BioStar Air

管理者ガイド

バージョン 2.13.0

日本語

JA 102.00.BSA

suprema
SECURITY & BIOMETRICS

目次

BioStar Airとは? 4

100% クラウド入退室管理プラットフォーム 4

比類のないクレデンシャルの柔軟性 4

オンプレミスインフラ不要 4

簡単なマルチサイト管理 4

エッジアーキテクチャによる将来に備えた拡張性 5

クラウド中心の企業に最適化 5

BioStar Airの機能 5

対応デバイス 6

セキュリティ体制 7

サイト管理者 10

はじめに 10

サイトセレクター(Site Selector) 21

BioStar Airアプリのはじめ方 23

サイトを管理する 25

サイトを設定する 210

SSO & SCIM を設定する 231

追加サイトの設定 262

パートナー／導入管理者 290

パートナーポータルの使い方 290

フェデレーションサイトの管理 292

パートナー管理者を招待する 294

サイト管理者を招待する 299

パートナー技術者の管理 304

ハードウェアのセットアップ 317

認証済みユーザー 338

モバイル認証情報の使い方 338

高度な機能の設定 340

感度を設定する 344

開発者 346

クイックスタート 346

API認証 348

ユーザー管理APIの使い方 351

トラブルシューティング 356

一括ユーザー追加の問題 356

モバイルカードが動作しません 359

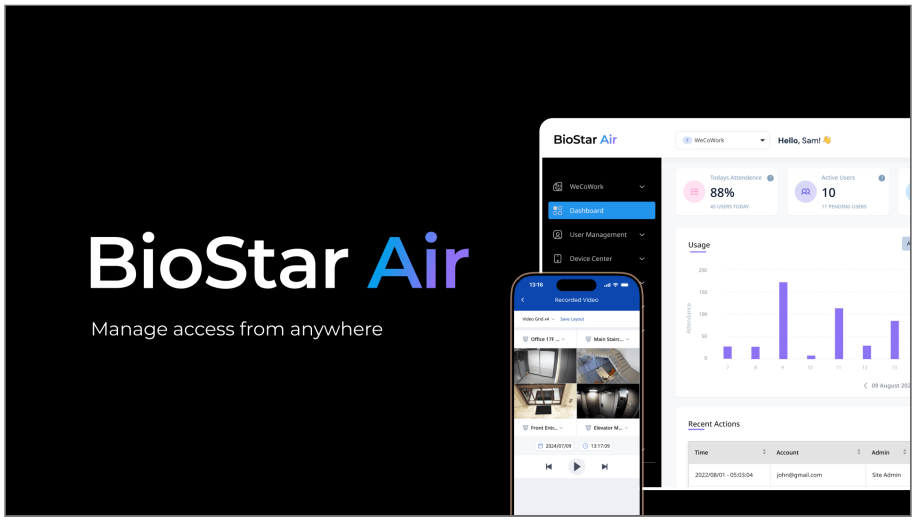
位置サービスを有効にする必要がありますか？ 361

ビデオ再生のトラブルシューティング 362

BioStar Airとは?

100% クラウド入退室管理プラットフォーム

BioStar Airは、生体認証セキュリティ分野の世界的リーダーであるSupremaが開発したクラウドネイティブな入退室管理ソリューションです。 オンプレミスインフラの必要性をなくすよう設計されたBioStar Airは、どこからでも管理できる安全で柔軟かつスケーラブルな入退室管理を提供します。 クラウドに直接接続されたスマートリーダーを通じて、企業は携帯電話やブラウザだけで複数の拠点の入退室を簡単に制御できます。



比類のないクレデンシャルの柔軟性

BioStar Airは、最も包括的な認証オプションを提供し、安全で便利なさまざまな方法で施設への入退室を管理できます。

- **顔認証**
- **iOSおよびAndroid向けカスタムモバイル認証**（無料）
- **各種RFIDフォーマット**
- **アプリ不要のDynamic QRおよびLinkPass**

オンプレミスインフラ不要

BioStar Airはオンサイトサーバー、仮想マシン、VPN、またはドアコントローラーの必要性をなくしました。 IT保守は不要です。 **スマートリーダー**（Smart reader）を設置してクラウドに接続すれば、すぐに入退室管理を始められます。 リーダー（Reader）は、同じネットワークや物理的な場所に関係なく複数のサイトで動作します。

簡単なマルチサイト管理

オフィス、倉庫、小売店舗、または遠隔拠点の入退室管理の有無にかかわらず、BioStar Airは単一のシステムで全拠点の入退室を制御できる包括的なソリューションを提供します。

エッジアーキテクチャによる将来に備えた拡張性

BioStar Airの**エッジアーキテクチャ**は、入退室管理をスマートリーダーに直接内蔵しており、別途ドアコントローラーを必要としません。 これにより企業は**容易に拡張**できます。 現在必要な機能だけを購入し、複雑なアップグレードなしで簡単に拡張できます。

クラウド中心の企業に最適化

BioStar Airは業界最高の生体認証技術を搭載した、クラウドネイティブな入退室管理ソリューションを求める**システムインテグレーター**および**顧客**のために設計されています。 クラウド中心の企業の入退室管理に対して、モダンで柔軟かつ高い安全性を備えた手段を提供します。

BioStar Airの機能

機能	説明
包括的な入退室管理ソリューション	対応
高いセキュリティ	ISO 27001 / 27701、TLS 1.2、AES-256
生体認証：顔および指紋	Supremaリーダーに対する基本サポートを提供しており、生体認証データベースを内蔵しています。
RFIDカード	MIFARE Classic、DesFire、Felica、EM4100、Custom Wiegand Formats、iClass、Seos。 1ユーザーあたり最大8枚のカードをサポートします。
モバイル認証情報	無料で無制限に提供されます。 セキュアなBLE/NFC認証情報（iOS、Android）、アプリ不要のLinkPassおよびQR認証を含みます。
展開	クラウドネイティブ
インターフェース	ブラウザ、iOSアプリ、Androidアプリ
価格モデル	サブスクリプションベース
統合	幅広いAPI、Webhook、およびSDK
エッジアーキテクチャ	リーダーには内蔵コントローラーがあり、イーサネットを介してクラウドに直接接続されます。 別途クラウドノードや入退室制御パネルは必要ありません。
ログイン	どこからでも利用できます。
サーバーの所在地	韓国（グローバル）およびドイツ（ヨーロッパ）

機能	説明
勤怠	リーダーの勤怠キー（key）はイベントログに記録され、勤務時間レポートが作成されて統合できます。
ビデオ	OnvifおよびUniviewをサポートする基本的なVMSです。 NVRは不要で、リーダーがゲートウェイの役割を果たします。
アラーム	侵入警報エリアに対する管理者への通知をサポートします。
データパーティショニング	標準
対象	フランチャイズ、複数拠点、マルチテナント、遠隔地など

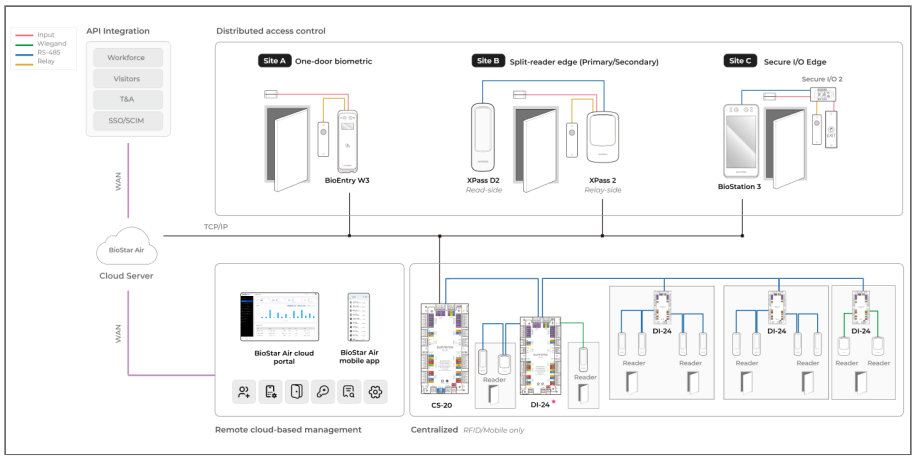
対応デバイス

BioStar Airは、分散型および集中型のアクセス制御アーキテクチャの両方をサポートする柔軟なデバイス管理を提供します。 クラウド経由で機器を登録、設定、監視、更新、運用できます。各サイト（Site）の出入口、配線、セキュリティ要件に応じて最適な設定を選択できます。

サイト（Site）では、クラウドに直接接続するエッジ機器を使用するか、RS-485またはWiegand経由でリーダーを管理するコントロールパネルを使用できます。 両アーキテクチャは同一サイト内で併用でき、新規導入、生体認証による出入管理、集中型パネルベースの構成など、さまざまな環境に対応します。

対応デバイス

BioStar Airはさまざまな入退室制御機器と互換性があり、Suprema製の機器とシームレスに連携してクラウドベースの入退室管理が可能です。



リーダー機器

- **XPass 2** (MDPB, GDPB, GKDPB)
- **X-Station 2** (DPB)
- **BioEntry W3**

- **BioStation 3**
- **XPass D2**

パネル

- **CoreStation 20** (CS-20)

Patch機器

- **Airfob Patch** (AP-H)
- **Airfob Tag** (AP-B)

その他の互換機器

- **Output Module** (OM-120)
- **Secure I/O 2** (SIO2)
- **Door Interface** (DI-24、予定)

セキュリティ体制

BioStar Airは、Supremaの安全なクラウドベースのモバイル入退室管理ソリューションです。 Supremaのハードウェア、ソフトウェア、ファームウェアのエンジニアリングチームは「設計時のセキュリティ」原則に基づいて作業します。 システムアーキテクチャの全レイヤーおよびすべての通信接点は、プライバシー保護とデータ完全性を維持するように設計されています。

主な対策：

- BioStar Air管理ポータルおよびデータベースのデータ保護と暗号化
- BioStar Air APIとクライアント間のデータ送信時の暗号化と保護
- スマートフォンに保存されたモバイルカードデータの暗号化
- スマートフォンとリーダー間の通信保護（Suprema Pass）
- モバイル資格情報の改ざん防止（Suprema Pass）

ISO 27001認証

SupremaはISO 27001認証を取得しており、データ保護管理、セキュリティ統制、および個人情報管理に関する国際基準を満たしています。 2019年8月に取得されたISO 27001準拠は、一般データ保護規則（GDPR）やカリフォルニア消費者プライバシー法（CCPA）などの類似の法律とも整合しています。

エンドツーエンド（End-to-End）セキュリティのための検証済み技術

ポータルアクセスおよびデータ保護

BioStar Air 管理ポータルは、AES-256 以上の暗号化を使用する AWS Amazon RDS 暗号化DBインスタンス上で実行されます。 すべての個人データには追加の暗号化が適用されます。

BioStar Air APIとの暗号化通信

BioStar Air REST APIとのすべての通信はHTTPS経由でTLS 1.2を使用して暗号化され、アクセストークン（デフォルトで1時間有効）が必要です。 AWS API Gatewayはブルートフォース攻撃を防ぐためにAPIリクエストを制限します。

暗号化およびハッシュ処理されたモバイルカードID

モバイルカードID番号は AES-256 で暗号化され、サードパーティのサーバーで露出するのを防ぎます。 カードデータには真正性確認のためにデジタル署名が行われます。

モバイル機器に保存されたモバイルカードの安全な保存

Suprema Passのモバイル資格情報および関連データはAES-256で暗号化されます。 暗号化キーはモバイル機器のトラステッド実行環境（TEE）、例えばSecure Enclave（Apple）やTrustZone（ARM）に保存されます。

モバイル機器とリーダー間の安全な通信

Bluetooth Low Energy（BLE）を介した「リプレイ攻撃」を防ぐため、BioStar Airは各接続に対してワンタイム暗号化キーを使用し、送信直後に接続を終了して中間者攻撃（MITM）を防ぎます。

モバイルカード改ざん防止

各Suprema Passのモバイルクレデンシャルは、各BioStar Airサイト固有のPKIベースのデジタル署名で保護されます。 独自の検証プロセスは改ざんや不正な変更の試みを検出します。

脆弱性管理

Supremaの情報セキュリティチームが脆弱性管理を主導し、外部のセキュリティ専門家が支援します。

- 継続的な自動化された脅威スキャン
- 全システムレビューを含む年次ISO 27001更新監査
- 主要リリース前のペネトレーションテストおよびリスク評価
- パスワード管理、ソーシャルエンジニアリング耐性、および手順遵守のためのチェック
- すべての脆弱性および修正措置に関する包括的な文書化および報告

リスク評価アプローチ

資産は機密性、完全性、可用性の評価に基づいて分類されます。 脅威が特定され、脆弱性が評価され、リスクは発生可能性と影響に基づいて評価されます。 緩和策はリスクの重大度に応じて優先順位付けされます。

多要素認証（MFA）

多要素認証（MFA）は段階的に実装されています。

- 管理者アカウントに対するメールベースの2FA
- BioStar Airアプリに対するパスコードベースの2FA
- 90日後に非アクティブな管理者アカウントを自動ロック

- パスワードの有効期限設定が可能（30、60、90日）

主なセキュリティポリシー

- 送信中データの暗号化: TLS 1.2
- 保存中データの暗号化: AES-256
- DoS保護: AWS API Gatewayによるリクエスト制限
- サービス可用性: 99.9% 稼働時間(SLA基準)
- APIセキュリティ: トークンベース認証、HTTPS専用、厳格なエンドポイント検証
- ポータルアクセス：グローバル管理向けのクラウドベースのサービスで、プライベートクラウドのオプションは現在開発中です

サイト管理者

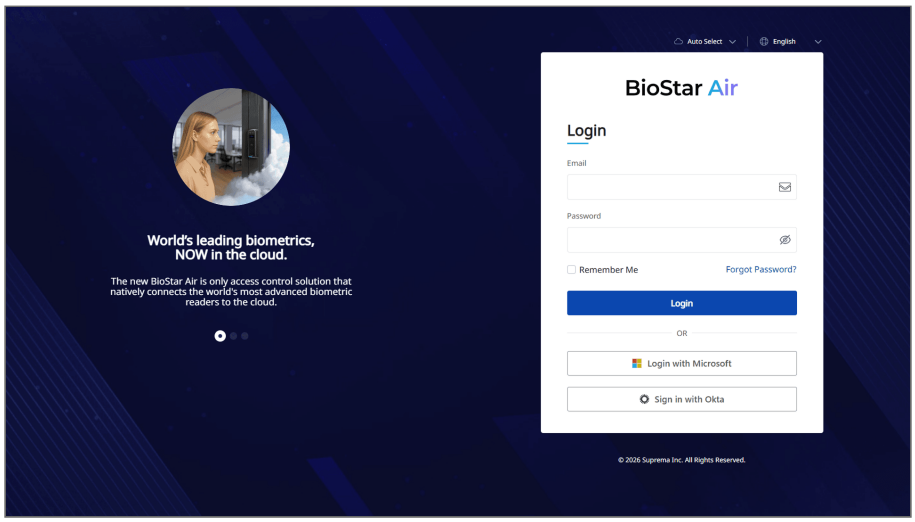
サイト管理者は BioStar Air サイトの運用全般を担当します。 ユーザー登録と認証情報の管理、デバイスや出入口、エレベーターの設定、アクセス権やスケジュールの設定、イベントの監視、システム設定やサービス構成など、必要なすべての管理作業を案内します。

はじめに

BioStar Air ポータルは、Web とモバイルアプリ全体で統合されたインターフェースを提供し、一貫したユーザー体験を実現します。 BioStar Air ポータルを通じて、管理者はアクセス制御の設定を管理し、サイトの利用状況を監視し、ユーザーやデバイスを円滑に構成できます。

ポータルへのアクセス

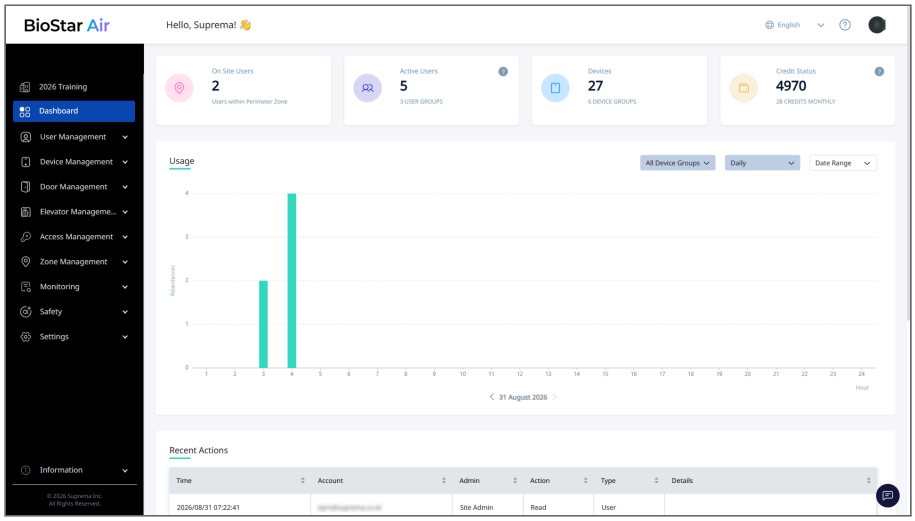
BioStar Air ポータルにアクセスするには、Web ブラウザーを開き、admin.biostarair.com に移動します。 ログインページが表示されたら、現在の所在地に応じて **グローバルサーバー** または **EUサーバー** を選択します。



> **情報**
> サインアップでアカウントを作成できません。 システム導入担当者または既存の管理者がサイトに招待する必要があります。 管理者アカウントの管理および招待に関する詳細は、管理者アカウントおよび役割の管理をご参照ください。

ダッシュボードの概要

ログインすると、サイトの主要情報を確認できる **ダッシュボード** が表示されます。



- **オンサイトのユーザー**：現在のサイトにいるユーザーをリアルタイムで確認できます。 システムは、**境界**（境界ゾーン）に設定した入退室装置の認証記録に基づいて在席（Presence）状態を算出します。 詳細については次のドキュメントを参照してください。
  - ゾーン管理
  - 在席を確認
- **アクティブユーザー**：登録および有効化されたユーザーの合計数を確認できます。 カードをクリックすると、**ユーザー管理** メニューに移動します。
- **デバイス**：登録されたデバイス数を確認できます。 カードをクリックすると、**デバイス管理** メニューに移動します。
- **クレジットステータス**：アカウントのクレジット残高を確認できます。 カードをクリックすると、**設定** → **クレジットセンター** メニューに移動します。
- **使用量**：デバイスグループ、頻度（日次、週次、月次）または任意の日付を指定して、範囲ごとに並べ替えできます。
- **最近の行動**：ログイン、デバイスの更新、ユーザー作成など、管理者が実行した操作のアクティビティログを表示します。

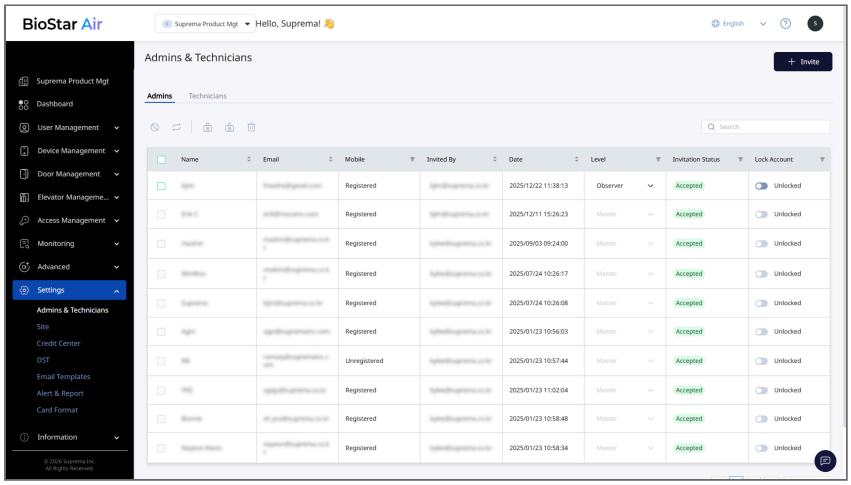
サイト設定のステップバイステップガイド

次の案内に従って新しいサイトを設定してください。

1 管理者の追加

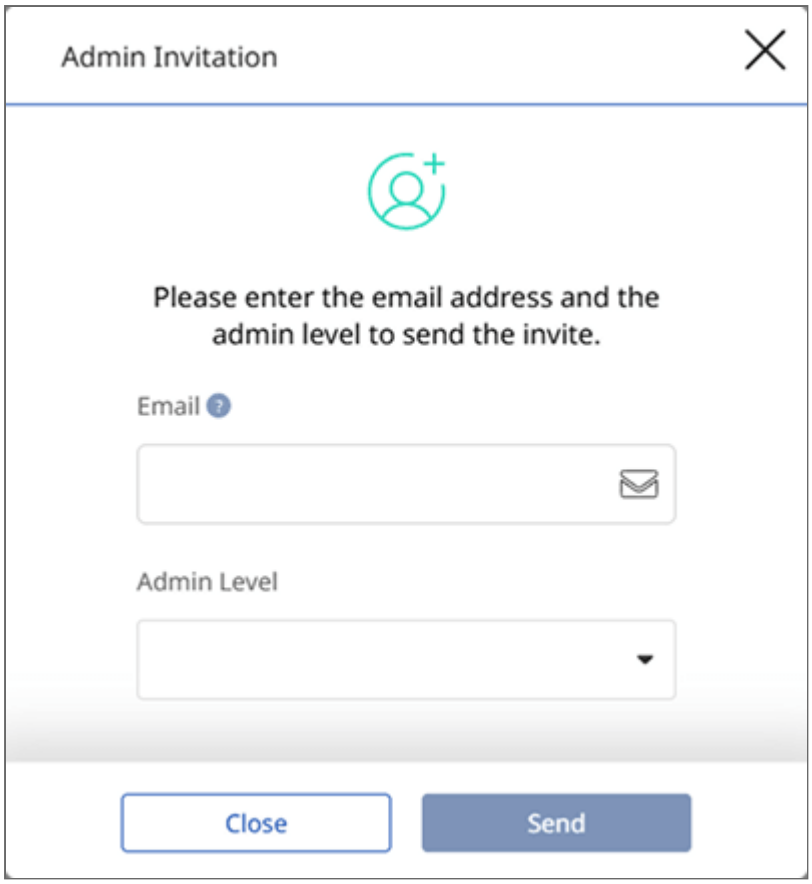
管理者を招待してください。

1. 画面左のサイドバーで **設定** → **デバイスのみ** をクリックしてください。



2. 画面右上の **招待** をクリックします。

3. **アドミンへの招待** ウィンドウが表示されたら、管理者のメールアドレスを入力し、役割を付与してください。

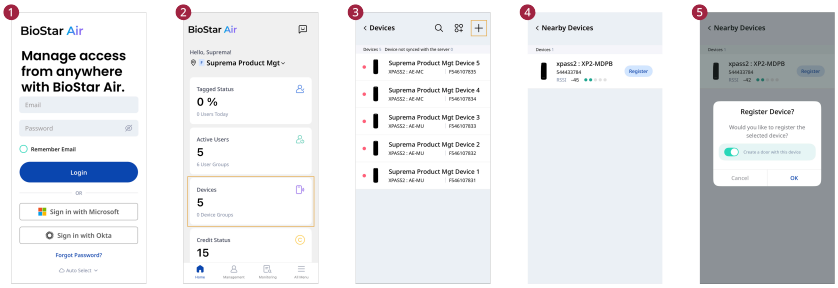


4. **送信** をクリックします。

> **情報**
> サイト管理者はサイトを管理でき、認証されたユーザーは**Suprema Pass**アプリを通じてのみアクセスできます。

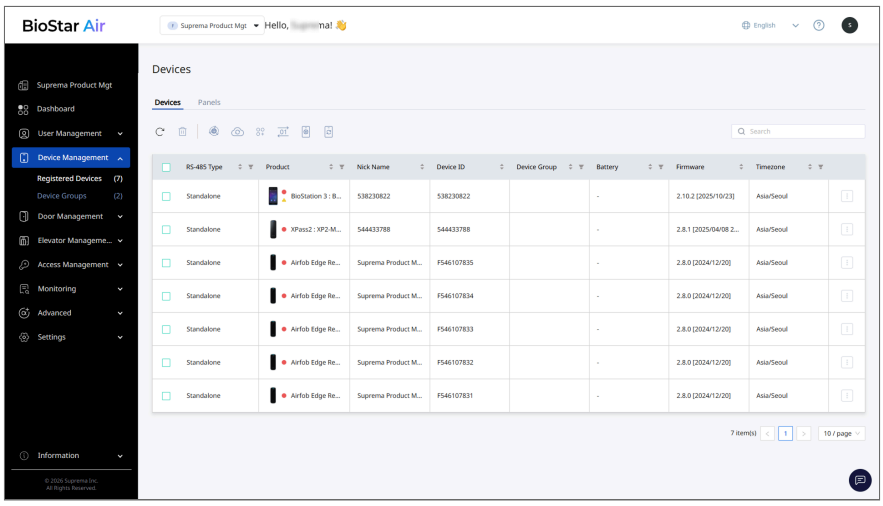
❷ デバイスの登録

BioStar Airモバイルアプリを使用してデバイスを登録してください。 デバイスの登録はBluetooth Low Energy（BLE）で行われ、登録されたデバイスはBioStar Airポータルで管理できます。



1. モバイル端末でBioStar Airアプリを起動してログインします。
2. **デバイス** カードをタップします。
3. 画面右上の ＋ ボタンをタップします。
4. デバイス検索画面で登録するデバイスの **登録** ボタンをタップします。
5. デバイス登録ウィンドウが表示されたら **OK** ボタンをタップします。

デバイス一覧に戻り、追加されたデバイスを確認します。 画面左のサイドバーで **デバイス管理** → **登録済みデバイス** をクリックします。

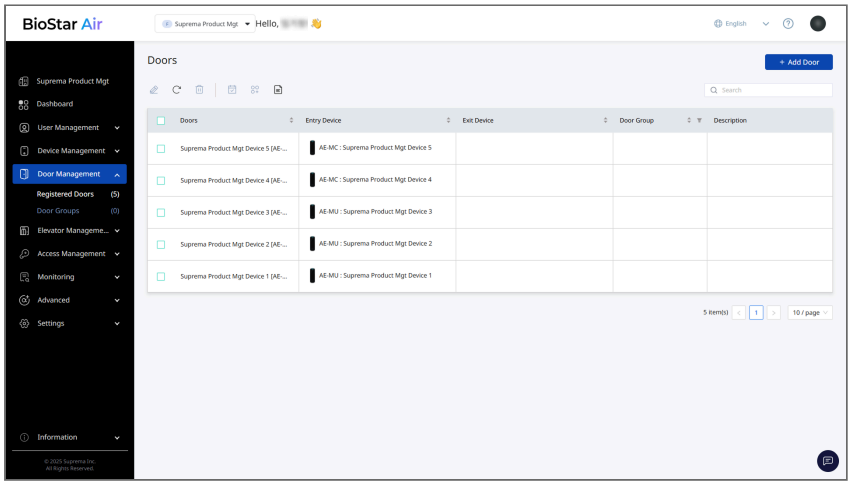


- デバイスを登録していない場合は、別の管理者が現場で BioStar Air モバイルアプリを使用して登録する必要があります。
- **登録済みデバイス** では、デバイスの削除、ファームウェアの更新、およびデバイスグループの管理ができます。

❸ ドアの作成と管理

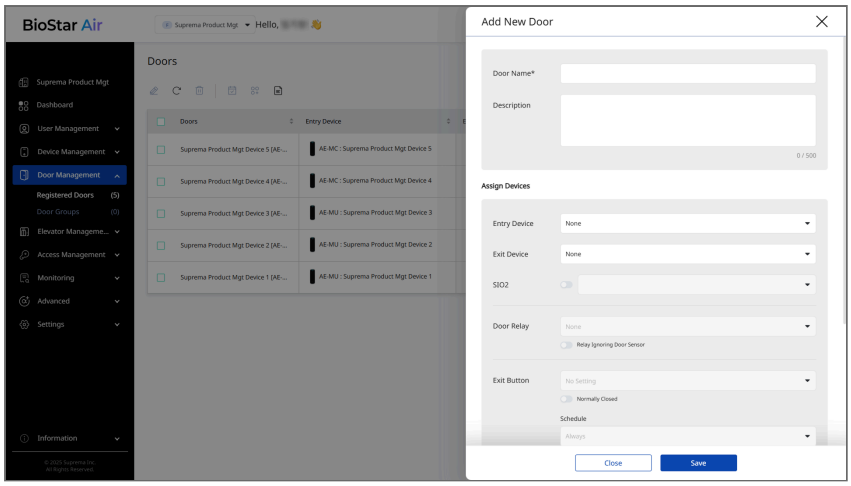
ドアを追加し、デバイスを割り当ててください。

1. 画面左のサイドバーで **ドア管理** → **登録されたドア** をクリックしてください。



2. ドアがない場合は、画面右上の **ドアを追加** をクリックしてください。

3. **ドアを追加** パネルが表示されたら、名前と説明を入力してください。



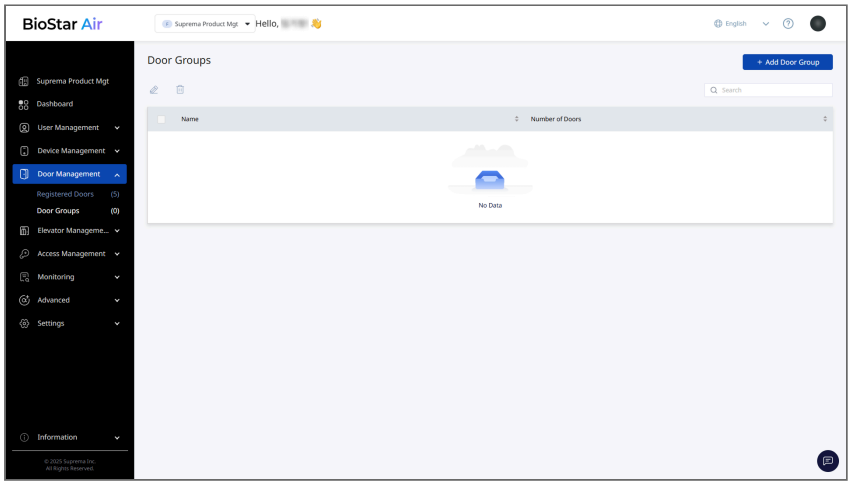
4. 登録済みのデバイスを **入室デバイス** と **退室デバイス** に割り当ててください。

ドア管理 では、ドアの編集・削除、アクセススケジュールの設定、グループでの管理ができます。

4 ドアをグループに分類

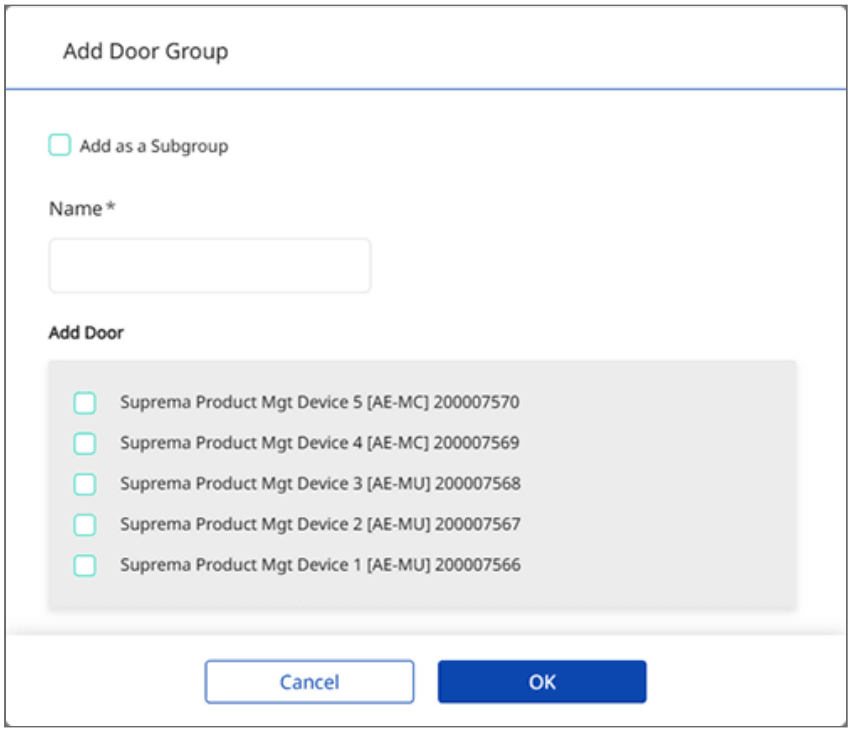
ドアをグループに分類してください。

1. 画面左のサイドバーで **ドア管理** → **ドアグループ** をクリックします。



2. 画面右上の **ドアグループを追加** をクリックします。

3. **ドアグループを追加** ウィンドウが表示されたら、グループ名を **屋内**、**屋外** または **Trap Doors** のように入力し、必要なドアを選択してください。



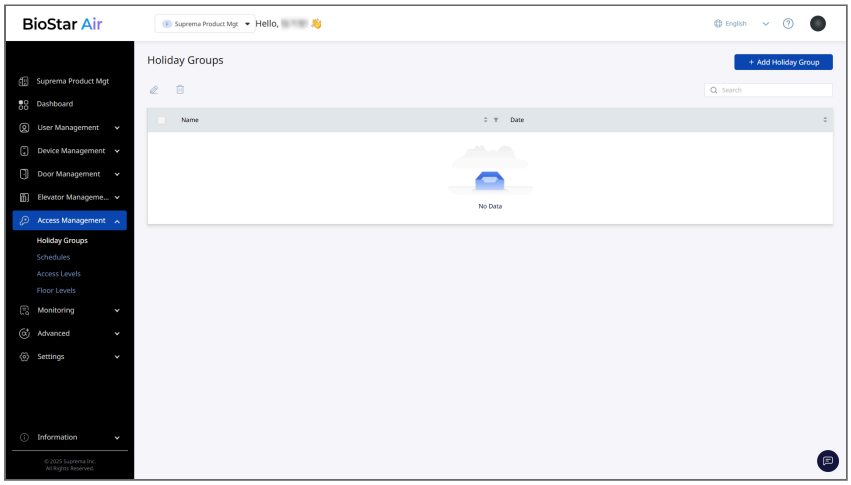
4. すべてのドアを選択したら、**OK** をクリックしてください。

5 アクセス権の設定

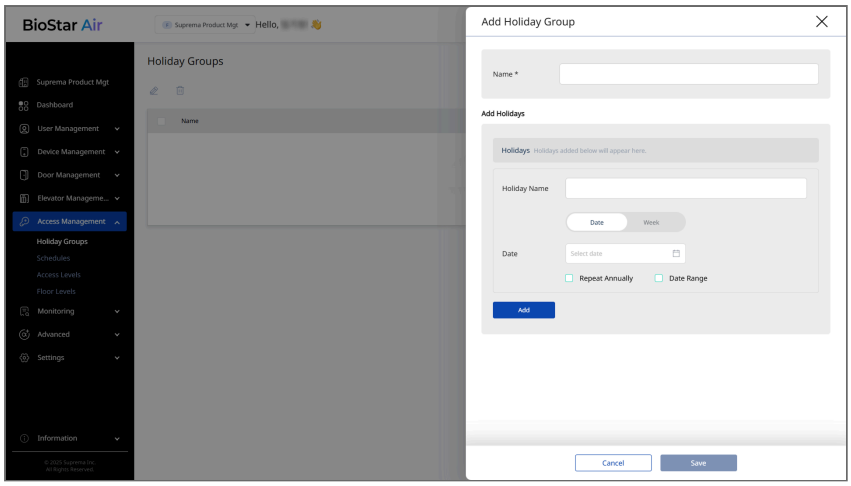
アクセス権を管理するには、次の手順に従ってください。

6 祝日グループの設定

1. 画面左のサイドバーで **アクセス管理** → **休日グループ** をクリックしてください。



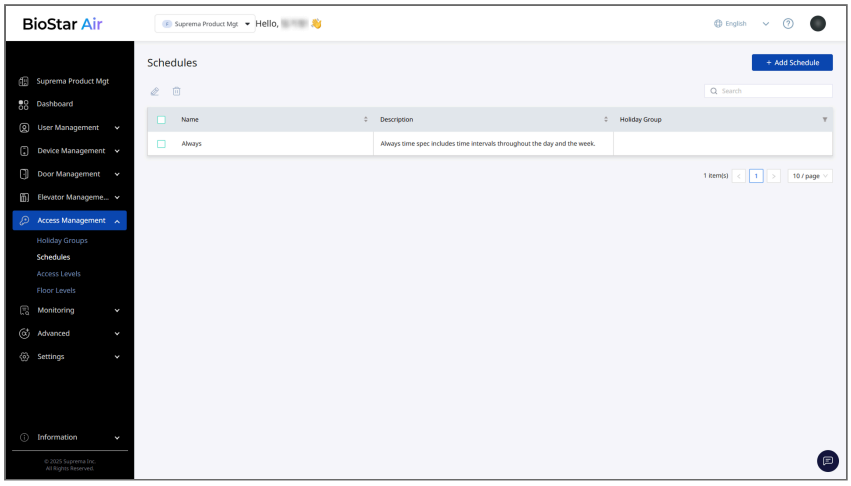
2. 画面右上の **休日グループの追加** ボタンをクリックします。
3. **休日グループの追加** パネルが表示されたら、名前を入力してください（例：「休日」）。



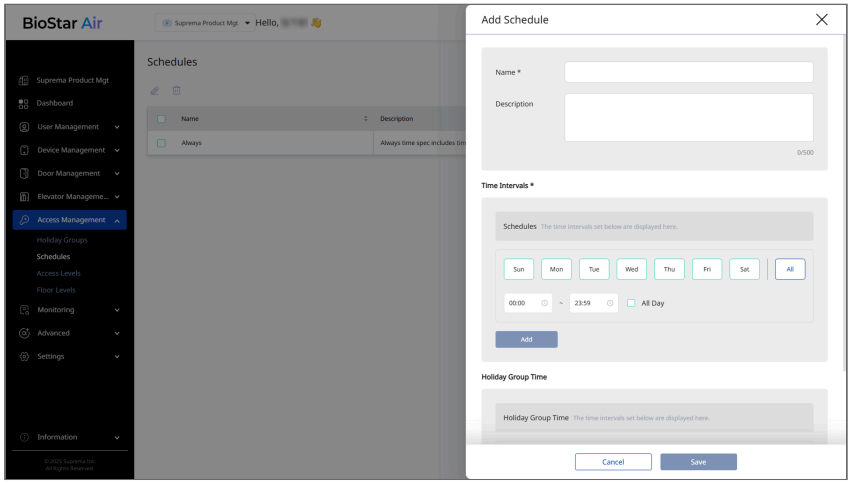
4. **休日の追加** セクションでアクセスを制限する祝日を設定し、**追加** をクリックしてください。
5. すべての祝日を追加したら、**保存** をクリックしてください。

7 スケジュールの作成

1. 画面左のサイドバーで **アクセス管理** → **スケジュール** をクリックします。



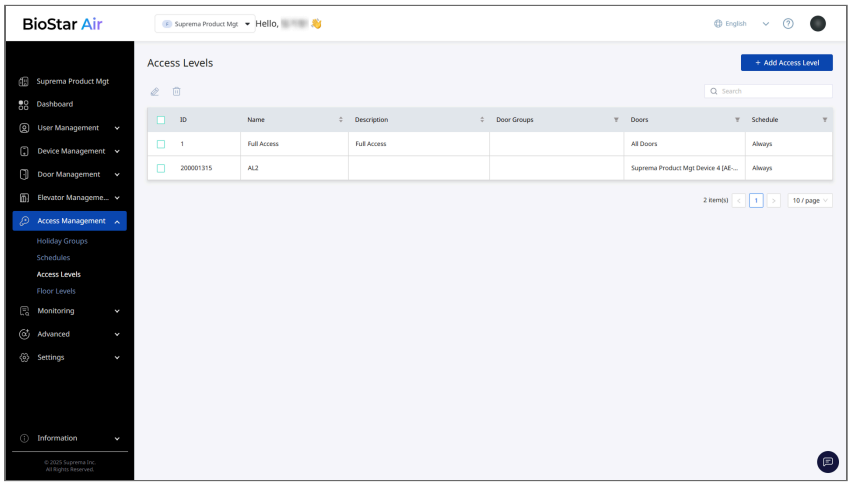
2. 画面右上の**スケジュールの追加**ボタンをクリックしてください。
3. **スケジュールの追加** パネルが表示されたら、名前を入力してください。



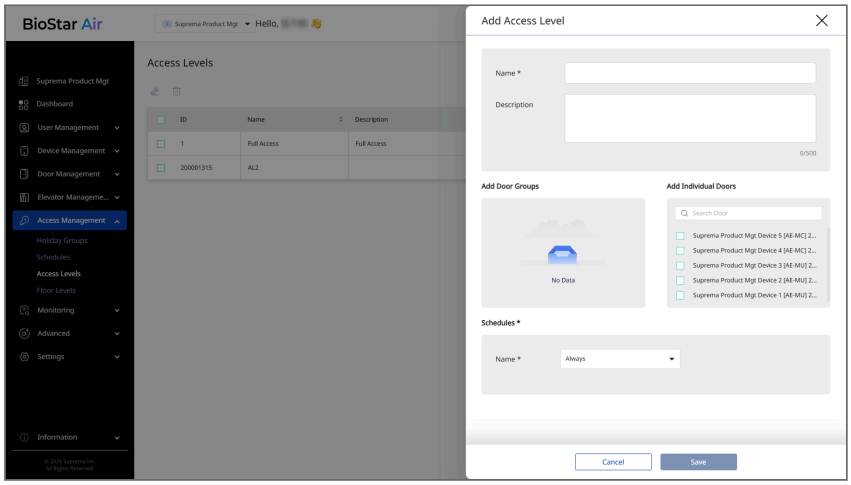
4. 有効にする曜日を選択し、祝日グループを関連付けてください。
5. スケジュール設定を完了したら、**保存** をクリックしてください。

8 アクセスレベルの設定

1. 画面左のサイドバーで **アクセス管理** → **アクセスレベル** をクリックしてください。



2. 画面右上の **アクセスレベルの追加** ボタンをクリックします。
3. **アクセスレベル** パネルが表示されたら名前を入力し、ドアグループ、個別ドア、およびスケジュールを割り当ててください。

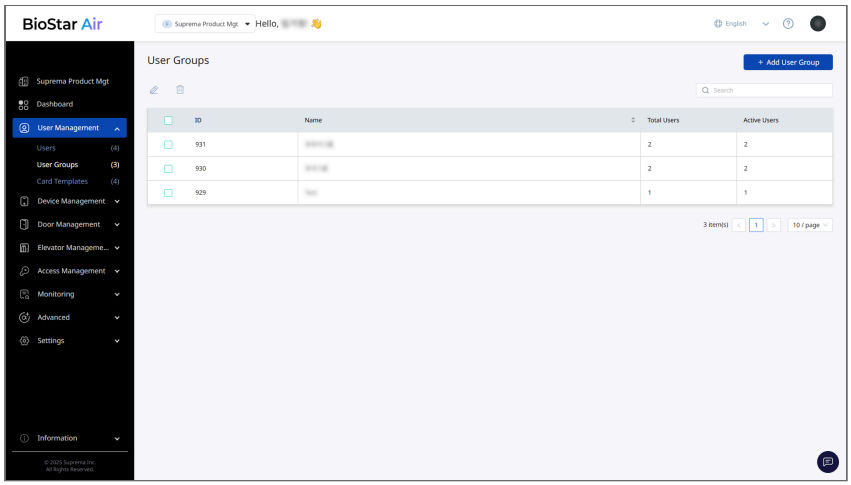


4. アクセスレベルの設定が完了したら、**保存**をクリックしてください。

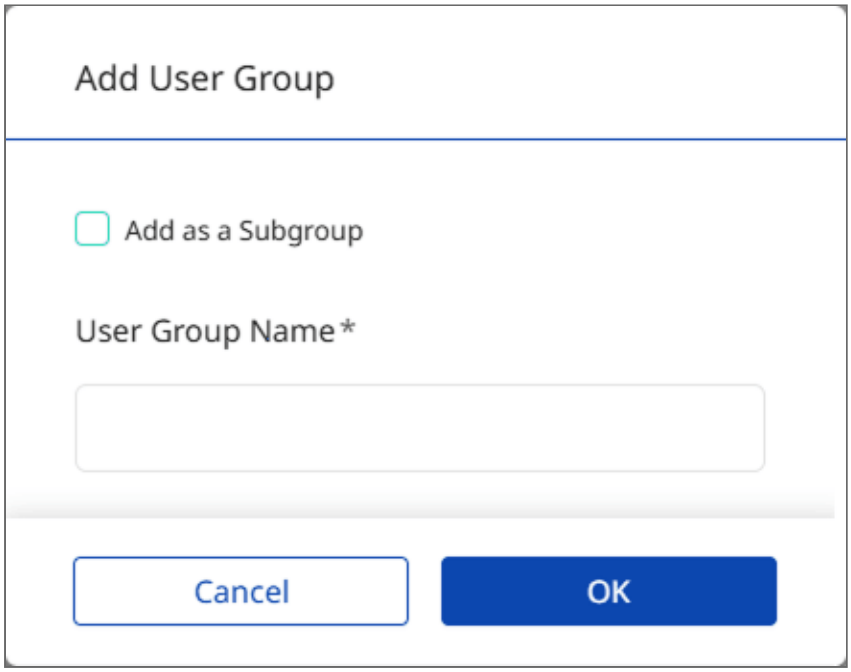
9 ユーザーグループの作成とユーザーの追加

ユーザーグループを作成し、新しいユーザーグループにユーザーを追加してください。

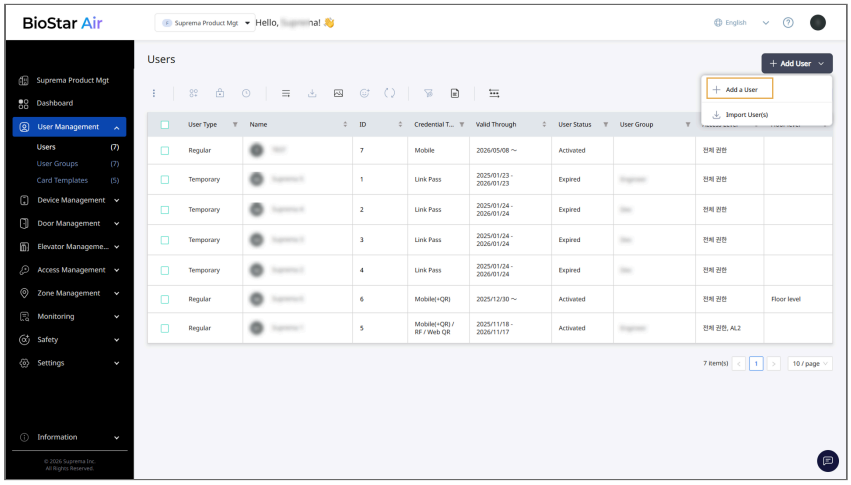
1. 画面左側のサイドバーで **ユーザー管理** → **ユーザーグループ** をクリックします。



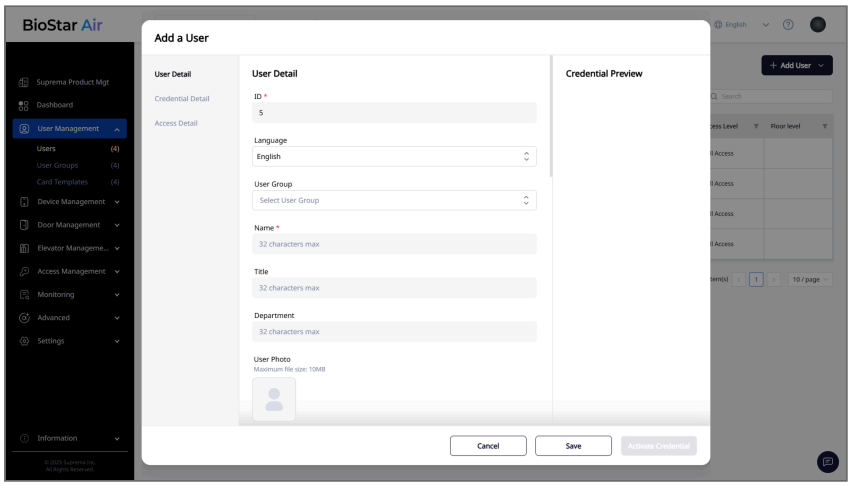
2. 画面右上の **ユーザーグループの追加** をクリックします。
3. **ユーザーグループの追加** ウィンドウが表示されたら、ユーザーグループ名を入力します。



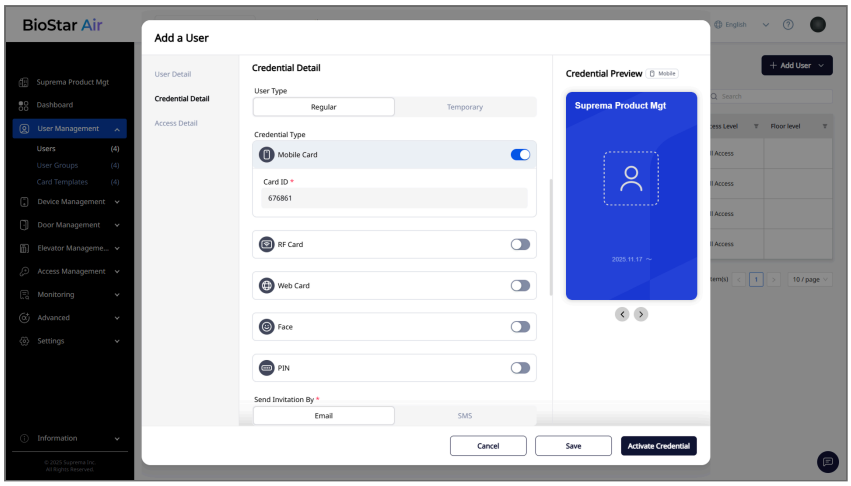
4. ユーザーグループを保存するには、**OK**をクリックしてください。
5. 画面左のサイドバーで **ユーザー管理** → **ユーザー** をクリックします。
6. 画面右上の **ユーザー追加** → **ユーザーを追加** をクリックしてください。



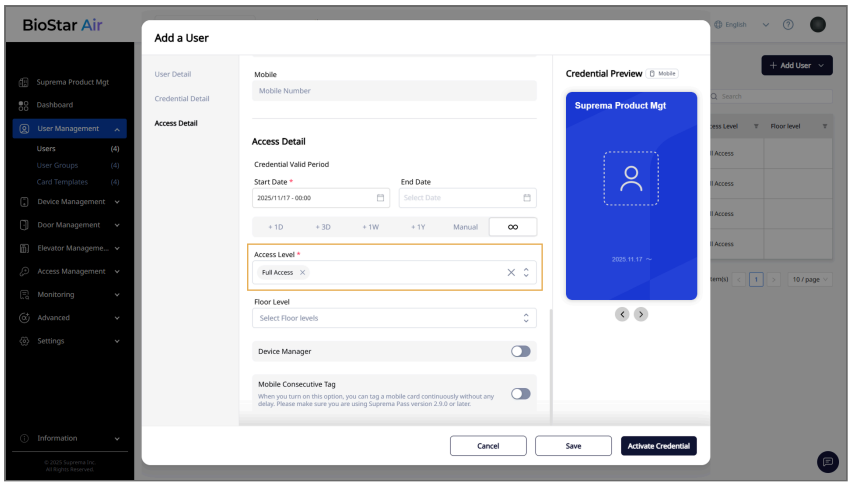
7. **ユーザーを追加** ウィンドウが表示されたら、**ユーザーの詳細** セクションでユーザーのIDや名前などを入力してください。



8. **認証情報の詳細** セクションで、1つ以上の認証方法を有効にしてください。



9. **アクセスの詳細** セクションでアクセスレベルを選択してください。



10. ユーザーのアクセス設定を完了するには、右下の **認証情報を有効化** をクリックしてください。

> **情報**
>
> **ユーザー管理** → **ユーザーグループ** メニューでは、ユーザーを一括管理し、再発行、停止、削除ができ、データのエクスポートやプロファイル画像の一括アップロードも可能です。

ヒント

チェックリスト

上記の手順を要約すると、次のステップに沿って進めます。

1. 管理者を追加してください。
2. デバイスを登録してください。
3. ドアを作成し、デバイスを割り当ててください。
4. ドアをグループに分類してください。
5. アクセス権を設定してください（祝日、スケジュール、アクセスレベル）。
6. ユーザーグループを作成し、ユーザーを追加してください。

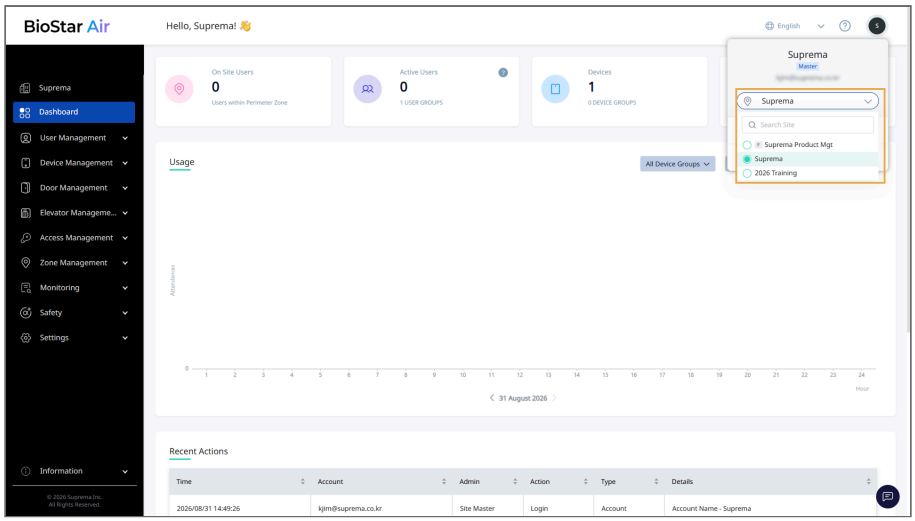
上記のステップに従うことで、BioStar Air サイトを円滑に設定できます。 提供されているユーザーガイドの個別ビデオチュートリアルを参照して、詳細を確認してください。

サイトセレクター(Site Selector)

BioStar Airポータルで**サイトセレクター**（Site Selector）機能を使うと、1つのメールアドレスで複数のサイトを管理でき、作業が簡素化されて何度もログインする手間が省けます。

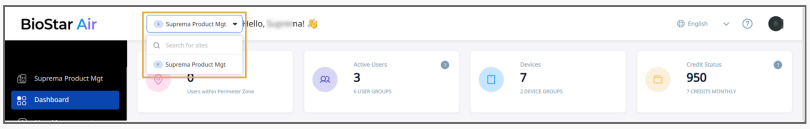
サイトセレクター(Site Selector)とは？

サイトセレクター機能を使用すると、複数のサイトを管理する場合でも1つの統合されたメールアドレスでBioStar Airポータルにログインできます。 各サイトごとに別のメールアドレスでログインする必要はありません。 1つのメールアドレスでログインし、**サイトセレクター**メニューを使用すると、管理するサイト間を簡単に切り替えられます。



情報

- 統合されたメールアドレスを使用しても、各サイトの権限と設定は独立して維持されます。 管理者の役割とアクセス権はサイトごとに個別に管理されます。
- **サイト選択**機能が表示されない、または誤ったサイトが表示される場合は、マイグレーションの依頼が完了しているか確認するか、サポートチームにお問い合わせください。
- **サイトセレクター**機能はログイン手順を簡素化し、複数のサイトを1つのアカウントに統合することで、BioStar Air で複数のサイトを管理する時間と労力を節約できます。
- サイト選択リストで F アイコンが表示されているサイトはフェデレーションサイト（Federation site）です。 フェデレーションサイトは画面左上に表示されます。 フェデレーションサイトの詳細はフェデレーションサイトの管理を参照してください。



新しいサイトの作成

パートナーポータルを通じて新しいサイトを作成する際、別のサイトの管理者アカウントとして登録されている既存のメールアドレスを使用できます。 システムは新しいサイトを既存のメールアドレスに自動的に紐付け、1つのアカウントで複数のサイトを管理できるようにします。

- 新しいサイトはパートナーポータルから作成してください。
- 管理者のメールアドレスを入力するよう促されたら、既に別のサイトに紐付けられているメールアドレスを使用してください。
- 新しいサイトは既存のアカウントに自動的に関連付けられます。

情報

パートナーポータルへの登録と利用に関する詳細はパートナーポータルの使い方を参照してください。

1つのメールアドレスで複数のサイトを管理

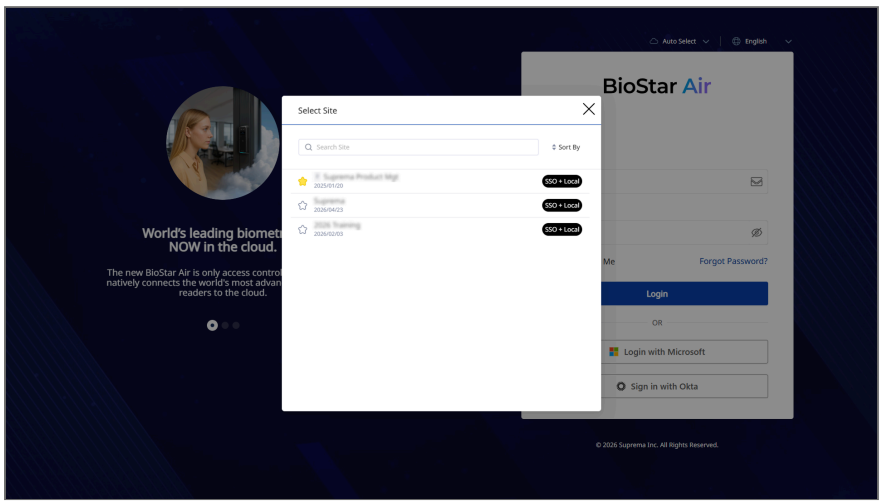
既に複数のサイトを管理していて、各サイトで別々のログイン認証を使用している場合は、**Suprema** に手動マイグレーションを依頼する必要があります。 このプロセスによりメールアドレスを統合し、すべてのサイトを単一のログインで管理できるようになります。

- サポートチームにご連絡のうえ、サイトの手動マイグレーションを依頼してください。
- bob+site1@example.com や bob+site2@example.com のようなエイリアスアドレスを使用している場合は、ルートのメールアドレス（bob@example.com）を提供してください。
- 各サイトごとに完全に固有のメールアドレスを使用している場合は、すべてのメールアドレスの一覧を提供する必要があります。
- マイグレーションが完了すると、**サイトセレクター**機能を通じて単一のメールアドレスで全サイトにアクセスできるようになります。

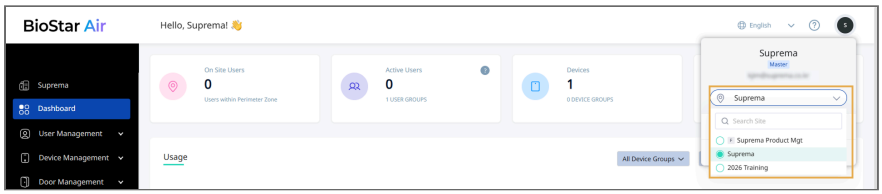
サイトセレクター（Site Selector）の使い方

複数のサイトを管理できるメールアドレスがあれば、ログインしてサイトを切り替えるのは簡単です。

1. メールアドレスとパスワードを入力してください。
2. 複数のサイトを管理している場合は、**サイトを選択** ウィンドウで目的のサイトを素早く見つけることができます。 サイトを選択するとダッシュボードに移動します。



3. ログインしたら、画面右上のプロフィールアイコンをクリックしてください。
4. ポップアップメニューが表示されたら、メールアドレスの下にある**サイトセレクター**機能をクリックしてください。



メールアドレスに紐づくすべてのサイトの一覧を確認できます。

BioStar Airアプリのはじめ方

BioStar Airアプリは、BioStar Airウェブポータルと同等のすべての機能を提供します。 ユーザーはモバイル端末から直接出入管理を行い、イベントログを監視し、デバイスを制御し、管理作業を実行できます。

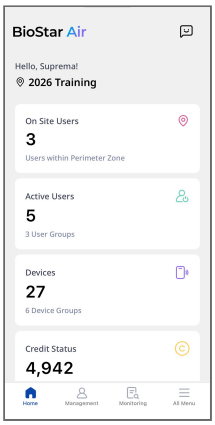
モバイルアプリのダウンロード

モバイル端末でBioStar Airアプリをダウンロードし、ログインします。

- モバイル端末にBioStar Airアプリをダウンロードしてインストールします。
  - iOS
  - Android
- BioStar Airウェブポータルで使用するIDとパスワードでログインします。

情報

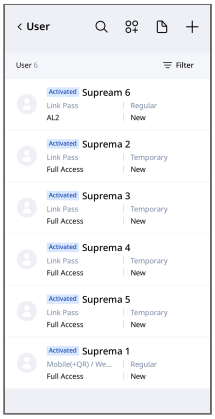
- ウェブ版と同じ認証情報でログインしていることを確認します。
- BLEモードで更新するにはデバイスに近づく必要があります。
- ライブビデオ監視などの一部の機能には接続されたカメラが必要です。



ダッシュボード

モバイルアプリにログインすると、初期画面の**ダッシュボード**で以下の情報が表示されます。

- 1日のユーザー入退室数
- 登録されているアクティブユーザーの総数
- 接続されたデバイス数
- クレジットの状態



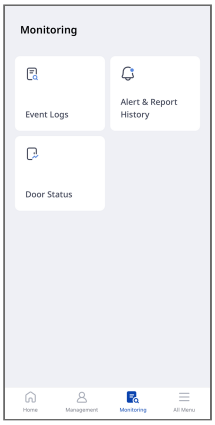
ユーザー管理

初期画面の**アクティブユーザー**カードをタップするか、**管理** → **ユーザー**の順にタップします。

- ユーザーを選択して詳細を確認します。
- ユーザーの状態を編集（再発行、一時停止、削除、または有効化）できます。
- 新しいユーザーを追加するには、＋ボタンをタップし、必要な詳細情報を入力します。

情報

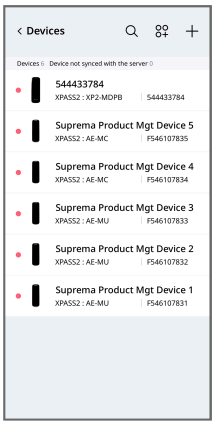
- モバイルアプリでのユーザー追加方法についてはユーザーの追加をご参照ください。
- BioStar Airポータルでのユーザー追加方法についてはユーザーの追加をご参照ください。
- ユーザー管理の詳細についてはユーザー管理をご参照ください。



モニタリング

モニタリングでは以下の情報が表示されます。

- **イベントログ**: イベントログと監査ログを監視および分析できます。 詳細については、イベントログの使い方および変更ログの使い方をご参照ください。
- **アラートとレポート履歴**: ウェブポータルとモバイルアプリで以前発生したアラートと作成されたレポートの履歴を確認できます。 詳細についてはアラートとレポート履歴の確認用ガイドをご参照ください。
- **ドアの状態**: サイトに接続されているドアの状態をリアルタイムで監視できます。 詳細についてはドアの状態を監視するをご参照ください。
  - ドアの状態を確認し、リモートで制御できます。
  - 1回タップしてドアを編集するか、長押しして複数のドアを選択し、一括操作を実行できます。
  - ドアを**解錠モード**または**施錠モード**に設定すると、リレー設定またはスケジュールが無視されます。
  - 必要に応じて使用していないドアを削除します。
- （接続されたカメラがある場合）ライブビデオ



デバイス

初期画面の**デバイス**カードをタップするか、**管理** → **デバイス**の順にタップします。

- 登録されているすべてのデバイスを確認できます。
- デバイスを選択して編集、ファームウェアの更新、または再起動ができます。
- ネットワークに接続されていないデバイスは、ファームウェア更新のためにモバイル端末と近い距離で**BLEモード**を使用します。
- 新しいデバイスを追加するには、＋ボタンをタップします。

> **情報**
> デバイス管理の詳細は以下のドキュメントをご参照ください。
> - BioStar Air App: エッジデバイスの登録と削除
> - BioStar Airポータル：デバイス

サイトを管理する

BioStar Airでの**サイト**は出入管理システムの中核となる単位であり、ユーザーが出入りできる物理的な場所を指します。 各サイトは固有の設定、ユーザー、デバイス、およびアクセス権を持つことができます。 管理者は複数のサイトを作成および管理することで、さまざまな場所での出入管理を効率的に運用できます。

以下のドキュメントを参照して、BioStar Airポータルでサイトを効果的に管理する方法を確認してください。

ユーザー

BioStar Airでユーザーアカウントを作成し、さまざまな資格情報（Mobile Card、RF Card、Web Card、Face、PIN）を設定し、アクセス権と有効期限を構成する方法を案内します。 個別のユーザー管理から複数ユーザーへの一括操作、ユーザーグループおよびフィルタリングの管理まで、ユーザー管理の全般的な作業を扱います。

> **ヒント**
> ユーザー管理機能は、以下の動画でよりわかりやすく理解できます。

ユーザーの追加

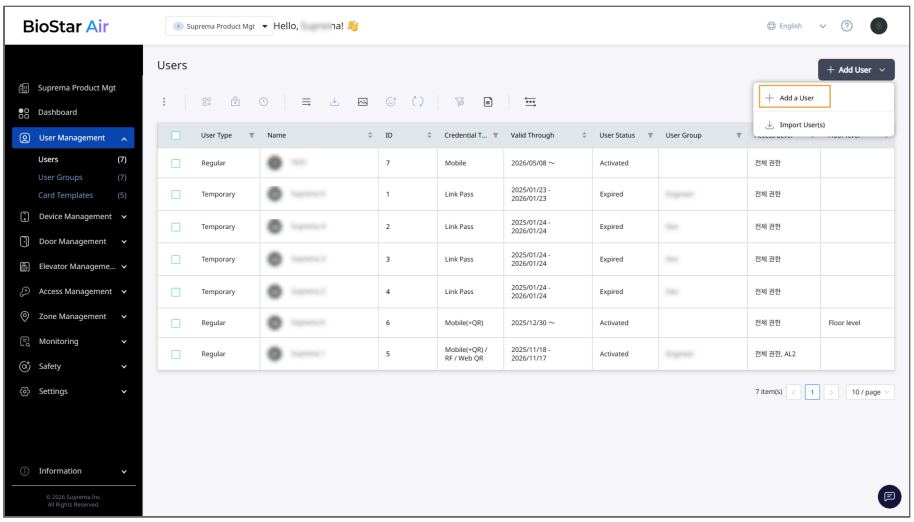
このドキュメントは、BioStar Airで個々のユーザーを追加および管理する方法を段階的に案内します。 ユーザータイプ（通常／一時）を選択し、各タイプに適したクレデンシャルを発行し、アクセスレベルと有効期限を設定する全プロセスを扱います。 追加したユーザー情報の編集や削除方法も含みます。

> **ヒント**
> 新しいユーザーの追加全プロセスを段階的に案内する以下の動画を参照してください。

ユーザーの追加を開始

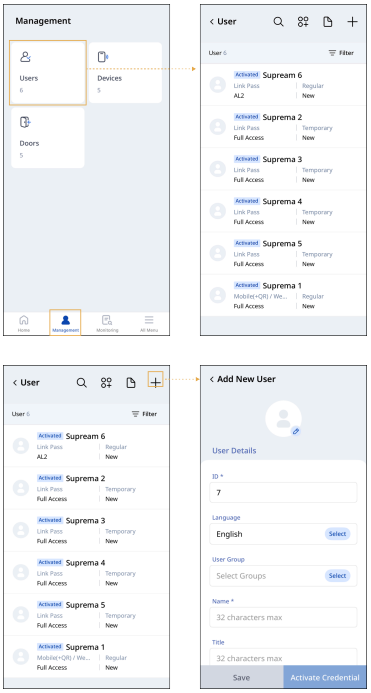
Web

1. 画面左のサイドバーで **ユーザー管理** → **ユーザー** をクリックします。
2. ユーザーリストが表示されます。
3. 画面右上の **ユーザー追加** → **ユーザーを追加** をクリックしてください。



ユーザーを追加 画面が表示されたら、各セクションに必要な情報を入力して設定してください。 すべてのセクションの必須項目を設定し、右下の **認証情報を有効化** をクリックしてください。

Mobile



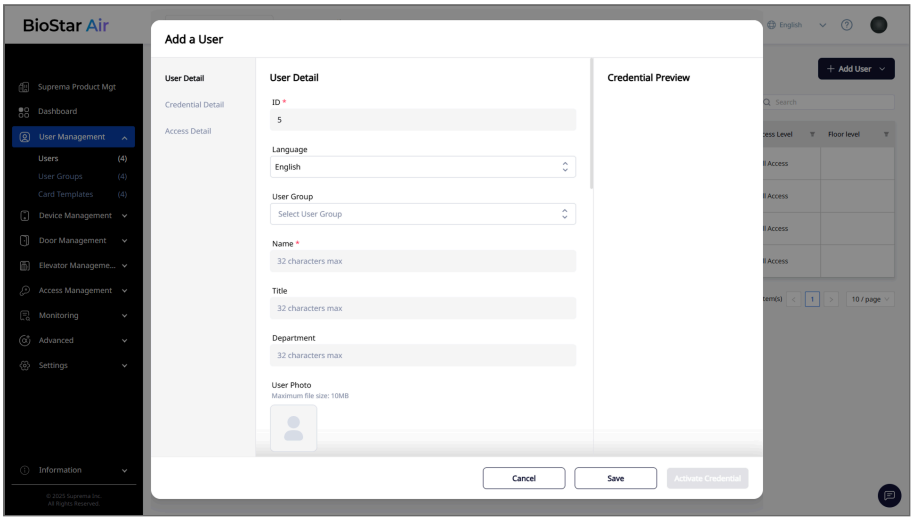
1. モバイルアプリにログインしてください。
2. 画面の下部にある **管理** をタップします。
3. **ユーザー** カードをタップしてください。
4. ユーザー一覧画面上部の ＋ ボタンをタップしてください。

ユーザーを追加 画面が表示されたら、各セクションに必要な情報を入力して設定してください。 すべてのセクションの必須項目を設定し、右下の **認証情報を有効化** をクリックしてください。

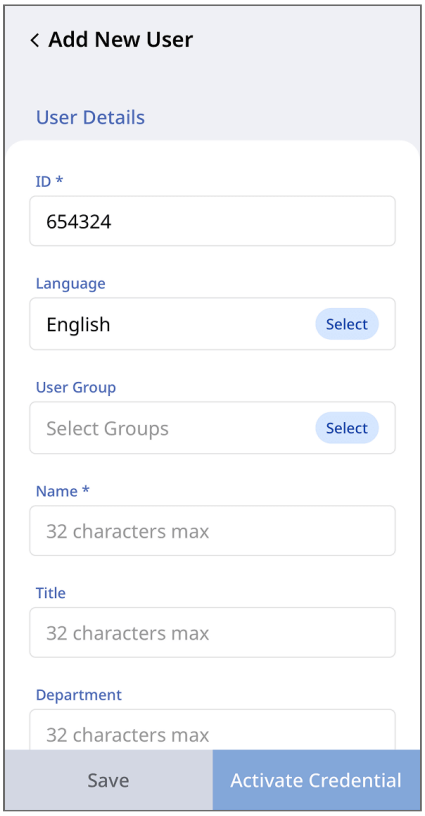
ユーザー情報の入力

ユーザーの詳細 セクションで追加するユーザーの基本情報を入力してください。

Web



Mobile



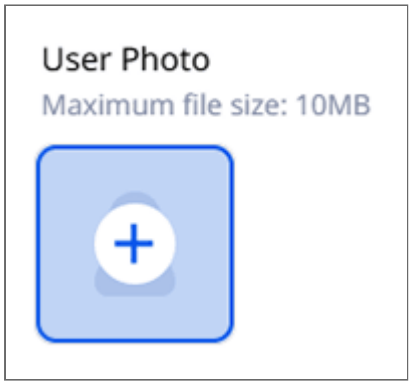
- **ID**：特定のIDを直接入力するか、システムに連番で生成させることができます。
- **言語**：ユーザーの基本言語を選択してください。
- **ユーザー グループ**：ユーザーが所属するグループを選択してください。
- **名前**：ユーザーの氏名を入力してください。
- **役職**：ユーザーの役職を入力してください。
- **部署**：ユーザーが所属する部署名を入力してください。
- **ユーザー写真**：ユーザーのプロフィール画像をアップロードできます。 詳細については プロフィール画像のアップロード を参照してください。

> **情報**
>
> - * は必須入力項目です。
> - ユーザーのメールアドレスと電話番号は、**認証情報の詳細** セクションの **招待の送信者** 項目で入力できます。

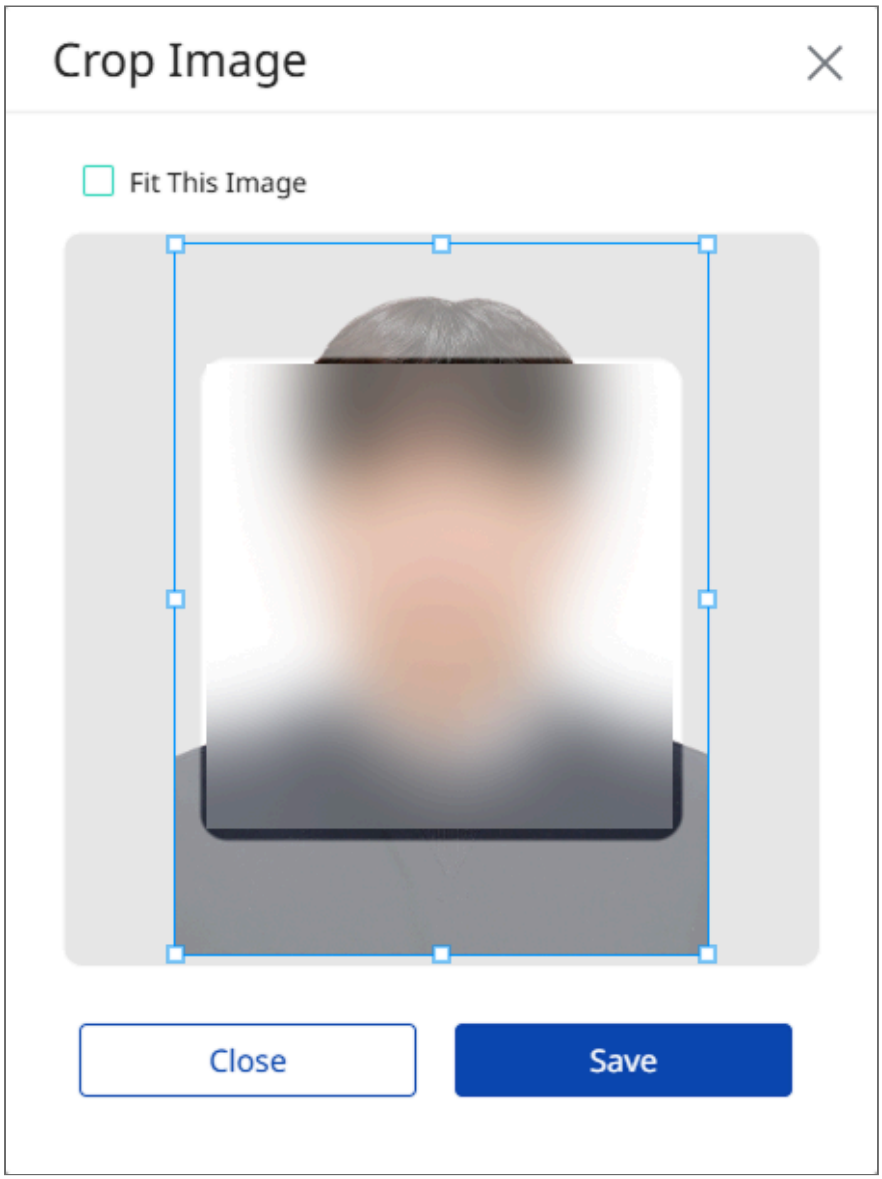
プロフィール画像のアップロード

Web

1. プロフィール画像領域にマウスオーバーし、プラスボタンをクリックしてください。

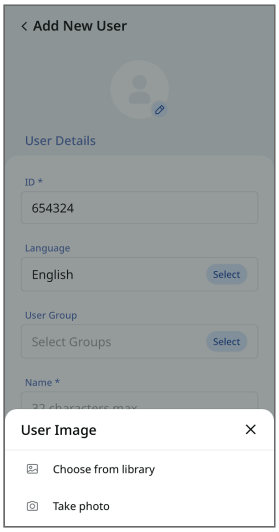


2. ローカルに保存された画像ファイルを選択してください。
3. **画像をクロップ** ウィンドウが表示されたら、写真のサイズを希望の大きさに調整してください。 画像サイズを自動調整するには、**サイズフィット** オプションをクリックしてください。



4. アップロードした画像をプロフィールとして保存するには、**保存** をクリックしてください。

Mobile



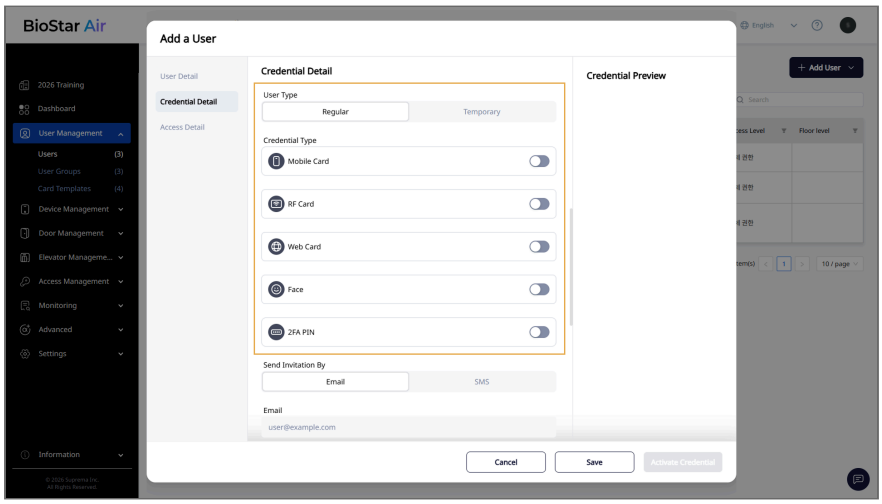
1. プロフィール画像をタップしてください。
2. 下部に表示されるメニューから、希望する方法で画像を追加してください。
   - **ライブラリから選択**：モバイル端末に保存された画像ファイルを選択してアップロードできます。
   - **写真を撮る**：モバイル端末のカメラで写真を撮影してアップロードできます。
3. アップロードした画像を適切なサイズに調整して保存してください。

ユーザー種類の選択

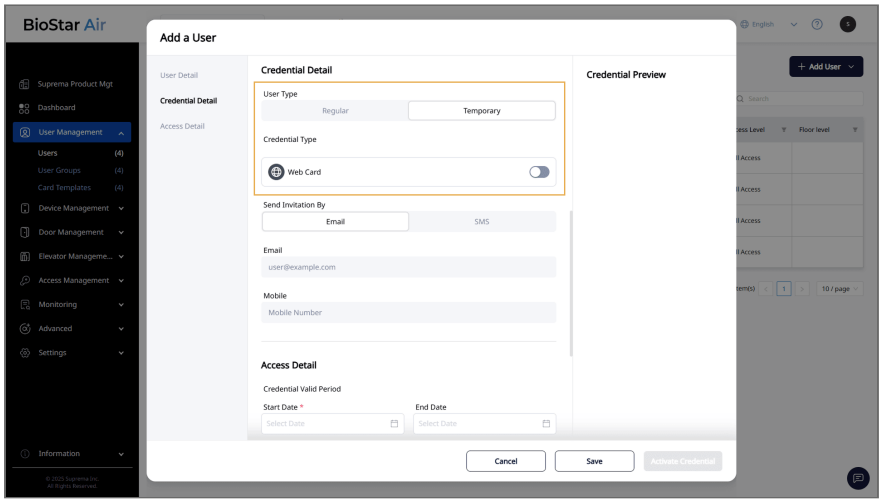
Web

認証情報の詳細 セクションで、追加するユーザーが通常ユーザーか一時訪問者かを選択してください。 ユーザーの種類により発行できるクレデンシャルの種類が異なります。

- **通常**：組織または施設の正規メンバーで、長期かつ継続的な入退室権限が必要なユーザーです。 すべてのクレデンシャルタイプを発行できます。

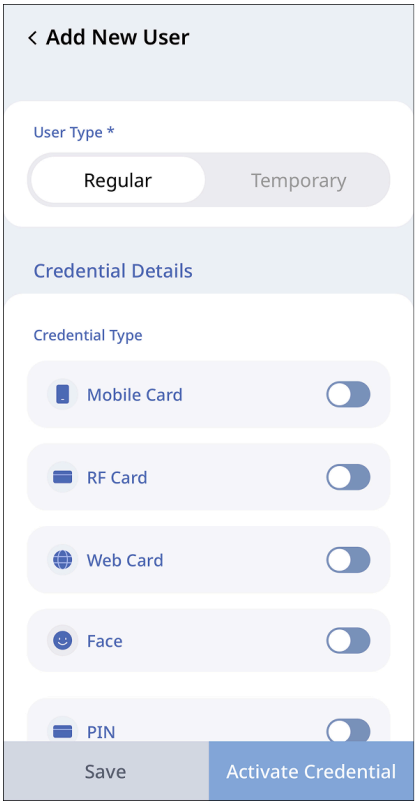


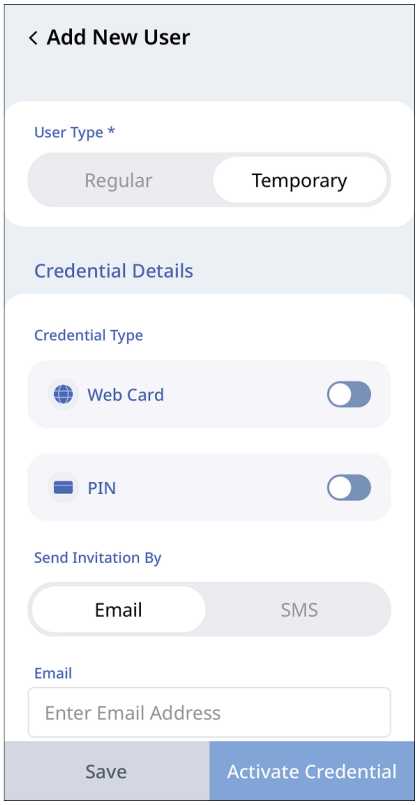
- **ゲスト**：短期かつ限定的な入退室権限を必要とする訪問者または非正規メンバーです。 ゲスト、外部来訪者、短期契約者、配達員などが該当します。 **ウェブカード** のクレデンシャルのみ発行でき、QRコードとLinkPassが含まれます。



Mobile

タイプ セクションで、追加するユーザーが通常ユーザーか一時訪問者かを選択してください。 ユーザーの種類により発行できるクレデンシャルの種類が異なります。





- **通常**：組織または施設の正規メンバーで、長期かつ継続的な入退室権限が必要なユーザーです。 すべてのクレデンシャルタイプを発行できます。
- **ゲスト**：短期かつ限定的な入退室権限を必要とする訪問者または非正規メンバーです。 ゲスト、外部来訪者、短期契約者、配達員などが該当します。 **ウェブカード** のクレデンシャルのみ発行でき、QRコードとLinkPassが含まれます。

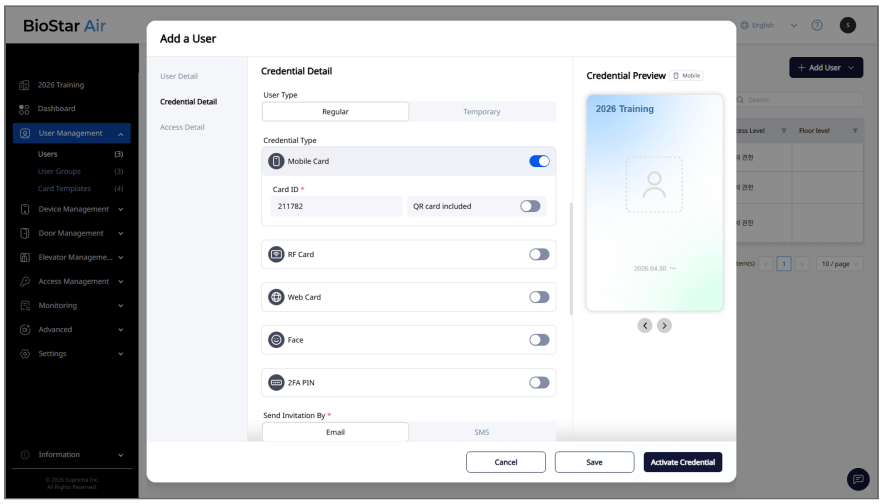
> **情報**
>
> - **通常** タイプのユーザーは自動的に全アクセスレベルが割り当てられる場合がありますが、**ゲスト** タイプのユーザーは手動でアクセスレベルを選択する必要があります。
> - **ユーザータイプ** は BioStar Air 2.6 以降でサポートされています。

クレデンシャルの発行

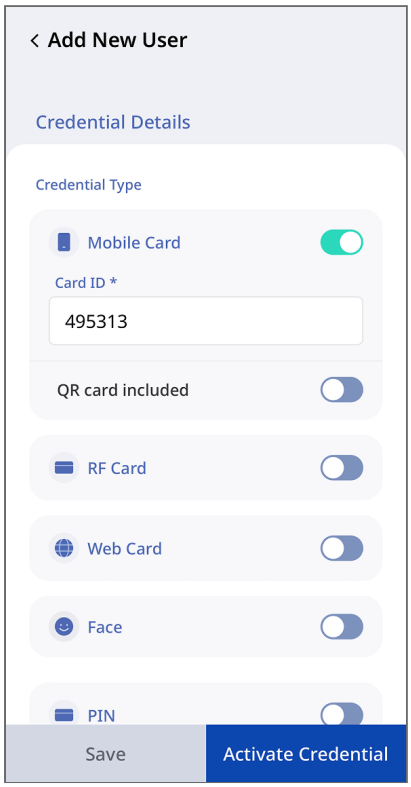
ユーザー情報を入力した後、**認証情報の詳細** セクションでアクセス認証手段として使用するクレデンシャルを設定してください。各クレデンシャルには有効化または無効化できるトグルスイッチがあります。

- **モバイルカード**：Suprema Pass モバイルアプリをアクセス認証手段として使用できます。 管理者はカードID番号を編集できます。

Web

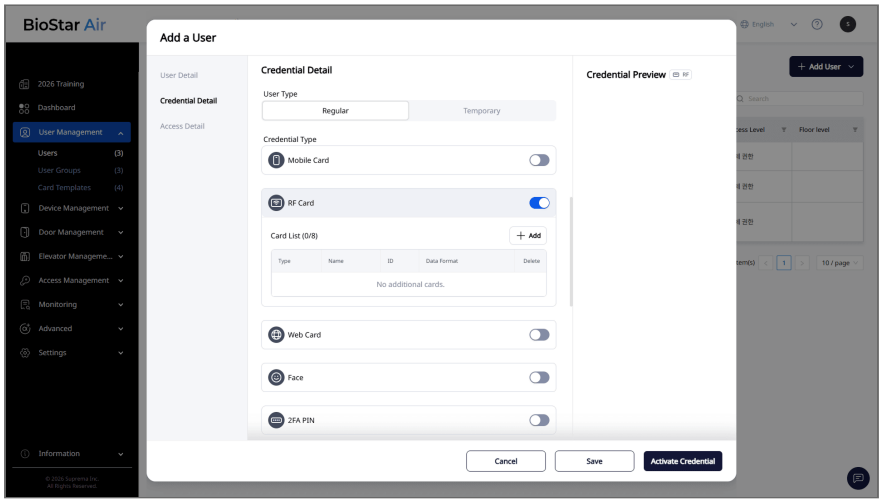


Mobile

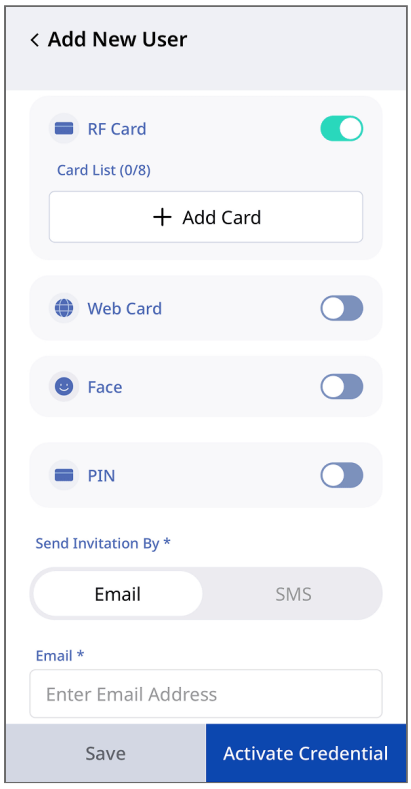


- **RFカード**：ユーザーごとに最大8枚のRFIDカードをアクセス認証手段として追加できます。 **追加** をクリックしてください。

Web

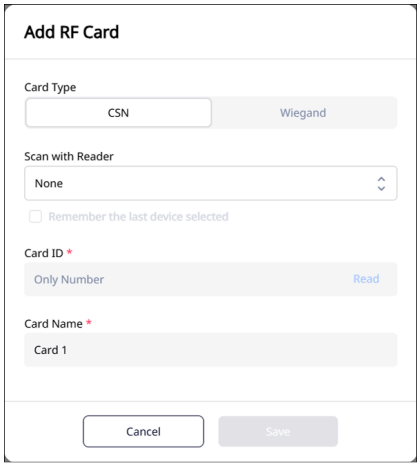


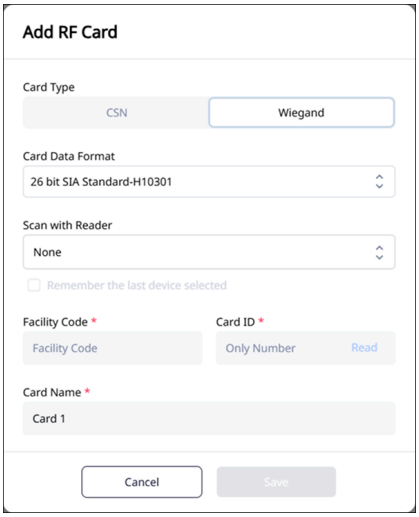
Mobile



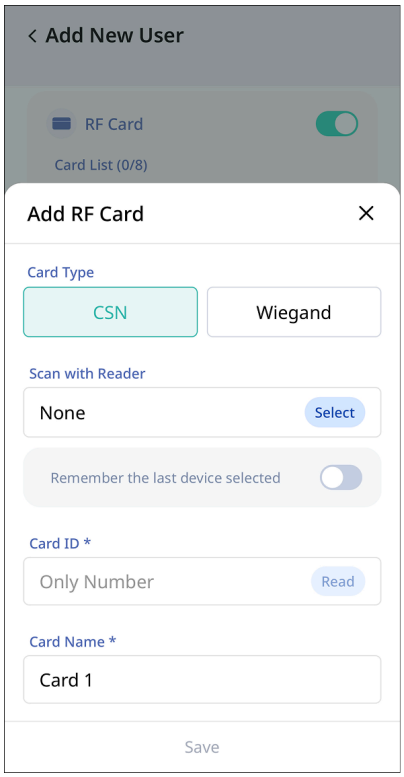
カードの種類（CSN / Wiegand）、カードIDおよびカード名を構成できます。 **リーダーでスキャン** 項目でリーダーを選択してください。 接続されたリーダーを使用して実物のRFIDカードをスキャンすることもできます。

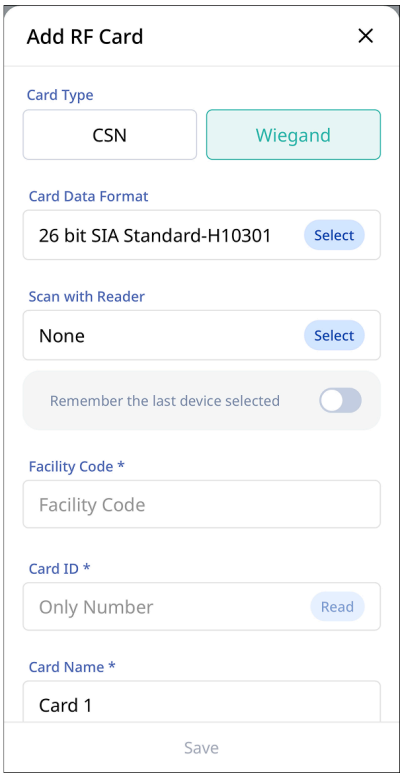
Web





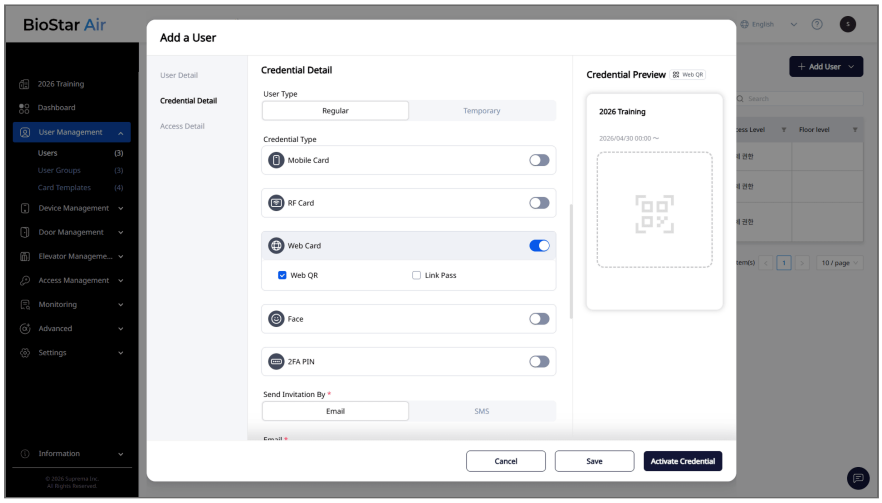
Mobile



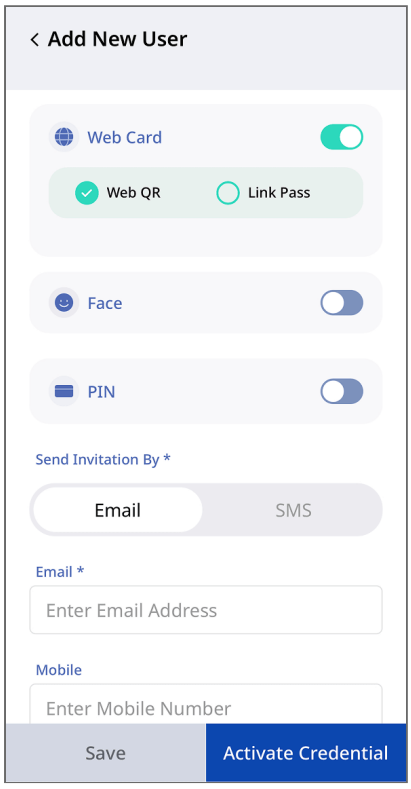


- **ウェブカード**：**Web QR** または **リンクパス** をアクセス認証手段として使用できます。

Web



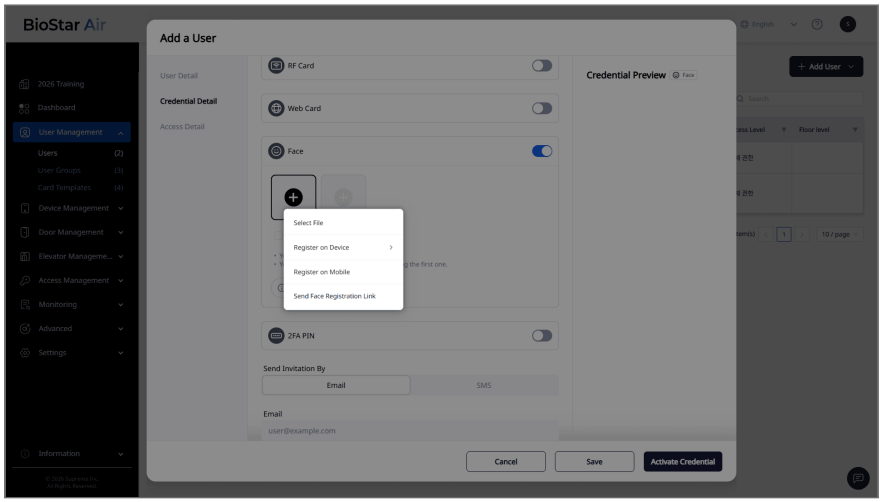
Mobile



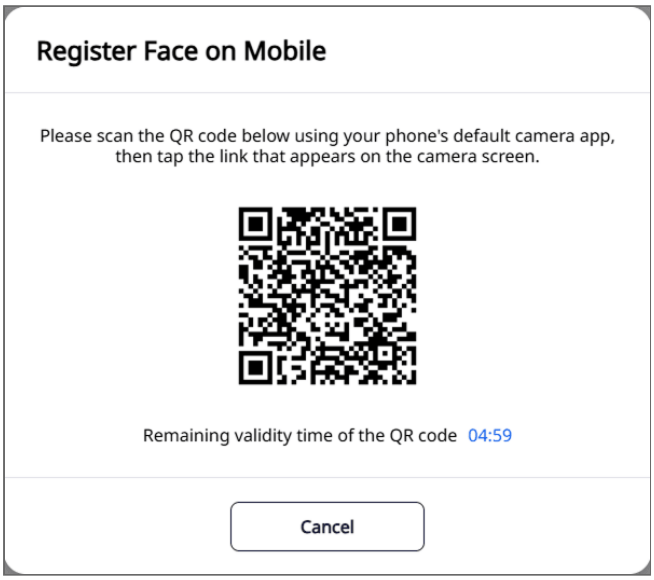
> **Web QR** は **設定** → **サイト** → **追加機能** で **QRリーダー** オプションを有効にする必要があります。

- **顔**：アクセス認証手段として顔のプロフィール画像を最大2つまで追加できます。 既存の画像をアップロードするか、デバイスで登録できます。 または、メールやSMSでリンクを送信して、ユーザーがモバイル端末のカメラで直接登録できます。

Web

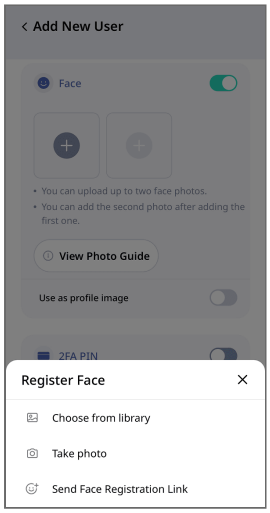


- **ファイルを選択**：ローカルに保存された画像ファイルを選択してアップロードできます。
- **デバイスに登録**：登録済みのデバイスを使用して顔画像を登録できます。
- **モバイルで登録**：モバイル端末のカメラで QR コードをスキャンすると、顔画像を登録できるリンクに移動できます。



- **顔登録リンクを送信**：ユーザーのメールやSMSに顔登録リンクを送信して、モバイル端末のカメラで顔を直接登録できます。

Mobile



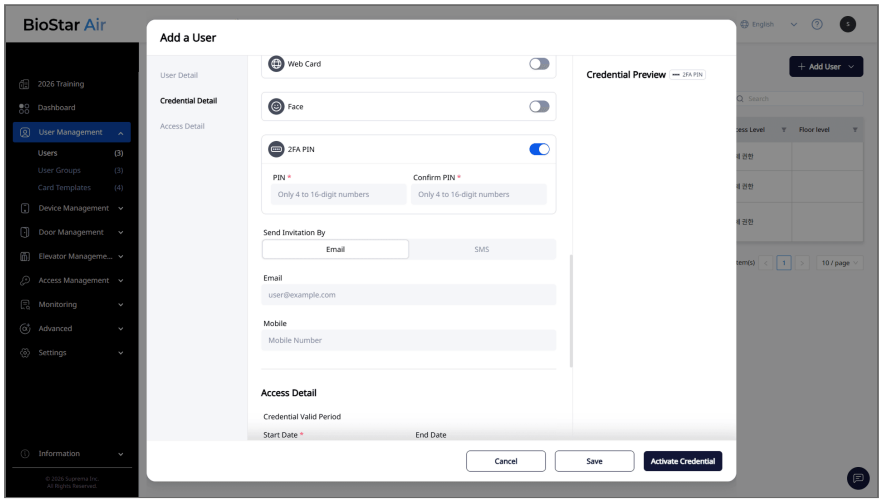
顔写真を追加するには ＋ ボタンをタップしてください。 画面下部に表示されるメニューから、任意の方法で顔写真を追加できます。

- **ライブラリから選択**：モバイル端末に保存された画像ファイルを選択してアップロードできます。
- **写真を撮る**：モバイル端末のカメラで写真を撮影してアップロードできます。
- **顔登録リンクを送信**：ユーザーのメールに顔登録リンクを送信し、モバイル端末のカメラで直接顔を登録できます.
- **プロフィール画像として使用**：プロフィール画像を顔認証用のクレデンシャルとして使用できます。

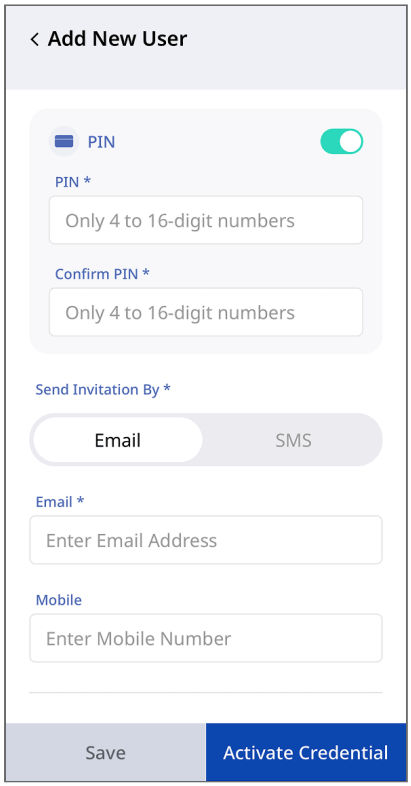
> 顔写真登録の詳細については、**写真ガイドを表示** ボタンをクリックしてください。

- **二要素認証 PIN**：4〜16桁のPINを設定して、2要素認証（2FA）の一部として使用できます.

Web



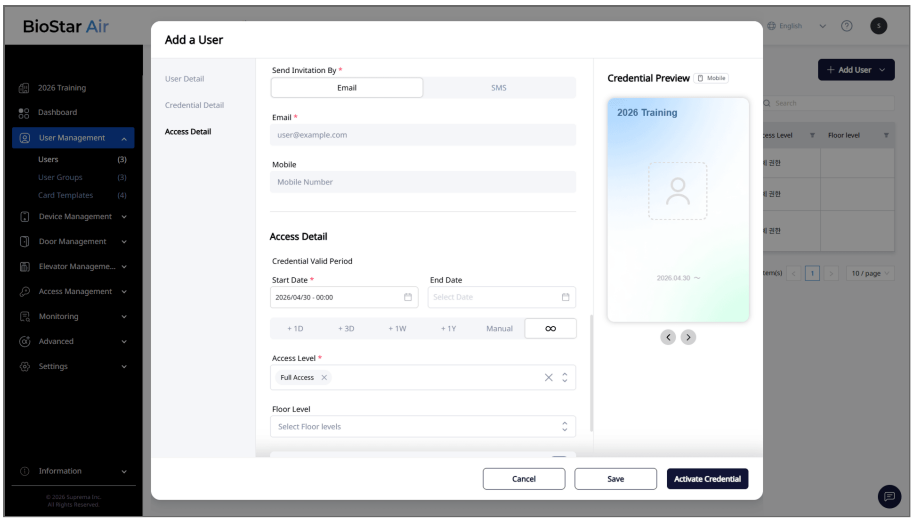
Mobile



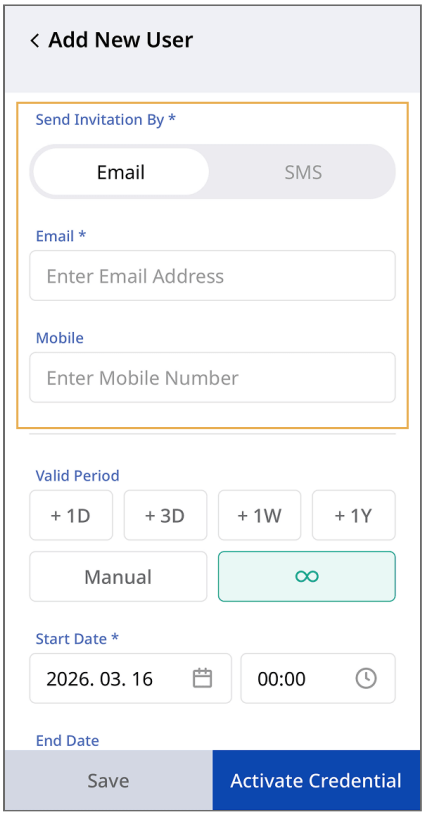
招待リンクの送信

モバイルカード または **ウェブカード** を使用するユーザーに、Suprema Pass アプリのダウンロードリンクをメールで送信できます。 メールアドレス（必須）と携帯電話番号（任意）を入力してください。

Web



Mobile



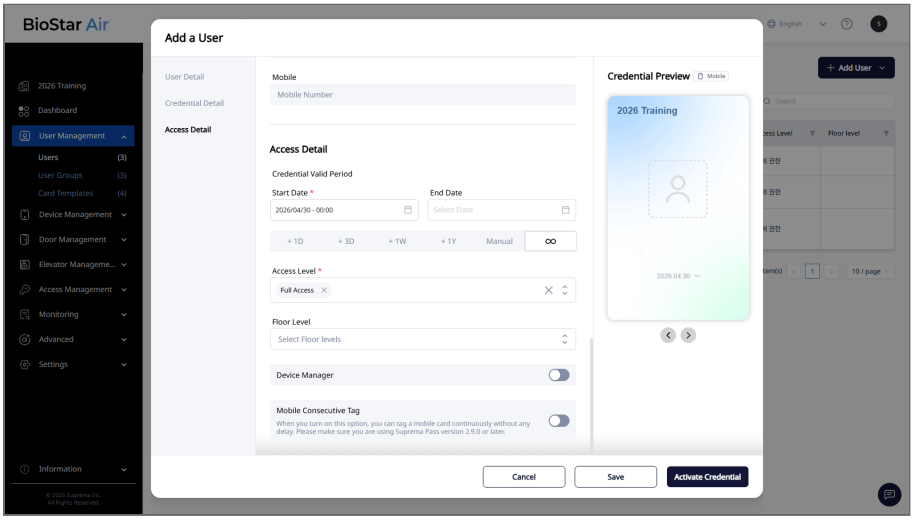
情報

SMS オプションは **設定** → **クレジットセンター** でSMSクレジットのチャージをリクエストする必要があります。

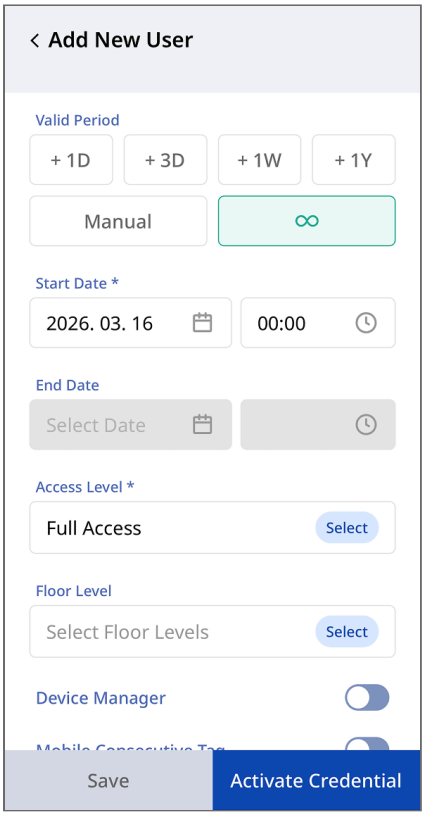
アクセスレベルと有効期限の設定

クレデンシャルを選択した後、**アクセスの詳細** セクションでユーザーのクレデンシャル有効期間、アクセスレベルおよびフロアレベルなどを構成してください。

Web



Mobile



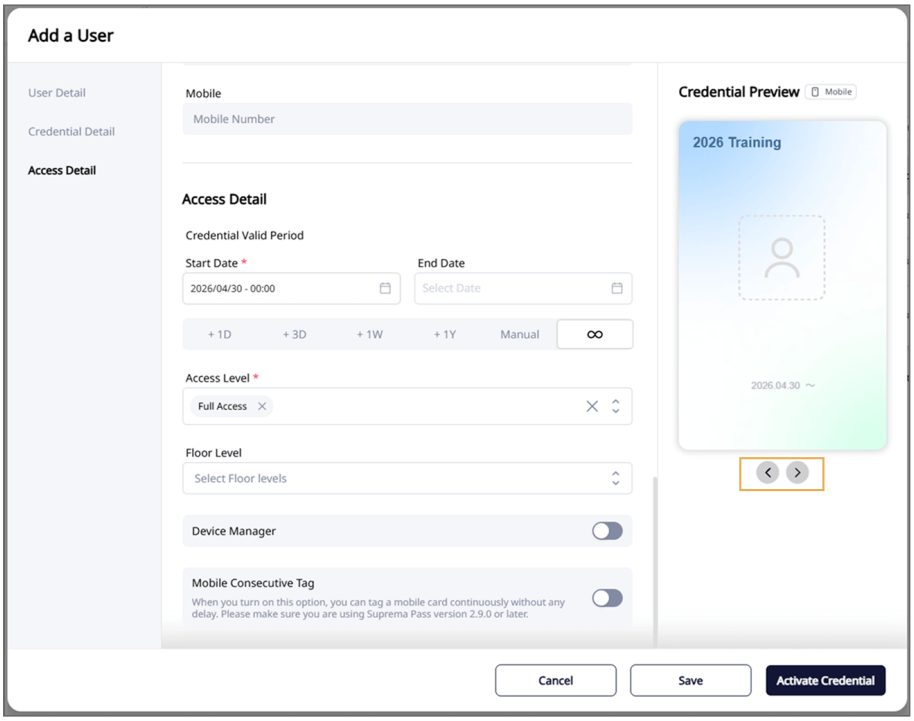
- **認証情報の有効期間**：ユーザーに発行したクレデンシャルの有効期間を設定してください。 終了日を設定しない場合は、∞ ボタンをクリックしてください。
- **アクセス レベル**：ユーザーがアクセスできる権限を選択してください。 全権限を付与するか、あらかじめ定義されたアクセスレベルを選択してください。
- **床面高さ**：ユーザーがアクセスできるフロアレベルを選択してください。
- **デバイスマネージャ**：ユーザーが特定のデバイスでアクセス権を管理できるように許可できます。
- **モバイル連続タグ**：ウェイトなしで連続してモバイルカードをタッチできるように許可できます。 この機能はSuprema Passアプリ2.9.0以降でサポートされています。

> **情報**
>
> - フロアレベルの設定に関する詳細は フロアレベルを管理する を参照してください。
> - **デバイスマネージャ** オプションは BioStation 3、X-Station 2 のユーザーのみ利用できます. デバイス管理者に設定されたユーザーは、BioStation 3、X-Station 2 の管理者メニューを利用できます.

カードテンプレートの選択

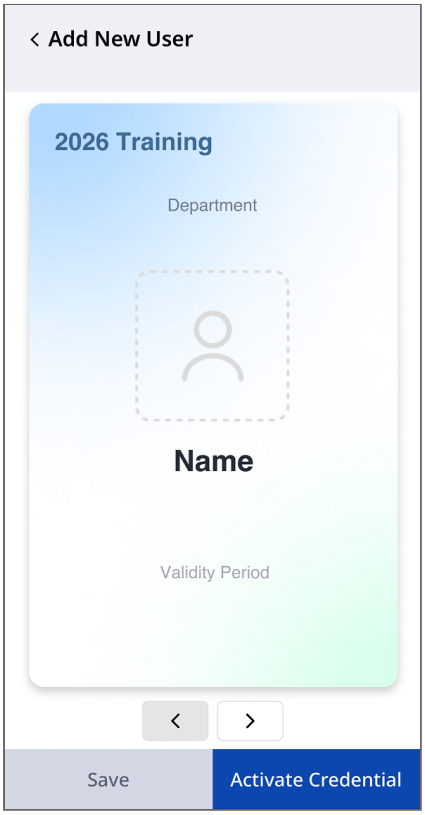
Web

カードテンプレートのデザインを変更するには、右パネルのカードテンプレートの下で ‹ または › ボタンをクリックして選択できます。



Mobile

資格情報のプレビューで ‹ または › ボタンをタップして選択できます。



情報

新しいカードテンプレートの作成方法に関する詳細は カードテンプレートの管理 を参照してください。

ユーザーの保存または有効化

ユーザーに関するすべての設定を構成したら、以下のオプションのいずれかを選択できます。

- ユーザーを保存して後で有効化するには、**保存** をクリックしてください。
- クレデンシャルを即時に発行して有効化するには、**認証情報を有効化** をクリックしてください。

次のステップ

個別ユーザーを追加する方法を確認したら、次に複数のユーザーを一度に登録する方法を学んでください。

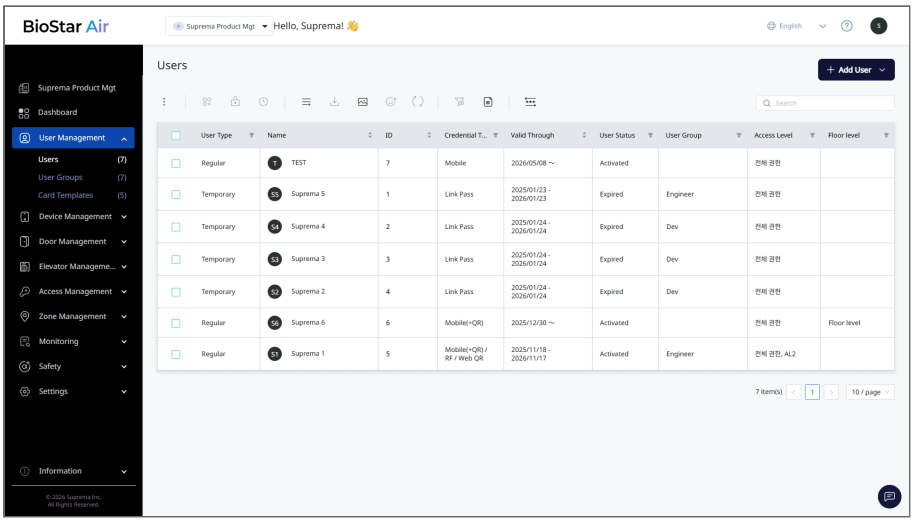
ユーザー管理
ユーザー一覧は、組織の出入管理を担当する管理者にとって必須のツールです。 ユーザーのグループ化による組織管理、リアルタイムの有効化／一時停止による入社や退職の社員への即時対応、さまざまなクレデンシャルの統合管理、有効期限の監視によるセキュリティ強化、フィルタリングやレポート作成による報告・監査対応まで、あらゆるユーザー管理業務を行えます。

ユーザー一覧の表示

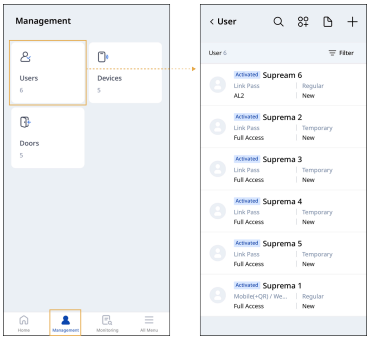
ユーザー一覧では、BioStar Air に登録されたすべてのユーザーを一目で確認できます。 各ユーザーの詳細を確認し、フィルターや並べ替え機能を活用して特定のユーザーを簡単に見つけることができます。 また、ユーザー一覧から直接ユーザーの編集、削除、グループ割り当てなどの操作を行うことができます。

Web

画面左のサイドバーで **ユーザー管理** → **ユーザー** をクリックします。



Mobile



BioStar Airアプリでユーザー管理機能を利用できます。

1. モバイル機器で **BioStar Air** アプリを起動してください。
2. 画面下部のナビゲーションバーで **管理** をタップします。
3. **ユーザー** をタップします。

ユーザーリストが表示されます。 新しいユーザーを追加したり、既存ユーザーの詳細情報を編集できます。

ユーザー情報

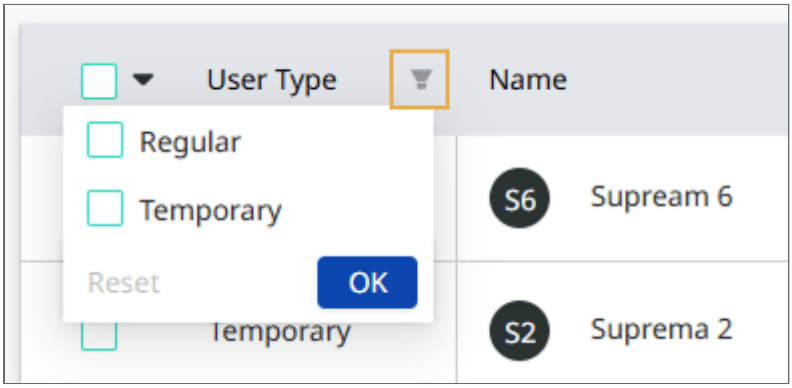
ユーザー一覧のテーブルで提供される情報は以下のとおりです。

- **ユーザータイプ**：ユーザーが一般ユーザーか一時ユーザーかを示します。 一般および一時ユーザーの詳細は ユーザーのカードとクレデンシャルの種類 を参照してください。
- **名前**：ユーザーの名前です。
- **ID**：ユーザーの固有 ID です。
- **認証情報の種類**：ユーザーに付与されたクレデンシャルを示します。 クレデンシャルの種類の詳細は ユーザーのカードとクレデンシャルの種類 を参照してください。
- **有効期間**：ユーザーに付与されたクレデンシャルの有効期限です。
- **ユーザーステータス**：該当ユーザーの有効化または無効化の状態を示します。
- **ユーザーグループ**：ユーザーが所属するグループです。 ユーザーグループの詳細は ユーザーグループを管理する を参照してください。
- **アクセスレベル**：ユーザーに割り当てた出入レベルです。 出入レベルの詳細は 出入レベルの管理性行する を参照してください。
- **床面高さ**：ユーザーが出入できるフロアに関する権限です。 フロアレベルの詳細は フロアレベルを管理する を参照してください。

フィルタリング

Web

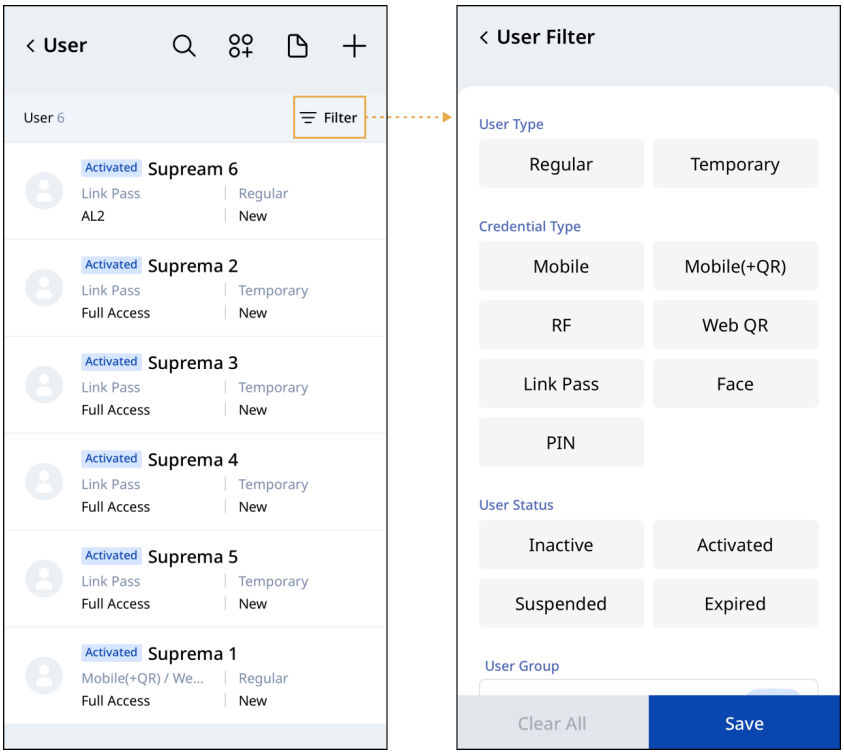
ユーザー一覧の上部ヘッダー領域でフィルター機能を利用できます。 ヘッダー領域の ボタンをクリックすると、条件を設定できます。



> **情報**
>
> 適用したフィルター条件を初期化するには、ユーザー一覧上部の ボタンをクリックしてください。

Mobile

モバイルアプリでは、ユーザー一覧を任意の基準でフィルタリングして表示できます。 ユーザー一覧の右上にある **フィルター** をタップします。 ユーザーは以下の基準でフィルタリングできます。

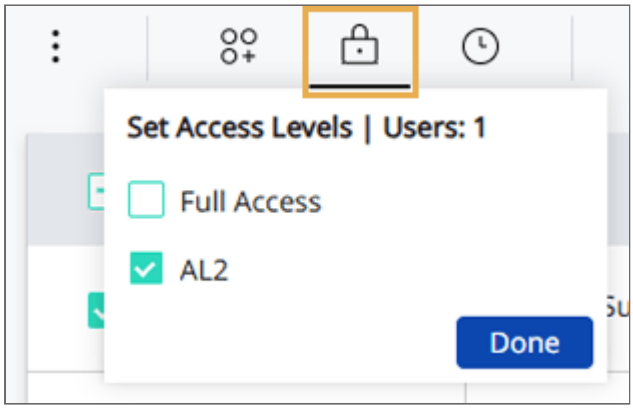


- **ユーザータイプ**：通常または一時ユーザーでフィルタリングします。
- **認証情報の種類**：クレデンシャルの種類でフィルタリングします。
- **ユーザーステータス**：有効状態でフィルタリングします。
- **ユーザーグループ**：ユーザーグループでフィルタリングします。

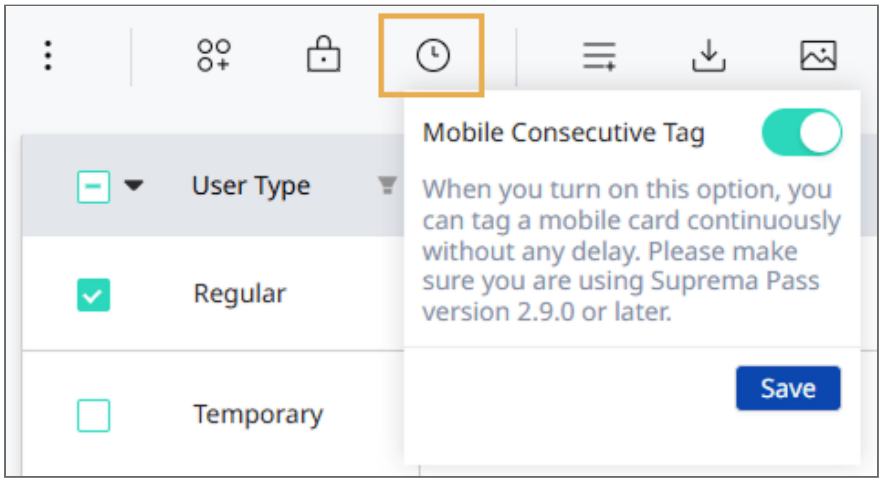
追加機能

ユーザー一覧上部で提供される機能は以下のとおりです。

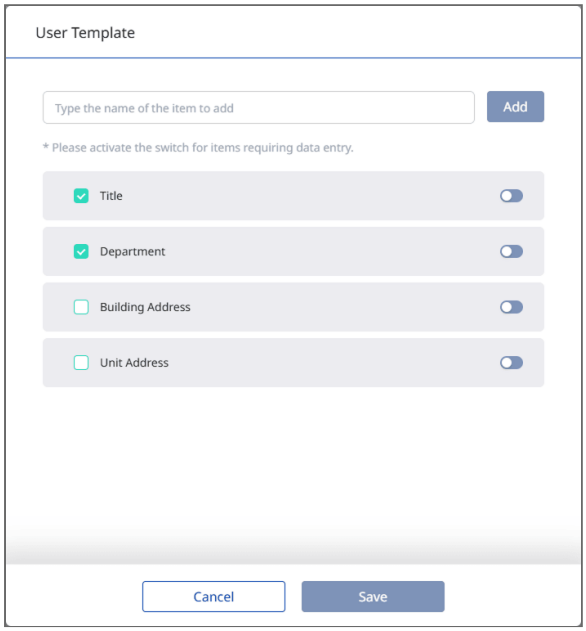
- ：選択したユーザーにグループを割り当てたり、除外・移動したりできます。 詳細は ユーザーグループの管理 を参照してください。
- ：選択したユーザーの出入レベルを変更できます。 アクセスレベル管理の詳細は 出入レベルの管理性行する を参照してください。



- ：選択したユーザーが待ち時間なしで連続してモバイルカードをタップできるように設定できます。 Suprema Pass アプリは 2.9.0 以上でサポートされています。



- ：選択したユーザーにユーザーテンプレートを適用できます。 既定のユーザー情報に加えて必要な情報を追加できます。



- ：選択したユーザー情報を PDF または CSV ファイルにエクスポートできます。
- ：ユーザー画像を一括アップロードできます。 アップロードする画像ファイルの名前はユーザーIDと一致している必要があります。

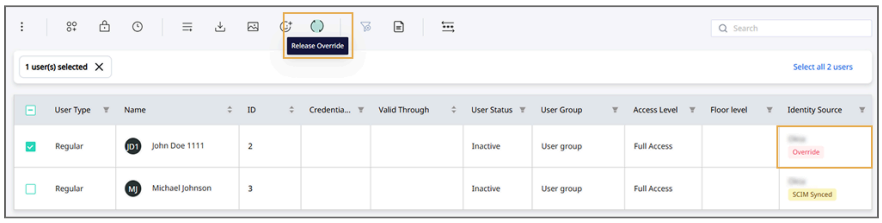
  例：601.jpg ファイルはユーザーID 601 に対応します。

> **ファイル形式の要件**
> - 対応形式: *.jpg, .jpeg, .png*
> - ファイルサイズ制限: 画像ごとに **1MB**

- : 選択したユーザーに顔登録リンクをメールまたはSMSで送信できます。 ユーザーがリンクをクリックしてウェブページで顔を登録すると、顔認証で出入できる権限が付与されます。

> メールまたは携帯電話番号が登録されていないユーザーにはリンクを送信できません。

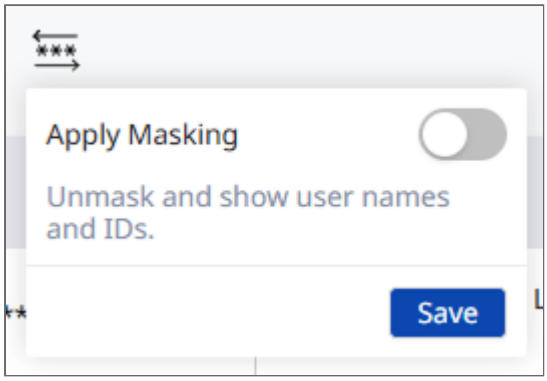
- : SCIMで同期されたユーザー情報をローカルで手動で変更すると、**オーバーライド** 状態になります。 ローカルの変更を取り消し、SCIM管理状態に戻してください。 詳しくは SSO & SCIM を設定する をご参照ください。



- : ユーザー一覧に適用されているフィルターをリセットします。 この機能はフィルターが適用されている状態で利用できます。 フィルタリングの適用方法の詳細は、フィルタリングを参照してください。

- : ユーザーのレポートを設定できます。 リポートの作成が完了すると、管理者のメールに送信されます。 レポート設定の詳細については、ユーザーリポートの作成を参照してください。

- : ユーザー一覧で個人情報保護のために氏名やIDなどをマスク（***）できます。 この機能は、個人情報保護が必要な環境で役立ちます。 トグルボタンで機能を有効にし、**保存**をクリックしてください。

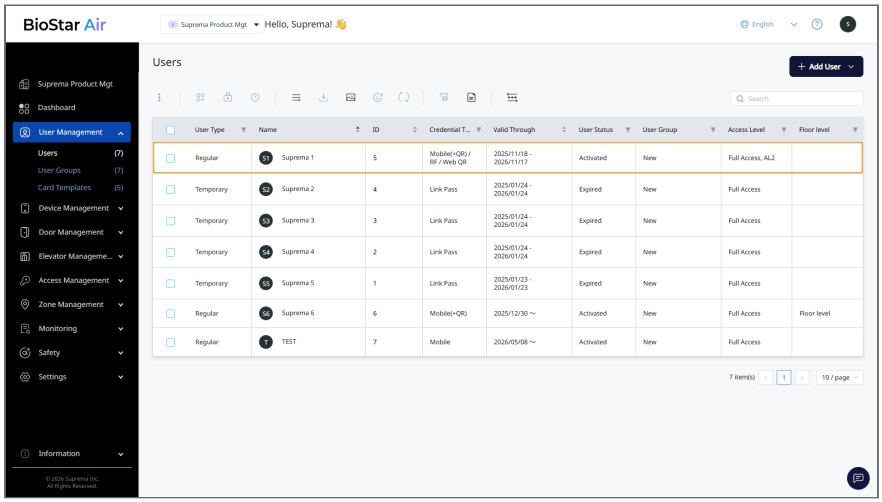


ユーザー情報の編集

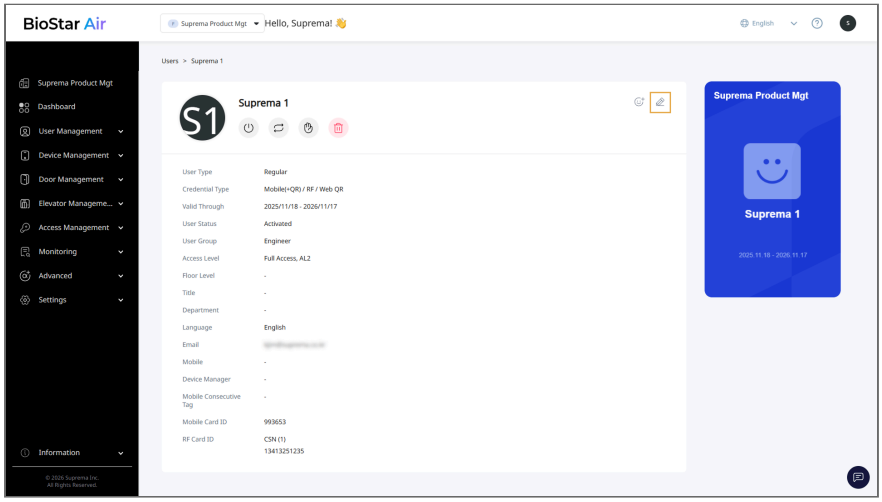
Web

ユーザーの詳細を編集するか、クレデンシャルを変更するには、次の手順に従ってください。

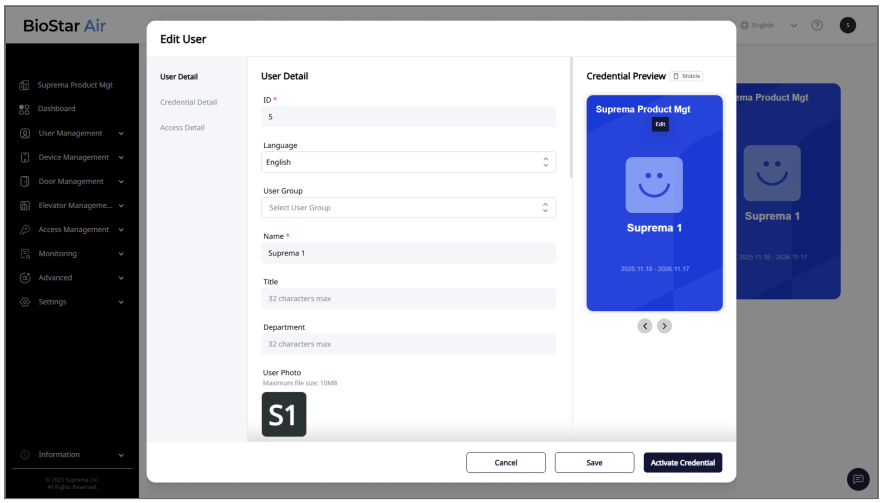
1. 画面左のサイドバーで **ユーザー管理** → **ユーザー** をクリックします。
2. 一覧で編集するユーザーをクリックします。



