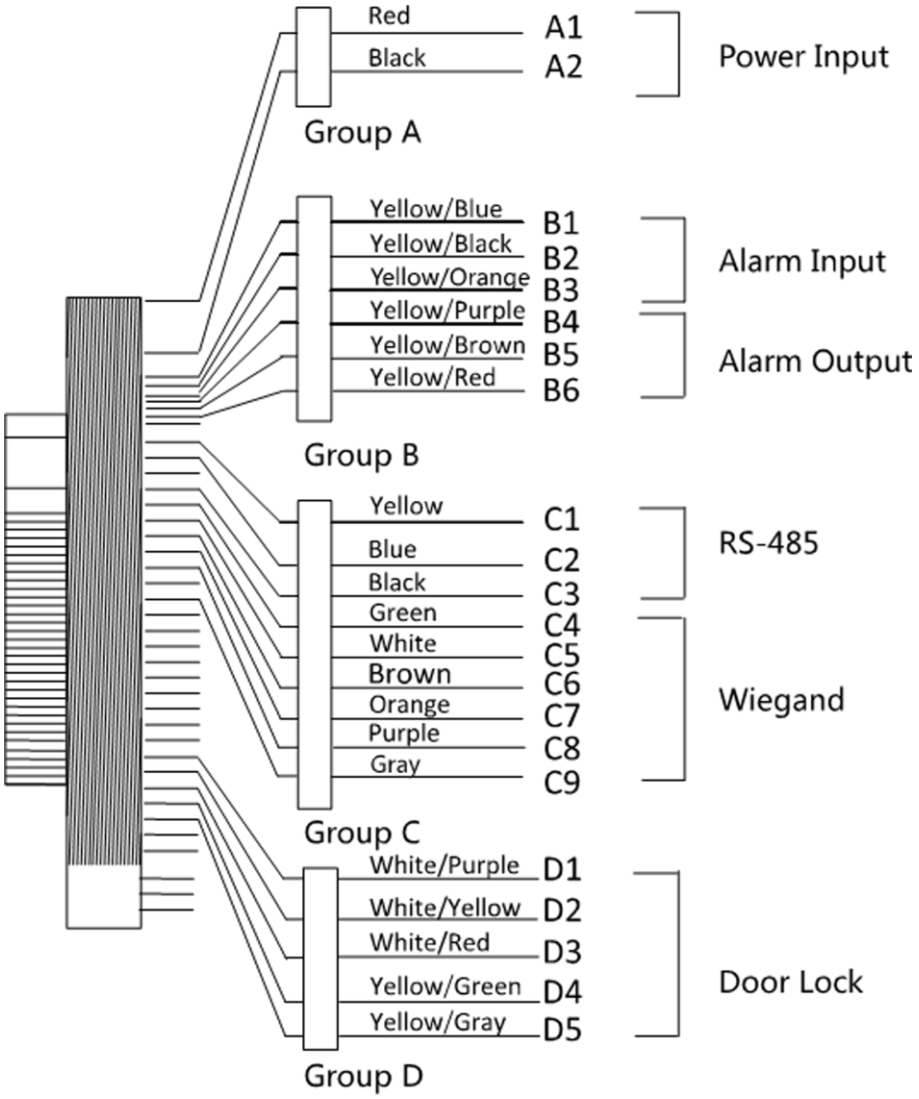


図4-1 端子図

端末の説明は次の通りである:

表4-1 ターミナルの説明

グループ	番号	機能	色	名前	説明
グループA	A1	電源入力	赤	+12 V	12 VDC電源
	A2		黒	GND	グランド
グループB	B1	アラーム入力	黄/青	IN1	アラーム入力1
	B2		黄/黒	GND	グランド
	B3		黄/オレンジ	IN2	アラーム入力2

グループ	番号	機能	色	名前	説明
	B4	アラーム出力	黄/紫	NC	アラーム出力配線
	B5		イエロー/ブラウン	COM	
	B6		黄/赤	NO	
グループC	C1	RS-485	黄色	485+	RS-485配線
	C2		青	485-	
	C3		黒	GND	グランド
	C4	ウィーガンド	緑	W0	Wiegand 配線 0
	C5		白	W1	ワイヤーガンド配線1
	C6		ブラウン	WG_OK	Wiegand 認証済み
	C7		橙	WG_ERR	Wiegand 認証失敗
	C8		紫	バザー	ブザー配線
	C9		グレー	タンパー	改ざん警報配線
グループD	D1	ドアロック	白/紫	NC	ロック配線(NC)
	D2		白/黄	COM	共通
	D3		白/赤	NO	ロック配線(NO)
	D4		黄/緑	センサ	ドア接点
	D5		黄/グレー	BTN	出口ドア配線

4.2 ワイヤノーマルデバイス

通常の周辺機器と接続できます。
安全なドア制御部を持たない場合の配線図は以下のとおりです。

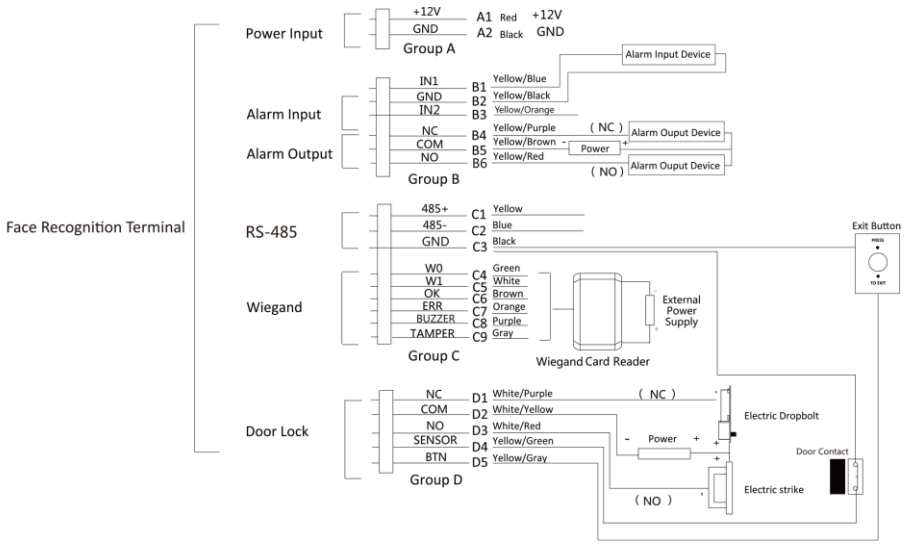


図4-2 デバイスの配線

注意

- Wiegand カードリーダーに接続するには、顔認識端末のWiegand 方向を「Input」に設定し、アクセスコントローラに接続する場合は、Wiegand 方向を「Output」に設定して、認証情報をアクセスコントローラに送信する必要があります。
- Wiegand 方向の設定については、通信設定のWiegand パラメータの設定を参照してください。
- ドアロック用の推奨外部電源は、12 V、1 A です。Wiegand カードリーダーに推奨される外部電源は、12 V、1A です。
- 推奨される電源ケーブルの直径: 22 AWG。他のケーブルの直径は26 AWG と提案されています。
- 本器を直接電源に配線しないでください。

警告

顔認識端子は、サージプロテクト機能付きの外付けクラス2電源を使用してください。

4.3 ワイヤ・セキュア・ドア・コントロール・ユニット

セキュアなドアコントロールユニットと端末を接続することができます。
配線図は以下の通りです。

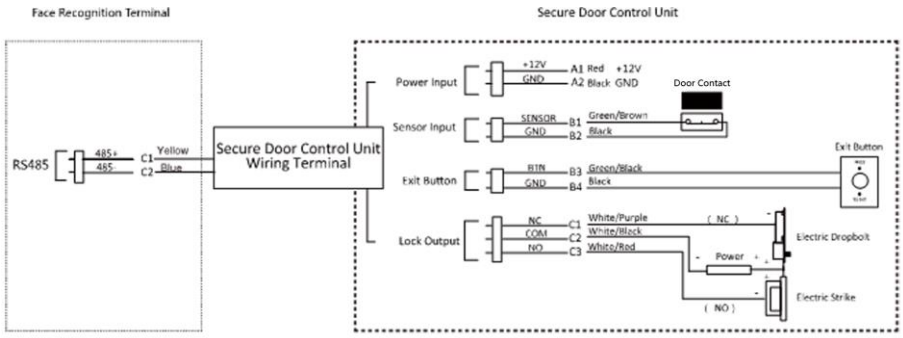


図4-3 安全なドアコントロールユニットの配線

注意

固定ドアコントロールユニットは、別々に外部電源に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 ワイヤファイヤモジュール

4.4.1 電源遮断時のドア開の配線図

ロックタイプ:アノードロック、マグネットロック、電動ボルト(NO)
セキュリティー・タイプ: 電源オフ時のドア・オープン
シナリオ: Fire Engine Access にインストール

タイプ1

注意

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。

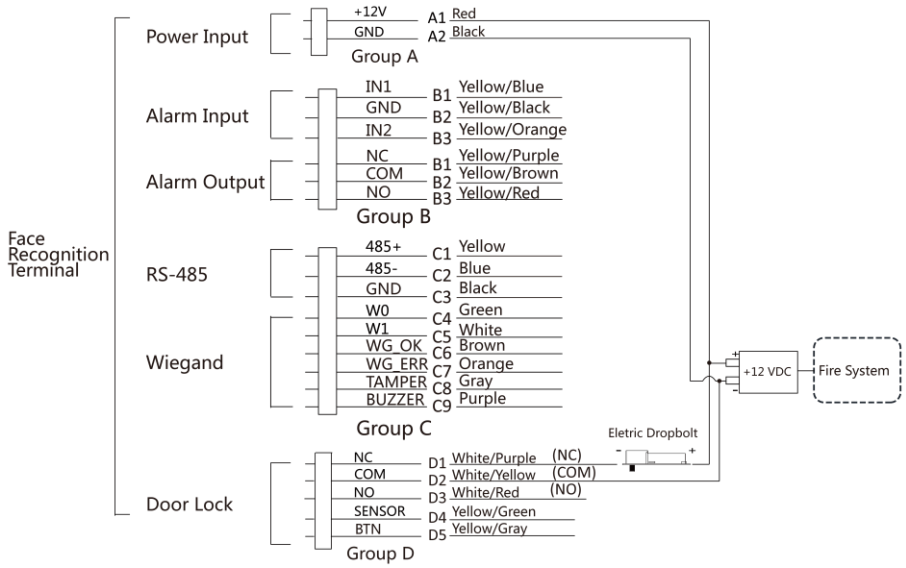


図4-4 ワイヤデバイス

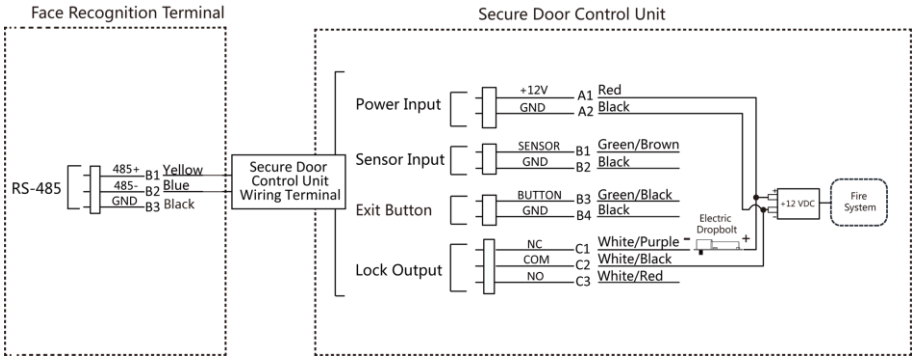


図4-5 ワイヤで固定されたドアコントロールユニット

タイプ2

注意

消防システム(NOとCOM、電源を切るとノーマルオープン)は、ロックと電源装置が直列に接続されています。火災アラームがトリガーされると、ドアは開いたままになります。通常は、NO とCOMはクローズされます。

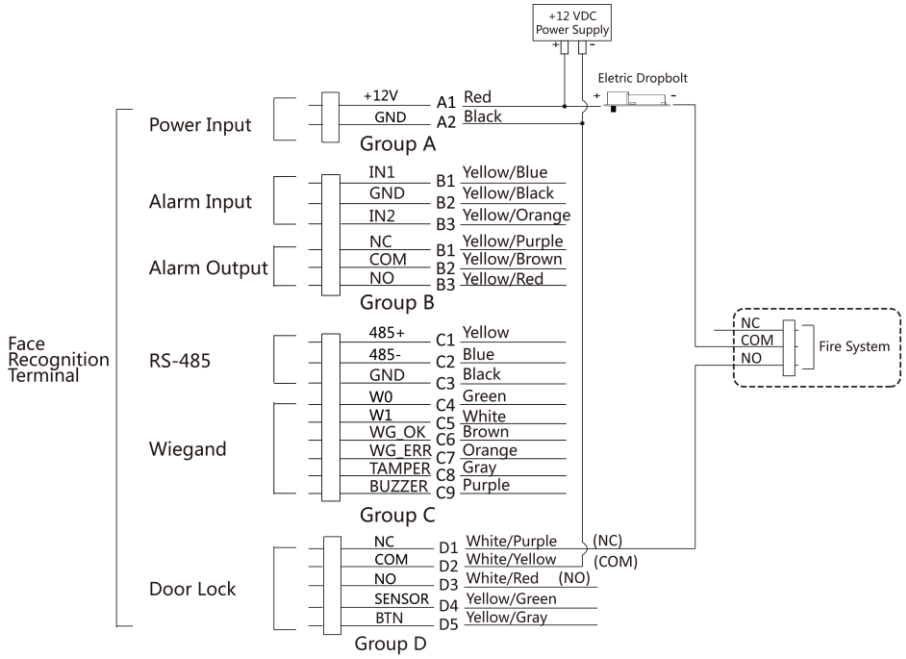


図4-6 配線機器

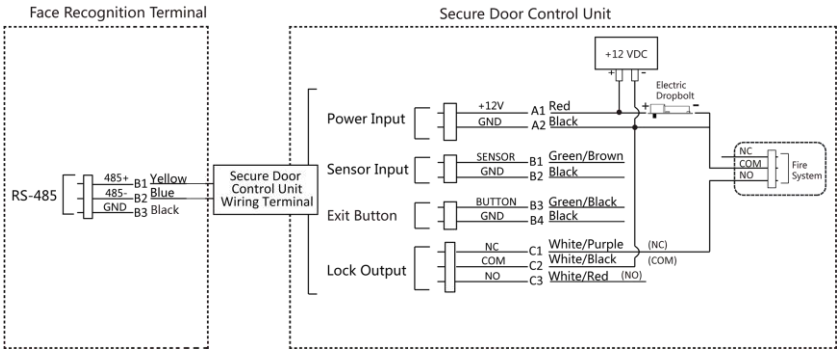


図4-7 安全ドアコントロールユニットの配線

4.4.2 電源遮断時にドアがロックされた場合の配線図

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: 電源を切るとドアがロックされる
シナリオ: Fire Linkage の入口/出口にインストール

注意

- UPS(Uninterpretable Power Supply)が必要です。
- 消防システム(NCとCOM、電源遮断時ノーマルクローズ)は、ロックと電源が直列に接続されています。火災アラームがトリガーされると、ドアは開いたままになります。通常は、NC とCOM が開いています。

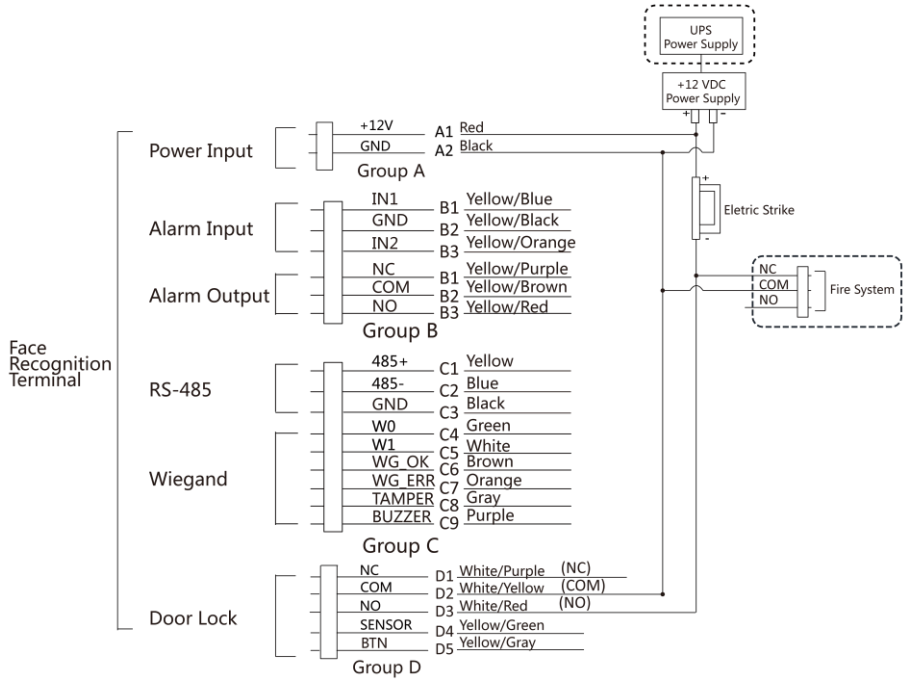


図4-8 デバイスの配線

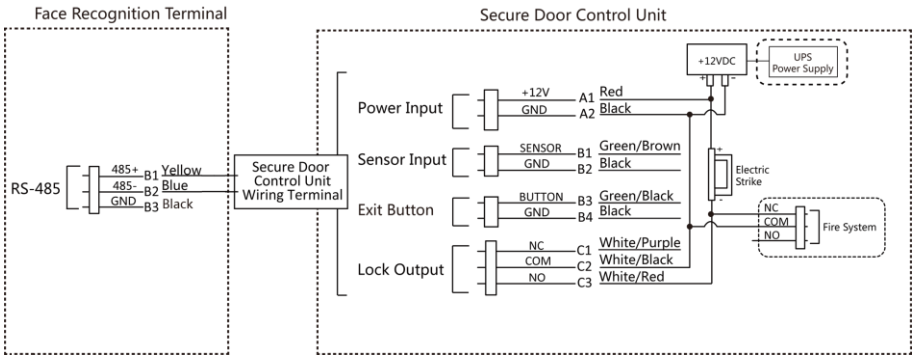


図4-9 配線図

第5章起動

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アクティブ化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によるアクティブ化がサポートされています。
デバイスの初期値は次のとおりです:

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

5.1 デバイス経由でアクティブ化

デバイスがアクティベートされていない場合は、電源を入れた後でデバイスをアクティベートできます。
Activate Device(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。
「アクティブ化」をタップすると、デバイスがアクティブ化されます。

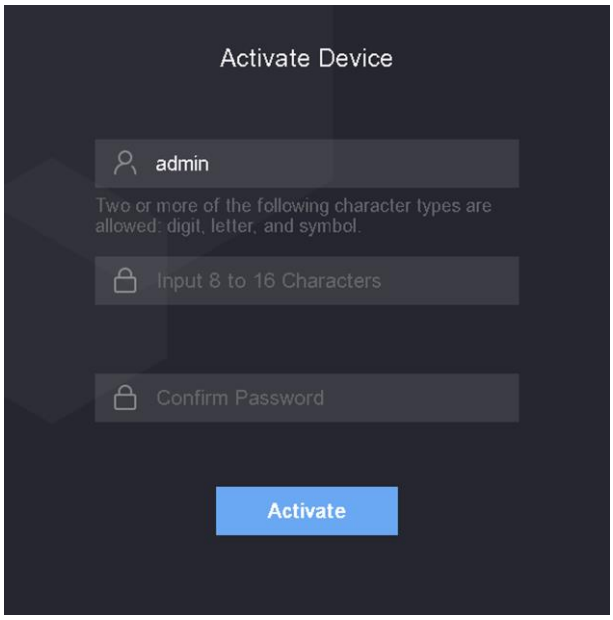


図5-1 「Activation」ページ

⚠注意

デバイスのパスワード強度を自動的に確認できます。製品のセキュリティを強化するために、独自のパスワードを変更することを強くお勧めします(大文字、小文字、数字、特殊文字の3 種類以上を含む8 文字以上を使用)。また、パスワードを定期的に変更することをお勧めします。特に高セキュリティシステムでは、パスワードを月単位または週単位で変更することで製品を保護できます。
すべてのパスワードおよびその他のセキュリティ設定を適切に構成するのは、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。

- 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、デバイスをクライアントソフトウェアまたはその他のプラットフォームに追加する必要がある場合は、デバイスのIP アドレスを編集する必要があります。詳細については、通信設定を参照してください。

5.2 SADP 経由でアクティブ化

SADP は、LAN を介してデバイスの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。

はじめる前に

- 付属のディスクまたは公式ウェブサイトからSADP ソフトウェアを入手し、プロンプトに従ってSADP をインストールします。
- SADP ツールを実行するデバイスとPC は、同じサブネット内にある必要があります。

次の手順では、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ます。一括有効化とIP アドレスの変更については、SADP のユーザーマニュアルを参照してください。

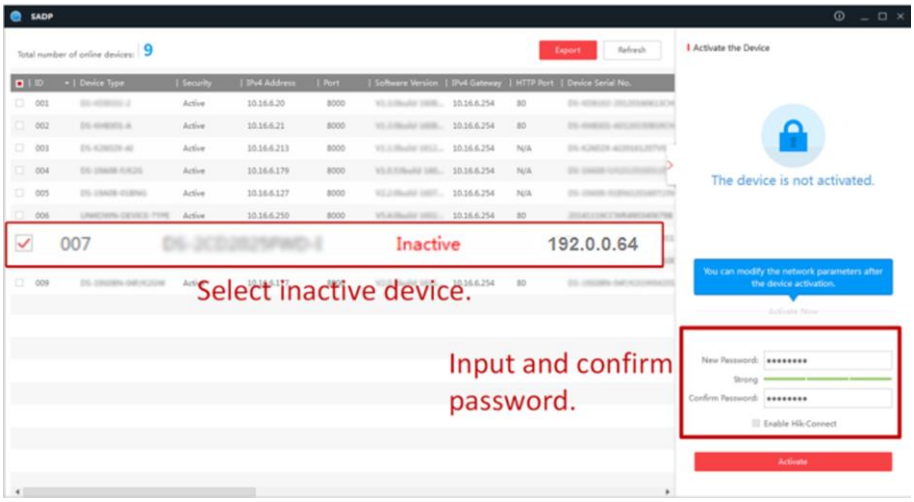
手順

1. SADP ソフトウェアを実行し、オンラインデバイスを検索します。
2. オンラインデバイスリストでデバイスを検索して選択します。
3. 新しいパスワード(admin password)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、(大文字、小文字、数字、特殊文字を含む8 文字以上を使用して) 独自の強力なパスワードを作成することを強くお勧めします。また、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。特に高セキュリティシステムでは、パスワードを月単位または週単位でリセットすると製品の保護が向上します。

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。



アクティブ化が成功すると、デバイスのステータスがアクティブになります。

5. デバイスのIP アドレスを変更します。
   1) デバイスを選択します。
   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と同じサブネットに変更します。
   3) admin パスワードを入力し、Modify をクリックしてIP アドレスの変更を有効にします。

5.3 クライアントソフトウェアによるデバイスのアクティブ化

一部のデバイスでは、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

注意

この機能はデバイスでサポートされている必要があります。

1. デバイス管理ページに入ります。
2. Device Management の右側のをクリックし、Device 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エリアを表示します。
   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(「Security Level」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. 「Activate」をクリックして「Activation」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強度を自動的に確認できます。製品のセキュリティを強化するために、独自のパスワードを変更することを強くお勧めします(大文字、小文字、数字、特殊文字の3 種類以上を含む8 文字以上を使用)。また、パスワードを定期的に変更することをお勧めします。特に高セキュリティシステムでは、パスワードを月単位または週単位で変更することで製品を保護できます。
すべてのパスワードおよびその他のセキュリティ設定を適切に構成するのは、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。

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章基本操作

6.1 アプリケーションモードの設定

デバイスをアクティブ化したら、デバイスアプリケーションを改善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。

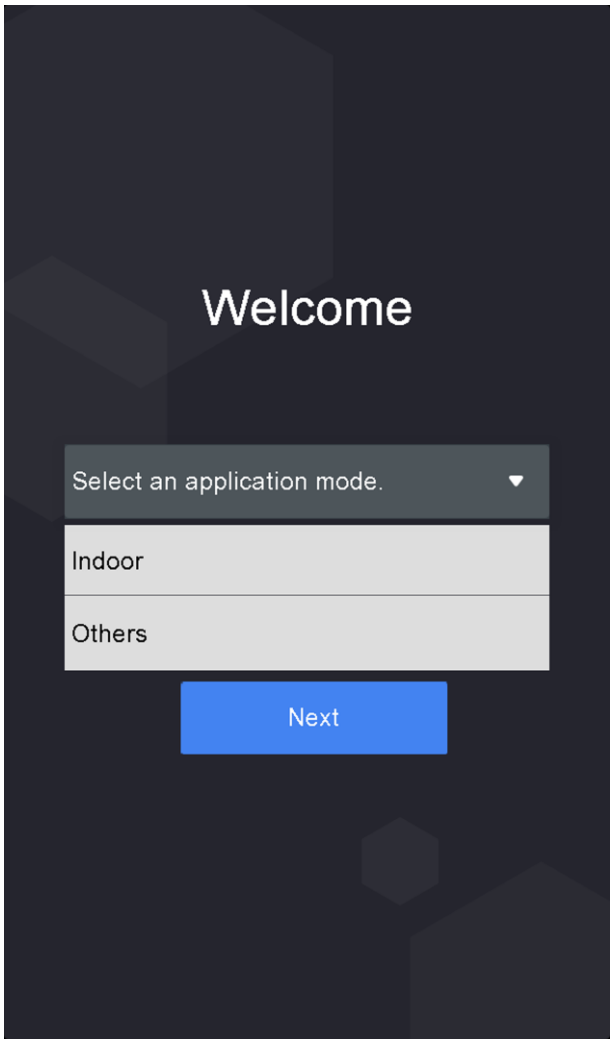


図6-1 ようこそページ

2. OK をタップして保存します。

注意

- システム設定で設定を変更することもできます。
- 装置を窓の近くに置いたり、顔認識機能がうまく作動しない場合は、「その他」を選択します。
- アプリケーションモードを設定せずに「次へ」をタップすると、システムはデフォルトで「屋内」を選択します。
- 他のツールを使用してリモートでデバイスをアクティブ化する場合、システムはデフォルトでアプリケーションモードとしてIndoor を選択します。

6.2 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。最初のログインには、デバイスアクティベーションパスワードを入力する必要があります。または、管理者の認証情報を追加している場合は、設定した認証情報を使用してログインできます。

6.2.1 初回ログイン

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。

手順

1. 最初のページで3秒間ロングタップすると、パスワード入力画面が表示されます。
2. パスワードフィールドをタップして、デバイスアクティベーション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を開きます。

注意

- パスワードの入力に5回失敗すると、デバイスは30分間ロックされます。
- 管理者認証モードの設定については、「ユーザーの追加」を参照してください。

図6-2 ホームページ

6.2.2 管理者によるログイン

デバイスの管理者を追加すると、管理者のみがデバイス操作のためにデバイスにログインできます。

手順

1. 最初のページを3秒間長押しして、管理者ログインページを開きます。

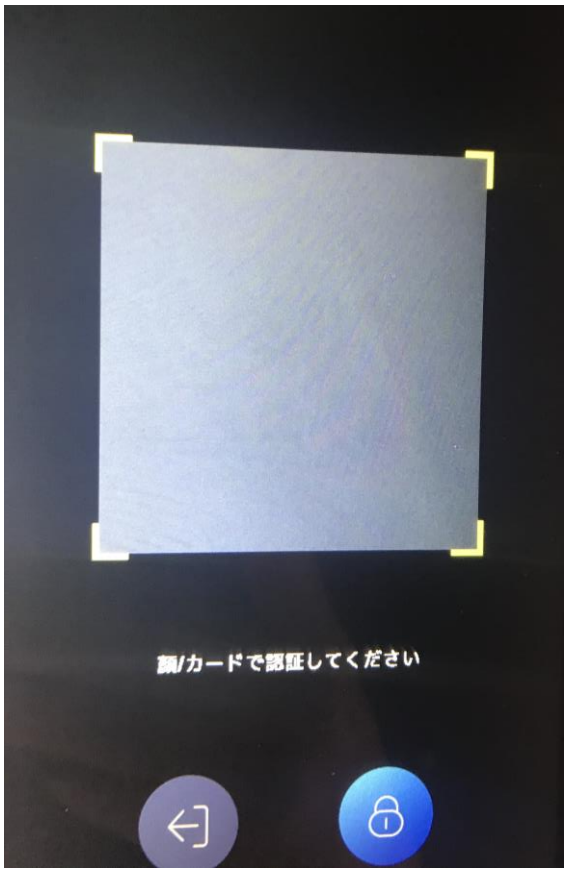


図6-3 管理者ログイン

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6-4 ホームページ

注意

顔またはカードの試行に5回失敗すると、デバイスは30分間ロックされます。

3. (オプション) をタップすると、ログインするためのデバイスアクティベーションパスワードを入力できます。
4. (オプション) をタップすると、admin ログインページを終了できます。

6.3 通信設定

通信設定ページで、ネットワークパラメータ、RS-485パラメータ、Wiegandパラメータを設定できます。

6.3.1 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、ゲートウェイなどのデバイスネットワークパラメータを設定できま

す。

手順

1. 「通信」をタップします。ホームページの(通信設定)で、通信設定ページに入ります。
2. 「通信設定」ページで、「ネットワーク」をタップして「ネットワーク」タブに入ります。

