顔認証アクセスコントローラーASC-F01

ユーザーマニュアル

法的情報

このドキュメントについて

- 本書には、本製品の使用方法および管理手順が記載されています。掲載されている画像、図表、説明文などの情報は、説明を目的として提供された参考情報です。
- 記載内容は、ファームウェアの更新やその他の理由により、予告なく変更される場合があります。

この製品について

- 本製品のアフターサービスサポートは、購入された国または地域においてのみ提供されます。

法的免責

- 運用される法律により認められる最大限の範囲において、本書および本製品（ハードウェア、ソフトウェア、ファームウェアを含む）は、「現状のまま」および「すべての不具合およびエラーを伴った状態」で提供されます。NSKは、明示的または黙示的ないかなる保証もいたしません。

いかなる場合においても、NSKは、本製品の仕様に関連して発生する特別、派生的、付随的、間接的損害（事業利益の喪失、事業中断、データの喪失、システムの破損、文書の損失などを含むが、これらに限定されない）について、お客様に対して責任を負いません。たとえNSKが当該損害の可能性について事前に通知されていた場合でも、契約違反、不法行為（過失を含む）、製品責任その他の根拠を問わず、責任は負わないものとします。

・お客様は、本製品をすべての運用法令に従って使用する責任を負います。また、第三者の権利（公開後、知的財産権、データ保護およびその他のプライバシー権など）を侵害しないよう、適切な方法で使用する義務があります。
・本製品は、大量破損兵器の開発・製造、化学・生物兵器の開発・製造、核爆発または安全でない核燃料サイクルに関連する活動、人権侵害の支援など、禁止されている用途には使用できません。
・本書の記載内容と適用される法律の間に矛盾がある場合には、運用法令が優先されます。

データ保護

・本製品には、設計段階からプライバシー保護原則（Privacy by Design）が組み込まれています。
例：顔認証機能搭載モデルでは、生体認証データは暗号化された形式でデバイス内部に保存
されます。
指紋認証モデルでは、保存されるのは「指紋テンプレート」のみであり、指紋画像自体を復元することはできません。

- 本製品は、データコントローラまたはデータプロセッサとして、個人データの収集、保存、使用、

処理、開示、削除などを行うことができます。
個人データの取扱いに当たっては、関連する適用法令を遵守し、適切なセキュリティ管理（合理的な管理的・物理的セキュリティ対策、定期的なレビュー、セキュリティ対策の有効性評価など）を実施することを推奨します。

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	回避しなければ、死亡または重傷につながる危険な状況を示します。
 注意	回避しなければ、機器の損傷、データ損失、パフォーマンスの低下、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	本文の重要なポイント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

適合する責任者によって明示的に承認されていない変更や修正を行うと、装置を操作するユーザーの権限が無効となる場合がありますのでご注意ください。

FCC 準拠

本装置は FCC 規則のパート15に従い、クラスBデジタル装置の制限に準拠することがテストで確認されています。これらの制限は、住宅環境における設置において、干渉を引き起こすことのないように設計されたものです。
本製品は高周波エネルギーを発生、使用、放出します。適切に設置・使用しない場合、無線通信に有害な干渉を与える可能性があります。ただし、特定の設置条件で干渉が発生しないことを保証するものではありません。

干渉が発生した場合は、次のいずれかの対策を実施することをお勧めします。

- 受信アンテナの向きを変更する、または設置場所を変える
- 本機と受信機の間隔を広げる
- 受信機が接続されている回路と異なるコンセントに本機を接続する
- 販売店または専門知識のあるラジオ/テレビ技術者に相談する

本装置は、放射体とユーザの身体の間に**最低20cmの距離**をおいて設置および操作してください。

FCC 条件

本装置は、FCC規制パート15に適合しています。運用は以下の2つの条件に基づきます。

1. 本装置が有害な干渉を引き起こさないこと。
2. このデバイスが、望ましくない動作の原因となる干渉を含め、被った妨害を受け入れる
必要があること

EU 適合性宣言

本製品および(該当する場合)付属品には「CE」マークが付いているため、欧州規格の適合規格に準拠しています。

WEEE 指令 (2012/19/EU)、EMC 2014/30/EU、RED 2014/53/EU、RoHS 2011/65/EU準拠

本製品に付されている記号は、欧州連合域内では本製品を一般廃棄物として処理できないことを示しています。
適切にリサイクルするには、同等の新しい装置を購入しつぁいに本製品を販売店へ返却するか、指定された回収場所で廃棄してください。

バッテリー指令 (2006/66/EC)

本製品には、EU内で一般廃棄物として処分できないバッテリーが含まれている場合があります。バッテリーに関する詳細は製品のマニュアルを参照してください。
バッテリーに付されている記号には、カドミウム (Cd) 、鉛 (Pb) 、水銀 (Hg) を示す文字が含まれる場合があります。
適切にリサイクルするため、使用済みバッテリー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、地域のリサイクルガイドラインを確認してください。

安全上の注意

これらの説明は、使用者が危険や所有物の損失を避けるために、製品を安全かつ正しく使用できるようにすることを目的としています。

注意事項は「危険」と「注意事項」に分かれています。
・危険: 重傷または死亡を防止するために、次の保護策に従ってください。
・注意: けがや物的損傷を防ぐために、次の注意事項に従ってください。

⚠	⚠
危険: **重傷または死亡を防止するために、** **次の保護策に従ってください。**	**注意:** **けがや物的損傷を防ぐために、次の注意事項に従ってください。**

⚠危険

- 製品の使用にあたっては、国および地域の電気安全規定に従って設置する必要があります。
- 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。
  →アダプタが過負荷になると、過熱や火災の危険があります。
- 機器から発煙・異臭・異音などが発生した場合は、直ちに電源を切り、電源ケーブルを抜いてから

サービスセンターに連絡してください。

- ソケットコンセントは容易にアクセスできる位置に設置してください。
- バッテリーを飲み込まないでください→化学的火傷の危険があります。
- 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/ボタン電池を飲み込んだ場合、わずか2時間で深刻な内蔵損傷が発生し、死亡につながる可能性があります。

→新しい電池や使用済みの電池はお子様の手の届かないところに保管してください。
→リモコンの電池カバーがしっかり閉まらない場合は、使用を中止して、
子どもの手の届かないところに保管してください。

- 電池を飲み込んだ疑いがある場合は、直ちに医師の診察を受けてください。
- **注意:** バッテリーを正しく扱わないと火災,やけど,化学的危害を引き起こす場合があります。
- 誤った種類のバッテリーを使用すると危険です。
  安全保護機能が無効になる可能性があります（例えば、リチウム電池の場合など）。
- バッテリーが破壊したり高温下で膨張したりした場合、発煙や発火の危険があります。
  直ちに使用を中止してください。
- 極端に高温の環境に放置しないでください。
  爆発や炎上の恐れがあります。
- バッテリーを極端に低圧の環境（高高度など）にさらさないでください。
  液漏れや破裂の危険があります。
- 使用済みのバッテリーは、指示に従って適切に廃棄してください。

⚠注意:

- 本製品を落としたり、衝撃を与えたり、高電磁放射にさらさないでください。
  振動のある場所や衝撃のある場所に設置することは避けてください（無視すると、装置が損傷する可能性があります）。
- デバイスを極端な高温・低温・ほこり・湿気の多い場所に置かないでください。
  詳細は製品仕様の動作温度範囲を参照してください。
  また、高電磁放射にさらさないでください。
- 本製品を直射日光やヒーター、ラジエーターなどの熱源にさらすことは禁止されています（無視すると火災の危険があります）。
- 屋内使用用のデバイスカバーは、雨水や湿気から保護します。
- 本製品を直射日光や、ヒーターやラジエーターなどの通気や熱源にさらすことは禁止されています（無視すると火災の危険があります）。
- デバイスカバーの外側を清掃する際は、アルカリ性洗浄剤を使用せず、柔らかく乾いた布を使用してください。
- 生体認証モデルは、スプーフィング対策が必要な環境には完全には対応できません。
  より高レベルのセキュリティが必要な場合は、複数の認証方式を併用してください。
- 本製品のシリアルポートは、デバッグ専用です。
- 本取扱説明書の指示に従って装置を設置してください。
  けがを防ぐため、装置は設置手順に従って床や壁にしっかりと取り付ける必要があります。
- バッテリーの不適切な使用や交換は、爆発の危険があります。同一タイプまたは同等のタイプのみ交換してください。
  使用済みバッテリーは、バッテリーメーカーの指示に従って廃棄してください。
- 本ブラケットは、装着されたデバイス専用です。
  他の機器と併用すると、けがをする可能性があります。
- 本装置は、付属のブラケットのみで使用してください。
  他のカート、スタンド、キャリアと一緒に使用すると、けがや不安定性の原因があります。

目次

内容

第1 章概要

1.1 概要

顔認識端末は、人物認証を用いたアクセス制御装置であり、主に工場，空港，大学キャンパス，警備センター，住宅施設など，各種セキュリティアクセス制御システムに適用されます。

1.2 機能

- 4.3 インチ LCD タッチスクリーン搭載、272 × 480 のスクリーン解像度、リアルタイムの検出および最大顔認識フレームを表示。
- 2 MP 広角デュアルレンズ搭載。
- 顔認証、カード、PIN コード、マルチコンビネーション認証など、複数の認証モードに対応。
- アクセス制御期間の制御（画面テンプレート）に対応し、オンデマンドでのドア開放を許可。
- ネットワーク運用に対応し、プラットフォーム経由で人員情報を発行可能。
- デバイスの比較結果や連動キャプチャ画像をリアルタイムでプラットフォームへアップロードできるデータネットワークアップロード機能に対応。
- デバイスがオフラインの場合でも、プラットフォームに再接続された際にキャッシュされたイベントが自動的にアップロードされます。
- NTP 連携および手動での時刻補正に対応。
- デバイス間のビデオインターコムをサポート。
- RTSP プロトコルを使用したリモートビデオプレビューおよび出力ビデオストリームに対応。
- ウォッチドッグガードメカニズムを内蔵し、デバイスが適切に動作するよう設計。
- 通常モードのリマインダー機能を含むマスク検出モードに対応し、マスクモードの有効化は任意。
- IP65 に準拠した防塵・防水性能。
- 標準の PoE による電源供給に対応し、同時にドアロック用電源（DC12V/1A）を供給可能。

第 2 章外観

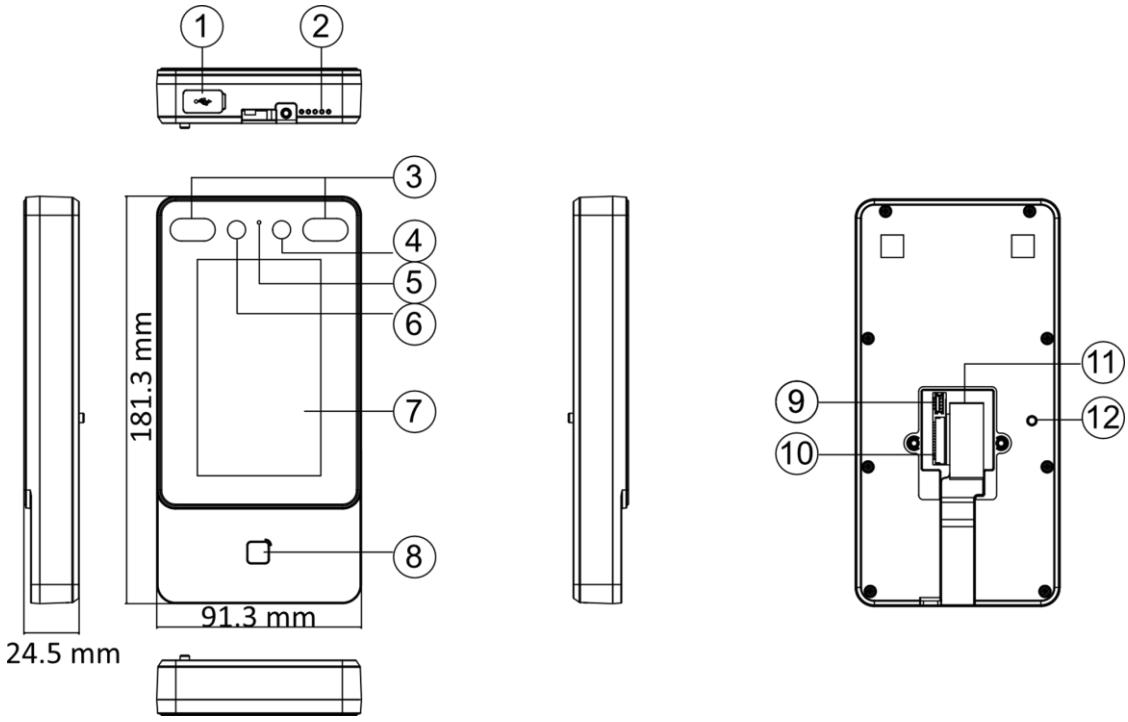


図2-2 指紋モジュールなし

表2-2 外観の説明

番号	名前
1	USB　インターフェイス
2	スピーカー
3	IR ライト
4	カメラ
5	MIC
6	カメラ
7	タッチスクリーン
8	カード提示領域
9	デバッグポート(デバッグ専用)
10	配線端子
11	ネットワークインタフェース
12	タンパー

第3章配線

アクセスコントローラーは、RS-485カードリーダ・ドアロック・ボタン・Wiegandデバイスなどの周辺機器と接続できます。
接続後、認証結果をドアロックへ制御信号として出力したり、アクセス情報をコントローラーへ送信することができます。

注意

- ケーブルサイズが18 AWG の場合、電源から端末までの距離は **20m以内**を推奨します。
- ケーブルサイズが15 AWG の場合、距離は 30m以内 を推奨します。
- ケーブルサイズが12 AWG の場合、距離は 40m以内 を推奨します。
- 外部カードリーダ、ドアロック、ボタン、またはアダプタ接続には個別の電源が必要な場合があります。

1.1 端末の説明

端子には以下の種類があります:

・電源入力

・RS-485通信

・Wiegand出力

・ドアロック制御

各端子の詳細は表 4-1を参照してください。

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	RS-485	黄	485+	RS-485 配線
	B2		青	485-	
	B3		黒	GND	グランド
グループC	C1	Wiegand Data0	緑	W0	Wiegandデータ0（入力/出力）

グループ	番号	機能	色	名前	説明
	C2	Wiegand Data1	白	W1	Wiegand データ1（入力/出力）
	C3	Wiegand GND	黒	GND	Wiegand グランド
グループD	D1	ドアロックNC	白/紫	NC	ロック制御(NC)
	D2	ドアロック共通	白/黄	COM	ロック制御共通端子
	D3	ドアロックNO	白/赤	NO	ロック制御(NO)
	D4	ドアセンサー入力	黄/緑	センサ	ドアステータス検出
	D5	センサーGND	黒	GND	センサー用グランド
	D6	EXITボタン入力	黄色/グレー	EXIT	出口ボタン信号入力

1.2 ワイヤノーマルデバイス

一般的な周辺機器（カードリーダー、EXITボタン、ドアセンサーなど)を接続できます。

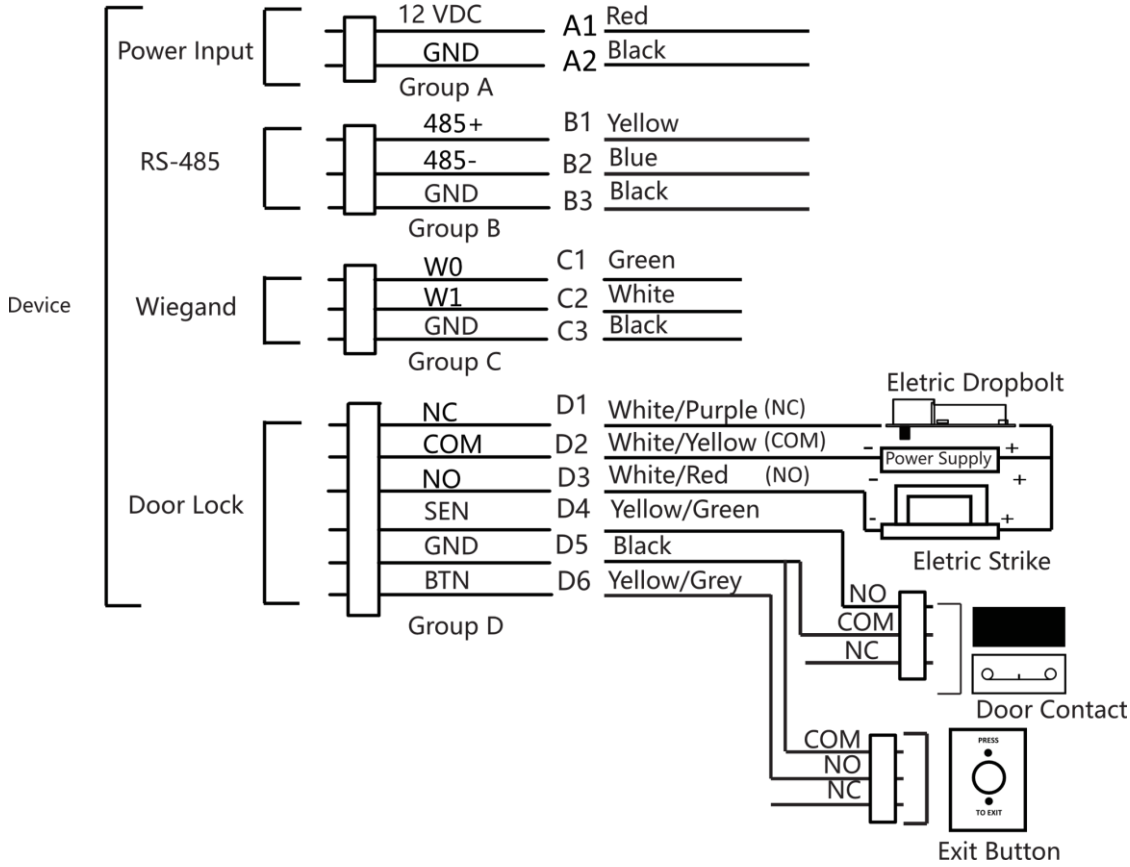


図4-1 機器の配線図

注意

- 顔認証端末からWiegand方向を Inputに設定し、外部カードリーダーに接続する必要があります。
- アクセスコントローラーに情報を送信する場合はOutputに設定してください。
- Wiegand の設定は「Wiegand Parameters」メニューで行います。
- 配線後、装置裏面の表示と端子位置をよく確認してください。

1.3 ワイヤ安全ドア制御ユニット

安全なドアコントロールユニットを使用することで、より安全に端

子を接続できます。

結線図は以下を参照してください。

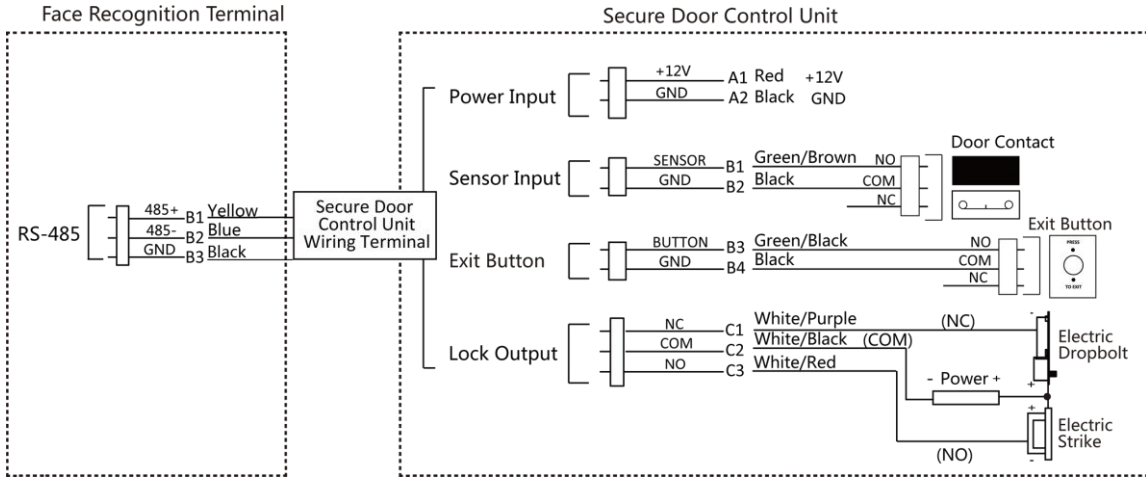


図4-2 安全ドアコントロールユニットの配線

注意

・安全ドア制御ユニットは外部電源（12V・0.5A以上）に接続してください。

・必要に応じて、ロック制御、EXITボタン、ドアセンサーとの配線を確認してください。

1.4 ワイヤファイアモジュール

1.4.1 火災時のドア開放（Fail-Safe）配線例

ロックタイプ:

・アノードロック（Fail Safe：無痛電で解錠）

・電気ロック(NO)

・電磁ロック(NO)

・ Fire Engine Access に対応

タイプ1

注意

火災時（火災検知器による信号入力時)に、ドアを自動で開放させるための配線です。

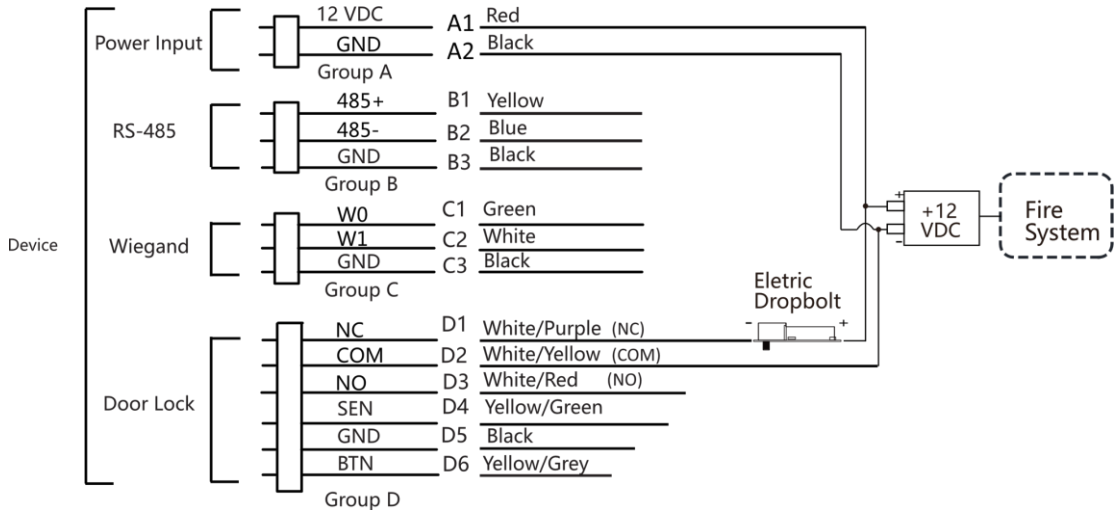


図4-3 ワイヤデバイス

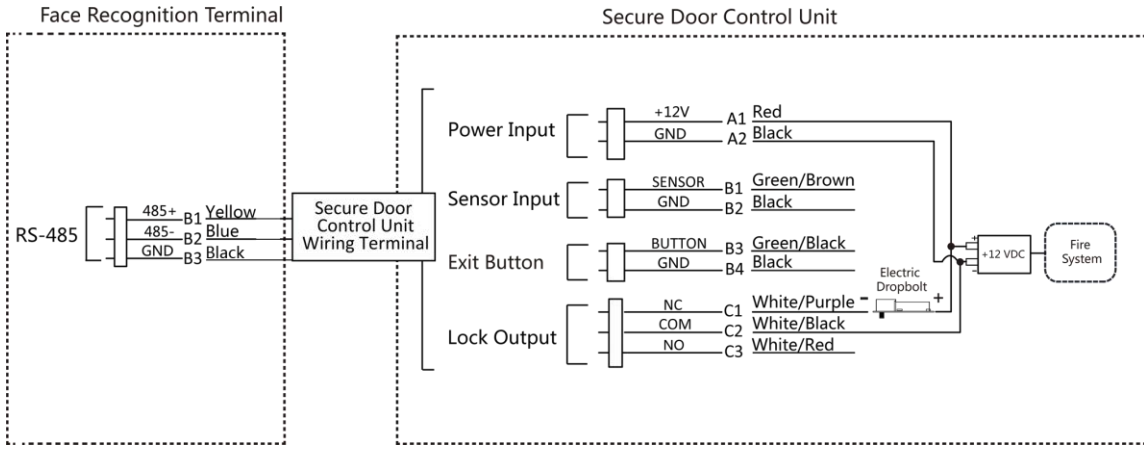


図4-4 ワイヤセキュア・ドア・コントロール・ユニット

タイプ2

注意

・火災システム（NO及びCOM、電源オフ時ノーマルオープン)は、ロックと電源が直列に接続されます。

・火災アラームが作動するとNOとCOMが解放され、ロックが改造状態になります。

・通常時はNOとCOMが閉じた状態です。(ロックは通電状態)