3. ユーザー詳細の右上にある ボタンをクリックします。

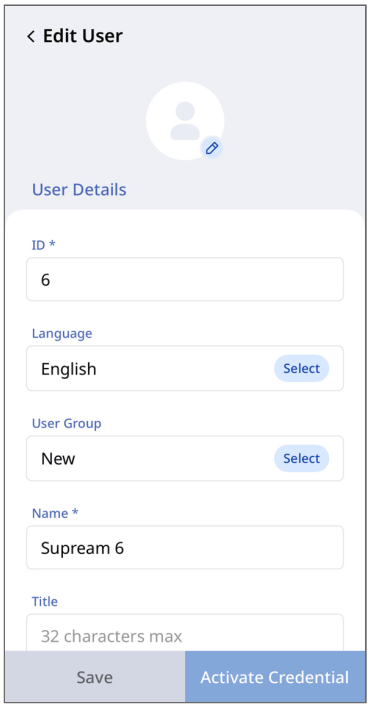


4. **ユーザーの編集** ウィンドウが表示されたら、必要な詳細を編集します。



5. 編集が完了したら、右下の **保存** ボタンをクリックします。

Mobile



モバイルアプリでユーザーの詳細情報を編集するには、次の手順に従ってください。

1. ユーザー一覧で編集するユーザーをタップします。
2. 右上の をタップします。
3. **ユーザーの編集** 画面で必要な情報を編集します。
4. 変更を保存するには **保存** をタップします。

   クレデンシャルを発行するには **認証情報を有効化** を使用します。

> **情報**
> ユーザー情報の詳細については、ユーザーの追加を参照してください。

ユーザーグループの管理

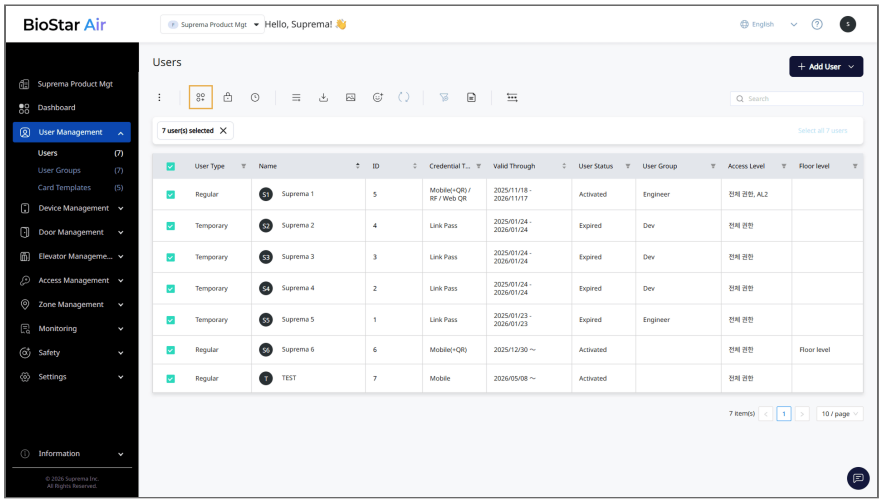
ユーザーをユーザーグループに割り当てる、移動する、またはグループから除外する方法をご案内します。 ユーザーグループの作成と管理の詳細については、ユーザーグループを管理するを参照してください。

Web

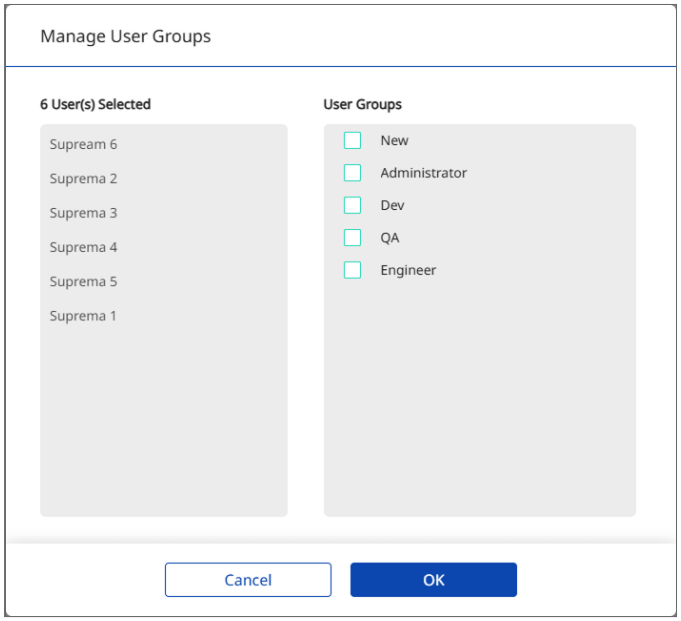
グループへのユーザー割り当て

ユーザーグループを作成した後、ユーザー一覧からユーザーを追加できます。

1. 画面左のサイドバーで **ユーザー管理** → **ユーザー** をクリックします。
2. ユーザー一覧で、先に作成したグループに割り当てるユーザーのチェックボックスをクリックします。
3. ユーザー一覧の左上にある をクリックしてください。

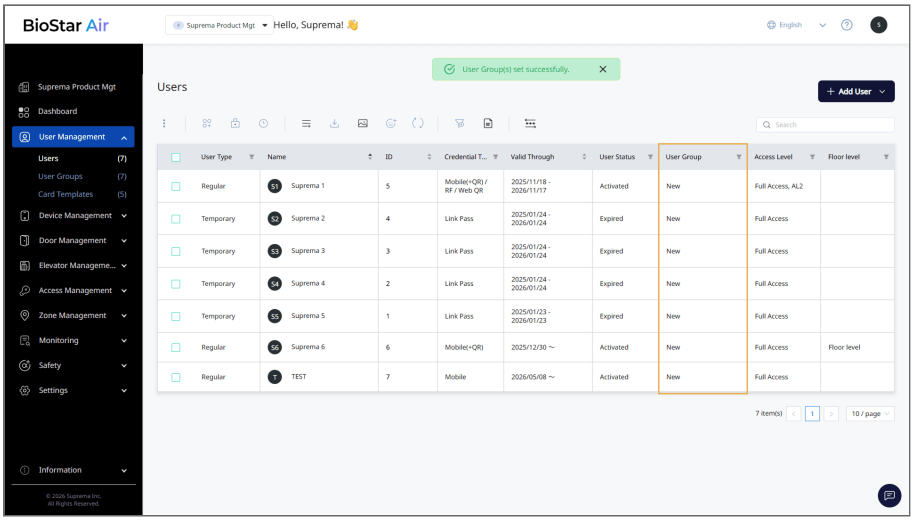


4. **ユーザーグループ管理** ウィンドウが表示されたら、ユーザーを割り当てる親グループまたはサブグループを選択します。



5. 選択を完了してグループ設定を保存するには、**OK**をクリックしてください。

ユーザー一覧の **ユーザーグループ** 列で、ユーザーが新しいグループに割り当てられていることを確認できます。



ユーザーグループ に戻ると、該当グループの **ユーザーの合計** が更新されていることを確認できます。

グループの解除または移動

ユーザーをグループから除外するか、別のグループに移動できます。

1. 画面左のサイドバーで **ユーザー管理** → **ユーザー** をクリックします。
2. ユーザー一覧で、グループから解除または移動するユーザーのチェックボックスをクリックします。

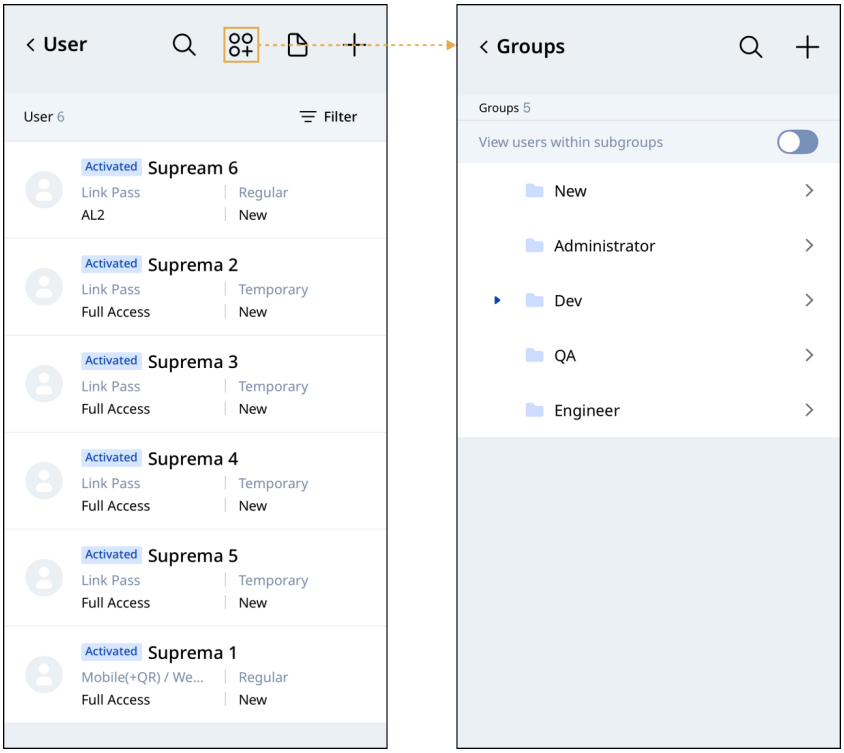
> グループを移動する場合は、同じグループのユーザーを選択してから操作を進めます。

3. ユーザー一覧の左上にある をクリックします。
4. **ユーザーグループ管理** ウィンドウが表示されたら、次のいずれかを行います。
   - グループを解除する場合は、選択したグループのチェックボックスをオフにします。
   - グループを移動する場合は、選択したグループのチェックボックスをオンにし、移動先のグループを選択します。
5. グループ設定を保存するには、**OK**をクリックしてください。

ユーザー一覧の **ユーザーグループ** 列でユーザーのグループ変更を確認できます。

Mobile

モバイルアプリでユーザーグループを管理できます。 ユーザー一覧の上部にある をタップします。 ユーザーグループの一覧を確認できます。



- グループに所属するユーザーを表示するには、対象グループの右側にある › をタップします。
- 新しいグループを追加するには、右上の ＋ をタップしてください。
- グループ名を編集するには、対象のグループを長押しし、下部の をタップしてください。

- グループを削除するには、対象のグループを長押ししてから下部の をタップしてください。 1つ以上のグループを選択して削除できます。

> **情報**
> ユーザーグループ管理の詳細については、ユーザーグループを管理するを参照してください。

ユーザー状態管理

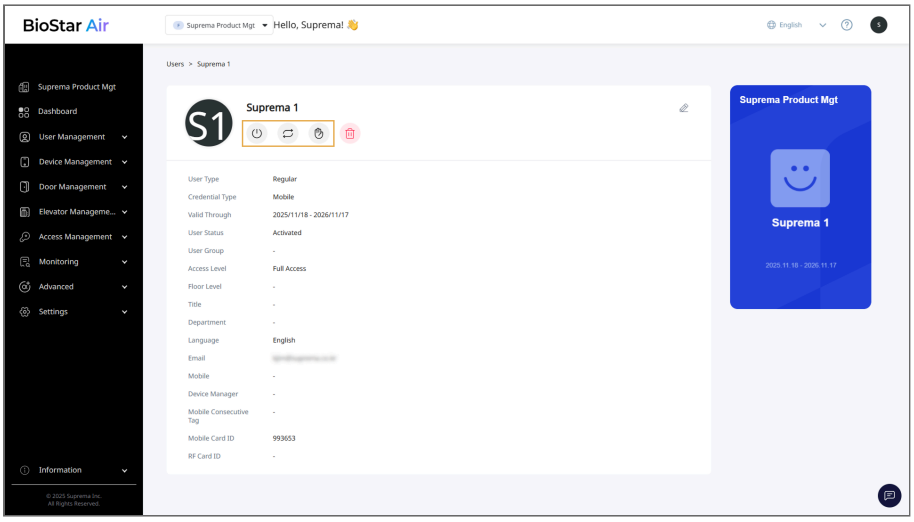
ユーザーの出入権限を有効化または一時停止できます。 また、クレデンシャルを再発行することもできます。

> **情報**
> 管理者がBioStar Airでユーザーのクレデンシャルを再発行すると、以前に発行されたモバイルクレデンシャル、QRコード、リンクパス（LinkPass）はすべて取り消され、新しいクレデンシャルに置き換えられます。 ユーザーは、サイト設定に応じてメールまたはSMSで新しいクレデンシャルリンクを受け取ります。 ユーザーはそのリンクから、Suprema Passアプリに新しいモバイルクレデンシャルをダウンロードするか、新しいQRコードまたはリンクパスを使用する必要があります。 取り消されたモバイルクレデンシャル、QRコード、またはリンクパスで入退室を試みると、失敗します。

個別ユーザー

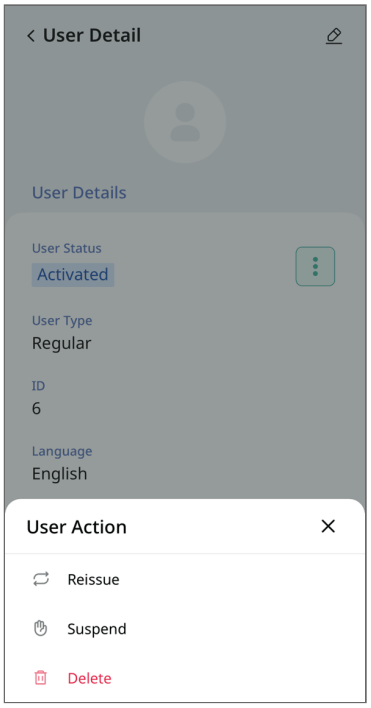
Web

1. 画面左のサイドバーで **ユーザー管理** → **ユーザー** をクリックします。
2. ユーザー一覧で状態を変更するユーザーをクリックします。
3. ユーザー詳細の上部で希望する機能を選択します。



- ：ユーザーの出入権限を有効にします。 新規ユーザーの初期有効化または一時停止されたユーザーの再有効化時に使用します。
- ：クレデンシャルを再発行します。 この機能は、ユーザーのクレデンシャルが期限切れになった場合やクレデンシャルが使用できず新しく発行する場合に使用できます。
- ：ユーザーの出入をブロックします。 この機能はユーザーが有効化されている状態で使用できます。

Mobile



モバイルアプリのユーザー一覧で、ユーザーをタップします。 **ユーザーの詳細** 画面で ⋮ をタップします。 **ユーザーアクション** メニューが表示されます。

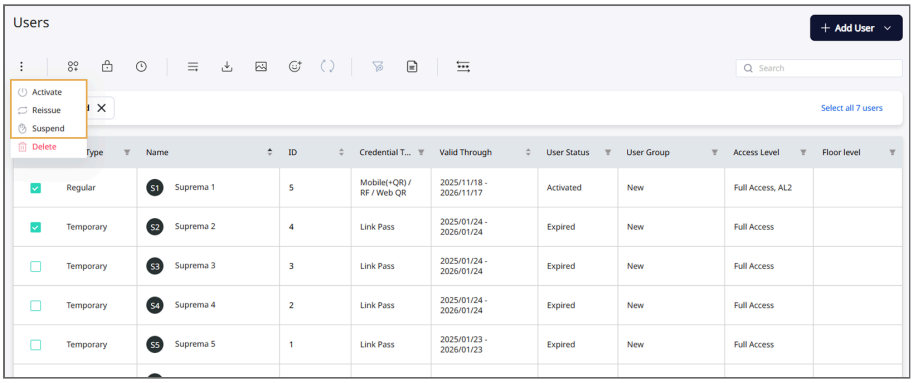
- **活性化** / **再活性化**: ユーザーのアクセス権を有効にします。 新規ユーザーの初期有効化または一時停止されたユーザーの再有効化時に使用します。
- **再発行**：ユーザーのクレデンシャルを再発行します。
- **一時停止**：ユーザーを一時的に無効にします。 一時停止されたユーザーは入退室できません。
- **削除**：ユーザーをシステムから削除します。

> **情報**
> **再活性化** オプションは一時停止されたユーザーにのみ表示されます。

一括操作

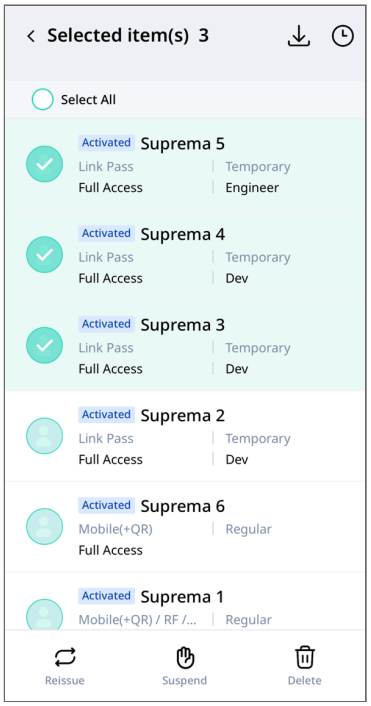
Web

1. 画面左のサイドバーで **ユーザー管理** → **ユーザー** をクリックします。
2. ユーザー一覧で状態を変更するユーザーのチェックボックスをクリックします。 1 人以上のユーザーを選択できます。
3. 画面左上の ⋮ ボタンをクリックし、ポップアップメニューで希望する操作を選択します。



- **活性化** / **再活性化**: ユーザーのアクセス権を有効にします。 新規ユーザーの初期有効化または一時停止されたユーザーの再有効化時に使用します。
- **再発行**：クレデンシャルを再発行します。 この機能は、ユーザーのクレデンシャルが期限切れになった場合やクレデンシャルが使用できず新しく発行する場合に使用できます。
- **一時停止**：ユーザーの出入をブロックします。 この機能はユーザーが有効化されている状態で使用できます。

Mobile



モバイルアプリのユーザー一覧で、状態を変更するユーザーを長押しします。 追加で状態を変更するユーザーを選択します。 画面下部の**ユーザーアクション**メニューで、希望する機能をタップします。

- **活性化** / **再活性化**: ユーザーのアクセス権を有効にします。 新規ユーザーの初期有効化または一時停止されたユーザーの再有効化時に使用します。
- **再発行**：ユーザーのクレデンシャルを再発行します。
- **一時停止**：ユーザーを一時的に無効にします。 一時停止されたユーザーは入退室できません。
- **削除**：ユーザーをシステムから削除します。

> **情報**
> **再活性化** オプションは一時停止されたユーザーにのみ表示されます。

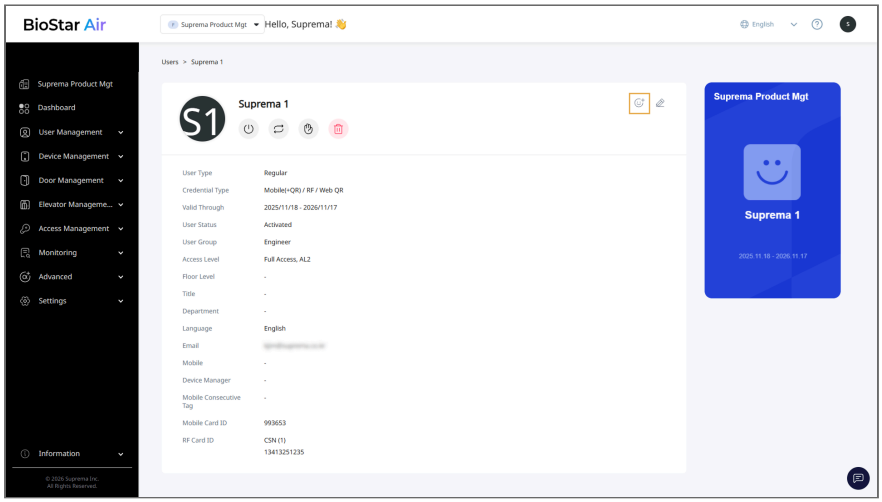
顔登録リンクを送信

登録済みユーザーに顔登録リンクをメールまたはSMSで送信して、顔登録を案内できます。 ユーザーがリンクをクリックしてウェブページで顔を登録すると、顔認証でアクセスできます。

> **情報**
> メールまたは携帯電話番号が登録されていないユーザーにはリンクを送信できません。

個別ユーザー

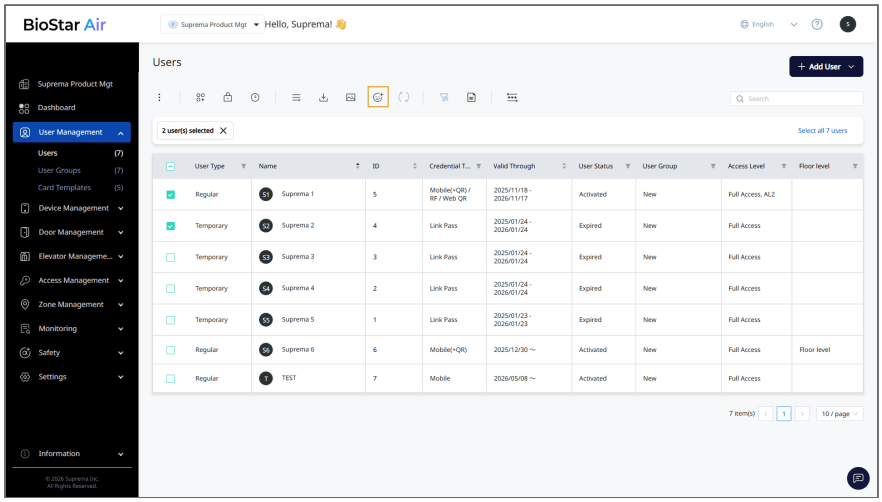
1. 画面左のサイドバーで **ユーザー管理** → **ユーザー** をクリックします。
2. ユーザー一覧でリンクを送信するユーザーをクリックします。
3. ユーザー詳細の右上にある ボタンをクリックします。



4. ポップアップメッセージが表示されたら、**はい** ボタンをクリックします。

一括操作

1. 画面左のサイドバーで **ユーザー管理** → **ユーザー** をクリックします。
2. ユーザー一覧でリンクを送信するユーザーのチェックボックスをクリックします。 1 人以上のユーザーを選択できます。
3. 画面左上の ボタンをクリックします。



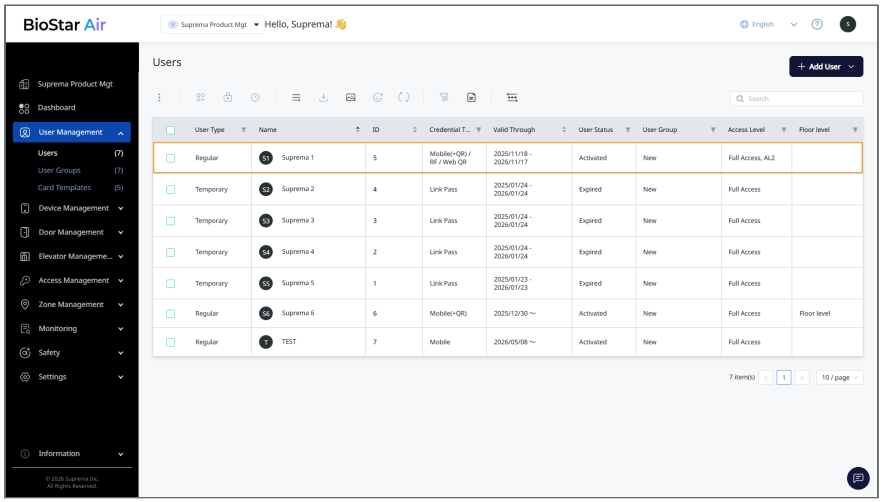
4. ポップアップメッセージが表示されたら、**はい** ボタンをクリックします。

ユーザー削除

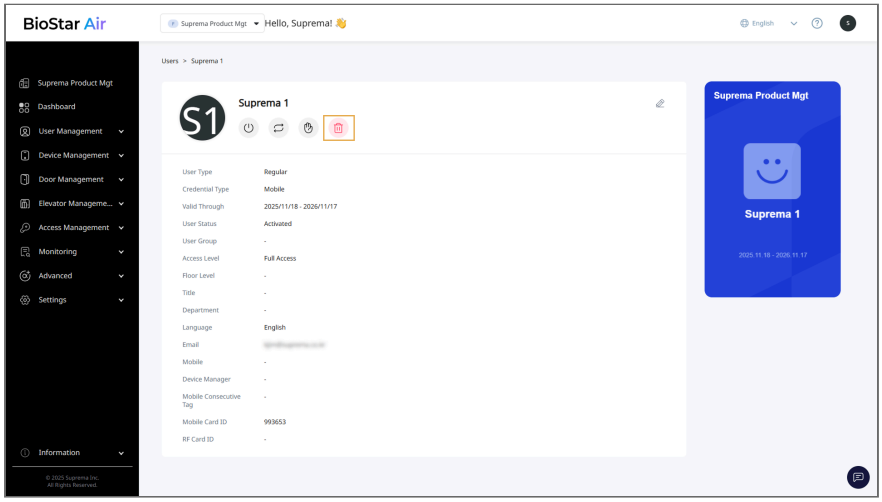
> **注意**
> 削除されたユーザーは復元できません。 削除する前に必ず確認してください。

個別ユーザー

1. 画面左のサイドバーで **ユーザー管理** → **ユーザー** をクリックします。
2. 一覧で削除するユーザーをクリックします。



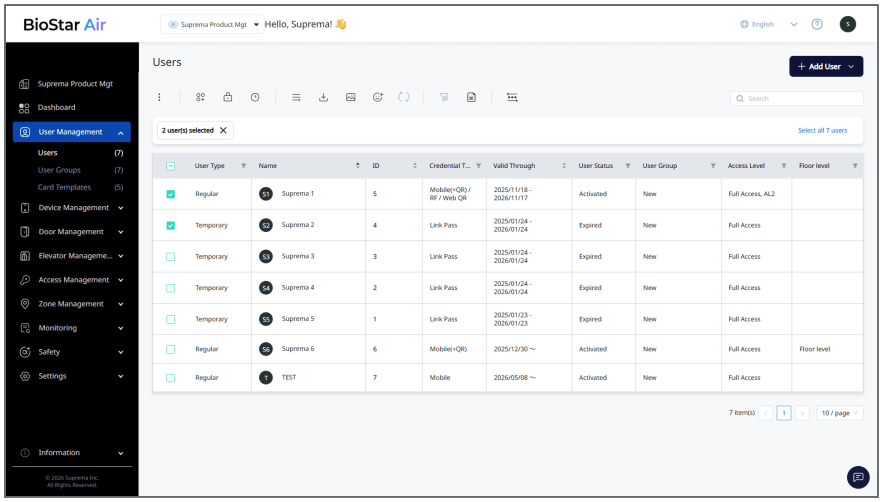
3. ユーザー詳細で 🗑 ボタンをクリックします。



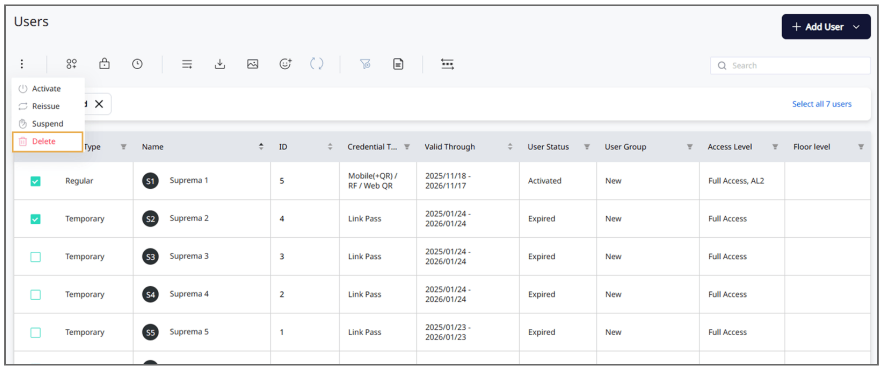
4. 警告メッセージが表示されたら、**はい** ボタンをクリックします。

一括削除

1. 画面左のサイドバーで **ユーザー管理** → **ユーザー** をクリックします。
2. 一覧で削除するユーザーのチェックボックスをクリックします。 1 人以上のユーザーを選択できます。



3. 画面左上の ⋮ → **削除** をクリックします。

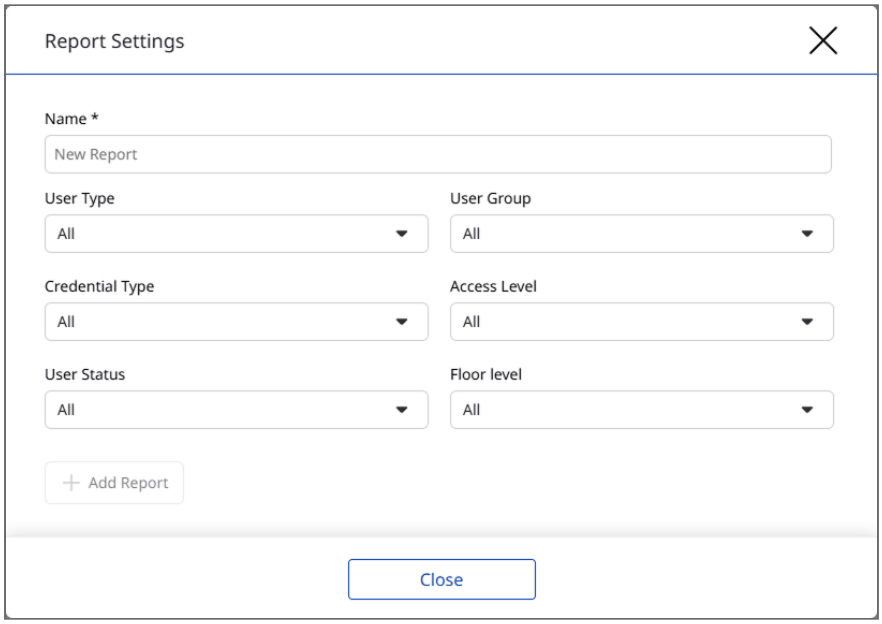


4. 警告メッセージが表示されたら、**はい** ボタンをクリックします。

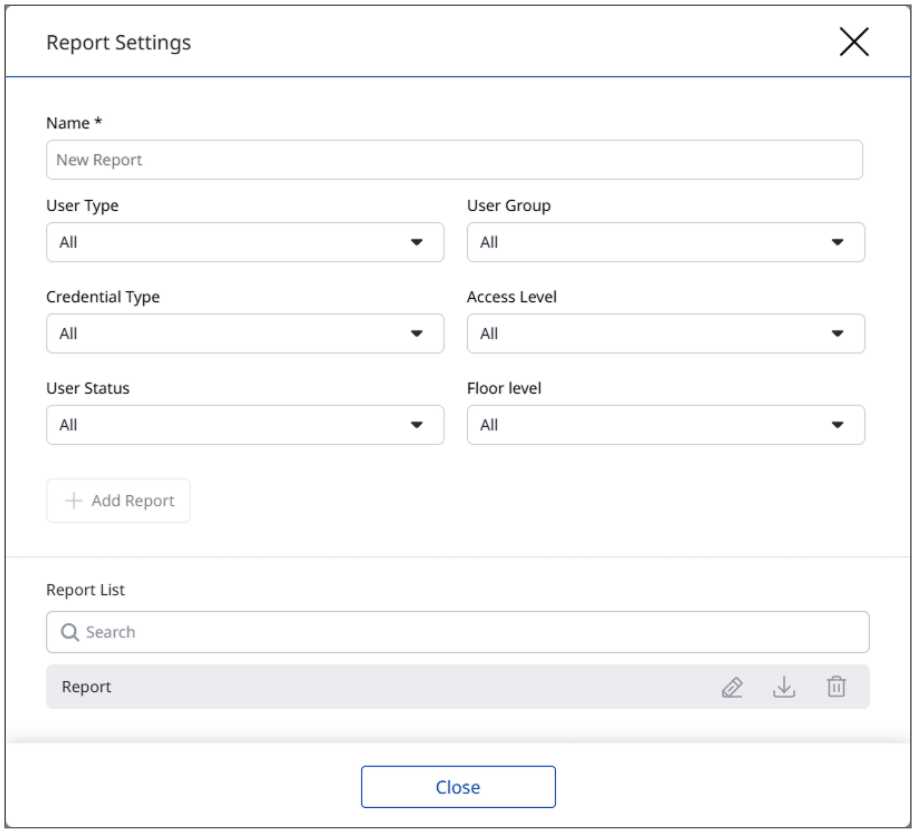
ユーザーリポートの作成

ユーザーリポートを生成して管理者のメールに送信できます。

1. ユーザー一覧上部の ボタンをクリックします。
2. **レポート設定** ウィンドウが表示されたら、レポート名を入力します。



3. 各フィルターオプションでレポートに含める項目を選択します。
4. 作成したレポートを保存するには、**レポートの追加** をクリックします。
5. **レポートリスト** が作成され、管理者のメールにダウンロードリンクが送信されます。

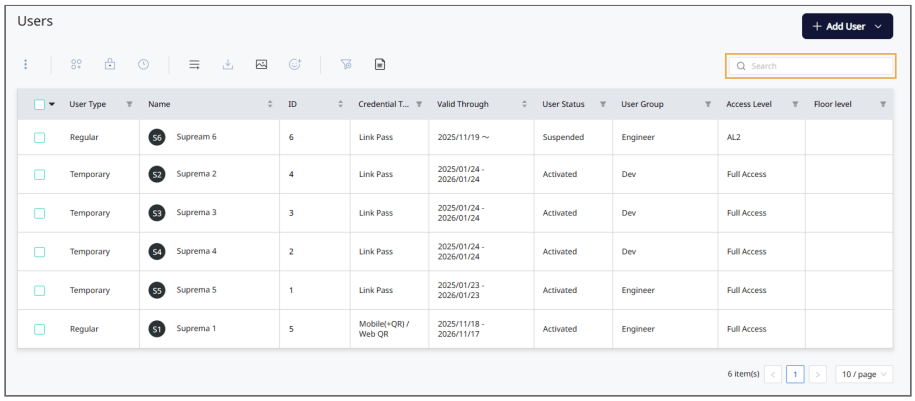


情報

レポートリスト で作成されたリポートを検索、編集、ダウンロード、削除できます。

ユーザー検索

ユーザー一覧右上の検索入力フィールドで特定のユーザーを素早く見つけることができます。 ユーザー名、ID、電話番号で検索できます。



ユーザーを一括で追加する

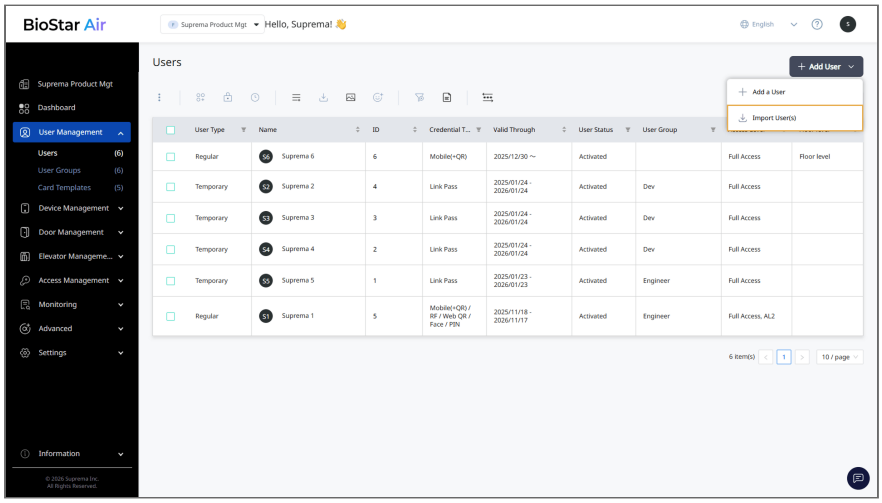
ユーザーをまとめて追加する必要がある場合は、BioStar Airの一括ユーザー追加機能をご利用ください。 CSVファイルをアップロードすることで、数十〜数百人分の従業員情報を数分でシステムに登録できます。 ユーザー情報を入力すると同時に、プロフィール画像を一括でアップロードすることもできます。 本ドキュメントでは、CSVテンプレートのダウンロード、ファイルの準備、アップロード、プロフィール画像の管理、およびアップロード後のユーザー情報の検証方法を手順に沿って案内します。

> **ヒント**
> 複数のユーザーを一括追加する全工程を段階的に説明する次のビデオを参照してください。

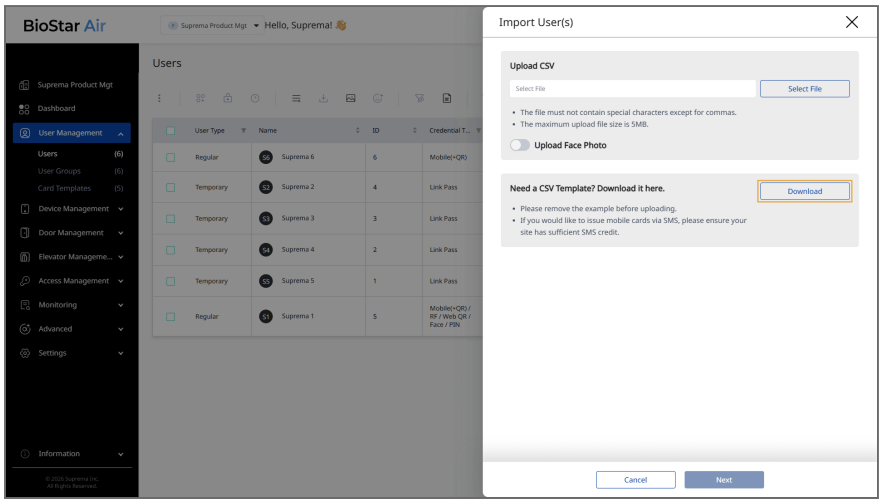
CSVテンプレートをダウンロード

次の手順に従ってCSVテンプレートファイルをダウンロードしてください。

1. 画面左のサイドバーで **ユーザー管理** → **ユーザー** をクリックします。
2. 画面右上の **ユーザー追加** → **ユーザーをインポートする** をクリックします。



3. **ユーザーをインポートする** パネルが表示されたら、**ダウンロード** ボタンをクリックします。



4. CSVテンプレートファイル(*biostar-import-user-csv-example.csv*)をローカルに保存します。

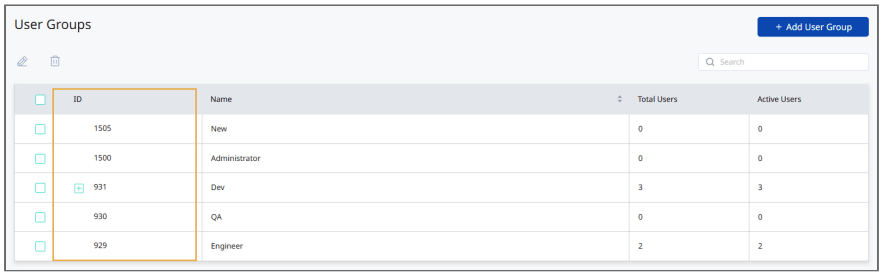
CSVファイルの準備

CSVテンプレートをダウンロードし、各ユーザーの必須情報を入力してください。

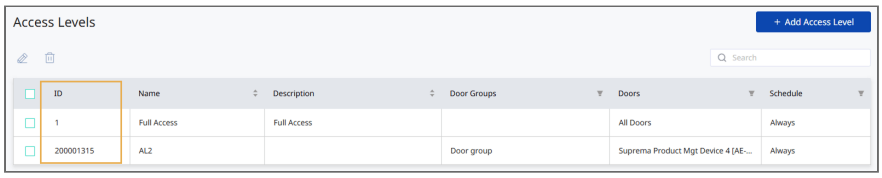
主要入力フィールド

入力する主なフィールドは以下の通りです。

- **ユーザー グループ ID**：**ユーザー管理** → **ユーザーグループ**でグループIDを確認できます。



- **アクセス レベル ID**：**アクセス管理** → **アクセスレベル**でアクセスレベルIDを確認できます。 **フルアクセス**は常に1に設定されます。 複数のアクセスレベルを指定する際はカンマ（`,`）を区切りとして使用できます。



- **メール**：メールで招待状を送信する場合は必須です。
- **モバイル**：モバイルSMSで招待状を送信する場合は必須です。

> **注意**
> **メール**と**モバイル**は重複してはいけません。 重複する値を入力してCSVファイルをアップロードするとエラーが発生する可能性があります。

カスタムWiegand形式のサポート

ファシリティコード、セグメント、パリティビットなどの情報を含むあらゆるWiegand形式を自由に構成できます。

- HID Corporate 1000およびiClass SE、SEOS形式をサポートします。
- CSVテンプレート
  - 各定義された形式（カスタムまたはデフォルト）はCSVファイル内で別々の列として表示されます。

    > ***26 bit SIA Standard-H10301***、***HID 37 bit-H10302***、***HID 37 bit-H10304***、***HID Corporate 1000***、***HID Corporate 1000 48bit***

  - 複数の項目を単一フィールドに入力する場合はスラッシュ（`/`）で区切ってください。
  - カード名は小さい引用符（`'`）で囲むことができます。 ダブルクォート（`"`）を使用するとエラーが発生する可能性があります。

    > ✓ *'CardName'* | ✗ *"CardName"*

> **例**
> - ファシリティコードがある場合：*1234567-100-'Main Office Card'*（`CardID` - `FacilityCode` - `'CardName'`）
> - 複数のセグメントがある場合：*12-3456-78-'Lab Entry Card'*

複数カードのサポート

- ユーザーごとに最大8つのCSNまたはWiegandカード形式を割り当てることができます。

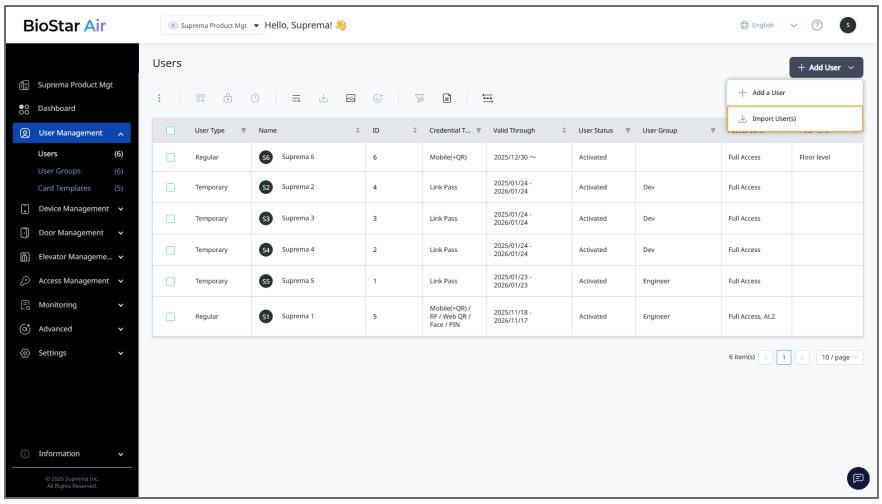
- **CSVテンプレート**
  - 単一カードの場合はCSNカード番号を入力します。
  - 複数のカードを登録する場合はCSNカード番号をスラッシュ（`/`）で区切ってください。

> **カード名の指定形式:** `CSN - 'Card Name'`
>
> 例：*1234567-'Main Entry' / 7654321-'Back Door'*

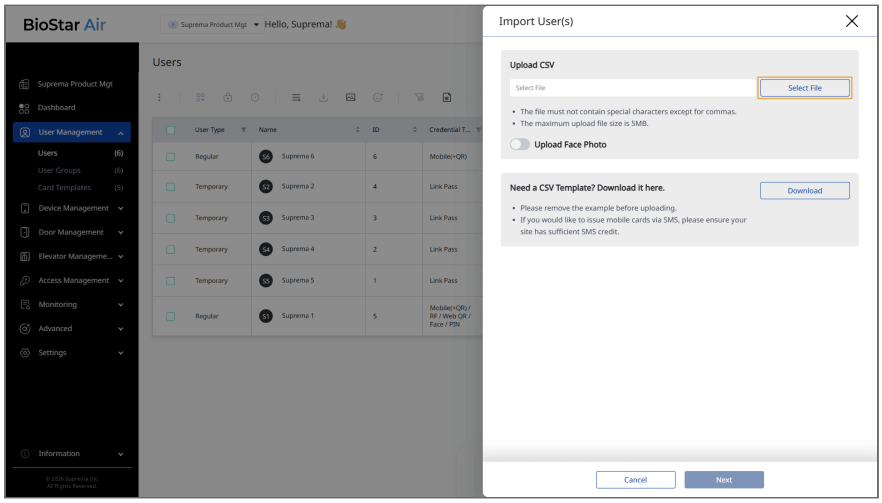
CSVファイルのアップロード

CSVファイルの準備が完了したらアップロードしてください。

1. 画面左のサイドバーで **ユーザー管理** → **ユーザー** をクリックします。
2. 画面右上の **ユーザー追加** → **ユーザーをインポートする** をクリックします。



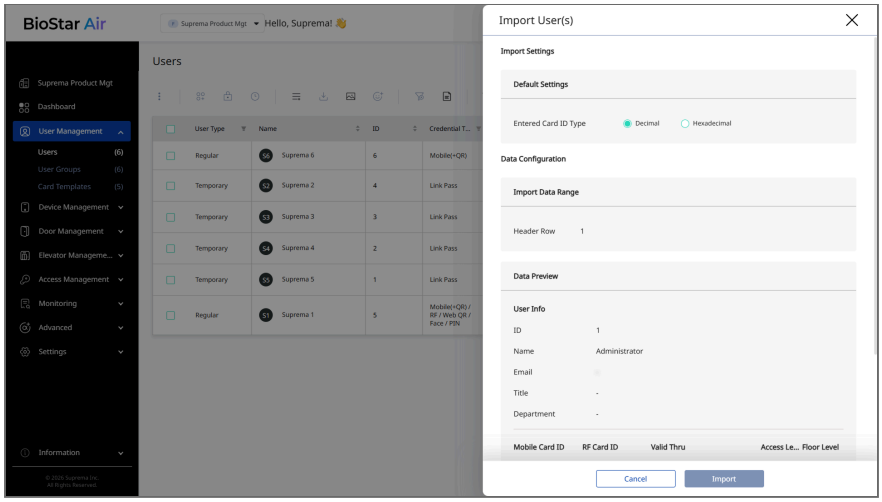
3. **ユーザーをインポートする**パネルが表示されたら、**ファイルを選択**ボタンをクリックします。



4. 事前に準備したCSVファイルを選択してください。

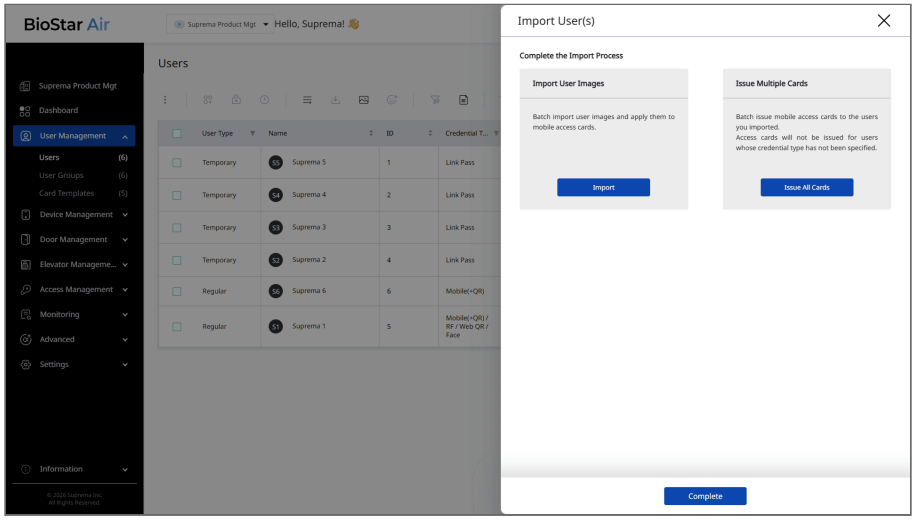
> ユーザーのプロファイル画像が用意されている場合は、**顔写真をアップロード**オプションを有効にします。 詳細については**ユーザープロファイル画像のアップロード**を参照してください。

5. 画面右下の **次へ** ボタンをクリックしてください。
6. **データプレビュー**セクションで最初の列のデータの正確性を確認してください。



7. データに問題がなければ、右下の **インポート** ボタンをクリックしてください。

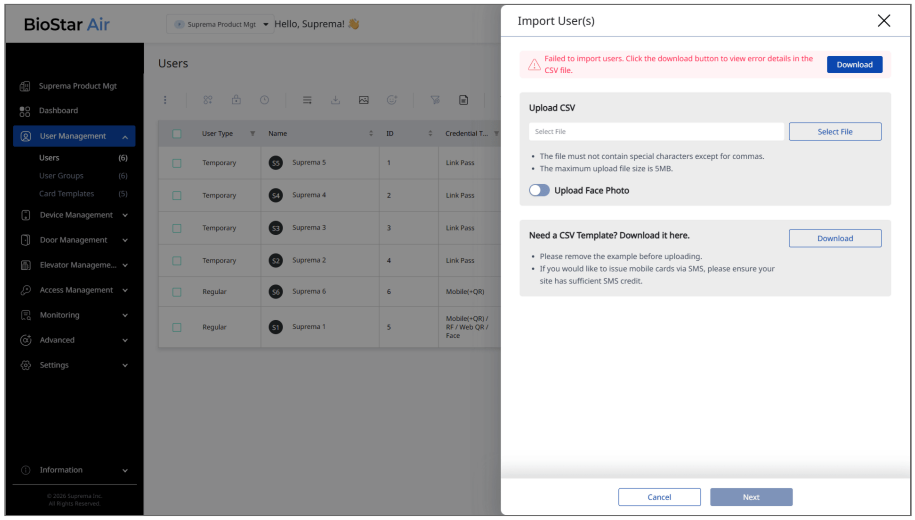
アップロードが完了すると、次の画面でユーザーの画像を読み込むか、モバイルカードを一括発行できます。 希望する操作を選択してください。



> **情報**
>
> - CSVファイル名にはカンマ（,）を除く特殊文字は使用できません。
> - アップロード可能なCSVファイルの最大サイズは5MBです。
> - **ユーザーをインポートする**パネルの**CSVファイルをアップロード**フィールドにCSVファイルをドラッグアンドドロップしてアップロードすることもできます。

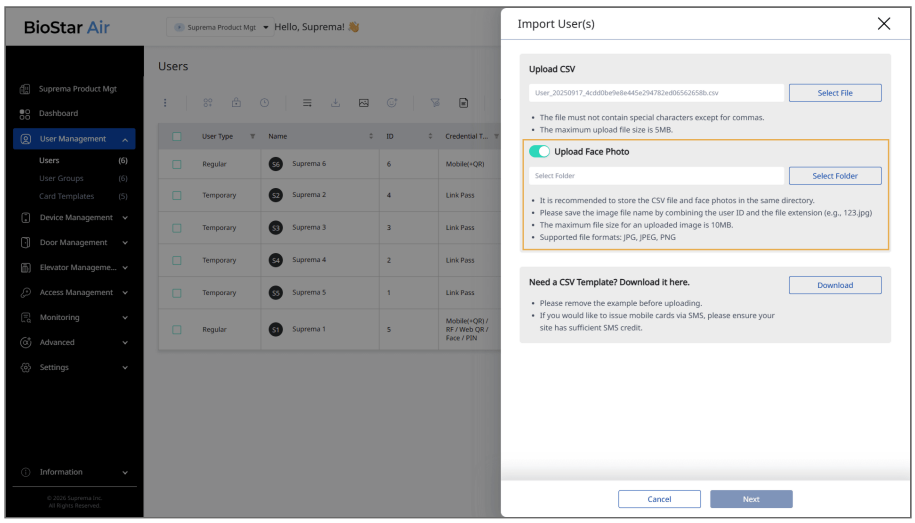
CSVファイルの検証

CSVアップロードプロセスが改善され、**行ごとのエラーのフィードバック**を提供するため、問題の解決が容易になりました。 アップロード中にエラーが発生した場合、エラー内容を確認できる詳細レポートを提供します。 レポートをダウンロードするには、**ダウンロード**ボタンをクリックしてください。



ユーザープロファイル画像のアップロード

プロファイル画像はCSVファイルと一緒に自動でアップロードするか、後で手動で一括アップロードできます。



1. CSVファイルの**ユーザー・キー**列と一致するプロファイル画像ファイルを用意してください。

   例えば、*601.jpg*ファイルはユーザーID**601**に対応します。

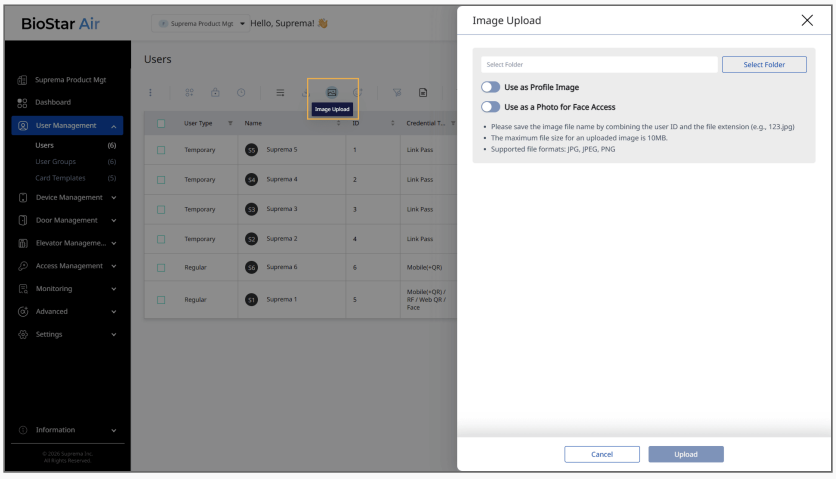
2. **ユーザーをインポートする**パネルでCSVファイルをアップロードした後、**顔写真をアップロード**オプションを有効にしてください。

3. **フォルダを選択**ボタンをクリックしてから、プロファイル画像が保存されているフォルダを選択してください。

ファイル形式の要件
- 対応形式: *.jpg, .jpeg, .png*
- ファイルサイズ制限: 画像ごとに **1MB**

ヒント

プロファイル画像がCSVファイルアップロード時に用意されていない場合は、ユーザーリストの**画像をアップロード**( )機能を使って後で追加できます。



一括アップロードの完了

すべてのユーザーデータと画像をアップロードすると、システムが項目を処理し、新しいユーザーが割り当てられたクレデンシャルとともにユーザーリストに表示されます。

トラブルシューティング

CSVアップロードに関して問題が発生した場合は、一般的な問題の解決に役立つ一括ユーザー追加の問題を確認してください。 このドキュメントには、データの検証と重複の除去に役立つExcelの式も含まれています。

ユーザーグループを管理する

ユーザーグループを使って、組織の部署、役割、拠点などでユーザーを分類・管理してください。 BioStar Airのユーザーグループは階層化されていないため、ユーザーは複数のグループに同時に所属できます。部門グループや役割グループ、拠点グループなどを組み合わせて運用できます。 グループを活用すると、入退室レベルの一括管理に加え、イベントログのフィルタリング、レポート作成、集合エリアへのデバイス割り当てなども効率的に行えます。

ヒント

ユーザーグループ管理のビデオガイドを視聴するには、以下のビデオを参照します。

開始する前に

ユーザーグループの構成

ユーザーグループは階層的に構成されていません。

- サブグループのユーザーは**自動的に**上位グループに表示されません。
- 上位グループの総ユーザー数には、サブグループのメンバーは手動で追加しない限り含まれません。
- サブグループを選択すると、該当サブグループに割り当てられたユーザーのみが表示されます。

複数のユーザーグループの構成

BioStar Airのユーザーは**複数のグループ**に所属できます。

BioStar 2では、ユーザーグループは通常単一の部門に紐づいていました。 BioStar Airではこれを分離し、より動的な方法で利用できます。

- グループごとにユーザー一覧をフィルターして出入レベルを素早く管理できます。

  > *例：人事部*

- 複数の部門をまたがる状況に合わせたグループを作成できます。

  > *例：男性更衣室*

- ユーザーグループは**イベントログフィルター**および**レポート作成**に使用されます。
- ユーザーグループを**点呼招集場所**用のデバイスまたはデバイスグループに割り当てて、特定の安全プロトコルを適用できます。

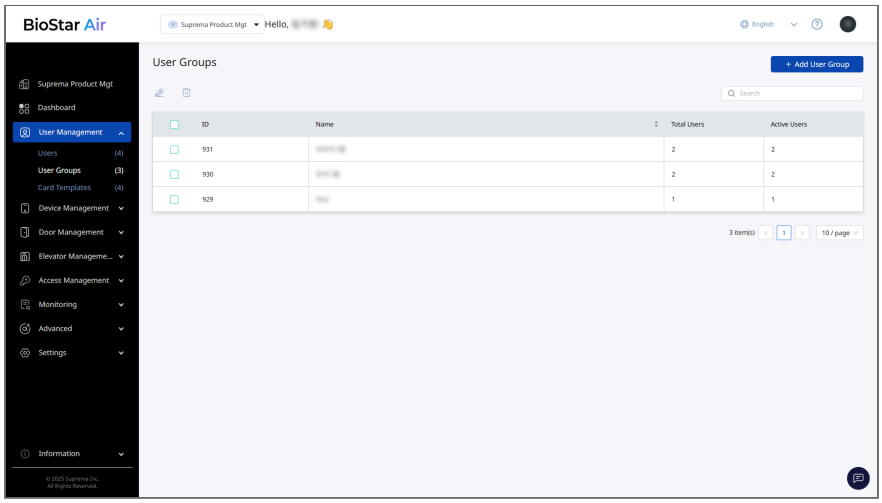
この柔軟性により、重複するユーザー役割やアクセスシナリオをより簡単に管理できます。

グループの作成

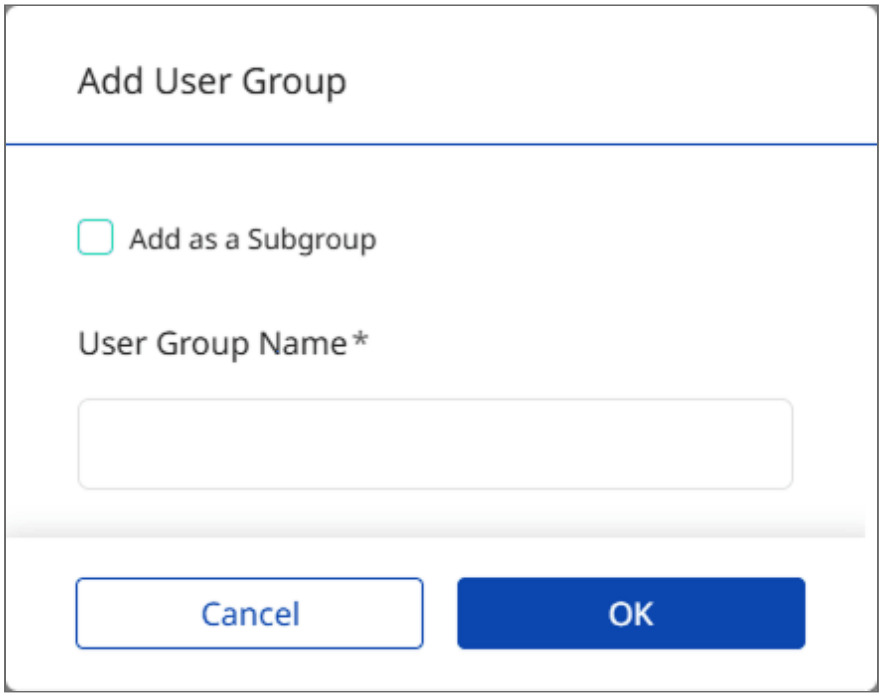
ユーザーグループの作成

新しいユーザーグループを作成します。

1. 画面左側のサイドバーで **ユーザー管理** → **ユーザーグループ** をクリックします。



2. 画面右上の **ユーザーグループの追加** をクリックします。
3. **ユーザーグループの追加** ウィンドウが表示されたら、ユーザーグループ名を入力します。



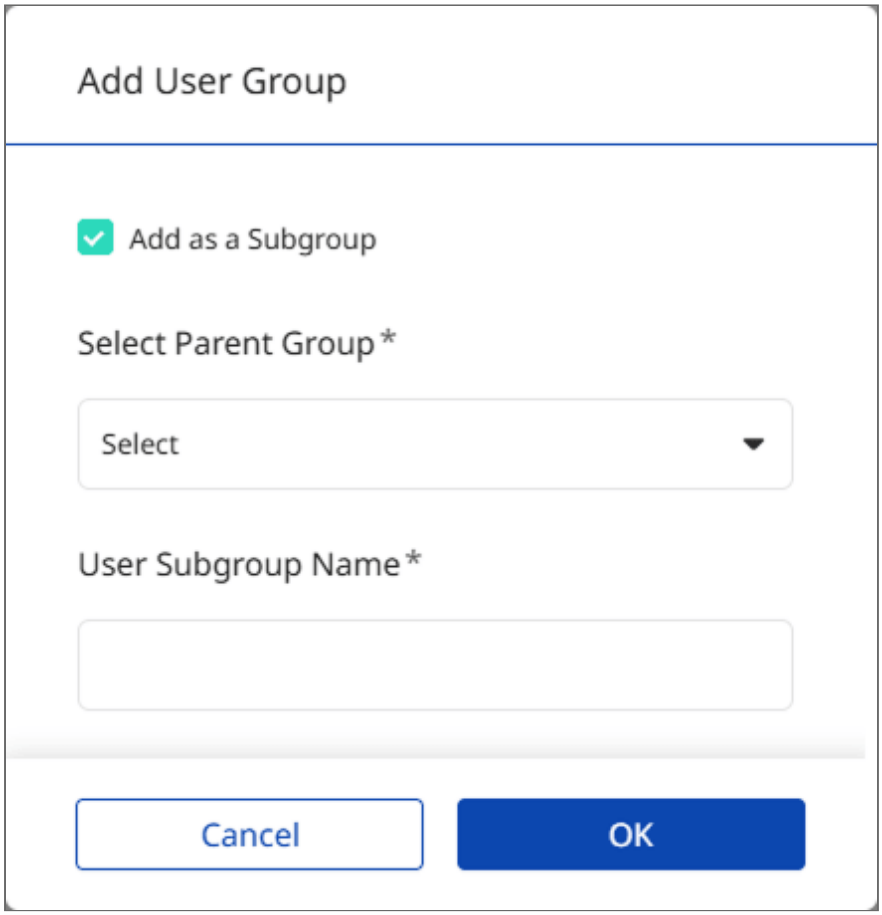
4. グループを作成するには、**OK** ボタンをクリックしてください。

> **情報**
>
> - グループを削除しても、当該グループに所属するユーザーは削除されません。 ユーザーはグループから解除されるだけです。
> - ユーザーをグループに割り当てる方法の詳細は、ユーザー管理 を参照してください。

サブグループの作成

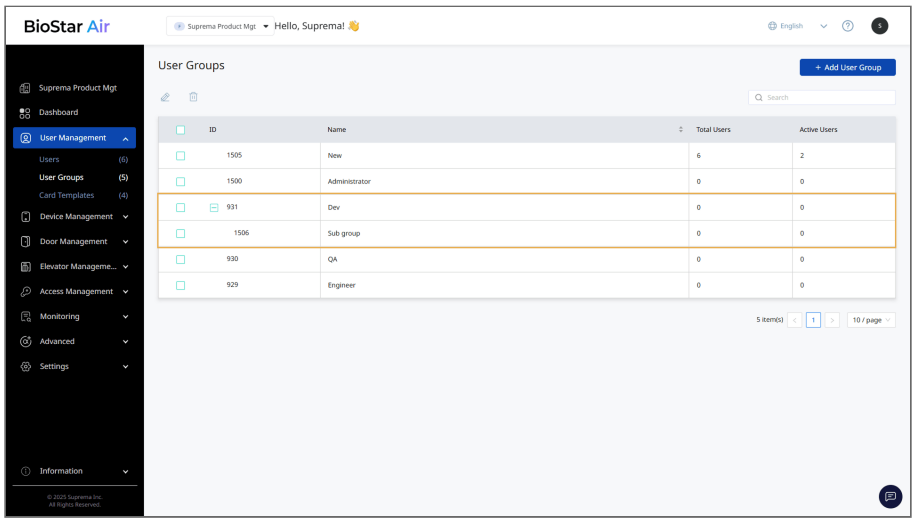
サブグループを使ってユーザーグループをより細かく分類できます。 ただし、サブグループは**階層的ではありません**。 つまり、サブグループのユーザーは親グループに自動的に含まれません。

1. 画面左側のサイドバーで **ユーザー管理** → **ユーザーグループ** をクリックします。
2. 画面右上の **ユーザーグループの追加** をクリックします。
3. **ユーザーグループの追加** ウィンドウが表示されたら、**サブグループとして追加** オプションをクリックします。



4. **マスターグループを選択** で親グループを選択します。
5. **サブグループ名** にグループ名を入力します。
6. サブグループを作成するには、**OK** ボタンをクリックしてください。

作成されたサブグループはユーザーグループ一覧で親グループの下にインデント表示されます。

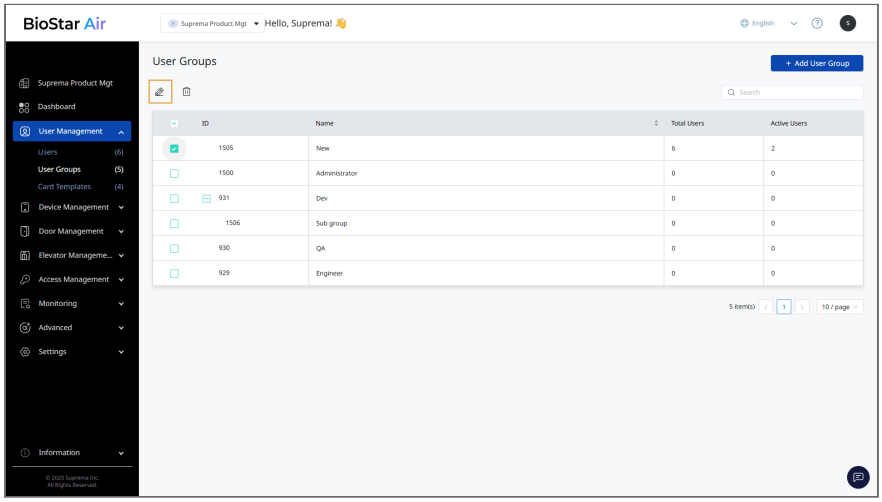


グループ名の編集

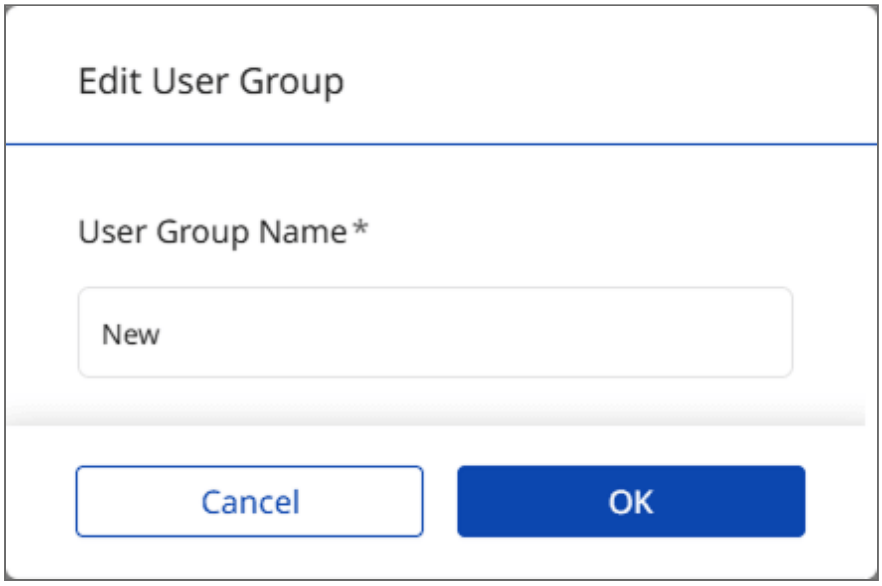
既に作成されたユーザーグループの名前を編集できます。

1. 画面左側のサイドバーで **ユーザー管理** → **ユーザーグループ** をクリックします。
2. 一覧で編集するユーザーグループのチェックボックスをクリックします。

3. ユーザーグループ一覧の左上にある ボタンをクリックしてください。



4. **ユーザーグループの編集** ウィンドウが表示されたら、グループ名を編集します。



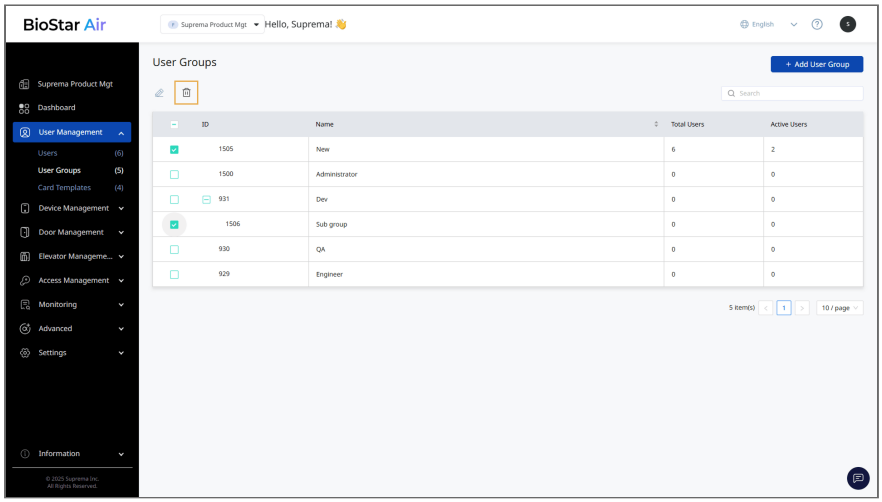
5. 編集内容を保存するには、**OK** ボタンをクリックしてください。

> **情報**
> グループ名の編集は、1つのグループを選択している場合にのみ行えます。

グループの削除

使用していないユーザーグループがある場合は削除できます。

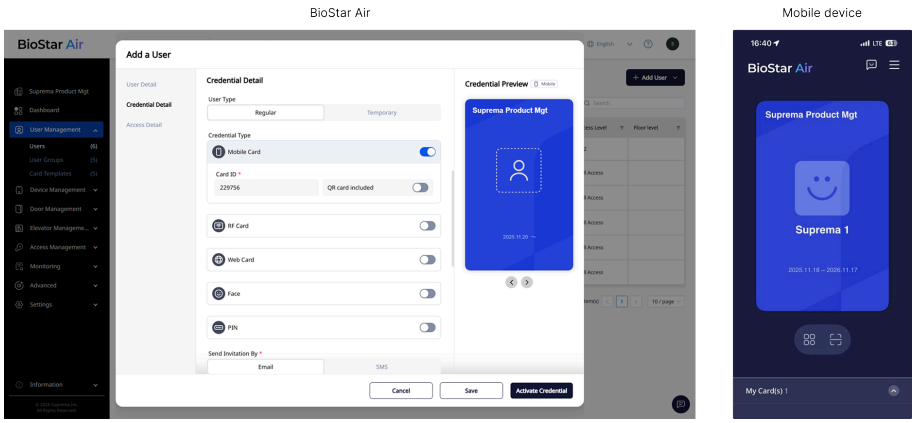
1. 画面左側のサイドバーで **ユーザー管理** → **ユーザーグループ** をクリックします。
2. 一覧で削除するユーザーグループのチェックボックスをクリックします。
3. ユーザーグループ一覧の左上にある ボタンをクリックしてください。



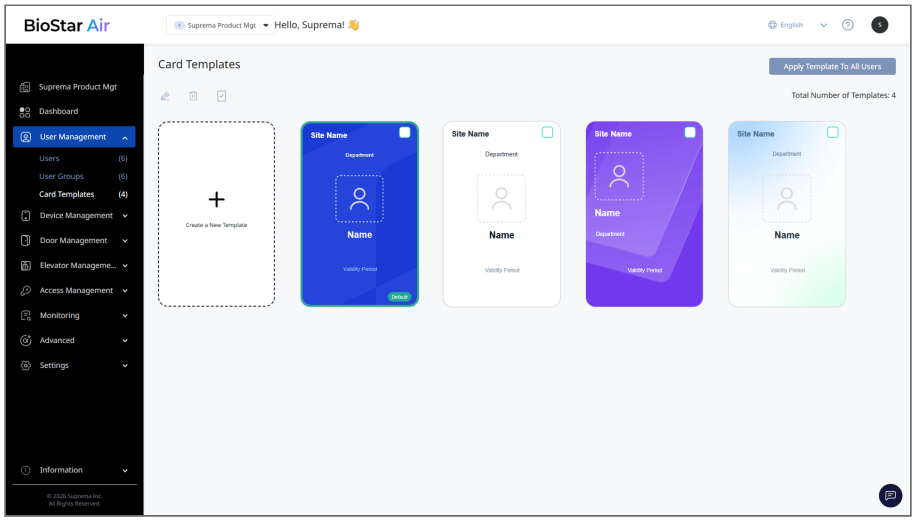
4. 警告メッセージが表示されたら、**はい** ボタンをクリックしてください。

カードテンプレートの管理

BioStar Airのカードテンプレートを使用すると、管理者はユーザー向けのモバイルカードをデザインし、カスタマイズできます。このテンプレートは、会社の色、ロゴ、およびパーソナライズされた詳細を含め、ブランディングを強化するのに役立ちます。 カードテンプレートはSuprema Passアプリで使用されるモバイルカードに適用されます。



BioStar Airのすべてのサイトには既定のテンプレートが含まれています。 画面左のサイドバーで **ユーザー管理** → **カードテンプレート** をクリックします。



既定のテンプレートを確認できます。 管理者は次の3つの方法のいずれかを選択してモバイルカードテンプレートを適用できます。

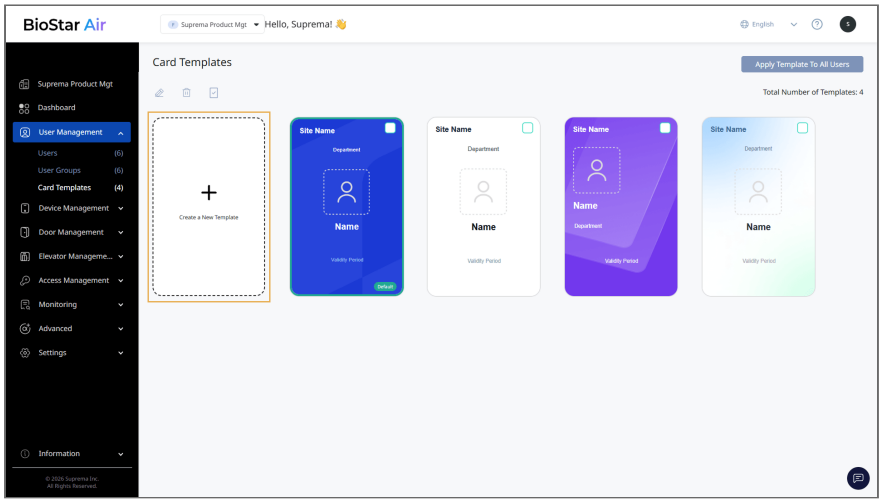
- 既定のカードテンプレートをユーザーのモバイルカードに適用する
- 既存テンプレートのパラメータを変更してカスタム設定したモバイルカードを適用する
- 新しいカスタムテンプレートを作成して既存テンプレートの代わりに適用する

> **ヒント**
> カードテンプレート管理のビデオガイドを見るには、次のビデオを参照してください。

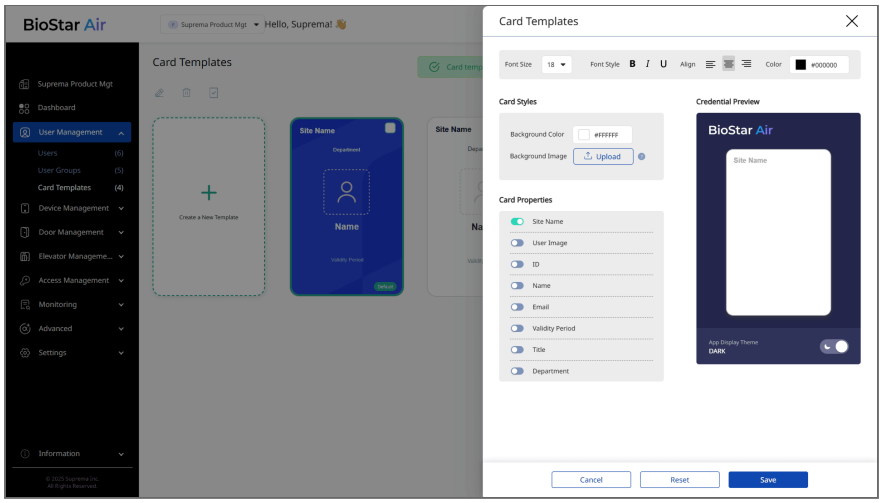
新しいカードテンプレートを作成する

新しいカードテンプレートを作成できます。

1. 画面左のサイドバーで **ユーザー管理** → **カードテンプレート** をクリックします。
2. **新しいテンプレートを作成** をクリックします。



3. **カードテンプレート** パネルが表示されたら、カードのデザインと構成を設定します。

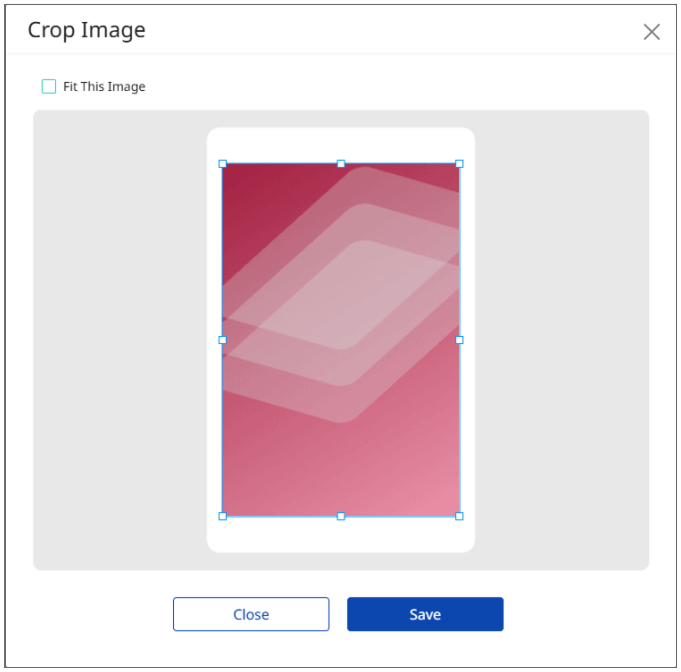


4. 必要な設定を適用した後、モバイルカードテンプレートを保存するには **保存** をクリックします。

カードスタイル

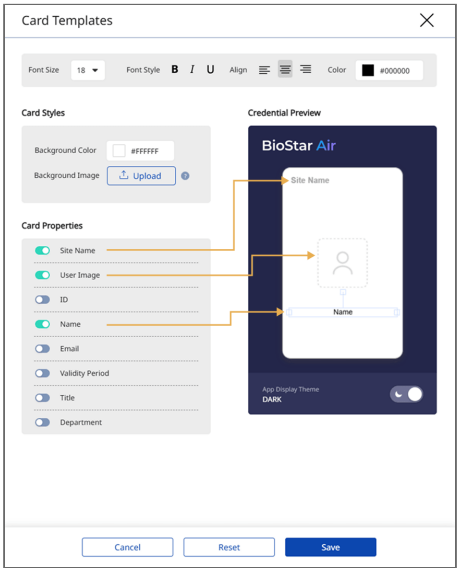
カードスタイル セクションではカードの背景色または背景画像を設定できます。

- **背景色**：モバイルカードの背景色を設定できます。
- **背景イメージ**：モバイルカードの背景画像をアップロードできます。 **アップロード** をクリックして、ローカルに保存されている背景画像ファイルを選択します。 その後、**画像をクロップ** ウィンドウが表示されたら、**サイズフィット** オプションをクリックするか、手動でサイズを調整します。 画像の調整設定を完了したら、**保存** をクリックします。

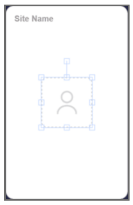


プロパティ

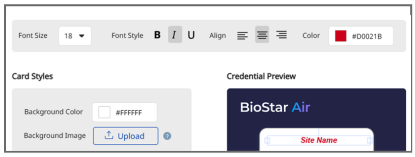
プロパティ セクションではモバイルカードに含める属性を選択できます。 トグルスイッチをクリックすると、右側の **資格情報のプレビュー** に選択した属性が表示されます。



- 希望する属性を配置し、**資格情報のプレビュー** で該当要素をクリックすると、サイズ、位置、角度を調整できるハンドルが表示されます。



- 各属性のフォントをカスタマイズできます。 配置した属性をクリックした後、上部のフォント設定オプションを使用します。 フォントサイズおよびスタイル、整列、色を調整できます。



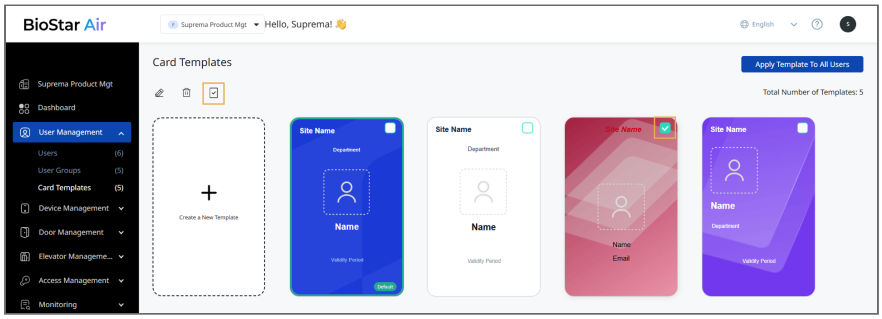
- **アプリ表示テーマ** でダークモードまたはライトモードを選択できます。
- 設定した構成とデザインを初期化するには、**リセット** をクリックします。

- すべての設定を完了したら、モバイルカードテンプレートを保存するには **保存** をクリックします。

既定のカードテンプレートの設定

新しく追加したモバイルカードテンプレートを既定のテンプレートに設定できます。

1. 画面左のサイドバーで **ユーザー管理** → **カードテンプレート** をクリックします。
2. 希望するテンプレートの右上のチェックボックスをクリックします。
3. テンプレート一覧の左上にある ☑ ボタンをクリックしてください。



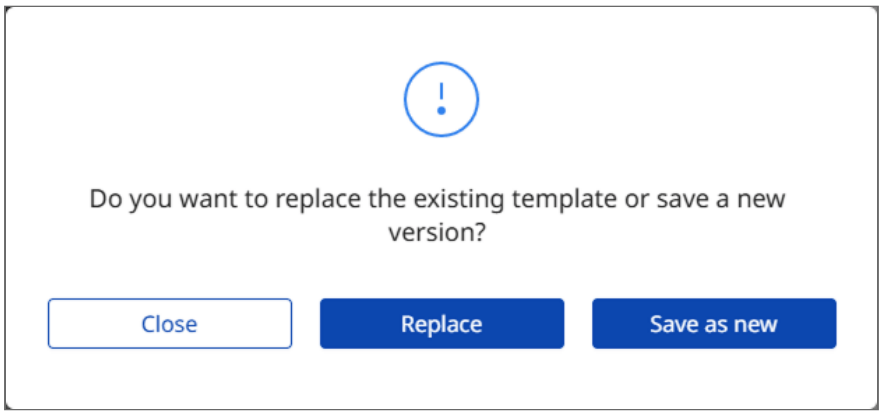
4. メッセージウィンドウが表示されたら、**はい** をクリックします。

既定として設定されたモバイルカードテンプレートは、ユーザーを新規追加する際に自動的に適用されます。

> **情報**
> 既定テンプレート設定機能は、1つのテンプレートのみを適用できます。

カードテンプレートの編集

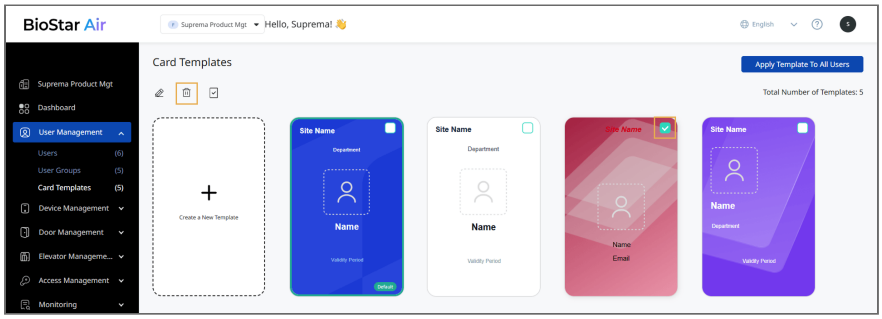
1. 画面左のサイドバーで **ユーザー管理** → **カードテンプレート** をクリックします。
2. テンプレート一覧から編集するテンプレートをクリックします。 またはテンプレートの右上のチェックボックスを選択してから、✎ ボタンをクリックしてください。
3. **カードテンプレート** パネルが表示されたら、カードのデザインと構成を変更します。
4. 変更を保存するには、**保存** をクリックします。
5. メッセージウィンドウが表示されたら、**上書き** または **新規保存** をクリックします。



- **上書き**：既存のテンプレートを編集して保存します。
- **新規保存**：編集した内容を新しいテンプレートとして保存します。

カードテンプレートの削除

1. 画面左のサイドバーで **ユーザー管理** → **カードテンプレート** をクリックします。
2. テンプレート一覧で削除するテンプレートの右上のチェックボックスをクリックします。 1つ以上のテンプレートを選択できます。
3. テンプレート一覧の左上にある ボタンをクリックしてください。

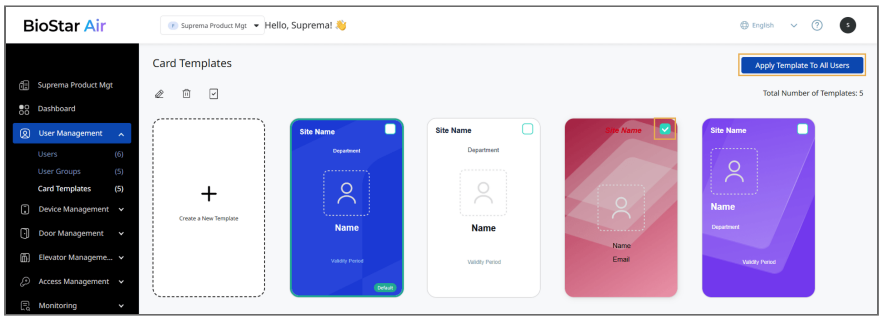


4. メッセージウィンドウが表示されたら、**はい** をクリックします。

> **情報**
> 既定のテンプレートは削除できません。

すべてのユーザーにテンプレートを適用する

1. 画面左のサイドバーで **ユーザー管理** → **カードテンプレート** をクリックします。
2. テンプレート一覧で適用するテンプレートの右上のチェックボックスをクリックします。
3. 画面右上の **すべてのユーザーにテンプレートを適用** ボタンをクリックします。



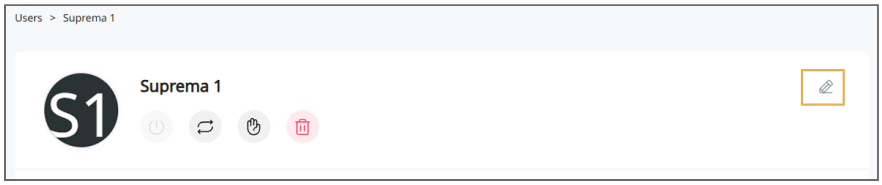
4. メッセージウィンドウが表示されたら、**はい** をクリックします。

> **情報**
>
> - 選択したカードテンプレートをすべてのユーザーに適用すると、既に設定されているテンプレートは置き換えられます。
> - 1つのカードテンプレートのみをすべてのユーザーに適用できます。

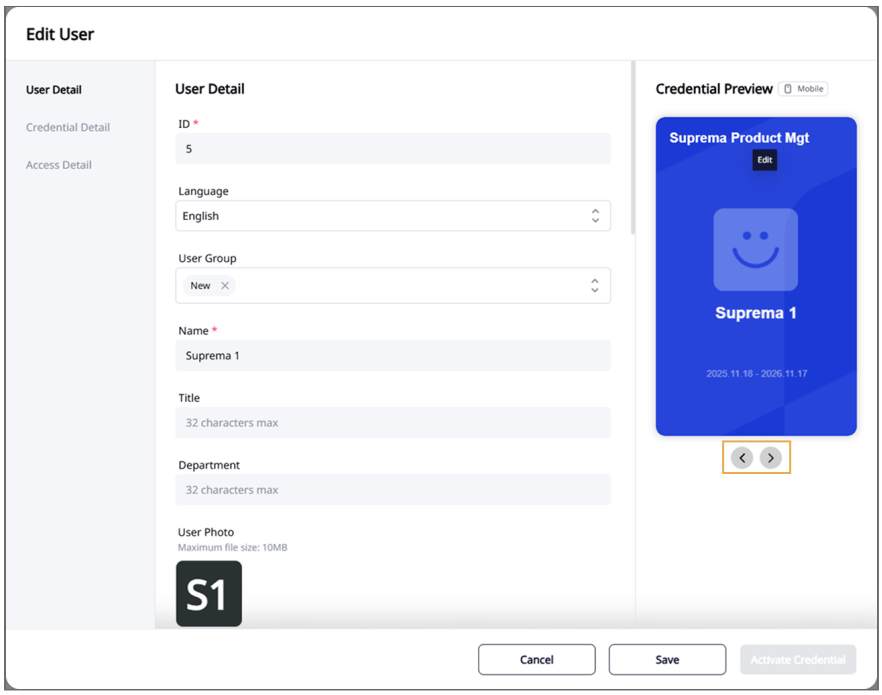
個別ユーザーのカードテンプレート変更

個別ユーザーのカードテンプレートを変更するには、以下の手順に従います。

1. 画面左のサイドバーで **ユーザー管理** → **ユーザー** をクリックします。
2. ユーザー一覧でカードテンプレートを適用するユーザーをクリックします。
3. ユーザー詳細の右上にある ボタンをクリックしてください。



4. **ユーザーの編集** ウィンドウが表示されたら、右側のパネルのカードテンプレート欄で、 または ボタンをクリックして、目的のカードテンプレートを選択してください。



5. 変更を適用するには、**保存** をクリックします。

ユーザーのカードとクレデンシャルの種類

BioStar Air 2.6 以降、ユーザー管理を改善するために2種類のユーザータイプが導入されました。

- **通常**：組織または施設の正規メンバーで、長期かつ継続的な入退室権限が必要なユーザーです。 すべてのクレデンシャルタイプを発行できます。
- **ゲスト**: 短期かつ限定的な入退室権限を必要とする訪問者または非正規メンバーです。 ゲスト、外部来訪者、短期契約者、配達員などが該当します。 **ウェブカード** のクレデンシャルのみ発行でき、QRコードとLinkPassが含まれます。

> **情報**
> ユーザーを追加または編集する際のクレデンシャル発行に関する詳細は、ユーザーの追加を参照してください。

> **ヒント**
> ユーザーとカードの種類に関するビデオガイドを視聴するには、以下の動画を参照してください。

一般ユーザーのカードタイプ

一般ユーザーに発行できるクレデンシャルの種類は以下の通りです。

> **情報**
> Suprema Pass アプリでのモバイルクレデンシャルの使い方については、モバイル認証情報の使い方を参照してください。

モバイルカード

- 固有の **カードID** は自動割り当てされますが、手動で設定することもできます。
- **Airfob Tag** または **Airfob Patch** を使用する場合、モバイルカード番号をカードのシリアル番号として使用し、既存の出入管理システムと統合できます。
- 既存システムとの互換性のため、モバイルカードIDは以前のサイトのRFカード番号と一致させることができます。

RFカード

- ユーザーごとに最大8枚のRFIDカードを追加できます。
- 複数のカードが割り当てられる場合に管理を簡素化するため、**カードタイプ**(CSNまたはWiegand)、**カード ID**、および **カード名** を構成できます。
- 接続されたSupremaデバイスを使用して既存のRFIDカードをスキャンするには、**リーダーでスキャン** 項目でリーダーを選択してください。
- 既存のRFカードに **CSN**（カードシリアル番号）がある場合、CSNを手動で入力できます。

Web QR

- 一般ユーザーはモバイルカードの **QRコード** を使用できます。
- QRコードはモバイルカードのインターフェースのボタンを押して使用できます。

リンクパス

- ユーザーのメールまたは携帯電話番号にウェブリンクを送信します。
- ユーザーは受け取ったリンクをウェブブラウザで開き、**オープン** ボタンをクリックして入退室できます。

> **情報**
> LinkPass クレデンシャルの詳細については、リンクパス クレデンシャルを参照してください。

顔認証

- ユーザーごとに最大2つの顔プロファイル画像を追加できます。

- 接続されたリーダーまたは画像アップロードで登録できます。
- ユーザーにメールリンクを送信した後、モバイル端末のカメラで写真を撮影して登録できます。

2FA PIN

4〜16桁のPINを設定し、2段階認証（2FA）の一部として使用できます。

一時ユーザーのカードタイプ

一時ユーザーはモバイルまたはRFIDカードを受け取りません。 代わりに、アプリのダウンロードが不要な **ウェブベースのクレデンシャル** を発行できます。 利用できるオプションは以下の通りです。

Web QR

- メールまたはSMSで送信します。
- ウェブブラウザでアクセスできます。
- セキュリティを強化するため、5分ごとに更新される **Dynamic QR Code**（動的QRコード）を使用します。

リンクパス

メールまたはSMSでウェブリンクをユーザーに送信します。 ユーザーはウェブブラウザで**オープン** ボタンをクリックすると入退室できます。

> **情報**
> LinkPass クレデンシャルの詳細については、リンクパス クレデンシャルを参照してください。

アクセスレベルの管理

一般ユーザーであれ一時ユーザーであれ、**アクセスレベル**を設定してクレデンシャルが許可される場所を制御する必要があります。

> **注意**
> 一時ユーザーの場合は、制限されたアクセスレベルを慎重に割り当て、無制限のアクセス権が付与されたクレデンシャルを付与しないよう注意してください。

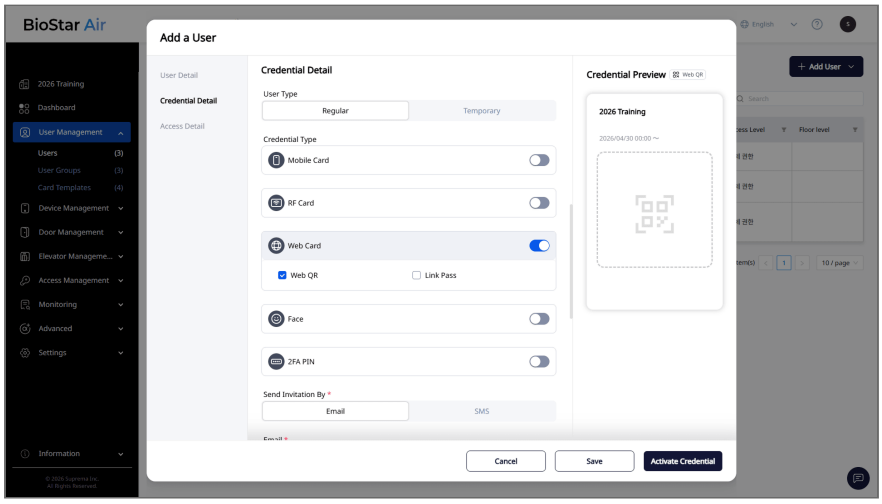
リンクパス クレデンシャル
リンクパス（LinkPass）は、BioStar Airでアプリなしで使用できるモバイルクレデンシャルです。 管理者はアプリのインストールやBLE/NFCを使用せずに、ユーザーにアクセス権を付与できます。 リンクパスはBioStar Airクラウドを介して動作し、安全なウェブリンクで有効化されるため、来訪者対応、配達、駐車場ゲートやロビーなどセキュリティレベルの低いドアでの使用に適しています。

- **認証情報の範囲**：リンクパスの認証情報は、ユーザーに割り当てられている他の認証情報と同じ出入口へのアクセスを許可します。 したがって、セキュリティレベルの高い区域へのアクセス権を持たないユーザーにリンクパスの認証情報を発行することは推奨されません。
- **アプリ不要**：リンクパスはウェブブラウザで動作するため、モバイルアプリ、Bluetooth、またはNFC通信は不要です。
- **クラウドベースのアクセス**：リンクパスのコマンドはBioStar Airのクラウドを通じて送信され、インターネットに接続されていればどこからでも有効化できます。 位置共有や位置追跡機能はありません。

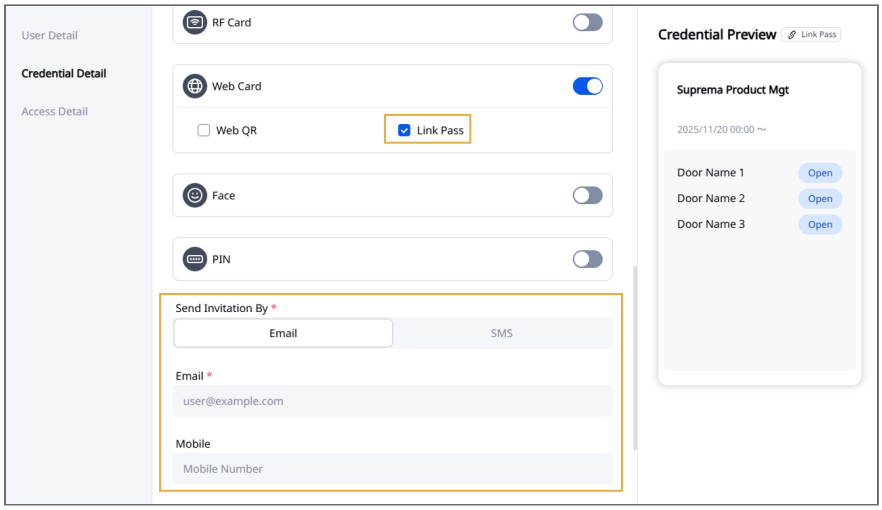
- **デバイスの接続性**：出入口デバイスでリンクパスが正しく動作するには、オンラインでありBioStar Airに接続されている必要があります。
- **推奨利用シーン**：リンクパスは一時的な来訪者、配達、ロビーや駐車場ゲートなど、セキュリティレベルの低い区域での使用に適しています。

リンクパス認証情報の有効化

1. BioStar Airのウェブサイトにログインします。
2. 画面左のサイドバーで **ユーザー管理** → **ユーザー** をクリックします。
3. 次のいずれかの方法で **ユーザーの編集** または **新しいユーザー追加** の画面に移動してください。
   - ユーザー一覧で既存ユーザーをクリックし、右上の をクリックします。
   - 画面右上の **ユーザー追加** → **ユーザー追加** をクリックします。
4. **認証情報の詳細** セクションに移動します。
5. **ウェブカード** オプションを有効にします。



6. **リンクパス** のチェックボックスをクリックします。
7. **招待の送信者** に、ユーザーがクレデンシャルリンクを受け取るための固有の **メールアドレス** または **携帯電話番号** を入力します。



8. 適切な **アクセスレベル** を選択し、ユーザーの **有効期間** を設定します。

9. クレデンシャルを発行するには、**認証情報を有効化** をクリックします。
10. ユーザーに固有のリンクパスURLを含む招待状をメールまたはSMSで送信します。

ユーザーによるリンクパスの利用

1. メールまたはSMSで受け取ったユーザーは、モバイル端末でメッセージ内のリンクパスURLを開きます。
2. ウェブページにはユーザーに割り当てられたすべてのドアが表示され、各ドアに **オープン** ボタンがあります。
3. **オープン** をクリックすると、クラウドベースの開錠コマンドがリーダーに送信され、ドアを開くことができます。

> **情報**
> リンクパスの使用にはBluetoothまたはNFC通信は必要ありません。

デバイス

BioStar Airの柔軟なデバイス管理設定により、各サイトの要件を正確に設定できます。 本ドキュメントでのデバイス管理は、登録、設定、ファームウェア管理、監視、継続的な運用を含むデバイスのライフサイクル全体を指します。

BioStar Airは2種類のデバイスアーキテクチャをサポートします。 両アーキテクチャは同一サイトで併用できるため、各出入口やエリアに最適な方式を選択できます。

エッジアーキテクチャ

各エッジデバイスにはコントローラーが内蔵され、イーサネット経由でクラウドに直接接続します。 ネットワークが切断されてもデバイスは独立して動作し、接続が復旧すると自動で同期します。

エッジデバイスはRS-485で接続された補助機器のコントローラーとしても機能します。

このアーキテクチャは主に次のような場合に適しています。

- 新規導入
- 生体認証機器
- インフラ構築を最小限に抑える必要がある場合

集中型アーキテクチャ

集中型アーキテクチャでは、デバイスがRS-485またはWiegandでコントロールパネルに接続されます。 コントロールパネルはイーサネット経由でクラウドに接続し、接続されたデバイスを管理するコントローラーとして動作します。

コントロールパネルはネットワークが切断された場合、接続されたデバイスの冗長性管理と入退室制御の判断を行います。

このアーキテクチャは主に次のような場合に適しています。

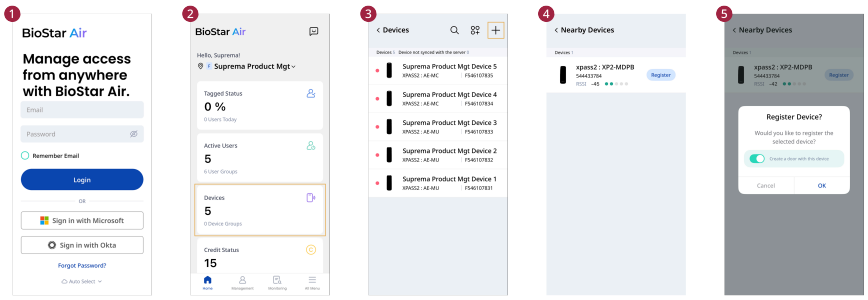
- 既存の低電圧配線を利用する再構築プロジェクト
- 既存の入退室管理システムを置き換えるサイト
- 中央監視室またはコントロールパネルを使用する導入環境

エッジデバイスの登録と削除

デバイスをBioStar Airに追加するには、BioStar Airモバイルアプリを使用する必要があります。 モバイルアプリでは、無線接続を使って新しいデバイスを登録したり、既存のデバイスを削除したり、ファームウェアをアップグレードしたりできます。

デバイス登録

BioStar Airモバイルアプリを使用してデバイスを登録してください。 デバイスの登録はBluetooth Low Energy（BLE）で行われ、登録されたデバイスはBioStar Airポータルで管理できます。



1. モバイル端末でBioStar Airアプリを起動してログインします。
2. **デバイス** カードをタップします。
3. 画面右上の ＋ ボタンをタップします。
4. デバイス検索画面で登録するデバイスの **登録** ボタンをタップします。
5. デバイス登録ウィンドウが表示されたら **OK** ボタンをタップします。

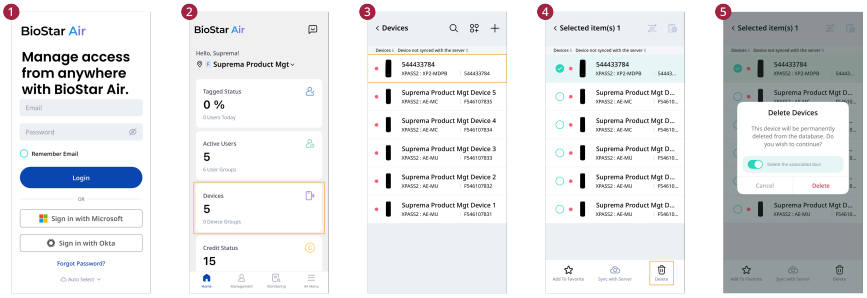
デバイス一覧に戻り、追加されたデバイスを確認します。

> **ヒント**
>
> 最高の性能と信頼性を維持し、最新機能を使用するには、装置を登録したらすぐにファームウェアのアップグレードを必ず確認してください。 装置が梱包された時点と設置された時点の間に、新しいファームウェアが配布されている可能性があります。 ファームウェアのアップグレードに関する詳細は ファームウェアをアップグレードする を参照してください。

> **情報**
>
> - ウェブポータルではデバイスを登録できません。 デバイスは必ずBioStar Airモバイルアプリで登録する必要があります。
> - デバイスを登録する際は、デバイスとモバイル端末を近くに置き、モバイル端末のBluetooth機能を有効にしてください。
> - 登録したデバイスをドアに設定しない場合は、デバイス登録ウィンドウで 이 장치로 출입문 만들기 オプションのチェックを外します。

デバイスの削除

BioStar Airポータルのデバイス一覧でデバイスがオフラインの場合は、モバイルアプリを使用してデバイスを削除できます。



1. モバイル端末で BioStar Air アプリを起動します。
2. **デバイス** カードをタップします。
3. 一覧で削除するデバイスを長押しします。 追加で削除するデバイスを選択します。
4. 画面右下の 🗑 ボタンをタップします。
5. ポップアップメッセージウィンドウで、接続されている出入り口を削除するか選択します。
6. **削除** をタップします。

> **情報**
>
> X-Station 2以外のデバイスはBioStar Airポータルから削除できます。 ただし、デバイスはオンラインである必要があります。 BioStar Airモバイルアプリを使用してデバイスを削除することを推奨します。

登録済みエッジデバイスの管理

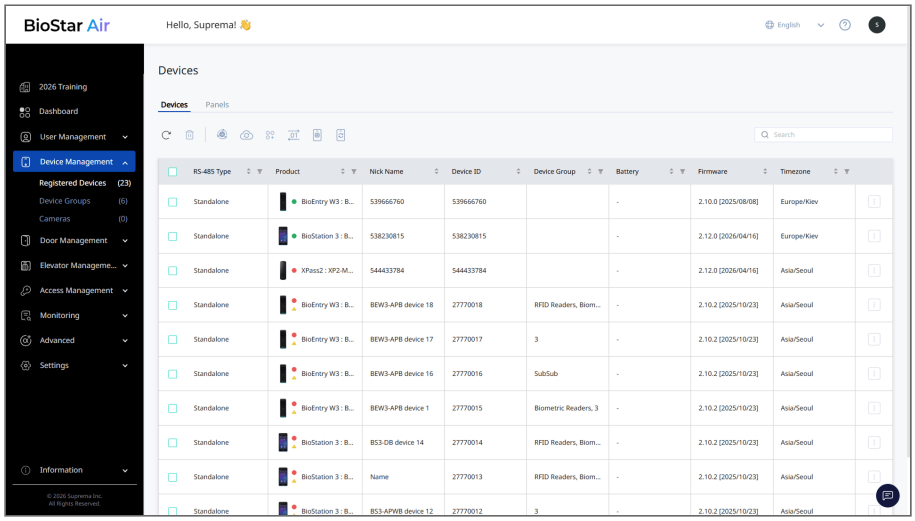
登録されたデバイスの接続状態を一目で確認し、生体認証やカード設定を変更したり、ファームウェアを更新できます。 少数のデバイスは個別に、多数のデバイスは一括で管理できるため、セキュリティシステムを効率的に運用できます。

> **情報**
>
> - デバイスは iOS または Android の **BioStar Air モバイルアプリ**でのみ登録できます。 ウェブポータルでは登録できない。 モバイルアプリでのデバイス登録方法の詳細は エッジデバイスの登録と削除 を参照してください。
> - **リモート接続、生体認証、QRコードによる入退室、ファームウェアの更新**など一部の機能を利用するには、デバイスがインターネットに接続されている必要があります。

> **ヒント**
>
> デバイスの登録と管理に関するビデオガイドを見るには、次のビデオを参照してください。

デバイス一覧の表示

デバイス一覧では、BioStar Air に登録されたすべてのデバイスを一目で確認できます。 各デバイスの接続状態、モデル名、ファームウェアバージョンなどの主要な情報を一目で確認できます。 また、各デバイスをクリックして詳細情報を確認し、設定を変更できます。



画面左のサイドバーで **デバイス管理** → **登録済みデバイス** をクリックします。

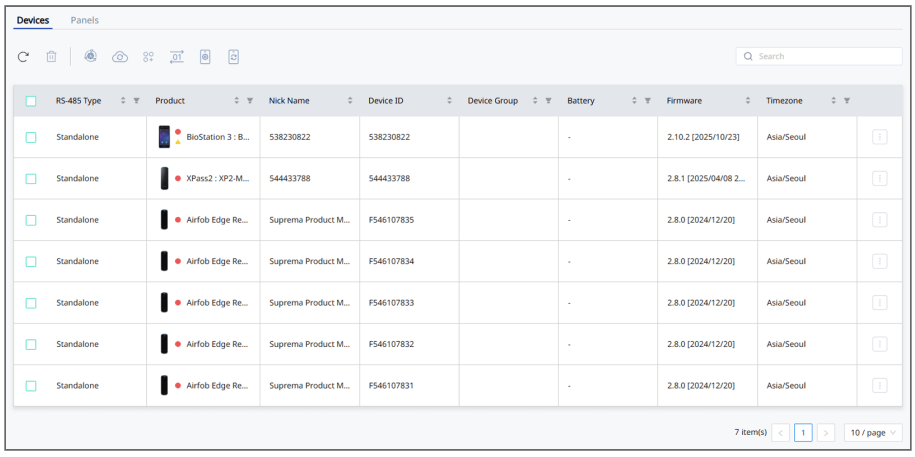
デバイス接続状況

デバイス一覧のステータスアイコンで各デバイスの接続状態を確認できます。

- 🟢 **緑**: オンライン状態で、該当デバイスをリモートで制御でき、QR認証を受け入れ、アップデートできます。
- 🔴 **赤**: オフライン状態のデバイスです。
- 🟠 **オレンジ**: ファームウェアをアップデート中です。
- ○ **接続なし**：ネットワークに接続されていないデバイスです。 (例：Airfob Patch)
- ⚠️ **注意**：サーバーとデバイス間の同期が必要な状態です。 再同期方法については オフラインデバイスの再同期 を参照してください。

デバイス情報

デバイス一覧の各列には、以下の情報が含まれます。

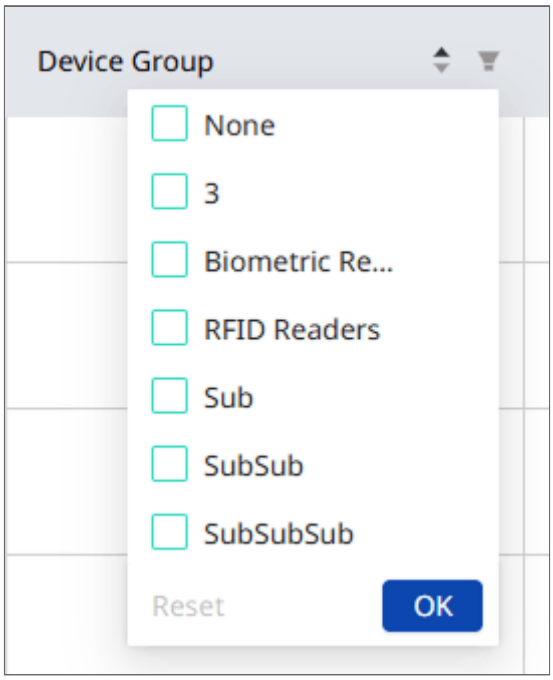


- **RS-485 タイプ**：RS-485通信をサポートするデバイスで確認できます。 該当デバイスがマスターかスレーブかを確認できます。 マスターまたはスレーブに設定されていないデバイスは **Standalone** と表示されます。
- **製品**：Supremaデータベースから取得したデバイス名とモデル名です。
- **ニックネーム**：識別しやすいようにユーザーが編集できる項目です。 デバイス一覧でデバイスをクリックすると表示される **デバイス編集** ウィンドウで変更できます。

- **デバイスID**：デバイスに割り当てられた固有識別子です。
- **デバイスグループ**：デバイスが属するグループです。
- **バッテリー**：バッテリー駆動のデバイスで確認できます。 エアポップタグ(AirFob Tag) デバイスのみ対応しています。
- **ファームウェア**：現在インストールされているファームウェアのバージョンです。
- **タイムゾーン**：デバイスに設定されているタイムゾーンです。

フィルタリング

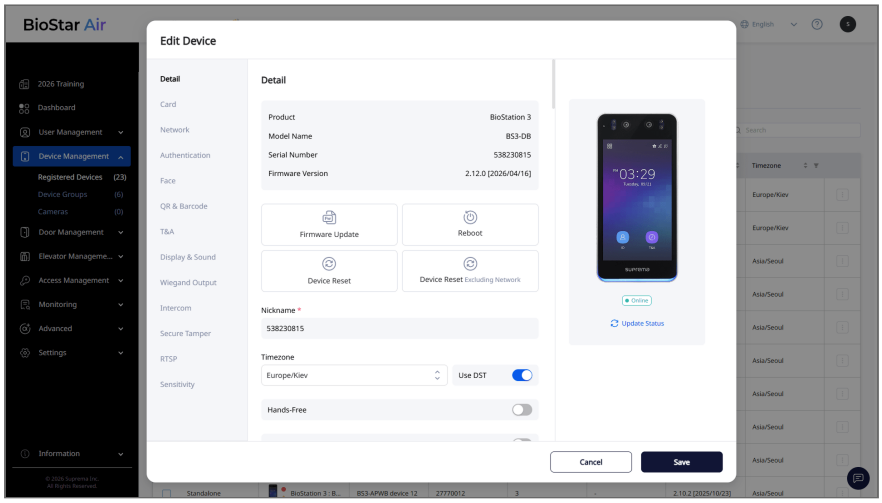
デバイス一覧の上部ヘッダー領域でフィルター機能を利用できます。 ヘッダー領域の ボタンをクリックすると、条件を設定できます。



> **情報**
> 適用したフィルター条件を初期化するには、 ボタンをクリックし、**リセット** ボタンを選択してください。

個別デバイス情報および設定の編集

1. 画面左のサイドバーで **デバイス管理** → **登録済みデバイス** をクリックします。
2. 一覧から編集するデバイスをクリックします。
3. **デバイス編集** ウィンドウが表示されます。



上記の画像は例示です。実際の画面とは異なる場合があります。

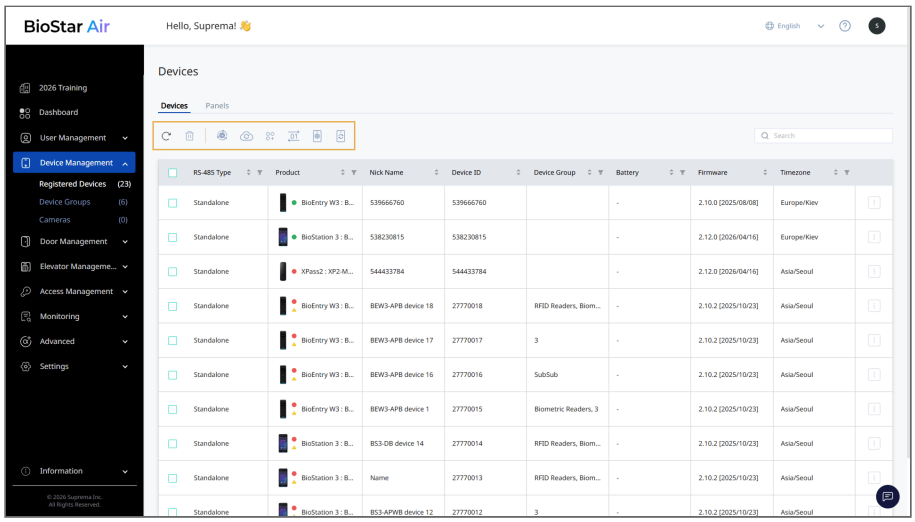
4. デバイスの詳細情報または設定を編集します。

5. 変更を保存するには、下部の **保存** をクリックします。

各セクションごとの詳細情報の編集および設定オプションの詳細は デバイスおよびパネルの設定オプションのご案内 を参照してください。

デバイス一括操作

デバイス一覧上部で提供される機能により、複数のデバイスを一度に管理できます。



- ：デバイス一覧を更新できます。
- ：サイトに登録されたデバイスを削除できます。

> **警告**
> オンラインのデバイスのみ永続的に削除できます。 デバイスがオフラインの場合、別のサイトに追加する前に BioStar Air モバイルアプリで先に削除してください。 モバイルアプリでのデバイス削除方法の詳細は エッジデバイスの登録と削除 を参照してください。

- ：デバイス一覧で選択したデバイスのファームウェアを更新できます。 ファームウェアの更新に関する詳細は ファームウェアをアップグレードする を参照してください。

- ：デバイス一覧で選択したデバイスからサーバーに生体認証テンプレートを同期できます。
- ：デバイス一覧で選択したデバイスをグループに割り当てることができます。 デバイスグループの管理の詳細については、デバイスグループの管理を参照してください。
- ：デバイス一覧で選択したデバイスのRFカードのバイト順を**MSB**または**LSB**に切り替えられます。
  - **MSB**：カードデータを処理するとき、大きいバイト単位から小さいバイト単位の順に処理し、カードシリアル番号 (CSN) を左から右へ順に保存します。
  - **LSB**：カードデータを処理するとき、小さいバイト単位から大きいバイト単位の順に処理してカードシリアル番号 (CSN) を保存します。
- ：スタンドアロンモードで、元の設定を持つデバイスの設定を読み込むことができます。
- ：デバイス一覧で選択したデバイスの状態を更新できます。

オフラインデバイスの再同期

デバイスが長期間オフラインだった場合、サーバーとの情報がずれ、手動で再同期する必要があります。

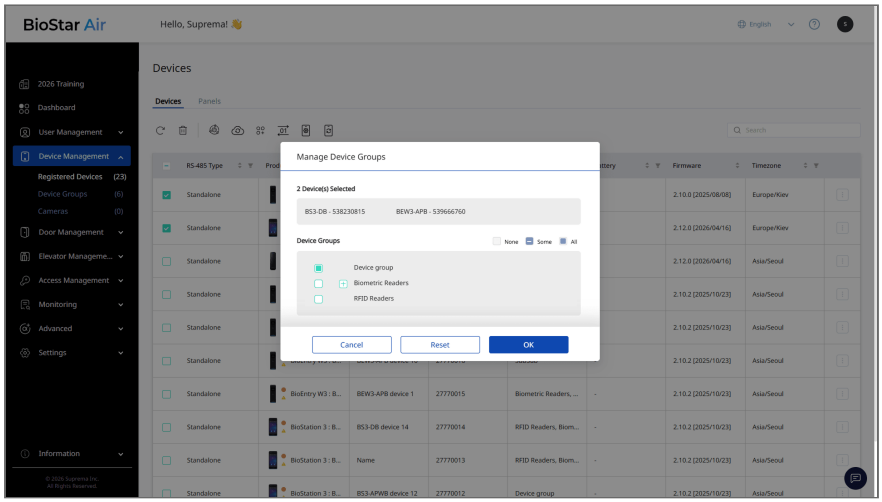
1. 画面左のサイドバーで **デバイス管理** → **登録済みデバイス** をクリックします。
2. デバイス一覧の **製品** 列で ⚠ アイコンが表示されているデバイスを確認します。
3. 該当するデバイスのチェックボックスを選択します。
4. 一覧上部のツールバーで ボタンをクリックします。

> **情報**
> 7日未満オフラインだったデバイスは、再接続時に自動で同期されるため、別途対応は不要です。

デバイスグループの管理

デバイス一覧で個別のデバイスを選択して、グループに追加したり既存のグループから削除したりできます。

1. 画面左側のサイドバーで **デバイス管理** → **登録済みデバイス** をクリックしてください。
2. デバイス一覧で、グループに追加または削除するデバイスのチェックボックスをクリックしてください。
3. デバイス一覧の上部にある ボタンをクリックしてください。
4. **デバイスグループの管理** ウィンドウが表示されたら、選択したデバイスをグループに追加または削除します。



デバイスグループ のチェックボックスの状態は、以下の意味を持ちます。

- **なし**：選択したデバイスをグループから削除します。
- **いくつか**：選択したデバイスの一部がグループに含まれている状態です。
- **すべて**：選択したデバイスをグループに追加します。

5. 変更内容を保存するには、**OK** ボタンをクリックします。

> **情報**
>
> - **デバイスグループの管理** ウィンドウで別のグループを選択すると、選択したデバイスはそのグループに移動します。
> - デバイスはグループに重複して所属できます。 1つのデバイスを複数のグループに割り当てることができます。
> - 変更内容を初期化するには、**リセット** ボタンをクリックします。

パネルの登録と削除

BioStar Air 2.12 では、CoreStation 20（CS-20）パネルを通じてアクセス制御システムを拡張できます。 既存の RS-485 配線を活用して追加機器をローカルに接続するため、インフラコストを削減しつつ複雑なドア構成をサポートできます。

本書では CS-20 パネルを登録し、RS-485、OSDP、Wiegand 通信方式の機器を補助デバイスとして構成する手順をステップごとに説明します。

> BioStar Airでは、コントローラとして動作するマスター（Primary）デバイスと、コントローラに接続されるセカンダリ（Secondary）デバイスに分類されます。 一部のシステムではこの概念をマスター（Master）/スレーブ（Slave）と表現しますが、BioStar Airの文書ではその用語は使用しません。

パネル登録

CoreStation 20（以下 CS-20）は RS-485 通信をサポートする機器と接続してアクセス制御システムを拡張する機能を提供します。 CS-20 を登録するには、次の手順に従ってください。

開始する前に

- CS-20 の電源が入っており、**INIT** ボタンを押すために本体へ物理的にアクセスできる必要があります。
- CS-20 は外部インターネットに接続されている必要があります。 ネットワーク接続が不安定な場合、登録時に問題が発生する

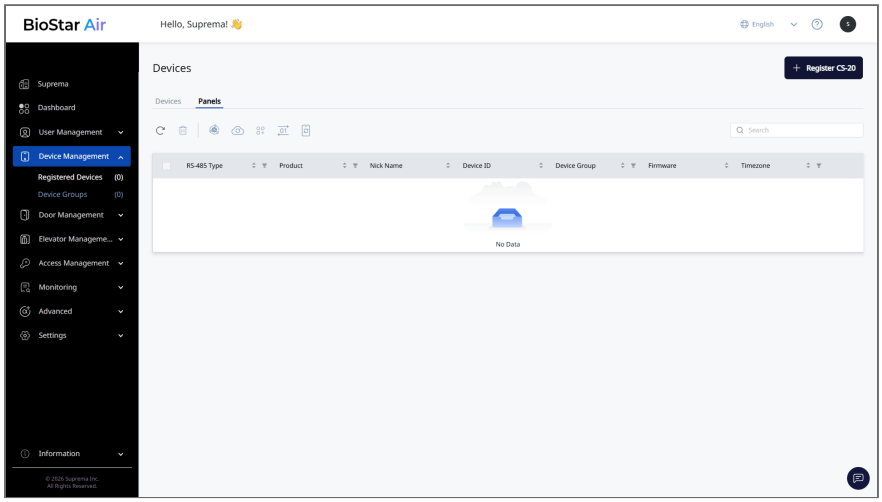
可能性があります。

- 9桁のシリアル番号が必要です。 シリアル番号は機器の背面ラベルで確認できます。

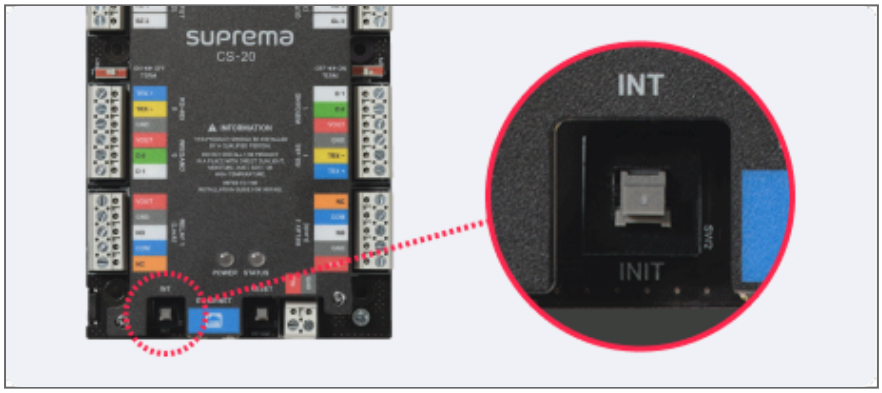
> **情報**
> CoreStation 20の詳細はCoreStation 20 インストールガイドを参照してください。

CS-20 登録

1. 画面左のサイドバーで **デバイス管理** → **登録済みデバイス** をクリックします。
2. **パネル** タブをクリックしてください。

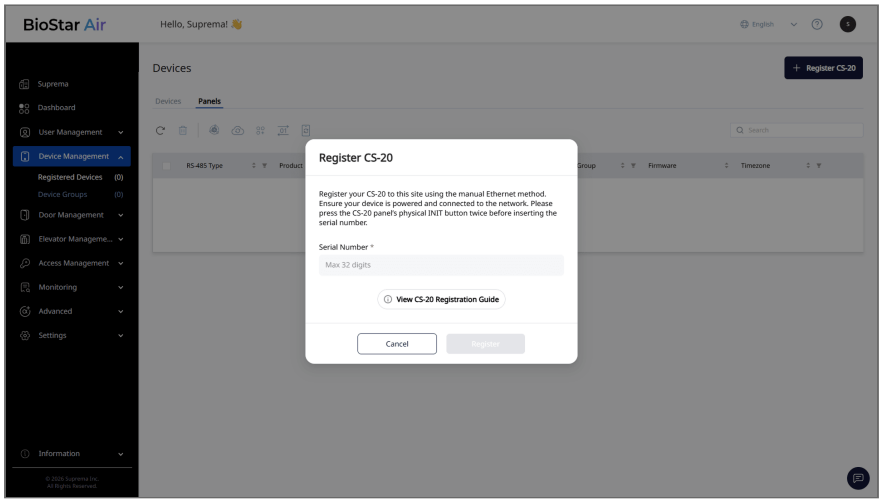


3. 画面右上の **CS-20の登録** ボタンをクリックしてください。
4. **CS-20の登録** ウィンドウが表示されたら、CS-20 パネルで INIT ボタンを2回押してください。



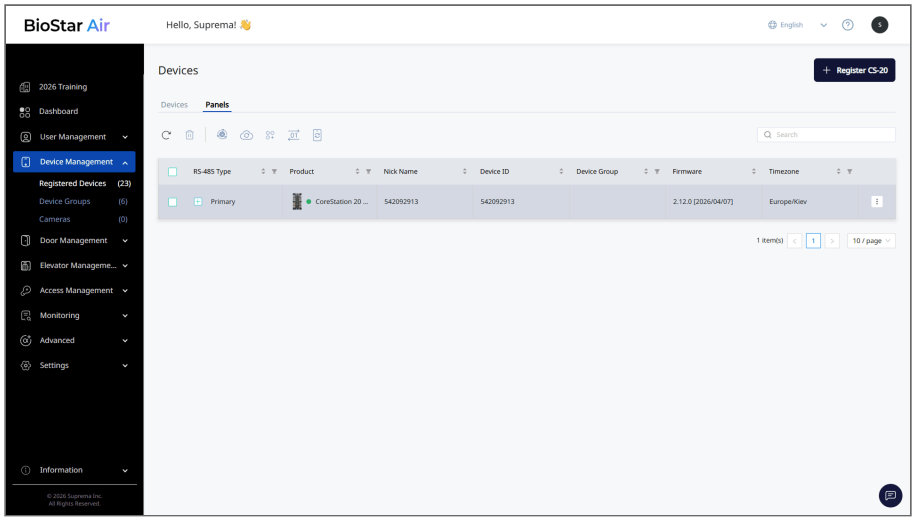
> **注意**
> INIT ボタンを押してから登録を完了できるのは5分間です。

5. シリアル番号を入力してください。



6. シリアル番号をすべて入力したら、**登録** ボタンをクリックしてください。

登録が完了すると、システムが安全な接続を自動で設定し、パネル一覧に新しい CS-20 が表示されます。 正常に登録されると、機器名の横に緑色の点が表示されます。



ヒント

最高の性能と信頼性を維持し、最新機能を使用するには、装置を登録したらすぐにファームウェアのアップグレードを必ず確認してください。 装置が梱包された時点と設置された時点の間に、新しいファームウェアが配布されている可能性があります。 ファームウェアのアップグレードに関する詳細は ファームウェアをアップグレードする を参照してください。

情報

CS-20 登録手順の詳細を確認するには、**CS-20登録ガイドを表示** ボタンをクリックしてください。

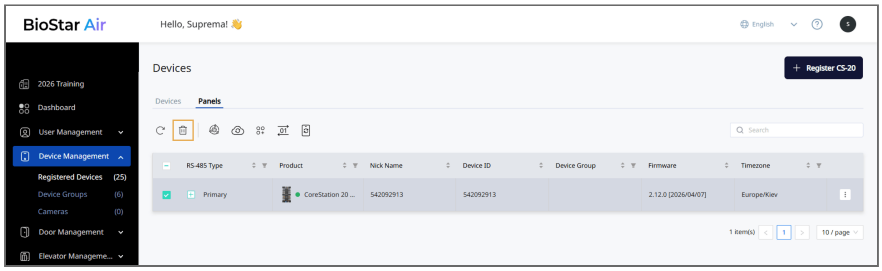
パネルの削除

BioStar Airに登録されたパネルを削除するには、次の手順に従ってください。 削除したパネルは復元できません。 パネルを削除する前に、そのパネルに接続されている補助機器がもう必要ないことを確認してください。

1. 画面左のサイドバーで **デバイス管理** → **登録済みデバイス** をクリックします。
2. **パネル** タブをクリックしてください。

3. 一覧で削除するパネルのチェックボックスをクリックしてください。

4. 画面左上の 🗑 ボタンをクリックします。



5. ポップアップメッセージが表示されたら、**OK** ボタンをクリックします.

> **注意**
> 接続された補助機器を再利用する必要がある場合、SCBキーがバインドされている可能性があるため、補助機器を先に削除してからパネルを削除することを推奨します。

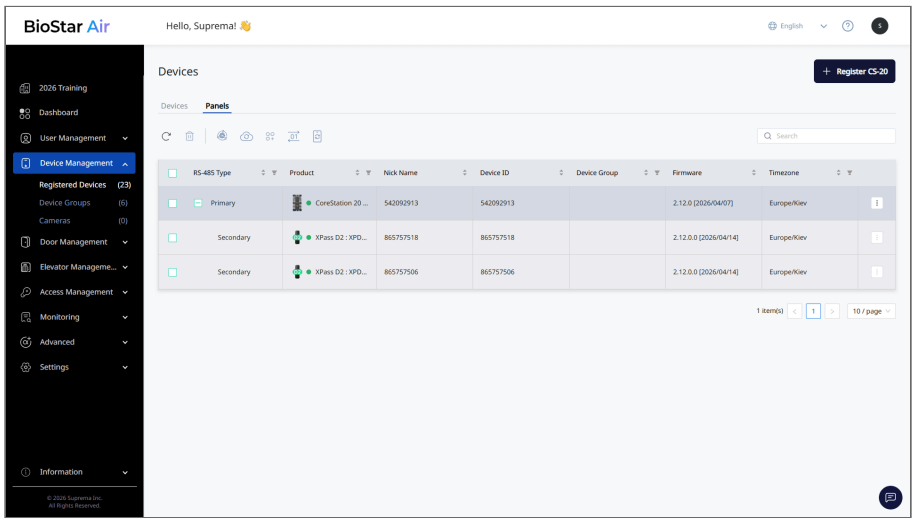
登録済みパネルの管理

BioStar Airでは、登録済みのすべてのパネルを一元管理できます。 各パネルの状態を監視し、必要に応じて情報を編集し、グループ化し、ファームウェアを更新できます。 本書では、パネル一覧の確認からグループ管理まで必要なすべての機能について説明します.