図6-5 ネットワーク設定

3. 「IP アドレス」、「サブネットマスク」、または「ゲートウェイ」をタップして、パラメータを入力します。
4. 「OK」をタップして設定を保存します。

注意

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

5. タップしてネットワークパラメータを保存します。

6.3.3 RS-485 パラメータの設定

顔認識端子は、RS-485端子を介して、外部アクセスコントローラ、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することができます。

手順

1. 「通信」をタップします。ホームページの(通信設定)で、通信設定ページに入ります。
2. 通信設定ページで、RS-485 をタップしてRS-485 タブに入ります。

図6-7 RS-485 パラメータの設定

3. 実際のニーズに合わせてペリフェラルタイプを選択します。

注意

- Controller はアクセスコントローラを表し、Unit はセキュアドア制御ユニットを表し、Reader はカードリーダーを表します。
- 「コントローラ」を選択した場合: RS-485 インターフェイスを介してデバイスをターミナルに接続する場合は、RS-485 アドレスを2 に設定します。コントローラに接続する場合は、ドアNo. に応じてRS-485のアドレスを設定してください。

4. タップしてネットワークパラメータを保存します。

注意

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

6.3.4 Wiegand パラメータの設定

Wiegandの送信方向を設定します。

手順

1. 「通信」をタップします。ホームページの(通信設定)で、通信設定ページに入ります。
2. 通信設定ページで、Wiegand をタップして、Wiegand タブに入ります。

図6-8 Wiegand の設定

3. Wiegand 機能を有効にします。
4. 送信方向を選択します。
   - 出力:顔認識端子に外部アクセスコントローラを接続できます。また、2つのデバイスは、Wiegand 26またはWiegand 34を介してカード番号を送信します。
   - 入力: 顔認識ターミナルは、Wiegand カードリーダーを接続できます。
5. タップしてネットワークパラメータを保存します。

注意

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

6.4 ユーザー管理

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

6.4.1 管理者の追加

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

手順

1. 最初のページをロングタップして、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」ページを開きます。
3. 従業員ID を編集します。

注意

- 従業員ID は32 文字未満にする必要があります。また、小文字、大文字、数字を組み合わせることもできます。
- 従業員ID は重複しないでください。

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

注意

- ユーザー名には、数字、大文字、小文字、特殊文字を使用できます。
- ユーザー名は32 文字まで入力できます。

5. (オプション) 管理者の顔写真、指紋、カード、またはパスワードを追加します。

注意

- 顔画像の追加について詳しくは、「顔画像の追加」を参照してください。
- カードの追加について詳しくは、「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、「パスワードの追加」を参照してください。

6. オプション: 管理者の認証タイプを設定します。

注意

認証タイプの設定については、「認証モードの設定」を参照してください。

7. Administrator Permission 機能を有効にします。

管理者権限の有効化

ユーザーは管理者です。通常の出席機能を除いて、ユーザは、許可を認証した後に操作するためにホームページを入力することもできます。

8. タップして設定を保存します。

6.4.2 フェイスピクチャー登録

ユーザーの顔画像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

1. 最初のページをロングタップして、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」ページを開きます。
3. 従業員ID を編集します。

注意

- 従業員ID は32 文字未満にする必要があります。また、小文字、大文字、数字を組み合わせることもできます。
- 従業員ID は重複しないでください。

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

注意

- ユーザー名には、数字、大文字、小文字、特殊文字を使用できます。
- ユーザー名は32 文字まで入力できます。

5. フェイスピクチャー欄をタップすると、フェイスピクチャー追加画面が表示されます。

図6-9 顔写真の追加

6. カメラを見ながら顔を配置します。

注意

- フェイスピクチャを追加するときは、フェイスピクチャがフェイスピクチャアウトラインにあることを確認してください。
- 取り込んだ顔画像の品質が良好で、正確であることを確認します。
- 顔写真を追加する方法については、顔写真を収集/比較するときのヒントを参照してください。

フェイスピクチャを完全に追加すると、撮影したフェイスピクチャ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)「もう一度試す」をタップして顔の位置を調整し、顔画像を再度追加します。

注意

顔画像の追加にかかる時間は最大15秒です。顔画像を追加するまでの残り時間をページの左側で確認できます。

9. Administrator Permission 機能を有効または無効にします。

管理者権限の有効化

ユーザーは管理者です。通常の出席機能を除いて、ユーザは、許可を認証した後に操作するためにホームページを入力することもできます。

管理者権限の無効化

User は通常のユーザーです。ユーザーは、最初のページでのみ認証または参加を行うことができます。

10. タップして設定を保存します。

6.4.3 カードの追加

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

手順

1. 最初のページをロングタップして、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」ページを開きます。
3. Employee ID. フィールドをタップし、従業員ID を編集します。

注意

- 従業員ID は32 文字未満にする必要があります。また、小文字、大文字、数字を組み合わせることもできます。
- 従業員ID は重複しないでください。

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

注意

- ユーザー名には、数字、大文字、小文字、特殊文字を使用できます。
- ユーザー名は32 文字まで入力できます。

5. Card欄をタップし、カード番号を入力します。
6. 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。カードをカードのスワイプエリアにスワイプすると、カード番号が表示されます。

注意

- カードNo.を空にすることはできません。

- カード番号は最大20文字まで入力できます。
- カード番号は重複できません。

7. オプション: Duress Card 機能を有効にします。追加したカード

この耐久性カードをスワイプしてユーザーを認証すると、デバイスは耐久性カードイベントをクライアントソフトウェアにアップロードします。

8. Administrator Permission 機能を有効または無効にします。

管理者権限の有効化

ユーザーは管理者です。通常の出席機能を除いて、ユーザは、許可を認証した後に操作するためにホームページを入力することもできます。

管理者権限の無効化

User は通常のユーザーです。ユーザーは、最初のページでのみ認証または参加を行うことができます。

9. タップして設定を保存します。

6.4.4 パスワードの追加

ユーザーのパスワードを追加します。ユーザーはパスワードを使用して認証できます。

手順

1. 最初のページをロングタップして、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」ページを開きます。
3. Employee ID. フィールドをタップし、従業員ID を編集します。

注意

- 従業員ID は32 文字未満にする必要があります。また、小文字、大文字、数字を組み合わせることもできます。
- 従業員ID は重複しないでください。

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

注意

- ユーザー名には、数字、大文字、小文字、特殊文字を使用できます。
- ユーザー名は32 文字まで入力できます。

5. パスワードフィールドをタップしてパスワードを作成し、パスワードを確認します。

注意

- パスワードには数字のみが許可されます。
- パスワードは8 文字まで入力できます。

6. Administrator Permission 機能を有効または無効にします。

管理者権限の有効化

ユーザーは管理者です。通常の出席機能を除いて、ユーザは、許可を認証した後に操作するためにホームページを入力することもできます。

管理者権限の無効化

User は通常のユーザーです。ユーザーは、最初のページでのみ認証または参加を行うことができます。

7. タップして設定を保存します。

6.4.5 認証モードの設定

ユーザーの顔写真、パスワード、またはその他の資格情報を追加したら、認証モードを設定する必要があります。ユーザーは、設定された認証モードを使用して自分のアイデンティティを認証できます。

手順

1. 最初のページをロングタップして、バックエンドにログインします。
2. 「ユーザー→追加」-「ユーザー→認証方式の編集」を選択します。
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。

装置

デバイスモードを選択する場合は、最初にAccess Control Settings ページでターミナル認証モードを設定する必要があります。詳細については、アクセス制御パラメータの設定を参照してください。

ユーザー設定

実際のニーズに応じて、さまざまな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。

6.4.6 ユーザーの検索と編集

ユーザーを追加したら、ユーザーを検索して編集できます。

ユーザーの検索

「ユーザ管理」ページで、検索領域をタップして「ユーザの検索」ページを開きます。ページの左側にある「カード」をタップし、ドロップダウンリストから検索タイプを選択します。検索する従業員ID、カード番号、ユーザ名を入力します。タップして検索します。

ユーザーの編集

User Management(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、Edit User(ユーザーの編集)ページに入ります。「ユーザ管理」の手順に従って、ユーザパラメータを編集します。

タップして設定を保存します。

注意

従業員ID は編集できません。

6.5 温度測定設定

温度検出、温度超過アラームしきい値、温度異常時にドアが開かない、温度測定モード、測定領域キャリブレーション、測定領域、黒体などの温度測定パラメータを設定できます。
ホームページで、Temp (Temperature) をタップしてTemperature Settings ページに入ります。このページで温度測定パラメータを編集し、をタップして設定を保存します。

図6-10 温度測定パラメータ

使用可能なパラメータの説明は次のとおりです:

表6-1 温度測定パラメータの説明

パラメータ	説明
温度検出の有効化	機能を有効にすると、デバイスは許可を認証すると同時に温度を取得します。デバイスを無効にすると、デバイスは権限のみを認証します。
Over-Temperature Alarm Threshold(最大/最小)	実際の状況に応じてしきい値を編集します。検出された温度が設定されたパラメータより高いまたは低い場合、アラームがトリガーされます。デフォルト値は37.3° です。
温度異常時ドアが開かない	この機能を有効にすると、検出された温度が設定されたしきい値を上回ったり下回ったりすると、ドアが開かなくなります。デ

パラメータ	説明
	フォルトでは、温度は有効になっています。
温度測定のみ	この機能を有効にすると、デバイスは権限を認証せず、温度のみを取得します。機能を無効にすると、デバイスは権限を認証すると同時に温度を取得します。
測定エリアの校正/測定エリアの設定	温度測定エリアと補正パラメータを設定します。
Black Body 設定	この機能を有効にすると、距離、温度、放射率など、黒体のパラメータを設定できます。

6.6 データのインポートとエクスポート

Transferページでは、イベント、ユーザデータ、ユーザピクチャ、および取り込んだピクチャをUSBフラッシュドライブにエクスポートできます。また、USBメモリーに保存されているユーザーデータやユーザー写真を取り込むこともできます。

6.6.1 データのエクスポート

手順

1. ホームページの転送をタップして転送ページに入ります。
2. 転送ページで、イベントのエクスポート、ユーザーデータのエクスポート、プロファイルフォトのエクスポート、およびキャプチャ画像のエクスポートをタップします。
3. ポップアップページで「はい」をタップすると、データがデバイスからUSBフラッシュドライブにエクスポートされます。

注意

- サポートされるUSB フラッシュドライブのフォーマットはDB です。
- システムは、1G～32Gのストレージを持つUSBフラッシュドライブをサポートしています。USBメモリーの空き容量が512M以上になっ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、編集できません。

6.6.2 データのインポート

手順

1. デバイスにUSBフラッシュドライブを差し込みます。

2. 「転送」ページで、「ユーザデータを読み込む」と「プロファイル写真を読み込む」をタップします。
3. ポップアップウィンドウで「はい」をタップすると、USBフラッシュドライブからデバイスにデータがインポートされます。

注意

- デバイスA から別のデバイスB にすべてのユーザー情報を転送する場合は、デバイスAからUSB フラッシュドライブに情報をエクスポートし、USB フラッシュドライブからデバイスBにインポートする必要があります。この場合、プロファイル写真をインポートする前にユーザーデータをインポートする必要があります。
- 対応しているOS 型フラッシュドライブのフォーマットは、FAT32 です。
- 取り込んだ画像はルートディレクトリ(enroll_pic)に保存され、画像ファイルの名前は以下の規則に従う必要があります:
  カードNo._Name_Department_Employee ID_Gender.jpg
- 従業員ID は32 文字未満にする必要があります。小文字、大文字、数字を組み合わせることができます。重複してはならず、0 で始めるべきではありません。
- 顔写真の要件は次の規則に従う必要があります:カメラに直接向いて、全面ビューで撮影してください。顔写真撮影時に、ハットやヘッドカバーを着用しないでください。フォーマットはJPEG またはJPG にする必要があります。解像度は640×480ピクセル以上、640×480ピクセル以上にしてください。画像サイズは 60KB～200KB にする必要があります。

6.7 アイデンティティ認証

ネットワーク設定、システムパラメータ設定、およびユーザ設定の後、アイデンティティ認証の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。1:1 一致または1:N 一致を使用してID を認証できます。

1: N 一致

キャプチャした顔画像をデバイスに保存されているすべての顔画像と比較します。

1: 1 一致

キャプチャした顔画像をデバイスに保存されているすべての顔画像と比較します。

6.7.1 複数の認証情報による認証

はじめる前に

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

手順

1. 認証モードがCard and Face、Password and Face、Card and Passwordの場合は、ライブビューページの指示に従って認証します。

注意

- カードは、通常のICカードでも、暗号化されたカードでもかまいません。
- QRコード読み取り機能が有効になっている場合は、QRコードをデバイスカメラの前に置いて、QRコードで認証できます。

2. 前の資格情報が認証された後、他の資格情報の認証を続行します。

注意

顔認証の詳細については、「顔画像を取得/比較するときのヒント」を参照してください。

認証に成功すると、プロンプト"Authenticated"がポップアップ表示されます。

6.7.2 単一の認証情報による認証

認証前のユーザー認証の種類を設定します。詳細については、「認証モードの設定」を参照してください。
顔、カード、QRコードを認証します。

フェイス

カメラで前を向き、顔による認証を開始します。

カード

カード提示エリアにカードを提示し、カードによる認証を開始する。

注意

カードは、通常のICカードでも、暗号化されたカードでもかまいません。

QRコード

QRコードで認証するには、QRコードをデバイスカメラの前に置きます。

注意

QR コードによる認証は、デバイスでサポートされている必要があります。

認証が完了すると、プロンプト「Authenticated」がポップアップ表示されます。

6.8 System Settings

System Settings(システム設定)ページでは、システム基本パラメータ、顔パラメータの設定、およ

びファームウェアのアップグレードを行うことができます。

6.8.1 動作パラメータの設定

コミュニティ番号、建物番号、ユニット番号、音声プロンプト、音声ボリューム、アプリケーションモード、白色の明るさを設定できます。
ホームページで、システム(システム設定)をタップしてシステム設定ページを開きます。

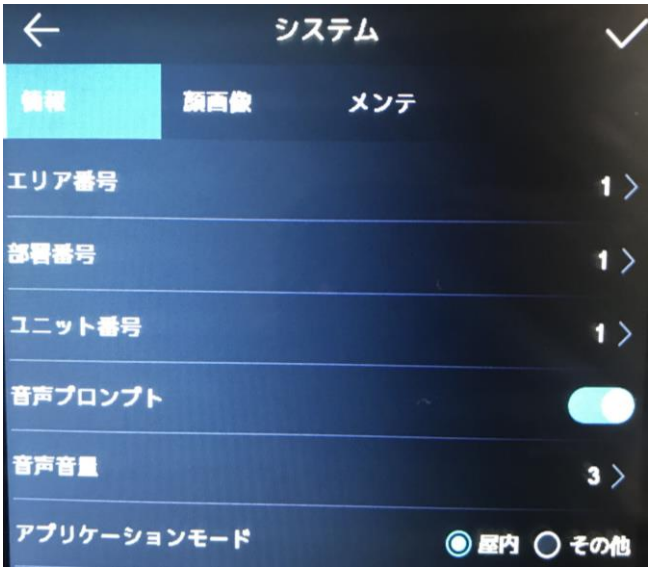


図6-11 基本パラメータ

表6-2 基本パラメータ

パラメータ	説明
コミュニティ番号	デバイス搭載コミュニティNo.を設定します。
ビル番号	機器設置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番号を設定します。
音声プロンプト	またはをタップして、音声プロンプトを無効または有効にします。
ボイスボリューム	音声の音量を調整します。値が大きいほど、音量は大きくなります。
アプリケーションモード	実際の環境に応じて、他と屋内のどちらかを選択できます。
白色ライトの明るさ	補助白色光の明るさを設定します。明るさの範囲は0 ～100 です。 0 はライトをオフにすることを表し、1 は最も暗いことを表し、100 は最も明るいことを表します。

6.8.2 顔画像のパラメータを設定する

顔1:N (セキュリティ)レベル、1:1(セキュリティ)レベル、認識間隔、ライブネスセキュリティレベル、WDRレベル、生徒距離、マスク付き顔検出、ECOモードを設定できます。
ホームページで、システム(システム設定)をタップしてシステム設定ページを開きます。

図6-12 顔画像のパラメータ

表6-3 顔写真のパラメータ

パラメータ	説明
1: N(セキュリティ)レベル	1:N 一致モードで認証する場合、一致しきい値を設定します。値が大きいほど、誤許可率は小さくなり、誤拒否率は大きくなります。デフォルト値は84 です。
1:1 (セキュリティ)レベル	1:1 一致モードで認証する場合、一致しきい値を設定します。値が大きいほど、誤許可率は小さくなり、誤拒否率は大きくなります。デフォルト値は75 です。
認識間隔	1人の許可を認証するときに、2つの連続した顔を認識する時間間隔を設定します。 **注意** 1 ～10 の数字を入力できます。

パラメータ	説明
ライブネスレベル (Liveness Security Level)	顔検出機能を有効にしたあと、顔認証を行うときに、一致するセキュリティレベルを設定できます。
WDRレベル	デバイスは、WDR 機能を自動的に有効にできます。レベルが高いほど、デバイスは簡単にWDR モードに入ることができます。0 は、WDRが無効であることを示します。
瞳孔距離	顔認識を開始するときの、2 人の生徒の間の最小解像度。実際の解像度は、設定値よりも大きくする必要があります。 デフォルトの解像度は40 です。
マスク検出付き顔	この機能を有効にすると、認証ページの権限を認証する際に、マスクの装着の有無を装置が認識し、構成に応じてマスクの装着を促します。
マスク付きフェースおよびマスク付きフェース(1:N)	マスク1 の顔の一致しきい値: N. 値が大きいほど、誤許可率は低くなり、誤拒否率は高くなります。最大値は100 です。
フェイスマスクを装着する必要があります	この機能を有効にした後、認証された人物は顔マスクを着用する必要があります。そうしないと、認証に失敗します。
フェイスマスク着用の注意事項	この機能を有効にした後、認証された人物が顔マスクを装着していない場合は、顔マスクを装着するように促すプロンプトがポップアップ表示されます。
エコモード	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:N)、ECO モード(1:1)を設定できます。
エコモードしきい値	ECO モードを有効にすると、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。指定可能な範囲:0 ～8。
エコモード(1:N)	ECO モード1:N 一致モードで認証する場合、一致しきい値を設定します。値が大きいほど、誤許可率は小さくなり、誤拒否率は大きくなります。デフォルト値は84 です。
エコモード(1:1)	ECO モード1:1 一致モードで認証する場合、一致しきい値を設定します。値が大きいほど、誤許可率は小さくなり、誤拒否率は大きくなります。デフォルト値は75 です。
フェースとマスク&フェース(1:N) (ECO)	ECO モードでマスク1: N を持つ顔の一致しきい値。値が大きいほど、誤許可率は小さくなり、誤拒否率は大きくなります。最大値は100 で

パラメータ	説明
	す。

6.8.3 時刻設定

このセクションでは、デバイスの時間とDST を設定できます。
ホームページの「時間(時間設定)」をタップして、「時間設定」ページに入ります。時間パラメータを編集し、をタップして設定を保存します。

図6-13 時間パラメータ

6.9 アクセス制御パラメータの設定

端末認証の機能など、アクセス制御の権限を設定できます。mode, reader auth.モード、QRコード、リモート認証、ドア接点、ドアロック時間など
ホームページでACS (アクセスコントロール設定)をタップして、アクセスコントロール設定ページに入ります。このページでアクセスコントロールパラメータを編集し、をタップして設定を保存します。

図6-14 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6-4 アクセス制御パラメータの説明

パラメータ	説明
ターミナル認証。モード	顔認識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。 **注意** ● フィンガープリントモジュールを持つデバイスのみがフィンガープリント関連機能をサポートします。 ● 生体認証製品は、スプーフィング対策環境には100%適用できません。より高いセキュリティレベルが必要な場合は、複数の認証モードを使用します。 ● 複数の認証モードを採用する場合は、顔を認証する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	カードリーダーの認証モードを選択します。
QRコード	QRコードの読み取り機能は、認証インターフェイスで使用できます。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。
リモート認証	権限を認証すると、プラットフォームによってアクセスをリモートで許可するかどうかが制御されます。
ドア接点	実際のニーズに応じて、「開く」または「閉じる」を選択できます。デフォルトでは、閉じています。
ドアロック時間	ドアのロック解除時間を設定します。設定した時間ドアを開けないと、ドアがロックされます。利用可能なドアロック時間の範

パラメータ	説明
	囲:1 ～255 秒。

6.10 メンテナンス

6.10.1 ファームウェアのアップグレード

USBメモリーを差し込みます。「維持」をタップします。「システム設定」ページの(メンテナンス)をタップして、「アップグレード」をタップします。デバイスはUSBフラッシュドライブ内のアップグレードファイルを自動的に読み取り、ファームウェアをアップグレードします。

注意

- デバイスのアップグレード中は電源を切らないでください。
- アップグレードするファイルはルートディレクトリにある必要があります。
- アップグレードするファイル名はdigicap.dav である必要があります。

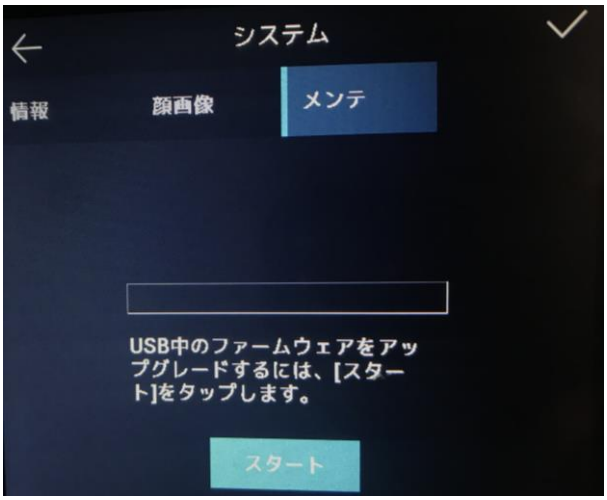


図6-15 アップグレード

6.10.2 データ管理

Data Management(データ管理)ページでは、ユーザーデータの削除、工場出荷時の設定への復元、またはデフォルト設定への復元を行うことができます。
「データ(Data Management)」をタップして、「データ管理」ページを開きます。ページ上のボタンをタップして、データを管理します。ポップアップウィンドウで「はい」をタップして設定を完了します。
使用可能なボタンの説明は次のとおりです:

表6-5 データの説明

パラメータ	説明
ユーザデータ削除	デバイス内のすべてのユーザーデータを削除します。
工場出荷時の状態に復元	システムを工場出荷時の設定に復元します。設定後、デバイスが再起動します。
デフォルトに戻す	システムをデフォルト設定に復元します。通信設定とリモートユーザー設定が保存されます。その他のパラメータはデフォルトに復元されます。設定後、デバイスは再起動します。

6.10.3 ログクエリ

従業員ID、カード番号、ユーザ名を入力することで、一定期間内に認証ログを検索することができます。

手順

1. ホームページで、「ログ(Log)」をタップして「ログ」ページに入ります。

図6-16 ログクエリ

2. ページの左側にある「カード」をタップし、ドロップダウンリストから検索タイプを選択します。
3. 入力ボックスをタップし、検索する従業員ID、カード番号、ユーザ名を入力します。
4. 時間を選択します。

注意

Custom、Yesterday、This Week、Last Week、This Month、Last Month、またはAll から選択できます。「カスタム(Custom)」を選択すると、検索の開始時刻と終了時刻をカスタマイズできます。

5. タップして検索を開始します。
   結果がページに表示されます。

6.11 時刻と出席状況の設定

時間と出席状況を設定します。実際の状況に応じて、出席モードをチェックイン、チェックアウト、ブレイクアウト、ブレイクイン、オーバータイムイン、オーバータイムアウトに設定できます。

注意

この関数は、クライアントソフトウェア上の時間と出席関数と協調して使用する必要があります。

6.11.1 デバイス経由の参加モードの無効化

参加モードを無効にすると、システムは最初のページに参加ステータスを表示しません。
「T&A状況」をタップして、「T&A状況」ページに入ります。

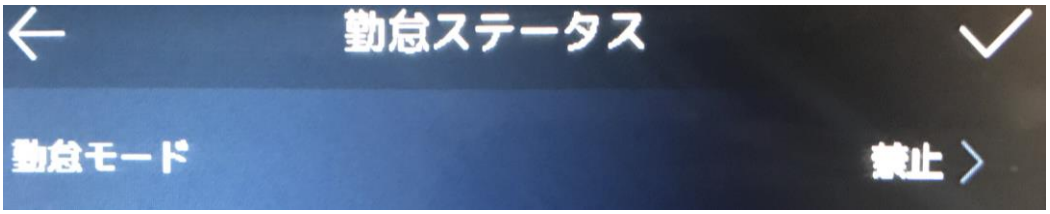


図6-17 アテンダンスモードの無効化

出席モードを無効に設定します。をタップします。
参加ステータスは、最初のページでは表示または設定しません。システムは、プラットフォームで設定された参加ルールに従います。

6.11.2 デバイスによる自動出席の設定

出席モードを自動に設定し、出席状況と利用可能なスケジュールを設定できます。システムは、設定されたパラメータに従って、参加ステータスを自動的に変更します。

はじめる前に

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状況」をタップして、「T&A状況」ページに入ります。
2. 出席モードを「自動」に設定します。

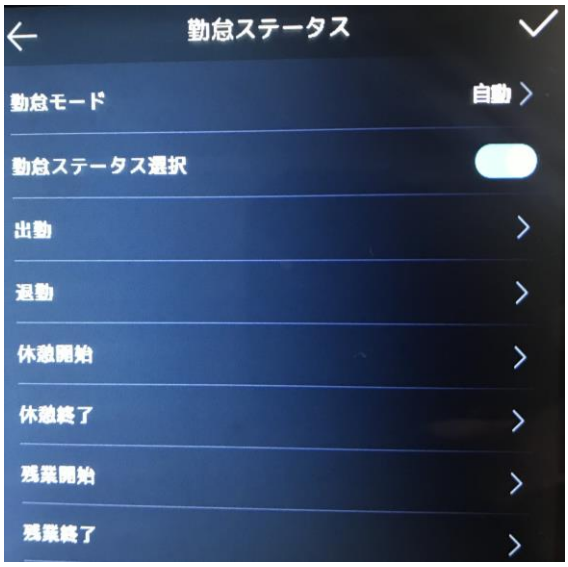


図6-18 自動参加モード

3. 出席状況を選択し、スケジュールを設定します。
   1) 出席状況として、「チェックイン」、「チェックアウト」、「ブレークアウト」、「ブレークイン」、「オーバータイムイン」、または「オーバータイムアウト」を選択します。
   2) 「スケジュール」をタップします。
   3) 月曜日、火曜日、水曜日、木曜日、金曜日、土曜日、日曜日を選択します。
   4) 選択した日付をタップし、選択した出席状況の開始時刻を設定します。
   5) 「確認」をタップします。
   6) 実際のニーズに応じて、手順1 ～5 を繰り返します。

注意

参加ステータスは、設定したスケジュール内で有効になります。

4. をタップします。

結果

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

例

ブレイクアウトスケジュールを月曜日11:00 に設定し、ブレイクインスケジュールを月曜日12:00 に設定すると、有効なユーザの認証が月曜日11:00 から12:00 にブレークとしてマークされます。

6.11.3 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すると、出席したときにステータスを手動で選択できます。

はじめる前に

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

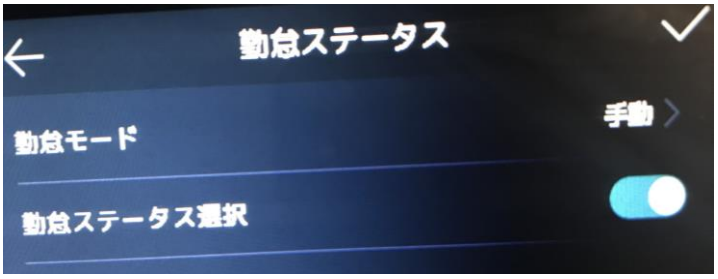


図6-19 手動出席モード

3. Attendance Status 機能を有効にします。

結果

認証後、参加ステータスを手動で選択する必要があります。

注意

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

6.11.4 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Manual(手動)およびAuto(自動)に設定すると、システムは設定されたパラメータに従って出席ステータスを自動的に変更します。同時に、認証後にアテンダンスステータスを手動で変更することもできます。

はじめる前に

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状況」をタップして、「T&A状況」ページに入ります。
2. 出席モードを手動および自動に設定します。

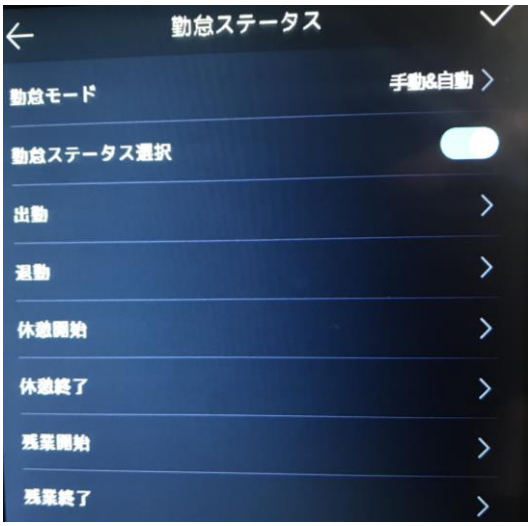


図6-20 手動モードと自動モード

3. 出席状況を選択し、スケジュールを設定します。
   1) 出席状況として、「チェックイン」、「チェックアウト」、「ブレークアウト」、「ブレークイン」、「オーバータイムイン」、または「オーバータイムアウト」を選択します。
   2) 「スケジュール」をタップします。
   3) 月曜日、火曜日、水曜日、木曜日、金曜日、土曜日、日曜日を選択します。
   4) 選択した日付をタップし、選択した出席状況の開始時刻を設定します。
   5) 「確認」をタップします。
   6) 実際のニーズに応じて、手順1 ～5 を繰り返します。