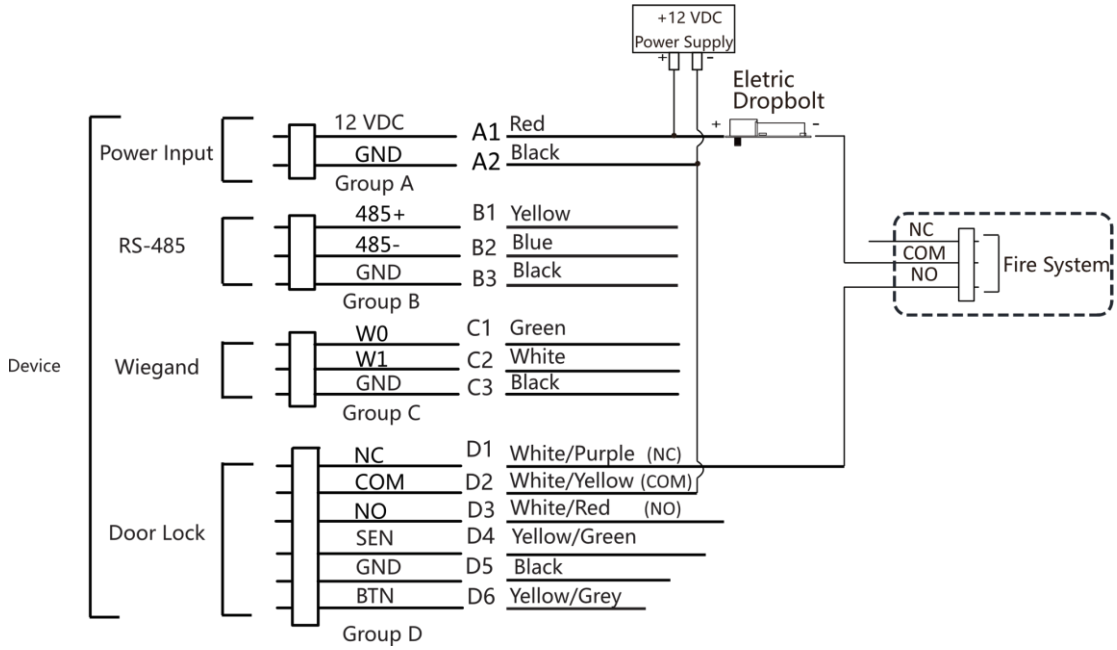


図4-5 配線デバイス

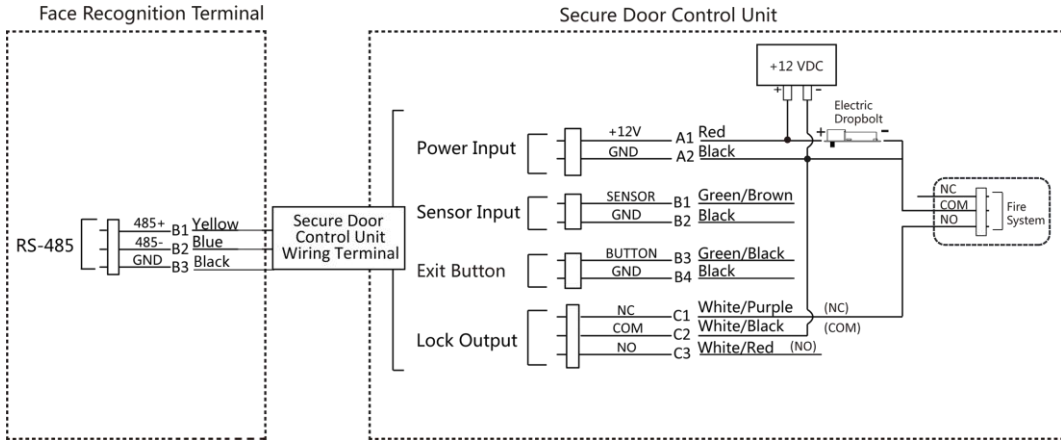


図4-6 セキュア・ドア制御ユニットの配線

1.4.2 電源断時ドアロック (Fail-Secure)の配線図

この構成では、電源が遮断された場合にドアが施錠状態を維持 (Fail Secure)します。

■運用ロックタイプ

・カードロック
・電磁ロック (NO)
・電気ボルト (NC)

■運用シナリオ

・Fire Linkageによる遠隔制御
・セキュリティ重視のエリア(停電時にドアを開放させない必要がある場所)

注意

- UPS（無停電電源装置）の併用を推奨します。

電源断時にドアロックがほぞされるため、安全運用に必要です。

- 火災システム(NCおよびCOM)は、ロックと電源が直列に接続される構成です。

火災アラームが動作すると、
→NOとCOMが開き、ロック制御が解除され、ドアが開いたままになります。
平常時はNOとCOMが閉状態（ロック通電)です。

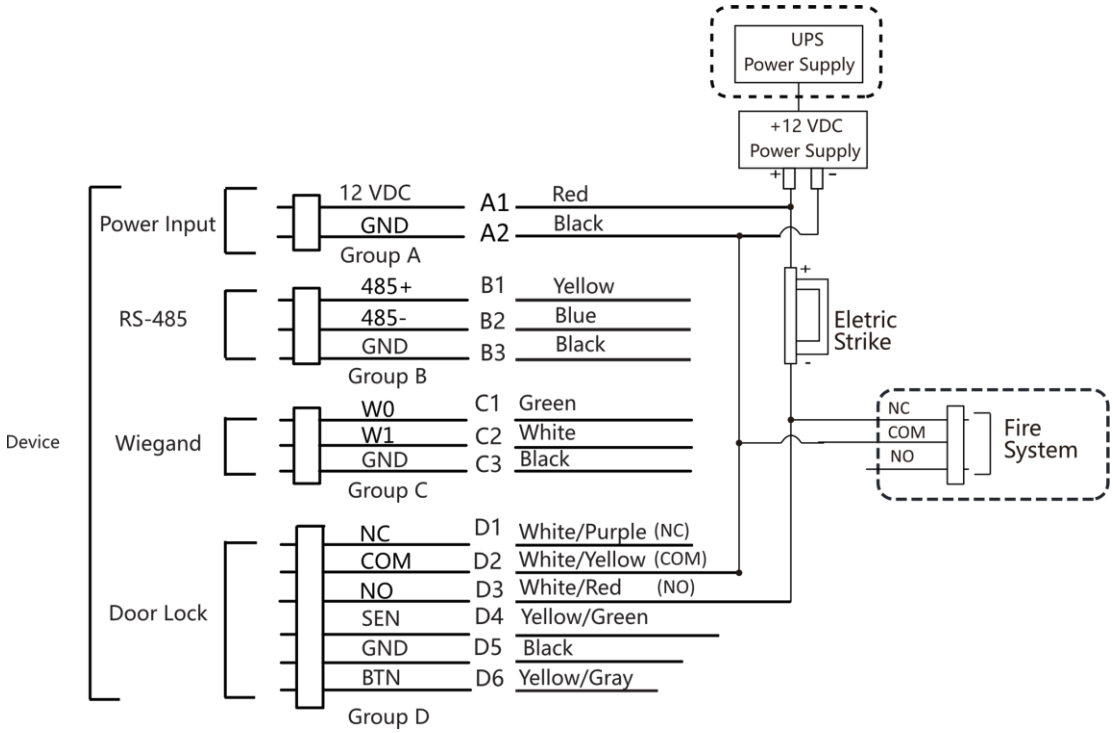


図4-7 デバイスの配線

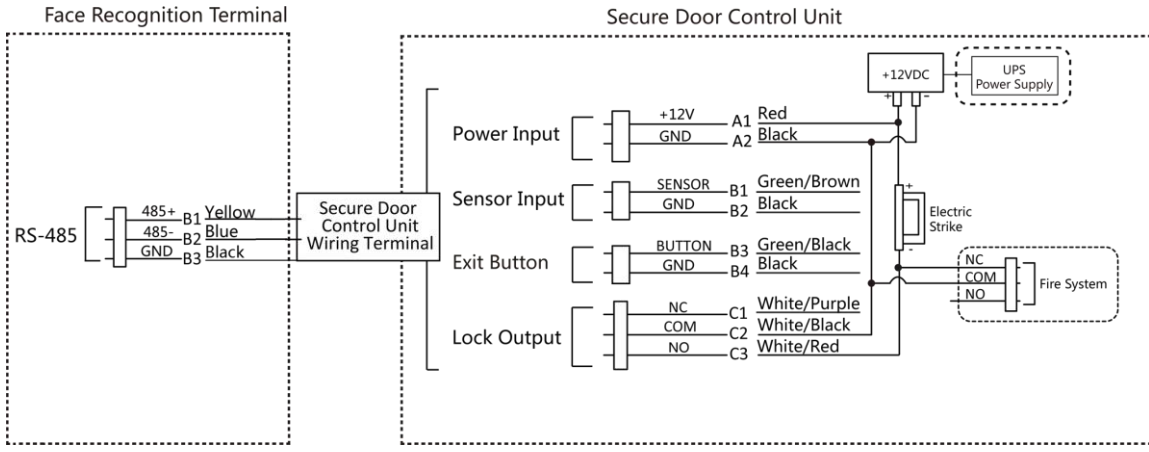


図4-8 配線図

第5 章アクティベーション

最初にデバイスを使用する前に、アクティベーション（初期有効化）を行う必要があります。
デバイスの電源投入後、システムは自動的にアクティベーションページへ切り替わります。
デバイス本体、SADPツール、およびクライアントソフトウェアを使用してアクティベーションを実行できます。

初期状態でのデフォルト設定は以下のとおりです。

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

1.1 デバイスから直接アクティブ化

デバイスが未アクティブの場合は、電源投入後に表示される Activate Device 画面からアクティベーションを行います。

手順

1. パスワードを作成します (8～16文字)
2. 確認用パスワードを入力します。
3. Activateをタップします。
   パスワードが正しく設定されると、デバイスがアクティブ化され、初期設定の続きを行えます。

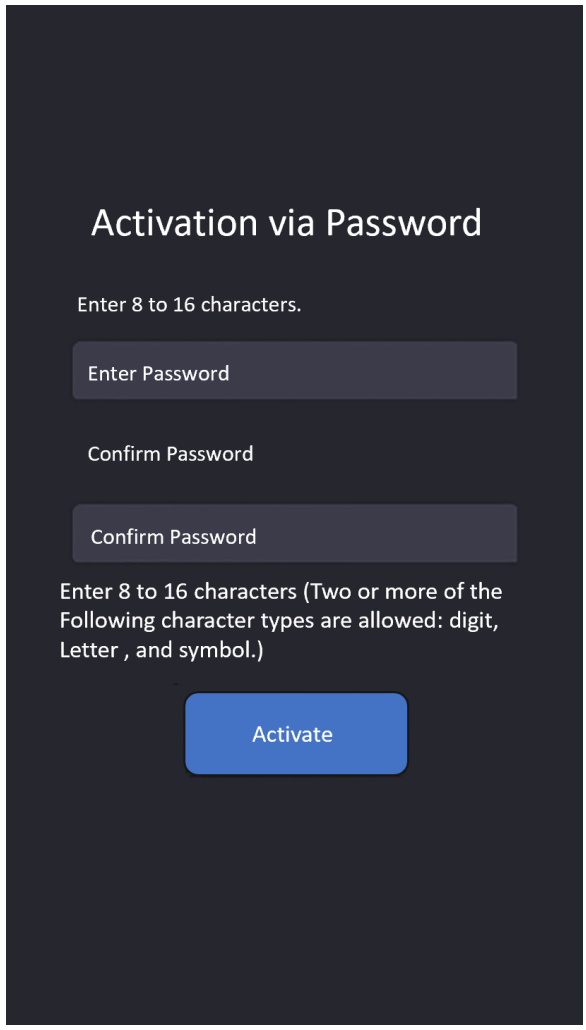


図5-1 アクティベーションページ

注意

・デバイスのパスワード強度はシステムが自動的に確認します。
・セキュリティ保護のため、初期設定後はパスワードを必ず変更することを推奨します。
・パスワードは8文字以上、数字・英字・記号のうち2種類以上の組み合わせ使用してください。

製品の安全性を高めるため：

大文字・小文字・数字・特殊文字の3種類以上を組み合わせたパスワードを使用してください。
また、パスワードを定期的に変更することも強く推奨します。
特に高セキュリティ環境では、パスワードを月次または運用ポリシーに従って変更してください。
すべてのパスワードおよびその他のセキュリティ設定の適切な管理は、インストーラまたはエンドユーザーの責任です。

・ デバイスのパスワード強度は自動的に判定されます。
・製品のセキュリティを高めるために、独自で選択するパスワードを推奨します（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）。
・パスワードは定期的に変更してください。特にセキュリティ要求の高い環境では、月次または定められた運用ルールに従って変更してください。
・すべてのパスワードおよびその他のセキュリティ設定の適切な管理は、サービスプロバイダおよび／またはエンドユーザーの責任です。
・「ユーザー名」「123」「admin」等、推測されやすいパスワードは使用しないでください。また、4 文字以下の短いパスワードや単語の連続は避けてください。

- アクティベーション後、実際のユースに応じて言語設定が必要となる場合があります。
- アクティベーション後、アプリケーション設定を行う場合があります。
  詳細は別途参照してください。
    - アクティベーション後、ネットワーク設定が必要となる場合があります。
      詳細は、通信パラメータ (Link)の設定をご覧ください。
    - アクティベーション後、デバイスをプラットフォームに追加できます。
      詳細はプラットフォーム(Link)への接続を参照してください。
    - 接続先の環境に応じて、プライバシー設定の変更が必要となる場合があります。
      詳細はプライバシー (Link)をご覧ください。
    - アクティベーション後、デバイスパラメータを管理するために、管理者を追加する必要がある場合は Administrator (Link)の追加を参照してください。

1.2 Web ブラウザ経由でアクティブ化

Web ブラウザからデバイスをアクティベートできます。

手順

1. Webブラウザのアドレスバーにデバイスのデフォルトip アドレス(192.0.0.64)を入力し、Enterを押します

注意

デバイスのIP アドレスとコンピュータのIP セグメントが同じであることを確認します。

2. 新しいパスワード(admin password)を入力し、確認します。

注意

- デバイスのパスワード強度は自動的に確認できます。
  製品のセキュリティを高めるために、独自に選択する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、パスワードを月次または週次で変更すると、製品をより適切に保護できます。
- すべてのパスワードおよびその他のセキュリティ設定の適切な設定は、サービスプロバイダおよび/またはエンドユーザの責任です。
- パスワードには、ユーザー名、123、admin (大文字と小文字の区別あり)、4 桁以上の連続した増減、または4 文字以上の連続した繰り返しを使用しないでください。
- パスワードには、NSK (大文字と小文字を区別しません) などの単語を含めることはできません。

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

1.3 Guarding Vision ソフトウェア経由でのデバイスのアクティブ化

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

注意

この機能はデバイスでサポートされている必要があります。

1. デバイス管理ページに入ります。
2. Device Management の右側をクリックし、Device を選択します。
3. オンラインデバイスがリストに表示されます。
4. デバイスのステータス(「セキュリティレベル」列に表示)を確認し、アクティブでないデバイスを選択します。

5. [アクティブ化（Activate）]をクリックし、アクティブ化（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、確認入力します。

注意

・デバイスのパスワード強度は自動的に判定されます。
・製品のセキュリティを高めるため、
・**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** の
パスワードを設定することを推奨します。
・パスワードは定期的に変更してください。
特に高セキュリティ環境では、**月次または週次での変更**が推奨されます。

注意

・すべてのパスワードおよびセキュリティ設定の適切な管理は、
インストーラまたはエンドユーザーの責任です。

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

7. [OK]をクリックして、デバイスをアクティブ化します。

第6章クイック操作

6.1 言語の選択

デバイスシステムの言語を選択できます。
デバイスのアクティベーション後、任意のシステム言語を選択できます。

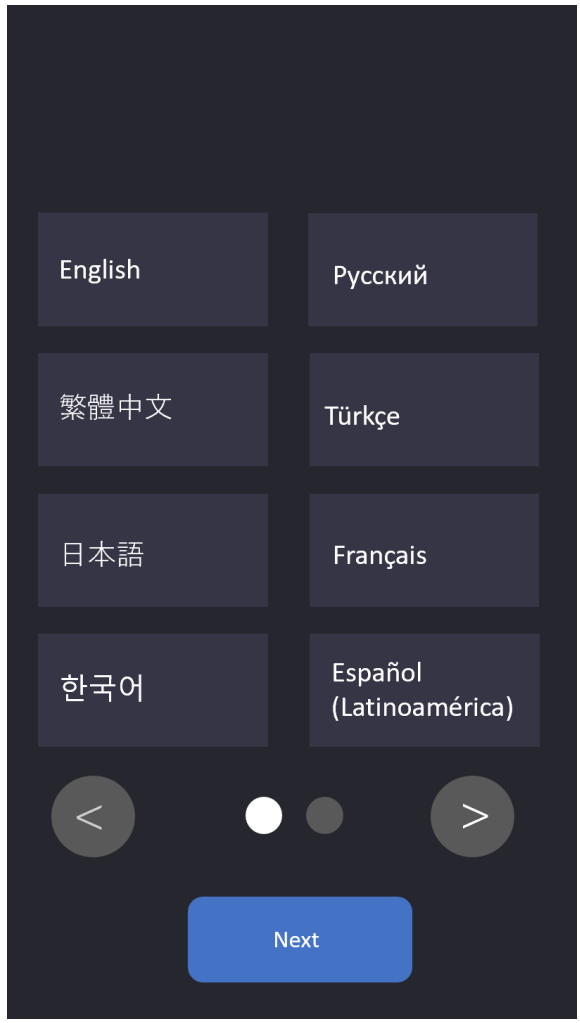


図6-1 システム言語の選択

デフォルトでは、システム言語は英語です。

注意

システム言語を変更すると、次ページから設定した言語へと変更されます。

6.2 パスワード変更タイプの設定

デバイスをアクティブ化した後、パスワード変更タイプをあらかじめ登録された **電子メールアドレス** または **セキュリティ質問** のいずれか、または両方で設定できます。デバイスのパスワードを忘れた場合、選択した変更タイプを使用してパスワードを再設定できます。

電子メールアドレスによるパスワードの変更

あらかじめパスワード変更を行う必要がある場合は、メールアドレスを入力し、
[**次へ**] をタップします。

セキュリティ質問による変更

セキュリティに関する質問でパスワードを変更する必要がある場合は、
質問に回答する形式で設定できます。

1. セキュリティ質問を選択します。
2. 回答を入力します。
3. [次へ] をタップします。

注意

・パスワード変更タイプは **1つのみ** でも **両方** でも設定できます。
・必要に応じて、Web ページから両方の設定が可能です。

6.3 ネットワークパラメータの設定

アクティベーション後、アプリケーションモードを選択すると、
デバイスのネットワーク設定を行うことができます。

手順

注意

デバイスモデルの一部は Wi-Fi 機能に対応していない場合があります。
対応状況は実際のデバイス仕様をご確認ください。

1. [Select Network（ネットワークの選択）]ページに入ったら、使用環境に合わせて
[Wired Network（有線ネットワーク）]または[Wi-Fi]をタップします。

図6-2 ネットワークの選択

注意

有線ネットワークを使用している場合は、Wi-Fi に接続する前に **有線ネットワークを切断** してください。

次へをタップします。有線ネットワーク

注意

1. Wi-Fi を選択し、Wi-Fi のパスワードを入力して接続します。
2. または、[Wi-Fi を追加] をタップし、Wi-FiのSSIDとパスワード入力して接続します。
3. 必要に応じて、[スキップ] をタップしてネットワーク設定をスキップできます。

6.4 プラットフォームへのアクセス

機能を有効にすると、デバイスは Guarding Vision を介して通信できます。
デバイスを Guarding Vision モバイルクライアントや PC クライアントに追加することができます。

図6-3 GuardingVision へのアクセス

1. 次へをタップします。

注意

- Wi-Fi 設定ページに戻った場合は、接続した Wi-Fi を再度タップするか、別の Wi-Fi を選択してプラットフォームページに戻り、再度設定する必要があります。

6.5 プライバシー設定

アクティベーション、アプリケーションモードの選択、ネットワーク設定の完了後、
画像のアップロード方法や保存方式など、プライバシーに関するパラメータを設定する必要があります。

実際の運用環境に応じて、以下の項目から設定を選択します。

キャプチャした画像のアップロード(認証時にキャプチャした画像をアップロードする場合)

プラットフォームへの認証時にキャプチャされた画像を自動的にアップロードします。

キャプチャ画像の保存(認証時にキャプチャした画像を保存)

この機能を有効にすると、機器への認証時に画像を保存できます。

登録した画像を保存します(登録画像保存)

登録した顔写真は、機能を有効にするとシステムに保存されます。

Picureのアップロード (リンクキャプチャ後(リンクキャプチャ後に画像をアップロード)

リンクカメラで撮影した画像を自動的にプラットフォームにアップロードします。

画像保存連動キャプチャ後(連動キャプチャ後の画像を保存)

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。

キャプチャした画像のアップロード(通話中)

通話中に撮影した画像を自動的にプラットフォームにアップロードします。

「次へ」をタップして設定を完了します。

6.6 管理者設定

デバイスのアクティベーション後、管理者を追加してデバイスパラメータを管理できます。

はじめる前に

デバイスをアクティブにし、アプリケーションモードを選択します。

手順

1. 必要に応じて、管理者の追加をスキップするには、「スキップ」をタップします。
2. 管理者の名前(オプション)を入力し、次へをタップします。

図6-4管理者追加 ページ

3.追加する認証情報を選択します。

注意

最大 1つ の認証情報を追加する必要があります。

– : カメラを前に向けます。
顔認識領域に顔があることを確認します。クリックしてキャプチャし、クリックして確定します。
- : デバイス画面の指示に従って指を押します。クリックして確定します。
: カード提示部にカード番号または現在のカードを入力します。OKをクリックします。

4. OKをクリックします。

認証ページに入ります。

ステータスアイコン説明:

→端末はプラットフォームに接続していない

(Guarding Vision)

／
GuardingVision は有効/無効です。

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

／ ／
デバイスのWi-Fi が有効で、接続されているか/接続されていないか/有効ですが、接続されていません。

ショートカットキー説明

注意

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

- デバイスルーム番号を入力し、OK をタップして発信します。
- タップしてセンターに電話します。

注

センターにデバイスを追加する必要があります。
そうしないと、発信操作が失敗します。

PINコードを入力して認証します。

第7章基本操作

7.1 ログイン

デバイスにログインして、デバイス基本パラメータを設定します。

7.1.1 管理者によるログイン

デバイスの管理者を追加した場合は、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 秒間ロングタップし、ジェスチャに従って左右にスライドして管理者ログインページに入ります。

図7-1 管理者ログイン

2. 管理者の顔、指紋、またはカードを認証してホームページに入ります。

図7-2 ホームページ

注意

指紋またはカードの入力に5回失敗すると、デバイスは30分間ロックされます。

3. タップログイン用のデバイスアクティベーションパスワードを入力できます。
4. をタップすると、管理者ログインページを終了できます。

7.1.2 アクティベーションパスワードによるログイン

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

手順

1. 最初のページを3 秒間ロングタップし、ジェスチャに従って左右にスライドしてパスワード入力ページに入ります。
2. パスワードを入力します。
   - デバイスの管理者を追加した場合は、をタップしてパスワードを入力します。
   - デバイスの管理者を追加していない場合は、パスワードを入力します。
3. 「OK」をタップしてホームページに入ります。

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。

図7-3 ホームページ

7.1.3 パスワード忘れ

認証時にパスワードを忘れた場合は、パスワードを変更できます。

手順

1. 最初のページを3 秒間保持し、ジェスチャに従って左/右にスライドし、ページにログインします。
2. (オプション) 管理者を設定している場合は、ポップアップの管理者認証ページで をタップします。
3. 「パスワードを忘れたとき」をタップします。
4. リストからパスワード変更タイプを選択します。

注

パスワード変更タイプを 1 つしか設定していない場合は、対応するパスワード変更ページに移動して詳細設定を行います。

5. セキュリティに関する質問に答えるか、電子メールアドレスに従ってパスワードを変更します。
   - セキュリティに関する質問:アクティベーション時に設定したセキュリティに関する質問に答えます。
   - 電子メールアドレス

注

デバイスがGuardingVision アカウントに追加されていることを確認します。

a. GuardingVisionアプリをダウンロードします。
b. その他→デバイスパスワードのリセットに移動します。
c. 機器のQRコードを読み取ると、確認コードがポップアップ表示されます。

