BioStar X Mobile

管理者ガイド

バージョン 1.0.5

日本語

JA 102.00.BSX

suprema
SECURITY & BIOMETRICS

目次

開始する前に 5

サポート環境 5

ライセンスとネットワーク要件 5

はじめに 7

BioStar Xモバイルアプリのダウンロード 7

アプリ権限 7

アプリの起動と初期設定 8

接続のトラブルシューティング 8

アプリの使用 9

アプリ設定 10

アプリのバージョン情報を確認 10

ログイン設定 11

標準タイムゾーン設定 13

日付と時刻の表示形式設定 14

生体認証で変更内容を確認 14

ライセンス情報とプライバシーポリシーを確認 15

ユーザー管理 16

ユーザー登録 16

ユーザーの編集と削除 31

ユーザーログイベントを確認する 32

ユーザーの検索とフィルタリング 34

ドア管理 36

ドアのリモート制御 36

ドア詳細情報を確認する 38

デバイス管理 42

デバイス情報の確認 42

デバイス状態の確認 42

認証失敗ロックの解除 43

デバイス検索 44

デバイス一覧をフィルタリングする 45

リアルタイムログモニタリング 46

リアルタイムログの確認 46

特定のログのみ表示 47

ログ詳細情報の確認 48

過去ログの照会 49

過去ログの照会 50

特定のログのみを表示 51

ログ詳細情報の確認 48

警報アラームの確認と解除 53

警報アラーム一覧 (Alert List) 53

警報アラーム履歴 (Alert History) 54

出席確認（Roll Call）を開始する 55

モバイルアプリで出席確認を使用する 55

クイックアクションを使用する 62

クイックアクションの実行 62

クイックアクションの詳細 62

アカウントのパスワードを変更する 64

付録 **65**

免責事項 65

著作権に関するお知らせ 66

オープンソースライセンス 66

開始する前に

BioStar X モバイルアプリを使用する前に、次の項目を確認してからアプリをインストールしてください。

サポート環境

次の条件で BioStar X モバイルアプリを使用できます。

- **対応システム**: BioStar X
- **サーバー要件**: API アクセスが可能な BioStar X サーバーが必要
- **ユーザー**: サポート対象の権限は、事前定義されたすべてのアカウントレベルです。将来的に、カスタムアカウントレベルのサポートを追加する予定です。
- **モバイルデバイス**: iOS 13.0 以上、または Android 7.0 以上

> **情報**
> BioStar X モバイルアプリは単独では動作できません。社内で運用中の BioStar X サーバーに接続する必要があります。
> - BioStar X インストールの最小仕様の詳細については システム最小要件 を参照してください。
> - BioStar X のインストールの詳細については 簡単インストール を参照してください。

ライセンスとネットワーク要件

BioStar X モバイルアプリを使用するには、BioStar X ライセンスが必要です。ライセンス追加オプションを購入して利用できます。ライセンスポリシーの詳細については、ライセンス ポリシーを参照してください。

接続環境	必要ライセンス
同じネットワーク	モバイルアプリライセンス
外部ネットワーク（公開 IP）	モバイルアプリライセンス
外部ネットワーク（公開 IP なし）	モバイルアプリライセンス + リモートアクセスライセンス

- BioStar X サーバーとモバイルアプリを連携して使用するには、**モバイルアプリ** ライセンスが必要です。
- 基本的に、同じネットワーク内から BioStar X サーバーに接続してモバイルアプリを使用できます。
- 外部ネットワークから接続するには公開 IP アドレスが必要です。ない場合は、**リモートアクセス** ライセンスを追加購入してください。

情報

- BioStar X のライセンス適用方法に関する詳しい情報は、BioStar Xライセンス をご参照ください。
- BioStar X のサーバー設定に関する詳しい情報は、サーバーの詳細を設定する をご参照ください。
- BioStar X のリモートアクセス機能に関する詳しい情報は、リモートアクセスを設定する をご参照ください。

次のステップ

事前準備が完了したら、BioStar X モバイルアプリのインストール方法を確認してください。

はじめに

BioStar Xモバイルアプリは iOSとAndroidで利用できます。案内に従ってアプリをインストールした後、BioStar Xサーバーに接続してください。

BioStar Xモバイルアプリのダウンロード

次の提供リンクまたはQRコードからアプリをダウンロードしてください。

プラットフォーム	ダウンロードリンク	QR コード
iOS	App Store	
Android	Google Play	

アプリ権限

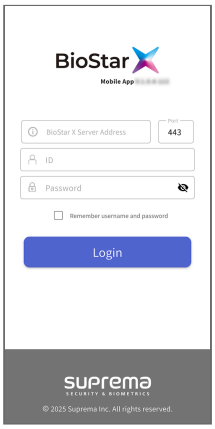
BioStar Xモバイルアプリは、特定の機能を使用する際に次の権限を要求します。初回インストール時には権限を要求しません。

権限	必須かどうか	用途
ストレージ	任意	ユーザー画像（ギャラリーや端末のストレージなど）を管理してアップロードするために必要です。
カメラ	任意	顔画像のエンロールと動画録画のための画像キャプチャに使用します。
生体認証	任意	モバイル端末のFingerprintまたは顔認証を使ったセキュアログインに必要です。

> **情報**
> すべての権限は必須ではなく、ユーザーはアプリの基本機能に影響を与えずに権限を任意で拒否できます。

アプリの起動と初期設定

アプリを起動すると、BioStar Xサーバー接続用の情報を入力する画面が表示されます。



- **BioStar X Server Address**: BioStar XサーバーのIPアドレスまたはドメインアドレスを入力してください。
- **Port**: BioStar Xサーバーのポート番号を入力してください。デフォルトは`443`です。
- **ID** / **Password**: BioStar Xサーバーにログインするための IDとパスワードを入力してください。

必要な情報をすべて入力した後、ログインするには**Login**をタップしてください。

> **情報**
>
> - アカウントIDとパスワードを入力欄に保存するには、**Remember username and password**オプションのチェックボックスを選択してください。次回のログイン時に、入力したIDとパスワードが自動入力されます。
> - BioStar XサーバーのIPアドレス、ポート番号を確認するには、サーバーの詳細を設定するを参照してください。

接続のトラブルシューティング

ログインに失敗した場合は、以下を確認してください。

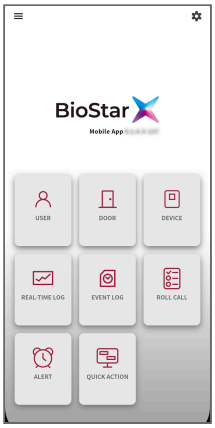
- BioStar Xサーバーのアドレスとポート番号が正しいか確認してください。
- アカウントIDとパスワードが正しいか確認してください。
- モバイル端末とBioStar Xがネットワークに接続されているか確認してください。

情報

外部ネットワークから接続するには公開 IP アドレスが必要です。ない場合は、**リモートアクセス** ライセンスを追加購入してください。詳しくは、開始する前にを参照してください。

アプリの使用

ログインに成功すると、BioStar Xモバイルアプリのホーム画面が表示されます。ホーム画面では、登録済みユーザー、ドア、リアルタイムログ、イベントログ、アラートを確認できます。サイドメニューと設定メニューにもアクセスできます。



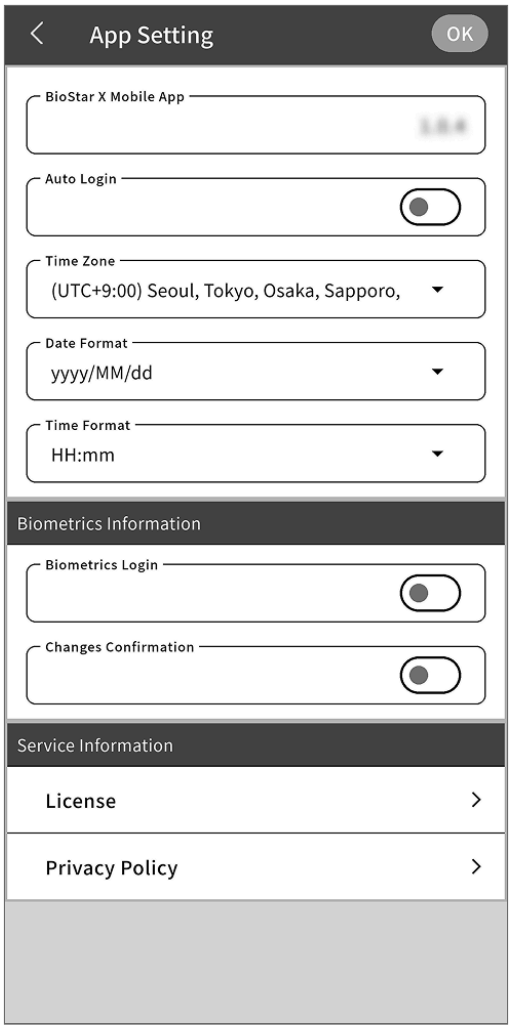
- ☰: サイドメニューを開けます。サイドメニューでは、パスワードの変更やログアウトができ、主要メニューにアクセスできます。
- ⚙: 設定メニューを開けます。アプリ設定の詳細は、アプリ設定を参照してください。
- **USER**: 登録済みユーザー一覧を確認し、ユーザーを管理できます。ユーザー管理の詳細は、ユーザー管理を参照してください。
- **DOOR**: 登録済みドア一覧を確認し、リモートで制御できます。ドア管理の詳細は、ドア管理を参照してください。
- **デバイス**：登録済みデバイス一覧で状態を確認し、ロック中のデバイスをリモートで解除できます。装置管理の詳細は、デバイス管理をご参照ください。
- **REAL-TIME LOG**: リアルタイムの入退室イベントログを確認できます。リアルタイムログの監視の詳細は、リアルタイムログモニタリングを参照してください。
- **EVENT LOG**: BioStar Xサーバーに保存されたすべてのイベントログを確認できます。ログの確認の詳細は、過去ログの照会を参照してください。
- **ROLL CALL**: 緊急時に、ユーザーがあらかじめ指定された場所の入室または退室デバイスで認証し、出席確認場所に到着したかどうかを確認できます。出席確認（Roll Call）機能は **エッセンシャル**（Essential）ライセンス以上で、追加オプションで利用できます。人員点検機能の詳細は、出席確認（Roll Call）を開始するを参照してください。
- **ALERT**: ドア、端末、高度な入退室制御アラートを確認できます。アラートの詳細は、アラームを設定するを参照してください。
- **クイックアクション**：緊急時に複雑な制御手順を自動化する機能です。あらかじめ定義した複数のデバイスの動作を1つのボタンで即時に実行し、迅速に対応できます。BioStar X Webインターフェースでクイックアクションを作成すると、モバイルアプリで使用できます。**クイックアクション**機能の詳細は、クイックアクションを使用するを参照してください。