注意

参加ステータスは、設定したスケジュール内で有効になります。

4. をタップします。

結果

最初のページで認証します。ステータスを選択しない場合、認証はスケジュールに従って設定された出席ステータスとしてマークされます。「状況の選択」をタップし、出席を希望する状況を選択した場合、認証は選択した出席状況としてマークされます。

例

ブレイクアウトスケジュールを月曜日11:00 に設定し、ブレイクインスケジュールを月曜日12:00 に設定すると、有効なユーザの認証が月曜日11:00 から12:00 にブレークとしてマークされます。

6.12 システム情報を表示する

デバイス容量、デバイス情報、およびオープンソースソフトウェアライセンスを表示します。

容量の表示

追加したユーザー番号、顔画像番号、マスク付き顔番号、カード番号、イベント番号を確認できます。

「情報」をタップします。(システム情報)ホームページの容量を→して、容量ページに入ります。

図6-21 容量

デバイス情報を表示する

デバイス情報を表示できます。

「情報」をタップします。(システム情報)デバイスを→してデバイスページに入ります。

オープンソースライセンス

オープンソースライセンス情報を表示します。

「情報」をタップします。(システムインフォメーション) →ライセンスを入力して、オープンソースソフトライセンスページに入力します。

デバイスQRコードの表示

デバイスの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追加できます。
「情報」をタップします。(システム情報) QR コードを→して、デバイスのQR コードを表示します。

6.13 ビデオインターコム

クライアントソフトウェアにデバイスを追加したら、クライアントソフトウェアからデバイスを呼び出したり、デバイスからマスターステーションを呼び出したり、デバイスからクライアントソフトウェアを呼び出したり、デバイスから屋内ステーションを呼び出したりできます。

6.13.1 デバイスからクライアントソフトウェアを呼び出す

手順

1. 付属のディスクまたは公式ウェブサイトからクライアントソフトウェアを入手し、プロンプトに従ってソフトウェアをインストールします。
2. クライアントソフトウェアを実行すると、ソフトウェアのコントロールパネルがポップアップ表示されます。
3. デバイス管理をクリックして、デバイス管理インタフェースに入ります。
4. デバイスをクライアントソフトウェアに追加します。

注意

デバイスの追加については、「デバイスの追加」を参照してください。

5. クライアントソフトウェアを呼び出します。
   1) デバイスの初期ページで「通話」をタップします。
   2) ポップアップウィンドウで0 を入力します。
   3) 「通話」をタップすると、クライアントソフトウェアに電話がかかります。
6. クライアントソフトウェアのポップアップページで「応答」をタップすると、デバイスとクライアントソフトウェアの間で双方向オーディオを開始できます。

注意

デバイスが複数のクライアントソフトウェアに追加され、デバイスがクライアントソフトウェアを呼び出している場合、最初に追加されたクライアントソフトウェアのみが呼び出し受信ウィンドウをポップアップ表示します。

6.13.2 デバイスからマスタ局を呼び出す

手順

1. 付属のディスクまたは公式ウェブサイトからクライアントソフトウェアを入手し、プロンプトに従ってソフトウェアをインストールします。
2. クライアントソフトウェアを実行すると、ソフトウェアのコントロールパネルがポップアップ表示されます。
3. デバイス管理をクリックして、デバイス管理インタフェースに入ります。
4. マスタ局とデバイスをクライアントソフトウェアに追加します。

注意

デバイスの追加については、「デバイスの追加」を参照してください。

5. リモート設定ページでマスタ局のIPアドレスとSIPアドレスを設定します。

注意

詳しい操作方法については、マスタ局のユーザーズマニュアルを参照してください。

6. マスタ局経由で応答し、双方向音声を開始します。

注意

タップすると、優先してマスタ局を呼び出します。

6.13.3 クライアントソフトウェアからのデバイスの呼び出し

手順

1. 付属のディスクまたは公式ウェブサイトからクライアントソフトウェアを入手し、プロンプトに従ってソフトウェアをインストールします。
2. クライアントソフトウェアを実行すると、ソフトウェアのコントロールパネルがポップアップ表示されます。
3. デバイス管理をクリックして、デバイス管理ページに入ります。
4. デバイスをクライアントソフトウェアに追加します。

注意

デバイスの追加については、「デバイスの追加」を参照してください。

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

注意

ライブビュー画面での操作については、クライアントソフトウェアの取扱説明書の「ライブビュー」をご覧ください。

6. ライブビュー映像を右クリックすると、右クリックメニューが表示されます。
7. デバイスとクライアントソフトウェア間で双方向オーディオを開始するには、「双方向オーディオを開始」をクリックします。

6.13.4 デバイスから屋内局を呼び出す

手順

1. 付属のディスクまたは公式ウェブサイトからクライアントソフトウェアを入手し、プロンプトに従ってソフトウェアをインストールします。
2. クライアントソフトウェアを実行すると、ソフトウェアのコントロールパネルがポップアップ表示されます。
3. デバイス管理をクリックして、デバイス管理インタフェースに入ります。
4. クライアントソフトウェアに屋内ステーションとデバイスを追加します。

注意

デバイスの追加については、「デバイスの追加」を参照してください。

5. ユーザーを室内局にリンクさせ、室内局の部屋番号を設定します。
6. デバイスの認証ページをタップします。
7. ダイヤルページに部屋番号を入力し、タップして室内ステーションに電話をかけます。
8. 室内局が応答すると、室内局と双方向音声を開始できます。

第7章クライアントソフトウェアの設定

7.1 クライアントソフトウェアの設定フロー

クライアントソフトウェアで設定するには、次のフロー図に従います。

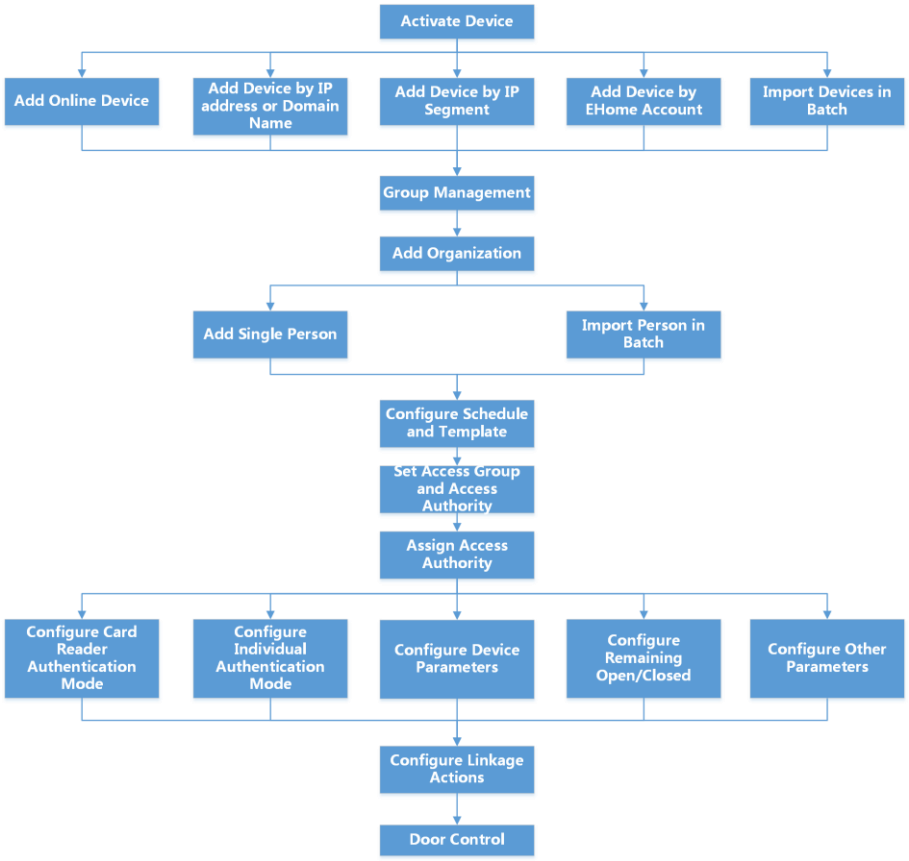


図7-1 クライアントソフトウェアの設定フロー

7.2 デバイス管理

クライアントは、アクセス制御デバイスおよびビデオインターコムデバイスの管理をサポートします。

例

クライアントにアクセスコントロールデバイスを追加した後、入退室管理や出席管理を行うことができます。屋内ステーションやドアステーションとビデオインターホンを行うことができます。

7.2.1 デバイスの追加

クライアントは、IP/ドメイン、IPセグメント、およびISUPプロトコルを含む3つのデバイス追加モードを提供します。また、クライアントは、大量のデバイスを追加する場合に、複数のデバイスを一括でインポートすることもできます。

オンラインデバイスの追加

クライアントソフトウェアと同じローカルサブネット内のアクティブなオンラインデバイスが、オンラインデバイスエリアに表示されます。Refresh Every 60s をクリックすると、オンラインデバイスの情報を更新できます。

検出されたオンラインデバイスの追加

オンラインデバイスリストに表示されている検出済みのオンラインデバイスを選択し、クライアントに追加できます。

手順

1. デバイス管理モジュールを入力します。
2. 右パネルの上部にある「デバイス(Device)」タブをクリックします。
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エリアを表示します。
   検索したオンラインデバイスがリストに表示されます。

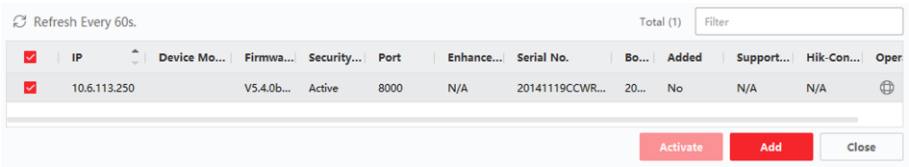


図7-2 オンラインデバイスの選択

4. 「オンラインデバイス」領域でオンラインデバイスを選択し、「追加」をクリックしてデバイス追加ウィンドウを開きます。

注意

非アクティブなデバイスの場合は、デバイスを正しく追加する前に、そのデバイスのパスワードを作成する必要があります。詳細な手順については、を参照してください。

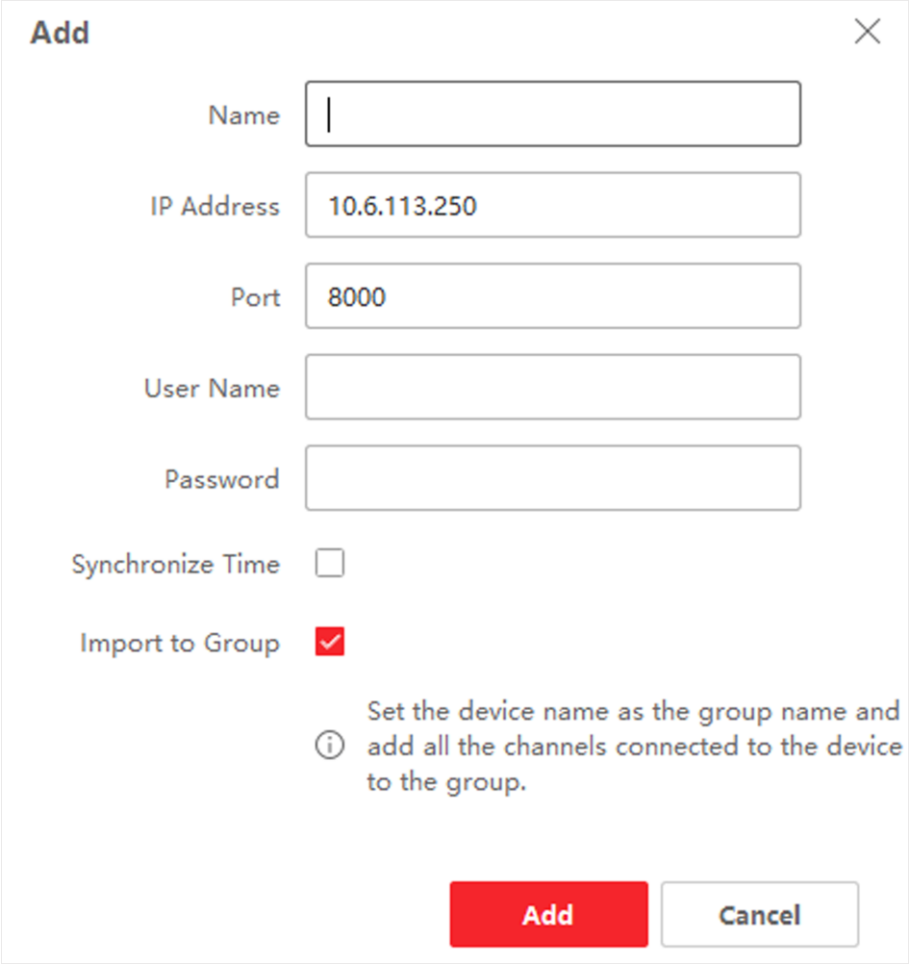


図7-3 オンラインデバイスの追加

5. 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入力します。

IP アドレス

デバイスのIP アドレスを入力します。この追加モードでは、デバイスのIP アドレスが自動的に取得されます。

ポート

ポート番号をカスタマイズできます。この追加モードでは、デバイスのポート番号が自動的に取得されます。

ユーザー名

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強度を自動的に確認できます。製品のセキュリティを強化するために、独自のパスワードを変更することを強くお勧めします(大文字、小文字、数字、特殊文字の3種類以上を含む8 文字以上を使用)。また、パスワードを定期的に変更することをお勧めします。特に高セキュリティシステムでは、パスワードを月単位または週単位で変更することで製品を保護できます。
すべてのパスワードおよびその他のセキュリティ設定を適切に構成するのは、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。

6. オプション: TLS (Transport Layer Security) プロトコルを使用してセキュリティ目的で送信暗号化を有効にするには、TLS (Transmission Encryption) をオンにします。

注意

- この機能はデバイスでサポートされている必要があります。
- 証明書の検証を有効にした場合は、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する必要があります。証明書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ブラウザで証明書ファイルを取得することができます。

7. 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するには、時刻の同期をオンにします。
8. 必要に応じて、「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

アクセスコントロールデバイスでは、アクセスポイント、アラーム入出力、エンコードチャンネル(存在する場合)がこのグループにインポートされます。

9. 追加をクリックします。

検出された複数のオンラインデバイスの追加

検出されたオンラインデバイスが同じユーザー名とパスワードを共有している場合は、それらをバッチでクライアントに追加できます。

はじめる前に

追加するデバイスがオンラインであることを確認します。

手順

1. デバイス管理モジュールを入力します。
2. 右パネルの上部にある「デバイス(Device)」タブをクリックします。
3. 「オンラインデバイス」をクリックすると、ページの下部にオンラインデバイス領域が表示されます。

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. 複数のデバイスを選択します。

注意

非アクティブなデバイスの場合は、デバイスを正しく追加する前に、そのデバイスのパスワードを作成する必要があります。詳細はを参照してください。

5. 「追加」をクリックして、デバイスの追加ウィンドウを開きます。
6. 必要な情報を入力します。

ユーザー名

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強度を自動的に確認できます。製品のセキュリティを強化するために、独自のパスワードを変更することを強くお勧めします(大文字、小文字、数字、特殊文字の3種類以上を含む8 文字以上を使用)。また、パスワードを定期的に変更することをお勧めします。特に高セキュリティシステムでは、パスワードを月単位または週単位で変更することで製品を保護できます。
すべてのパスワードおよびその他のセキュリティ設定を適切に構成するのは、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。

7. オプション: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するには、時刻の同期をオンにします。
8. 必要に応じて、「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

アクセスコントロールデバイスでは、アクセスポイント、アラーム入出力、エンコードチャンネル(存在する場合)がこのグループにインポートされます。

9. 追加をクリックして、デバイスを追加します。

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. 右パネルの上部にある「デバイス(Device)」タブをクリックします。

追加したデバイスが右側のパネルに表示されます。

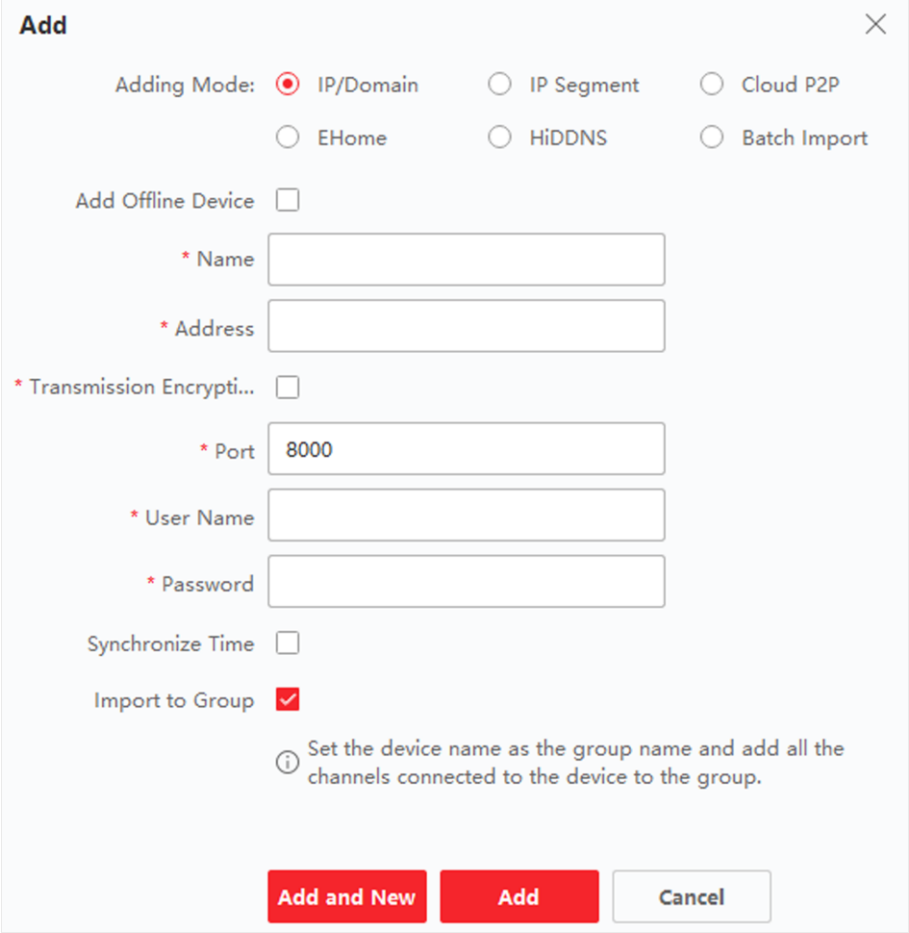


図7-4 IP アドレスまたはドメイン名によるデバイスの追加

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。例えば、装置のロケーションまたはフィーチャーを示すニックネームを使用することができます。

アドレス

デバイスのIP アドレスまたはドメイン名。

ポート

追加するデバイスは、同じポート番号を共有します。デフォルト値は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強度を自動的に確認できます。製品のセキュリティを強化するために、独自のパスワードを変更することを強くお勧めします(大文字、小文字、数字、特殊文字の3種類以上を含む8 文字以上を使用)。また、パスワードを定期的に変更することをお勧めします。特に高セキュリティシステムでは、パスワードを月単位または週単位で変更することで製品を保護できます。
すべてのパスワードおよびその他のセキュリティ設定を適切に構成するのは、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: TLS (Transport Layer Security) プロトコルを使用してセキュリティ目的で送信暗号化を有効にするには、TLS (Transmission Encryption) をオンにします。

注意

- この機能はデバイスでサポートされている必要があります。
- 証明書の検証を有効にした場合は、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する必要があります。証明書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ブラウザで証明書ファイルを取得することができます。

6. 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するには、時刻の同期をオンにします。
7. 必要に応じて、「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

アクセスコントロールデバイスでは、アクセスポイント、アラーム入出力、エンコードチャンネル(存在する場合)がこのグループにインポートされます。

8. デバイスの追加を完了します。
   - Add(追加)をクリックしてデバイスを追加し、デバイスリストページに戻ります。
   - 「追加」および「新規」をクリックして設定を保存し、続けて他のデバイスを追加します。

IP セグメントによるデバイスの追加

同じIPセグメント内で同じポート番号、ユーザ名、パスワード、IPアドレス範囲を共有している場合は、デバイスの先頭IPアドレス、末尾IPアドレス、ポート番号、ユーザ名、パスワードなどを指定してクライアントに追加できます。

手順

1. デバイス管理モジュールを入力します。
2. 右パネルの上部にある「デバイス(Device)」タブをクリックします。

追加し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ます。

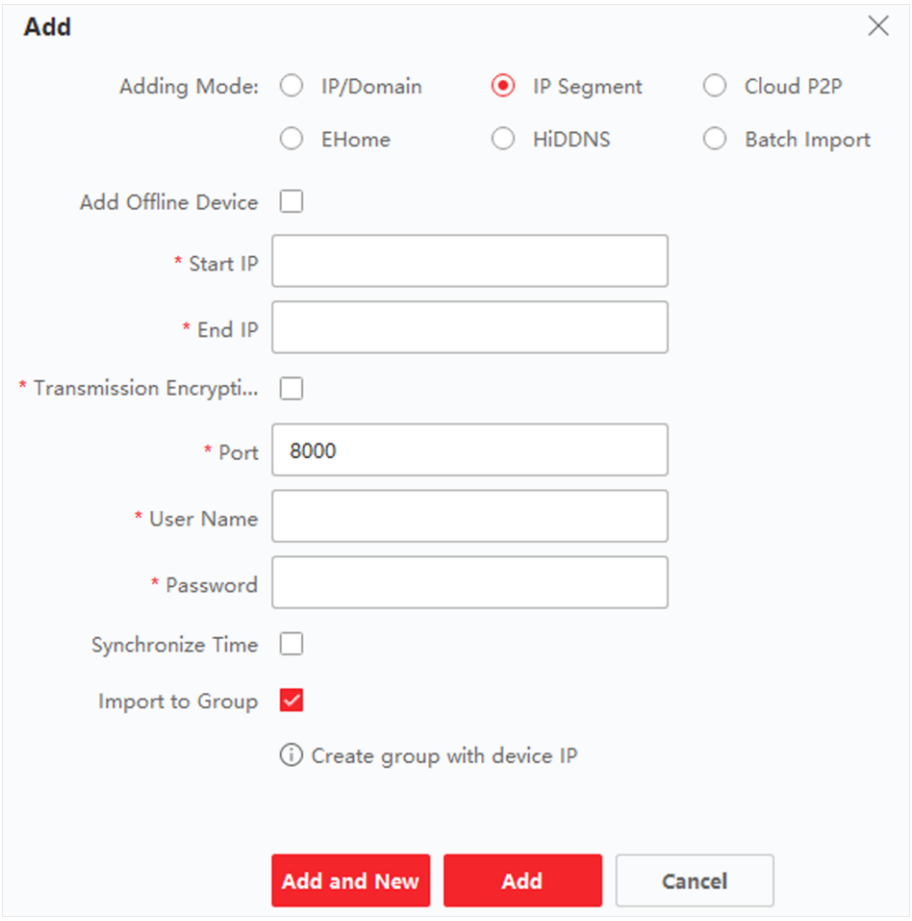


図7-5 IP セグメントによるデバイスの追加

4. 追加モードとして「IP Segment」を選択します。
5. 必要な情報を入力します。

開始IP

開始IP アドレスを入力します。

エンドIP

開始IP と同じネットワークセグメントに終了IP アドレスを入力します。

ポート

デバイスポート番号を入力します。初期値は8000です。

ユーザー名

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強度を自動的に確認できます。製品のセキュリティを強化するために、独自のパスワードを変更することを強くお勧めします(大文字、小文字、数字、特殊文字の3種類以上を含む8 文字以上を使用)。また、パスワードを定期的に変更することをお勧めします。特に高セキュリティシステムでは、パスワードを月単位または週単位で変更することで製品を保護できます。
すべてのパスワードおよびその他のセキュリティ設定を適切に構成するのは、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。

6. オプション: TLS (Transport Layer Security) プロトコルを使用した送信暗号化をセキュリティ目的で有効にするには、TLS (Transmission Encryption) をオンにします。

注意

- この機能はデバイスでサポートされている必要があります。
- 証明書の検証を有効にした場合は、証明書フォルダ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する必要があります。証明書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ブラウザで証明書ファイルを取得することができます。

7. 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するには、時刻の同期をオンにします。
8. 必要に応じて、「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グループにインポートします。
9. デバイスの追加を完了します。
   – Add(追加)をクリックしてデバイスを追加し、デバイスリストページに戻ります。
   – 「追加」および「新規」をクリックして設定を保存し、続けて他のデバイスを追加します。

ISUP アカウントによるデバイスの追加

アクセスコントロールデバイスがISUP 5.0 プロトコルをサポートしている場合、デバイスID とキーを入力した後、サーバアドレス、ポート番号、およびデバイスID を設定していれば、ISUP プロトコルによってそれらをクライアントに追加できます。

はじめる前に

デバイスがネットワークに正しく接続されていることを確認します。

手順

1. デバイス管理モジュールに入ります。
   追加したデバイスが右側のパネルに表示されます。
2. 追加をクリックして、追加ウィンドウを開きます。
3. 追加モードとしてISUP を選択します。

4. 必要な情報を入力します。

デバイスアカウント

ISUPプロトコルに登録されているアカウント名を入力します。

ISUPキー

ISUP 5.0 デバイスの場合、デバイスのネットワークセンターパラメータを設定するときに ISUP キーを入力します(設定している場合)。

注意

この機能はデバイスでサポートされている必要があります。

5. オプション: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するには、時刻の同期をオンにします。
6. 必要に応じて、「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グループにインポートします。
7. デバイスの追加を完了します。
   - Add(追加)をクリックしてデバイスを追加し、デバイスリストに戻ります。
   - 「追加」および「新規」をクリックして設定を保存し、続けて他のデバイスを追加します。

注意

DS-K1T671シリーズ、DS-K1T331シリーズ以外のISUPアカウントで登録した機器には顔写真を適用できません。

8. オプション: 以下の操作を実行します。

装置の状況	Operation 列をクリックして、デバイスのステータスを表示します。
デバイス情報の編集	「操作」列をクリックして、デバイス名、デバイスアカウント、ISUPキーなどのデバイス情報を編集します。
オンラインユーザーの確認	「操作」列をクリックして、デバイスにアクセスするオンラインユーザ(ユーザ名、ユーザタイプ、ユーザのIPアドレス、ログイン時間など)を確認します。
リフレッシュ	「Operation」列をクリックして、最新のデバイス情報を取得します。
デバイスの削除	1 つまたは複数のデバイスを選択し、削除をクリックして、選択したデバイスをクライアントから削除します。

デバイスの一括インポート

定義済みのCSV ファイルにデバイスパラメータを入力することで、複数のデバイスをクライアントに一括して追加できます。

手順

1. デバイス管理モジュールを入力します。
2. 右パネルの上部にある「デバイス(Device)」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。

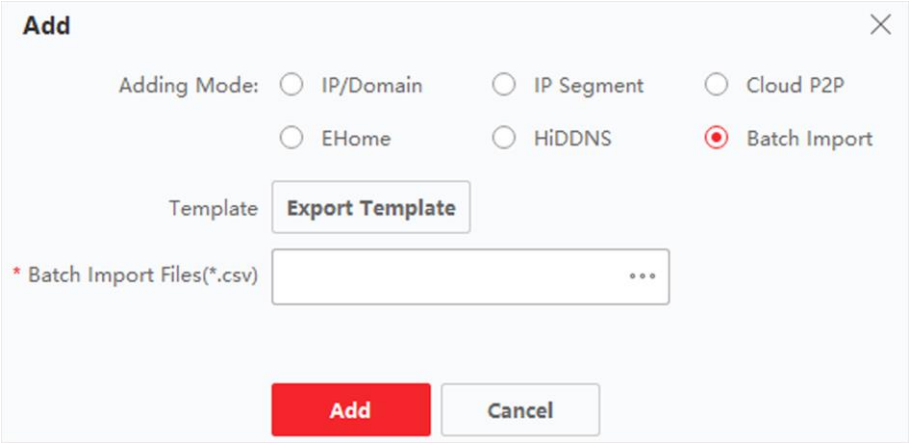


図7-6 デバイスの一括追加

4. Export Template (テンプレートのエクスポート)をクリックし、定義済みテンプレート(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。

注意

必須フィールドの詳細については、テンプレートの「はじめに」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。

アドレス

デバイスのアドレスを編集します。

ポート

デバイスのポート番号を入力します。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強度を自動的に確認できます。製品のセキュリティを強化するために、独自のパスワードを変更することを強くお勧めします(大文字、小文字、数字、特殊文字の3種類以上を含む8 文字以上を使用)。また、パスワードを定期的に変更することをお勧めします。特に高セキュリティシステムでは、パスワードを月単位または週単位で変更することで製品を保護できます。
すべてのパスワードおよびその他のセキュリティ設定を適切に構成するのは、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。

グループにインポート

1 を入力して、デバイス名でグループを作成します。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. デバイスをインポートするには、追加をクリックします。