> **情報**
> BioStar Airでは、コントローラとして動作するマスター（Primary）デバイスと、コントローラに接続されるセカンダリ（Secondary）デバイスに分類されます。 一部のシステムではこの概念をマスター（Master）/スレーブ（Slave）と表現しますが、BioStar Airの文書ではその用語は使用しません。

パネル一覧の確認

登録済みのパネルは **パネル** タブで管理できます。 パネル一覧では、各パネルまたは補助デバイスの種類・状態・名前・ID・グループ・ファームウェア情報・タイムゾーンなどの主要情報を一目で確認できます。



パネルおよびデバイスの状態

パネル一覧のステータスアイコンで、各パネルまたは補助デバイスの接続状態を確認できます。

- 🟢 **緑**：オンライン状態で、該当のパネルまたは補助デバイスをリモートで制御および更新できます。
- 🔴 **赤**：オフライン状態のパネルまたは補助デバイスです。
- 🟠 **オレンジ**：ファームウェアをアップデート中です。
- ⚠️ **注意**：サーバーとパネルまたは補助デバイス間で同期が必要な状態です. 再同期方法については オフラインのパネルおよび補助装置の再同期 を参照してください。

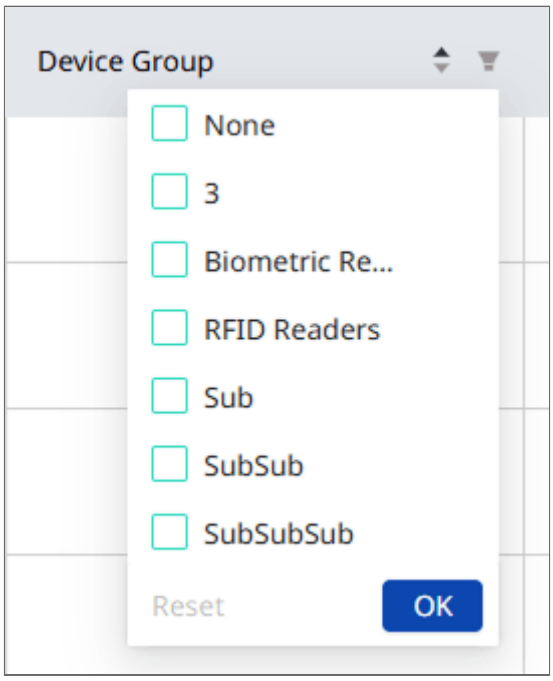
パネルおよびデバイス情報

パネル一覧の各列には以下の情報が含まれます。

- **RS-485 タイプ**：RS-485通信をサポートするパネルまたは補助デバイスで表示されます。 該当のデバイスがマスターか補助かを確認できます。
- **製品**：Supremaデータベースから取得したパネルまたは補助デバイスの名称、モデル名、状態を確認できます。
- **ニックネーム**：識別しやすいようにユーザーが編集できる項目です。 一覧でパネルまたは補助デバイスをクリックすると表示される情報編集ウィンドウで変更できます。
- **デバイスID**：パネルまたは補助デバイスに割り当てられた固有識別子です。
- **デバイスグループ**：パネルが所属するグループです。
- **ファームウェア**：現在インストールされているファームウェアのバージョンです。
- **タイムゾーン**：パネルまたは補助デバイスに設定されたタイムゾーンです。

フィルタリング

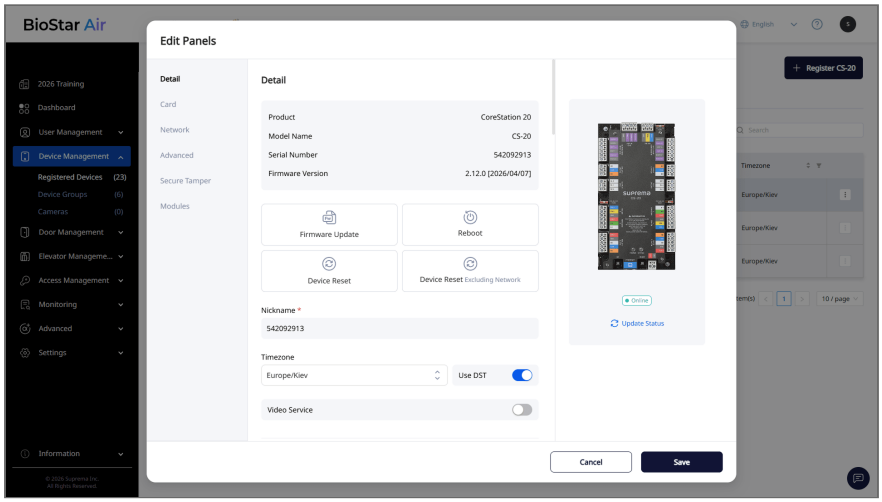
パネル一覧の上部ヘッダー領域でフィルター機能を利用できます。 ヘッダー領域の ボタンをクリックすると、条件を設定できます。



> **情報**
> 適用したフィルター条件を初期化するには、 ボタンをクリックし、**リセット** ボタンを選択してください。

パネル情報の編集

1. 画面左のサイドバーで **デバイス管理** → **登録済みデバイス** をクリックします。
2. **パネル** タブをクリックしてください。
3. 一覧で情報を編集するパネルをクリックすると、**パネルの編集** ウィンドウが表示されます。

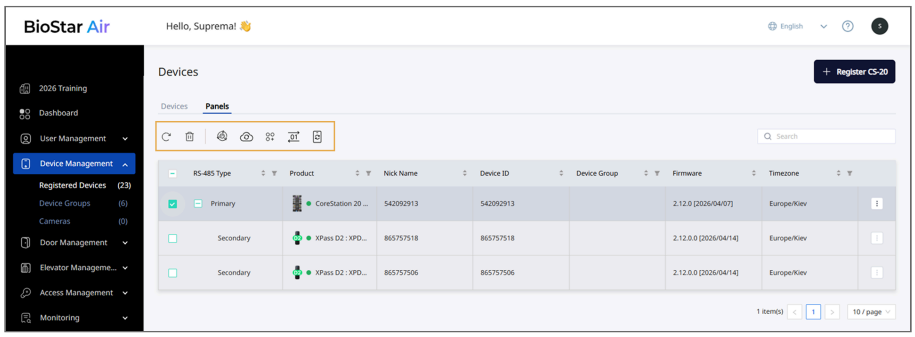


4. パネルの詳細情報または設定を編集してください。
5. 変更を保存するには、下部の **保存** をクリックします。

> **情報**
> 各セクションの詳細情報の編集および設定オプションの詳細は デバイスおよびパネルの設定オプションのご案内 を参照してください。

パネル管理機能

パネル一覧でパネルを選択すると、一覧上部にある管理機能を使用できます。



- ：一覧を更新できます。
- ：登録済みのパネルまたは補助デバイスを削除できます。

- ：パネル一覧で選択したパネルまたは補助デバイスのファームウェアを更新できます。 ファームウェアの更新に関する詳細は ファームウェアをアップグレードする を参照してください。

  - CS-20に接続された補助デバイスは、同時に1台ずつのみアップグレードできます。
  - XPass D2のファームウェアアップグレードの詳細はファームウェアをアップグレードするを参照してください。

- ：一覧で選択したパネルからサーバーへ生体認証テンプレートを同期できます。
- ：一覧で選択したパネルをグループに割り当てることができます。 グループ管理の詳細は パネルグループの管理 を参照してください。
- ：一覧で選択したパネルのRFカードのバイト順を**MSB**または**LSB**に切り替えられます。
  - **MSB**：カードデータを処理するとき、大きいバイト単位から小さいバイト単位の順に処理し、カードシリアル番号 (CSN) を左から右へ順に保存します。
  - **LSB**：カードデータを処理するとき、小さいバイト単位から大きいバイト単位の順に処理してカードシリアル番号 (CSN) を保存します。
- ：スタンドアロンモードで、元の設定を持つパネルの設定を読み込めます。
- ：一覧で選択したパネルの状態を更新できます。

> **情報**
> CS-20に接続された補助デバイスは、更新()、デバイス削除()、ファームウェア更新()の機能のみ提供します。

オフラインのパネルおよび補助装置の再同期

パネルまたは補助装置が長期間オフラインだった場合、サーバーとの情報にずれが生じるため、手動で再同期する必要があります。

1. 画面左のサイドバーで **デバイス管理** → **登録済みデバイス** をクリックします。
2. **パネル** タブをクリックしてください。
3. 一覧の **製品** 列で、 アイコンが表示されたパネルまたは補助装置を確認してください。
4. 該当するパネルまたは補助装置のチェックボックスを選択してください。
5. 一覧上部のツールバーで ボタンをクリックします。

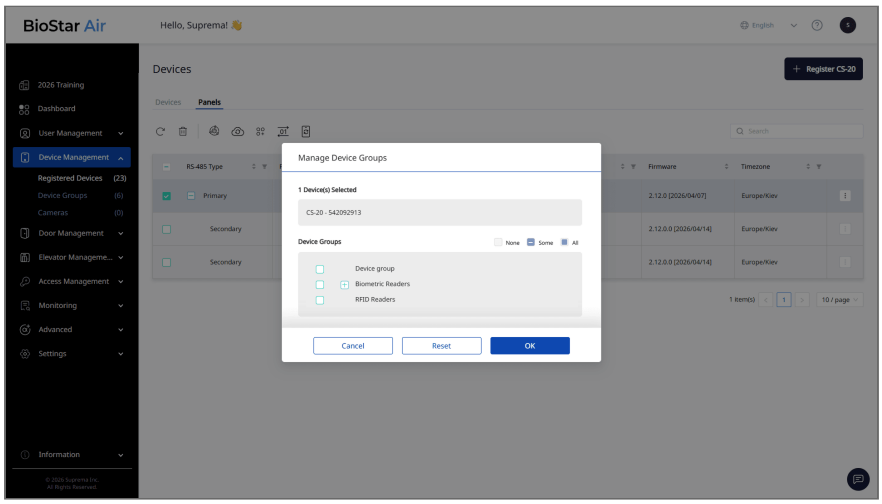
> **情報**
> 7日未満オフラインだったパネルまたは補助装置は、再接続時に自動で同期されるため、追加の操作は不要です。

パネルグループの管理

パネル一覧で個別のパネルを選択して、グループに追加するか既存のグループから削除できます。

1. 画面左のサイドバーで **デバイス管理** → **登録済みデバイス** をクリックします。

2. **パネル** タブをクリックしてください。
3. パネル一覧でグループに追加または削除するパネルのチェックボックスをクリックしてください。
4. パネル一覧の上部にある ボタンをクリックしてください。
5. **デバイスグループの管理** ウィンドウが表示されたら、選択したパネルをグループに追加または削除してください。



デバイスグループ のチェックボックスの状態は、以下の意味を持ちます。

- **なし**：選択したパネルをグループから削除します。
- **いくつか**：選択したパネルの一部がグループに含まれている状態です。
- **すべて**：選択したパネルをグループに追加します。

6. 変更内容を保存するには、**OK** ボタンをクリックします。

> **情報**
>
> - **デバイスグループの管理** ウィンドウで別のグループを選択すると、選択したパネルはそのグループに移動します。
> - パネルはグループに重複して所属できます。 1つのパネルを複数のグループに割り当てることができます。
> - パネル一覧の補助デバイスはファームウェアアップグレード機能のみ提供します。
> - 変更内容を初期化するには、**リセット** ボタンをクリックします。

パネルへのデバイスの追加と管理

BioStar Airシステムは、マスター機器であるCS-20パネルを中心に、複数種類の補助デバイスを接続できます. RS-485、OSDP、Wiegandなどの通信プロトコルをサポートし、既存のセキュリティシステムと容易に統合できます. 本書では、補助デバイスの設定、管理、削除方法を案内します.

補助デバイスの構成

CS-20 を登録した後、次のいずれかの方法で補助デバイスを構成できます：

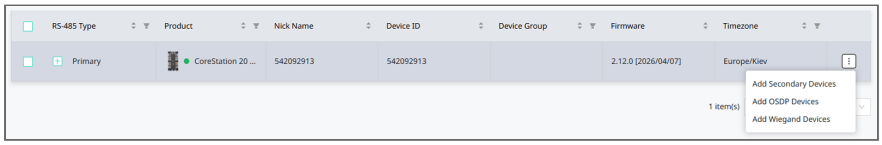
補助デバイス	説明
Suprema RS-485 デバイス	XPass D2およびOM-120で既存のRS-485配線と標準通信プロトコルを使用します.

補助デバイス	説明
OSDP 機器	セキュリティ強化された通信プロトコルを使用します。
Wiegand 機器	カードリーダーなど既存の Wiegand 対応機器。

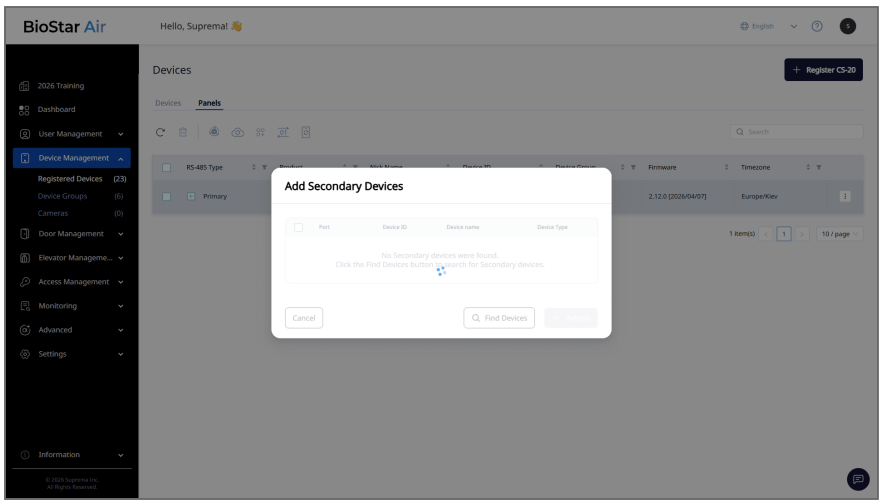
スレーブ装置の構成

RS-485 通信をサポートする機器を CS-20 に接続してスレーブ装置として構成できます。 スレーブ装置はパネル一覧で CS-20 の下に階層表示されます。

1. パネル一覧で登録済みの CS-20 パネルの一番右にある ⋮ ボタンをクリックしてください。



2. ポップアップメニューで **セカンダリデバイスの追加** をクリックすると、**セカンダリデバイスの追加** ウィンドウが表示されます。

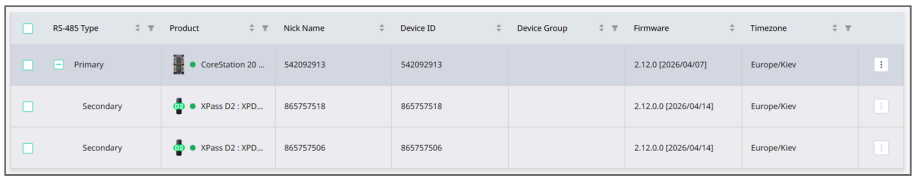


> 検索されたスレーブ装置がない場合は、**デバイスの検索** ボタンをクリックして CS-20 に接続された機器を再検索できます。

3. 接続されたスレーブ装置が一覧に表示されたら、各機器の横にあるチェックボックスをクリックして追加する機器を選択してください。

4. 選択が完了したら、**追加** ボタンをクリックしてください。

接続されたスレーブ装置が CS-20 の下に階層表示されます。 これでパネル一覧で CS-20 に接続されたすべての機器を一目で確認できます。



ヒント

最高の性能と信頼性を維持し、最新機能を使用するには、装置を登録したらすぐにファームウェアのアップグレードを必ず確認してください。 装置が梱包された時点と設置された時点の間に、新しいファームウェアが配布されている可能性があります。 ファームウェアのアップグレードに関する詳細は ファームウェアをアップグレードする を参照してください。

情報

- スレーブデバイスの情報編集および管理方法の詳細は 登録済みエッジデバイスの管理 を参照してください.
- スレーブデバイスの情報および設定オプションの詳細は デバイスおよびパネルの設定オプションのご案内 を参照してください.
- XPass D2のファームウェアアップグレードの詳細はファームウェアをアップグレードするを参照してください。

OSDP 機器の構成

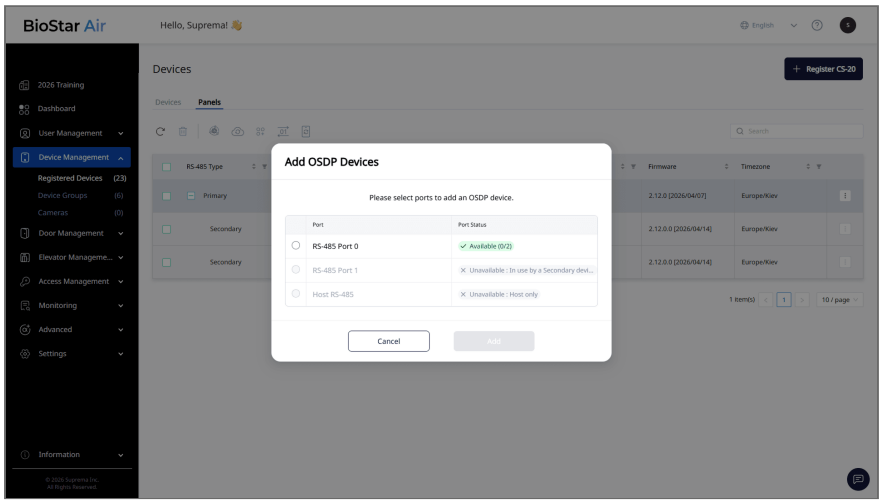
OSDP(Open Supervised Device Protocol) はセキュリティが強化された通信プロトコルです。 高いセキュリティが要求される環境では、OSDP 対応機器を CS-20 に接続してください。

1. パネル一覧で登録済みの CS-20 パネルの一番右にある ⋮ ボタンをクリックしてください。



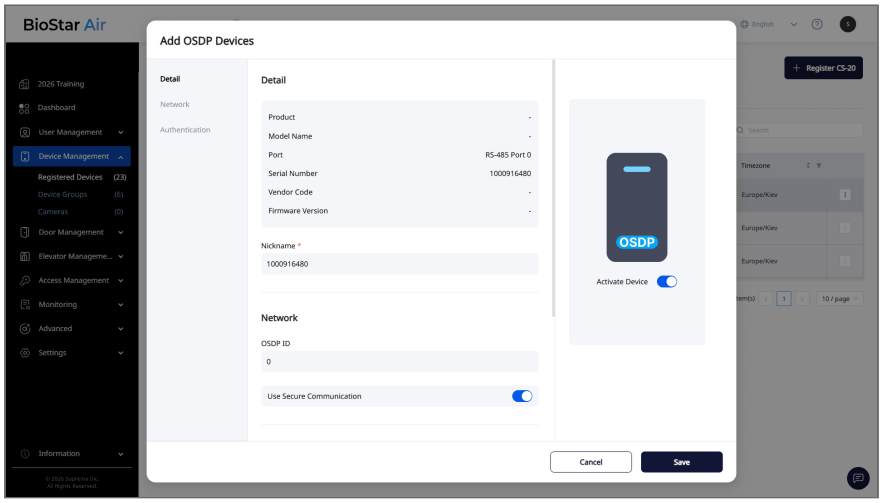
2. ポップアップメニューで **OSDPデバイスの追加** をクリックしてください。

3. **OSDPデバイスの追加** ウィンドウが表示されたら、機器を追加するポートを選択してください。



4. ポートを選択したら、**追加** ボタンをクリックしてください。

5. **OSDPデバイスの追加** ウィンドウで必要な設定を完了したら、**保存** ボタンをクリックしてください。



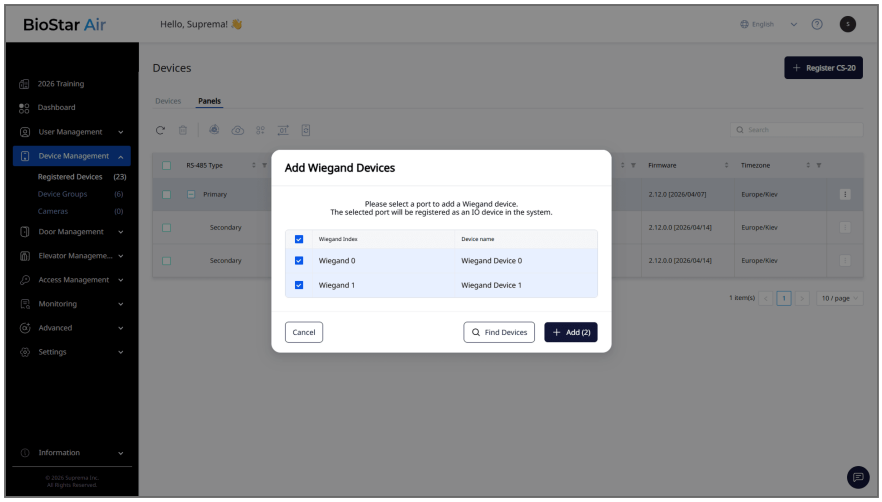
Wiegand 機器の構成

Wiegand はアクセス制御システムで広く使われている通信プロトコルです。 CS-20 に Wiegand 機器を接続して Wiegand スレーブ装置として構成できます。

1. パネル一覧で登録済みの CS-20 パネルの一番右にある ⋮ ボタンをクリックしてください。



2. ポップアップメニューで **Wiegandデバイスの追加** をクリックしてください。
3. **Wiegandデバイスの追加** ウィンドウが表示されたら、機器を追加するポートを選択してください。

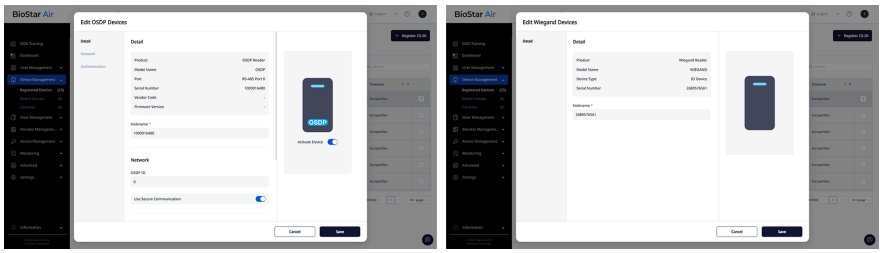


4. ポートを選択したら、**追加** ボタンをクリックしてください。

OSDP/Wiegand デバイス情報の編集

1. 画面左のサイドバーで **デバイス管理** → **登録済みデバイス** をクリックします。
2. **パネル** タブをクリックしてください。
3. 一覧でマスター機器の「+」アイコンをクリックして、接続された補助デバイスの一覧を展開してください.
4. 情報を編集するOSDPまたはWiegandの補助デバイスをクリックしてください.

5. デバイス情報編集ウィンドウが表示されたら、詳細情報または設定を編集してください.

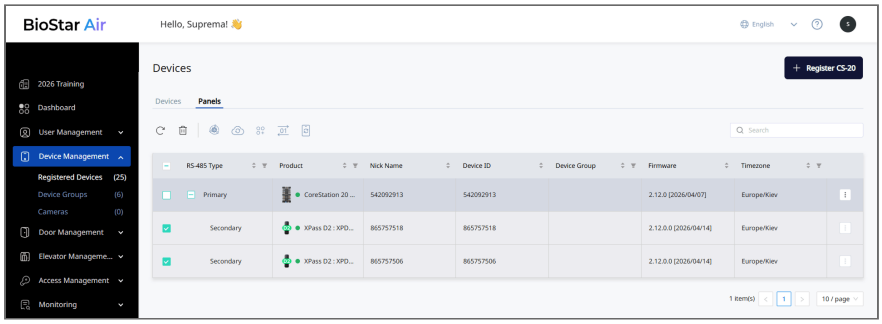


- OSDPデバイス：デバイス名、ネットワーク設定、認証設定（RFカード、RFカード＋PIN）、認証待機時間を設定できます.
- Wiegandデバイス：デバイス名を編集できます.

6. 変更を保存するには、下部の **保存** をクリックします。

補助デバイスの削除

1. 画面左のサイドバーで **デバイス管理** → **登録済みデバイス** をクリックします。
2. **パネル** タブをクリックしてください。
3. 一覧でマスター機器の「+」アイコンをクリックして、接続された補助デバイスの一覧を展開してください.
4. 削除する補助デバイスのチェックボックスをクリックします.
5. 一覧上部の🗑 ボタンをクリックします.



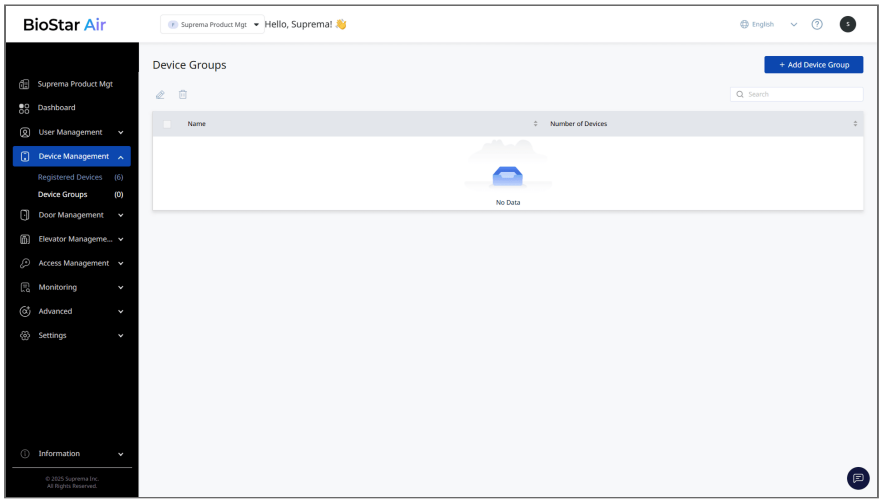
6. ポップアップメッセージが表示されたら、**OK** ボタンをクリックします.

デバイスとパネルのグループを管理する

BioStar Airでは複数のデバイスとパネルをグループにまとめて効率的に管理できます。 デバイスグループを使用すると、同じ設定を複数のデバイスに一括適用したり、特定のグループのデバイスの状態を簡単に監視できます。

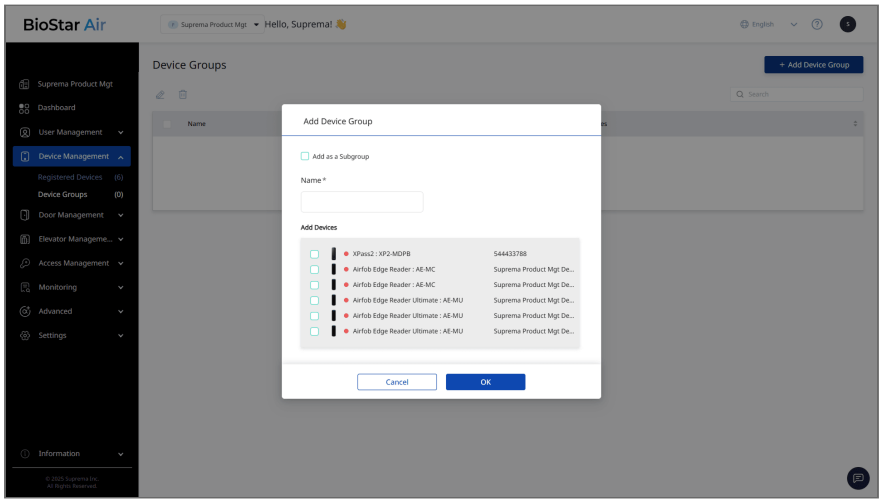
デバイスグループの追加

1. 画面左のサイドバーで **デバイス管理** → **デバイスグループ** をクリックします。



2. 画面右上の **デバイスグループの追加** ボタンをクリックします。

3. **デバイスグループの追加** ウィンドウが表示されたら、グループ名を入力します。

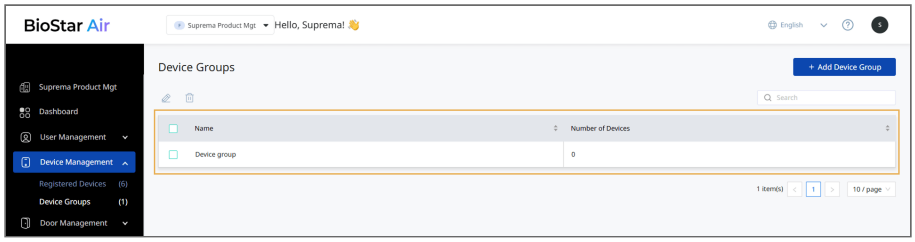


> 特定グループのサブグループとしてデバイスグループを追加するには、**サブグループとして追加** オプションをクリックし、親グループを選択します。

4. **デバイス追加** でグループに含めるデバイスを選択します。

5. すべてのデバイスを選択したら、**OK** ボタンをクリックします。

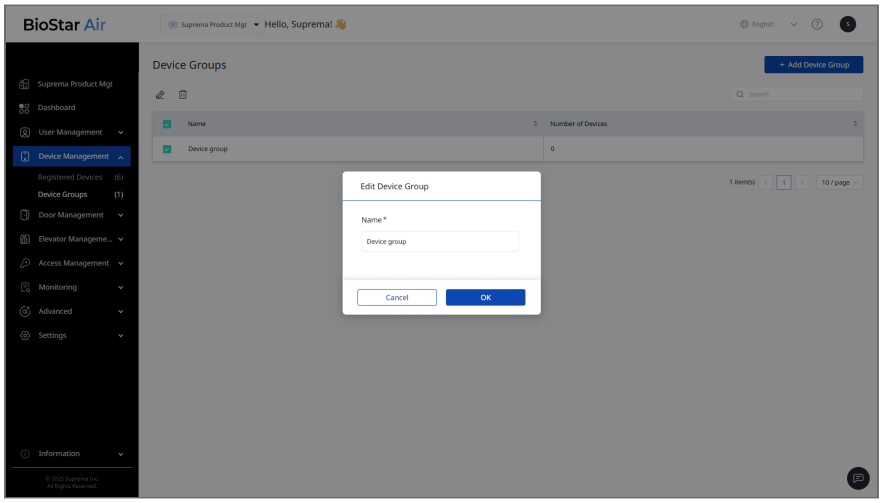
デバイスグループ一覧で、追加されたグループとそのグループに属するデバイスの数を確認できます。 デバイスグループをクリックすると、そのグループに属するデバイスを確認できます。



> **情報**
> デバイスをグループに追加したり既存のグループから削除したりする方法の詳細は、登録済みエッジデバイスの管理をご確認ください。

デバイスグループ名の変更

1. 画面左のサイドバーで **デバイス管理** → **デバイスグループ** をクリックします。
2. デバイスグループ一覧で、名前を変更するグループのチェックボックスをクリックします。
3. デバイスグループ一覧の上部にあるボタンをクリックしてください。
4. **デバイスグループ編集** ウィンドウが表示されたら、新しいグループ名を入力します。



5. 変更したグループ名を保存するには、**OK** ボタンをクリックします。

デバイスグループの削除

1. 画面左のサイドバーで **デバイス管理** → **デバイスグループ** をクリックします。
2. デバイスグループ一覧で、削除するグループのチェックボックスをクリックします。
3. デバイスグループ一覧の上部にある ボタンをクリックします。
4. 警告メッセージのウィンドウが表示されたら、**はい** をクリックします。

デバイスグループ一覧で選択したグループが削除されます。 そのグループのサブグループもすべて削除されます。 グループを削除してもデバイスは削除されません。

エッジデバイスをマスター装置として使用する

エッジデバイスをマスター装置に設定すると、XPass D2 を補助装置として接続できます。 これにより、すべての入退室制御はエッジデバイスで管理できます。 ドアに入口と出口のデバイスがある構成を、ネットワーク接続を2つ用意することなく構成できます.

この文書では、XPass 2 をマスター装置に設定し、XPass D2 を補助装置として接続する手順を段階的に説明します。 また、マスター-補助デバイス構成でサポートされる機能と制限についても説明します.

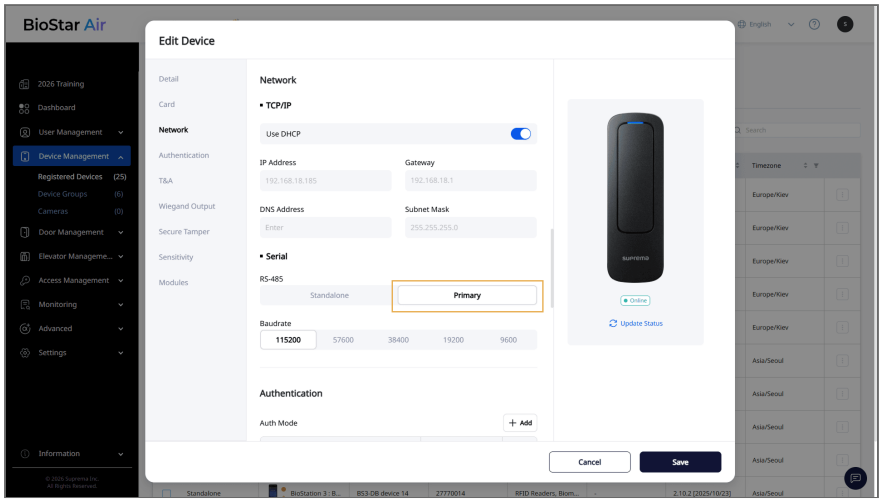
開始する前に

XPass 2をマスターデバイスに設定する前に、ファームウェアを **2.12** 以上に更新する必要があります. ファームウェアの更新に関

する詳細は ファームウェアをアップグレードする を参照してください。

XPass 2をマスターデバイスに変更する

1. 画面左のサイドバーで **デバイス管理** → **登録済みデバイス** をクリックします。
2. デバイス一覧でXPass 2をクリックします.
3. **デバイス編集** ウィンドウが表示されたら、**ネットワーク** セクションに移動します.
4. **RS-485** 設定を **プライマリ** に変更します.

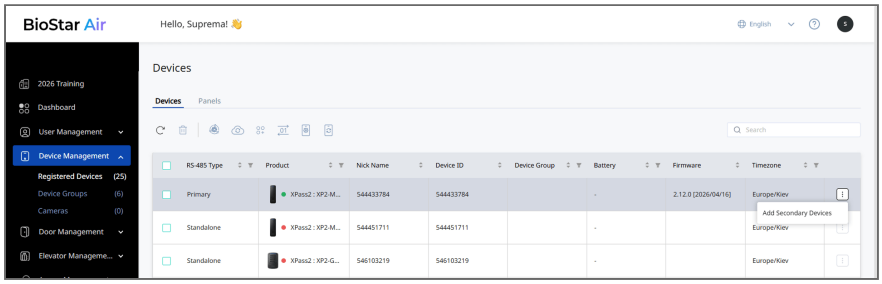


5. 変更を保存するには、下部の **保存** をクリックします。

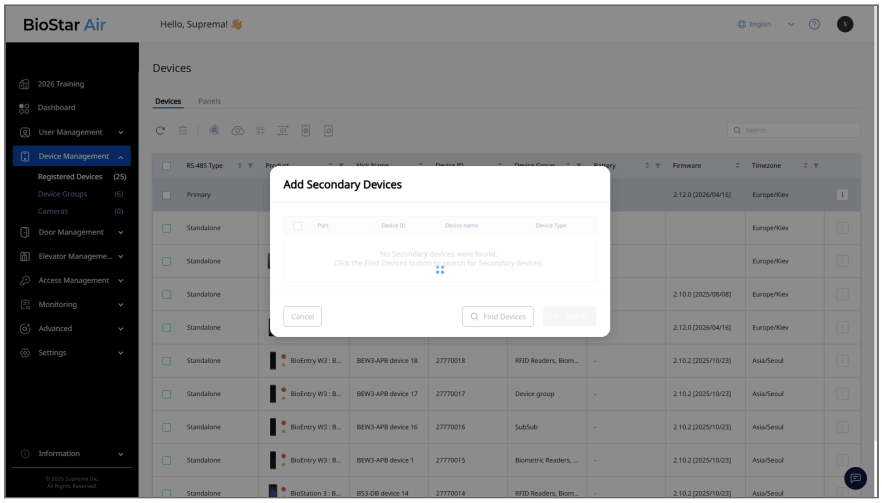
補助デバイスの追加

XPass D2 や Secure I/O 2（SIO2）などの補助デバイスを追加できます。

1. デバイス一覧でマスターに設定したXPass 2の最も右にある ⋮ ボタンをクリックします.



2. ポップアップメニューで **セカンダリデバイスの追加** をクリックすると、**セカンダリデバイスの追加** ウィンドウが表示されます。



> スレーブデバイスが見つからない場合は、**デバイスの検索** ボタンをクリックしてXPass 2に接続されたデバイスを再検索できます.

3. 接続されたスレーブデバイスが一覧に表示されたら、追加するデバイスの横にあるチェックボックスをクリックして選択します.

4. 選択が完了したら、**追加** ボタンをクリックしてください。

接続されたスレーブデバイスがXPass 2の下に階層的に表示されます. これでパネル一覧でXPass 2に接続されたすべてのデバイスを一目で確認できます.

> **情報**
>
> - XPass D2 の詳細は XPass D2 インストールガイド を参照してください。
> - マスターに設定した XPass 2 は最大 31 台の補助デバイスを割り当て可能です。
> - Secure I/O 2（SIO2）の詳細は、Secure I/O 2 インストールガイドを参照してください。

デバイスおよびパネルの設定オプションのご案内
このドキュメントは、BioStar Airのデバイスおよびパネル設定に関する参照資料です。 管理者は基本ハードウェア情報の確認、ファームウェアの更新、再起動、リセットなどの操作を実行できます。 ネットワーク、認証、カード形式、勤怠管理、Wiegand出力、感度、モジュール接続などの動作設定を構成できます。 デバイスのモデルとパネルによって使用可能な設定は異なる場合があります。

▼ AirFob Edge

詳細

詳細 セクションでは、デバイスの名前、モデル名、シリアル番号、ファームウェアバージョンなどの基本情報と、機能を操作するアクションメニューや基本設定オプションが表示されます。

基本情報

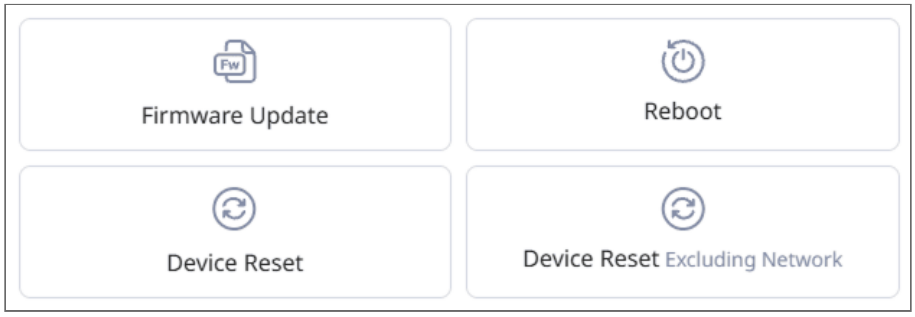
デバイスの基本情報を確認できます。 この情報は編集できません。

- **製品**：デバイスの製品名です。
- **モデル名**：デバイスのモデル名です。

- **シリアルナンバー**：デバイスのシリアル番号です。
- **ファームウェアバージョン**：デバイスにインストールされているファームウェアのバージョンです。

アクション機能

デバイスの機能を制御できる**アクション**（Action）機能です。



- **ファームウェアアップデート**：デバイスのファームウェアを最新バージョンに更新できます。
- **再起動**：デバイスに問題や異常が発生した場合、リモートで再起動できます。
- **デバイスのリセット**：デバイスに保存されているすべての設定を初期化します。 この操作を実行すると、デバイスのすべての設定とデータが削除されます。
- **デバイスのリセット ネットワーク設定を除く**：ネットワーク設定を除くすべての設定を初期化します。 この操作を実行すると、デバイスのすべての設定とデータが削除されますが、ネットワーク設定は保持されます。

基本設定

デバイスの基本設定を変更できます。

- **ニックネーム**：デバイス一覧およびログに表示されるデバイスの別名です。 直接編集できます。
- **タイムゾーン**：サイトとデバイスの時計が異なる場合にログを一貫して保つために、デバイスのタイムゾーンを設定します。サマータイム（Daylight Saving Time、DST）を適用するには、**夏時間を使用** オプションを有効にします。
- **ハンズフリ**：BLEの範囲を拡張できます。
- **QRリーダー**：デバイスにRS-485のQRリーダーが接続されていることを確認できます。

  - QRリーダーを該当デバイスと接続して使用する場合、他のRS-485デバイスを使用できません。
  - SIO2を使用する場合、その出入り口に接続されているデバイスでQRリーダーを使用できません。

- **NFC/RFカード**：カード認証を有効または無効にできます。 DESFire、Felicaカード形式をサポートしています。
- **ビープ音の設定**：入退室認証成功時の通知音を設定できます。

専用カード

Wiegandカードとして、**iClass (SE / SEOS)** と **HID Prox** のカードを選択できます。 トグルスイッチをクリックして機能を有効にした後、**専用カード**で希望するカード形式を選択してください。

情報

- この機能はデバイスによってサポートされない場合があります。
- Wiegand形式には5つの基本形式が含まれています。 **設定** → **カードフォーマット** で、さらに多くの形式を追加できます。 カスタムカード形式の設定の詳細は カスタムWiegandカード形式を設定する を参照してください。

ネットワーク

デバイスのネットワーク設定を変更できます。

- **DHCP使用**：デバイスがIPアドレスを自動的に取得するように設定できます。

  ネットワーク設定を手動で構成するには、**DHCP使用** オプションを無効にして次のフィールドに入力します。
  - **IPアドレス**
  - **ゲートウェイ**
  - **DNSアドレス**
  - **サブネットマスク**

T&A(Time & Attendance, T&A)

この機能を有効にすると、**勤怠イベント** が **イベントログ** に記録され、**T&Aレポート** に使用されます。

- **T&Aを使用**：トグルスイッチをクリックして勤怠管理機能をオンまたはオフにできます。
- **勤怠管理モード**：希望する勤怠モードを選択します。
  - **スケジュール**：設定したスケジュールに従って勤怠イベントが自動で切り替わります。 勤怠イベントに適用するスケジュールを選択できます。
  - **固定**：選択した勤怠イベントのみを使用できます。
  - **携帯**：モバイルクレデンシャルを提示する際、Suprema Passアプリで勤怠イベントを選択できます。

情報

勤怠管理の構成に関する詳細は 勤怠管理（T&A）の設定 を参照してください。

ウィーガンド出力

外部システム（例：アラームパネル）との統合のための機能です。 この機能を使用するには、**ウィーガンド出力を使用する** オプションを有効にします。

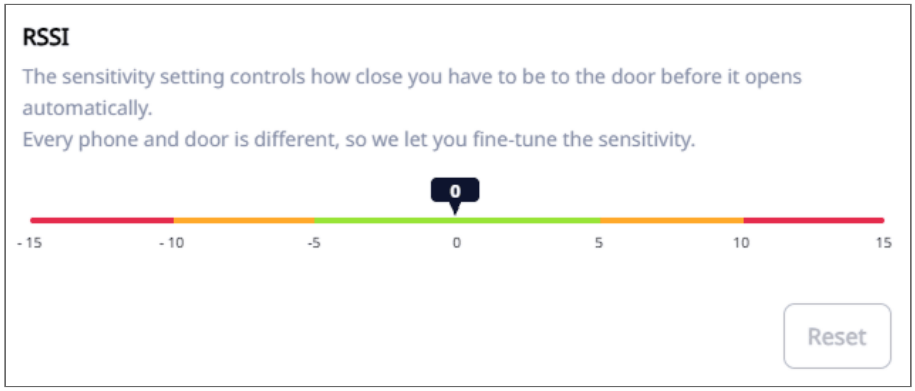
- **出力モード**：Wiegand 信号の出力モードを設定します。
  - **通常**：設定済みの Wiegand フォーマットでカードをスキャンします。
    - **フェイルコードを使用する**：エラーコードを設定でき、Wiegand を使用したカード認証に失敗した場合に送信する値を選択できます。

  - **バイパス**：Wiegand 認証に関係なく CSN を送信します。 ドア制御機能のないデバイスとして使用する場合に設定します。
- **出力情報**：認証時にデバイスへ出力する情報を選択します。
- **パルス幅**：Wiegand 信号のパルス幅を設定します。
- **パルス間隔**：Wiegand 信号のパルス間隔を設定します。
- **モバイル連続タグ**：待機時間なしで連続してモバイルカードをタグ付けできます。
- **連続タグの制限**：モバイルカードを連続でタグ付けできる最大回数を設定できます。

> **情報**
> **モバイル連続タグ** 機能は Suprema Passアプリ 2.9.0 以上でサポートされています。

感度

入退室のロックを解除するために、モバイル機器とデバイスがどれほど近くにある必要があるかを示すRSSI値を調整できます。



- 値が小さいほど、意図しない作動を防ぎます。
- 値が大きいほど、干渉が多い場所での検出が改善されます。

> **情報**
> 設定した値を初期化するには、**リセット** ボタンをクリックしてください。

モジュール

接続されている OM-120 モジュールを検出するためのオプションです。 **追加** ボタンをクリックしてモジュールを検出できます。

▼ XPass 2

詳細

詳細 セクションでは、デバイスの名前、モデル名、シリアル番号、ファームウェアバージョンなどの基本情報と、機能を操作するアクションメニューや基本設定オプションが表示されます。

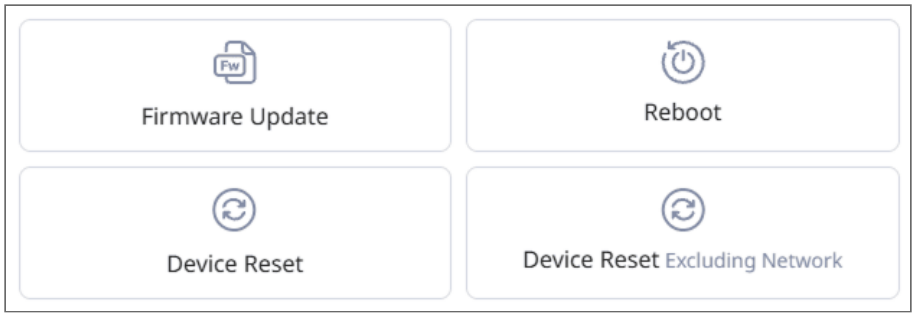
基本情報

デバイスの基本情報を確認できます。 この情報は編集できません。

- **製品**：デバイスの製品名です。
- **モデル名**：デバイスのモデル名です。
- **シリアルナンバー**：デバイスのシリアル番号です。
- **ファームウェアバージョン**：デバイスにインストールされているファームウェアのバージョンです。

アクション機能

デバイスの機能を制御できる**アクション**（Action）機能です。



- **ファームウェアアップデート**：デバイスのファームウェアを最新バージョンに更新できます。
- **再起動**：デバイスに問題や異常が発生した場合、リモートで再起動できます。
- **デバイスのリセット**：デバイスに保存されているすべての設定を初期化します。 この操作を実行すると、デバイスのすべての設定とデータが削除されます。
- **デバイスのリセット ネットワーク設定を除く**：ネットワーク設定を除くすべての設定を初期化します。 この操作を実行すると、デバイスのすべての設定とデータが削除されますが、ネットワーク設定は保持されます。

基本設定

デバイスの基本設定を変更できます。

- **ニックネーム**：デバイス一覧およびログに表示されるデバイスの別名です。 直接編集できます。
- **タイムゾーン**：サイトとデバイスの時計が異なる場合にログを一貫して保つために、デバイスのタイムゾーンを設定します。サマータイム（Daylight Saving Time、DST）を適用するには、**夏時間を使用** オプションを有効にします。
- **RFIDカード番号をPINに**：RFカード番号をキーパッドで入力して使用できます。

> この機能はキーパッドをサポートする**XP2-GKDPB**モデルのみで利用できます。

- **ハンズフリ**：BLEの範囲を拡張できます。
- **QRリーダー**：デバイスにRS-485のQRリーダーが接続されていることを確認できます。

> – QRリーダーを該当デバイスと接続して使用する場合、他のRS-485デバイスを使用できません。
> – SIO2を使用する場合、その出入り口に接続されているデバイスでQRリーダーを使用できません。

- **ビープ音の設定**：入退室認証成功時の通知音を設定できます。

- **ビデオサービス**：デバイスに接続したIPカメラのライブ映像と録画映像を確認できます。 IPカメラ接続の設定の詳細は**IPカメラのサポートおよび設定**を参照してください。

カード

カード セクションでは、カード認証に関する設定を変更できます。

NFC/RFカード

- **NFC/RFカード**：トグルスイッチをクリックしてカードによる入退室認証をオンまたはオフにできます。 カード認証に対応するカードの種類を選択してください。
  - **EM4100 (125 KHz)**
  - **Mifare Classic/Mifare DESFire/FeliCa**
- **バイトオーダー**
  - **MSB**：カードデータを処理するとき、大きいバイト単位から小さいバイト単位の順に処理し、カードシリアル番号 (CSN) を左から右へ順に保存します。
  - **LSB**：カードデータを処理するとき、小さいバイト単位から大きいバイト単位の順に処理してカードシリアル番号 (CSN) を保存します。
- **データ読み取り方法**：CSN（デフォルト）または Wiegand 形式を選択できます。

> Wiegand形式には5つの基本形式が含まれています。 **設定** → **カードフォーマット** で、さらに多くの形式を追加できます。 カスタムカード形式の設定の詳細は **カスタムWiegandカード形式を設定する** を参照してください。

専用カード

Wiegandカードとして、**iClass (SE / SEOS)** と **HID Prox** のカードを選択できます。 トグルスイッチをクリックして機能を有効にした後、**専用カード**で希望するカード形式を選択してください。

> **情報**
>
> - この機能はデバイスによってサポートされない場合があります。
> - Wiegand形式には5つの基本形式が含まれています。 **設定** → **カードフォーマット** で、さらに多くの形式を追加できます。 カスタムカード形式の設定の詳細は **カスタムWiegandカード形式を設定する** を参照してください。

ネットワーク

デバイスのネットワーク設定を変更できます。

- **DHCP使用**：デバイスがIPアドレスを自動的に取得するように設定できます。

  ネットワーク設定を手動で構成するには、**DHCP使用** オプションを無効にして次のフィールドに入力します。
  - **IPアドレス**
  - **ゲートウェイ**
  - **DNSアドレス**

  - **サブネットマスク**
- **RS-485**：装置をマスターモードに設定して、XPass D2を補助装置として追加できます。
- **ボーレート**：装置と補助装置間のシリアル通信速度を設定できます。

認証

- **認証モード**：認証方式を追加できます。 **追加** をクリックして認証方式を追加してください。
  - XP2-MDPB / XP2-GDPB：認証方式としてRFカードのみを選択できます。
  - XP2-GKDPB：認証方式としてRFカードとPINを組み合わせて選択できます。
- **認証タイムアウト**：設定した時間内にクレデンシャルを認証できない場合、認証は失敗します。

> この機能は XP2-GKDPB モデルでのみ利用できます。

> **情報**
> 選択したスケジュールに応じて認証方式を個別に設定できます。 例えば、勤務時間中はカード認証のみを許可し、勤務時間外はカードとPINの組み合わせを許可できます。

T&A(Time & Attendance, T&A)

この機能を有効にすると、**勤怠イベント** が **イベントログ** に記録され、**T&Aレポート** に使用されます。

- **T&Aを使用**：トグルスイッチをクリックして勤怠管理機能をオンまたはオフにできます。
- **勤怠管理モード**：希望する勤怠モードを選択します。
  - **スケジュール**：設定したスケジュールに従って勤怠イベントが自動で切り替わります。 勤怠イベントに適用するスケジュールを選択できます。
  - **固定**：選択した勤怠イベントのみを使用できます。
  - **携帯**：モバイルクレデンシャルを提示する際、Suprema Passアプリで勤怠イベントを選択できます。

> **情報**
> 勤怠管理の構成に関する詳細は 勤怠管理（T&A）の設定 を参照してください。

ウィーガンド出力

外部システム（例：アラームパネル）との統合のための機能です。 この機能を使用するには、**ウィーガンド出力を使用する** オプションを有効にします。

- **出力モード**：Wiegand 信号の出力モードを設定します。

  - **通常**：設定済みの Wiegand フォーマットでカードをスキャンします。
    - **フェイルコードを使用する**：エラーコードを設定でき、Wiegand を使用したカード認証に失敗した場合に送信する値を選択できます。
  - **バイパス**：Wiegand 認証に関係なく CSN を送信します。 ドア制御機能のないデバイスとして使用する場合に設定します。
- **出力情報**：認証時にデバイスへ出力する情報を選択します。
- **パルス幅**：Wiegand 信号のパルス幅を設定します。
- **パルス間隔**：Wiegand 信号のパルス間隔を設定します。
- **モバイル連続タグ**：待機時間なしで連続してモバイルカードをタグ付けできます。
- **連続タグの制限**：モバイルカードを連続でタグ付けできる最大回数を設定できます。

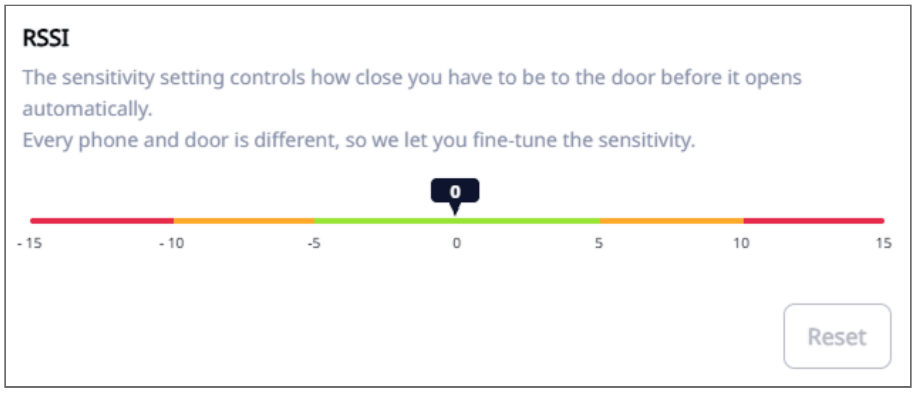
> **情報**
> **モバイル連続タグ** 機能は Suprema Passアプリ 2.9.0 以上でサポートされています。

セキュアタンパー

デバイスでタンパーイベントが発生した場合、保存されている**全ユーザー情報**、**全ログ**、**セキュリティキー**を削除するように設定できます。

感度

入退室のロックを解除するために、モバイル機器とデバイスがどれほど近くにある必要があるかを示すRSSI値を調整できます。



- 値が小さいほど、意図しない作動を防ぎます。
- 値が大きいほど、干渉が多い場所での検出が改善されます。

> **情報**
> 設定した値を初期化するには、**リセット** ボタンをクリックしてください。

モジュール

接続されている OM-120 モジュールを検出するためのオプションです。 **追加** ボタンをクリックしてモジュールを検出できます。

▼ XPass D2

詳細

詳細 セクションでは、デバイスの名前、モデル名、シリアル番号、ファームウェアバージョンなどの基本情報と、機能を操作するアクションメニューや基本設定オプションが表示されます。

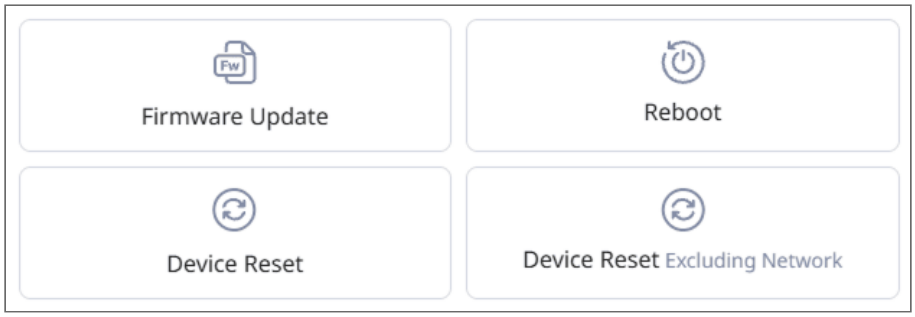
基本情報

デバイスの基本情報を確認できます。 この情報は編集できません。

- **製品**：デバイスの製品名です。
- **モデル名**：デバイスのモデル名です。
- **シリアルナンバー**：デバイスのシリアル番号です。
- **ファームウェアバージョン**：デバイスにインストールされているファームウェアのバージョンです。

アクション機能

デバイスの機能を制御できる**アクション**（Action）機能です。



- **ファームウェアアップデート**：デバイスのファームウェアを最新バージョンに更新できます。
- **再起動**：デバイスに問題や異常が発生した場合、リモートで再起動できます。
- **デバイスのリセット**：デバイスに保存されているすべての設定を初期化します。 この操作を実行すると、デバイスのすべての設定とデータが削除されます。
- **デバイスのリセット ネットワーク設定を除く**：ネットワーク設定を除くすべての設定を初期化します。 この操作を実行すると、デバイスのすべての設定とデータが削除されますが、ネットワーク設定は保持されます。

基本設定

デバイスの基本設定を変更できます。

- **ニックネーム**：デバイス一覧およびログに表示されるデバイスの別名です。 直接編集できます。
- **ハンズフリ**：BLEの範囲を拡張できます。
- **ビープ音の設定**：入退室認証成功時の通知音を設定できます。

カード

カード セクションでは、カード認証に関する設定を変更できます。

NFC/RFカード

- **NFC/RFカード**：トグルスイッチをクリックしてカードによる入退室認証をオンまたはオフにできます。 カード認証に対応するカードの種類を選択してください。
  - **EM4100 (125 KHz)**
  - **Mifare Classic/Mifare DESFire/FeliCa**
- **バイトオーダー**
  - **MSB**：カードデータを処理するとき、大きいバイト単位から小さいバイト単位の順に処理し、カードシリアル番号 (CSN) を左から右へ順に保存します。
  - **LSB**：カードデータを処理するとき、小さいバイト単位から大きいバイト単位の順に処理してカードシリアル番号 (CSN) を保存します。
- **データ読み取り方法**：CSN（デフォルト）または Wiegand 形式を選択できます。

> Wiegand形式には5つの基本形式が含まれています。 **設定** → **カードフォーマット** で、さらに多くの形式を追加できます。 カスタムカード形式の設定の詳細は カスタムWiegandカード形式を設定する を参照してください。

専用カード

Wiegandカードとして、**iClass (SE / SEOS)** と **HID Prox** のカードを選択できます。 トグルスイッチをクリックして機能を有効にした後、**専用カード**で希望するカード形式を選択してください。

> **情報**
>
> - この機能はデバイスによってサポートされない場合があります。
> - Wiegand形式には5つの基本形式が含まれています。 **設定** → **カードフォーマット** で、さらに多くの形式を追加できます。 カスタムカード形式の設定の詳細は カスタムWiegandカード形式を設定する を参照してください。

認証

- **認証モード**：認証方式を追加できます。 **追加** をクリックして認証方式を追加してください。 認証方式としてRFカードのみを選択できます。

> **情報**
>
> 選択したスケジュールに応じて認証方式を個別に設定できます。 例えば、勤務時間中はカード認証のみを許可し、勤務時間外はカードとPINの組み合わせを許可できます。

T&A(Time & Attendance, T&A)

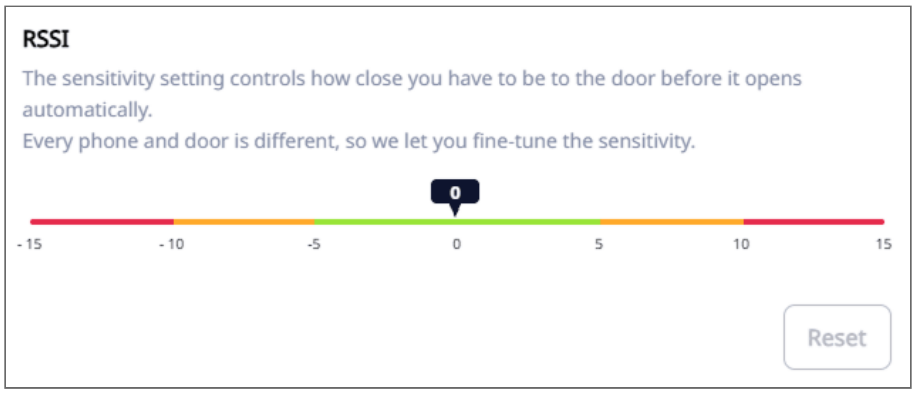
この機能を有効にすると、**勤怠イベント** が **イベントログ** に記録され、**T&Aレポート** に使用されます。

- **T&Aを使用**：トグルスイッチをクリックして勤怠管理機能をオンまたはオフにできます。
- **勤怠管理モード**：希望する勤怠モードを選択します。
  - **スケジュール**：設定したスケジュールに従って勤怠イベントが自動で切り替わります。 勤怠イベントに適用するスケジュールを選択できます。
  - **固定**：選択した勤怠イベントのみを使用できます。

> **情報**
> 勤怠管理の構成に関する詳細は 勤怠管理（T&A）の設定 を参照してください。

感度

入退室のロックを解除するために、モバイル機器とデバイスがどれほど近くにある必要があるかを示すRSSI値を調整できます。



- 値が小さいほど、意図しない作動を防ぎます。
- 値が大きいほど、干渉が多い場所での検出が改善されます。

> **情報**
> 設定した値を初期化するには、**リセット** ボタンをクリックしてください。

▼ X-Station 2

詳細

詳細 セクションでは、デバイスの名前、モデル名、シリアル番号、ファームウェアバージョンなどの基本情報と、機能を操作するアクションメニューや基本設定オプションが表示されます。

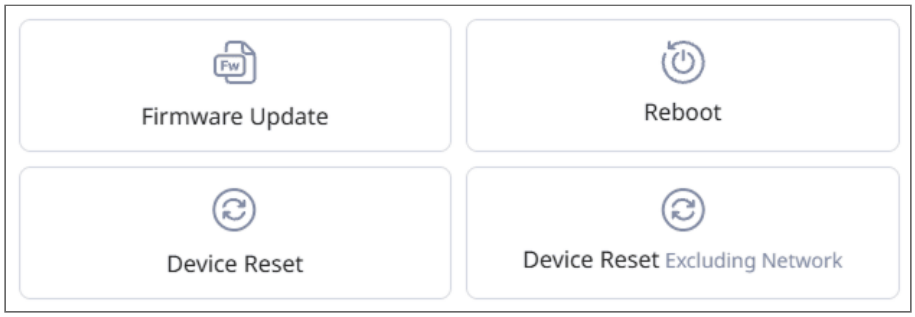
基本情報

デバイスの基本情報を確認できます。 この情報は編集できません。

- **製品**：デバイスの製品名です。
- **モデル名**：デバイスのモデル名です。
- **シリアルナンバー**：デバイスのシリアル番号です。
- **ファームウェアバージョン**：デバイスにインストールされているファームウェアのバージョンです。

アクション機能

デバイスの機能を制御できる**アクション**（Action）機能です。



- **ファームウェアアップデート**：デバイスのファームウェアを最新バージョンに更新できます。
- **再起動**：デバイスに問題や異常が発生した場合、リモートで再起動できます。
- **デバイスのリセット**：デバイスに保存されているすべての設定を初期化します。 この操作を実行すると、デバイスのすべての設定とデータが削除されます。
- **デバイスのリセット ネットワーク設定を除く**：ネットワーク設定を除くすべての設定を初期化します。 この操作を実行すると、デバイスのすべての設定とデータが削除されますが、ネットワーク設定は保持されます。

基本設定

デバイスの基本設定を変更できます。

- **ニックネーム**：デバイス一覧およびログに表示されるデバイスの別名です。 直接編集できます。
- **タイムゾーン**：サイトとデバイスの時計が異なる場合にログを一貫して保つために、デバイスのタイムゾーンを設定します。 サマータイム（Daylight Saving Time、DST）を適用するには、**夏時間を使用** オプションを有効にします。
- **ハンズフリ**：BLEの範囲を拡張できます。
- **QRリーダー**：デバイスにRS-485のQRリーダーが接続されていることを確認できます。

  - QRリーダーを該当デバイスと接続して使用する場合、他のRS-485デバイスを使用できません。
  - SIO2を使用する場合、その出入り口に接続されているデバイスでQRリーダーを使用できません。

- **NFC/RFカード**：カード認証を有効または無効にできます。 DESFire、Felicaカード形式をサポートしています。

専用カード

Wiegandカードとして、**iClass (SE / SEOS)** と **HID Prox** のカードを選択できます。 トグルスイッチをクリックして機能を有効にした後、**専用カード**で希望するカード形式を選択してください。

情報

- この機能はデバイスによってサポートされない場合があります。
- Wiegand形式には5つの基本形式が含まれています。 **設定** → **カードフォーマット** で、さらに多くの形式を追加できます。 カスタムカード形式の設定の詳細は カスタムWiegandカード形式を設定する を参照してください。

ネットワーク

デバイスのネットワーク設定を変更できます。

- **DHCP使用**：デバイスがIPアドレスを自動的に取得するように設定できます。

  ネットワーク設定を手動で構成するには、**DHCP使用** オプションを無効にして次のフィールドに入力します。
  - **IPアドレス**
  - **ゲートウェイ**
  - **DNSアドレス**
  - **サブネットマスク**

T&A(Time & Attendance, T&A)

この機能を有効にすると、**勤怠イベント** が **イベントログ** に記録され、**T&Aレポート** に使用されます。

- **T&Aを使用**：トグルスイッチをクリックして勤怠管理機能をオンまたはオフにできます。
- **勤怠管理モード**：希望する勤怠モードを選択します。
  - **スケジュール**：設定したスケジュールに従って勤怠イベントが自動で切り替わります。 勤怠イベントに適用するスケジュールを選択できます。
  - **固定**：選択した勤怠イベントのみを使用できます。
  - **携帯**：モバイルクレデンシャルを提示する際、Suprema Passアプリで勤怠イベントを選択できます。

> **情報**
> 勤怠管理の構成に関する詳細は 勤怠管理（T&A）の設定 を参照してください。

感度

入退室のロックを解除するために、モバイル機器とデバイスがどれほど近くにある必要があるかを示すRSSI値を調整できます。



- 値が小さいほど、意図しない作動を防ぎます。
- 値が大きいほど、干渉が多い場所での検出が改善されます。

> **情報**
> 設定した値を初期化するには、**リセット** ボタンをクリックしてください。

モジュール

接続されている OM-120 モジュールを検出するためのオプションです。 **追加** ボタンをクリックしてモジュールを検出できます。

▼ BioEntry W3

詳細

詳細 セクションでは、デバイスの名前、モデル名、シリアル番号、ファームウェアバージョンなどの基本情報と、機能を操作するアクションメニューや基本設定オプションが表示されます。

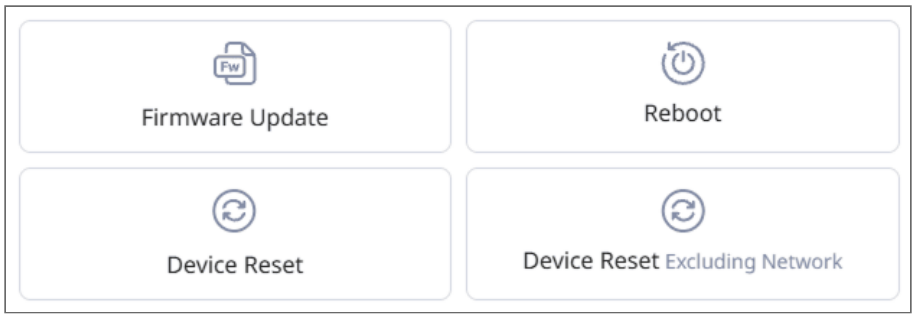
基本情報

デバイスの基本情報を確認できます。 この情報は編集できません。

- **製品**：デバイスの製品名です。
- **モデル名**：デバイスのモデル名です。
- **シリアルナンバー**：デバイスのシリアル番号です。
- **ファームウェアバージョン**：デバイスにインストールされているファームウェアのバージョンです。

アクション機能

デバイスの機能を制御できる**アクション**（Action）機能です。



- **ファームウェアアップデート**：デバイスのファームウェアを最新バージョンに更新できます。
- **再起動**：デバイスに問題や異常が発生した場合、リモートで再起動できます。
- **デバイスのリセット**：デバイスに保存されているすべての設定を初期化します。 この操作を実行すると、デバイスのすべての設定とデータが削除されます。
- **デバイスのリセット ネットワーク設定を除く**：ネットワーク設定を除くすべての設定を初期化します。 この操作を実行すると、デバイスのすべての設定とデータが削除されますが、ネットワーク設定は保持されます。

基本設定

デバイスの基本設定を変更できます。

- **ニックネーム**：デバイス一覧およびログに表示されるデバイスの別名です。 直接編集できます。

- **タイムゾーン**：サイトとデバイスの時計が異なる場合にログを一貫して保つために、デバイスのタイムゾーンを設定します。サマータイム（Daylight Saving Time、DST）を適用するには、**夏時間を使用** オプションを有効にします。
- **ハンズフリ**：BLEの範囲を拡張できます。

カード

カード セクションでは、カード認証に関する設定を変更できます。

NFC/RFカード

- **NFC/RFカード**：トグルスイッチをクリックしてカードによる入退室認証をオンまたはオフにできます。 カード認証に対応するカードの種類を選択してください。
  - **EM4100 (125 KHz)**
  - **Mifare Classic/Mifare DESFire/FeliCa**
- **バイトオーダー**
  - **MSB**：カードデータを処理するとき、大きいバイト単位から小さいバイト単位の順に処理し、カードシリアル番号 (CSN) を左から右へ順に保存します。
  - **LSB**：カードデータを処理するとき、小さいバイト単位から大きいバイト単位の順に処理してカードシリアル番号 (CSN) を保存します。
- **データ読み取り方法**：CSN（デフォルト）または Wiegand 形式を選択できます。

> Wiegand形式には5つの基本形式が含まれています。 **設定** → **カードフォーマット** で、さらに多くの形式を追加できます。 カスタムカード形式の設定の詳細は カスタムWiegandカード形式を設定する を参照してください。

専用カード

Wiegandカードとして、**iClass (SE / SEOS)** と **HID Prox** のカードを選択できます。 トグルスイッチをクリックして機能を有効にした後、**専用カード**で希望するカード形式を選択してください。

> **情報**
>
> - この機能はデバイスによってサポートされない場合があります。
> - Wiegand形式には5つの基本形式が含まれています。 **設定** → **カードフォーマット** で、さらに多くの形式を追加できます。 カスタムカード形式の設定の詳細は カスタムWiegandカード形式を設定する を参照してください。

ネットワーク

デバイスのネットワーク設定を変更できます。

- **DHCP使用**：デバイスがIPアドレスを自動的に取得するように設定できます。

  ネットワーク設定を手動で構成するには、**DHCP使用** オプションを無効にして次のフィールドに入力します。
  - **IPアドレス**
  - **ゲートウェイ**

- **DNSアドレス**
- **サブネットマスク**

認証

- **認証モード**：認証方式を追加できます。 **追加** をクリックして認証方式を追加してください。 認証方式としてRFカードと顔認証を組み合わせて選択できます。

> **情報**
> 選択したスケジュールに応じて認証方式を個別に設定できます。 例えば、勤務時間中はカード認証のみを許可し、勤務時間外はカードとPINの組み合わせを許可できます。

顔

安全

- **偽造検出**：写真などの偽造顔を用いたユーザー認証を防止できます。
- **重複チェック**：顔を登録する際に重複登録をチェックできます。

検出

- **モーション センサーの感度**：デバイス周囲の動きを検知する感度を設定します。
- **最大ヘッド ポーズ角度**：許容される顔の最大回転角度を設定します。
- **広範囲検索**：カメラ映像全体で顔を認識する範囲を広げることができます。
- **検出距離 (cm)**：顔を認識する最小および最大距離を設定します。
- **登録時間 秒**：ユーザーの顔を登録する際、設定した時間内に登録できないと顔登録がキャンセルされます。

マスク検出

マスク検出機能を設定するには、**マスク検出** オプションを有効にします。

- **マスク検出レベル**：マスク検出感度を選択します。
- **マスク検出に失敗した場合**
  - **アクセスを拒否**：マスク未着用のユーザーは認証が拒否され、マスク未着用イベントがログに記録されます。
  - **ログイン後にアクセスを許可**：マスク未着用のユーザーも認証できますが、マスク未着用イベントがログに記録されます。
- **マスク チェック**
  - **アクセス後**：認証を実行した後にユーザーのマスク着用を確認するか、体温を測定します。
  - **アクセス前**：ユーザーのマスク着用を確認するか体温を測定した後に認証を実行します。 この場合、マスクを着用していない、または基準温度を超えているユーザーは認証できません。
  - **アクセスなし**：デバイスをマスク着用の確認または体温測定専用としてのみ使用できます。 この場合、認証に関係なく、マスクを着用しているか基準温度以下のユーザーはすべて入場できます。
- **デバイスのカメラでQRコードまたはバーコードを認証**：デバイスのカメラによるQR/バーコード認証の使用可否を設定でき

ます。

- **QRコードでカード番号を認証**：付与した CSN カードまたは Wiegand カードと同じデータを持つ QR コードで認証できるように設定できます。 この機能を使用するには、**デバイスのカメラでQRコードまたはバーコードを認証** オプションを有効にする必要があります。

> **情報**
> 顔以外のクレデンシャルを使用する際は、主に「前」と「後」が重要です。

T&A(Time & Attendance, T&A)

この機能を有効にすると、**勤怠イベント** が **イベントログ** に記録され、**T&Aレポート** に使用されます。

- **T&Aを使用**：トグルスイッチをクリックして勤怠管理機能をオンまたはオフにできます。
- **勤怠管理モード**：希望する勤怠モードを選択します。
  - **スケジュール**：設定したスケジュールに従って勤怠イベントが自動で切り替わります。 勤怠イベントに適用するスケジュールを選択できます。
  - **固定**：選択した勤怠イベントのみを使用できます。

> **情報**
> 勤怠管理の構成に関する詳細は 勤怠管理（T&A）の設定 を参照してください。

ウィーガンド出力

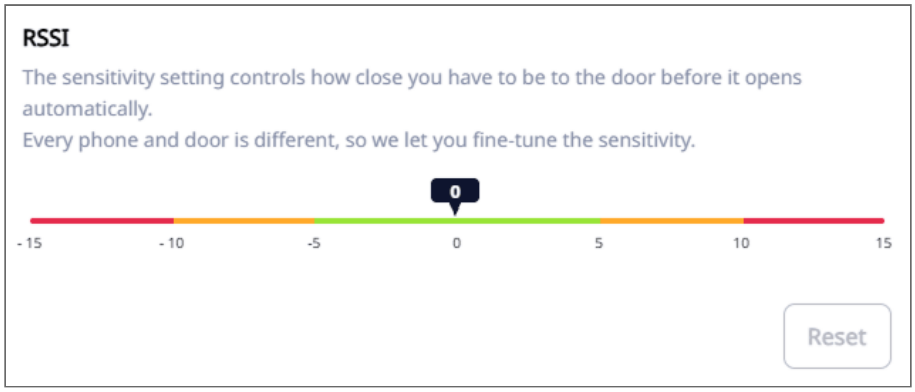
外部システム（例：アラームパネル）との統合のための機能です。 この機能を使用するには、**ウィーガンド出力を使用する** オプションを有効にします。

- **出力モード**：Wiegand 信号の出力モードを設定します。
  - **通常**：設定済みの Wiegand フォーマットでカードをスキャンします。
    - **フェイルコードを使用する**：エラーコードを設定でき、Wiegand を使用したカード認証に失敗した場合に送信する値を選択できます。
  - **バイパス**：Wiegand 認証に関係なく CSN を送信します。 ドア制御機能のないデバイスとして使用する場合に設定します。
- **出力情報**：認証時にデバイスへ出力する情報を選択します。
- **パルス幅**：Wiegand 信号のパルス幅を設定します。
- **パルス間隔**：Wiegand 信号のパルス間隔を設定します。
- **モバイル連続タグ**：待機時間なしで連続してモバイルカードをタグ付けできます。
- **連続タグの制限**：モバイルカードを連続でタグ付けできる最大回数を設定できます。

> **情報**
> **モバイル連続タグ** 機能は Suprema Passアプリ 2.9.0 以上でサポートされています。

感度

入退室のロックを解除するために、モバイル機器とデバイスがどれほど近くにある必要があるかを示すRSSI値を調整できます。



- 値が小さいほど、意図しない作動を防ぎます。
- 値が大きいほど、干渉が多い場所での検出が改善されます。

> **情報**
> 設定した値を初期化するには、**リセット** ボタンをクリックしてください。

▼ BioStation 3

詳細

詳細 セクションでは、デバイスの名前、モデル名、シリアル番号、ファームウェアバージョンなどの基本情報と、機能を操作するアクションメニューや基本設定オプションが表示されます。

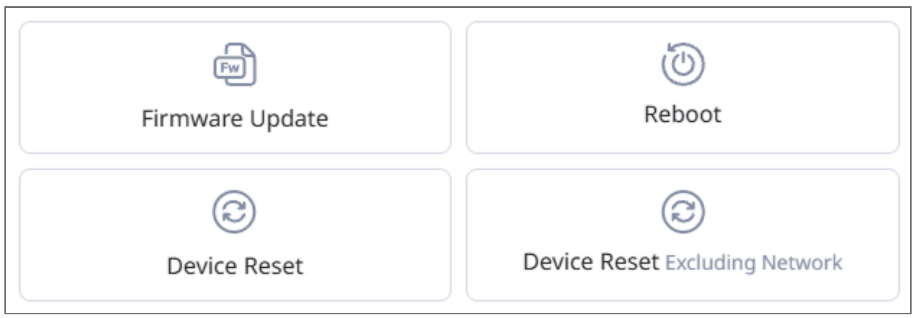
基本情報

デバイスの基本情報を確認できます。 この情報は編集できません。

- **製品**：デバイスの製品名です。
- **モデル名**：デバイスのモデル名です。
- **シリアルナンバー**：デバイスのシリアル番号です。
- **ファームウェアバージョン**：デバイスにインストールされているファームウェアのバージョンです。

アクション機能

デバイスの機能を制御できる**アクション**（Action）機能です。



- **ファームウェアアップデート**：デバイスのファームウェアを最新バージョンに更新できます。
- **再起動**：デバイスに問題や異常が発生した場合、リモートで再起動できます。
- **デバイスのリセット**：デバイスに保存されているすべての設定を初期化します。 この操作を実行すると、デバイスのすべての設定とデータが削除されます。
- **デバイスのリセット ネットワーク設定を除く**：ネットワーク設定を除くすべての設定を初期化します。 この操作を実行すると、デバイスのすべての設定とデータが削除されますが、ネットワーク設定は保持されます。

基本設定

デバイスの基本設定を変更できます。

- **ニックネーム**：デバイス一覧およびログに表示されるデバイスの別名です。 直接編集できます。
- **タイムゾーン**：サイトとデバイスの時計が異なる場合にログを一貫して保つために、デバイスのタイムゾーンを設定します。 サマータイム（Daylight Saving Time、DST）を適用するには、**夏時間を使用** オプションを有効にします。
- **ハンズフリ**：BLEの範囲を拡張できます。
- **ビデオサービス**：デバイスに接続したIPカメラのライブ映像と録画映像を確認できます。 IPカメラ接続の設定の詳細はIPカメラのサポートおよび設定を参照してください。

カード

カード セクションでは、カード認証に関する設定を変更できます。

NFC/RFカード

- **NFC/RFカード**：トグルスイッチをクリックしてカードによる入退室認証をオンまたはオフにできます。 カード認証に対応するカードの種類を選択してください。
  - **EM4100 (125 KHz)**
  - **Mifare Classic/Mifare DESFire/FeliCa**
- **バイトオーダー**
  - **MSB**：カードデータを処理するとき、大きいバイト単位から小さいバイト単位の順に処理し、カードシリアル番号 (CSN) を左から右へ順に保存します。
  - **LSB**：カードデータを処理するとき、小さいバイト単位から大きいバイト単位の順に処理してカードシリアル番号 (CSN) を保存します。
- **データ読み取り方法**：CSN（デフォルト）または Wiegand 形式を選択できます。

> Wiegand形式には5つの基本形式が含まれています。 **設定** → **カードフォーマット** で、さらに多くの形式を追加できます。 カスタムカード形式の設定の詳細は カスタムWiegandカード形式を設定する を参照してください。

専用カード

Wiegandカードとして、**iClass (SE / SEOS)** と **HID Prox** のカードを選択できます。 トグルスイッチをクリックして機能を有効にした後、**専用カード**で希望するカード形式を選択してください。

情報

- この機能はデバイスによってサポートされない場合があります。
- Wiegand形式には5つの基本形式が含まれています。 **設定** → **カードフォーマット** で、さらに多くの形式を追加できます。 カスタムカード形式の設定の詳細は カスタムWiegandカード形式を設定する を参照してください。

ネットワーク

デバイスのネットワーク設定を変更できます。

- **DHCP使用**：デバイスがIPアドレスを自動的に取得するように設定できます。

  ネットワーク設定を手動で構成するには、**DHCP使用** オプションを無効にして次のフィールドに入力します。
  - **IPアドレス**
  - **ゲートウェイ**
  - **DNSアドレス**
  - **サブネットマスク**

認証

- **認証モード**：認証方式を追加できます。 **追加** をクリックして認証方式を追加してください。 認証方式として、RFカード、顔認証、ID、PINを組み合わせて選択できます。
- **ユーザー名を表示** / **ユーザーIDを表示**：認証画面にユーザー名またはIDを表示するかどうかを選択できます。 画面に表示しないように設定するには、**非表示** オプションを選択します。
- **認証タイムアウト**：設定した時間内にクレデンシャルを認証できない場合、認証は失敗します。

情報

選択したスケジュールに応じて認証方式を個別に設定できます。 例えば、勤務時間中はカード認証のみを許可し、勤務時間外はカードとPINの組み合わせを許可できます。

顔

安全

- **偽造検出**：写真などの偽造顔を用いたユーザー認証を防止できます。
- **重複チェック**：顔を登録する際に重複登録をチェックできます。

検出

- **モーション センサーの感度**：デバイス周囲の動きを検知する感度を設定します。

- **最大ヘッド ポーズ角度**：許容される顔の最大回転角度を設定します。
- **広範囲検索**：カメラ映像全体で顔を認識する範囲を広げることができます。
- **検出距離 (cm)**：顔を認識する最小および最大距離を設定します。
- **登録時間 秒**：ユーザーの顔を登録する際、設定した時間内に登録できないと顔登録がキャンセルされます。

マスク検出

マスク検出機能を設定するには、**マスク検出** オプションを有効にします。

- **マスク検出レベル**：マスク検出感度を選択します。
- **マスク検出に失敗した場合**
  - **アクセスを拒否**：マスク未着用のユーザーは認証が拒否され、マスク未着用イベントがログに記録されます。
  - **ログイン後にアクセスを許可**：マスク未着用のユーザーも認証できますが、マスク未着用イベントがログに記録されます。
- **マスク チェック**
  - **アクセス後**：認証を実行した後にユーザーのマスク着用を確認するか、体温を測定します。
  - **アクセス前**：ユーザーのマスク着用を確認するか体温を測定した後に認証を実行します。 この場合、マスクを着用していない、または基準温度を超えているユーザーは認証できません。
  - **アクセスなし**：デバイスをマスク着用の確認または体温測定専用としてのみ使用できます。 この場合、認証に関係なく、マスクを着用しているか基準温度以下のユーザーはすべて入場できます。
- **デバイスのカメラでQRコードまたはバーコードを認証**：デバイスのカメラによるQR/バーコード認証の使用可否を設定できます。
- **QRコードでカード番号を認証**：付与した CSN カードまたは Wiegand カードと同じデータを持つ QR コードで認証できるように設定できます。 この機能を使用するには、**デバイスのカメラでQRコードまたはバーコードを認証** オプションを有効にする必要があります。

> **情報**
> 顔以外のクレデンシャルを使用する際は、主に「前」と「後」が重要です。

T&A(Time & Attendance, T&A)

この機能を有効にすると、**勤怠イベント** が **イベントログ** に記録され、**T&Aレポート** に使用されます。

- **T&Aを使用**：トグルスイッチをクリックして勤怠管理機能をオンまたはオフにできます。
- **勤怠管理モード**：希望する勤怠モードを選択します。
  - **手動**：画面に勤怠キーを表示し、認証時にユーザーが勤怠イベントを選択できます。

    > **T&A が必要です**オプションを有効にすると、ユーザーが認証する際に必ず勤怠イベントを登録する必要があります。

  - **スケジュール**：設定したスケジュールに従って勤怠イベントが自動で切り替わります。 勤怠イベントに適用するスケジュールを選択できます。
  - **手動固定**：ユーザーが最後に使用した勤怠イベントを継続して使用できます。
  - **固定**：選択した勤怠イベントのみを使用できます。

> **情報**
> 勤怠管理の構成に関する詳細は 勤怠管理（T&A）の設定 を参照してください。

ディスプレイとサウンド

ディスプレイ

- **スクリーンセーバーを使用**：デバイスを使用していないときに LCD 画面の明るさを下げて不要な電力消費を削減できます。
- **常時点灯バックライト**：画面の照明を常にオンにするか、無効化後に暗くなるように設定できます。
- **バックライトタイムアウト**：画面バックライトが自動でオフになるまでの時間を設定します。
- **言語**：デバイスの画面に表示する言語を設定できます。
- **ホーム画面**：デバイスのホーム画面の背景に表示する項目を設定します。
  - **通常表示**：既定の画像をホーム画面に表示します。
  - **ロゴ**：ユーザーが登録した画像をデバイスのホーム画面に表示できます。
  - **お知らせ**：管理者が入力した内容をホーム画面に表示できます。

> **アップデート** ボタンをクリックして保存すると、画像や通知が編集画面に表示されませんが、デバイスには引き続き表示されます。

サウンド

- **音声指示を使用**：通知音の代わりに音声ガイダンスを使用できます。
- **デバイス音量**：デバイスから出る音量を調整できます。
- **インターホンスピーカー音量** / **インターホンマイク音量**：IP インターホン機能を使用するときにデバイスから出力または入力される音量を設定できます。

ウィーガンド出力

外部システム（例：アラームパネル）との統合のための機能です。 この機能を使用するには、**ウィーガンド出力を使用する** オプションを有効にします。

- **出力モード**：Wiegand 信号の出力モードを設定します。
  - **通常**：設定済みの Wiegand フォーマットでカードをスキャンします。
    - **フェイルコードを使用する**：エラーコードを設定でき、Wiegand を使用したカード認証に失敗した場合に送信する値を選択できます。
  - **バイパス**：Wiegand 認証に関係なく CSN を送信します。 ドア制御機能のないデバイスとして使用する場合に設定します。
- **出力情報**：認証時にデバイスへ出力する情報を選択します。
- **パルス幅**：Wiegand 信号のパルス幅を設定します。
- **パルス間隔**：Wiegand 信号のパルス間隔を設定します。
- **モバイル連続タグ**：待機時間なしで連続してモバイルカードをタグ付けできます。

- **連続タグの制限**：モバイルカードを連続でタグ付けできる最大回数を設定できます。

> **情報**
> **モバイル連続タグ** 機能は Suprema Passアプリ 2.9.0 以上でサポートされています。

インターコム

- **インターコムを使用する**：IPインターホン機能を有効または無効にできます。
- **SIPサーバートランスポート**：IPインターホンのSIPサーバー設定の際にSIPトランスポート方式を選択してください。
- **SIPサーバーアドレス**：SIPサーバーのアドレスを入力してください。
- **SIPサーバーポート**：SIPサーバーのポートを入力してください。
- **登録期間**：登録維持時間を入力します。 デバイスは登録維持時間が終了するたびにSIPサーバーへの登録を試みます。
- **SIPユーザー名**：SIPアカウントのユーザー名を入力してください。
- **パスワード**：SIPアカウントのパスワードを入力してください。
- **認証ID**：SIPアカウントの認証IDを入力してください。
- **発信プロキシサーバー**：別の（アウトバウンド）プロキシサーバー経由でSIPサービスを使用できます。
- **内線番号**：内線番号を追加または編集できます。
- **ビデオ解像度**：IPインターホン使用時に出力される映像の解像度を選択してください。
- **ドア開閉ボタン**：通話中にデバイスのドアを開けるためのボタンを指定してください。

セキュアタンパー

デバイスでタンパーイベントが発生した場合、保存されている**全ユーザー情報**、**全ログ**、**セキュリティキー**を削除するように設定できます。

RTSP

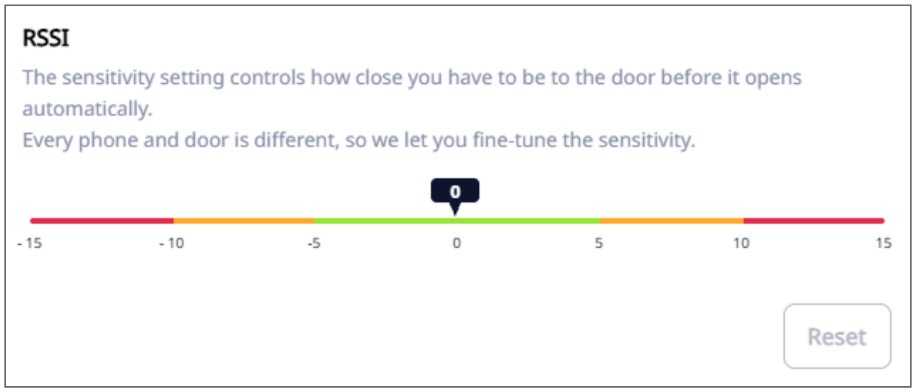
Real Time Streaming Protocol（RTSP）ストリーミングの詳細項目を設定できます。 デバイスのカメラを通じてリアルタイムで映像を配信できます。

- **RTSPを使用**：RTSPストリーミング機能をオンまたはオフに切り替えます。
- **アドレス**：RTSPサーバーのアドレスです。
- **ポート**：RTSPサーバーのポートを入力します。
- **ID** / **パスワード**：RTSPサーバーのIDとパスワードを入力します。
- **RTSPビデオ解像度**：RTSP 使用時に出力される映像の解像度を選択します。

> **情報**
> RTSPストリーミング機能は BioStation 3 デバイスでのみサポートされます。

感度

入退室のロックを解除するために、モバイル機器とデバイスがどれほど近くにある必要があるかを示すRSSI値を調整できます。



- 値が小さいほど、意図しない作動を防ぎます。
- 値が大きいほど、干渉が多い場所での検出が改善されます。

> **情報**
> 設定した値を初期化するには、**リセット** ボタンをクリックしてください。

▼ CoreStation 20

詳細

詳細 セクションでは、デバイスの名前、モデル名、シリアル番号、ファームウェアバージョンなどの基本情報と、機能を操作するアクションメニューや基本設定オプションが表示されます。

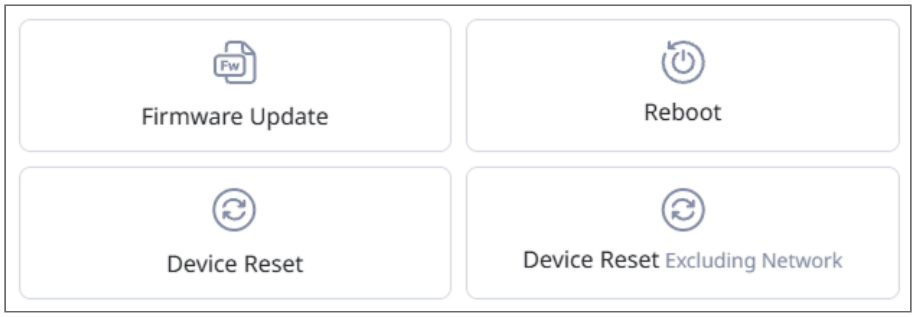
基本情報

デバイスの基本情報を確認できます。 この情報は編集できません。

- **製品**：デバイスの製品名です。
- **モデル名**：デバイスのモデル名です。
- **シリアルナンバー**：デバイスのシリアル番号です。
- **ファームウェアバージョン**：デバイスにインストールされているファームウェアのバージョンです。

アクション機能

デバイスの機能を制御できる**アクション**（Action）機能です。



- **ファームウェアアップデート**：デバイスのファームウェアを最新バージョンに更新できます。
- **再起動**：デバイスに問題や異常が発生した場合、リモートで再起動できます。
- **デバイスのリセット**：デバイスに保存されているすべての設定を初期化します。 この操作を実行すると、デバイスのすべての設定とデータが削除されます。
- **デバイスのリセット ネットワーク設定を除く**：ネットワーク設定を除くすべての設定を初期化します。 この操作を実行すると、デバイスのすべての設定とデータが削除されますが、ネットワーク設定は保持されます。

基本設定

デバイスの基本設定を変更できます。

- **ニックネーム**：デバイス一覧およびログに表示されるデバイスの別名です。 直接編集できます。
- **タイムゾーン**：サイトとデバイスの時計が異なる場合にログを一貫して保つために、デバイスのタイムゾーンを設定します。 サマータイム（Daylight Saving Time、DST）を適用するには、**夏時間を使用** オプションを有効にします。
- **ビデオサービス**：パネルに接続されたIPカメラのライブ映像と録画映像を確認できます。 IPカメラ接続の設定の詳細はIPカメラのサポートおよび設定を参照してください。

カード

カード セクションでは、カード認証に関する設定を変更できます。

NFC/RFカード

- **NFC/RFカード**：トグルスイッチをクリックしてカードによる入退室認証をオンまたはオフにできます。 カード認証に対応するカードの種類を選択してください。
  - **EM4100 (125 KHz)**
  - **Mifare Classic/Mifare DESFire/FeliCa**
- **バイトオーダー**
  - **MSB**：カードデータを処理するとき、大きいバイト単位から小さいバイト単位の順に処理し、カードシリアル番号 (CSN) を左から右へ順に保存します。
  - **LSB**：カードデータを処理するとき、小さいバイト単位から大きいバイト単位の順に処理してカードシリアル番号 (CSN) を保存します。
- **データ読み取り方法**：CSN（デフォルト）または Wiegand 形式を選択できます。

> Wiegand形式には5つの基本形式が含まれています。 **設定** → **カードフォーマット** で、さらに多くの形式を追加できます。 カスタムカード形式の設定の詳細は カスタムWiegandカード形式を設定する を参照してください。

ネットワーク

デバイスのネットワーク設定を変更できます。

- **DHCP使用**：デバイスがIPアドレスを自動的に取得するように設定できます。

  ネットワーク設定を手動で構成するには、**DHCP使用** オプションを無効にして次のフィールドに入力します。
  - **IPアドレス**
  - **ゲートウェイ**
  - **DNSアドレス**
  - **サブネットマスク**
- **SCBキー**：Serial Communication Block (SCB) のセキュリティキーを入力してください。 最大 32 文字まで入力できます。シリアル通信のセキュリティに使用します。
- **SCBキーの確認**：セキュリティキーの誤入力を防ぐため、同じ値を再入力してください。
- **ボーレート**：パネルと補助装置間のシリアル通信速度を設定できます。
  - **Host**：パネルの通信速度
  - **0** / **1**：補助装置が接続された各ポートの通信速度

> **情報**
>
> - OSDP機器を追加する前に、SCBキーを設定してください。 既に追加されたOSDP機器がある場合、SCBキーを変更できません。
> - サードパーティのOSDP機器メーカーが特定のSCBキーを使用する場合、CS-20でそのOSDP機器と同じキーを設定できます。
> - CS-20とOSDP機器のSCBキーが一致しないと、**Secure Session**経由で機器に接続できません。
> - **ボーレート**は独立して別の速度を設定でき、既定値は `115200` です。

詳細設定

デバイス入力ステータス

タンパー、電源障害検知器、火災検知器をAUX IN端子に接続している場合、使用するかどうかを設定できます。

- **タンパー**
- **AC障害**
- **火災**

> **情報**
>
> Fail Safe Lockを使用するには**N/C**リレーを、Fail Secure Lockを使用するには**N/O**リレーを接続してください。 リレー接続の詳細はCoreStation 20 インストールガイドを参照してください。

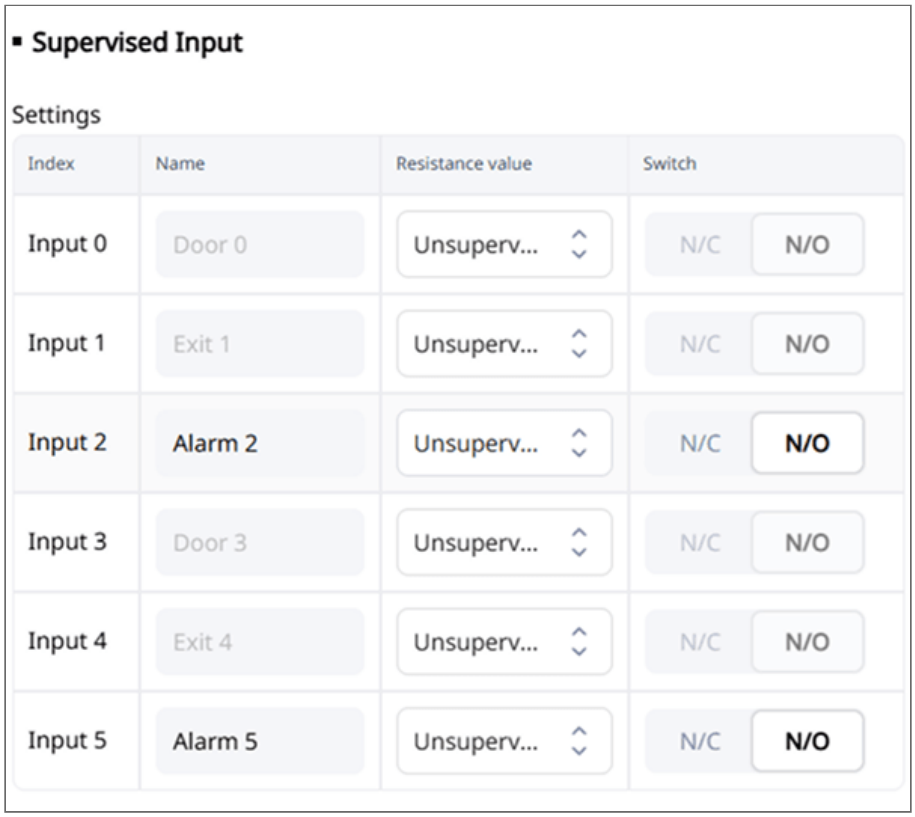
Wiegand入力

Wiegand入力に関連する詳細項目を設定できます。

- **Wiegand入力を使用**：Wiegand入力機能を有効化または無効化できます。
- **入力フォーマット**：Wiegand入力形式を選択してください。
- **パルス幅**：Wiegand 信号のパルス幅を設定します。
- **パルス間隔**：Wiegand 信号のパルス間隔を設定します。

監視入力

Supervised InputポートをInputポートとして使用するよう設定でき、Supervised Inputで使用する抵抗値を設定できます。 抵抗値は 1 kΩ、2.2 kΩ、4.7 kΩ、10 kΩ を設定できます。



セキュアタンパー

パネルでタンパーイベントが発生した場合、パネルに保存されている**全ユーザー情報**、**全ログ**、**セキュリティキー**を削除するように設定できます。

モジュール

パネルに接続されたOM-120モジュールを検出するためのオプションです。 **追加** ボタンをクリックしてモジュールを検出できます。

Airfob PatchとTagを構成する

BioStar Airアプリでのエアポップパッチ登録

開始する前に

- モバイル端末にBioStar Airアプリがインストールされている必要があります。 モバイルアプリは次のリンクからインストールできます。
  - iOS
  - Android
- BioStar Air管理者ポータルで使用するIDとパスワードでログインしてください。
- モバイル端末でBLEが有効になっていることを確認してください。
- エアポップパッチを入退室制御デバイスに恒久的または一時的に取り付けます。 詳細はAirfob Patchのインストールを参照してください。

> **情報**
> BioStar Airモバイルアプリの詳細は、BioStar Airアプリのはじめ方を参照してください。

エアポップパッチ登録

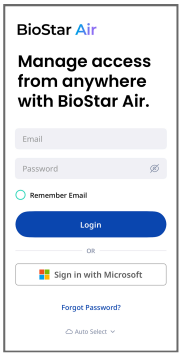
1. モバイル端末でBioStar Airアプリを起動してログインします。
2. BioStar Airアプリの初期画面で**デバイス**カードをタップします。
3. モバイル端末をエアポップパッチに10cm以内まで近づけ、画面右上の ＋ ボタンをタップします。
4. デバイス検索画面で、登録するエアポップパッチの**登録**ボタンをタップします。
5. デバイス登録ウィンドウが表示されたら **OK** ボタンをタップします。

デバイス一覧に戻り、追加されたエアポップパッチを確認します。

構成手順

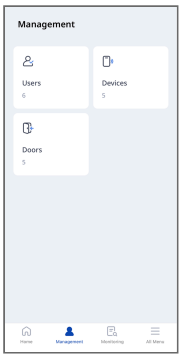
Airfob PatchまたはTagを取り付け、BioStar Airアプリに登録してください。 次の手順に従ってデバイスを構成してください。

1 アプリを起動



1. モバイル機器で **BioStar Air** アプリを起動してください。
2. Airfob PatchまたはTagを登録したサイトにログインしてください。

2 デバイス設定に移動



1. **BioStar Air** アプリの初期画面で下部の **管理** をタップしてください。
2. 登録済みデバイスの一覧を確認するには **デバイス** をタップしてください。
3. デバイス一覧からAirfob PatchまたはTagを選択してください。

3 BLEモードの有効化

- モバイル機器をデバイスに近づけてください。
- アプリで **BLE モード** を有効にしてください。

4 カードID出力方法の設定

- **Card ID Output Method** までスクロールし、**Edit** をタップしてください。
- **User Card ID** の横にある **Select** をタップしてください。

5 出力方法を選択

- **None**：カードIDを送信しない場合はこのオプションを選択してください。 バッテリー寿命を延ばすための勤怠管理(T&A)用途に有用です。
- **Fixed Device**：あらかじめプログラムされた固定カードIDを送信します。 個別にRFIDカードをプログラムする必要があるドアロックやインターホンに適しています。 機器ログにはこの固定カードIDのみが表示されます。
- **User Card ID**：各ユーザーごとに固有のカードIDを送信し、入退室管理システムの既存RFIDカード番号と一致します。 これにより、新しい物理カードを発行せずにシームレスに統合できます。

- **Direct Input**：送信するカードIDを手動で指定します。 複数のデバイスで1つのIDを使用する必要があるカスタム設定に有用です。

6 設定の保存

- モバイル機器をデバイスの近くに置き、 **保存** ボタンをタップして選択内容を確認してください。
- 更新完了のメッセージが表示されます。

バイオメトリクスリーダーとクレデンシャル
BioStar Airはバイオメトリクスリーダーとバイオメトリッククレデンシャルをサポートし、安全な入退室管理を提供します。 BioStation 3（以下BS3）およびBioEntry W3（以下W3）などの互換性のあるバイオメトリクスリーダーを登録して設定し、顔認証でユーザーを認証できます。 この機能は単一認証および二要素認証の両方をサポートし、柔軟性とセキュリティを向上させます。

- **デバイスの登録**：BioStar Airモバイルアプリを使用してバイオメトリクスリーダーを登録できます。
- **デバイスの設定**： BioStar Airポータル → **デバイス管理** → **登録済みデバイス** に移動し、デバイスの顔認証設定を構成します。
- **ユーザー顔クレデンシャルの設定**： BioStar Airポータル → **ユーザー管理** → **ユーザー** に移動し、ユーザーを追加するかユーザー情報を編集します。 **認証情報の詳細** セクションで顔クレデンシャルを有効にしてください。

開始する前に

- バイオメトリクスリーダーが正常に動作するには、BioStar Air互換のファームウェアがインストールされている必要があります。
- 顔テンプレートはユーザーごとに最大2つまで使用できます。
- 高度な構成については、BioEntry W3またはBioStation 3のユーザーガイドを参照してください。
- 二要素認証を使用するには、クレデンシャルを2つ以上登録する必要があります。 例えば、RFカードと顔クレデンシャルの両方を登録する必要があります。

ステップバイステップの手順

1 バイオメトリクスリーダーの登録

BioEntry W3またはBioStation 3にBioStar Air互換のファームウェアがインストールされていることを確認してください。 モデル名が `-AIR` で終わるデバイスには、Supremaが提供する標準ファームウェアが既にインストールされています。

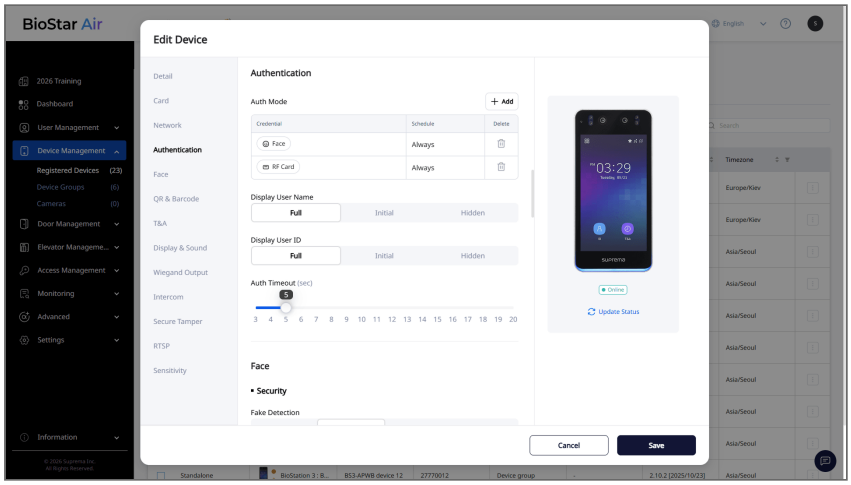
モバイルデバイスでBioStar Airアプリを起動し、管理者IDとパスワードでログインしてください。 他のデバイスを登録するのと同じ方法でデバイスを登録してください。

> **情報**
> デバイス登録の詳細は、エッジデバイスの登録と削除をご参照ください。

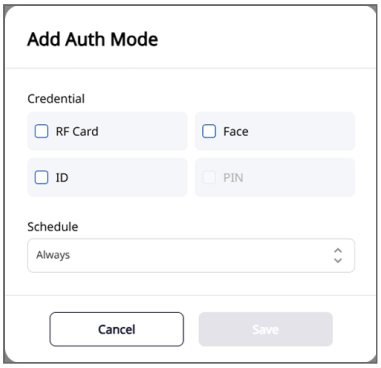
2 デバイス設定

1. BioStar Airポータルに管理者アカウントでログインしてください。

2. 画面左のサイドバーで **デバイス管理** → **登録済みデバイス** をクリックします。
3. デバイス一覧でバイオメトリクスリーダーをクリックしてください。
4. **デバイス編集** ウィンドウが表示されたら、**認証** セクションに移動してください。



5. **認証モード** を設定してください。
   - **シングルファクター**：RFカードまたは顔のいずれかを使用して認証できます。
   - **二要素**：RFカードまたは顔認証のいずれかを削除し、RFカードと顔の両方を再登録することで二要素認証を構成できます。 **追加** ボタンをクリックし、希望する認証方式を組み合わせてください。

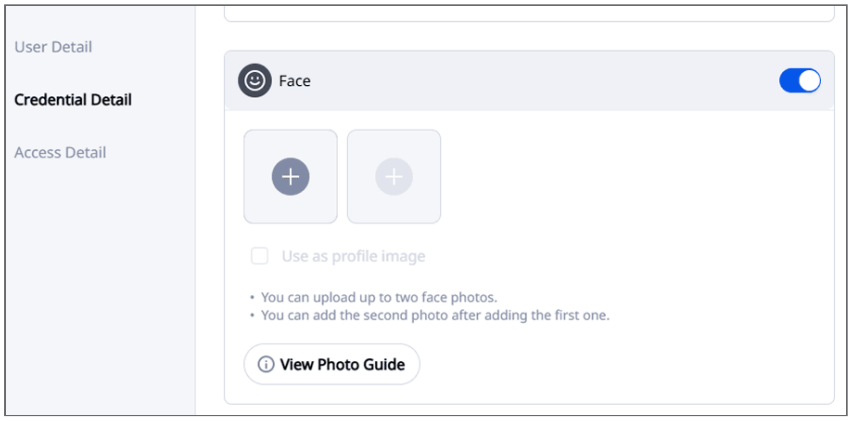


6. **認証タイムアウト** を設定してください。 設定した時間内にクレデンシャルを認証できないと、認証に失敗します。
7. **顔** セクションで次のオプションを設定してください。
   - **偽造検出**
   - **モーション センサーの感度**
   - **最大ヘッド ポーズ角度**
   - **検出距離**
8. 追加オプションを設定してください。
   - **重複チェック**
   - **登録時間**
   - **マスク検出**

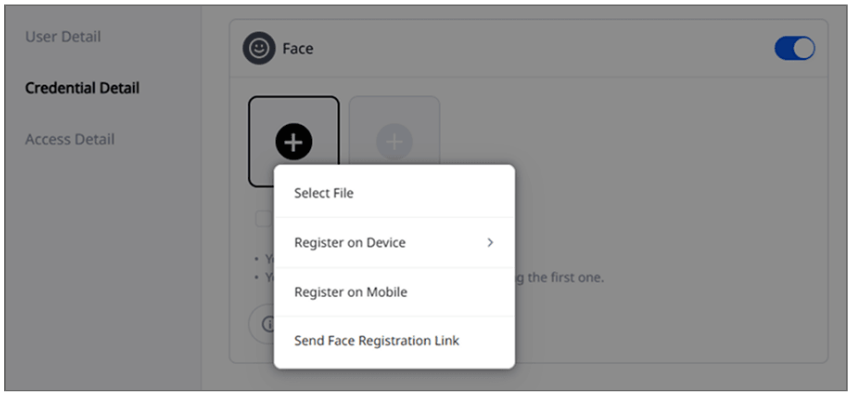
> **情報**
> **認証** セクションの設定の詳細は、デバイスおよびパネルの設定オプションのご案内をご参照ください。

3 ユーザーの顔登録

1. 画面左のサイドバーで **ユーザー管理** → **ユーザー** をクリックします。
2. 新しいユーザーを追加するか既存のユーザーを編集するウィンドウを開いてください。
   - **新しいユーザーの追加**：ユーザーリスト右上の **ユーザー追加** をクリック
   - **既存ユーザーの編集**: ユーザー一覧でユーザーをクリックし、 ボタンをクリック
3. ユーザー情報ウィンドウで **認証情報の詳細** セクションに移動し、**顔** クレデンシャルを有効にしてください。



4. ＋ ボタンをクリックして顔テンプレートを追加してください。



- **ファイルを選択**：ローカルに保存された写真ファイルを選択
- **デバイスに登録**：接続されたバイオメトリクスリーダー（BioEntry W3またはBioStation 3）を使用
- **モバイルで登録**：ユーザーのモバイルデバイスに送信したQRコードをスキャンし、モバイルデバイスで顔を登録する
- **顔登録リンクを送信**：ユーザーのメールまたはSMSで顔登録リンクを送信し、モバイル端末のカメラで直接顔を登録する

ユーザーごとに顔写真は2枚までアップロードできます。 通常は1枚の写真で十分です。

5. 顔登録を完了するには **保存** ボタンをクリックしてください。

情報
ユーザーの顔写真を一括でアップロードする方法の詳細は、ユーザーを一括で追加するをご参照ください。

ファームウェアをアップグレードする

BioStar Airのファームウェアをアップグレードして装置のパフォーマンスを向上させ、セキュリティを強化し、新機能を活用できます。 この手順は簡単で、BioStar AirのウェブポータルまたはBioStar Airのモバイルアプリから実行できます。

開始する前に

- ファームウェアをアップデートするには、装置が**オンライン状態**である必要があります。 **製品** 列で装置の状態を確認してください。 装置の画像の横に緑の点(🟢)が表示されていればオンライン状態です。
- ファームウェア更新中はデバイスが**一時的にオフライン状態**になりますが、**3~5分**以内に再接続されます。
- ファームウェア更新中は装置が一時的にオフラインになりますので、業務時間外に実施することをおすすめします。
- 新しいファームウェアがアップデートされると通知を受け取るよう設定できます。 通知設定の詳細は、アラートとレポートの設定をご参照ください。

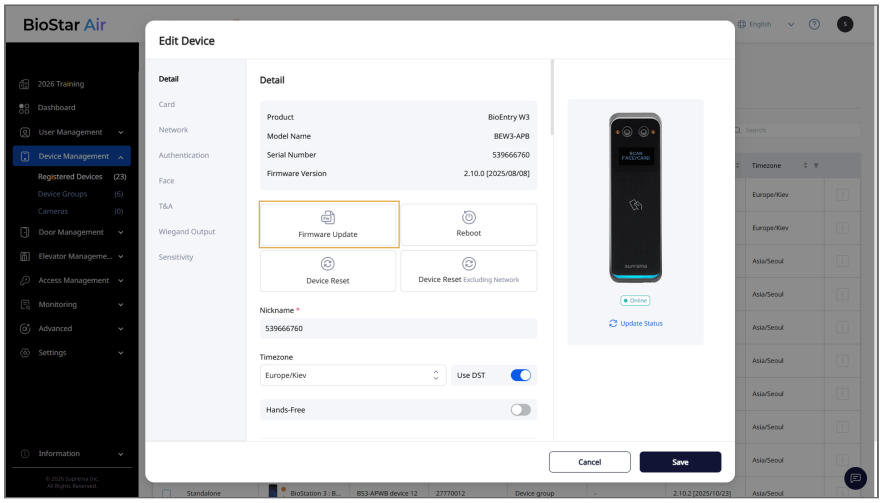
情報
装置管理の詳細は、登録済みエッジデバイスの管理をご参照ください。

個別の装置のファームウェアアップグレード

Web

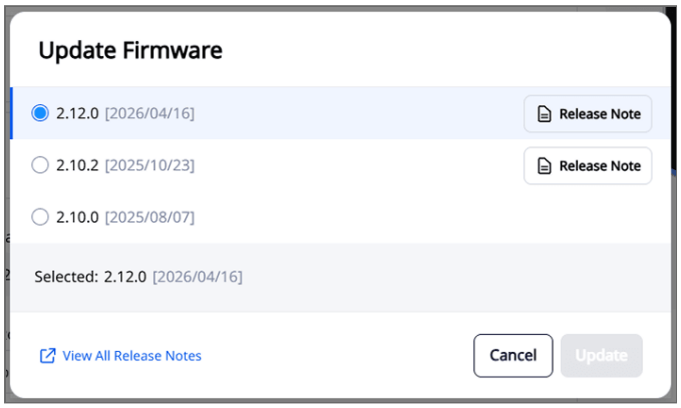
BioStar Air ポータルにログインした後、次の手順に従ってファームウェアをアップグレードします。

1. 画面左のサイドバーで **デバイス管理** → **登録済みデバイス** をクリックします。
2. 装置一覧でアップグレードする装置をクリックします。
3. **デバイス編集** ウィンドウが表示されたら、**詳細** セクションに移動してください。
4. **ファームウェアアップデート** をクリックします。



上記の画像は例示です。実際の画面とは異なる場合があります。

5. **ファームウェア更新** ウィンドウが表示されたら、最新のファームウェアバージョンを選択して **更新** ボタンをクリックします。



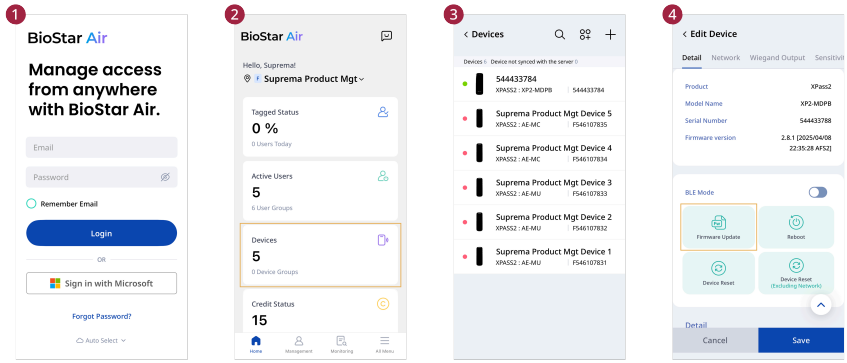
該当デバイスが自動で再起動し、オンラインに戻るまで待ってください。 一覧のデバイスに緑の点(🟢)が表示されていれば、オンラインです。

情報

- **リリースノート** ボタンをクリックして、該当ファームウェアのリリースノートを確認してください。
- **すべてのリリースノートを表示** ボタンをクリックして、すべてのデバイスのファームウェアリリースノートを確認してください。

Mobile

モバイルアプリでのファームウェアアップグレード手順を説明します。

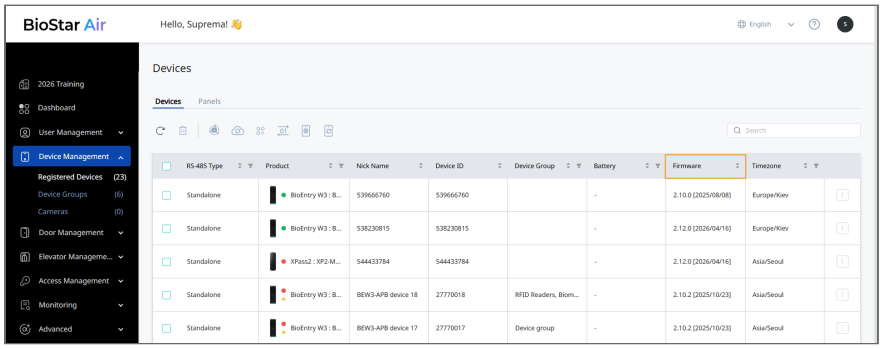


1. モバイル端末でBioStar Airアプリを起動してログインします。
2. **デバイス** カードをタップします。
3. 装置一覧でアップグレードする装置をタップします。
4. **ファームウェアアップデート** をタップします。
5. 最新のファームウェアバージョンを選択して **OK** をタップします。
6. メッセージウィンドウが表示されたら、内容を確認して **OK** をタップしてください。

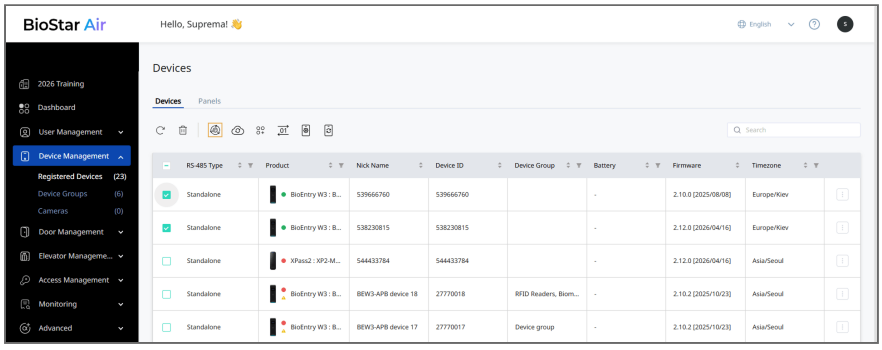
> **情報**
>
> - ファームウェアのアップグレードには約5～10分かかる場合があり、その間装置は使用できません。
> - 装置の電源を切らないでください。
> - ファームウェアアップグレード完了後、装置は自動的に再起動します。

複数の装置を一括でアップグレード

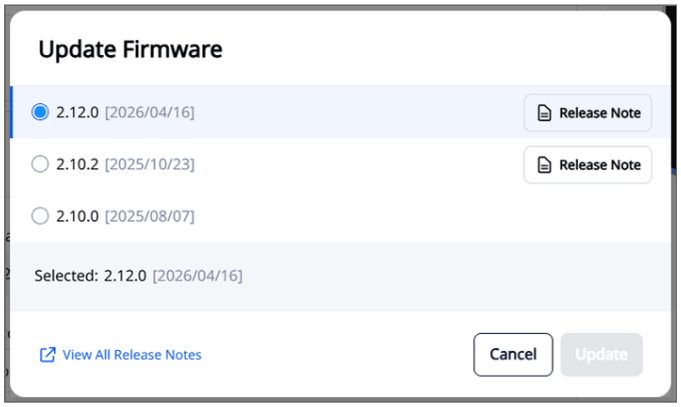
1. 画面左のサイドバーで **デバイス管理** → **登録済みデバイス** をクリックします。
2. 装置一覧の **ファームウェア** 列で各装置の現在のバージョンを確認します。
3. 装置をファームウェアバージョンごとに並べ替えるには、**ファームウェア** 列の右側にある矢印ボタンをクリックします。



4. アップグレードする各装置の左側にあるチェックボックスをクリックします。 同じ種類のデバイスを選択してください。
5. 装置一覧の上部にある ボタンをクリックしてください。



6. **ファームウェア更新** ウィンドウが表示されたら、最新のファームウェアバージョンを選択して **更新** ボタンをクリックします。



選択したデバイスが自動で再起動し、オンラインに戻るまで待ってください。 一覧のデバイスに緑の点(🟢)が表示されていれば、オンラインです。

> **情報**
>
> - ファームウェアのアップグレードには約5〜10分かかる場合があり、その間装置は使用できません。
> - 装置の電源を切らないでください。
> - ファームウェアアップグレード完了後、装置は自動的に再起動します。
> - **リリースノート** ボタンをクリックして、該当ファームウェアのリリースノートを確認してください。
> - **すべてのリリースノートを表示** ボタンをクリックして、すべてのデバイスのファームウェアリリースノートを確認してください。

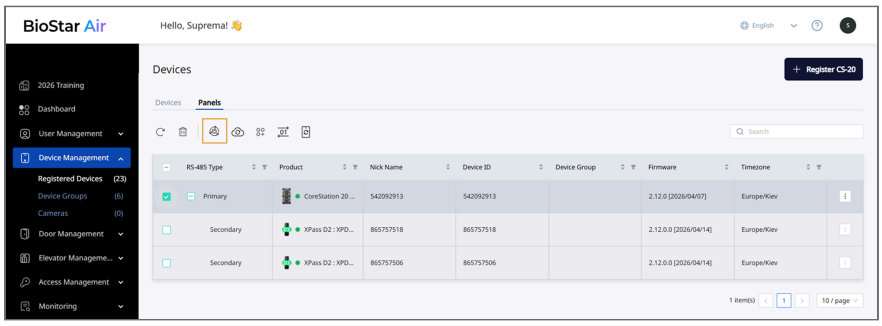
XPass D2 ファームウェアアップグレード

XPass D2 デバイスは 2 つのファームウェアコンポーネントを使用します。

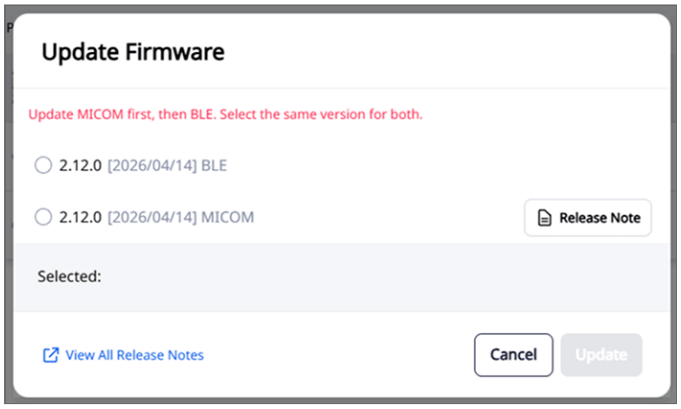
- **MICOM**：デバイスの動作、RS-485 通信、認証処理、安定性、一般的なバグ修正などに関する更新を含みます。
- **BLE**：Bluetooth 通信に関する更新を含みます。

XPass D2 デバイスは必ず **MICOM** → **BLE** の順でファームウェアをアップグレードしてください。

1. 画面左のサイドバーで **デバイス管理** → **登録済みデバイス** をクリックします。
2. **パネル** タブをクリックしてください。
3. XPass D2 デバイスのチェックボックスをクリックしてください。 1 台のみ選択できます。



4. 一覧上部の ボタンをクリックしてください。
5. **ファームウェア更新** ウィンドウが表示されたら、**MICOM** ファームウェアバージョンを選択してください。



6. **更新** ボタンをクリックしてください。
7. 該当デバイスが自動で再起動し、オンラインに戻るまで待ってください。 一覧のデバイスに緑の点(🟢)が表示されていれば、オンラインです。
8. 同じ手順を繰り返して **BLE** ファームウェアバージョンを選択し、アップデートしてください。

> **注意**
>
> - 画面に表示されるファームウェアバージョン情報だけでは、**MICOM** と **BLE** 各コンポーネントのインストール状況を個別に確認することは困難です。 BLE のアップグレードが完了するまで、ファームウェアのアップグレードを続けてください。
> - デバイスは **MICOM** 更新後と **BLE** 更新後に、それぞれオンラインに復帰します。 緑のオンライン表示(🟢)だけでアップグレードが完了したと判断しないでください。 両方の手順を確実に完了したか、もう一度確認してください。
> - CS-20 を介して接続されたスレーブデバイスは、一度に 1 台のみファームウェアをアップグレードできます。

ドア

BioStar Airのドア管理は、セキュリティとアクセス制御を効率的に運用するための重要な要素です。 ドアを登録し、入口と出口のデバイスを構成し、グループとスケジュールで大規模なドア制御を管理します。 また、自動化されたロック／アンロックポリシーと認証ベースのアクセス制御によりセキュリティを強化できます。

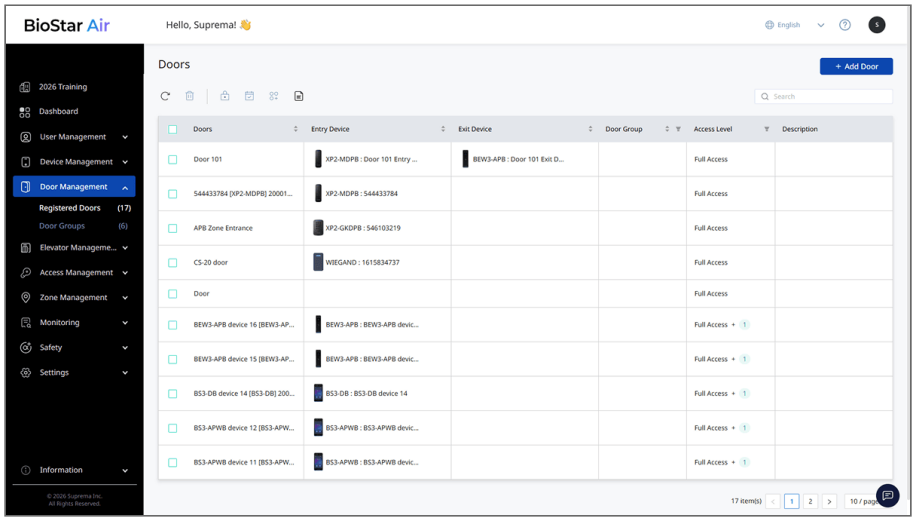
登録済みドアの管理
登録済みのドアに入退室デバイスを割り当て、リレーと出入レベルを設定し、入退室スケジュールを設定します。 セキュリティ、避難、勤怠管理（T&A）のために、体系的に入退室を制御できます。

> **ヒント**
> ドアの登録と管理に関するビデオガイドを見るには、次のビデオを参照してください。

ドア一覧を確認

ドア一覧では、BioStar Airに登録されたすべてのドアを一目で確認できます。 各ドアの名前、割り当てられたデバイス、グループ、アクセスレベルなどの主要な情報を確認できます。 また、各ドアをクリックして詳細を確認し、設定を変更できます。

登録済みドアを確認するには、画面左のサイドバーで **ドア管理** → **登録されたドア** をクリックします。



ドア情報

ドア一覧には次の情報が表示されます。

- **ドア**：ドアの名前です。 通常はデバイス登録時に自動で割り当てられ、管理者はドア名を変更できます。
- **入室デバイス**：入室するユーザーを認証するデバイスです。
- **退室デバイス**：退室するユーザーを認証するデバイスです。
- **ドアグループ**：ドアに割り当てられたグループ名です。
- **アクセスレベル**：ドアに割り当てられたアクセスレベルです。 アクセスレベルの割り当ての詳細は アクセスレベルの一括割り当て を参照してください。
- **説明**：ドアに関する説明です。
- **カメラ**：ドアに接続されているカメラ情報が表示されます。 **カメラ** 列は **設定** → **サイト** → **追加機能** で **ビデオ管理** 機能を有効にする必要があります。

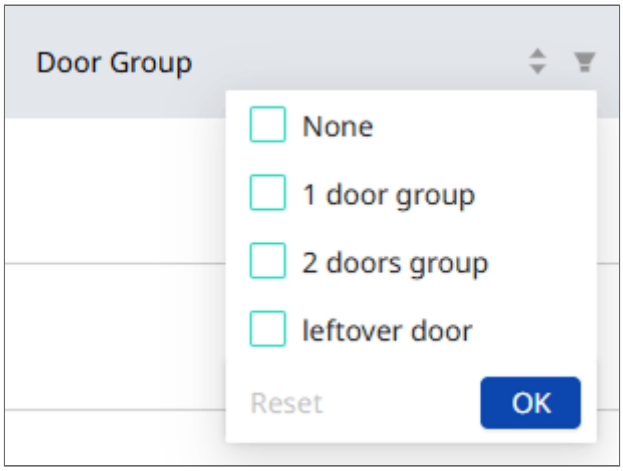
追加機能

一覧で1つまたは複数のドアを選択すると、管理者は以下の追加機能を使ってドアを管理できます。

- ：ドア一覧を更新できます。
- ：一覧で選択したドアを削除します。
- ：一覧で選択したドアの出入レベルを設定できます。 詳しくは アクセスレベルの一括割り当て をご参照ください。
- ：ドアの開閉状態のスケジュールを設定します。 詳細については 出入口スケジュールの管理 を参照してください。
- ：一覧で選択したドアをグループ化できます。 グループ管理の詳細については ドアグループを管理する を参照してください。
- ：ドアレポートを生成できます。 レポート作成の詳細については ドアレポートの生成 を参照してください。

フィルタリング

ドア一覧では、ドアグループで絞り込んで表示できます。 **ドアグループ** 列の ボタンをクリックして、目的のグループを選択してください。 **OK** をクリックすると、選択したグループに属するドアのみが表示されます。



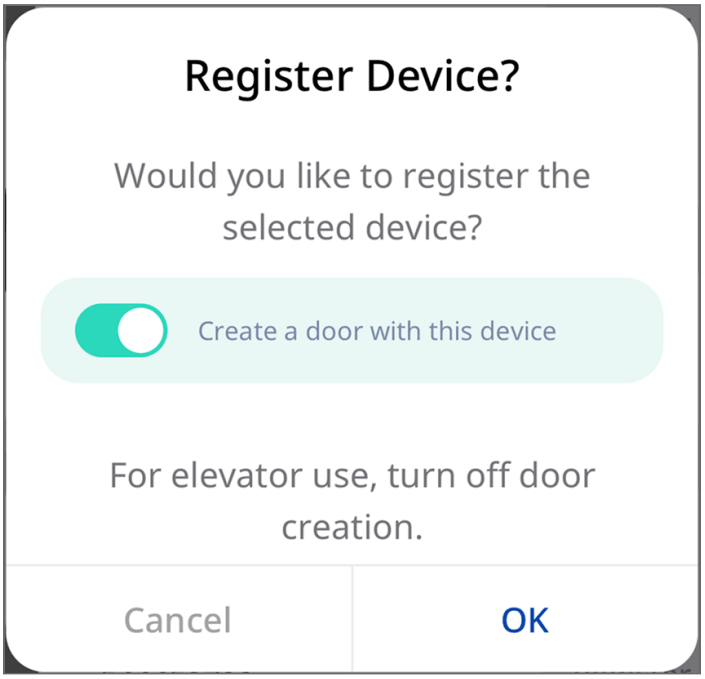
情報

適用したフィルター条件を初期化するには、 ボタンをクリックし、**リセット** ボタンを選択してください。

ドアの追加

デバイスと一緒に追加する

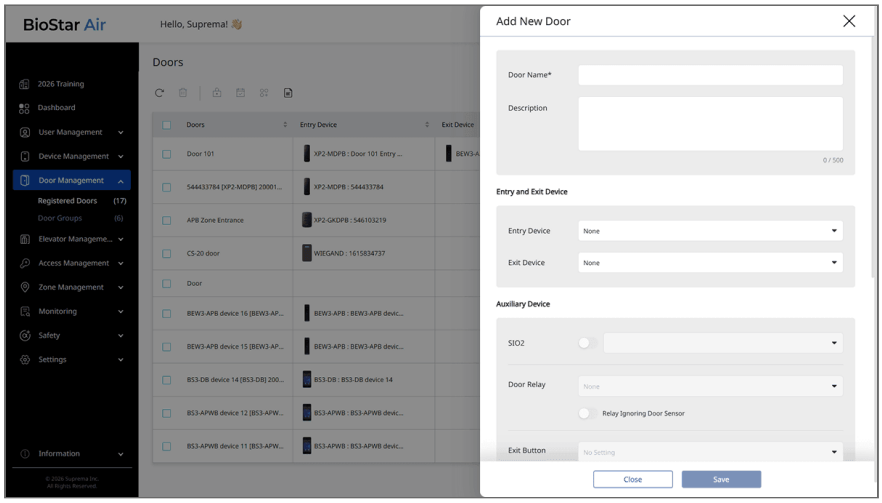
モバイルアプリでデバイスを登録する際、最終段階で **このデバイスでドアを作成する** オプションを選択すると、ドアが作成されます。 モバイルアプリでデバイスを登録する方法の詳細は、エッジデバイスの登録と削除 を参照してください。



Webポータルで追加

BioStar Air ポータルで新しいドアを追加するには、次の手順に従ってください。

1. 画面左のサイドバーで **ドア管理** → **登録されたドア** をクリックしてください。
2. 画面右上の **ドアを追加** ボタンをクリックします。
3. **ドアを追加** パネルが表示されたら、**ドアの名前** を入力します。



4. **入室デバイス** と **退室デバイス** を選択します。
5. ドア設定を保存して追加するには、**保存** ボタンをクリックします。

ドアのデバイス割り当てルール

- 各デバイスは**1つのドア**のみに割り当てることができます。
- デバイスが既に登録されているのに利用可能なデバイス一覧に表示されない場合は、そのデバイスが他のドアに割り当てられていないか確認してください。 他のドアに割り当てられている場合は、そのドアから削除してから再試行してください。
- **1台の装置を出入口とエレベーターに同時に割り当てることはできません。**

マスター/スレーブ装置を使用する出入口

- 出入口はマスター装置（XPass 2、CoreStation 20）が制御します。
- マスター装置に設定されたXPass 2は、割り当てられた補助装置やモジュールの数に関係なく、1つの出入口にのみ割り当て可能です。
- XPass 2をマスター装置に設定すると、最大31台の補助装置を割り当て、補助Secure I/O 2（SIO2）でリレーを制御する新しいドアを追加できます。
- CoreStation 20（CS-20）とSecure I/O 2（SIO2）を使用するドアは作成できません。