情報

すべての機能には、サイドメニュー（☰）からもアクセスできます。

アプリ設定

BioStar Xモバイルアプリの設定メニューで、ログイン、タイムゾーン、セキュリティなど、アプリの主な機能を管理できます。アプリ設定メニューにアクセスするには、ホーム画面の右上で⚙をタップします。



アプリのバージョン情報を確認

BioStar X Mobile App項目で、現在インストールされているBioStar Xモバイルアプリのバージョン情報を確認できます。インストールしたアプリが最新バージョンか確認するには、**BioStar X Mobile App**項目をタップします。

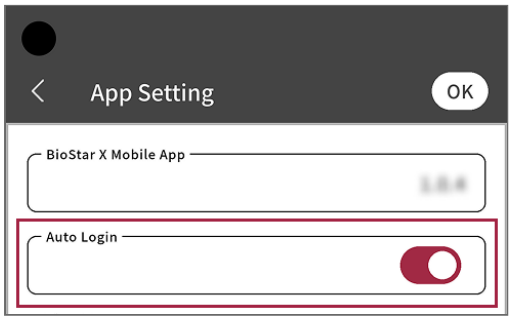
> **情報**
> アプリのバージョン情報は、問題解決時にサポートチームへ問い合わせる際に役立ちます。

ログイン設定

自動ログイン設定

ユーザーがアプリを開くたび、またはセッションの有効期限が切れて再度ログインするたびに、ログイン情報を入力する代わりに自動ログイン機能を有効にできます。

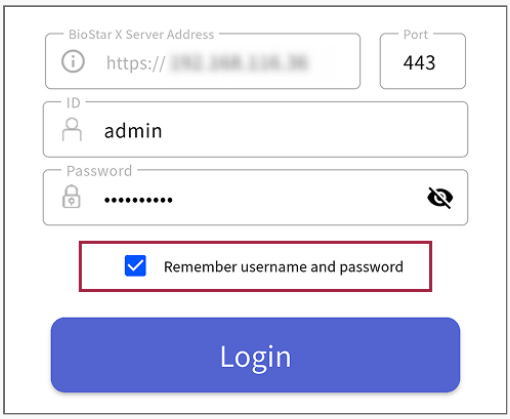
1. 自動ログイン機能を有効にするには、**Auto Login**オプションを有効にします。



2. 変更を保存するには、画面右上の**OK**をタップします。
3. 確認メッセージが表示されたら、**Yes** をタップします。

情報

- 自動ログイン機能は、ログイン画面で**Remember username and password**オプションを有効にしている場合に使用できます。このオプションを有効にしていない場合、自動ログイン機能は使用できません。

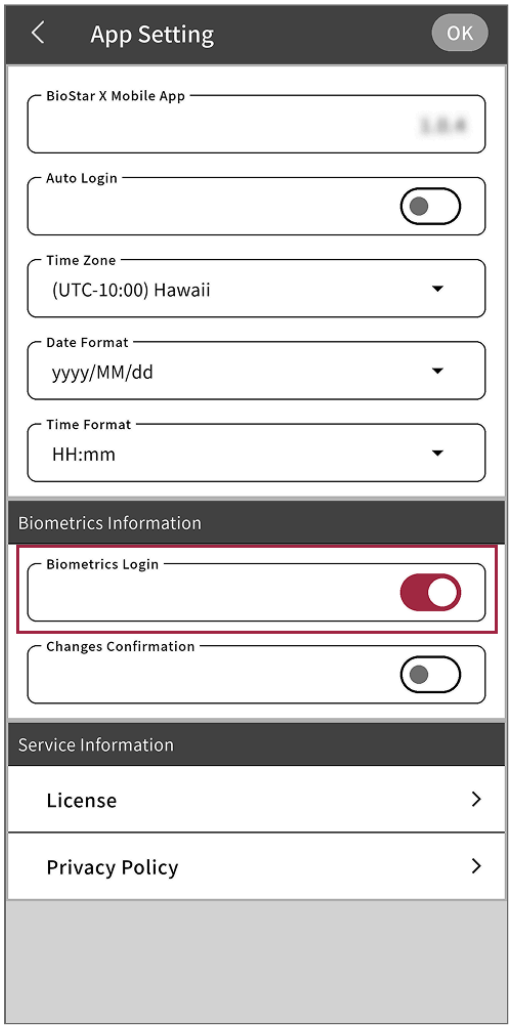


- 自動ログイン機能が有効な場合、ログアウトできません。ログアウトするには、自動ログイン機能を無効にしてからログアウトします。

生体認証ログイン設定

生体認証機能があるモバイル端末では、生体認証ログイン機能を有効にできます。この機能を有効にすると、ユーザーはIDとパスワードの代わりに、モバイル端末に登録した指紋でログインできます。

1. 生体認証ログイン機能を有効にするには、**Biometrics Information** → **Biometrics Login**項目をタップします。



2. 変更を保存するには、画面右上の**OK**をタップします。
3. 確認メッセージが表示されたら、**Yes** をタップします。

ログイン画面で生体認証機能を使用できます。

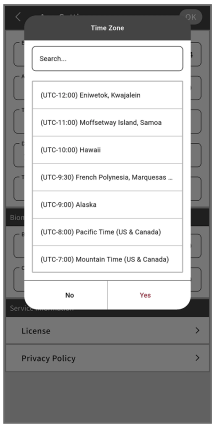


情報

この機能を使用するには、モバイル端末に生体認証機能が必要で、ログイン画面で**Remember username and password**オプションを有効にしている必要があります。

標準タイムゾーン設定

BioStar Xサーバーが設置されている場所に対応するタイムゾーンを設定できます。正しいタイムゾーン設定は、イベントログと通知の正確な時刻記録に重要です。

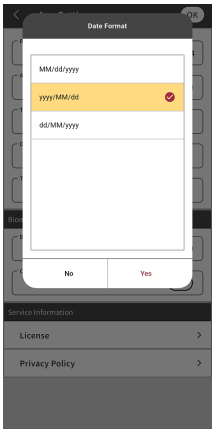


1. **Time Zone**をタップします。
2. タイムゾーン一覧で、BioStar Xサーバーが設置されている場所に対応するタイムゾーンを選択します。
3. **Yes**をタップします。
4. 変更を保存するには、画面右上の**OK**をタップします。
5. 確認メッセージが表示されたら、**Yes** をタップします。

> **情報**
> 変更内容はBioStar Xサーバーにも適用され、アプリに表示されるイベントログと通知の時刻記録に変更後のタイムゾーンが反映されます。

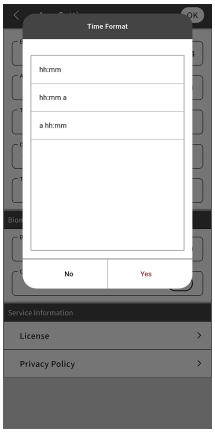
日付と時刻の表示形式設定

システム全体で使用する日付と時刻の表示形式を設定できます。



日付表示形式

1. **Date Format**をタップします。
2. **Date Format**一覧で、希望する日付表示形式を選択します。
   - **MM/dd/yyyy**: 01/31/2025
   - **yyyy/MM/dd**: 2025/01/31
   - **dd/MM/yyyy**: 31/01/2025
3. **Yes**をタップします。
4. 変更を保存するには、画面右上の**OK**をタップします。
5. 確認メッセージが表示されたら、**Yes** をタップします。

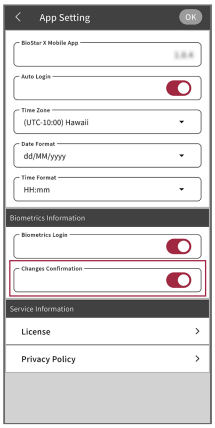


時刻表示形式

1. **Time Format**をタップします。
2. **Time Format**一覧で、希望する時刻表示形式を選択します。
   - **hh:mm**: 23:59、24時間形式
   - **hh:mm a**: 11:59 PM、12時間形式
   - **a hh:mm**: PM 11:59、12時間形式
3. **Yes**をタップします。
4. 変更を保存するには、画面右上の**OK**をタップします。
5. 確認メッセージが表示されたら、**Yes** をタップします。

生体認証で変更内容を確認

重要なシステム変更を実行するときに、生体認証を追加で要求できます。これにより、他のユーザーによる不正な変更を防げます。

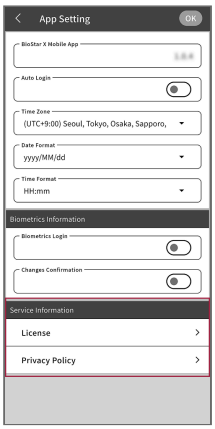


1. **Biometrics Information** → **Changes Confirmation**項目をタップします。
2. 変更を保存するには、画面右上の**OK**をタップします。
3. 確認メッセージが表示されたら、**Yes** をタップします。

生体認証が必要な変更内容は次のとおりです。

- アカウントパスワードの変更
- アプリ設定の変更
- 新しいユーザーの追加
- ユーザー情報の編集
- ユーザーの削除

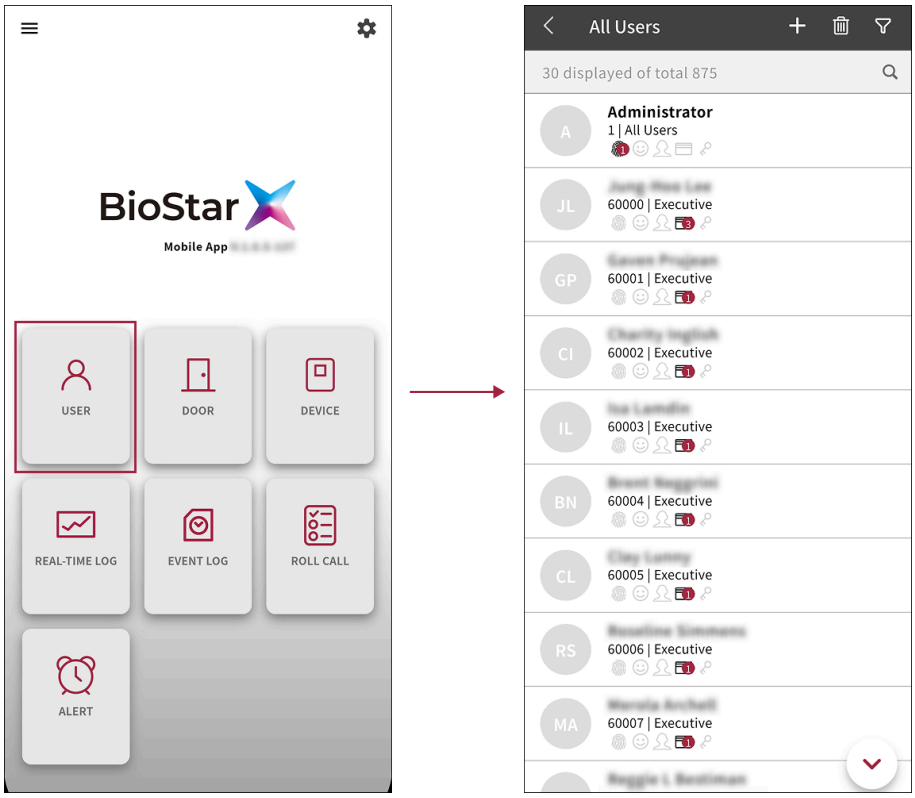
ライセンス情報とプライバシーポリシーを確認



- BioStar Xモバイルアプリに適用されているライセンス情報を確認するには、**Service Information** → **License**をタップします。
- Supremaのプライバシーポリシーを確認するには、**Service Information** → **Privacy Policy**をタップします。アプリに用意されたリンクから、Supremaの公式Webサイトに掲載されているプライバシーポリシーを確認できます。