7.2.2 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、クライアント経由で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エリアを表示します。
   同じサブネットを共有するすべてのオンラインデバイスがリストに表示されます。
3. リストからデバイスを選択し、「操作(Operation)」コラムをクリックします。
4. デバイスのパスワードをリセットします。
   - Generate(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表示し、Download(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コードの写真を撮影して端末に保存することもできます。画像を当社のテクニカルサポートに送信します。

注意

以下のパスワードのリセット操作については、弊社テクニカルサポートにお問い合わせください。

注意

デバイスのパスワード強度を自動的に確認できます。製品のセキュリティを強化するために、独自のパスワードを変更することを強くお勧めします(大文字、小文字、数字、特殊文字の3 種類以上を含む8 文字以上を使用)。また、パスワードを定期的に変更することをお勧めします。特に高セキュリティシステムでは、パスワードを月単位または週単位で変更することで製品を保護できます。
すべてのパスワードおよびその他のセキュリティ設定を適切に構成するのは、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。

7.3 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グループ化できます。

例

例えば、1階には、16のドア、64のアラーム入力、16のアラーム出力が取り付けられています。管理しやすいように、これらのリソースを1つのグループ(1st Floorという名前)にまとめることができます。リソースをグループ別に管理した後で、ドアステータスを制御したり、デバイスのその他の操作を実行したりできます。

7.3.1 グループの追加

グループを追加して、管理しやすいように追加したデバイスを整理できます。

手順

1. デバイス管理モジュールを入力します。
2. 「デバイス管理→グループ」を選択して、グループ管理画面を表示します。
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。
   – デバイス名でグループを作成をクリックし、追加したデバイスを選択して、選択したデバイスの名前で新しいグループを作成します。

   注意

   デフォルトでは、本機のリソース(アラーム入出力、アクセスポイントなど)がグループにインポートされます。

7.3.2 グループへのリソースのインポート

追加したグループにデバイスリソース(アラーム入出力、アクセスポイントなど)を一括でインポート

できます。

はじめる前に

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を入力します。
2. 「デバイス管理→グループ」を選択して、グループ管理画面を表示します。
3. グループリストからグループを選択し、Access Point、Alarm Input、Alarm Outputなどのリソースタイプを選択します。
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。

注意

またはをクリックすると、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。

7.3.3 リソースパラメータの編集

リソースをグループにインポートしたら、リソースパラメータを編集できます。アクセスポイントの場合は、アクセスポイント名を編集できます。アラーム入力の場合、アラーム入力名を編集できます。ここでは、アクセスポイントを例に説明します。

はじめる前に

リソースをグループにインポートします。「グループへのリソースのインポート」を参照してください。

手順

1. デバイス管理モジュールを入力します。
2. 「デバイス管理→グループ」を選択して、グループ管理画面を表示します。
   追加されたすべてのグループが左側に表示されます。
3. グループリストでグループを選択し、「アクセスポイント」をクリックします。
   グループにインポートされたアクセスポイントが表示されます。
4. 「操作」列をクリックして、「リソースの編集」ウィンドウを開く。
5. リソース名を編集します。
6. 「OK」をクリックして、新しい設定値を保管する。

7.3.4 グループからのリソースの削除

追加したリソースをグループから削除できます。

手順

1. デバイス管理モジュールを入力します。
2. 「デバイス管理→グループ」を選択して、グループ管理画面を表示します。
   追加されたすべてのグループが左側に表示されます。
3. グループをクリックすると、このグループに追加されたリソースが表示されます。
4. リソースを選択し、削除をクリックしてグループからリソースを削除します。

7.4 個人管理

アクセスコントロール、ビデオインターコム、時間と出席などの操作をさらに進めるために、個人情報をシステムに追加できます。一括してカードを発行したり、個人情報を一括で取り込んだり、書き出したりするなど、追加した個人を管理できます。

7.4.1 組織の追加

組織を追加し、個人情報を組織にインポートして、個人を効果的に管理できます。また、追加した組織には、Surbodinate 組織を追加することもできます。

手順

1. Person モジュールを入力します。
2. 左側の列で親組織を選択し、左上の「追加」をクリックして組織を追加します。
3. 追加した組織の名前を作成します。

注意

最大10 レベルの組織を追加できます。

4. オプション: 以下の操作を実行します。

組織の編集	追加した組織の上にマウスを置き、クリックして名前を編集します。
組織の削除	追加した組織にマウスを置き、クリックして削除します。

注意

- 組織を削除すると、下位の組織も削除されます。
- 組織の下に個人が追加されていないことを確認します。そうでない場合は、組織を削除できません。

サブ組織での個人の表示	Show Persons in Sub Organization をオンにし、組織を選択してそのサブ組織の個人を表示します。

7.4.2 基本情報の設定

人物をクライアントソフトウェアに1人ずつ追加し、名前、性別、電話番号などの人物の基本情報を設定できます。

手順

1. Person モジュールを入力します。
2. 組織リストで組織を選択し、個人を追加します。
3. 「追加」をクリックして、個人の追加ウィンドウを開きます。
   個人ID が自動的に生成されます。
4. 個人名、性別、電話、メールアドレスなどの基本情報を入力します。
5. オプション: 個人の有効期間を設定します。有効期限が切れると、個人の資格情報とアクセスコントロールの設定は無効になり、個人はdoors¥floors にアクセスする権限を持ちません。

   例

   例えば、ビジターである場合、その有効期間は短くて一時的である可能性があります。
6. 個人を追加することを確認します。
   – 「追加」をクリックして個人を追加し、「個人の追加」ウィンドウを閉じます。
   – 「追加」および「新規」をクリックして人物を追加し、他の人物の追加を続行します。

7.4.3 ローカルモードによるカードの発行

カード登録ステーションが使用可能な場合は、ローカルモードでカードを発行できます。カード番号を読み取るには、カード登録ステーションを、USBインタフェースまたは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ステーションに置く必要があります。

手順

1. Person モジュールを入力します。
2. 組織リストで組織を選択して個人を追加し、「追加」をクリックして「個人を追加」パネルに入ります。

注意

まず、個人の基本情報を入力します。個人の基本情報の設定については、「基本情報の設定」を参照してください。

3. 資格情報→カード領域で、をクリックします。
4. 設定をクリックして、設定ページに入ります。
5. カード発行モードとして「ローカル」を選択します。

6. その他の関連パラメータを設定します。

カード登録ステーション

接続されているカード登録ステーションのモデルを選択します。

注意

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

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。カードの種類は、実際のカードの種類に合わせて、EMカードまたはMifareカードを選択してください。

ブザー

カード番号の読み取りに成功したときのブザー音を有効または無効にします。

カード番号タイプ

カード番号の種類は、実際のニーズに合わせて選択してください。

M1 カード暗号化

このフィールドは、モデルがDS-K1F100-D8、DS-K1F100-D8E、またはDS-K1F180-D8E の場合のみ使用できます。カードがM1 カードの場合は、M1 カード暗号化機能を有効にして、暗号化するカードのセクターを選択できます。

7. OK をクリックして操作を確認します。
8. カードをカード登録ステーションに置き、読み取りをクリックしてカード番号を取得します。
   カード番号が「カード番号」欄に自動的に表示されます。
9. 追加をクリックします。
   カードは個人に発行されます。

7.4.4 ローカルPCから顔写真をアップロードする

人物を追加するときに、ローカルPCに保存されている顔写真を人物のプロフィールとしてクライアントにアップロードできます。

手順

1. Person モジュールを入力します。
2. 組織リストで組織を選択して個人を追加し、「追加」をクリックします。

注意

まず、個人の基本情報を入力します。個人の基本情報の設定については、「基本情報の設定」を参照してください。

3. 基本情報パネルで顔の追加をクリックします。
4. アップロードを選択します。
5. クライアントを起動しているパソコンから画像を選択します。

注意

画像は、JPG またはJPEG 形式で200KB 未満である必要があります。

6. オプション:クライアントで管理されている顔認識デバイスが写真の顔を認識できるかどうかを確認するには、「デバイスによる検証」を有効にします。
7. 個人を追加することを確認します。
   – 「追加」をクリックして個人を追加し、「個人の追加」ウィンドウを閉じます。
   – 「追加」および「新規」をクリックして人物を追加し、他の人物の追加を続行します。

7.4.5 クライアント経由で写真を撮影する

人物を追加するときは、クライアント経由で自分の写真を撮影し、その写真を人物のプロフィールとして設定できます。

はじめる前に

クライアントを実行しているPC にカメラが搭載されていること、または他のUSB カメラをPC に接続していることを確認します。

手順

1. Person モジュールを入力します。
2. 組織リストで組織を選択して個人を追加し、「追加」をクリックして「個人の追加」ウィンドウに入ります。

注意

まず、個人の基本情報を入力します。詳細については、「基本情報の設定」を参照してください。

3. 基本情報領域で顔の追加をクリックします。
4. Take Photo を選択してTake Photo ウィンドウに入ります。
5. オプション: デバイスによる検証を有効にして、キャプチャされた顔写真がアップロード要件を満たすことができるかどうかを確認します。
6. 写真を撮影します。
   1) カメラに向かって、顔が収集ウィンドウの中央にあることを確認します。
   2) クリックして顔写真を撮影します。

3) (オプション) をクリックして再度キャプチャします。
4) 「OK」をクリックして、撮影した写真を保存します。

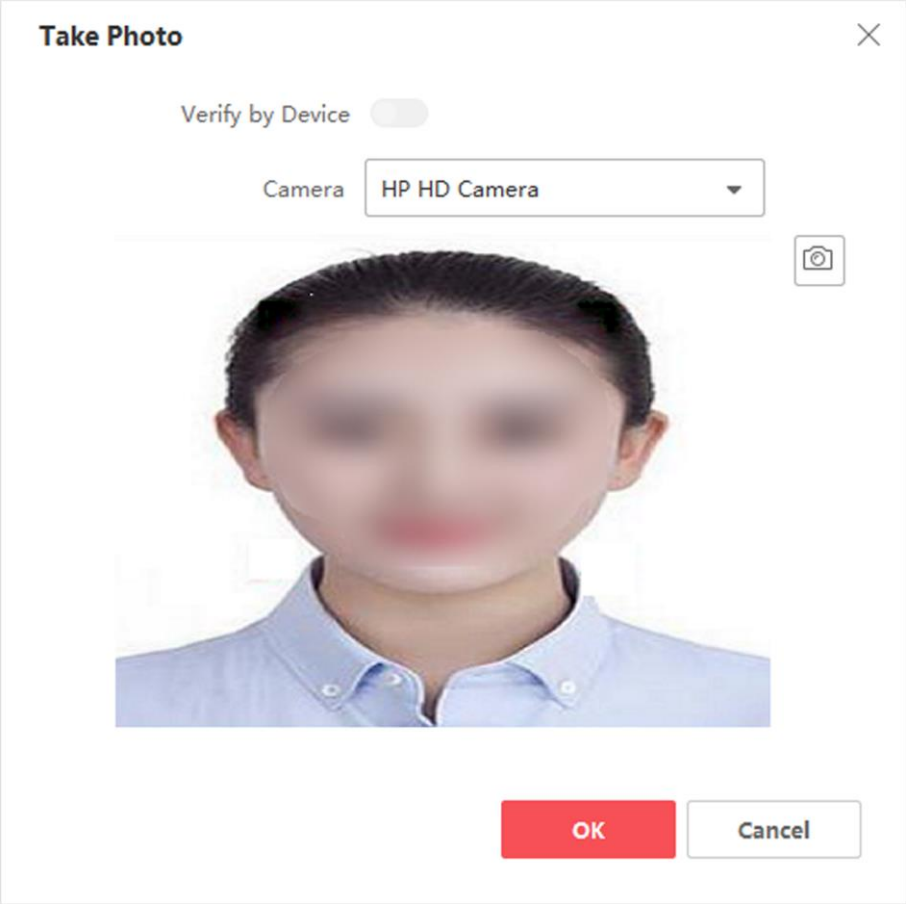


図7-7 クライアント経由での写真の撮影

7. 個人を追加することを確認します。
   – 「追加」をクリックして個人を追加し、「個人の追加」ウィンドウを閉じます。
   – 「追加」および「新規」をクリックして人物を追加し、他の人物の追加を続行します。

7.4.6 アクセスコントロールデバイスによる顔の収集

人物を追加するときに、顔認識機能をサポートするクライアントに追加されたアクセスコントロールデバイスを使用して、人物の顔を収集できます。

手順

1. Person モジュールを入力します。
2. 組織リストで組織を選択して個人を追加し、「追加」をクリックします。

注意

まず、個人の基本情報を入力します。個人の基本情報の設定については、「基本情報の設定」を参照してください。

3. 基本情報パネルで顔の追加をクリックします。
4. リモートコレクションを選択します。
5. ドロップダウンリストから、追加したアクセスコントロールデバイスまたは登録ステーションを選択します。

注意

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て、IPアドレス、ポート番号、ユーザー名、パスワードなど、デバイスの関連パラメータを設定する必要があります。また、フェイスアンチスプーフィングをチェックして、ライブレベルを「低」、「中」、または「高」から選択することもできます。

スプーフィング防止に直面する

この機能をチェックすると、装置は収集する顔が本物であるかどうかを検出することができます。

6. 顔を集める。
   1) 選択したアクセスコントロールデバイスのカメラに向かって、顔が収集ウィンドウの中央にあることを確認します。
   2) クリックして写真を撮影します。
   3) 「OK」をクリックして、撮影した写真を保存します。
7. 個人を追加することを確認します。
   – 「追加」をクリックして個人を追加し、「個人の追加」ウィンドウを閉じます。
   – 「追加」および「新規」をクリックして人物を追加し、他の人物の追加を続行します。

7.4.7 アクセス制御情報の設定

個人を追加する場合は、アクセスコントロールグループを個人と結びつける、PINコードを設定する、訪問者を設定する、ブラックリスト利用者を設定する、スーパーユーザを設定するなど、アクセスコントロール情報を設定できます。

手順

1. Person モジュールを入力します。
2. 組織リストで組織を選択して個人を追加し、「追加」をクリックします。
3. Access Control(アクセスコントロール)領域で、をクリックして個人のアクセスグループを選択します。

注意

詳細については、「アクセス許可を個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。

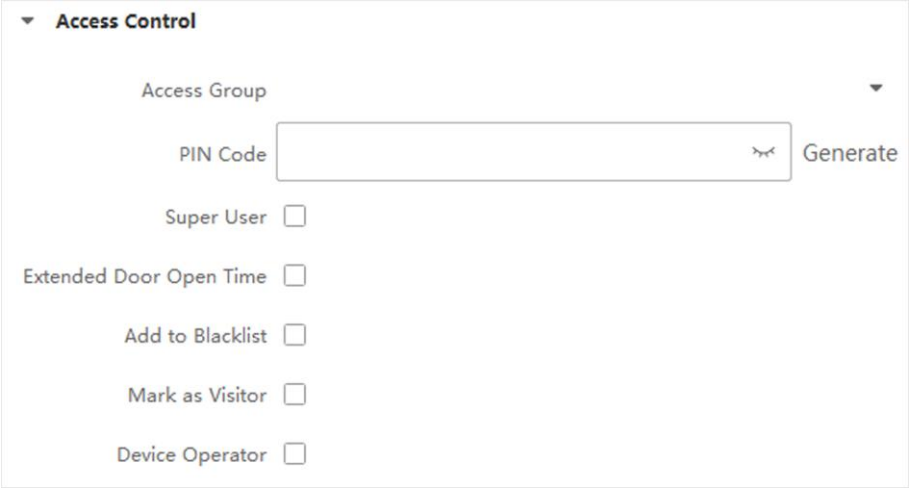


図7-8 アクセス制御情報の設定

4. アクセス認証に使用できる相手に固有のPINコードを設定します。
   - 4～8桁の暗証番号を手動で入力します。

     注意

     相手のPINコードを繰り返すことはできません。

   - Generate(生成)をクリックして、6 桁の無制限の PIN コードをランダムに生成します。

     注意

     PINコードが繰り返されている場合は、クライアントにプロンプトがポップアップ表示されます。管理者は、新しいPIN コードを生成して、繰り返されるPIN コードを置き換え、関連するユーザに通知することができます。

5. 個人の操作権限を確認します。

スーパー・ユーザー

スーパーユーザとして設定されている場合、そのユーザはすべてのドア/フロアにアクセスする権限を持ち、閉鎖制限の残り、すべてのパスバック防止ルール、およびファーストパーソン認証から除外されます。

延長ドア開放時間

この機能は、モビリティが低下しているユーザーに使用します。ドアにアクセスすると、他の人よりもドアを通過する時間が長くなります。
ドアの開放時間の設定については、「ドアのパラメータの設定」を参照してください。

ブラックリストに追加

個人をブラックリストに追加し、ドア/フロアにアクセスしようとすると、イベントがトリガーされてクライアントに送信され、セキュリティ担当者に通知されます。

ビジターとしてマーク

訪問者の場合は、訪問の有効期間を設定する必要があります。

注意

ビジットの有効時間は1 ～100 です。「制限なし」をオンにすると、ビジターがドア/フロアにアクセスする時間が制限されなくなります。

デバイスオペレータ

デバイスオペレータの役割を有する者は、アクセス制御装置上での操作を許可される。

注意

Super User、Extended Door Open Time、Add to Blacklist、およびMark as Visitor の各機能を同時に有効にすることはできません。たとえば、1人がスーパーユーザーに設定されている場合は、拡張ドアの開放時間を有効にしたり、ブラックリストに追加したり、ビジターに設定したりすることはできません。

6. 個人を追加することを確認します。
   – 「追加」をクリックして個人を追加し、「個人の追加」ウィンドウを閉じます。
   – 「追加」および「新規」をクリックして人物を追加し、他の人物の追加を続行します。

7.4.8 個人情報のカスタマイズ

実際のニーズ(出生地など)に応じて、クライアントで事前定義されていない個人プロパティをカスタマイズできます。カスタマイズ後、個人を追加するときに、カスタム情報を入力して個人情報を完成させることができます。

手順

1. Person モジュールを入力します。
2. カスタム情報のフィールドを設定します。
   1) カスタムプロパティをクリックします。
   2) 「追加」をクリックして、新しいプロパティを追加します。
   3) プロパティ名を入力します。
   4) OKをクリックします。
3. 個人を追加するときにカスタム情報を設定します。

1）組織リストで組織を選択して個人を追加し、「追加」をクリックします。

注意

まず、個人の基本情報を入力します。個人の基本情報の設定については、「基本情報の設定」を参照してください。

2）カスタム情報パネルで、個人情報を入力します。
3）「追加」をクリックして人物を追加し、「個人を追加」ウィンドウを閉じるか、「追加して新規」をクリックして人物を追加し、続けて他の人物を追加します。

7.4.9 常駐情報の設定

居住者の場合、ビデオインターコムのために、部屋番号を設定し、屋内ステーションをバインドする必要があります。バウンド後、屋内ステーションに電話してビデオインターホンを実行することで、この相手に電話をかけることができます。

手順

1. Person モジュールを入力します。
2. 組織リストで組織を選択して個人を追加し、「追加」をクリックします。

注意

まず、個人の基本情報を入力します。個人の基本情報の設定については、「基本情報の設定」を参照してください。

3. 住民情報パネルで、屋内ステーションを選択して人物にバインドします。

注意

「Analog Indoor Station」を選択すると、「Door Station」フィールドが表示され、アナログの屋内ステーションと通信するためにドアステーションを選択する必要があります。

4. 人のフロアNo.とルームNo.を入力します。
5. 個人を追加することを確認します。
   – 「追加」をクリックして個人を追加し、「個人の追加」ウィンドウを閉じます。
   – 「追加」および「新規」をクリックして人物を追加し、他の人物の追加を続行します。

7.4.10 追加情報の設定

個人を追加する場合は、実際のニーズに応じて、個人のアイデンティティタイプ、アイデンティティ番号、国など、個人の追加情報を設定できます。

手順

1. Person モジュールを入力します。

2. 組織リストで組織を選択して個人を追加し、「追加」をクリックします。

注意

まず、個人の基本情報を入力します。個人の基本情報の設定については、「基本情報の設定」を参照してください。

3. 「追加情報」パネルで、実際のニーズに応じて、個人のID タイプ、ID 番号、職位など、個人の追加情報を入力します。
4. 個人を追加することを確認します。
   – 「追加」をクリックして個人を追加し、「個人の追加」ウィンドウを閉じます。
   – 「追加」および「新規」をクリックして人物を追加し、他の人物の追加を続行します。

7.4.11 輸出入者識別情報

複数の人物の情報や写真を一括してクライアントソフトウェアに読み込むことができます。また、個人情報や画像をエクスポートしてパソコンに保存することもできます。

7.4.12 輸入者情報

定義済みのテンプレート(CSV/Excelファイル)に複数の人物の情報を入力して、情報を一括してクライアントに取り込むことができます。

手順

1. Person モジュールを入力します。
2. リストで追加した組織を選択するか、左上隅の「追加」をクリックして組織を追加し、選択します。
3. 「読み込み(Import)」をクリックして読み込みパネルを開きます。
4. 読み込みモードとして個人情報を選択します。
5. 「個人をインポートするためのテンプレートのダウンロード」をクリックして、テンプレートをダウンロードします。
6. ダウンロードしたテンプレートに個人情報を入力します。

注意

- 複数のカードがある場合は、カード番号をセミコロンで区切ります。
- アスタリスクの付いた項目は必須です。
- デフォルトでは、雇用日付は現在の日付です。

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。

注意

- 相手先データベースに個人番号が存在する場合は、既存の情報を削除してから反映してください。
- 2000人以内の情報を取り込むことができます。

7.4.13 個人画像のインポート

追加した人物の顔画像をクライアントに取り込んだ後、追加した顔認識端末で画像内の人物を識別することができます。人物の画像を1枚ずつ読み込んだり、必要に応じて複数の画像を一度に読み込んだりできます。

はじめる前に

あらかじめ、個人情報をクライアントに取り込んでおいてください。

手順

1. Person モジュールを入力します。
2. リストで追加した組織を選択するか、左上隅の「追加」をクリックして組織を追加し、選択します。
3. 「読み込み」をクリックして「読み込み」パネルを開き、「顔」をオンにします。
4. オプション:クライアントで管理されている顔認識デバイスが写真の顔を認識できるかどうかを確認するには、「デバイスによる検証」を有効にします。
5. クリックしてフェイスピクチャーファイルを選択します。

注意

- 顔写真の(フォルダ)はZIP形式にしてください。
- 各ピクチャファイルは、JPG形式でなければならず、200KB以下でなければならない。
- 各ピクチャファイルには「個人ID_Name」という名前を付ける必要があります。個人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。
   インポートの進捗状況と結果が表示されます。

7.4.14 輸出者情報

追加した個人情報をCSV/Excelファイルとしてローカルにエクスポートできます。

はじめる前に

組織に個人を追加したことを確認します。

手順

1. Person モジュールを入力します。

2. オプション: リストから組織を選択します。

注意

組織を選択しない場合は、すべての個人の情報がエクスポートされます。

3. 「書き出し」をクリックして、書き出しパネルを開きます。
4. エクスポートするコンテンツとして個人情報をチェックします。
5. エクスポートしたい項目をチェックします。
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 のCSV/Excel ファイルに保存します。

7.4.15 輸出者映画

追加した人物の顔画像ファイルをエクスポートして、パソコンに保存できます。

はじめる前に

個人とその顔の写真を組織に追加していることを確認します。

手順

1. Person モジュールを入力します。
2. オプション: リストから組織を選択します。

注意

組織を選択しない場合は、すべての人の顔画像がエクスポートされます。

3. 「書き出し」をクリックして書き出しパネルを開き、書き出す内容として「顔」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。

注意

- エクスポートされたファイルはZIP形式です。
- 書き出される顔画像は「Person ID_Name_0」と命名されます(「0」は全面の顔です)。

7.4.16 アクセスコントロールデバイスからの個人情報の取得

追加されたアクセスコントロールデバイスに個人情報(個人情報、指紋、発行されたカード情報など)が設定されている場合は、デバイスから個人情報を取得し、クライアントにインポートして、詳細な操作を行うことができます。

手順

注意

- デバイスに保存されている個人名が空の場合は、クライアントにインポート後、発行されたカード番号で個人名が入力されます。
- デフォルトでは、個人の性別は「オス」になります。
- デバイスに保存されているカード番号または個人ID (従業員ID)がすでにクライアントデータベースに存在する場合、このカード番号または個人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. Person モジュールを入力します。
2. 個人をインポートする組織を選択します。
3. デバイスから取得をクリックします。
4. ドロップダウンリストから、追加したアクセスコントロールデバイスまたは登録ステーションを選択します。

注意

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て、デバイスのIPアドレス、ポート番号、ユーザー名、パスワードを設定します。

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

注意

最大2000人、5000枚のカードを取り込むことができます。

個人の詳細、個人の指紋情報(設定されている場合)、リンクされたカード(設定されている場合)などの個人情報が、選択した組織にインポートされます。

7.4.17 個人を別の組織に移動する

必要に応じて、追加した個人を別の組織に移動できます。

はじめる前に

- 少なくとも2 つの組織を追加していることを確認します。
- 個人情報をインポートしていることを確認します。

手順

1. Person モジュールを入力します。
2. 左側のパネルで組織を選択します。
   右側のパネルに、組織内の個人が表示されます。
3. 移動する人物を選択します。
4. 組織の変更をクリックします。
5. 移動先の組織を選択します。
6. OKをクリックします。

7.4.18 バッチでの個人へのカードの発行

クライアントは、複数のユーザーに一括でカードを発行する便利な方法を提供します。

手順

1. Person モジュールを入力します。
2. 「バッチ発行カード」をクリックします。
   追加されたカードが発行されていない人はすべて、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(名前または個人ID) を入力して、カードを発行する必要がある人物をフィルタリングします。
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。詳細はを参照してください。
5. カード登録ステーションまたはカードリーダーを初期化してカード発行の準備を整えるには、初期化をクリックします。
6. 「カード番号」欄をクリックし、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。
   リストの人物はカードと共に発行されます。

7.4.19 レポートカード損失

個人が自分のカードを紛失した場合は、カードの関連するアクセス許可が無効になるように、カードの紛失を報告することができます。

手順

1. Person モジュールを入力します。
2. カード紛失を報告する人物を選択し、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. 資格情報→カードパネルで、追加したカードを選択して、このカードを紛失したカードとして設定します。 
   カードの損失を報告した後、このカードのアクセス許可は無効になり、非アクティブになります。このカードを受け取った他人は、この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、をクリックして消失を取り消すことができます。 
   カードの紛失を取り消した後、個人のアクセス権限が有効でアクティブになります。
5. 消失したカードが1つのアクセスグループに追加され、そのアクセスグループがすでにデバイスに適用されている場合、カードの消失を報告するか、カードの消失をキャンセルした後、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、これらの変更をデバイスで有効にできます。

7.4.20 カード発行パラメータの設定

クライアントは、カードの番号を読み取るために、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の2 つのモードを提供します。カード登録ステーションが使用可能な場合は、USBインタフェースまたはCOMでクライアントを実行しているPCに接続し、カード登録にカードを置いてカード番号を読み取ります。そうでない場合は、追加したアクセスコントロール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別カード発行

カード登録ステーションをクライアントを実行しているPC に接続します。カードをカード登録ステーションに置いて、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。

注意

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

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。

カードの種類は、実際のカードの種類に合わせてEMカードまたはICカードを選択してください。

シリアルポート

機種がDS-K1F100-M の場合のみ有効です。

カード登録ステーションが接続するCOM を選択します。

ブザー

カード番号の読み取りに成功したときのブザー音を有効または無効にします。

カード番号タイプ

カード番号の種類は、実際のニーズに合わせて選択してください。

M1 カード暗号化

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

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、この機能を有効にして、暗号化するカードのセクターを選択する必要があります。

リモートモード:カードリーダーによるカード発行

クライアントに追加されたアクセスコントロールデバイスを選択し、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。

7.5 スケジュールとテンプレートの設定

休日と週のスケジュールを含むテンプレートを設定できます。テンプレートを設定した後、アクセスグループを設定するときに、設定したテンプレートをアクセスグループに適用して、テンプレートの期間内にアクセスグループが有効になるようにすることができます。

注意

アクセスグループの設定については、「アクセスグループを設定してアクセス許可を個人に割り当てる」を参照してください。

7.5.1 休日登録

休日を作成し、休日の日数(開始日、終了日、休日期間を含む)を1日で設定できます。

手順

注意

ソフトウェアシステムには、64 日までの休日を追加できます。

1. 「アクセスコントロール→予定→休日」を選択して、「休日」ページを表示します。
2. 左パネルの「追加」をクリックします。
3. 休日の名前を作成します。
4. (オプション) 「注釈」ボックスに、この休日の説明または一部の通知を入力します。
5. 休日リストに休日期間を追加し、休日期間を設定します。

注意

休日は最大16 期間まで追加できます。

1) 「休日リスト」フィールドの「追加」をクリックします。
2) カーソルをドラッグすると、時間が表示されます。つまり、設定したアクセスグループが有効になります。

注意

1つの休日期間には、最大8つの期間を設定できます。

3) (オプション) 時間間隔を編集するには、次の操作を実行します。
- カーソルを時間の継続時間に移動し、カーソルがに変わったらタイムラインバーの時間の継続時間を希望の位置にドラッグします。
- 時間の長さをクリックし、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。
- 時間の開始位置または終了位置にカーソルを移動し、カーソルがに変わったときに時間を長くしたり短くしたりするには、カーソルをドラッグします。

4) オプション: 削除する必要がある継続時間を選択し、操作列をクリックして、選択した継続時間を削除します。

5) 必要に応じて、「操作(Operation)」コラムをクリックして、タイムバーのすべての時間継続時間をクリアします。

6) (オプション)この追加された休日期間を休日リストから削除するには、「操作」列をクリックします。

6. 保存をクリックします。

7.5.2 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ます。週スケジュールを設定して、別の人またはグループにアクセス許可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した休日を選択することもできます。