注

QRコードをタップすると画像が大きくなります。

d. デバイスページで確認コードを入力します。

6. 新しいパスワードを作成して確認します。
7. OKをタップします。

7.2 通信設定

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

7.2.1 有線ネットワークパラメータの設定

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

手順

1. システム設定→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、有線ネットワークをタップします。

3. IPアドレス、サブネットマスク、ゲートウェイを設定します。
- DHCP を有効にすると、IP アドレス、サブネットマスク、ゲートウェイが自動的に割り当てられます。
- DHCP を無効にします。
  IP アドレス、サブネットマスク、ゲートウェイを手動で設定する必要があります。

注意

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

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

7.2.2 Wi-Fi パラメータの設定

Wi-Fi 機能を有効にし、Wi-Fi 関連のパラメータを設定できます。

手順

注

この機能はデバイスでサポートされている必要があります。

1. システム設定→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. 通信設定ページでをタップします。

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

注

パスワードには、数字、文字、および特殊文字のみを使用できます。

5. Wi-Fi のパラメータを設定します。
- デフォルトでは、DHCP は有効です。
  IP アドレス、サブネットマスク、ゲートウェイが自動的に割り当てられます。
- DHCP を無効にする場合は、IP アドレス、サブネットマスク、ゲートウェイを手動で入力する必要があります。
6. OK をタップして設定を保存し、Wi-Fi タブに戻ります。
7. をタップしてネットワークパラメータを保存します。

7.2.3 RS-485パラメータの設定

顔認識端子は、RS-485端子経由で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、カードリーダを接続することができます。

手順

1. システム設定→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。

3. 実際のニーズに応じて、周辺機器のタイプを選択します。

注意

「Access Controller」を選択した場合: 機器をRS-485 インターフェース経由でターミナルに接続する場合、RS-485 アドレスを2 に設定します。

機器をコントローラに接続する場合は、ドアNo.に合わせてRS-485アドレスを設定してください。

4. 左上隅にある戻るアイコンをタップすると、パラメータを変更した場合にデバイスを再起動する必要があります。

7.2.4 Wiegand パラメータの設定

Wiegand の送信方向を設定します。

手順

1. システム設定→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。

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

注
外付けデバイスを変更した場合、デバイスパラメータを保存すると、デバイスは自動的に再起動します。

7.2.5 ISUP パラメータの設定

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

はじめる前に
デバイスがネットワークに接続されていることを確認します。

手順
1. システム設定→通信をタップします→ ホームページのISUP (通信設定)で設定ページに入ります。

2.ISUP 機能を有効にし、ISUP サーバーのパラメータを設定します。

ISUPバージョン

実際のニーズに合わせてISUP のバージョンを設定します。

セントラルグループ

中央グループを有効にすると、データがセンターグループにアップロードされます。

メインチャンネル

N1 またはNone をサポートします。

ISUP

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

アドレスタイプ

実際のニーズに応じてアドレスタイプを選択します。

IP アドレス

ISUP サーバーのIP アドレスを設定します。

ポート番号

ISUPサーバのポート番号を設定します。

注

ポート番号の範囲:0～65535

デバイスID

デバイスシリアル番号設定

パスワード

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

注

- ISUP アカウントとISUP キーを覚えておいてください。
  デバイスがISUP プロトコルを介して他のプラットフォームと通信する必要がある場合は、アカウント名またはキーを入力する必要があります。
- ISUP キーの範囲:8 ～32 文字。

7.2.6 プラットフォームアクセス

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

はじめる前に

デバイスがネットワークに接続されていることを確認します。

手順

1. システム設定→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、GuardingVision へのアクセスをタップします。
3. GuardingVision へのアクセスの有効化
4. サーバーIP を入力します。
5. 検証コードを作成し、GuardingVision でデバイスを管理するときに検証コードを入力する必要があります。

7.2.7 SNMP 設定

SNMP パラメータを設定できます。

手順

1. システム設定→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、SNMP をタップします。
3. SNMP を有効にします。
4. トラップコミュニティ文字列を設定します。
5. NMS IP アドレスとNMS ポートを設定します。

7.3 ユーザ管理

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

7.3.1 管理者の追加

管理者は、デバイスバックエンドにログインして、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、バックエンドにログインします。
2. 「ユーザー」→「+」をタップして、「ユーザーの追加」ページに入ります。

3. ユーザーID を編集します。

注

- ユーザー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、数字の組み合わせも可能です。
- 従業員ID は重複しないようにしてください。

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

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。
- ユーザー名には32 文字まで使用できます。

5.必要に応じて、管理者用の顔写真、指紋、カード、またはピンを追加します。

注意

- 顔画像の追加について詳しくは、顔Pictureの追加を参照してください。

注意

フィンガープリントの追加について詳しくは、Fingerprint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。
- パスワードの追加について詳しくは、PINの追加を参照してください。

6.オプション: 管理者の認証タイプを設定します。

注意

認証種別の設定については、認証Mode (Link)の設定を参照してください。

7.「個人種別」と「個人ロール」を設定します。

8.管理者権限機能を有効にします。

管理者権限の有効化

ユーザーは管理者です。

通常の出席機能を除き、ユーザーは、許可を認証した後に操作するためにホームページに入ることもできます。

9.「出席確認のみ」を有効にすることができます。

有効にすると、この人にアクセス制御権限は付与されません。

10. タップして設定を保存します。

7.3.2 顔写真を追加

ユーザーの顔画像をデバイスに追加します。

また、ユーザーは顔画像を使用して認証することができます。

手順

注意

顔画像は最大1500件まで追加できます。

1.最初のページを3 秒間ロングタップし、ジェスチャに従って左右にスライドし、バックエンドにログインします。

2.「ユーザー」→「+」をタップして、「ユーザーの追加」ページに入ります。

3.従業員ID を編集します。

注

- 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、数字の組み合わせも可能です。
- 従業員ID は重複しないようにしてください。

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

注

- 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。
- 推奨されるユーザー名は32 文字以内にする必要があります。

5. 顔写真欄をタップすると、顔写真追加ページに入ります。

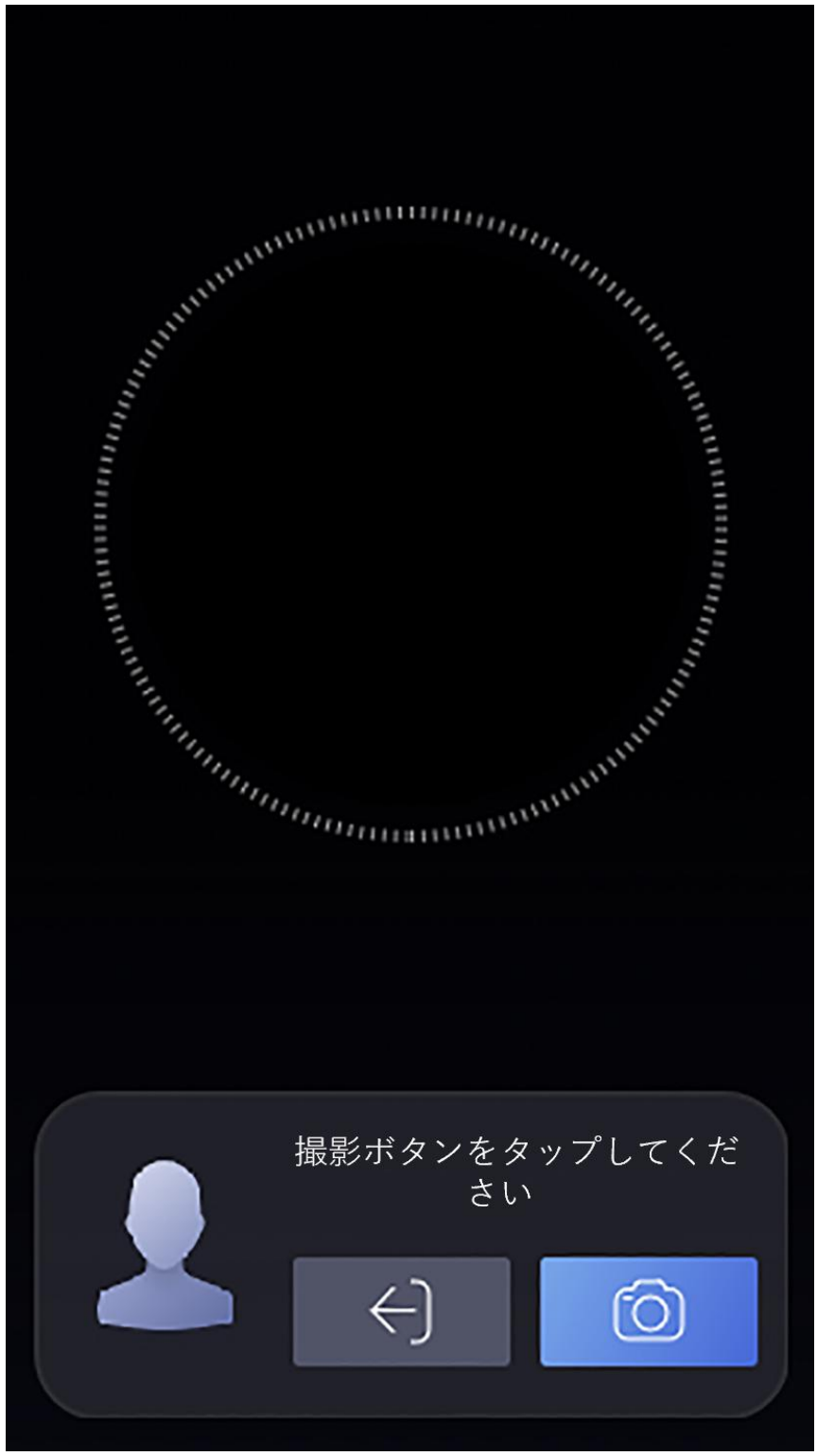


図7-9 顔画像の追加

- カメラを見てください。

注意

- 顔画像を追加するときは、顔画像が顔画像の輪郭にあることを確認します。
- キャプチャされた顔画像の品質が良好で、正確であることを確認します。
- 顔画像の追加方法について詳しくは、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。

顔画像を完全に追加すると、キャプチャされた顔画像がページの右上隅に表示されます。

6.「保存」をタップして顔写真を保存します。

7.必要に応じて、「再試行」をタップし、顔の位置を調整して顔の画像を再度追加します。

8.ユーザーロールを設定します。

管理者

ユーザーは管理者です。

通常の出席機能を除き、ユーザーは、許可を認証した後に操作するためにホームページに入ることもできます。

一般ユーザ

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。

7.3.3 カードの追加

ユーザー用のカードを追加し、ユーザーは追加したカードを介して認証できます。

手順

注

最大3000枚のカードを追加できます。

1.最初のページを3 秒間ロングタップし、ジェスチャに従って左右にスライドし、バックエンドにログインします。

2.「ユーザー」→「+」をタップして、「ユーザーの追加」ページに入ります。

3.配線図に従って外付けカードリーダを接続します。

4.「従業員ID」フィールドをタップし、従業員ID を編集します。

注

- 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、数字の組み合わせも可能です。
- 従業員ID は重複しないようにしてください。

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

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。
- 推奨されるユーザー名は32 文字以内にする必要があります。

6.「カード」欄をタップし、+をタップします。
7.カード番号を設定します。
- カード番号を手動で入力します。
- カードプレゼンテーションエリアにカードを乗せてカード番号を取得します。

注意

- カードNo.を空欄にできません。
- カード番号は20文字まで入力できます。
- カード番号は重複できません。

8.カードタイプを設定します。
9.ユーザーロールを設定します。

管理者

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

一般ユーザ

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。

7.3.4 PIN の追加

ユーザーのPIN を追加し、ユーザーはPIN を介して認証できます。

はじめる前に

注意

パスワードモードがローカルパスワードまたはプラットフォームパスワードであることを確認します。
ローカルパスワードを選択すると、デバイスまたはWeb でPIN を追加できます。
「Platform Password」を選択すると、デバイスまたはWeb でPIN を追加できなくなります。
代わりに、プラットフォームでPIN を追加する必要があります。
パスワードモードの設定については、「認証SeFngs (Link)」を参照してください。

手順

1.最初のページを3 秒間ロングタップし、ジェスチャに従って左右にスライドし、バックエンドにログインします。
2.「ユーザー」→「+」をタップして、「ユーザーの追加」ページに入ります。
3.「従業員ID」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、数字の組み合わせも可能です。
- 従業員ID は重複しないようにしてください。

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

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。
- 推奨されるユーザー名は32 文字以内にする必要があります。

5. PIN コードをタップし、ユーザー用のPIN を作成します。

注意

パスワードモードがローカルパスワードになっているか、PIN エリアを結合できないことを確認します。

6. ユーザーロールを設定します。

管理者

ユーザーは管理者です。

通常の出席機能を除き、ユーザーは、許可を認証した後に操作するためにホームページに入ることもできます。

一般ユーザ

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。

7.3.5 認証モードの設定

ユーザの顔画像、パスワード、またはその他の認証情報を追加したら、認証モードを設定する必要があります。

ユーザは、設定された認証モードを介して自分のID を認証できます。

手順

1. 最初のページを3 秒間ロングタップし、ジェスチャに従って左右にスライドし、バックエンドにログインします。

2. ユーザー→ユーザーの追加/ユーザーの編集→認証モードをタップします。

3. 認証モードとしてデバイスまたはカスタムを選択します。

デバイス

デバイスモードを選択する場合は、まず「アクセス制御設定」ページで端末認証モードを設定する必要があります。

詳細は、アクセス制御パラメータの設定を参照してください。

カスタム

実際のニーズに応じて、異なる認証モードを組み合わせることができます。

4. タップして設定を保存します。

7.3.6 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」ページに入ります。
ページの左側にある「カード」をタップし、ドロップダウンリストから検索タイプを選択します。
従業員ID、カード番号、または検索するユーザー名を入力します。
タップして検索します。

ユーザーの編集

「User Management」ページで、ユーザリストからユーザを選択して「Edit User」ページに入ります。ユーザManagement (Link)の手順に従って、ユーザーパラメータを変更します。
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。

7.4 時刻と出席状況の設定

参加モードは、実際の状況に応じて、チェックイン、チェックアウト、ブレイクアウト、ブレークイン、オーバータイムイン、およびオーバータイムアウトとして設定できます。

注意

クライアントソフトウェアでは、時間・出席機能と連携して使用すること。

7.4.1 デバイス経由の出席モードの無効化

アテンダンスモードを無効にすると、システムは最初のページにアテンダンスステータスを表示しません。

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

出席モードを無効に設定します。

最初のページでは、参加ステータスの表示や設定は行いません。
システムは、プラットフォームで設定されたアテンションルールに従います。

7.4.2 デバイス経由の手動出席の設定

参加モードを手動に設定します。
参加するときは、手動でステータスを選択する必要があります。

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

3.必要な出席ステータスを有効にします。
4.参加状況のグループを有効にします。

注意

Attendance プロパティは変更されません。

5.オプション: ステータスを選択し、必要に応じて名前を変更します。

T & A Statusページと認証結果ページに名前が表示されます。

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、有効な出席としてマークされません。

7.4.3 デバイス経由の自動出席の設定

参加モードを自動に設定し、参加状況とその利用可能なスケジュールを設定できます。
システムは、設定されたスケジュールに従って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.Platform Attendanceをタップして、T&A Statusページに入ります。
2.出席モードを自動に設定します。

3. Attendance Status機能を有効にします。
4. 参加状況のグループを有効にします。

注意

Attendance プロパティは変更されません。

5. オプション: ステータスを選択し、必要に応じて名前を変更します。

T & A Statusページと認証結果ページに名前が表示されます。

6. 状況のスケジュールを設定します。
1)出席予定をタップします。
2)月曜日、火曜日、水曜日、木曜日、金曜日、土曜日、または日曜日を選択します。
3)選択した出席状況のその日の開始時刻を設定します。
4)確認をタップします。
5)実際のニーズに応じて、手順1 ～4 を繰り返します。

注

参加ステータスは、設定されたスケジュール内で有効になります。

結果

最初のページで認証を行うと、設定されたスケジュールに従って、認証が設定された参加ステータスとしてマークされます。

例

Break Out をMonday 11:00、Break In をMonday 12:00 に設定すると、有効なユーザの月曜11:00 から12:00 までの認証がブレークとしてマークされます。

7.4.4 デバイス経由の手動および自動出席の設定

参加モードを手動と自動に設定すると、システムは設定されたスケジュールに従って参加ステータスを自動的に変更します。
同時に、認証後に参加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. Platform Attendanceをタップして、T&A Status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。

3. Attendance Status機能を有効にします。

4. 参加状況のグループを有効にします。

注意

Attendance プロパティは変更されません。

5. オプション: ステータスを選択し、必要に応じて名前を変更します。

T & A Statusページと認証結果ページに名前が表示されます。

6. 状況のスケジュールを設定します。

1)出席予定をタップします。

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

3)選択した出席状況のその日の開始時刻を設定します。

4)OKをタップします。

5)実際のニーズに応じて、手順1 ～4 を繰り返します。

注意

参加ステータスは、設定されたスケジュール内で有効になります。

結果

最初のページで認証を行います。
認証は、スケジュールに従って設定された参加ステータスとしてマークされます。
結果タブの編集アイコンをタップすると、ステータスを選択して手動で参加することができ、認証は編集された参加ステータスとしてマークされます。

例
Break Out をMonday 11:00、Break In をMonday 12:00 に設定すると、有効なユーザの月曜11:00 から12:00 までの認証がブレークとしてマークされます。

7.5 データマネジメント

データの削除、データのインポート、データのエクスポートができます。

7.5.1 データを削除します

ユーザーデータを削除します。

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

7.5.2 データをインポートします

手順

1. USB フラッシュドライブをデバイスに差し込みます。

2. ホームページで、データ→データのインポートをタップします。

T & A Statusページと認証結果ページに名前が表示されます。

7.状況のスケジュールを設定します。

1)出席予定をタップします。

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

3)選択した出席状況のその日の開始時刻を設定します。

4)OKをタップします。

5)実際のニーズに応じて、手順1 ～4 を繰り返します。

注意

参加ステータスは、設定されたスケジュール内で有効になります。

結果

最初のページで認証を行います。
認証は、スケジュールに従って設定された参加ステータスとしてマークされます。
結果タブの編集アイコンをタップすると、ステータスを選択して手動で参加することができ、認証は編集された参加ステータスとしてマークされます。

例
Break Out をMonday 11:00、Break In をMonday 12:00 に設定すると、有効なユーザの月曜11:00 から12:00 までの認証がブレークとしてマークされます。

7.6 データマネジメント

データの削除、データのインポート、データのエクスポートができます。

7.6.1 データを削除します

ユーザーデータを削除します。

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

7.6.2 データをインポートします

手順

3.USB フラッシュドライブをデバイスに差し込みます。

4.ホームページで、データ→データのインポートをタップします。

5.ユーザーデータ、顔データ、アクセス制御パラメータをタップします。

注意

インポートされたアクセス制御パラメータは、デバイスの設定ファイルです。

6.データをエクスポートしたときに作成されたパスワードを入力します。
データのエクスポート時にパスワードを作成しない場合は、入力ボックスに空白のままにして、すぐにOK をタップします。

注意

- あるデバイス(デバイスA)から別のデバイス(デバイスB)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てから、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。
- サポートされるUSB フラッシュドライブ形式はFAT32 です。
- インポートされた画像はルートディレクトリのフォルダ(enroll_picという名前)に保存され、画像の名前は以下のルールに従う必要があります:

カードNo._Name_Department_Employee ID_Gender.jpg

- フォルダenroll_pic がインポートされたすべての画像を保存できない場合は、ルートディレクトリの下にenroll_pic1、enroll_pic2、enroll_pic3、enroll_pic4 という名前の別のフォルダを作成できます。
- 従業員ID は32 文字未満にする必要があります。
  ※小文字、大文字、数字の組み合わせが可能です。
  重複してはならず、0 から始まってはいけません。
- フェイスピクチャの要件は、以下のルールに従う必要があります。
  フルフェイスビューで、カメラに直接向かって撮影する必要があります。
  顔写真を撮るときは、ハットやヘッドカバーを着用しないでください。
  形式はJPEG またはJPG にしてください。
  解像度は640 ×480 ピクセル、または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。

7.6.3 データをエクスポートします

手順

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

注意

エクスポートされたアクセス制御パラメータは、デバイスの設定ファイルです。

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

注意

- サポートされるUSB フラッシュドライブ形式はDB です。
- システムは、1G ～32G のストレージのUSB フラッシュドライブをサポートします。
  USBメモリーの空き容量が512Mを超えていることを確認してください。
- エクスポートされたユーザーデータは、編集できないDB ファイルです。

7.7 ID 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個人を認証します。

7.7.1 単一の認証情報による認証

認証前のユーザー認証タイプを設定します。

詳しくは、認証Mode (Link)の設定を参照してください。

顔、カードを認証します。

フェイス

カメラを手前にして、顔で認証を開始します。

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します。

注意

カードには、通常のICカードまたは暗号化されたカードがあります。

PIN

PINで認証するためのPINコードを入力します。

認証が完了すると、「Authenticated」というプロンプトが表示されます。

7.7.2 複数の認証情報を使用した認証

はじめる前に

認証前のユーザー認証タイプを設定します。
詳しくは、認証Mode (Link)の設定を参照してください。

手順

1. 認証モードが「カードと顔」、「パスワードと顔」、「カードとパスワード」、「カードと顔と指紋」の場合は、ライブビューページの指示に従って認証を行います。

注意

- カードには、通常のICカードまたは暗号化されたカードがあります。

2. 前の認証情報が認証されたら、他の認証情報の認証を続行します。

注意

- 顔認証の詳細については、顔写真を収集/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、「Authenticated」というプロンプトがポップアップ表示されます。

7.8 基本設定

サウンド、時間、スリープ(s)、言語、コミュニティ番号、ビルディング番号、ユニット番号、プライバシー、ビデオ規格を設定できます。

最初のページを3秒間ロングタップし、ジェスチャに従って左右にスライドし、デバイスのホームページにログインします。システム設定→基本をタップします。

サウンド設定

音声プロンプト機能を有効/無効にしたり、音声音量を調整したりできます。

注意

音量は0 ～10 の間で設定できます。
※0 は無音を表します。

時刻設定

タイムゾーン、デバイスの時刻、DST を設定します。

スリープ中(s)

デバイスのスリープ待ち時間(分)を設定します。
最初のページでスリープ時間を30 分に設定すると、デバイスは何も操作せずに30 分後にスリープ状態になります。

注意

スリープ時間を0 に設定すると、デバイスはスリープモードに入りません。

言語の選択

実際のニーズに合わせて言語を選択します。

コミュニティ番号

デバイス搭載コミュニティ番号を設定します。

ビル番号

機器設置建物番号を設定します。

ユニット番号

デバイス装着ユニット番号を設定します。

通話設定

ダイヤル後の自動発信

「発信後に自動発信」を有効にしたり、タイムアウト時間を設定したりできます。

コールセンターボタンの呼び出し対象

発信先を選択

VoIP Server

VoIPサーバを選択します。

プライバシー

名前/従業員ID

認証時に名前の表示/非表示とEmploy ID を選択できます。

フェイスピクチャ

認証時に顔画像を表示/非表示にすることができます。

登録画像保存

登録した顔写真は、機能を有効にするとシステムに保存されます。

認証時に画像を保存します

この機能を有効にすると、デバイスへの認証時に画像を保存できます。

認証時に画像をアップロード

プラットフォームへの認証時にキャプチャされた画像を自動的にアップロードします。

キャプチャした画像のアップロード。
通話中

通話中に撮影した画像を自動的にプラットフォームにアップロードします。

ビデオ規格

リモートでライブビューを行うときのビデオフレームレートを設定します。
標準を変更したら、デバイスを再起動して有効にする必要があります。

PAL(50HZ)

毎秒25 フレーム。中国、中東国、ヨーロッパなどに適しています。

NTSC(60HZ)

毎秒30 フレーム。米国、カナダ、日本、台湾(中国)、韓国、フィリピンなどに適しています。

7.9 生体認証パラメータの設定

顔パラメータをカスタマイズして、顔認識のパフォーマンスを向上させることができます。
設定可能なパラメータには、顔の生存レベル、認識距離、顔認識間隔、顔1:Nセキュリティレベル、顔1:1セキュリティレベル、ECOモード設定、マスク検出があります。