ユーザー管理

新しいユーザーを enroll したり、退職者を削除したり、ユーザー情報を変更したりする場合は、ユーザー一覧で管理できます。ユーザー検索とログ照会もサポートします。

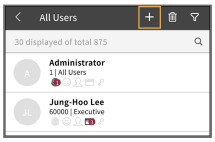


情報

BioStar Xでのユーザー管理の詳細は、ユーザーを参照してください。

ユーザー登録

新しいユーザーや一時的な訪問者をシステムに追加する場合は、基本情報、権限、認証情報をまとめて登録できます。

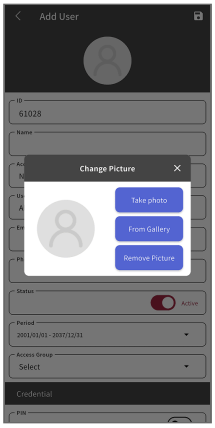


1. アプリのホーム画面で **USER** をタップします。

   サイドメニューからも開けます。☰ → **User** をタップします。

2. 画面右上の ＋ をタップします。
3. 登録するユーザーの基本情報を入力し、クレデンシャルを設定します。

プロフィール画像の登録

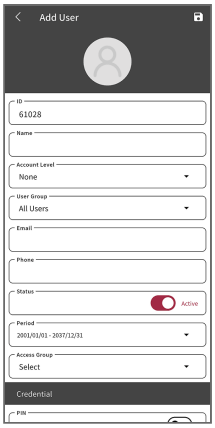


ユーザーのプロフィール画像を登録するには、画面上部のプロフィールアイコンをタップします。

- **Take photo**：モバイル端末のカメラで写真を撮影し、プロフィール画像として登録できます。
- **From Gallery**：モバイル端末に保存された写真を選択し、プロフィール画像として登録できます。

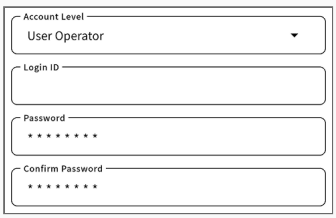
> **情報**
> 登録したプロフィール画像を削除するには、**Remove Picture** をタップします。

ユーザー情報の入力と権限設定



- **ID**：ユーザーに付与される固有 ID です。システムで自動生成された値が既定で入力されています。直接入力することもできます。
- **Name**：ユーザー名を入力します。
- **Account Level**：ユーザーの管理者レベルを選択できます。

管理者レベル	メニュー別権限	
None	-	なし
Administrator	すべてのメニュー	すべての権限
User Operator	User	読み取り、書き込み
Monitoring Operator	Monitoring, Data, Dashboard	読み取り、書き込み
T&A Operator	TIME ATTENDANCE	読み取り、書き込み
Visitor Operator	VISITOR	読み取り、書き込み

> 管理者レベルを設定すると、ログイン ID とパスワードを設定してそのユーザーが BioStar X サーバーにログインできます。
>
> 
>

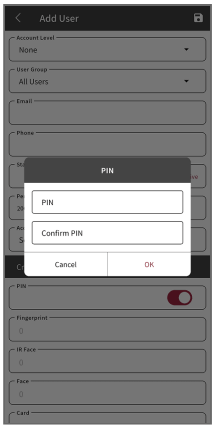
- **User Group**：ユーザーが所属するグループを選択します。

- **Email**：ユーザーのメールアドレスを入力します。
- **Phone**：ユーザーの電話番号を入力します。
- **Status**：ユーザーアカウントを有効または無効にできます。
- **Period**：ユーザーアカウントを使用する期間を設定します。開始日と終了日を設定すると、その期間内だけユーザーアカウントを使用できます。
- **Access Group**：ユーザーの入退室グループを選択できます。

> **情報**
>
> - ユーザー ID は、**Settings** → **Server** メニューの **User ID Type** オプションによって、設定できる値が異なる場合があります。詳しくは サーバーの詳細を設定する を参照してください。
> - **T&A Operator** および **Visitor Operator** レベルには、別途ライセンスが必要です。ライセンスポリシーの詳細については、ライセンス ポリシーを参照してください。
> - 入退室グループの追加と設定の詳細は、アクセスグループを管理する を参照してください。

クレデンシャルの登録

ユーザーを登録するとき、入退室制御システムにアクセスできるようにクレデンシャルも登録できます。ユーザーの指紋や顔、カード情報、パスワードなどをクレデンシャルとして登録できます。クレデンシャルはユーザーを新規登録または編集する際に追加または変更できます。

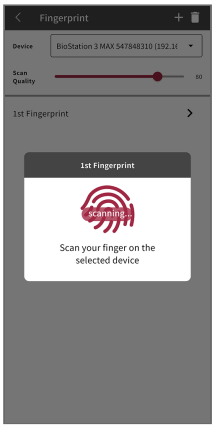


PIN登録

ユーザーがデバイスに PIN を入力して入退室できるように、PIN クレデンシャルを登録できます。

1. **Credential** → **PIN** をタップします。
2. PIN 入力画面が表示されたら、希望する PIN を順に入力します。
3. 入力が完了したら、**OK** をタップします。

> **情報**
>
> - PINは4~16桁で、数字のみを入力してください。
> - ユーザーごとに登録できるPINクレデンシャルは最大1つです。



指紋登録

入退室の認証手段としてユーザーの指紋を登録して使用できます。指紋認証をサポートするデバイスでユーザーの指紋情報を登録します。

指紋を登録する前に…

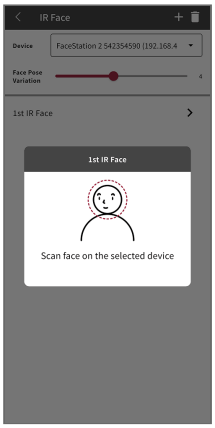
- ユーザーの指紋が清潔で濡れていないことを確認します。
- 傷がある指や指紋が薄い指は登録しないでください。

1. **Credential** → **Fingerprint** をタップします。
2. 指紋を登録するデバイスを選択するには、**Device** をタップします。
3. **Add Device** ポップアップで、指紋登録デバイスを選択し、**Yes** をタップします。
4. **Scan Quality** で指紋の品質を調整できます。既定値は 80 です。設定した品質レベルに達しない場合、指紋情報を登録できません。
5. 画面右上の ＋ をタップします。
6. 一覧に **1st Fingerprint** が追加されたら、それをタップします。
7. **scanning...** ポップアップが表示されたら、選択したデバイスで指紋をスキャンします。
8. 指紋を確認するため、同じ指紋をもう一度スキャンします。
9. 指紋のスキャンが完了したら、**OK** をタップします。



情報

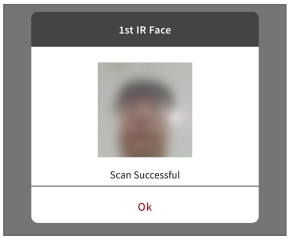
- デバイス一覧には、BioStar X サーバーに登録された指紋認証デバイスのうち、指紋登録が可能なデバイスのみ表示されます。
- 指紋を追加登録するには、手順 5 ～ 9 を繰り返します。ユーザーごとに最大 10 個まで指紋を登録できます。
- 登録した指紋を編集するには、該当する指紋クレデンシャルをタップして、上記の手順を繰り返します。



IR フェイスの登録

入退室の認証手段としてユーザーの顔を登録して使用できます。 IRフェイス登録は、ユーザーの顔を赤外線カメラで撮影して行う認証手段です。

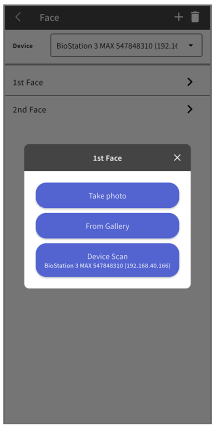
1. **Credential** → **IR Face** をタップします。
2. **Device** をタップし、IR フェイスを登録できるデバイスを選択して、**Yes** をタップします。
3. 顔の位置、角度、距離に対する感度を設定するには、**Face Pose Variation** を調整します。既定値は **4** です。精度の高いIRフェイステンプレートを取得するには、高く設定します。
4. 画面右上の ＋ をタップします。
5. 一覧に **1st IR Face** が追加されたら、それをタップします。
6. 顔登録のポップアップが表示されたら、選択したデバイスで顔をスキャンします。顔が認識されると、ポップアップに顔画像が表示されます。



7. IR フェイスの登録を完了するには、**OK** をタップします。

情報

- IRフェイスを登録できるデバイスについては、以下を参照してください。
  - FaceStation 2
  - FaceLite
- IR フェイスは最大 5 件まで登録できます。
- 顔認証率が低い場合は顔情報を削除し、新しい顔情報を登録します。
- 登録した IR フェイスを編集するには、該当する IR フェイス クレデンシャルをタップして、上記の手順を繰り返します。



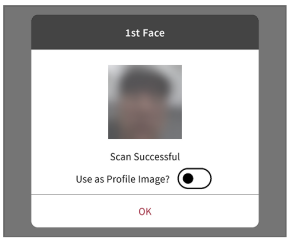
顔登録

入退室の認証手段としてユーザーの顔を登録して使用できます。顔登録は、ユーザーの顔をカメラで撮影して行う認証手段です。 BioStar X モバイルアプリでは、モバイル端末に保存された顔画像を読み込むか、カメラで撮影して顔を登録できます。また、顔認識対応デバイスで顔をスキャンして登録することもできます。