手順

注意

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」を選択して、「テンプレート」ページに入ります。

注意

デフォルトのテンプレートには、オールデイオーソライズドとオールデイディデニードの2つがあり、編集や削除はできません。

全日与信

アクセス許可は、曜日ごとに有効であり、休日はありません。

終日拒否

アクセス権限は、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(Add)」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. 注釈ボックスに、このテンプレートの説明または通知を入力します。
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「週のスケジュール」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時間を表示します。

注意

週スケジュールでは、1 日につき最大8 つの時間を設定できます。

3) (オプション) 時間間隔を編集するには、次の操作を実行します。
- カーソルを時間の継続時間に移動し、カーソルがに変わったらタイムラインバーの時間の継続時間を希望の位置にドラッグします。
- 時間の長さをクリックし、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。
- 時間の開始位置または終了位置にカーソルを移動し、カーソルがに変わったときに時間を長くしたり短くしたりするには、カーソルをドラッグします。

4) 上記の2 つの手順を繰り返して、他の曜日にさらに時間を表示します。

6. 休日を追加してテンプレートに適用します。

注意

1つのテンプレートには、休日を4つまで登録できます。

1) 休日タブをクリックします。
2) 左側のリストで休日を選択すると、右側のパネルで選択した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。

注意

休日の追加について詳しくは、「休日の追加」を参照してください。

4) 必要に応じて、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、または「クリア」をクリックして右側のリストで選択した休日をすべてクリアします。

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。

7.6 アクセス許可を個人に割り当てるアクセスグループの設定

個人を追加して個人の資格情報を設定したら、アクセスグループを作成して、どの個人がどのドアにアクセスできるかを定義し、そのアクセスグループをアクセスコントロールデバイスに適用して有効にすることができます。

手順

アクセスグループの設定を変更した場合は、再度デバイスにアクセスグループを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、テンプレートの変更、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、関連する個人の詳細(カード番号、指紋、顔写真、カード番号と指紋の連動、カード番号と指紋の連動、パスワードカード、カードの有効期限など)が含まれます。

1. 「アクセス制御→許可→アクセスグループ」を選択して、アクセスグループインターフェースに入ります。
2. 追加をクリックして、追加ウィンドウを開きます。
3. 「名前」テキストフィールドで、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。

注意

アクセスグループの設定を行う前に、テンプレートを設定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. Select Person(個人の選択)フィールドの左側のリストで、アクセス権限を割り当てる個人を選択します。
6. 「アクセスポイントの選択」フィールドの左側のリストで、選択した人がアクセスできるドア、ドアステーション、またはフロアを選択します。
7. 保存をクリックします。
   選択した人物と選択したアクセスポイントをインターフェースの右側に表示できます。

図7-9 選択したユーザとアクセスポイントの表示

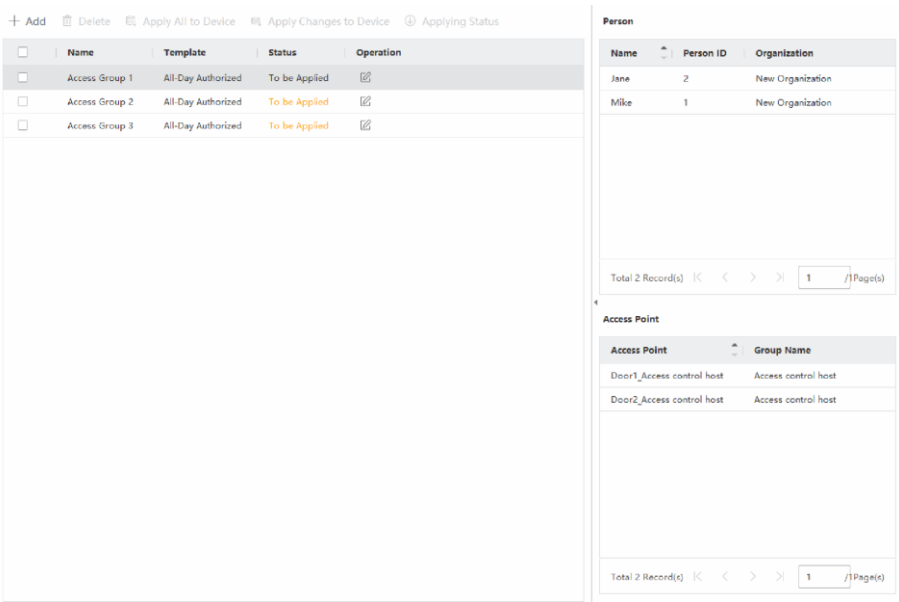


図7-10 選択したユーザとアクセスポイントの表示

8. アクセスグループを追加したら、それらをアクセスコントロールデバイスに適用して有効にする必要があります。
   1) アクセスコントロール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」をクリックすると、選択したすべてのアクセスグループがアクセスコントロールデバイスまたはドアステーションに適用されます。
   3) Apply All to Devices または Apply Changes to Devices 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部分のみがデバイスに適用されます。

4) 「状況」列に適用状況を表示するか、「状況の適用」を選択して、適用されているすべてのアクセスグループを表示します。

注意

Display Failure Only をオンにすると、適用結果をフィルタリングできます。

適用されたアクセスグループ内の選択された個人には、リンクされたカードまたは指紋を使用して、選択されたドア/ドアステーションに出入りする権限が付与されます。

9. 必要に応じて、をクリックしてアクセスグループを編集します。

注意

個人のアクセス情報またはその他の関連情報を変更すると、クライアントの右隅に「適用するアクセスグループ」というプロンプトが表示されます。
プロンプトをクリックして、変更されたデータをデバイスに適用できます。今すぐ適用または後で適用を選択できます。

7.7 詳細機能の設定

アクセスコントロールの高度な機能を設定して、さまざまなシーンの特殊な要件を満たすことができます。

注意

- カードに関する機能(アクセスコントロールカードの種類)については、カードの追加時にアクセスグループが適用されたカードのみが一覧表示されます。
- デバイスで高度な機能がサポートされている必要があります。
- Advanced Function(詳細機能)にカーソルを合わせ、クリックして表示する詳細機能をカスタマイズします。

7.7.1 デバイスパラメータの設定

アクセスコントロールデバイスを追加したら、アクセスコントロールデバイス、アクセスコントロール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

アクセスコントロールデバイスを追加した後、画像上のユーザー情報のオーバーレイ、キャプチャー後の写真のアップロード、キャプチャーされた写真の保存など、そのパラメータを設定できます。

手順

1. 「入退室管理→詳細機能→機器パラメータ」を選択します。

注意

Advanced FunctionリストにDevice Parameterがある場合は、Advanced Functionにカーソルを合わせ、クリックして表示するDevice Parameterを選択します。

2. アクセスデバイスを選択すると、そのパラメータが右ページに表示されます。
3. スイッチをオンにすると、対応する機能が有効になります。

注意

- 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。
- 次のパラメータの一部は、基本情報ページにリストされていません。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。デバイスで操作しているときに、音声プロンプトが聞こえます。

画像のアップロードリンク取り込み後

カメラ連動で撮影した画像を自動的にシステムにアップロードします。

画像保存リンク取り込み後

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

顔認識モード

通常モード

カメラで顔を正常に認識します。

深部モード

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

NFC カードの有効化

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

M1 カードの有効化

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

EM カードの有効化

機能を有効にすると、デバイスはEM カードを認識できます。デバイスにEM カードを提示することができます。

CPUカード有効

予約済み。この機能を有効にすると、デバイスはCPU カードを認識できます。デバイスにCPU カードを提示することができます。

IDカード有効

予約済み。この機能を有効にすると、デバイスはID カードを認識できます。デバイスにID カードを提示することができます。

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、ページのパラメータを選択したデバイスにコピーするアクセスコントロールデバイスを選択します。

ドアのパラメータの設定

アクセスコントロールデバイスを追加したら、アクセスポイント(ドア)パラメータを設定できます。

手順

1. 「入退室管理→詳細機能→機器パラメータ」を選択します。
2. 左パネルでアクセスコントロールデバイスを選択し、をクリックして、選択したデバイスのドアまたはフロアを表示します。
3. ドアまたはフロアを選択すると、そのパラメータが右ページに表示されます。
4. ドアまたはフロアのパラメータを編集します。

注意

- 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。
- 次のパラメータの一部は、基本情報ページにリストされていません。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名を編集します。

ドア接点

ドアセンサーは、閉じたまま、または開いたままにしておくように設定できます。通常、閉じたままになります。

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しておくように設定できます。通常、それは開いたままである。

ドアロック時間

通常のカードとリレー動作をスワイプすると、ドアをロックするタイマーが作動します。

長時間オープン

拡張アクセスを持つ人がカードをスワイプする必要がある場合、ドアコンタクトを適切な遅延で有効にすることができます。

ドア左開タイムアウトアラーム

設定した時間内にドアが閉まっていない場合は、アラームをトリガーすることができます。0に設定すると、アラームはトリガーされません。

デュース・コード

強迫感がある場合には、強迫コードを入力することにより、ドアを開けることができる。同時に、クライアントは耐久イベントを報告できます。

スーパーパスワード

スーパーパスワードを入力することで、特定の人がドアを開けることができます。

注意

- 強さコードとスーパーパスワードは異なる必要があります。
- 強制コードおよびスーパーパスワードは、認証パスワードとは異なる必要があります。
- デュレスコードとスーパーパスワードの長さは、デバイスに応じて決まります。通常は4 ～8桁です。

5. OKをクリックします。
6. 必要に応じて、「コピー先」をクリックし、ページのパラメータを選択したドアにコピーするドアを選択します。

注意

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

カードリーダーのパラメータの設定

アクセスコントロールデバイスを追加したら、カードリーダーのパラメータを設定できます。

手順

1. 「入退室管理→詳細機能→機器パラメータ」を選択します。
2. 左側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、右側のカードリーダーのパラメーターを編集できます。
3. Basic Information ページでカードリーダーの基本パラメータを編集します。

注意

- 表示されるパラメータは、アクセスコントロールデバイスによって異なる場合があります。パラメータには、次のような部分があります。詳しくは機器の取扱説明書をご覧ください。
- 次のパラメータの一部は、Basic Information(基本情報)ページに表示されません。パラメータを編集するには、Advanced(詳細設定)をクリックします。

基本情報

名前

必要に応じてカードリーダー名を編集します。

カードの最小スワイプ間隔

同じカードのカードスワイプ間隔が設定値以下の場合、カードスワイプは無効になります。0 ～255 の範囲で設定できます。

最大値のアラーム失敗した試行

カード読み取りが設定値に達したときにアラームを報告することができます。

カードリーダータイプ/カードリーダーの説明

カードリーダーのタイプと説明を取得します。それらは読み取り専用です。

詳細設定

カードリーダーの有効化

機能を有効にすると、e デバイスをカードリーダーとして使用できます。

OK LED極性/エラーLED極性/ブザー極性

カードリーダーのパラメータに応じて、メインボードのOK LED 極性/エラーLED 極性/

ブザーLED 極性を設定します。通常は初期設定を採用しています。

最大PWD 入力時のインターバル

カードリーダーでパスワードを入力する際、2桁押しの間隔が設定値を超えると、前に押した数字が自動的にクリアされます。

改ざん検知

カードリーダーの不正防止検出を有効にします。

すべてのコントローラと通信アクセスコントロールデバイスが設定時間以上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。

顔1:N 一致しきい値

1:N 一致モードで認証する場合、一致しきい値を設定します。値が大きいほど、誤許可率は小さくなり、認証時の誤拒否率は大きくなります。

顔認識間隔

認証時の2つの連続した顔の認識間の時間間隔。デフォルトは2s です。

顔のなりすまし防止

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、本人であるかどうかをデバイスが認識できます。

顔1:1一致しきい値

1:1 一致モードで認証する場合、一致しきい値を設定します。値が大きいほど、誤許可率は小さくなり、認証時の誤拒否率は大きくなります。

アプリケーションモード

実際の環境に応じて、屋内などのアプリケーションモードを選択できます。

Lock Authentication Failed Face

Live Face Detection機能を有効にした後、ライブ顔検出が設定した回数を超えて失敗した場合、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分以内に偽の顔を介して認証することはできません。5分以内に、ユーザーは実際の顔を介して連続的に2回認証し、ロックを解除できます。

ライブネス検出のセキュリティレベル

顔検出機能を有効にしたあと、顔認証を行うときに、一致するセキュリティレベルを設定できます。

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、ページのパラメータを選択したカードリーダーにコピーするカードリーダーを選択します。

アラーム出力のパラメータの設定

アクセスコントロール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。

手順

1. 「アクセス制御→詳細機能→機器パラメータ」を選択して、アクセス制御パラメータ設定画面に入ります。
2. 左側のデバイスリストで、をクリックしてドアを展開し、アラーム入力を選択して、右側のアラーム入力のパラメータを編集できます。
3. アラーム出力の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名を編集します。

   アラーム出力有効時間

   トリガー後のアラーム出力の継続時間。
4. OKをクリックします。
5. オプション: アラーム出力をトリガーするには、右上隅のスイッチをON に設定します。

7.7.2 残りのオープン/クローズの設定

ドアのステータスをオープンまたはクローズに設定できます。たとえば、休日にドアを閉じたままにしておき、そのドアが開いたままの状態を指定した平日の期間に設定することができます。

はじめる前に

アクセスコントロールデバイスをシステムに追加します。

手順

1. 「アクセスコントロール→詳細機能」→の「開く/閉じる」を選択して、「開く/閉じる」画面を表示します。
2. 左側のパネルで構成する必要があるドアを選択します。
3. 平日にドアステータスを設定するには、平日スケジュールをクリックして、次の操作を実行します。
   1) Remain Open または Remain Closed をクリックします。
   2) カーソルをドラッグすると、時間が表示されます。つまり、設定したアクセスグループが有効になります。

   注意

   週スケジュールでは、各曜日に最大8つの期間を設定できます。

   3) (オプション) 時間間隔を編集するには、次の操作を実行します。
   - カーソルを時間の継続時間に移動し、カーソルがに変わったらタイムラインバーの時間の

継続時間を希望の位置にドラッグします。
- 時間の長さをクリックし、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。
- 時間の開始位置または終了位置にカーソルを移動し、カーソルがに変わったときに時間を長くしたり短くしたりするには、カーソルをドラッグします。

4) 保存をクリックします。

関連操作

週全体にコピー	時間バーで継続時間を1つ選択し、「週全体にコピー」をクリックして、この時間バーのすべての継続時間設定を他の週の日にコピーします。
選択削除	タイムバーでデュレーションを1 つ選択し、Delete Selected をクリックしてこのデュレーションを削除します。
クリア	「消去」をクリックすると、週のスケジュールのすべての継続時間設定が消去されます。

4. 休日のドアステータスを設定するには、休日をクリックし、次の操作を実行します。
   1) Remain Open または Remain Closed をクリックします。
   2) 追加をクリックします。
   3) 開始日と終了日を入力します。
   4) カーソルをドラッグすると、時間が表示されます。つまり、設定したアクセスグループが有効になります。

注意

1つの休日期間には、最大8つの期間を設定できます。

   5) 時間を編集するには、以下の操作を行います。
   - カーソルを時間の継続時間に移動し、カーソルがに変わったらタイムラインバーの時間の継続時間を希望の位置にドラッグします。
   - 時間の長さをクリックし、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。
   - 時間の開始位置または終了位置にカーソルを移動し、カーソルがに変わったときに時間を長くしたり短くしたりするには、カーソルをドラッグします。

   6) オプション: 削除する必要がある継続時間を選択し、操作列をクリックして、選択した継続時間を削除します。
   7) 必要に応じて、「操作(Operation)」コラムをクリックして、タイムバーのすべての時間継続時間をクリアします。
   8) (オプション)この追加された休日期間を休日リストから削除するには、「操作」列をクリックします。
   9) 保存をクリックします。
5. オプション:コピーをクリックして、このドアのドアステータス設定を他のドアにコピーします。

7.7.3 多要素認証の設定

1台のアクセスコントロールポイント(ドア)で、グループごとに管理したり、複数人の認証を設定したりできます。

はじめる前に

アクセスグループを設定し、アクセスコントロールデバイスにアクセスグループを適用します。詳細については、「アクセス許可を個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。

1つのアクセスコントロールポイント(ドア)の複数のカードの認証を設定する場合は、このタスクを実行します。

手順

1. 「アクセスコントロール→詳細機能→多要素認証」を選択します。
2. 左パネルのデバイスリストでアクセスコントロールデバイスを選択します。
3. アクセスコントロールデバイスに個人/カードグループを追加します。
   1) 右側のパネルで「追加」をクリックします。
   2) 必要に応じてグループの名前を作成します。
   3) 個人/カードグループの有効期間の開始時刻と終了時刻を指定します。
   4) 「選択可能」リストでメンバーとカードを選択すると、選択したメンバーとカードが「選択済み」リストに追加されます。

   注意

   個人にカードを発行していることを確認します。
   アクセスグループが設定され、アクセスコントロールデバイスにアクセスグループが正常に適用されていることを確認します。

   5) 保存をクリックします。
   6) 必要に応じて、個人/カードグループを選択し、「削除」をクリックして削除します。
   7) (オプション)個人/カードグループを選択し、適用をクリックして、以前にアクセスコントロールデバイスに適用されなかったアクセスグループを再適用します。
4. 左パネルで選択したデバイスのアクセスコントロールポイント(ドア)を選択します。
5. パスワードを入力する際の最大間隔を入力します。
6. 選択したアクセスコントロールポイントの認証グループを追加します。
   1) 「認証グループ」パネルで「追加」をクリックします。
   2) ドロップダウンリストから、設定済みのテンプレートを認証テンプレートとして選択します。

   注意

   テンプレートの設定については、「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。

3）「ローカル認証」、「ローカル認証とリモートオープンドア」、または「ローカル認証とスーパーパスワード」の認証タイプをドロップダウンリストから選択します。

ローカル認証

アクセス制御装置による認証。

ローカル認証とリモートオープンドア

アクセス制御デバイスおよびクライアントによる認証。ユーザーがカードをデバイス上でスワイプすると、ウィンドウがポップアップ表示されます。クライアント経由でドアのロックを解除できます。

図7-11 扉を遠隔操作で開ける

注意

「オフライン認証」をオンにすると、アクセス制御デバイスがクライアントと切断されたときにスーパーパスワード認証を有効にできます。

ローカル認証とスーパーパスワード

アクセス制御装置およびスーパーパスワードによる認証。

4）下の左側のリストで追加した人/カードグループを選択すると、右側の「選択済み」リストに認証グループとして追加されます。

5）右側のリストで追加した認証グループをクリックして、「認証時間」列に認証時間を設定します。

注意

- 認証時間は0 より大きく、人事グループに追加された人員数よりも小さくする必要があります。
- 認証時間の最大値は16 です。

6）保存をクリックします。

注意

- アクセスコントロールポイント(ドア)ごとに、最大4 つの認証グループを追加できます。
- 認証種別が「ローカル認証」の認証グループは、認証グループに最大8人まで登録できます。
- 認証種別が「ローカル認証」、「スーパーパスワード」、「ローカル認証」、「リモートオープンドア」の認証グループは、認証グループに最大7 人/カードグループまで追加できます。

7. 保存をクリックします。

7.7.4 カードリーダー認証モードとスケジュールの設定

実際のニーズに応じて、アクセスコントロールデバイスのカードリーダーの通過ルールを設定できます。

手順

1. 「アクセス制御→詳細機能→認証」を選択して、認証モードコンフィギュレーションページを開きます。
2. 左側のカードリーダーを選択して設定します。
3. カードリーダー認証モードを設定します。
   1) 設定をクリックします。

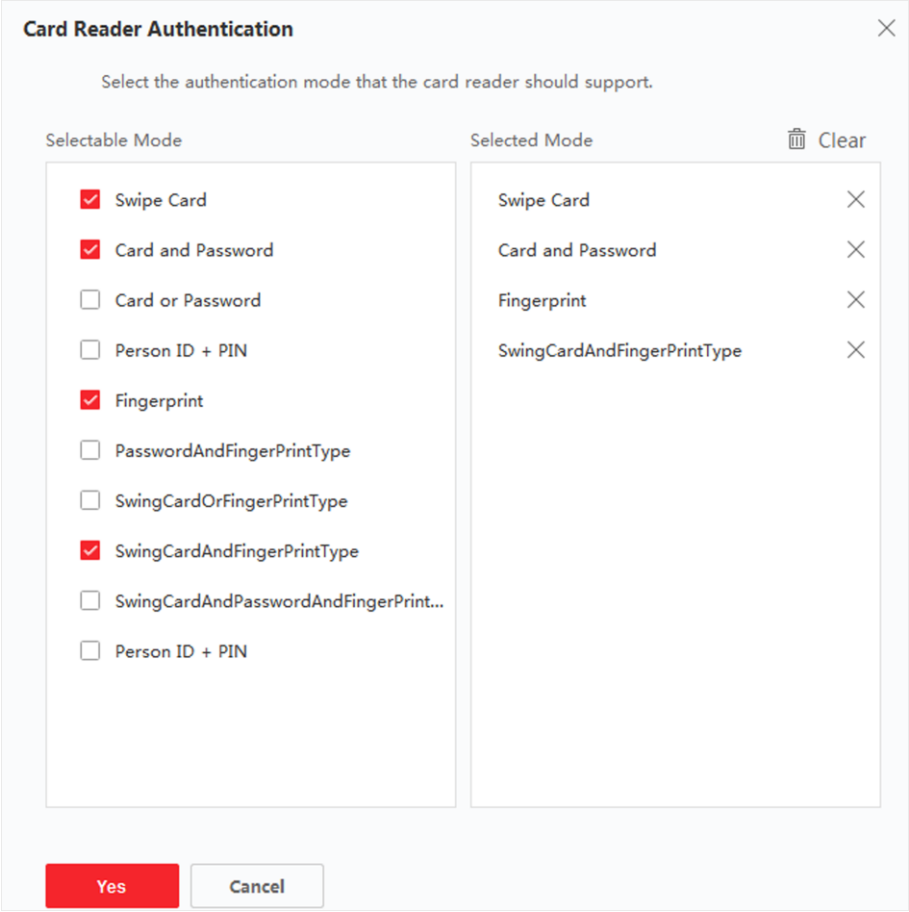


図7-12 カードリーダー認証モードの選択

注意

PIN とは、ドアを開けるために設定されたPIN コードのことです。「アクセス制御情報の設定」を参照してください。

2) 「使用可能なモード(Available Mode)」リストでモードをチェックすると、選択したモードリストに追加されます。

3) OKをクリックします。
モードを選択すると、選択したモードが異なる色のアイコンとして表示されます。

4. アイコンをクリックしてカードリーダー認証モードを選択し、カーソルをドラッグしてスケジュールにカラーバーを描きます。これは、カードリーダー認証が有効であることを意味します。
5. 上記の手順を繰り返して、他の時間帯を設定します。

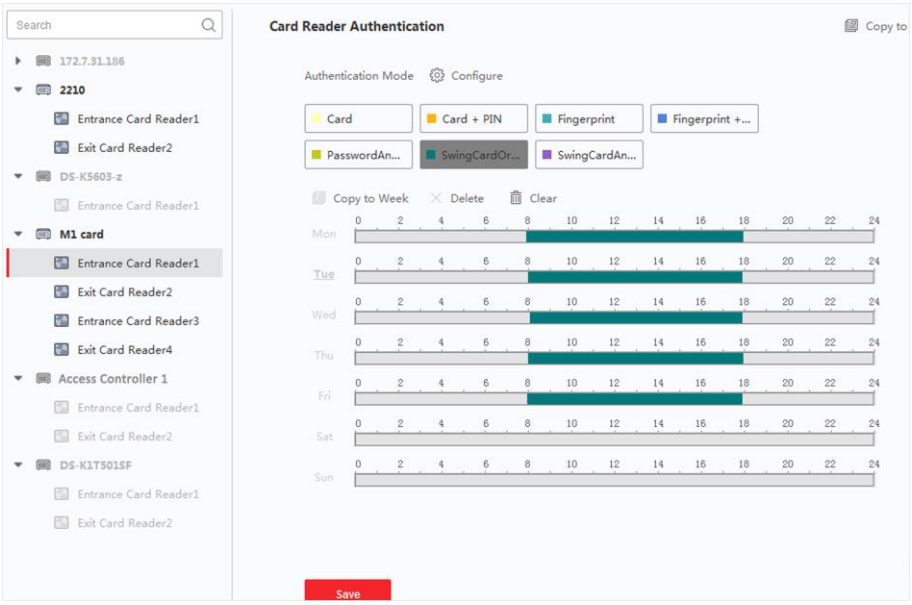


図7-13 カードリーダーの認証モードの設定

6. 必要に応じて、設定した曜日を選択し、「週にコピー」をクリックして、同じ設定を週全体にコピーします。
7. オプション:コピーをクリックして、設定を他のカードリーダーにコピーします。
8. 保存をクリックします。

7.7.5 ファーストパーソンの設定1つのアクセスコントロールポイントに複数のファーストパーソンを設定できます。最初の人が承認されると、複数の人が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。

はじめる前に

アクセスグループを設定し、アクセスコントロールデバイスにアクセスグループを適用します。詳細については、「アクセス許可を個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。

このタスクは、第一者とのドアの開閉を設定する場合に実行します。

手順

1. アクセスコントロール→の詳細機能→の「最初のユーザー入力」を選択して、「最初のユーザー入力」ページに入ります。

2. 左パネルのリストでアクセスコントロールデバイスを選択します。
3. 選択したデバイスの各アクセスコントロールポイントのドロップダウンリストから、現在のモードを「最初のユーザの後に残りのオープンを有効にする」または「最初のユーザの後に残りのオープンを無効にする」として選択します。

最初の個人の後に残りのオープンを有効にする

開いたままの期間が終了するまで、最初の人物が承認された後、ドアは設定された期間だけ開いたままになります。このモードを選択した場合は、オープン状態の継続時間を設定する必要があります。

注意

開いたままの時間は0 ～1440 分にする必要があります。デフォルトでは、オープン状態の継続時間は10 分です。

最初の人の後の残りのオープンを無効にする

ファーストパーソンの機能、つまり通常の認証を無効にします。

注意

ファーストパーソンモードを無効にするには、ファーストパーソンで再度認証を行うことができます。

4. First Person List パネルでAdd をクリックします。
5. 左側のリストで人物を選択すると、その人物がドアの最初の人物として選択した人物に追加されます。
   追加された第一人者が第一人者リストに記載する。
6. 必要に応じて、リストから最初の人を選択し、「削除」をクリックして、その人を最初の人リストから削除します。
7. 保存をクリックします。

7.7.6 アンチパスバックの設定

指定されたパスに従ってアクセスコントロールポイントのみを通過させるように設定でき、カードをスワイプした後にアクセスコントロールポイントを通過させることができるのは1 人だけです。

はじめる前に

アクセスコントロールデバイスのアンチパッシングバック機能を有効にします。

アクセスコントロールデバイスにアンチパッシングバックを設定する場合は、次の作業を実行します。

手順

注意

また、アクセス制御装置には、戻り防止機能またはマルチドアインタロック機能を同時に設定することができます。マルチドアインターロッキングの構成については、を参照してください。

1. 「アクセスコントロール→詳細機能→アンチパスバック」を選択して、「アンチパスパック設定」画面を表示します。
2. 左パネルでアクセスコントロールデバイスを選択します。
3. 「最初のカードリーダー」フィールドで、パスの先頭にカードリーダーを選択します。
4. Card Reader Afterward 列で選択した最初のカードリーダーをクリックして、Select Card Reader ダイアログを開きます。
5. 1 台目のカードリーダーの後ろ側のカードリーダーを選択します。

注意

1 つのカードリーダーの後続カードリーダーとして、最大4 つの後続カードリーダーを追加できます。

6. ダイアログで「OK」をクリックして、選択内容を保存します。
7. 「アンチパスバック設定」ページの「保存」を選択して設定を保存し、有効にします。

例

カードのスワイピングパスを設定する先頭にReader In_01 を選択し、リンクされたカードリーダーとしてReader In_02、Reader Out_04 を選択します。その後、カードをReader In_01、Reader In_02、Reader Out_04 の順序でスワイプすることによってのみ、アクセスコントロールポイントを通過させることができます。

7.7.7 デバイスパラメータの設定

アクセスコントロールデバイスを追加したら、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。

複数の NIC パラメータの設定

機器が複数のネットワークインターフェースをサポートしている場合、IPアドレス、MACアドレス、ポート番号など、これらのNICのネットワークパラメータをクライアント経由で設定できます。

手順

注意

この機能はデバイスでサポートされている必要があります。

1. アクセス制御モジュールに入ります。
2. 左側のナビゲーションバーで、「Advanced Function → More Parameters」と入力します。
3. デバイスリストでアクセスコントロールデバイスを選択し、NIC をクリックして複数のNIC 設定ページに入ります。
4. ドロップダウンリストから設定するNIC を選択します。
5. IPアドレス、デフォルトゲートウェイ、サブネットマスクなどのネットワークパラメータを設定します。

MAC住所

メディアアクセス制御アドレス(MAC アドレス)は、物理ネットワークセグメント上の通信用にネットワークインタフェースに割り当てられる一意の識別子です。

MTU

ネットワークインターフェイスの最大転送単位(MTU)。

6. 保存をクリックします。

ネットワークパラメータの設定

アクセスコントロールデバイスを追加した後、デバイスログのアップロードモードを設定したり、有線ネットワーク経由でISUP アカウントを作成したりできます。

ログアップロードモードの設定

ISUP プロトコルを使用してログをアップロードするデバイスのモードを設定できます。

手順

1. アクセス制御モジュールに入ります。
2. 左側のナビゲーションバーで、「Advanced Function → More Parameters」と入力します。
3. デバイス一覧でアクセスコントロールデバイスを選択し、ネットワーク→アップロードモードに入ります。
4. 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。
5. アップロードモードを設定するには、有効をオンにするをオンにします。
6. ドロップダウンリストからアップロードモードを選択します。
   – メインチャネルとバックアップチャネルに対してN1 またはG1 を有効にします。

「閉じる」を選択して、メインチャネルまたはバックアップチャネルを無効にします。

注意

メインチャネルとバックアップチャネルは、同時にN1 またはG1 を有効にすることはできません。

7. 保存をクリックします。

有線通信モードでISUP アカウントを作成する

有線通信モードでISUPプロトコルのアカウントを設定できます。その後、ISUP プロトコルを使用し

てデバイスを追加できます。

手順

注意

この機能はデバイスでサポートされている必要があります。

1. アクセス制御モジュールに入ります。
2. 左側のナビゲーションバーで、「Advanced Function → More Parameters」と入力します。
3. デバイス一覧でアクセスコントロールデバイスを選択し、ネットワーク→ネットワークセンターに入ります。
4. 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。
5. 「アドレスタイプ」で「IP アドレス」または「ドメイン名」を選択します。
6. アドレスタイプに応じてIP アドレスまたはドメイン名を入力します。
7. プロトコルのポート番号を入力します。

注意

ワイヤレスネットワークおよび有線ネットワークのポート番号は、ISUP のポート番号と一致している必要があります。

8. 「ISUP」として「プロトコルタイプ」を選択します。
9. ネットワークセンターのアカウント名を設定します。
10. 保存をクリックします。

デバイスキャプチャパラメータの設定

手動キャプチャやイベントトリガによるキャプチャなど、アクセスコントロールデバイスのキャプチャパラメータを設定できます。

注意

- キャプチャ機能はデバイスでサポートされている必要があります。
- キャプチャパラメータを設定する前に、最初に画像ストレージを設定して、イベントトリガされた画像を保存する場所を定義する必要があります。詳しくは、クライアントソフトウェアの取扱説明書「ピクチャー保存先を設定する」をご覧ください。.