出入口構成の制限事項

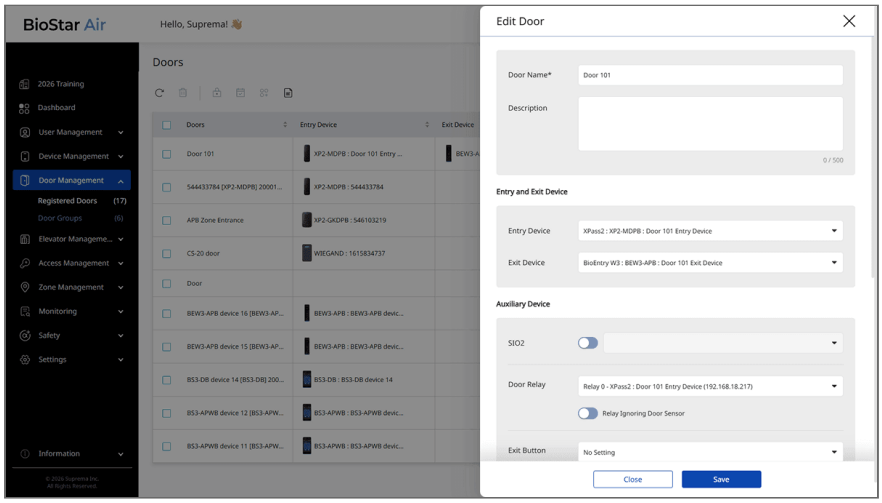
出入口の構成には、以下の制限があります。

- XPass D2 1台 + SIO2（リレーはSIO2所有）
- XPass 2 1台 + XPass D2（リレーはXPass 2所有）
- XPass D2 2台（リレーはXPass 2所有）
- OSDP/Wiegand装置1台または2台（リレーはCS-20所有）
- 出入口あたりSIO2は1台のみ許可（リレーはI/O用）：XPass D2と同じXPass 2に配線する必要があります。

ドアの編集

ドアの詳細と設定を編集するには、次の手順に従います。

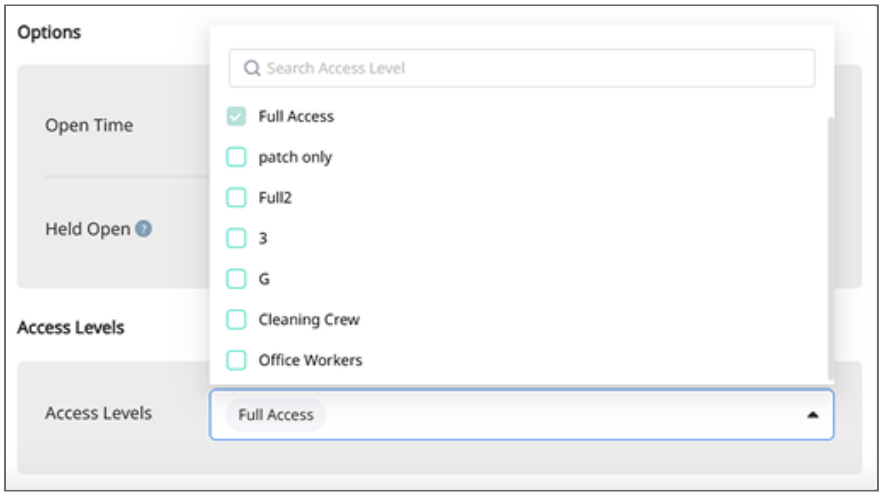
1. 画面左のサイドバーで **ドア管理** → **登録されたドア** をクリックしてください。
2. 一覧で編集するドアをクリックします。 または、ドアの左にあるチェックボックスをクリックしてから、画面上部の左側サイドバーの ボタンをクリックします。
3. **ドアを編集** パネルが表示されたら、**ドアの名前** と **説明** を編集します。



4. **入退出装置** セクションでドアのユーザー認証用デバイスを選択します。
   - **入室デバイス**：入室するユーザーを認証するデバイスを選択します。
   - **退室デバイス**：退室するユーザーを認証するデバイスを選択します。
5. **補助装置** セクションでリレー装置を設定します。
   - **カメラ**：イベントログ用のCCTVカメラを接続できます。
   - **ドアリレー**：ドアロックを制御するリレー装置を選択します。
   - **ドアセンサーを無視するリレー**：出入口センサーを無視するようにリレーを設定できます。

> カメラは **設定** → **サイト** → **追加機能** で **ビデオ管理** 機能を有効にする必要があります。

6. 追加の設定を構成します。
   - 設置されている場合は、**退出ボタン** に設定するポートを選択します。
   - **ドアセンサー** に設定するポートを選択します。
   - **開いている時間** でドアが開いた状態を保つ時間を設定します。 （既定値：3秒）
7. **アクセスレベル** セクションで、該当ドアに割り当てる、または解除する出入レベルのチェックボックスをクリックしてください。



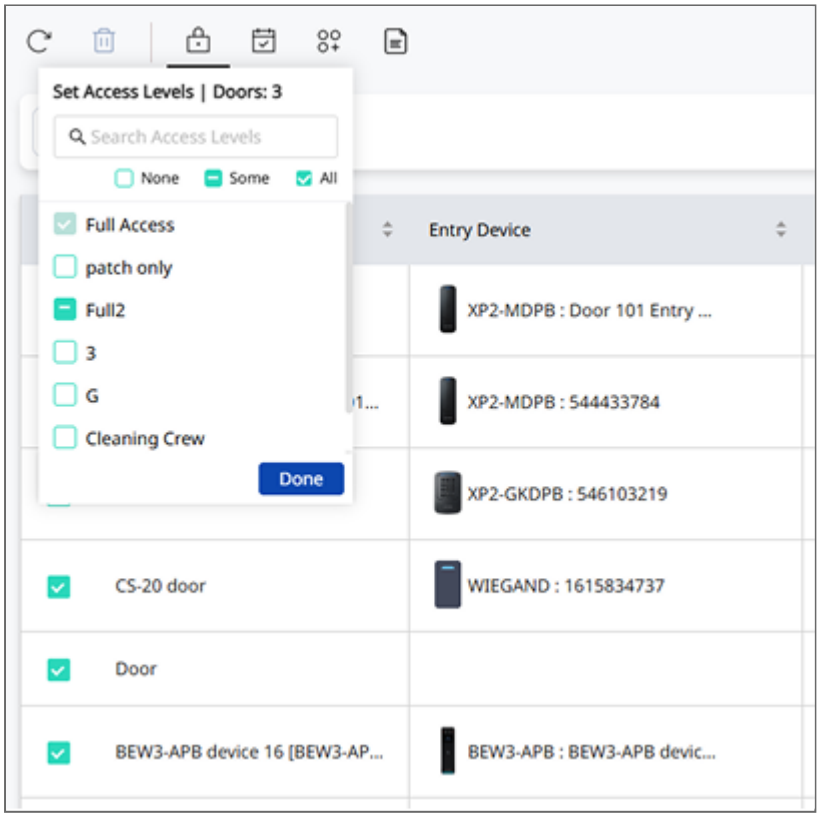
8. 変更を適用するには、**保存** ボタンをクリックします。

> **情報**
>
> - セキュリティ上、リレーは常に出入口のセキュリティ側にある装置に接続する必要があります。 通常は出口装置のリレーを使用するか、SIO2モジュールを利用することを推奨します。
> - クラウドに直接接続して構成する場合、入口装置と出口装置にそれぞれネットワークケーブルを接続する必要があります。
> - マスター-補助装置構成では、マスター（通常は出口装置）はネットワーク接続が必要で、補助装置はRS-485を介してマスターに接続されます。
> - SIO2セキュリティモジュールの構成に関する詳細は、SIO2 セキュリティモジュールの構成 ご参照ください。

アクセスレベルの一括割り当て

複数のドアに同じアクセスレベルを割り当てる場合、ドアを個別に編集せず、一覧でアクセスレベルを一括で割り当て、または解除できます。

1. 画面左のサイドバーで **ドア管理** → **登録されたドア** をクリックしてください。
2. 出入レベルを設定するドアのチェックボックスを一つ以上選択してください。
3. ドア一覧の上部にある ボタンをクリックしてください。
4. **アクセスレベル設定** ポップアップメニューが表示されたら、選択したドアに適用する出入レベルのチェックボックスをクリックしてください。



必要に応じて、検索フィールドでアクセスレベルを検索してください。

- **なし**：選択したドアからこの出入レベルが解除されます。
- **いくつか**：選択したドアの一部にのみ、この出入レベルが割り当てられています。
- **すべて**：選択したすべてのドアに、この出入レベルが割り当てられます。

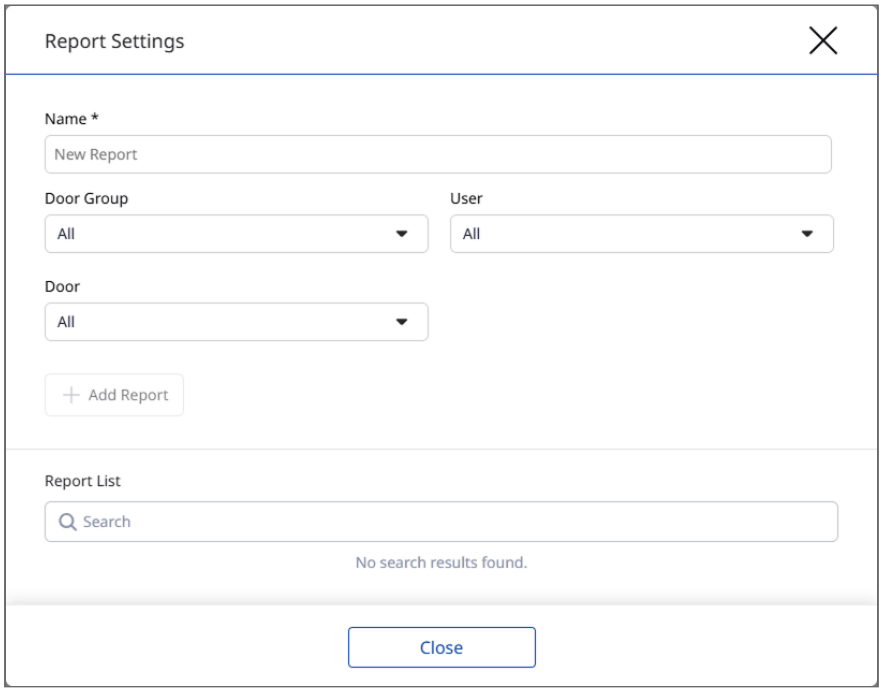
5. 設定を完了するには、**終了** をクリックしてください。

> **情報**
>
> - ドアの一つ以上がオフライン状態の場合、変更した出入レベルはデバイスが再接続されたときに適用されます。
> - **フルアクセス** 出入レベルはシステムが自動管理するため、変更できません。
> - 設定変更中に一部のドアでエラーが発生し、出入レベルの一部が適用されない場合があります。 出入レベルの変更に失敗したドアは、案内ウィンドウに表示されます。 再試行するには、**失敗分を再試行** ボタンをクリックしてください。

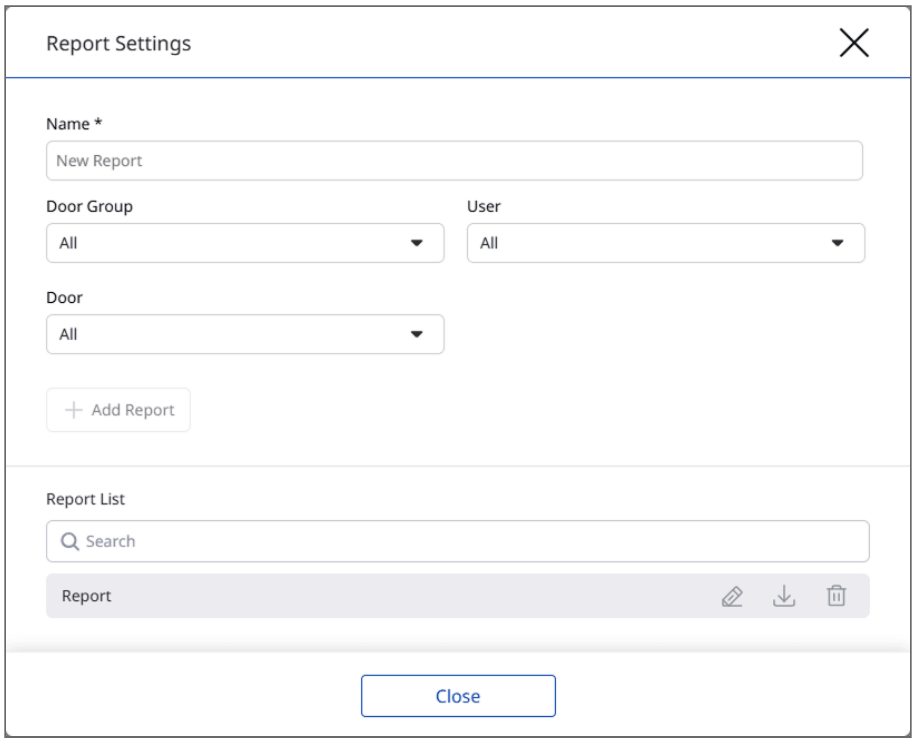
ドアレポートの生成

ドアレポートを生成して管理者のメールに送信できます。 ドアレポートはドアを通過したユーザーに関する情報を提供します。

1. 画面左のサイドバーで **ドア管理** → **登録されたドア** をクリックしてください。
2. 出入口一覧の上部にある ボタンをクリックします。
3. **レポート設定** ウィンドウが表示されたら、レポート名を入力します。



4. レポートに含める項目を選択します。
5. 作成したレポートを保存するには、**レポートの追加** をクリックします。
6. **レポートリスト** が作成され、管理者のメールにダウンロードリンクが送信されます。



情報

レポートリスト で作成されたリポートを検索、編集、ダウンロード、削除できます。

ドアグループを管理する

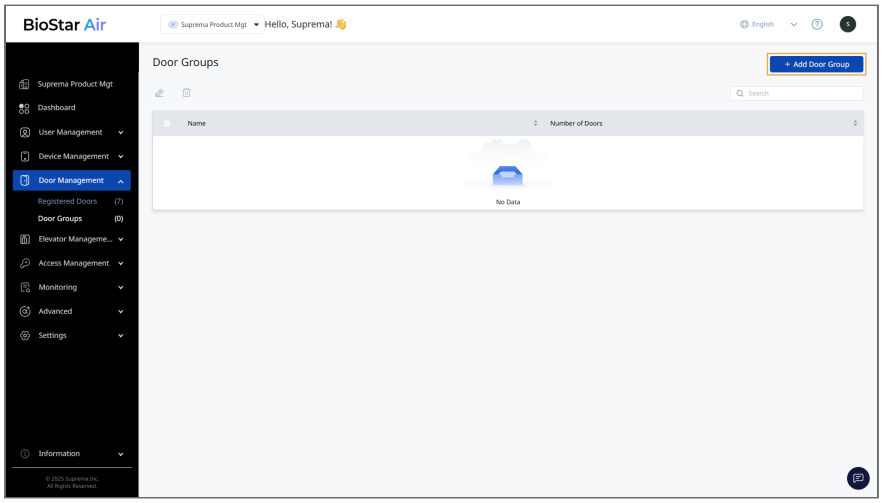
ドアをグループ化すると、アクセス制御ポリシーを効率的に管理できます。 グループごとにアクセスレベルと権限を一括設定して、複数のドアに一貫したセキュリティポリシーを適用できます。

情報

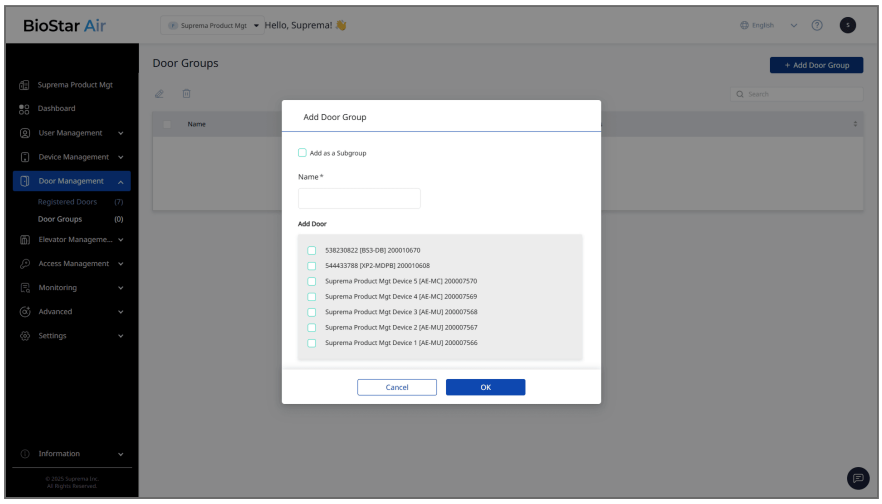
- ドアの管理に関する詳細は、登録済みドアの管理をご参照ください。
- アクセスレベル管理の詳細は 出入レベルの管理性行する を参照してください。

ドアグループを追加

1. 画面左のサイドバーで **ドア管理** → **ドアグループ** をクリックします。
2. 画面右上の **ドアグループを追加** をクリックします。



3. **ドアグループを追加** ウィンドウが表示されたら、ドアグループ名を入力します。



> 特定のグループのサブグループとしてデバイスグループを追加するには、**サブグループとして追加** オプションをクリックし、親グループを選択します。

4. **ドアを追加** でグループに含めるドアを選択します。
5. ドアグループを保存するには、**OK** をクリックします。

ドアグループ一覧で、新しく追加されたグループとそのグループに含まれるドアの数を確認できます。 ドアグループをクリックすると、そのグループに含まれるドアを確認できます。

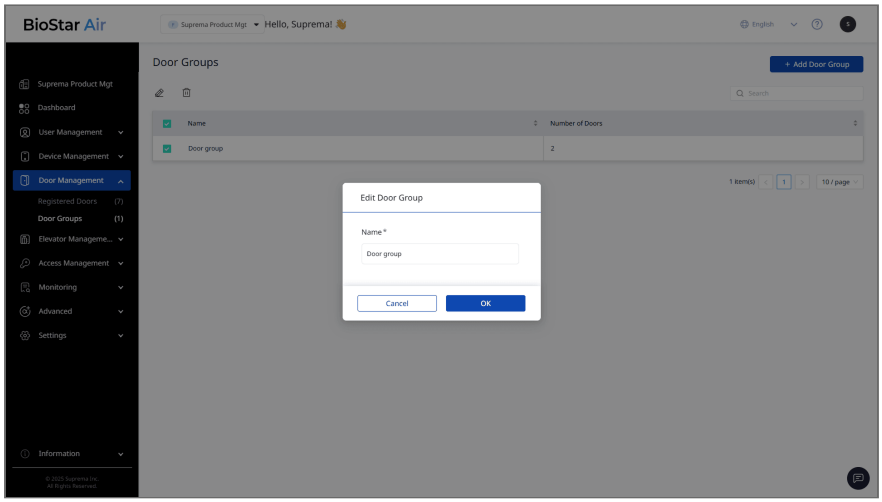


情報

- サブグループにドアを追加しても、親グループに自動的に含まれません。
- デバイスやドアがない空の親グループを追加できます。

ドアグループ名を変更

1. 画面左のサイドバーで **ドア管理** → **ドアグループ** をクリックします。
2. ドアグループ一覧で、名前を変更するドアグループのチェックボックスをクリックします。
3. ドアグループ一覧上部の✎ボタンをクリックしてください。
4. **ドアグループを編集** ウィンドウが表示されたら、新しいグループ名を入力します。



5. 変更したグループ名を保存するには、**OK**ボタンをクリックしてください。

ドアグループを削除

1. 画面左のサイドバーで **ドア管理** → **ドアグループ** をクリックします。
2. ドアグループ一覧で、削除するドアグループのチェックボックスをクリックします。
3. ドアグループ一覧上部の🗑ボタンをクリックしてください。
4. 警告メッセージのウィンドウが表示されたら、**はい** をクリックします。

ドアグループ一覧で選択したドアグループが削除されます。 そのグループのサブグループもすべて削除されます。 グループを削除してもドアは削除されません。

出入口スケジュールの管理

出入口のスケジュールを設定すると、時間帯ごとに自動で施錠・解錠できます。 施錠および解錠の時刻を設定し、**初回認証後に解**

錠などの高度なオプションを利用して、安全で管理された入退室を実現します。

> **情報**
>
> - スケジュールは、インターネットに接続されている出入口および機器にのみ適用できます。
> - 休日グループは別途構成されていない限り、解錠スケジュールを無視します。
> - 緊急時に備えて、制限のない入退室権限を持つ管理者を少なくとも1人以上配置する必要があります。

スケジュールが必要な場合

ドアのスケジュールは必須ではありません。 ほとんどの施設では基本的なアクセス制御だけで十分です。 認証済みのユーザーが資格情報を提示すると自動的にドアが開くため、追加のスケジュール設定がなくても正常に動作します。

次のような場合にスケジュールを設定してください。

- 特定の時間帯に誰でも自由に出入りできるようにしたい場合
- 特定の時間にすべてのユーザーの出入りを禁止したい場合
- 時間帯ごとにアクセス方針を変えて適用したい場合

アンロックスケジュールと **ロックスケジュール**の混同を避けるため、それぞれの動作と使用タイミングを明確に理解してください。

アンロックスケジュール と ロックスケジュール

区分	開錠スケジュール	施錠スケジュール
スケジュール適用中の状態	常時開錠	常時施錠
認証の要否	不要、誰でも自由に出入り可能	資格情報認証では開錠できない
手動開錠	可能	サイト管理者のみ可能
リレー動作	作動し続ける	作動しない

> **情報**
>
> サイト管理者は、BioStar Air 管理ポータルまたはモバイルアプリで指定された管理者を指します。

開錠スケジュール

スケジュールの時間帯中はドアが常に開いており、リレーは作動し続けます。 認証は不要なので、誰でも自由に出入りできます。

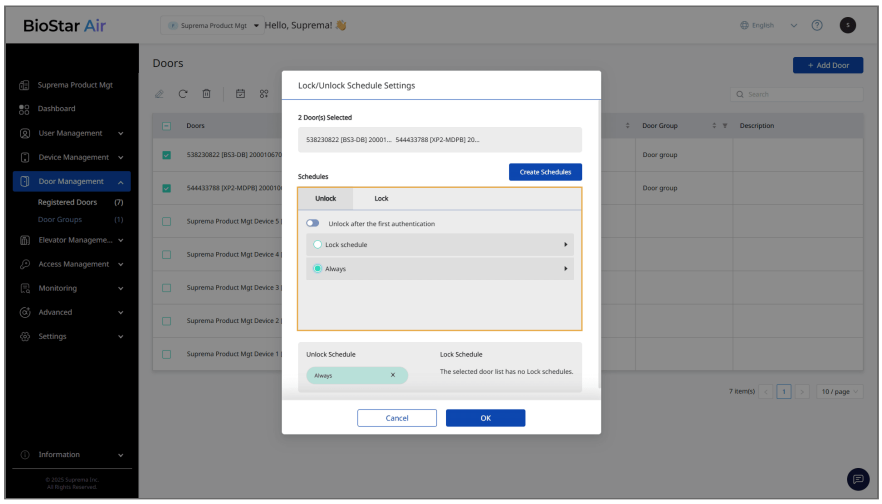
利用例

- 共用スペースのメイン入口
- 住宅団地内の共用施設
- 勤務時間中のオフィスロビーの入口

開錠スケジュールの設定

次の手順に従って解錠スケジュールを構成します。

1. 画面左のサイドバーで **ドア管理** → **登録されたドア** をクリックしてください。
2. 出入口一覧で、解錠スケジュールを設定するドアのチェックボックスをクリックしてください。
3. 出入口一覧の上部にある ボタンをクリックしてください。
4. **ロック/アンロックスケジュール設定** ウィンドウが表示されたら、**アンロック** タブで事前定義されたスケジュールを選択するか、新しいスケジュールを作成します。



5. 解錠スケジュールを適用するには、**OK** ボタンをクリックします。

> **情報**
>
> - **最初の認証後にアンロック** オプションを有効にすると、ユーザーが初回に認証した後、選択したスケジュールに従ってドアの解錠状態を維持できます。 このオプションは、次のようなケースで有効です。
>   - 従業員が到着してから顧客の入店を許可する小売店
>   - 最初の従業員が建物を開錠すれば、その後は他の従業員が自由に出入りできるオフィス
>   - 担当者が開錠すれば会員が自由に利用できる会員制施設
> - スケジュール登録の詳細は 新しいスケジュールの登録 を参照してください。

施錠スケジュール

スケジュール時間中はドアが常に施錠され、リレーは作動しません。 有効なクレデンシャルを提示しても認証で解錠できず、サイト管理者のみが手動で解錠できます。

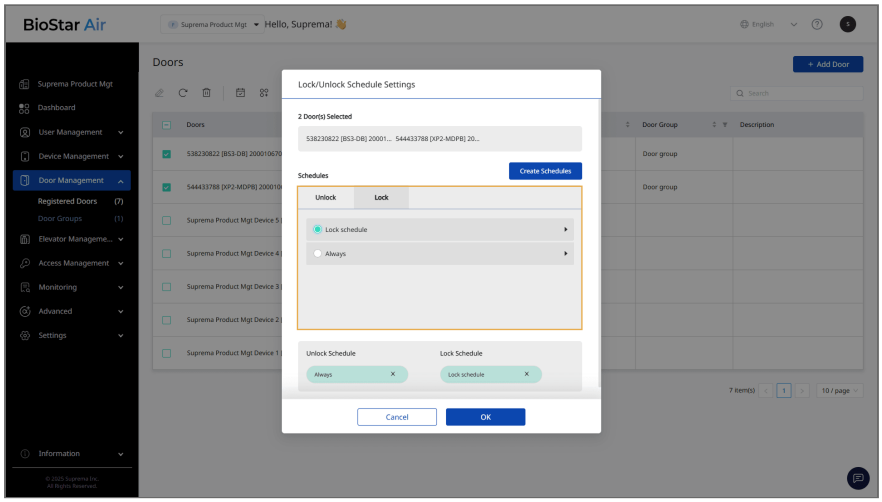
利用例

- 特定の時間以降厳格に閉鎖しなければならない区域
- プールやジム、その他出入り制限のある施設

施錠スケジュールの構成

次の手順に従って施錠スケジュールを構成します。

1. 画面左のサイドバーで **ドア管理** → **登録されたドア** をクリックしてください。
2. 出入口一覧で、施錠スケジュールを設定するドアのチェックボックスをクリックしてください。
3. 出入口一覧の上部にある ボタンをクリックしてください。
4. **ロック/アンロックスケジュール設定** ウィンドウが表示されたら、**ロック** タブで事前定義されたスケジュールを選択するか、新しいスケジュールを作成します。



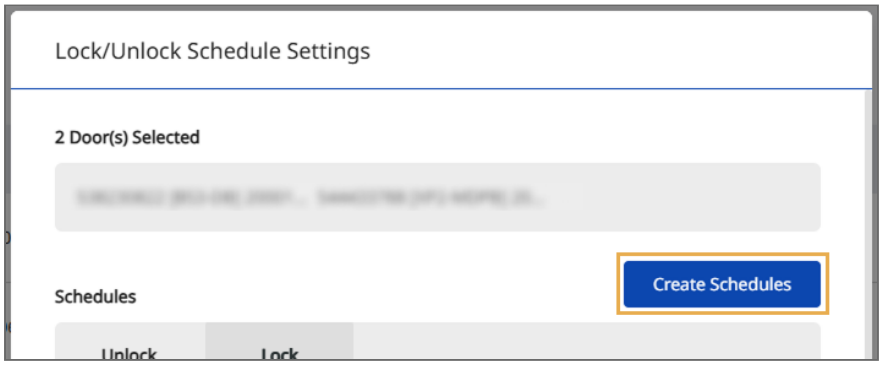
5. 施錠スケジュールを適用するには、**OK** ボタンをクリックします。

> **情報**
>
> - 施錠スケジュールは標準のアクセス権を無視するため、ユーザーは施錠時間中にドアを解錠状態に変更することはできません。
> - 新しいスケジュールの登録に関する詳細は 新しいスケジュールの登録 を参照してください。

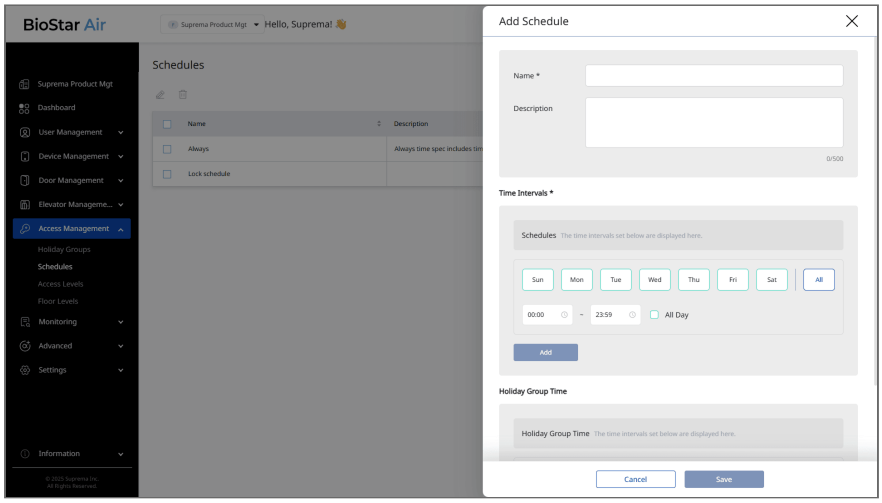
新しいスケジュールの登録

以下の手順に従って新しいスケジュールを登録します。

1. **ロック/アンロックスケジュール設定** ウィンドウで、**スケジュール作成** ボタンをクリックします。



2. スケジュール追加画面に移動したら、**名前** と **説明**(任意)を入力します。



3. **タイムスケジュール *** セクションで、認証なしでドアが開いている必要がある曜日と時間を選択し、**追加** ボタンをクリックします。

4. スケジュールを登録するには、**保存** ボタンをクリックします。

スケジュールを新規登録した後、**ドア管理** → **登録されたドア** に戻って、出入口のスケジュールを設定してください。

エレベーター

SupremaのOM-120モジュールを使用して、エレベーターのアクセス制御をサポートします。 OM-120モジュールを利用することで、管理者はBioStar Airと互換性のある機器と統合し、階ごとのアクセスを制御できます。 デイジーチェーン方式で接続されたOM-120装置により、最大144階まで対応します。

> **ヒント**
> エレベーター管理のビデオガイドを見るには、以下のビデオを参照してください。

エレベーター管理

エレベーターの入退室制御を構成するには、まず入退室制御装置にOM-120モジュールを接続します。 次に各階の名称とリレー番号を設定し、各階ごとにアクセス可能な時間帯をスケジュールで制限することで、セキュリティを強化できます。

要件

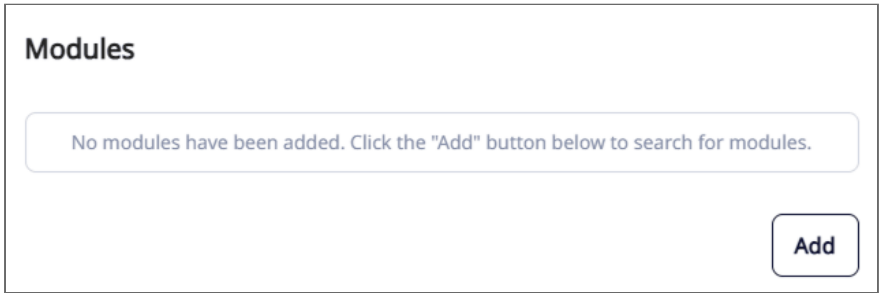
エレベーター出入制御機能を有効にするには、次の要件を満たす必要があります。

- Suprema OM-120モジュール: 各モジュールは最大12階まで対応します。 最大12台のOM-120モジュールを1つの出入制御デバイスに接続し、最大144階まで対応できます。
- OM-120を接続できるBioStar Air対応のデバイスが必要です。
- エレベーター制御盤への適切な配線作業が必要です。 配線の詳細はエレベーターの製造元にお問い合わせください。
- 階別のアクセススケジュールが優先され、休日設定によって通常のアクセスルールを上書きできます。

デバイスとモジュールの接続

1. 画面左のサイドバーで **デバイス管理** → **登録済みデバイス** をクリックします。

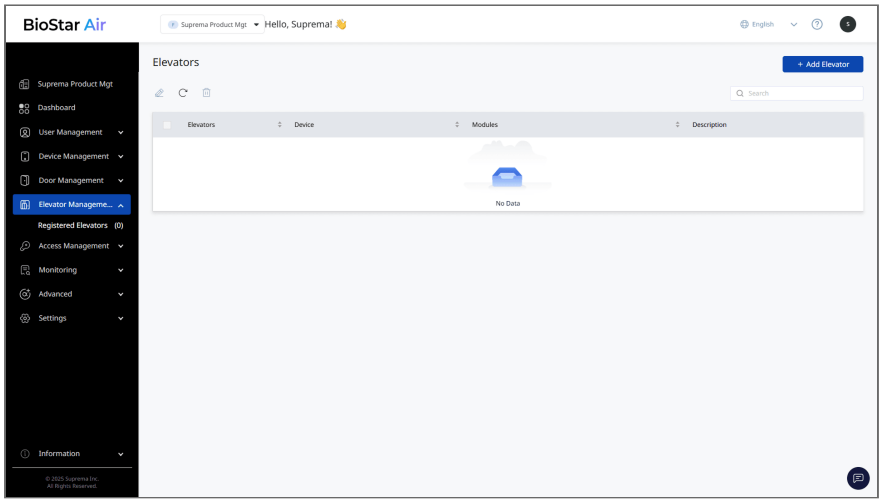
2. デバイス一覧でOM-120モジュールが接続された出入制御デバイスをクリックします。
3. **モジュール** セクションで **追加** ボタンをクリックしてください。



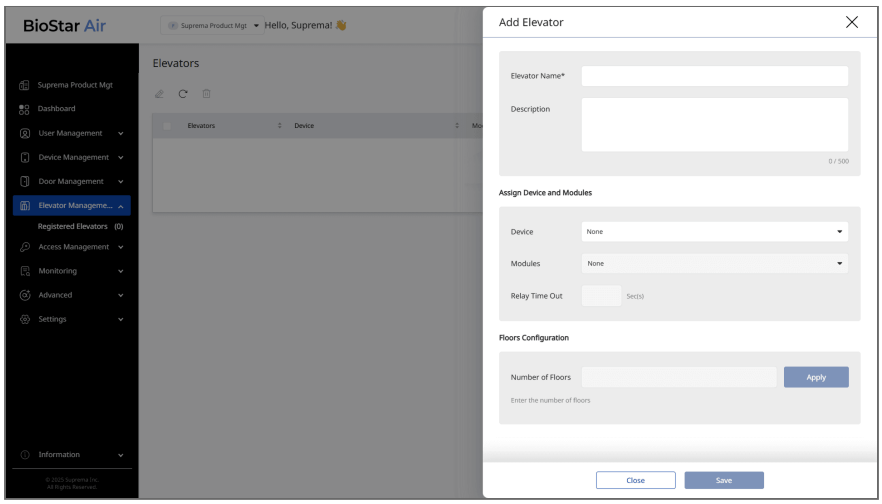
4. デバイスに接続されているOM-120モジュールを選択し、**保存** ボタンをクリックしてください。

エレベーター登録

1. 画面左のサイドバーで **エレベーター管理** → **登録エレベーター** をクリックします。
2. 画面右上の **エレベーターの追加** をクリックします。



3. **エレベーターの追加** パネルが表示されたら、**エレベーター名** および **説明**(オプション) を入力します。

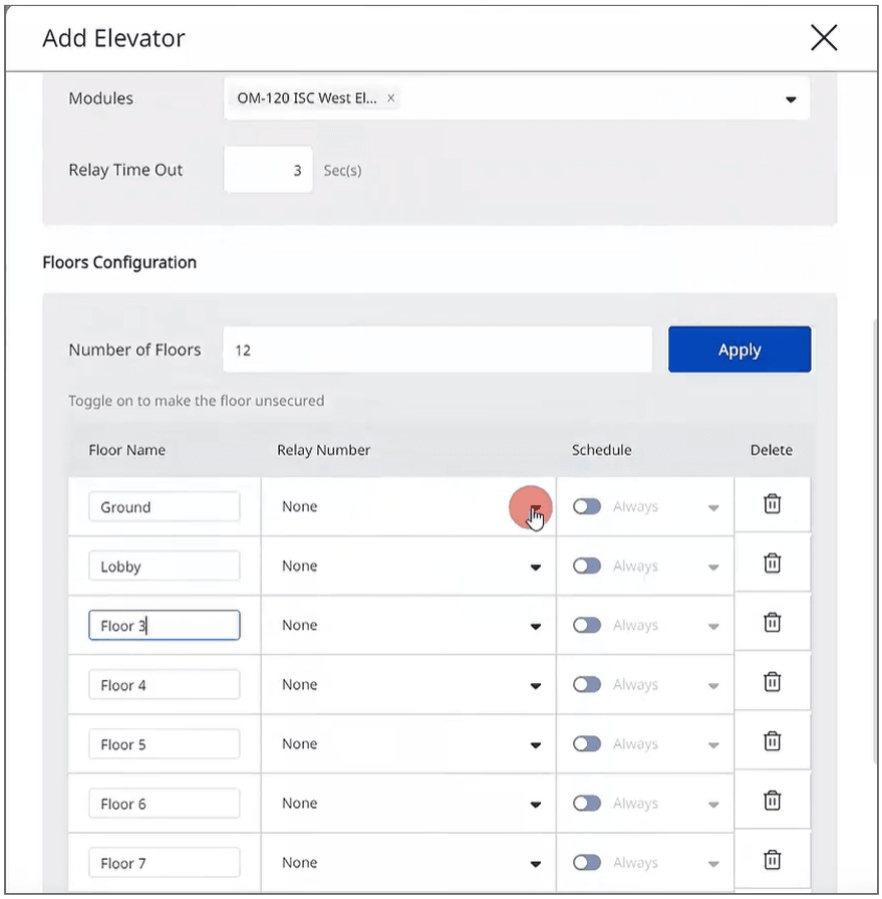


4. **デバイスとモジュールの割り当て** セクションで出入認証に使用するデバイスとモジュールを選択します。
   - **デバイス**：出入認証に使用するデバイスを選択します。

> **注意**
> デバイスが一覧に表示されない場合は、そのデバイスがドアに割り当てられているか確認してください。 デバイスはドアとエレベーターに同時に割り当てられません。

- **モジュール**：エレベーターボタンリレーを制御するOM-120モジュールを選択します。
- **リレータイムアウト**：認証完了後に階ボタンが有効な状態を維持する時間を設定します。 この時間を過ぎると、リレーは階ボタンに信号を送りません。

5. **フロア構成** セクションで制御する階数を入力し、**適用** をクリックします。
6. 各階の名前、リレー番号、スケジュールを設定します。



上記の画像は例示です。実際の画面とは異なる場合があります。

- **フロア名**：階の名前を入力します。 1階、ロビー、会議室の階など、識別しやすい名前を使用してください。
- **リレー番号**：エレベーター制御盤で各階のボタンに対応するリレー出力を選択します。
- **スケジュール**：各階にアクセスできるスケジュールを設定します。 例えば、勤務時間外はメンテナンス階へのアクセスを制限できます。

7. エレベーター設定を保存して登録するには、**保存** をクリックします。

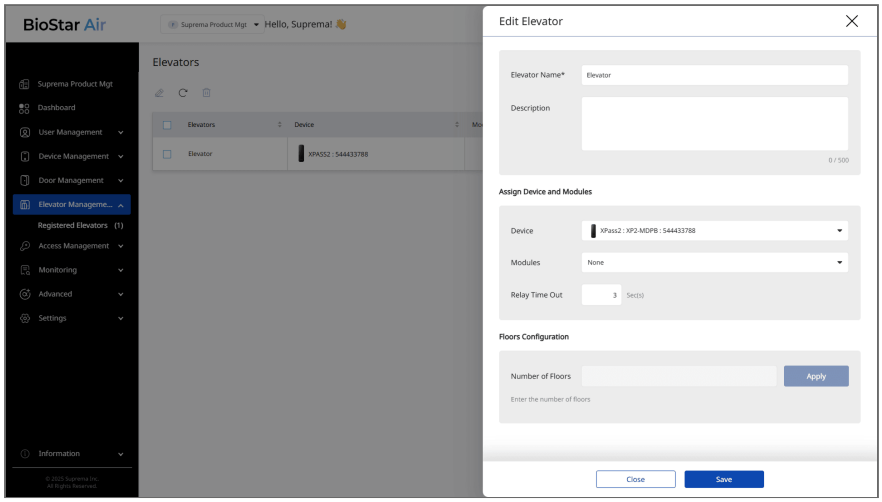
情報

- OM-120モジュールあたり最大12階を対応します。 複数のOM-120モジュールをデイジーチェーン方式で接続して、最大144階まで拡張できます。
- **フロア構成** セクションで階を削除するには、 ボタンをクリックしてください。
- スケジュール登録方法に関する詳細は、スケジュールを管理する を参照してください。

エレベーター編集

登録済みのエレベーターの詳細を変更するか、設定を編集するには、次の手順に従ってください。

1. 画面左のサイドバーで **エレベーター管理** → **登録エレベーター** をクリックします。
2. 一覧から編集するエレベーターをクリックします。 またはエレベーターのチェックボックスをクリックし、一覧上部の ボタンをクリックしてください。
3. **エレベーターの編集** パネルが表示されたら、必要な情報を変更するか設定を編集します。



4. 変更を保存するには、**保存** をクリックします。

エレベーター削除

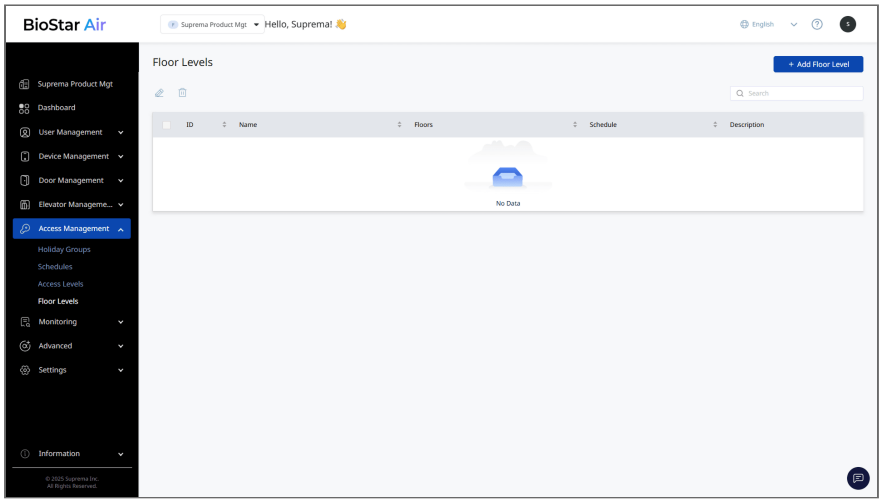
登録されたエレベーターを削除するには、次の手順に従ってください。

1. 画面左のサイドバーで **エレベーター管理** → **登録エレベーター** をクリックします。
2. 一覧で削除するエレベーターのチェックボックスをクリックします。 1台以上のエレベーターを選択できます。
3. 一覧上部の ボタンをクリックしてください。
4. 警告メッセージのウィンドウが表示されたら、**はい** をクリックします。

階別アクセス権の設定

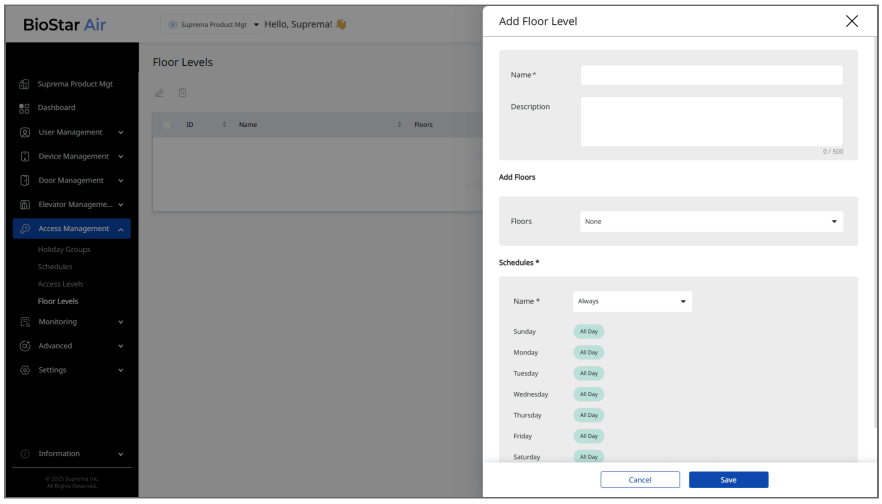
エレベーターを登録し、階レベルを定義して、ユーザーやグループがアクセスできる階を制限します。 各階レベルごとにアクセススケジュール（例：勤務時間内）と休日ポリシーを設定し、セキュリティと利便性を両立して管理できます。

1. 画面左のサイドバーで **アクセス管理** → **フロアレベル** をクリックします。
2. 画面右上の **フロアレベルを追加** をクリックします。



3. **フロアレベルを追加** パネルが表示されたら、**名前** と **説明**(オプション) を入力します。

   > *例：セキュリティチーム、清掃スタッフ*



4. **フロアを追加する** セクションで階レベルを適用する階を選択します。
5. **スケジュール** セクションでアクセススケジュールを設定してください。

   > *例：清掃スタッフの場合は勤務時間外のみアクセスを許可します。*

6. 必要に応じて、**休日グループ** を追加して特定の日のアクセスを制限します。
7. 階レベルを追加するには、**保存** をクリックします。

> **情報**
> 階レベルの追加・編集・削除の詳細は フロアレベルを管理するを参照してください。

アクセス権限

入退室権限の管理はセキュリティシステムの中核です。 休暇グループ、スケジュール、アクセスレベル、フロアレベルを組み合わせて、ユーザーがいつどこで入退室できるかを細かく制御します。

ヒント
入退室権限管理のビデオガイドを視聴するには、次の動画を参照します。

祝日グループを管理する

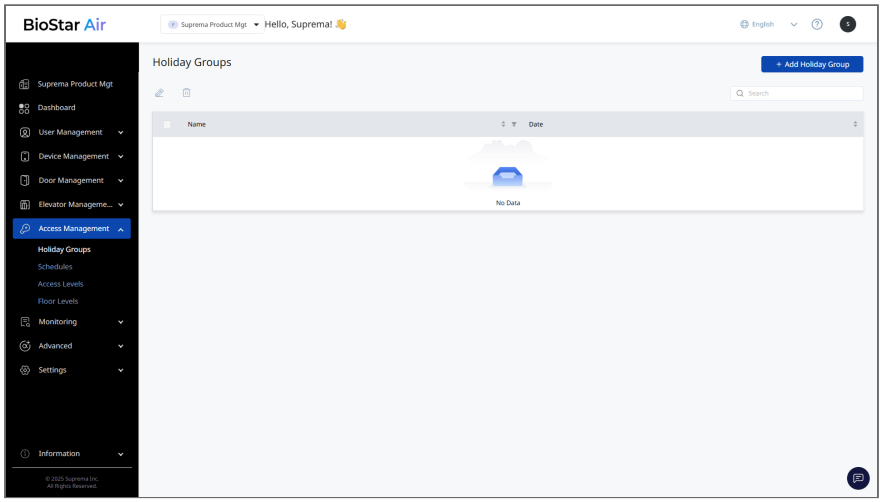
BioStar Airでは、祝日グループは特定の日付や期間の間に出入ルールを調整するために使用されます。 祝日グループを設定すると、管理者は祝日や特別な日に出入権限を制限または変更できます。 これにより、セキュリティレベルを維持しながら柔軟な出入管理を実現できます。

ヒント
出入管理に関するビデオガイドを視聴するには、次の動画を参照してください。

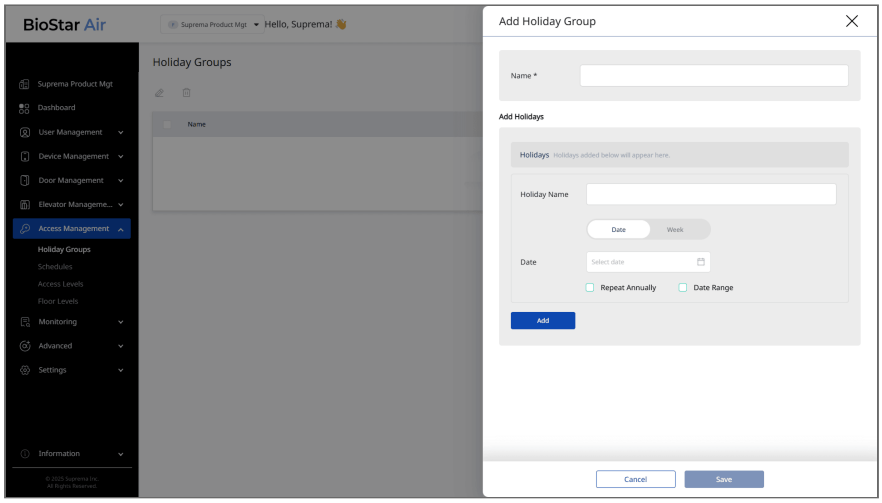
祝日グループを追加

祝日グループは、毎年繰り返される祝日や特定期間の休日を定義し、その期間中に出入権限を制限または変更するために使用されます。

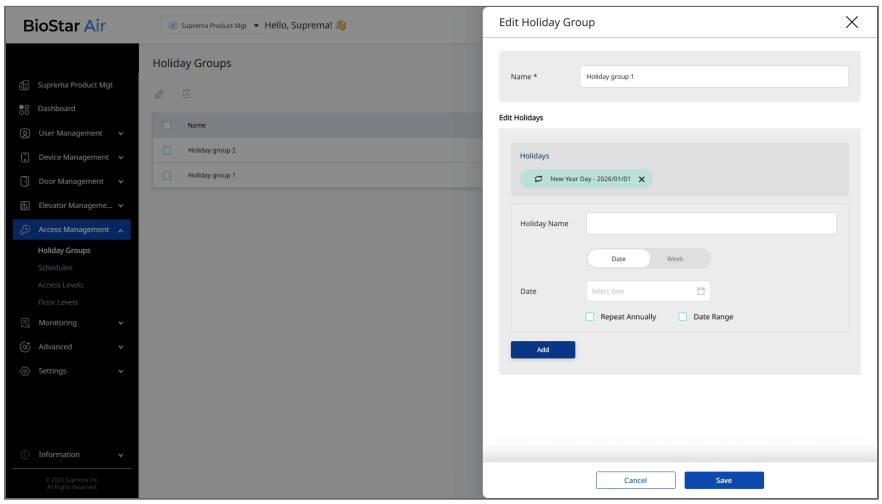
1. 画面左のサイドバーで **アクセス管理** → **休日グループ** をクリックしてください。
2. 画面右上の **休日グループの追加** ボタンをクリックします。



3. **休日グループの追加** パネルが表示されたら、グループ名を入力します。



4. **休日の追加** セクションで休日名と日付を指定し、**追加** ボタンをクリックします。
   - 日付が固定された祝日を追加するには、名前と日付を設定し、**毎年繰り返す** オプションを選択します。
   - 毎年繰り返されるが、一定期間を持つ休日の場合は、名前と日付を設定し、**日付範囲** オプションを選択します。
5. 同じ方法で他の休日を追加します。

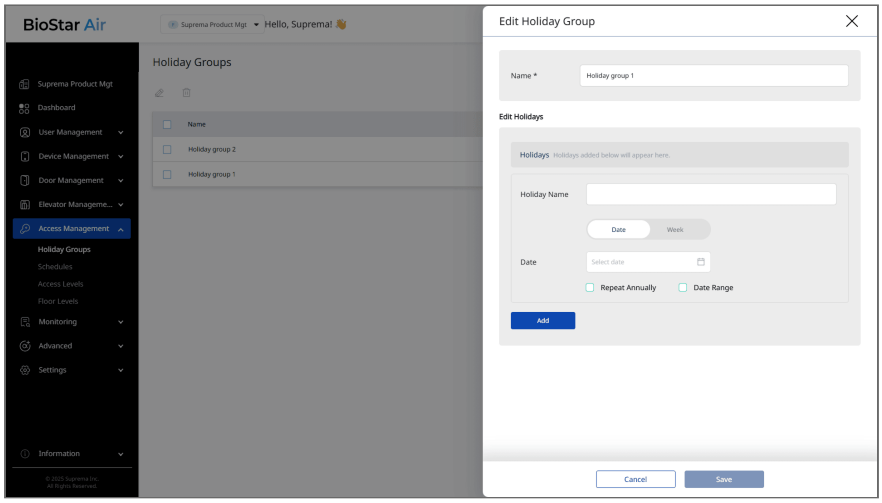


6. 休日グループの設定を保存するには、**保存** ボタンをクリックします。

> **情報**
>
> - 祝日グループはスケジュールより優先されます。 常に出入りが必要なユーザーには、制限のないアクセス権を付与してください。
> - 1つのドアには、1つの祝日グループしか適用できません。

祝日グループを編集

1. 画面左のサイドバーで **アクセス管理** → **休日グループ** をクリックしてください。
2. 一覧から編集する祝日グループをクリックしてください。 または、祝日グループのチェックボックスをクリックして選択し、一覧の上部にある ボタンをクリックしてください。
3. **休日グループの編集** パネルが表示されたら、希望の項目を編集してください。



4. 変更を保存するには、**保存** をクリックします。

祝日グループを削除

1. 画面左のサイドバーで **アクセス管理** → **休日グループ** をクリックしてください。
2. 一覧で祝日グループのチェックボックスをクリックしてください。 1つ以上の祝日グループを選択できます。
3. 一覧上部の🗑 ボタンをクリックしてください。
4. 警告メッセージのウィンドウが表示されたら、**はい** をクリックします。

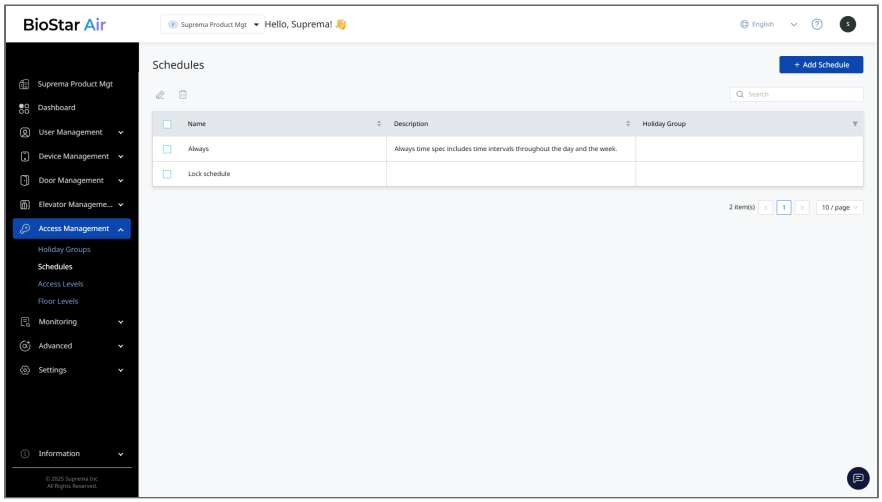
スケジュールを管理する

スケジュールを作成して、特定の曜日と時間帯にドアやエレベーターへの入退室を許可または制限します。 祝日グループと併用すると、出入りルールをさらに細かく調整できます。

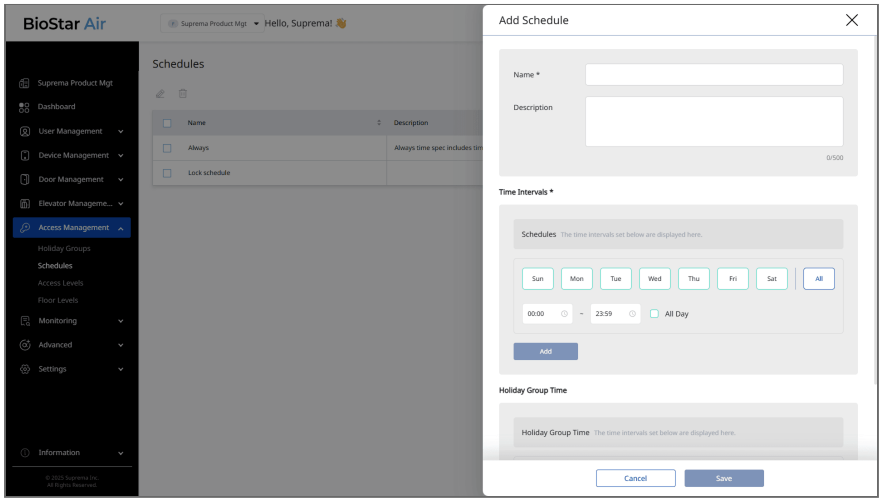
> **情報**
>
> - 祝日グループはスケジュールより優先されます。 常に出入りが必要なユーザーには、制限のないアクセス権を付与してください。
> - 祝日グループの設定の詳細については 祝日グループを管理する をご参照ください。
> - ドアにスケジュールを適用する方法の詳細については 出入口スケジュールの管理 をご参照ください。
> - エレベーターの各階での入退室を制御するスケジュール設定の詳細については エレベーター をご参照ください。

スケジュールを追加

1. 画面左のサイドバーで **アクセス管理** → **スケジュール** をクリックします。
2. 画面右上の**スケジュールの追加**ボタンをクリックしてください。



3. **スケジュールの追加** パネルが表示されたら、**名前** と **説明**（オプション）を入力します。

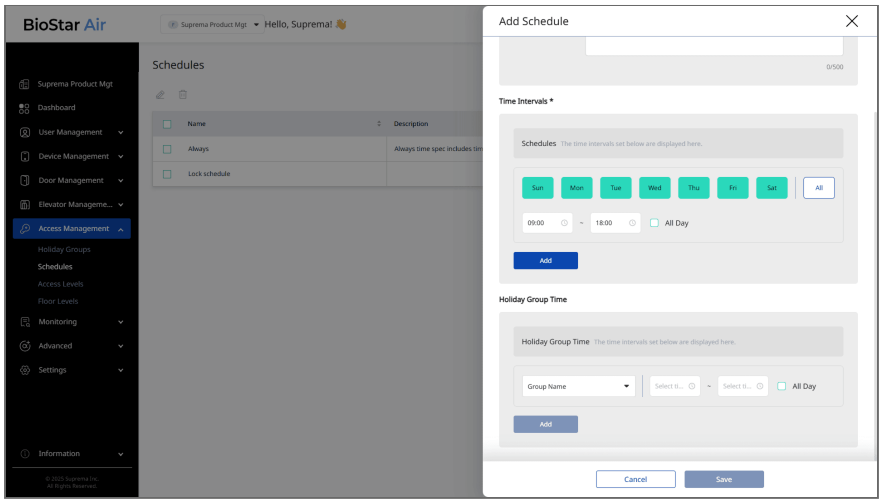


4. **タイムスケジュール** * セクションで曜日と時間を選択します。

> *たとえば、勤務時間を設定するには、月曜日から金曜日まで、午前9時から午後6時まで選択します。逆に勤務時間外のスケジュールを設定するには、土曜日と日曜日、または毎日午後6時から翌朝午前9時まで選択します。*

5. 選択したスケジュールを適用するには、**追加** ボタンをクリックします。

6. **休日グループタイム** セクションでスケジュールに適用する休日グループを選択し、時間を設定します。



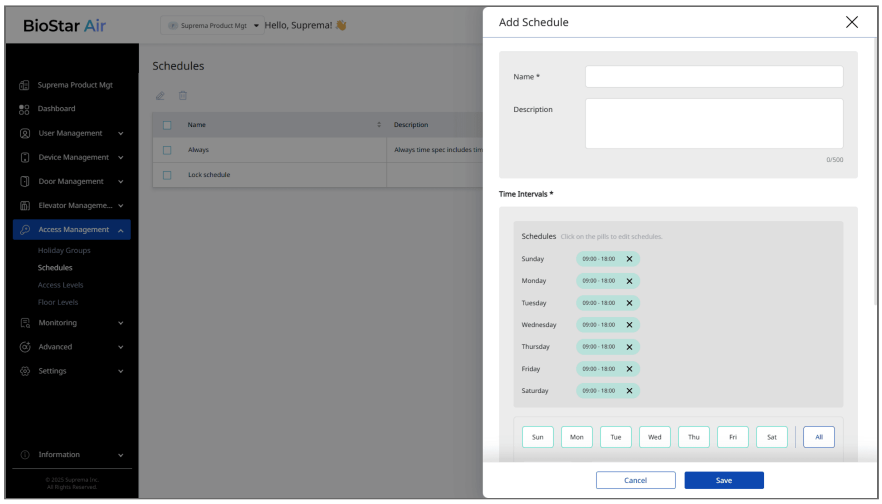
7. 休日グループを適用するには、**追加** ボタンをクリックします。

8. スケジュールを追加するには、**保存** ボタンをクリックします。

> **情報**
>
> - 入室を許可する開錠スケジュールと入室を制限する施錠スケジュールを追加して、ドアに適用できます。 ドアにスケジュールを適用する方法の詳細については 出入口スケジュールの管理 をご参照ください。
> - 1つのスケジュールには、1つの祝日グループしか適用できません。
> - エレベーターの各階での入退室を制御するスケジュール設定の詳細については エレベーター をご参照ください。

スケジュールを編集

1. 画面左のサイドバーで **アクセス管理** → **スケジュール** をクリックします。
2. 一覧から編集するスケジュールをクリックします。 または、スケジュールのチェックボックスをクリックして、一覧上部の ボタンをクリックしてください。
3. **スケジュールの編集** パネルが表示されたら、必要な情報を変更するかスケジュールを編集します。



4. 変更を保存するには、**保存** をクリックします。

スケジュールを削除

1. 画面左のサイドバーで **アクセス管理** → **スケジュール** をクリックします。
2. 一覧から削除するスケジュールのチェックボックスをクリックします。 1件以上のスケジュールを選択できます。
3. 一覧上部の ボタンをクリックしてください。
4. 警告メッセージのウィンドウが表示されたら、**はい** をクリックします。

> **情報**
>
> スケジュールを削除すると、すべての関連セクションからスケジュールが削除されます。 例えば、ドアやエレベーターに適用されているスケジュールが削除されると、当該ドアやエレベーターにはもはやスケジュールが適用されません。

出入レベルの管理性行する

出入レベルを使用してユーザーの入退室権限を細かく制御してください。 出入レベルは、誰がいつどこで入退室できるかを定義する重要な要素です。 出入レベルは以下の要素で構成されます。

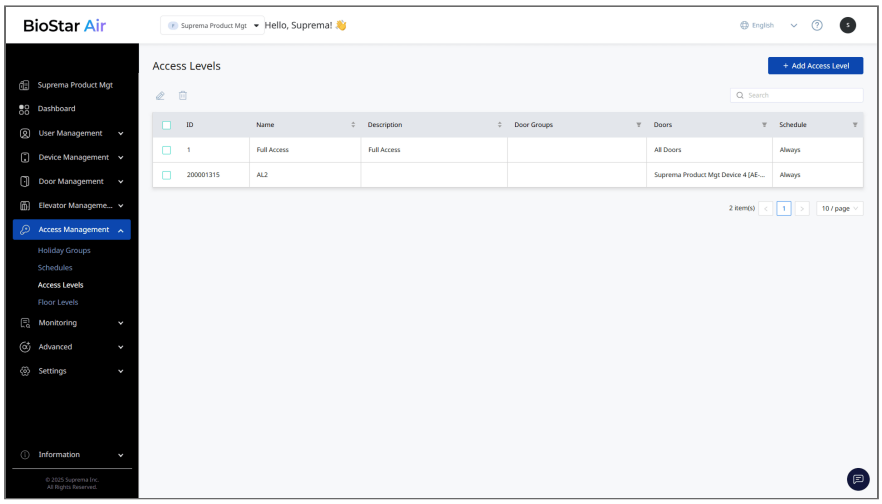
- **出入口 / 出入口グループ**: 入退室を許可する場所
- **スケジュール**: 入退室を許可する時間
- **休日グループ**: 入退室を制限または調整する日付および期間

ユーザーを追加する前に出入レベルを設定すると、ユーザー管理プロセスを簡素化できます。

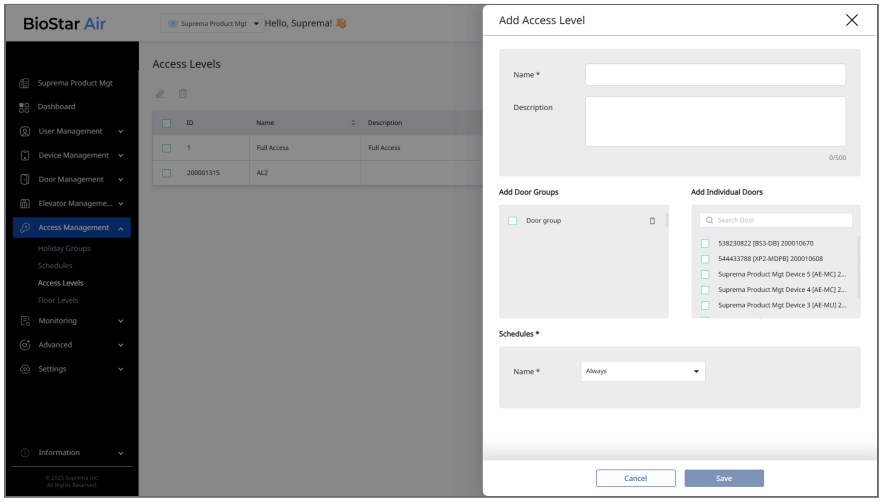
出入レベルの追加

出入レベルを使用して、出入口、スケジュール、および休日に基づいてユーザーの権限を設定できます。

1. 画面左のサイドバーで **アクセス管理** → **アクセスレベル** をクリックしてください。
2. 画面右上の **アクセスレベルの追加** ボタンをクリックします。



3. **アクセスレベルの追加**パネルが表示されたら、**名前**と**説明**(任意)を入力してください。

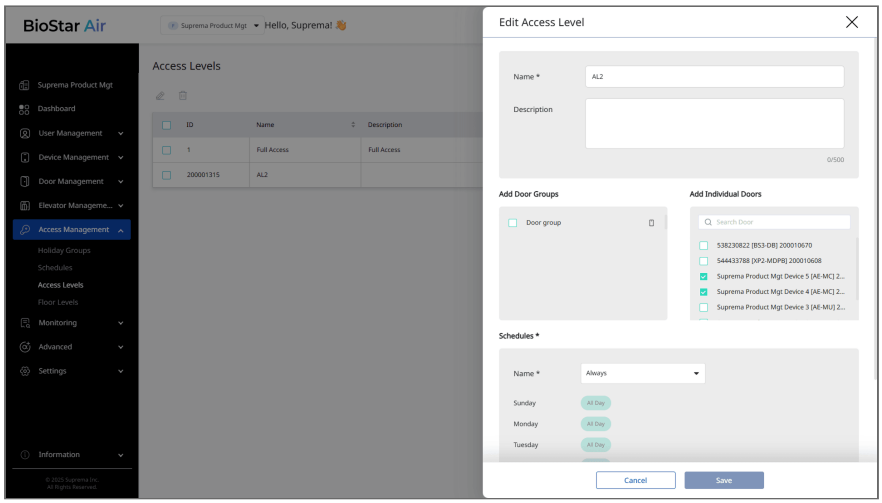


4. **ドアグループを追加** または **個別のドアを追加** セクションでドアグループまたは個別のドアを選択します。
5. **スケジュール**セクションで、アクセスレベルに適用するスケジュールを選択してください。 **常時**を選択して、制限のないアクセスを許可します。
6. アクセスレベルを追加するには、**保存** ボタンをクリックします。

出入レベルの編集

1. 画面左のサイドバーで **アクセス管理** → **アクセスレベル** をクリックしてください。

2. リストから編集する出入レベルをクリックしてください。 または、編集したい出入レベルのチェックボックスを選択し、リスト上部の ボタンをクリックしてください。



3. **アクセスレベルの編集** パネルが表示されたら、必要な情報を修正するか設定を変更してください。

4. 変更を保存するには、**保存** をクリックします。

出入レベルの削除

1. 画面左のサイドバーで **アクセス管理** → **アクセスレベル** をクリックしてください。

2. リストで削除する出入レベルのチェックボックスをクリックしてください。 1つ以上の出入レベルを選択できます。

3. 一覧上部の ボタンをクリックしてください。

4. 警告メッセージのウィンドウが表示されたら、**はい** をクリックします。

フロアレベルを管理する

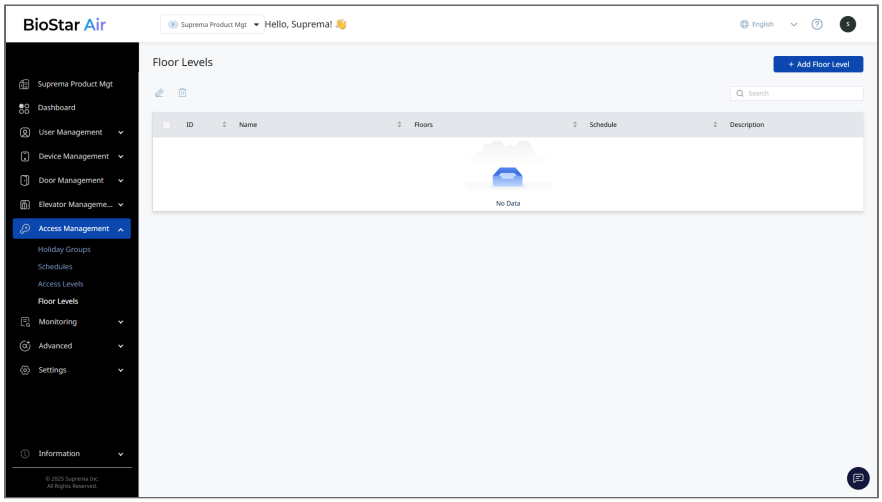
フロアレベルはエレベーターのアクセス制御設定で使用されます。 フロアレベルを使用して、各フロアへのアクセス権限を細かく制御します。 例えば、特定のユーザーグループを特定のフロアのみにアクセスさせるよう設定します。

フロアレベルを追加

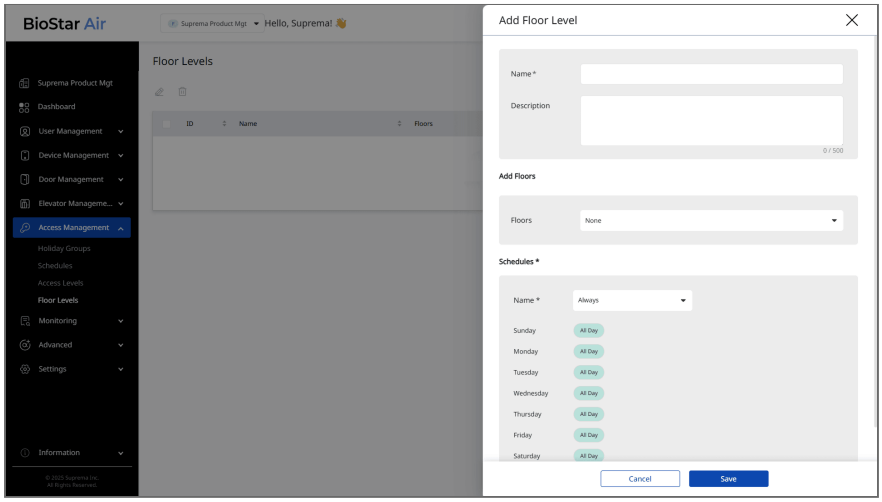
特定のフロアにアクセスできるユーザーまたはグループを設定します。

1. 画面左のサイドバーで **アクセス管理** → **フロアレベル** をクリックします。

2. 画面右上の **フロアレベルを追加** をクリックします。



3. **フロアレベルを追加**パネルが表示されたら、**名前**および**説明**(任意)を入力します。



4. **フロアを追加する**セクションで、フロア権限を適用するフロアを選択します。

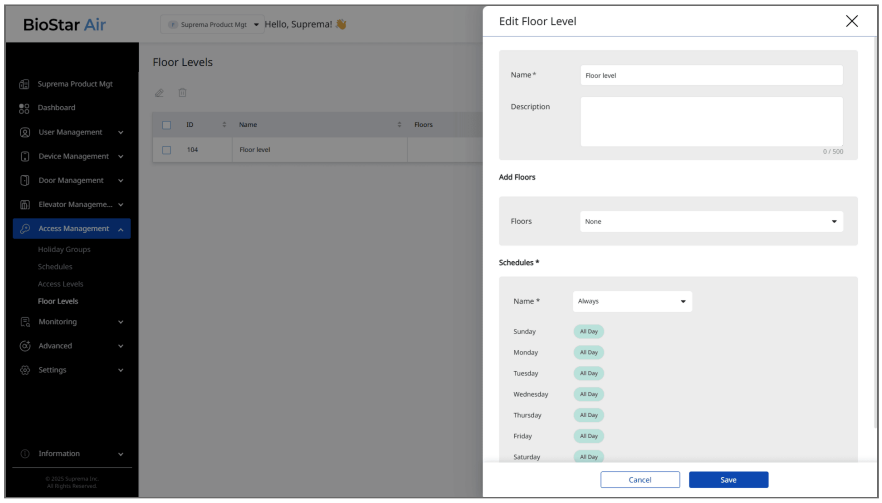
5. **スケジュール**セクションで、フロアレベルに適用するスケジュールを選択します。 **常時**を選択して、制限のないアクセスを許可します。

6. 階レベルを追加するには、**保存** をクリックします。

フロアレベルを編集

1. 画面左のサイドバーで **アクセス管理** → **フロアレベル** をクリックします。

2. 一覧で編集するフロアレベルをクリックします。 または、編集するフロアレベルのチェックボックスをクリックし、一覧上部の ボタンをクリックしてください。



3. **フロアレベルの編集**パネルが表示されたら、必要な情報を編集するか設定を変更します。
4. 変更を保存するには、**保存** をクリックします。

フロアレベルを削除

1. 画面左のサイドバーで **アクセス管理** → **フロアレベル** をクリックします。
2. 一覧で削除するフロアレベルのチェックボックスをクリックします。 1つ以上のフロアレベルを選択できます。
3. 一覧上部の ボタンをクリックしてください。
4. 警告メッセージのウィンドウが表示されたら、**はい** をクリックします。

ゾーン管理

ゾーン(Zone)は、出入口と装置を論理的にまとめた単位です。アンチパスバック(Anti-passback、APB)の適用、在場状況の確認、人数集計に加え、今後追加されるさまざまな機能にも活用できます。

ゾーンとアンチパスバック(APB)の理解

ゾーンにアンチパスバック機能を適用するには、まず管理者が対象ゾーンの出入ポイント(入室ポイントと退室ポイント)を設定する必要があります。 システムはこの設定に基づき、ユーザーがゾーン内かゾーン外かを判断します。 ゾーンから退室していないユーザーは、別の認証手段を使用しても同じゾーンに再入室できません。 また、アンチパスバック機能は入室と退室のポイントを明確に定義し、来た経路への戻りや、入室した扉からの退出を防ぎます。

境界ゾーン(Perimeter Zone)

BioStar Airは、アンチパスバックと同様にユーザーの在場状況を把握できる**境界ゾーン**(Perimeter Zone)の概念を提供します。 境界ゾーンは、**在場者確認**(On-Site Now)と**緊急点呼**(Roll Call)機能で中核的な役割を果たします。 必要に応じて、境界ゾーンにもアンチパスバック機能を適用できます。

以下のドキュメントを参照して、BioStar Airポータルでゾーンと APB違反を管理する方法を確認してください。

ゾーン管理
BioStar Airの**ゾーン**(Zone)機能を使用すると、出入口を論理的なゾーンに分け、必要に応じて**アンチパスバック**(Anti-Passback, APB)ルールを適用し、ユーザーが正しい順序で入室・退室するように強制します。 アンチパスバックルールはゾーンごとに任意で適用でき、適用しないゾーンでも在席者の確認など、他のゾーン機能はそのまま使用できます。 **ゾーン**は、サイト全体を対象に

する境界ゾーンから、建物内の特定エリアまで自由に構成できます。

開始前に

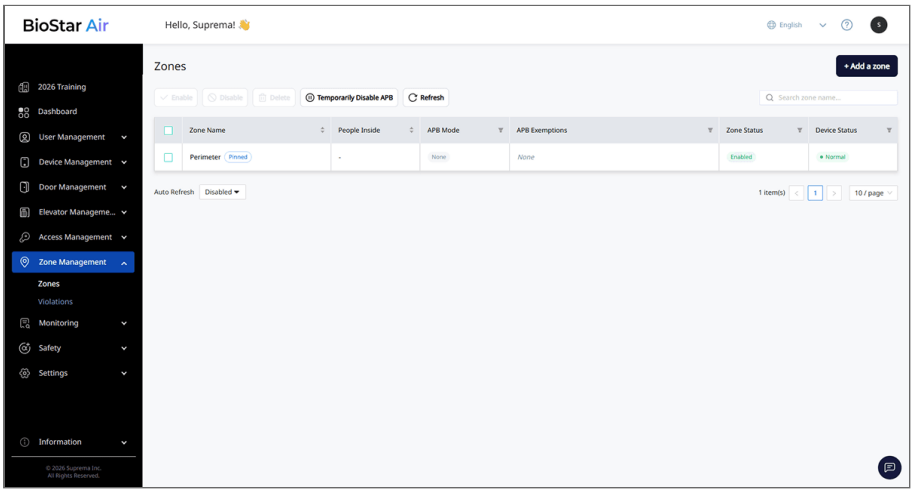
ゾーンを作成する前に、次の事項を確認してください。

- ゾーンに割り当てるドアを先に登録する必要があります。 ドアの登録方法については、登録済みドアの管理をご参照ください。
- 一台のデバイスは、一度に一つのゾーンでしか使用できません。
- ゾーンの入室/退室デバイスを変更しても、ドア自体の設定は変更されません。
- ゾーンの入室/退室デバイスを正しく設定しないと、APBの動作と在席人数が実際の移動と異なって表示される場合があります。
- オフラインデバイスは、オンラインデバイスより変更内容の反映が遅れる場合があります。 変更内容はオンラインデバイスに先に適用され、オフラインデバイスはオンラインに再接続した後に適用されます。
- ファームウェアが **v2.13** 以上のデバイスのみ、ゾーンに割り当てできます。 ゾーンに割り当てるデバイスが最新ファームウェアであることを確認してください。
- APBゾーンで使用中のドアは、設定の競合を防ぐために保護されます。 ドア設定でAPBの動作に影響する内容を変更する前に、該当ドアをゾーンから除外してください。

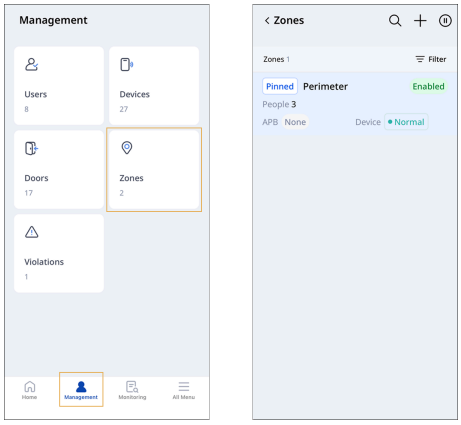
ゾーン一覧の概要

Web

画面左側のサイドバーで **ゾーン管理** → **ゾーン** をクリックしてください。



Mobile



1. モバイル端末でBioStar Airアプリを起動してログインします。
2. 画面の下部にある **管理** をタップします。
3. **ゾーン** カードをタップしてください。

ゾーン一覧では、サイトに設定したすべてのゾーンを一目で確認できます。

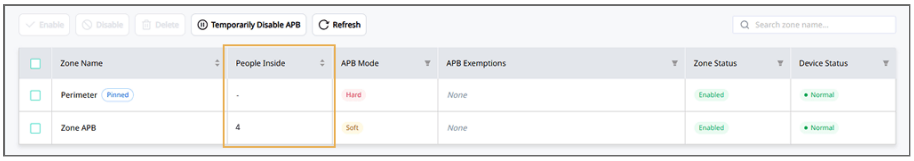
- **ゾーン名**：ゾーン名です。 **境界** では、名前の横に **ピン留め** バッジが表示されます。
- **入室人数**：現在、そのゾーン内に在席していると記録されたユーザー数です。 詳細については、内部在席人数の確認をご参照ください。
- **APBモード**：ゾーンに適用したAPBモード（**Hard**/**Soft**/**なし**）です。
- **APB免除**：ゾーンに指定したAPB例外グループです。
- **ゾーンステータス**：ゾーンの有効化状況です。
- **デバイスステータス**：ゾーンに割り当てたデバイスのオンライン状態です。

> **境界と内部ゾーン**
>
> サイトを最初に設定すると、**境界**(Perimeter Zone)がデフォルトで提供されます。 **境界**はサイトの正門のようなゾーンです。名前の変更や削除はできず、一覧では**ピン留め**バッジで表示されます。
> - **境界**で使用する入室・退室デバイスは、**ダッシュボード**メニューの**オンサイトのユーザー**と、**安全** → **在席**メニューで在席状態を算出する基準にもなります。
> - 境界以外にも、内部統制が必要な領域（例：サーバールーム、特定の階）ごとに別のゾーンを追加作成し、サイト内でも細かな移動制御を適用できます。

内部在席人数の確認

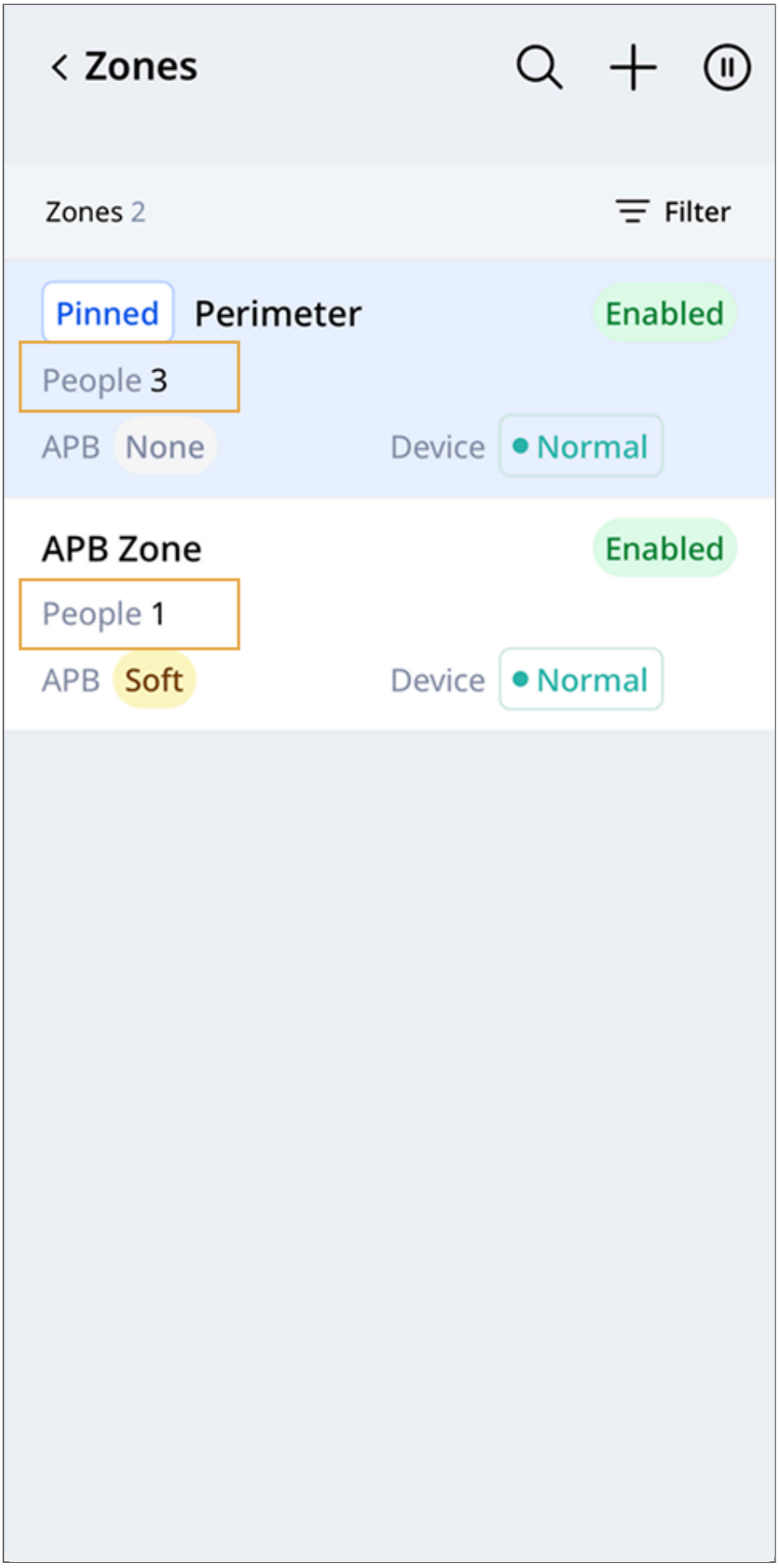
Web

ゾーン一覧の**入室人数**列で、各ゾーンの現在の在席人数を確認します。



Mobile

ゾーン一覧の**People**項目で、各ゾーンに現在何人いるかを確認できます。

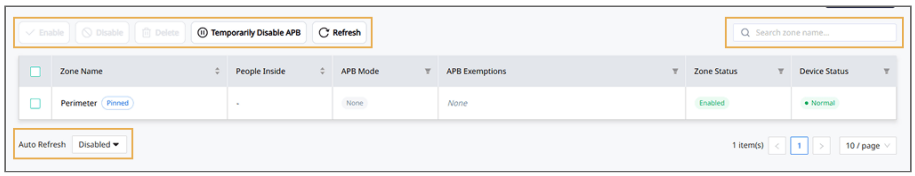


- この数値は、ゾーンに設定した入室・退室デバイスの認証記録を基に算出します。 入室デバイスで認証すると人数が増え、退室デバイスで認証すると人数が減ります。

- APB例外グループに属するユーザーはAPBルールの適用対象外ですが、在席人数には引き続き含めます。
- ゾーンを無効化すると、そのゾーンの在席人数を0に初期化します。
- 最新の値を維持するには、一覧上部の**リフレッシュ**ボタンをクリックするか、自動更新間隔を設定してください。

ゾーン管理機能

ゾーン一覧の上部と下部にある管理機能で、次の作業を実行します。



- **有効化** / **無効化**: 選択したゾーンを有効化または無効化します。
- **削除**：選択したゾーンを削除します。 **境界**は削除できません。
- **APBを一時停止**：境界を含むサイトのすべてのゾーンで、APBの適用を一括で停止します。
- **リフレッシュ**：一覧をすぐに更新し、最新状態にします。 一覧下部の**自動更新**で自動更新間隔(**無効**/**５秒**/**１分**)を選択すると、設定した周期で一覧を自動更新します。
- **ゾーン名を検索…**：ゾーン名で一覧を検索します。

ゾーンリストのフィルタリング

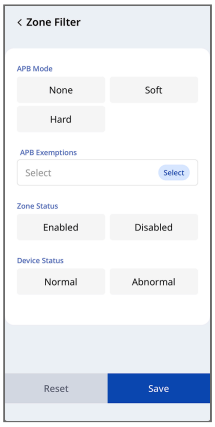
Web

リスト上部ヘッダーの **APBモード**, **APB免除**, **ゾーンステータス**, **デバイスステータス** 列にある ボタンをクリックすると、該当条件でリストをフィルタリングします。



> **情報**
> フィルターを解除するには **リセット** ボタンをクリックします。

Mobile



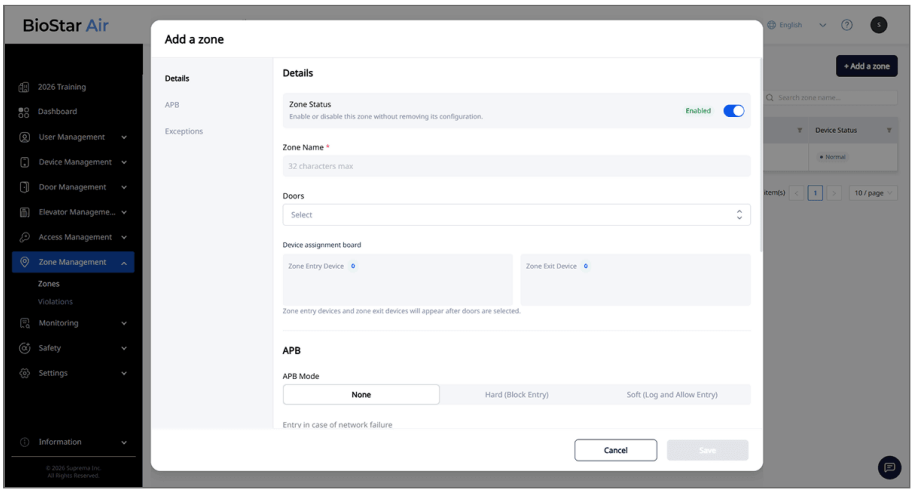
1. ゾーン一覧の右上にある **フィルター** をタップします。
2. **APBモード**、**APB免除**、**ゾーンステータス**、**デバイスステータス**で必要な条件を選択します。
3. 選択した条件で一覧をフィルタリングするには **保存** ボタンをタップします。

> **情報**
> フィルターを解除するには **リセット** ボタンをタップします。

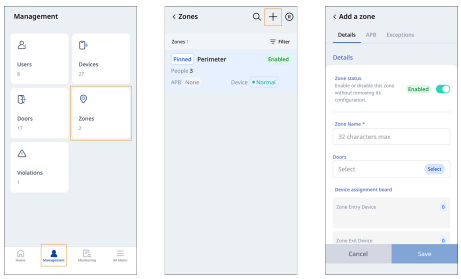
ゾーンの追加

Web

画面左側のサイドバーで **ゾーン管理** → **ゾーン** をクリックしてください。 画面右上の**+ ゾーンを追加**ボタンをクリックしてください。



Mobile

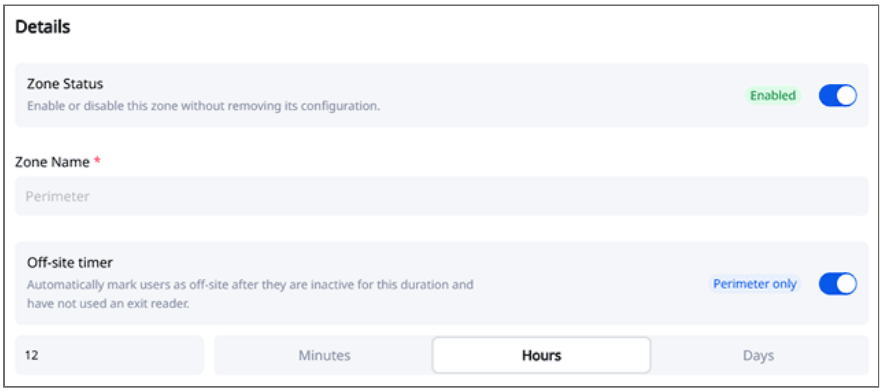


1. BioStar Air アプリ画面下部の **管理**をタップします。
2. **ゾーン** カードをタップしてください。
3. 画面右上の ＋ ボタンをタップします。

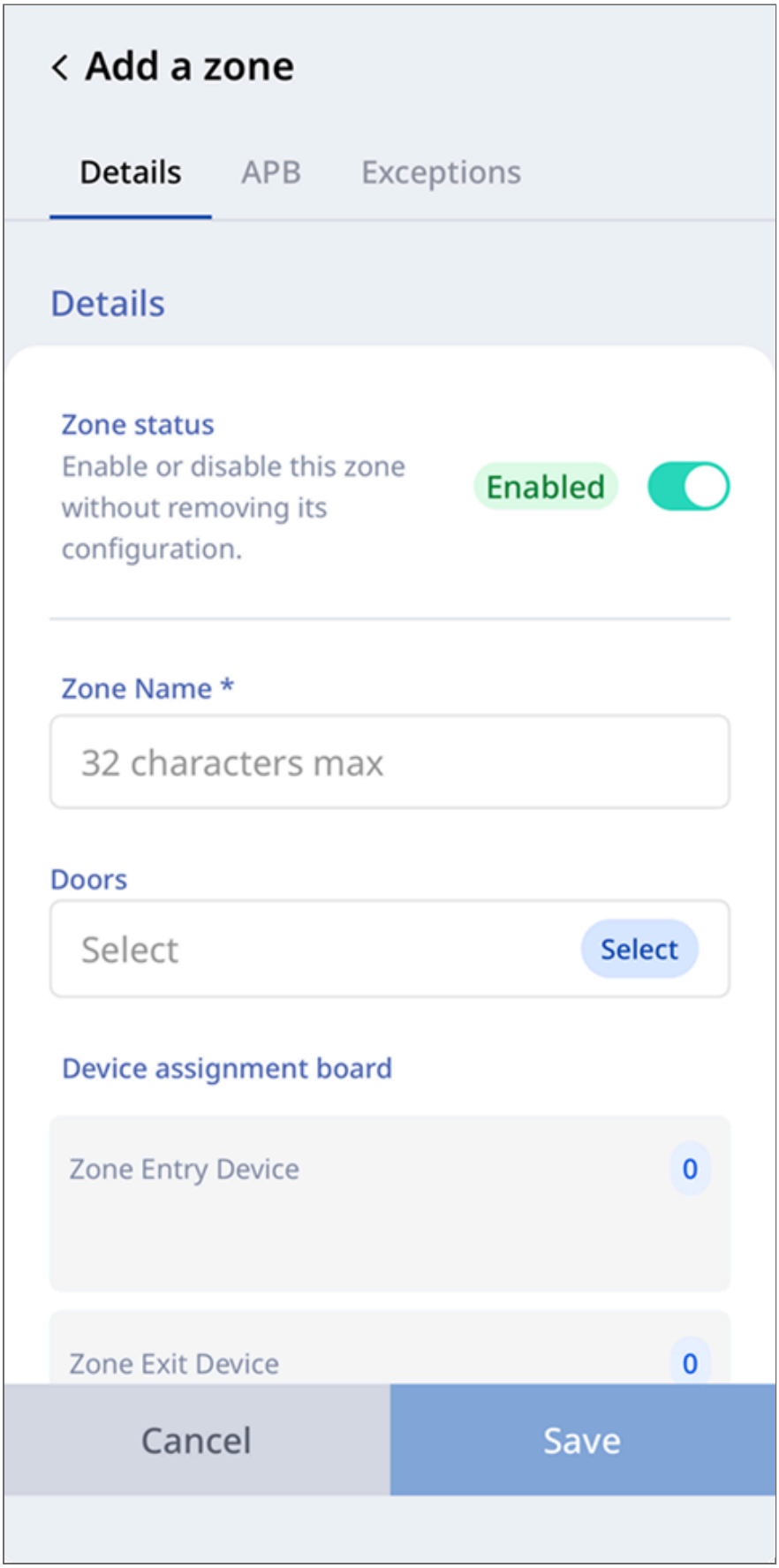
1 基本情報の入力

詳細 セクションでゾーンの基本情報を入力します。

Web


Details
Zone Status
Enable or disable this zone without removing its configuration.
Enabled
Zone Name *
Perimeter
Off-site timer
Automatically mark users as off-site after they are inactive for this duration and have not used an exit reader.
Perimeter only
12
Minutes
Hours
Days

Mobile



- **ゾーンステータス**：ゾーンをすぐに有効化するか選択します。 設定を保持したまま、後で有効化または無効化できます。
- **ゾーン名**：32文字以内で入力してください。 複数の建物があるサイトでは、場所がすぐ分かる名前の使用を推奨します。

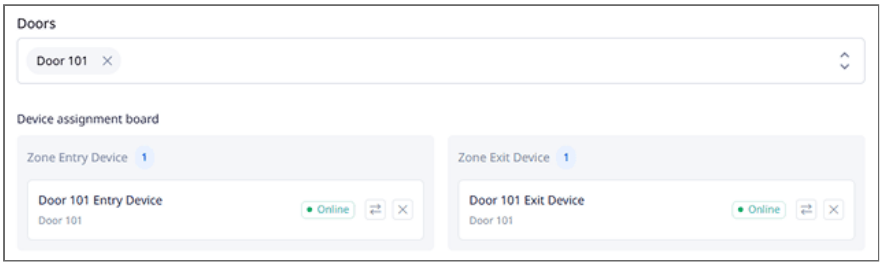
- **オフサイトタイマー**: 設定した時間、アクティビティがなく、退室デバイスも使用しないユーザーは **オフサイト** 状態に自動的に切り替わります。 境界に退室デバイスを指定していない場合は、必ず設定してください。

> **情報**
> **オフサイトタイマー** オプションは、境界の設定時にだけ表示される専用オプションです。

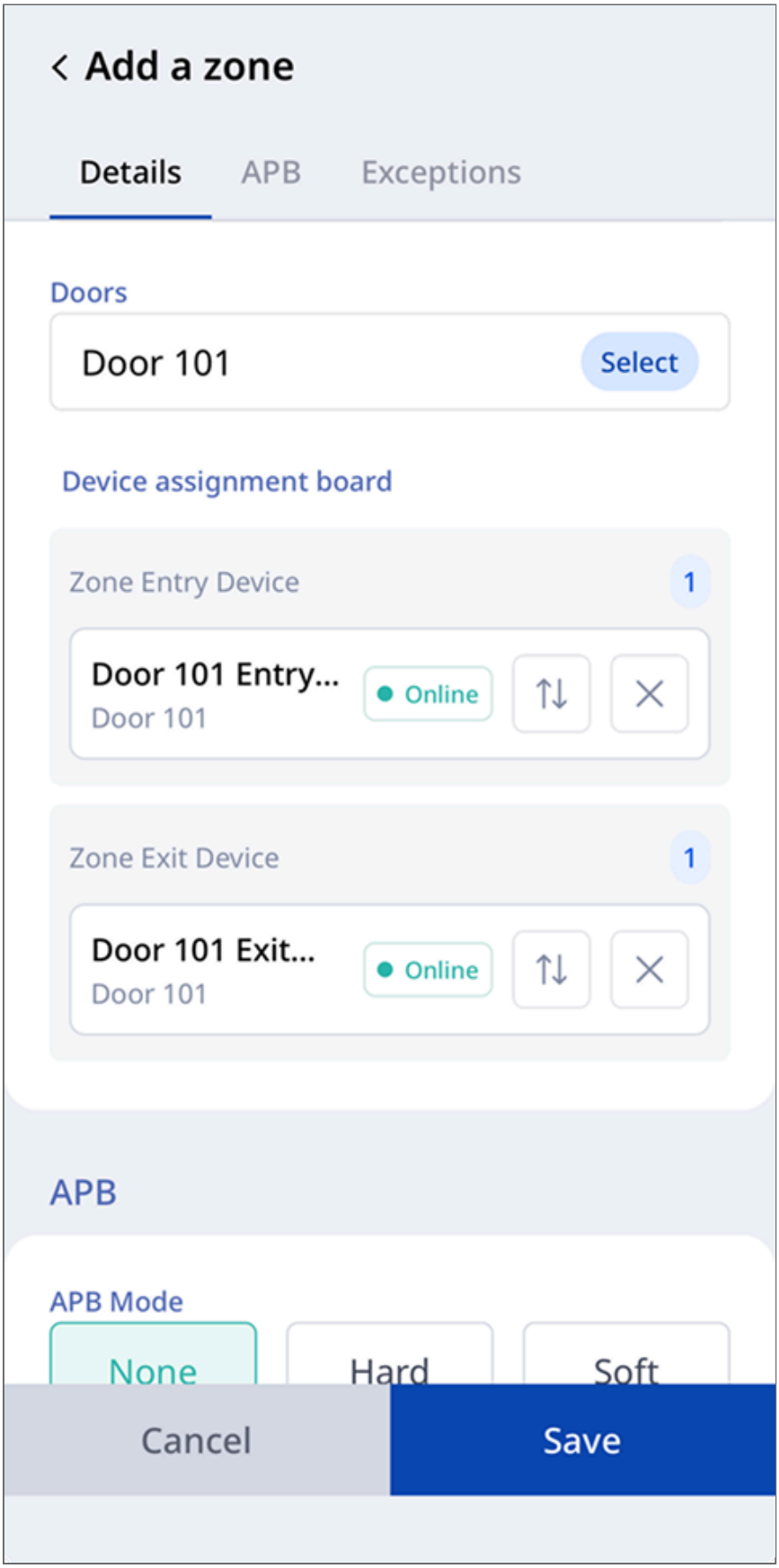
2 ドアとデバイスの割り当て

ゾーンに割り当てるドアとデバイスを選択します。

Web



Mobile



- **ドア**：ゾーンに含めるドアを選択します。 1つ以上のドアを選択できます。 ドアを選択すると、システムはそのドアのデバイスを **デバイス割り当てボード** に表示します。
- **デバイス割り当てボード**：各デバイスを **ゾーン入室デバイス** または **ゾーン退室デバイス** に指定します。 装置は**デバイス**

IDで区別して表示します。「移動（⇄）」ボタンをクリックして、装置を入室装置または退室装置に移動します。

> **情報**
>
> - システムは、ファームウェアがv2.13以降の装置のみを**デバイス割り当てボード**に表示します。 ゾーンに割り当てるデバイスのファームウェアが最新であることを必ず確認してください。
> - 装置管理の詳細は、デバイスとパネルのグループを管理するをご参照ください。
> - ドアの管理に関する詳細は、登録済みドアの管理をご参照ください。

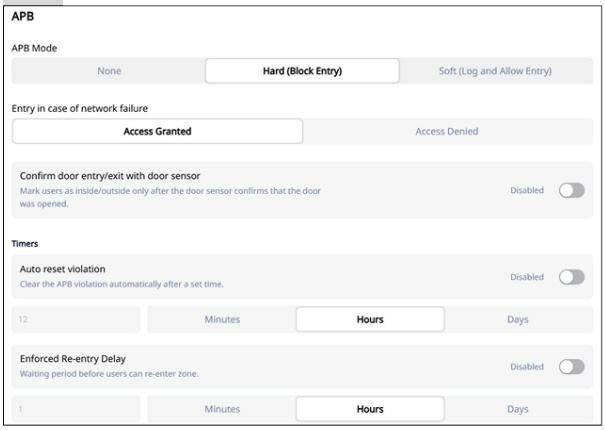
3 APBモードの設定

APB セクションでアンチパスバックルールを設定してください。 アンチパスバックルールの適用は任意のため、ゾーン内の移動を厳格に管理する必要がなければ **なし** モードを選択し、在席者の確認にのみゾーンを使用します。

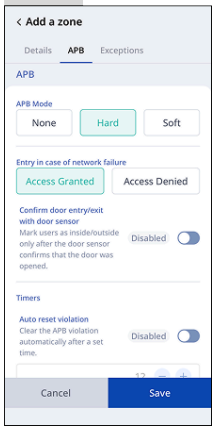
Hard

Hard（入室をブロック）

Web



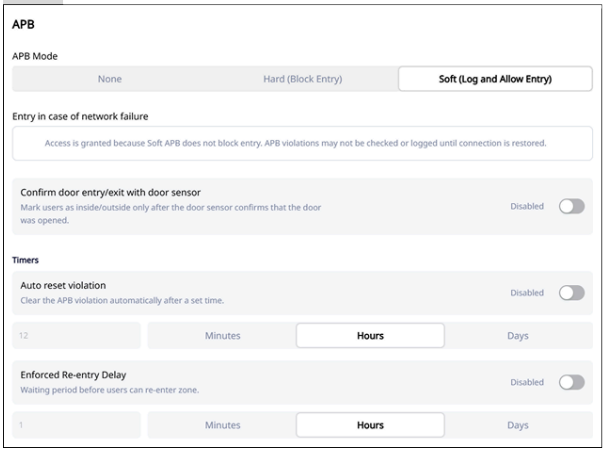
Mobile



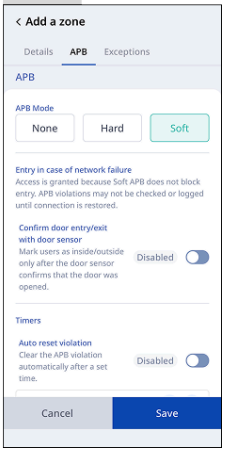
Soft

Soft（ログを記録し入室を許可）

Web



Mobile



- **APBモード**：希望するAPBモードを選択します。

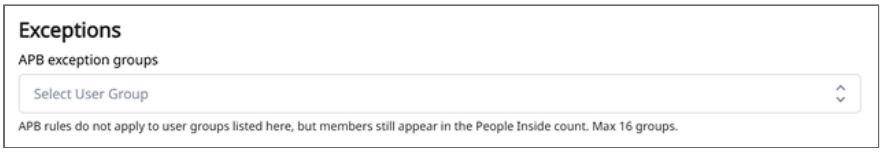
  - **Hard（入室をブロック）**：ユーザーがAPBルールに違反すると、入退室を遮断し、イベントログに違反として記録します。
  - **Soft（ログを記録し入室を許可）**：入退室は許可しますが、イベントログにAPB違反として記録します。
  - **なし**：ゾーンにAPBを適用しません。 APBモードを設定していないゾーンは、在席人数を計算する用途で引き続き使用されます。

- **ネットワーク障害時の入室**：ネットワーク障害でBioStar Airサーバーと通信できない場合に、アクセスを許可するか拒否するかを選択します。 **Soft** モードでは入退室を遮断しないため、アクセスは常に許可されます。ネットワーク接続が復旧するまで、違反を確認または記録できない場合があります。
- **ドアセンサーで入室・退室を確認**：このオプションを有効にすると、ドアセンサーが出入口ドアの開放を確認した後にのみ、ユーザーを **オンサイト** または **オフサイト** 状態として表示します。
- **タイマー**
  - **違反の自動リセット**：設定した時間が経過すると、APB違反を自動解除します。
  - **再入室の遅延**：ユーザーが同じゾーンに再入室できるまでの待機時間です。

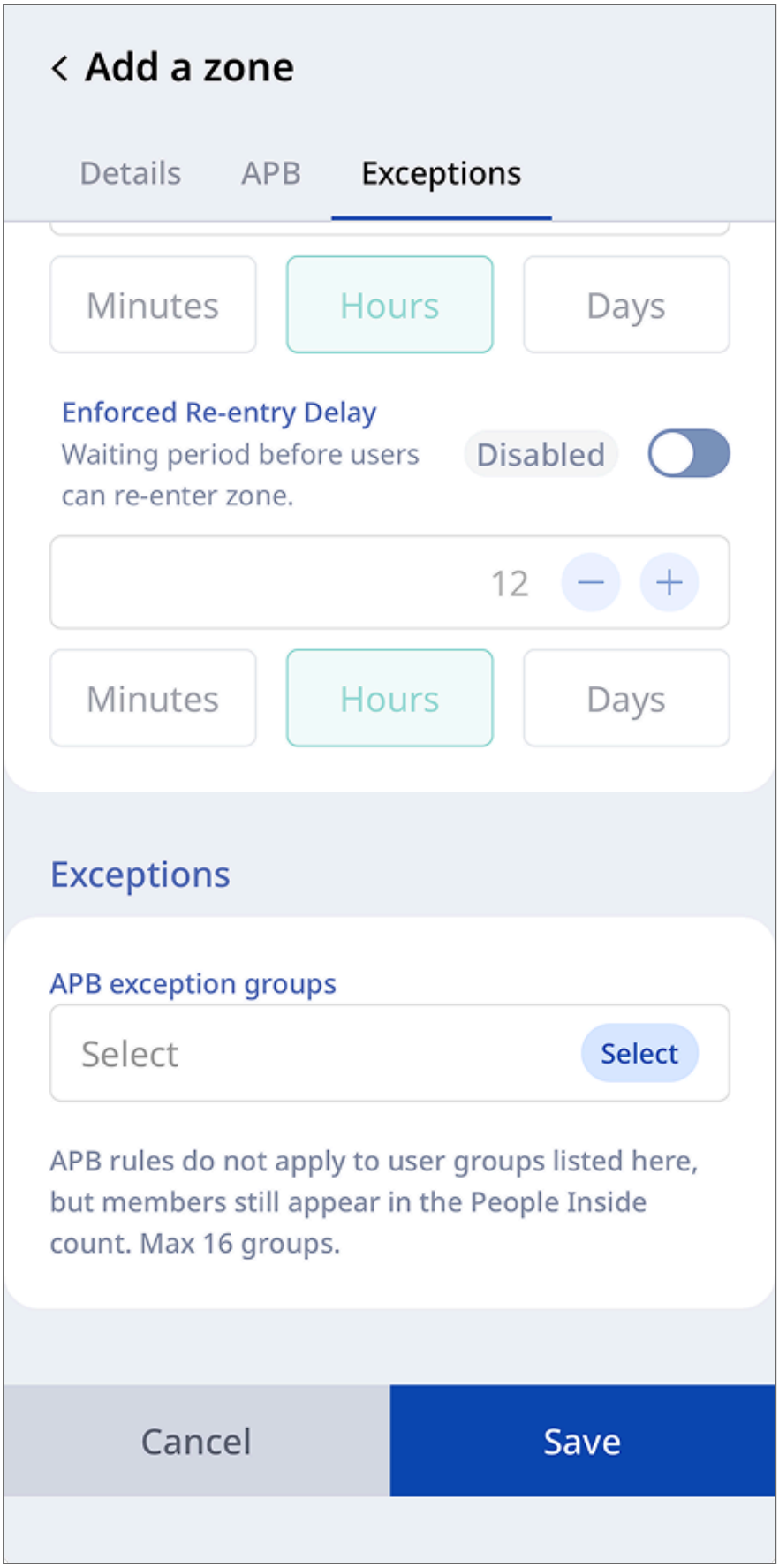
4 例外の設定

例外 セクションで、APBルールを適用しないユーザーグループを選択してください。

Web



Mobile



- ゾーンごとに最大16個のユーザーグループを例外に指定できます。
- 例外グループに属するユーザーにはAPBルールが適用されませんが、在席人数には引き続き含まれます。

- **APBモード** が **なし** の場合、**例外** セクションは無効になります。

> **情報**
> ユーザーグループ管理の詳細については、ユーザーグループを管理するを参照してください。

5 ゾーンの保存

ゾーン設定を保存するには、**保存**をクリックしてください。

> **ゾーン追加時の注意事項**
> - ドア選択リストには、すでに別のAPBゾーンに割り当てられているドア、装置がないドア、エアフォブパッチ（Airfob Patch）専用ドアを表示しません。
> - 退室装置を指定しないゾーンは、**違反の自動リセット**(境界でない場合) または **オフサイトタイマー**(境界の場合) を必ず有効にしないと保存できません。
> - 同じ名前のゾーンは作成できません。
> - ゾーン設定で **APBモード** を **なし** に変更すると、そのゾーンの詳細設定(**APBモード**, **タイマー**, **APB例外グループ**)がすべて初期化されます。 設定を保持したままAPBの適用だけを一時停止するには、ゾーンの無効化またはAPBの一時無効化を使用してください。

ゾーンの有効化/無効化

ゾーンを有効化または無効化できます。 設定値は削除されず、そのまま保持されます。 ゾーンを無効化すると、そのゾーンの在席人数が0に初期化されます。 ただし、すでに発生したAPB違反は残り、APB違反を確認する メニューで解除できます。

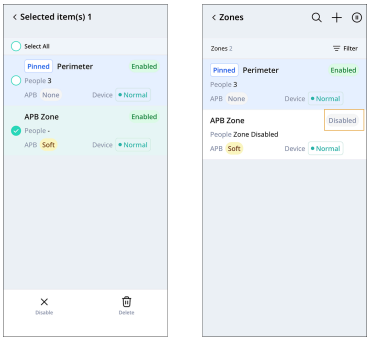
Web

1. 一覧で有効化または無効化するゾーンのチェックボックスをクリックします。 一つ以上のゾーンを選択できます。
2. 一覧上部の **有効化** または **無効化** ボタンをクリックします。
3. 確認メッセージが表示されたら **有効化** または **無効化** ボタンをクリックします。

各ゾーンの有効化状態は、一覧の **ゾーンステータス** 列で確認できます。



Mobile



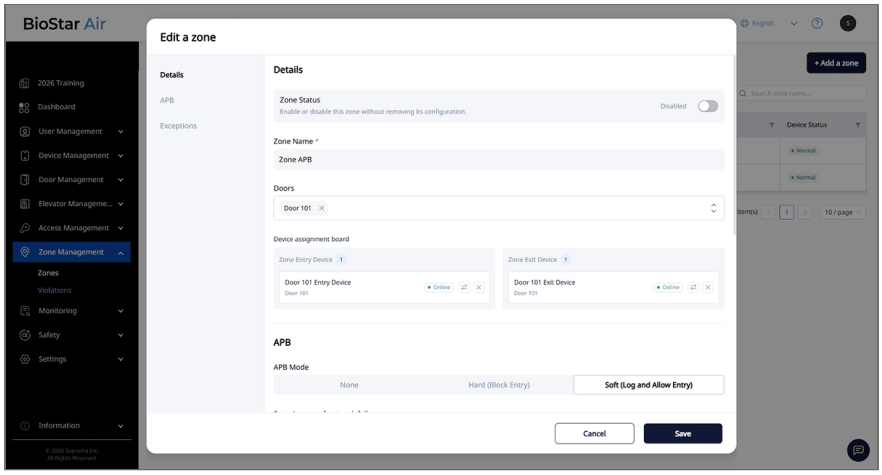
1. 一覧で有効化または無効化するゾーンを長押しします。
2. 有効化または無効化するゾーンを選択します。 一つ以上のゾーンを選択できます。
3. 画面下部の **有効化** または **無効化** ボタンをタップします。
4. 確認メッセージが表示されたら **有効化** または **無効化** ボタンをクリックします。

ゾーンを編集

設定済みゾーンの詳細情報、APB、例外設定などを編集できます。

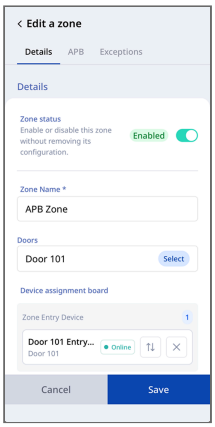
Web

1. 一覧で編集するゾーンをクリックします。
2. **ゾーンを編集** ウィンドウが表示されます。



3. **詳細**/**APB**/**例外** セクションで必要な項目を編集します。
4. 変更を保存するには、**保存** をクリックします。

Mobile



1. 一覧で編集するゾーンをタップします。
2. **ゾーンを編集** 画面が表示されます。
3. **詳細**/**APB**/**例外** セクションで必要な項目を編集します。
4. 変更を保存するには **保存** をタップします。

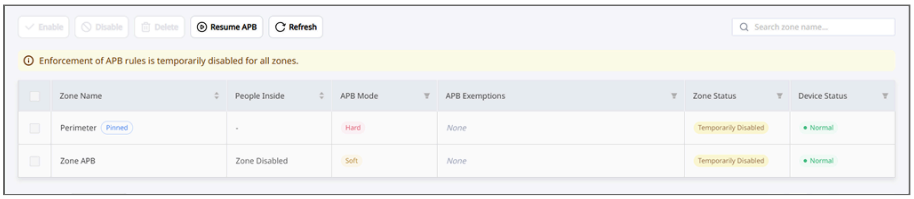
> **情報**
> **詳細**/**APB**/**例外** セクションの設定の詳細は、ゾーンの追加をご参照ください。

APBを一時停止

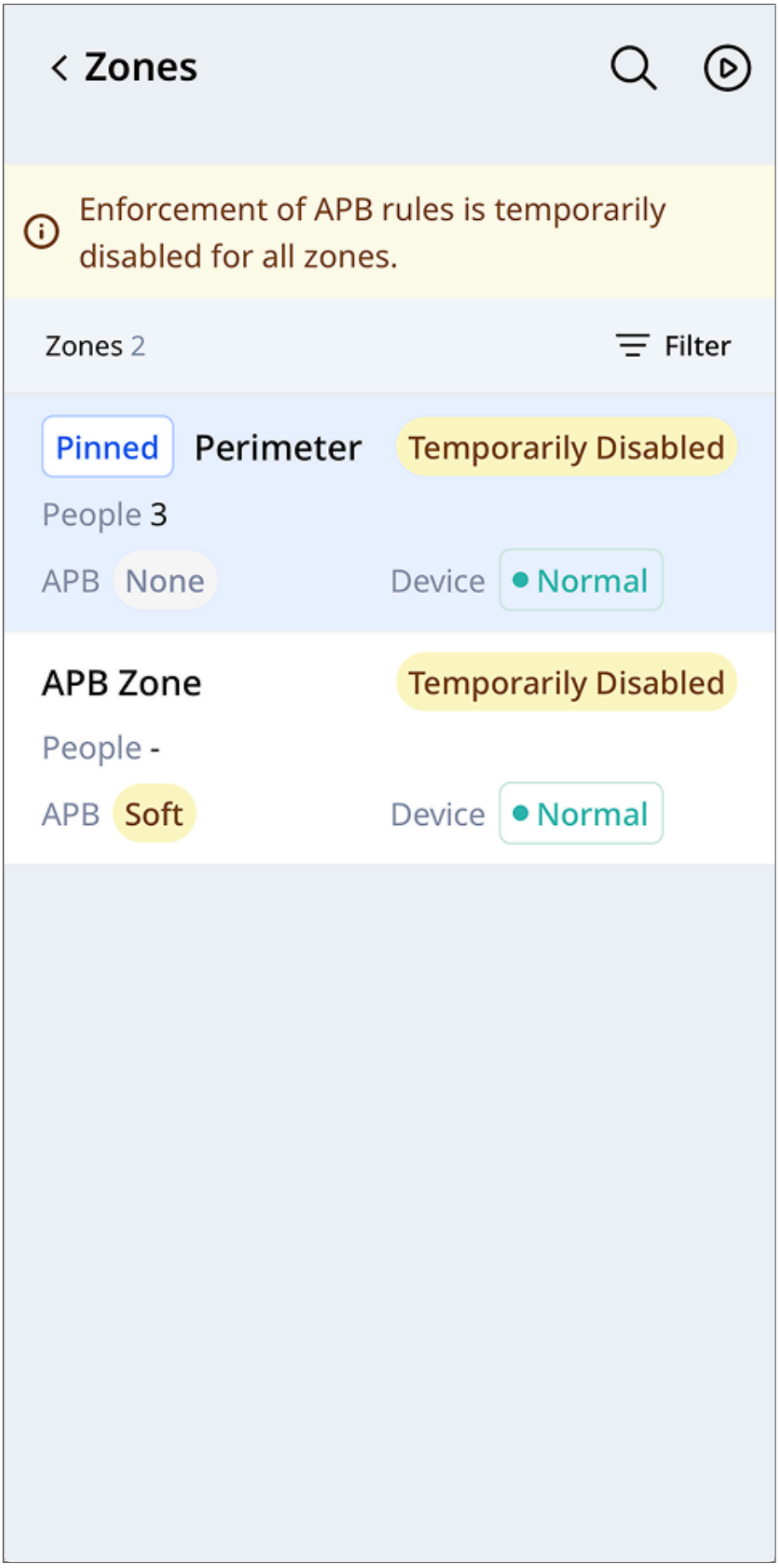
サイト全体へのAPB適用を一時停止する場合（例: 特別行事、大規模な移動が予想される時間帯）は、一覧上部の**APBを一時停止**(⏸) ボタンをクリックしてください。 境界を含むすべてのゾーンのAPB適用を停止します。再開すると、各ゾーンは一時無効化前の有効化/無効化状態に復元されます。 一時無効化中はゾーン一覧がロックされ、変更できません。

ゾーンに設定したAPBモードを再開するには、**APBを再開**(▶) ボタンをクリックしてください。

Web



Mobile

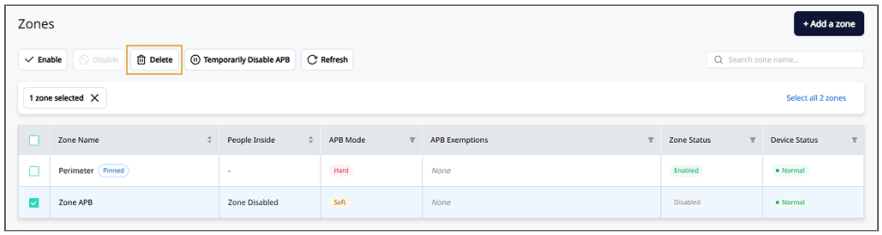

Zones
Enforcement of APB rules is temporarily disabled for all zones.
Zones 2
Filter
Pinned
Perimeter
Temporarily Disabled
People 3
APB None
Device Normal
APB Zone
Temporarily Disabled
People -
APB Soft
Device Normal

点呼(Roll Call)の実施中は、アンチパスバックゾーンを有効化できません。 点呼が終了したら、再試行してください。
点呼の詳細については、ロールコールをご参照ください。

ゾーンを削除する

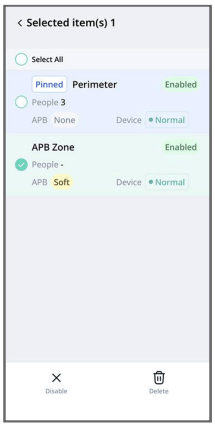
Web

1. 一覧で削除するゾーンのチェックボックスをクリックします。 一つ以上のゾーンを選択できます。
2. 一覧上部の**削除** ボタンをクリックしてください。



3. 確認メッセージが表示されたら、**削除** ボタンをクリックします。

Mobile



1. 一覧で削除するゾーンを長押しします。
2. 削除するゾーンを選択してください。 一つ以上のゾーンを選択できます。
3. 画面下部の **削除** ボタンをタップします。
4. 確認メッセージが表示されたら、**削除** ボタンをクリックします。

情報

- **境界**は削除できません。
- 選択したゾーンのみ削除され、ゾーンに割り当てられたドアとデバイスは削除されません。 削除操作は取り消せません。
- ゾーンに割り当てたデバイスがオフライン、同期中、またはファームウェアアップグレード中の場合、ゾーンを削除できません。 デバイスが再接続されるまで待つか、ゾーンから該当デバイスを先に削除してから再試行してください。

APB違反を確認する

ゾーン管理 → **違反** メニューでは、ゾーンに設定したアンチパスバック（APB）ルールに違反したユーザーを確認し、必要に応じて違反状態を解除できます。 ゾーンとAPBモードをまだ設定していない場合は、先に ゾーン管理 を参照してください。

違反が発生する場合

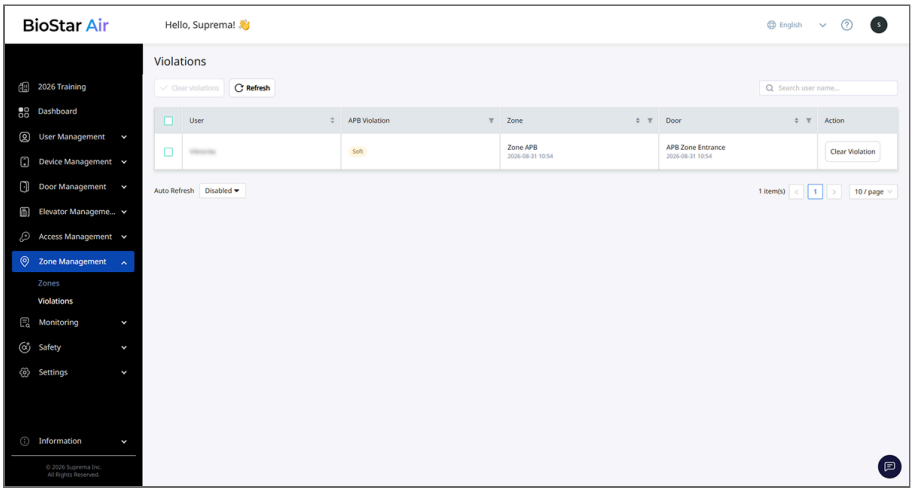
ユーザーがゾーンに設定したAPBモードに反する順序で入退室を試みると、システムはAPB違反を記録します。

- **Hard**モードに設定したゾーンでは、APB違反が発生すると入退室をブロックし、APB違反として記録します。
- **Soft**モードに設定したゾーンでは、APB違反が発生しても入退室は許可しますが、APB違反として記録します。
- APB例外グループに属するユーザーにはAPBルールが適用されないため、システムは違反一覧に表示しません。

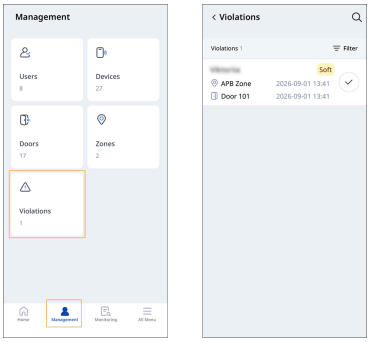
違反一覧を確認する

Web

画面左のサイドバーで **ゾーン管理** → **違反** をクリック。



Mobile



1. モバイル端末でBioStar Airアプリを起動してログインします。
2. 画面の下部にある **管理** をタップします。
3. **違反** カードをタップしてください。

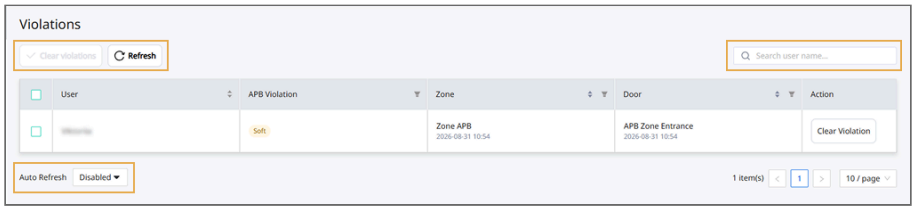
一覧で、現在アクティブなAPB違反のユーザーを確認できます。 アクティブなAPB違反がない場合、システムは一覧の代わりに空の状態画面を表示します。

- **ユーザー**：APB違反を発生させたユーザーです。
- **APB違反**：APB違反が発生したモード（Hard/Soft）です。
- **ゾーン**：APB違反が発生したゾーンです。
- **ドア**：APB違反が発生したドアです。
- **アクション**：個別のAPB違反を解除できます。

> **情報**
> 解除済みのAPB違反と過去のAPB違反履歴は、**モニタリング** → **イベントログ** で引き続き確認できます。

違反一覧の管理機能

一覧の上部と下部にある管理機能で、次の作業を実行できます。

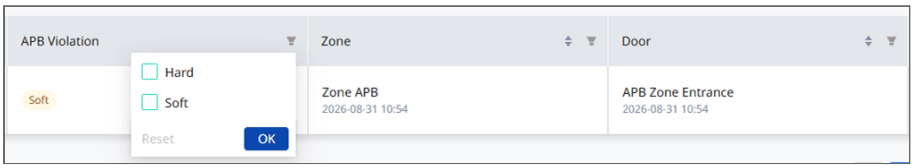


- **違反を解除**：一覧で選択したユーザーのAPB違反を解除できます。 詳しくは 違反の解除 をご参照ください。
- **リフレッシュ**：一覧をすぐに更新し、最新状態にします。 一覧下部の**自動更新**で自動更新間隔(**無効**/**５秒**/**１分**)を選択すると、設定した周期で一覧を自動更新します。
- **ユーザー名を検索…**：ユーザー名で検索できます。

違反一覧のフィルタリング

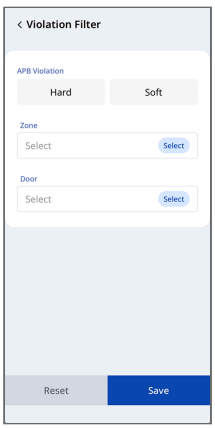
Web

一覧上部ヘッダーの **APB違反**、**ゾーン**、**ドア** 列にある ボタンをクリックすると、該当条件で一覧を絞り込みます。



> **情報**
> フィルターを解除するには **リセット** ボタンをクリックします。

Mobile



1. 違反一覧の右上にある **フィルター** をタップします。
2. **APB違反**、**ゾーン**、**ドア**で条件を選択します。
3. 選択した条件で一覧をフィルタリングするには **保存** ボタンをタップします。

> **情報**
> フィルターを解除するには **リセット** ボタンをタップします。

違反の解除

APB違反を解除すると、システムはユーザーのアクティブなAPB違反状態を初期化し、ユーザーは再びゾーンに正常に出入りします。

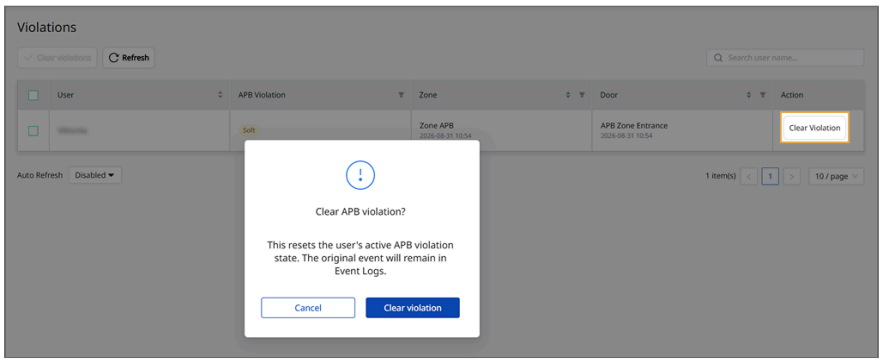
情報

- **違反を解除** はユーザーのアクティブなAPB違反状態のみを初期化します。 システムは、APB違反が発生した元のイベントを削除せず、イベントログにそのまま残します。
- ゾーンを無効化しても、システムは既に発生したAPB違反を維持し、違反一覧から解除できます。
- システムはAPB例外グループに属するユーザーをこの一覧に表示しませんが、ゾーンの在席人数には引き続き含めます。

個別ユーザーの違反解除

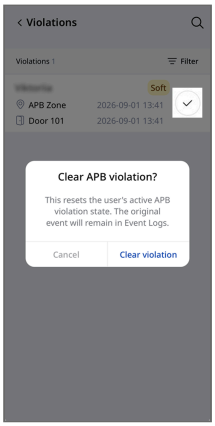
Web

1. 一覧でAPB違反を解除するユーザーの **アクション** 列で **違反を解除** ボタンをクリックします。



2. 確認メッセージが表示されたら、**違反を解除** ボタンをクリックします。

Mobile

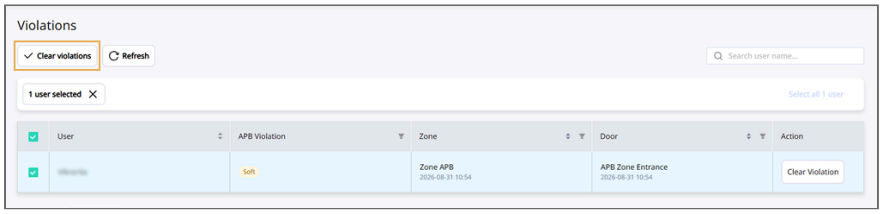


1. 一覧でAPB違反を解除するユーザーの ⌄ ボタンをタップします。
2. 確認メッセージが表示されたら、**違反を解除** ボタンをタップします。

複数ユーザーの違反解除

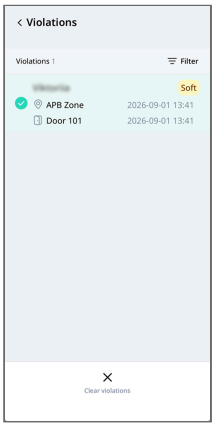
Web

1. 一覧でAPB違反を解除するユーザーのチェックボックスをクリックします。 一人以上のユーザーを選択できます。
2. 一覧上部の**違反を解除** ボタンをクリックしてください。



3. 確認メッセージが表示されたら **違反を解除** ボタンをクリックします。

Mobile



1. 一覧でAPB違反を解除するユーザーを長押しします。
2. 解除するユーザーを選択します。 一人以上のユーザーを選択できます。
3. 画面下部の **違反を解除** ボタンをタップします。
4. 確認メッセージが表示されたら、**違反を解除** ボタンをタップします。

モニタリング

BioStar Airのモニタリング機能により、システムの主要な活動をリアルタイムで追跡し、管理します。 イベントおよび変更ログを監視してシステム活動を分析し、ドアの状態をリアルタイムで確認してリモートで制御し、生成された通知とレポートを通じてセキュリティ活動を総合的に管理します。

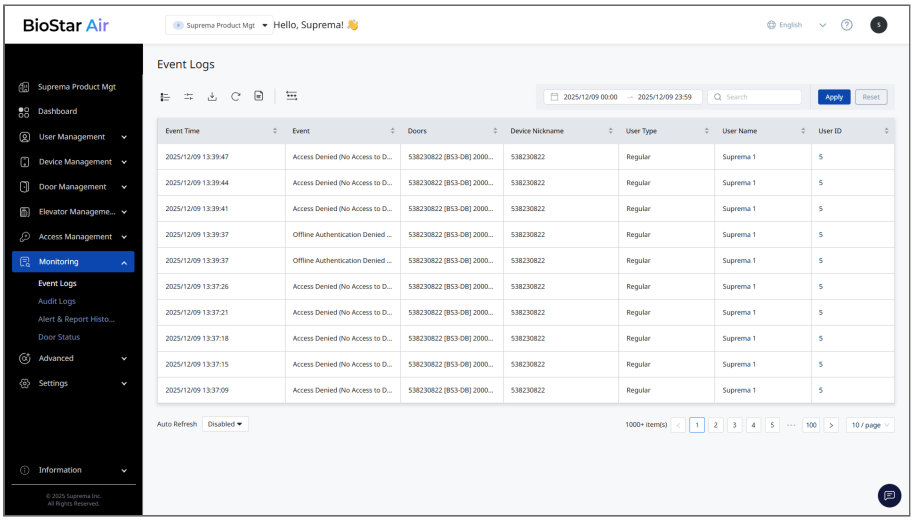
イベントログの使い方
クラウド出入管理プラットフォームの主な利点の一つは、いつでもどこでもサイト活動を監視できることです。 このドキュメントでは、BioStar Airでイベントログを監視および分析する方法について説明します。

> **ヒント**
> イベントログの動画ガイドを視聴するには、以下の動画をご覧ください。

イベントログの確認

Web

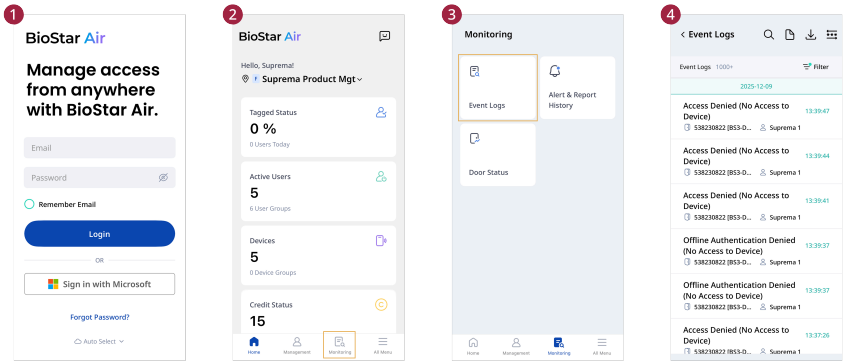
イベントログを確認するには、**イベントログ** に移動します。 画面左のサイドバーで **モニタリング** → **イベントログ** をクリックします。



イベントログ 画面にはイベント発生時間、イベント名、ドア名、デバイス名、ユーザータイプ、ユーザー名などの詳細を含むテーブル一覧が表示されます。

Mobile

モバイルアプリでイベントログを確認する方法について説明します。



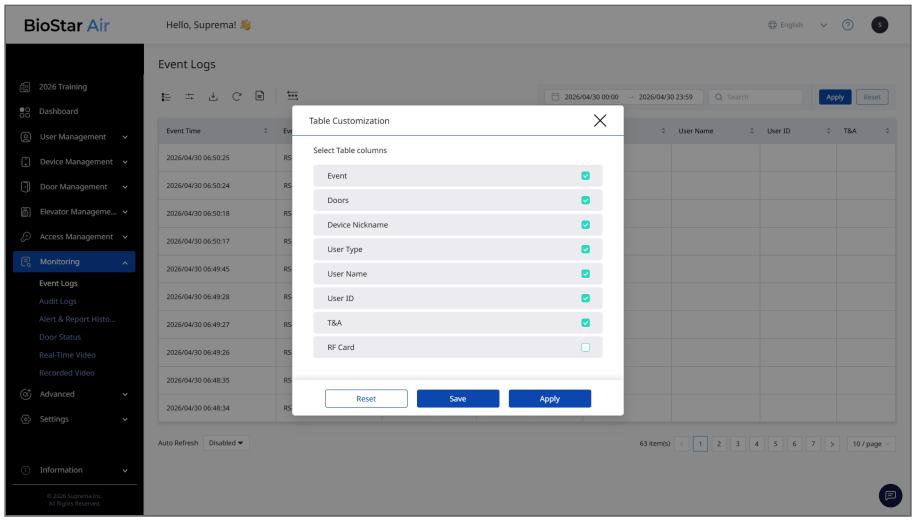
1. モバイル端末でBioStar Airアプリを起動してログインします。
2. 初期画面の下部にある **モニタリング** をタップします。
3. **イベントログ** カードをタップします。
4. イベントログ一覧をスクロールして内容を確認できます。

情報

- **フィルター**：イベントログをフィルタリングできます。
- 🔍：特定のキーワードを検索できます。 RFカードID、ユーザーID、メールアドレス、氏名のいずれかを入力します。
- 📄：レポートを作成できます。 レポート作成に関する詳細については、レポート設定を参照してください。
- ⬇：レポートをCSVまたはPDF形式でダウンロードできます。
- ***：個人情報のマスキングを適用できます。

チャット設定の変更

テーブルの列をカスタマイズして、表示または非表示にする情報を選択できます。 順序を変更して、よく使う列を前方に配置することもできます。 イベントログ一覧の上部にある をクリックしてください。 **チャット設定の変更** ウィンドウが表示されます。



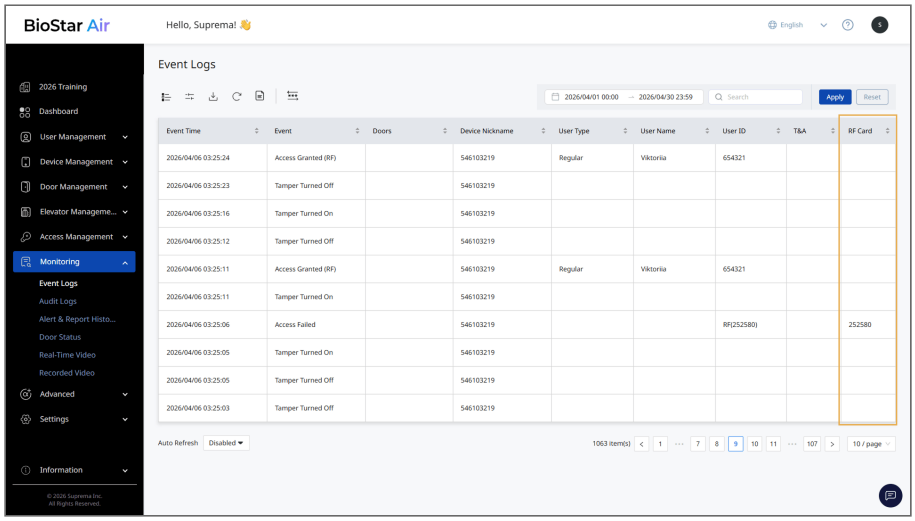
- 表示または非表示にする列のチェックボックスを選択または解除します。
- 列の順序を変更するには、該当する列をクリックしたまま目的の位置にドラッグします。
- **チャット設定の変更** を保存するには、**保存** をクリックします。
- **チャット設定の変更** を保存せずにログ一覧に適用するには、**適用** をクリックします。
- **チャット設定の変更** の変更を取り消して初期状態に戻すには、**リセット** をクリックします。

> **情報**
>
> - **保存** をクリックすると設定が保存され、他のメニューに移動しても保持されます。 **適用** をクリックすると変更は現在の一覧にのみ適用され、他のメニューに移動すると以前の設定に戻ります。
> - **監査ログ** では **チャット設定の変更** 機能はサポートされていません。

RFカード番号列を表示日るかんが?