1. **Credential** → **Face** をタップします。
2. **Device** をタップし、顔を登録できるデバイスを選択して、**Yes** をタップします。

   - デバイスを選択しない場合は、モバイル端末の写真を読み込むか、カメラで撮影して顔を登録できます。
   - デバイスを選択すると、そのデバイスで顔をスキャンして登録できます。

3. 画面右上の ＋ をタップします。
4. 一覧に **1st Face** が追加されたら、それをタップします。
5. ポップアップで希望する顔の登録方法を選択します。
   - **Take photo**：モバイル端末のカメラで写真を撮影し、顔を登録できます。
   - **From Gallery**：モバイル端末に保存された写真を選択し、顔を登録できます。
   - **Device Scan**：**Device** 項目で選択したデバイスを使って顔をスキャンできます。
6. 顔が認識されると、ポップアップに顔画像が表示されます。



7. 顔の登録を完了するには、**OK** をタップします。

情報

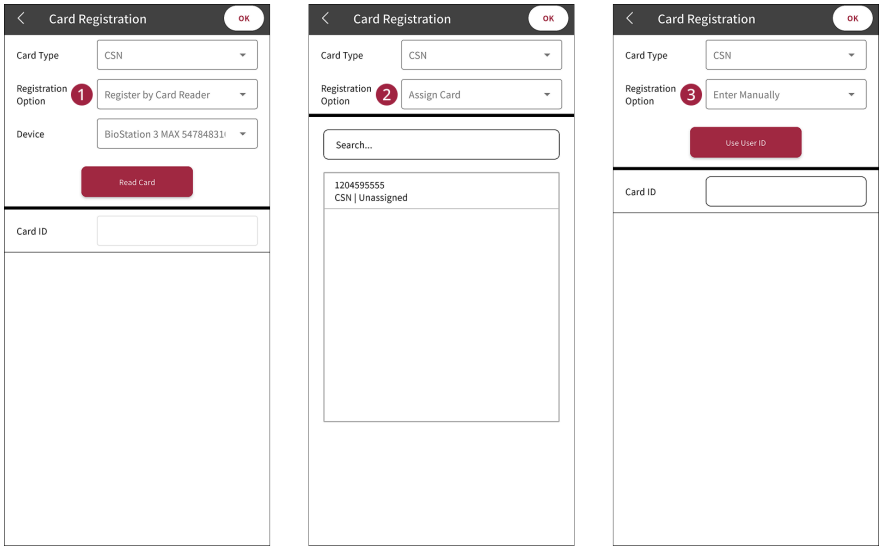
- 登録した顔画像をプロフィール画像として使用するには、**Use as Profile Image?** オプションを有効にします。
- モバイル端末のカメラで顔写真を撮影する場合や、保存済みの写真を読み込む場合は、アクセス権限が必要です。権限リクエストのポップアップで許可を選ぶと、顔写真を登録できます。
- 登録した顔を編集するには、該当する顔クレデンシャルをタップして、上記の手順を繰り返します。

入退室カードの登録

入退室用の認証情報として、新しい入退室カードを登録したり、登録済みの入退室カードを割り当てたりできます。入退室カードの登録には、カードリーダーでスキャンして登録する方法、登録済みのカードを割り当てる方法、カード番号を手動で入力する方法があります。

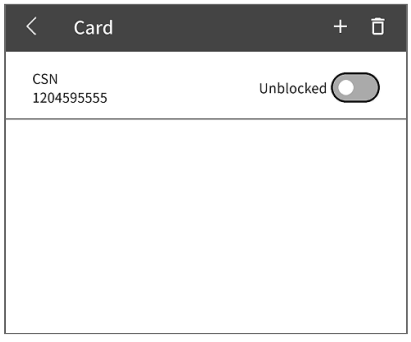
CSN カード

1. **Credential** → **Card** をタップします。
2. 画面右上の ＋ をタップします。
3. **Card Type** で **CSN** を選択し、**Yes** をタップします。
4. **Registration Option** で希望する登録方法を選択します。



- 1 **Register by Card Reader**：カードリーダーでカードをスキャンして登録できます。 **Device** でカードを読み取るデバイスを選択し、**Read Card** をタップします。カードリーダーにカードをかざしてスキャンします。カードのスキャンに成功すると、**Card ID** にカード番号が入力されます。
- 2 **Assign Card**：登録済みの入退室カードをユーザーに割り当てられます。一覧から登録済みのカード番号を 1 つ選択します。
- 3 **Enter Manually**：カード番号を手動で入力できます。 **Card ID** 入力欄にカード番号を入力します。ユーザー ID をカード番号として使用するには、**Use User ID** をタップします。

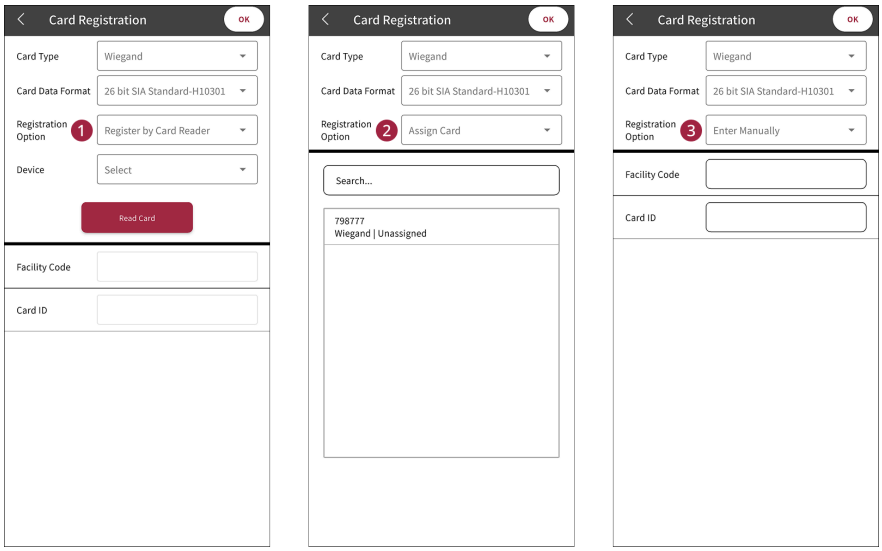
5. カード登録を完了するには、画面右上の **OK** をタップします。
6. カード一覧に戻ると、登録したカード番号が表示されます。



> **情報**
> 登録したカードの使用を停止するには、カードのトグルスイッチをタップして **Blocked** に設定します。

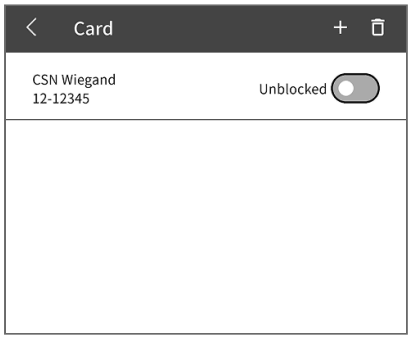
Wiegandカード

1. **Credential** → **Card** をタップします。
2. 画面右上の ＋ をタップします。
3. **Card Type** で **Wiegand** を選択し、**Yes** をタップします。
4. **Card Data Format** で希望するカード形式を選択します。
5. **Registration Option** で希望する登録方法を選択します。



- 1 **Register by Card Reader**：カードリーダーでカードをスキャンして登録できます。 **Device** でカードを読み取るデバイスを選択し、**Read Card** をタップします。カードリーダーにカードをかざしてスキャンします。カードのスキャンに成功すると、**Facility Code** と **Card ID** にカード番号が入力されます。
- 2 **Assign Card**：登録済みの入退室カードをユーザーに割り当てられます。一覧から登録済みのカード番号を 1 つ選択します。
- 3 **Enter Manually**：カード番号を手動で入力できます。 **Facility Code** と **Card ID** の入力欄にカード番号を入力します。

6. カード登録を完了するには、画面右上の **OK** をタップします。
7. カード一覧に戻ると、登録したカード番号が表示されます。



情報

登録したカードの使用を停止するには、カードのトグルスイッチをタップして **Blocked** に設定します。

スマートカード

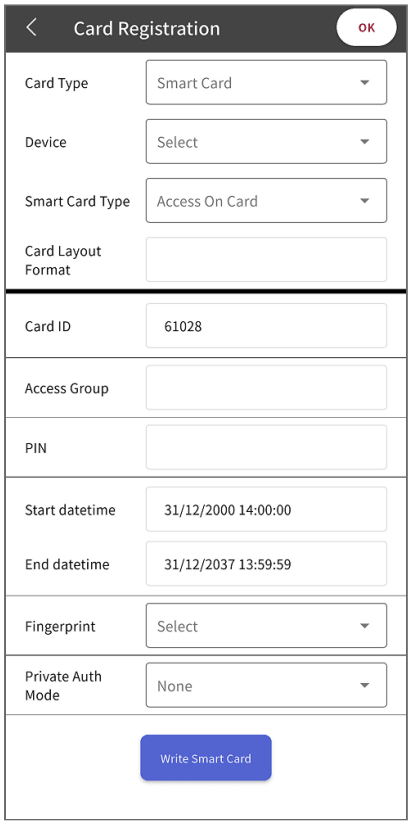
情報

- スマートカードを発行するには、正しいカードフォーマットを設定する必要があります。カード形式の詳細は、スマートカード形式を設定する を参照してください。
- スマートカードに保存されるユーザー情報は **BioStar X** に保存された情報を使用します。変更したユーザー情報を保存しない場合、スマートカードに誤ったユーザー情報が保存される可能性があります。また、変更したユーザー情報をデバイスと同期しないと、デバイスが認証を実行できない場合があります。
- PIN 認証情報を追加するには、先に PIN を登録する必要があります。 PIN 登録の詳細は、PIN登録 を参照してください。
- 指紋クレデンシャル情報を追加するには、先に指紋を登録する必要があります。指紋登録の詳細は、指紋登録 を参照してください。