トリガ・キャプチャ・パラメータの設定

イベントが発生すると、アクセス・コントロール・デバイスのカメラをトリガして、イベントが発生したときの動作を記録する画像をキャプチャすることができる。イベントセンターでイベントの詳細を確認するときに、撮影した画像を見ることができます。その前に、一度に撮影する枚数など、撮影するためのパラメータを設定する必要があります。

はじめる前に

キャプチャパラメータを設定する前に、最初に画像ストレージを設定して、キャプチャされた画像を保存する場所を定義する必要があります。詳しくは、クライアントソフトウェアの取扱説明書「ピクチャー保存先を設定する」をご覧ください。

手順

注意

この機能は、デバイスでサポートされている必要があります。

1. アクセス制御モジュールに入ります。
2. 左側のナビゲーションバーで、Advanced Function → More Parameters → Capture と入力します。
3. デバイスリストでアクセスコントロールデバイスを選択し、「リンクキャプチャ」を選択します。
4. 画像サイズと画質を設定します。
5. 1 回に何枚の画像を取り込むかを定義する、トリガーされた1 回の取り込み時間を設定します。
6. キャプチャ時間が1 を超える場合は、各キャプチャの間隔を設定します。
7. 保存をクリックします。

手動取り込みパラメータの設定

ステータスモニタリングモジュールでは、ボタンをクリックすることで、アクセスコントロールデバイスのカメラの画像を手動でキャプチャできます。その前に、画質などのキャプチャのパラメータを設定する必要があります。

はじめる前に

キャプチャパラメータを設定する前に、最初に保存パスを設定して、キャプチャされた画像を保存する場所を定義する必要があります。詳しくは、クライアントソフトウェアの取扱説明書「ピクチャー保存先を設定する」をご覧ください。

手順

注意

この機能は、デバイスでサポートされている必要があります。

1. アクセス制御モジュールに入ります。
2. 左側のナビゲーションバーで、Advanced Function → More Parameters → Capture と入力します。
3. デバイスリストでアクセスコントロールデバイスを選択し、手動キャプチャを選択します。
4. ドロップダウンリストから、キャプチャした画像の解像度を選択します。
5. 高、中、低のいずれかの画質を選択します。画質が高いほど、画像サイズは大きくなります。
6. 保存をクリックします。

顔認識端子のパラメータを設定する

顔認識端末では、顔画像データベースなどの各種パラメータを設定できます。

手順

注意

この機能はデバイスでサポートされている必要があります。

1. アクセス制御モジュールに入ります。
2. 左側のナビゲーションバーで、「Advanced Function → More Parameters」と入力します。
3. デバイスリストでアクセスコントロールデバイスを選択し、顔認識ターミナルをクリックします。
4. パラメータを設定します。

注意

表示されるパラメータは、機器の機種によって異なります。

アルゴリズム

顔写真データベースとしてDeep Learningを選択します。

顔画像を認証して保存

有効にすると、認証時にキャプチャされた顔画像がデバイスに保存されます。

エコモード

ECO モードを有効にした後、デバイスは低明るい環境または暗い環境で顔を認証できます。また、ECO モードしきい値、ECO モード(1:N)、ECO モード(1:1)を設定できます。

エコモード(1:1)

ECO モード1:1 一致モードで認証する場合、一致しきい値を設定します。値が大きいほど、誤許可率は小さくなり、誤拒否率は大きくなります。

エコモード(1:N)

ECO モード1:N 一致モードで認証する場合、一致しきい値を設定します。値が大きいほど、

誤許可率は小さくなり、誤拒否率は大きくなります。

エコモードしきい値

ECO モードを有効にすると、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。指定可能な範囲:0 ～8。

ワークモード

デバイスのワークモードをアクセス制御モードに設定します。アクセス制御モードは、デバイスノーマルモードです。アクセスするために認証情報を認証する必要があります。

5. 保存をクリックします。

M1 カード暗号化の有効化

M1 カード暗号化は、認証のセキュリティレベルを向上させることができます。

手順

注意

この機能は、アクセスコントロール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. 左側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コントロールデバイスを選択し、「M1 Card Encryption」をクリックして「M1 Card Encryption」ページに入ります。
4. スイッチをオンに設定して、M1 カード暗号化機能を有効にします。
5. セクタID を設定します。

注意

- セクタID の範囲は1 ～100 です。
- デフォルトでは、セクタ13 は暗号化されます。セクタ13 を暗号化することを推奨します。

6. 保存をクリックして設定を保存します。

RS-485 パラメータの設定

アクセスコントロールデバイスの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、パリティの種類、フロー制御の種類、通信モード、ワークモード、接続モードがあります。

手順

注意

RS-485 設定が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. 左側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コントロールデバイスを選択し、RS-485 をクリックしてRS-485 Settings 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. ドロップダウンリストで、ボーレート、データビット、ストップビット、パリティの種類、通信モード、動作モード、接続モードを設定します。

注意

接続モードがConnect Access Control Device の場合、出力タイプとしてカード番号または個人ID を選択できます。

6. 保存をクリックします。
   - 設定されたパラメータがデバイスに自動的に適用されます。
   - 動作モードまたは接続モードを変更すると、デバイスは自動的に再起動します。

Wiegand パラメータの設定

アクセスコントロールデバイスのWiegand チャンネルと通信モードを設定できます。Wiegand パラメータを設定すると、デバイスはWiegand 通信を介してWiegand カードリーダーに接続できます。

手順

注意

この機能はデバイスでサポートされている必要があります。

1. アクセス制御モジュールに入ります。
2. 左側のナビゲーションバーで、「Advanced Function → More Parameters」と入力します。
3. デバイスリストでアクセスコントロールデバイスを選択し、Wiegand をクリックしてWiegand Settings 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Wiegand 機能を有効にします。
5. ドロップダウンリストからWiegandのチャンネル番号と通信モードを選択します。

注意

「通信方向」を「送信」に設定した場合は、Wiegand モードを「Wiegand 26」または「Wiegand 34」に設定する必要があります。

6. Wiegand 機能を有効にするには、Wiegand を有効にするをオンにします。
7. 保存をクリックします。
   - 設定されたパラメータがデバイスに自動的に適用されます。
   - 通信方向を変更すると、デバイスは自動的に再起動します。

7.8 アクセス制御のためのリンクアクションの設定

アクセス制御装置が検出したイベントに対して、異なる連携動作を設定できます。その後、イベントが発生すると、連携動作がトリガされます。このメカニズムは、セキュリティ担当者にイベントを通知したり、リアルタイムで自動アクセス制御をトリガするために使用されます。

2 種類の連携動作がサポートされています:

- **クライアントアクション:イベントが検出されると、クライアントが警告音を鳴らすなど、クライアントのアクションがトリガーされます。**
- **デバイスアクション:イベントが検出されると、カードリーダーのブザー、ドアの開閉など、特定のデバイスのアクションがトリガされます。**

7.8.1 アクセス・イベントのクライアント・アクションの構成

アクセスポイントから離れていても、クライアントでアクセスイベントのリンクアクションを設定することで、イベントの発生状況と緊急度を把握できます。イベントがトリガーされるとクライアントで通知されるため、イベントに即座に応答できます。アクセスポイントのクライアントアクションを一度にまとめて設定することもできます。

手順

注意

ここでの連携動作とは、クライアントソフトウェア自身の動作(警告音、メール連動など)を連動させる動作のことです。

1. 「イベント管理→アクセスコントロールイベント」を選択します。
   追加したアクセスコントロールデバイスがデバイスリストに表示されます。
2. デバイスリストからリソース(デバイス、アラーム入力、ドア/エレベーター、カードリーダーを含む)を選択します。
   選択したリソースがサポートするイベントタイプが表示されます。
3. イベントを選択し、優先度の編集をクリックして、イベントの優先度を定義します。これは、イベントセンターでイベントをフィルタリングするために使用できます。
4. イベントの連動動作を設定します。
   1) イベントを選択し、リンクの編集をクリックして、イベントがトリガーされたときのクライアントアクションを設定します。

      音声警告

      アラームがトリガーされると、クライアントソフトウェアは警告音を出します。警告音を鳴らすアラーム音を選択できます。

注意

アラーム音の設定については、クライアントソフトウェアの取扱説明書の「アラーム音を設定する」を参照してください。

電子メールの送信

アラーム情報の電子メール通知を1 つ以上の受信者に送信します。
メールパラメータの設定については、クライアントソフトウェアの取扱説明書の「メールパラメータの設定」を参照してください。

2) OKをクリックします。

5. イベントを有効にして、イベントが検出されると、クライアントにイベントが送信され、連携アクションがトリガーされるようにします。
6. オプション:コピー先。。。をクリックして、イベント設定を他のアクセスコントロールデバイス、アラーム入力、ドア、またはカードリーダーにコピーします。

7.8.2 アクセスイベントのデバイスアクションの設定

アクセスコントロールデバイスのトリガイベントに対するアクセスコントロールデバイスの連携動作を設定できます。イベントがトリガされると、アラーム出力、ホストブザー、および同じデバイスでのその他のアクションをトリガできます。

手順

注意

デバイスでサポートされている必要があります。

1. 「アクセスコントロール→連携設定」を選択します。
2. 左側のリストからアクセスコントロールデバイスを選択します。
3. 「追加」ボタンをクリックして、新しいリンケージを追加します。
4. イベントソースをイベントリンクとして選択します。
5. 連動を設定するイベント種別と詳細イベントを選択します。
6. Linkage Target 領域で、このアクションを有効にするプロパティターゲットを設定します。

コントローラのブザー

アクセスコントロールデバイスの警告音がトリガされます。

キャプチャ

リアルタイムキャプチャがトリガされます。

アクセスポイント

開、閉、開のまま、閉のドアステータスがトリガされます。

注意

ターゲットドアとソースドアを同じにすることはできません。

7. 保存をクリックします。
8. オプション: デバイス連携を追加した後、次の1 つ以上を実行できます:

連携設定の編集 デバイスリストで設定した連動設定を選択すると、イベントソースや連動先などのイベントソースパラメータを編集できます。

連携設定の削除 デバイスリストで設定済みの連携設定を選択し、削除をクリックして削除します。

7.8.3 カードスワイプのためのデバイスアクションの設定

指定したカードスワイプに対して、アクセス制御装置の連携動作を設定できます。指定したカードをスワイプすると、同じデバイスでホストブザーやその他のアクションをトリガーできます。

手順

注意

デバイスでサポートされている必要があります。

1. 「アクセスコントロール→連携設定」を選択します。
2. 左側のリストからアクセスコントロールデバイスを選択します。
3. 「追加」ボタンをクリックして、新しいリンケージを追加します。
4. イベントソースをカードリンクとして選択します。
5. カード番号を入力するか、ドロップダウンリストからカードを選択します。
6. カードがリンクされたアクションをトリガーするためにスワイプするカードリーダーを選択します。
7. Linkage Target 領域で、このアクションを有効にするプロパティターゲットを設定します。

コントローラのブザー

アクセスコントロールデバイスの警告音がトリガされます。

キャプチャ

リアルタイムキャプチャがトリガされます。

アクセスポイント

開、閉、開のまま、または閉じたままのドアステータスがトリガされます。

8. 保存をクリックします。

カード(手順5 で設定)がカードリーダー(手順6 で設定)をスワイプすると、リンクされたアクショ

ン(手順7 で設定)をトリガできます。

9. オプション: デバイス連携を追加した後、次の1 つ以上を実行できます:

連携設定の削除 デバイスリストで設定済みの連携設定を選択し、削除をクリックして削除します。

連携設定の編集 デバイスリストで設定した連動設定を選択すると、イベントソースや連動先などのイベントソースパラメータを編集できます。

7.8.4 個人ID のデバイスアクションの設定

指定した個人IDに対して、アクセス制御装置の連携動作を設定できます。アクセス制御装置は、指定された個人IDを検出すると、カードリーダ上でブザーをトリガしたり、その他のアクションを実行したりすることができます。

手順

注意

デバイスでサポートされている必要があります。

1. 「アクセスコントロール→連携設定」を選択します。
2. 左側のリストからアクセスコントロールデバイスを選択します。
3. 「追加」をクリックして、新しいリンケージを追加します。
4. イベントソースとしてPerson Linkage を選択します。
5. 従業員番号を入力するか、ドロップダウンリストから個人を選択します。
6. カードがスワイプするカードリーダーを選択します。
7. Linkage Target 領域で、このアクションを有効にするプロパティターゲットを設定します。

コントローラのブザー

アクセスコントロールデバイスの警告音がトリガされます。

リーダーのブザー

カードリーダーの警告音がトリガーされます。

キャプチャ

選択したイベントが発生すると、イベント関連の画像がキャプチャされます。

記録

選択したイベントが発生すると、イベント関連の画像がキャプチャされます。

注意

デバイスは録音をサポートする必要があります。

アクセスポイント

開、閉、開のまま、または閉じたままのドアステータスがトリガされます。

8. 保存をクリックします。
9. オプション: デバイス連携を追加した後、次の1 つ以上を実行できます:

連携設定の削除	デバイスリストで設定済みの連携設定を選択し、削除をクリックして削除します。
連携設定の編集	デバイスリストで設定した連動設定を選択すると、イベントソースや連動先などのイベントソースパラメータを編集できます。

7.9 ドア制御

モニタリングモジュールでは、追加されたアクセスコントロールデバイスによって管理されているドアのリアルタイムステータスを表示できます。ドアを開閉したり、クライアントを介してドアを開閉したままにしたりするなど、ドアをリモートで制御することもできます。このモジュールには、リアルタイムアクセスイベントが表示されます。アクセスの詳細と個人の詳細を表示できます。

注意

ドア制御許可を持つユーザーの場合、ユーザーはモニタリングモジュールに入り、ドアを制御することができます。または、コントロールに使用するアイコンが表示されません。ユーザ権限の設定については、「個人管理」を参照してください。

7.9.1 コントロールドアの状態

ドアを開く、ドアを閉める、ドアを開いたままにする、ドアを閉じたままにする、ドアを閉じたままにするなど、単一のドアのステータスを制御できます。

手順

1. 「監視」をクリックして、状況監視ページに入ります。
2. 右上隅のアクセスポイントグループを選択します。

注意

アクセスポイントグループの管理については、クライアントソフトウェアの取扱説明書の「グループ管理」を参照してください。

選択したアクセスコントロールグループのドアが表示されます。

3. ドアアイコンをクリックしてドアを選択するか、Ctrl キーを押しながら複数のドアを選択します。
4. ドアを制御するには、次のボタンをクリックします。

ドアを開ける

ドアがロックされている場合は、ロックを解除すると、ドアが1 回開きます。開いている時間が経過すると、ドアは閉じられ、再び自動的にロックされます。

ドアを閉じる

ドアがロック解除されると、ロックされて閉じられます。アクセス権限を持つユーザは、クレデンシャルを使用してドアにアクセスできます。

オープンのまま

ドアはロック解除されます(閉じていても開いていても)。すべての人が資格情報なしでドアにアクセスできます。

閉じたまま

ドアが閉じてロックされます。スーパーユーザ以外は、承認されたクレデンシャルを持っていてもドアにアクセスできません。

キャプチャ

画像を手動でキャプチャします。

注意

キャプチャーボタンは、デバイスがキャプチャー機能をサポートしている場合に使用できます。画像は、クライアントを実行しているPC に保存されます。保存先の設定については、クライアントソフトウェアの取扱説明書「ファイル保存先を設定する」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に変化します。

7.9.2 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・スワイピング・レコード、顔認識レコード、指紋比較レコードなどを含むリアルタイムで表示されます。人物の情報を見たり、アクセス中に撮影した画像を見ることができます。

手順

1. 「監視」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がリアルタイムで表示されます。カード番号、人名、所属、イベント時間などの履歴の詳細を確認できます。
2. オプション: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、イベントタイプとイベントステータスを確認します。未チェックの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) 「最新のイベントを表示」をオンにすると、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. 必要に応じて、イベントをクリックして、アクセスした人物の詳細(人物の写真(キャプチャされた写真とプロフィール)、人物番号、人名、組織、電話、連絡先アドレスなど) を表示します。

注意

撮影した画像をダブルクリックすると、拡大して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。

7.10 イベントセンター

クライアントが受信したイベント情報(たとえば、デバイスがオフライン)が表示されます。イベントセンターでは、リアルタイムイベントと履歴イベントの詳細情報の確認、イベントにリンクされたビデオの表示、イベントの処理などを行うことができます。

クライアントがデバイスからイベント情報を受信できるようにするには、まずリソースのイベントを有効にして、デバイスを準備する必要があります。詳細については、「デバイスからのイベント受信の有効化」を参照してください。

7.10.1 デバイスからのイベント受信の有効化

クライアントソフトウェアがデバイスからイベント通知を受信するには、まずデバイスをアームする必要があります。

手順

1. 「→ Tool → Device Arming Control」を選択して、「Device Arming Control」を開きます。 追加したすべてのデバイスがこのページに表示されます。
2. 「自動アーミング(Auto-Arming)」コラムで、スイッチをオンにして自動アーミングを有効にします。

図7-14 アームデバイス

電源を入れると、デバイスが準備されます。また、アームされたデバイスによってトリガーされたイベントに関する通知は、リアルタイムでクライアントソフトウェアに自動的に送信されます。

7.10.2 リアルタイムイベントの表示

接続されたリソースのクライアントが受信したリアルタイム・イベント情報が表示されます。イベントソース、イベント時間、優先順位など、リアルタイムのイベント情報を確認できます。

はじめる前に

クライアントがデバイスからイベントを受信できるようにする前に、デバイスからのイベントの受信を有効にします。詳細については、「デバイスからのイベントの受信を有効にする」を参照してください。

手順

1. 「イベントセンター→リアルタイムイベント」を選択すると、リアルタイムイベントページが開き、クライアントが受信したリアルタイムイベントを表示できます。

   イベント時間

   エンコードデバイスの場合、イベント時間はイベントを受信したクライアント時間です。その他のデバイスタイプの場合、イベント時間はイベントがトリガーされる時間です。

   優先度

   優先度は、イベントの緊急度を表します。
2. イベントをフィルタリングします。

デバイスタイプおよび(または)優先順位によるフィルタ	イベントをフィルタするデバイスタイプおよび(または)優先順位を選択します。
キーワードによるフィルタリング	キーワードを入力して、イベントをフィルタリングします。

3. (オプション) イベントリストのテーブルヘッダーを右クリックして、イベントリストに表示されるイベント関連項目をカスタマイズします。
4. イベントの詳細を表示します。
   1) イベントリストでイベントを選択します。
   2) ページの右下隅にある「展開」をクリックします。
   3) イベントの詳細説明と処理レコードを表示します。
5. (オプション) 必要に応じて、以下の操作を実行します。

   単一イベントの処理 「ハンドル」をクリックして処理候補を入力し、「コミット」をクリックします。

   > **注意**
   >
   > イベントが処理されると、Handle ボタンがAdd Remark になります。この処理済みイベントに注釈を追加するには、「注釈の追加」をクリックします。

イベントのバッチ処理	処理する必要があるイベントを選択し、「バッチで処理(Handle in Batch)」をクリックします。処理候補を入力し、「コミット」をクリックします。
アラームオーディオの有効化/無効化	「オーディオを有効にする/オーディオを無効にする」をクリックして、イベントのオーディオを有効/無効にします。
最新のイベントを自動的に選択する	自動-最新イベントを選択をオンにすると、最新のイベントが自動的に選択され、イベント情報の詳細が表示されます。
イベントのクリア	「消去(Clear)」をクリックすると、イベント・リスト内のすべてのイベントが消去されます。
電子メールの送信	イベントを選択し、「電子メールを送信」をクリックすると、このイベントの詳細情報が電子メールで送信されます。

注意

最初に電子メールパラメータを設定する必要があります。詳細については、を参照してください。

7.10.3 履歴イベントの検索

イベント・センター・ページのイベント検索モジュールでは、指定された装置タイプに応じて、時間、装置タイプ、およびその他の条件を介して履歴イベントを検索し、イベントを処理することができます。

はじめる前に

クライアントがデバイスからイベント情報を受信できるようにする前に、デバイスからのイベントの受信を有効にします。詳細については、「デバイスからのイベントの受信を有効にする」を参照してください。

手順

1. 「イベントセンター→イベント検索」を選択して、イベント検索ページを開きます。

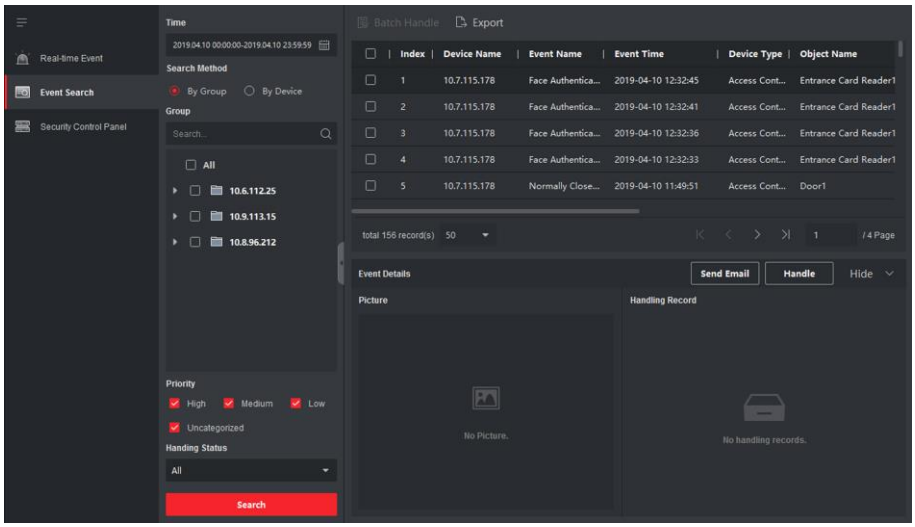


図7-15 検索履歴イベント

2. 必要なイベントのみを表示するようにフィルタ条件を設定します。

時間

イベントが開始するクライアントの時刻。

グループで検索:選択したグループ内のリソースで発生したイベントを検索します。
デバイス:選択したデバイスで発生したイベントを検索します。

デバイスタイプ

イベントが発生したデバイスのタイプ。

すべて

すべてのデバイスタイプで、グループ、優先度、ステータスのフィルタ条件を設定できます。

ビデオインターコム

ビデオインターコムのイベントでは、検索範囲として「All Record」と「Only Unlocking」を選択する必要があります。

- すべてのレコード
- : すべてのビデオインターコムイベントからイベントをフィルタリングできます。フィルタリング条件として、デバイス、優先度、ステータスを設定する必要があります。
- ロック解除のみ
- : すべてのビデオインターコムロック解除イベントからイベントをフィルタリングできます。また、デバイス、ロック解除タイプのフィルター条件を設定する必要があります。

アクセス制御

アクセス制御のイベントには、デバイス、優先度、ステータス、イベントタイプ、カードリーダータイプ、個人名、カード番号、組織のフィルター条件を設定できます。

注意

イベントタイプ、カードリーダータイプ、個人名、カード番号、組織を設定するには、「その他を表示」をクリックします。

グループ

イベントが発生したデバイスのグループ。グループ条件は、Device Type as All を選択した場合にのみ設定してください。

装置

イベントが発生したデバイス。

優先度

イベントの緊急度を示す、低、中、高、未分類を含む優先度。

ステータス

イベントの処理ステータス。

3. 「検索」をクリックして、設定した条件に従ってイベントを検索します。
4. (オプション) イベントリストのテーブルヘッダーを右クリックして、イベントリストに表示されるイベント関連項目をカスタマイズします。

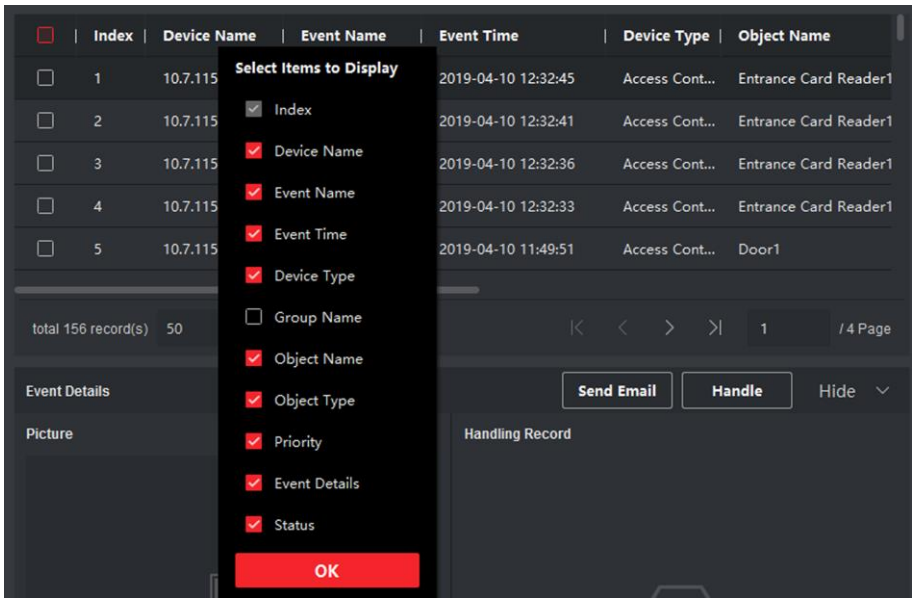


図7-16 表示するイベント関連項目のカスタマイズ

5. オプション: イベントを処理します。
   - 単一イベントの処理:処理する必要があるイベントを1 つ選択し、イベント情報の詳細ページで処理をクリックして、処理候補を入力します。
   - バッチでイベントを処理する:処理する必要があるイベントを選択し、「バッチで処理(Handle in Batch)」をクリックして、処理の提案を入力します。

注意

イベントが処理されると、Handle ボタンがAdd Remark になり、Add Remark をクリックして、この処理されたイベントに注釈を追加します。

6. 必要に応じて、イベントを選択して「電子メールを送信」をクリックすると、このイベントの詳細情報が電子メールで送信されます。

注意

最初に電子メールパラメータを設定する必要があります。詳細については、クライアントソフトウェアのユーザーマニュアルの「電子メールパラメータの設定」を参照してください。

7. オプション: イベントログまたはイベント写真をCSV形式でローカルPCにエクスポートするには、「エクスポート」をクリックします。保存パスは手動で設定できます。
8. 関連する画像にカーソルを合わせ、画像の右上隅にあるダウンロードアイコンをクリックして、ローカルPC にダウンロードします。保存パスは手動で設定できます。

7.11 時間と出勤

Time and Attendance モジュールには、従業員がいつ業務を開始および停止するかを追跡および監視し、遅延到着、早期退職、休職や欠勤などの従業員の勤務時間を完全に制御するための複数の機能が用意されています。

注意

このセクションでは、参加レポートを取得する前に設定を紹介します。これらの設定後に記録されたアクセスレコードは、統計で計算されます。

7.11.1 アテンダンスパラメータの設定

一般ルール、時間外パラメータ、出席チェックポイント、休日、脱退タイプなどの出席パラメータを設定できます。

週末を設定

週末の曜日は、国や地域によって異なる場合があります。クライアントは週末定義関数を提供します。実際の要件に応じて1 つ以上の曜日を週末として選択し、平日と平日で異なる出席ルールを設定できます。