イベントログでユーザーがRFカードで認証した場合、**RFカード** 列を追加してRFカード番号を確認できます。

1. イベントログ一覧の上部にある をクリックしてください。
2. **チャット設定の変更** ウィンドウが表示されたら、**RFカード** のチェックボックスをクリックし、目的の位置にドラッグします。
3. **保存** または **適用** ボタンをクリックします。
4. イベントログ一覧に **RFカード** 列が表示されます。

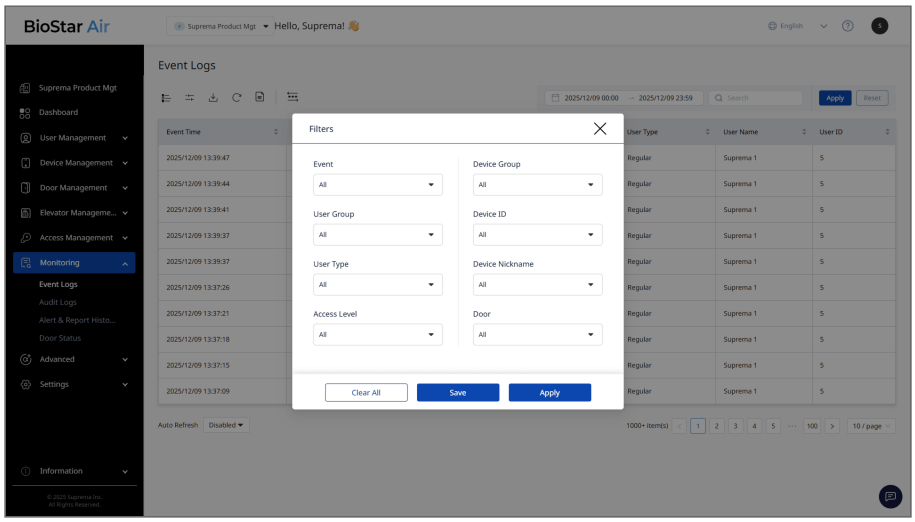


情報

イベントログに表示されるRFカード番号は、ユーザーに割り当てられたカードが1枚の場合のみ表示されます。 ユーザーが複数のRFカードを持っている場合、カード番号は表示されません。

ログのフィルタリング

ログをフィルタリングして、目的の情報を素早く見つけることができます。 ログ一覧の上部にある をクリックしてください。 **フィルター** ウィンドウが表示されたら、各項目で希望の値を選択します。



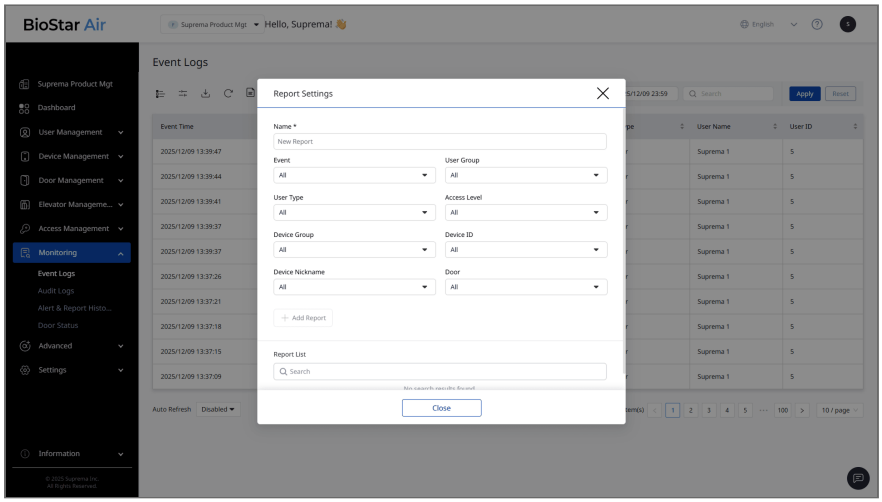
情報

- **保存** または **フィルターの保存** をクリックすると設定が保存され、他のメニューに移動しても保持されます。 **適用** または **フィルターの適用** をクリックすると変更は現在の一覧にのみ適用され、他のメニューに移動すると以前の設定に戻ります。
- **リセット** または **フィルタークリア** をクリックして変更を取り消し、初期状態に戻します。

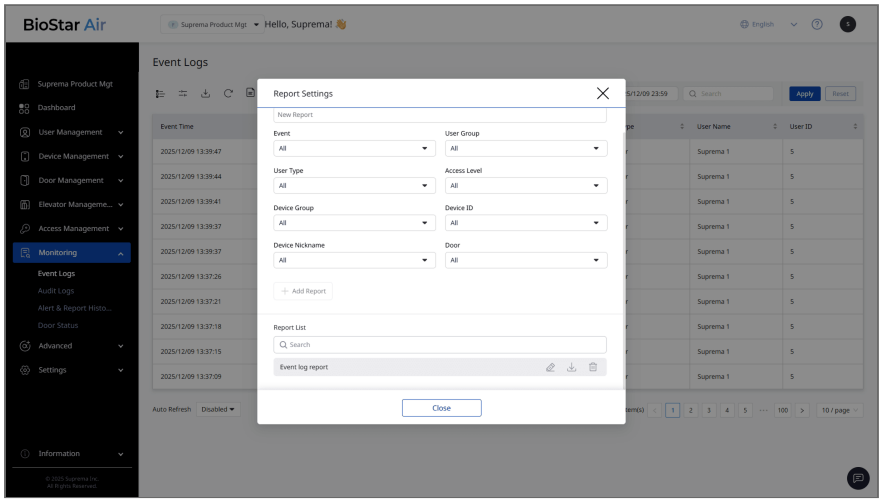
レポート設定

ログデータをフィルタリングして、特定の期間に発生したイベントのレポートを生成できます。

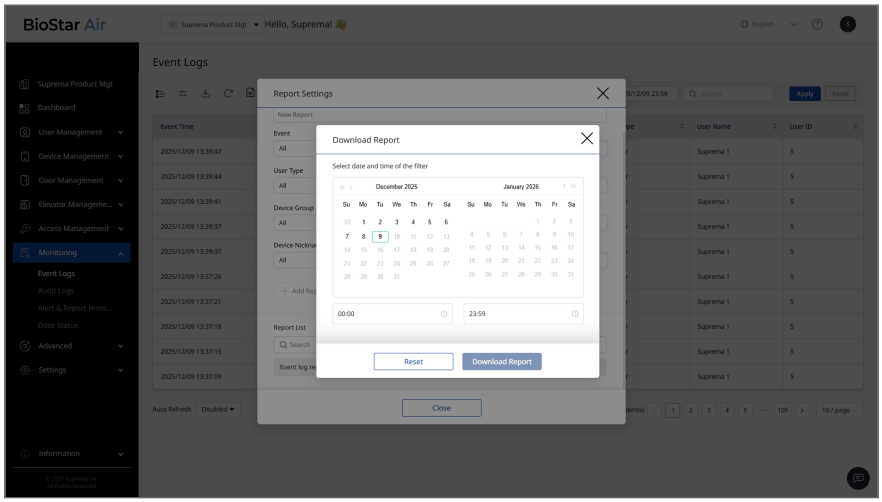
1. ログ一覧の上部にある をクリックします。
2. **レポート設定** ウィンドウが表示されたら、レポート名を入力します。



3. レポートに含める項目を選択します。
4. **レポートの追加** をクリックして設定したレポートを保存します。
5. **レポートリスト** に指定した名前でレポートが作成されます。



6. 作成されたレポートをダウンロードするには、レポート名の横にある をクリックします。
7. **レポートのダウンロード** ウィンドウが表示されたら、イベントを照会する期間を選択し、**レポートDL** をクリックします。



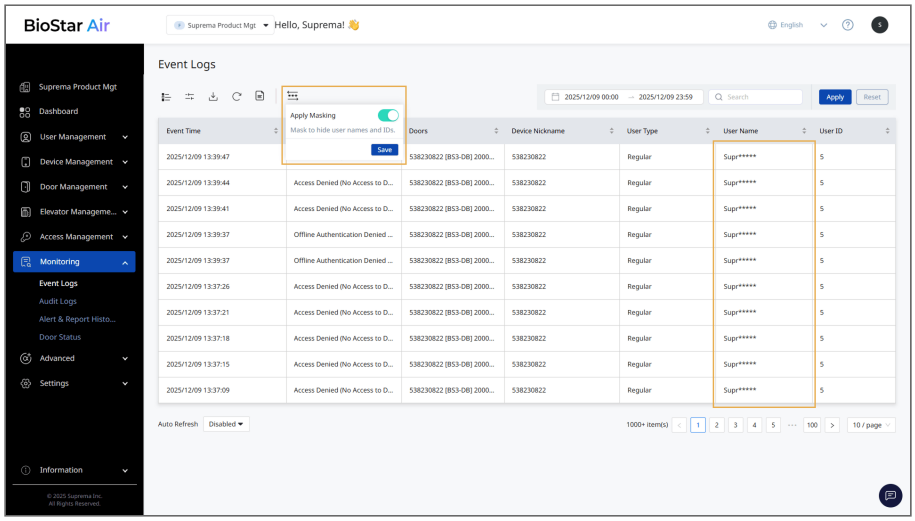
管理者のメールアドレスにダウンロードリンクが送信されます。

> **情報**
> **レポートリスト** で作成したレポートを検索、編集、ダウンロード、削除できます。

個人情報のマスキング

ログ内の個人情報をマスキングして、機密情報を保護できます。 個人情報のマスキングを有効にすると、ユーザー名、メールアドレス、電話番号などの情報が部分的に隠されます。

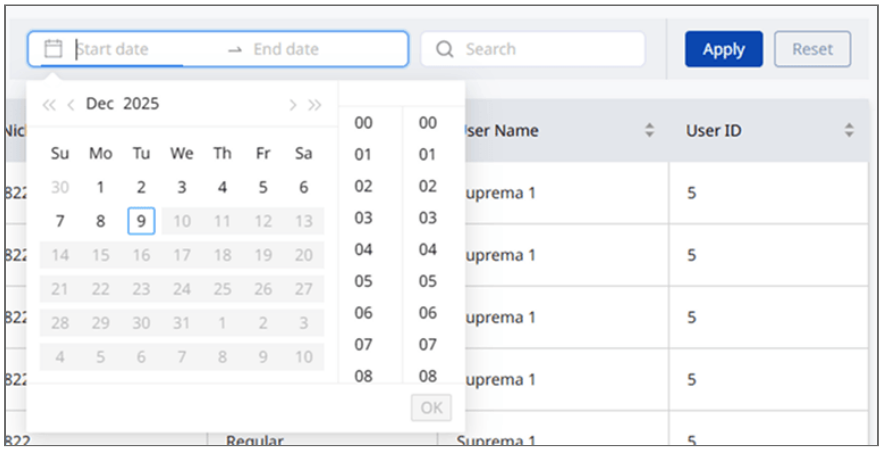
個人情報のマスキングを有効にするには、ログ一覧の上部にある をクリックします。 ポップアップメニューで **マスキングを適用** オプションを有効にし、**保存** をクリックします。



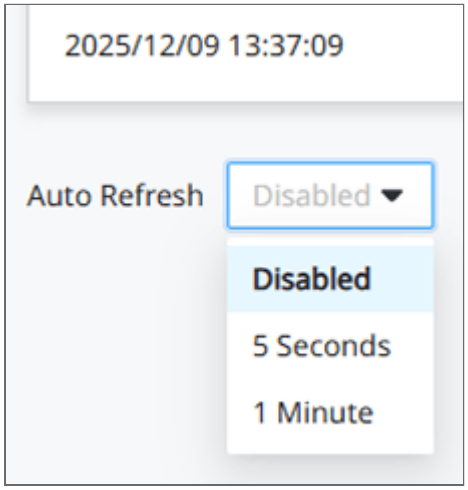
その他の機能

ログ一覧の上部にあるツールバーを使用して、ログをより効率的に管理できます。

- ログを日付で並べ替えるには、日付と時間の範囲を選択してから **適用** をクリックします。 日付をリセットするには、**リセット** をクリックします。



- **検索** 入力フィールドに特定のキーワードを入力してログを検索できます。 RFカードID、ユーザーID、メールアドレス、氏名のいずれかを入力します。
- ログをCSVまたはPDFファイルとして保存するには、 をクリックします。
- ログを更新するには、一覧の上部にある をクリックします。
- 特定の間隔で自動更新するには、一覧の左下にある **自動更新** で5秒または1分を選択します。

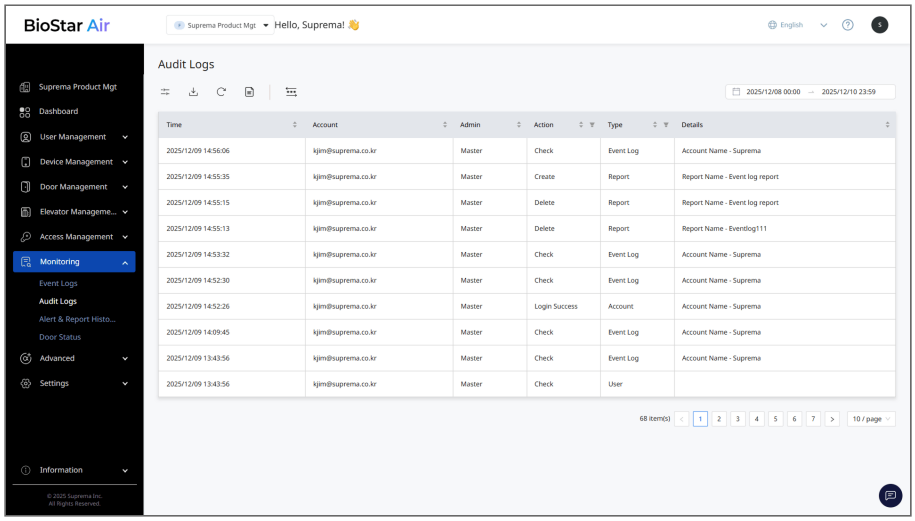


変更ログの使い方
クラウド出入管理プラットフォームの主な利点の一つは、いつでもどこでもサイト活動を監視できることです。 このドキュメントでは、BioStar Airで変更ログを監視・分析する方法を説明します。

> **ヒント**
> 変更ログの動画ガイドを視聴するには、以下の動画をご覧ください。

変更ログの確認

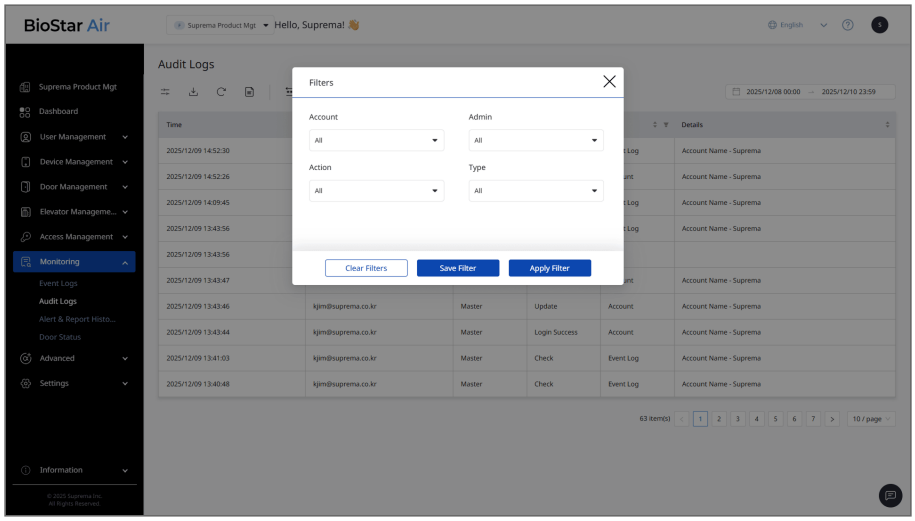
変更ログを確認するには、**監査ログ** に移動します。 画面左側のサイドバーで **モニタリング** → **監査ログ** をクリックします。



監査ログでは、管理者が行った操作を追跡できます。 ログ一覧では、作業日時、メールアドレス、管理者権限、操作の種類、メニューのパス、操作の詳細などが表示されます。

ログのフィルタリング

ログをフィルタリングして、目的の情報を素早く見つけることができます。 ログ一覧の上部にある をクリックしてください。 **フィルター** ウィンドウが表示されたら、各項目で希望の値を選択します。



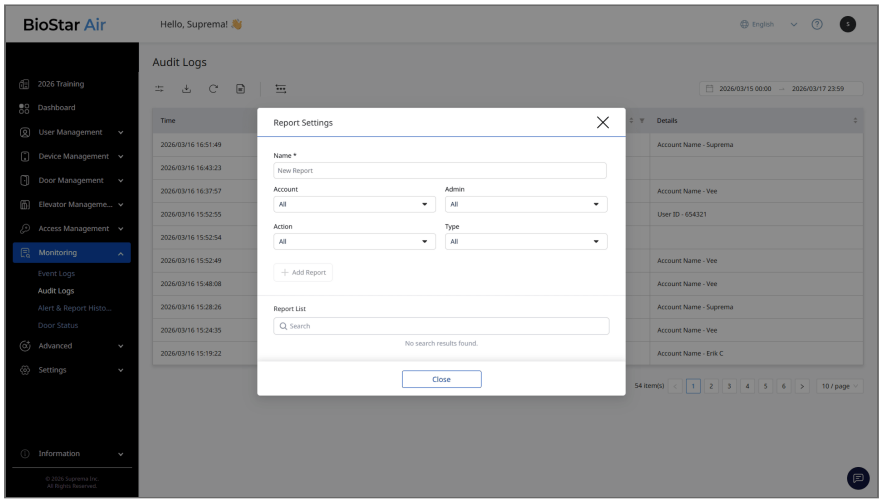
情報

- **保存** または **フィルターの保存** をクリックすると設定が保存され、他のメニューに移動しても保持されます。 **適用** または **フィルターの適用** をクリックすると変更は現在の一覧にのみ適用され、他のメニューに移動すると以前の設定に戻ります。
- **リセット** または **フィルタークリア** をクリックして変更を取り消し、初期状態に戻します。

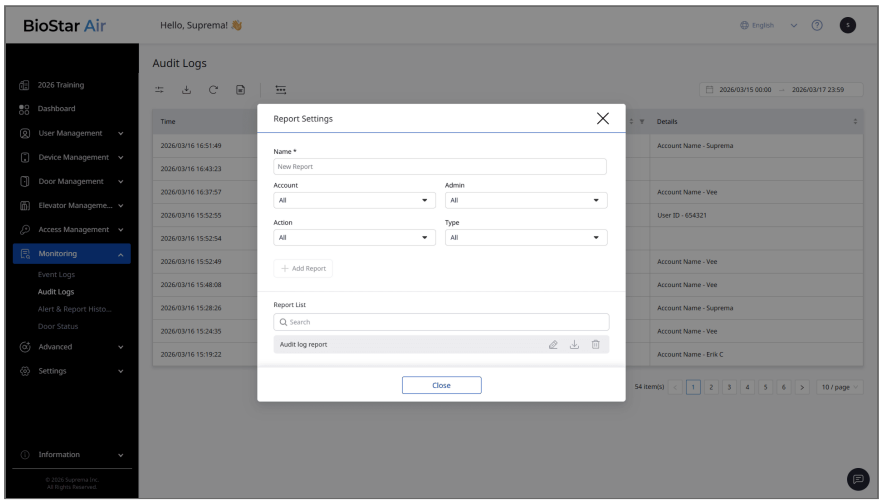
レポート設定

ログデータをフィルタリングして、特定の期間に発生したイベントのレポートを生成できます。

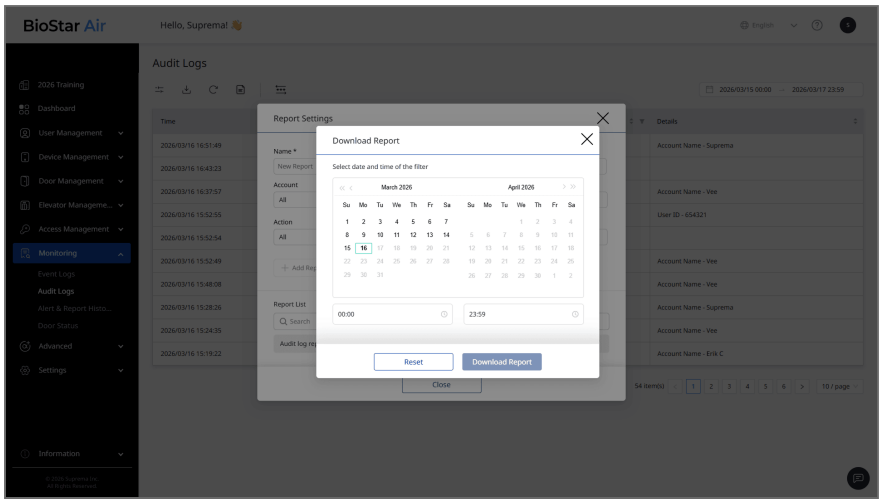
1. ログ一覧の上部にある をクリックします。
2. **レポート設定** ウィンドウが表示されたら、レポート名を入力します。



3. レポートに含める項目を選択します。
4. **レポートの追加** をクリックして設定したレポートを保存します。
5. **レポートリスト** に指定した名前でレポートが作成されます。



6. 作成されたレポートをダウンロードするには、レポート名の横にある ⭳ をクリックします。
7. **レポートのダウンロード** ウィンドウが表示されたら、イベントを照会する期間を選択し、**レポートDL** をクリックします。



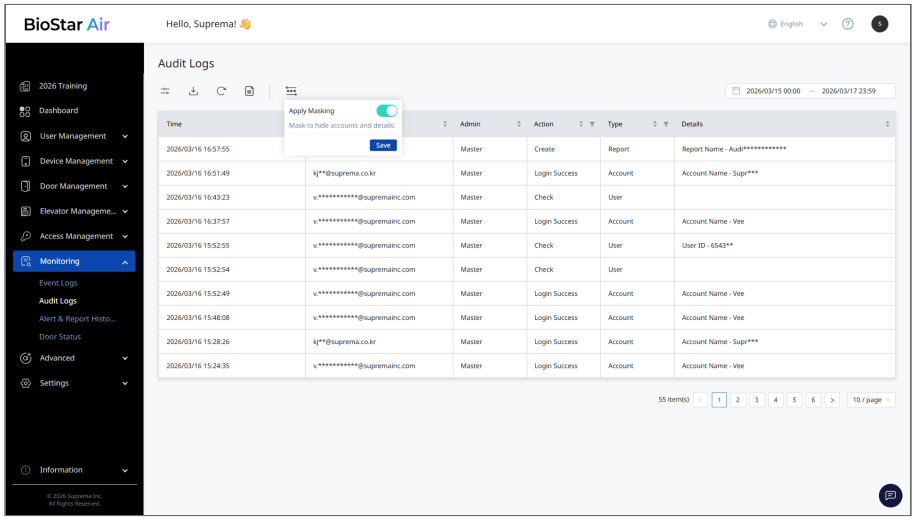
管理者のメールアドレスにダウンロードリンクが送信されます。

> **情報**
> **レポートリスト** で作成したレポートを検索、編集、ダウンロード、削除できます。

個人情報のマスキング

ログ内の個人情報をマスキングして、機密情報を保護できます。 個人情報のマスキングを有効にすると、ユーザー名、メールアドレス、電話番号などの情報が部分的に隠されます。

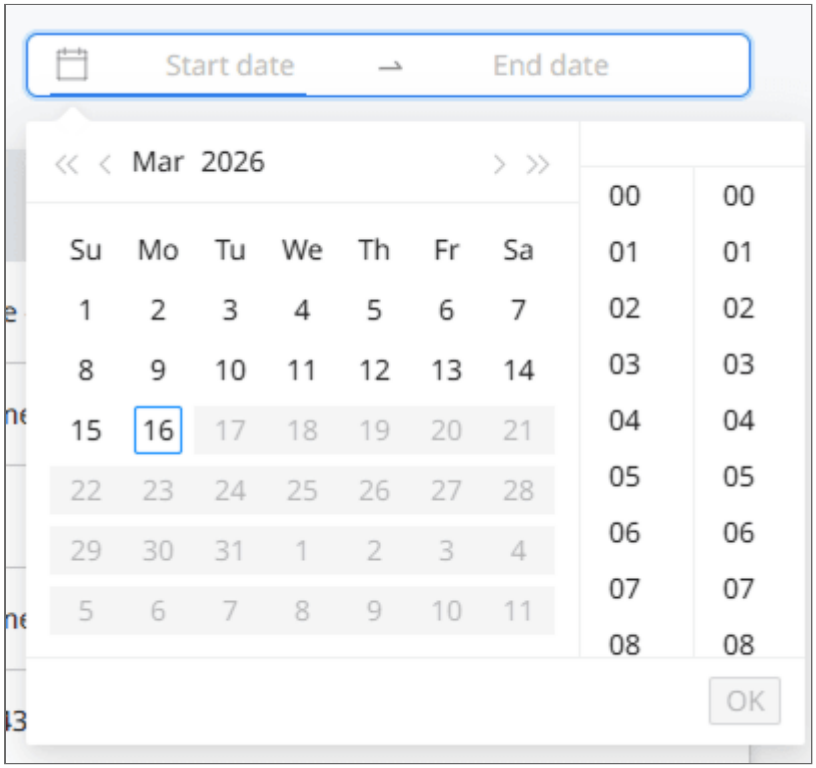
個人情報のマスキングを有効にするには、ログ一覧の上部にある をクリックします。 ポップアップメニューで **マスキングを適用** オプションを有効にし、**保存** をクリックします。



その他の機能

ログ一覧の上部にあるツールバーを使用して、ログをより効率的に管理できます。

- ログを日付順に並べ替えるには、日付と時間の範囲を選択して、**OK**をクリックしてください。



- ログをCSVまたはPDFファイルとして保存するには、 をクリックします。
- ログ一覧を更新するには、一覧上部の ボタンをクリックしてください。

アラートとレポート履歴の確認用ガイド

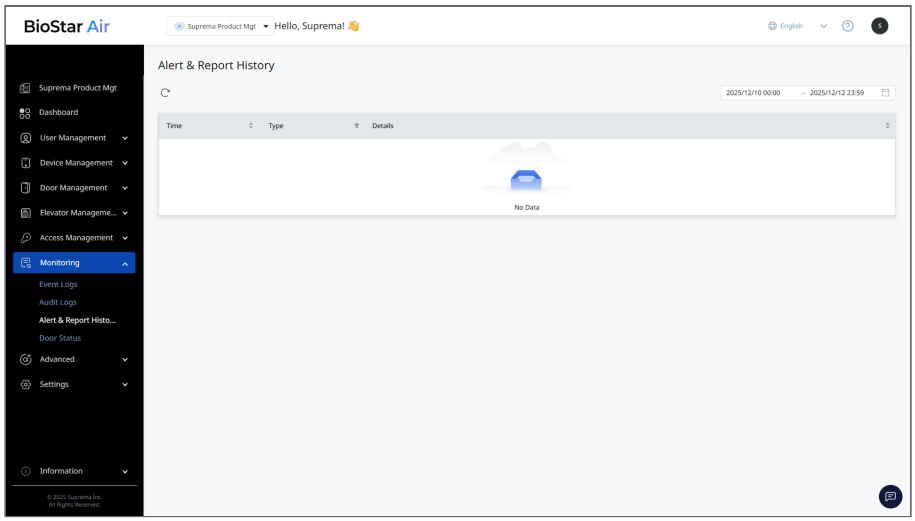
BioStar Airで生成されたアラートおよびレポートの履歴を確認する方法を説明します。 管理者はウェブポータルとモバイルアプリを通じて、過去に発生したアラートおよび作成されたレポートの履歴を参照できます。

開始する前に

アラートおよびレポートの履歴は、**設定** → **アラートとレポート履歴**で設定したアラートおよびレポート作成ルールによって生成されたもののみ確認できます。 アラートおよびレポートの作成ルールの設定に関する詳細は、アラートとレポートの設定を参照してください。

アラートとレポート履歴の確認

画面左のサイドバーの **モニタリング** → **アラートとレポート履歴** をクリックしてください。 アラートおよびレポートの履歴を確認できます。



- アラートやレポートの作成時間、種類、詳細を一覧で確認できます。
- 画面右上の日付検索エリアをクリックして希望の期間を設定し、該当期間内のアラートおよびレポート履歴をフィルタリングできます。
- 一覧の上部にある ボタンをクリックしてください。

ドアの状態を監視する

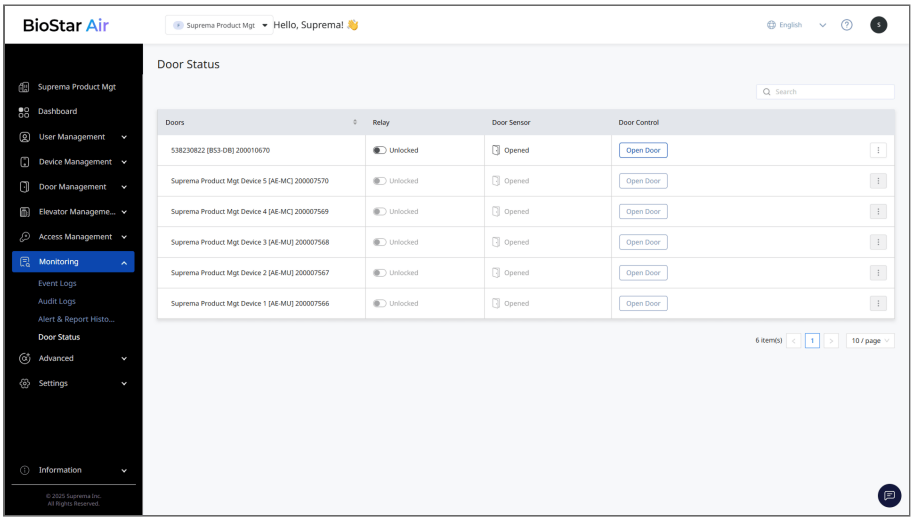
BioStar Airシステムに接続されているドアの状態をリアルタイムで監視できます。 管理者はドアの施錠／解錠状態やリレーセンサーの状態を確認し、ドアを施錠または解錠してリモートでドアのアクセスを制御できます。

> **ヒント**
> ドアの状態監視に関するビデオガイドを見るには、以下の動画を参照してください。

出入口の状態モニタリング

Web

BioStar Airのウェブポータルでドアの状態を監視できます。 画面左側のサイドバーで **モニタリング** → **ドアの状態** をクリックします。 BioStar Airに登録されたドアの一覧を確認できます。

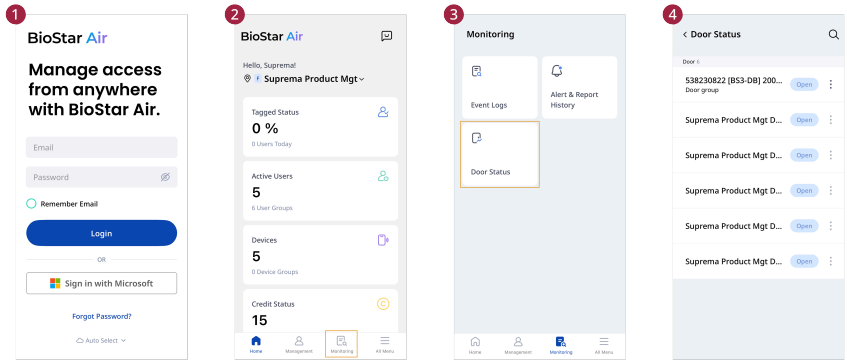


各ドアでは以下の項目を確認できます。

- **リレー**：ドアの施錠/解錠状態を表示します。
- **ドアセンサー**：ドアが物理的に開いているか閉じているかを表示します。

Mobile

モバイル端末でBioStar Airアプリを使ってドアの状態を確認できます。



1. モバイル端末でBioStar Airアプリを起動してログインします。
2. 初期画面の下部にある **モニタリング** をタップします。
3. **ドアの状態** カードをタップします。
4. BioStar Airに登録されたドアの一覧を確認できます。

> **情報**
> 出入口の登録と管理の詳細については、登録済みドアの管理 を参照してください。

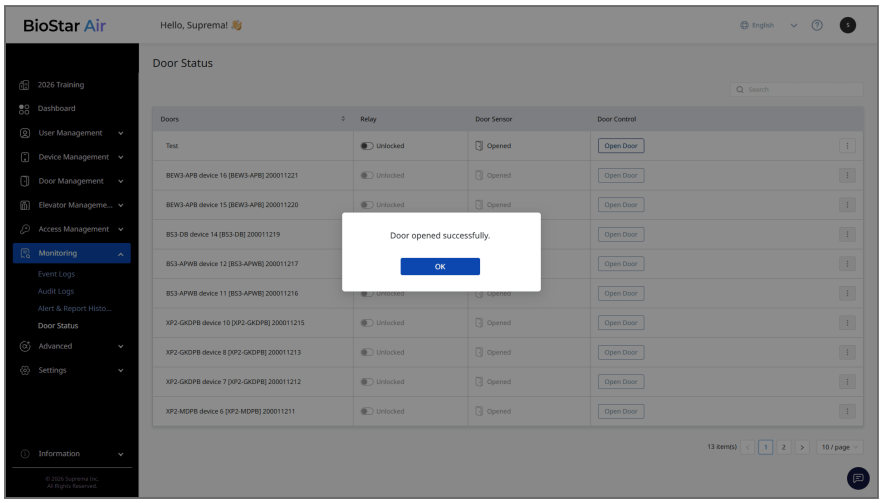
ドアの解錠

ドアがオンラインでBioStar Airに接続されている場合、リモートで解錠できます。

Web

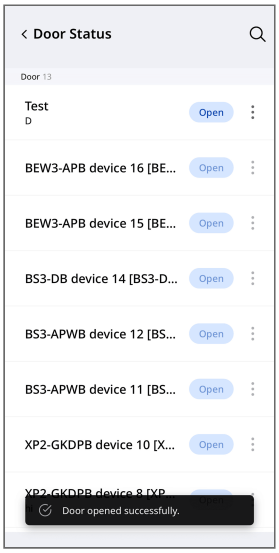
1. **ドア制御** 列で **ドアを開ける** ボタンをクリックします。

2. **リレー** 列の状態が解錠に変更され、成功メッセージが表示されます。



3. 設定された時間が経過すると、ドアは再び施錠状態に戻ります。

Mobile



1. 遠隔で出入口を解錠するには、**ドアを開ける** ボタンをタップします。
2. 画面下部に成功メッセージが表示されます。
3. 設定された時間が経過すると、ドアは再び施錠状態に戻ります。

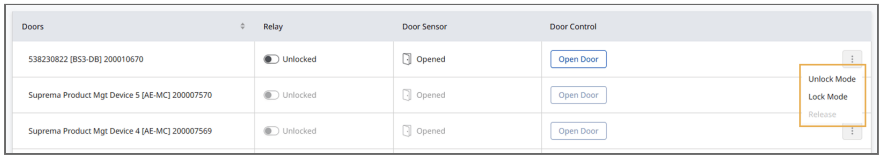
> **情報**
> 出入口が開いたままの時間を設定する方法については、登録済みドアの管理 を参照してください。

常時開放モードの設定

ドアを無期限に開放状態にできます。 訪問者や一時的な入場が必要な場合に便利です。

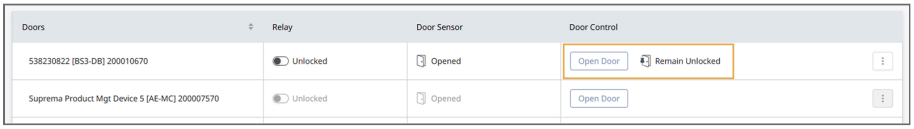
Web

1. ドア一覧で開放状態にするドアの最も右にある ⋮ ボタンをクリックします。



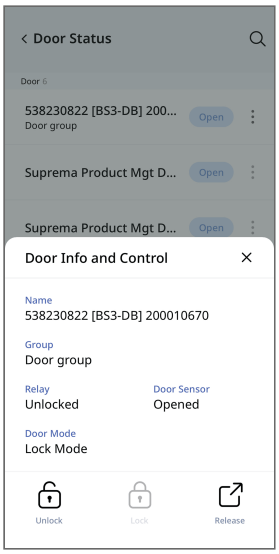
2. ポップアップメニューで **解錠モード** をクリックします。

3. **ドア制御** 列に **ロック解除されたままにする** として状態が変更されます。



正常な動作に戻すには ⋮ → **解放** をクリックします。

Mobile



1. ドアの最も右にある ⋮ ボタンをタップします。

2. **出入口情報と制御** オプションが表示されたら、**常時開放モード** をタップします。

3. 画面下部に成功メッセージが表示されます。

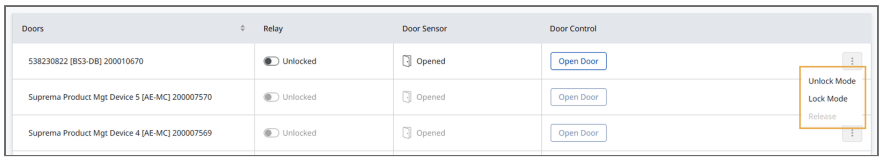
正常な動作に戻すには ⋮ → **解放** をタップします。

施錠モードの設定

現在のスケジュールに関係なくドアを施錠状態に維持できます。 セキュリティを強化する必要がある場合に有用です。

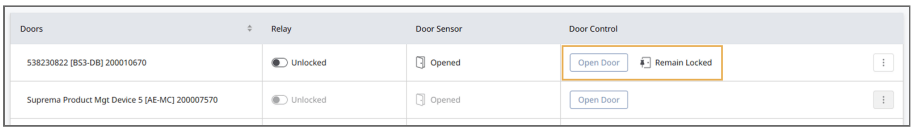
Web

1. ドアー覧で施錠状態にするドアの最も右にある ⋮ ボタンをクリックします。



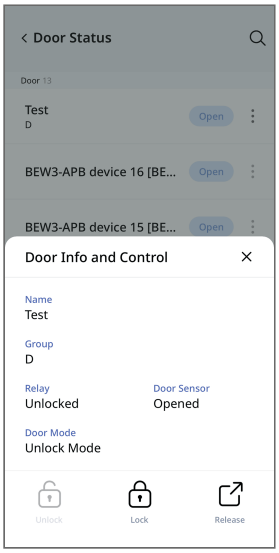
2. ポップアップメニューで **施錠モード** をクリックします。

3. **ドア制御** 列に **ロックされたままにする** として状態が変更されます。



正常な動作に戻すには ⋮ → **解放** をクリックします。

Mobile



1. ドアの最も右にある ⋮ ボタンをタップします。
2. **出入口情報と制御** オプションが表示されたら、**施錠モード** をタップします。
3. 画面下部に成功メッセージが表示されます。

正常な動作に戻すには ⋮ → **解放** をタップします。

安全

BioStar Airの**安全管理**機能は、通常運用時は現場内の人員を把握し、非常時は避難プロセスの管理を支援します。 **現場在留者確認**(On-Site Now)および**ゾーン**機能を含む在場(Presence)機能により、管理者は入退室権限を持つユーザーが現在現場にいるか、現場内のどこにいるかをリアルタイムで確認できます。 また、管理者は各人の状況を手動で変更することもできます。

人員点呼（Roll Call）機能は、指定された管理者が特定の集合場所を担当し、そのエリアに割り当てられた人員の安全を監督することで、秩序ある避難を支援します。 この機能は、**On-Site Now** 機能と同じ現場の人員把握エンジンを基に動作します。

以下のドキュメントを参照して、BioStar Airポータルで在席と点呼を管理する方法を確認してください。

在席を確認

安全 → **在席** メニューでは、現在サイトにいるユーザーをリアルタイムで確認できます。 在席（Presence）状態は **境界**(Perimeter Zone) に設定した入室および退室装置の認証記録に基づいて計算します。境界をまだ設定していない場合は、先に ゾーン管理を参照してください。

在席状態の決定方法

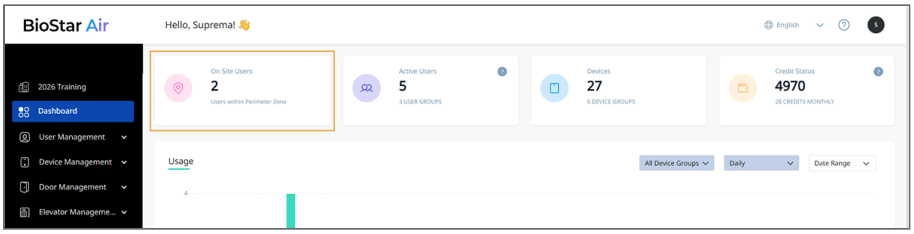
ユーザーは境界の入室装置で認証すると **オンサイト** 状態に、退室装置で認証すると **オフサイト** 状態に切り替わります。

- 境界に退室装置を指定していないサイトでは、**オフサイトタイマー**を必ず設定してください。 設定した時間の間に活動がない場合、ユーザーは **オフサイト** 状態に自動で切り替わります。
- 境界の入室および退室装置と **オフサイトタイマー** の設定方法は ゾーン管理を参照してください。
- 管理者は複数のメニューから現場にいる人の一覧と人数を確認できます。
  - **ダッシュボード** ウィジェット
  - **安全** → **在席**
  - **ゾーン管理** → **ゾーン** → **入室人数** (境界)

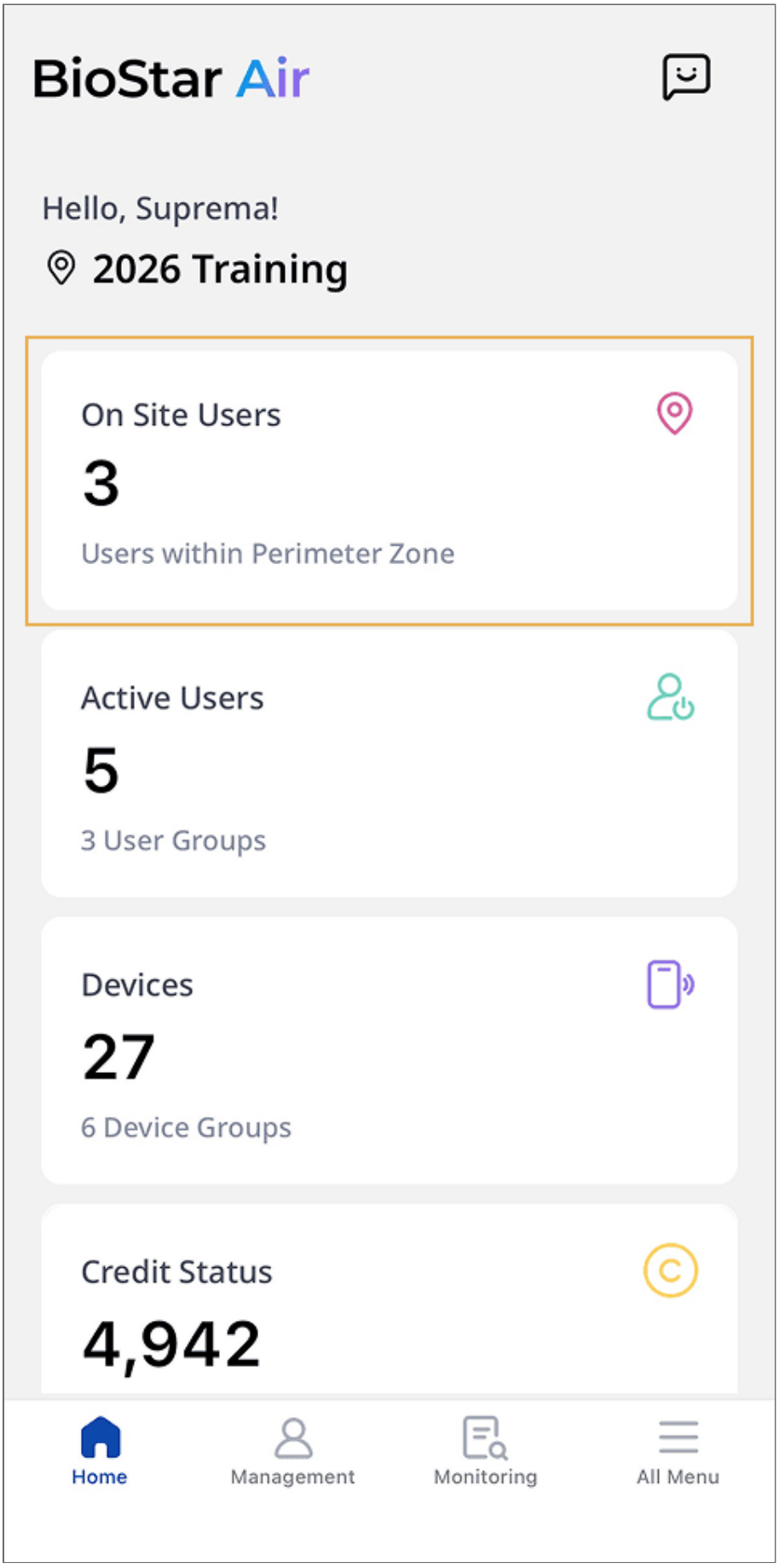
ダッシュボードで確認

ダッシュボード メニューでも **オンサイトのユーザー** カードで現在のサイトに在席しているユーザー数をすばやく確認できます。

Web


BioStar Air
Hello, Suprema!
English
2026 Training
Dashboard
User Management
Device Management
Door Management
Elevator Manageme...
On Site Users
2
Users within Perimeter Zone
Active Users
5
3 USER GROUPS
Devices
27
6 DEVICE GROUPS
Credit Status
4970
28 CREDITS MONTHLY
Usage
All Device Groups
Daily
Date Range

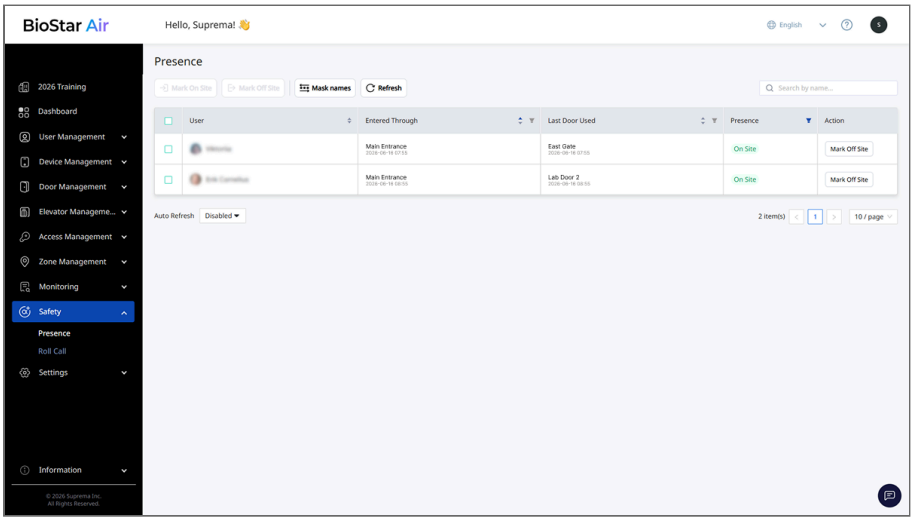
Mobile


BioStar Air
Hello, Suprema!
2026 Training
On Site Users
3
Users within Perimeter Zone
Active Users
5
3 User Groups
Devices
27
6 Device Groups
Credit Status
4,942
Home
Management
Monitoring
All Menu

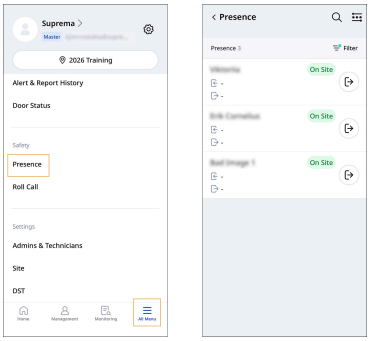
在席リストを確認

Web

画面左側のサイドバーで **安全** → **在席** をクリックしてください。



Mobile



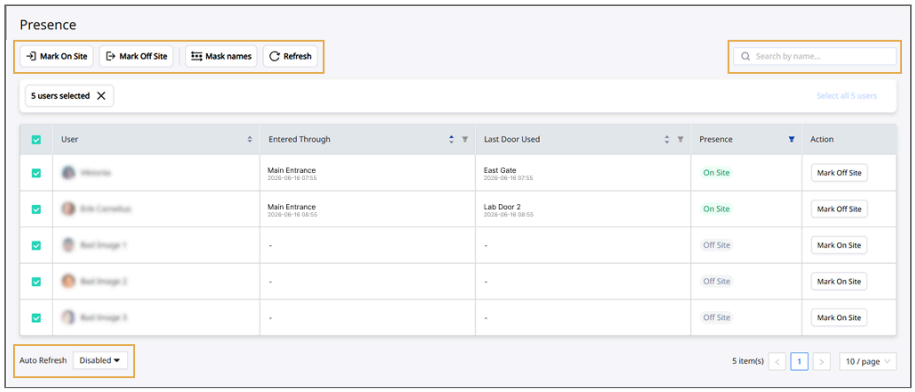
1. モバイル端末でBioStar Airアプリを起動してログインします。
2. 画面下部の **All Menu** → **在席** をタップしてください。

在席リストは、デフォルトで **オンサイト** 状態のユーザーのみを表示します。

- **ユーザー**：ユーザーのプロフィール写真と名前です。
- **入室ドア**：ユーザーがサイトに入るときに認証した入室装置と時刻です。
- **最後に使用したドア**：ユーザーが最後に使用した出入口と時刻です。
- **在席**：ユーザーの現在の在席状態（**オンサイト**/**オフサイト**）です。
- **操作**：ユーザーごとの在席状態を変更できます。

在席リストの管理機能

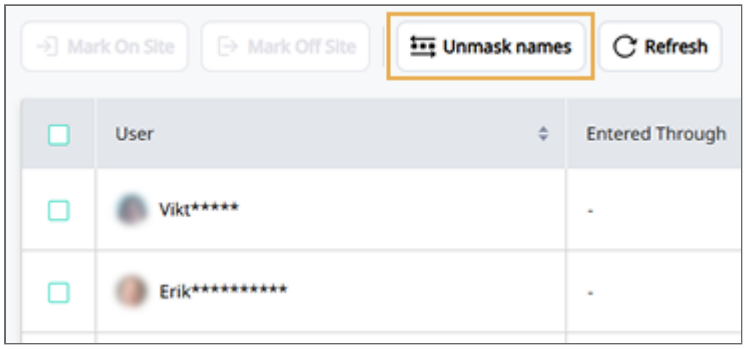
一覧の上部と下部にある管理機能で、次の作業を実行できます。



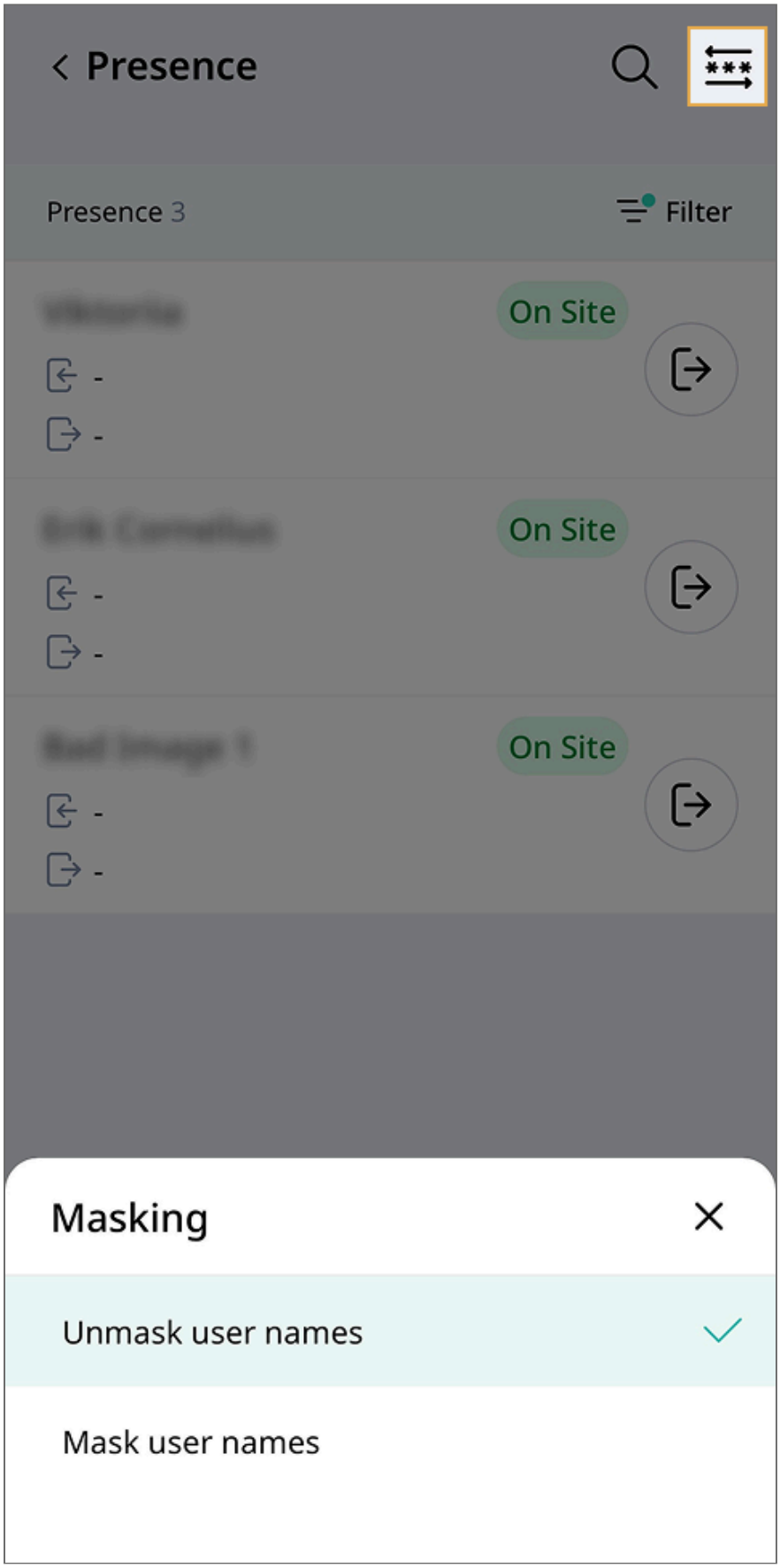
- **在席にする** / **不在にする**：ユーザーの在席状態をサイト内またはサイト外に変更できます。 詳細については、在席状態の手動変更をご参照ください。

- **名前をマスク** / **名前のマスク解除** (***)：ユーザー名を非表示にしたり、再表示したりします。 情報が機微な環境で画面を共有するときに役立ちます。

Web



Mobile



- **リフレッシュ**：一覧をすぐに更新し、最新状態にします。 一覧下部の**自動更新**で自動更新間隔(**無効**/**５秒**/**１分**)を選択すると、設定した周期で一覧を自動更新します。
- **名前で検索...**：ユーザー名でリストを検索します。

在席一覧のフィルタリング

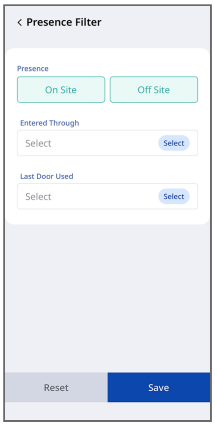
Web

在席 列の ボタンをクリックし、**オンサイト**、**オフサイト**、または全ユーザーを選択して一覧をフィルタリングします。 さらに、**入室ドア**、**最後に使用したドア** 列でも条件を選択してフィルタリングします。



> **情報**
> フィルターを解除するには **リセット** ボタンをクリックします。

Mobile



1. 在席一覧の右上にある **フィルター** をタップします。
2. **オンサイト** または **オフサイト** の状態を選択するか、両方を選択します。
3. **Entered Through**、**Last Door Used**で条件を選択します。
4. 選択した条件で一覧をフィルタリングするには **保存** ボタンをタップします。

> **情報**
> フィルターを解除するには **リセット** ボタンをタップします。

> **情報**
>
> - 全ユーザーを確認するには、**在席** 列で **オンサイト**、**オフサイト** を両方選択します。
> - 在席一覧は **オンサイト** 状態のユーザーをデフォルトで表示します。

在席状態の手動変更

実際の状況とシステムに記録された在席状態が異なる場合、管理者が状態を直接変更できます。

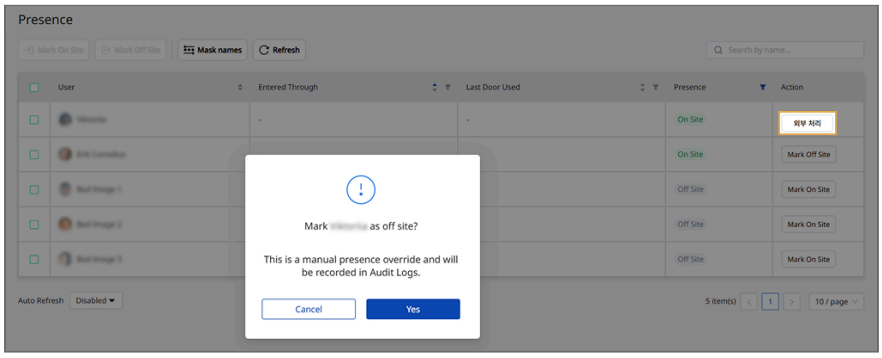
- 在席の精度は、サイトの入室および退室デバイス設定によって異なります。 入室および退室デバイスを明確に設定したサイトほど、信頼性の高い在席情報を提供します。
- デバイスがオフラインだった場合、またはイベント送信が遅延した場合、同期完了後に在席状態が更新されることがあります。
- 在席状態は入退室権限とは異なります。 **オンサイト** 状態で表示されたユーザーでも、すべてのドアにアクセスできるとは限りません。
- 期限切れ、無効、停止状態のユーザーは、アカウントが有効になるまで在席状態を変更できません。

> **情報**
> 手動変更はシステムに記録された状態を変更するだけで、ユーザーの実際の位置を物理的に確認する機能ではありません。 変更履歴は **モニタリング** → **監査ログ**で確認できます。

個別ユーザーの在席状態の変更

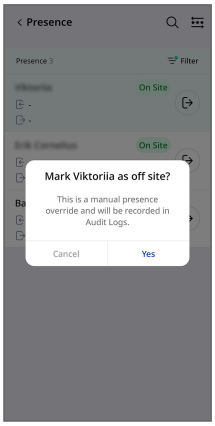
Web

1. 一覧で状態を変更するユーザーの **操作** 列にある **在席にする** または **不在にする** ボタンをクリックします。



2. 確認メッセージが表示されたら **はい** ボタンをクリックします。

Mobile

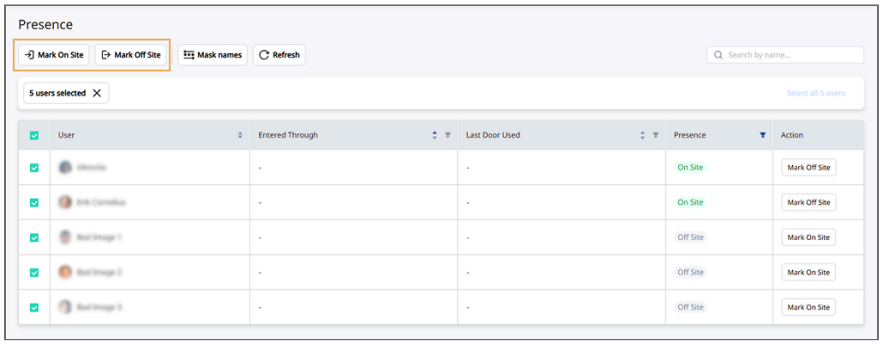


1. 一覧で状態を変更するユーザーの または ボタンをタップします。
2. 確認メッセージが表示されたら **はい** ボタンをタップします。

複数ユーザーの在席状態の変更

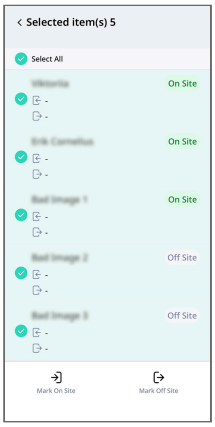
Web

1. 一覧で状態を変更するユーザーのチェックボックスをクリックします。 一人以上のユーザーを選択できます。
2. 一覧上部の **在席にする** または **不在にする** ボタンをクリックします。



3. 確認メッセージが表示されたら **はい** ボタンをクリックします。

Mobile



1. 一覧で状態を変更するユーザーを長押しします。
2. 状態を変更するユーザーを選択します。 一人以上のユーザーを選択できます。
3. 画面下部の **Mark On Site**( ) または **Mark Off Site**( ) ボタンをタップします。
4. 確認メッセージが表示されたら **はい** ボタンをクリックします。

ロールコール

BioStar Airの点呼（Roll Call）機能により、組織は緊急時にどのユーザーが安全に避難したかを追跡できます。 集結ゾーンを設定し、BioStar Airモバイルアプリで点呼を実施すると、管理者は在席情報に基づき現場にいたユーザーを迅速に把握し、安全を確認できます。

在席（Presence）に基づく正確な集結名簿

- 点呼は、すべてのユーザーが現場にいる前提ではありません。 在席（Presence）判定を併用し、緊急発生時点で現場にいると確認されたユーザーだけを集結対象として表示します。
- ユーザーグループを特定の集結ゾーンに割り当て、担当管理者を指定できます。安全担当者は担当ユーザーだけを集中的に管理できます。
- Suprema Passアプリは、現場にいるモバイルクレデンシャル利用者に正しい集結ゾーンを案内し、外部にいるユーザーには緊急中は施設へ入らないよう警告します。

情報

- 混乱を防ぐため、ユーザーグループに集結ゾーンが正しく割り当てられていることを確認してください。
- 実際の緊急時に備え、点呼機能を定期的にテストしてください。
- 出入記録により、出席を確認できます。

> **ヒント**
> ロールコールと集結地点に関する動画ガイドを視聴するには、次の動画を参照してください。

開始前に

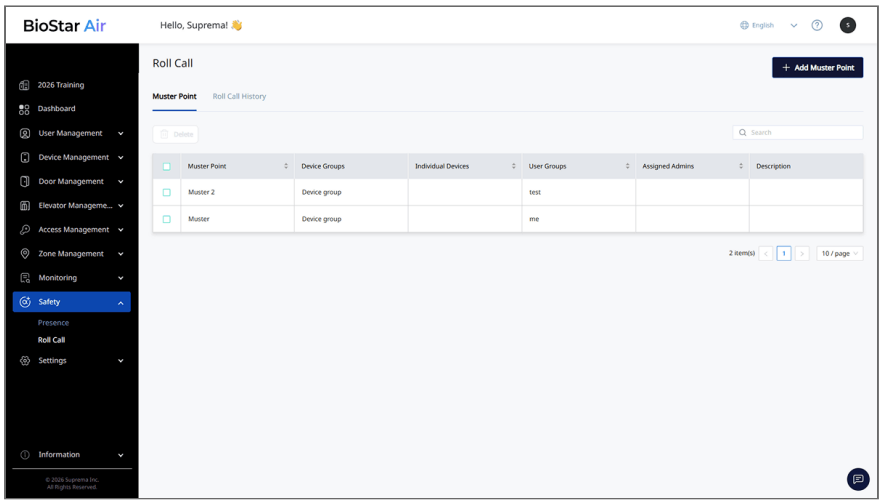
- 点呼の精度は在席検知に左右されます。 **境界**が正しく設定されていない場合、点呼リストが実際の現場人数と異なることがあります。
- モバイル通知にはSuprema Passアプリが必要です。 RFカードまたはバイオメトリッククレデンシャルのみを使用するユーザーは、モバイルの点呼通知を受け取れません。
- 集結ゾーンに割り当てられていない現場ユーザーは、集結場所の案内を受け取れないことがあります。
- **割り当て管理者** 設定が正しくない場合、担当者は想定した点呼画面を表示できないことがあります。
- デバイスがオフラインになったり、イベント送信が遅延したりすると、在席情報と点呼精度に影響することがあります。
- 無効なユーザーは点呼通知を受け取りません。

> **情報**
> 旧バージョンのSuprema PassまたはBioStar Airアプリを使うユーザーと管理者は従来の点呼方式を継続できます。ただし、新機能を使うには最新版へ更新してください。

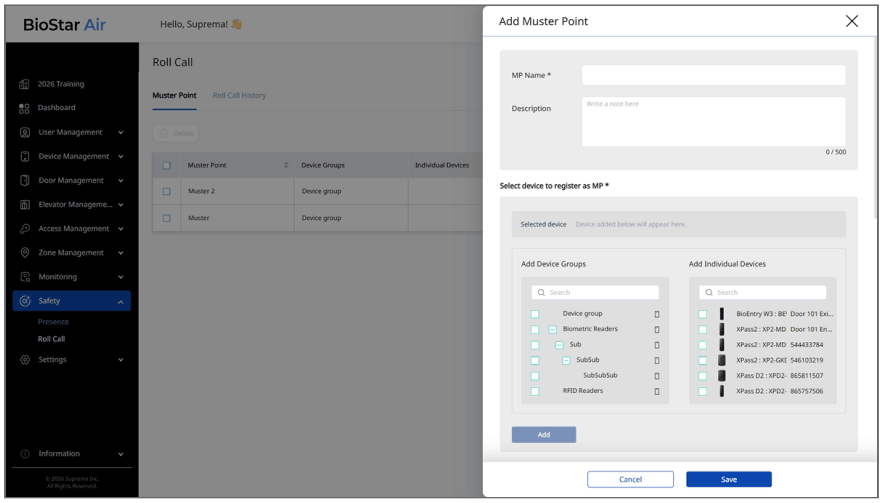
集結地点の設定

集結地点は、ユーザーが緊急時に自身の安全を示すためにクレデンシャルを認証できる指定場所です。

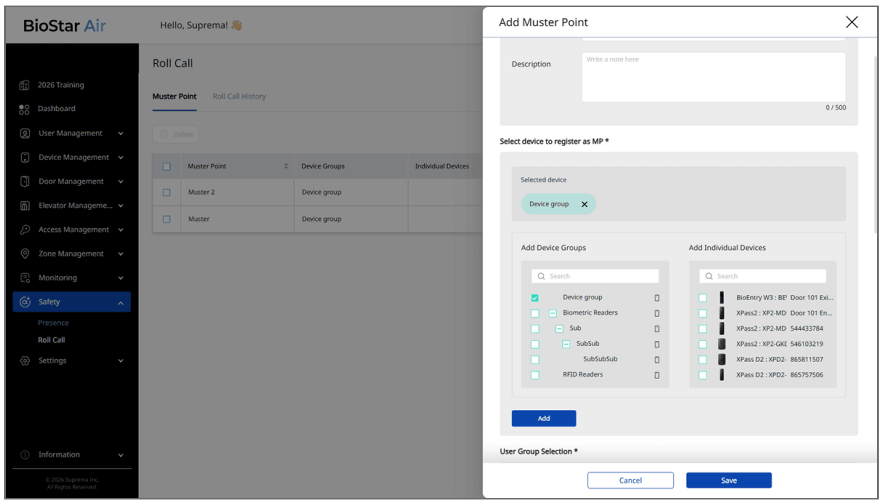
1. 画面左側のサイドバーで **安全** → **点呼** をクリックしてください。
2. 画面右上の **集合ポイントを追加** をクリックします。



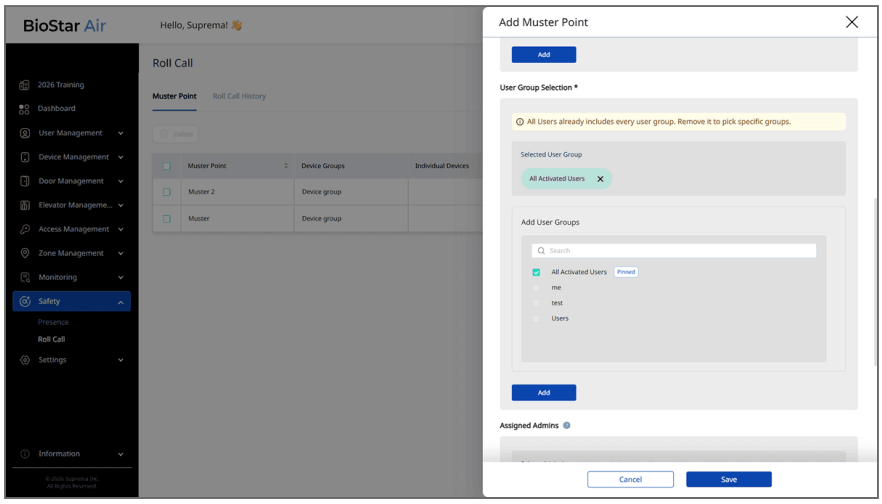
3. **集合ポイントの追加** パネルが開いたら、集結地点の名前と説明（任意）を入力してください。



4. **集合ポイントとして登録するデバイスを選択してください。 *** セクションで、集結地点に割り当てるデバイスグループまたはデバイスを追加します。 デバイスグループまたはデバイスのチェックボックスをクリックし、**追加** をクリックします。



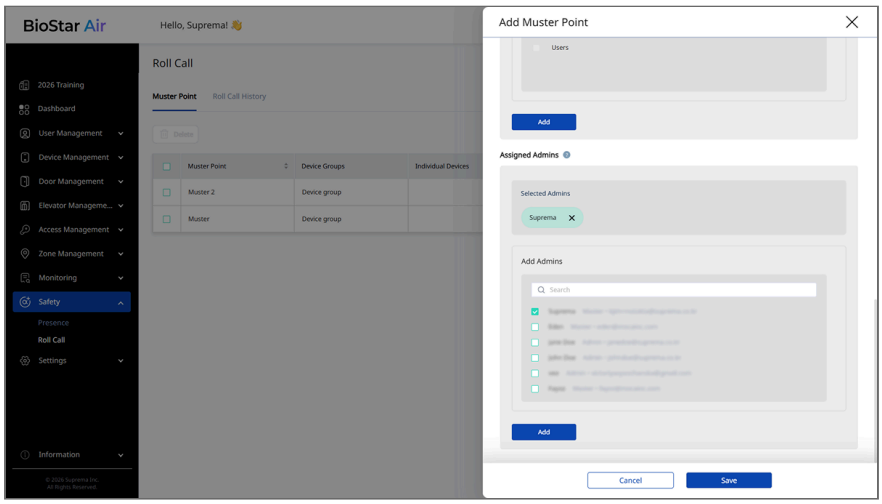
5. **ユーザーグループの選択 *** セクションで、集結地点に到着した際に報告すべきユーザーグループを選択します。



- 特定のユーザーグループを選択するには、該当グループのチェックボックスを選択し、**追加** ボタンをクリックしてください。

- **すべての有効なユーザー**: BioStar Air サイトで、現在アクティブな全ユーザーを選択した招集エリアに割り当てます。 実際に緊急招集を実行すると、全アクティブユーザーが現場にいるとみなさず、在室検知に基づいてサイトにいることが確認されたユーザーのみを招集対象にします。 このオプションをオンにすると、ユーザーグループを個別に選択する機能は無効になります。特定のグループのみを選択するには、先にこのオプションをオフにしてください。

6. **割り当て管理者** セクションで、該当する集合場所で点呼を実施する管理者のチェックボックスを選択し、**追加** ボタンをクリックします。



- **割り当て管理者**を選択した場合、選択した管理者のみが該当する点呼を開始できます。また、進行中の点呼でも、自分が担当するゾーンのユーザーだけを確認して管理できます。
- **割り当て管理者**を指定しない場合、**マスター**、**アドミン**、**オペレーター** などのロールのユーザーが点呼を開始できます。
- 管理者は同時に複数の点呼ゾーンの指定管理者として割り当てられることはできません。

7. 集結地点の設定を保存するには、**保存** をクリックします。

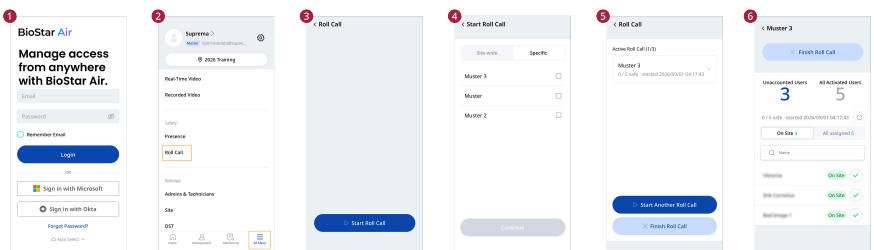
集結地点に関するベストプラクティス

- 集結地点の名前と説明は、明確で分かりやすく指定してください。 例：'東側駐車場'または'本館ロビー'のように指定できます。
- 集結地点に複数のデバイスを追加する場合は、個別のデバイスを選択するよりもデバイスグループを選択することを推奨します。 デバイスグループを使用すると、複数のデバイスを一度に管理できます。 デバイスグループ管理の詳細については、デバイスとパネルのグループを管理するをご参照ください。
- 複数の建物がある大規模キャンパスでは、**関連するユーザーのみ**を特定の集結地点に割り当ててください。
- 有線の入退室制御デバイスはモバイルとカード認証の両方をサポートしますが、Airfob TagやAirfob Patchはモバイルクレデンシャルのみをサポートします。

点呼を開始する

モバイルで開始

BioStar Airモバイルアプリでロールコールを開始し、出席を確認します。



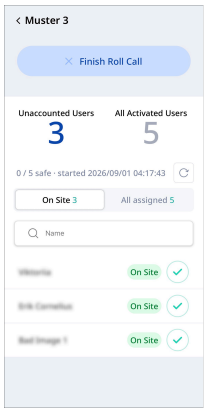
1. モバイル端末でBioStar Airアプリを起動してログインします。
2. 画面下部の **すべてのメニュー** → **点呼** を順にタップします。
3. **Start Roll Call** ボタンをタップします。
4. 点呼を開始するゾーンを選択し、**Continue** ボタンをクリックします。

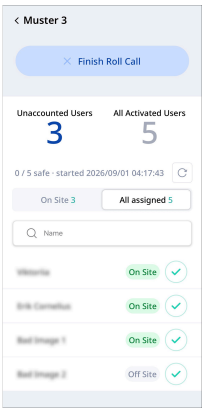
   すべてのゾーンで点呼を実施する場合、**Site-wide**を選択し、**Continue** ボタンをクリックします。
5. 進行中の点呼一覧でゾーンを選択します。
6. 集結場所に集まるべきすべてのユーザーの一覧が表示されます。

> **管理者の役割による違い**
> - ゾーンの **割り当て管理者**に指定されていない **マスター**、**アドミン**、**オペレーター** は、上記の順に点呼一覧を直接確認し、新しい点呼を開始します。
> - **割り当て管理者** は、自分が担当するゾーンで点呼が開始されると通知を受け取ります。 通知をタップすると、一覧を開かずに担当ゾーンの進行画面へ移動します。

進行中の点呼画面を確認する

点呼が開始されると、ゾーン名とともに進行状況が表示されます。

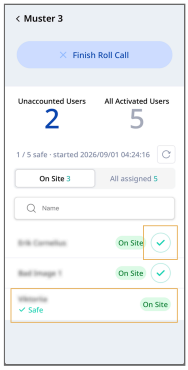




- 画面上部で **Unaccounted Users** と **All Activated Users'** の人数を確認できます。

  人数の下に **安全と表示された人数/総人数** と **点呼開始時刻** が表示されます。 更新(↻) ボタンをタップして最新状態を確認します。
- 一覧に表示するユーザー範囲を切り替えられます。
  - **On Site**: 現在、在席状態が現場（On Site）のユーザーのみを表示します。
  - **All assigned**: 在席状態に関係なく、このゾーンに割り当てられたユーザー全員を表示します。 安全と表示されたユーザーは、一覧の末尾に移動します。
- 検索機能で特定のユーザーを探せます。
- 一覧の各ユーザーの右側で在席状態（**オンサイト**/**オフサイト**）を確認できます。

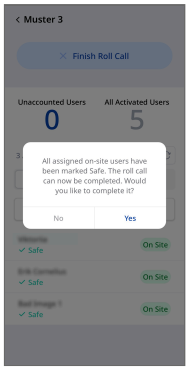
ユーザーを安全とマークする



管理者またはユーザーは、以下の方法で自身を安全とマークできます。

- 管理者はモバイルアプリでユーザー名の横にある**チェックマーク**ボタンを長押しして、ユーザーを安全にチェックできます。
- ユーザーは指定された集結地点でデバイスに自身のクレデンシャルをタグ付けします。

ロールコールの完了



以下の条件を満たしたら、ロールコールを完了します。

- 点呼範囲に含まれる オンサイト ユーザー、つまり **Unaccounted Users** が0になった完了メッセージ画面で **Yes** をタップするとき
- 管理者が全ユーザーを手動で安全とマークし、**Finish Roll Call** をタップするとき
- 24時間経過したとき

役割別の終了範囲

- サイトマスターは、点呼を個別に終了するか、複数件を選択して一括で終了するか、サイトで進行中のすべての点呼を一括で終了できます。
- **割り当て管理者**で選択した アドミン または オペレーター は、自分が担当する点呼ゾーンの点呼のみ終了できます。

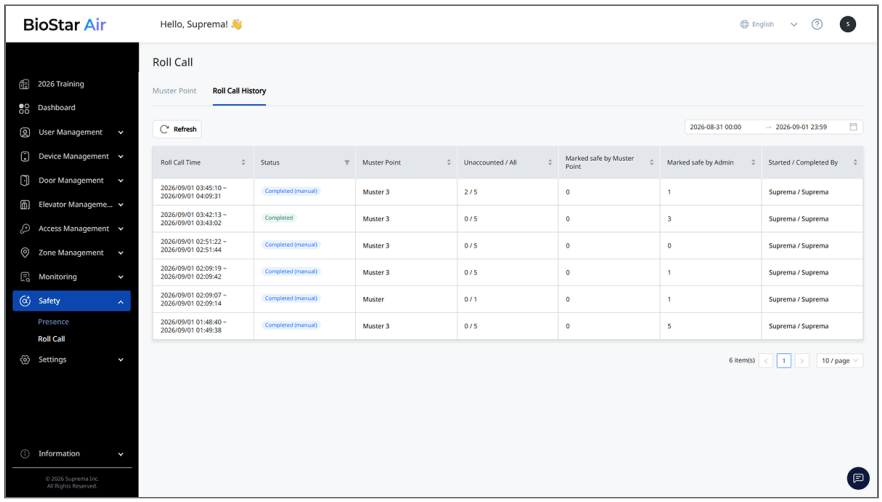
情報

オフサイト 状態のユーザーも手動で安全とマークできます。 例えば、当日在宅勤務のユーザーの安全を事前に確認できます。

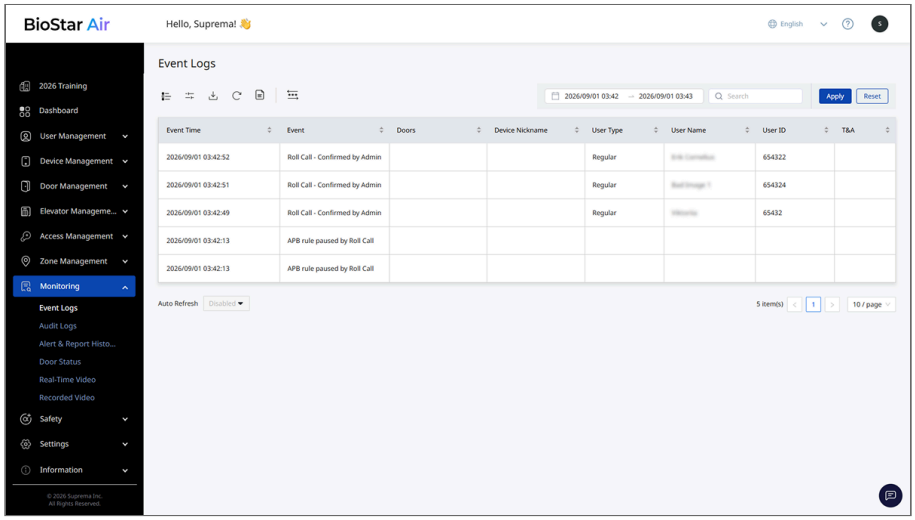
ロールコール履歴の表示

以前に実施したロールコールの履歴を確認できます。

1. 画面左側のサイドバーで **安全** → **点呼** をクリックしてください。
2. **点呼履歴** タブをクリックしてください。



3. 詳細を確認するには、完了したロールコール項目をクリックします。



- ロールコール中に記録されたすべての入退室イベントの一覧を確認できます。
- ユーザーが安全とマークされているか確認されていないかの詳細を確認できます。
- ロールコールの開始および完了時間を確認できます。

サイトを設定する

BioStar Airシステムを円滑に運用するための基本設定を管理します。 運用権限を持つ管理者アカウントの管理、組織の基本情報設定、タイムゾーンおよび通知の構成、メールテンプレートのカスタマイズ、カード形式の設定などを通じて、システムを組織の要件に合わせて構成できます。

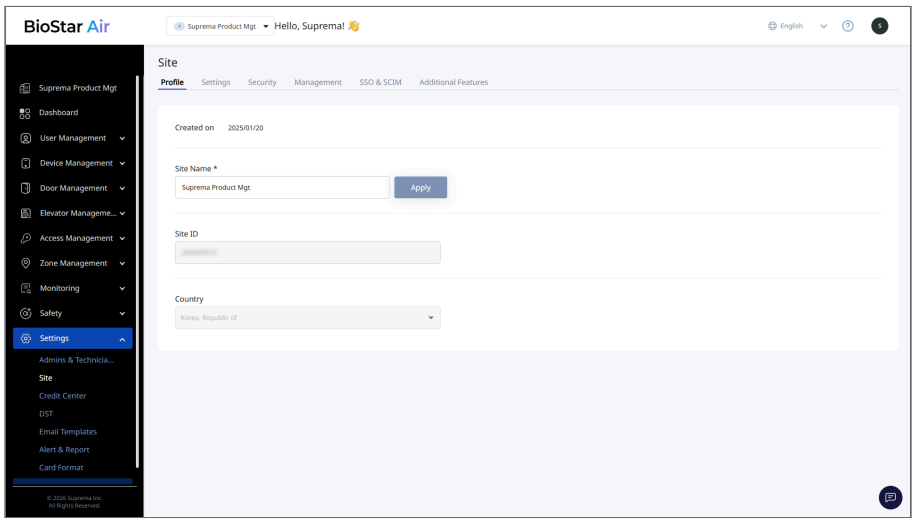
> **ヒント**
> サイト設定の動画ガイドを視聴するには、以下の動画を参照してください。

基本情報を設定する

サイト情報はBioStar Airの基本設定です。 本書では、サイト名や識別子などの基本情報を管理する方法と、必要に応じてサイトを削除する方法を説明します。

サイト情報の設定

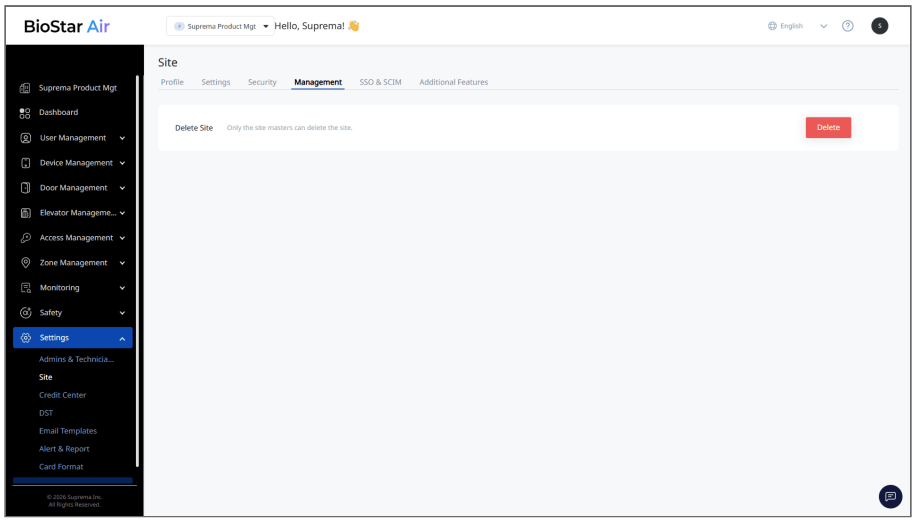
画面左のサイドバーで **設定** → **サイト** をクリックします。 **プロフィール**：サイトの基本情報を編集できます。



- **サイト名**：サイトの名前です。 新しい名前を入力して **適用** ボタンをクリックします。 いつでも変更できます。
- **サイトID**：サポート要求時に必要な固有識別子です。 MOCAチームと連絡する際に、サイトIDをコピーして提供できます。
- **国**：サイト作成時に設定され、後で変更できません。 変更が必要な場合は、BioStar Airパートナーポータルで手続きをしてください。

サイトの削除

画面左のサイドバーで **設定** → **サイト** をクリックします。 **管理** タブで使用できる唯一のオプションは **サイト削除** 機能です。 この操作は元に戻せず、**マスター管理者**のみサイトを削除できます。

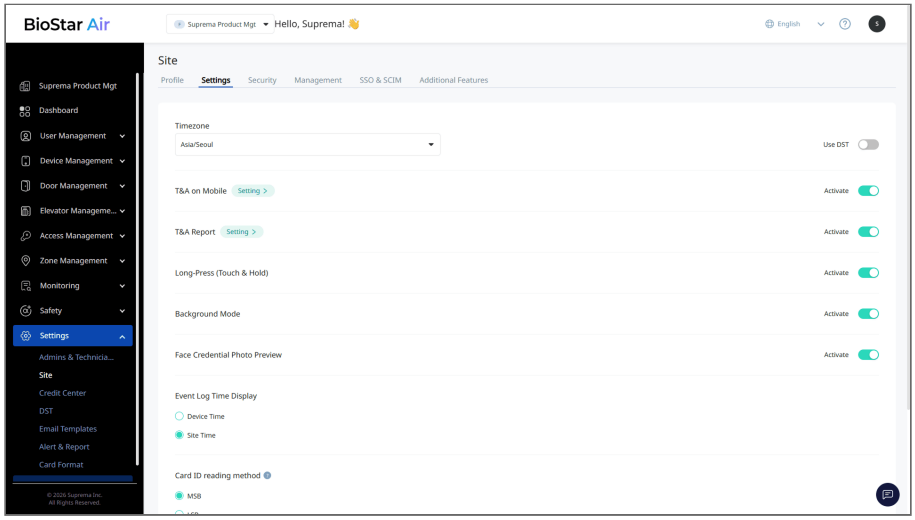


高度設定

高度なオプションを設定して、BioStar Air を組織の業務環境に合わせて最適化してください。 タイムゾーンとサマータイムを設

定し、勤怠管理を有効にし、モバイル認証方式やイベントログの表示方法を調整できます。

画面左のサイドバーで **設定** → **サイト** をクリックします。 **Settings**：サイトの設定を構成できます。



- **タイムゾーン**：タイムゾーンはいつでも変更できます。 設定したタイムゾーンに従ってログとイベントを記録します。 詳細については、サマータイム（DST）の設定を参照してください。
  - **夏時間を使用**：特定地域で適用されるサマータイムを有効化または無効化できます。
- **モバイルでのT&A**：勤怠管理（T&A）機能を有効化できます。 勤怠管理機能を有効化した後、**設定** ボタンをクリックして詳細設定を構成してください。 詳細については、勤怠管理（T&A）の設定を参照してください。
- **T&Aレポート**：勤怠レポート（T&A Report）を生成できます。 勤怠レポート機能を有効化した後、**設定** ボタンをクリックしてレポート生成条件を構成してください。 詳細については、勤怠レポートを構成するを参照してください。
- **長押し（タッチ＆ホールド）**：一定距離離れた出入口を遠隔で開けられるロングタッチ（Long Touch）機能を有効化できます。
- **バックグラウンド モード**：Suprema Passアプリがバックグラウンドモードのときにモバイルカードの使用を許可します。 この設定を有効化すると、ユーザーはアプリを開かなくてもドアを開けられます。
- **顔認証写真のプレビュー**：顔クレデンシャル発行時に顔写真プレビューを表示できます。
- **イベントログの時間表示**：イベントログの時刻表示方法を設定します。
  - **デバイス時間**：各デバイスの設定で構成したタイムゾーンに基づいてイベントログを表示します。
  - **サイト時間**：サイトのタイムゾーンに従ってログを表示します。 すべてのデバイスが同一場所にあるサイトに適しています。 **タイムゾーン** オプションを参照してください。
- **カードIDの読み取り方法**：Airfob Patchをサードパーティ製リーダーと併用する際のカードデータ送信方法を設定します。

> パッチデバイス専用の設定で、パッチを取り付けるサードパーティ製デバイスのタイプに合わせて設定できます。

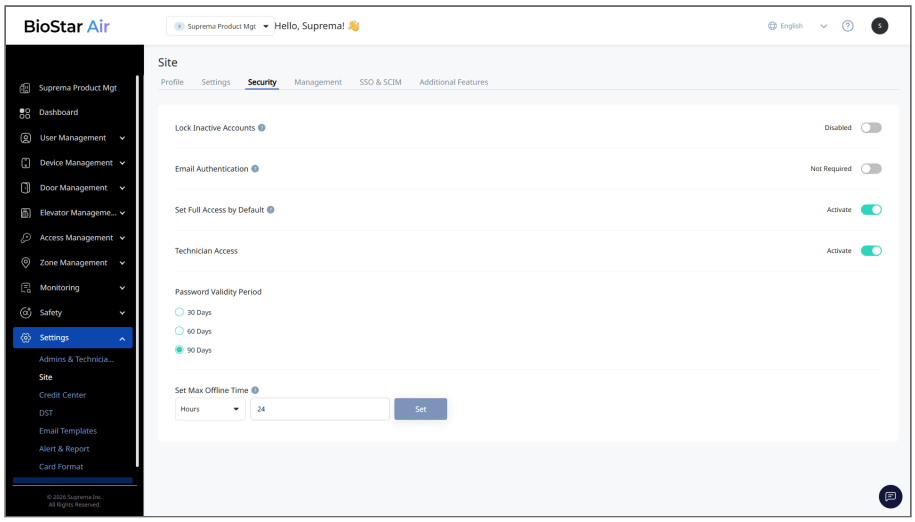
- **モバイル アクセス カードの有効化/再発行リンクの有効期間**：モバイルクレデンシャルのデフォルト有効期間を設定します。

> 管理者は個々のユーザーのクレデンシャルに対して個別の有効期限を設定できます。 詳細については、ユーザーの追加を参照してください。

セキュリティの設定

不正アクセスを防ぎ、サイトを安全に運用するには、適切なセキュリティポリシーを構成する必要があります。 非アクティブな管理者アカウントのロック、メールによる2段階認証、パスワード変更の周期設定などにより、サイトのセキュリティレベルを強化できます。

画面左のサイドバーで **設定** → **サイト** をクリックします。 **安全** タブでサイトのセキュリティに関する設定を構成できます。



- **非アクティブアカウントのロック**：90日以上アクセスしていない管理者アカウントをロック状態に変更できます。
- **メール認証**：管理者アカウントでログインするたびにメールによる2段階認証を要求できます。
- **デフォルトでフルアクセスを設定**：他のアクセス権が選択されていない場合、新規ユーザーに「全アクセス権」をデフォルトで付与します。 この設定を無効にすると、アクセスレベルを手動で割り当てる必要があります。 一時ユーザーは、上記の設定が有効でも自動的に全アクセス権を付与されません。

> アクセスレベル管理の詳細は 出入レベルの管理性行する を参照してください。

- **技術者アクセス**：技術者アカウントがサイトにアクセスできるようにします。 この設定を無効にすると、技術者アカウントはサイトにアクセスできません。

> 技術者アカウントのサイトアクセス権の管理方法の詳細は サイトに技術者を割り当てる を参照してください。

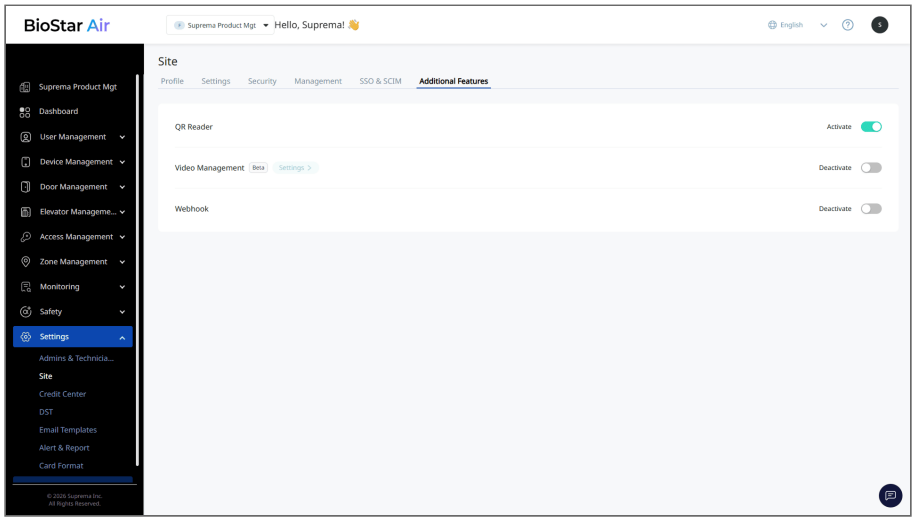
- **パスワードの有効期限**：30日、60日、90日ごとにパスワードをリセットするように設定できます。
- **最大オフライン時間の設定**：モバイルデバイスがネットワークに接続されていなくてもモバイルクレデンシャルが有効である時間を設定できます。

> – デフォルトは5分で、1分から8日の間で設定できます。
> – セキュリティと利便性のバランスをとるのに役立ち、特にネットワーク接続が制限される遠隔サイトで有用です。

拡張機能の設定

QRコードリーダーの利用可否、ONVIFカメラ連携、外部システムへのイベント送信（Webhook）など、サイト運営に必要な拡張機能を有効化または無効化できます。

画面左のサイドバーで **設定** → **サイト** をクリックします。 **追加機能** タブで追加機能を有効化または無効化できます。



- **QRリーダー**：QRコードリーダーをサポートします。 QRリーダーを使用しない場合は、該当オプションを無効にしてください。
- **ビデオ管理**：ONVIF互換のIPカメラをサポートします。 BioStar Airとビデオ監視を統合するには、この機能を有効化してください。 機能を有効化した後、**設定** ボタンをクリックするとイベントログの再生時間を設定できます。

> ビデオ管理の詳細については、IPカメラのサポートおよび設定をご参照ください。

- **Webhook**：Webhookを有効化して、BioStar Airのイベントを外部システムに送信できます。 この機能を有効化した後、以下の項目を設定してください。



  - **Webhook URL**：イベントを受信する外部サーバーのエンドポイントアドレスを入力してください。 例：`https://example.com/webhook-endpoint`
  - **シークレット**：Webhookリクエストが信頼できる送信サーバーから送信されたかを検証するためのセキュリティトークンです。 発信サーバーはセキュリティキーを使用してデータ本文（Payload）をSHA256で暗号化し、ヘッダーに `X-Signature` として送信します。
  - **テストの送信**：Webhookが正しく動作するかどうかを確認できます。 テストメッセージを送信して外部サーバーがリクエストを受信し応答するかを検証してください。

情報

- 必要な情報をすべて入力したら、**保存** ボタンをクリックしてください。
- 入力した情報を初期化するには、**リセット** ボタンをクリックしてください。

管理者アカウントおよび役割の管理

BioStar Airの管理者アカウントおよび役割管理により、サイトのアクセス権を効果的に制御できます。 オブザーバー（Observer）、オペレーター（Operator）、管理者（Administrator）、マスター（Master）の4つの役割を割り当て、各担当者に必要な権限のみを付与することで、セキュリティと運用効率を両立させます。

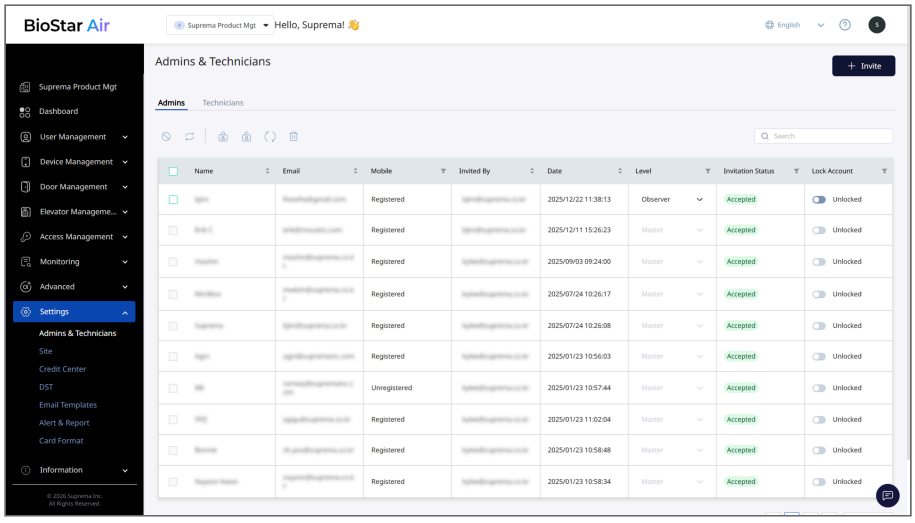
本書では、管理者の招待から役割割当、権限管理、アカウントのロックまで、管理者アカウントのライフサイクル全体を案内します。

ヒント

管理者管理に関するビデオガイドを見るには、次の動画を参照してください。

管理者の表示

画面左のサイドバーで **設定** → **デバイスのみ** をクリックしてください。



情報

技術者アクセス オプションを有効にすると、**設定** → **アドミン** メニューが **デバイスのみ** メニューに変更されます。 **アドミン** と **技術者** タブに分かれ、管理者アカウントと技術者アカウントをそれぞれ管理できます。

技術者アクセス オプションを有効にする方法の詳細は 技術者アカウントを管理する を参照してください。

管理者一覧

デバイスのみ メニューではすべての管理者の一覧を確認できます。 管理者一覧には次の情報が含まれます。

- **名前**：管理者の名前です。

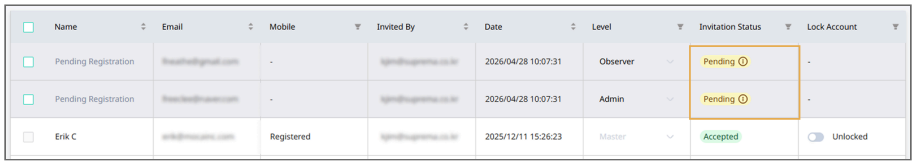
- **メール**：管理者のメールアドレスです。
- **モバイル**：管理者の電話番号です。
- **招待者**：管理者を招待した人のメールアドレスです。
- **日付**：管理者が招待された日付です。
- **レベル**：管理者の権限レベルです。 詳しくは 管理者レベル を参照してください。
- **招待ステータス**：管理者アカウントの招待状況です。 詳しくは 招待状況 を参照してください。
- **アカウントをロック**：管理者アカウントのロック状態です。 アカウントをロックまたはロック解除できます。 詳しくは 管理者のロック/ロック解除 を参照してください。

招待状況

管理者一覧で各管理者の招待状況を確認できます。

登録待ち

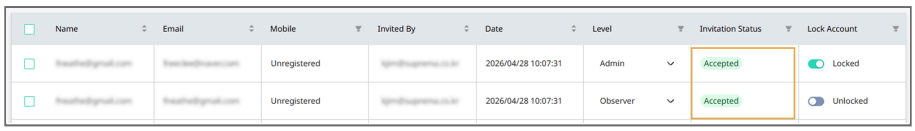
招待された管理者がメールでの招待を受け入れ、登録を完了するまで、招待状況は **保留中** と表示されます。 招待された管理者はメール内のリンクをクリックしてアカウントを登録するか、ログインしてサイトにアクセスできます。



> **情報**
> 招待された管理者は最大7日以内に招待を承諾できます。7日を過ぎると招待は失効し、状態は **期限切れ** に変更されます。 招待が失効した場合、該当アカウントが再登録できるよう招待リンクを再送できます。 招待リンクの再送の詳細は 招待リンクの再送 を参照してください。

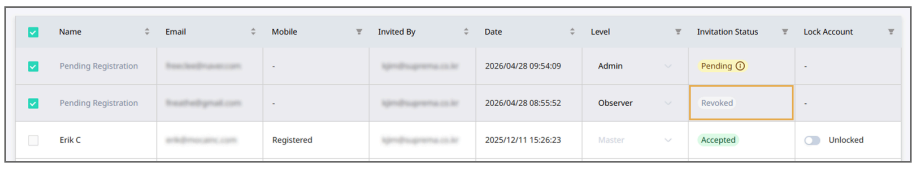
登録完了

招待された管理者がメールの招待を受け入れて登録を完了すると、招待状況は **承諾済み** に変更されます。 登録が完了した管理者はログインして、付与された役割に応じたメニューと機能にアクセスできます。



招待の取り消し状態

招待した管理者のメールアドレスを誤って入力した場合や、もはや管理者招待が不要になった場合、招待を取り消せます。 招待を取り消すと、招待状況が **無効** に変更されます。 管理者招待の取り消しの詳細は 招待の取り消し を参照してください。



管理者レベル

BioStar Airの各管理者レベルは特定の権限を持ち、高いレベルは低いレベルの権限を継承します。

> **情報**
> 各管理者の役割は、BioStar Air全体で異なる権限を持っています。 **オブザーバー** は最も制限されたアクセス権を持ち、画面に表示されない制限されたメニューがあります。

権限比較

機能	オブザーバー	オペレーター	管理者	マスター
ダッシュボード/ログの参照	✔	✔	✔	✔
ログのエクスポートおよびレポート作成	✔	✔	✔	✔
ユーザー管理	✕	✔	✔	✔
ユーザーグループの管理	✕	✔	✔	✔
出入レベルの管理	✕	✔	✔	✔
スケジュールの管理	✕	✔	✔	✔
祝日グループの管理	✕	✔	✔	✔
デバイスの制御および設定	✕	✕	✔	✔
管理者の招待	✕	✕	✔	✔
マスター役割の割り当て	✕	✕	✕	✔
マスター管理者の編集/削除	✕	✕	✕	✔
サブサイトの作成	✕	✕	✕	✔
サイト設定の構成	✕	✕	✕	✔

オブザーバー（最低レベル）

- **ダッシュボード** とログを**表示できます。**
- ログを**エクスポートして**レポートを作成できます。
- 設定、ユーザー、またはデバイスを変更することは**できません。**
- メニューへのアクセスが制限されます。 ほとんどのメニューは画面に表示されません。

オペレーター

- **ユーザー**および **ユーザーグループ**、**アクセスレベル**、**スケジュール**、**休日グループ** を管理できます。
- デバイスの制御や管理設定へのアクセス権は**ありません**。
- 日常的なユーザーと入退室構成の管理に適しています。

アドミン

- 新しい管理者を**招待できます**。 ただし、**マスター** 役割を割り当てることはできません。
- **すべてのデバイス制御権限**があり、設定を変更して接続されたデバイスを管理できます。
- **マスター** 役割の管理者を削除または変更することはできません。
- 一般的に、システム管理を担当するIT担当者にこの役割を割り当てることを推奨します。

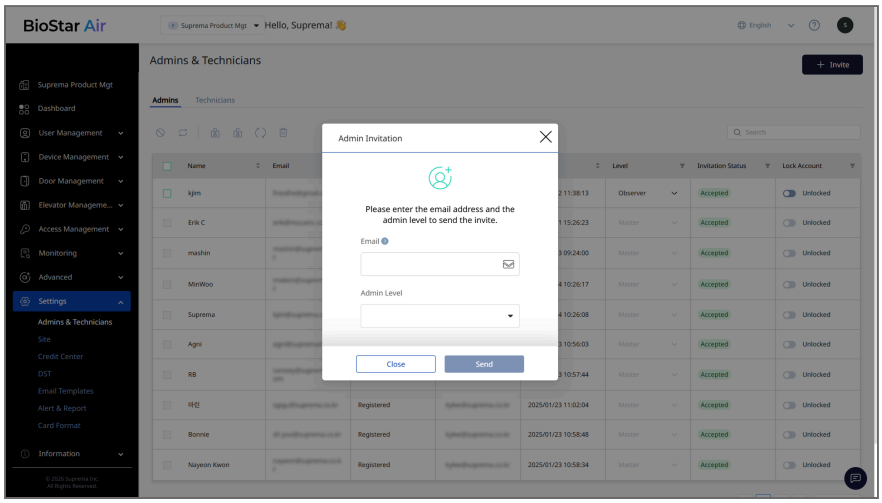
マスター（最高レベル）

- すべての設定と機能に**完全なアクセス**権があります。
- 他の**Administrators**によって削除または変更されることは**ありません**。
- **サブサイト**を作成して、さまざまな場所や組織を管理できます。
- **サイト設定**を構成でき、ここには重要なシステム全体の構成も含まれます。
- 他の管理者がログインする前に**利用規約**に同意させる責任があります。
- 一般的に会社の所有者や高い信頼を受ける役員に割り当てることができます。

新しい管理者の招待

新しい管理者を追加できます。

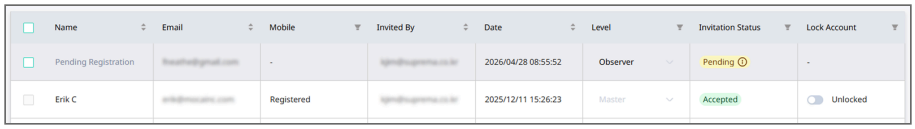
1. 画面左のサイドバーで **設定** → **デバイスのみ** をクリックしてください。
2. 画面右上の **招待** をクリックします。
3. **アドミンへの招待** ダイアログが表示されたら、メールアドレスを入力します。



4. **アドミンレベル** で新しい管理者に割り当てる役割を選択します。

5. 招待状を送信するには、**送信** をクリックします。

招待されたアカウントは管理者一覧で **招待ステータス** が **保留中** と表示されます。 招待されたアカウントがメールで招待を受け入れると、**招待ステータス** は **承諾済み** に変更されます。

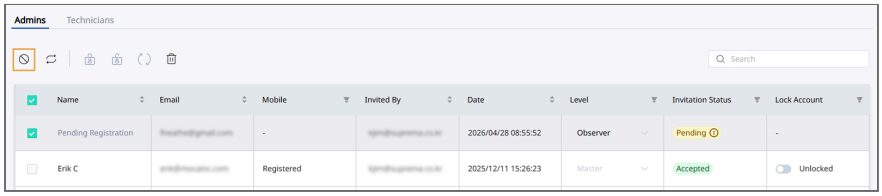


- 招待されたアカウントは最大7日以内に招待を承諾できます。7日を過ぎると招待は失効し、状態は **期限切れ** に変更されます。
- 各管理者は固有のメールアドレスを持つ必要があります。 必要に応じてエイリアスアドレス（例：erik+training@example.com）を使用できます。
- 招待メールを受け取った管理者は、メール内のリンクをクリックします。 アカウントを持っていない管理者は登録を行います。 既にアカウントを持っている管理者は、ログイン後すぐに**サイト**にアクセスできます。

招待の取り消し

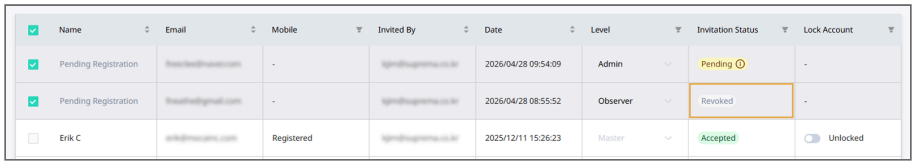
招待されたアカウントがまだ招待を承諾していない場合、招待を取り消せます。 招待を取り消すと、登録待ちのアカウントはメールの招待リンクで登録できなくなります。

1. 管理者一覧で招待状況が **保留中** のアカウントのチェックボックスをクリックします。 1人以上のアカウントを選択できます。
2. 管理者一覧の左上にある ⃠ ボタンをクリックします。



3. ポップアップメッセージが表示されたら内容を確認し、**はい** ボタンをクリックしてください。

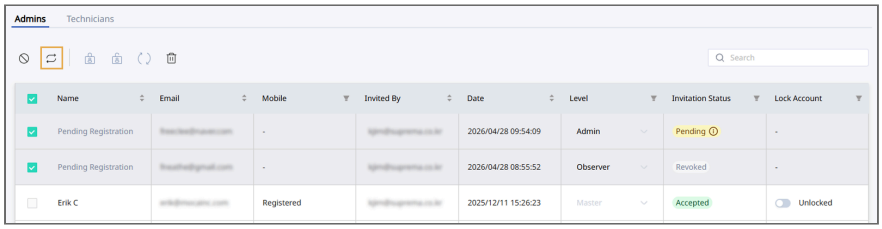
管理者一覧で招待を取り消したアカウントは、招待状況が **無効** に変更されます。



招待リンクの再送

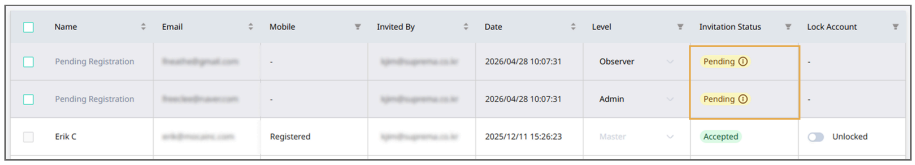
招待されたアカウントが招待メールを受け取っていない、招待メールを紛失した、または招待リンクが期限切れになった場合、招待リンクを再送できます。 招待リンクを再送すると、当該ユーザーは新しい招待リンクで登録できます。

1. 管理者一覧で招待状況が **保留中**、**期限切れ**、または **無効** のアカウントのチェックボックスをクリックします。 1人以上のアカウントを選択できます。
2. 管理者一覧の左上にある ⟲ ボタンをクリックします。



3. ポップアップメッセージが表示されたら内容を確認し、**はい** ボタンをクリックしてください。

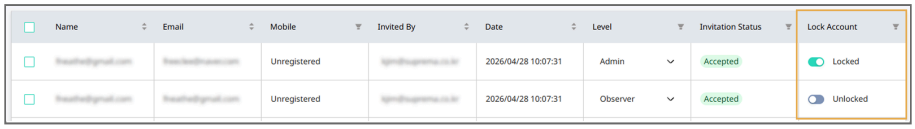
招待リンクを再送したアカウントは、招待状況が **保留中** に変更されます。



管理者のロック/ロック解除

メール招待を受け入れて登録を完了した管理者は、**アカウントをロック** オプションでアカウントをロックまたはロック解除できます。 アカウントをロックすると、その管理者はサイトにログインできなくなります。アカウント情報は保持され、必要に応じて後で再有効化できます。

ロックされた管理者は **アカウントをロック** 列が **ロック済み** と表示され、ロック解除された管理者は **ロック解除済み** と表示されます。

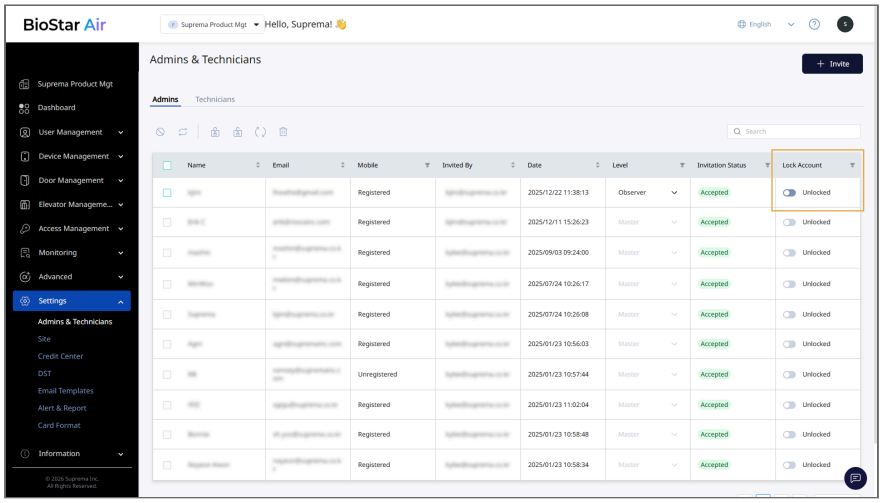


情報

- 登録が完了した管理者アカウントのみロックまたはロック解除できます。
- 管理者の **アカウントをロック** 機能は、管理者の権限によって制限される場合があります。 **マスター** 権限を持つ管理者は、他の **マスター** 管理者をロックできません。

個別の管理者ロック/ロック解除

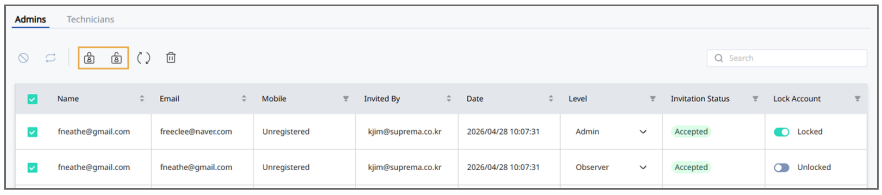
1. 管理者一覧でロックまたはロック解除する管理者を探します。
2. **アカウントをロック** 列でトグルスイッチをクリックします。



3. 確認ダイアログが表示されたら、**OK** をクリックしてください。

複数管理者のロック/ロック解除

1. 管理者一覧でロックまたはロック解除する管理者のチェックボックスをクリックします。 1人以上の管理者を選択できます。
2. 画面左上の または ボタンをクリックします。

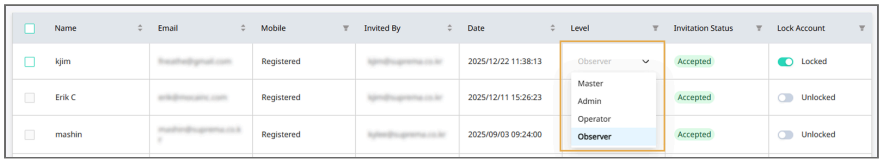


3. ポップアップメッセージが表示されたら内容を確認し、**はい** ボタンをクリックしてください。

管理者の役割変更

管理者は自分より低いレベルの管理者の役割を変更できます。 従業員の業務変更、責任範囲の拡大・縮小、組織再編などの際に役割を調整します。 役割を縮小すると、該当の管理者は以前アクセスできた機能にアクセスできなくなります。

1. 管理者一覧で役割を変更する管理者を探します。
2. **レベル** 列で新しい管理者レベルを選択します。



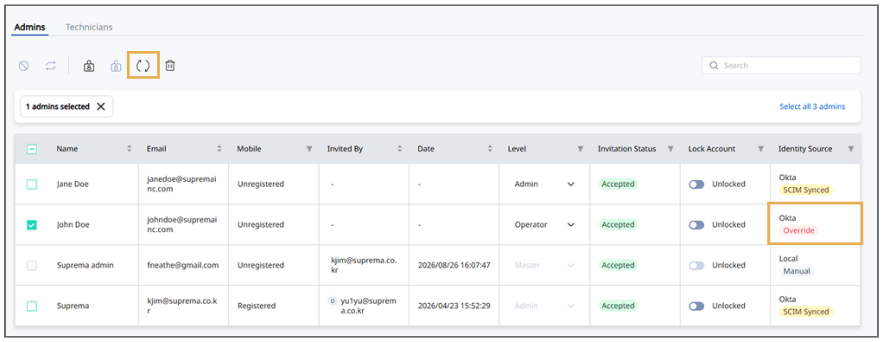
3. 確認ダイアログが表示されたら、**OK** をクリックしてください。

> **マスター** 管理者のみが他の管理者に **マスター** 権限を割り当てたり変更したりできます。

オーバーライド状態の解除

SCIMで同期された管理者の権限またはロック状態をローカルで手動で変更すると、**オーバーライド** 状態になります。 ローカルの変更を取り消し、SCIM管理状態に戻せます。

1. 管理者一覧で **オーバーライド** 状態の管理者のチェックボックスをクリックします。 1人以上の管理者を選択できます。
2. 画面左上の ボタンをクリックします。



3. ポップアップメッセージが表示されたら内容を確認し、**はい** ボタンをクリックしてください。

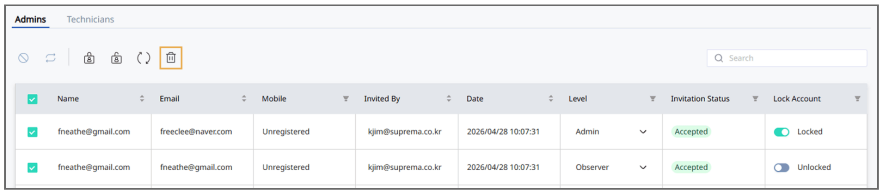
選択した管理者アカウントの **オーバーライド** 状態が解除され、**SCIM同期済み** 状態に変わります。

> **情報**
> SSOとSCIM設定の詳細については[SSO & SCIM を設定する]を参照してください。

管理者アカウントの削除

管理者アカウントを削除すると、該当の管理者はサイトにログインできなくなり、削除されたアカウント情報は復元できません。

1. 管理者一覧で削除する管理者のチェックボックスをクリックします。 1人以上の管理者を選択できます。
2. 画面左上の ボタンをクリックします。



3. ポップアップメッセージが表示されたら内容を確認し、**はい** ボタンをクリックしてください。

削除した管理者アカウントは管理者一覧に表示されなくなります。

技術者アカウントを管理する

技術者は顧客サイトへのアクセス権を付与された専門家です。 技術者アカウントを管理するには、パートナーポータルで技術者を招待し、各サイトに割り当てて権限レベルを設定します。

BioStar Air ポータルでは、サイトに招待された技術者のアクセス権を変更したり、サイトへのアクセスをロックまたは解除したりできます。 また、技術者アカウントを完全に削除してサイトへのアクセス権を取り消すこともできます。

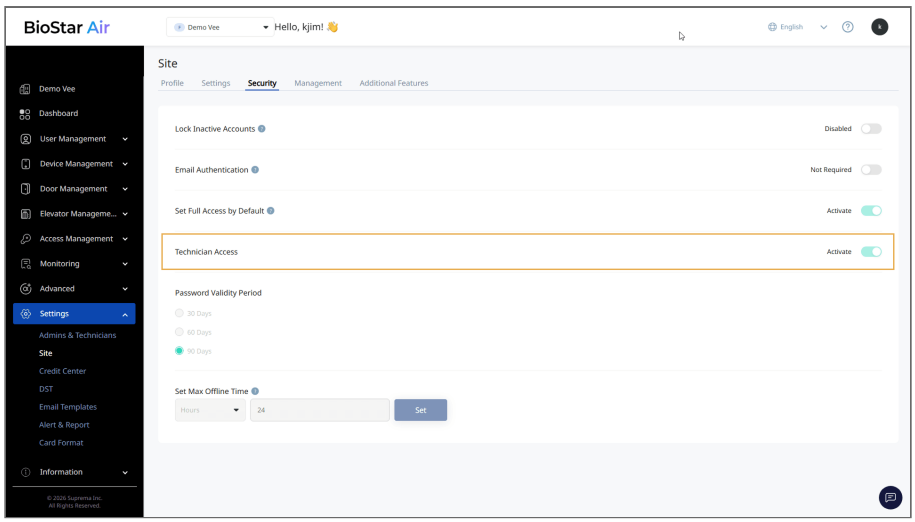
情報

- パートナーポータルで技術者を招待しサイトに割り当てる方法の詳細は、パートナー技術者の管理を参照してください。
- 技術者として招待されたユーザーの活動は、**モニタリング** → **イベントログ**/**監査ログ**で個別アカウントごとに記録され、追跡できます。

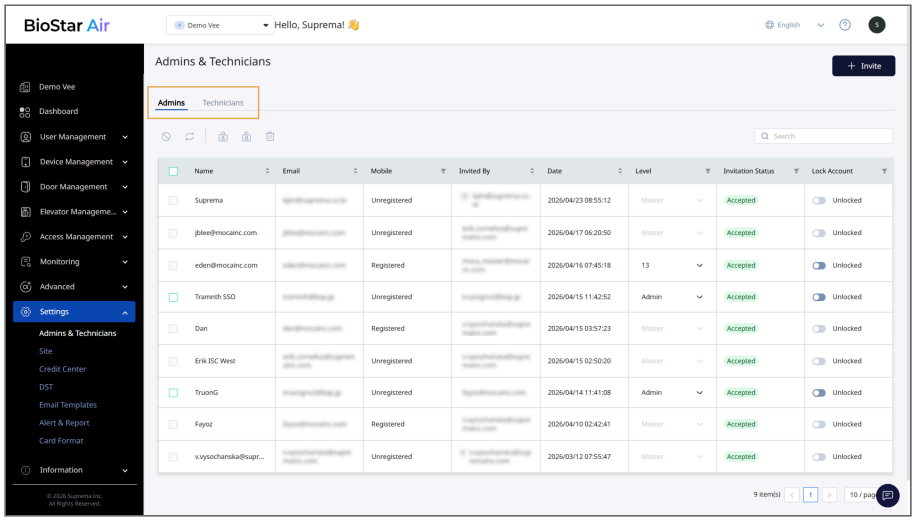
開始する前に

技術者アカウントを管理する前に、サイトのセキュリティ設定で技術者アカウントがサイトにアクセスできるよう許可されているか確認してください。 サイトのセキュリティ設定で技術者アカウントのサイトアクセスが許可されていない場合、技術者アカウントを管理できません。

1. 画面左のサイドバーで **設定** → **サイト** をクリックします。
2. **安全** タブをクリックしてください。
3. **技術者アクセス** オプションを有効にしてください。



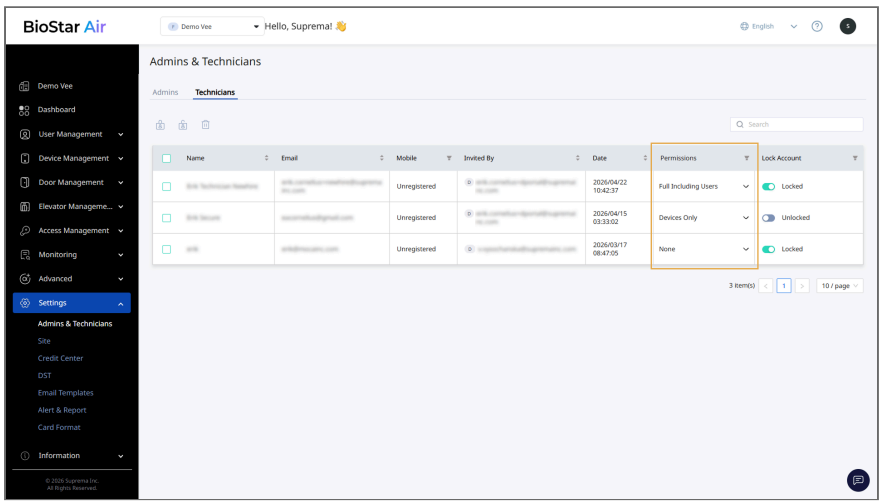
技術者アクセス オプションを有効にすると、**設定** → **アドミン** メニューが **デバイスのみ** メニューに変更されます。 **アドミン** と **技術者** タブに分かれ、管理者アカウントと技術者アカウントをそれぞれ管理できます。



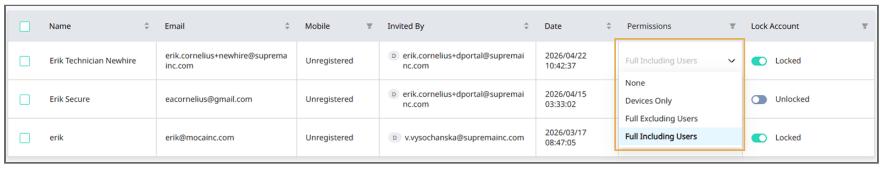
技術者の権限変更

サイトに招待された技術者のアクセス権を変更するには、次の手順に従ってください。

1. 画面左のサイドバーで **設定** → **デバイスのみ** をクリックしてください。
2. **技術者** タブをクリックしてください。
3. 技術者一覧でアクセス権を変更する技術者の **アクセス権限** 列をクリックしてください。



4. アクセス権の選択リストで希望する権限レベルを選択してください。



- ：サイトにログインできません。
- **デバイスのみ**：**ダッシュボード** と **デバイス管理** メニューのみアクセスできます。
- **ユーザーを完全に除外**：**ユーザー管理** メニューを除くすべてのメニューにアクセスできますが、一部の設定機能へのアクセスは制限されます。
- **ユーザーを完全に含む**：**ユーザー管理** メニューを含むすべてのメニューにアクセスできますが、一部の設定機能へのアクセスは制限されます。

5. 変更の確認ダイアログが表示されたら、**はい** ボタンをクリックしてください。

画面上部に成功メッセージが表示され、該当する技術者のアクセス権が変更されます。

> **情報**
> **ユーザーを完全に除外** および **ユーザーを完全に含む** は、次のメニューパスに対して閲覧権限はありますが、編集権限はありません。
>
> - **設定** → **デバイスのみ**
> - **設定** → **サイト**

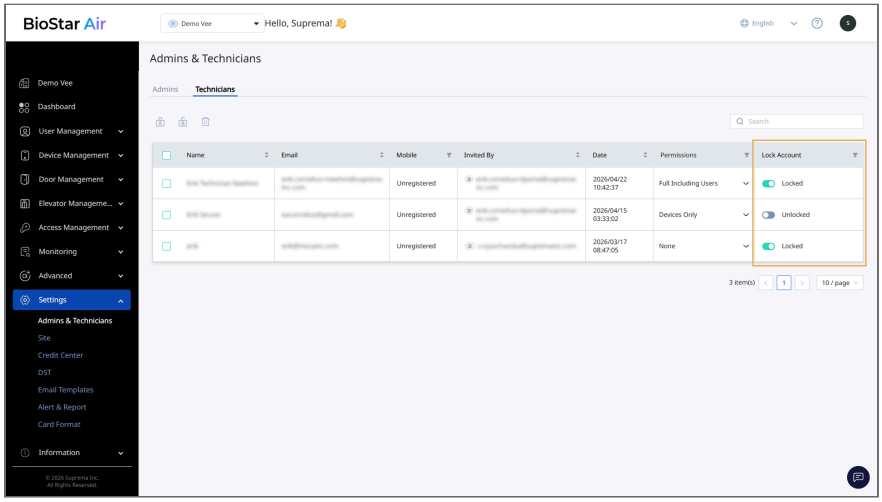
技術者アカウントのロック/解除

技術者のサポートが不要になった場合やセキュリティ上の理由でサイトアクセスを制限する必要がある場合は、技術者のアカウントをロックしてサイトアクセスをブロックできます。 逆に、技術者のサポートが再度必要になった場合は、アカウントのロックを解除してサイトへのアクセスを許可できます。