Access On Card

ユーザー情報（カード ID、PIN、入退室グループ、期間、指紋テンプレート、顔テンプレート、個人認証モード）をカードに保存できます。

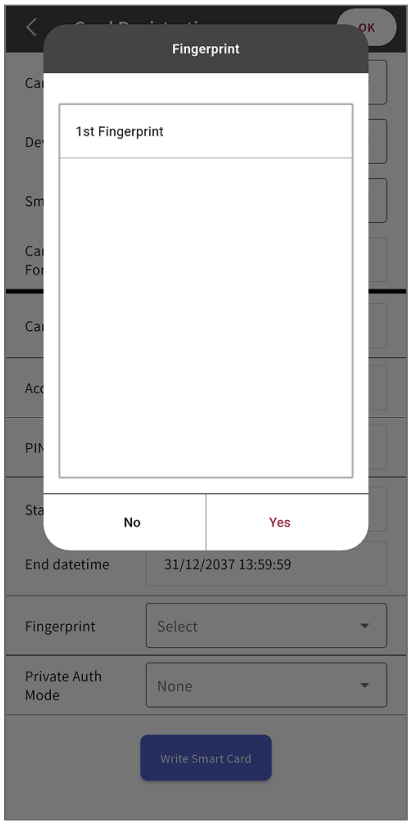
1. **Credential** → **Card** をタップします。
2. 画面右上の ＋ をタップします。
3. **Card Type** で **Smart Card** を選択し、**Yes** をタップします。



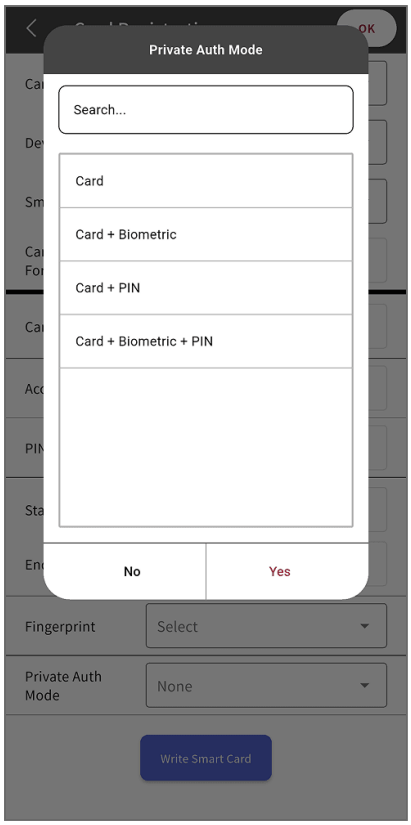
4. **Device** でカードを登録するデバイスを選択し、**Yes** をタップします。

> **Device** で選択したデバイスに設定されたカードレイアウトが、**Card Layout Format** に表示されます。

5. (任意) 指紋認証を追加するには、**Figerprint** をタップして登録済みの指紋を選択します。



6. (任意) 個人認証モードを追加するには、**Private Auth Mode** をタップして希望する認証方法を選択します。

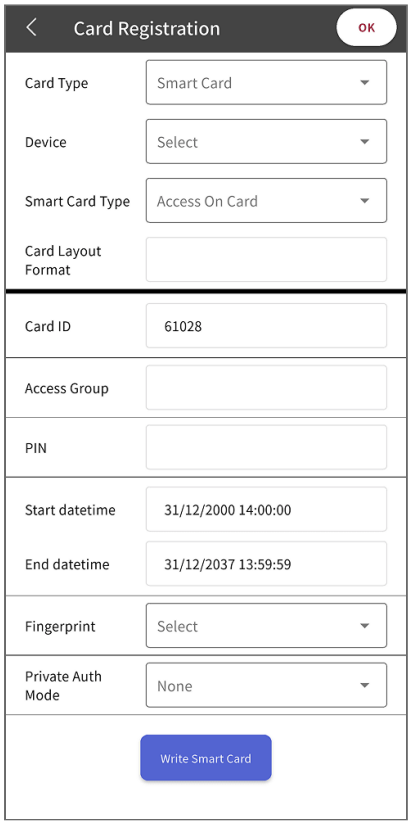


7. カードを登録するには、**Writes Smart Card** をタップします。
8. 選択したデバイスに、ユーザー情報を登録するカードをかざします。
9. カード登録が完了したら、画面右上の **OK** をタップします。

セキュア クレデンシャル カード（Secure Credential Card）

ユーザー情報（カード ID、PIN、指紋テンプレート、顔テンプレート）をカードに保存できます。

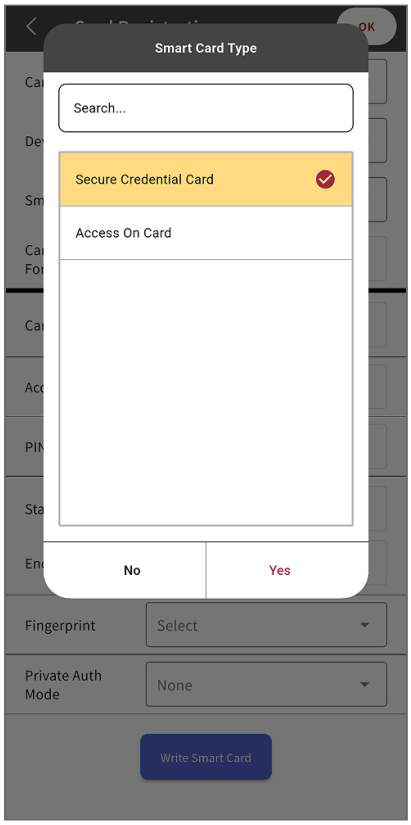
1. **Credential** → **Card** をタップします。
2. 画面右上の ＋ をタップします。
3. **Card Type** で **Smart Card** を選択し、**Yes** をタップします。



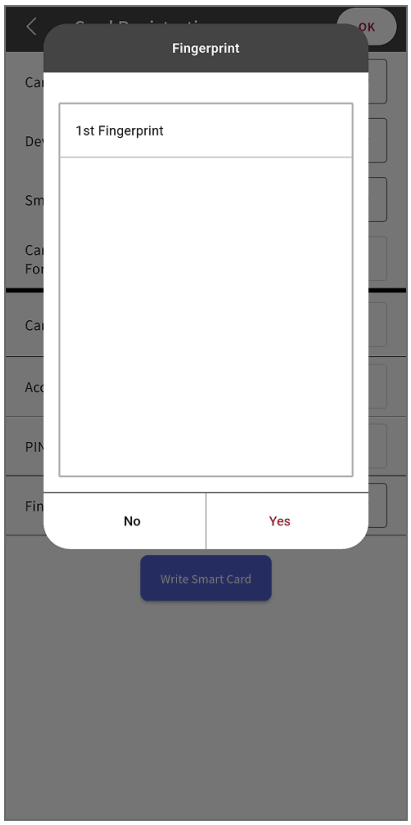
4. **Device** でカードを登録するデバイスを選択し、**Yes** をタップします。

> **Device** で選択したデバイスに設定されたカードレイアウトが、**Card Layout Format** に表示されます。

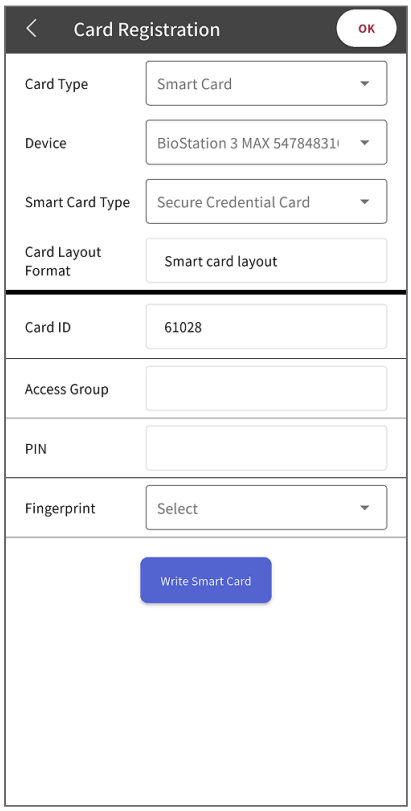
5. **Smart Card Type** をタップし、**Secure Credential Card** を選択してから、**Yes** をタップします。



6. (任意) 指紋認証を追加するには、**Figerprint** をタップして登録済みの指紋を選択します。



7. カードを登録するには、**Writes Smart Card** をタップします。



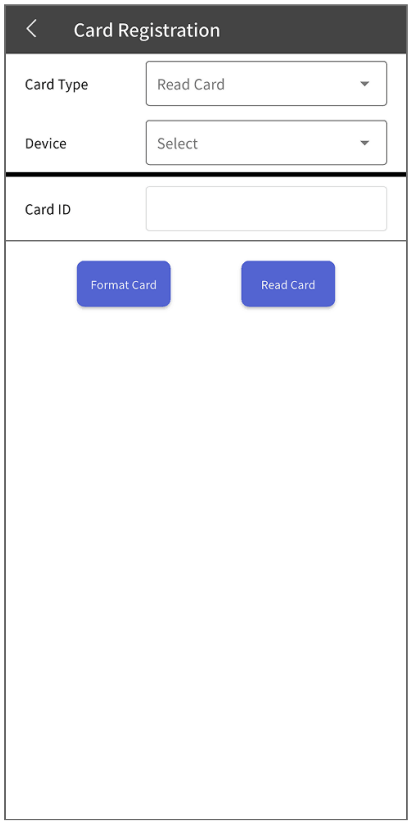
8. 選択したデバイスに、ユーザー情報を登録するカードをかざします。

9. カード登録が完了したら、画面右上の **OK** をタップします。

カードの読み取り/フォーマット

スマートカードをフォーマットして情報を書き込み直すことができます。

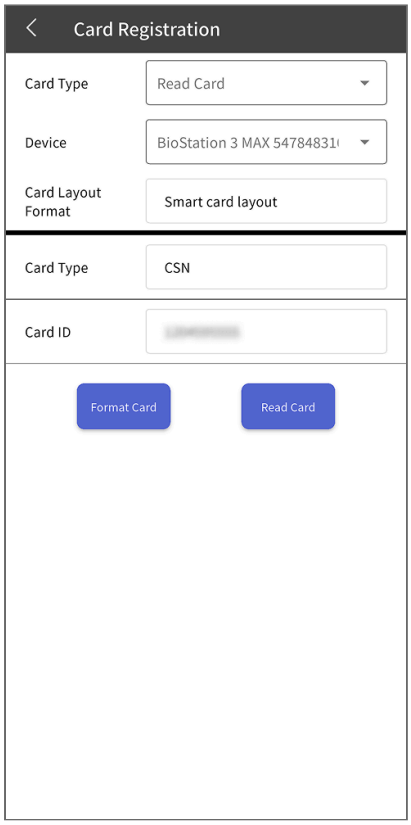
1. **Credential** → **Card** をタップします。
2. 画面右上の ＋ をタップします。
3. **Card Type** で **Read Card** を選択し、**Yes** をタップします。