手順

注意

ここで設定したパラメータは、新しく追加された期間のデフォルトとして設定されます。存在するものには影響しません。

1. Time & Attendance モジュールを入力します。
2. 出席設定→の基本規則を選択します。
3. 週末として曜日を選択します(土曜や日曜など)。
4. 保存をクリックします。

時間外パラメータの設定

残業レベル、勤務時間率、残業のアテンダンスステータスなど、勤務日と週末の残業パラメータを設定できます。

手順

1. 「時刻と出席→の出席設定」→「残業」を選択します。
2. 必要な情報を設定します。

勤務日の残業レベル

労働日の終業時間後、一定期間働くと、残業レベル1、残業レベル2、残業レベル3と、異なる残業レベルになります。3 つの残業レベルにそれぞれ異なる勤務時間レートを設定できます。

労働時間率

勤務時間率は、それに残業時間を掛けて勤務時間を計算します。平日の勤務終了後、一定の期間勤務すると、異なる残業レベルに達します。3 つの残業レベルに異なる勤務時間レート(1 ～10、10 進数) を設定できます。たとえば、有効な残業時間が1 時間(残業レベル1) で、残業レベル1 の勤務時間レートが2 に設定されている場合、その期間の勤務時間は2 時間として計算されます。

週末の時間外勤務規則

週末の時間外ルールを有効にして、計算モードを設定できます。

3. 保存をクリックします。

Attendance Check Point の設定

アクセスポイントのカードリーダーを出席チェックポイントに設定して、カードリーダーの認証が出席用に記録されるようにすることができます。

はじめる前に

出席チェックポイントを設定する前に、アクセスコントロールデバイスを追加する必要があります。詳細については、「デバイスの追加」を参照してください。

手順

注意

デフォルトでは、追加されたアクセスコントロールデバイスのすべてのカードリーダーが出席チェックポイントとして設定されます。

1. Time & Attendance モジュールを入力します。
2. 出席チェック・ポイントの→にある出席チェック・ポイントの設定をクリックして、出席チェック・ポイントの設定ページに入ります。
3. オプション:すべてのカードリーダーをチェック・ポイントのスイッチがオフになるように設定します。
   リスト内のカードリーダーのみが出席チェックポイントとして設定されます。
4. デバイスリストで、出席チェックポイントとして必要なカードリーダーを確認します。
5. チェックポイント機能は、Start/End-Work、Start-Work、End-Work のいずれかに設定します。
6. Set as Check Point をクリックします。
   設定されたアテンダンスチェックポイントが右側のリストに表示されます。

休日の設定

チェックインやチェックアウトが記録されない休日を追加できます。

通常の休日を追加

年末年始、独立日、クリスマス日など、有効期間内の定期的な日に毎年有効になる休日を設定できます。

手順

1. Time & Attendance モジュールを入力します。
2. 「休日→の出席設定」を選択して、「休日設定」ページを開きます。
3. 休日の種類として通常の休日をチェックします。
4. 休日の名前をカスタマイズします。
5. 休日の最初の日を設定します。
6. 休日数を記入する。
7. 従業員が休日に働いている場合の出席状況を設定します。
8. オプション:この休日設定を毎年有効にするには、「毎年繰り返す」をオンにします。
9. OKをクリックします。
   追加した休日は休日リストとカレンダーに表示されます。
   異なる休日を選択した場合は、最初に追加された休日として記録されます。
10. (オプション) 休日を追加したら、次のいずれかの操作を実行します。

休日編集	クリックして休日情報を編集します。
休日削除	追加した休日を1つ以上選択し、「削除」をクリックして休日リストから休日を削除します。

不定期休日登録

休日は、銀行の休日など、有効期間中の不定期な日に毎年有効になるように設定できます。

手順

1. Time & Attendance モジュールを入力します。
2. 「休日→の出席設定」を選択して、「休日設定」ページを開きます。
3. 「追加」をクリックして、「休日の追加」ページを開きます。
4. 休日の種類として不規則休日をチェックします。
5. 休日の名前をカスタマイズします。
6. 休日の開始日を設定します。

   例

   2019年11 月の4 つ目の木曜日を休日に設定する場合は、4 つのドロップダウンリストから2019年、11 月、4 日、木曜日を選択する必要があります。
7. 休日数を記入する。
8. 従業員が休日に働いている場合の出席状況を設定します。

9. オプション:この休日設定を毎年有効にするには、「毎年繰り返す」をオンにします。
10. OKをクリックします。
    追加した休日は休日リストとカレンダーに表示されます。
    異なる休日を選択した場合は、最初に追加された休日として記録されます。
11. (オプション) 休日を追加したら、次のいずれかの操作を実行します。

休日編集	クリックして休日情報を編集します。
休日削除	追加した休日を1つ以上選択し、「削除」をクリックして休日リストから休日を削除します。

脱退タイプの設定

リーブ・タイプ(メジャー・リーブ・タイプとマイナー・リーブ・タイプ)は、実際のニーズに合わせてカスタマイズできます。リーブタイプを編集または削除することもできます。

手順

1. Time & Attendance モジュールを入力します。
2. 「Leave Type」→に「Leave Type」をクリックして、「Leave Type Settings」ページに入ります。
3. 左側の「追加」をクリックして、メジャーリーブタイプを追加します。
4. オプション: メジャーリーブタイプに対して、次のいずれかの操作を実行します。

編集	メジャーリーブタイプの上にカーソルを移動し、をクリックしてメジャーリーブタイプを編集します。
削除	メジャーリーブタイプを1つ選択し、左側のDeleteをクリックしてメジャーリーブタイプを削除します。

5. 右側の「追加」をクリックして、マイナーリーブタイプを追加します。
6. オプション: マイナーリーブタイプに対して、次のいずれかの操作を実行します。

編集	マイナーリーブタイプの上にカーソルを移動し、をクリックしてマイナーリーブタイプを編集します。
削除	1 つまたは複数のメジャーリーブタイプを選択し、右側の「削除」をクリックして、選択したマイナーリーブタイプを削除します。

認証レコードのサードパーティデータベースへの同期

クライアントソフトウェアに記録された出席データは、他のシステムで計算やその他の操作に使用することができます。同期機能を有効にして、クライアントソフトウェアからの認証レコードをサードパーティデータベースに自動的に適用することができます。

手順

1. Time & Attendance モジュールを入力します。
2. 出席設定→サードパーティデータベースをクリックする。
3. Apply to Database switch をon に設定して、同期機能を有効にします。
4. データベースタイプをSQLServer またはMySql として選択します。

注意

MySql を選択した場合は、ローカルPC から設定ファイル(libmysql.dll) をインポートする必要があります。

5. サーバのIP アドレス、データベース名、ユーザ名、パスワードなど、サードパーティデータベースのその他の必須パラメータを設定します。
6. 実際の構成に応じて、データベースのテーブルパラメータを設定します。
   1) サードパーティデータベースのテーブル名を入力します。
   2) クライアントソフトウェアとサードパーティデータベース間のマッピングされたテーブルフィールドを設定します。
7. 「保存」をクリックして、データベースが接続可能かどうかをテストし、正常な接続の設定を保存します。
   - 参加データはサードパーティのデータベースに書き込まれます。
   - 同期中に、クライアントがサードパーティデータベースとの接続を切断すると、クライアントは30 分ごとに再接続を開始します。再接続後、クライアントは切断期間中に記録されたデータをサードパーティデータベースに同期します。

ブレーク時間の設定

ブレーク時間を追加したり、ブレークの開始時間、終了時間、期間、計算モードなどのパラメータを設定したりできます。追加したブレークタイムは、編集または削除することもできます。

手順

1. 「時刻と出席→時刻表」を選択します。
   追加された時刻表がリストに表示されます。
2. 追加した時刻表を選択するか、「追加」をクリックして設定時刻表ページに入ります。
3. Break Time をクリックして、Break Time ページに入ります。
4. ブレーク時間の設定をクリックします。
5. ブレークタイムを追加します。
   1) 追加をクリックします。
   2) ブレークタイムの名前を入力します。

3) ブレイク時間に関するパラメータを設定します。

開始時刻/終了時刻

ブレークの開始時刻と終了時刻を設定します。

No Earlier Than / No Later Than

ブレイクを開始する最初のスワイプ時間と、ブレイクを終了する最後のスワイプ時間を設定します。

ブレーク時間

ブレークの開始時刻から終了時刻までの期間。

計算

自動減算

休止時間は、勤務時間から除外されます。

チェックが必要

実際のチェックイン時間とチェックアウト時間に応じて、ブレーク時間が計算され、業務時間から除外されます。

注意

計算方法として「必ず確認する」を選択した場合は、中断からの復帰が遅れたり早まったりする場合の出席状況を設定する必要があります。

6. 保存をクリックして設定を保存します。
7. (オプション) 「追加」をクリックして、ブレーク時間の追加を続行します。

レポート表示の設定

会社名、ロゴ、日付形式、時刻形式、マークなど、参加レポートに表示される表示内容を設定できます。

手順

1. Time & Attendance モジュールを入力します。
2. 出席統計→レポート画面を押す。
3. 参加レポートの表示設定を設定します。

商号

レポートに名前を表示する会社名を入力します。

出席状況マーク

マークを入力し、色を選択します。レポート内の参加ステータスの関連フィールドには、マークと色が表示されます。

週末マーク

マークを入力し、色を選択します。レポートの週末フィールドには、マークと色が表示されます。

4. 保存をクリックします。

7.11.2 一般予定表の追加

時刻表ページでは、固定の開始時刻と終了時刻を必要とする従業員の一般的な時刻表を追加できます。また、有効なチェックイン/チェックアウト時間、遅延および早退の許容タイムテーブルを設定することができます。

手順

1. 「時刻と出席→時刻表」を選択して、時刻表設定ページに入ります。
2. 「追加」をクリックして、時刻表の追加ページを入力します。

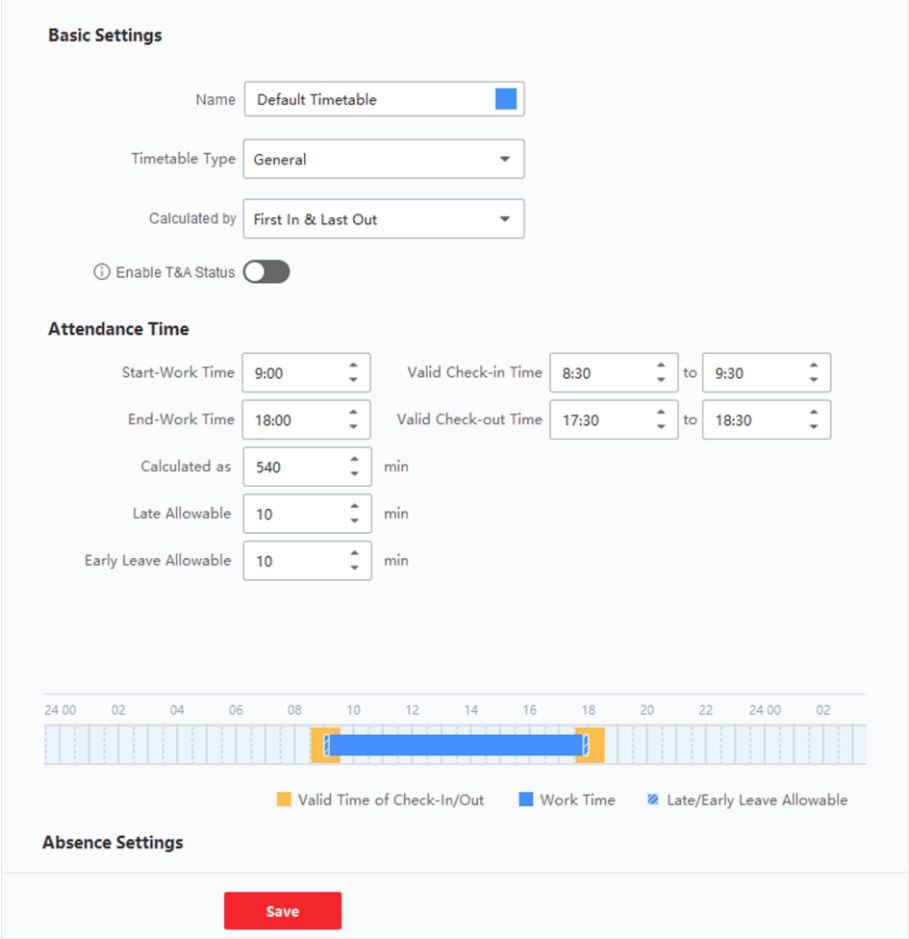


図7-17 タイムテーブルの追加

3. 時刻表の名前を作成します。

注意

名前の横にある色のアイコンをクリックして、設定結果領域のタイムバーにある有効なタイムテーブルの色をカスタマイズできます。

4. 一般的な時刻表の種類を選択します。
5. 計算方法を選択します。

ファーストイン&ラストアウト

最初のチェックイン時間は開始作業時間として記録され、最後のチェックアウト時間は終了作業時間として記録されます。

各チェックイン/アウト

各チェックイン時間とチェックアウト時間は有効であり、隣接するチェックイン時間とチェックアウト時間の間の全期間の合計が有効な作業時間として記録されます。
この計算方法にはValid Authentication Interval を設定する必要があります。たとえば、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になります。

6. オプション: デバイスの出席状況に基づいて計算するには、Enable T&A Status スイッチをオンに設定します。

注意

この機能はデバイスでサポートされている必要があります。

7. 関連する参加時間パラメータを以下のように設定します:

開始/終了時刻

作業開始時刻と作業終了時刻を設定します。

有効なチェックイン/アウト時間

タイムバーで黄色のバーを調整して、チェックインまたはチェックアウトが有効なタイムテーブルを設定します。

計算結果実際の作業時間として計算された継続時間を設定します。

遅刻・早期休暇許可

レイトリーブまたはアーリーブの時刻表を設定します。

8. 不在関連のパラメータを設定します。

チェックイン、レイト:チェックインしたが、仕事に遅れている従業員の遅延時間を設定できます。必要時間を超えた場合は、出勤データに欠席と表示されます。

チェックアウト、早期退職の場合、通常の休業時間よりも前にチェックアウトした従業員の早

期退職期間を設定できます。また、その従業員の出席データは「不在」としてマークされます。

チェックインなし

本人がチェックインしない場合は、出勤データを欠勤・遅刻と表記することがあります。

チェックアウトなし

チェックアウトしない場合は、勤怠データを欠勤・早退と表記する場合があります。

9. 保存をクリックして、時刻表を追加します。
10. (オプション) 時刻表を追加した後、1 つ以上の以下の操作を実行します。

予定表の編集	リストから時刻表を選択し、関連情報を編集します。
時刻表の削除	リストから時刻表を選択し、「削除」をクリックして削除します。

7.11.3 シフトの追加

シフト期間(日、週、月)や有効出席時間などの従業員のシフトを追加できます。実際の要件に応じて、従業員ごとに1 つのシフトで複数のタイムテーブルを追加できます。この場合、各タイムテーブルのチェックインとチェックアウトが必要になります。

はじめる前に

まず時刻表を追加します。詳細については、「一般予定表の追加」を参照してください。

手順

1. 「時刻と出席→の移動」を選択して、シフト設定画面に入ります。
2. 「追加」をクリックして「シフトの追加」ページに入ります。
3. シフトの名前を入力します。
4. ドロップダウンリストからシフト期間を選択します。
5. 追加した時刻表を選択し、タイムバーをクリックして時刻表を適用します。

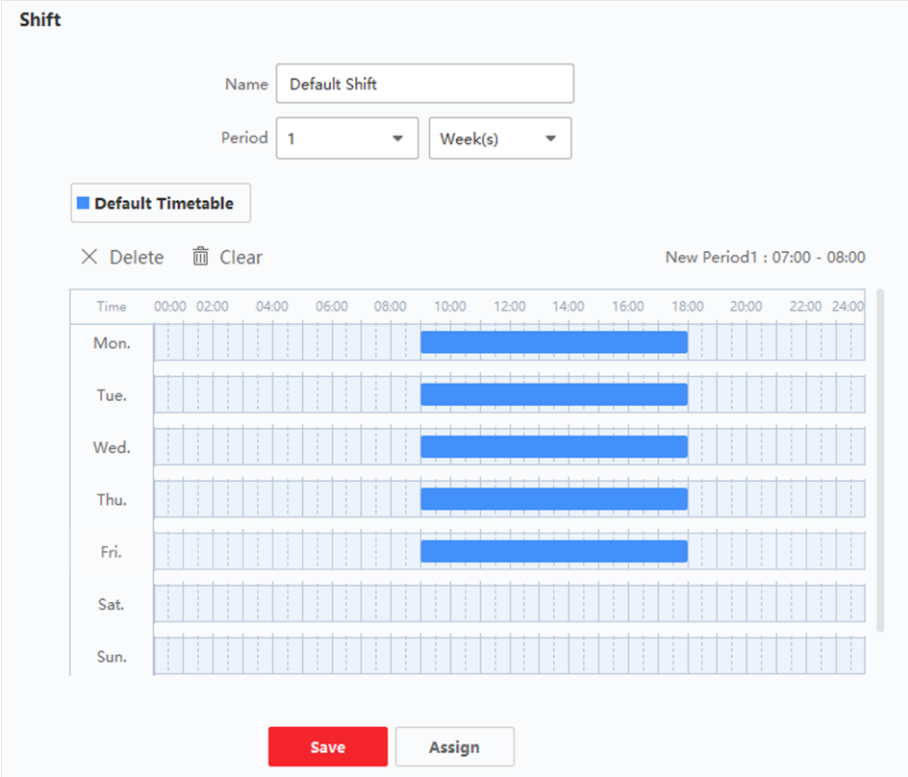


図7-18 シフトの追加

注意

複数の時刻表を選択できます。異なるタイムテーブルの開始および終了の作業時間と有効なチェックインおよびチェックアウト時間は重複できません。

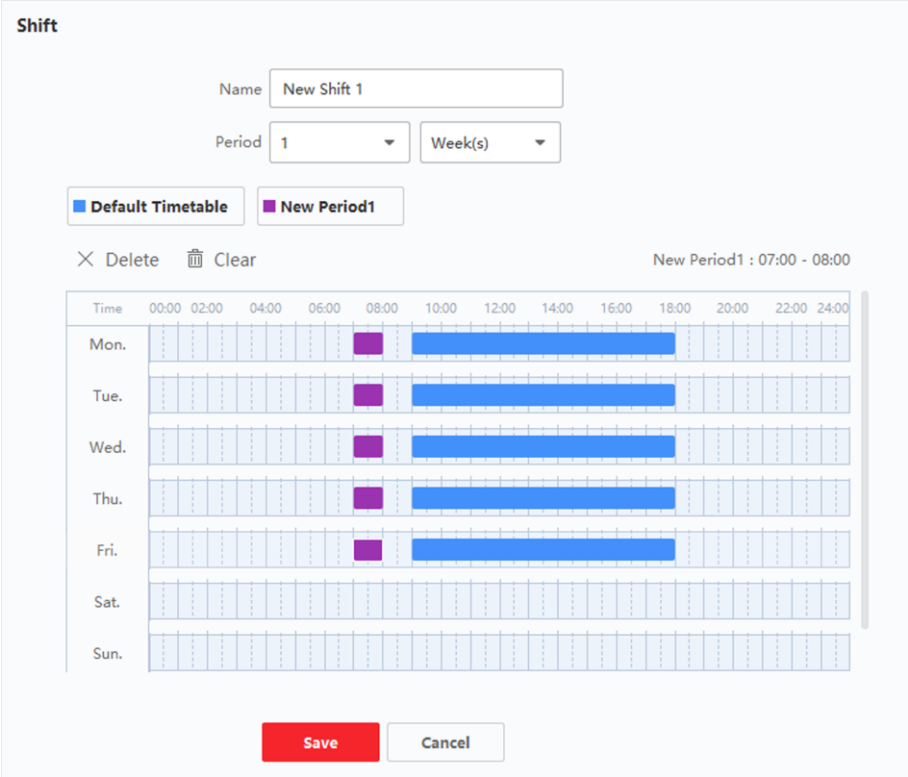


図7-19 複数のタイムテーブルの追加

6. 保存をクリックします。
   追加されたシフトリストは、ページの左パネルに表示されます。最大64 のシフトを追加できます。
7. オプション: クイックシフトスケジュールのために、シフトを組織または個人に割り当てます。
   1) 割り当てをクリックします。
   2) 組織または個人タブを選択し、目的の組織または個人ボックスをオンにします。
      選択した組織または個人が右ページに一覧表示されます。
   3) シフトスケジュールの失効日を設定します。
   4) スケジュールのその他のパラメータを設定します。

      チェックイン不要

      このスケジュールのユーザーは、作業に入ったときにチェックインする必要はありません。

      チェックアウト不要

      このスケジュールのユーザーは、作業終了時にチェックアウトする必要はありません。

      休日予定

      休日には、このスケジュールは引き続き有効であり、スケジュールに従って仕事に進む必要があります。

      残業有効

      この日程については、人の残業時間を記録します。
   5) 保存をクリックして、クイックシフトスケジュールを保存します。

7.11.4 シフトスケジュールの管理

シフト・ワークは、毎日24時間の時計をすべて利用するように設計された雇用慣行である。実際には、通常、シフトに分割された日、異なるシフトが業務を実行する期間を設定する日がわかります。

部門スケジュール、個人スケジュール、および一時スケジュールを設定できます。

部門スケジュールの設定

1 つの部署にシフトスケジュールを設定し、部署内のすべての担当者にシフトスケジュールを割り当てることができます。

はじめる前に

Time & Attendance モジュールでは、部門リストは組織と同じです。まず、Person モジュールに組織と個人を追加する必要があります。詳細は、個人管理を参照してください。

手順

1. 「時刻と出席→のシフトスケジュール」を選択して、「シフトスケジュール管理」ページに入ります。
2. 部門スケジュールをクリックして、部門スケジュールページを入力します。
3. 左側の組織リストから部門を選択します。

注意

「サブ組織を含める」をオンにすると、組織を選択するときに、そのサブ組織も同時に選択されます。

---

4. ドロップダウンリストからシフトを選択します。
5. 必要に応じて、「複数のシフトスケジュール」を有効にし、追加した人物のタイムテーブルから有効期間を選択します。

注意

これは、1つのタイムテーブルのみのシフトにのみ使用できます。

複数のシフトスケジュール

それは複数の時刻表を含む。タイムテーブルのチェックイン/チェックアウトができ、出席が有効になります。

複数のシフトスケジュールに3 つのタイムテーブル(00:00 ～07:00、08:00 ～15:00、16:00 ～23:00) が含まれている場合。この複数のシフトスケジュールを採用した人の出席は、3つのタイムテーブルのいずれかで有効になります。07:50にチェックインすると、直近の08:00から15:00までの時刻表が出席者に適用されます。

---

6. 開始日と終了日を設定します。
7. スケジュールのその他のパラメータを設定します。

チェックイン不要

このスケジュールのユーザーは、作業に入ったときにチェックインする必要はありません。

チェックアウト不要

このスケジュールのユーザーは、作業終了時にチェックアウトする必要はありません。

休日予定

休日には、このスケジュールは引き続き有効であり、スケジュールに従って仕事に進む必要があります。

残業有効

この日程については、人の残業時間を記録します。

8. 保存をクリックします。

スケジュール設定

1人以上の人にシフトスケジュールを割り当てることができます。個人スケジュールの詳細を表示および編集することもできます。

はじめる前に

Person モジュールに部門と個人を追加します。詳細は、個人管理を参照してください。

手順

注意

個人のスケジュールは、部門のスケジュールよりも優先されます。

1. 「時刻と出席→のシフトスケジュール」を選択して、「シフトスケジュール」ページに入ります。
2. 「Person Schedule」をクリックして、「Person Schedule」ページに入ります。
3. 組織を選択し、個人を選択します。
4. ドロップダウンリストからシフトを選択します。
5. 必要に応じて、「複数のシフトスケジュール」を有効にし、追加した人物のタイムテーブルから有効期間を選択します。

注意

これは、1つのタイムテーブルのみのシフトにのみ使用できます。

複数のシフトスケジュール

それは複数の時刻表を含む。タイムテーブルのチェックイン/チェックアウトができ、出席が有効になります。

複数のシフトスケジュールに3 つのタイムテーブル(00:00 ～07:00、08:00 ～15:00、16:00 ～23:00) が含まれている場合。この複数のシフトスケジュールを採用した人の出席は、3つのタイムテーブルのいずれかで有効になります。07:50にチェックインすると、直近の08:00から15:00までの時刻表が出席者に適用されます。

6. 開始日と終了日を設定します。
7. スケジュールのその他のパラメータを設定します。

チェックイン不要

このスケジュールのユーザーは、作業に入ったときにチェックインする必要はありません。

チェックアウト不要

このスケジュールのユーザーは、作業終了時にチェックアウトする必要はありません。

休日予定

休日には、このスケジュールは引き続き有効であり、スケジュールに従って仕事に進む必要があります。

残業有効

この日程については、人の残業時間を記録します。

8. 保存をクリックします。

テンポラリスケジュールの設定

一時的なスケジュールを追加して、一時的にシフトスケジュールを割り当てることができます。また、一時的なスケジュールの詳細を表示および編集することもできます。

はじめる前に

Person モジュールに部門と個人を追加します。詳細は、個人管理を参照してください。

手順

注意

一時スケジュールは、部門のスケジュールおよび個人のスケジュールよりも優先されます。

1. 「時刻と出席→のシフトスケジュール」を選択して、「シフトスケジュール管理」ページに入ります。
2. Temporary Schedule をクリックして、Temporary Schedule ページに入ります。
3. 組織を選択し、個人を選択します。
4. 1つの日付をクリックするか、クリックしてドラッグし、一時スケジュールの複数の日付を選択します。
5. 「平日」または「非平日」をドロップダウンリストから選択します。

「休業日」を選択した場合は、以下のパラメータを設定する必要があります。

通常レベルまたは残業レベルとして計算され、一時スケジュールの出席ステータスをマークします。

時刻表

ドロップダウンリストから時刻表を選択します。

複数シフトスケジュール

それは複数の時刻表を含む。タイムテーブルのチェックイン/チェックアウトができ、出席が有効になります。
複数のシフトスケジュールに3 つのタイムテーブル(00:00 ～07:00、08:00 ～15:00、16:00 ～23:00) が含まれている場合。この複数のシフトスケジュールを採用した人の出席は、3つのタイムテーブルのいずれかで有効になります。07:50にチェックインすると、直近の08:00から15:00までの時刻表が出席者に適用されます。

ルール

スケジュールの他のルール(Check-in Not Required、Check-out Not Requiredなど)を設定します。

6. 保存をクリックします。

シフトスケジュールの確認

カレンダーモードまたはリストモードで、シフトスケジュールを確認できます。また、シフトスケジュールを編集または削除することもできます。

手順

1. 「時刻と出席→のシフトスケジュール」を選択して、「シフトスケジュール管理」ページに入ります。
2. 組織と対応する個人を選択します。
3. またはをクリックすると、カレンダーモードまたはリストモードでシフトスケジュールが表示されます。

カレンダー

カレンダーモードでは、1 か月に1 日のシフトスケジュールを表示できます。一時スケジュールを1日クリックして、編集または削除することができます。

リスト

リストモードでは、シフト名、タイプ、有効期間など、1 人の人または組織に関するシフトスケジュールの詳細を表示できます。シフトスケジュールをチェックし、削除をクリックして選択したシフトスケジュールを削除します。

7.11.5 チェックイン/チェックアウト記録の手動修正

参加ステータスが正しくない場合は、チェックインまたはチェックアウトレコードを手動で修正でき

ます。また、チェックインまたはチェックアウトレコードを編集、削除、検索、またはエクスポートすることもできます。

はじめる前に

- Person モジュールに組織と個人を追加する必要があります。詳細については、個人管理を参照してください。
- 出席状況が不正です。

手順

1. 出席→の「時刻と出席者の取り扱い」を選択して、出席者の取扱い画面に入ります。
2. Correct Check-In/Out をクリックして、チェックイン/チェックアウト修正ページを追加します。
3. 修正する人を左側のリストから選択します。
4. 修正日を選択します。
5. チェックイン/チェックアウトの補正パラメータを設定します。

チェックインを選択し、実際の作業開始時刻を設定します。チェックアウトを選択し、実際のエンドワーク時間を設定します。

注意

クリックすると、複数のチェックイン/チェックアウト項目を追加できます。最大8 つのチェックイン/アウト項目をサポートできます。⊕

6. オプション: 必要に応じて注釈情報を入力します。
7. 保存をクリックします。
8. (オプション) チェックイン/チェックアウト修正を追加した後、次のいずれかの操作を実行します。

ビュー

またはをクリックすると、追加した出席処理情報がカレンダーまたはリストモードで表示されます。

注意

カレンダーモードでは、Calculate をクリックして、1 か月以内に個人の出席状況を取得する必要があります。

編集

- カレンダーモードで、日付の関連ラベルをクリックして詳細を編集します。
- リストモードで、Date、Handling Type、Time、またはRemark 列の関連フィールドをダブルクリックして、情報を編集します。

削除

選択した項目を削除します。

エクスポート

出席処理の詳細をローカルPC にエクスポートします。

注意

エクスポートされた詳細は、CSV形式で保存されます。

7.11.6 脱退およびビジネス・トリップの追加

社員が休暇を求めたい時や出張したい時などに休暇や出張を追加することができます。

はじめる前に

Person モジュールに組織と個人を追加する必要があります。詳細については、個人管理を参照してください。

手順

1. 出席→の「時刻と出席者の取り扱い」を選択して、出席者の取扱い画面に入ります。
2. 「休暇/出張申請」をクリックして、「休暇/出張ページ」を追加します。
3. 左側のリストから人を選択します。
4. 退職または出張の日付を設定します。
5. ドロップダウンリストからメジャーリーブタイプとマイナーリーブタイプを選択します。