最初のページを3秒間ロングタップし、ホームページにログインします。
システム設定→生体認証をタップします。

表7-1 顔画像パラメータ

パラメータ	説明
フェイスライブネスレベル	フェイスアンチスプーフィング機能を有効にしたあと、ライブフェイス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。
認識距離	認証時のユーザーとカメラの間の有効距離を設定します。
顔認識時間	認証時の2つの連続した顔認識の時間間隔。 注意 1～10まで入力できます。
フェイス1:N セキュリティレベル	1:N マッチングモードで認証する場合のマッチングしきい値を設定します。 値が大きいほど、誤受理率は小さくなり、誤拒否率は大きくなります。
フェイス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の一致しきい値を設定します。 値が大きいほど、誤受理率は小さくなり、誤拒否率は大きくなります。
ECOモードの設定	ECO モードを有効にすると、本機は赤外線カメラを使用して、薄暗い環境で顔を認証します。 また、ECOモードのしきい値、ECOモード(1:N)、ECOモード(1:1)を設定できます。 ECO モードのしきい値 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。 ECO モード(1:1) ECO モード1:1 マッチングモードで認証する場合のマッチングしきい値を設定します。 値が大きいほど、誤受理率は小さくなり、誤拒否率は大きくなります。 ECOモード(1:N) ECO モード1:N マッチングモードで認証する場合のマッチングしきい値を設定します。 値が大きいほど、誤り受入率は小さくなり、誤り拒否率は大きくなります
マスク設定	マスク検出機能を有効にすると、システムはキャプチャされた顔をマスクピクチャで認識します。 マスク&フェイス付きフェイス(1:1)、マスク&フェイス付きフェイス(1:N)、ECO (1:1)しきい値、ECO モード(1:N)しきい値、プロンプト方法を設定できます。 マスク&フェイス付きフェイス(1:1)

パラメータ	説明
	1:1照合モードでフェイスマスクで認証する場合の照合値を設定します。 値が大きいほど、誤受理率は小さくなり、誤拒否率は大きくなります。 **マスク&フェイス付きフェイス(1:N)** 1:N マッチングモードでフェイスマスクで認証する場合のマッチング値を設定します。 値が大きいほど、誤受理率は小さくなり、誤拒否率は大きくなります。 **ECO モード(1:1)しきい値** ECOモード1:1マッチングモードでフェイスマスクで認証する場合のマッチング値を設定します。 値が大きいほど、誤受理率は小さくなり、誤拒否率は大きくなります。 **ECO モード(1:N)しきい値** ECOモード1:Nマッチングモードでフェイスマスクで認証する場合のマッチング値を設定します。 値が大きいほど、誤受理率は小さくなり、誤拒否率は大きくなります。 **プロンプト方式** None、Reminder of Wearing、Must Wear ストラテジを設定します。 **装着時の注意事項** 認証時に顔マスクを装着しないと、デバイスは通知を促し、ドアが開きます。 **着用必須** 認証時に顔マスクを装着しないと、デバイスは通知を促し、ドアは閉じたままになります。 **なし** 認証時に顔マスクを装着しないと、デバイスは通知を促しません。

7.10 環境設定

環境設定のパラメータを設定できます。

手順

1. システム設定→環境設定をタップして、環境設定ページに入ります。

ショートカットキー

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

注意

コールタイプは、コールルーム、コールセンター、コール指定ルーム番号、コールAPP から選択できます。

パスワード

この機能を有効にすると、パスワードで認証するためのパスワードを入力できます。

QRコード

認証インターフェースでQRコード読み取り機能を利用できます。

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。

コールルーム

認証ページのコールボタンをタップすると、部屋番号をダイヤルして発信する必要があります。

コールセンター

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

コール指定ルーム番号

部屋番号を設定する必要があります。
認証ページのコールボタンをタップすると、ダイヤルせずに設定した部屋に直接電話をかけることができます。

APPと呼びます

認証ページのコールボタンをタップすると、デバイスが追加されているモバイルクライアントを呼び出します。

コール室内局番

有効にすると、認証ページに室内局番が表示されます。

コール管理センター/コールVoIPセンター

有効にした後、認証ページでManagement Center またはVoIP Center を呼び出すことができます。

テーマ

認証ページでプロンプトウィンドウのテーマを設定できます。

認証/シンプルとしてのテーマ

デバイス認証ページにライブビューページが表示されます。
そして、人名、従業員ID、顔写真はすべて認証後に表示されます。

シンプル

このモードを選択すると、認証ページのライブビューが無効になり、その間、個人の名前、従業員ID、顔画像はすべて非表示になります。

インターコムモード

このモードを選択すると、認証ページの下部にショートカットが表示されます。

チェック中に出席記録を表示

チェック中に出席記録を表示を有効にすることができます。

有効にした後、チェック中に出席記録が表示されます。

7.11 デバイスパスワードの変更

古いパスワードを入力して、デバイスパスワードを変更できます。

手順

1. 最初のページを3秒間ロングタップし、ホームページにログインします。
2. システム→パスワードをタップします。
3. デバイスパスワードの変更をタップします。
4. デバイスの古いパスワードを入力します。

注意

パスワードを忘れた場合は、「パスワードを忘れたとき」をタップしてパスワードを変更できます。

詳しくは忘れたPassword (Link)をご覧ください。

5. 新しいパスワードを入力し、パスワードを確認します。

注意

デバイスのパスワード強度は自動的に確認できます。

製品のセキュリティを高めるために、独自に選択する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、パスワードを月次または週次で変更すると、製品をより適切に保護できます。

すべてのパスワードとその他のセキュリティ設定を適切に設定することは、インストーラまたはエンドユーザの責任です。

6. OKをタップします。

7.12 認証設定

認証モードの機能、NFC カードの有効化、M1 カードの有効化、ドア接点、開放時間(s)、認証間隔(s)、認証結果表示時間(s)、パスワードモードなどのアクセス制御権限を設定できます。

ホームページで、認証設定をタップして設定ページに入ります。

使用可能なパラメータの説明は次のとおりです

表7-2 アクセス制御パラメータの説明

パラメータ	説明
端末認証。モード(端末認証モード)	顔認証端末の認証モードを選びます。 認証モードをカスタマイズすることもできます。 注意 • 指紋関連機能をサポートしているのは、指紋モジュールを搭載したデバイスのみです。 • 生体認証製品は、スプーフィング対策環境に完全には適用できません。より高いセキュリティレベルが必要な場合は、複数の認証モードを使用します。 • 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。
リーダ認証。モード(カードリーダ認証モード)	カードリーダの認証モードを選択します。
NFC カードを有効にします	機能を有効にし、NFC カードに認証を提示できます。
M1 カードを有効にします	機能を有効にすると、M1 カードに認証を要求できます。
M1 カードの暗号化	M1カードの暗号化機能を有効にすると、カードのセキュリティレベルが向上します。 カードは簡単にコピーされません。
ドア接点	実際のニーズに合わせて「オープン(残りオープン)」または「クローズ(残りクローズ)」を選択できます。 デフォルトでは、Close (Remian Closed) です。
継続時間を開きます	ドアのロック解除時間を設定します。 設定した時間、ドアが開かないと、ドアはロックされます。 使用可能なドアロック時間の範囲: 1 ～255 秒。
認証間隔	デバイスの認証間隔を設定します。 使用可能な認証間隔の範囲: 0 ～65535。
認証結果表示時間(秒)	認証後の認証結果表示時間を設定します。

パスワードモード	プラットフォーム対応パーソナルPIN PIN はプラットフォームによって管理および配布されます。 Web のデバイスではPIN を設定できません。 デバイスセットパーソナルPIN

表7-2 アクセス制御パラメータの説明

パラメータ	説明
端末認証。モード(端末認証モード)	顔認証端末の認証モードを選びます。 認証モードをカスタマイズすることもできます。 注意 • 生体認証製品は、スプーフィング対策環境に完全には適用できません。 より高いセキュリティレベルが必要な場合は、複数の認証モードを使用します。 • 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。
リーダ認証。モード(カードリーダ認証モード)	カードリーダの認証モードを選択します。
NFC カードを有効にします	機能を有効にし、NFC カードに認証を提示できます。
M1 カードを有効にします	機能を有効にすると、M1 カードに認証を要求できます。
M1 カードの暗号化	M1カードの暗号化機能を有効にすると、カードのセキュリティレベルが向上します。 カードは簡単にコピーされません。
ドア接点	実際のニーズに合わせて「オープン(残りオープン)」または「クローズ(残りクローズ)」を選択できます。 デフォルトでは、Close (Remian Closed) です。
継続時間を開きます	ドアのロック解除時間を設定します。 設定した時間、ドアが開かないと、ドアはロックされます。 使用可能なドアロック時間の範囲: 1 ～255 秒。
認証間隔	デバイスの認証間隔を設定します。使用可能な認証間隔の範囲: 0 ～65535。
認証結果表示時間(秒)	認証後の認証結果表示時間を設定します。

パスワードモード	プラットフォーム対応パーソナルPIN PIN はプラットフォームによって管理および配布されます。 Web のデバイスではPIN を設定できません。 デバイスセットパーソナルPIN

パラメータ	説明
	PIN はデバイスまたはWeb で設定されます。 他のプラットフォームではPIN を設定できません。

7.13 メンテナンス

デバイスのシステム情報と容量を表示できます。
また、デバイスのアップグレード、デバイスのユーザーマニュアルの表示、システムの工場出荷時設定への復元、デフォルト設定、システムの再起動を行うこともできます。

最初のページを3秒間ロングタップし、ホームページにログインします。
「メンテナンス」をタップします。

図7-17 メンテナンスページ

メンテナンス

デバイスモデル、シリアル番号、ファームウェアバージョン、MACアドレス、製造データ、ライセンスなどのデバイス情報を表示できます。

注意

ページは、デバイスモデルによって異なる場合があります。
詳細は、実際のページを参照してください。

ロングタップして管理者パスワードを入力すると、デバイスのバージョン情報が表示されます。

面パラメータ

カスタムスプーフィング対策検出フェイ

スライブネスレベル

フェイスアンチスプーフィング機能を有効にしたあと、ライブフェイス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。

スプーフィング対策の検出しきい値

値が大きいほど、誤受理率は小さくなり、誤拒否率は大きくなります。
値が小さいほど、誤り受け入れ率が大きくなり、誤り拒否率が小さくなります。

スプーフィング対策保護のためのロック面

この機能を有効にした後、アンチスプーフィング検出に失敗すると、デバイスは自動的にロックします。

ロック時間

スプーフィング対策検出に失敗した場合の、スプーフィング対策保護のためのフェイスロックを有効にした後のロック期間。

バージョン情報

デバイス情報を表示できます。

容量

人物、顔写真、カード、イベントの数を表示できます。

注意

詳細は、実際のページを参照してください。

デバイスアップグレード

オンラインアップデ

ート

デバイスがGuardingVisionとネットワークに接続されている場合、GuardingVisionに新しいインストールパッケージがあるときに、デバイスのアップグレード→オンラインアップデートをタップしてデバイスシステムをアップグレードできます。

USB 経由のアップデート

USB フラッシュドライブをデバイスのUSB インターフェースに差し込みます。
「De vice Upgrade」→「Update via USB」をタップすると、デバイスはUSBフラッシュドライブ内のdigicap.davファイルを読み取り、アップグレードを開始します。

ユーザーマニュアル

QR コードをスキャンして、デバイスのユーザーマニュアルを表示します。

工場出荷時設定に復元します

すべてのパラメータが工場出荷時の設定に復元されます。

システムが再起動して有効になります。

デフォルト設定に戻します

リモートでインポートしたユーザ情報は、通信設定を除くすべてのパラメータが初期設定に戻ります。
システムが再起動して有効になります。

再起動

確認後、デバイスは再起動します。

第8 章モバイルアプリ を使用したデバイスの設定

8.1 ログイン

モバイルブラウザからログインできます。

注意

- 一部のモデルはWi-Fi 設定をサポートしています。
- デバイスがアクティブになっていることを確認します。
- デバイスと携帯電話が同じWi-Fi 内にあることを確認します。

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

デバイスのユーザー名とパスワードを入力します。ログインをタップします。

8.2 概要

ドアの状態、ネットワークの状態、基本情報を表示したり、ショートカットエントリで個人管理、スマート設定、認証設定、ドアパラメータを設定したりできます。

関数の説明:

ドアの状態

／ ／ ／

ドアの状態は、開/閉/開残/閉です。
タップすると、実際のニーズに合わせてオープン/クローズ/オープン残/クローズ状態を選択できます。

ショートカット登録

ショートカット入力により、個人管理、スマート設定、認証設定、ドアパラメータを設定できます。

ネットワークステータス

ネットワークの接続状態や登録状態を確認できます。

基本情報

モデル、シリアル番号、ファームウェアバージョンを表示できます。

8.3 パスワードを忘れます

ログイン時にパスワードを忘れた場合は、電子メールアドレスまたはセキュリティ上の質問でパスワードを変更できます。

ログインページで「パスワードを削除」をタップします。

検証モードを選択します。セキュリ

ティ質問の検証

セキュリティに関する質問に答えます。

電子メール検証

1. QRコードをエクスポートし、添付ファイルとして指定の宛先に送信します。
2. 予約メールで5分以内に確認コードが届きます。
3. 確認コードを確認コードフィールドに入力して、ID を確認します。

Next(次へ)をクリックし、新しいパスワードを作成して確認します。

8.4 構成

8.4.1 デバイス情報を表示します

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

ホームページで→システム設定→基本情報をタップします。

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

保存をタップします。

8.4.2 時刻設定

タイムゾーン、時刻同期モード、表示時刻を設定します。

→システム設定→時刻設定をタップして、設定ページに入ります。

保存をタップして設定を保存します。

時間帯

デバイスが配置されているタイムゾーンをドロップダウンリストから選択します。

時刻同期。モードマニュ

アル

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

NTP

NTP サーバのIP アドレス、ポート番号、および間隔を設定します。

8.4.3 DSTの設定

手順

1. →システム設定→時刻設定をタップして、設定ページに入ります。

2.サマータイムを有効にするをタップします。
3.開始時刻、終了時刻、DST バイアスを設定します。
4.保存をタップします。

8.4.4 ユーザ管理

手順

1.「User Management」→「User Management」→「admin」をタップして、設定ページに入ります。
2.古いパスワードを入力し、新しいパスワードを作成します。
3.新しいパスワードを確認します。
4.保存をタップします。

注

デバイスのパスワード強度は自動的に確認できます。
お客様の製品の安全性を高めるために、お客様独自の選択(大文字、小文字、数字、特殊文字の2種類以上を含む8 ～16 文字の使用)のパスワードを変更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、パスワードを月次または週次で変更すると、製品をより適切に保護できます。

8.4.5 ネットワーク設定

有線ネットワーク、Wi-Fiパラメータ、デバイスポートを設定できます。

有線ネットワーク

有線ネットワークを設定します。

設定ページに入るには、→通信設定→有線ネットワークの順にタップします。

DHCP

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

この機能を有効にすると、IPv4 アドレス、IPv4 サブネットマスク、IPv4 デフォルトゲートウェイが自動的に割り当てられます。

DNSサーバ

実際の必要に応じて、優先DNS サーバと代替DNS サーバを設定します。

Wi-Fi パラメータの設定

デバイスのワイヤレス接続用のWi-Fi パラメータを設定します。

手順

注

この機能はデバイスでサポートされている必要があります。

1. →「通信設定」→「Wi-Fi」を順にタップし、設定ページに入ります。
2. Wi-Fi を有効にします。

3.Wi-Fiを追加します。
1)「Wi-Fiを追加」をタップします。
2)「Wi-Fi 名」と「Wi-Fi パスワード」を入力し、「暗号化タイプ」を選択します。
3)保存をタップします。
4.Wi-Fi 名を選択し、接続をタップします。
5.パスワードを入力し、保存をタップします。

ポートパラメータの設定

ネットワーク経由でデバイスにアクセスする場合は、実際のニーズに応じてHTTP およびHTTPS を設定できます。

→ネットワークサービス→ HTTP(S)をタップして、設定ページに入ります。

HTTP

これは、ブラウザがデバイスにアクセスするポートを参照します。
たとえば、HTTP ポートが81 に変更された場合、ログイン用にブラウザにhttp://192.0.0.65:81と入力する必要があります。

HTTPS

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

プラットフォームアクセス

プラットフォームアクセスでは、プラットフォームを介してデバイスを管理するオプションが提供されます。

手順

1. →デバイスアクセス→ GuardingVisionをタップして、設定ページに入ります。

注

GuardingVision は、モバイルデバイス用のアプリケーションです。
アプリでは、デバイスのライブ画像の表示、アラーム通知の受信などを行うことができます。

2.有効をチェックして機能を有効にします。
3.「カスタム」を有効にすると、サーバアドレスを入力できます。

注

- 6～12文字(a～z、A～Z)または数字(0～9)で、大文字と小文字を区別します。
  8文字以上の英数字を組み合わせて使用することをお勧めします。
- 確認コードを123456 またはabcdef (大文字と小文字を区別しない0) にすることはできません。

4.Register Status とBinding Status を表示できます。
5.ビデオ暗号化を有効にし、パスワードを作成して確認します。

注

デバイスをAPP に追加した後、デバイスをライブビューするにはビデオ暗号化パスワードを入力する必要があります。

6. アカウントのバインド→QR コードの表示をタップし、QR コードをスキャンしてアカウントをバインドできます。

7.「保存」をタップして設定を有効にします。

ISUP パラメータの設定

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

手順

注意

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. →デバイスアクセス→ ISUPをタップして、設定ページに入ります。
2. ISUP を有効にします。
3. ISUP のバージョン、サーバアドレス、ポート、デバイスID、暗号化キーを設定します。

注意

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

4. 保存をタップして設定を保存します。

OTAP の設定

OTAPプロトコルを介してデバイスをプラットフォームに接続し、デバイス情報の取得、動作ステータスとアラーム情報のアップロード、デバイスの再起動とアップグレードを行います。

手順

1. →デバイスアクセス→ OTAPをタップして、設定ページに入ります。
2. OTAPを有効にするタップします。
3. サーバアドレス、ポート、デバイスID、暗号化キーを設定します。
4. 「テスト」をタップして、デバイスがサーバに接続して正常に登録できることを確認します。
   ページを更新するか、デバイスを再起動して、レジスタステータスを確認します。
5. 保存をタップします。

ネットワーク侵入サービスの設定

LAN にデバイスを展開すると、侵入サービスを有効にしてデバイスのリモート管理を実現できます。

手順

1. →デバイスアクセス→ネットワーク侵入サービスをタップして、設定ページに入ります。
2. 侵入サービスを有効にするタップします。
3. サーバのIP アドレスとサーバーポートを設定します。
   ユーザー名とパスワードを作成します。
4. ハートビートタイムアウトを設定できます。
   値の範囲は1 ～6000です。
5. 侵入サービスのステータスを表示できます。
   Refresh(更新)をクリックしてステータスを更新します。

6.保存をタップします。

注意

48 時間が経過すると、侵入サービスは自動的に無効になります。

8.4.6 ユーザ管理

モバイルWeb ブラウザを使用して、ユーザを追加、編集、削除、検索できます。

手順

1.→個人管理をタップして、設定ページに入ります。

2.ユーザーを追加します。

1)+をタップ。

2)以下のパラメータを設定します。

従業員ID

従業員ID を入力します。

従業員ID は、0 または32 文字を超えることはできません。

大文字、小文字、数字の組み合わせが可能です。

名前

名前を入力します。

名前は、数字、大文字と小文字の英語、および文字をサポートします。

名前は32 文字以内にすることをお勧めします。

長期有効利用者

ユーザ権限を長期有効に設定します。

開始日/終了日

ユーザ権限の開始日と終了日を設定します。

ユーザーロール

ユーザーロールを選択します。

人の役割

個人ロールを選択します。

出席確認のみ

有効にすると、このユーザーにアクセス制御権限は付与されません。

フェイス

顔画像を追加します。

「顔」をタップしてから、「カメラ」をタップして顔を追加するか、「アルバムから選択」をタップして顔を読み込みます。

カード

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

3)保存をタップします。

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

8.4.7 検索イベント

「検索」をタップして、「検索」ページに入ります。
従業員ID、名前、カード番号、開始時刻、終了時刻などの検索条件を入力し、「検索」をタップします。

注意
32 桁以内の名前の検索をサポートします。

8.4.8 アクセス制御設定

認証パラメータの設定

認証パラメータを設定します。

手順
1.→アクセスコントロール→認証設定をタップします。
2.保存をタップします。
設定する端末を選択します。
ターミナルタイプ/ターミナルモデル
端末の説明を取得します。
これらは読み取り専用です。
認証デバイスの有効化
認証機能を有効にします。
認証
実際のニーズに応じて、ドロップダウンリストから認証モードを選択します。
顔連続認識間隔(秒)
認証中に同じ人物を連続2 回認識する間隔を設定できます。
設定されたインターバルでは、Person A は一度しか認識できません。
インターバル中に別の人(人B)が認識した場合、人Aは再び認識できます。
認証間隔
認証時に同じ相手の認証間隔を設定できます。
同じ人が認証できるのは、設定された間隔内の1 回だけです。
2 回目の認証は失敗します。

最大値のアラーム失敗した試行

カードの読み取り試行が設定値に達したときにアラームを報告するようにします。

メインインターフェイスモード

メインインターフェイスモードを「認証モード」または「シンプル」に設定することができます。

改ざん検出を有効にします

カードリーダの改ざん防止検出を有効にします。

カード番号反転有効

機能を有効にすると、カード番号が逆順になります。

ドアパラメータの設定

→アクセスコントロール→ドアパラメータをタップします。

設定後に設定を保存するには、保存をタップします。

ドア名

ドアの名前を作成できます。

継続時間を開きます

ドアのロック解除時間を設定します。
設定した時間、ドアが開かないと、ドアはロックされます。

終了ボタンタイプ

終了ボタンは、実際のニーズに応じて、Remain Open またはRemain Closed として設定できます。
デフォルトでは、Remain Open です。

1人目のドアが開いたままの時間(分)

ファーストパーソンが入るときのドア開放時間を設定します。
最初の人が許可されると、複数の人がドアやその他の認証アクションにアクセスできます。

ドア開放タイムアウトアラーム

設定された時間内にドアが閉じられなかった場合、アラームがトリガーされます。

ドア接点

実際のニーズに応じて、ドアコンタクトをRemain Open またはRemain Closed に設定できます。
デフォルトでは、Remain Closed です。

ドアロック電源オフ

ドアロック電源オフは、実際のニーズに応じて、開いたままにするか、閉じたままにするかを設定できます。
デフォルトでは、Remain Closed です。

拡張オープン継続時間

拡張アクセスが必要な人がカードをスワイプした後、適切な遅延でドアコンタクトを有効にすることができます。

Duressコード

強迫がある場合には、強迫コードを入力することでドアを開くことができます。
同時に、クライアントは脅迫通知を報告することができます。

スーパーパスワード

特定の人はスーパーパスワードを入力することでドアを開くことができます。

注意

脅迫コードとスーパーコードは異なっている必要があります。
※また、数字は4 ～8 の範囲です。

端末パラメータ

アクセスするためのターミナルパラメータを設定で

きます。→アクセスコントロール→

ターミナルパラメータをタップします。

「作業モード」を「アクセス制御モード」に設定できます。
アクセス制御モードは、デバイスのノーマルモードです。
アクセスするための認証情報を認証する必要があります。

リモート認証

リモート認証を有効にした後、認証時に、デバイスは認証情報をプラットフォームにアップロードし、プラットフォームはドアを開くかどうかを確認します。

ローカルでの認証情報の確認

機能を有効にすると、デバイスは権限を確認しますが、計画テンプレートは見積もりません。

タイムアウト時間

リモート認証のタイムアウト時間を設定できます。

設定後に設定を保存するには、保存をタップします。

カードセキュリティの設定

→アクセスコントロール→カードセキュリティをタップして、設定ページに入ります。

パラメータを設定し、保存をタップします。

NFC カードを有効にします

携帯電話がアクセス制御のデータを取得できないようにするために、NFCカードを有効にしてデータのセキュリティレベルを上げることができます。

M1 カードを有効にします

M1カードを有効にし、M1カードの提示による認証が可能です。

M1 カードの暗号化

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

セクタ

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

EM カードを有効にします

EMカードを有効にし、EMカードの提示による認証が可能です。

注意

EM カードは、デバイスがEM カードの提示をサポートする周辺機器カードリーダを接続する場合にサポートされます。

DESFireカードを有効にします

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

Felicaカードを有効にします

FeliCaカード機能を有効にすると、デバイスはFeliCaカードからデータを読み出すことができます。

RS-485パラメータの設定

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

→ Access Control → RS-485 をタップします。

設定後に設定を保存するには、保存をタップします。

ペリフェラルタイプ

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

注意

ペリフェラルを変更して保存した後、デバイスは自動的に再起動します。

RS-485 プロトコルプラ

イベート

デバイスはRS-485 経由でサードパーティ製デバイスと接続できます。

OSDP

標準RS-485 プロトコル。

RS-485 アドレス

実際のニーズに応じて、RS-485 アドレスを設定します。

注意

「Access Controller」を選択した場合: 機器をRS-485 インターフェース経由でターミナルに接続する場合、RS-485 アドレスを2 に設定します。
機器をコントローラに接続する場合は、ドアNo.に合わせてRS-485アドレスを設定してください。

通信速度

デバイスがRS-485 プロトコルを介して通信しているときのボーレート。

データビット

デバイスがRS-485 プロトコルを介して通信しているときのデータビット。

ストップビット

デバイスがRS-485 プロトコルを介して通信しているときのストップビットです。

パリティ/フローCtrl/通信モード

デフォルトで有効。

8.4.9 ビデオインタ

ーコム設定デバイスID 設

定

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

手順

1. →インターコム→デバイスID設定をタップします。
2. 以下のパラメータを設定します。

デバイスタイプ

このデバイスは、ドアステーションまたは外部ドアステーションとして使用できます。
ドロップダウンリストからデバイスの種類を選択します。

注意

デバイスタイプを変更した場合は、デバイスを再起動する必要があります。

周期番号

デバイス周期番号を設定します。

ビル番号

デバイスのビルド番号を設定します。

ユニット番号

デバイスユニット番号を設定します。

注意

番号を変更した場合は、デバイスを再起動してください。

フロア番号

デバイスの設置フロア番号を設定します。

ドアステーション番号

デバイスの設置フロア番号を設定します。

注意

- 番号を変更した場合は、デバイスを再起動してください。
- メイン扉のステーションNo.は0、サブ扉のステーションNo.は1～16です。

機器種別を「外部ドア」または「局番」に設定した場合は、外部ドア局番、コミュニティ番号を設定できます。

屋外ドアステーション番号

デバイスタイプとして外側のドアステーションを選択した場合は、
1～の数値を入力する必要があります。
99.