4. **Device** でカードを読み取るデバイスを選択し、**Yes** をタップします。

> **Device** で選択したデバイスに設定されたカードレイアウトが、**Card Layout Format** に表示されます。

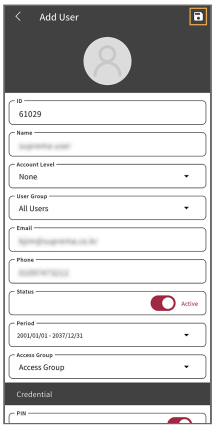
5. **Read Card** をタップして、カードをデバイスにかざしてスキャンします。



6. カード情報を確認したら、カードをフォーマットするには **Format Card** をタップします。

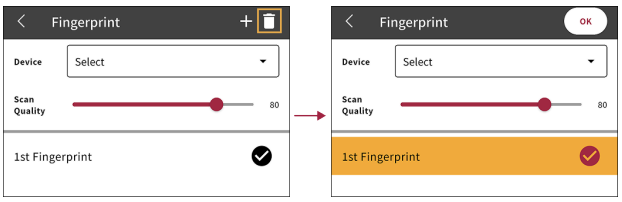
> **情報**
> カスタムスマートカードはフォーマットできません。

ユーザー登録の完了



ユーザーの基本情報、権限、クレデンシャルを設定したら、画面右上の をタップしてユーザー登録を完了します。

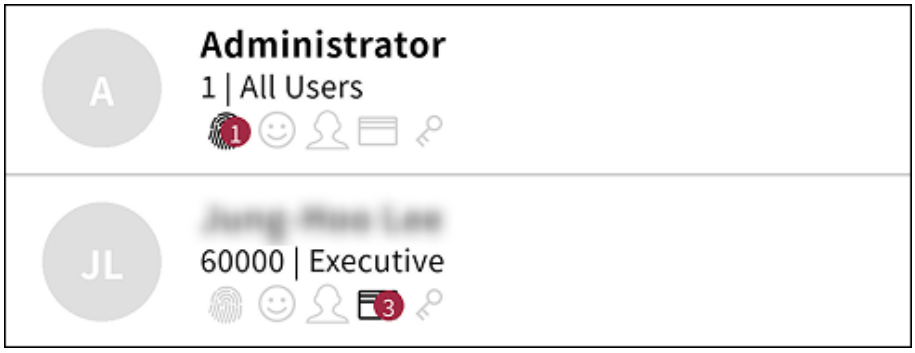
- **Credential** セクションでは、各クレデンシャルの登録数を確認できます。
- 登録済みクレデンシャルを削除するには、削除するクレデンシャル項目をタップし、画面右上の をタップします。削除するクレデンシャルを選択し、**OK** をタップします。



> **情報**
> BioStar X でのユーザー登録と管理の詳細は、ユーザー を参照してください。

ユーザー情報の確認

登録したユーザーは、ユーザー一覧で確認できます。各ユーザーには、次の情報が含まれます。

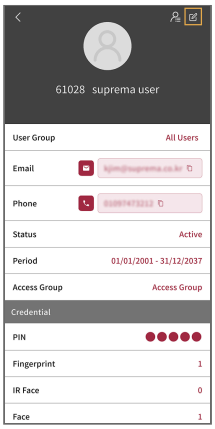


- ユーザー名
- ユーザー ID | ユーザー グループ
- 登録済みクレデンシャル情報：指紋 / IR フェイス / 顔 / カード / PIN

ユーザーの編集と削除

ユーザーの所属が変わった場合や権限を調整する場合は、情報を編集できます。退職や契約終了時には、ユーザーを削除してセキュリティを強化する方法も確認してください。

ユーザーの編集



ユーザー情報、権限、クレデンシャルはユーザー詳細情報で編集できます。

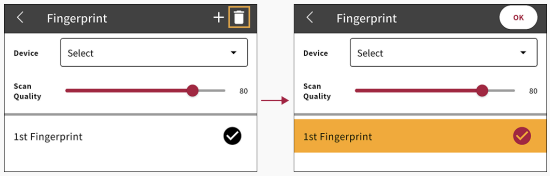
1. アプリのホーム画面で **USER** をタップします。

   > サイドメニューからも開けます。☰ → **User** をタップします。

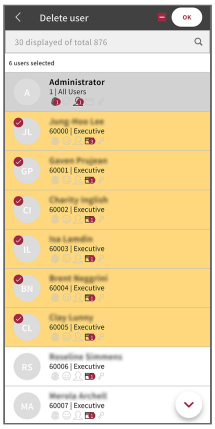
2. ユーザー一覧で、編集するユーザーをタップします。
3. ユーザー詳細情報で、画面右上の をタップします。
4. **Edit User** では、ユーザーの基本情報の編集、権限の変更、クレデンシャルの管理を行えます。
5. 変更内容を保存するには、画面右上の をタップします。

情報

- ユーザー情報、権限、クレデンシャル項目の詳細は、ユーザー登録 を参照してください。
- ユーザーを一時的に無効にするには、**Status** でトグルスイッチをタップし、**Inactive** に設定します。無効化されたユーザーは入退室が制限されます。
- 登録済みクレデンシャルを削除するには、削除するクレデンシャル項目をタップし、画面右上の をタップします。削除するクレデンシャルを選択し、**OK** をタップします。



ユーザーの削除



ユーザーを削除する場合は、次の案内に従って削除します。

1. アプリのホーム画面で **USER** をタップします。

   サイドメニューからも開けます。 → **User** をタップします。

2. ユーザー一覧で、画面右上の をタップします。
3. 削除するユーザーを選択します。 1 人以上のユーザーを選択できます。
4. 画面右上の **OK** をタップします。
5. 確認メッセージが表示されたら、**Yes** をタップします。

選択したユーザーが削除されます。削除したユーザーは復元できません。

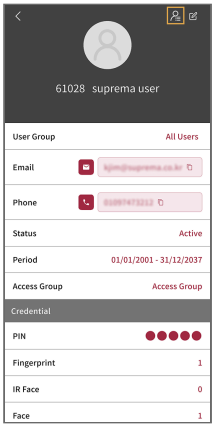
情報

IDが 1 の管理者アカウントは削除できません。

ユーザーログイベントを確認する

ユーザーの入退室履歴を確認して、異常なアクセスや許可されていない時間帯の入退室を確認できます。ログイベントをフィルタリングすると、必要な期間と場所の履歴を簡単に見つけられます。

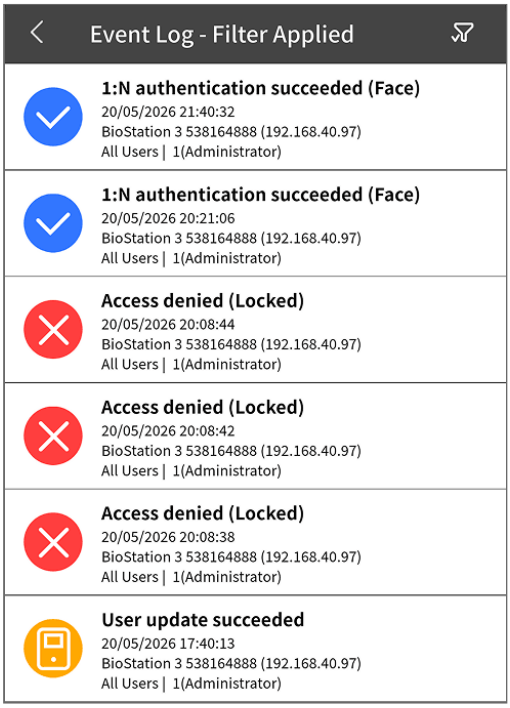
ユーザー入退室履歴の確認



1. アプリのホーム画面で **USER** をタップします。

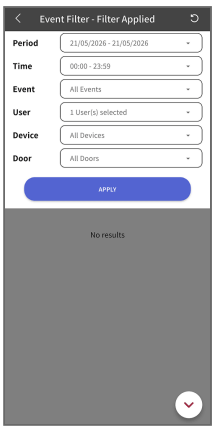
   > サイドメニューからも開けます。 ☰ → **User** をタップします。

2. ユーザーリストで、ログイベントを確認するユーザーをタップします。
3. ユーザー詳細情報で、右上の  をタップします。
4. **Event Log**でユーザーの入退室履歴を確認できます。



最新のログイベントが先に表示され、入退室場所とイベント情報を確認できます。

ログイベントのフィルタリング



ユーザーのログイベントを日付と時刻、イベント種類、入退室場所など、さまざまな条件でフィルタリングできます。

1. イベントログの右上にある  をタップします。
2. フィルター条件が表示されたら、必要な条件を設定します。
   - **Period**: ログイベントが発生した期間を設定します。
   - **Time**: ログイベントが発生した時間を設定します。
   - **Event**: ログイベントの種類を選択します。たとえば、正常（Normal）、管理者手動開放（Operator Unlocked）、管理者手動施錠（Operator Locked）などがあります。
   - **User**: 現在のユーザー以外のログイベントも確認できます。

- **Device**: ログイベントが発生したデバイスを選択できます。
- **Door**: ログイベントが発生した入退室扉を選択できます。

3. 設定した条件でログイベントをフィルタリングするには、**Apply**をタップします。

> **情報**
> フィルタリング条件を初期化するには、画面右上の → をタップします。

ユーザーの検索とフィルタリング

ユーザー一覧が多く、目的のユーザーを見つけにくい場合は、検索機能とフィルタリング機能を使ってすばやく探せます。

ユーザー検索



ユーザーのID、名前、メールアドレスを基準に検索できます。

1. アプリのホーム画面で **USER** をタップします。

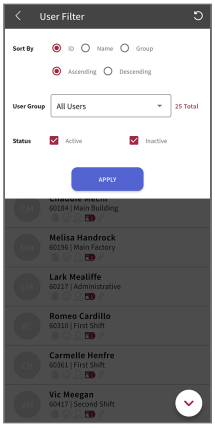
> サイドメニューからも開けます。 → **User** をタップします。

2. ユーザー一覧の上部にある をタップします。
3. 検索入力フィールドに検索語を入力します。 ID、名前、メールアドレスを組み合わせて検索できます。
4. 検索語の入力を完了したら、 をタップします。

検索語と一致するユーザーが検索結果に表示されます。検索結果から目的のユーザーをタップすると、ユーザー詳細情報に移動できます。

> **情報**
>
> - 検索入力フィールドの下には、最近の検索履歴が表示されます。最近の検索履歴をタップすると、その検索語で再度検索できます。
> - 検索入力フィールドを閉じるには ✕ をタップします。