サイトに招待された技術者のアカウントをロックすると、その技術者はサイトにログインできません。

個別の技術者のロック/解除

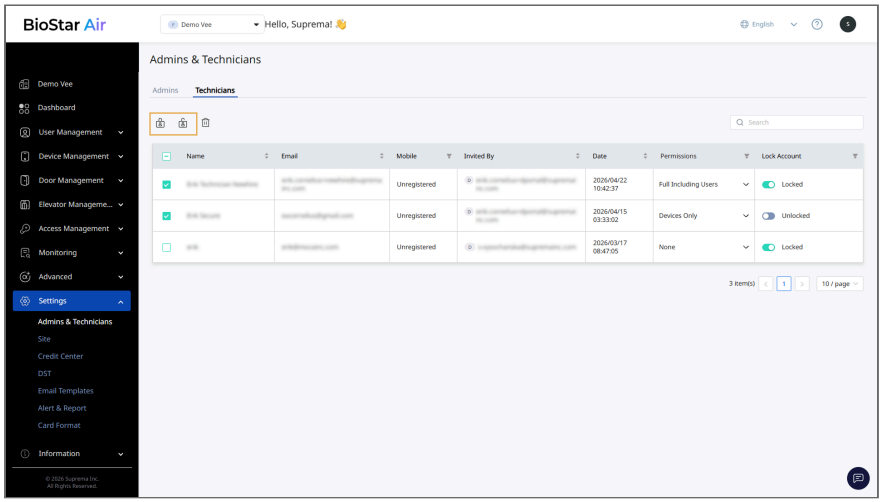
1. 画面左のサイドバーで **設定** → **デバイスのみ** をクリックしてください。
2. **技術者** タブをクリックしてください。
3. 技術者一覧でアカウントをロック/解除する技術者の **アカウントをロック** 列のトグルボタンをクリックしてください。



4. ポップアップメッセージが表示されたら内容を確認し、**はい** ボタンをクリックしてください。

複数の技術者のロック/解除

1. 画面左のサイドバーで **設定** → **デバイスのみ** をクリックしてください。
2. **技術者** タブをクリックしてください。
3. 技術者一覧でアカウントをロック/解除する技術者のチェックボックスをクリックしてください。 1人以上の技術者を選択できます。
4. 技術者一覧上部で または ボタンをクリックしてください。



5. ポップアップメッセージが表示されたら内容を確認し、**はい** ボタンをクリックしてください。

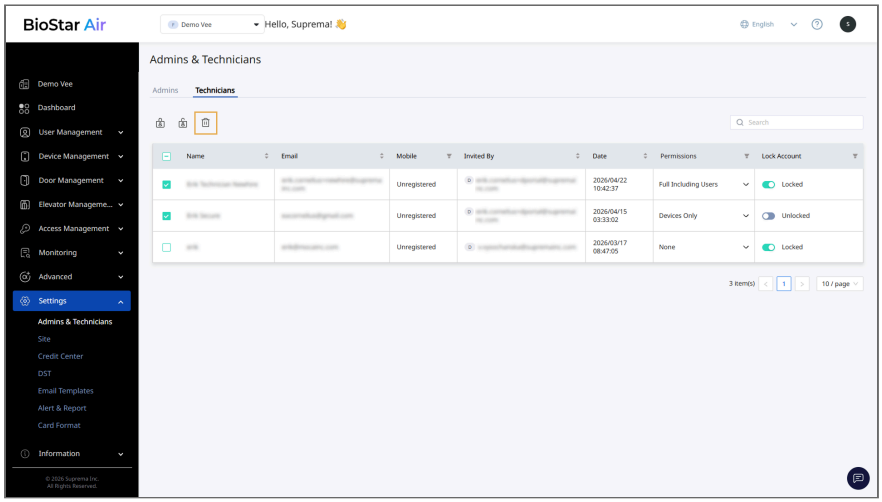
画面上部に成功メッセージが表示され、選択した技術者のアカウントがロックまたは解除されます。

> **情報**
> 一括操作を実行すると、選択したすべての技術者が同じ状態（すべてロック、またはすべて解除）になります。

技術者アカウントの削除

サイトに招待された技術者のアカウントを削除すると、その技術者のサイトアクセス権が完全に削除されます。

1. 画面左のサイドバーで **設定** → **デバイスのみ** をクリックしてください。
2. **技術者** タブをクリックしてください。
3. 技術者一覧でアカウントを削除する技術者のチェックボックスをクリックしてください。 1人以上の技術者を選択できます。
4. 技術者一覧上部の 🗑 ボタンをクリックしてください。



5. ポップアップメッセージが表示されたら内容を確認し、**はい** ボタンをクリックしてください。

画面上部に成功メッセージが表示され、選択した技術者のアカウントが削除され、技術者一覧に表示されなくなります。

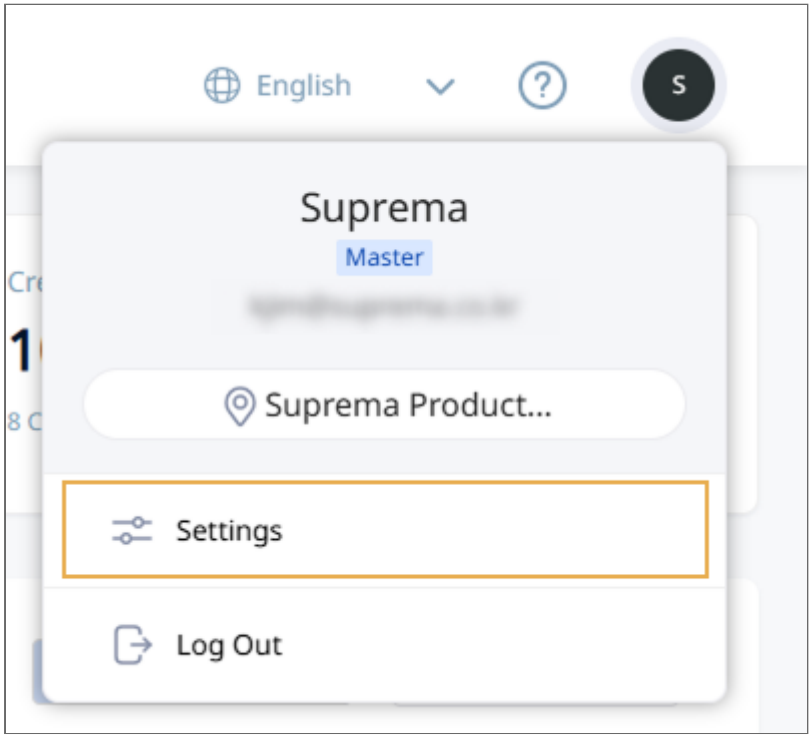
> **情報**
> 技術者アカウントは削除すると復元できません。 サイトから削除した技術者は、パートナーポータルで再度サイトに割り当てることができます。 パートナーポータルで技術者をサイトに割り当てる方法は、サイトに技術者を割り当てるを参照してください。

個人アカウントの設定

パスワードの変更、通知の受信方法の調整、IPインターホンの設定など、アカウントに関する個人設定を自分で管理できます。 サイトを退会したり、アカウントを永久に削除したりすることもできます。

アカウント設定へのアクセス

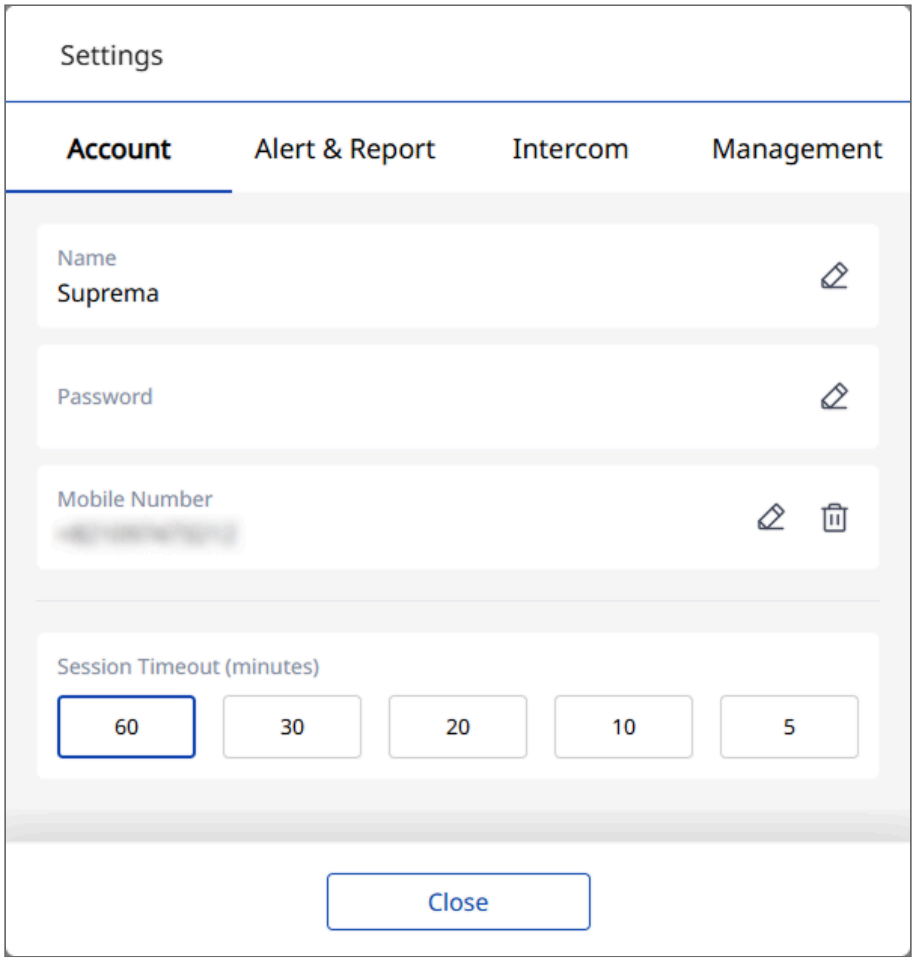
1. BioStar Air ポータルにログインします。
2. 画面右上のユーザープロフィールアイコンをクリックします。
3. ドロップダウンメニューで **設定** をクリックします。



4. **設定** ウィンドウが表示されたら、必要なオプションを設定します。
   - **アカウント**：ユーザー名、パスワード、電話番号などを編集できます。 詳しくはアカウント情報の変更を参照してください。
   - **アラートとレポート**：通知の受信方法を設定できます。 詳しくは通知設定を参照してください。
   - **インターコム**：SIPインターホンの設定情報を管理できます。 詳しくはIPインターホンの設定を参照してください。
   - **管理**：サイトを退会するかアカウントを削除できます。 詳しくは退会またはアカウント削除を参照してください。

アカウント情報の変更

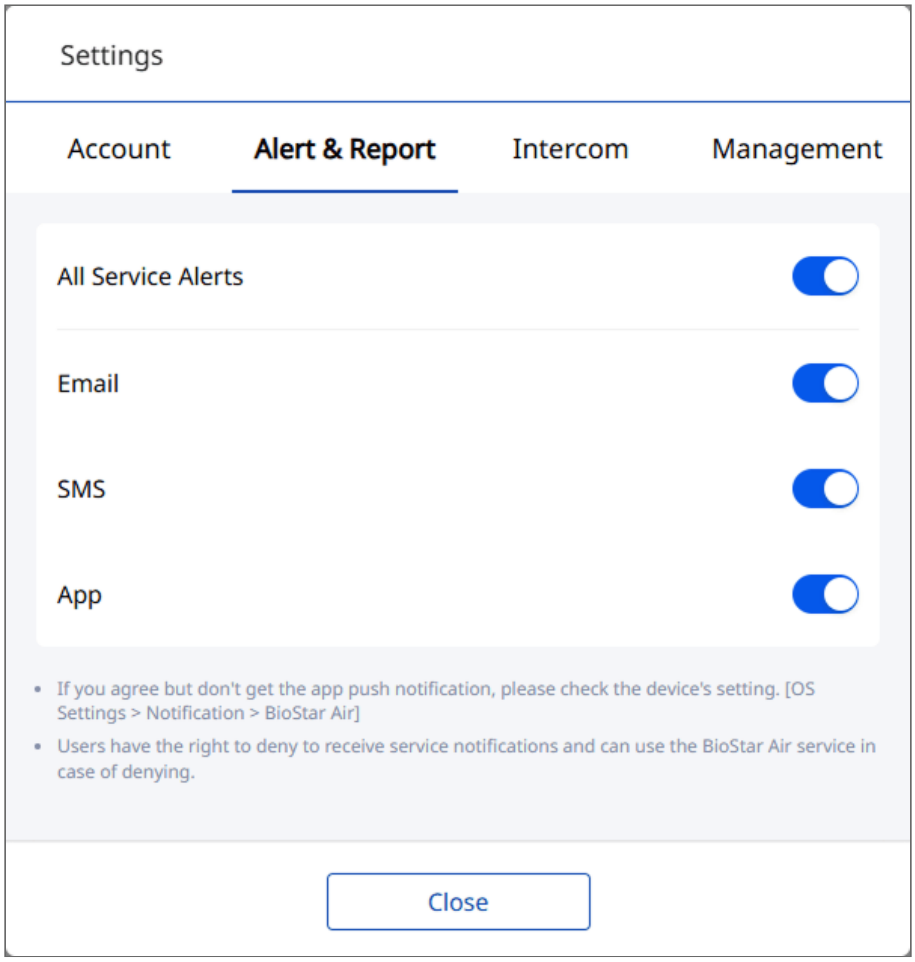
アカウント タブでは、現在ログインしているユーザーの情報を変更できます。



- ユーザーの名前、パスワード、電話番号を変更できます。 各項目の ボタンをクリックします。
- **セッションタイムアウト（分）**：選択した時間が経過すると自動的にログアウトします。 希望の時間を選択します。

通知設定

アラートとレポート：通知の受信方法を設定できます。 すべての通知を受信するには **すべてのサービスアラート** オプションを有効にします。 不要な通知は個別に無効化できます。

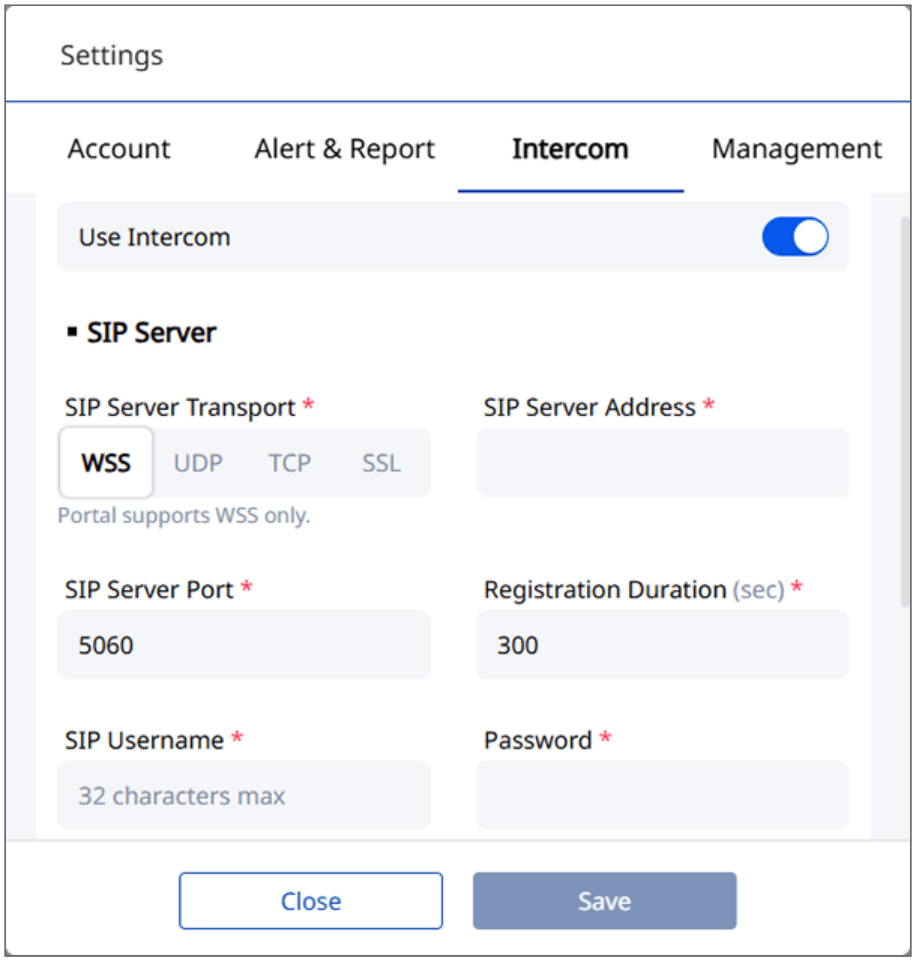


情報

- アプリ通知の受信を許可しているのに通知が届かない場合は、モバイルの設定を確認します。 iOSまたはAndroid端末でアプリ通知を許可する必要があります。
- ユーザーはサービス通知の受信を拒否できます。拒否してもサービスの利用に制限はありません。

IPインターホンの設定

インターコム タブではSIPインターホンの設定情報を管理できます。

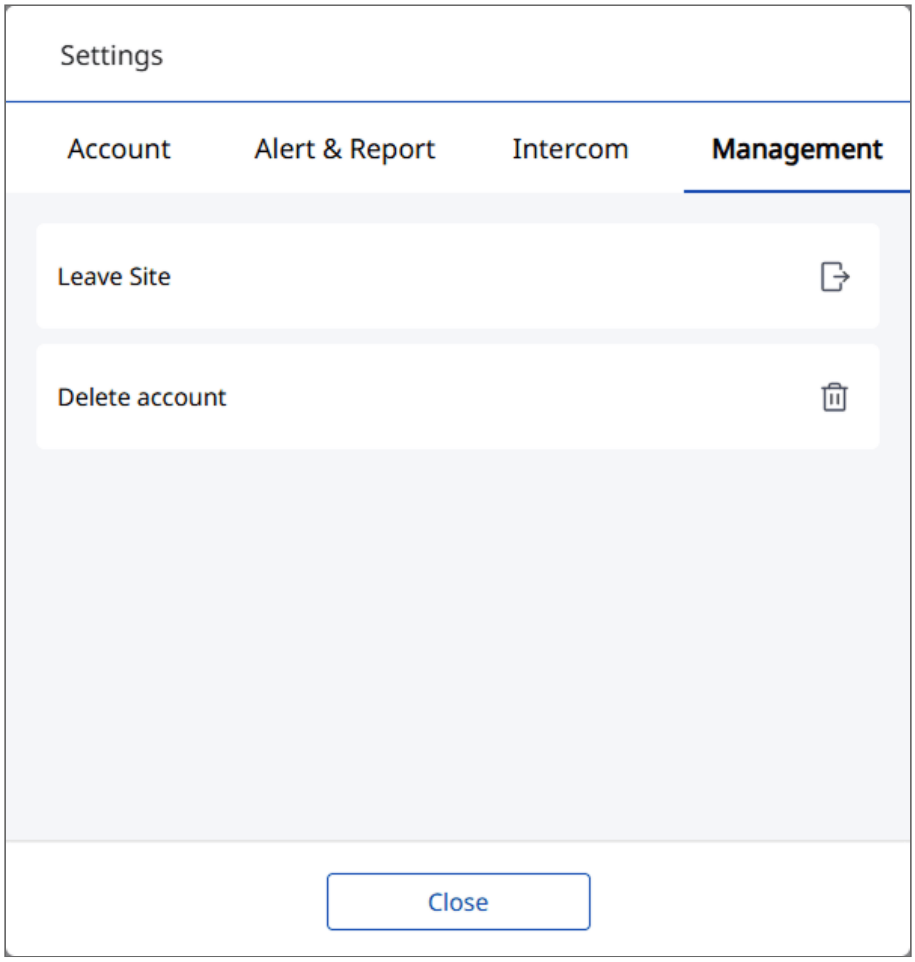


情報

SIPインターホン設定の詳細については[BioStation 3 SIPインターホンの設定]を参照してください。

退会またはアカウント削除

管理 タブではサイトを退会するかアカウントを削除できます。



- **サイトを離れる**：サイトを退会できます。 サイトを退会した後に再度サイトに参加するには、当該サイトの管理者から招待を受ける必要があります。
- **アカウント削除**：アカウントを永久に削除できます。 アカウントを削除すると、すべての個人情報と設定が永久に削除され、復元できません。

SSO & SCIM を設定する

企業規模に関係なく、多くの組織がすでに Microsoft Entra ID または Okta で社内システムのアクセス権限を管理しています。 BioStar Air は、既存の ID プロバイダーと連携し、管理者アカウントとクレデンシャルユーザーを単一のソースで統合管理できるようにします。

SSO（Single Sign-On）を適用すると、組織で使用中の ID ポリシーを BioStar Air 管理者ログインにもそのまま適用して、セキュリティを強化できます。 SCIM（System for Cross-domain Identity Management）でユーザーアカウントの作成と削除を自動化すると、権限を失ったユーザーのアカウントを停止し忘れて発生するセキュリティ事故を減らせます。 これにより、管理者はユーザー、ユーザーグループ、管理者アカウントを個別に作成、修正、削除する反復作業の負担を軽減できます。

画面左のサイドバーで **設定** → **サイト** をクリックします。**SSO & SCIM** タブでログインポリシーとIDプロバイダーを選択し、設定します。 基本設定方法については SSO と SCIM を有効にする をご参照ください。

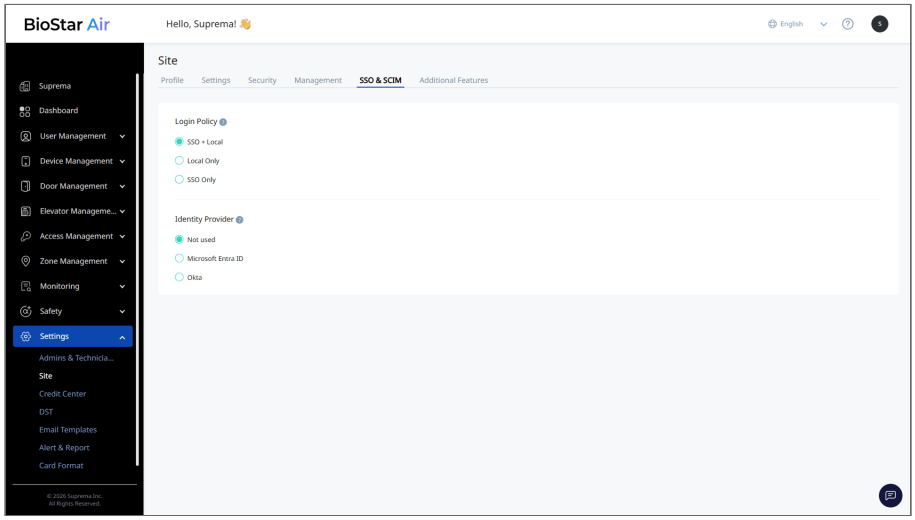
BioStar Airは、**Microsoft Entra ID**または**Okta**を通じたサイト管理者とクレデンシャルユーザーのプロビジョニングをサポートします。 該当するIDプロバイダーを使用する場合は、次のドキュメントを参照し、BioStar AirサイトのSSOとSCIMを設定してください。

最小要件

- BioStar Air SSO & SCIM ライセンス
- Microsoft Entra ID または Okta の有効なサブスクリプション
- IDプロバイダーで新しいアプリケーションを作成できる権限
- IDプロバイダーでグループを作成し、プッシュして割り当てできる権限
- BioStar Air マスター権限

SSO と SCIM を有効にする

画面左のサイドバーで **設定** → **サイト** をクリックします。 **SSO & SCIM** タブでログインポリシーと ID プロバイダーを選択し、設定または解除してください。



注意

IDプロバイダーの設定を変更する前に、ローカルログイン可能なマスター管理者アカウントを少なくとも一つは維持してください。 そうしないと、ID プロバイダー連携に問題が発生した場合、サイトにアクセスできないロック状態になることがあります。

情報

- SSO および SCIM の設定は、サイトのマスター管理者のみが管理できます。
- クレデンシャルユーザーは BioStar Air にログインしないため、SSO および SCIM の設定の影響を受けません。
- パートナーポータルは、SSO および SCIM の設定の適用範囲に含まれません。

ログインポリシー

ログインポリシーでは BioStar Air 管理者のログイン方法を設定できます。

- **SSO**：管理者は ID プロバイダーを通じて認証します。

- **ローカル**：管理者は BioStar Air に設定したメールアドレスとパスワードで認証します。

次の三つのオプションのいずれかを選択してください。

- **SSO + ローカル**：SSO ログインとローカルログインの両方を使用できます。
- **ローカルのみ**：ローカルログインのみ使用できます。
- **SSOのみ**：SSO ログインのみ使用できます。

ID プロバイダー連携の設定

IDプロバイダーでは BioStar Air 管理者アカウントと連携する外部 ID プロバイダーを選択できます。 サイトでは同時に有効化できるIDプロバイダーは一つだけです。

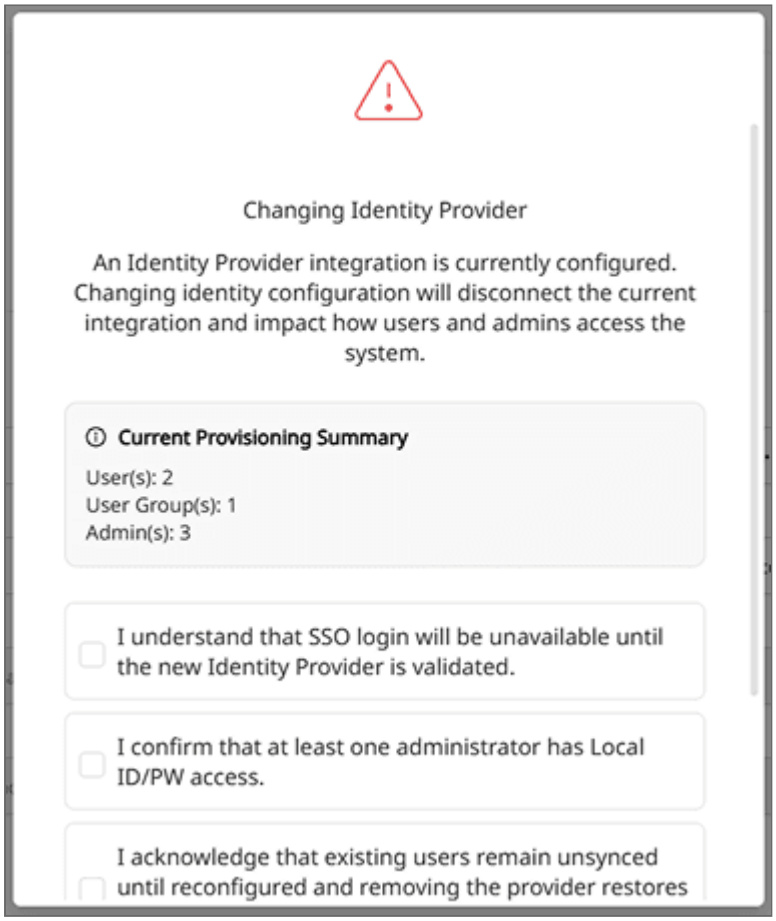
- **使用しない**
- **Microsoft Entra ID**: Microsoft Entra ID 連携を設定する
- **Okta**: Okta連携を設定する

> **情報**
> 接続済みの ID プロバイダーを別のプロバイダーに変更する場合は、先に **使用しない** に設定して既存の接続を解除し、次に新しい ID プロバイダーを選択してください。 接続を解除しないと、別の ID プロバイダーへ直接切り替えられません。

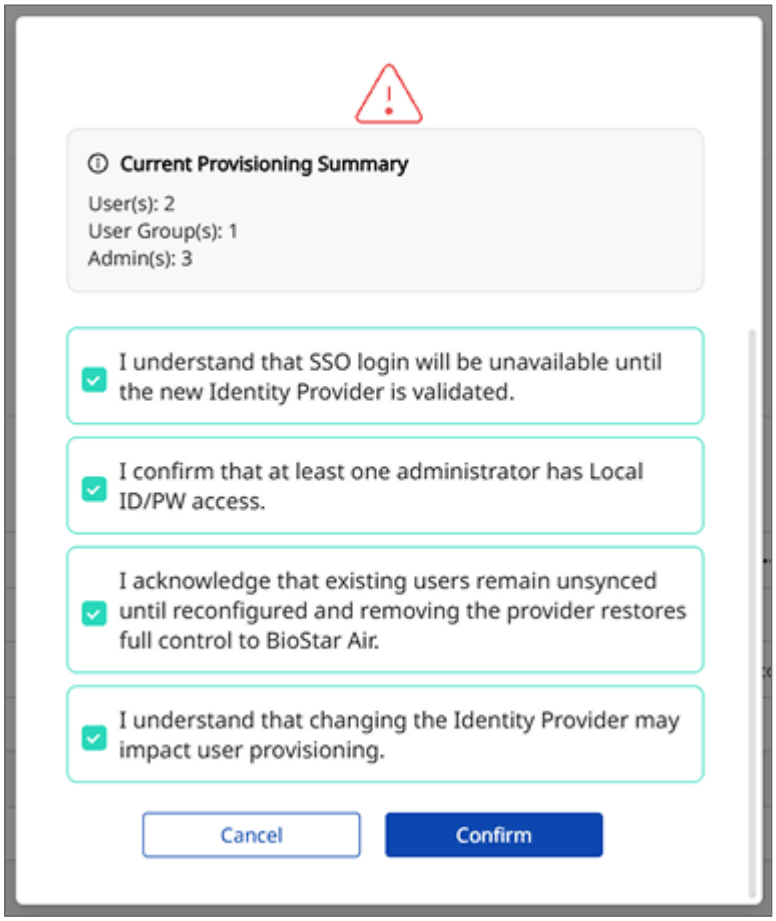
SSO & SCIM 設定の解除

ID プロバイダー連携設定を解除してください。

1. **IDプロバイダー** セクションで **使用しない** を選択してください。
2. 警告ポップアップのメッセージを確認してください。



3. 設定変更による影響範囲を確認し、チェックボックスをクリックしてください。



4. **確認** ボタンをクリックします。

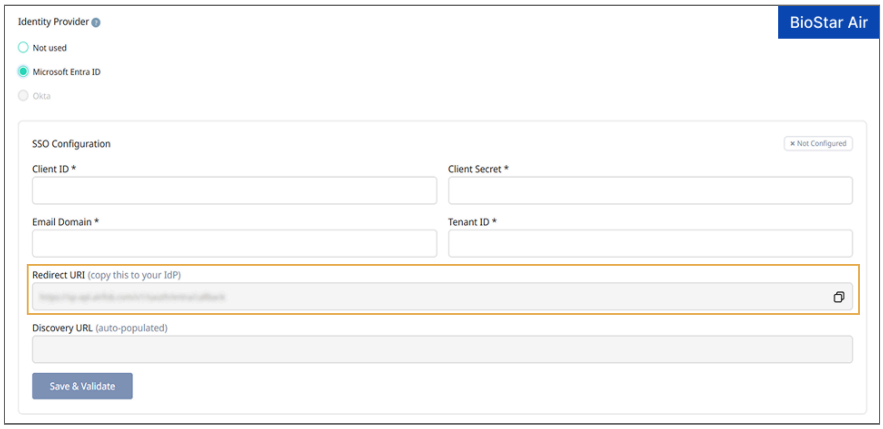
Microsoft Entra ID 連携を設定する

BioStar AirにMicrosoft Entra IDでログインするには、組織のID管理者がEntra IDにアプリを登録し、BioStar AirのSSO設定に接続する必要があります。

Entra ID SSO 接続

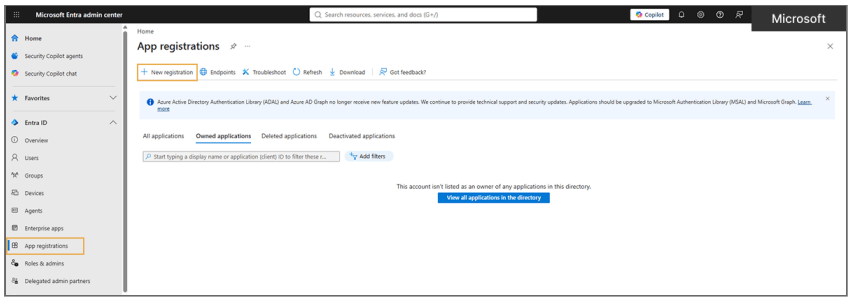
1 BioStar Air: リダイレクト URI の準備

1. BioStar Air 画面左のサイドバーで **設定** → **サイト** をクリックします。
2. **SSO & SCIM** タブをクリックします。
3. **IDプロバイダー** で **Microsoft Entra ID** を選択します。
4. **リダイレクトURI** フィールドに URI が表示されます。その値をコピーします。



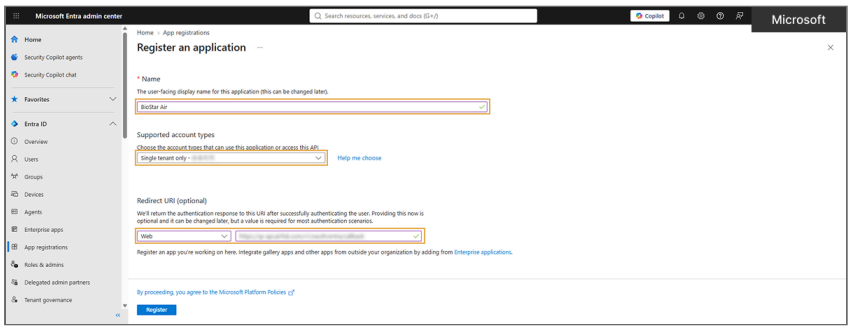
2 Microsoft Entra 管理センター: アプリ登録

1. Microsoft Entra 管理センター にサインインします。
2. **Entra ID** → **App registrations** に移動します。
3. **New registration** ボタンをクリックします。



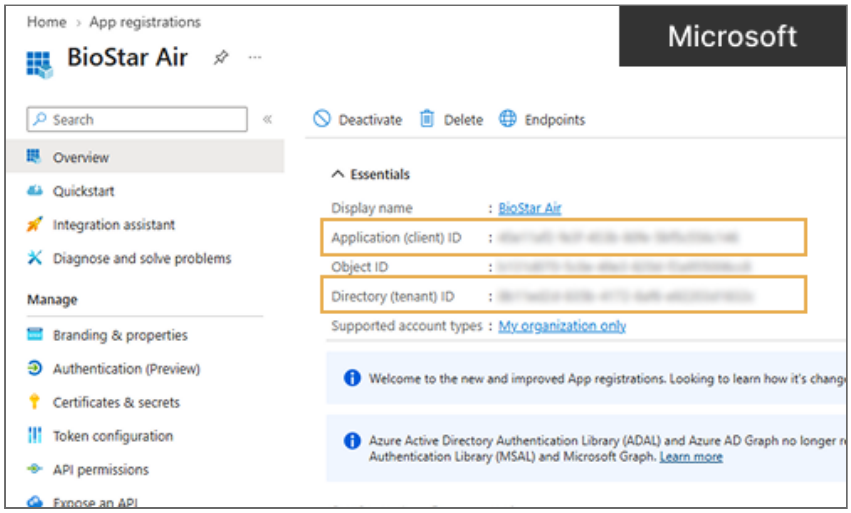
4. アプリ名を「BioStar Air」に入力します。
5. **Supported account types** で **Single tenant only** を選択します。

6. **Redirect URI** セクションで **Web** を選択し、BioStar Air: リダイレクト URI の準備 の手順でコピーした URI を入力欄に貼り付けます。



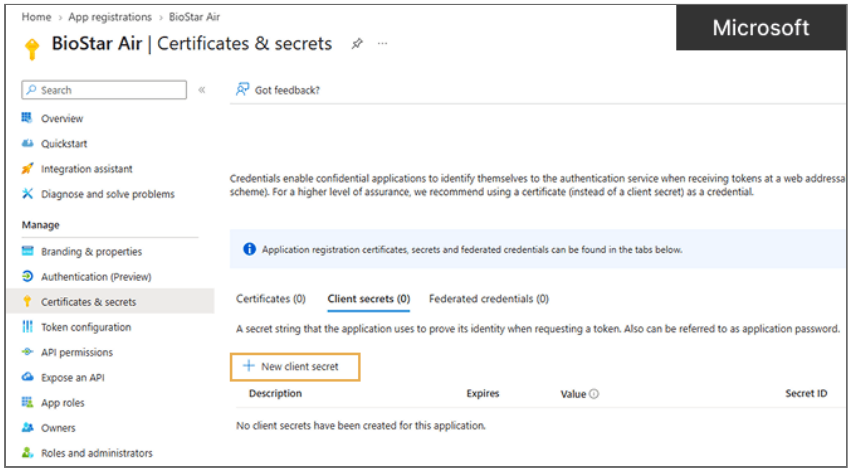
7. **Register** ボタンをクリックします。

8. 登録した BioStar Air アプリの **Overview** で、次の値をコピーします。

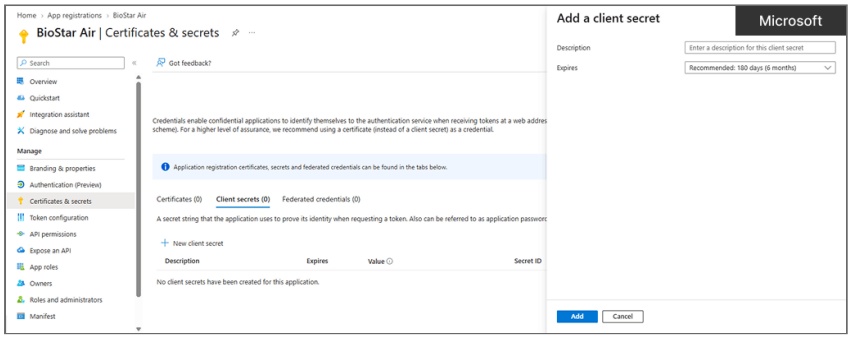


- **Application (client) ID**
- **Directory (tenant) ID**

9. **Certificates & secrets** → **Client secrets** で **New client secret** をクリックします。

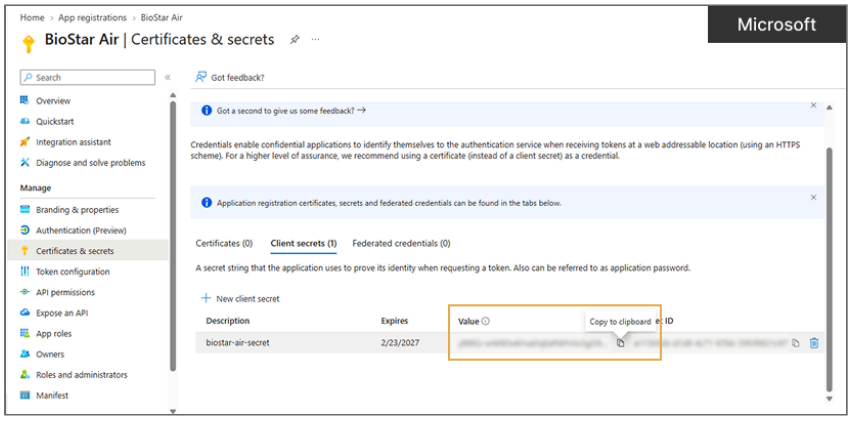


10. 説明を入力し、有効期限を選択します。



11. 「**Add**」ボタンをクリックする。

12. 生成したクライアント シークレットの **Value** をコピーします。



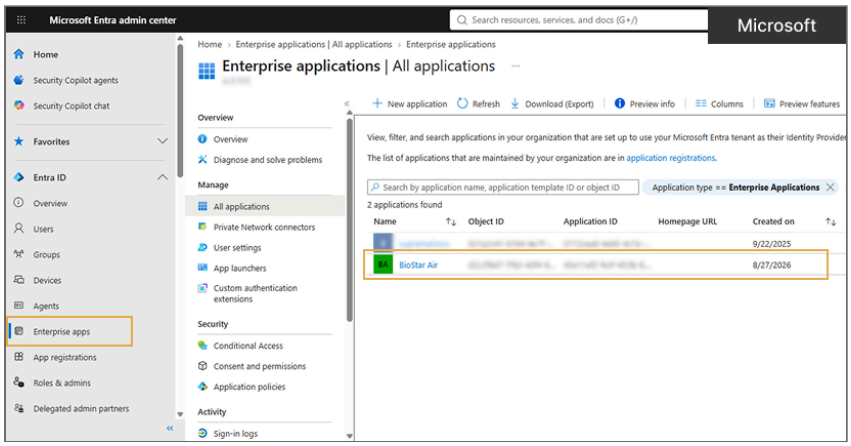
コピーした **Application (client) ID**、**Directory (tenant) ID**、**Value** を次の手順で入力します。

> **注意**
> **Secret ID** ではなく **Value** を使用します。 **Value** はこの後再表示されないため、必ずコピーしてください。

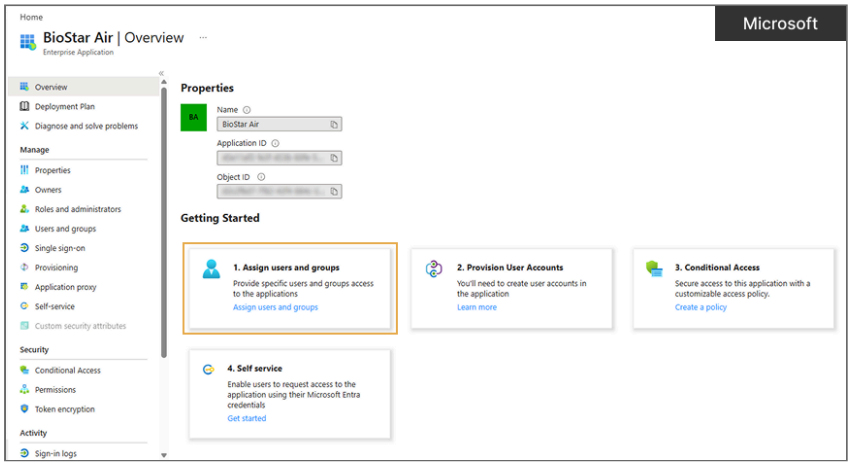
3 Microsoft Entra 管理センター: ユーザーとグループの割り当て

ユーザーとグループを割り当てる前に、ユーザーとグループを先に作成する必要があります。

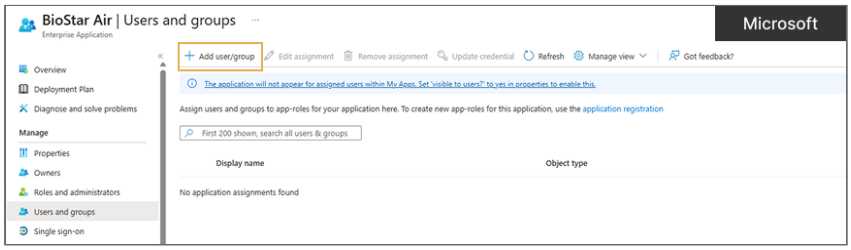
1. **Enterprise apps** で、先ほど作成したアプリ（BioStar Air）をクリックします。



2. **Assign users and groups** をクリックします。



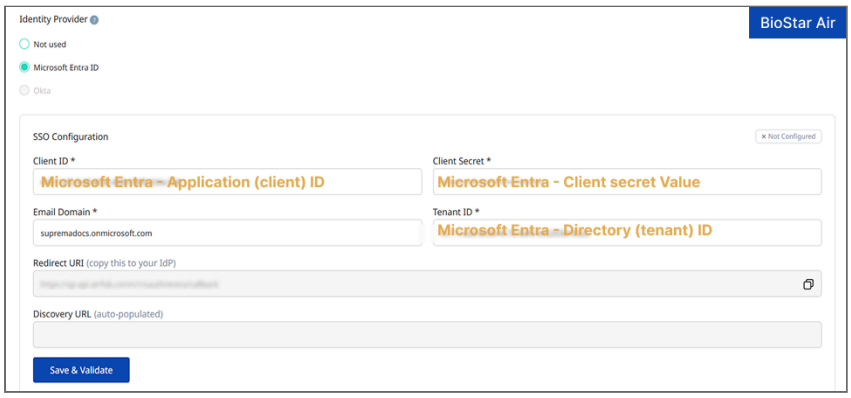
3. ユーザーとグループを割り当てるには、**Add user/group** をクリックします。



4. ユーザーとグループの割り当てが完了したら、**Assign** ボタンをクリックします。

4 BioStar Air：SSO 設定

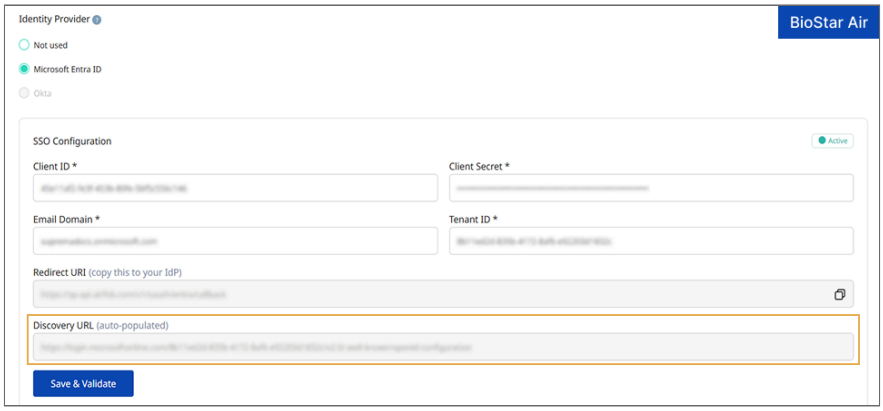
1. BioStar Airの設定画面に戻り、Microsoft Entra 管理センター: アプリ登録 手順でコピーした値を各フィールドに入力します。



- **クライアントID**: Application (client) ID
- **クライアントシークレット**: Value
- **テナントID**: Directory (tenant) ID

2. **メールドメイン** フィールドに、組織のメールドメインを入力します。
3. **保存して検証** ボタンをクリックします。

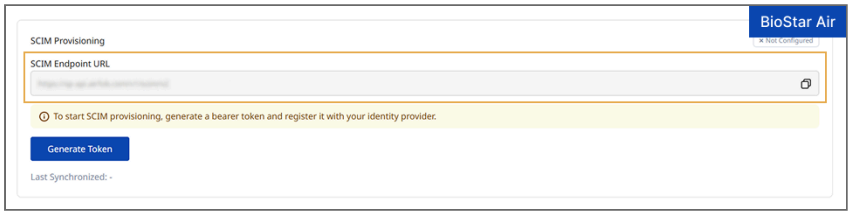
保存と検証に成功すると、システムが **ディスカバリーURL** フィールドの値を自動的に生成します。



Entra ID SCIM プロビジョニング接続

1 BioStar Air: SCIM トークンをコピー

1. BioStar Air 画面左のサイドバーで **設定** → **サイト** をクリックします。
2. **SSO & SCIM** タブをクリックします。
3. **SCIMプロビジョニング** セクションで **SCIMエンドポイントURL** の値をコピーします。

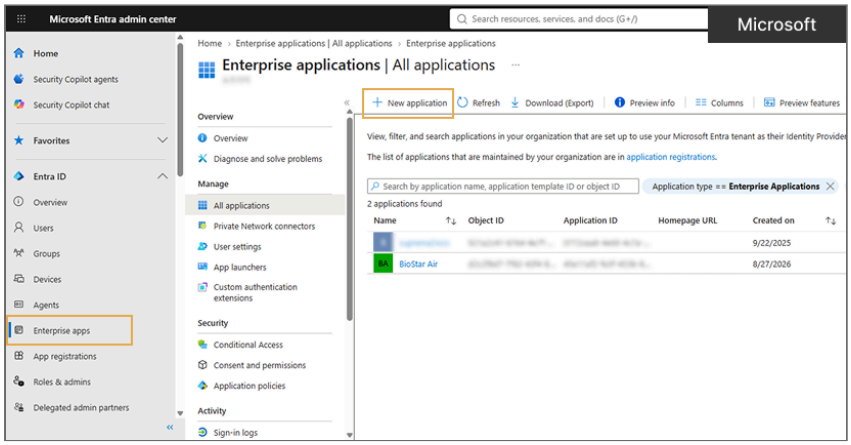


4. **トークン生成** をクリックします。
5. トークン生成完了ダイアログでトークンをコピーします。

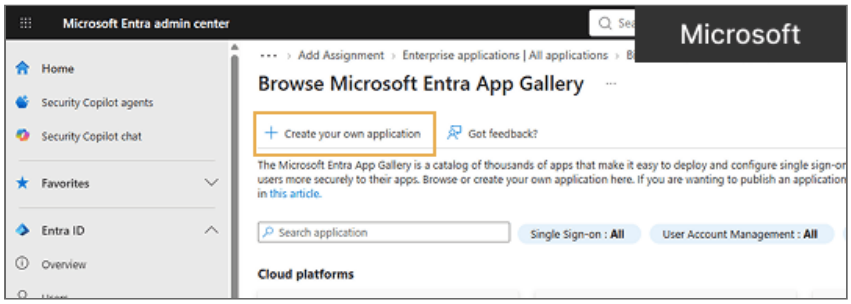
> **情報**
>
> - 生成されたトークンをすぐにコピーします。 トークンは生成時にのみコピーできます。 ダイアログボックスを閉じると、トークンを再度コピーできません。
> - トークンを紛失した場合は、新しいトークンを生成するには **トークン更新** ボタンをクリックします。 新しいトークンを ID プロバイダーに再入力する必要があります。
> - この手順でコピーした SCIM エンドポイント URL とトークンを、次の手順で入力する必要があります。

2 Microsoft Entra 管理センター：SCIM プロビジョニングアプリの作成

1. **Enterprise apps** で **New application** をクリックします。

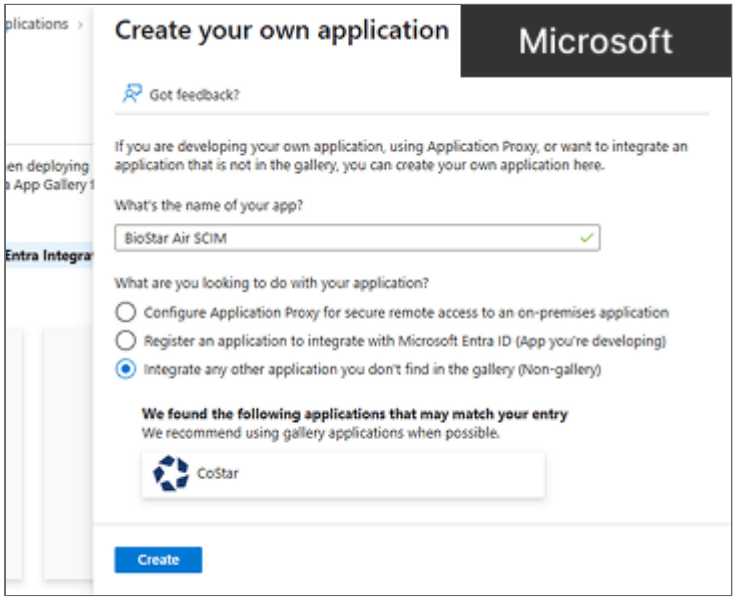


2. **Create your own application** をクリックします。



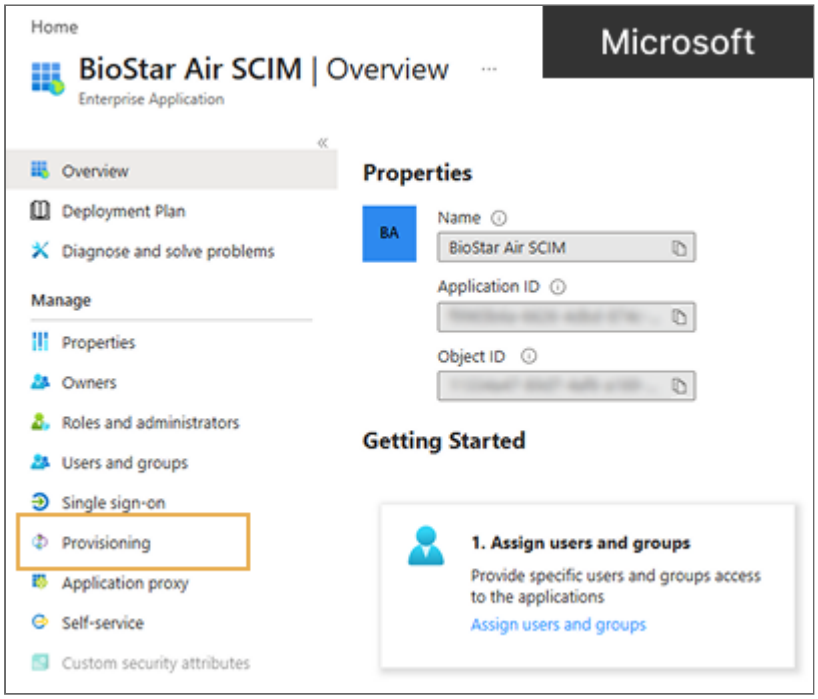
3. アプリ名に「BioStar Air SCIM」を入力します。

4. **Integrate any other application you don't find in the gallery (Non-gallery)** オプションを選択します。



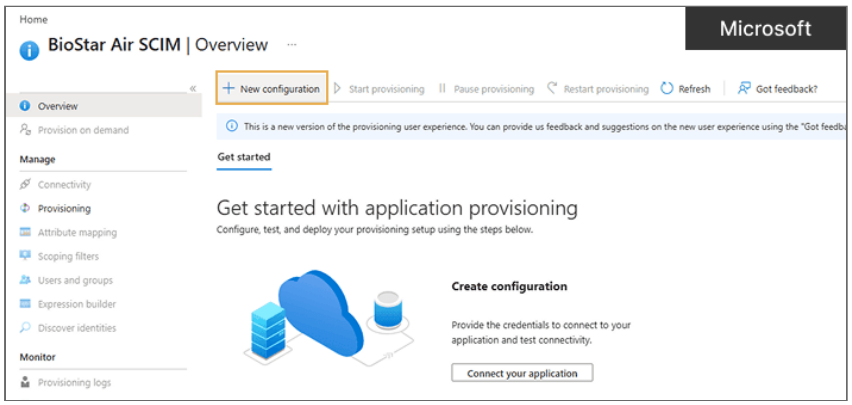
5. **Create** ボタンをクリックします。

6. 作成した BioStar Air SCIM アプリで、**Manage** → **Provisioning** をクリックします。

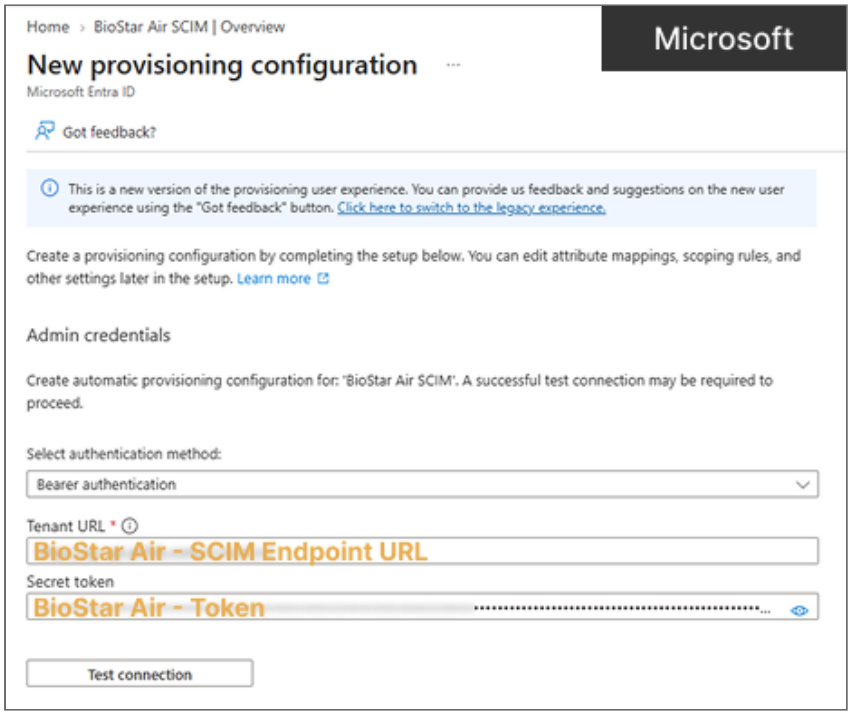


❸ Microsoft Entra 管理センター：管理者資格情報の設定とプロビジョニングの開始

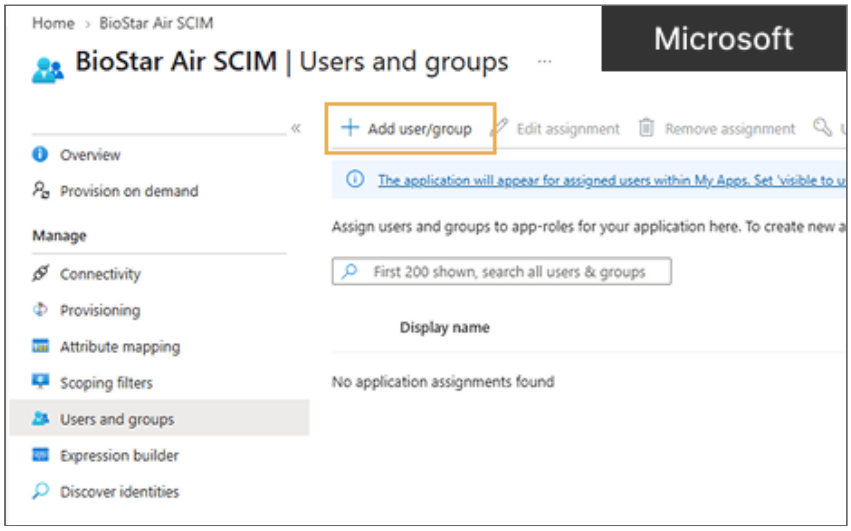
1. **New Configuration** をクリックします。



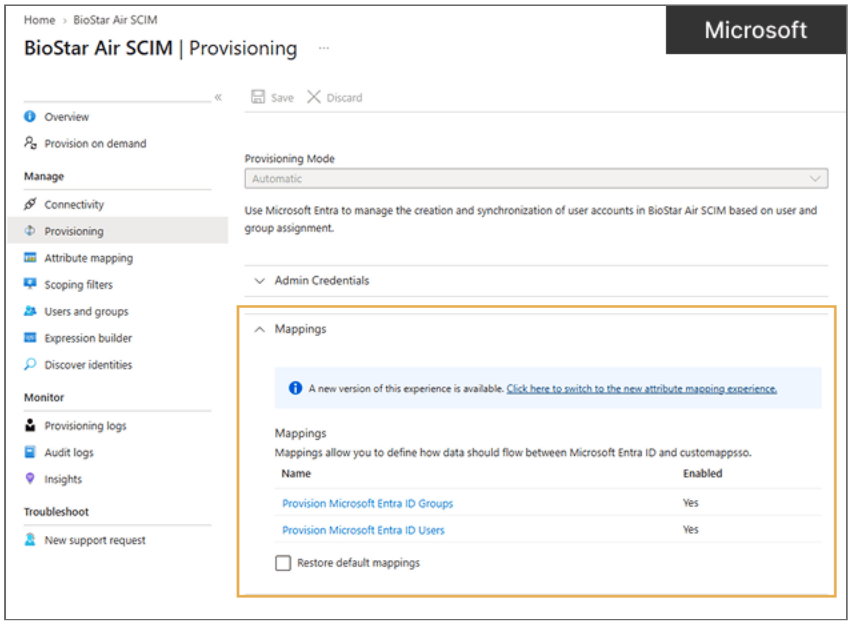
2. BioStar Air: SCIM トークンをコピー 手順でコピーした SCIM エンドポイント URL とトークン値を、**Admin credentials** の **Tenant URL** と **Secret token** フィールドに入力します。



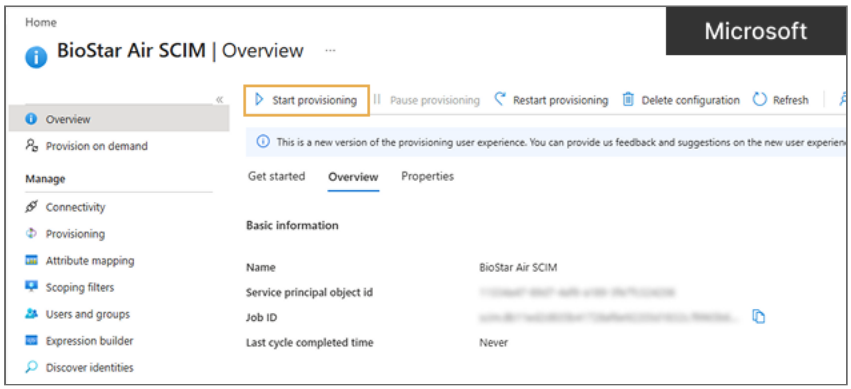
3. 同期が正常に動作するかテストするには、**Test Connection** ボタンをクリックします。
4. **Create** ボタンをクリックします。
5. **Users and groups** で **Add user/group** をクリックします。



6. プロビジョニングするユーザーとセキュリティグループを割り当てます。
7. **Assign** ボタンをクリックします。
8. **Provisioning** → **Mappings** に移動し、ユーザーとグループの同期が有効になっているか確認します。



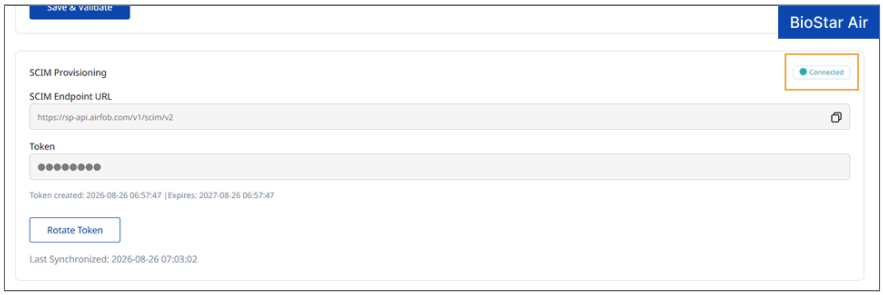
9. 属性マッピングを変更する前に、マッピング内容を確認します。
10. SCIM アプリの **Overview** で **Start provisioning** をクリックします。



> **情報**
> 小規模なテストグループから先に開始することを推奨します。 グループメンバーシップの変更がBioStar Airに反映されるまで、最大約40分かかる場合があります。

4 BioStar Air: 接続の確認

1. BioStar Air 画面左のサイドバーで **設定** → **サイト** をクリックします。
2. **SSO & SCIM** タブをクリックします。
3. **SCIMプロビジョニング** セクションで **接続済み** の表示を確認します。



グループマッピング

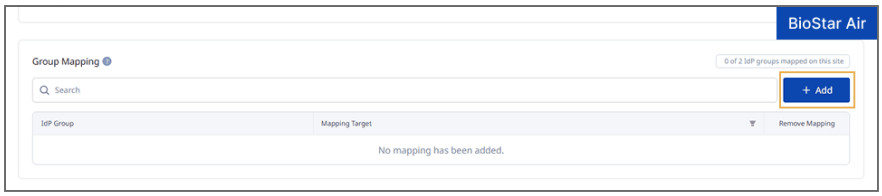
SSO と SCIM の接続を完了し、ID プロバイダーのグループを BioStar Air にプッシュした場合、サイト管理者はプッシュされたグループを BioStar Air のグループにマッピングする必要があります。

マッピングルール

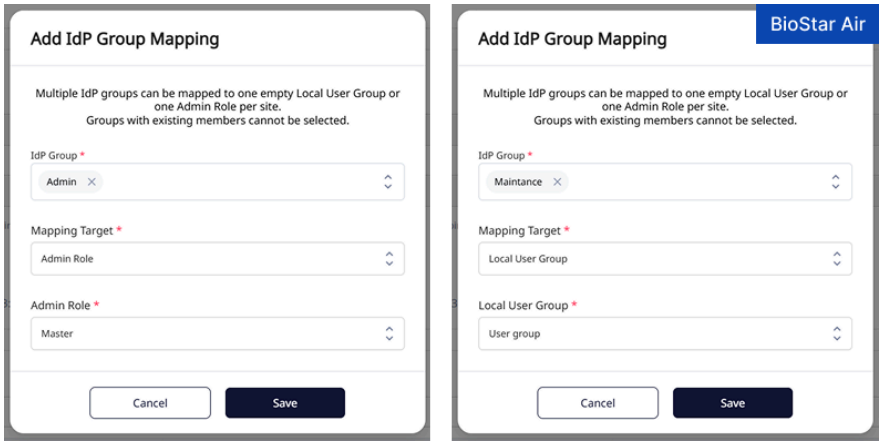
- 一つの BioStar Air ユーザーグループに複数の ID プロバイダーグループをマッピングできます。
- BioStar Air ユーザーグループは、マッピングする前に空である必要があります。
- すでにメンバーがいる BioStar Air グループは、マッピング先として選択できません。
- ID プロバイダーグループのマッピングは、サイトマスター管理者のみ管理できます。
- ID プロバイダーグループをマスターロールにマッピングすると、その後ロールを変更できません。

管理者/ユーザーグループをマッピングする

1. BioStar Air 画面左のサイドバーで **設定** → **サイト** をクリックします。
2. **SSO & SCIM** タブをクリックします。
3. **グループマッピング** セクションに移動し、**追加** ボタンをクリックします。

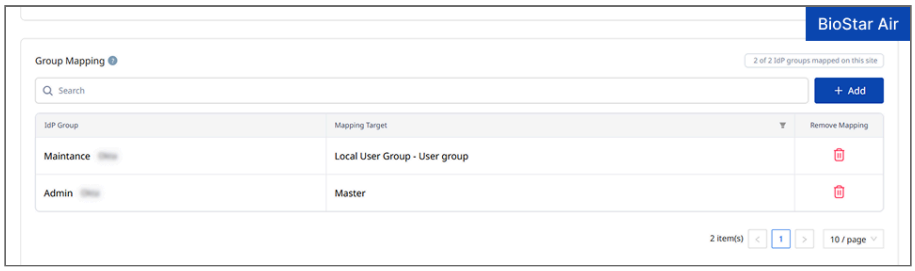


4. **IdPグループ** で ID プロバイダーグループを選択します。
5. **マッピング先** で、選択した IdP グループに応じて **管理者ロール** または **ローカルユーザーグループ** を選択します。
6. マッピング先に応じて、管理者ロールを指定するか、ユーザーグループを選択します。



7. マッピングを保存するには、**保存** ボタンをクリックします。

グループマッピング セクションで、ID プロバイダーグループとマッピングされた BioStar Air グループを確認できます。

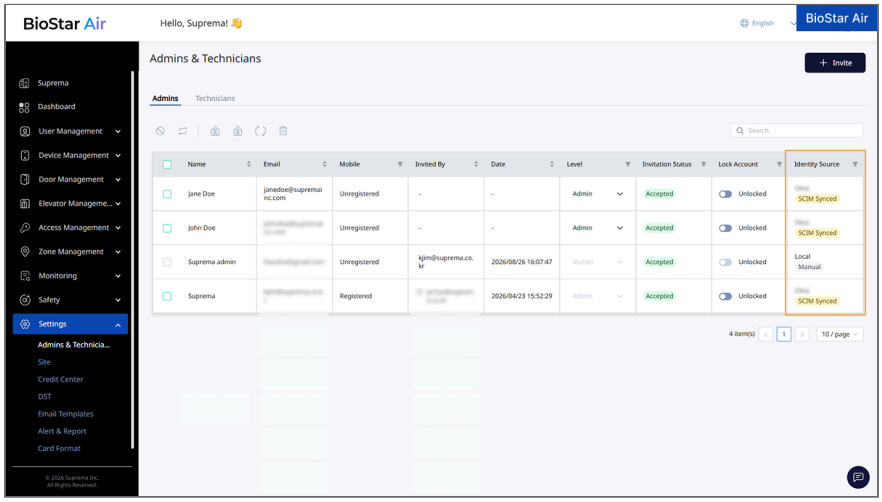


> **情報**
>
> - 管理者ロールの詳細については 管理者アカウントおよび役割の管理 をご覧ください。
> - ユーザーグループの詳細は ユーザーグループを管理する を参照してください。

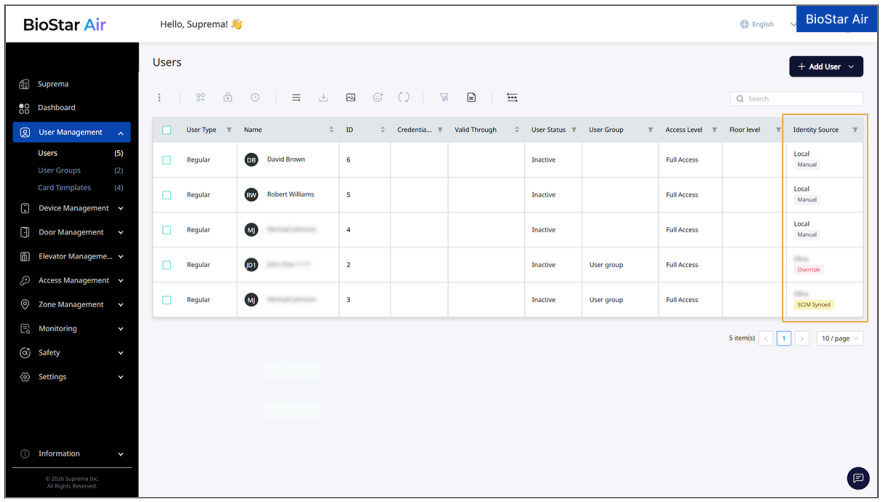
同期された管理者/ユーザー/グループの管理

プロビジョニングを有効にすると、BioStar Airは各管理者、ユーザー、ユーザーグループがローカルで直接管理されているか、ID プロバイダーから同期されているかを画面に表示します。

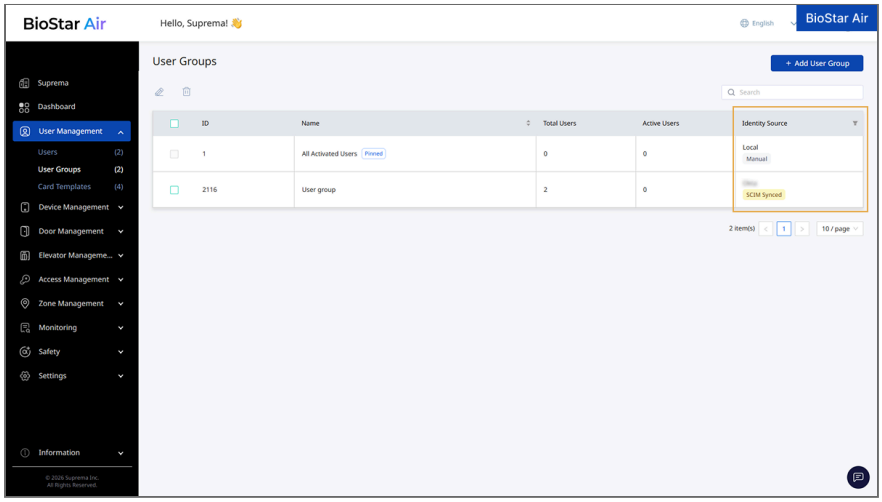
- **設定** → **デバイスのみ** メニューの管理者リストで、**IDソース** 列を確認してください。



- **ユーザー管理** → **ユーザー** メニューのユーザーリストで、**IDソース** 列を確認してください。

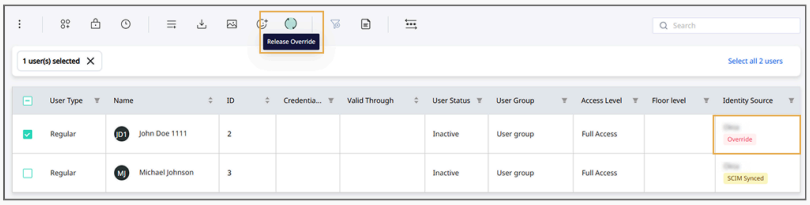


- **ユーザー管理** → **ユーザーグループ** メニューのユーザーグループリストで、**IDソース** 列を確認してください。



SCIM同期項目の動作の仕組み

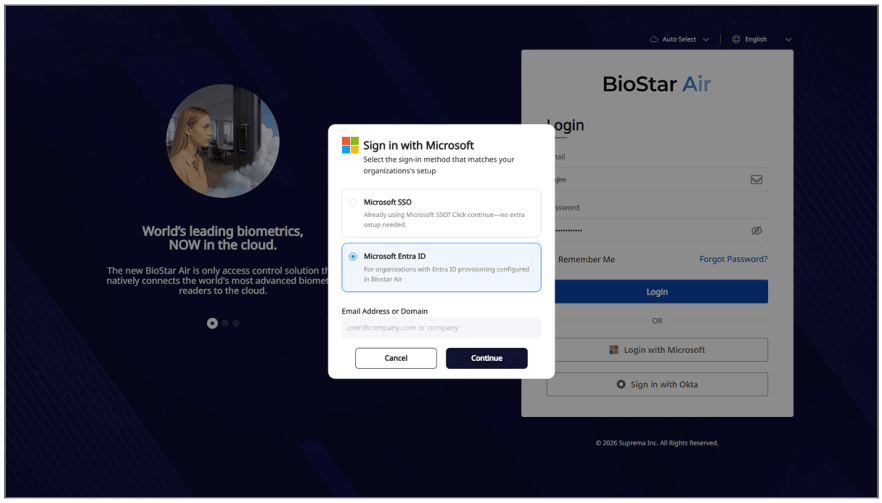
- 既存の手動で作成したユーザーと管理者は、引き続き手動管理のままです。
- SCIMで同期された項目は、BioStar Airで手動で削除できません。
- SCIMで同期されたグループでは、ユーザーを手動で追加または削除できません。
- 同期された項目をローカルで手動で変更すると、**オーバーライド** 状態になります。 **オーバーライド解除** を実行すると、ローカルの変更が取り消され、項目が再びSCIM管理状態に戻ります。



Entra IDでログイン

Entra ID SSO接続を完了すると、ユーザーはBioStar Airのログイン画面でMicrosoftアカウントでログインできるようになります。

1. BioStar Airのログイン画面で **Microsoftでログイン** ボタンをクリックします。
2. **Microsoft Entra ID** を選択します。



> すでにMicrosoft SSOを使用している組織は、**Microsoft SSO** を選択すると、追加の設定なしでログインできます。

3. **メールアドレスまたはドメイン** フィールドに組織のメールアドレスまたはドメインを入力します。（例: `user@company.com` または `company`）
4. **続行** ボタンをクリックします。
5. Microsoft Entra IDのログイン画面に移動したら、組織アカウントのメールアドレスとパスワードを入力します。
6. 認証を完了すると、BioStar Airに自動的にリダイレクトされ、ログインが完了します。

> **情報**
> 入力したメールドメインに対してEntra ID SSOが設定されていない場合、エラーメッセージが表示されます。 この場合は、サイト管理者に問い合わせてください。

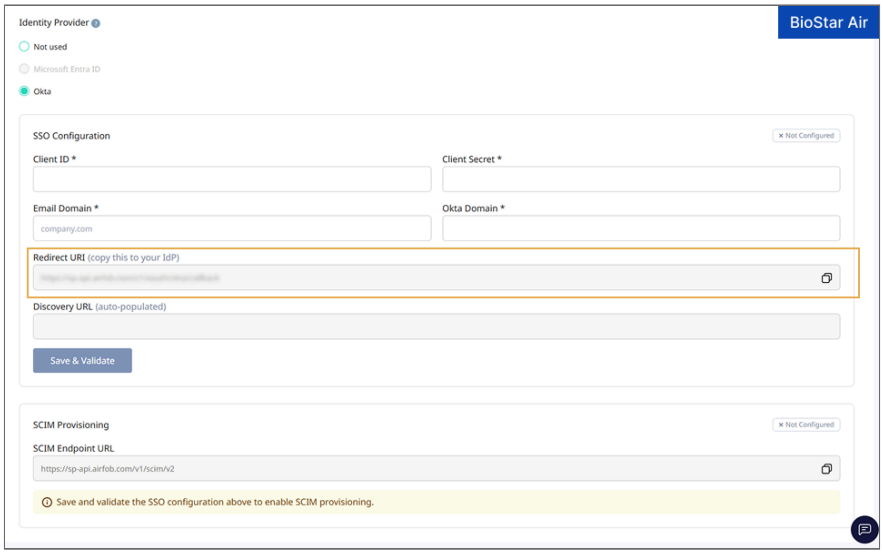
Oktaを連携を設定する

BioStar Air に Okta でログインするには、組織の ID 管理者が Okta で OIDC アプリケーションを作成し、BioStar Air の SSO 設定と連携する必要があります。

Okta SSO連携

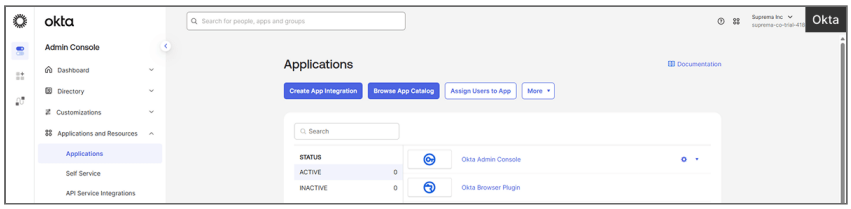
1 BioStar Air: リダイレクト URI の準備

1. BioStar Air 画面左のサイドバーで **設定** → **サイト** をクリックします。
2. **SSO & SCIM** タブをクリックします。
3. **IDプロバイダー** で **Okta** を選択します。
4. **リダイレクトURI** フィールドに URI が表示されます。その値をコピーします。

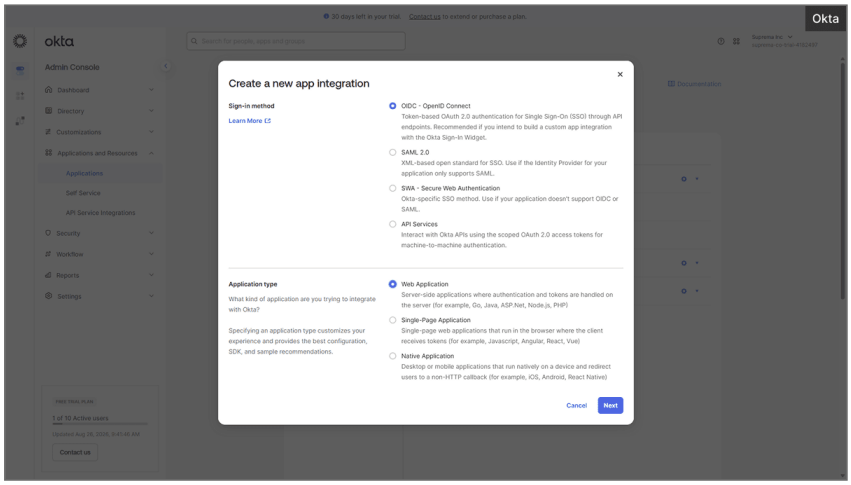


2 Okta：アプリを作成する

1. **Okta管理者コンソール**にログインします。
2. **Applications and Resources** → **Applications** メニューに移動します。

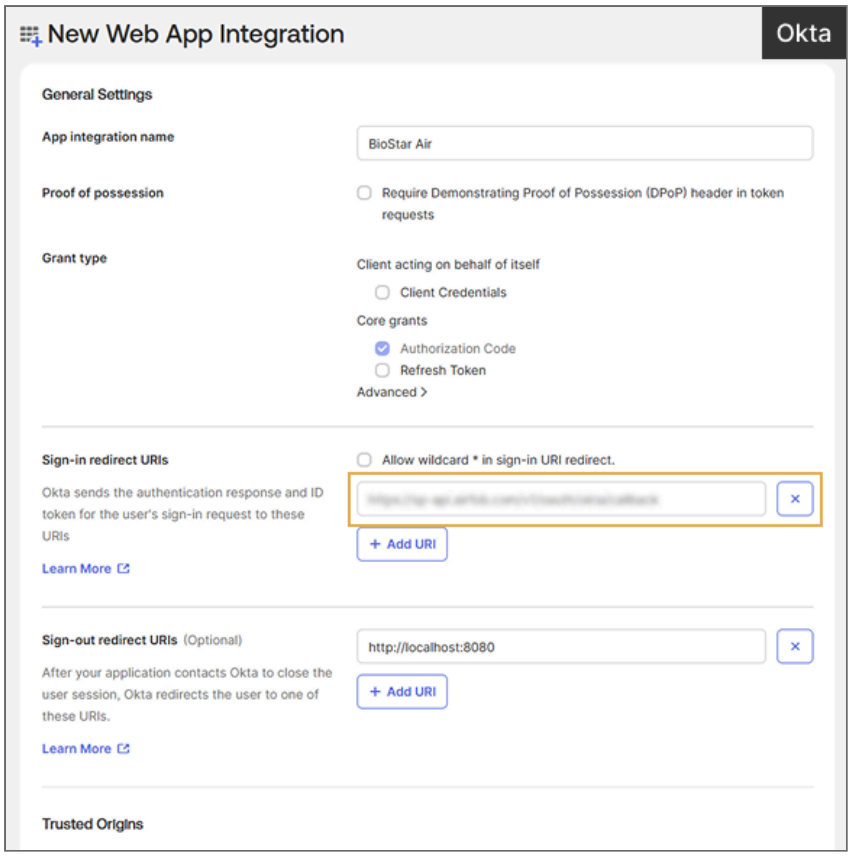


3. **Create App Integration** ボタンをクリックします。
4. **Sign-in method** で **OIDC - OpenID Connect** を選択します。
5. **Application type** でクライアントシークレット（Client secret）を発行できるように、**Web Application** を選択します。

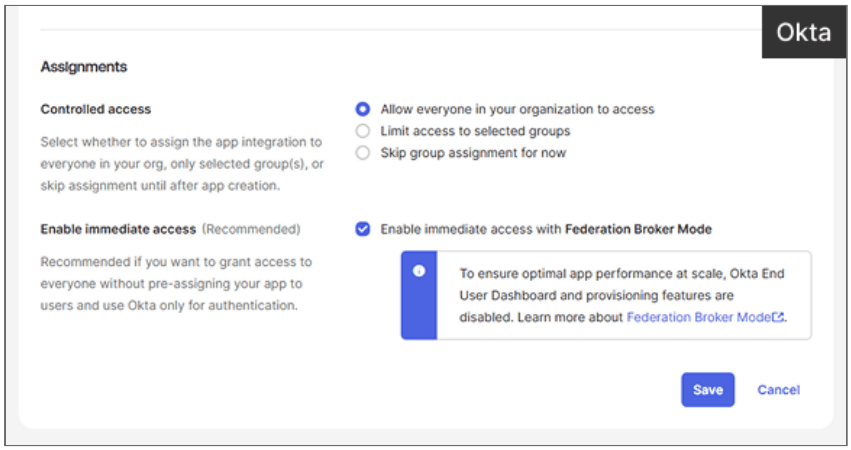


6. **Next** ボタンをクリックします。
7. **App Integration name** フィールドに「BioStar Air」を入力します。
8. BioStar Air: リダイレクト URI の準備 の手順でコピーしたURI値を、**Sign-in redirect URIs** セクションの入力フィールド

に貼り付けます。



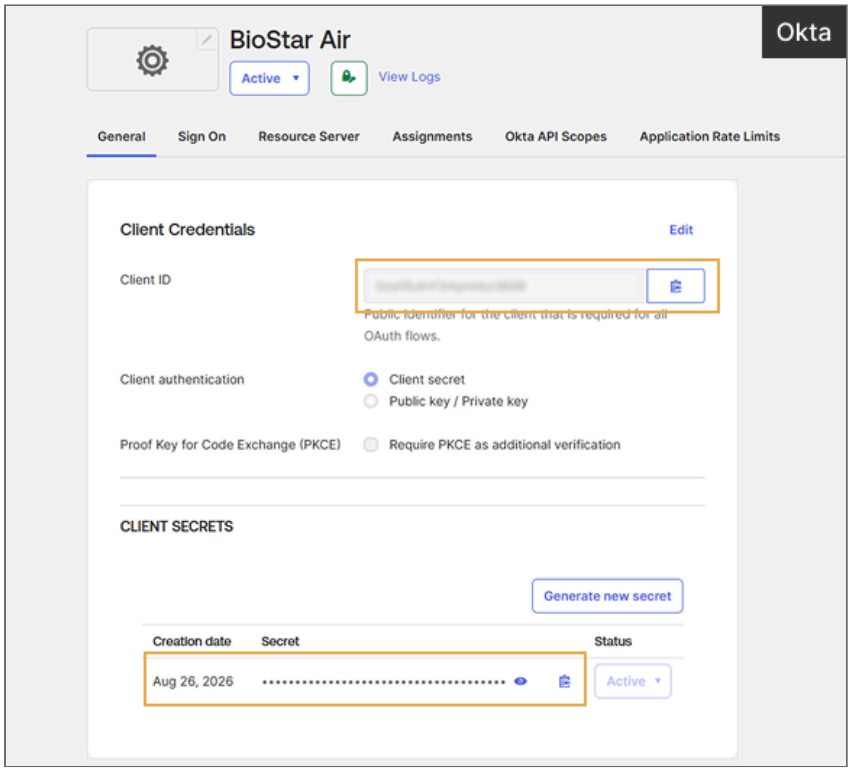
9. **Assignments** セクションに移動し、組織内のユーザーがアプリケーションにアクセスできるように **Allow everyone in your organization to access** を選択します。



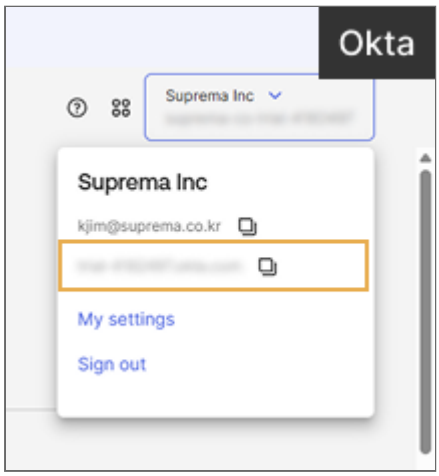
10. **Save** をクリックします。

3 Okta：アプリのクライアント情報をコピーする

1. アプリケーションを作成したら、**General** タブで **Client ID** と **Client Secret** をコピーします。



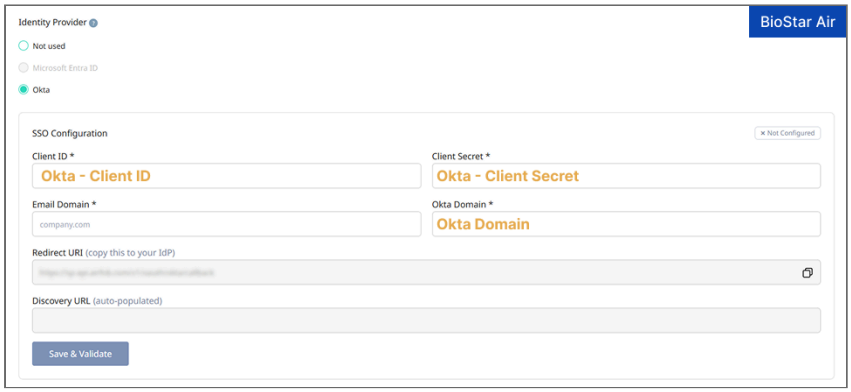
2. 画面右上のプロフィールをクリックし、**Okta Domain** をコピーします。



コピーした **Client ID**、**Client Secret**、**Okta Domain** の値を次の手順で入力します。

4 BioStar Air：SSO 設定

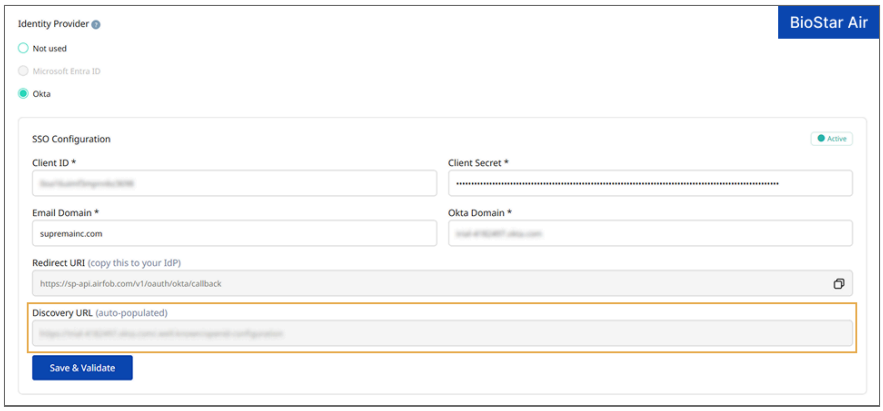
1. BioStar Airの設定画面に戻り、Okta：アプリのクライアント情報をコピーする の手順でコピーした値を各フィールドに入力します。



- **クライアントID**: Client ID
- **クライアントシークレット**: Client Secret
- **Oktaドメイン**: Okta Domain

2. **メールドメイン** フィールドに、組織のメールドメインを入力します。
3. **保存して検証** ボタンをクリックします。

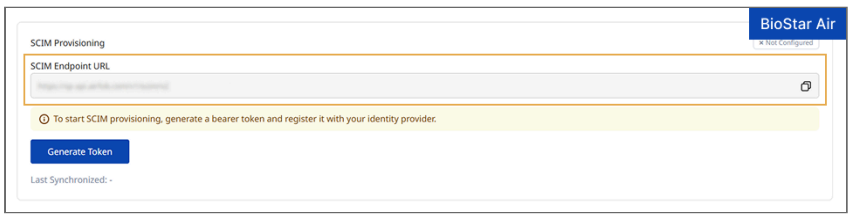
保存と検証に成功すると、システムが **ディスカバリーURL** フィールドの値を自動的に生成します。



Okta SCIMプロビジョニング連携

1 BioStar Air: SCIM トークンをコピー

1. BioStar Air 画面左のサイドバーで **設定** → **サイト** をクリックします。
2. **SSO & SCIM** タブをクリックします。
3. **SCIMプロビジョニング** セクションで **SCIMエンドポイントURL** の値をコピーします。



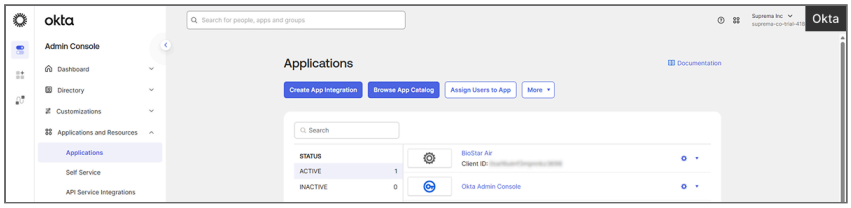
4. **トークン生成** をクリックします。

5. トークン生成完了ダイアログでトークンをコピーします。

> **情報**
>
> - 生成されたトークンをすぐにコピーします。 トークンは生成時にのみコピーできます。 ダイアログボックスを閉じると、トークンを再度コピーできません。
> - トークンを紛失した場合は、新しいトークンを生成するには **トークン更新** ボタンをクリックします。 新しいトークンを ID プロバイダーに再入力する必要があります。
> - この手順でコピーした SCIM エンドポイント URL とトークンを、次の手順で入力する必要があります。

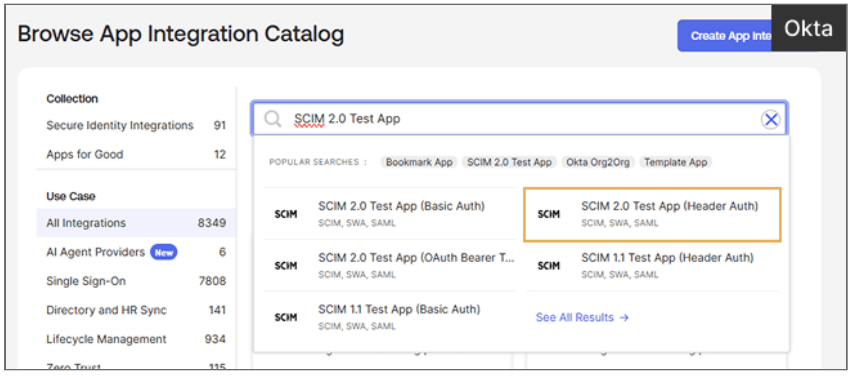
2 Okta：SCIMプロビジョニングアプリを作成する

1. **Okta管理者コンソールで Applications and Resources → Applications** メニューに移動します。



2. **Browse App Catalog** ボタンをクリックします。

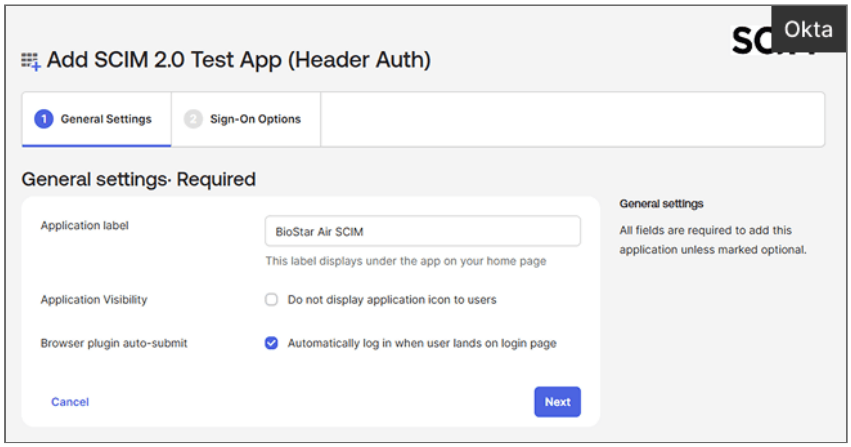
3. 「SCIM 2.0 Test App」を検索します。



4. 検索結果で**SCIM 2.0 Test App (Header Auth)**を選択してください。

5. **Add Integration**ボタンをクリックしてください。

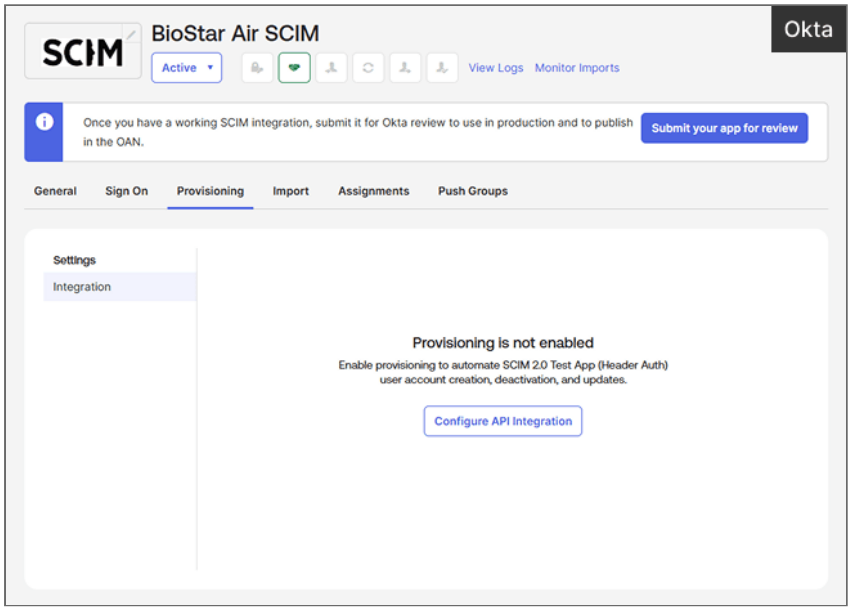
6. **Application label**入力フィールドに「BioStar Air SCIM」と入力してください。



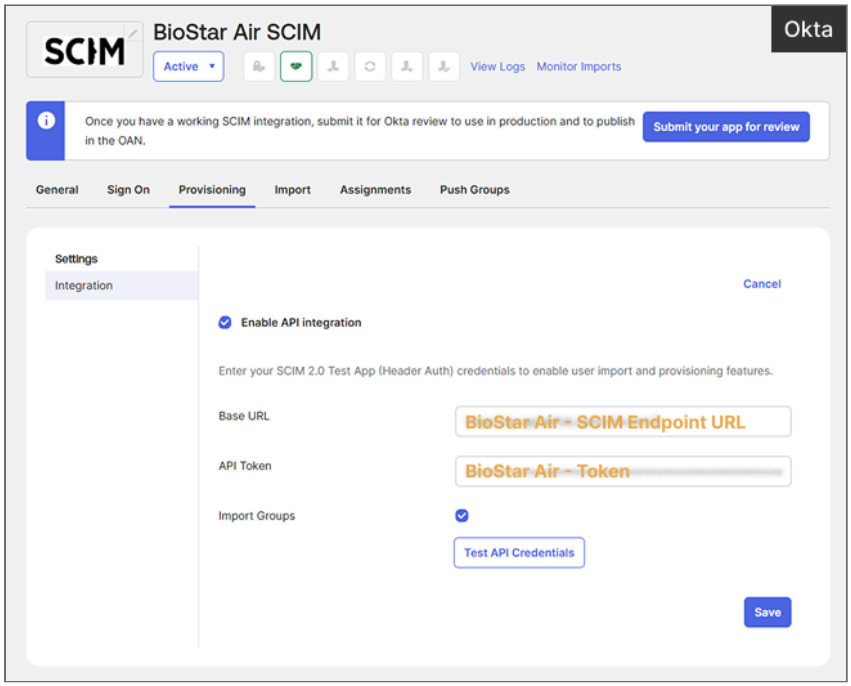
7. **Next** ボタンをクリックします。
8. **Sign-on options**ステップでは、設定を変更せずに下へスクロールし、**Done**ボタンをクリックしてください。

❸ Okta: API統合の設定

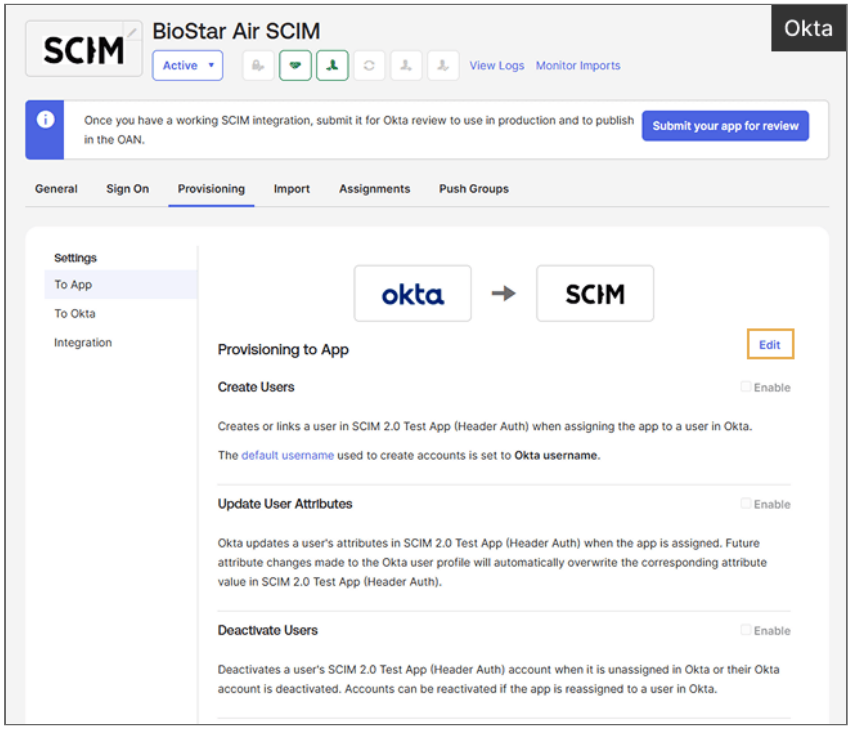
1. プロビジョニングアプリの作成が完了したら、**Provisioning**タブをクリックしてください。



2. **Configure API Integration**ボタンをクリックしてください。
3. **Enable API integration**をクリックしてください。
4. BioStar Air: SCIM トークンをコピーステップでコピーしたSCIMエンドポイントURLとSCIMベアラートークンの値を、**Base URL**フィールドと**API Token**フィールドに入力してください。

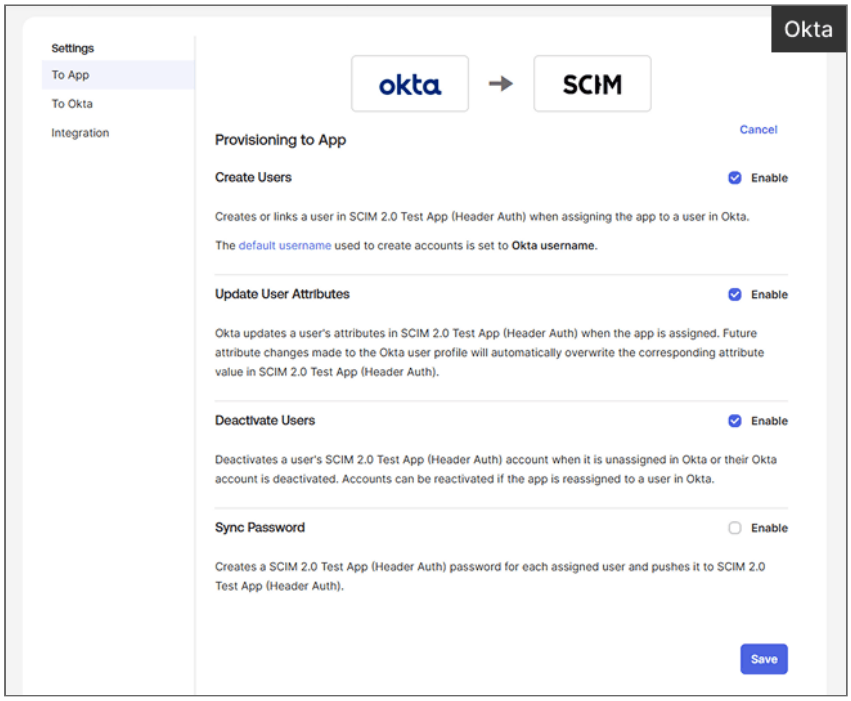


5. 同期が正常に動作するかをテストするには、**Test API Credentials**ボタンをクリックしてください。
6. **Save**ボタンをクリックしてください。
7. グループプッシュの動作を設定するには、**Provision**タブをクリックしてください。
8. **Edit**をクリックし、次の属性を有効にしてください。



- **Create Users**
- **Update User Attributes**
- **Deactivate Users**

9. 変更した設定を保存するには、**Save**ボタンをクリックしてください。

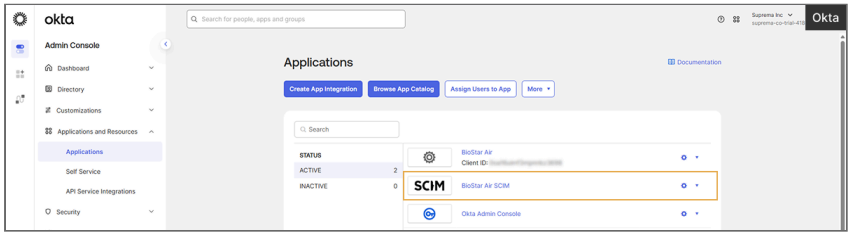


IdP グループを BioStar Air にプッシュ

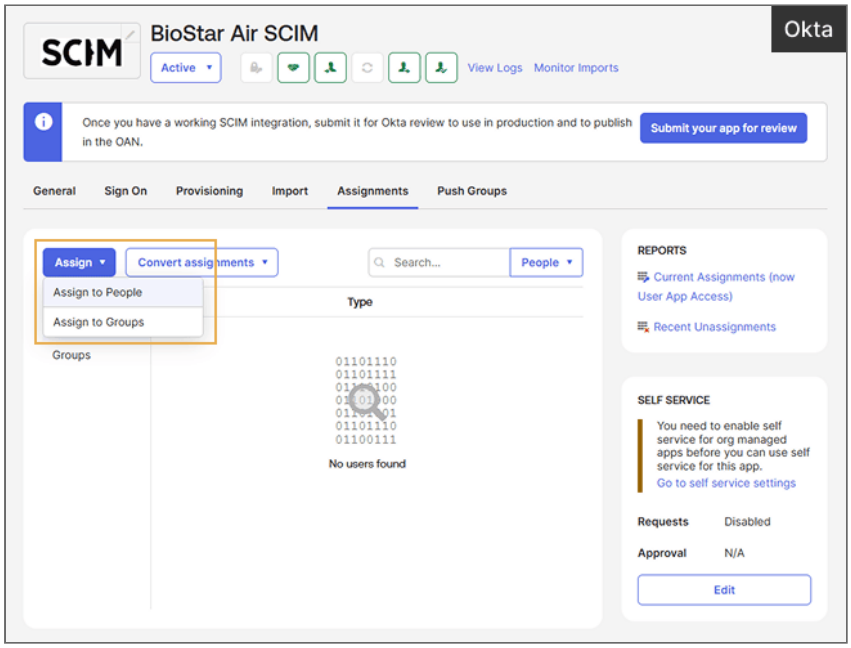
IdP グループを BioStar Air にプッシュするには、先にユーザーグループとユーザーを Okta に用意する必要があります。 ユーザーグループとユーザーを用意したら、SCIM を通じて BioStar Air にプッシュできます。

1 Okta: ユーザーグループの割り当て

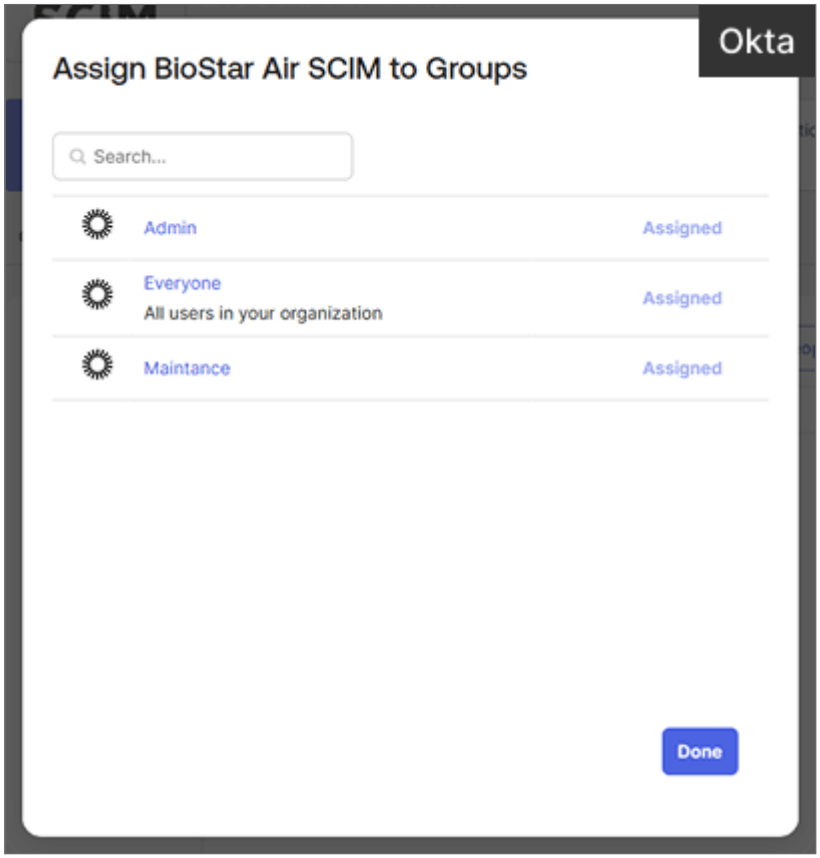
1. **Okta管理者コンソール**にログインします。
2. **Applications and Resources** → **Applications** メニューに移動します。
3. SCIMアプリケーションを選択してください。



4. **Assignments**タブをクリックしてください。
5. **Assign** → **Assign to Groups**をクリックしてください。

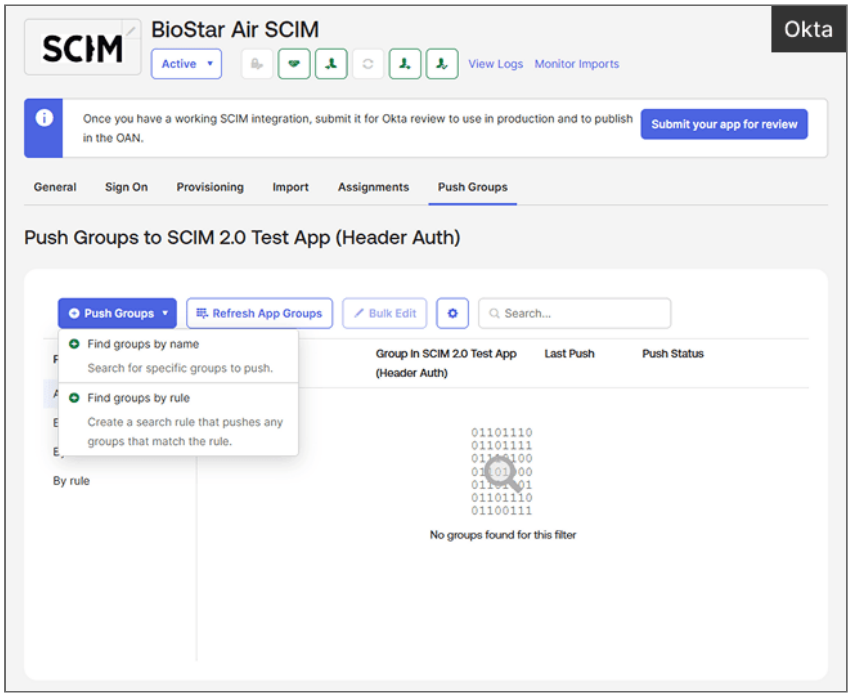


6. SCIMアプリケーションに割り当てるユーザーグループで**Assign**をクリックしてください。
7. グループの割り当てが完了したら、**Done** ボタンをクリックしてください。



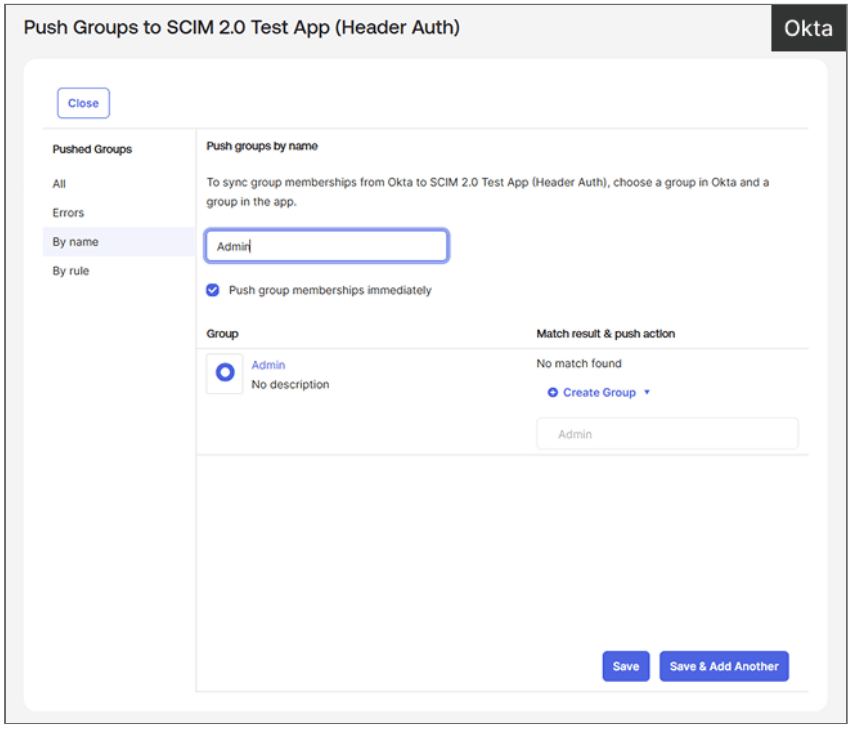
❷ Okta: ユーザーグループのプッシュ

1. **Push Groups** タブをクリックしてください。
2. **Push Groups → Find groups by name** をクリックしてください。



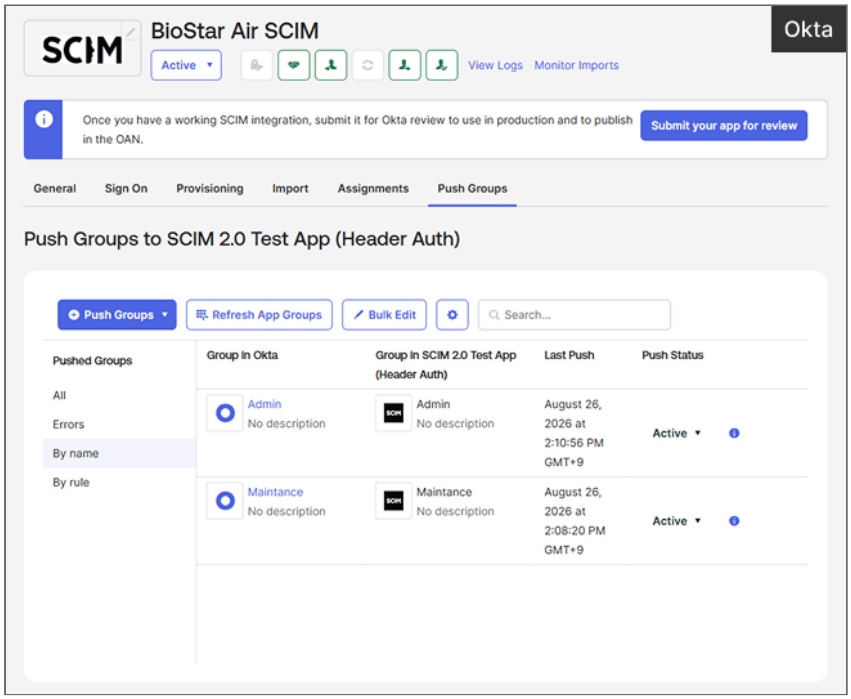
3. 入力欄にプッシュするグループ名を入力してください。

4. 一致するユーザーグループが表示されたら、選択してください。



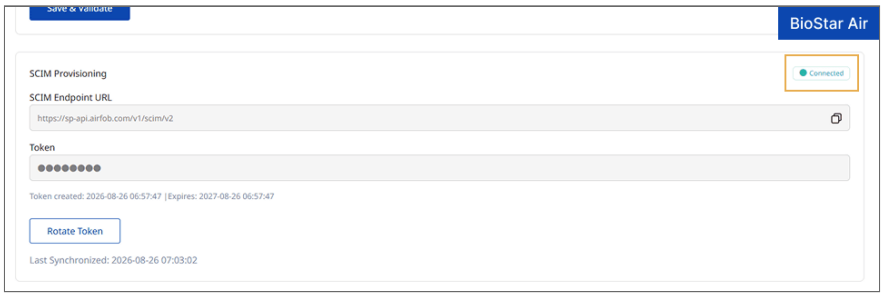
5. ユーザーグループの選択が完了したら、**Save** ボタンをクリックしてください。続けてユーザーグループを追加する場合は、**Save & Another** ボタンをクリックしてください。

6. **Push Groups** タブで、プッシュされたユーザーグループを確認できます。



❸ BioStar Air: 接続の確認

1. BioStar Air 画面左のサイドバーで **設定** → **サイト** をクリックします。
2. **SSO & SCIM** タブをクリックします。
3. **SCIMプロビジョニング** セクションで **接続済み** の表示を確認します。



グループマッピング

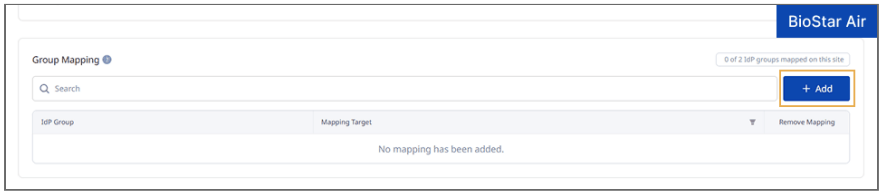
SSO と SCIM の接続を完了し、ID プロバイダーのグループを BioStar Air にプッシュした場合、サイト管理者はプッシュされたグループを BioStar Air のグループにマッピングする必要があります。

マッピングルール

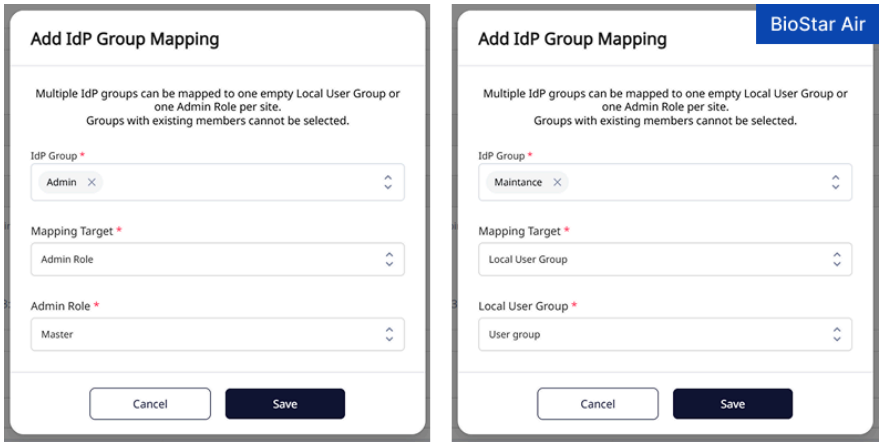
- 一つの BioStar Air ユーザーグループに複数の ID プロバイダーグループをマッピングできます。
- BioStar Air ユーザーグループは、マッピングする前に空である必要があります。
- すでにメンバーがいる BioStar Air グループは、マッピング先として選択できません。
- ID プロバイダーグループのマッピングは、サイトマスター管理者のみ管理できます。
- ID プロバイダーグループをマスターロールにマッピングすると、その後ロールを変更できません。

管理者/ユーザーグループをマッピングする

1. BioStar Air 画面左のサイドバーで **設定** → **サイト** をクリックします。
2. **SSO & SCIM** タブをクリックします。
3. **グループマッピング** セクションに移動し、**追加** ボタンをクリックします。

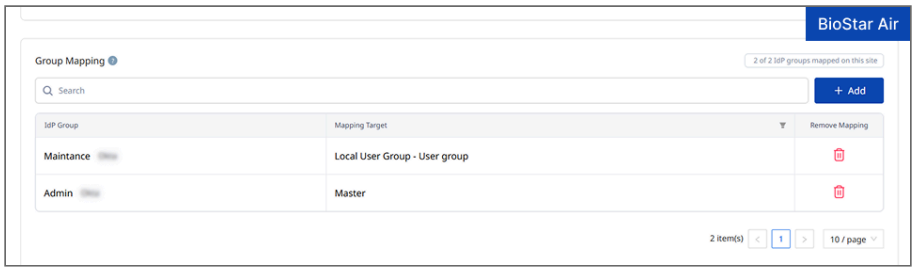


4. **IdPグループ** で ID プロバイダーグループを選択します。
5. **マッピング先** で、選択した IdP グループに応じて **管理者ロール** または **ローカルユーザーグループ** を選択します。
6. マッピング先に応じて、管理者ロールを指定するか、ユーザーグループを選択します。



7. マッピングを保存するには、**保存** ボタンをクリックします。

グループマッピング セクションで、ID プロバイダーグループとマッピングされた BioStar Air グループを確認できます。

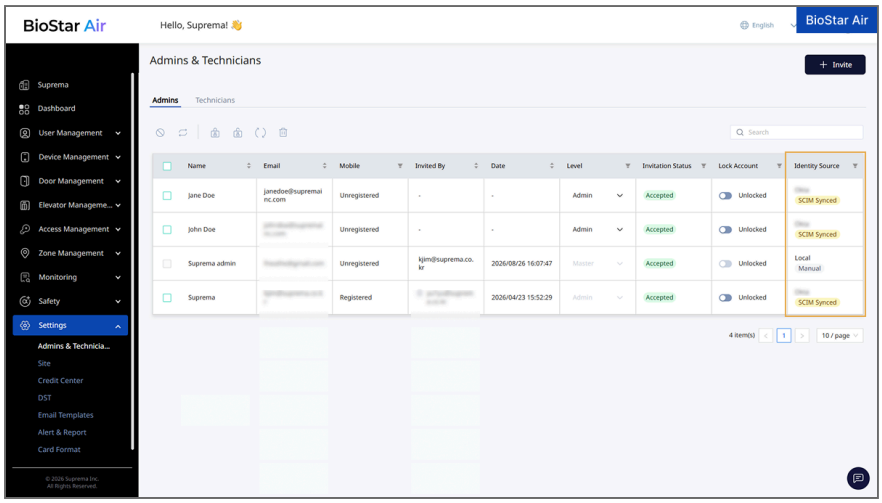


> **情報**
>
> - 管理者ロールの詳細については 管理者アカウントおよび役割の管理 をご覧ください。
> - ユーザーグループの詳細は ユーザーグループを管理する を参照してください。

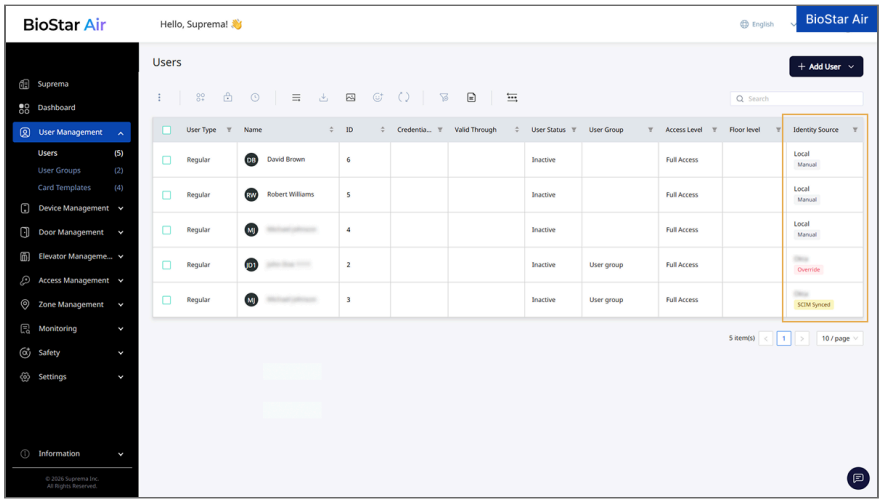
同期された管理者/ユーザー/グループの管理

プロビジョニングを有効にすると、BioStar Airは各管理者、ユーザー、ユーザーグループがローカルで直接管理されているか、ID プロバイダーから同期されているかを画面に表示します。

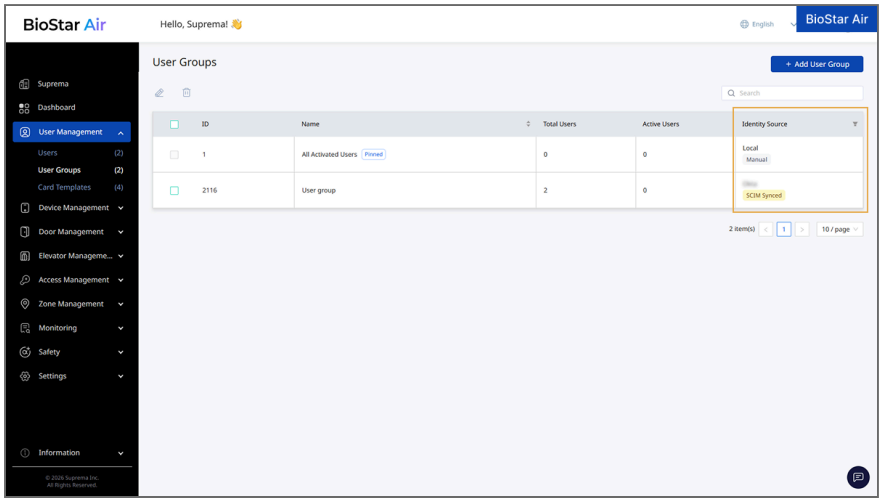
- **設定** → **デバイスのみ** メニューの管理者リストで、**IDソース** 列を確認してください。



- **ユーザー管理** → **ユーザー** メニューのユーザーリストで、**IDソース** 列を確認してください。

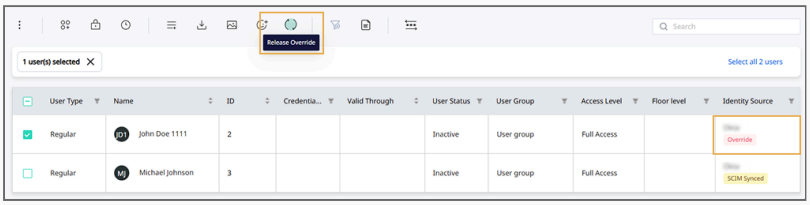


- **ユーザー管理** → **ユーザーグループ** メニューのユーザーグループリストで、**IDソース** 列を確認してください。



SCIM同期項目の動作の仕組み

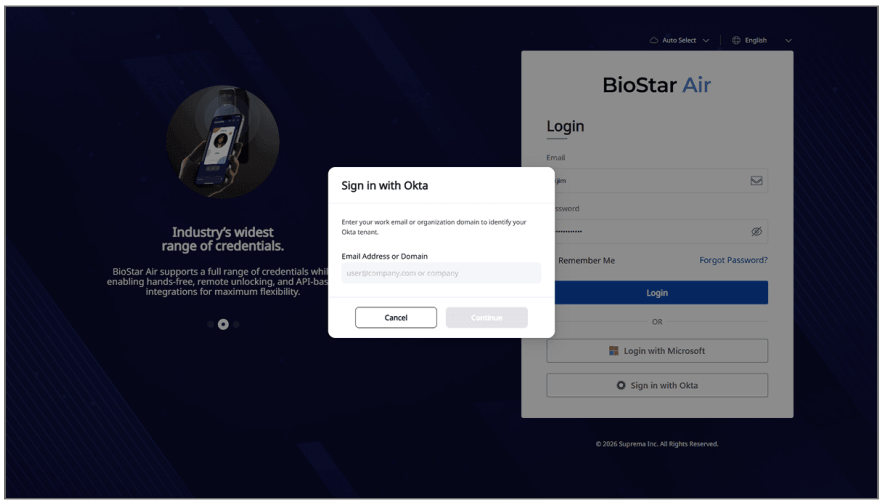
- 既存の手動で作成したユーザーと管理者は、引き続き手動管理のままです。
- SCIMで同期された項目は、BioStar Airで手動で削除できません。
- SCIMで同期されたグループでは、ユーザーを手動で追加または削除できません。
- 同期された項目をローカルで手動で変更すると、**オーバーライド** 状態になります。 **オーバーライド解除** を実行すると、ローカルの変更が取り消され、項目が再びSCIM管理状態に戻ります。



Okta にログイン

Okta SSO 連携を完了すると、ユーザーは BioStar Air のログイン画面で Okta アカウントを使用してログインできます。

1. BioStar Air のログイン画面で **Okta アカウントでサインイン** ボタンをクリックしてください。



2. **メールアドレスまたはドメイン** フィールドに組織のメールアドレスまたはドメインを入力します。 （例: `user@company.com` または `company`）
3. **続行** ボタンをクリックします。
4. Okta のログイン画面に移動したら、組織アカウントのメールアドレスとパスワードを入力してください。
5. 認証を完了すると、BioStar Airに自動的にリダイレクトされ、ログインが完了します。

情報

入力したメールドメインに Okta SSO が設定されていない場合、エラーメッセージが表示されます。 この場合は、サイト管理者に問い合わせてください。

追加サイトの設定

サイトの基本設定に加え、時間ポリシー、メールテンプレート、通知の受信方法、勤怠記録など、BioStar Airサービス全体に影響を与える詳細な機能を設定できます。 カスタムWiegandカード形式を追加したり、勤怠管理の運用方式やレポート作成基準を直接設定することもできます。

サマータイム（DST）の設定

サマータイム（Daylight Saving Time、DST）を設定することで、サイトの時刻の調整方法を構成できます。 これは、特に複数のタイムゾーンにまたがるデバイスやログがあるサイトを管理する際に、一貫して正確な時刻の追跡を確保するために重要です。

BioStar Airで正確な時刻管理を行うには、**3箇所でDSTを設定する**必要があります：

- **DSTプロファイル**：各タイムゾーンごとにDSTの開始と終了日時を定義します。
- **サイトの時刻**：サイトとイベントログに適用されるタイムゾーンを設定します。
- **デバイスの時刻**：各デバイスが正しく時刻を調整するように設定します。

サマータイムを採用しているタイムゾーンにある場合、これら3つの設定すべてが正しく構成されている必要があります。

> **ヒント**
> 日光節約時間（Daylight Saving Time、DST）の設定に関するビデオガイドを見るには、次のビデオを参照してください。

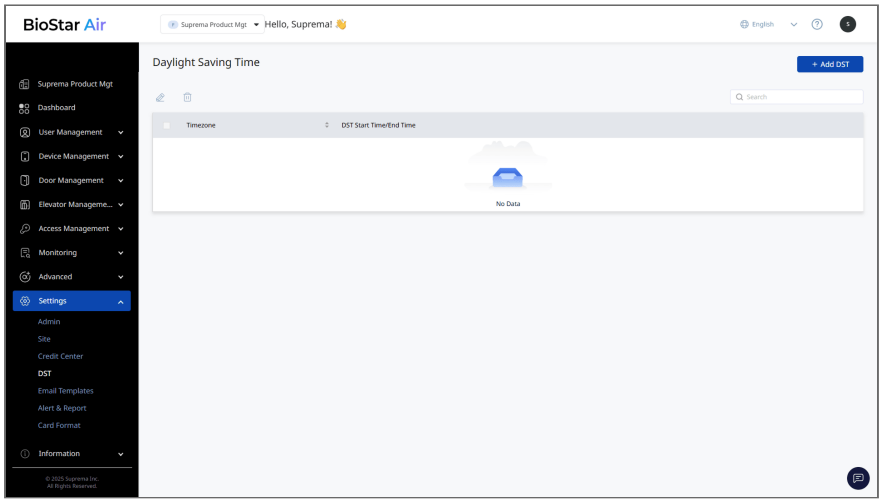
> **情報**
> イベントログを確認する際は、以下の点に注意してください。
> - デバイスの時刻が設定されている場合、イベントログのタイムスタンプは各デバイスのDST時間に合わせて調整されます。
> - サイトの時刻が設定されている場合、タイムスタンプはデバイスごとではなくサイトのDST構成に従って調整されます。

ステップ1: DSTプロファイルを作成する

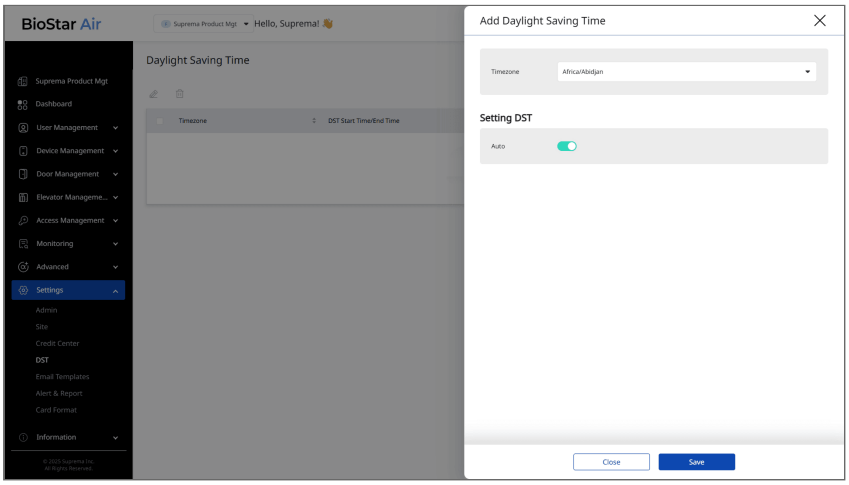
DSTプロファイルは、特定のタイムゾーンにおけるDSTの開始日時と終了日時を定義します。 サイトやデバイスがある各タイムゾーンごとにDSTプロファイルを作成する必要があります。

新しいプロファイルを追加

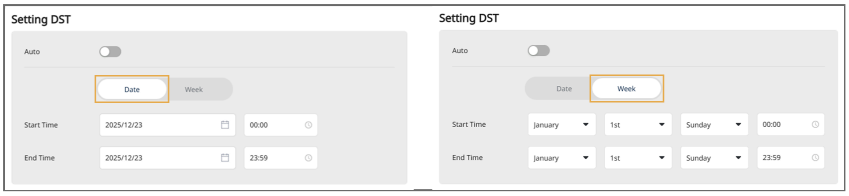
1. 画面左のサイドバーで **設定** → **DST** をクリックします。
2. 画面右上の **夏時間を追加** をクリックします。



3. **夏時間を追加**パネルが表示されたら、**タイムゾーン**で希望する項目を選択します。
4. **夏時間の設定**で自動または手動による構成を選択してください。
   - **自動構成**: 選択したタイムゾーンのDST構成が自動的に追加されます。 DSTの開始・終了日は、当該タイムゾーンの標準ルールに従って設定されます。



   - **手動構成**: 手動で設定するには、該当タイムゾーンの適切な開始時刻と終了時刻を設定してください。

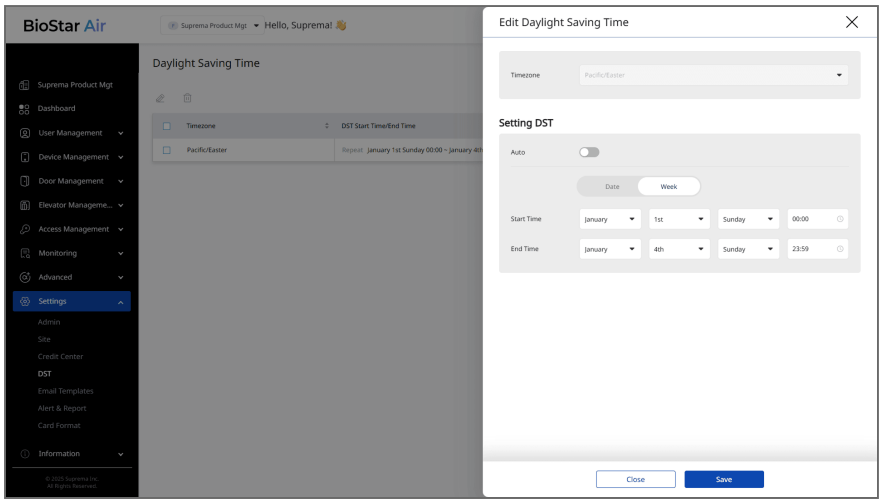


     - **日付**：DSTが開始および終了する日付を選択できます。
     - **週**：DSTが開始および終了する週を選択できます。
5. DSTプロファイルを保存するには、下部の **保存** をクリックしてください。