注意

番号を変更した場合は、デバイスを再起動してください。

周期番号

デバイス周期番号を設定します。

セッション設定

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

手順

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

登録パスワード

メインステーションの有効化パスワード。

メインステーションIP

メインステーションのIP アドレス。

プライベートサーバーIP

プライベートサーバーのIP アドレス。

プロトコル1.0を有効にします

有効にすると、デバイスは以前のプロトコルを介してメインステーションに登録されます。
無効にすると、デバイスは新しいプロトコルを介してメインステーションに登録されます。

3. 保存をタップします。

継続時間の設定

最大通話時間を設定します。

→インターコム→通話設定をタップします。

最大通信時間を設定します。
保存をタップします。

注意

最大通話時間の範囲は90s ～s です。

ボタンを押して発信

手順

1. タップ→インターコム→ボタンを押して通話します。
2. 必要に応じて、「コール」または「コールセンター」をタップします。

電話番号設定

部屋のSIPに電話して部屋に電話をかけることができます。

手順

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

8.4.10 オーディオ設定

手順

1. →オーディオをタップします。
2. 入出力ボリュームを設定します。

8.4.11 顔パラメータ設定

顔パラメータを設定します。

顔パラメータ設定

→スマート→顔認識パラメータをタップします。

顔アンチスプーフィング

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

ライブ顔検出セキュリティレベル

フェイスアンチスプーフィング機能を有効にした後、ライブフェイス認証を実行するときに、一致するセキュリティレベルを設定できます。

1:1 一致しきい値

1:1 一致モードで認証する場合の一致しきい値を設定します。
値が大きいほど、誤受理率は小さくなり、誤拒否率は大きくなります。

1: N 一致しきい値

1:N マッチングモードで認証する場合のマッチングしきい値を設定します。
値が大きいほど、誤受理率は小さくなり、誤拒否率は大きくなります。
最大値は100 です。

顔認識タイムアウト値(秒)

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

フィンガープリントパラメータ

→スマート→指紋パラメータをタップします。

指紋セキュリティレベル

フィンガープリントのセキュリティレベルを設定できます。
設定したセキュリティレベルが高いほど、False Acceptance Rate (FAR) は低くなります。
設定したセキュリティレベルが高いほど、False Rejection Rate (FRR) は低くなります。

フェイスマスク検出パラメータ

マスク付き顔検出

マスク検出で顔を有効にすると、キャプチャされた顔がマスクピクチャで認識されます。
マスク1:N 一致しきい値、ECO モード、ストラテジで面を設定できます。

なし

認証時に顔マスクを装着しないと、デバイスは通知を促しません。

装着時の注意事項

認証時に顔マスクを装着しないと、デバイスは通知を促し、ドアが開きます。

着用必須

認証時に顔マスクを装着しないと、デバイスは通知を促し、ドアは閉じたままになります。

マスク&フェイス付きフェイス(1:1)

1:1照合モードでフェイスマスクで認証する場合の照合値を設定します。
値が大きいほど、誤受理率は小さくなり、誤拒否率は大きくなります。

マスク1:N がしきい値に一致する面

1:Nマッチングモードでフェイスマスクで認証する場合のマッチングしきい値を設定します。
値が大きいほど、誤受理率は小さくなり、誤拒否率は大きくなります。

注意

機種により機能が異なります。詳細は実際のデバイスを参照してください。

保存をタップして設定を保存します。

8.4.12 プライバシーパラメータの設定

ディスプレイ設定、画像のアップロードおよび保存パラメータを設定

します。

→設定→セキュリティ→プライバシー設定の順にタップします。

認証設定

画像表示/名前表示/従業員ID

タップすると、「写真」、「名前」、または「従業員ID」を表示できます。
認証が完了すると、選択した内容が結果に表示されます。

名前/ID 識別解除

名前/ID 情報はアスタリスクで区別されます。

画像のアップロードと保存画像のアップロードと保存ができます。

登録画像保存

登録した顔写真は、機能を有効にするとシステムに保存されます。

認証時に画像を保存。

この機能を有効にすると、デバイスへの認証時に画像を保存できます。

認証時にキャプチャされた画像をアップロードします。

プラットフォームへの認証時にキャプチャされた画像を自動的にアップロードします。

リンクキャプチャ後の画像の保存

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。

リンクキャプチャ後に画像をアップロード

リンクカメラで撮影した画像を自動的にプラットフォームにアップロードします。

8.4.13 パスワードモード

パスワードを設定する前に、パスワードがデバイスセットのパーソナルPIN であるか、プラットフォーム適用のパーソナルPIN であるかを明確にする必要があります。
デバイスセットの個人用PINである場合は、デバイスまたはWeb上で作成または編集でき、他のプラットフォームで設定することはできません。
個人用PINを適用したプラットフォームである場合は、プラットフォームで作成または編集し、使用前にデバイスに発行することができます。
機器やWeb上で設定することはできません。

手順

1. **→「セキュリティ設定」→「PINモードデバイス設定」を順にタップします**

デバイスまたはWeb で作成または編集でき、他のプラットフォームでは設定できません。

プラットフォーム対応パーソナルPIN

プラットフォームで作成または編集し、デバイスに発行してから使用できます。
機器やWeb上で設定することはできません。

2.保存をタップします。

8.4.14 アップグレードとメンテナンス

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

デバイスの再起動

→「デバイスの再起動」をタップします。

再起動をタップして、デバイスを再起動します。

アップグレード

→アップグレードをタップします。

「アップグレード」をタップしてデバイスをアップグレードします。

注意

アップグレード中は電源を切らないでください。

復元パラメータ

→「デフォルト」をタップします。

デフォルト設定に戻します

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

工場出荷時設定に復元します

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

8.4.15 オンラインドキュメントの表示

→「オンラインドキュメント表示」をタップします。

「オンラインドキュメントを表示」をタップすると、QRコードを携帯電話でスキャンして詳細を確認できます。

8.4.16 オープンソースソフトウェアのライセンスの表示

設定→システム→システム設定→情報をタップし、ライセンスの表示をタップしてデバイスライセンスを表示します。

第9章Webブラウザによるクイック操作

9.1 パスワードの変更

デバイスのパスワードを変更できます。

Web ページの右上の をクリックして、Change Password ページに入ります。
ドロップダウンリストからセキュリティに関する質問を設定し、回答を入力できます。

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

9.2 言語の選択

デバイスシステムの言語を選択できます。

ウェブページの右上の をクリックして、デバイス言語設定ページに入ります。
デバイスシステムの言語をドロップダウンリストから選択できます。

デフォルトでは、システム言語は英語です。

注意

システム言語を変更すると、デバイスは自動的に再起動します。

9.3 時刻設定

Web ページの右上の をクリックして、ウィザードページを入力します。
デバイスの言語を設定した後、Next(次へ)をクリックしてTime Settings(時刻設定)ページに入ります。

時間帯

ドロップダウンリストからデバイスの検出されたタイムゾーンを選択します。

時刻同期。

NTP

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

マニュアル

デフォルトでは、デバイスの時刻は手動で同期する必要があります。
デバイスの時刻を手動で設定するか、Sync。with Computer Time(コンピュータの時刻と同期)をオンにして、デバイスの時刻をコンピュータの時刻と同期させることができます。

サーバアドレス/NTP ポート/インターバル

サーバアドレス、NTP ポート、インターバルを設定できます。

DST

DST 開始時間、終了時間、バイアス時間を表示できます。

「次へ」をクリックして設定を保存し、次のパラメータに進みます。
または、スキップをクリックして時間設定をスキップします。

9.4 プライバシー設定

画像のアップロードと保存パラメータを設定します。

Web ページの右上の をクリックして、ウィザードページを入力します。

画像のアップロードと保存

認証時に画像を保存します

自動認証時に画像を保存します。

認証時に画像をアップロード

プラットフォームへの認証時に自動的に画像をアップロードします。

登録画像保存

登録した顔写真は、機能を有効にするとシステムに保存されます。

リンクキャプチャ後に画像をアップロード

リンクカメラで撮影した画像を自動的にプラットフォームにアップロードします。

リンクキャプチャ後の画像の保存

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。
「次へ」をクリックして設定を保存し、次のパラメータに進みます。
または、スキップをクリックしてプライバシー設定をスキップします。

9.5 管理者設定

手順

1. Web ページの右上の をクリックして、ウィザードページを入力します。
2. 管理者の従業員ID と名前を入力します。
3. 追加する認証情報を選択します。

注意

少なくとも1つの認証情報を選択する必要があります。

1)顔を追加をクリックして、ローカルストレージから顔写真をアップロードします。

注意

アップロードされる画像は、JPG、JPEG、PNG 形式で200 K 以内にする必要があります。

2)カードの追加をクリックしてカード番号を入力し、カードのプロパティを選択します。

注意

最大50 枚のカードをサポートできます。

9.6 番号とシステムネットワーク

手順

1. Web ページの右上の をクリックして、ウィザードページを入力します。
   前回の設定後、Next(次へ)をクリックしてNo.とNetwork System Network settings (ネットワーク設定)ページに入ります。
2. デバイスタイプを設定します。

注意

- デバイスタイプをドアステーションに設定すると、フロアNo.、ドアステーションNo.、コミュニティNo.、建物No.、ユニットNo.、フロアNo.、ドアステーションNo.を設定できます。
- デバイスタイプをアウタードアステーションに設定すると、アウタードアステーション番号を設定できます

コミュニティ番号

デバイスタイプ

このデバイスは、ドアステーションまたは外部ドアステーションとして使用できます。
ドロップダウンリストからデバイスの種類を選択します。

コミュニティ番号

デバイスコミュニティ番号を設定します。

ビル番号

デバイスのビルド番号を設定します。

ユニット番号

デバイスユニット番号を設定します。

フロア番号

デバイスの設置フロア番号を設定します。

ドアステーション番号

デバイス搭載ドアステーションNo.を設定します。

注意

メイン扉のステーションNo.は0、サブ扉のステーションNo.は1～16です。

屋外ドアステーション番号

デバイス設置外扉連数を設定します。

注意

番号の範囲は1～99です。

3. ビデオインターコムネットワークパラメータを設定します。

登録パスワード

通信用の親局の登録パスワードを設定します。
通信用の親局の登録パスワードを設定します。

メインステーションIP

通信に使用するメインステーションのIP アドレスを入力します。

プライベートサーバーIP

SIP サーバIP を指します。
通信に使用するメインステーションのIP アドレスを入力します。
このとき、メインステーションはSIP サーバとして使用されます。
他のインターコムデバイスは、このサーバアドレスに登録して通信を実現する必要があります。

プロトコル1.0を有効にします

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

4. 設定後に設定を保存するには、「完了」をクリックします。

第10章Webブラウザによる操作

10.1 ログイン

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

注意

デバイスがアクティブになっていることを確認します。

Web ブラウザ経由のログイン

Web ブラウザのアドレスバーにデバイスのIP アドレスを入力し、Enter を押してログインページに入ります。
デバイスのユーザー名とパスワードを入力します。
ログインをクリックします。

クライアントソフトウェアのリモート設定によるログイン

デバイスを追加したら、 をクリックしてConfiguration(設定)ページに入ります。

10.2 パスワードを忘れます

ログイン時にパスワードを忘れた場合は、メールアドレスまたはセキュリティ上の質問でパスワードを変更できます。

ログインページで、パスワードを忘れた場合を

クリックします。

セキュリティ質問の検証

セキュリティに関する質問に答えます。

電子メール検証

1. QRコードをエクスポートし、添付ファイルとして設定したメールに送信します。
2. 予約メールで5分以内に確認コードが届きます。
3. 確認コードを確認コード項目に入力して、確認コードを確認します。

Next(次へ)をクリックし、新しいパスワードを作成して確認します。

10.3 ヘルプ

10.3.1 オープンソースソフトウェアのライセンス

オープンソースのソフトウェアライセンスを表示できます。

右上隅にある→オープンソースソフトウェアステートメントをクリックして、ライセンスを表示します。

10.3.2 オンラインヘルプ文書の表示

Web 設定のヘルプドキュメントを表示できます。

Webページ右上の→「オンラインドキュメント」を順にクリックすると、ドキュメントが表示されます。

10.4 ログアウト

アカウントをログアウトします。

管理者→ログアウト→ OKをクリックしてログアウトします。

10.5 Webブラウザによるクイック操作

10.5.1 パスワードの変更

デバイスのパスワードを変更できます。

Web ページの右上のをクリックして、Change Password ページに入ります。
ドロップダウンリストからセキュリティに関する質問を設定し、回答を入力できます。
「次へ」をクリックして設定を完了します。
または、「スキップ」をクリックしてステップをスキップします。

10.5.2 言語の選択

デバイスシステムの言語を選択できます。

ウェブページの右上のをクリックして、デバイス言語設定ページに入ります。
デバイスシステムの言語をドロップダウンリストから選択できます。

デフォルトでは、システム言語は英語です。

注意

システム言語を変更すると、デバイスは自動的に再起動します。

10.5.3 時刻設定

Web ページの右上のをクリックして、ウィザードページを入力します。
デバイスの言語を設定した後、Next(次へ)をクリックしてTime Settings(時刻設定)ページに入ります。

時間帯

ドロップダウンリストからデバイスの検出されたタイムゾーンを選択します。

時刻同期。

NTP

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

マニュアル

デフォルトでは、デバイスの時刻は手動で同期する必要があります。
デバイスの時刻を手動で設定するか、
Sync。with Computer Time(コンピュータの時刻と同期)をオンにして、デバイスの時刻をコンピュータの時刻と同期させることができます。

サーバアドレス/NTP ポート/インターバル

サーバアドレス、NTP ポート、インターバルを設定できます。

DST

DST 開始時間、終了時間、バイアス時間を表示できます。

「次へ」をクリックして設定を保存し、次のパラメータに進みます。
または、スキップをクリックして時間設定をスキップします。

10.5.4 プライバシー設定

画像のアップロードと保存パラメータを設定します。

Web ページの右上の  をクリックして、ウィザードページを入力します。

画像のアップロードと保存

認証時に画像を保存します

自動認証時に画像を保存します。

認証時に画像をアップロード

プラットフォームへの認証時に自動的に画像をアップロードします。

登録画像保存

登録した顔写真は、機能を有効にするとシステムに保存されます。

リンクキャプチャ後に画像をアップロード

リンクカメラで撮影した画像を自動的にプラットフォームにアップロードします。

リンクキャプチャ後の画像の保存

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。
「次へ」をクリックして設定を保存し、次のパラメータに進みます。
または、スキップをクリックしてプライバシー設定をスキップします。

10.5.5 管理者設定

手順

1. Web ページの右上の  をクリックして、ウィザードページを入力します。
2. 管理者の従業員ID と名前を入力します。
3. 追加する認証情報を選択します。

注意

少なくとも1つの認証情報を選択する必要があります。

1)顔を追加をクリックして、ローカルストレージから顔写真をアップロードします。

注意

アップロードされる画像は、JPG、JPEG、PNG 形式で200 K 以内にする必要があります。

2)カードの追加をクリックしてカード番号を入力し、カードのプロパティを選択します。

注意

最大50 枚のカードをサポートできます。

10.5.6 番号とシステムネットワーク

手順

1. Web ページの右上の をクリックして、ウィザードページを入力します。
   前回の設定後、Next(次へ)をクリックしてNo.とNetwork System Network settings(ネットワーク設定)ページに入ります。
2. デバイスタイプを設定します。

注意

- デバイスタイプをドアステーションに設定すると、フロアNo.、ドアステーションNo.、コミュニティNo.、建物No.、ユニットNo.、フロアNo.、ドアステーションNo.を設定できます。
- デバイスタイプをアウタードアステーションに設定すると、アウタードアステーション番号を設定できます

コミュニティ番号

デバイスタイプ

このデバイスは、ドアステーションまたは外部ドアステーションとして使用できます。
ドロップダウンリストからデバイスの種類を選択します。

コミュニティ番号

デバイスコミュニティ番号を設定します。

ビル番号

デバイスのビルド番号を設定します。

ユニット番号

デバイスユニット番号を設定します。

フロア番号

デバイスの設置フロア番号を設定します。

ドアステーション番号

デバイス搭載ドアステーションNo.を設定します。

注意

メイン扉のステーションNo.は0、サブ扉のステーションNo.は1～16です。

屋外ドアステーション番号

デバイス設置外扉連数を設定します。

注意

番号の範囲は1～99です。

3.ビデオインターコムネットワークパラメータを設定します。

登録パスワード

通信用の親局の登録パスワードを設定します。通信用の親局の登録パスワードを設定します。

メインステーションIP

通信に使用するメインステーションのIP アドレスを入力します。

プライベートサーバーIP

SIP サーバIP を指します。通信に使用するメインステーションのIP アドレスを入力します。
このとき、メインステーションはSIP サーバとして使用されます。

他のインターコムデバイスは、このサーバアドレスに登録して通信を実現する必要があります。

プロトコル1.0を有効にします

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

4.設定後に設定を保存するには、「完了」をクリックします。

10.6 人事管理

「追加」をクリックして、基本情報、証明書、認証設定などの個人の情報を追加します。

基本情報の追加

個人管理→追加をクリックして、個人の追加ページを入力します。
従業員ID、個人の名前、性別、個人種別など、個人の基本情報を追加します。
個人種別で「訪問者」を選択した場合は、訪問時間を設定できます。
カスタムタイプを選択すると、名前を編集できます。変更した名前がデバイスに適用されます。
個人ロールを選択します。
保存をクリックして設定を保存します。

許可時間の設定

個人管理→追加をクリックして、個人の追加ページを入力します。
Long-Term Effective User を有効にするか、Long-Term Effective User を設定します。
個人は、実際のニーズに応じて、設定された期間内にのみ権限を持つことができます。
アテンダンスチェックのみを有効にできます。
有効にすると、このユーザーにアクセス制御権限は付与されません。
保存をクリックして設定を保存します。

デバイス番号設定

個人管理→個人の追加→追加をクリックして、個人の追加ページに入ります。
Floor No。とRoom No.のテキストボックスをクリックし、1 ～999 の数値を入力して
Floor NoとRoom No。を設定します。
保存をクリックして設定を保存します。

認証設定

個人管理→追加をクリックして、個人の追加ページを入力します。
認証タイプを設定します。
保存をクリックして設定を保存します。

カードの追加

個人管理→追加をクリックして、個人の追加ページを入力します。
Add Cardをクリックし、Card No.を入力してプロパティを選択し、OKをクリックしてカードを追加
します。保存をクリックして設定を保存します。

顔写真を追加

個人管理→追加をクリックして、個人の追加ページを入力します。
「+アップロード」をクリックして、ローカルPCから顔写真をアップロード
します。

注意

画像形式はJPG、JPEG、PNG、サイズは200kb未満にしてください。

保存をクリックして設定を保存します。

PIN の追加

PIN を設定する前に、PIN がデバイスセットのパーソナルPIN であるか、プラットフォーム適用のパーソナルPIN であるかを明確にする必要があります。
デバイスセットのパーソナルPINである場合は、デバイスまたはWeb上で作成または編集でき、他のプラットフォームでは設定できません。
プラットフォーム適用のパーソナルPINである場合は、プラットフォームで作成または編集し、
使用前にデバイスに発行できます。
機器やWeb上で設定することはできません。
PIN モードをデバイス設定個人用PIN に設定していることを確認します。
ページのPIN モードをクリックして、設定に移動します。
個人管理→追加をクリックして、個人の追加ページを入力します。
PIN を設定します。
または、「自動生成」を選択して、PIN を自動的に生成します。
「追加」をクリックして設定を保存します。
Save and Continue(保存して続行)をクリックして設定を保存し、次のユーザーを追加します。

デバイス番号設定

個人管理→追加をクリックして、個人の追加ページを入力します。
個人の基本情報を追加します。
デバイス番号モジュールに移動します。
「追加」をクリックし、所属する部屋番号とフロア番号を入力します。
「追加」または「保存して続行」をクリックします。

個人の削除

個人管理ページで、削除する必要がある個人をチェックし、削除をクリックします。
すべての人物をクリアするには、すべてクリアをクリックします。

個人の編集

個人管理ページで、編集する必要がある個人を確認します。
クリック個人情報の編集

フィルタ

個人管理ページで、従業員ID /名前/カード番号を入力します。
資格情報ステータスを選択し、フィルタをクリックして個人をフィルタリングします。
すべての条件をクリアするには、リセットをクリックします。

10.7 概要

デバイス、リンクデバイス、個人情報、ネットワークステータス、基本情報、およびデバイス容量のライブビデオを表示できます。

をクリック

関数の説明:

ドアの状態

ビデオをクリックして、デバイスのライブビデオを表示します。

ライブビュー起動時の音量を設定します。

注意

双方向オーディオを開始するときに音量を調整すると、繰り返し音が聞こえることがあります。

ライブビュー起動時に画像をキャプチャできます。

／／／

ドアの状態は、開/閉/開残/閉です。

ライブビュー起動時に録音できます。

ライブビュー起動時のストリーミングタイプを選択します。
メインストリーム、サブストリームから選択できます。

全画面表示。

管理ステータス

実際のニーズに応じて、開閉するドア、開いたままにするドア、閉じたままにするドアを制御できます。

リアルタイムのイベント

イベントのEmployee ID、Name、Card No、Event Type、Time、Operation を表示できます。
「詳細表示」をクリックして、イベント検索のページを入力することもできます。
イベントタイプの選択、従業員ID、名前、カード番号、開始時刻、終了時刻を入力し、検索をクリックできます。
結果が右パネルに表示されます。

リンクデバイス

リンクされたデバイスの数量とステータスを表示できます。

注意

「詳細表示」をクリックして、に移動できます。

個人情報

個人認証情報の追加された情報と追加されていない情報を表示できます。

ネットワークステータス

有線ネットワーク、無線ネットワークGuardingVision、ISUP、OTAP、VoIP の接続状態と登録状態を表示できます。

基本情報

モデル、シリアル番号、ファームウェアバージョンを表示できます。

デバイス容量

人物、顔、カード、イベント容量を表示できます。

10.8 アクセス制御アプリケーション

10.8.1 アンチパスバック設定

デバイス間のアンチパスバック機能では、設定されたルートに従って順番に認証を行う必要があります。サブデバイスのみがこの機能をサポートし、認証付きの一方向通過のみがサポートされます。

手順

1. アクセスコントロール→アクセスコントロールアプリケーション→クロスデバイスアンチパスバックをクリックします。
2. 機能を有効にします。
3. Main Device IP Address、Main Device Port No.、Main Device Passwordなどのアクセスコントローラのパラメータを設定します。
4. デバイス登録コードを設定し、登録状況を確認できます。
5. カードリーダを確認します。
   アンチパスバックでは、チェックマークの付いていないカードリーダは相互接続できません。

10.8.2 マルチドア連動設定

同じ入退室管理装置の複数のドア間で、マルチドアインタロックを設定します。
ドアを開くには、他のドアを閉じておく必要があります。

手順

1. 入退室管理 → Access Control Application →クロスデバイスマルチドアインターロックをクリックします。
2. 機能を有効にします。
3. デバイスタイプの選択
   - 本体に設定されている場合は、Port No.を設定し、「追加」をクリックしてアクセスポイントを追加する必要があります。
     デバイス管理 をクリックすると、デバイスのステータスを表示したり、デバイスを削除したりできます。
   - サブデバイスとして設定されているデバイスの場合、Main Device IP Address、Main Device Port No.、Main Device Passwordなどのアクセスコントローラパラメータを設定する必要があります。デバイス登録コードを設定し、登録状況を確認できます。カードリーダーを確認します。アンチパスバックでは、チェックマークの付いていないカードリーダーは相互接続できません。
4. アンチパスバックルールを
   設定します。
   認証ステータス別
   Anti-Passback カードによる認証により判定されるルーチン。
   実際のトラフィックステータス別
   アンチ・パスバック・ルーチンは実際のカード開封で判断されます。
5. OKをクリックします。