ユーザー一覧のフィルタリング



ユーザー一覧をさまざまな条件でフィルタリングして、目的のユーザーをすばやく見つけられます。

1. アプリのホーム画面で **USER** をタップします。

   > サイドメニューからも開けます。☰ → **User** をタップします。

2. ユーザー一覧の上部にある をタップします。

3. **User Filter** で必要な条件を設定します。

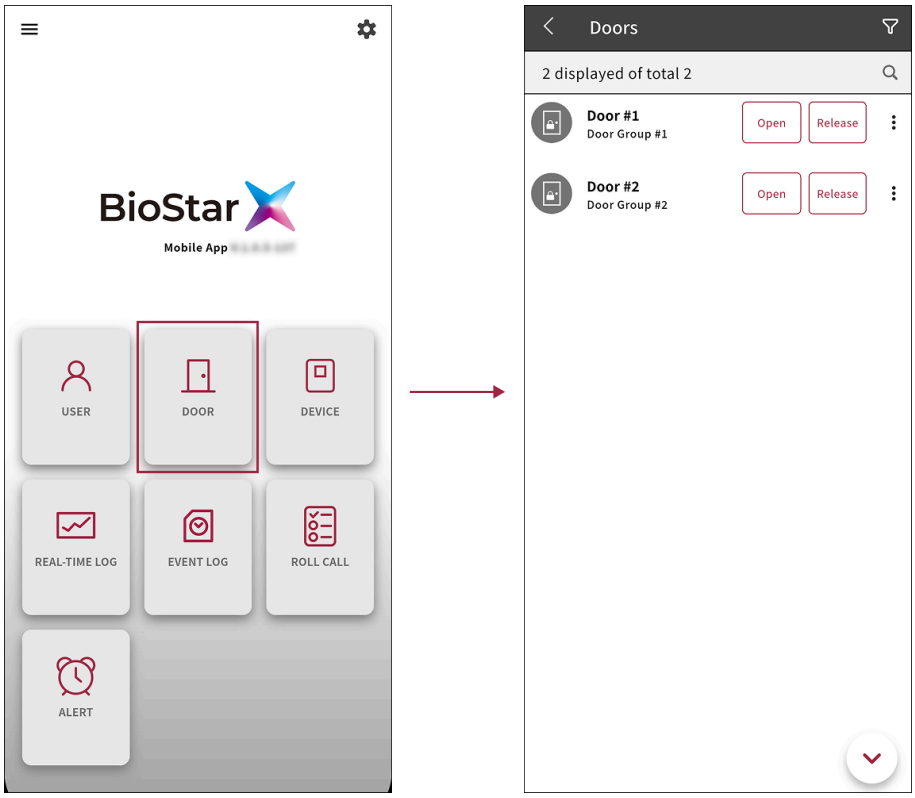
   - **Sort By**: ユーザーID、名前、グループを基準に、昇順または降順の並べ替えを選択できます。
   - **User Group**: 特定のユーザーグループを選択して、そのグループに属するユーザーだけを表示できます。
   - **Status**: 有効なユーザーだけを表示するには **Active** を選択します。無効なユーザーだけを表示するには **Inactive** を選択します。

4. 設定した条件でユーザー一覧をフィルタリングするには **Apply** をタップします。

> **情報**
> フィルタリング条件を初期化するには、画面右上の → をタップします。

ドア管理

ドアをリモートで制御して、便利に出入を管理できます。ドアの状態をリアルタイムで確認し、必要に応じてドアの設定を変更できます。ドアに関連するログイベントも確認できます。



情報

BioStar Xでドアを監視および管理する方法の詳細は、次の文書を参照してください。

- ドアをモニタリング
- ドア管理

ドアのリモート制御

ドア一覧で各ドアの状態をリアルタイムで確認し、必要に応じて制御できます。通常運用時は基本制御機能で管理し、セキュリティ強化や緊急時には追加制御オプションを活用できます。

アプリのホーム画面で**DOOR**をタップしてください。 BioStar Xに登録されたドア一覧が表示されます。

情報

サイドメニューからも開けます。 ☰ → **Door**をタップしてください。

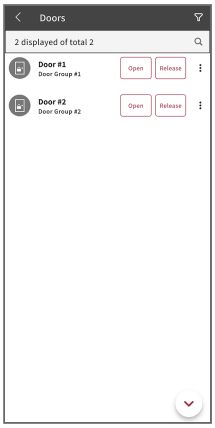
ドア状態の確認

ドア一覧では、ドアの状態アイコンで各ドアに割り当てられたデバイスの異常状態をひと目で確認できます。ドア状態アイコンは、ドアが開いているか、閉じているか、アラームが発生したかなどを示します。



ステータスアイコン	説明
	ドアに問題が発生した状態です。出入口ドアに割り当てた機器との接続が切断されているか、マルチコミュニケーションサーバーエラーや同期エラーなどが発生している異常状態です。
	ドアが開いている状態です。
	ドアが閉じている状態です。
	ドアでアラームが発生した状態です。
	ドアでAPBアラームが発生した状態です。

ドアの開閉

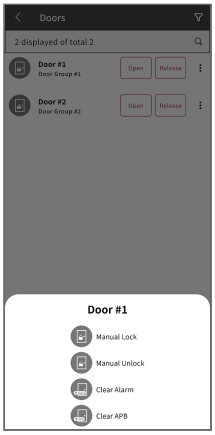


ドアのリモート制御機能で、ドアを開けたりロックしたりして、入室を許可または遮断できます。

- **Open**: ドアを一時的に開けて入室を許可します。ドアは設定した時間後に自動で閉じます。
- **Release**: 認証されたユーザーのみ入室できるように設定します。ドアに設定したスケジュールに従って、ドアの状態が変更されます。

> **情報**
> ドアを一時的に開けて自動で閉じる時間を設定する方法は、ドアを登録するの **Open** → **Open Time**を参照してください。

追加制御



セキュリティ強化が必要な場合や長時間入室を制御する必要がある場合は、時間制限なしでドアを手動でロックまたは開放できます。発生したアラームを解除することもできます。

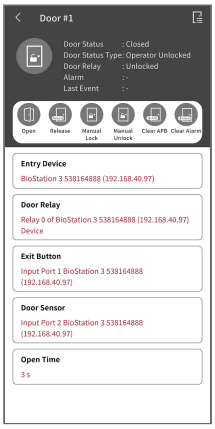
ドアの右端で ⋮ をタップすると、追加制御オプションを使用できます。

- **Manual Lock**: ドアを手動でロックして入室を遮断します。この機能では、時間制限なしでドアをロックできます。この状態では、すべてのユーザーの入室を遮断します。
- **Manual Unlock**: ドアを手動で開放して入室を許可します。この機能では、時間制限なしでドアを開放します。この状態では、すべてのユーザーの入室を許可します。
- **Clear Alarm**: ドアで発生したアラームを解除できます。
- **Clear APB**: 選択したドアのすべてのユーザーに対するAPBアラームを解除できます。

> **情報**
> ドアを手動でロックまたは開放した後は、ドアの状態は自動で変更されません。セキュリティのため、ドアの状態を設定したスケジュールに合わせて動作させるには、**Release**機能を使用してください。

ドア詳細情報を確認する

ドアを選択すると、現在の状態と設定済みのデバイスを確認できます。問題が発生した場合は、すぐに制御したり、最近の活動履歴を確認したりできます。



ドアの状態情報、リモート制御機能、ドアに割り当てられたデバイス情報と開放時間を確認できます。

1. アプリのホーム画面で**DOOR**をタップしてください。

   > サイドメニューからも開けます。 ☰ → **Door**をタップしてください。

2. ドア一覧で、詳細情報を確認するドアをタップします。

ドア状態情報

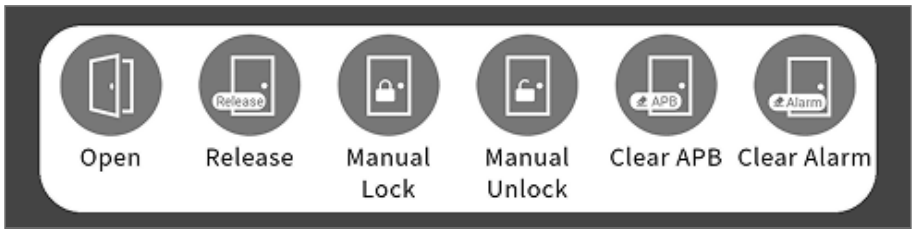
ドアの現在の状態をリアルタイムで確認できます。



- **Door Status**: ドアの開閉状態を表示します。
- **Door Status Type**: ドアの状態タイプを表示します。たとえば、正常（Normal）、管理者手動開放（Operator Unlocked）、管理者手動施錠（Operator Locked）などがあります。
- **Door Relay**: ドアに接続されたリレーの状態を表示します。
- **Alarm**: ドアで発生したアラームイベントを表示します。
- **Last Event**: ドアで発生した最後のイベントの日付、時刻、イベントタイプを表示します。