既存のDST構成を編集する

1. 画面左のサイドバーで **設定** → **DST** をクリックします。
2. 一覧から編集するDSTプロファイルをクリックしてください。 またはチェックボックスをクリックし、上部の ボタンをクリックしてください。

3. **夏時間編集**パネルが表示されたら、開始時刻と終了時刻を修正します。



上記の画像は例示です。実際の画面とは異なる場合があります。

4. 変更を保存するには、下部の **保存** をクリックします。

プロファイルの削除

1. 画面左のサイドバーで **設定** → **DST** をクリックします。
2. 一覧で削除するDSTプロファイルのチェックボックスをクリックしてください。 1つ以上のプロファイルを選択できます。
3. 画面上部の 🗑 ボタンをクリックしてください。
4. メッセージウィンドウが表示されたら、**はい** をクリックしてください。

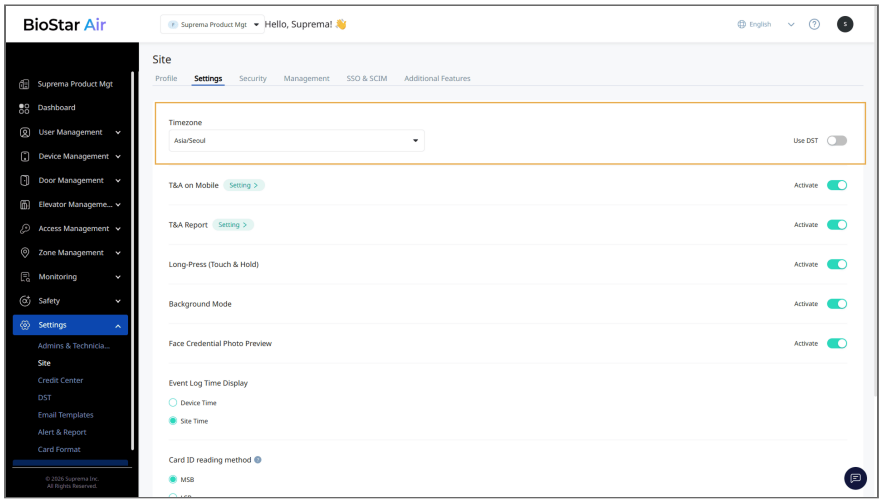
ステップ2: サイトの時刻を設定する

サイトの時間はシステム全体で使用されるデフォルトのタイムゾーンを決定します。 この設定の影響を受ける項目は以下のとおりです。

- イベントログおよび記録のタイムスタンプ
- レポートおよび監視データ
- 新しいデバイスを登録する際に適用されるデフォルトのタイムゾーン

以下の手順に従ってサイトのタイムゾーンを設定し、DSTを有効にしてください。

1. 画面左のサイドバーで **設定** → **サイト** をクリックします。
2. **Settings** タブをクリックしてください。
3. **タイムゾーン** で希望するタイムゾーンを選択してください。



4. 選択したタイムゾーンでDSTが適用される場合は、 **夏時間を使用** オプションを有効にしてください。

> **注意**
> DSTが適用されるタイムゾーンで **夏時間を使用** オプションを有効にしないと、システムが自動で時刻を調整せず、イベントログに誤った時刻が表示される可能性があります。

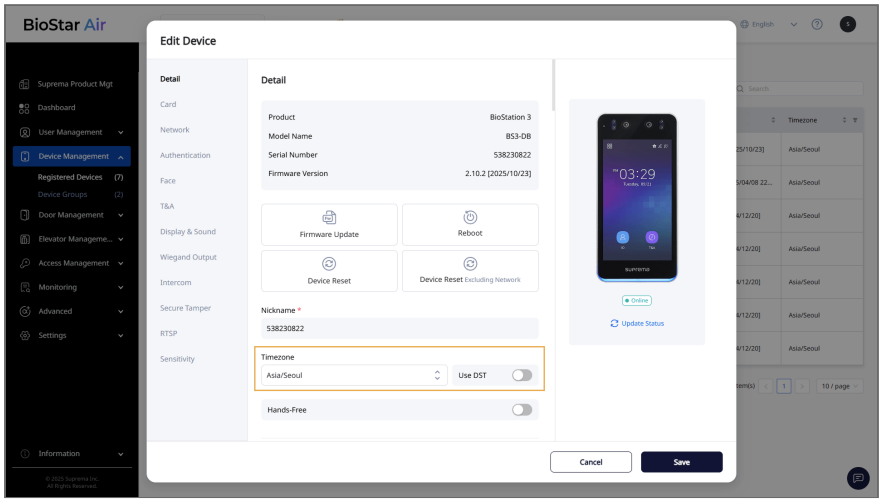
ステップ3: デバイスでDSTを有効にする

BioStar Airに接続されている各デバイスは内蔵時計を保持しており、入退室管理や勤怠記録に使用されます。 DSTが適用されるタイムゾーンにあるデバイスでは、必ずDST設定を行ってください。

BioStation 3のような画面付きのデバイスは、ユーザーに時刻を表示します。 XPass 2のような画面のないデバイスも内部で時刻を維持し、入退室管理や勤怠記録に使用します。

画面の有無にかかわらず、すべてのデバイスでDSTを設定する必要があります。そうしないと、イベントログ、入退室記録、勤怠データが正確に記録されません。

1. 画面左のサイドバーで **デバイス管理** → **登録済みデバイス** をクリックします。
2. 一覧からDST設定を適用するデバイスをクリックしてください。
3. **タイムゾーン** セクションで希望するタイムゾーンを選択し、**夏時間を使用** オプションを有効にします。



> DSTを適用するタイムゾーンでは、この設定はデフォルトで有効になります。

4. 変更を保存するには、下部の **保存** をクリックします。

> **情報**
> デバイスの時刻が正しく設定されていないと、以下のような問題が発生する可能性があります：
> - **入室拒否エラー**：入室時間が07:00からに設定されている場合、デバイスが06:00と認識するとユーザーの入室が拒否されます。
> - **スケジュールエラー**：予約された時間の施錠/解錠が正確でない可能性があります。
> - **記録エラー**：イベントログと勤怠記録の時刻が実際の時刻と一致しません。

チェックリスト

夏時間が適用される地域で正確な時刻管理を保証するには、次の3つの手順をすべて完了したことを確認してください。

- **DSTプロファイルの作成**：タイムゾーンごとに必要なDSTプロファイルを作成しましたか？
- **サイトの時刻設定**：サイトのタイムゾーンを設定し、**夏時間を使用** オプションを有効にしましたか？
- **デバイスのDST適用**：各デバイスのタイムゾーンを設定し、**夏時間を使用** オプションを有効にしましたか？

これら3つがすべて正しく設定されていれば、イベントログやアクセス時間、勤怠記録はすべて正しい時刻で表示されます。

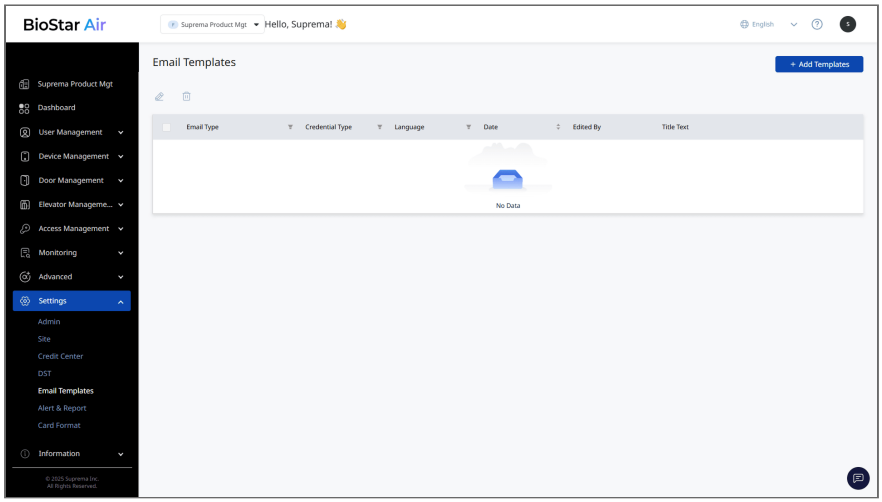
メールテンプレートのカスタマイズ

メールテンプレート機能を使って、サイト利用者に送信されるメールを会社のブランドやメッセージに合わせてカスタマイズできます。 メールテンプレートには招待状、アクティベーションメール、およびその他の通知が含まれます。

> **ヒント**
> メールテンプレート設定のビデオガイドを視聴するには、次の動画を参照してください。

メールテンプレートの追加

1. 画面左のサイドバーで **設定** → **Eメールテンプレート** をクリックします。
2. 画面右上の **メールテンプレートを追加** をクリックします。

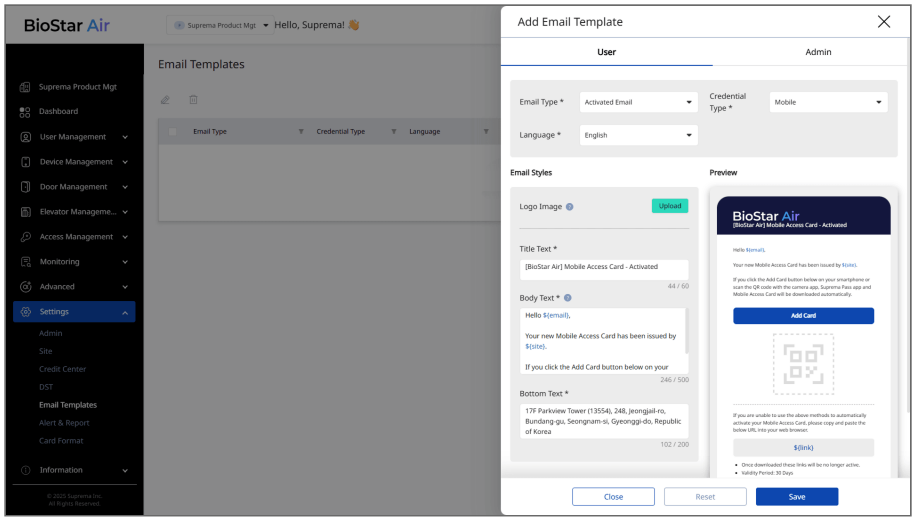


3. **メールテンプレートを追加** パネルが表示されたら、各項目の設定を構成します。 **ユーザー** または **アドミン** タブを選択して、ユーザーまたは管理者のメールテンプレートを設定できます。

> **情報**
>
> 言語ごとにメールテンプレートを個別に作成できます。 **言語** オプションで言語を選択できます。 サポートされている言語は以下のとおりです。
>
> > *English, 한국어, 日本語, Nederlands, Español, Português*
>
> 今後さらに多くの言語をサポートする予定です。

ユーザー

ユーザーに送信されるメールテンプレートをカスタマイズできます。



- **Eメールの種類**：作成するメールテンプレートの種類を選択します。 利用可能なオプションは以下のとおりです。
  - **アクティベーションのメール**：通常、モバイルカードをダウンロードするための招待状として使用します。
  - **再アクティブ化された電子メール**：モバイルカードが再アクティブ化されたことをユーザーに通知します。
  - **再発行メール**：新しいモバイルカードを発行する際に使用します。
  - **削除メール**：カード削除に関する通知をユーザーに送信します。
  - **一時停止メール**：カードが一時停止されたことをユーザーに通知します。

  - **顔登録リクエストメール**：ユーザーに顔写真の登録を依頼する際に使用します。

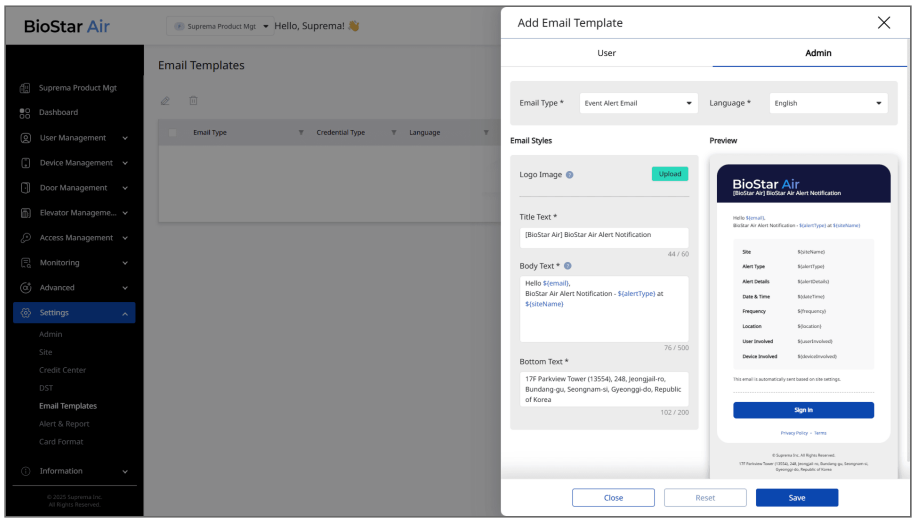
- **認証情報の種類**：**アクティベーションのメール** および **再発行メール** のように、モバイルカードのダウンロードを許可するメール種類で選択できます。

  - **Mobile**
  - **Web QR**
  - **リンクパス**

> クレデンシャルの種類の詳細については、ユーザーのカードとクレデンシャルの種類をご参照ください。

アドミン

管理者に送信されるメールテンプレートをカスタマイズできます。

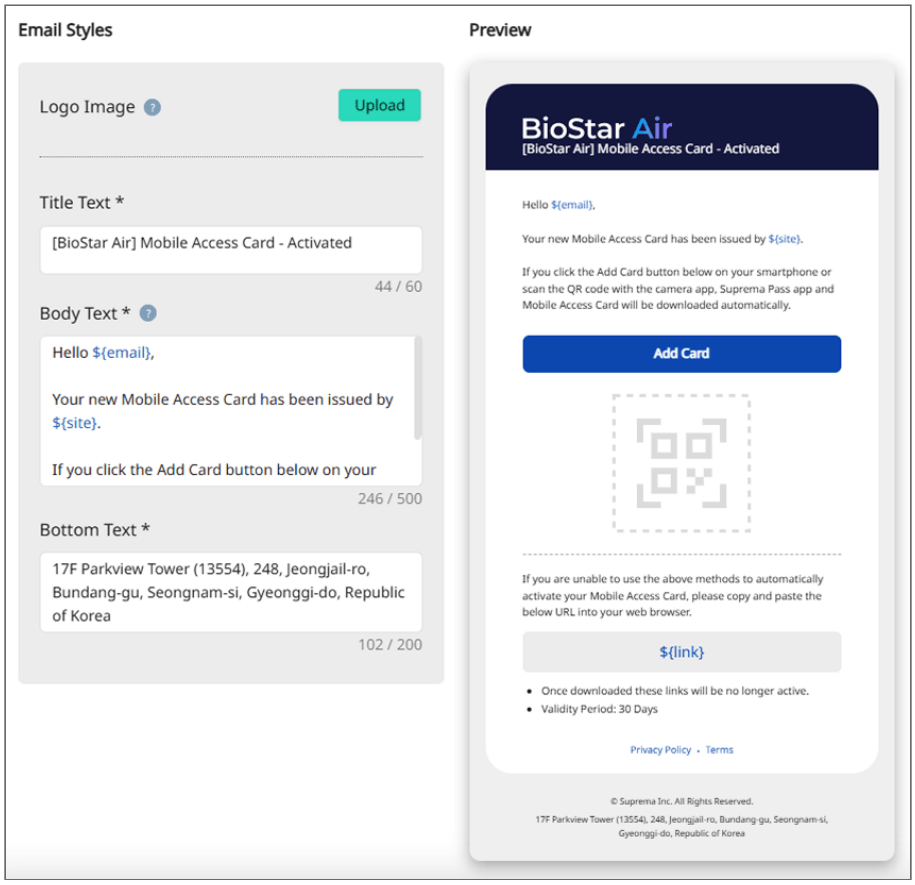


Eメールの種類：作成するメールテンプレートの種類を選択します。 利用可能なオプションは以下のとおりです。

- **イベントアラートメール**：サイトで発生したイベントに関する通知を管理者に送信します。
- **システムアラートメール**：システムアラートを管理者に送信します。
- **レポート通知Eメール**：レポートを生成した後、ダウンロードリンクを管理者に送信します。

Eメール・スタイル

メールのロゴと内容をカスタマイズできます。 **プレビュー** でリアルタイムに変更を確認できます。



- **ロゴ画像**：メールに表示するロゴ画像をアップロードします。

  - ファイル形式: JPG、JPEG、PNG
  - 最小解像度: 200 x 60
  - ファイルサイズ: 1 MB以下

- **タイトルテキスト**：メールの件名を入力します。
- **本文テキスト**：メール本文に表示するメッセージを入力します。

メール本文にはHTMLキー（key）が含まれている必要があります。 キー（key）はそれぞれ受信者のメールアドレスやサイト名などに置き換えられます。 **Eメールの種類**で選択した値によって使用できるキー（key）は異なる場合があります。
  - **ユーザー** タブ
  - `${email}`：メールアドレス
  - `${siteName}`：サイト名
  - **管理者** タブ
  - `${email}`：メールアドレス
  - `${siteName}`：サイト名
  - `${alertType}`：通知の種類
  - `${alertDetails}`：通知の詳細
  - `${frequency}`：通知の発生頻度
  - `${location}`：通知が発生した場所
  - `${userInvolved}`：通知に関連するユーザー
  - `${deviceInvolved}`：通知に関連するデバイス
  - `${dateTime}`：通知が発生した日時

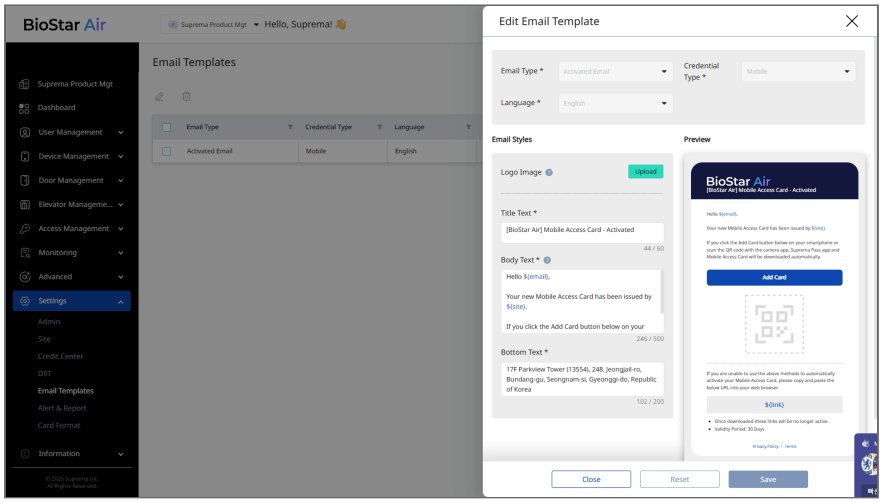
- **フッター**：メール下部に表示する追加情報を入力します。 規制遵守のため、またはユーザーに場所の詳細を提供するために、会社の住所や連絡先情報を追加します。

情報

- ロゴ画像がメールで適切に表示されるよう、正しい形式とサイズであることを確認します。
- 現在使用している言語がサポートされていない場合は、今後のアップデートを確認してください。 さらに多くの言語を追加する予定です。
- 住所欄は規制遵守と明確性のために重要なので、正確に入力してください。
- メールテンプレートを保存するには、下部の **保存** をクリックします。
- 既存の内容を変更した後に復元するには、下部の **リセット** をクリックします。

メールテンプレートの編集

1. 画面左のサイドバーで **設定** → **Eメールテンプレート** をクリックします。
2. 一覧から編集するメールテンプレートをクリックします。 またはチェックボックスをクリックし、上部の ボタンをクリックしてください。
3. **メールテンプレートの編集** パネルが表示されたら、必要な項目を修正します。



4. 変更を保存するには、下部の **保存** をクリックします。

メールテンプレートの削除

1. 画面左のサイドバーで **設定** → **Eメールテンプレート** をクリックします。
2. 一覧で削除するメールテンプレートのチェックボックスをクリックします。 1つ以上のテンプレートを選択できます。
3. 一覧上部の をクリックします。
4. メッセージウィンドウが表示されたら、**削除** をクリックします。

アラートとレポートの設定

アラートとレポートを設定すると、システムイベントやセキュリティ状況を自動で検知して追跡できます。 この文書では、BioStar Airでアラートとレポートの設定を構成する方法を案内します。

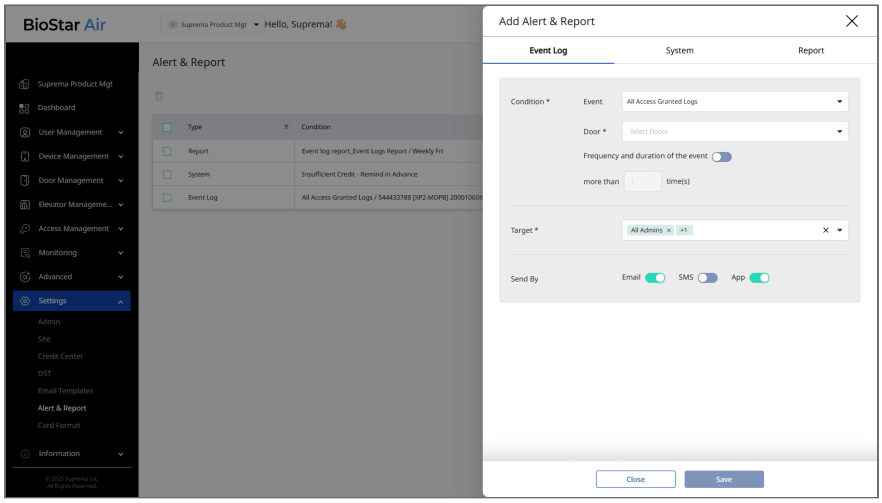
アラートおよびレポートの設定により、次の効果が得られます。

- セキュリティ脅威やシステムの問題を即座に検知し、管理者にリアルタイムで通知します。
- システム状況やユーザーの活動に関するレポートを自動生成して管理効率を高めます。

アラートの追加

サイトで発生する特定のイベントログやシステムに関する通知を設定できます。

1. 画面左のサイドバーで **設定** → **アラートとレポート** をクリックします。
2. 画面右上の **アラートとレポートの追加** をクリックします。
3. **アラートとレポートの追加** パネルが表示されたら、**イベントログ**、**システム** のいずれかのタブを選択します。

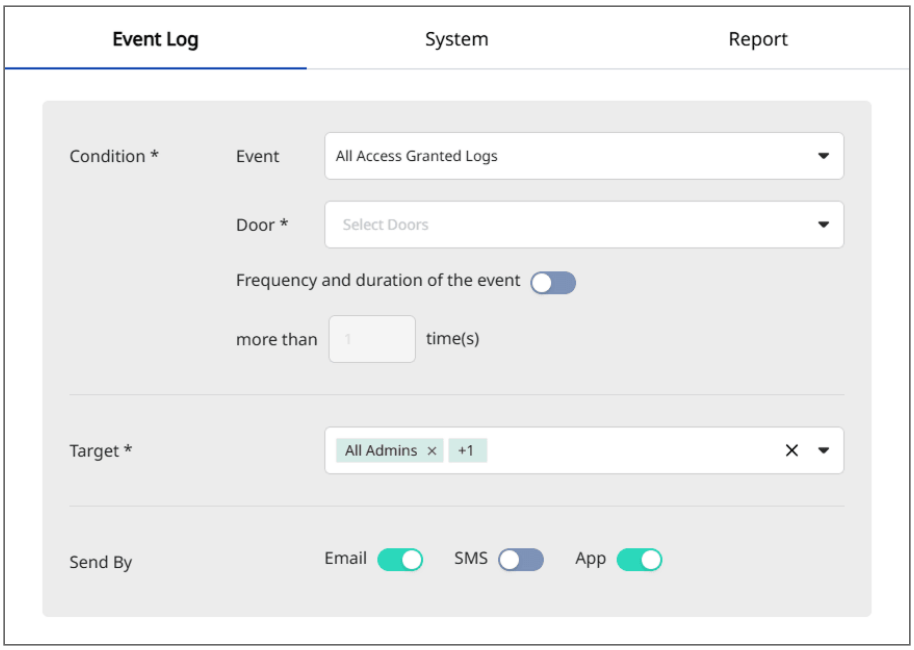


4. 設定を保存するには、**保存** をクリックします。

条件の設定

イベントログ

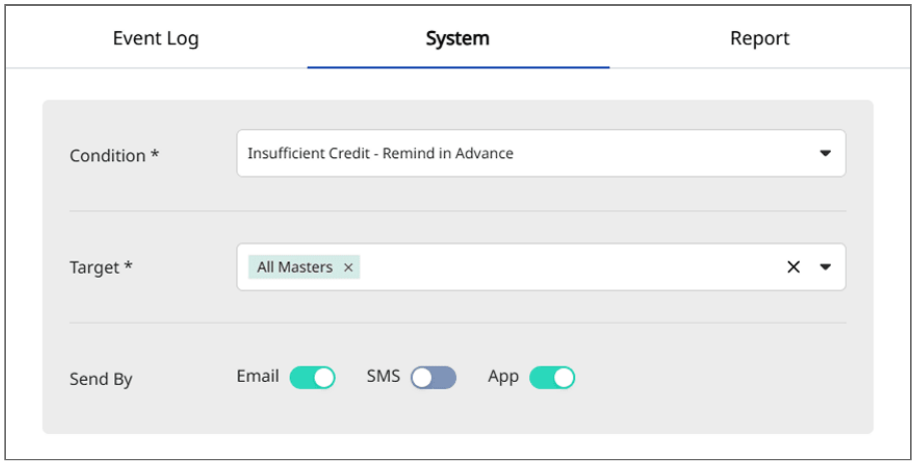
イベントログ タブで、イベント種類に応じて通知発生条件を設定できます。



- **イベント**：通知を設定するイベント種類を選択します。 事前定義された **プリセットイベント** を選択できます。
- **ドア**：ドアを選択します。 選択したドアでイベントが発生した場合に通知を送信します。 1つ以上のドアを選択できます。
- **イベントの頻度と期間**：設定した時間内に特定の頻度でイベントが発生した場合に通知を送信します。 例えば、5分間に3回以上イベントが発生した場合に通知を送信するよう設定できます。

> **ヒント**
> BioStar Air 2.12 以上では、デバイスのネットワーク切断イベントをリアルタイム通知として設定できます。

システム



システム タブでシステムの状態に応じて通知発生条件を設定できます。選択できるオプションは次のとおりです。

- **クレジット不足 - 事前に通知**
- **クレジット不足 - サイトが停止**
- **クレジット不足 - SMS (10 未満)**
- **APB バッテリー残量が少なくなっています**
- **新しいファームウェアが利用可能です**
- **ネットワークから切断しました（デバイスによって検出）**

通知対象の設定

ターゲット で通知を受け取る対象を設定できます。 管理者権限別にユーザーを選択したり、個別のユーザーを選択できます。

送信方法の設定

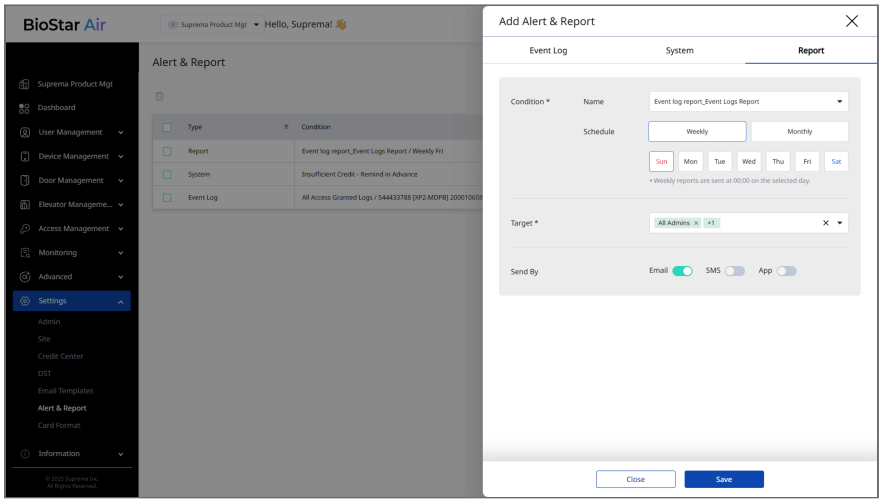
送信者 で通知の送信手段を選択します。 メール、SMS、アプリのプッシュ通知の方法で通知を送信できます。

> **情報**
> SMS送信を利用するには、SMSクレジットをチャージする必要があります。 残りのSMSクレジットは**設定** → **クレジットセンター**で確認できます。

レポート作成

特定の時間間隔でレポートを自動生成して管理者に送信できます。 イベントログの発生状況およびユーザー状況に関するレポートを作成できます。

1. 画面左のサイドバーで **設定** → **アラートとレポート** をクリックします。
2. 画面右上の **アラートとレポートの追加** をクリックします。
3. **アラートとレポートの追加** パネルが表示されたら、**レポート** タブを選択します。



4. 設定を保存するには、**保存** をクリックします。

条件設定

レポートの種類と作成周期を設定します。

- **名前**：作成するレポートの種類を選択します。
  - **T&Aレポート**：選択した期間のユーザーの勤怠状況に関するレポートを作成します。
  - **監査ログレポート**：選択した期間の変更履歴に関するレポートを作成します。
  - **イベントログレポート**：選択した期間のイベントログの発生状況に関するレポートを作成します。
  - **ユーザーレポート**：選択した期間のユーザー状況に関するレポートを作成します。
- **スケジュール**：レポート作成の頻度を選択してください。 **毎週**、**毎月** の中から選択できます。

通知対象の設定

ターゲット で通知を受け取る対象を設定できます。 管理者権限別にユーザーを選択したり、個別のユーザーを選択できます。

送信方法の設定

送信者 で通知の送信手段を選択します。

> **情報**
> レポートは**メールのみで送信**できます。 SMSやアプリのプッシュ通知で送信することはできません。

アラートおよびレポートの編集

1. 画面左のサイドバーで **設定** → **アラートとレポート** をクリックします。
2. 一覧から編集するアラートまたはレポートをクリックします。
3. **アラートを編集** または **レポートの編集** パネルが表示されたら、必要な項目を編集します。
4. 変更を保存するには、下部の **保存** をクリックします。

アラートおよびレポートの削除

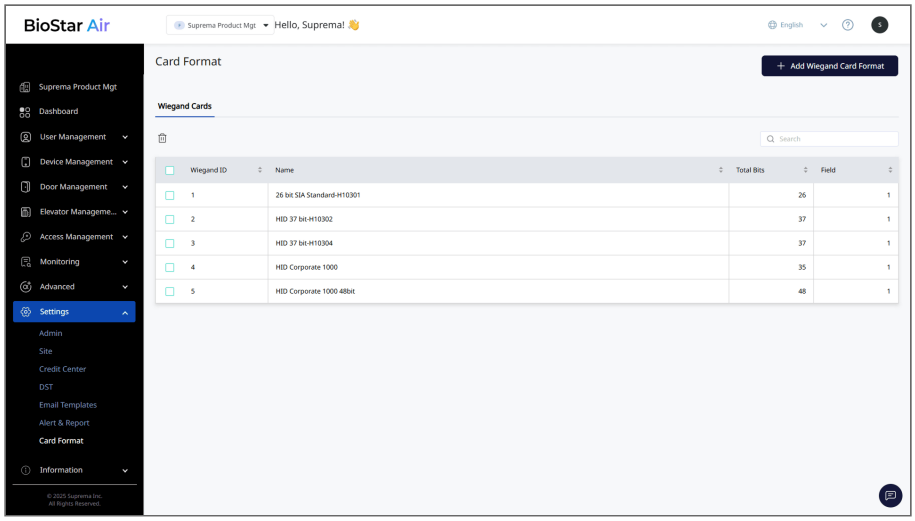
1. 画面左のサイドバーで **設定** → **アラートとレポート** をクリックします。
2. 一覧で編集するアラートまたはレポートのチェックボックスをクリックします。 1つ以上の項目を選択できます。
3. 一覧の左上にあるボタンをクリックしてください。
4. メッセージウィンドウが表示されたら、**削除** をクリックします。

カスタムWiegandカード形式を設定する

既存のアクセス制御システムから円滑にマイグレーションするためのファシリティコード、IDセグメント、パリティビット、ビット割り当てなどについて、BioStar Air v2.10でカスタムWiegandカード形式を作成および構成する方法を案内します。

Wiegandカード形式一覧

画面左のサイドバーで **設定** → **カードフォーマット** をクリックします。 **Wiegand形式**および**SIA、HID形式**を含む、特別なカード形式を作成、管理、参照できます。 既存のカードが提供されているアクセス制御ソリューションからマイグレーションするサイトで役立ちます。

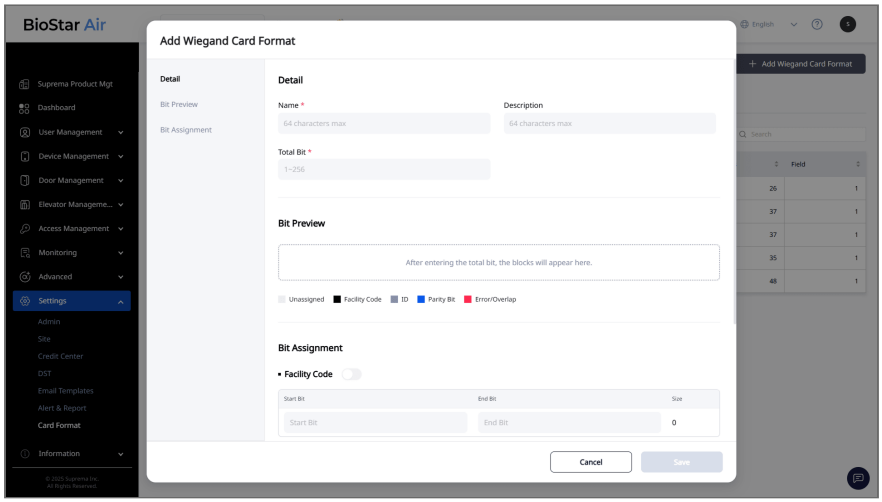


- BioStar Airに含まれるデフォルト形式を含め、登録されているすべてのWiegandカード形式を参照できます。
- カード形式の名前、説明、総ビット数、ビットプレビューおよび詳細なビット割り当てを確認できます。
- 名前、説明、総ビット数および詳細なビット割り当てを含めて、新しいカスタムカード形式を構成できます。 システムは視覚的確認のためのビットプレビューを提供します。

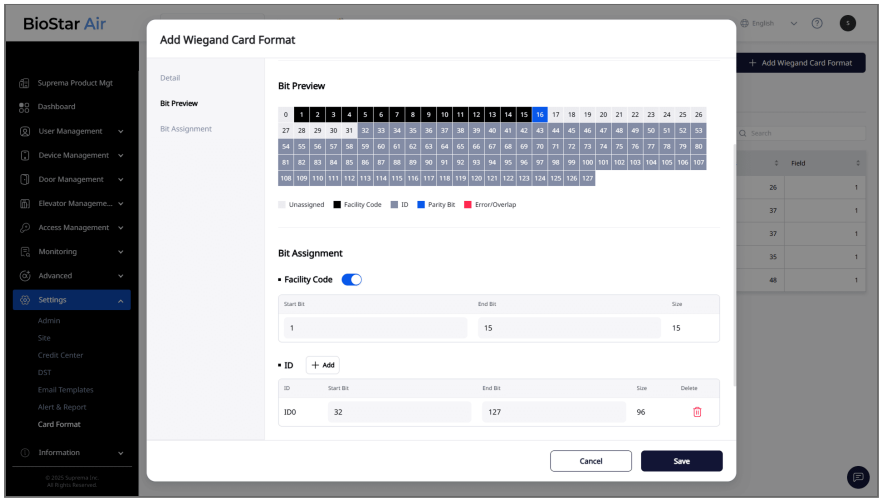
カード形式を追加する

デフォルトのWiegandカード形式に加えて、新しいカスタムWiegandカード形式を追加できます。

1. 画面左のサイドバーで **設定** → **カードフォーマット** をクリックします。
2. 画面右上の **Wiegand カードフォーマットの追加** ボタンをクリックします。
3. **Wiegand カードフォーマットの追加** ウィンドウが表示されたら、**詳細** セクションで名前と説明（省略可）、総ビット数を入力します。



4. 総ビット数を入力すると、**ビットプレビュー**が有効になり、**ビット割り当て** セクションでビット割り当てを構成します。



上記の画像は例示です。実際の画面とは異なる場合があります。

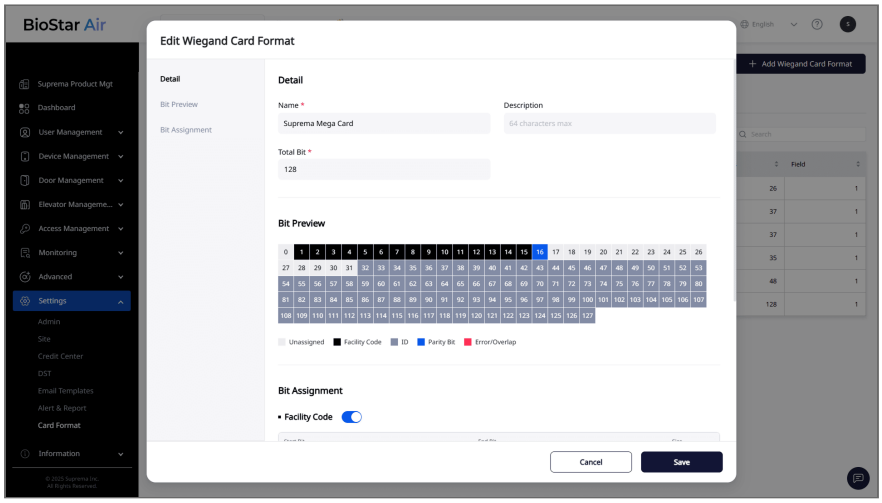
- **ファシリティコード**：識別コードを使用するにはトグルスイッチをクリックして有効にします。**開始ビット** と **終了ビット** を入力します。
- **ID**：開始ビットと終了ビットを指定して1つ以上のIDセグメントを追加します。
- **パリティビット**: 開始ビットと終了ビットを指定して、奇数/偶数のパリティビットを追加します。

5. 新しいカード形式を追加するには、**保存** ボタンをクリックします。

カード形式を編集する

既存のWiegandカード形式を編集するには、次の手順に従います。

1. 画面左のサイドバーで **設定** → **カードフォーマット** をクリックします。
2. 編集するカード形式をクリックします。
3. **Wiegand カードフォーマットの編集** ウィンドウが表示されたら、必要な項目を修正します。



4. 編集したカード形式を保存するには、**保存** ボタンをクリックします。

カード形式を削除する

1. 画面左のサイドバーで **設定** → **カードフォーマット** をクリックします。
2. 削除するカード形式のチェックボックスをクリックします。 1つ以上のカード形式を選択できます。
3. 一覧上部の 🗑 ボタンをクリックしてください。
4. メッセージウィンドウが表示されたら、**はい** ボタンをクリックします。

> **情報**
> デフォルトで提供される5つのWiegandカード形式は削除できません。

勤怠管理（T&A）の設定

BioStar Airは交代勤務と休憩時間を記録し、基本的な**勤怠管理**(T&A)の追跡機能を提供します。外部勤怠管理システムと連携したりエクスポートしたりできます。 BioStar Airは完全な勤怠管理システムを提供するわけではありませんが、イベントログの記録や給与・勤怠管理システムとのAPI連携をサポートします。 また基本的な**勤務時間**レポートを生成できます。

> **ヒント**
> 勤怠管理の設定に関する動画ガイドを視聴するには、次のビデオを参照してください。

勤怠イベント

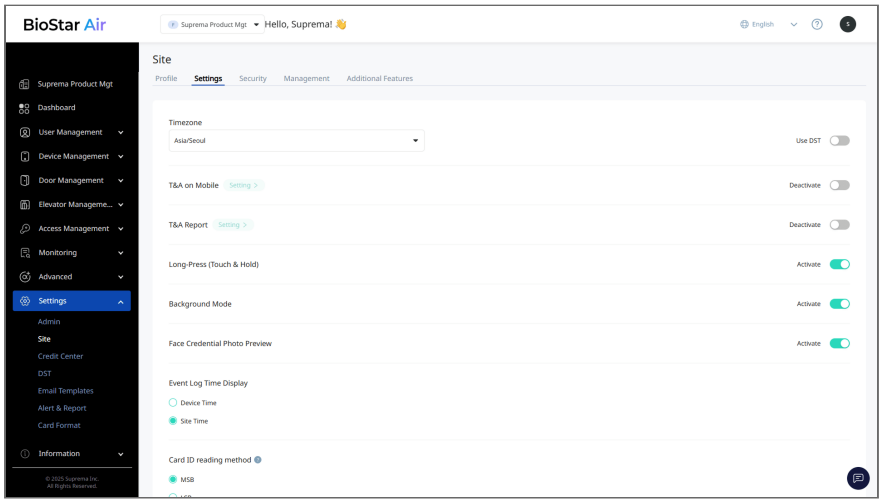
ユーザーは以下の勤怠イベントを記録できます。 勤怠イベントはイベントログに記録され、CSVファイルとしてエクスポートしたりAPIを介して取得したりできます。

- **シフト開始**
- **シフト終了**
- **休憩開始**
- **休憩終了**

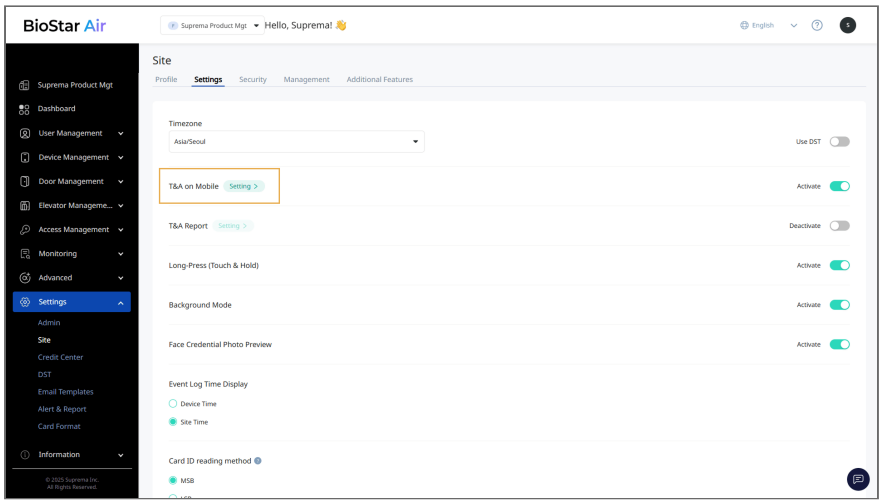
勤怠管理の設定

勤怠管理の設定を有効にし、詳細設定を構成するには次の手順に従ってください。

1. 画面左のサイドバーで **設定** → **サイト** をクリックします。
2. 画面上部の **Settings** タブをクリックします。

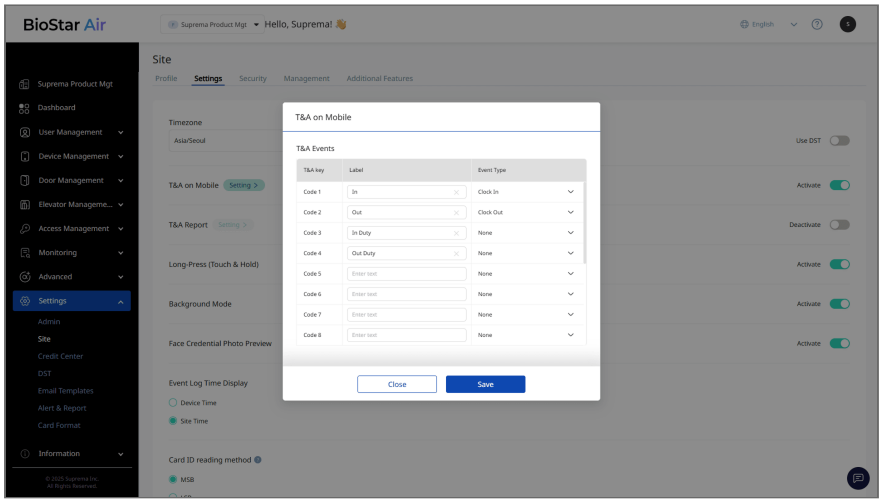


3. **モバイルでのT&A** 機能を有効にします。
4. 確認ダイアログが表示されたら、**OK**をクリックしてください。
5. **モバイルでのT&A** 機能で **設定** ボタンをクリックします。



6. **モバイルでのT&A** ウィンドウが表示されたら、**勤怠コード** のラベルを設定します。

> *例：シフト開始、シフト終了、休憩開始、休憩終了*

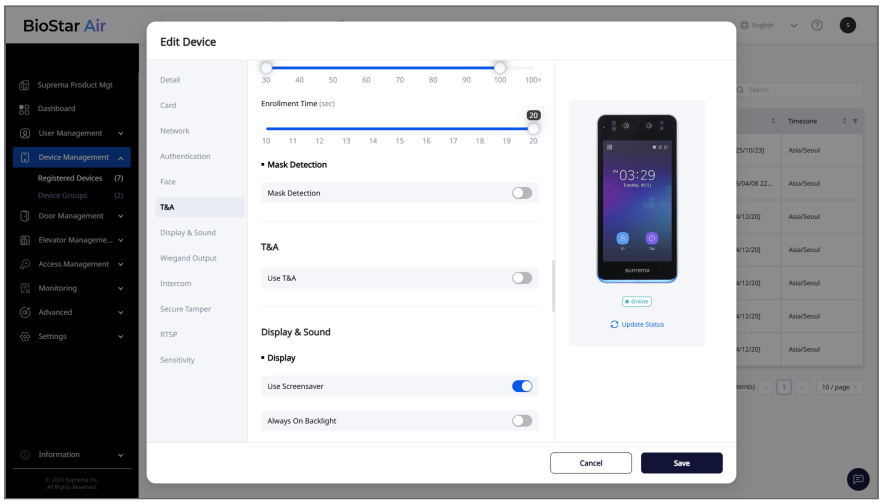


7. **勤怠コード** に対するイベント種別が **Clock-In** または **Clock-Out** かを選択します。
8. 設定を保存するには、**保存** をクリックします。

デバイスで勤怠機能を設定する

モバイルでのT&A 機能を有効にすると、これを使用するデバイスを指定できます。

1. 画面左のサイドバーで **デバイス管理** → **登録済みデバイス** をクリックします。
2. デバイス一覧から勤怠管理機能を設定するデバイスをクリックします。
3. **デバイス編集** ウィンドウが表示されたら、**T&A** セクションに移動します。



上記の画像は例示です。実際の画面とは異なる場合があります。

4. **T&Aを使用** オプションのトグルボタンをクリックして勤怠管理機能を有効にします。
5. 設定を保存するには、**保存** をクリックします。

- **勤怠管理モード** を **携帯** に設定すると、入退室認証時に勤怠の選択を必須にできる **T&A が必要です** オプションを利用できます。
- 勤怠イベントのラベルは**サイト**レベルで管理され、デバイスごとに変更できません。

勤怠管理モード

デバイスはさまざまな方法で勤怠イベントを記録できます。 **勤怠管理モード**で希望する勤怠管理モードを選択してください。

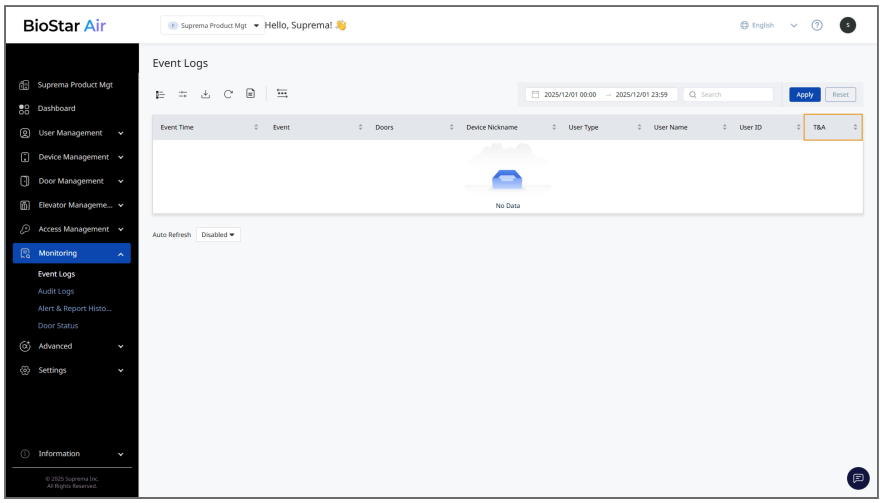
- **手動**：画面に勤怠キーを表示し、認証時にユーザーが勤怠イベントを選択できます。
- **スケジュール**：設定されたスケジュールに従って出勤および退勤時間を記録します。 例えば、8:00 AM ～ 12:00 PM の間に記録されたイベントは **Clock-In** として、1:00 PM ～ 5:00 PM の間に記録されたイベントは **Clock-Out** として記録されます。
- **手動固定**：ユーザーが最後に使用した勤怠イベントを継続して使用できます。
- **固定**：固定の勤怠コードをデバイスに割り当てます。 そのデバイスで認証されるたびに同じ勤怠イベントが記録されます。このオプションにより、該当デバイスを出勤用または退勤用に使用できます。
- **携帯**：ユーザーは認証する前に勤怠コードを選択する必要があります。 選択した勤怠イベントは入退室ログとともに記録されます。

> **情報**
> 機種によって対応している勤怠管理モードが異なる場合があります。 詳細はデバイスおよびパネルの設定オプションのご案内の機種別勤怠モードを参照してください。

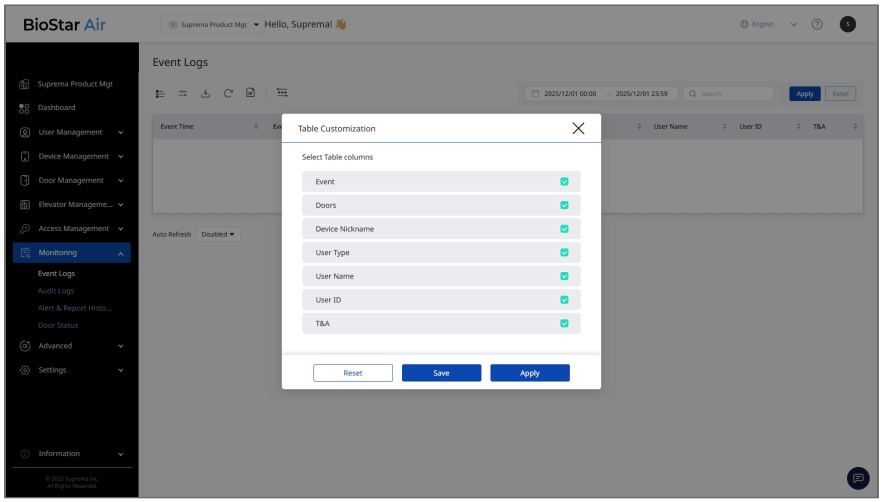
勤怠ログの表示およびエクスポート

勤怠イベントはイベントログに記録され、これを確認したりCSVファイルとしてエクスポートしたりできます。

1. 画面左のサイドバーで **モニタリング** → **イベントログ** をクリックします。
2. ログテーブルで**T&A**列(column)を探してください。



3. ログテーブル上部の⚙ボタンをクリックし、カスタマイズして**T&A**列が見やすい位置に移動してください。



4. データをCSVファイルとしてダウンロードするには、ボタンをクリックし、**CSV のダウンロード**を選択してください。

勤怠レポートを構成する

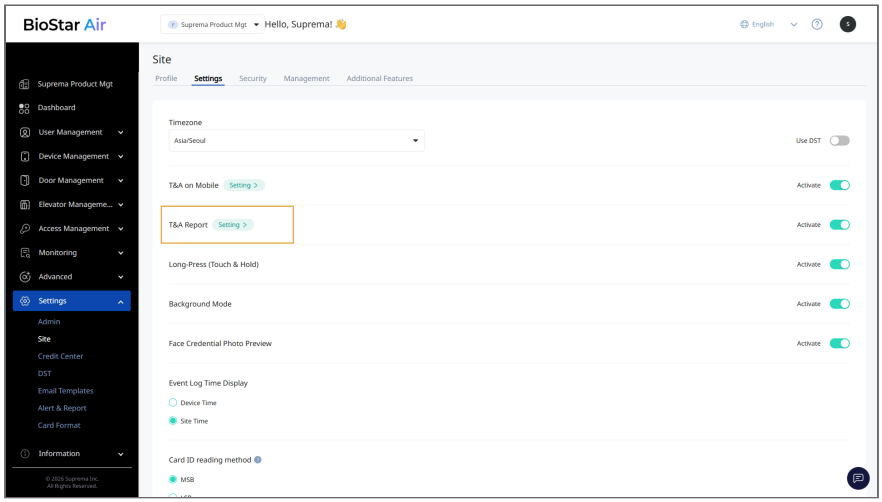
BioStar Airの勤怠レポート（T&A Report）は、簡単な**現場の勤務時間**レポートです。 イベントログに基づき、従業員の出勤時刻と退勤時刻を表示します。

この機能は、複雑な構成オプションを必要としない基本的なレポート向けに設計されています。 勤怠システムは地域の規制によりさまざまな要件がある場合があります。 標準の勤怠レポートが組織の要件を満たさない場合は、サードパーティのT&Aソリューションを使用することを推奨します。 イベントログは**CSVでエクスポート**するか、BioStar Air APIを使用してサードパーティの勤怠ソフトウェアと直接統合できます。

> **情報**
>
> - 標準の勤怠レポートは意図的に簡素に設計されており、すべてのコンプライアンス要件を満たさない場合があります。
> - 複雑な勤怠ルール（例：地域の労働法、シフトパターン）がある場合は、サードパーティの勤怠ソリューションを使用してください。
> - イベントログをCSVにエクスポートして手動で処理するか、APIを使用して他のシステムと自動的に統合できます。

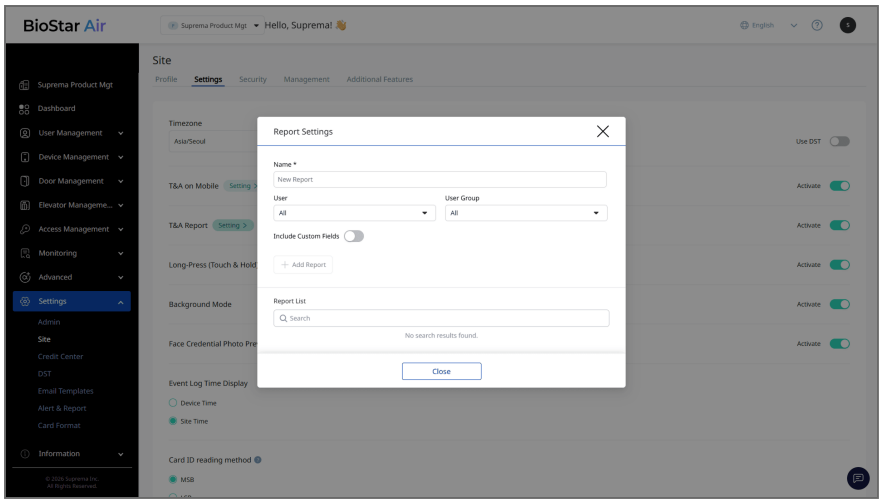
勤怠レポート（T&A Report）を作成するには、次の手順に従ってください。

1. 画面左のサイドバーで **設定** → **サイト** をクリックします。
2. **Settings** タブで **T&Aレポート** → **設定** をクリックします。



> **T&Aレポート** 機能を有効にするには、右側のトグルスイッチをクリックします。

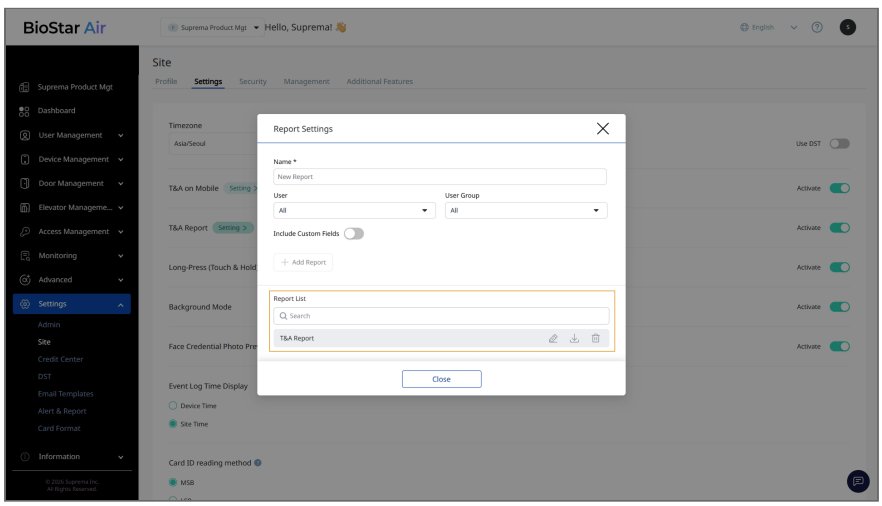
3. **レポート設定** ウィンドウが表示されたら、レポート名を入力します。



4. レポートに含めるユーザーまたはユーザーグループを選択します。

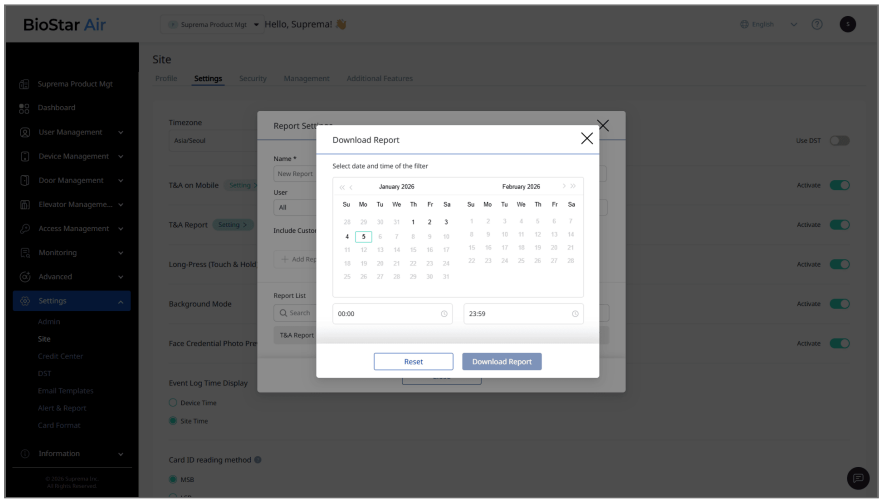
5. **レポートの追加** をクリックします。

6. **レポートリスト** にダウンロード可能なレポートが生成されます。



7. レポートをダウンロードするには、 をクリックします。

8. **レポートのダウンロード** ウィンドウが表示されたら、日付と時刻の範囲を選択します。



9. **レポートDL** をクリックします。

レポートの生成が完了すると、管理者のメールアドレスにダウンロードリンクが送信されます。 メールからPDFまたはCSV形式でレポートをダウンロードできます。

> **情報**
>
> - レポートにユーザーテンプレートを含めるには、**ユーザーテンプレート項目** を有効にし、希望するテンプレート項目を選択します。
> - レポートダウンロード用のメールを受信してから24時間以内にレポートをダウンロードできます。 期間が終了すると、ダウンロードできなくなります。
> - **アラートとレポート** で自動化されたスケジュールを設定することもできます。 詳細はアラートとレポートの設定をご参照ください。

レポートの作成とスケジュール設定

BioStar Airのレポートは、レポートの種類に応じてさまざまな画面で構成できます。 本書では、ユーザー、イベントログ、および変更ログのレポートを作成し、スケジュールする方法を案内します。

リポート構成に移動

レポートの種類によってアクセス経路が異なります。

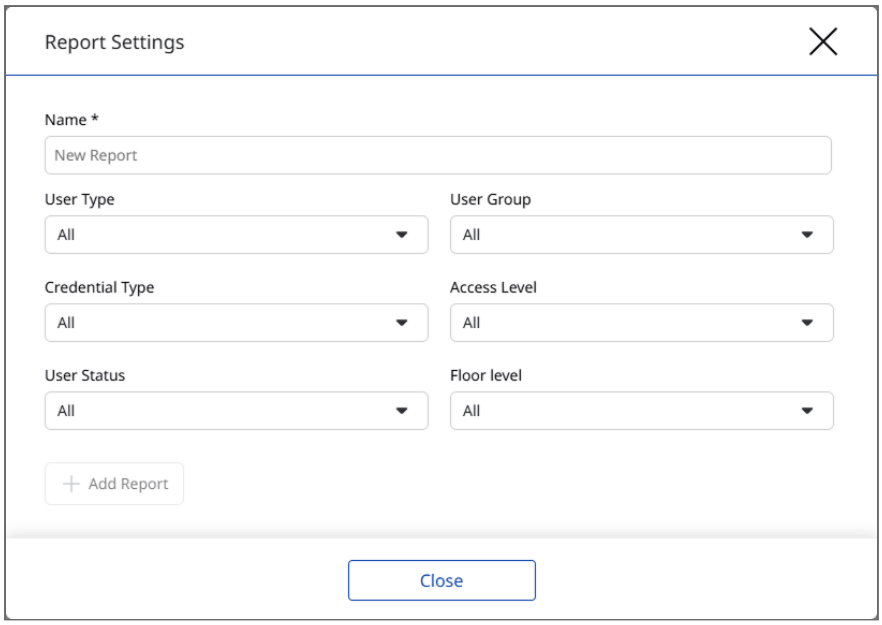
- ユーザー レポート： **ユーザー管理** → **ユーザー**
- イベントログ レポート： **モニタリング** → **イベントログ**
- 変更ログ レポート： **モニタリング** → **監査ログ**

上記のメニューの一覧上部のツールバーで、 をクリックします。 レポート設定画面に移動します。

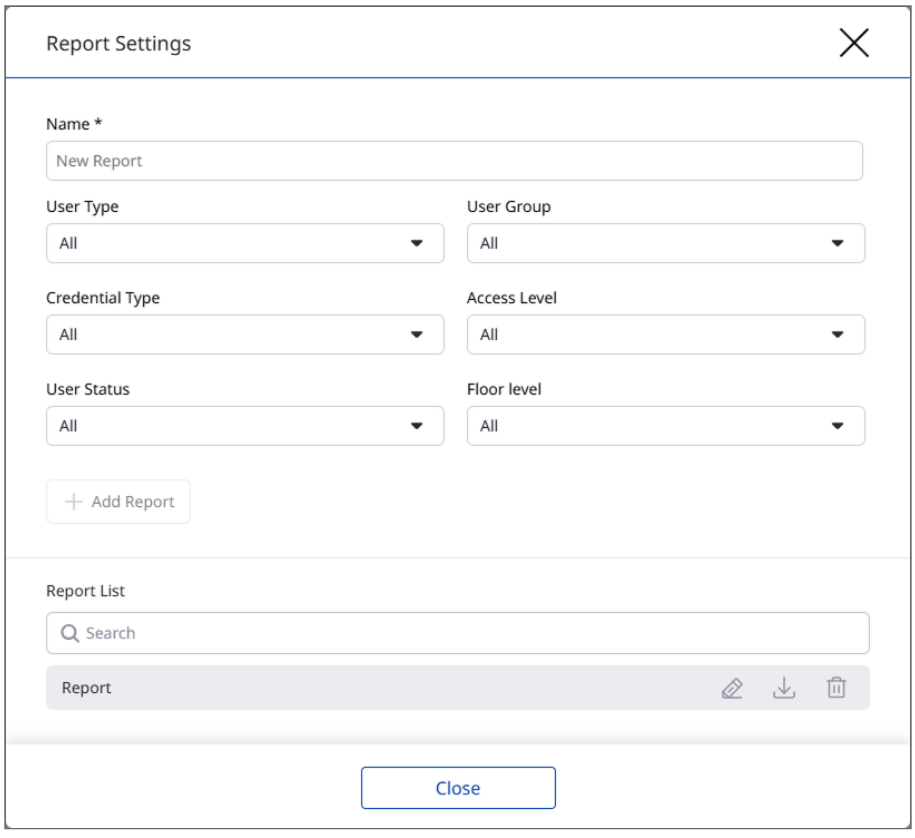
ユーザーレポートの構成

サイトに登録されているユーザーの状況を把握できるユーザーレポートを構成できます。

1. 画面左のサイドバーで **ユーザー管理** → **ユーザー** に移動します。
2. ユーザー一覧の上部にあるツールバーで、 をクリックします。
3. **レポート設定** ウィンドウが表示されたら、レポート名を入力します。



4. 各フィルターオプションでレポートに含める項目を選択します。
5. 作成したレポートを保存するには、**レポートの追加** をクリックします。
6. 下部に **レポートリスト** が作成され、管理者のメールにダウンロードリンクが送信されます。



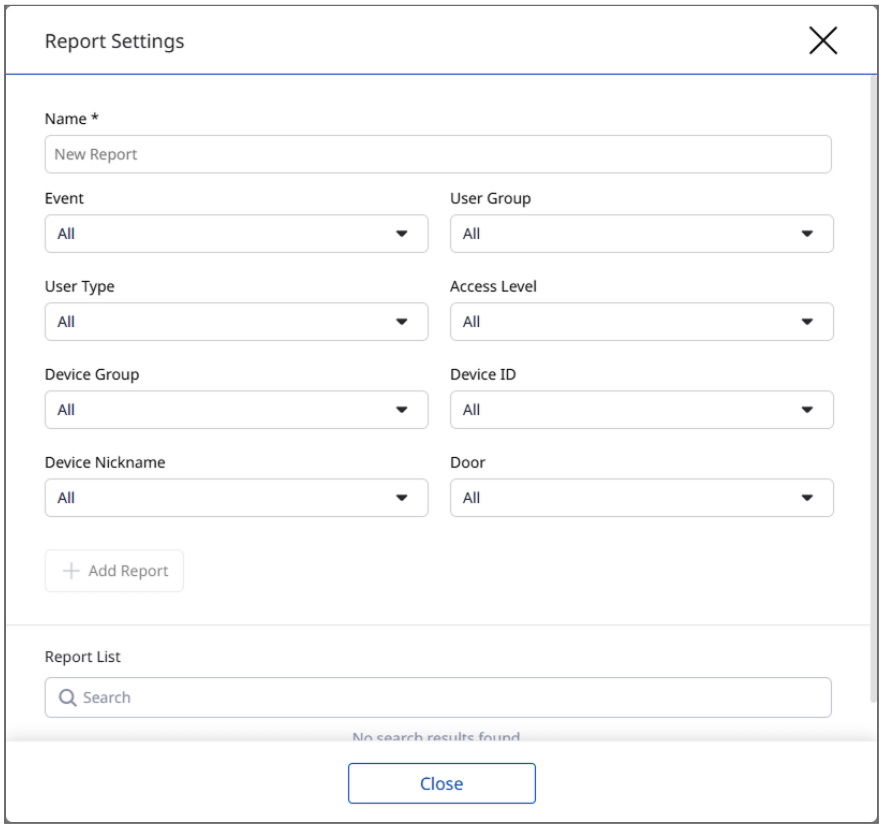
情報

- 作成したレポートを編集するには ボタンをクリックします。
- レポートをPDFまたはCSVファイルとしてエクスポートするには ボタンをクリックします。
- レポートを削除するには ボタンをクリックします。
- ユーザー管理の詳細については、ユーザー をご参照ください。

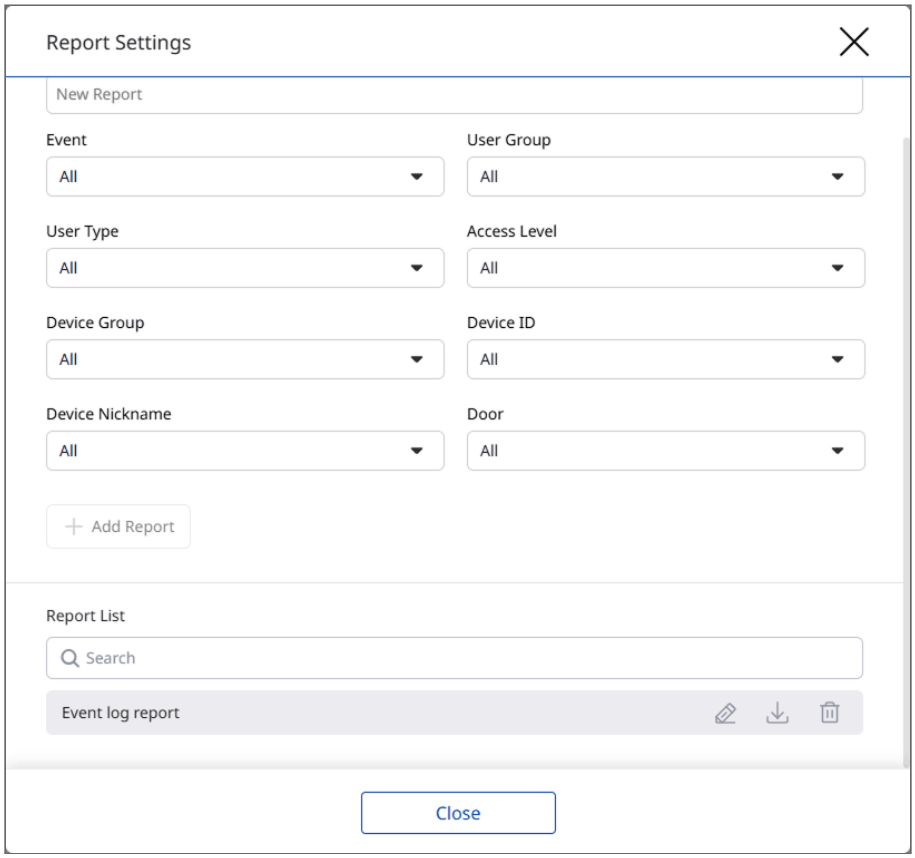
イベントログレポートの構成

サイトで発生したイベントログのレポートを構成できます。

1. 画面左のサイドバーで **モニタリング** → **イベントログ** に移動します。
2. ログ一覧の上部にあるツールバーで、 をクリックします。
3. **レポート設定** ウィンドウが表示されたら、レポート名を入力します。



4. 各フィルターオプションでレポートに含める項目を選択します。
5. 作成したレポートを保存するには、**レポートの追加** をクリックします。
6. 下部に **レポートリスト** が作成され、管理者のメールにダウンロードリンクが送信されます。



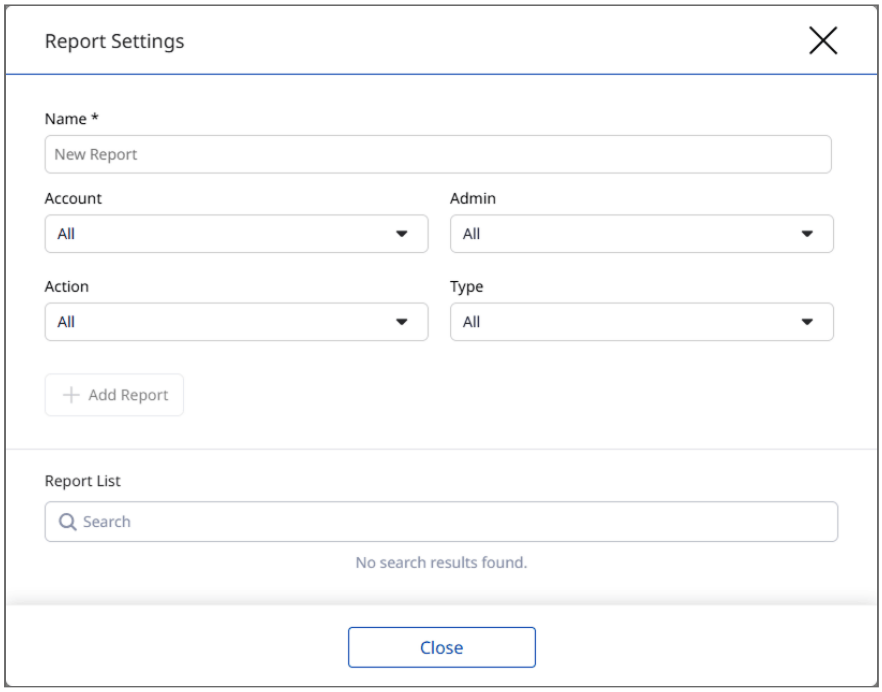
情報

- 作成したレポートを編集するには ボタンをクリックします。
- レポートをPDFまたはCSVファイルとしてエクスポートするには ボタンをクリックします。
- レポートを削除するには ボタンをクリックします。
- イベントログの詳細については、イベントログの使い方をご参照ください。

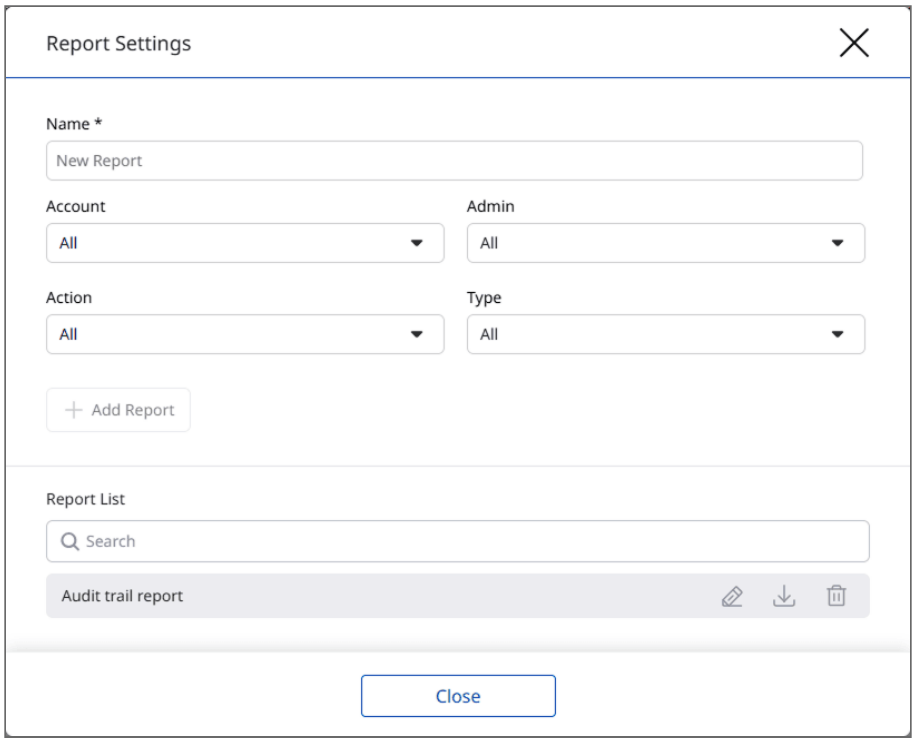
変更ログレポートの構成

管理者が行った変更に関する変更ログのレポートを構成できます。

1. 画面左のサイドバーで **モニタリング** → **監査ログ** に移動します。
2. ログ一覧の上部にあるツールバーで、 をクリックします。
3. **レポート設定** ウィンドウが表示されたら、レポート名を入力します。



4. 各フィルターオプションでレポートに含める項目を選択します。
5. 作成したレポートを保存するには、**レポートの追加** をクリックします。
6. 下部に **レポートリスト** が作成され、管理者のメールにダウンロードリンクが送信されます。



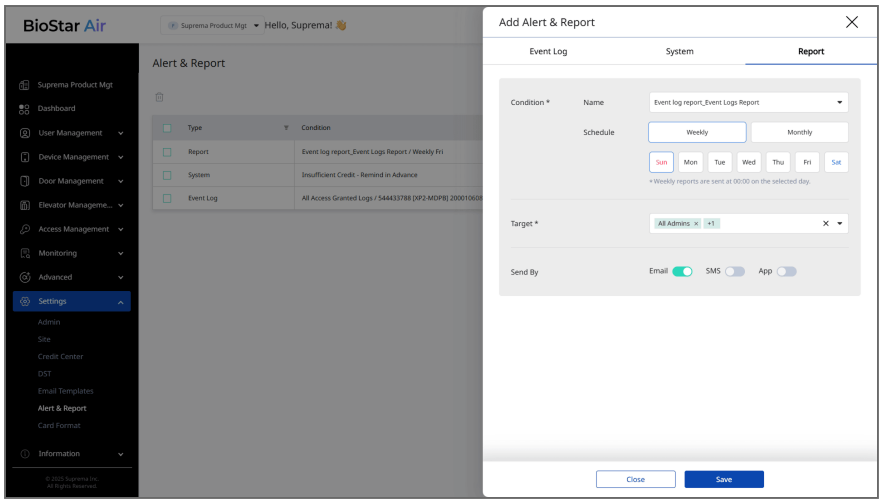
情報

- 作成したレポートを編集するには ボタンをクリックします。
- レポートをPDFまたはCSVファイルとしてエクスポートするには ボタンをクリックします。
- レポートを削除するには ボタンをクリックします。
- 変更ログの詳細については、変更ログの使い方をご参照ください。

レポート作成のスケジュール

特定の時間間隔でレポートを自動生成して管理者に送信できます。

1. 画面左のサイドバーで **設定** → **アラートとレポート** に移動します。
2. 画面右上の **アラートとレポートの追加** をクリックします。
3. **アラートとレポートの追加** パネルが表示されたら、**レポート** タブを選択します。



4. **条件** セクションの **名前** から作成するレポートの種類を選択します。
5. **スケジュール** でレポート作成の周期を選択します。
   - **毎週** または **毎月** を選択します。
   - レポートを送信する具体的な日付を選択します。
   - すべてのレポートは、選択した日の午前0時に送信されます。
6. **ターゲット** で通知を受け取る対象を選択します。
   - 特定の管理者レベルのすべての管理者
   - 個別の管理者
7. **送信者** で通知の送信手段を選択します。
   - レポートはメールでのみ送信できます。
   - SMSやアプリのプッシュ通知で送信することはできません。
8. 設定を保存するには、**保存** をクリックします。

情報

レポート生成のスケジュールの詳細については、アラートとレポートの設定 をご参照ください。

パートナー／導入管理者

BioStar Airのパートナーポータルは、流通契約を締結した付加価値リセラー（VAR）向けの専用プラットフォームです。 パートナーポータル上で顧客サイトを作成したり、クレジットを配布したり、フェデレーションサイトを構築して複数のサイトを一元管理できます。

SIPインターホン、IPカメラ、QRスキャナーなどの現場でのハードウェア設置やネットワーク構成の方法についてもご案内します。

パートナーポータルの使い方

BioStar Air パートナーポータルは付加価値再販業者（VAR）向けの専用ツールで、顧客サイトを管理し、クレジットを配分し、管理機能を効率的に監督できます。

パートナーポータルにログインすると、次の操作を行えます。

- 顧客向けの新しいサイトを作成します。
- 該当サイトにクレジットを割り当て、配布します。

> **情報**
>
> - パートナーポータルは付加価値再販業者（VAR）専用であり、サイト管理者やエンドカスタマー向けではありません。
> - 招待メールが届かない場合は迷惑メールフォルダを確認するか、パートナーポータル管理者に連絡してください。
> - 登録に使用したメールアドレスが正しいか確認してください。 後で変更できません。

> **ヒント**
> BioStar Air パートナーポータルの使い方に関するビデオガイドを視聴するには、以下の動画を参照してください。

パートナーポータルへのアクセス

パートナーポータルはウェブポータルでのみ提供されます。 次のリンクからアクセスできます。 https://partner.biostarair.com/

パートナーポータルの会員登録

1. 流通契約を締結すると、パートナーポータルの会員登録招待メールが届きます。
2. メール内の **サインアップ** リンクをクリックしてください。
3. プライバシーポリシーおよび利用規約を確認して同意してください。
4. メールが事前に入力された登録画面が表示されたら、必須情報を入力してください。
5. 会員登録プロセスを完了し、ポータルにログインしてください。

情報

- パートナーポータルは承認されたリセラー専用であり、サイト管理者または最終ユーザーはアクセスできません。
- メールの招待を受け取っていない場合は、迷惑メールフォルダを確認するか、パートナーポータル管理者に問い合わせてください。
- 登録に使用したメールアドレスが正しいか確認してください。 会員登録後は変更できません。

サイトの管理

パートナーポータルにログインすると、アカウントに紐づくサイトの一覧を確認できます。

- サイト名、国、割り当てられたクレジットなど、サイトの詳細を確認できます。
- 各サイトの月額費用を監視して、追加クレジットが必要な時期を判断してください。
- ユーザー数および登録済みデバイス数を追跡できます。
- 内部追跡用のメモを追加してください。

サイト詳細の編集

サイト一覧から詳細を編集するサイトをクリックしてください。 サイト編集画面で次の操作を行えます。

- サイトのタイムゾーンおよび国の情報を含む詳細を更新できます。
- サイトに関連するメモを追加または編集できます。
- 割り当てられたクレジット数を調整できます。
- サイトに追加の管理者を招待できます。
- 必要に応じてサイトを削除できます。

クレジット履歴の追跡

クレジット履歴 セクションではすべてのクレジット変動を確認できます。

- 特定期間のクレジット変動を確認するための期間を設定できます。
- 顧客サイトへの最近のクレジット追加を監視できます。

管理者の管理

管理者 セクションでは他のユーザーをパートナーポータルに招待できます。

1. 管理者レベルを選択してください。
2. 招待するユーザーのメールアドレスを入力してください。
3. 招待状を送信するには、**確認**をクリックしてください。

> **情報**
> エンドカスタマーはパートナーポータルに追加してはいけません。 サイト作成およびクレジット配分は、付加価値再販業者（Value-Added Reseller、VAR）のみが管理する必要があります。

役割と権限の理解

パートナーポータルには4つの権限レベルがあります。

- **オブザーバー**：サイト情報を閲覧できますが、変更はできません。
- **オペレーター**：新しいサイトを設定しクレジットを割り当てることはできますが、管理者権限の変更や新しい管理者の招待はできません。
- **アドミン**：他の管理者を招待および管理できますが、マスターレベルのユーザーを削除することはできません。
- **マスター**：ポータルに対する完全な管理権限を持ち、ユーザー管理、サイト作成、クレジット配分を含みます。 パートナーポータルアカウントを初めて有効化できるのはマスターレベルのみです。

> **情報**
> マスター管理者以外の権限を持つユーザーがポータルにアクセスするには、まずマスターアカウントを設定して有効化する必要があります。

フェデレーションサイトの管理

BioStar Airは**フェデレーションサイト**を作成し、親サイトから複数のサブサイトを円滑に管理できる機能を提供します。 この機能はマルチテナントビルや複数拠点を運営する組織に適しており、分散した入退室管理に対して集中管理を提供します。

BioStar Airのフェデレーションサイト機能を活用することで、管理者は複雑な環境の入退室を効果的に管理し、すべての利害関係者に対して安全でスケーラブルかつ簡素化された体験を提供します。

フェデレーションサイトとは？

フェデレーションサイトは、**プライマリサイト**が1つ以上の**サブサイト**を管理する階層構造をサポートします。 **フェデレーション管理者**と呼ばれるプライマリサイトの管理者は、BioStar Airの画面から直接サブサイトにアクセスして管理できます。

フェデレーションサイトは次のような状況で有用です。

マルチテナントビル

例えば、各フロアに異なる会社が入居している商業ビルでは、以下のように構成できます。

- ビル用の**マスターアカウント**
- 各テナント会社用の**サブアカウント**

この構成により、特定フロアへのアクセスが許可された従業員のみがアクセスできるようにして、ビル管理者の管理を簡素化できます。

複数拠点の組織

複数の場所にオフィスがある会社は、以下のように構成できます。

- **マスターアカウント**でグローバル設定を管理
- 各拠点用の**サブアカウント**を作成

例えば、世界中に10のオフィスがある企業は、フェデレーション構造を使って管理を簡素化できます。

フェデレーションサイトの設定

1 パートナーポータルにアクセス

アクセスURL: https://partner.biostarair.com

- BioStar Airのパートナーポータルはパートナーおよび導入業者のみが利用できます。
- 最終顧客がこの機能を設定するには導入業者にお問い合わせください。

2 プライマリサイトの作成

1. パートナーポータルにログインしてください。
2. をクリックし、でを選択します。
    - この手順はサイトを初めて設定する際に**必ず**実行する必要があります。
    - 通常のサイトは後からフェデレーションサイトに変更できません。
3. 同じ画面でフェデレーションサイト管理者を追加してください。
    - パートナーポータルで追加された**フェデレーションサイト管理者**は、プライマリサイトとすべてのサブサイトにアクセスできます。
    - BioStar Air上で追加された**一般管理者**は個別サイトのみ管理できます。

3 サブサイトの追加

1. プライマリサイトがフェデレーションサイトに設定されると、にサブサイトを作成するオプションが表示されます。
2. ボタンをクリックし、他のサイトと同様に構成してください。

重要な考慮事項

ユーザーおよびデバイス管理

- ユーザーとデバイスは各サブサイトごとに個別に追加する必要があります。
- デバイスは一度に1つのサイトにのみ登録できます。 プライマリサイトまたはサブサイトのいずれかを選択してください。

プライマリサイトの使用

- 一部の顧客はプライマリサイトをサブサイト管理のアクセスポイントとしてのみ使用し、プライマリサイトにユーザーやデバイスを登録しません。
- **例1:** 3つの支社オフィスを持つ企業は、デバイスを持たないプライマリサイトを設定し、各支社ごとにサブサイトを作成します。
- **例2:** 本社と3つの支社を持つ会社は、本社（プライマリサイト）でユーザーとデバイスを登録し、支社用のサブサイトを設定します。

請求

- 請求はサイトごとに登録されたデバイス（リーダー）の数に基づいて計算されます。
- 登録されたデバイスがないプライマリサイトを作成する際に追加料金は発生しません。

パートナー管理者を招待する

パートナーポータルでパートナー管理者アカウントの招待、役割の割り当て、権限の管理方法を案内します。 パートナー管理者は顧客サイトへのアクセス権を制御して、セキュリティと運用効率を確保できます。

パートナー管理者はオブザーバー(Observer)、オペレーター(Operator)、管理者(Administrator)、マスター(Master)の4つの役割のいずれかに割り当てられ、各役割に応じてアクセス権が異なります。 このドキュメントでは各役割の権限差を比較し、管理者アカウントの招待から権限管理、アカウントのロック/解除、削除までの全工程を段階的に案内します。

管理者の役割と権限

パートナーポータルでは管理者に以下の4つの役割のいずれかを割り当てることができます。

- **オブザーバー**：サイト情報を閲覧できますが、変更はできません。
- **オペレーター**：新しいサイトを設定しクレジットを割り当てることはできますが、管理者権限の変更や新しい管理者の招待はできません。
- **アドミン**：他の管理者を招待および管理できますが、マスターレベルのユーザーを削除することはできません。
- **マスター**：ポータルに対する完全な管理権限を持ち、ユーザー管理、サイト作成、クレジット配分を含みます。 パートナーポータルアカウントを初めて有効化できるのはマスターレベルのみです。

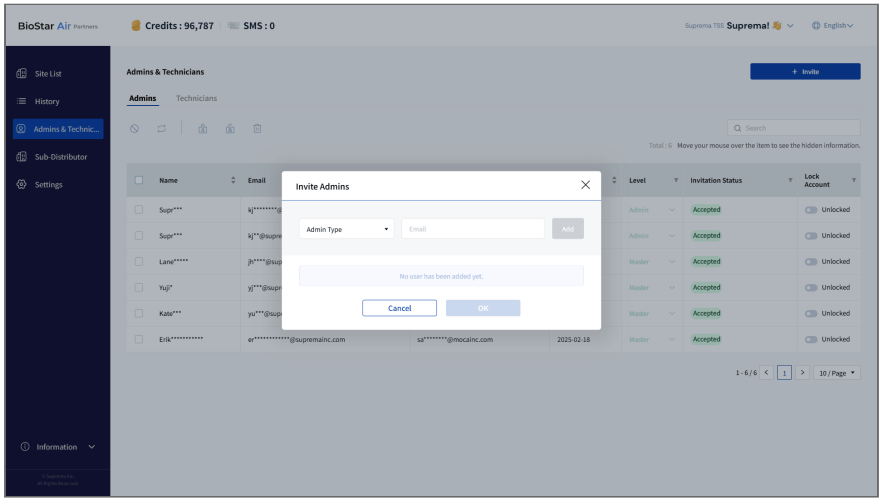
> **情報**
> マスター管理者以外の権限を持つユーザーがポータルにアクセスするには、まずマスターアカウントを設定して有効化する必要があります。

管理者の招待

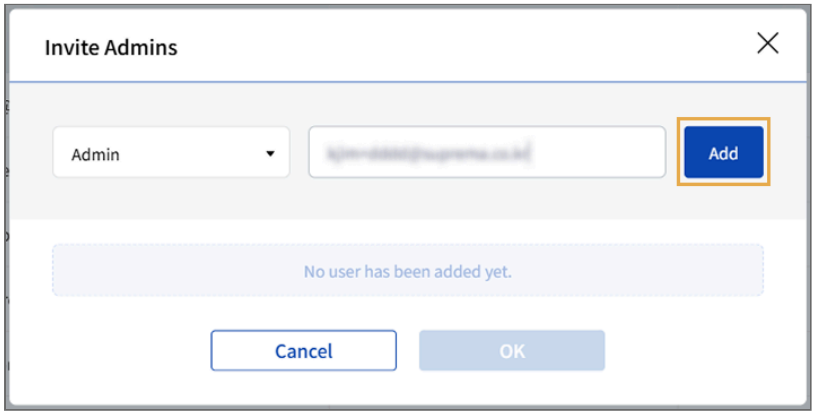
管理者を招待するには、次の手順に従います。

1. パートナーポータルに **アドミン** 権限以上のアカウントでログインします。
2. 画面左のサイドバーで をクリックします。

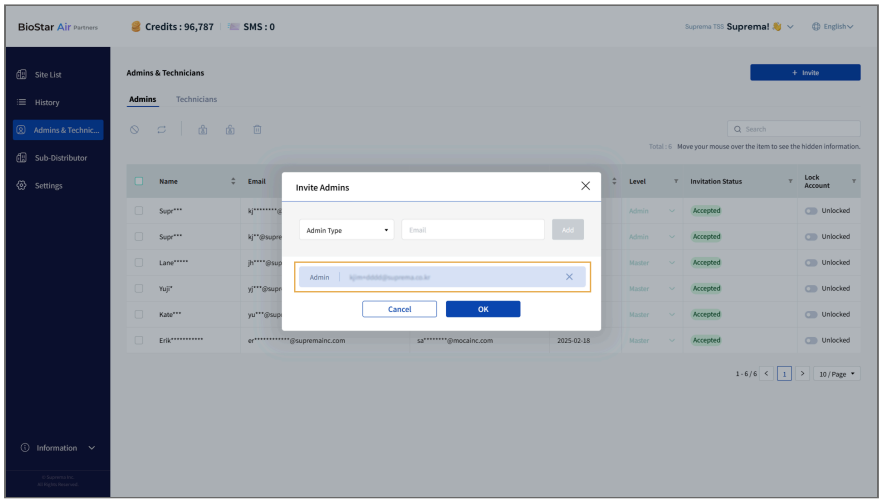
3. 画面右上の ボタンをクリックします。
4. ウィンドウが表示されたら、 で招待する管理者の役割を選択します。



5. 招待する管理者のメールアドレスを入力します。
6. ボタンが有効になったらクリックします。



7. 追加した管理者はメールアドレス入力欄の下に表示されます。 さらに管理者を招待するには、手順4～6を繰り返します。



8. すべての管理者を追加したら、**OK** ボタンをクリックします。
9. 送信確認メッセージが表示されたら、**確認** ボタンをクリックします。

> **情報**
> パートナーポータルに管理者アカウントを招待しても、各サイトへの招待は別途行う必要があります。

招待状況

管理者を招待した後、管理者一覧で招待したアカウントの招待状況を確認できます。

登録待ち

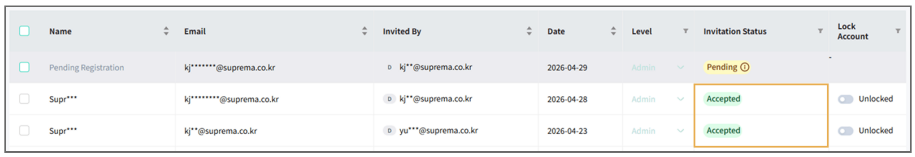
招待された管理者がメールで招待を承諾してアカウントを有効化するまでは、 状態です。 招待された管理者はメール内のリンクをクリックしてアカウントを登録するか、ログインしてパートナーポータルにアクセスできます。



> **情報**
> 招待された管理者は最大7日間招待を承諾できます。7日を過ぎると招待は期限切れとなり、 状態に変更されます。 招待が失効した場合、該当アカウントが再登録できるよう招待リンクを再送できます。 招待リンクの再送の詳細は 招待リンクの再送 を参照してください。

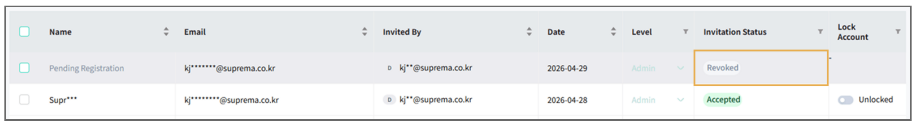
登録完了

招待された管理者がメールの招待を承諾して登録を完了すると、招待状況は に変更されます。



招待の取り消し状態

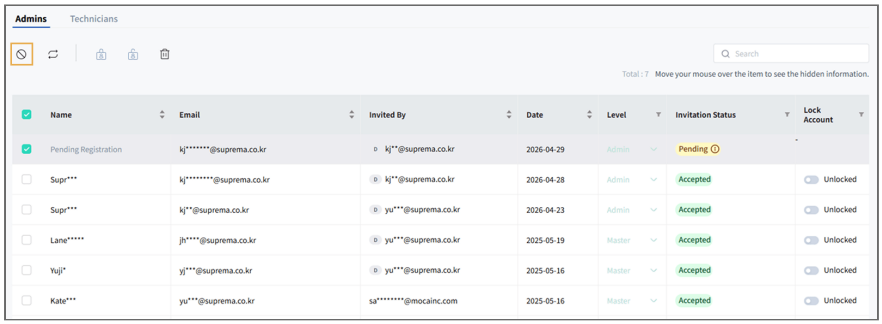
招待した管理者のメールアドレスを誤って入力した場合や、もはや管理者招待が不要になった場合、招待を取り消せます。 招待を取り消すと、招待状況は に変更されます。 管理者招待の取消しの詳細は 招待取り消し を参照してください。



招待取り消し

パートナーが招待した管理者のメールアドレスを誤って入力した場合や、もはや招待が不要な場合は、招待を取り消せます。 招待を取り消すと、該当ユーザーは招待リンクから登録できなくなります。

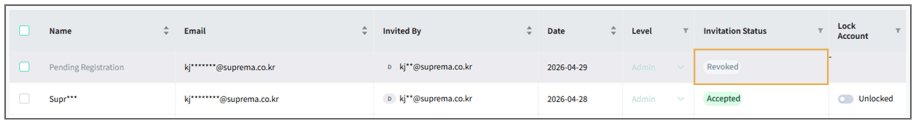
1. 管理者一覧で招待状況が の管理者のチェックボックスをクリックします。 1人以上の管理者を選択できます。
2. 管理者一覧の左上にある ⃠ ボタンをクリックします。



状態が の管理者のみ招待を取り消せます。

3. ポップアップメッセージが表示されたら内容を確認し、 ボタンをクリックしてください。
4. 招待取り消しの成功メッセージが表示されたら、**閉じる** ボタンをクリックしてください。

管理者一覧で招待を取り消した管理者の招待状況は に変更されます。



招待リンクの再送

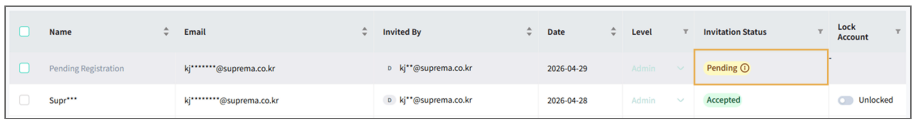
招待された管理者が招待メールを受け取っていない、メールを紛失した、または招待リンクが期限切れになった場合は、招待リンクを再送できます。

1. 管理者一覧で招待状況が 、、 のいずれかの管理者のチェックボックスをクリックします。 1人以上の管理者を選択できます。
2. 管理者一覧の左上にある ボタンをクリックします。



3. ポップアップメッセージが表示されたら内容を確認し、 ボタンをクリックしてください。
4. 招待リンク再送信の成功メッセージが表示されたら、**閉じる** ボタンをクリックしてください。

管理者一覧で招待リンクを再送した管理者の招待状況は に変更されます。



管理者の管理

招待された管理者がメールの招待を承諾して登録を完了すると、管理者一覧で当該管理者を管理できます。 管理者のアカウントをロック/解除したり、権限を変更したりできます。 もはや管理者が不要な場合は、管理者アカウントを削除することもできます。

管理者アカウントのロック/解除

メール招待を承諾して登録を完了した管理者は、 オプションでアカウントをロックまたは解除できます。 アカウントをロックすると管理者はパートナーポータルにログインできなくなりますが、アカウント情報は保持され、必要な時に再度有効化できます。

ロック状態の管理者は 列が と表示され、解除された管理者は と表示されます。



情報

- 登録を完了した管理者のアカウントは、デフォルトでロック解除されています。
- **アドミン** 権限以上のアカウントはロック/解除できません。

個別の管理者ロック/ロック解除

管理者一覧で 列のトグルボタンをクリックして、個別の管理者アカウントをロックまたは解除できます。

1. 管理者一覧で 列のトグルボタンをクリックします。

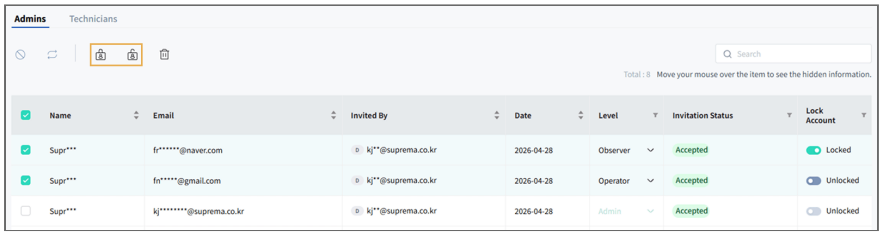


2. ポップアップメッセージが表示されたら内容を確認し、**確認** ボタンをクリックします。

複数管理者のロック/ロック解除

管理者一覧で複数の管理者アカウントを選択して、一括でロックまたは解除できます。

1. 管理者一覧でロックまたはロック解除する管理者のチェックボックスをクリックします。 1人以上の管理者を選択できます。
2. 画面左上の または ボタンをクリックします。

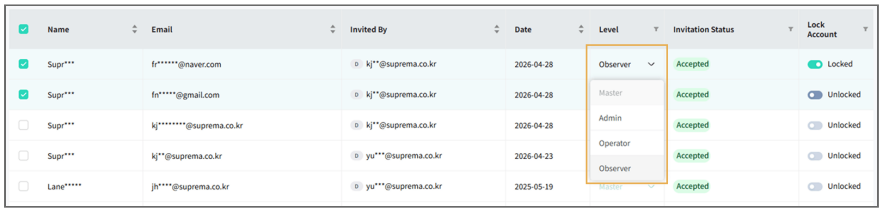


3. ポップアップメッセージが表示されたら内容を確認し、 ボタンをクリックしてください。
4. アカウントのロック/解除の成功メッセージが表示されたら、**閉じる** ボタンをクリックします。

管理者の権限変更

管理者の権限を変更できます。 管理者権限の詳細は 管理者の役割と権限 を参照してください。

1. 管理者一覧で権限を変更する管理者の 列をクリックします。



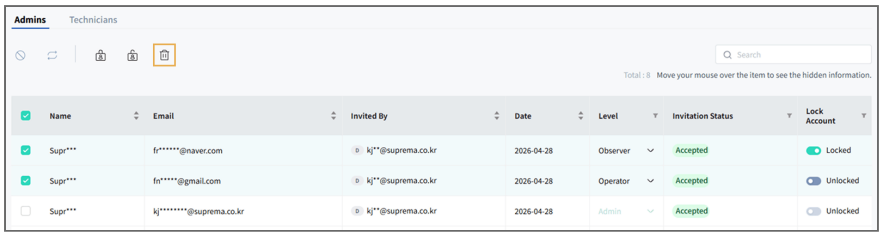
2. 一覧から変更する権限を選択します。
3. ポップアップメッセージが表示されたら、**確認** ボタンをクリックします。

管理者一覧で当該ユーザーの権限が変更されます。

管理者アカウントの削除

管理者が不要になった場合、管理者アカウントを削除できます。 管理者アカウントを削除すると、該当管理者はパートナーポータルにログインできず、アカウント情報は完全に削除され復元できません。

1. 管理者一覧で削除する管理者のチェックボックスをクリックします。 1人以上の管理者を選択できます。
2. 画面左上の ボタンをクリックします。



3. ポップアップメッセージが表示されたら内容を確認し、**確認** ボタンをクリックします。
4. アカウント削除の成功メッセージが表示されたら、**閉じる** ボタンをクリックします。

削除した管理者アカウントは管理者一覧に表示されなくなります。

サイト管理者を招待する

パートナーは顧客サイトに管理者を招待し、権限を設定できます。 各管理者ごとに必要なアクセス権レベルを細分化して管理し、顧客サイトのセキュリティと運用効率を確保できます。

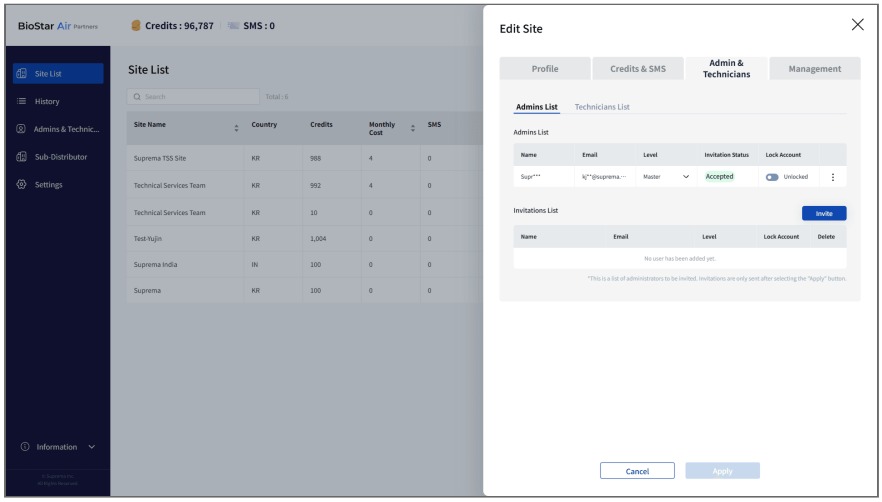
> **情報**
>
> - サイトの管理者権限および役割の詳細は 管理者アカウントおよび役割の管理 を参照してください。
> - BioStar Air ポータルでの管理者招待および役割設定の詳細は 管理者アカウントおよび役割の管理 を参照してください。

サイトに管理者を招待

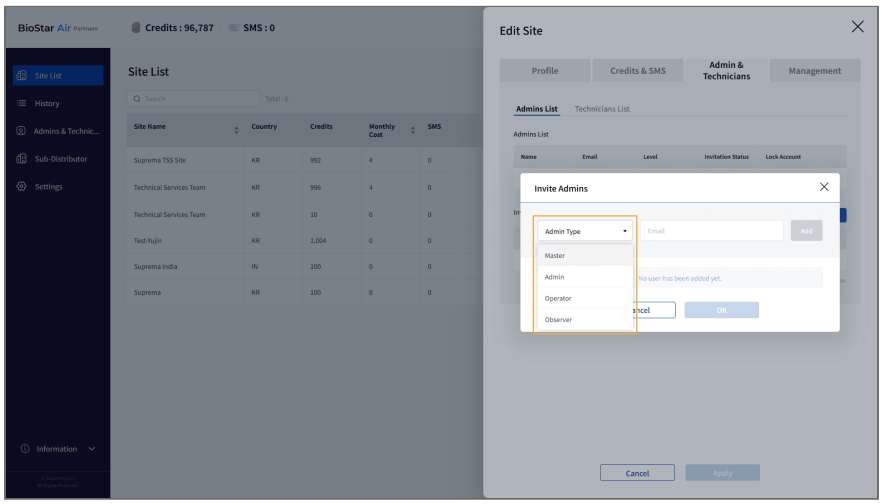
パートナーポータルで顧客サイトに管理者を招待し、権限を設定する方法を案内します。

1. パートナーポータルに **アドミン** 権限以上のアカウントでログインします。
2. 画面左のサイドバーで をクリックしてください。

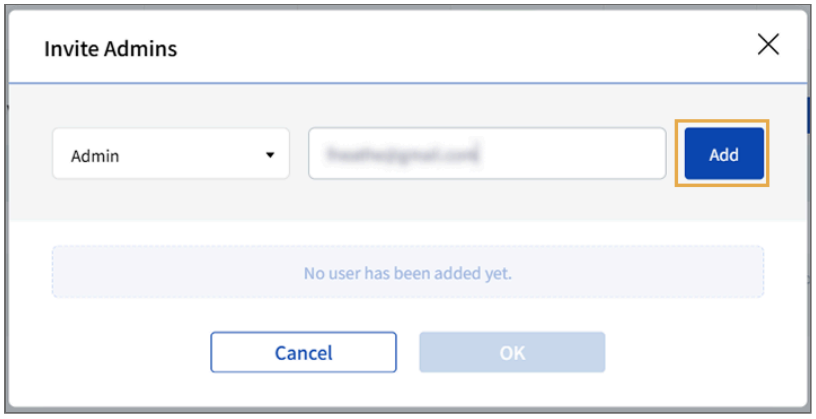
3. サイト一覧から管理者を割り当てるサイトをクリックしてください。
4. パネルが表示されたら、 → タブを順にクリックします。



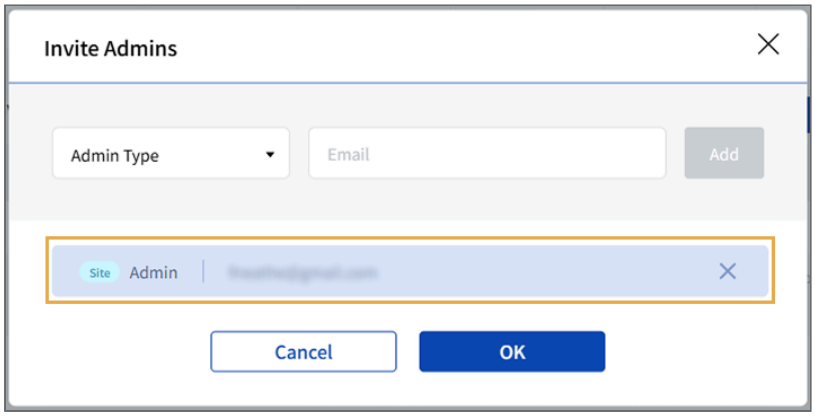
5. をクリックしてください。
6. ウィンドウが表示されたら、 で招待する管理者の役割を選択します。



7. 招待する管理者のメールアドレスを入力します。
8. ボタンが有効になったらクリックします。



9. 追加した管理者はメールアドレス入力欄の下に表示されます。 追加で管理者を招待するには、6~8の手順を繰り返してください。



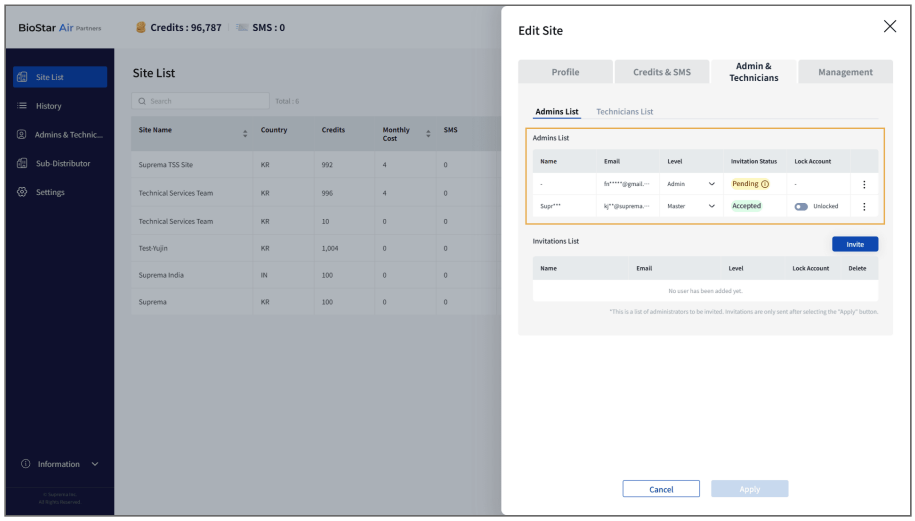
10. すべての管理者を追加したら、**OK** ボタンをクリックします。
11. で追加した管理者を確認した後、招待メールを送信するにはボタンをクリックします。
12. 成功メッセージが表示されたら、**確認** ボタンをクリックしてください。

招待状況の確認

サイトに招待された管理者の招待ステータスを確認できます。 招待された管理者がメールを受け入れるまで、招待状態は と表示されます。 招待された管理者は最大7日間招待を承諾できます。7日を過ぎると招待は期限切れとなり、 状態に変更されます。

1. サイト一覧から管理者を招待したサイトをクリックしてください。
2. パネルが表示されたら、 → タブを順にクリックします。
3. で招待状況を確認できます。

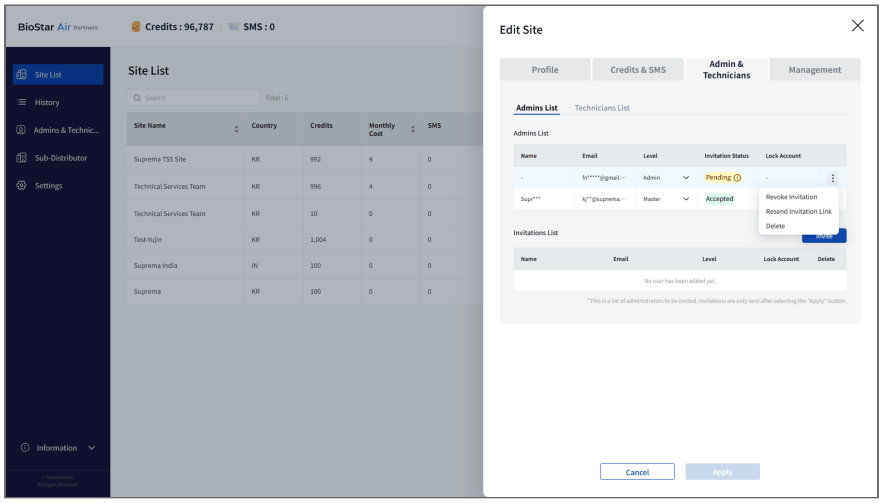
管理者がサイトへの登録を完了すると、 から に状態が変更されます。



招待の取り消し

サイトに招待した管理者のメールアドレスを誤って入力した場合や、もはや管理者の招待が不要な場合は、招待を取り消せます。

1. サイト一覧から管理者を招待したサイトをクリックしてください。
2. パネルが表示されたら、 → タブを順にクリックします。
3. の 状態の管理者の右端にある ⋮ ボタンをクリックします。



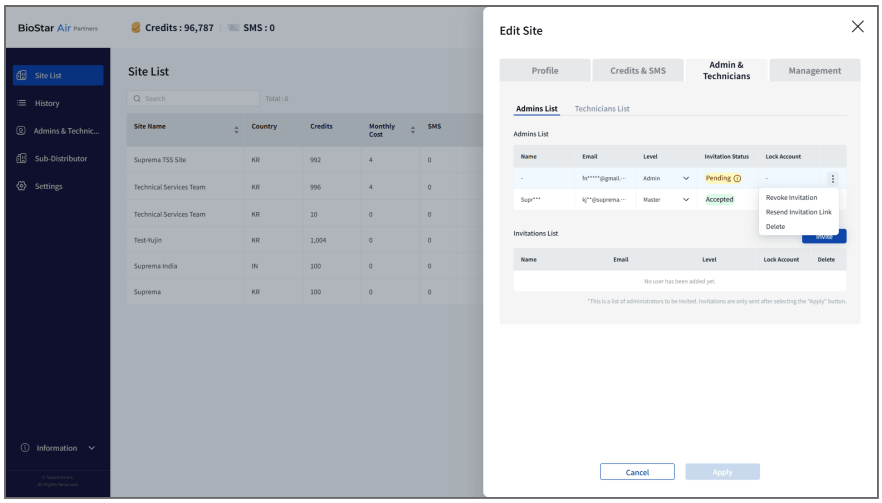
4. ポップアップメニューで をクリックしてください。
5. ポップアップメッセージが表示されたら内容を確認し、 ボタンをクリックしてください。
6. 招待取り消しの成功メッセージが表示されたら、**閉じる** ボタンをクリックしてください。

招待を取り消した管理者は、招待状態が から に変わります。

招待リンクの再送信

サイトに招待した管理者が招待メールを受け取っていないか紛失した場合、招待リンクを再送できます。

1. サイト一覧から管理者を招待したサイトをクリックしてください。
2. パネルが表示されたら、 → タブを順にクリックします。
3. から または 、 状態の管理者の右端にある ⋮ ボタンをクリックします。

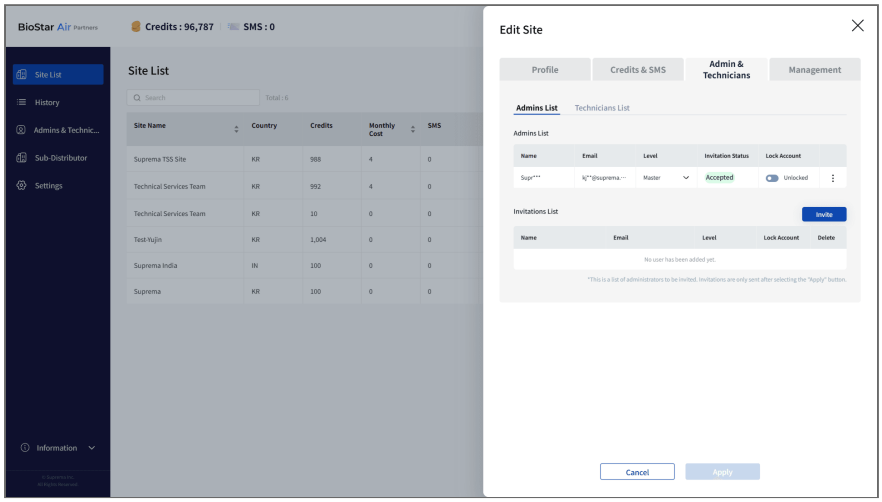


4. ポップアップメニューで をクリックしてください。
5. ポップアップメッセージが表示されたら内容を確認し、 ボタンをクリックしてください。
6. 招待リンク再送信の成功メッセージが表示されたら、**閉じる** ボタンをクリックしてください。

管理者アカウントのロック/解除

サイトに割り当てられた管理者アカウントをロックまたは解除できます。

1. 画面左のサイドバーで をクリックしてください。
2. サイト一覧で管理者のアクセスを管理するサイトをクリックしてください。
3. パネルが表示されたら、 → タブを順にクリックします。

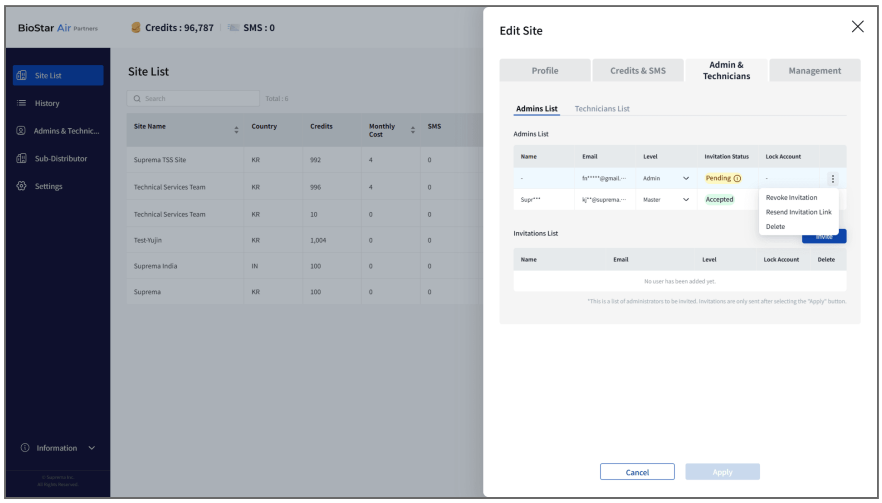


4. で管理者アカウントをロックまたは解除するには、列のトグルボタンをクリックしてください。
5. 変更を適用するには、下部の ボタンをクリックします。

管理者の削除

サイトに招待された管理者のアカウントを削除できます。 管理者のアカウントが削除されると、当該管理者はサイトにログインできず、サイトへのアクセス権が完全に削除されます。 管理者アカウントは削除後に復元できません。

1. サイト一覧から管理者を招待したサイトをクリックしてください。
2. パネルが表示されたら、 → タブを順にクリックします。
3. で削除する管理者の右端にある ⋮ ボタンをクリックします。



4. ポップアップメニューで **削除** をクリックしてください。

5. ポップアップメッセージが表示されたら内容を確認し、**確認** ボタンをクリックします。
6. 管理者削除の成功メッセージが表示されたら、**閉じる** ボタンをクリックしてください。

パートナー技術者の管理

技術者アカウントを使用することで、パートナーや設置担当者は管理者アカウントを共有せずに顧客サイトをサポートできます。 パートナーはパートナーポータルで技術者を招待し、特定のサイトに割り当てます。 割り当て後、顧客およびサイト管理者はBioStar Air管理者ポータルで技術者のサイト権限を有効化または更新できます。 これによりパートナーのサポートアクセスを制御し、監査記録を実装し、必要なサイトにのみ制限できます。

技術者管理の利点

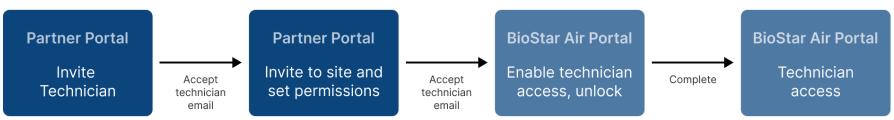
技術者アカウントは、複数の顧客サイトでシステムの設置、保守、技術サポートを行う専門担当者向けに設計されています。 パートナーは各技術者の役割と権限レベルを定義し、次のことを実行できます。

- **セキュリティ強化**：共有管理者アカウントを排除し、不正アクセスのリスクを低減
- **コンプライアンス**：個人情報保護規則の遵守、ユーザーデータへのアクセス除外オプション
- **効率的な管理**：複数サイトにわたる個別の技術者活動の追跡と監査
- **柔軟な権限管理**：技術者ごと、サイトごとの細分化された権限設定

制限事項

- **パートナーポータルとBioStar Airポータルは別アカウントが必要**：各ポータルで別途サインアップが必要です。 パスワードは各ポータル間で同期されません。
- **有効期限や時間ベースのアクセス制御なし**：技術者のアクセスは自動的に無効になりません。 サイト管理者が手動でロック処理または削除する必要があります。
- **権限が固定**：4つの事前定義された権限レベルのみを提供します。 カスタムの役割やより細かい権限分割は作成できません。
  - **なし / デバイスのみ / ユーザーを完全に除外 / ユーザーを完全に含む**
- **技術者の割り当てには顧客側の有効化が必要**：パートナーが割り当てた技術者はサイト管理者がロック解除するまでアクセスできません。 指示が不明確だと、サポートや設置が遅れることがあります。
- **一括割り当てなし**：技術者はサイトごとに個別に割り当てる必要があります。
- **技術者と管理者の役割で同一メールは使用不可**：パートナーポータルで既に技術者として登録されているメールは管理者として招待できません。 役割を変更する場合、既存アカウントを削除してから新しい役割で再招待する必要があります。

全体のプロセス



パートナーポータルに技術者を招待する

技術者アカウントにより、共有管理者アカウントなしでパートナーや施工業者に限定的なサイトアクセス権を付与できます。 技術者はパートナーポータルで集中管理され、各サイトごとに個別に割り当てられます。

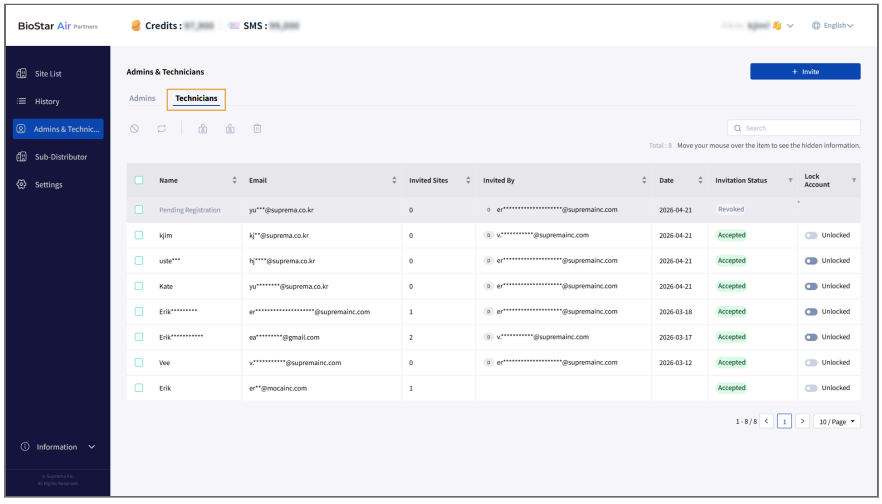
技術者アカウント使用の主な利点

- **セキュリティ強化**：共有管理者アカウントを排除し、不正アクセスのリスクを低減
- **コンプライアンス**：個人情報保護規則（GDPR等）の準拠が可能、ユーザーデータへのアクセス除外オプションを提供
- **アクセス制御**：機器アクセスから完全な管理者権限まで、細かい権限設定が可能
- **監査追跡性**：監査ログに個々の技術者の操作が記録され、責任を追跡できます
- **効率性の向上**：ログイン競合なしで複数サイトに技術者を割り当て・管理できます
- **迅速な解除**：技術者のアクセス権をいつでも即座に取り消せます

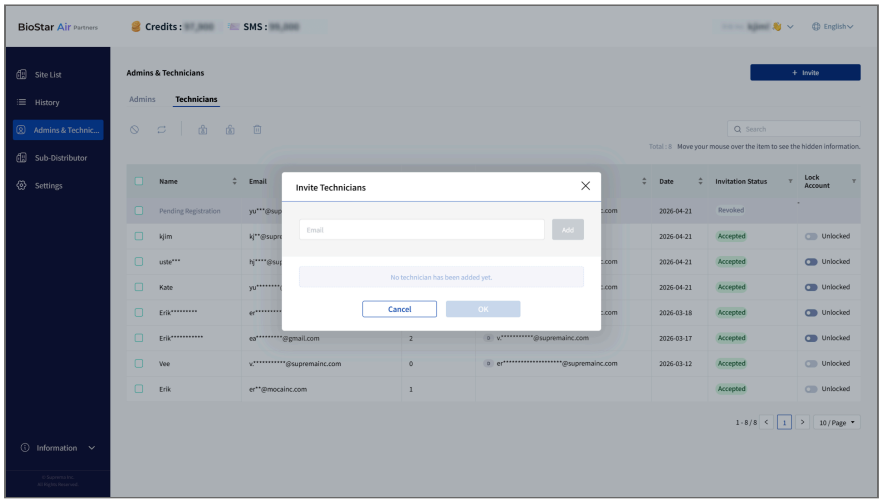
技術者の招待

サイトへのアクセス権を付与する前に、パートナーは技術者を招待して技術者アカウントを作成する必要があります。 技術者アカウントはメールアドレスを基に作成され、招待された技術者はメールで招待を受け入れてアカウントを有効化できます。

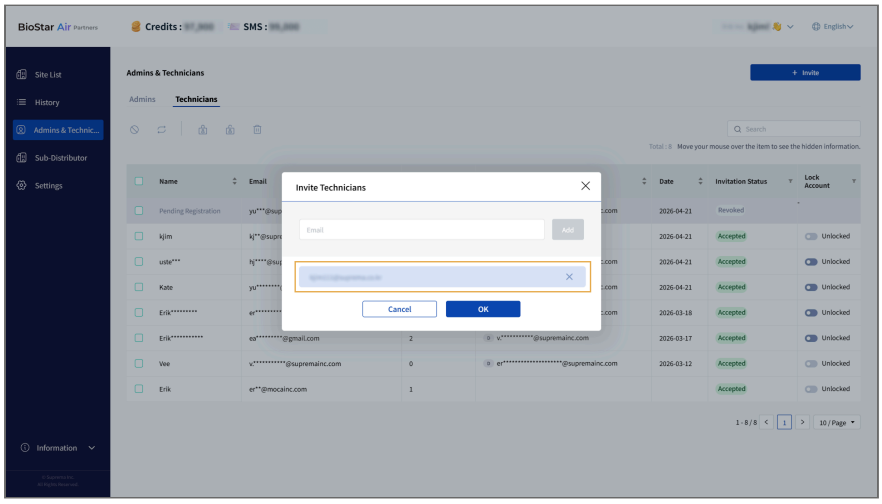
1. パートナーポータルにログインしてください。
2. 画面左のサイドバーで をクリックします。
3. タブをクリックします。



4. 画面右上の ボタンをクリックします。
5. ウィンドウが表示されたら、招待する技術者のメールアドレスを入力します。



6. ボタンが有効になったらクリックします。
7. 追加した技術者はメールアドレス入力欄の下に表示されます。 技術者を追加で招待するには、手順5～6を繰り返します。



8. すべての技術者を追加したら、**OK** ボタンをクリックします。
9. 送信確認メッセージが表示されたら、**確認** ボタンをクリックします。

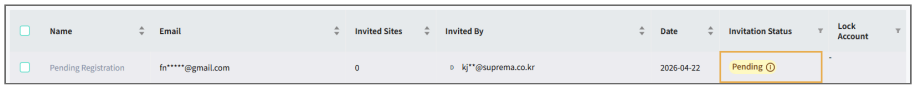
> **情報**
>
> - パートナーポータルに技術者アカウントを招待しても、各サイトへの招待は別途行う必要があります。 サイトへの技術者招待の詳細は サイトに技術者を割り当てる を参照してください。
> - 招待メール経由で登録した技術者はパートナーポータルにログインできますが、すべてのメニューへのアクセスは制限されます。 技術者は自身のアカウントのパスワード変更・アカウント削除・言語設定のみ利用できます。

招待状況

パートナーは技術者を招待後、技術者一覧で招待状況を確認できます。

登録待ち

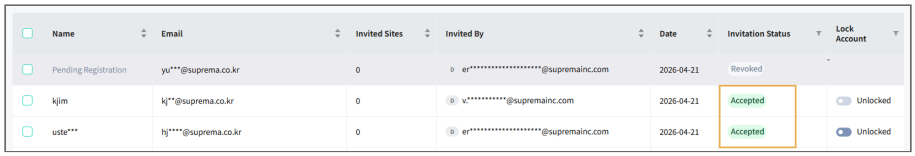
招待された技術者がメールを承諾するまでは、招待状況は と表示されます。 招待された技術者は、メール内のリンクをクリックしてアカウントを登録するか、ログインしてパートナーポータルにアクセスできます。



> **情報**
>
> 招待された技術者は最大7日間招待を承諾できます。7日を過ぎると招待は期限切れとなり、 状態に変更されます。 招待が期限切れになった場合、技術者が再度登録できるように招待リンクを再送できます。 招待リンクの再送の詳細は 招待リンクの再送 を参照してください。

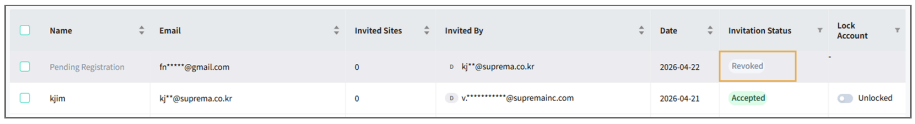
登録完了

技術者がメールの招待を受け入れて登録を完了すると、招待状況が に変更されます。



招待の取り消し状態

招待された技術者のメールアドレスを誤入力した場合や問題が解決して技術者の招待が不要になった場合、パートナーは技術者の招待を取り消せます。 招待状況が に変更されます。 技術者招待の取り消しの詳細は 招待取り消し を参照してください。



招待取り消し

パートナーが招待した技術者のメールアドレスを誤入力した場合や問題が解決して技術者の招待が不要になった場合、招待を取り消せます。 招待を取り消すと、該当ユーザーは招待リンクから登録できなくなります。

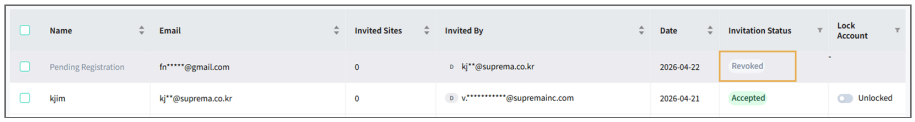
1. 技術者一覧で招待状況が の技術者のチェックボックスをクリックします。 1人以上の技術者を選択できます。
2. 技術者一覧の左上にある ボタンをクリックします。



> 状態の技術者のみ招待を取り消せます。

3. ポップアップメッセージが表示されたら内容を確認し、 ボタンをクリックしてください。
4. 招待取り消しの成功メッセージが表示されたら、**閉じる** ボタンをクリックしてください。

技術者一覧で招待を取り消した技術者の招待状況は に変更されます。



招待リンクの再送

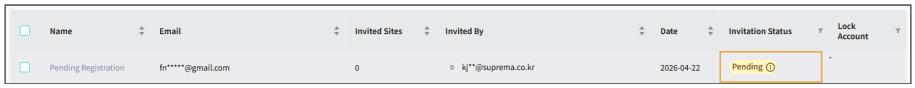
招待された技術者が招待メールを受け取っていない、またはメールを紛失した、招待リンクが期限切れの場合は、招待リンクを再送できます。

1. 技術者一覧で招待状況が 、または 、 の技術者のチェックボックスをクリックします。 1人以上の技術者を選択できます。
2. 技術者一覧の左上にある ボタンをクリックします。



3. ポップアップメッセージが表示されたら内容を確認し、 ボタンをクリックしてください。
4. 招待リンク再送信の成功メッセージが表示されたら、**閉じる** ボタンをクリックしてください。

技術者一覧で招待リンクを再送した技術者の招待状況は に変更されます。



技術者管理

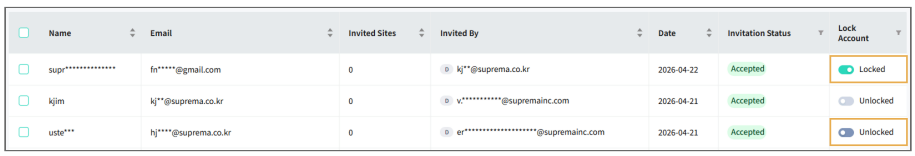
招待された技術者がメールの招待を受け入れて登録を完了した後、パートナーは技術者一覧で次の項目を管理できます。

- 技術者アカウントのロックまたは解除
- サイトへのアクセス権の変更
- 不要な技術者アカウントの削除

技術者アカウントのロック/解除

パートナーは オプションで技術者アカウントをロックまたは解除できます。 アカウントをロックすると、技術者はパートナーポータルおよび割り当てられたサイトにログインできません。 アカウント情報は保持されるため、必要なときに再度有効化できます。

ロック状態の技術者は 列が と表示され、解除された技術者は と表示されます。

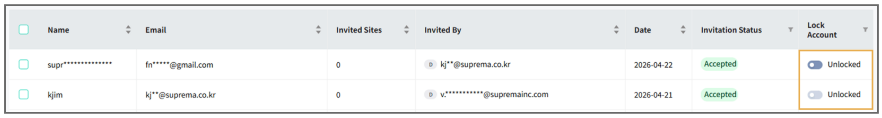


> **情報**
>
> - 登録完了した技術者のアカウントは、デフォルトでロック解除されています。
> - パートナーポータルの管理者アカウントが一部サイトで技術者のアクセス権を持っていても技術者一覧に表示されることがありますが、当該管理者アカウントは技術者一覧でロックまたは解除できません。