10.9 アクセスコントロールの管理

10.9.1 検索イベント

「イベント検索」をクリックして、「検索」ページに入ります。

イベントタイプ、従業員ID、名前、カード番号、開始時刻、終了時刻を含む検索条件を入力し、検索をクリックします。

結果が右パネルに表示されます。

10.9.2 ドアパラメータ設定

ドアをロック解除するためのパラメータを設定します。

ドア番号を選択

相対パラメータを設定するドアを選択します。

Access Control Parameter → ドアパラメータの順にクリックして設定ページに入ります。

ドアNo.を選択します。

通常、ドア1 が装置とリンクしたドアで、ドア2 が安全ドア制御ユニットとリンクしたドアです。

その他のドアパラメータを設定し、保存をクリックします。

デバイスオンラインステータスの表示

デバイスのステータスを表示して更新します。

入退室管理→Access Control Parameter →ドアパラメータの順にクリックして設定ページに入ります。

デバイスのオンラインステータスを表示できます。

Refresh(更新)をクリックしてデバイスのステータスを更新します。

ドア名の設定

ドア名を作成します。

入退室管理→Access Control Parameter → ドアパラメータ の順にクリックして設定ページに入ります。

ドア名を設定し、保存をクリックします。

PC Web 経由でのオープン継続時間の設定

カードをかざした後にドアロックが開くまでの時間を設定できます。

入退室管理→Access Control Parameter →ドアパラメータの順にクリックして設定ページに入ります。

開放時間、つまりドアがロック解除された後のアクション時間を設定します。
設定した時間内にドアが開かないと、ドアは自動的にロックされます。
設定可能な時間: 1 ～255 秒。
保存をクリックします。

PC Web 経由でのドア開放タイムアウトアラームの設定

ロック動作時間に達してもドアが閉まっていない場合、アクセスコントロールポイントからアラームが鳴ります。

入退室管理→Access Control Parameter → ドアパラメータ の順にクリックして設定ページに入ります。
ドア開タイムアウトアラームを設定します。
ロック動作時間に達してもドアが閉まっていない場合、アクセスコントロールポイントからアラームが鳴ります。
0に設定すると、アラームは有効になりません。
保存をクリックします。

ドア閉時のロックドアの設定

ドアを閉じた状態でロックドアを設定できます。

入退室管理→Access Control Parameter → ドアパラメータの順にクリックして設定ページに入ります。
ドア閉時にロックドアを有効にすることができます。
保存をクリックします。

PC Web 経由でのドア磁気センサータイプの設定

配線方法に応じて、ドアコンタクトタイプを選択できます。

入退室管理→Access Control Parameter →ドアパラメータの順にクリックして設定ページに入ります。
磁気センサタイプは、閉じたままか、開いたままにするかを選択します。
デフォルトでは、Remain Closed(特別なニーズを除く)。

保存をクリックします。

PC Web 経由で終了ボタンを設定します

実際の配線方法に従って、出口ボタンを開いたままにするか、閉じたままにします。

入退室管理→Access Control Parameter →ドアパラメータの順にクリックして設定ページに入ります。
終了ボタンの種類を設定します。
デフォルトでは、Remain Open (特別なニーズを除きます) です。
保存をクリックします。

PCのWeb経由でドアロックの電源オフ状態を設定します

ドアロックの電源がオフのときのドアロック状態を設定できます。

入退室管理→Access Control Parameter →ドアパラメータの順にクリックして設定ページに入ります。

ドアロックの電源オフステータスを設定します。

※デフォルトでは、閉じたままになります。

保存をクリックします。

PC Web 経由で拡張オープン継続時間を設定します

拡張アクセスが必要な人がカードをスワイプした後、適切な遅延でドアコンタクトを有効にすることができます。

Access Control → Parameter Settings → Door Parameters の順にクリックして設定ページに入ります。

拡張オープン継続時間を設定します。

拡張アクセスが必要な人がカードをスワイプした後、適切な遅延でドアコンタクトを有効にすることができます。

保存をクリックします。

PC Web 経由でFirst Person とのドア残りオープン期間を設定します

最初の人が許可されると、複数の人がドアやその他の認証アクションにアクセスできます。

Access Control → Parameter Settings → Door Parameters の順にクリックして設定ページに入ります。ファーストパーソンがいるときのドアの開放時間を設定し、保存をクリックします。

パソコンのWeb経由で暗証番号を設定します

脅迫コードを設定した後、脅迫に遭遇したら、コードを入力してドアを開きます。
同時に、アクセス・コントロール・システムは脅迫イベントを報告します。

Access Control → Parameter Settings → Door Parameters の順にクリックして設定ページに入ります。脅迫コードを設定し、保存をクリックします。

注意

脅迫コードとスーパーパスワードは複製できません。
通常は4～8桁で構成されます。

パソコンのWeb経由でスーパーパスワードを設定します

管理者または指定された人がスーパーパスワードを入力してドアを開くことができます。

Access Control Parameter → ドアパラメータ の順にクリックして設定ページに入ります。

スーパーパスワードを設定すると、指定された人がスーパーパスワードを入力してドアを開くこ

とができます。

保存をクリックします。

注意

脅迫コードとスーパーパスワードは複製できません。
通常は4～8桁で構成されます。

10.9.3 認証設定

PC Web 経由でメインまたはサブカードリーダーを選択

個人認証用の端末を設定します。

入退室管理→Access Control Parameter → 認証設定 の順にクリックして、設定ページに入ります。

端末をメインまたはサブカードリーダーとして選択します。

その他のパラメータを設定し、保存をクリックします。

PC Web 経由でのターミナルタイプとモデルの表示

ターミナルタイプとモデルを表示できます。

入退室管理→Access Control Parameter → 認証設定 の順にクリックして、設定ページに入ります。

ターミナルタイプとターミナルモデルの表示。

PC Web 経由の認証デバイスの有効化

有効にすると、認証端末をカードスワイプに使用できます。

手順

1. 入退室管理→Access Control Parameter → 認証設定 の順にクリックして、設定ページに入ります。
2. 認証デバイスを有効にします。有効にすると、ターミナルは通常のカードスワイプに使用できます。
3. 保存をクリックします。

PC Web 経由での認証の設定

認証を設定します。

Access Control Parameter → 認証設定 の順にクリックして、設定ページに入ります。

ターミナルとしてメインカードリーダーを選択すると、ドロップダウンリストから認証を選択できます。
複数の認証がある場合は、単一資格情報認証タイムアウトと初期認証タイプの制御を設定する必要があります。

単一クレデンシャル認証タイムアウト

各証明書の期間を設定できます。

注意

パスワード認証のタイムアウトはデフォルトで20 秒ですが、これは上記の設定による制限を受けません。

初期認証タイプの制御

有効にすると、選択したすべてのタイプを初回認証に使用できます。

ターミナルとしてサブカードリーダーを選択すると、ドロップダウンリストから認証を選択できます。

保存をクリックします。

PC Web でフェイス経由の認証を手動でトリガーします

顔による認証の手動トリガーを有効にした後、顔認識のためにデバイスの画面を手動でタッチする必要があります。

Access Control Parameter → 認証設定 の順にクリックして、設定ページに入ります。

メインカードリーダーがターミナルとして選択されている場合、をクリックして顔による認証の手動トリガーを有効にし、認証モードを選択します。

単一認識

前の顔認識が完了したら、成功したか失敗したかにかかわらず、画面をタップして次の認識をトリガーする必要があります。

連続

認識をトリガーすると、デバイスがスリープモードに入るまで、顔経由で認識できます。

保存をクリックします。

パソコンのWeb経由で認識間隔を設定します

認証時に顔を連続で認識する時間間隔を設定します。

Access Control Parameter → 認証設定 の順にクリックして、設定ページに入ります。

端末をメインまたはサブカードリーダーとして選択した場合は、認識間隔を設定し、保存をクリックします。

注意

1～10の数字を入力してください。

PC Web 経由での認証間隔の設定

認証時に同じ相手の認証間隔を設定できます。同じ人が認証できるのは、設定された間隔内の1 回だけです。2 回目の認証は失敗します。
設定された間隔で他の人が認証すると、その人は再度認証を受けることができます。

Access Control Parameter → 認証設定 の順にクリックして、設定ページに入ります。

端末をメインカードリーダーとして選択した場合は、認証間隔を設定し、保存をクリックします。

最大アラームを有効にします。PC Web 経由の失敗試行

カードの読み取り試行が設定値に達したときにアラームを報告するようにします。

Access Control Parameter→ 認証設定 の順にクリックして、設定ページに入ります。

端末をメインまたはサブカードリーダーとして選択すると、スライドして最大のアラームを有効にします。失敗した試行、および最大を設定します。

認証失敗の試行。

保存をクリックします。

PC Web 経由の改ざん検出の有効化/無効化

改ざん検出を有効にすると、カードリーダが取り外されたとき、または取り外されたときに、デバイスが自動的に改ざんイベントを生成します。

Access Control Parameter → 認証設定 の順にクリックして、設定ページに入ります。

実際のニーズに応じて、改ざん検出を有効または無効にします。

機能を有効にすると、カードリーダが取り外されるか取り外されると、デバイスは自動的に

改ざんイベントを生成します。
この機能を無効にすると、アラームイベントは生成されません。

保存をクリックします。

PC Web 経由のカード番号反転の有効/無効

カードNo.反転機能の有効/無効を設定します。

Access Control Parameter → 認証設定 の順にクリックして、設定ページに入ります。

カードNo.反転を有効にすると、読み出したカードNo.が逆順になります。

保存をクリックします。

サブカードリーダー位置の設定

サブカードリーダーの位置を選択できます。

Access Control Parameter → 認証設定 の順にクリックして、設定ページに入ります。

ターミナルでサブカードリーダーを選択した場合は、メインカードリーダーとは異なる面、
またはメインカードリーダーと同じ面としてサブカードリーダーの位置を選択できます。

PC Web 経由でコントローラとの通信を設定します

サブカードリーダーごとにコントローラとの通信を設定できます。
カードリーダが設定した時間内にアクセスコントローラと接続できない場合、カードリーダはオフラインです。

Access Control Parameter → 認証設定 の順にクリックして、設定ページに入ります。

端末をサブカードリーダーとして選択した場合は、「コントローラごとの通信」を設定し、「保存」をクリックします。

Webクライアントからパスワードを入力するまでのタイムアウト時間を設定します

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

Access Control Parameter → 認証設定 の順にクリックして、設定ページに入ります。

ターミナルとしてサブカードリーダーを選択すると、Max を設定できます。
パスワードを入力して保存をクリックする間隔。

PC Web経由でOK LED極性とエラーLED極性を設定

デフォルトの正極性で、実際の配線に従ってOK およびERR インターフェースのダイオードの極性を選択します。

Access Control Parameter →認証設定 の順にクリックして、設定ページに入ります。

サブカードリーダーとして端子を選択した場合は、OK LED極性とエラーLED極性を設定し、保存をクリックします。

10.9.4 認証連携設定

認証連携の設定を行います。

手順

1. Access Control Parameter → 認証設定 の順にクリックして、設定ページに入ります。
2. 連動機能を設定します。

認証済みの場合のコールへのリンク

これを有効にすると、個人が認証をパスした場合、ボタン設定の呼び出しターゲットを自動的に呼び出し、リモートでドアを開きます。

認証に失敗した場合のコールへのリンク

有効にすると、認証に失敗した試行が設定した回数に達した場合、ボタン設定の呼び出しターゲットを自動的に呼び出してリモートでドアを開きます。

3. 保存をクリックします。

10.9.5 認証計画の設定

認証計画を設定できます。

入退室管理→Access Control Parameter → 認証設定の順にクリックして、設定ページに入ります。

認証タイプを選択し、時間バーで期間をドラッグします。

保存をクリックします。

10.9.6 顔パラメータの設定

Webブラウザによるフェイスアンチスプーフィングの有効化/無効化

有効にすると、デバイスは人物がライブであるかどうかを認識できます。

入退室管理→Access Control Parameter → スマート の順にクリックして、設定ページに入ります。フェイスアンチスプーフィングを有効にし、「保存」をクリックします。

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

顔重複チェックの有効化/無効化

顔の重複チェックを有効にし、人物の顔を追加するたびに、顔の重複がチェックされます。
顔の重複が検出されると、プロンプトが表示されます。

注意

顔を遠隔で追加したり、顔を一括で適用したりする場合は、サポートされません。

入退室管理→Access Control Parameter → スマート の順にクリックして、設定ページに入ります。

顔重複チェックを有効にし、保存をクリックします。

PC Web 経由のスプーフィング対策検出レベルの設定

フェイスアンチスプーフィング機能を有効にした後、ライブフェイス認証を実行するときに、一致するセキュリティレベルを設定できます。

Access Control → Parameter Settings → Smart の順にクリックして、設定ページに入ります。
スプーフィング対策検出レベルを選択し、「保存」をクリックします。
一般、上級、プロフェッショナルから選択できます。
レベルが高いほど偽の認識率が低くなり、拒否率が高くなります。

パソコンのWeb経由で認識距離を設定します

認証ユーザーとデバイスカメラの距離を設定できます。

入退室管理→Access Control Parameter → Smart の順にクリックして、

設定ページに入ります。

認識距離を選択し、保存をクリックします。

PC Web 経由でのピッチ角度の設定

顔認識・認証時のレンズのピッチ角度を設定できます。

入退室管理→Access Control Parameter Settings → スマート の順にクリックして、

設定ページに入ります。

注意

モデルによって異なるパラメータをサポートする場合があります。実際のページを参照してください。

「ピッチアングル」を設定し、「保存」をクリックします。

PC Web 経由でYaw Angle を設定します

顔認識・認証時のレンズのヨー角度を設定できます。Access Control Parameter →

スマート の順にクリックして、設定ページに入ります。

注意

モデルによって異なるパラメータをサポートする場合があります。実際のページを参照してください。

角度を設定し、「保存」をクリックします。

パソコンのWeb経由で適用するときの顔の画質のグレードを設定します

顔認証のグレードは、成功するにはしきい値よりも高くする必要があります。

Access Control Parameter → スマート の順にクリックして、設定ページに入ります。

注意

モデルによって異なるパラメータをサポートする場合があります。
実際のページを参照してください。

Face Picture Quality Grade for Apply を設定すると、顔認証のグレードがしきい値より高くなる必要があります。
保存をクリックします。

PC Web で1:1 Face Grade Threshold を設定します

フェイスグレードしきい値を1:1 に設定します。

入退室管理→Access Control Parameter→スマートと移動します。1:1 Face Picture Grade Threshold を設定し、Save をクリックします。
しきい値を高くするほど、前面カメラの取り込み画像の品質に対する要求が高くなり、認証失敗のプロンプトが容易になります。

PC Web 経由で顔1:1 一致しきい値を設定

面1:1 一致しきい値を設定します。

Access Control → Parameter Settings → Smart の順にクリックして、設定ページに入ります。

1:1 の一致しきい値を設定し、保存をクリックします。
しきい値の値が大きいほど、障害許容率は低くなり、顔経由で認証する場合の誤拒否率は高くなります。
最大値は100 です。

PC Web 経由で1:N 一致しきい値を設定

顔1:N マッチングのマッチングしきい値を設定できます。

入退室管理 → Access Control Parameter → スマート の順にクリックして、設定ページに入ります。

1:N 一致しきい値を設定し、保存をクリックします。
値が大きいほど、誤受理率は小さくなり、誤拒否率は大きくなります。
最大値は100 です。

Webブラウザで顔認証エリアを設定します

顔認識・認証時のレンズの認識範囲を設定します。

入退室管理→Access Control Parameter→スマート→エリア設定 の順にクリックして、設定ページに入ります。
プレビュー画面の黄色のボックスをドラッグして、左右、上下の顔認識の有効領域を調整します。

または、ブロックをドラッグするか、数値を入力して有効エリアを設
定します。保存をクリックします。
クリック , , またはフルスクリーン表示にするには、キャプチャ、録画、または移動します。

PC Web 経由のECO モードの有効化/無効化

ECO モードが有効になっている場合は、赤外線カメラを使用して、薄暗い環境または暗い環境で顔を認証できます。

Access Control → Parameter Settings → Smart の順にクリックして、設定ページに入ります。

ECO モードが有効になっている場合は、赤外線カメラを使用して、薄暗い環境または暗い環境で顔を認証できます。
ECOモード(1:N)とECOモード(1:1)を設定できます。

マスク検出付き顔が有効な場合は、顔マスク検出パラメータも設定できます。

ECO モード(1:1)しきい値

ECO モード1:1 マッチングモードで認証する場合のマッチングしきい値を設定します。

値が大きいほど、誤受理率は小さくなり、誤拒否率は大きくなります。

最大値は100 です。

ECO モード(1:N)しきい値

ECO モード1:N マッチングモードで認証する場合のマッチングしきい値を設定します。

値が大きいほど、誤受理率は小さくなり、誤拒否率は大きくなります。

最大値は100 です。

マスク1:1 一致しきい値(ECO)の面

ECOモード1:1マッチングモードでフェイスマスクで認証する場合のマッチングしきい値を設定します。
値が大きいほど、誤受理率は小さくなり、誤拒否率は大きくなります。

最大値は100 です。

マスク1:N 一致しきい値(ECO)の面

ECOモード1:Nマッチングモードでフェイスマスクで認証する場合のマッチングしきい値を設定します。
値が大きいほど、誤受理率は小さくなり、誤拒否率は大きくなります。

最大値は100 です。

保存をクリックします。

PC Web 経由でのマスク検出による顔の有効化/無効化

マスク検出で顔を有効にすると、システムはマスク画像でキャプチャされた顔を認識します。

Access Control → Parameter Settings → Smart の順にクリックして、設定ページに入ります。

マスク検出で顔を有効にした後、マスクストラテジを使用せずに顔、マスクと顔(1:1)、マスク1:N 一致しきい値で顔(ECO)、マスク1:1 一致しきい値で顔、マスク1:N 一致しきい値で顔(ECO)を設定できます。

マスクストラテジのない面

「なし」、「フェイスマスク装着の注意」、「フェイスマスク着必須」を選択できます。

フェイスマスク装着時の注意事項

認証時に顔マスクを装着しないと、デバイスがプロンプトを表示し、ドアが開きます。

フェイスマスクを着用する必要

認証時に顔マスクを装着しないと、デバイスがプロンプトを表示し、ドアが閉じたままになります。

マスク&フェイス付きフェイス(1:1)

1:1照合モードでフェイスマスクで認証する場合の照合値を設定します。

値が大きいほど、誤受理率は小さくなり、誤拒否率は大きくなります。

最大値は100 です。

マスク付き面&面(1:N)

1:Nマッチングモードでフェイスマスクで認証する場合のマッチングしきい値を設定します。

値が大きいほど、誤受理率は小さくなり、誤拒否率は大きくなります。

最大値は100 です。

マスク1:1 一致しきい値(ECO)の面

ECOモード1:1マッチングモードでフェイスマスクで認証する場合のマッチング値を設定します。

しきい値が大きいほど、顔認証時の認識エラー率が低くなり、拒否率が高くなります。

最大値は100 です。

マスク1:N 一致しきい値(ECO)の面

ECOモード1:Nマッチングモードでフェイスマスクで認証する場合のマッチング値を設定します。

しきい値が大きいほど、顔認証時の認識エラー率が低くなり、拒否率が高くなります。

最大値は100 です。

保存をクリックします。

10.9.7 カード設定

Webクライアント経由でのM1カードの有効化/無効化

有効にすると、デバイスはM1 カードを認識し、ユーザーはデバイス経由でM1 カードをスワイプできます。

Access Control → Parameter Settings → Card Settings の順にクリックして、設定ページに入ります。

クリックしてM1 カードを有効にします。

M1 カードの暗号化

M1カード暗号化を有効にすると、エントランスカードのセキュリティレベルを向上できます。
そのため、エントランスカードのコピーが困難になります。

セクタ

M1 カード暗号化を有効にした後、暗号化セクタを設定する必要があります。

注意

セクタ13を暗号化することをお勧めします。

保存をクリックします。

DESFire カードの設定

DESFire カードの読み取りコンテンツを有効にできます。
Parameter Settings → Card Settings をクリックして、設定ページに入ります。
Enable DESFire Card and DESFire Card Read Content を選択し、Save をクリックします。

注意
デュアル周波数カードモジュールが接続されている場合、
EM カードとDESfire カードの両方を同時にスワイプできます。
ただし、デバイス上のカードのスワイプは無効です。

FeliCaカードを設定します

FeliCaカードを有効にします。

Parameter Settings → Card Settings をクリックして、設定ページに入ります。

「FeliCaカード有効」を選択します。

Web 経由でのカード番号認証パラメータの設定

デバイスでカード経由で認証するときのカード読み取り内容を設定します。

アクセスコントロール→パラメータ設定→カード設定と移動します。

カード認証モードを選択し、保存をクリックします。

カード番号フル

すべてのカード番号が読み出されます。

3バイト

デバイスは、読み取り3バイトを介してカードを読み取ります。

4バイト

デバイスは4 バイトを介してカードを読み取ります。

10.9.8 リモート検証の設定

デバイスは個人の認証情報をプラットフォームにアップロードします。

プラットフォームはドアを開くかどうかを判断します。

アクセスコントロール→パラメータ設定→ターミナルパラメータと移動します。

パラメータが設定されたら、ClickSave をクリックします。

リモート検証

リモート検証を有効にした後、認証時に、デバイスは認証情報をプラットフォームにアップロードし、

プラットフォームはドアを開くかどうかを確認します。

リモートでの個人タイプの確認

リモートで個人のタイプを確認して選択します。

ローカルでの認証情報の確認

機能を有効にすると、デバイスは権限を確認しますが、計画テンプレートは見積もりません。

リモート検証のタイムアウト時間

リモート検証のタイムアウト時間を設定します。

オフラインリモート検証ロック解除

オフラインリモート検証のロック解除を有効にできます。

結果戻りモード

結果の戻りモードを設定します。

10.9.9 プライバシー設定

PC Web ブラウザでイベントストレージタイプを設定します

イベントストレージタイプを設定できます。

入退室管理→Access Contorol Parameter →プライバシー設定 の順にクリックして設定ページに入ります。

イベントストレージタイプは、古いイベントの定期的な削除、指定時間ごとの古いイベントの削除、または上書きとして選択できます。

古いイベントを定期的に削除します

ブロックをドラッグするか番号を入力して、イベントの削除期間を設定します。
設定された期間に従って、すべてのイベントが削除されます。

指定時刻による古いイベントの削除

時間を設定すると、設定した時間にすべてのイベントが削除されます。

上書き

最も早い5%のイベントは、保存されているイベントが全領域の95%を超えていることをシステムが検出すると削除されます。

保存をクリックします。

PC Web 経由での認証結果の設定

画像、名前、従業員ID、温度などの認証結果の内容を設定します。

入退室管理→Access Contorol Parameter →プライバシー設定の順にクリックします。
画像、名前、従業員IDなど、認証結果の表示内容を確認します。
Name De-identificationとID De-identificationを実際のニーズに応じてチェックします。
識別を解除すると、名前とID にコンテンツの一部が表示されます。
認証結果表示期間を設定すると、認証結果に設定した期間が表示されます。
保存をクリックします。

PC Web を使用した画像のアップロードと保存の設定

画像のアップロードと保存パラメータを設定できます。

入退室管理 → Access Contorol Parameter → プライバシー設定 の順にクリックして設定ページに入ります。

認証時に画像を保存。

自動認証時に画像を保存します。

認証時に画像をアップロードします。

プラットフォームへの認証時に自動的に画像をアップロードします。

ピクチャーモード

デフォルトとして選択すると、デバイスはパノラマビューをキャプチャします。
最大画像サイズと画像解像度を設定できます。
マッティングピクチャーモードとして選択すると、デバイスは顔のみをキャプチャします。
最大画像サイズを設定します。