注意

出席設定で脱退タイプを設定できます。詳細については、「脱退タイプの設定」を参照してください。

6. 脱退時間を設定します。
7. オプション: 必要に応じて注釈情報を入力します。
8. 保存をクリックします。
9. (オプション) リーブおよび出張を追加した後、以下のいずれかの操作を実行します。

ビュー

またはをクリックすると、追加した出席処理情報がカレンダーまたはリストモードで表示されます。

注意

カレンダーモードでは、Calculate をクリックして、1 か月以内に個人の出席状況を取得する必要があります。

編集

- カレンダーモードで、日付の関連ラベルをクリックして詳細を編集します。
- リストモードで、Date、Handling Type、Time、またはRemark 列のフィールドをダブルクリックして、関連情報を編集します。

削除	選択した項目を削除します。
エクスポート	出席処理の詳細をローカルPC にエクスポートします。

注意

エクスポートされた詳細は、CSV形式で保存されます。

7.11.7 出席データの計算

出席データの概要、従業員の詳細な出席データ、従業員の異常出席データ、従業員の残業データ、およびカードスワイピングログを検索して表示する前に、出席データを計算する必要があります。

出席データの自動計算

スケジュールを設定して、毎日設定した時刻に、クライアントが前日の出席データを自動的に計算できるようにすることができます。

手順

注意

1. Time & Attendance モジュールを入力します。
2. 出席設定→の基本規則を選択します。
3. 出席者の自動計算領域で、クライアントがデータを計算する時刻を設定します。
4. 保存をクリックします。
   クライアントは、設定した時刻から前日の出席データを計算します。

出席データの手動計算

データ範囲を設定することで、出席データを手動で計算できます。

手順

1. Time & Attendance モジュールを入力します。
2. 出席統計→の算出を選択します。
3. 出席データの範囲を定義するには、開始時刻と終了時刻を設定します。
4. 部門、名前、個人ID、出席状況など、その他の条件を設定します。
5. Calculate をクリックします。

注意

3 か月以内の出席データのみを計算できます。

6. 次のいずれかの操作を行います。

正しいチェックイン/アウト	チェックイン/チェックアウトを修正を追加するには、修正チェックイン/チェックアウトをクリックします。
表示する項目の選択	レポートに表示する項目を選択するには、各項目のタイトルをクリックまたは右クリックします。
レポートの生成	出席レポートを生成するには、「レポート」をクリックします。
レポートのエクスポート	出席データをローカルPCにエクスポートするには、エクスポートをクリックします。

注意

エクスポートされた詳細は。CSV に保存されます。 形式。

7.11.8 出席統計

オリジナルの出席記録を確認し、計算された出席データに基づいて出席報告書を生成およびエクスポートすることができます。

従業員の出席データの概要の取得

出席時刻、出席状況、チェックポイントなど、従業員の出席記録をクライアント上で検索および表示できます。

はじめる前に

- 個人モジュールに組織と個人を追加し、個人がカードをスワイプしている必要があります。詳細については、個人管理を参照してください。
- 出席データを計算します。

注意

- クライアントは、翌日の午前1 時に前日の出席データを自動的に計算します。
- クライアントを午前1:00 に実行したままにすると、前日の出席データを自動的に計算できなくなります。自動計算されない場合は、出席データを手動で計算できます。詳細については、「出席データの手動計算」を参照してください。

手順

1. Time & Attendance モジュールを入力します。
2. 出席統計→の出席記録を選択します。
3. 検索する出席開始時刻と終了時刻を設定します。
4. 部門、名前、個人ID など、その他の検索条件を設定します。
5. データ・ソースを「デバイス上のオリジナル・レコード」または「マニュアル・ハンドリング・レコード」として選択します。
6. オプション:デバイスからイベントを取得をクリックして、デバイスから参加データを取得します。
7. (オプション) 「リセット」をクリックして、すべての検索条件をリセットし、検索条件を再度編集します。
8. 検索をクリックします。
   結果がページに表示されます。従業員の必要な出席ステータスとチェックポイントを表示できます。
9. (オプション) 結果を検索した後、以下のいずれかの操作を実行します。

レポートの生成	出席レポートを生成するには、「レポート」をクリックします。
レポートのエクスポート	エクスポートをクリックして、結果をローカルPC にエクスポートします。
カスタムエクスポート	詳細はを参照してください。

インスタントレポートの生成

従業員の出席結果を表示するために、一連の出席レポートを手動で生成することができます。

はじめる前に

出席データを計算します。

注意

出席データを手動で計算することも、クライアントがデータを毎日自動的に計算できるようにスケジュールを設定することもできます。詳細については、「出席データの計算」を参照してください。

手順

1. Time & Attendance モジュールを入力します。
2. 出席統計→レポートを選択します。
3. レポートタイプを選択します。
4. 参加レポートを表示する部署または担当者を選択します。
5. 出席データがレポートに表示される開始時刻と終了時刻を設定します。
6. レポートをクリックして統計レポートを生成し、開きます。

カスタム出席レポート

クライアントは複数のレポートタイプをサポートしており、レポートコンテンツを事前定義し、設定した電子メールアドレスにレポートを自動的に送信できます。

手順

注意

電子メールの自動送信機能を有効にする前に、電子メールパラメータを設定します。詳細については、クライアントソフトウェアのユーザーマニュアルの「メールパラメータの設定」を参照してください。

1. Time & Attendance モジュールを入力します。
2. 出席統計→の「ユーザ定義レポート」を選択します。
3. レポートを事前定義するには、追加をクリックします。
4. レポートの内容を設定します。

レポート名

レポートの名前を入力します。

レポートタイプ

1つのレポートタイプを選択すると、このレポートが生成されます。

レポート時間

選択する時間は、レポートの種類によって異なる場合があります。

人

レポートに対して出席レコードが生成される、追加された個人を選択します。

5. オプション: レポートを電子メールアドレスに自動的に送信するようにスケジュールを設定します。
   1) この機能を有効にするには、「電子メールの自動送信」をオンにします。
   2) 選択した送信日にクライアントがレポートを送信する有効期間を設定します。
   3) クライアントがレポートを送信する日付を選択します。
   4) クライアントがレポートを送信する時刻を設定します。

例

適用期間を2018年3月10日～2018年4月10日に設定し、送信日を金曜日、送信時刻を20:00:00に設定した場合、クライアントは2018年3月10日～2018年4月10日金曜日の午後8時にレポートを送信します。

注意

出席記録が送信時刻より前に計算されていることを確認してください。出席データを手動で計算することも、クライアントがデータを毎日自動的に計算できるようにスケジュールを設定することもできます。詳細については、「出席データの計算」を参照してください。

5) 受信者の電子メールアドレスを入力します。

注意

「+」をクリックして、新しいメールアドレスを追加できます。最大5 つの電子メールアドレスを使用できます。

6) オプション:プレビューをクリックして、電子メールの詳細を表示します。

6. OKをクリックします。

7. オプション:カスタムレポートを追加した後、次のいずれかを実行できます:

レポートの編集	追加したレポートを1つ選択し、編集をクリックして設定を編集します。
レポートの削除	追加したレポートを1つ選択し、削除をクリックして削除します。
レポートの生成	追加したレポートを1つ選択し、レポートをクリックすると、レポートを即座に生成し、レポートの詳細を表示できます。

7.12 リモート設定(Web)

デバイスパラメータをリモートで設定します。

7.12.1 デバイス情報を表示する

デバイス名、デバイス種別、シリアル番号、バージョン、リレー番号、ロック番号を表示/設定します。

Device for Management タブからデバイスを選択し、→ System → Device Information をクリックして、Device Information ページに入ります。

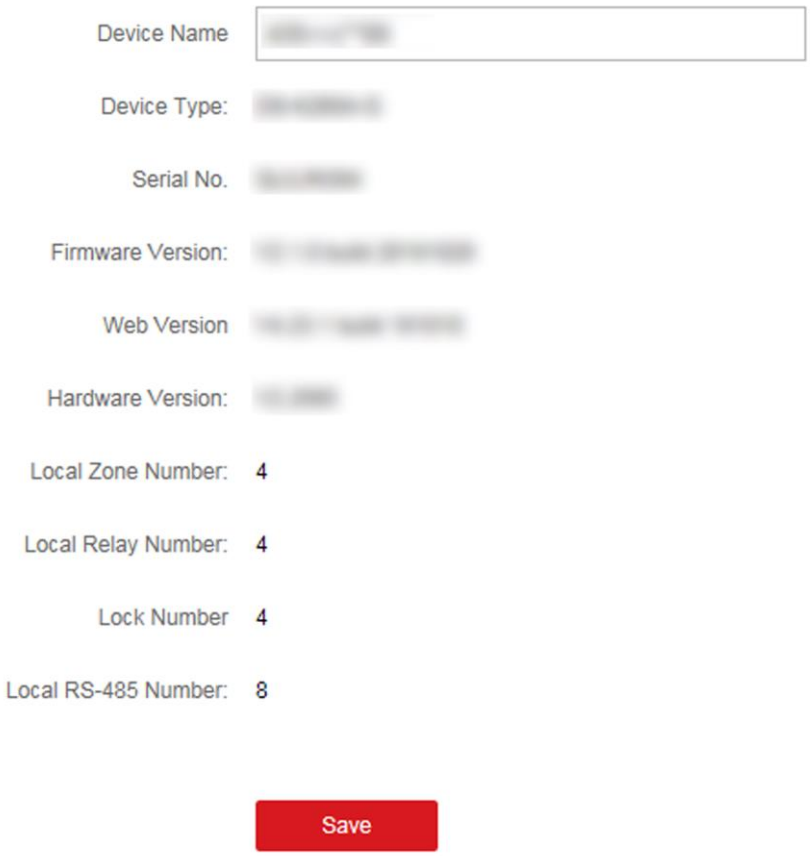


図 7-20 デバイス情報の表示

デバイス名の設定、デバイスの種類、シリアル番号、バージョン、リレー番号、ロック番号の表示ができます。保存をクリックして設定を保存します。

7.12.2 デバイスパスワードの変更

デバイスのパスワードを変更できます。

はじめる前に

デバイスがアクティブになっていることを確認します。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。

手順

1. Device for Management ページで、→ System → User をクリックして、User タブに入ります。

2. ユーザーを選択し、編集をクリックして編集ページに入ります。
3. 古いパスワードを入力し、新しいパスワードを作成して、新しいパスワードを確認します。

⚠注意

デバイスのパスワード強度を自動的に確認できます。製品のセキュリティを強化するために、独自のパスワードを変更することを強くお勧めします(大文字、小文字、数字、特殊文字の3 種類以上を含む8 文字以上を使用)。また、パスワードを定期的に変更することをお勧めします。特に高セキュリティシステムでは、パスワードを月単位または週単位で変更することで製品を保護できます。
すべてのパスワードおよびその他のセキュリティ設定を適切に構成するのは、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。

4. OKをクリックします。

結果

デバイスのパスワードが変更されます。デバイスを再接続するには、Device for Management(管理用デバイス)ページに新しいパスワードを入力する必要があります。

7.12.3 時間管理

デバイスのタイムゾーン、時刻同期、およびDST パラメータを管理します。

タイムゾーンと時刻の同期

Device for Management ページで、デバイスを選択し、→ System → Time をクリックして、Time タブに入ります。

タイムゾーンの選択、NTP パラメータの設定、または手動による時刻の同期を行うことができます。

時間帯

ドロップダウン・リストから時間帯を選択します。

NTP

デバイスはNTP と自動的に時刻を同期します。NTP を有効にした後、NTP サーバアドレス、NTP ポート、および同期間隔を設定する必要があります。

手動時刻同期

手動時刻同期を有効にした後、デバイスの時刻を手動で設定できます。
「コンピュータの時刻と同期」をオンにすると、「時刻の設定」に現在のコンピュータの時刻が表示されます。この時点で、コンピューターの時刻と同期をオフにしてをクリックすると、デバイスの時刻を手動で編集できます。

保存をクリックして設定を保存します。

DST

「管理用デバイス」ページで、「リモート設定→システム→タイム→サマータイム」を選択して、「サマータイム」タブを開きます。

DST を有効にして、DST バイアス時間、DST 開始時間、および終了時間を編集できます。

保存をクリックします。

7.12.4 System Maintenance

デバイスをリモートで再起動したり、デバイスをデフォルト設定に復元したり、設定ファイルをインポートしたり、デバイスをアップグレードしたりできます。

再起動

Device for Management ページで、→ System → System Maintenance をクリックしてSystem Maintenance タブを開きます。

Reboot(再起動)をクリックすると、デバイスの再起動が開始されます。

設定の復元

Device for Management ページで、Remote Configuration → System → System Maintenance をクリックして、System Maintenance タブを開きます。

デフォルトの復元

パラメータは、IP アドレスを除き、デフォルトのパラメータに復元されます。

設定の一部を復元

通信設定とリモートユーザー設定を除くすべての設定をお買い上げ時の状態に戻します。

すべて復元

すべてのデバイスパラメータがデフォルトのパラメータに復元されます。デバイスは、復元後にアクティブ化する必要があります。

インポートとエクスポート

Device for Management ページで、Remote Configuration → System → System Maintenance をクリックして、System Maintenance タブを開きます。

設定ファイルをインポートまたはエクスポートします。

設定ファイルのインポート

設定ファイルをローカルPC からデバイスにインポートします。

注意

設定ファイルには、デバイスパラメータが含まれます。

設定ファイルのエクスポート

設定ファイルをデバイスからローカルPC にエクスポートします。

注意

設定ファイルには、デバイスパラメータが含まれます。

アップグレード

Device for Management ページで、Remote Configuration → System → System Maintenance をクリックして、System Maintenance タブを開きます。

ドロップダウンリストからデバイスタイプを選択し、参照をクリックしてローカルコンピュータからアップグレードファイルを選択し、アップグレードをクリックします。

注意

- デバイスタイプとしてカードリーダーを選択した場合は、ドロップダウンリストからカードリーダー番号も選択する必要があります。
- アップグレードは約2 分間続きます。アップグレード中は、電源を切らないでください。アップグレード後、デバイスは自動的に再起動します。

7.12.5 RS-485 パラメータの設定

ボーレート、データビット、ストップビット、パリティの種類、通信モード、ワークモード、接続モードなどRS-485のパラメータを設定できます。

手順

1. 「保守管理→機器」を選択して、機器一覧を入力します。
2. クリックしてリモート設定ページを開きます。
3. →ユーティリティRS-485 設定をクリックして、RS-485 パラメータの設定タブに入ります。
4. ドロップダウンリストからポートのシリアルNo.を選択し、RS-485パラメータを設定します。
5. ドロップダウンリストからボーレート、データビット、ストップビット、パリティ、フロー制御、通信モード、ワーキングモード、接続モードを設定します。
6. Save をクリックすると、設定したパラメータがデバイスに自動的に適用されます。

注意

動作モードを変更すると、デバイスはリブートされます。作業モードを変更すると、プロンプトが表示されます。

7.12.6 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、→ System → Security をクリックしてセキュリティモードタブに入ります。

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。

SSH を有効にして、より安全なネットワークを取得することもできます。

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ときのユーザー情報検証のための高セキュリティレベル。

互換モード

ログイン時のユーザー情報検証は、古いクライアントソフトウェアバージョンと互換性があります。

7.12.7 ネットワークパラメータ設定

NIC タイプ、DHCP、および HTTP を含むデバイスのネットワークパラメータを設定します。

Device for Management ページで、→ Network → Network Parameters をクリックして、Network Parameters Settings タブに入ります。

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。自己適応型、10M、または 100M のいずれかを選択できます。

DHCP

この機能を無効にする場合は、デバイスの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、およびポートを手動で設定する必要があります。
この機能を有効にすると、システムはデバイスにIPv4 アドレス、IPv4 サブネットマスク、IPv4 デフォルトゲートウェイを自動的に割り当てます。

HTTP

HTTPポート、DNS1サーバアドレス、DNS2サーバアドレスを設定します。

7.12.8 レポートストラテジの設定

EHome 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。

「管理用デバイス」ページで、「ネットワーク→レポートストラテジの→」を選択して、「レポートストラテジ設定」タブに入ります。

センターグループを設定すると、EHomeプロトコル経由でログが転送されます。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。

Main Channel

デバイスは、メインチャネルを介してセンターと通信します。

注意

N1 は有線ネットワークを指します。

7.12.9 ネットワークセンターのパラメータ設定

通知監視センター、センターのIPアドレス、ポート番号、プロトコル(EHome)、EHomeアカウントのユーザー名などを設定できます。EHomeプロトコル経由でデータを送信します。

Device for Management ページで、→ Network → Network Center Parameters をクリックして、Network Center Parameters Settings タブに入ります。

ドロップダウンリストからセンターを選択します。

有効にしたあと、センターのアドレスタイプ、IPアドレス/ドメイン名、ポート番号、EHomeユーザー名などを設定できます。

保存をクリックします。

7.12.11 SIP パラメータの設定

マスタ局のIPアドレスとSIPサーバのIPアドレスを設定します。パラメータ設定後、アクセス制御装置、ドアステーション、屋内局、マスタ局、プラットフォーム間で通信ができます。

注意

アクセスコントロール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、マスタステーション、プラットフォームなど)のみが同じIP セグメントにあり、双方向オーディオを実行できます。

「保守管理→機器」を選択して、機器一覧を入力します。

クリックしてリモート設定ページを開きます。

Network → Linked Network Configuration をクリックして、マスタ局の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。

7.12.12 リレーパラメータの設定

「保守管理→機器」を選択して、機器一覧を入力します。

クリックしてリモート設定ページを開きます。

アラーム→中継を押す。リレーを選択してクリックし、リレー名と出力遅延時間を設定します。設定を保存するには、OKをクリックします。

7.12.13 アクセス制御パラメータの設定

手順

1. Device for Management ページで、→ Others → Access Control Parameters をクリックして、Access Control Parameters タブに入ります。
2. チェックボックスをオンにすると、機能が有効になります。

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。デバイスで操作しているときに、音声プロンプトが聞こえます。

キャプチャ後の画像のアップロード

この機能を有効にすると、撮影した画像がクライアントソフトウェアに送信されます。

キャプチャ画像の保存

この機能を有効にすると、撮影した画像が保存されます。

3. 保存をクリックします。

7.12.14 顔認識ターミナルのパラメータを設定する

「保守管理→機器」を選択して、機器一覧を入力します。

Ctrlキーを押しながらクリックして、リモート設定ページを開きます。

「他の→顔認識端末パラメータ」を選択すると、装置パラメータを設定できます。

フェイスピクチャーデータベース

顔写真データベースとしてDeep Learningを選択します。

顔画像を認証して保存

有効にすると、認証時にキャプチャされた顔画像がデバイスに保存されます。

CPUカード読み出し

カード番号やファイルを読み込むときに選択します。

ワークモード

デバイスのワークモードをノーマルモードに設定します。アクセスするために認証情報を認証する必要があります。

エコモード

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:N)、ECO モード(1:1)を設定できます。

エコモード(1:1)

ECO モード1:1 一致モードで認証する場合、一致しきい値を設定します。値が大きいほど、誤許可率は小さくなり、誤拒否率は大きくなります。

エコモード(1:N)

ECO モード1:N 一致モードで認証する場合、一致しきい値を設定します。値が大きいほど、誤許可率は小さくなり、誤拒否率は大きくなります。

エコモードしきい値

ECO モードを有効にすると、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。指定可能な範囲:0 ～8。

保存をクリックして設定を保存します。

7.12.15 顔画像パラメータの設定

手順

1. 「保守管理→機器」を選択して、機器一覧を入力します。
2. クリックしてリモート設定ページを開きます。
3. 「他の→顔画像パラメータ」を選択して、「顔画像パラメータの設定」ページを開きます。

ピッチ角度

顔認証時の最大ピッチ角度です。

ヤウ・アングル

顔認証時の最大ヨー角度。

余白(左)

認識エリアの顔の左側から左側の余白までの距離(%)。
顔画像認証を行う場合は、設定値よりも実際の距離の割合を大きくしてください。他のパーセンテージ、距離、および角度もそれらの条件を満たす必要があります。

余白(右)

認識エリアの顔の右側から右側の余白までの距離(%)。
顔画像認証を行う場合は、設定値よりも実際の距離の割合を大きくしてください。他のパーセンテージ、距離、および角度もそれらの条件を満たす必要があります。

余白(上)

認識エリア内の顔の上端から上端までの距離(パーセント)。
顔画像認証を行う場合は、設定値よりも実際の距離の割合を大きくしてください。他のパーセンテージ、距離、および角度もそれらの条件を満たす必要があります。

余白(下)

認識エリアの顔の下側から下側の余白までの距離(%)。
顔画像認証を行う場合は、設定値よりも実際の距離の割合を大きくしてください。他のパー

センテージ、距離、および角度もそれらの条件を満たす必要があります。

瞳孔距離

顔認識時の2人の生徒の間の最小解像度。
実際の解像度は、設定値よりも大きくする必要があります。

スコア

装置は、ヨーアングル、ピッチアングル、およびピピラー距離に応じて、取り込まれたピクチャーをスコアリングします。スコアが設定値を下回ると顔認識に失敗します。

認証時の顔画像のパラメーターを設定します。

4. 保存をクリックします。

7.12.16 補助ライトパラメータの設定

補助ライトをオンまたはオフにできます。補助光の明るさを調整することもできます。

手順

1. 「保守管理→機器」を選択して、機器一覧を入力します。
2. クリックしてリモート設定ページを開きます。
3. 「他の→補助光パラメータ」を選択して、「補助光パラメータの設定」画面を表示します。
4. ドロップダウンリストから補足ライトの種類を選択します。
5. ドロップダウンリストからサプリメントライトモードを選択します。
6. オプション:補助光の明るさを設定します。
7. 保存をクリックして設定を保存します。

7.12.17 デバイス番号設定

機器の種類、コミュニティNo.、建物No.、フロアNo.、ユニットNo.を設定し、部屋No.を設定します。

「保守管理→機器」を選択して、機器一覧を入力します。

クリックしてリモート設定ページを開きます。

「他→ No.設定」を選択し、機器種別、コミュニティNo.、建物No.、階数、ユニットNo.、No.を設定します。

7.12.18 「ビデオ」および「オーディオ」パラメータを設定する

デバイスカメラの画質、解像度、およびその他のパラメータを設定できます。

手順

1. 「保守管理→機器」を選択して、機器一覧を入力します。
2. クリックしてリモート設定ページを開きます。
3. 映像→映像と音声を選択して、設定画面に入ります。

4. ストリームタイプ、ビットレートタイプ、ビデオ品質、フレームレート、オーディオエンコーディングタイプ、ビデオタイプ、ビットレート、解像度、I フレームインターバルなど、デバイスカメラのパラメータを設定します。
5. 保存をクリックします。

7.12.19 ボリュームの入出力の構成

手順

1. Device for Managementページで、→ Image → Audio InputまたはOutputをクリックして、Audio InputまたはOutputタブに入ります。
2. ブロックを動かして、デバイスの入出力ボリュームを調整します。
3. 保存をクリックします。

7.12.20 動作リレー

手順

1. 「保守管理→機器」を選択して、機器一覧を入力します。
2. クリックしてリモート設定ページを開きます。
3. オペレーション→中継を押す。
4. リレーを有効または無効にします。

7.12.21 リレーステータスの表示

「保守管理→機器」を選択して、機器一覧を入力します。

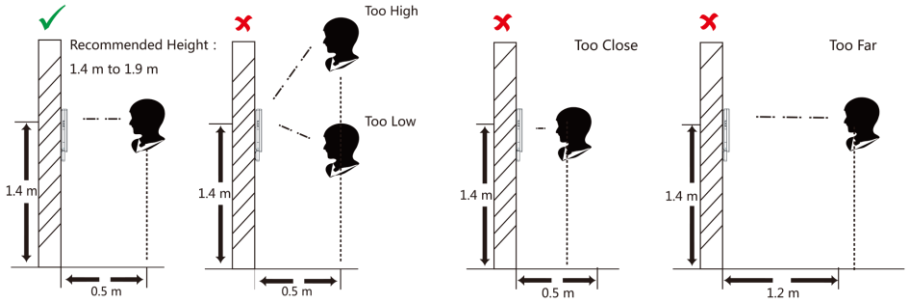
クリックしてリモート設定ページを開きます。

「状態→中継」を選択すると、中継の状態を確認できます。

A. 顔画像を取得/比較するときのヒント

顔画像の取得・比較時の位置は以下のようになります:

位置(推奨距離:0.5m)



式

- 顔画像を収集または比較するときは、下の図のように、式を自然に維持します。

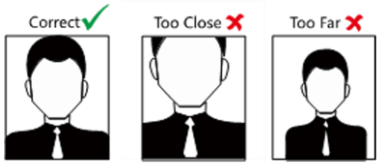
- 顔認識機能に影響を与える可能性のあるハット、サングラス、その他のアクセサリを着用しないでください。
- 目や耳などをヘアカバーで覆わないでください。重いメイクアップはできません。

姿勢

高品質で正確な顔画像を取得するには、顔画像を収集または比較するときに、カメラを見ている顔を配置します。

サイズ

顔が収集ウィンドウの中央にあることを確認します。



B. 設置環境に関するヒント

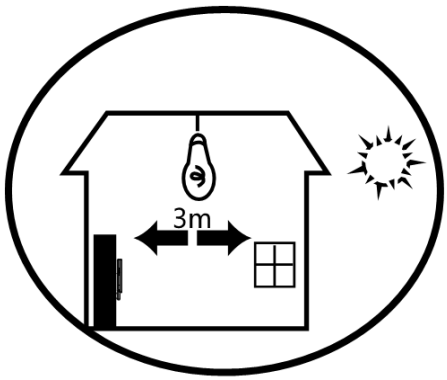
1. 光源照度基準値

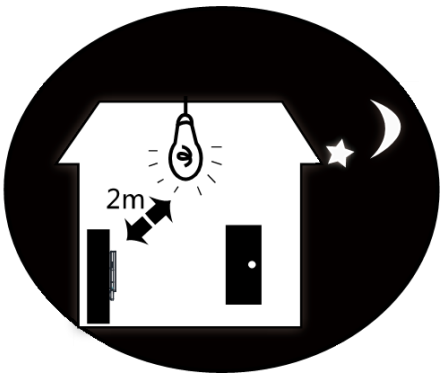
キャンドル: 10Lux

バルブ: 100～850Lux

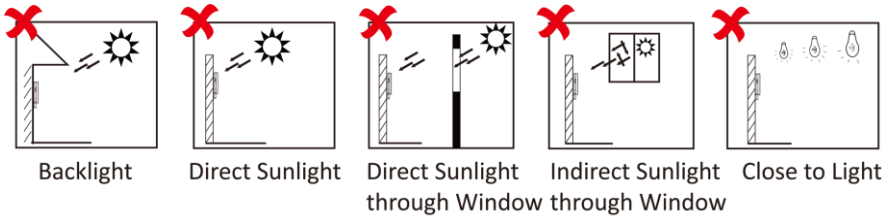
太陽光: 1200Lux 以上

2. デバイスをライトから2メートル以上離し、ウィンドウまたはドアから3メートル以上離して設置します。

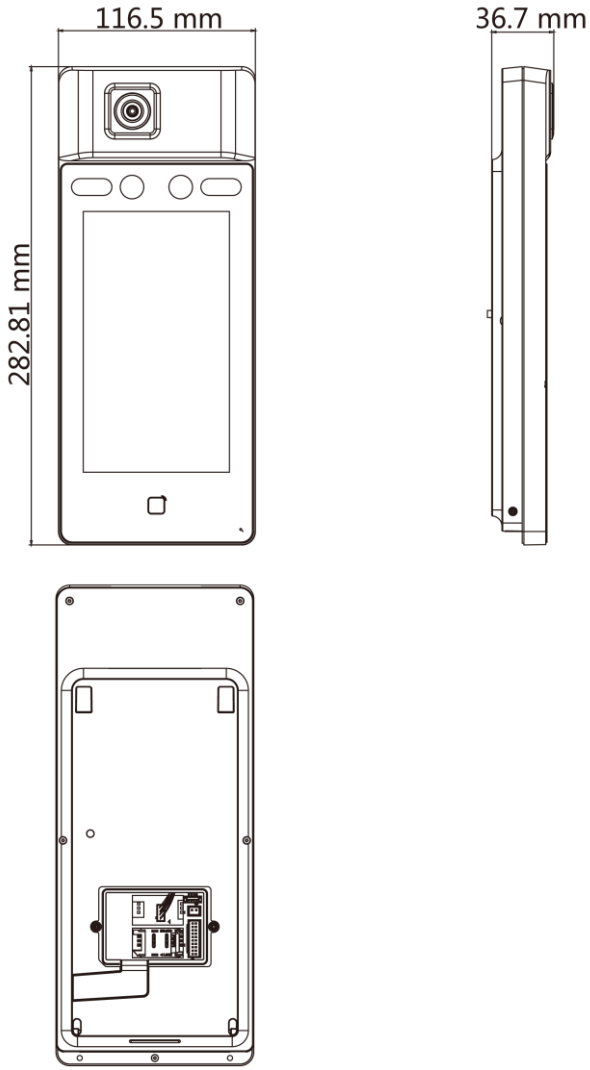




3. バックライト、直射日光、間接日光を避ける



C. 寸法



■ 製品の設置･施工･アフターサービスについてのお問い合わせ

サポートコール　**0800-111-5300**（通話料無料）

〈受付時間〉平日9:00～17:00、土･日･祝日9:00～12:00／13:00～17:00
（年末年始･夏期休業期間･会社都合による休日を除く）