個別の技術者のロック/解除

列のトグルボタンをクリックして、個々の技術者アカウントをロックまたは解除できます。

1. 列のトグルボタンをクリックします。

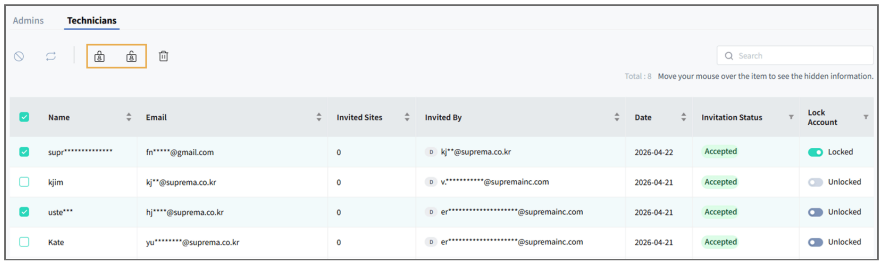


2. ポップアップメッセージが表示されたら内容を確認し、 ボタンをクリックしてください。
3. アカウントのロック/解除の成功メッセージが表示されたら、**閉じる** ボタンをクリックします。

複数の技術者のロック/解除

技術者一覧で複数の技術者アカウントを選択して一括でロックまたは解除できます。

1. 技術者一覧でロックまたは解除する技術者のチェックボックスをクリックします。 1人以上の技術者を選択できます。
2. 画面左上の または ボタンをクリックします。

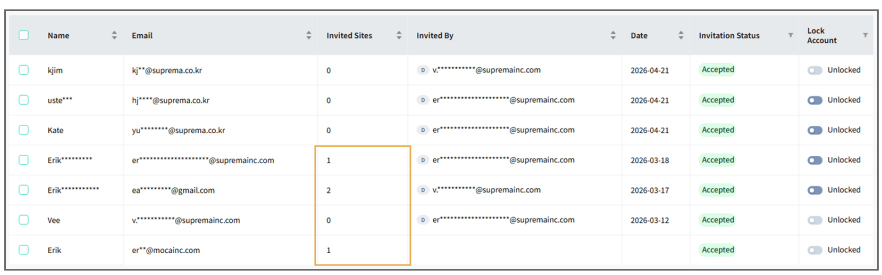


3. ポップアップメッセージが表示されたら内容を確認し、 ボタンをクリックしてください。
4. アカウントのロック/解除の成功メッセージが表示されたら、**閉じる** ボタンをクリックします。

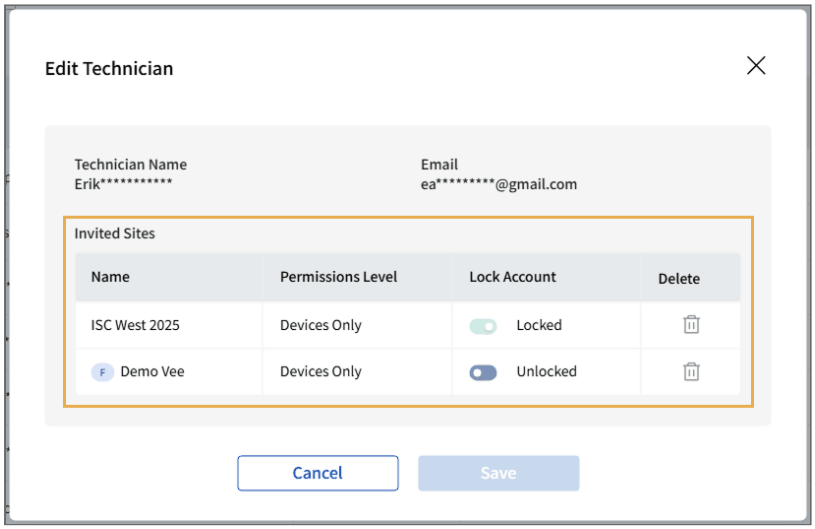
サイトアクセス権の編集

技術者のサイトアクセス権を変更できます。

1. 技術者一覧の 列で1つ以上のサイトがある技術者をクリックします。



2. ウィンドウが表示されたら、 で技術者が招待されたサイト一覧を確認します。



3. 列のトグルボタンをクリックして、サイトアクセスを許可またはブロックします。
4. 変更を保存するには、 ボタンをクリックします。
5. サイトアクセス権の変更成功メッセージが表示されたら、**閉じる** ボタンをクリックします。

> **情報**
>
> - パートナーポータルで技術者をサイトに割り当てて権限を設定した後は、BioStar Air管理ポータルの管理者アカウントでのみ権限を変更できます。
> - BioStar Air 管理者ポータルでサイト管理者が技術者のサイトアクセスをロックした場合、パートナーポータルからはロックを解除できません。 サイトの技術者アクセス権を変更するには、BioStar Air 管理者ポータルで当該サイトの管理者権限を持つアカウントで変更できます。
> - 技術者にサイトアクセス権を付与する方法の詳細は サイトに技術者を割り当てる を参照してください。

技術者アカウントの削除

もはや技術者のサポートが不要になった場合、技術者アカウントを削除できます。 技術者アカウントを削除すると、当該技術者はパートナーポータルにログインできなくなり、技術者アカウントに関連するすべての情報がシステムから完全に削除されます。

1. 技術者一覧で削除する技術者のチェックボックスをクリックします。 1人以上の技術者を選択できます。
2. 画面左上の ボタンをクリックします。



3. ポップアップメッセージが表示されたら内容を確認し、**確認** ボタンをクリックします。
4. アカウント削除の成功メッセージが表示されたら、**閉じる** ボタンをクリックします。

削除した技術者アカウントは技術者一覧に表示されなくなります。

サイトに技術者を割り当てる

パートナーは顧客サイトに技術者を割り当て、権限を設定できます。 各技術者ごとに必要なアクセス権限レベルを細かく管理し、機密の個人情報を保護できます。

サイト別技術者割り当ての主な機能

- **細かな権限設定**：デバイスへのアクセスから完全な管理者権限まで柔軟に設定可能
- **ユーザーデータ保護**：ユーザーデータへのアクセス除外オプションで個人情報規制に準拠
- **効率的な管理**：パートナーが定義した権限レベルに従ってサイトごとに技術者を管理

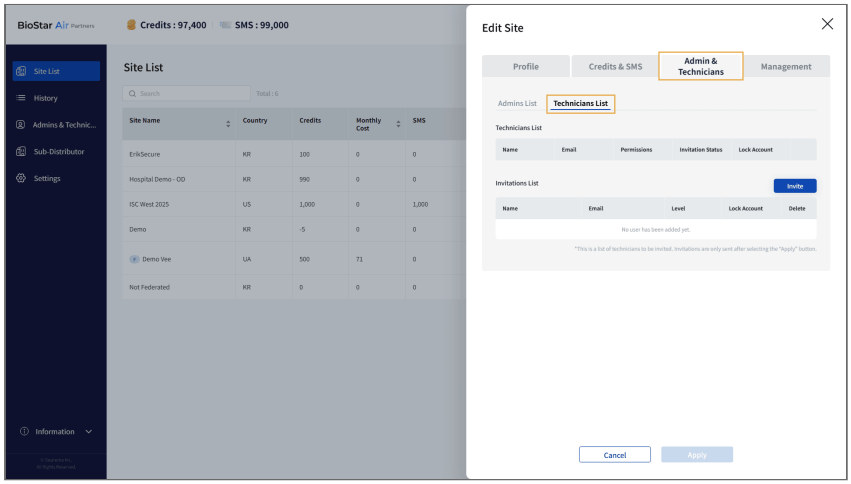
> **情報**
>
> - サイトに技術者を招待する前に、パートナーポータルで先に技術者アカウントを招待する必要があります。 詳しくは パートナーポータルに技術者を招待する をご参照ください。
> - BioStar Air 管理者ポータルで技術者をサイトに割り当てる方法の詳細は 技術者アカウントを管理する を参照してください。

サイトに技術者を割り当てる

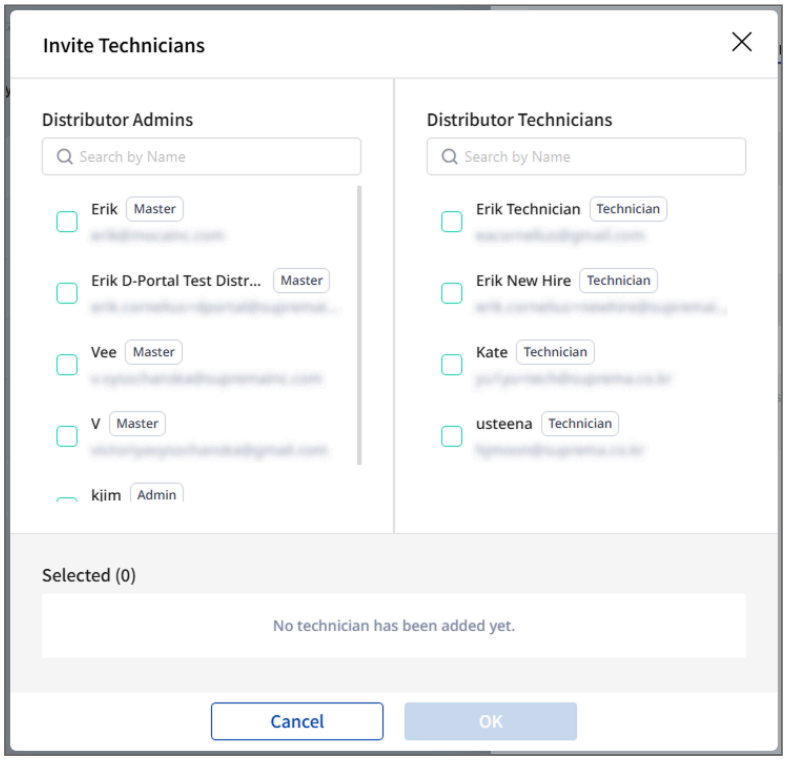
パートナーポータルで技術者を招待した後、技術者が該当サイトにアクセスできるように、個別のサイトに技術者を割り当てる必要があります。 サイトに技術者を割り当てるには、次の手順に従ってください。

1 サイト一覧へ移動

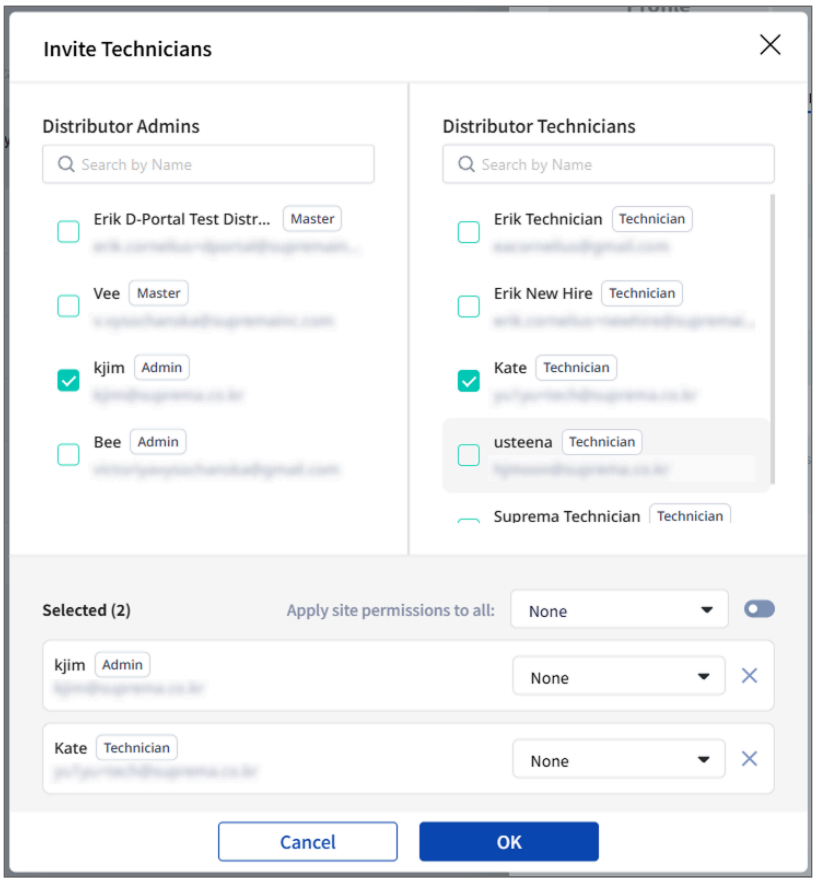
1. パートナーポータルにログインしてください。
2. 画面左のサイドバーで をクリックしてください。
3. サイト一覧から技術者を割り当てるサイトをクリックしてください。
4. パネルが表示されたら → タブを順にクリックしてください。



5. をクリックしてください。
6. ウィンドウが表示されたら、 または の一覧から目的のアカウントを選択してください。



選択したアカウントは下部の 一覧に表示されます。



情報

- 名前検索欄に管理者または技術者の名前を入力して検索できます。
- 選択を解除するには、 一覧で該当アカウントの右側にある ✕ ボタンをクリックしてください。
- サイトに管理者として登録済みのアカウントや、既に登録された技術者アカウントは一覧に表示されません。

2 サイトアクセス権限の設定

招待する技術者をすべて選択したら、サイトアクセス権限を適用してください。 適用できる権限は以下の通りです。

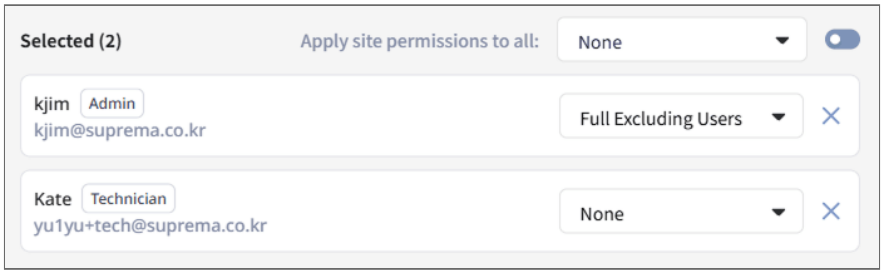
- ：サイトに参加できますが、ログインはできません。
- ：**ダッシュボード** および **デバイス管理** メニューのみアクセスできます。
- ：**ユーザー管理** メニューを除くすべてのメニューにアクセスできますが、一部の設定機能へのアクセスは制限されます。
- ：**ユーザー管理** メニューを含むすべてのメニューにアクセスできますが、一部の設定機能へのアクセスは制限されます。

情報

- および は、以下のメニューパスに対して閲覧権限はありますが、編集権限はありません。
  - **設定** → **デバイスのみ**
  - **設定** → **サイト**
- パートナーポータルで技術者をサイトに割り当てて権限を設定した後は、BioStar Air管理ポータルの管理者アカウントでのみ権限を変更できます。

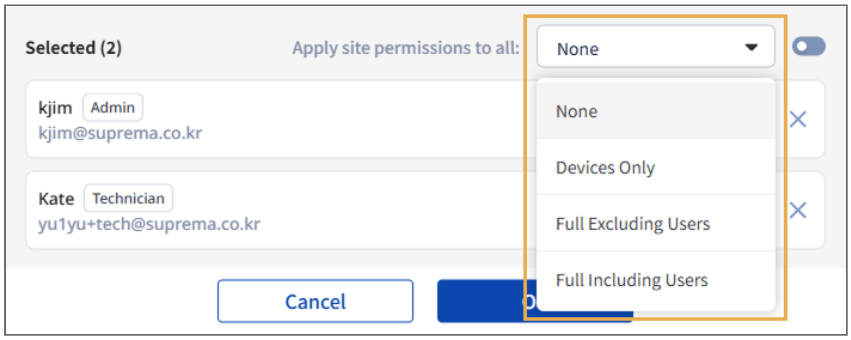
3 個別技術者の権限設定

個別の技術者ごとに異なる権限を適用できます。 各アカウントの右側で希望する権限レベルを選択してください。

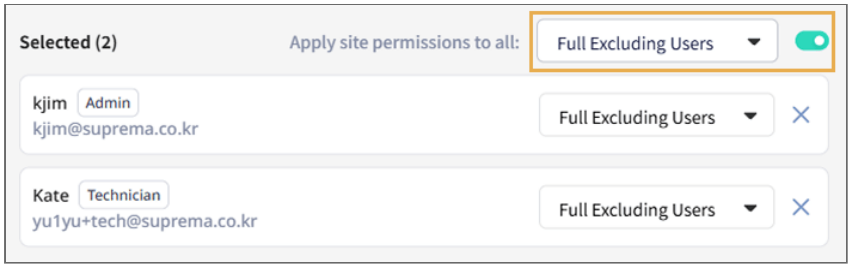


4 すべての技術者に同じ権限を適用

1. 選択したすべてのアカウントに同じ権限を適用するには、 オプションで希望する権限レベルを選択し、右側のトグルボタンをクリックしてください。

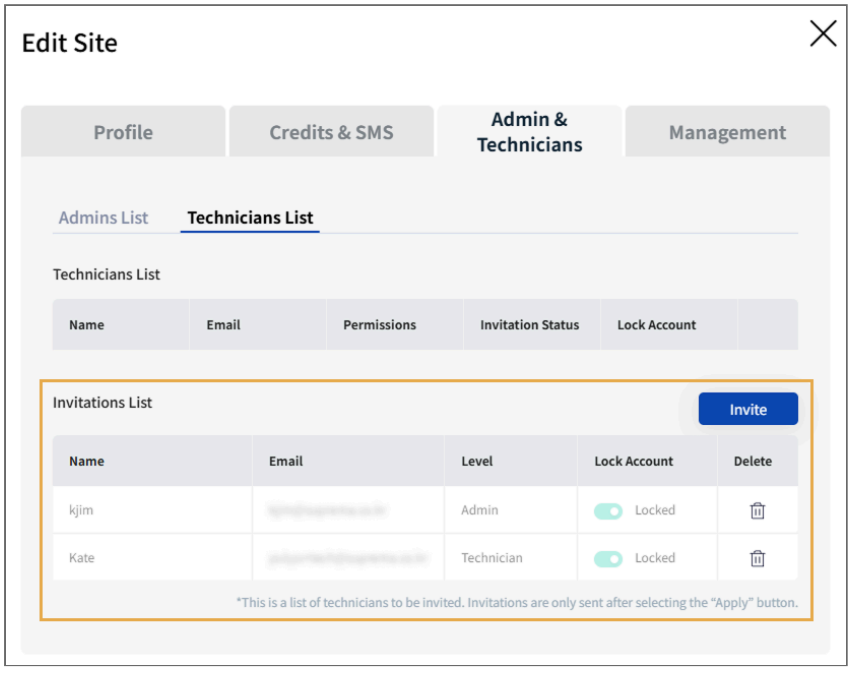


2. 確認メッセージが表示されたら、 ボタンをクリックしてください。
3. 一覧のすべてのアカウントに選択した権限が適用されます。



5 技術者招待の完了

1. 技術者の招待と権限設定を完了したら、 ウィンドウで **確認** ボタンをクリックしてください。
2. ウィンドウが閉じると、 パネルの に招待した技術者が表示されます。



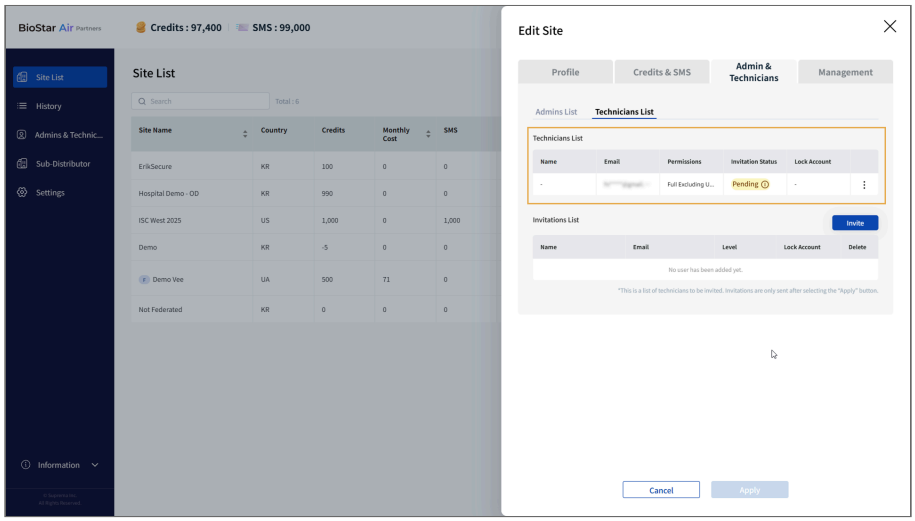
3. 招待メールを送信して技術者にサイトアクセスを許可するには、 パネル下部の ボタンをクリックしてください。

招待状況の確認

サイトに招待された技術者の招待状況を確認できます。 招待された技術者がメールを承諾するまでは、招待状況は と表示されます。 招待された技術者は最大7日間招待を承諾できます。7日を過ぎると招待は期限切れとなり、 状態に変更されます。

1. サイト一覧で技術者を招待したサイトをクリックしてください。
2. パネルが表示されたら → タブを順にクリックしてください。
3. で招待状況を確認できます。

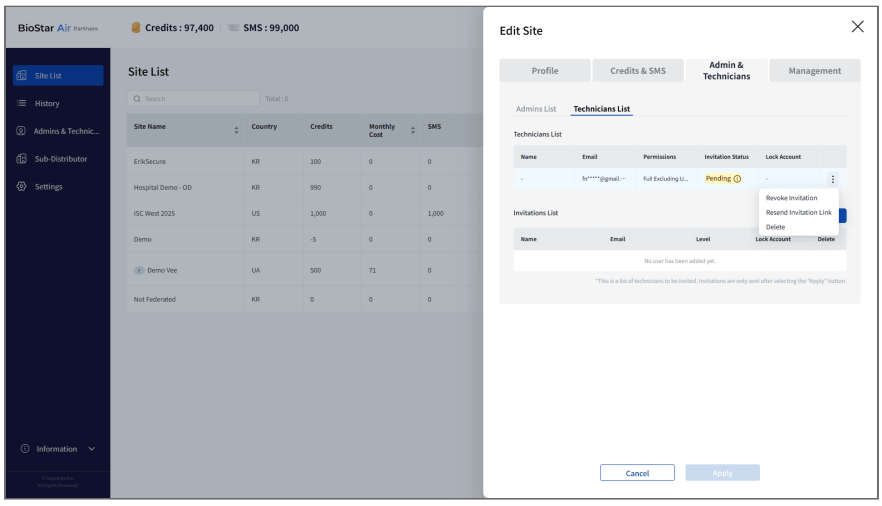
技術者がサイトへの参加を完了すると、 の状態から の状態に変更されます。



招待の取り消し

サイトに招待した技術者のメールアドレスを誤入力した場合や問題が解決して招待が不要になった場合、招待を取り消せます。

1. サイト一覧で技術者を招待したサイトをクリックしてください。
2. パネルが表示されたら → タブを順にクリックしてください。
3. で 状態の技術者の一番右にある ⋮ ボタンをクリックしてください。



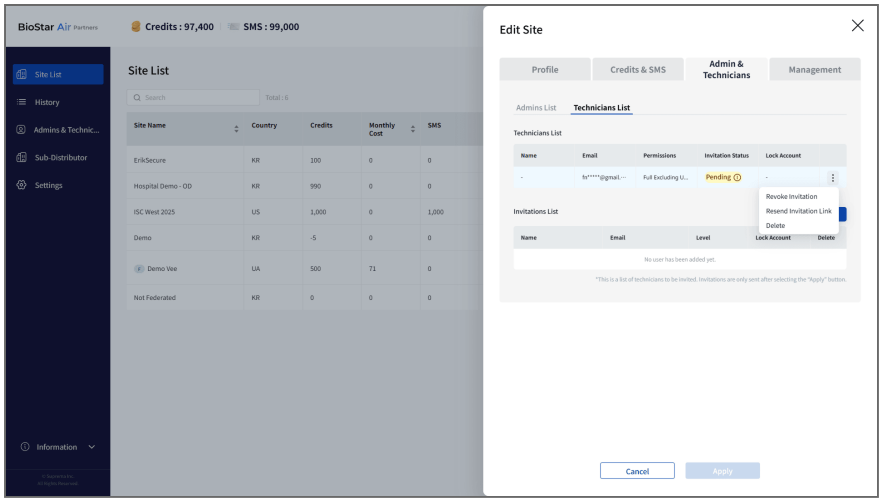
4. ポップアップメニューで をクリックしてください。
5. ポップアップメッセージが表示されたら内容を確認し、 ボタンをクリックしてください。
6. 招待取り消しの成功メッセージが表示されたら、**閉じる** ボタンをクリックしてください。

取り消された招待の技術者は、招待状況が から に変更されます。

招待リンクの再送信

サイトに招待された技術者が招待メールを受け取っていないか紛失した場合、招待リンクを再送信できます。

1. サイト一覧で技術者を招待したサイトをクリックしてください。
2. パネルが表示されたら → タブを順にクリックしてください。
3. で 、 、 状態の技術者の一番右にある ⋮ ボタンをクリックしてください。

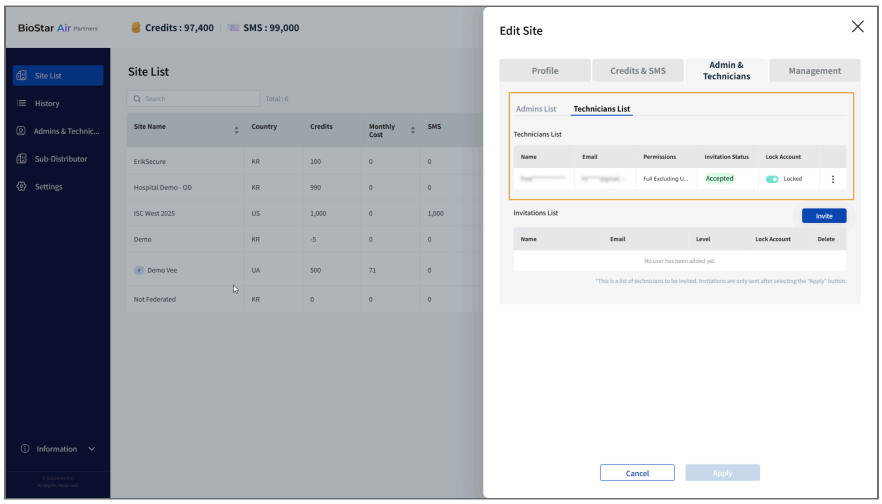


4. ポップアップメニューで をクリックしてください。
5. ポップアップメッセージが表示されたら内容を確認し、 ボタンをクリックしてください。
6. 招待リンク再送信の成功メッセージが表示されたら、**閉じる** ボタンをクリックしてください。

技術者アカウントのロック/解除

サイトに割り当てられた技術者のアカウントをロックまたは解除できます。

1. 画面左のサイドバーで をクリックしてください。
2. サイト一覧で技術者のアクセスを管理するサイトをクリックします。
3. パネルが表示されたら → タブを順にクリックしてください。



4. で技術者アカウントをロックまたは解除するには、列のトグルボタンをクリックしてください。

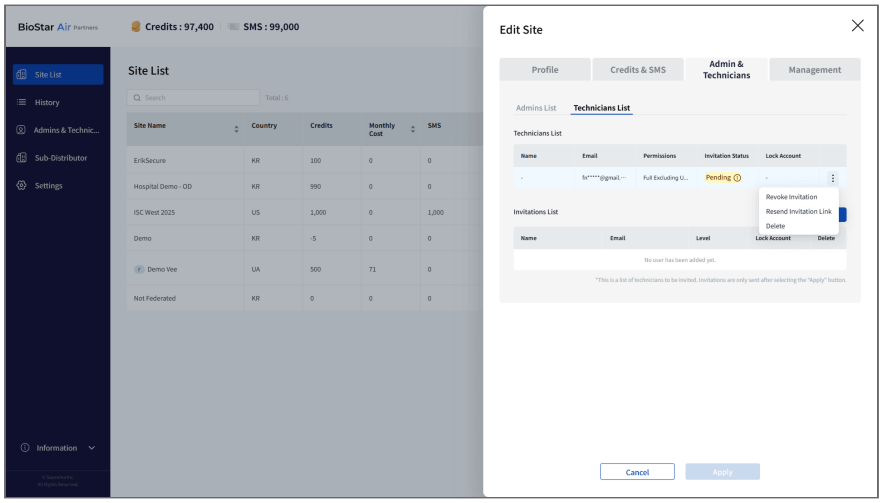
5. 変更を適用するには、下部の ボタンをクリックします。

> **情報**
> 初回登録された技術者アカウントはサイトへのアクセス権が 状態になっています。 状態を解除するには、BioStar Air ポータルで当該サイトの管理者権限を持つアカウントで解除できます。

技術者の削除

サイトに招待された技術者のアカウントを削除できます。 技術者のアカウントが削除されると、その技術者はサイトにログインできず、サイトへのアクセス権が削除されます。

1. サイト一覧で技術者を招待したサイトをクリックしてください。
2. パネルが表示されたら → タブを順にクリックしてください。
3. で削除する技術者の一番右にある ⋮ ボタンをクリックしてください。



4. ポップアップメニューで **削除** をクリックしてください。
5. ポップアップメッセージが表示されたら内容を確認し、**確認** ボタンをクリックします。
6. 技術者削除の成功メッセージが表示されたら、**閉じる** ボタンをクリックしてください。

> **情報**
> 削除された技術者アカウントは完全に削除されるわけではなく、当該サイトへのアクセス権のみが解除されます。 削除された技術者アカウントはサイトに再招待してアクセス権を付与できます。

ハードウェアのセットアップ

BioStar Airシステムを正しく構成するためのハードウェアのインストールおよび設定ガイドです。 SIPインターホン、IPカメラ、QRスキャナー、エアパッチなど、各デバイスの接続と設定方法、ネットワークポートの設定、およびセキュリティモジュールの設定を案内します。

BioStation 3 SIPインターホンの設定

BioStar Air v2.10以降、**BioStation 3**(BS3)はSIPインターホン機能をサポートします。 これによりリーダーと管理者間の双方向音声通話だけでなく、リモートでドアを解錠できます。

> **情報**
> この機能を使用するにはSIPサーバーが必要で、別途購入および構成する必要があります。 SupremaはSIPサービスを提供していません。

SIP

セッション開始プロトコル（Session Initiation Protocol, SIP）は、IPネットワーク上でリアルタイムの音声およびビデオ通話を開始、維持、終了するために広く使用される通信プロトコルです。 この場合、SIPはBioStation 3をインターホンエンドポイントとして動作させ、対応するSIPサービスを通じて発信・着信できるようにします。

着信

BioStation 3で受信した通話は、以下の方法で受信できます。

- **BioStar Air Web**：ウェブブラウザで直接通話を受ける
- **BioStar Air Mobile App** (iOS / Android)：移動中でも通話を受ける

リモートドア制御

SIP通話中に、**DTMFコマンド**を使用してドアを開けます：

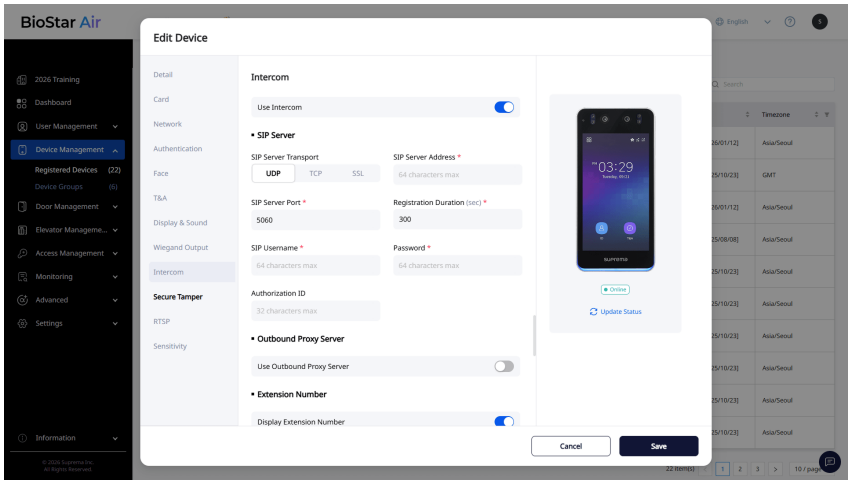
- 物理的なSIP電話
- BioStar Air モバイルアプリ
- BioStar Air Webインターフェース

構成手順

デバイス設定および管理者アカウント設定から構成できます。

1 デバイス設定

1. BioStar Air ポータルにログインします。
2. 画面左のサイドバーで **デバイス管理** → **登録済みデバイス** をクリックします。
3. デバイス一覧で **BioStation 3** をクリックします。
4. **インターコム** セクションに移動し、**インターコムを使用する** オプションを有効にします。
5. SIPサーバー情報を入力します。



上記の画像は例示です。実際の画面とは異なる場合があります。

- **SIPサーバーアドレス**
- **SIPサーバーポート**
- **SIPユーザー名** / **パスワード**

6. 変更を保存するには、**保存** をクリックします。

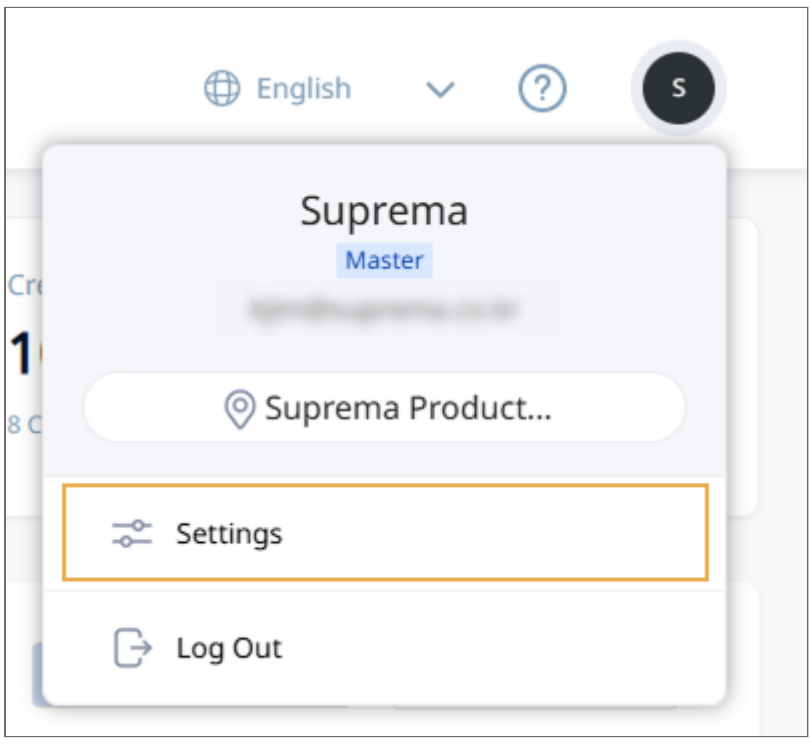
❷ アカウント設定

BioStation 3の通話をブラウザやアプリにルーティングできます。

1. 通話を受ける各管理者はBioStar Airポータルまたはモバイルアプリにログインします。
2. **アカウント設定**に移動します。

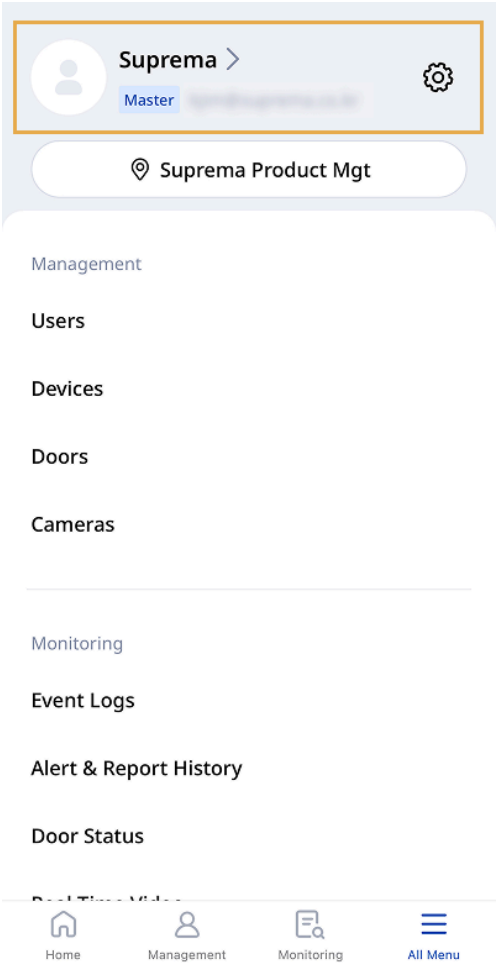
Web

画面右上のユーザープロフィールアイコンをクリックした後、**設定**を選択してください。



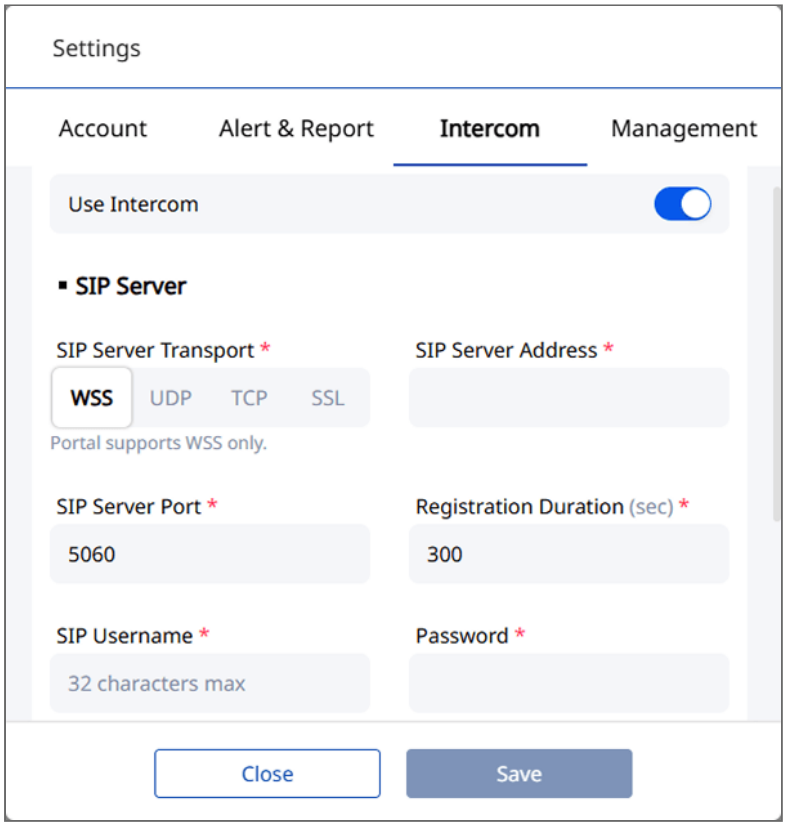
Mobile

初期画面の下部にある **すべてのメニュー** をタップし、その後ユーザープロフィール領域をタップしてください。

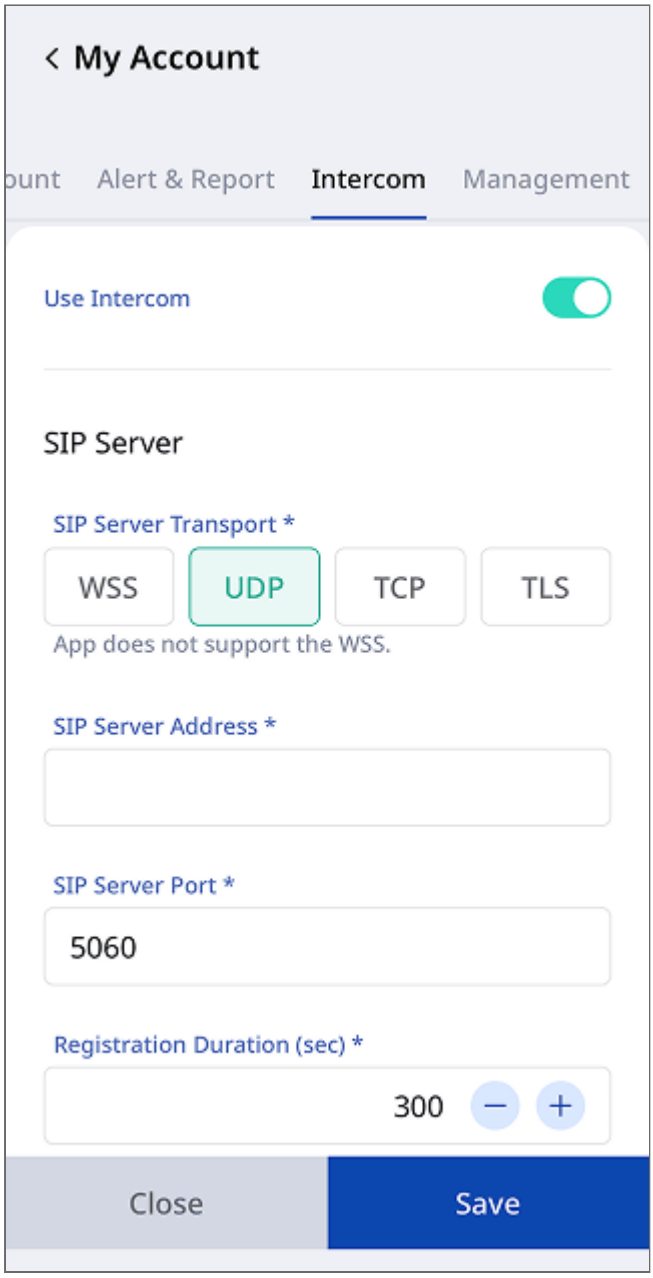


3. **設定** ウィンドウが表示されたら、**インターコム** タブをクリックしてSIPサーバーのログイン情報を追加します。

Web


Settings
Account
Alert & Report
Intercom
Management
Use Intercom
SIP Server
SIP Server Transport *
WSS
UDP
TCP
SSL
Portal supports WSS only.
SIP Server Address *
SIP Server Port *
5060
Registration Duration (sec) *
300
SIP Username *
32 characters max
Password *
Close
Save

Mobile



4. 設定を保存するには、**保存** をクリックします。

検証済みのSIPプロバイダー

BioStation 3は以下のプロバイダーで正常に動作することを確認済みです。

- RingCentral
- FreePBX
- Linphone
- Linhome

IPカメラのサポートおよび設定

BioStar Airは、互換デバイスと同じネットワークに接続されたIPカメラを自動的に検出します。 カメラはデバイスをゲートウェイとして使用するため、ネットワークビデオレコーダー（Network Video Recorder, NVR）は不要です。 代わりにカメラは内蔵SDカ

ードストレージを使用します。

互換機器を設置している場合、BioStar Airは以下のような同時ライブビューを表示できます。

- 最大2台のカメラでFull HD解像度（1080p）
- 最大4台のカメラでHD解像度（720p）

この仕様はX-Station 2を使用する場合に2倍になります。

> **情報**
> BioStar Airにカメラを登録した後、録画されたビデオが再生されない場合は、ビデオ再生のトラブルシューティングを参照してください。

互換性

- **Onvif Profiles**：IPカメラはOnvifプロファイルSまたはGと互換性がある必要があります。
  - **Onvif Profile S**：ライブビデオストリーミング
  - **Onvif Profile G**：録画済みビデオをSDカードに保存
- **SDカード**：IPカメラは後で録画した映像を再生できるように内蔵SDカードを備えている必要があります。

  > SanDisk microSDXC Class10 Max Endurance 256GBまたは512GBを推奨します。

- **エンコーディング**：カメラはH.264(AVC)をサポートし、有効なコーデックとして設定されている必要があります。 BioStar Airは現在H.265をサポートしていません。
- **推奨ブランド**：Hanwhavision、Hikvision、Dahuaのカメラとの互換性が高いです。 他ブランドとの互換性はOnvifプロファイルの準拠状況によって異なる場合があります。 テスト済みおよび検証済みデバイスの一覧の詳細については、テストおよび検証済みデバイス一覧を参照してください。
- テストしたい別のカメラブランドがある場合は、サービスチームにお問い合わせください。

機能紹介

BioStar Airポータルまたはモバイルアプリで以下の操作を行えます。

- リアルタイムのカメラフィードを表示できます。
- 録画されたカメラ映像を表示できます。
- 出勤イベントに関連するカメラ映像にアクセスできます。

使用方法

1 IPカメラの接続

- **ネットワーク接続**：IPカメラがBioStar Airと互換性のある機器と同じネットワークに接続されていることを確認してくだ

さい。

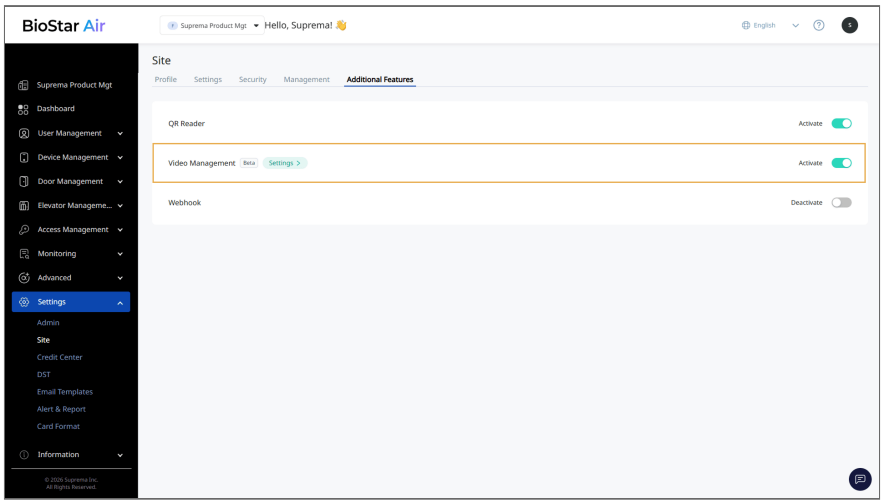
- **Onvifの有効化**：カメラでOnvifが有効になっていることを確認します。
- **デバイス登録**：デバイスがBioStar Airポータルに登録されていることを確認します。

2 BioStar Airへのログイン

マスター管理者のみビデオ管理の有効化などサイト設定を変更できます。 BioStar Airポータルに**マスター**権限でログインします。

3 ビデオ管理の有効化

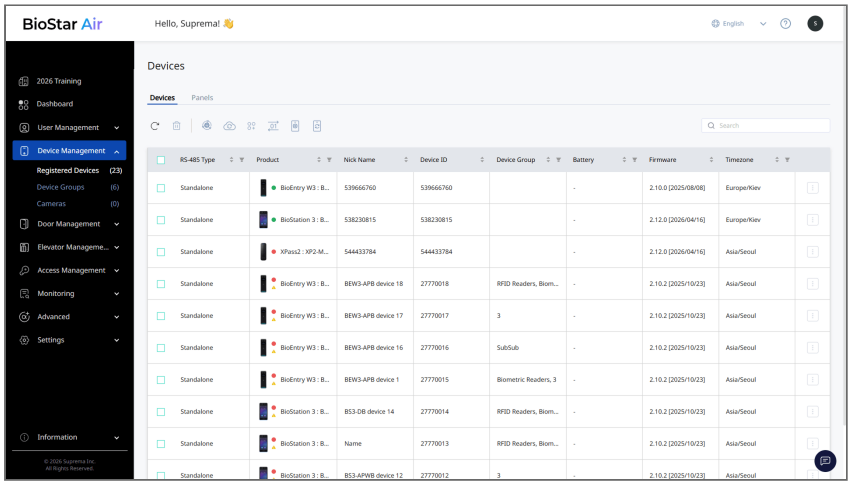
1. 画面左のサイドバーで **設定** → **サイト** をクリックします。
2. **追加機能** タブをクリックします。
3. **ビデオ管理** オプションを有効にします。



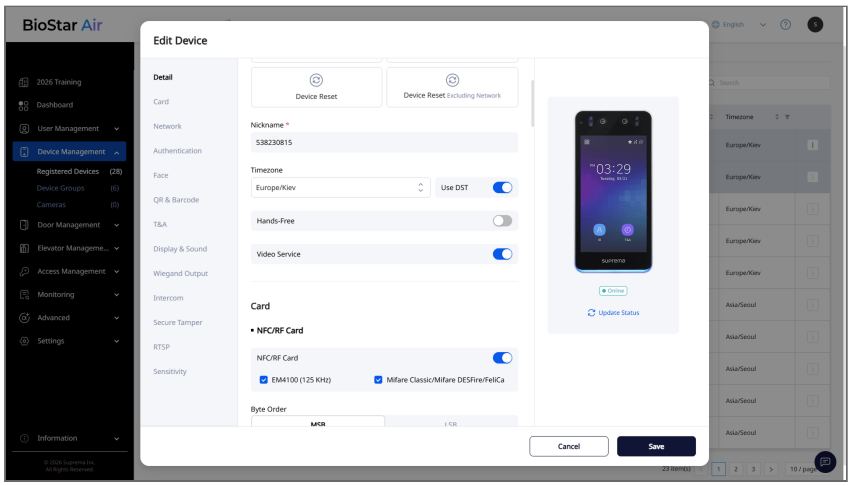
> **情報**
> この機能は**マスター**レベルの管理者のみ有効にできます。

4 ビデオサービスを有効にする

1. 画面左のサイドバーで **デバイス管理** → **登録済みデバイス** をクリックします。



2. 一覧でBioStar Airに対応するデバイス（例: BioStation 3）をクリックしてください。
3. **デバイス編集** ウィンドウが表示されます。
4. **詳細** セクションの **ビデオサービス** オプションを有効にしてください。

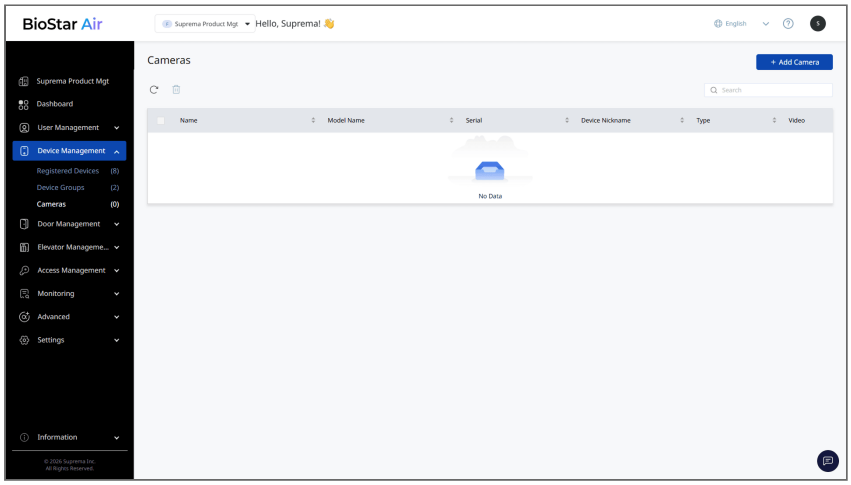


5. 変更を保存するには、下部の **保存** をクリックします。

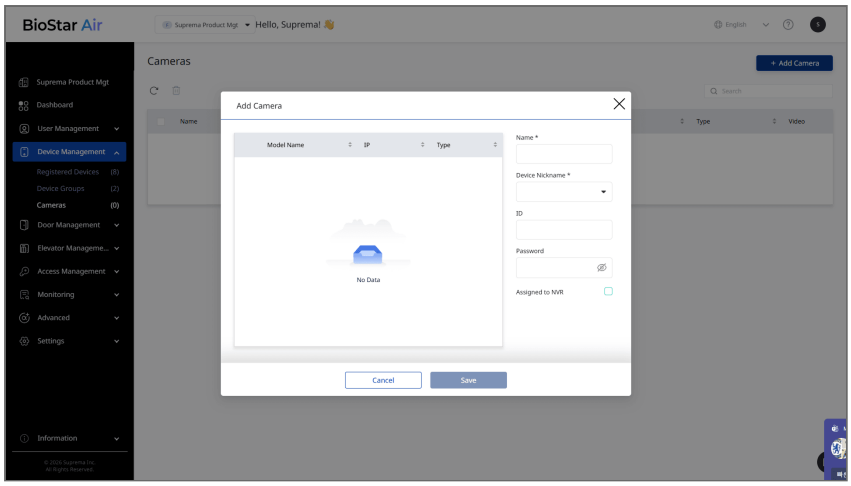
> **情報**
> デバイスにはファームウェア2.5.1以上がインストールされ、カメラと同じネットワーク上にある必要があります。

5 カメラの追加

1. 画面左のサイドバーで **デバイス管理** → **カメラ** をクリックします。



2. 画面右上の **カメラの追加** ボタンをクリックします。
3. **カメラの追加** ウィンドウが表示されたら、ゲートウェイとして機能するデバイスを選択します。



上記の画像は例示です。実際の画面とは異なる場合があります。

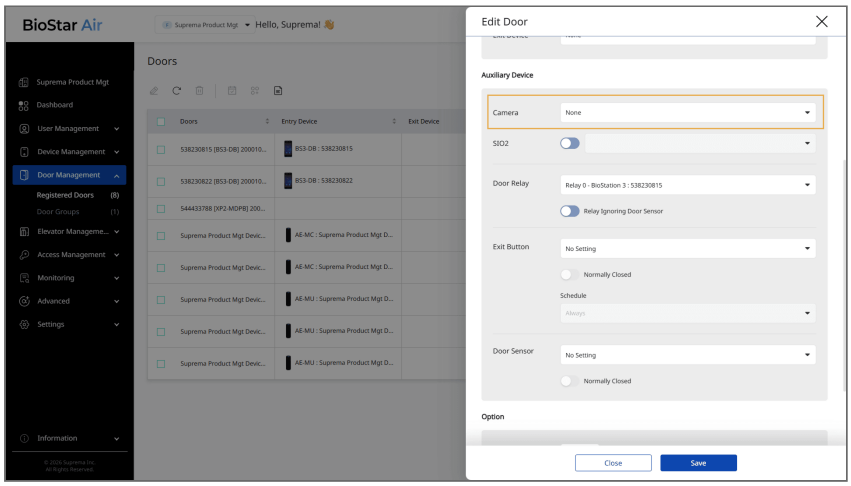
4. カメラを追加するには、以下の情報を設定します。
   - **カメラ名**：カメラ名を入力します。
   - **デバイスニックネーム**：カメラを区別する名前を選択してください。
   - **ID**：カメラにアクセスするIDを入力します。
   - **パスワード**：カメラにアクセスするパスワードを入力します。
5. 選択したカメラを追加するには **保存** ボタンをクリックします。

> **情報**
>
> - デバイスにはファームウェア2.5.1以上がインストールされ、カメラと同じネットワーク上にある必要があります。
> - BioStar Airはネットワーク上のカメラを自動的に検出します。

6 ドアとの接続

追加したカメラをドアに割り当て、入退室イベントに関連する映像を連携できます。

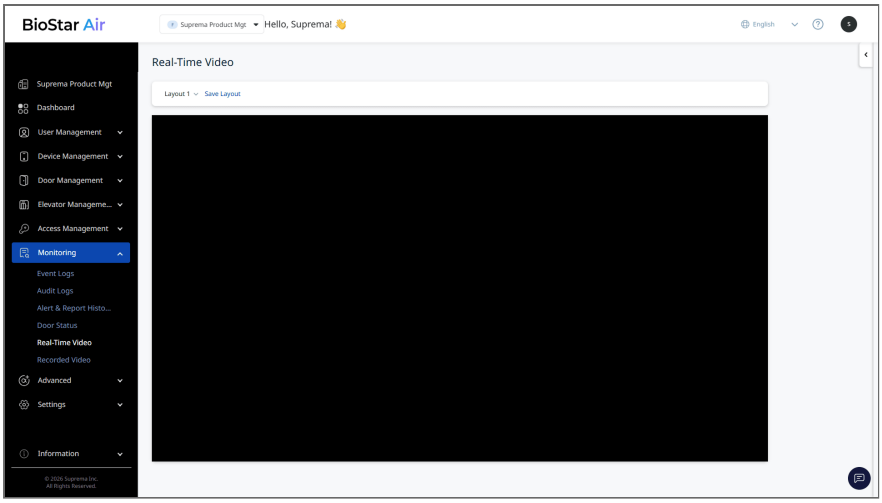
1. 画面左のサイドバーで **ドア管理** → **登録されたドア** をクリックしてください。
2. リストからカメラを割り当てるドアをクリックします。
3. **ドアを編集** パネルが表示されたら、**補助装置** セクションまでスクロールします。
4. **カメラ** オプションで追加したカメラを選択します。



5. 変更を保存するには、**保存** をクリックします。

7 リアルタイムカメラ映像の表示

追加したカメラの映像をリアルタイムで確認できます。 画面左のサイドバーで **モニタリング** → **リアルタイム動画** をクリックします。



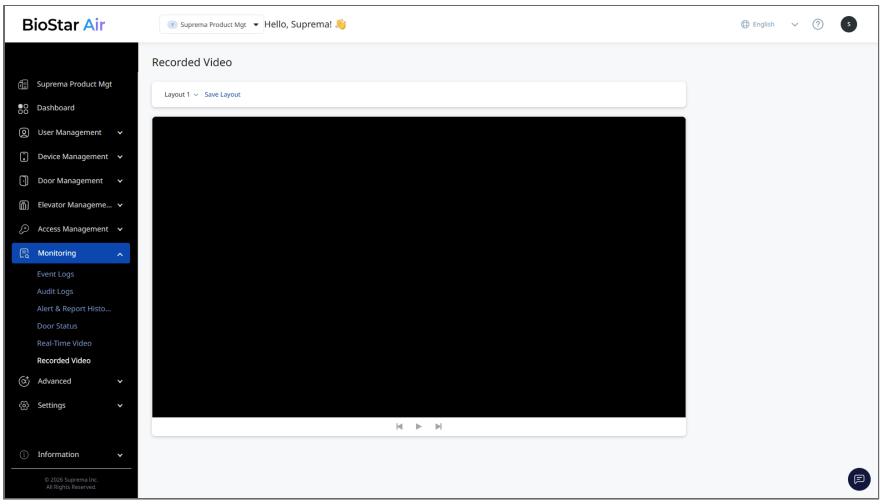
上記の画像は例示です。実際の画面とは異なる場合があります。

- BioStar Airと互換性のある機器ごとに、最大2つのフルHD（1080p）ライブストリームを表示できます。
- より多くのリアルタイムストリームを表示するには、デバイスを追加するかカメラの解像度を下げてください。

  > ***デバイス管理*** → ***カメラ*** → リストでカメラをクリック → ***ビデオ プロファイル***

8 録画済みカメラ映像の表示

録画されたビデオストリームを表示できます。 画面左のサイドバーで **モニタリング** → **録画された動画** をクリックします。



上記の画像は例示です。実際の画面とは異なる場合があります。

9 イベント映像の表示

画面左のサイドバーで **モニタリング** → **イベントログ** をクリックします。 関連するビデオクリップがあるイベントログを見つけ、再生ボタンをクリックすると映像を視聴できます。

テストおよび検証済みデバイス一覧

No	メーカー	モデル番号	機器タイプ	Onvifプロファイル	解像度
1	Hanwha Techwin	QNV-C8011R	カメラ	S, G, T, M	2592x1944
2	Hanwha Techwin	QND-6022R	カメラ	S, G, T	1920x1080
3	Hanwha Techwin	MMI-600R	カメラ	S, T	1920x1080
4	HIKVISION	DS-2CD2025FWD-I	カメラ	S, G, T	1920x1080
5	HIKVISION	DS-2CD2166G2-I	カメラ	S, G, T	3200×1800
6	HIKVISION	DS-2CD1121-I	カメラ	S	1920x1080
7	Dahua	DHI-NVR2104HS-P-S3	NVR	S, G, T	12MP
8	Dahua	IPC-HDBW3249E-AS-NI	カメラ	S, G, T	1920×1080
9	Dahua	SD22204UEN-GN	カメラ	S, G, T	1920×1080
10	Dahua	DH-IPC-HFW1230DT-STW-VN	カメラ	S, T	1920×1080
11	Marruy	IPC-A32E-L	カメラ	S, T	2304×1296

No	メーカー	モデル番号	機器タイプ	Onvifプロファイル	解像度
12	TP-Link	Tapo C210	カメラ	S	2304×1296

IPカメラでのONVIF有効化方法

1. ウェブブラウザを開き、カメラのIPアドレスを入力します。
2. 管理者資格情報で認証してログインします。
3. **Network**または**Configuration**セクションに移動します。
4. ONVIF、またはオープンネットワークビデオインターフェースを有効にします。
5. 必要に応じてONVIF専用のユーザープロファイルを作成します。
6. 設定を保存し、BioStar AirでONVIF接続をテストします。

ヒント

- **ファームウェア更新**：カメラとデバイスを最新のファームウェアに更新してください。
- **ポートフォワーディング**：必要に応じてONVIF用のポートフォワーディングを設定します。
- **サードパーティツール**：ONVIF Device Managerを使用してカメラの設定と機能を確認します。

Airfob Patchのインストール

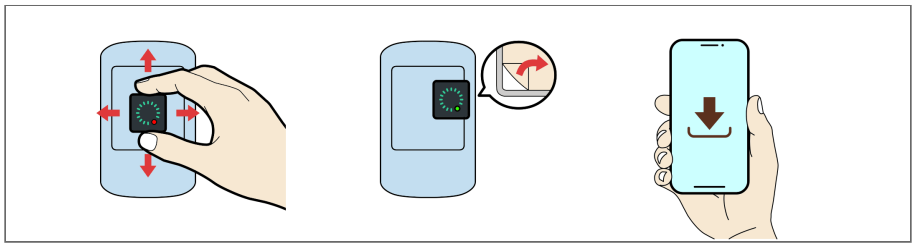
Airfob Patchのインストール方法を案内します。 Airfob Patchは、既存の入退室管理システムをBioStar Airモバイルクレデンシャルと互換性を持たせるためのデバイスです。

情報

- Airfob PatchはMIFARE 1K技術と互換性がありますが、125 KHzの低周波リーダーとは互換性がありません。
- Airfob Patchは、モバイル機器上の暗号化されたBioStar Airクレデンシャルを Bluetoothで認証し、リーダーにMIFARE RFID信号をエミュレートして動作します。 テープを使用して入退室管理デバイスに貼り付け、配線は不要です。
- Airfob PatchをBioStar Airアプリに登録する方法の詳細は、Airfob PatchとTagを構成するを参照してください。

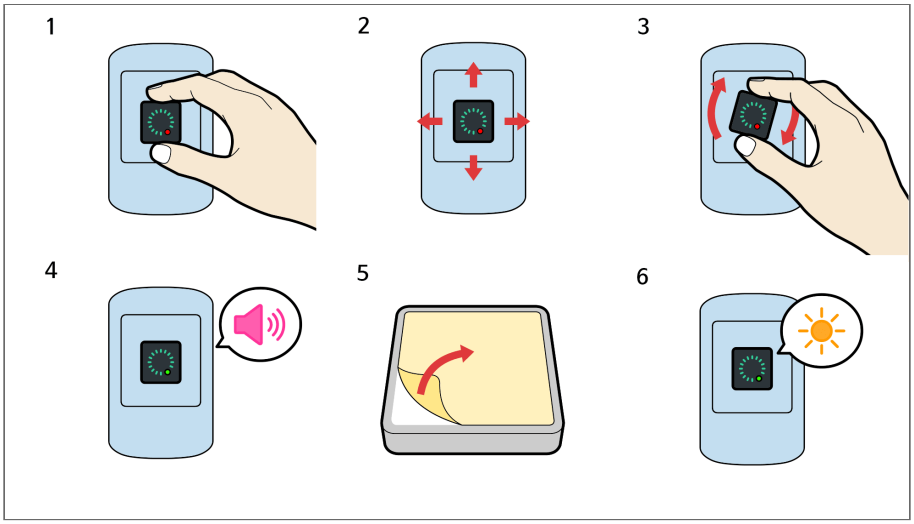
インストール概要

Airfob PatchがデバイスのRFフィールドから電源を供給される位置を見つけてください。



Airfob Patchの設置場所を確認する

付属の粘着テープでAirfob Patchを入退室管理デバイスに貼り付ける前に、下の図と手順に従って、デバイスで最適な位置を見つけてください。



1. Airfob Patchを入退室管理デバイスに接触するように配置してください。
2. Airfob PatchのLEDが1秒に1回以上緑に点滅する位置を見つけてください。
3. Airfob Patchをデバイスに当てるか、取り外し可能なテープを使って一時的に貼り付けてください。 BioStar Airアプリを使用してAirfob Patchを登録してください。 詳しくは、Airfob PatchとTagを構成するを参照してください。
4. AirfobまたはBioStar Airモバイルクレデンシャルを使用して、少なくとも5回のテスト認証を実行してください。
5. Airfob Patchの裏面に貼られた両面粘着テープの保護フィルムを剥がしてください。
6. 入退室管理デバイスにAirfob Patchを貼り付けてください。

情報

- Airfob Patchに別途電源供給は不要です。 入退室管理デバイスに貼り付けると、自動的に電源が入ります。
- 付属の両面テープでAirfob Patchをデバイスに貼り付けると、恒久的に固定されます。 Airfob Patchを取り外すと、Airfob Patchが損傷し、再利用できない場合があります。

トラブルシューティング

▼ Q. 入退室管理デバイスで連続5回の動作音が発生しません。

入退室管理デバイスで連続5回の動作音が発生しない場合は、Airfob Patchを再起動してください。

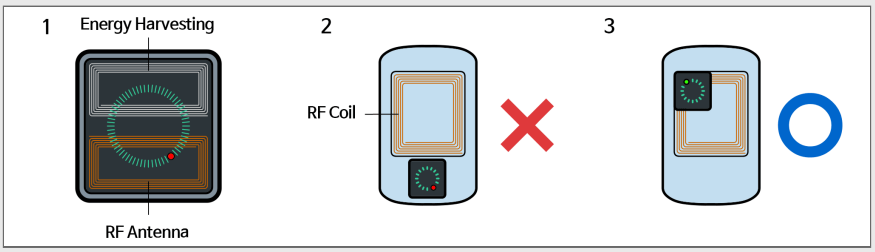
1. 入退室管理デバイスからAirfob Patchを取り外してください。
2. 電源が切れると、Airfob PatchのLEDは約6秒間赤く点滅してから消灯します。
3. Airfob Patchの電源がオフになっていることを確認し、最初からやり直してください。

▼ Q. Airfob PatchのLEDが赤く点滅します。

Airfob Patchの赤いLEDが点滅する場合は、Airfob Patchの位置を調整してください。

1. Airfob Patchを入退室管理デバイスの別の位置に移動し、LEDが緑に点滅するか確認してください。
2. 電力が十分強い場合、LEDは0.5秒または1秒間隔で点滅します。
3. Airfob Patchの位置を変更した場合は、Airfob Patchを再起動して最初からやり直してください。

▼ Q. 入退室管理デバイスがAirfob Patchを認識しません。



- 入退室管理デバイスのRFコイル位置とAirfob PatchのRFアンテナ位置が一致すると、両方のデバイスは正常に動作します。
- モバイル機器で入退室管理デバイスにタッチしたときに有効なアクセス権限が付与されない場合は、Airfob Patchの位置を調整するか回転させて、正常に動作する位置を見つけてください。
- Airfob Patchの位置と向きは、入退室管理デバイスによって異なる場合があります。
- Airfob Patchの動作範囲は、入退室管理デバイスのRF信号強度とRFコイルの位置およびサイズによって、小さくも大きくもなります。

SIO2 セキュリティモジュールの構成

SIO2 セキュリティモジュールは、BioStar Airと互換性のあるデバイスとリレーの間を仲介し、入退室管理システムのセキュリティを強化します。 **RS485ケーブル**を介してリーダーと通信し、暗号化された通信によりセキュリティ違反を防ぎます。

> **注意**
> **SIO2 セキュリティモジュール**の正確な設置手順は、製品パッケージに同梱されている配線図を参照してください。 環境により設置方法が異なる場合があるため、Supremaの代理店に専門的なサポートを依頼してください。

BioStar Air ポータルで SIO2 を有効化する

SIO2 セキュリティモジュールを正常に統合し、入退室管理システムのセキュリティを強化するには、次の手順に従って **SIO2** オプションを有効にしてください。

> **情報**
> SIO2 を設置しても、BioStar Air ポータルで設定を変更しないと動作しないことがあります。

1 リーダーの登録

- リーダー、SIO2、およびドアリレーが正常に接続されていることを確認してください。
- **BioStar Air アプリ**を使ってサイトにリーダーを登録してください。

❷ デバイス接続の確認

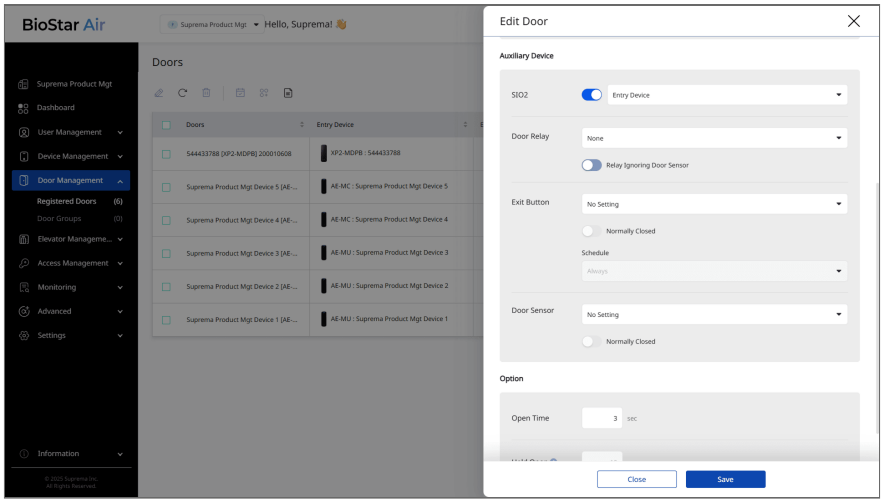
1. BioStar Air ポータルにアクセスしてください。
2. 画面左のサイドバーで **デバイス管理** → **登録済みデバイス** をクリックします。
3. デバイス一覧で該当デバイスが緑(🟢)で表示され、接続が完了していることを確認してください。

❸ SIO2 をドアに割り当てる

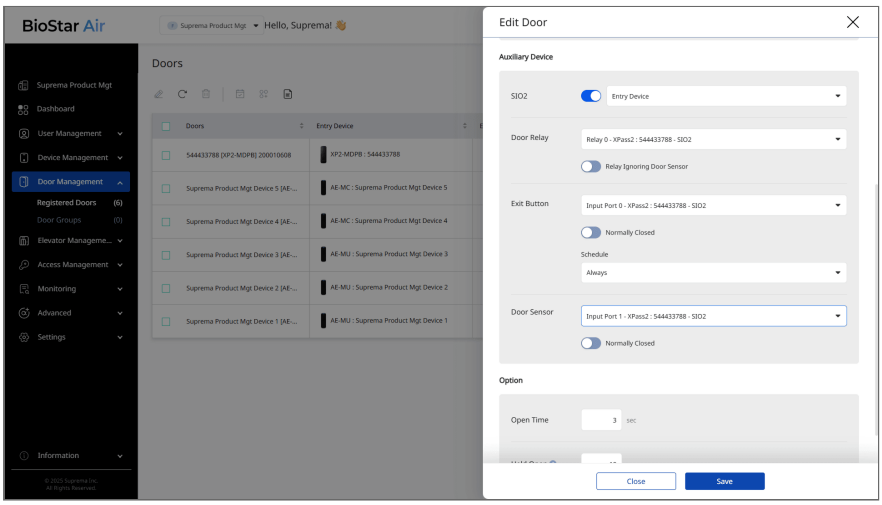
1. 画面左のサイドバーで **ドア管理** → **登録されたドア** をクリックしてください。
2. 一覧からデバイスが接続されているドアをクリックしてください。 デバイスが登録されると、ドアが自動的に作成されます。

❹ SIO2 を有効化する

1. **ドアを編集** パネルが表示されたら、**補助デバイス** セクションに移動してください。
2. **SIO2** オプションを有効にしてください。



❺ リレーおよびセンサーの構成



上記の画像は例示です。実際の画面とは異なる場合があります。

- **ドアリレー** では **Relay 0** を選択してください。

> SIO2 モジュールには1つのドアリレーポートのみがあります。

- **ドアセンサー** で、接続されている SIO2 の入力ポート番号を選択してください。
- **退出ボタン** が接続されている場合は、SIO2 の該当する入力ポートを選択してください。
- 別のタイプの出口デバイスを使用する場合は、**退室デバイス** を選択してください。

6 設定の保存

- 設定を適用するには、**保存** をクリックしてください。
- これで SIO2 セキュリティモジュールは正常に動作します。

E200 QRスキャナの配線と設定

ステップ 1: 配線

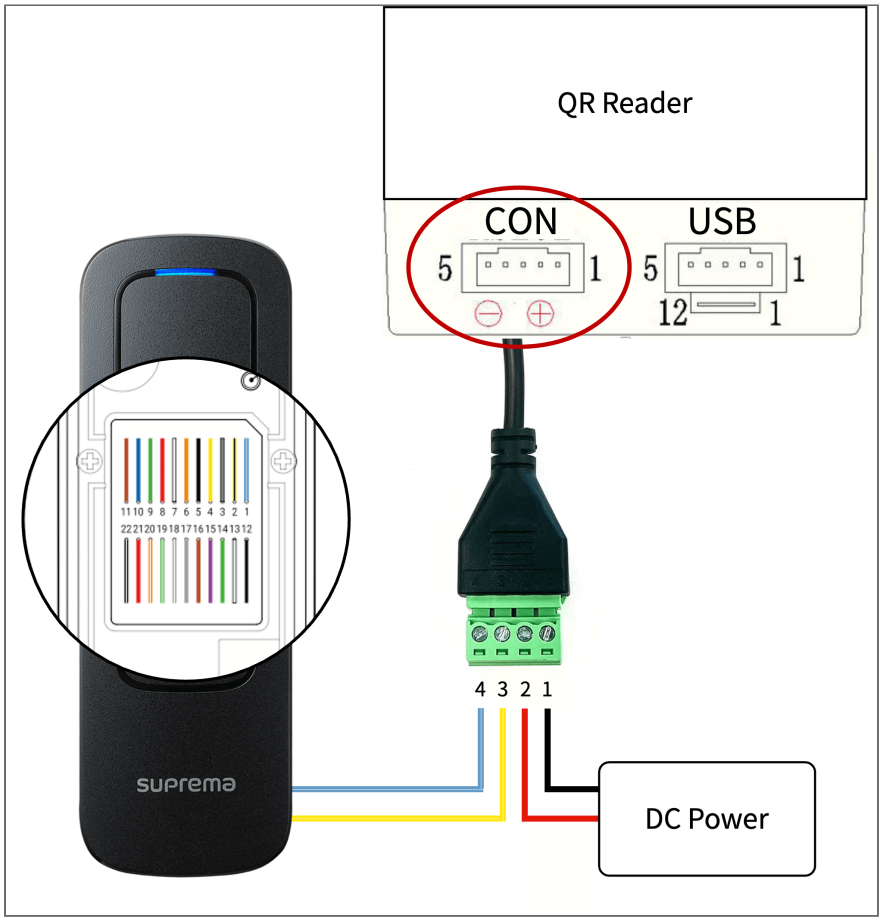
以下のように同梱のアダプターケーブルを使用して E200 シリーズの QRスキャナを接続します。

- 緑色の端子ブロックには **1から4** までラベルが付いたピンがあり、コネクタの正面を見たとき **右から左** に並んでいます。

ピン	配線色	機能
1	黒	Negative / Ground
2	赤	Positive (V+)
3	黄（白線）	RS-485 TRXN
4	青 (白線)	RS-485 TRXP

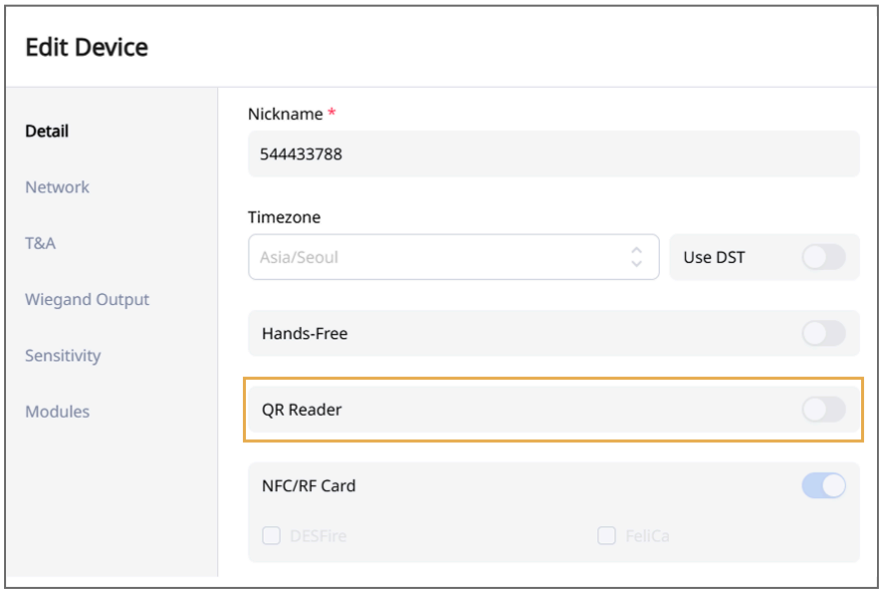
> **情報**
> 他の多くのコネクタとは配線の向きが正反対です。 配線する前に向きをもう一度確認してください。

- QRスキャナ下部の CON ポートに 4ピンコネクタを接続します。 このコネクタは **極性**（キー溝がある）ため、1方向にしか合いません。



ステップ 2: QRリーダーを有効化

1. BioStar Air ポータル(Web またはアプリ)にログインします。
2. 画面左のサイドバーで **デバイス管理** → **登録済みデバイス** をクリックします。
3. 一覧から E200 QRスキャナを接続した機器をクリックします。
4. **詳細** セクションで **QRリーダー** オプションを有効にしてください。



5. 変更を保存するには、**保存** をクリックします。

> **情報**
> QRリーダーを有効にすると、同じリーダーで他の RS-485 接続機器（例: SIO2）を使用できません。

ステップ 3: QRスキャナの構成

デフォルトで **E200 QRスキャナ** は **115,200** の伝送速度に設定されています。 Suprema 機器で使用する場合は、伝送速度を **9,600** に変更する必要があります。

QRスキャナを機器に接続し、**以下のバーコードをスキャン**して新しい伝送速度を適用します。



配線が正しく、Suprema 機器がネットワークに接続されている場合、BioStar Air を通じて提供される **ダイナミック QR クレデンシャル** を使用できます。

ネットワークポートとデバイスの特定

BioStar Air対応デバイスが円滑に接続するためには、特定のネットワークポートへのアクセスが必要です。 ネットワークポートを介して、対応デバイス、クラウドサービス、およびユーザーアプリケーション間で安全に通信できます。 管理者はネットワーク設定を行う際、BioStar Air対応デバイスのシリアル番号からMACアドレスを確認する必要がある場合があります。

必須ネットワークポート

次のポートがネットワークファイアウォールで開いていることを確認してください。

- **6379, 6381**：Redis ポート

  ユーザー情報の同期、迅速なイベントロギングの処理、セッション管理、デバイスとクラウド間のシグナル処理のためのメッセージブローカーとして使用されます。

- **5671**：TLS上のAMQP (RabbitMQ)

  サービス間のリアルタイム通信のための安全なメッセージングプロトコルを提供します。

- **443**：HTTPS (TLS)

標準のセキュアなウェブトラフィックとして使用され、以下のサービスで必要です：

- ウェブブラウザで管理ポータルのWebアプリにアクセスする
- BioStar Airモバイルアプリ (iOS/Android)
- API呼び出し
- クラウド経由でのデバイスのファームウェア更新
- デバイスのログインおよび認証サービス

- BioStar Airの組み込みビデオ管理機能を使用する場合：
  - WebSocketドメイン：eu-wss-api.airfob.com
  - WebSocketポート：3500
  - TURN/STUNポート：80, 443, 3478, 5349

> **情報**
> デバイスのログインおよび認証のために、次のエンドポイントへのアクセスを確認してください。
> - https://e-afs-api.airfob.com/v1/device/login（ヨーロッパ）
> - https://afs-api.airfob.com/v1/device/login（その他の地域）

シリアル番号からMACアドレスを確認する

場合によっては、BioStar Air対応リーダーのMACアドレスをシリアル番号のみで確認する必要があることがあります。 これは、デバイスをネットワークに追加する前にホワイトリストに登録するなどの作業に便利です。

手順

1. **シリアル番号を見つける：**

   デバイスの背面で9桁のシリアル番号を探してください。

2. **シリアル番号を16進数に変換する：**

   電卓やオンラインツールを使用して、シリアル番号を10進数から16進数に変換してください。

3. **最後の3バイトを抽出する：**

   16進値から最後の6文字を取得してください。 最後の6文字は最後の3バイトを表します。

4. **MACアドレスの構成：**

   MACアドレスは常に `00:17:FC:` で始まります。 16進値から最後の3バイト（6文字）を取り出し、各ペアをコロンで区切って追加してください。

例

1. **シリアル番号**：546089489
2. **16進数に変換**：208CAA11
3. **最後の3バイトを抽出**：8CAA11

4. **MACアドレスの構成**：00:17:FC:8C:AA:11

これらの手順に従うことで、シリアル番号を使用してネットワーク上のBioStar Air対応リーダーを正確に特定できます。

MACアドレス変換ツール

下にデバイスのシリアル番号を入力すると、MACアドレスをすぐに確認できます。

認証済みユーザー

Suprema Passアプリを使えば、スマートフォン1台で出入口を開けられます。 Bluetooth・NFC・QRコード認証の選択から2段階認証の設定、Bluetoothの検出感度の調整まで、アプリの利用に必要な主要機能をご案内します。

モバイル認証情報の使い方

Suprema Passアプリを使用すると、プラスチックのRFIDカードの代わりにモバイルクレデンシャルでドアを開けることができます。 モバイルデバイスをBluetoothまたはNFCでタグ付けするか、カードを長押しして、QRコードをスキャンしてドアを開けることができます。

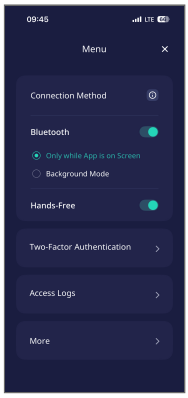
> **情報**
> Suprema PassアプリはBioStar Airシステムのユーザーインターフェースとして機能し、主にモバイル認証情報用のデジタルウォレットとして使用されます。 ユーザーはアプリ内でモバイル入退室カードを発行・保存し、モバイル機器を使って安全な場所に出入りできます。

必須要件と準備

モバイル認証情報で出入り口を開くには、次の要件を満たす必要があります。

- Suprema Passのモバイル認証情報に対応した入退室制御装置が設置されている必要があります。
- ユーザーのモバイルデバイスにSuprema Passアプリがインストールされている必要があります。
  - iOS
  - Android
- モバイルデバイスでBluetoothまたはNFC通信が有効でなければなりません。
- 2段階認証を有効にすると**バックグラウンドモード**は無効になります。
- QR認証は管理者がBioStar Airポータルで有効にする必要があります。
- ハンズフリー入退室機能を使用するには、その入退室方法がサイトでサポートされているか確認してください。

> **情報**
> - モバイル機器のSuprema Passアプリでモバイル入退室カードにより認証を行うには、位置情報サービスが必要です。 位置サービスを有効にする必要がありますか？で関連するFAQを確認してください。
> - モバイルカードが機器と認証されているがドアが開かない場合は、案内に従って問題を解決してください。 モバイルカードが動作しませんで関連するFAQを確認してください。



接続方法の設定

Suprema Pass アプリで、ユーザーは2種類の動作モードから選択できます。 Suprema Passアプリの初期画面で、右上の☰アイコンをタップした後、**Connection Method**から希望のモードを選択してください。

- **Only while App is on Screen**: アプリが画面に表示され、モバイルカードが見えているときのみ出入口を開けることができます。
- **Background Mode**: アプリがバックグラウンドで実行されている場合、端末がロックされていても出入口を開けることができます。

> **情報**
> モードに関係なく、ユーザーは常にモバイル機器をデバイスにかざして認証できます。

出入口を開ける

Suprema Passアプリを使用して、ユーザーはさまざまな方法で出入口を開けることができます。

モバイル機器をデバイスにかざす

モバイル機器をBioStar Airと互換性のあるデバイスに近づけ、BluetoothまたはNFCで認証して出入口を開けることができます。

1. Suprema Passアプリが実行中であることを確認してください。
2. モバイル機器のBluetoothまたはNFCアンテナ部分をデバイスに近づけてください。
3. モバイルクレデンシャルが認証されると出入口が開きます。

> **情報**
> - ユーザーは2つの通信モードから選択できます。 詳細については 高度な機能の設定 を参照してください。
>   - **Bluetoothモード**: モバイル機器がデバイスとワイヤレスで通信します。
>   - **NFCモード**: Android端末でのみ使用でき、モバイル機器をデバイスにかざして認証できます。
> - モバイル機器のBluetoothまたはNFCアンテナの位置はモデルによって異なる場合があります。 最適な接触ポイントはモバイル機器の仕様を参照してください。

モバイルカードを長押し

Suprema Passアプリでモバイルカードを長押しすることで出入口を開けることができます。

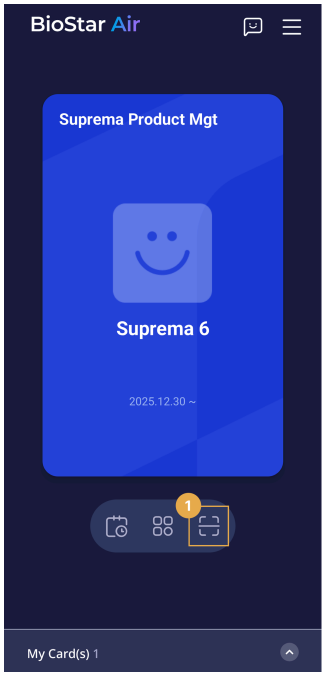
1. Suprema Passアプリの初期画面を表示してください。
2. BioStar Airと互換性のあるデバイスの近くで、モバイルカードを2-3秒間長押ししてください。
3. モバイルクレデンシャルが認証されると出入口が開きます。

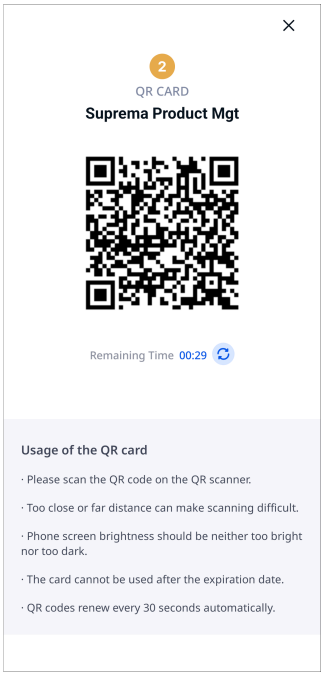
情報

- この機能を使用するには、**接続方式**設定で必ず**Background Mode**を選択してください。 詳細については 接続方法の設定 を参照してください。
- セキュリティ上の理由により、**サイト管理者がこの機能を無効にする場合があります。**
- **有効範囲はモバイル機器のBluetooth強度によって異なります。**
- 近隣の入退室制御リーダーが意図しない認証を引き起こす可能性があります。

QR コード認証

管理者がBioStar Airポータルで**QRリーダー**オプションを有効にしている場合、Suprema PassアプリでQRコードをQRリーダーにかざして出入口を開けることができます。 Suprema Passアプリのホーム画面で、モバイルカードの下にあるアイコンをタップしてください。





情報

- **QRリーダー**オプションの詳細は 拡張機能の設定 を参照してください。
- QRコード認証はQRリーダーが設置された出入口でのみ使用できます。

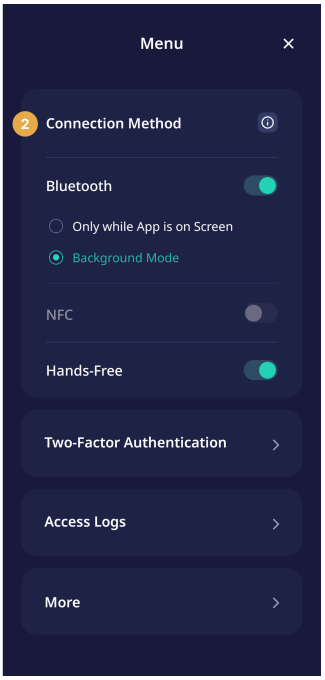
高度な機能の設定

Suprema Passアプリは、ユーザー体験と入退室管理機能を向上させるための高度な設定とセキュリティオプションを含みます。 ユーザーは認証方法の構成、2段階認証の有効化、アクセスログの確認、問題の報告およびサポート機能の利用ができます。

接続方式の設定

ユーザーは入退室管理機器との通信で使用する接続方式を選択できます。 Suprema Passアプリの初期画面で右上の ☰ アイコンをタップし、**接続方式**から希望のモードを選んでください。





Bluetooth

ユーザーは2つのBluetooth認証モードから選択できます。

- **アプリ起動時**: モバイル端末でアプリが開いているときのみモバイルカードで認証できます。 このモードはバッテリーを節約しますが、ドアに近づく前に手動でアプリを起動する必要があります。
- **バックグラウンドモード**: アプリがバックグラウンドで実行されている場合、端末の画面がオフでもモバイルカードで認証できます。 このモードはより便利ですが、バッテリーをより消費します。 アプリが終了した場合、バックグラウンド機能を再開するためにアプリを再起動する必要があります。

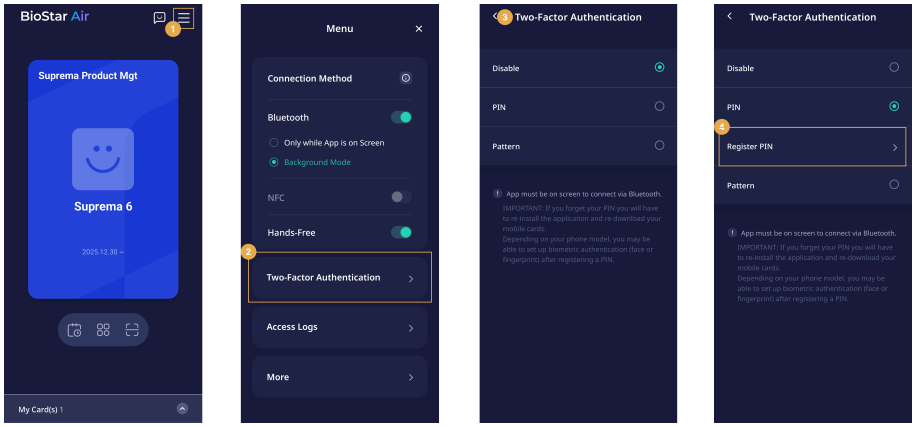
NFC

NFC認証はAndroid端末でのみ利用できます。 ユーザーは迅速な入退室のためにNFCを単独で使用するか、Bluetoothと併用できます。

> **情報**
> NFC対応端末を使用するAndroidユーザーは、Bluetoothと併用してNFCを使用できます。

二段階認証(2FA)

追加のセキュリティのために、ユーザーは**PIN、パターン、または生体認証**（顔または指紋）を使用して二段階認証を有効にできます。



情報

- この機能は入退室認証時にアプリ画面が開いている必要があるため、**バックグラウンドモード**の接続方式ではサポートされません。
- PINまたはパターンを忘れた場合は、アプリを再インストールしてモバイルカードを再有効化する必要があります。
- 端末によってサポートされる機能は異なる場合があります。

iOSユーザー

1. Suprema Passアプリの初期画面で右上の ☰ アイコンをタップしてください。
2. 接続方式を**アプリ起動時**に設定してください。
3. **二段階認証**をタップしてください。
4. **PIN番号登録**をタップしてください。
5. 6桁のPIN番号を入力してください。
6. 成功の通知メッセージが表示されたら、**OK**をタップしてください。

情報

- PIN番号を変更するには、**PIN番号変更**をタップしてから新しいPIN番号を入力してください。
- 生体認証機能を使用するには、**生体認証**を有効にして設定の案内に従ってください。

Androidユーザー

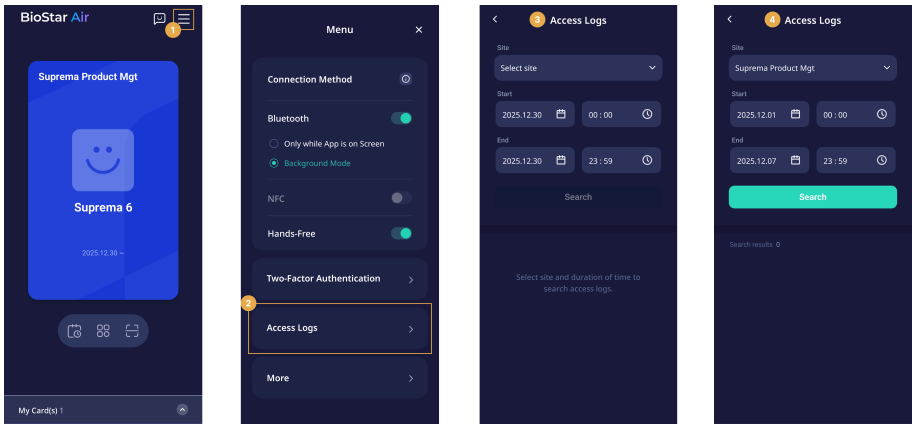
1. Suprema Passアプリの初期画面で右上の ☰ アイコンをタップしてください。
2. 接続方式を**アプリ起動時**または**NFC**に設定してください。
3. **二段階認証**をタップしてください。
4. **PIN番号** → **PIN番号登録** または **パターン** → **パターン登録** をタップしてください。
5. 選択したPIN番号またはパターンを入力してください。
6. 成功の通知メッセージが表示されたら、**OK**をタップしてください。

情報

- PIN番号を変更するには、**PIN番号変更**をタップしてから新しいPIN番号を入力してください。
- パターンを変更するには、**パターン変更**をタップしてから新しいパターンを入力してください。
- 生体認証機能を使用するには、**生体認証**を有効にして設定の案内に従ってください。

アクセスログ

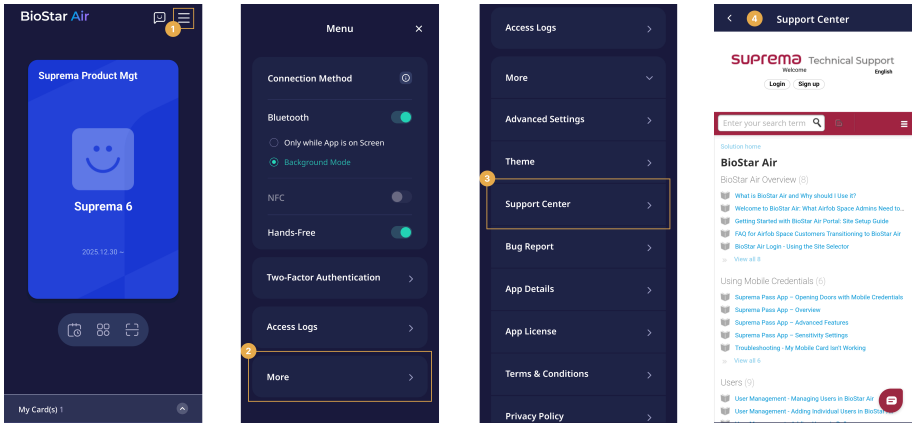
アクセス記録を通じてユーザーの入退室の試行を追跡し、入退室に関する問題を解決できます。



1. Suprema Passアプリの初期画面で右上の ☰ アイコンをタップしてください。
2. **出入記録**をタップしてください。
3. サイトを選択し、開始日と終了日を設定してください。
4. **検索**ボタンをタップしてください。

サポートセンター

追加サポートが必要なユーザーは、**サポートセンター**に入り、支援を受けることができます。



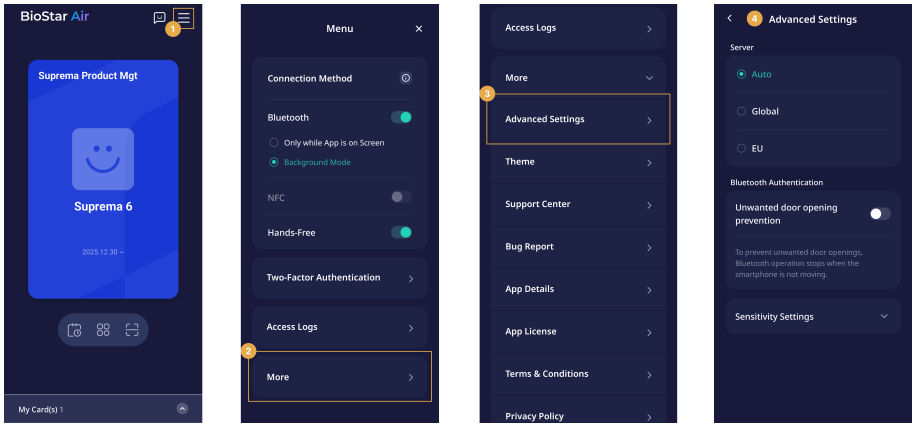
1. Suprema Passアプリの初期画面で右上の ☰ アイコンをタップしてください。
2. **その他**をタップしてください。
3. **サポートセンター**をタップしてください。

4. **Suprema Technical Support**ページに移動します。

> - 疑問点を検索するか、よくある質問を確認してください。
> - サポートが必要な場合は、右下のチャットアイコンをタップしてMOCAシステムチームにサポートチケットを送信できます。

高度な設定

Suprema Passアプリの初期画面で右上の ☰ アイコンをタップし、**その他** → **高度な設定**から次の追加機能を利用できます。



- **位置設定**：ユーザーの位置に応じて **グローバル** または **EU** サーバーを選択してください。 **自動**を選択すると、アプリが位置を検出して適切なサーバーを選択します。
- **Bluetooth認証**：モバイル端末が動いていないときにBluetooth認証が作動しないようにするには、**不要なドア開放の防止**オプションを有効にしてください。
- **感度設定**：モバイル端末とBioStar Air対応機器間のBluetooth検出感度を調整できます。 詳細については感度を設定するを参照してください。

追加機能

Suprema Passアプリの初期画面で右上の ☰ アイコンをタップし、**その他**から次の追加機能を利用できます。

- **テーマ**：アプリのカラーモードを設定できます。 **ライト**、**ダーク**、**システム**モードを選択できます。
- **バグレポート**：エラー発生状況や再現手順などの詳細を記入して開発者にバグレポートを提出できます。
- **アプリ詳細**：モバイル端末のモデル名、OSバージョン、BLEサポートおよび状態などの関連情報を確認できます。
- **アプリライセンス**：Suprema Passアプリに適用されるオープンソースライセンス情報を確認できます。
- **利用規約**：BioStar Airプラットフォームの利用規約を確認できます。

感度を設定する

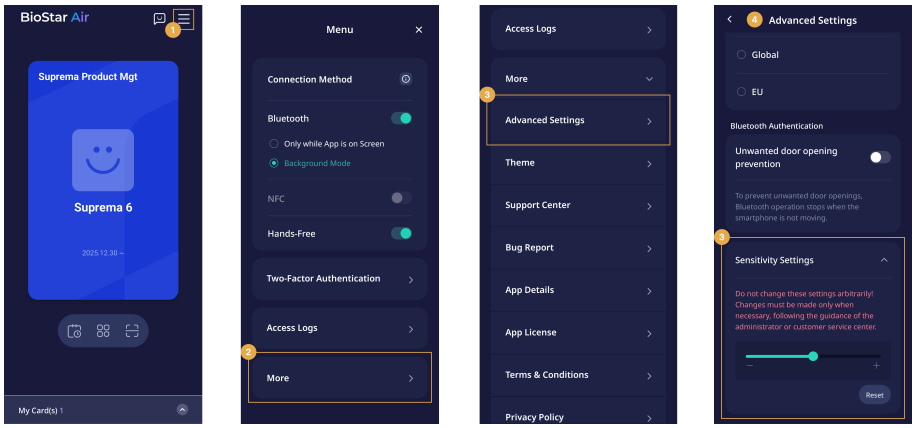
感度設定機能では、ユーザーがモバイル端末とBioStar Air対応機器間のBluetooth検出感度を調整できます。 この機能は円滑な認証を確保し、不要なアクセス試行や認証失敗を減らすのに役立ちます。

情報

モバイル機器のモデルごとにBluetooth信号の強さが異なるため、ユーザーは異なる認識距離を経験することがあります。 また、壁や干渉、BioStar Air対応機器の配置などの環境要因がBluetoothの検出に影響を与えることがあります。

感度設定の調整方法

ユーザーはモバイル機器のBluetooth強度と個人の好みに応じてBluetooth認証の感度を微調整できます。



1. Suprema Passアプリの初期画面で右上の ☰ アイコンをタップしてください。
2. **その他**をタップしてください。
3. **詳細設定**をタップ。
4. **感度設定**をタップして、スライダーを移動して感度を調整する。

情報

- 意図しない認証を防ぐには、 ー方向にスライダーを移動して感度を下げる。

  > *例：モバイル機器が机の上にあるとき*

- 認証に失敗する場合は、 十方向にスライダーを移動して感度を上げる。 ただし、モバイル端末はBioStar Air対応機器の非常に近くにある必要があります。

ヒント

iOSユーザー向けのヒント

Apple Payを利用しているiPhoneをBioStar Air対応機器に近づけると、Apple Payが起動します。 これは、モバイル端末のNFC領域がモバイルカード認証として検出されるためです。

解決策：感度設定を 十方向に調整すると、BioStar Air対応機器がモバイル端末のBluetooth信号をより早く検出するようになり、機器に直接触れる必要がなくなります。 これにより、Apple Payがトリガーされるのを防ぎつつ、スムーズに出入りできます。

開発者

BioStar AirはクラウドベースのRESTful APIを提供しています。 外部システムとの連携、ユーザーライフサイクルの自動化、認証情報の管理をAPIで行うことができます。 デモ環境を構築し、認証フローを理解したうえで、ユーザー管理APIを使って実際の統合を実装してください。

クイックスタート

BioStar Airのデモサイトを設定し、対応デバイスを接続・登録してクラウドAPI連携をテストする方法をご案内します。 BioStar 2で作業した経験があるなら、多くの概念が馴染み深く感じられるでしょう。 BioStar Airは完全なクラウドベースのシステムです。

事前要件

開始する前に次の項目を確認する。

- 工場出荷時に初期化されたファームウェアを搭載した**BioStar Air対応機器**を用意する。
  - XP2-AIR、XS2-AIR、BEW3-AIR、BS3-AIR、BLN2-AIR
  - 機器は認定のSuprema販売代理店を通じて購入できる。
- 機器はイーサネット経由でインターネットに接続されている必要がある。
- ネットワークでアウトバウンドアクセスを許可する。
  - Port 443 (HTTPS)
  - Port 5671 (MQTT over TLS)

デモ環境とAPIキーの設定

1 サインアップとログイン

1. BioStar Air Developer に移動する。
2. 「**サインアップ**」をクリックし、フォームを記入して承認を待つ。
3. 承認が完了したら、ユーザーのメールアドレスとパスワードを使って開発者ポータルにログインしてください。

> **情報**
> 開発者ポータルのメールアドレスとパスワードはデモポータルでは使用できません。

2 デモアプリケーションの作成

1. 「**API**」→「**Management**」に移動する。

2. 「+ Register」ボタンをクリックする。
3. アプリケーションタイプをDemoに選択する。
4. アプリケーション名を入力し、Registerボタンをクリックする。
5. デモアプリケーションの登録が完了すると、*site_info.csv* ファイルをダウンロードできます。

> **情報**
>
> - *site_info.csv* ファイルには、エイリアスのメールアドレスとパスワードが含まれています。
> - デモポータルにログインする際は、必ずこのエイリアスのメールアドレスとパスワードを使用してください。
> - **開発者ポータルにログインするためのメールアドレスとパスワードをデモポータルで使用しないでください。**

3 APIキーの発行

1. 「API」→「Management」に移動する。
2. 登録済みのアプリケーションをクリックしてください。
3. 「API Management」までスクロールする。
4. 「Add」ボタンをクリックする。
5. 名前を入力して確認する。
6. 生成されたAPIキーをコピーして安全に保存してください。

このAPIキーを使って、デモ環境へのAPIリクエストを認証できます。

4 デモポータルへのログイン

1. 開発者ポータルのメニューでDemo Portalをクリックするか、https://demo.airfobspace.com/login に直接アクセスしてください。
2. *site_info.csv* ファイルに記載されているエイリアスのメールアドレスとパスワードでログインしてください。

> **情報**
> **開発者ポータルにログインするためのメールアドレスとパスワードをデモポータルで使用しないでください。**

デバイスの登録

モバイル機器でBioStar Air Demo App（Android専用）を使用する。

1. BioStar Air Developers に移動してデモアプリをダウンロードしてください。
2. デモアプリを起動し、*site_info.csv* ファイルに記載されているエイリアスのメールアドレスとパスワードでログインしてください。
3. Android端末をリーダーの近く（BLEの範囲内）に持っていく。

- 「All Menu」→「Devices」で右上の＋ボタンをタップする。
- デバイスを検索して**Register**ボタンをタップする。

4. 機器が音を出して再起動し、登録済みデバイス一覧に表示される。

> **情報**
> デバイスはモバイルアプリを通じてのみ登録できる。 ウェブポータルでは登録できない。 APIベースの登録には、パートナーに提供されない暗号化証明書が必要である。

デバイス管理

デモアプリまたはデモウェブポータルでデバイスを管理できる。

- **BioStar Air Demo App**
- **Demo Web Portal:** https://demo.airfobspace.com/login

Demo vs Production

- **Demo**サイト（テスト用）は開発者ポータルから作成される。
- **Production**サイトはパートナーポータルから作成され、サイトID、ユーザーのメールアドレスおよびパスワードが必要となる。 Productionサイトは承認された販売店またはSupremaの支店のみが作成できる。

> **情報**
> - ユーザーIDとアカウントIDは異なる。 混同しないこと。
> - 複数のサイトを管理する場合は、パスワードを安全に保管する。
> - 常に最新のBearerトークンを使用する。
> - ブラウザからコピーしたBearerトークンはPostmanで再利用できる。

サポートが必要ですか？

Supremaのテクニカルサポートポータルでチケットを作成する。 https://support.supremainc.com

API認証

BioStar Air Cloud APIはBearerトークン（JWT）ベースの認証を使用します。 APIを呼び出す前にログインしてトークンを取得し、すべてのリクエストのAuthorizationヘッダーにトークンを含める必要があります。

APIベースURL

環境	Base URL	説明
Demo（TEST）	https://sp-demo-api.airfob.com/v1	アプリケーションの種類を「Demo」として登録すると、デモ環境のサイトとサイトマスターのアカウント情報をCSVファイルでダウンロードできます。
Production（LIVE）	https://sp-api.airfob.com/v1	（**自動ルーティング**）クライアントの地域に応じて、グローバルまたはEUのサーバーを自動で選択します。
	https://sp-a-api.airfob.com/v1	（**グローバル専用**）グローバルサーバー環境に接続されます。
	https://sp-e-api.airfob.com/v1	（**EU専用**）EUサーバー環境に接続されます。

> **自動ルーティング**環境では、地域検出により予期しないルーティング（routing）が発生することがあります。

APIログイン手順

Postman またはプログラムからAPI呼び出しを行うことができる。

ログイン

- **Endpoint**：`login`
- **Payload**：

```
{
  "username": "your_email",
  "password": "your_password"
}
```

Bearerトークン（JWT）を返す。

アカウント情報の取得

- **Endpoint**：`getSelfAccounts`
- **Authorization**：Bearer Token

アクセス可能なサイトおよびアカウントの一覧を返す。

アカウントにログイン

- **Endpoint**：`loginAccount`
- **Authorization**：Bearer Token

特定サイトのトークンを返す。

ウェブブラウザでBearerトークンを取得する方法

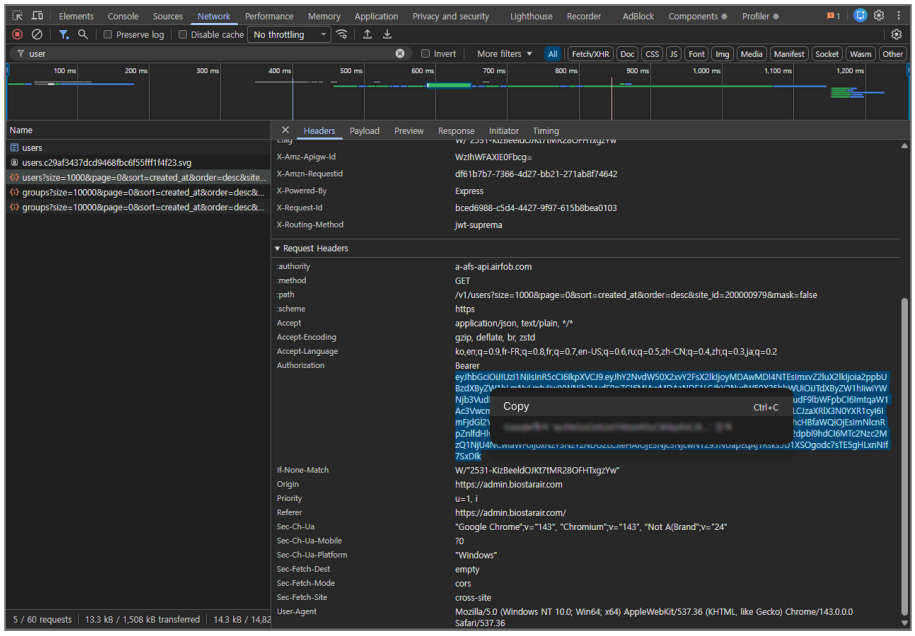
Postmanを使わずに、ブラウザの開発者ツールで直接Bearerトークンを取得できます。

Chrome/Edge（WindowsまたはMac）

1. ウェブブラウザで `F12` または `Ctrl/Cmd + Shift + I` を押す。
2. **Network** タブに移動する。
3. ページをリロードする。
4. API呼び出しを検索する。

   > *例:* `groups`, `login`

5. リストからリクエストをクリックする。
6. 「**Headers**」タブに移動する。
7. リクエストヘッダで `Authorization: Bearer ...` を探す。
8. 右クリックしてトークンをコピーしてください。



Safari（Mac）

1. 「開発者」メニューを有効にしてください。 Safari → Preferences → Advanced → **Show Develop menu**をチェックする。
2. **Develop → Show Web Inspector** に移動する。

3. **Network** タブに移動する。
4. ページをリロードする。
5. API呼び出しをフィルタリングして検査する。
6. リクエストヘッダから `Authorization: Bearer` トークンをコピーする。

> **情報**
> ブラウザからコピーしたBearerトークンはPostmanで再利用できる。 常に最新のBearerトークンを使用してください。

ユーザー管理APIの使い方

認証トークンを取得したら、APIを使ってユーザーのライフサイクルを管理できます。 ユーザーの取得、作成、更新、停止などのエンドポイントを使用して、BioStar Airサイトのユーザーを自動化して管理できます。

推奨されるAPI統合範囲

API統合は可能な限り以下の範囲に限定する。

- ユーザーライフサイクル（作成/更新/削除）の管理
- クレデンシャル管理（mobile、RFカード、生体認証）

管理者が既存のBioStar Airウェブおよびモバイル管理アプリを使用できるようにする。

- 入退室レベル
- スケジュール
- ドアおよびデバイス設定
- サイト設定

ユーザー管理API呼び出し

ログイン後、次のエンドポイントを使用してユーザーを管理する。

- `getUsers`
- `createUser`
- `updateUser`
- `suspendUsers`

常にAuthorizationヘッダにBearerトークンを含める。

> ユーザーを有効化するには、少なくとも1つのクレデンシャルタイプを割り当てる必要がある。
>
> > *例: RFカード、mobile、LinkPass*

アプリケーション例

以下は、APIを介してCSVファイルをアップロードし、ユーザーを一括で停止できるPythonアプリのサンプルコードです。

Python

```
import requests
import csv
import getpass
from pathlib import Path

def select_server():
    servers = {
        "1": ("Demo", "https://demo-afs-api.airfob.com/v1"),
        "2": ("Global", "https://a-afs-api.airfob.com/v1"),
        "3": ("EU", "https://e-afs-api.airfob.com/v1")
    }

    print("Please select a server:")
    for key, (name, _) in servers.items():
        print(f"{key}: {name}")

    choice = input("Enter server number: ").strip()
    return servers.get(choice, (None, None))[1]

def login(base_url, username, password):
    url = f"{base_url}/login"
    payload = {"username": username, "password": password}
    response = requests.post(url, json=payload)
    response.raise_for_status()
    data = response.json()
    token = data.get("access_token")
    if not token:
        raise ValueError("Login succeeded but no access_token returned.")
    print("✅ Login successful.")
    return token

def login_to_account(base_url, token, account_id):
    url = f"{base_url}/login/{account_id}"
    headers = {"Authorization": f"Bearer {token}"}
    response = requests.post(url, headers=headers)
    response.raise_for_status()
    new_token = response.json().get("access_token")
    if new_token:
        print(f"✅ Switched to account ID: {account_id}")
        return new_token
    return token

def get_accounts(base_url, token):
    url = f"{base_url}/accounts/self"
    headers = {"Authorization": f"Bearer {token}"}
    response = requests.get(url, headers=headers)
    response.raise_for_status()
    accounts = response.json().get("accounts", [])
    return [{"id": acc["id"], "name": acc["site"]["name"]} for acc in accounts]

def suspend_users_from_csv(base_url, csv_path, token):
    if not Path(csv_path).exists():
        print(f"❌ File not found: {csv_path}")
        return

    headers = {"Authorization": f"Bearer {token}"}
```

```
    with open(csv_path, newline='', encoding='utf-8-sig') as f:
        reader = csv.DictReader(f)

        # Normalize headers
        reader.fieldnames = [field.strip().lower() for field in reader.fieldnames]
        if 'email' not in reader.fieldnames:
            print("❌ Missing required 'email' column in CSV.")
            return

        for row in reader:
            email = row.get("email")
            if not email:
                print("⚠️ Skipping row with missing email.")
                continue

            # Search user
            search_url = f"{base_url}/users/search"
            payload = {"filters": [{"field": "email", "equals": email}]}
            search_resp = requests.post(search_url, headers=headers, json=payload)
            if search_resp.status_code != 200:
                print(f"❌ Failed to search user {email}: {search_resp.text}")
                continue

            users = search_resp.json().get("users", [])
            if not users:
                print(f"❌ No user found with email: {email}")
                continue

            user_id = users[0]["id"]

            # Suspend user
            suspend_url = f"{base_url}/users/suspend"
            suspend_payload = {
                "ids": [user_id],
                "certify_by": "none",
                "use_site_template": True
            }
            suspend_resp = requests.post(suspend_url, headers=headers, json=suspend_payload)
            if suspend_resp.status_code == 200:
                print(f"✅ Suspended user: {email}")
            else:
                print(f"❌ Failed to suspend user {email}: {suspend_resp.text}")

def main():
    base_url = select_server()
    if not base_url:
        print("❌ Invalid selection. Exiting.")
        return

    print("\n🔑 BioStar Air Login")
    username = input("Email: ")
    password = getpass.getpass("Password: ")

    token = login(base_url, username, password)
    accounts = get_accounts(base_url, token)

    print("\n🌐 Available Sites:")
```

```
    for i, acc in enumerate(accounts):
        print(f"{i}: {acc['name']} (ID: {acc['id']})")

    selected = int(input("\nSelect site number to log into: "))
    account_id = accounts[selected]["id"]
    token = login_to_account(base_url, token, account_id)

    csv_path = input("Enter path to CSV file with user emails: ").strip()
    suspend_users_from_csv(base_url, csv_path, token)

if __name__ == "__main__":
    main()
```

トラブルシューティング

BioStar Airのご利用中に予期せぬ問題が発生しましたか？ このドキュメントでは、BioStar Airの使用中によく発生する問題の原因を特定し、解決方法を案内します。

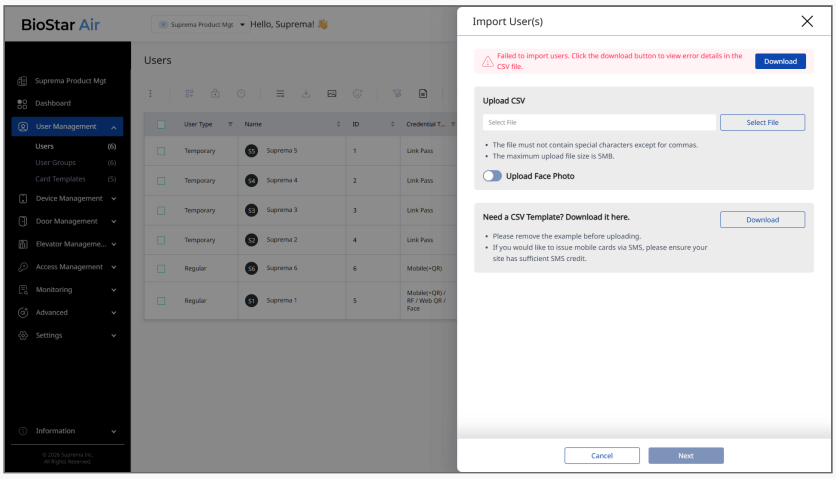
以下の問題を選択して、段階的な解決手順を確認してください。

一括ユーザー追加の問題

複数の顧客やパートナーから、ユーザーリストを一括で追加する際に問題が発生するという報告がありました。 ほとんどの問題は、形式が不正なCSVファイルが原因です。 一括追加機能が期待通りに動作するよう、以下の指示に正確に従ってください。

情報

v2.10から、BioStar Airは不正な項目を含むCSVファイルをアップロードした場合、検証レポートを返します。 エラーを修正した後、ファイルを再アップロードしてください。



CSVファイルの準備

CSVテンプレートのダウンロード

1. 画面左のサイドバーで **ユーザー管理** → **ユーザー** に移動します。
2. 画面右上の **ユーザー追加** → **ユーザーをインポートする** をクリックします。
3. **ユーザーをインポートする** パネルが表示されたら、**ダウンロード** ボタンをクリックします。
4. CSVテンプレートファイル(*biostar-import-user-csv-example.csv*)をローカルに保存します。

CSVテンプレートの正確な形式を使用する

- **列(column)を手動で追加または削除しないでください。** 予期しない列(column)があるとエラーが発生する可能性があります。
- 追加フィールド（例：従業員IDまたは部署）を含める必要がある場合は、ユーザー一覧の上部にある**ユーザーテンプレート**(

)機能を使って該当するフィールドを追加してください。 フィールドを追加すると、ダウンロードしたCSVファイルに該当する列が自動的に含まれます。

各列の要件を参照してデータを正しく入力してください。

ユーザー・キー

- 各ユーザーの一意の数値IDです。
- **ユーザー・キー** 列は**空にすることができ**、システムが自動的に値を割り当てます。
- ユーザーIDを手動で入力する場合
  - **数字のみ** を使用してください。
  - **一意の値** を使用してください。
  - 文字、空白、ハイフン、または特殊文字を含めないでください。

> **注意**
> 文字を含む会社固有の従業員IDを使用する場合は、**ユーザー・キー** フィールドを使用しないでください。 代わりに、**ユーザーテンプレート** 機能を使用して別のカスタムユーザーフィールドを作成してください。

メール

- 有効なメール形式を使用してください。 検証式を参照してメール形式を検証できます。
  - 空白を含めることはできません。
  - `@`（アットサイン）を含める必要があります。
  - ドメインにはピリオド(`.`)およびトップレベルドメインを含める必要があります。

    例：example.com、gmail.com、suprema.co.kr
  - アドレスの末尾に追加のピリオドがあってはなりません。
  - 特殊文字または不可視文字があってはなりません。
  - メールアドレスである必要があります。 '提供されていません' または '提供しない' のようなエラーが発生する可能性があります。
- メールアドレスは**一意である必要があります**。 ファイル内や既存ユーザー間での重複は許可されません。
- 以下のクレデンシャルを発行する場合、メールアドレスは必須です。
  - **モバイルカード**
  - **Web QR**
  - **リンクパス**
- RFIDカードのみを所持しているユーザーはメールアドレスの入力は不要です。

モバイル

- モバイルSMSでクレデンシャルを送信しない場合は任意です。

- メールアドレスと同様に**一意である必要があり**、ファイル内や既存ユーザー間での重複は許可されません。
- クレデンシャルを配布する際は、メールを推奨します。 SMSメッセージは追加料金が発生します。

日付 (開始日 / 有効期限)

すべての日付フィールドは以下の正確な形式に従う必要があります。

```
YYYY-MM-DDTHH:MM:SS.sssZ

Example:
1995-05-09T00:00:00.000Z
```

'Z'を欠いていたり、ダッシュ(`—`)の代わりにスラッシュ(`/`)を使用したり、時間を省略するなどの些細な違いもアップロード失敗の原因になります。

クレデンシャルの要件

クレデンシャル形式	メールまたは電話番号
RFカード Only	いいえ。
モバイルカード / **Web QR** / **リンクパス**	はい、1つ必要です。

- クレデンシャルはメールアドレスまたは電話番号を通じて送信される必要があります。
- 両方を提供することはできますが、**モバイル形式のクレデンシャル**には**最低1つが必要**です。
- メールは無料です。 SMSは料金が発生します。

事前検証のためのExcel数式

データをアップロードする前に、**ヘルパー列**で次の数式を使ってデータを確認することを推奨します。

メールまたは電話番号の重複検証

Detect Duplicate Emails or Phone Numbers

```
=IF(E2="", "", IF(COUNTIF(E$2:E2, E2)>1, "Duplicate", "First Occurrence"))
```

日付形式の検証

Validate ISO 8601 Date Format (Column Q)

```
=IF(Q2="", "", IF(AND(LEN(Q2)=24,
  ISNUMBER(VALUE(MID(Q2,1,4))), MID(Q2,5,1)="-",
  ISNUMBER(VALUE(MID(Q2,6,2))), MID(Q2,8,1)="-",
  ISNUMBER(VALUE(MID(Q2,9,2))), MID(Q2,11,1)="T",
  ISNUMBER(VALUE(MID(Q2,12,2))), MID(Q2,14,1)=":",
  ISNUMBER(VALUE(MID(Q2,15,2))), MID(Q2,17,1)=":",
  ISNUMBER(VALUE(MID(Q2,18,2))), MID(Q2,20,1)=".",
  ISNUMBER(VALUE(MID(Q2,21,3))), RIGHT(Q2,1)="Z"),
  "Valid", "Invalid"))
```

メール形式の検証

Validate Email Format (Column E)

```
=IF(TRIM(E2)="", "", IF(AND(
  ISNUMBER(FIND("@", E2)),
  ISNUMBER(FIND(".", E2)),
  FIND("@", E2) > 1,
  FIND(".", E2, FIND("@", E2)) > FIND("@", E2) + 1,
  LEN(E2) - LEN(SUBSTITUTE(E2, "@", "")) = 1,
  ISERROR(FIND(" ", E2))
), "Valid", "Invalid"))
```

エラーが発生しますか？

- 正しいテンプレートをダウンロードし、列を追加していませんか？
- モバイルクレデンシャルを受け取るユーザーのすべての必須フィールドが記入されていますか？
- メールアドレスと電話番号はファイル内および既存ユーザー間で一意ですか？
- 日付とメール形式は上記の通り正確ですか？

情報

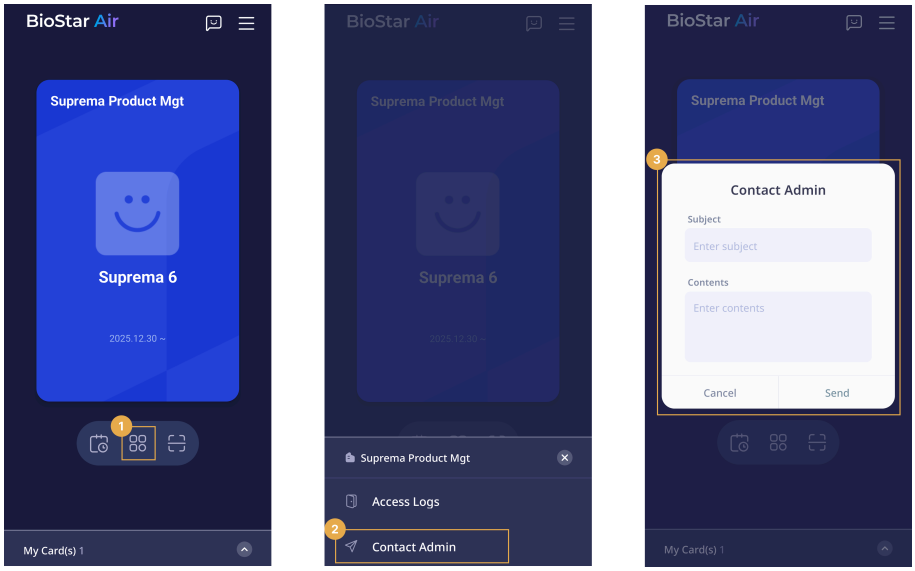
- サービスチームはファイルの修正サービスを提供しません。 ファイルがアップロードされない場合は、上記の検証ツールを使用して問題を特定し、解決してください。
- この文書は、サービスチームによる手動のトラブルシューティングなしでアップロードを正常に完了できるように支援するために作成されています。

モバイルカードが動作しません

モバイルカードは機器と認証されているが、ドアが開かない場合は、以下の案内に従って問題を解決してください。

BioStar Air 管理者に問い合わせる

サイト管理者はモバイルカードの再発行、一時的なモバイル端末の問題、設定の問題を支援できます。



1. Suprema Passアプリでモバイルカードの下にある アイコンをタップしてください。
2. 下部のパネルが表示されたら、**管理者に問い合わせる**をタップします。
3. ポップアップが表示されたら、タイトルと内容を入力してください。
4. メッセージを管理者に送信するには、**送信**をタップします。

モバイルカードが削除されましたか？

モバイル端末を変更したりSuprema Passアプリを再インストールした場合、セキュリティ上の理由によりすべてのモバイルカードが削除されます。 以下はモバイルカード再発行の問い合わせ先です。

- **Company Spaces:** HR、IT、セキュリティまたは運用チーム
- **Shared Spaces:** エリア管理者またはカスタマーサービスチーム

> **情報**
> 管理者がBioStar Airでユーザーのクレデンシャルを再発行すると、以前に発行されたモバイルクレデンシャル、QRコード、リンクパス（LinkPass）はすべて取り消され、新しいクレデンシャルに置き換えられます。 ユーザーは、サイト設定に応じてメールまたはSMSで新しいクレデンシャルリンクを受け取ります。 ユーザーはそのリンクから、Suprema Passアプリに新しいモバイルクレデンシャルをダウンロードするか、新しいQRコードまたはリンクパスを使用する必要があります。 取り消されたモバイルクレデンシャル、QRコード、またはリンクパスで入退室を試みると、失敗します。

ステップ別トラブルシューティング

1 Suprema Passアプリでエラーメッセージが表示されましたか？

- ドアが開かない場合は、Suprema Passアプリで再認証を試してください。
- エラーメッセージが表示されたら、スクリーンショットを撮ってサイト管理者と共有してください。

❷ モバイル端末のBluetoothはオンになっていますか？

モバイルカードはモバイル端末と出入管理機器間のBluetooth通信に依存します。

- Bluetoothがオンになっていることを確認してください。
- Bluetoothを一度オフにしてから再度オンにしてください。
- 必要に応じてモバイル端末を再起動してください。

❸ Suprema Passアプリの位置情報権限を許可してください

BluetoothおよびNFC認証には位置情報権限が必要です。

1. モバイル端末の**設定** → **アプリ**に移動します。
2. **Suprema Pass**アプリを選択します。
3. **権限** → **位置情報**で位置アクセス許可を**常に許可**または**アプリ使用中のみ許可**に設定します。

❹ 無線ネットワークとWi-Fi接続を確認してください

モバイルカード認証には安定した無線ネットワークまたはWi-Fi接続が必要です。

❺ 選択した接続方法を使用しましたか？

Suprema Passアプリで接続方式を確認してください。

- Suprema Passアプリの初期画面で右上の ☰ アイコンをタップしてください。
- **接続方式**で認証モードを確認してください。
- **バックグラウンドモード**を使用する場合、アプリがバックグラウンドで起動している必要があります。

❻ 認証時にモバイル端末が振動しましたか？

- 端末が振動したがドアが開かなかった場合は、Suprema Passアプリを開いて再認証を試してください。
- エラーメッセージが表示されたら、スクリーンショットを撮ってサイト管理者と共有してください。

位置サービスを有効にする必要がありますか？

モバイル機器のSuprema Passアプリでモバイル入退室カードにより認証を行うには、位置情報サービスが必要です。 これにより、モバイル端末と入退室管理装置との安全なBluetooth通信が確保されます。

Q. Airfob Space から BioStar Air へ移行する必要がありますか？

いいえ。既存の Airfob Space のお客様は、そのままプラットフォームをご利用いただけます。現在、強制的なマイグレ

ーションはありません。

Q. 自分のデバイスやデータに影響はありますか？

いいえ。両プラットフォームは同じバックエンドを共有しています。デバイス、ユーザーデータ、設定は両サービス間で完全に互換性があります。

Q. Suprema PassをAirfob Spaceアプリの代わりに使用する必要がありますか？

既存のモバイル認証ユーザーをBioStar Airに移行する必要はありません。app.airfobspace.com のURLまたはAirfob Proアプリを使用してユーザーを管理しモバイル認証を発行する場合、当該ユーザーはAirfob Spaceアプリを使用するための招待を受け取ります。admin.biostarair.com またはBioStar Airアプリを使用してユーザーを管理しモバイル認証を発行する場合、当該ユーザーはSuprema Passアプリを使用するための招待を受け取ります。

Q. サポート体制や料金は変更されますか？

サポートや料金のプロセスに即時の変更はありません。ただし、時間の経過とともに、BioStar Air がドキュメント、サポート、機能発表の主要ブランドになります。

Q. 希望する場合、BioStar Airに切り替えることはできますか？

はい。バックエンドを共有しているため移行は簡単ですが、ブランディングや機能の提供に若干の違いが生じる場合があります。admin.biostarair.com と BioStar Air アプリを使用してサイト管理を開始してください。app.airfobspace.com の既存の管理者ログイン情報をそのまま利用できます。

Q. BioStar Air の利点は何ですか？

BioStar Air は将来志向のブランドです。今後の改善、統合強化、UI/UX の更新、そして Airfob Space には戻らない可能性のある新機能を継続的に提供していきます。

Q. 今後の機能は Airfob Space と互換性がありますか？

一部は互換性がありますが、すべてではありません。新機能は今後 BioStar Air だけの専用となる場合があります。最適な体験とサポートを得るには、新しい導入には BioStar Air をご利用ください。

ビデオ再生のトラブルシューティング

BioStar Airにカメラを登録した後、録画ビデオが再生されない場合は、以下の手順に従って問題を診断し解決してください。 この手順に従うことで、ビデオ再生の問題を解決し、BioStar Airで正常に動作することを確認できます。

情報

カメラ登録の詳細については、IPカメラのサポートおよび設定をご参照ください。

Q. Airfob Space から BioStar Air へ移行する必要がありますか？

いいえ。既存の Airfob Space のお客様は、そのままプラットフォームをご利用いただけます。現在、強制的なマイグレーションはありません。

Q. 自分のデバイスやデータに影響はありますか？

いいえ。両プラットフォームは同じバックエンドを共有しています。デバイス、ユーザーデータ、設定は両サービス間で完全に互換性があります。

Q. Suprema PassをAirfob Spaceアプリの代わりに使用する必要がありますか？

既存のモバイル認証ユーザーをBioStar Airに移行する必要はありません。app.airfobspace.com のURLまたはAirfob Proアプリを使用してユーザーを管理しモバイル認証を発行する場合、当該ユーザーはAirfob Spaceアプリを使用するための招待を受け取ります。admin.biostarair.com またはBioStar Airアプリを使用してユーザーを管理しモバイル認証を発行する場合、当該ユーザーはSuprema Passアプリを使用するための招待を受け取ります。

Q. サポート体制や料金は変更されますか？

サポートや料金のプロセスに即時の変更はありません。ただし、時間の経過とともに、BioStar Air がドキュメント、サポート、機能発表の主要ブランドになります。

Q. 希望する場合、BioStar Airに切り替えることはできますか？

はい。バックエンドを共有しているため移行は簡単ですが、ブランディングや機能の提供に若干の違いが生じる場合があります。admin.biostarair.com と BioStar Air アプリを使用してサイト管理を開始してください。
app.airfobspace.com の既存の管理者ログイン情報をそのまま利用できます。

Q. BioStar Air の利点は何ですか？

BioStar Air は将来志向のブランドです。今後の改善、統合強化、UI/UX の更新、そして Airfob Space には戻らない可能性のある新機能を継続的に提供していきます。

Q. 今後の機能は Airfob Space と互換性がありますか？

一部は互換性がありますが、すべてではありません。新機能は今後 BioStar Air だけの専用となる場合があります。最適な体験とサポートを得るには、新しい導入には BioStar Air をご利用ください。

Suprema Inc.

17F Parkview Tower, 248, Jeongjail-ro, Bundang-gu, Seongnam-si, Gyeonggi-do, 13554, Rep. of KOREA

電話: +82 31 783 4502 | Fax: +82 31 783 4503 | お問い合わせ: sales_sys@supremainc.com

Supremaのグローバル支社の詳細については、
QRコードをスキャンして以下のWebページにアクセスしてください。
https://www.supremainc.com/en/about/contact-us.asp

© 2026 Suprema, Inc. 本書に記載されている Suprema および Suprema 社の製品名および番号は、Suprema, Inc. の登録商標です。Suprema 社以外のすべてのブランドおよび製品名は、それぞれの企業の商標または登録商標です。製品の外観、ビルドステータスおよび/または仕様は、予告なく変更されることがあります。