登録画像保存

登録した顔写真は、機能を有効にするとシステムに保存されます。

リンクキャプチャ後の画像の保存

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。

リンクキャプチャ後に画像をアップロード

リンクカメラで撮影した画像をプラットフォームに自動的にアップロードします

通話中に撮影した画像をアップロードします

有効にすると、通話中に自動的に画像がキャプチャされ、自動的にアップロードされます。
保存をクリックします。

PC Web 経由でデバイス画像をクリア

登録、認証、撮影した顔や画像をすべて消去します。

入退室管理 → Access Contorol Parameter → プライバシー設定 の順にクリックして設定ページに入ります。

クリアをクリックすると、登録済み、認証済み、キャプチャされた顔画像、またはパームプリント画像がすべてクリアされます。

PCのWeb経由でPINモードを設定します

設定を行う前に、PIN がプラットフォームに適用された個人用PIN またはデバイス設定の個人用PIN であることを確認してください。

PIN がデバイス設定の個人用PIN の場合、デバイスまたはPC Web でPIN を編集できますが、プラットフォームでは設定できません。

PIN がプラットフォームに適用された個人用PIN の場合は、プラットフォームでPIN を設定する必要がありますが、デバイスまたはPC Web では設定しないでください。

アクセスコントロール→パラメータ設定→プライバシー設定と移動します。

PINモードモジュールでは、次のパラメータを設定できます。

パラメータ設定後に保存をクリックします。

プラットフォーム対応パーソナルPIN

プラットフォームで個人PIN を作成できます。

※PIN をデバイスに適用する必要があります。

デバイスまたはPC Web でPIN を作成または編集することはできません。

デバイスセットパーソナルPIN

デバイスまたはPC Web でPIN を作成または編集できます。

プラットフォームではPIN を設定できません。

保存をクリックします。

10.9.10 通話

設定

Web経由でデバイス番号を設定します

このデバイスは、ドアステーションまたは外部ドアステーションとして使用できます。

使用前にデバイス番号を設定してください。

ビデオインターコム→通話設定→デバイス番号をクリックします。

図10-1 デバイス番号の設定

デバイスタイプをドアステーションに設定すると、フロア番号、ドアステーション番号、コミュニティ番号、建物番号、ユニット番号を設定できます。

デバイスタイプ

このデバイスは、ドアステーションまたは外部ドアステーションとして使用できます。

ドロップダウンリストからデバイスの種類を選択します。

注意

デバイスタイプを変更した場合は、デバイスを再起動する必要があります。

フロア番号

デバイスの設置フロア番号を設定します。

ドアステーション番号

デバイスの設置フロア番号を設定します。

注意

- 番号を変更した場合は、デバイスを再起動してください。
- メイン扉のステーションNo.は0、サブ扉のステーションNo.は1～16です。

コミュニティ番号

デバイスコミュニティ番号を設定します。

ビル番号

デバイスのビルド番号を設定します。

ユニット番号

デバイスユニット番号を設定します。

注意

番号を変更した場合は、デバイスを再起動してください。

設定後に設定を保存するには、保存をクリックします。

機器種別を「外部ドア」または「局番」に設定した場合は、外部ドア局番、コミュニティ番号を設定できます。

屋外ドアステーション番号

デバイスタイプとして外側のドアステーションを選択した場合は、1～の数値を入力する必要があります

注意

番号を変更した場合は、デバイスを再起動してください。

コミュニティ番号

デバイスコミュニティ番号を設定します。

Web ブラウザを使用したビデオインターコムネットワークパラメータの設定

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

Video Intercom → Call Settings → Video Intercom Network の順にクリックして、設定ページに入ります。

登録パスワード

通信用の親局の登録パスワードを設定します。

通信用の親局の登録パスワードを設定します。

メインステーションIP

通信に使用するメインステーションのIP アドレスを入力します。

プライベートサーバーIP

SIP サーバIP を指します。

通信に使用するメインステーションのIP アドレスを入力します。
このとき、メインステーションはSIP サーバとして使用されます。

他のインターコムデバイスは、このサーバアドレスに登録して通信を実現する必要があります。

プロトコル1.0を有効にします

有効にすると、古いプロトコルバージョンでドアステーションをメインステーションに登録できます。

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

図10-2 ビデオインターコムネットワーク

コンフィグレーション後、アクセス制御装置とビデオインターコムドアステーション、屋内ステーション、メインステーション、プラットフォームなどの間の通信を実現できます。

保存をクリックします。

PCのWeb経由で通信時間を設定します

最大通信時間を設定します。

ビデオインターコム→通話設定と移動します。

Max を入力します。

通信時間：自動応答を有効にできます。

注意

最大通信時間の範囲は90s ～ 300s です。

保存をクリックします。

ボタンを押してPCのWeb経由で電話をかけます

手順

1. ビデオインターコム→ボタンを押下して呼び出すをクリックして、設定ページに入ります。

図10-3 ボタンを押して呼び出し

2. 必要に応じて、コール指定屋内ステーション、コール管理センター、コール屋内ステーションまたはAPP を選択します。

注意

フロア番号を入力した場合は、部屋番号の室番も入力する必要があります。

3. 必要に応じて、コールへのリンク認証を有効にします。
   有効にすると、個人が認証をパスしたときに、自動呼び出し用のボタンが設定されているターゲットによってドアがリモートで開かれます。
4. 保存をクリックします。

通話優先度

通話優先度を設定します。

手順

1. 「ビデオインターコム」→「通話設定」→「通話優先順位」の順にクリックして、設定ページに入ります。
2. 発信の種類を確認し、3つの優先順位ごとに呼出時間を設定します。
3. 保存をクリックして設定を有効にします。

注意

レベルが高いほど、デバイスの呼び出しが簡単になります。

通話時間が終了すると、次のレベルの通話がトリガーされます。

PC Web 経由の番号設定

部屋のSIP番号を設定します。

部屋はSIP番号を介して互いに通信することができます。

手順

1. ビデオインターコム→番号設定と移動します。

図10-4 数値設定

2. 「追加」をクリックし、部屋番号とSIP1電話番号を入力します。
3. 必要に応じて、「Add」をクリックしてSIP 番号を追加するか、をクリックして番号を削除します。
4. ClickSave.
5. (オプション) 「削除(Delete)」をクリックすると、部屋番号とそのSIP 番号を削除できます。

10.10　デバイス管理

機器番号、タイプ、IP、シリアル番号、モデル、バージョン、フロア番号、ルーム番号、番号、アーミング状態、ユーザ名、ネットワーク状態、操作を表示できます。また、デバイス管理ページで室内ステーションやサブドアステーションを追加したり、デバイスの管理、アップグレード、削除を行うこともできます。

手順

1. デバイス管理をクリックします。
2. 追加をクリックします。
3. デバイスタイプを選択し、ユーザー名 (admin固定)、デバイスパスワード、登録パスワード、シリアル番号の入力をします。
4. ネットワークパラメータ

IPアドレス・IPv4サブネットマスク・IPv4デフォルトゲートウェイを入力します。
デバイス番号を入力します。※フロア番号.・部屋番号を入力

5. 保存をクリックします。
6. 次の操作も実行できます。

デバイスの削除　デバイスを削除する必要があることを確認し、削除をクリックします。

デバイスのインポートUSBフラッシュドライブ(デバイス情報を含みます)を
デバイスに差し込み、をクリックします

インポートしてデバイス情報をインポートします。

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

10.11　システム設定

10.11.1　PC Web 経由でのデバイス情報の表示

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

「システムとメンテナンス」→「システム設定」→「システム設定」→「基本情報」をクリックして、設定ページを開きます。

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

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

10.11.2　時刻設定

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

システムとメンテナンス→システム欄のシステム設定→時間設定をクリックします。

図10-5 時間設定

設定後に設定を保存するには、保存をクリックします。

時間帯

ドロップダウンリストからデバイスの検出されたタイムゾーンを選択します。

時刻同期。

NTP

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

マニュアル

デフォルトでは、デバイスの時刻は手動で同期する必要があります。

デバイスの時刻を手動で設定するか、Sync。with Computer Time(コンピュータの時刻と同期)をオンにして、デバイスの時刻をコンピュータの時刻と同期させることができます。

サーバアドレスタイプ/サーバアドレス/NTP ポート/間隔

サーバアドレスタイプ、サーバアドレス、NTP ポート、インターバルを設定できます。

10.11.3 管理者パスワードの変更

手順

1. システムとメンテナンス→システム構成→システム→ユーザー管理→ユーザー管理の順にクリックします。
2. クリッ.

3.古いパスワードを入力し、新しいパスワードを作成します。
4.新しいパスワードを確認します。
5.保存をクリックします。

注意

デバイスのパスワード強度は自動的に確認できます。

製品のセキュリティを高めるために、独自に選択する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、パスワードを月次または週次で変更すると、
製品をより適切に保護できます。
すべてのパスワードとその他のセキュリティ設定を適切に設定することは、
インストーラまたはエンドユーザの責任です。

10.11.4 PC Web 経由のアカウントセキュリティ設定

セキュリティの質問と回答、またはデバイスの電子メールアドレスを変更できます。

設定を変更した後、デバイスパスワードを忘れた場合は、新しい質問に答えるか、
新しい電子メールアドレスを使用してデバイスパスワードをリセットする必要があります。

手順

1.システムとメンテナンス→システム構成→システム→ユーザー管理→ユーザー管理→アカウントセキュリティ設定の順にクリックします。
2.実際のニーズに応じて、セキュリティに関する質問または電子メールアドレスを変更します。
3.デバイスパスワードを入力し、OK をクリックして変更を確認します。

10.11.5 PC Web 経由でのデバイスのアーミング/消滅情報の表示

デバイスのアーミングタイプとアーミングIP アドレスを表示します。

システムとメンテナンス→システム設定→ユーザー管理→**警戒/警戒解除情報を表示できます。**

更新をクリックしてページを更新します。

10.11.6 PC Web 経由での作業モードの設定

デバイスのターミナルパラメータを設定できます。

注意

一部のモデルのみがこの機能をサポートしています。

特定のデバイスを参照してください。

入退室管理→Access Control Parameters の順にクリックして、設定ページに入ります。

作業モード

作業モードは、アクセス制御モードまたはパーミッションフリーモードとして設定できます。

アクセス制御モード

アクセス制御モードは、デバイスのノーマルモードです。

アクセスするための認証情報を認証する必要があります。

10.11.7 ネットワーク設定

PC Web 経由での基本的なネットワークパラメータの設定

システムとメンテナンス→システム欄のネットワーク設定部分の TCP/IP の順にクリックします。

図10-6「TCP/IP 設定」ページ

パラメータを設定し、保存をクリックして設定を保存します。

NIC タイプ

ドロップダウンリストからNIC タイプを選択します。

デフォルトでは、Auto です。

DHCP

チェックを外した場合は、IPv4アドレス、IPv4サブネットマスク、IPv4デフォルトゲートウェイ、Macアドレス、MTUを設定してください。

機能を確認すると、IPv4 アドレス、IPv4 サブネットマスク、IPv4 デフォルトゲートウェイが自動的に割り当てられます。

DNSサーバ

実際の必要に応じて、優先DNS サーバと代替DNS サーバを設定します。

Wi-Fi パラメータの設定

デバイスのワイヤレス接続用のWi-Fi パラメータを設定します。

手順

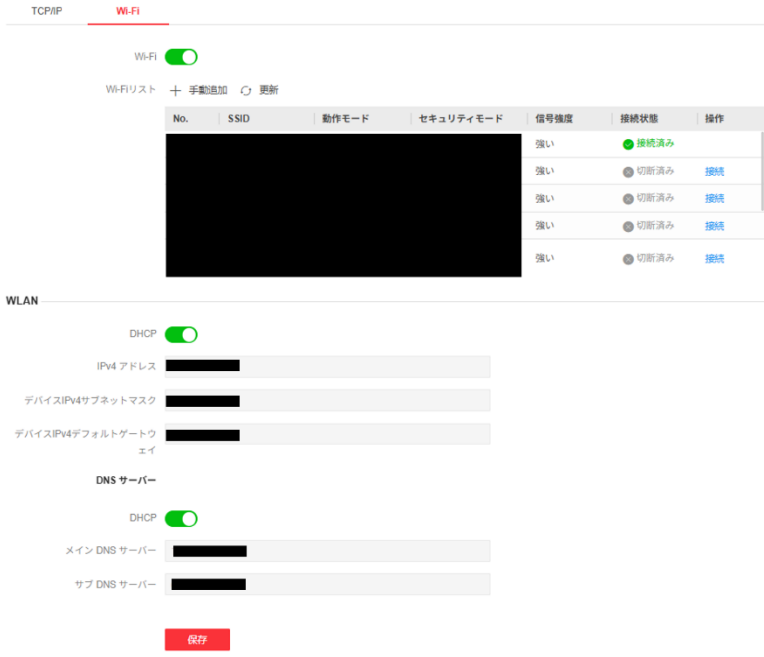
注意

この機能はデバイスでサポートされている必要があります。

1. システムとメンテナンス→システム欄のネットワーク部分にあるネットワーク設定→ WiFi の順にクリックします。

図10-7 Wi-Fi 設定ページ

2. Wi-Fi を確認します。
3. Wi-Fiを選択



- リスト内のWi-Fi をクリックし、Wi-Fi パスワードを入力します。
- 追加をクリックし、Wi-Fi の名前、パスワード、および暗号化タイプを入力します。
- 接続をクリックします。
- Wi-Fi が接続されたら、OK をクリックします。

4. WLAN パラメータを設定します。

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

5.保存をクリックします。

PC Web 経由でのポートの設定

システムとメンテナンス→システム欄のネットワーク部分のネットワークサービスへ移動します。

HTTP の有効化/無効化

HTTP 機能を有効にすると、ブローサーの訪問セキュリティが向上します。

システムとメンテナンス→システム欄のネットワーク部分にあるネットワークサービスから HTTP(S)

へ移動します。

パラメータが設定されたら、ClickSave をクリックします。

HTTP ポート

ブラウザでログインする場合は、アドレスの後に変更したポート番号を追加する必要があります。

たとえば、HTTP ポート番号が81 に変更された場合、ブラウザでログインするときに
http://192.0.0.65:81 と入力する必要があります。

HTTPS ポート

Visiting ブラウザのHTTPS ポートを設定します。

ただし、認証が必要です。

HTTP リスニング

デバイスは、HTTP プロトコルによって宛先IP またはドメイン名にアラーム情報を送信します。

宛先IP またはドメイン名はHTTP プロトコルをサポートする必要があります。

宛先IP またはドメイン名、URL、およびポートを入力します。プロトコルタイプを選択します。

PC Web 経由でRTSP ポートを表示します

RTSPポートは、リアルタイムストリーミングプロトコルのポートです。

システムとメンテナンス→システム欄のネットワーク部分のネットワークサービスからRTSP と移動します。

ポートを表示します。

PC Web 経由でWebSocket を設定します

WebSocket およびWebSockets ポートを表示します。

システムとメンテナンス→システム欄のネットワーク部分のネットワークサービス→ WebSocket(s)
へ移動します。
WebSocket およびWebSockets のポートがともに表示されます。

SDK サービスの有効化

SDK サービスを有効にした後、デバイスをSDK サーバに接続できます。

システムとメンテナンス→システム欄のネットワーク部分にあるデバイスアクセス→ SDKサーバー
の順にクリックして、設定ページに入ります。
サーバーポートを入力します。
保存をクリックして設定を有効にします。

PC Web 経由でのISUP パラメータの設定

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

手順

注意

この機能はデバイスでサポートされている必要があります。

1. システムとメンテナンス→システム設定→ネットワークのデバイスアクセス→ ISUPをクリックします。
2. 有効をチェックします。
3. ISUP のバージョン、サーバアドレス、デバイスID、およびISUP ステータスを設定します。

注意

バージョンとして5.0 を選択されます。
※暗号化キーも設定する必要があります。

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

PC Web 経由でOTAP を設定します

OTAPプロトコルを介してデバイスをプラットフォームに接続し、デバイス情報の取得、動作ステータスとアラーム情報のアップロード、デバイスの再起動とアップグレードを行います。

手順

1. システムとメンテナンス→システム設定→ネットワーク→デバイスアクセス→ OTAPをクリックします

図10-8 OTAP の設定

2. OTAPを有効にするをクリックします。
3. サーバのIPアドレス、ポート、デバイスID、暗号化キーを設定します。
4. Test(テスト)をクリックして、デバイスがサーバに接続して正常に登録できることを確認します。
   ページを更新するか、デバイスを再起動して、レジスタステータスを確認します。
5. 「その他」をクリックすると、ネットワークの種類とアクセスの優先順位が表示されます。
   操作アイコンを上下にドラッグして、ネットワーク優先度を調整します。
6. 保存をクリックします。

PC Web 経由のプラットフォームアクセス

プラットフォームアクセスでは、プラットフォームを介してデバイスを管理するオプションが提供されます。

手順

1. システムとメンテナンス→システム構成→ネットワーク→デバイスアクセス→Guariding Visionの順にクリックして、設定ページに入ります。

注意

GuardingVision は、モバイルデバイス用のアプリケーションです。

アプリでは、デバイスのライブ画像の表示、アラーム通知の受信などを行うことができます。

2. 有効をチェックして機能を有効にします。
3. 「カスタム」のチェックボックスをオンにすると、自分でサーバアドレスを設定できます。

4. 確認コードを入力します。
5. デバイスのQRコードを表示するには、表示をクリックします。QR コードをスキャンしてアカウントをバインドします。

注意

8～32文字(a～z、A～Z)または数字(0～9)で、大文字と小文字を区別します。
8文字以上の英数字を組み合わせて使用することをお勧めします。

6. 保存をクリックして設定を有効にします。

VoIP アカウント設定

ネットワークで音声通話を実現できます。

手順

1. システムとメンテナンス→システム欄のネットワーク→デバイスアクセス→ VoIPへ移動します。
2. コールタイプを選択し、VoIP 1/2/3のどれかを選択します。
3. VoIPゲートウェイを有効化をONにします。
4. 登録ユーザ名、登録したパスワード、サーバーのIPアドレス、サーバーポート、有効期限、
5. 登録状況、番号、ユーザ名の表示とセンター番号を設定します。
6. 保存をクリックします。

10.11.8 PC Web 経由でのビデオおよびオー

ディオパラメータの設定Web ブラウザ経由でのビ

デオパラメータの設定

デバイスカメラの品質、解像度などのパラメータを設定できます。

システムとメンテナンス→システム欄のビデオとオーディオの順にクリックして、設定ページに入ります。

・カメラ名

・ストリームタイプ (メイン・サブストリーム まで)

・ビデオタイプ (ビデオストリーム・映像＆音声)

・解像度(1920×1080・1280×720)

・ビットレートタイプ (定数・可変)

・ビデオの品質

・フレームレート

・最大ビットレート

・ビデオエンコーディング

・Iフレーム間隔を設定します。

保存をクリックします。

Web ブラウザを使用したオーディオパラメータの設定

機器の音量を設定します。

システムとメンテナンス→システム欄のビデオとオーディオの順にクリックして、設定ページに入ります。

実際のニーズに応じて、ストリームタイプとオーディオエンコードを設定します。スライドして入出力の音量を設定します。

スライドして音声プロンプトの有効化をONにします。

音声ミキサーを有効にしたり、「出力音量」を設定したりできます。

「SIP 音声符号化」を選択します。

保存をクリックします。

10.11.9 アクセス設定

PC Web 経由でのRS-485 パラメータの設定

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

システムとメンテナンス→システム欄のアクセス設定→ RS-485の順にクリックします。

RS-485 プロトコルを選択します。

RS-485を有効にするをチェックし、パラメータを設定します。

設定後に設定を保存するには、保存をクリックします。

番号

RS-485番号を設定します。

ペリフェラルタイプ

実際の状況に応じて、ドロップダウンリストから周辺機器を選択します。

注意

ペリフェラルを変更して保存した後、デバイスは自動的に再起動します。

RS-485 アドレス

実際のニーズに応じて、RS-485 アドレスを設定します。

注意

「Access Controller」を選択した場合: 機器をRS-485 インターフェイス経由でターミナルに接続する場合、RS-485 アドレスを2 に設定します。
機器をコントローラに接続する場合は、ドアNo.に合わせてRS-485アドレスを設定してください。

通信速度

デバイスがRS-485 プロトコルを介して通信しているときのボーレート。

PCのWeb経由でWiegandパラメータを設定します

Wiegand の送信方向を設定します。

手順

注意

対応していない機種もあります。
構成時には実際の製品を参照してください。

1. システムとメンテナンス→システム欄のアクセス設定→ Wiegand 設定の順にクリックします。

図10-9 Wiegand ページ

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

入力

デバイスはWiegand カードリーダを接続できます。

出力

外部アクセスコントローラを接続できます。

そして、2つのデバイスはWiegand 26または34を介してカード番号を送信します。

4. 保存をクリックして設定を保存します。

注意

ペリフェラルを変更し、デバイスパラメータを保存した後、デバイスは自動的に再起動します。

10.11.10 画像パラメータ設定

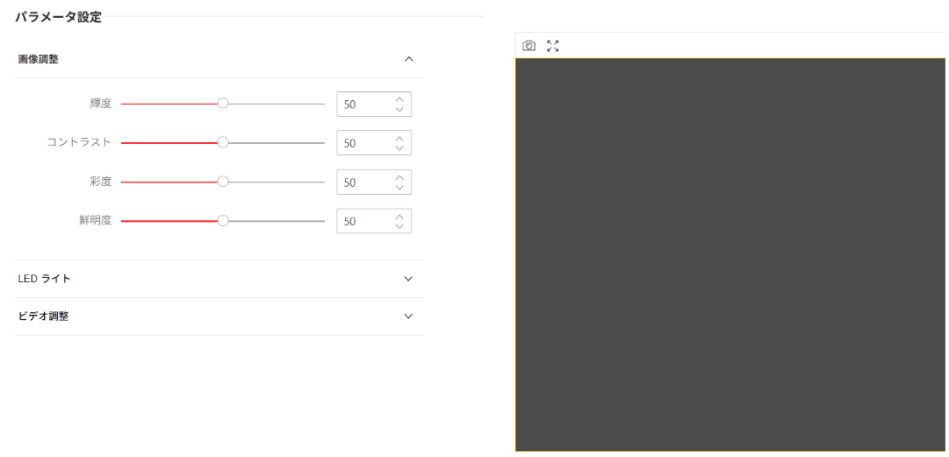


図10-10 画像調整設定

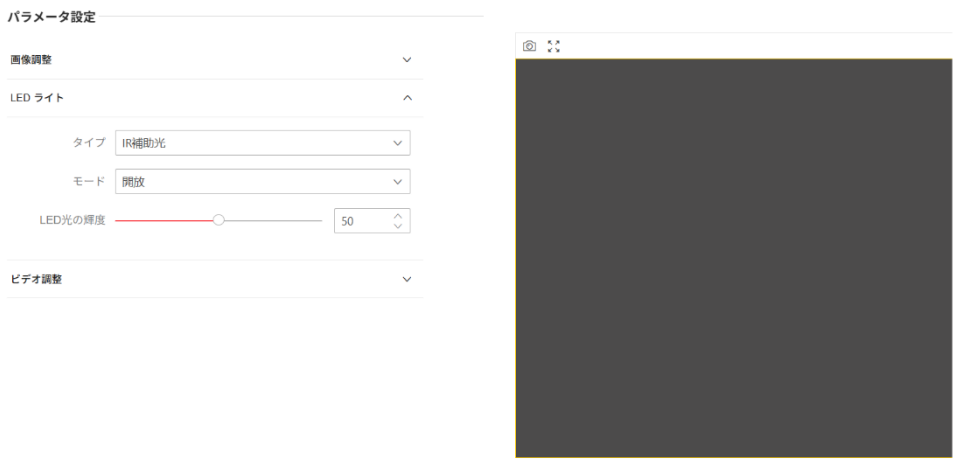


図10-11 LEDライト 設定

PC Web 経由で輝度/コントラスト/彩度/シャープネスを設定します

ライブビューページの、輝度、コントラスト、彩度、鮮明度などの画像情報を設定できます。

システムとメンテナンス→システム欄の画像→表示設定の順にクリックして、設定ページに入ります。

画像調整

ブロックをドラッグするか数値を入力して、輝度、コントラスト、彩度、鮮明度を設定します。

Restore Default Settings(デフォルト設定の復元)をクリックしてデフォルトに戻します。

パソコンのWeb経由でLEDライトを設定します

補光の明るさを調整します。

手順

1. システムとメンテナンス→システム欄→画像表示設定のLEDライトからページに入ります。
2. IR補助光のタイプ、モード (無効・開放を設定します。
3. **(オプション)「デフォルト設定に戻す(Restore Default Settings)」をクリックしてデフォルトに戻します。**

PC Web 経由でビデオ規格を設定します

ライブビューページのビデオ規格を設定します。

システムとメンテナンス→システム欄のビデオとオーディオをクリックして設定ページに入ります。

映像調整

リモートプレビュー時のビデオフレームレートを設定します。
設定を有効にするには、ビットレートタイプを [可変] へ変更し、フレームレートの設定ができます。

PAL

毎秒25 フレーム。中国、中東国、ヨーロッパなどに適しています。

NTSC

毎秒30 フレーム。米国、カナダ、日本、台湾(中国)、韓国、フィリピンなどに適しています。

Restore Default Settings(デフォルト設定の復元)をクリックしてデフォルトに戻します。

10.11.11 連携設定

設定したイベントがトリガーされたら、設定した方法に従ってイベント情報をセントラルプラットフォームにアップロードします。

手順

1. システムとメンテナンス→システム設定→イベント→リンケージ設定の順にクリックして、設定ページに入ります。
2. + をクリック
3. イベントソースを設定します。
「イベントリンク」、「カードリンク」、「従業員IDをリンク」から、イベントリンクにしたいタイプを選択します。

- 「イベントリンク」で「リンケージタイプ」を選択すると、実際のニーズに合わせてイベントタイプを選択できます。
- 「カードリンク」で「リンケージタイプ」を選択し、カード番号を入力して「カードリーダー」を選択します。
- リンケージタイプを選択したうえで、カード番号を入力し、使用するカードリーダーを選択します。

4. 連携動作を設定します。

1)ドアリンクを有効にし、ドアアクションをチェックして選択します。

2)リンクされたキャプチャを有効にします。

5. 保存 で設定を有効にします。

10.11.12 時間と出席の設定

人の勤務時間、遅れての到着、早発、休止、不在などを記録する場合は、シフトグループに人を追加し、シフトスケジュール(スケジュールの繰り返し方法、シフトタイプ、ブレーク設定、およびカードスワイプルールを定義する出席ルール)をシフトグループに割り当てて、シフトグループ内の人物の出席パラメータを定義できます。

Web 経由の出席モードの無効化

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

手順

1. システムとメンテナンス→システム設定→プラットフォーム出席をクリックして、設定ページに入ります。

2. 時間と出席を無効にし

ます。

結果

最初のページでは、参加ステータスの表示や設定は行いません。
システムは、プラットフォームで設定されたアテンションルールに従います。

Web による手動出席の設定

参加モードを手動に設定します。
参加するときは、手動でステータスを選択する必要があります。

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. システムとメンテナンス→システム設定→プラットフォーム参加をクリックして、設定ページに入ります。

2. 出勤モードを手動に設定します。

3.出席ステータスが必要の機能を有効にし、出勤ステータスの継続時間を設定します。
4.参加状況のグループを有効にします。

注意

出席プロパティは変更されません。

5.オプション: ステータスを選択し、必要に応じて名前を変更します。

結果

認証後、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、有効な出席としてマークされません。

ウェブ経由で自動出席を設定します

参加モードを自動に設定し、参加状況とその利用可能なスケジュールを設定できます。
システムは、設定されたスケジュールに従って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.システムとメンテナンス→システム設定→プラットフォーム参加をクリックして、設定ページに入ります。
2.出勤モードを自動に設定します。
3.出勤ステータスが必要の機能を有効にします。
4.作業中/作業買いを有効にするのグループを有効にします。

注意

出席プロパティは変更されません。

5.オプション: ステータスを選択し、必要に応じて名前を変更します。
6.状況のスケジュールを設定します。

ウェブ経由で手動と自動出席を設定します

参加モードを手動と自動に設定すると、システムは設定されたスケジュールに従って参加ステータスを自動的に変更します。
同時に、認証後に参加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. システムとメンテナンス→システム設定→プラットフォーム参加をクリックして、設定ページに入ります。
2. 出席モードを手動および自動に設定します。
3. 出席ステータスが必要の機能を有効にします。
4. 参加状況のグループを有効にします。

注意

出席プロパティは変更されません。

5. **オプション: ステータスを選択し、必要に応じて名前を変更します。**
6. 状況のスケジュールを設定します。

結果

最初のページで認証を行います。
認証は、スケジュールに従って設定された参加ステータスとしてマークされます。

結果タブの編集アイコンをタップすると、ステータスを選択して手動で参加することができ、
認証は編集された参加ステータスとしてマークされます。

例

- **月曜日の「Break In（開始時刻）」を11時、「Break In（中継）」を12時に設定した場合、有効ユーザーによる月曜日11時～12時のすべての認証は「Break」として記録されます。**

10.12 環境設定

10.12.1 パソコンのWeb経由で待受画像を設定します

待受画面に入る時間、スクリーンセーバーの画像、表示されるエフェクト、スライドショーの間隔など、待受画像のパラメータを設定します。

システムとメンテナンス →お好み→ スクリーンディスプレイ と移動します。

図10-12 待受画像設定

スタンバイ画像パラメータを設定し、保存をクリックします。待受画面に入る時間を設定した時間が経過すると、デバイスにスタンバイイメージが表示されます。

スクリーンセーバー画像

待受画像をお買い上げ時の画像またはカスタム画像に設定します。
カスタムを選択し、+をクリックしてローカルブラウズからスタンバイ画像をアップロードします。

注意

3 枚以下の画像を使用できます。
1画面サイズ:1024KB以下、フォーマット: jpg。

表示効果

待受画像の表示効果をストレッチ、適応、または塗りつぶしに設定します。

スライドショー間隔

複数の画像を追加する場合は、画像の切り替え時間を設定できます。

10.12.2 PC Web 経由でのスリープ時間の設定

設定した時間が経過すると、デバイスはスリープモードになります。消費電力を低減できます。

システムとメンテナンス → お好み →スクリーンディスプレイ へ移動します。

図10-13 スリープ設定

スリープをスライドさせ、スリープ時間
を設定します。保存をクリックします。

10.12.3 PC Web 経由での認証デスクのカスタマイズ

認証ページ/デスクでモジュールをカスタマイズします。

手順

1. システムとメンテナンス→お好み→カスタムホームページと移動します。
2. アプリケーションモードを選択します。
   アクセス種別
   デバイス認証ページにライブビューページが表示されます。
   そして、人名、従業員ID、顔写真はすべて認証後に表示されます。

インターコムモード

認証インターフェースには、クイック操作エリアと認証エリアが表示されます。
クイック操作エリアは、機能のカスタマイズ可能なショートカットキーをサポートしています。

シンプル

このモードを選択すると、認証ページのライブビューが無効になります。
個人の名前、従業員ID、顔画像はすべて認証後に非表示になります。

3.適用をクリックします。

10.12.4 PC Web 経由で通知の公表についてを設定します

デバイスの通知の発行を設定できます。

システムとメンテナンス → お好み → 通知の公表 と移動します。

図10-14 通知発行ダウンロード

MP4 フォーマット変換ツール

フォーマットを変更する必要がある場合は、MP4形式変換ツールをダウンロード をクリックできます。

マテリアル管理

+プログラムを追加をクリックして、プログラム名 とプログラムタイプ（※タイプは画像で固定）を設定できます。

アップロードをクリックし、+をクリックしてローカルPCから画像またはビデオをアップロードします。

注意

現在のところ、追加できるテーマは1 つだけです。

プログラムの追加

プログラム名の設定、プログラムタイプの選択ができます。

ピクチャ

ピクチャを選択した場合は、+をクリックしてピクチャを追加できます。

ようこそメッセージ

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

標準

標準を選択すると、背景色と画像を設定できます。

スケジュール再生

テーマを作成したら、テーマを選択し、タイムラインにスケジュールを描くことができます。

描画したスケジュールを選択すると、正確な開始時刻と終了時刻を編集できます。

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

スライドショー間隔

ブロックをドラッグするか番号を入力して、スライドショーの間隔を設定します。間隔に応じて画像と動画が変更されます。

10.12.5 PC Web 経由のプロンプトスケジュールの設定

認証に成功し、失敗した場合の出力音声コンテンツをカスタマイズします。

手順

1. システムとメンテナンス→お好み→プロンプトスケジュールと移動します。

図10-15 プロンプトスケジュール

2. 機能を有効にします。

3. 名称を設定します。

4. タイムスケジュールを選択します。

5. 認証に成功した時間帯を設定します。

1)継続時間の追加 をクリックします。

2)時間を設定します。

注意

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

3)音声プロンプトの内容を設定します。

4)**オプション:サブステップ1 ～3 を繰り返します。**

5)**(オプション) 設定した時間を削除します。**

6. 認証に失敗した時間を設定します。

1)Add Time Duration をクリックします。

2)時間を設定します。

注意

設定された時間内に認証に失敗した場合、デバイスは設定されたコンテンツをブロードキャストします。

3)音声の内容を設定します。

4)**オプション:サブステップ1 ～3 を繰り返します。**

5)**(オプション) 設定した時間を削除します。**

7. 保存をクリックして設定を保存します。

10.12.6 PC Web 経由のプロンプト音声のカスタマイズ

デバイスのプロンプトボイスをカスタマイズできます。

手順

1. システムとメンテナンス→お好み→カスタムプロンプトと移動します。

図10-16 カスタムプロンプト

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

注意

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

10.12.7 PC Web 経由での認証結果テキストの設定

手順

1.システムとメンテナンス →お好み→認証結果テキストへ移動します。

図10-17 認証結果テキスト

2.認証結果テキストのカスタマイズを有効にします。

3.カスタムテキストを入力します。

4.保存をクリックします。

10.13 システムとメンテナンス

10.13.1 再起動

デバイスを再起動できます。

システムとメンテナンス→メンテナンス→再起動をクリックして、設定ページに入ります。

再起動をクリックして、デバイスを再起動します。

10.13.2 アップグレード

PC Web 経由でローカルにアップグレード

デバイスをローカルでアップグレードできます。

システムとメンテナンス→メンテナンス→アップグレードの順にクリックして、設定ページに入ります。

ドロップダウンリストからアップグレードタイプを選択します。

ローカルPC からアップグレードファイルをクリックして選択します。

アップグレードをクリックして、アップグレードを開始します。

PC Webによるオンラインアップグレーディング

デバイスをオンラインでアップグレードできます。

システムとメンテナンス→メンテナンス→アップグレードの順にクリックして、

設定ページに入ります。

デバイスがネットワークに接続されていて、GuardingVision アプリに追加されている場合は、デバイスのアップグレード→デバイスのオンラインアップグレードをタップしてGuardingVision アプリに更新されたバージョンがあるときにアップグレードできます。

Keyfobのアップグレード

注意

- 周辺モジュールがオンラインになっていることを確認します。
- keyfob をアップグレードするときは、顔認識端末を1 つだけ保持し、キーフォブを動かさないでください。

システムとメンテナンス→メンテナンス→アップグレードの順にクリックします。
「アップグレード設定」ドロップダウンリストで、「Keyfob」を選択します。
ローカルPC からアップグレードファイルを選択します。
アップグレード→ OKをクリックします。
アップグレードするには、キーフォブのいずれかのボタンを押します。

10.13.3 復元

Web ブラウザから工場出荷時の設定に復元

デバイスを工場出荷時の設定に復元できます。

システムとメンテナンス→メンテナンス→バックアップとリセットをクリックして、設定ページに入ります。

すべて復元をクリックすると、すべてのパラメータが工場出荷時の設定に復元されます。

使用前にデバイスをアクティブ化する必要があります。

PC Web 経由でデフォルト設定に復元

デバイスをデフォルト設定に復元できます。

システムとメンテナンス→メンテナンス→バックアップとリセットをクリックして、設定ページに入ります。

Restore(復元)をクリックすると、デバイスのIP アドレスとユーザー情報を除き、

デバイスはデフォルト設定に復元されます。

10.13.4 PC Web 経由でのデバイスパラメータのエクスポート

デバイスパラメータのエクスポート。

システムとメンテナンス→メンテナンス→バックアップとリセットへ移動します。

バックアップ

エクスポートをクリックして、デバイスパラメータをエクスポートします。

注意

デバイスパラメータをエクスポートし、他のデバイスにインポートします。

10.13.5 PC Web 経由でのデバイスパラメータのインポート

設定パラメータをインポートします。

システムとメンテナンス→メンテナンス→バックアップとリセットへ移動します。

設定ファイルのインポート

ローカルPC からファイルをクリックして選択します。インポートをクリックします。

10.13.6 デバイスのデバッグ

デバイスのデバッグパラメータを設定できます。

Web ブラウザ経由のSSH の有効化/無効化

SSH を有効にしてリモートデバッグを実行できます。

システムとメンテナンス→メンテナンス→デバイスのデバッグ→デバッグ用ログの順にクリックします。

SSH の有効化

SSH はリモートデバッグに使用されます。
このサービスを使用する必要がない場合は、SSH を無効にしてセキュリティを向上させることをお勧めします。

PC Web 経由でのデバイスログの印刷

デバイスログを印刷できます。

システムとメンテナンス→メンテナンス→デバイスのログとクリックして、
設定ページに入ります。
デバイスログを印刷するには、エクスポートをクリックします。

PC Web 経由でのネットワークパケットのキャプチャ

キャプチャパケットの期間とサイズ、および開始キャプチャを設定します。
キャプチャ結果に従ってログとデバッグを表示できます。

システムとメンテナンス →メンテナンス → デバイスのデバッグ → デバッグ用ログ と移動します。

「キャプチャパケット期間」、「キャプチャパケットサイズ」を設定し、「キャプチャ開始」をクリックします。

PC Web経由のテストプロトコル

プロトコルアドレスを選択し、テストするプロトコルを入力します。
レスポンスヘッダと返り値に従ってデバイスをデバッグできます。

システムとメンテナンス → メンテナンス → デバイスのデバッグ → プロトコルのテスト へ移動します。

図10-18 プロトコルテスト

プロトコルアドレスを選択し、プロトコルを入力します。実行をクリックします。
レスポンスヘッダと返り値に従ってデバイスをデバッグします。

PC Web によるネットワーク診断

デバイスのIP アドレスまたはドメイン名を入力すると、PING 設定を実行できます。
PING の結果に従ってネットワークをデバッグします。

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

図10-19 ネットワーク診断

PING 操作用のデバイスIP を入力し、ネットワーク接続モード、PING 期間、およびPing データパッケージサイズ(デフォルトパラメータを推奨)を選択します。
診断をクリックします。
PING Resultに結果が表示されます。

パソコンのWeb経由でネットワーク侵入サービスを設定します

LAN にデバイスを展開すると、侵入サービスを有効にしてデバイスのリモート管理を実現できます。

手順

1. システムとメンテナンス→メンテナンス→デバイスデバッグ→ネットワーク侵入サービスと移動します。
2. 眼識サービスの有効化をON
3. サーバのIP アドレスとサーバーポートを設定します。ユーザー名とパスワードを作成します。
4. **オプション: ハートビートタイムアウトを設定できます。**
   値の範囲は1 ～6000 です。
5. **オプション: 侵入サービスのステータスを表示できます。Refresh(更新)をクリックしてステータスを更新します。**
6. 保存をクリックします。

注意

48 時間が経過すると、侵入サービスは自動的に無効になります。

10.13.7 PC Web 経由でログを表示

デバイスログを検索して表示できます。

システムとメンテナンス→メンテナンス→ログと移動します。

ログタイプのメジャーおよびマイナータイプを設定します。
検索の開始時刻と終了時刻を設定し、「検索」をクリックします。

その下に、No.、時間、メジャータイプ、マイナータイプ、チャネル番号、ローカル/リモートユーザー情報、リモートホストIP などの結果が表示されます。

10.13.8 PC Web 経由の詳細設定

顔パラメータ、手のひらパラメータを設定し、バージョン情報を表示できます。

システムとメンテナンス→メンテナンス→詳細設定と移動します。

デバイスアクティベーションパスワードを入力し、Enter をクリックします。

面パラメータ

カスタムスプーフィング対策検出を有効にし、スプーフィング対策検出しきい値1:1、スプーフィング対策検出しきい値1:N を設定できます。
認証時に顔をロックを有効にし、ロック時間を設定します。
スプーフィング対策検出の試行制限に達すると、フェイスは設定されたロック期間ロックされます。
保存をクリックします。

パームプリントパラメータ

カスタムスプーフィング対策検出を有効にし、スプーフィング対策検出しきい値を設定できます。保存をクリックします。

バージョン情報

ここでは、さまざまなバージョン情報を表示できます。

10.13.9 セキュリティ管理

PC Webログイン時のセキュリティレベルを設定します。

システムとメンテナンス→安全→セキュリティサービスと移動します。

セキュリティモード

ログイン時の高度なセキュリティレベルとユーザー情報の確認。

互換モード

古いユーザ検証方法と互換性があります。

保存をクリックします。

10.13.10 証明書管理

これは、サーバ/クライアント証明書とCA証明書の管理に役立ちます。

注意

この機能は特定のデバイスモデルでのみサポートされています。

自己署名証明書の作成とインポート

手順

1.システムとメンテナンス→安全→証明書管理と移動します。

2.証明書ファイル 領域で、ドロップダウンリストから証明書タイプを選択します。

3.作成をクリックします。

4.証明書情報を入力します。

5.「OK」をクリックして証明書を保存し、インストールします。

作成された証明書が証明書の詳細領域に表示されます。証明書が自動的に保存されます。

6.証明書をダウンロードし、ローカルコンピュータの要求ファイルに保存します。

7.要求ファイルを認証局に送信して署名を求めます。

8.署名済み証明書をインポートします。

1)「Import Key」領域で証明書タイプを選択し、ローカルから証明書を選択して、「Import」をクリックします。

2)「Import Communication Certificate」領域で証明書タイプを選択し、ローカルから証明書を選択して、「Import」をクリックします。

他の認証済み証明書のインポート

認証済み証明書(デバイスで作成されていない証明書)がすでにある場合は、デバイスに直接インポートできます。

手順

1.システムとメンテナンス→安全→証明書管理と移動します。

2.「鍵のインポート」領域と「通信証明書のインポート」領域で、証明書の種類を選択し、証明書をアップロードします。

3.インポートをクリックします。

CA 証明書のインポート

はじめる前に

あらかじめCA証明書を用意しておきます。

手順

1. システムとメンテナンス→安全→証明書管理と移動します。
2. 「CA 証明書のインポート」領域にID を作成します。

注意

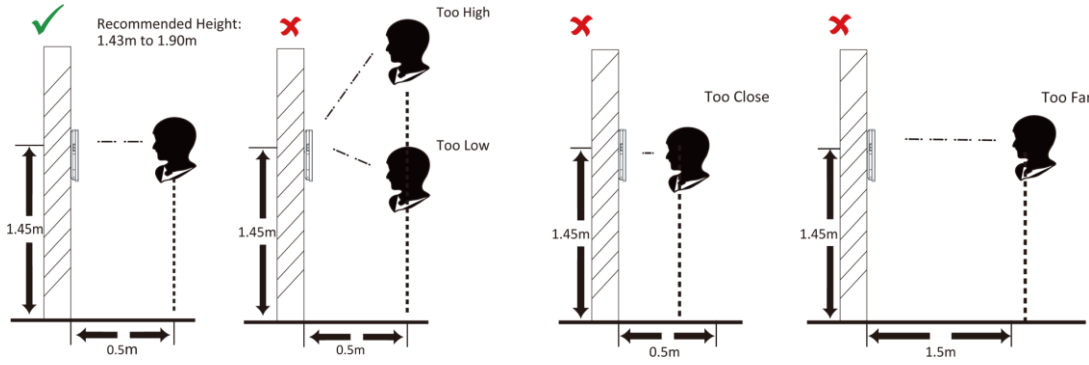
入力証明書ID を既存のものと同じにすることはできません。

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

付録A。顔画像を収集/比較するときのヒント

顔画像を収集または比較するときの位置は次のとおりです:

位置(推奨距離:0.5m)



式

- 顔画像を収集または比較するときは、下の図の式のように、式を自然な状態に保ちます。

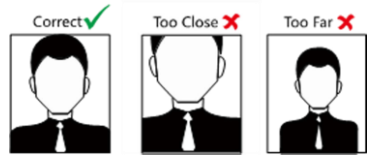
- 顔認識機能に影響を与える可能性のあるハット、サングラス、その他のアクセサリーを着用しないでください。
- 目、耳などを覆わないでください。重いメイクアップはできません。

姿勢

良好な品質と正確な顔画像を得るために、顔画像を収集または比較するときは、カメラを見て顔を配置します。

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。



付録B。設置環境に関するヒント

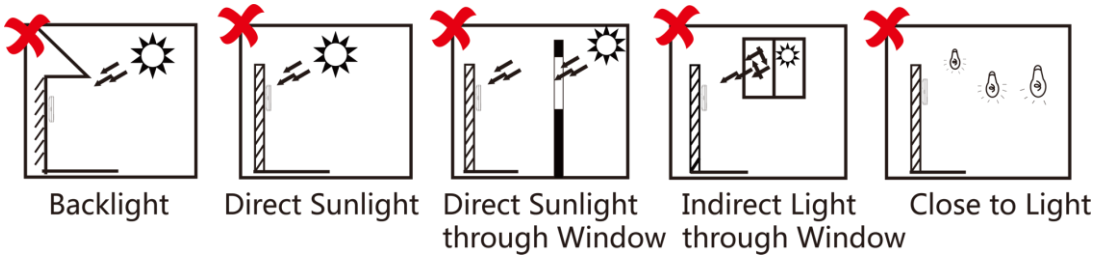
1.光源照度基準値

キャンドル: 10Lux

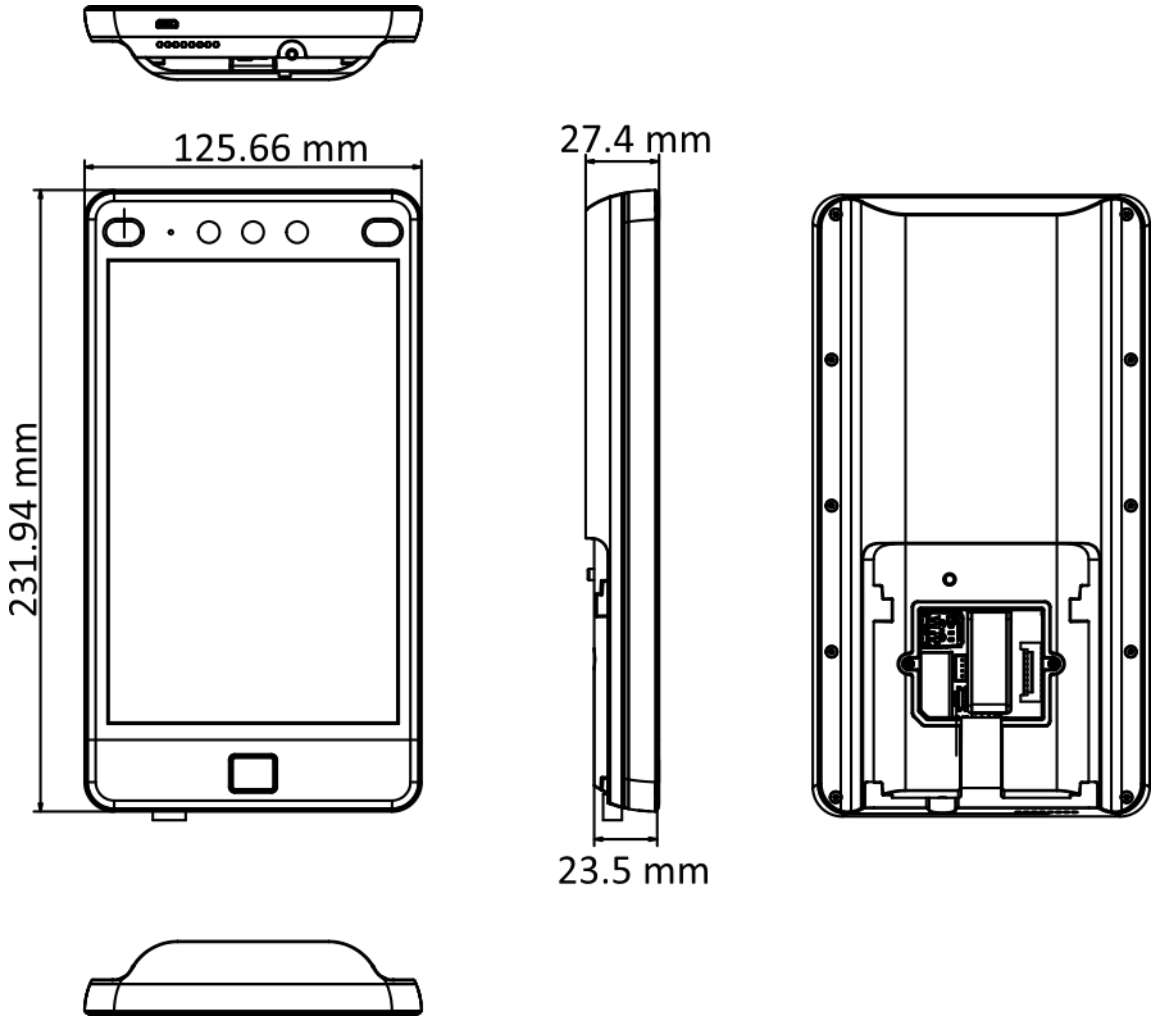
バルブ: 100～850Lux

日光: 1200Lux 以上

2.バックライト、直接および間接日光
を避けます



付録C。ディメンション



図D-1 寸法