リモート制御機能

ドアをリモートで制御して、出入を管理できます。



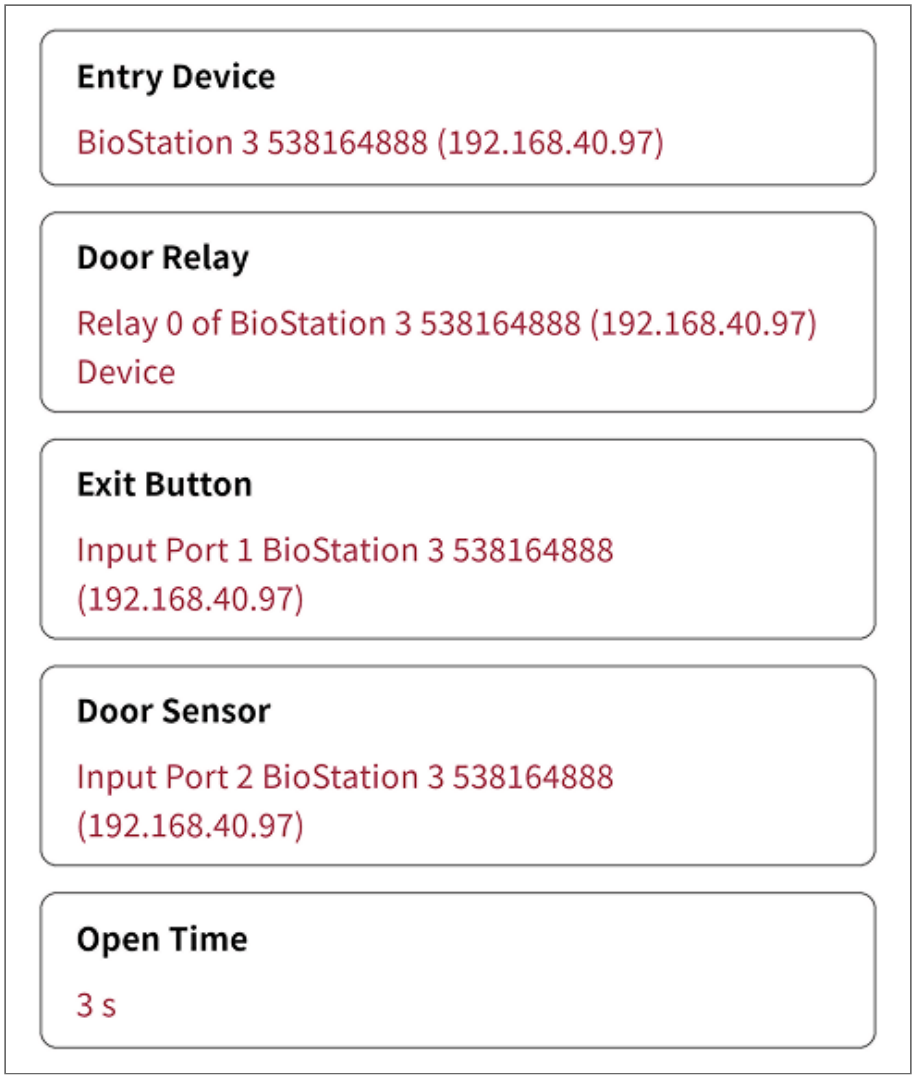
- **Open**: ドアを一時的に開けて入室を許可します。ドアは設定した時間後に自動で閉じます。
- **Release**: 認証されたユーザーのみ入室できるように設定します。ドアに設定したスケジュールに従って、ドアの状態が変更されます。
- **Manual Lock**: ドアを手動でロックして入室を遮断します。この機能では、時間制限なしでドアをロックできます。この状態では、すべてのユーザーの入室を遮断します。
- **Manual Unlock**: ドアを手動で開放して入室を許可します。この機能では、時間制限なしでドアを開放します。この状態では、すべてのユーザーの入室を許可します。
- **Clear APB**: 選択したドアのすべてのユーザーに対するAPBアラームを解除できます。
- **Clear Alarm**: ドアで発生したアラームを解除できます。

情報

- ドアを一時的に開き、オートクローズまでの時間は下部の**Open Time**で確認できます。
- ドアを手動でロックまたは開放した後は、ドアの状態は自動で変更されません。セキュリティのため、ドアの状態を設定したスケジュールに合わせて動作させるには、**Release**機能を使用してください。

ドアデバイス情報

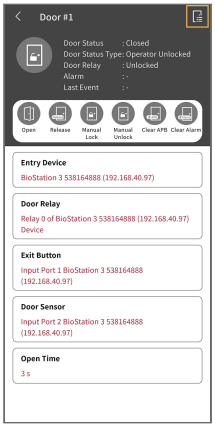
ドアに割り当てられたデバイス情報を確認できます。



- **Entry Device**: 入室デバイスとして割り当てられたデバイス情報です。
- **Door Relay**: ドアのロックデバイスとして動作するリレー情報です。
- **Exit Button**: 退室ボタンとして使用するデバイスのポート情報です。
- **Door Sensor**: ドアの開閉を検知するセンサーとして割り当てられたデバイスのポート情報です。
- **Open Time**: ドアを一時的に開いたとき、ドアが自動で閉じるまで維持される時間です。

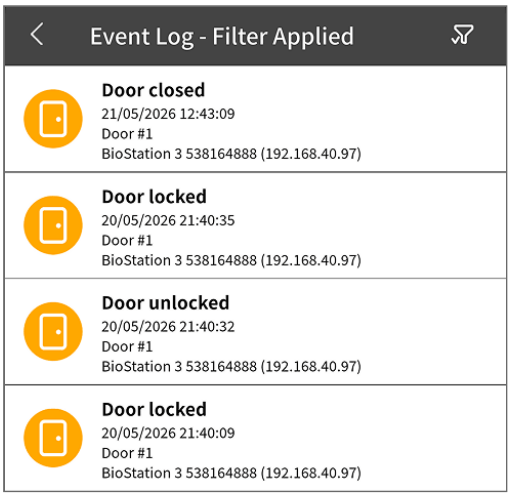
> **情報**
> **Open Time**設定の詳細は、ドアを登録するの**Open** → **Open Time**を参照してください。

ドアログイベントの確認

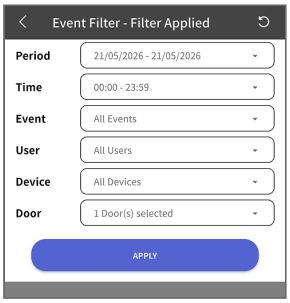


ドアで発生したログイベントを確認し、出入試行、アラームなどのイベントを確認できます。

1. ドア詳細情報画面の右上にあるをタップします。



2. ドアログイベントをフィルタリングするには、画面右上のをタップします。



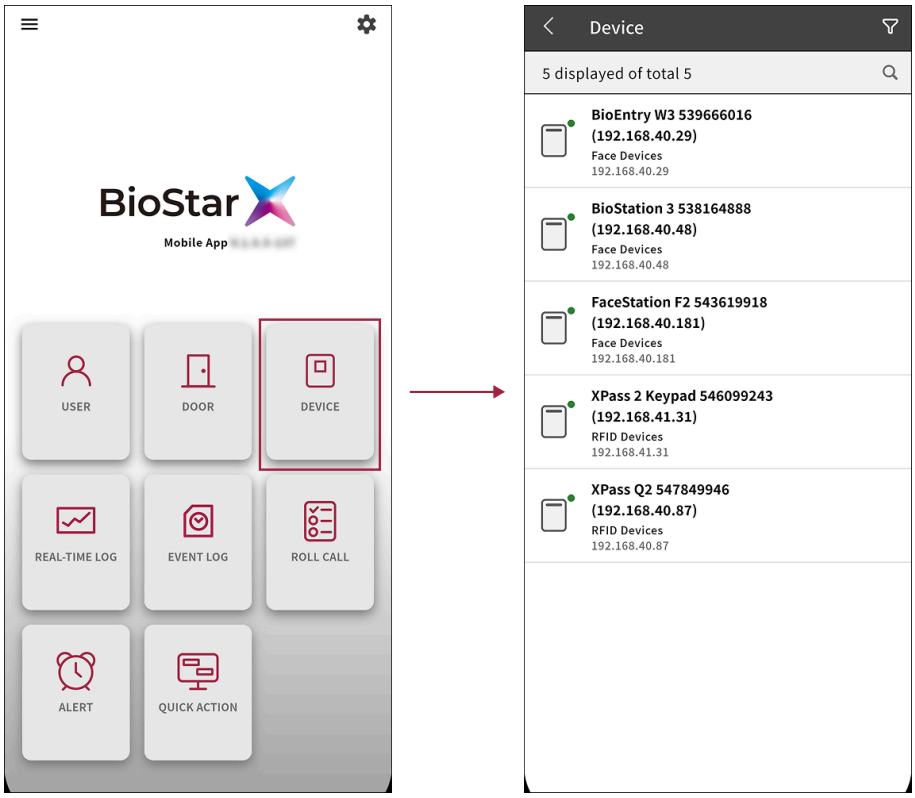
- **Period**: ログイベントが発生した期間を設定します。
- **Time**: ログイベントが発生した時間を設定します。
- **Event**: ログイベントの種類を選択します。たとえば、正常（Normal）、管理者手動開放（Operator Unlocked）、管理者手動施錠（Operator Locked）などがあります。
- **User**: ログイベントを発生させたユーザーを選択できます。
- **Device**: ログイベントが発生したデバイスを選択できます。
- **Door**: 現在のドア以外のドアのログイベントも確認できます。

3. フィルター条件が表示されたら、必要な条件を設定します。
4. 設定した条件でログイベントをフィルタリングするには、**Apply**をタップします。

> **情報**
>
> フィルタリング条件を初期化するには、画面右上の → をタップします。

デバイス管理

デバイス一覧で各デバイスの状態を確認し、ロック状態のデバイスをリモートで解除できます。アプリのホーム画面で **DEVICE** をタップしてください。



情報

- モバイルアプリではデバイスを登録または編集できません。
- サイドメニューからも開けます。☰ → **Device** をタップしてください。

デバイス情報の確認



デバイス一覧の各デバイスには、以下の情報が含まれます。

- デバイス名
- デバイスグループ名（グループに含まれていない場合は、**All Devices** と表示）
- デバイス IP アドレス

デバイス状態の確認

デバイス一覧のステータスアイコンでデバイスの状態を確認できます。

ステータスアイコン	説明
	デバイスが正常に接続されています。
	デバイスの電源がオフ、または接続が解除されています。

> **情報**
> デバイス状態を更新するには、デバイス一覧を下にスワイプしてください。

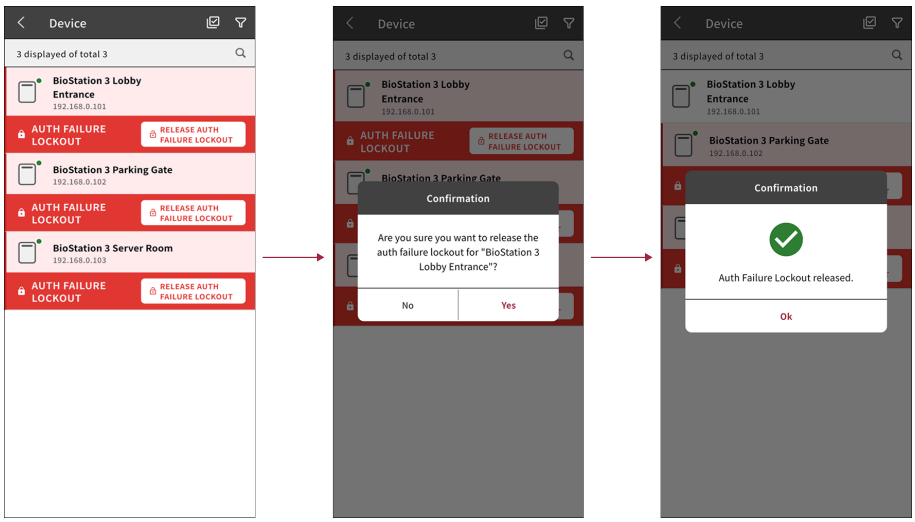
認証失敗ロックの解除

認証が連続して失敗してデバイスがロック状態に切り替わった場合、モバイルアプリでロックを解除できます。

> **情報**
> BioStar X で認証失敗ロック設定の詳細については 認証を設定する を参照してください。

個別のデバイスのロック解除

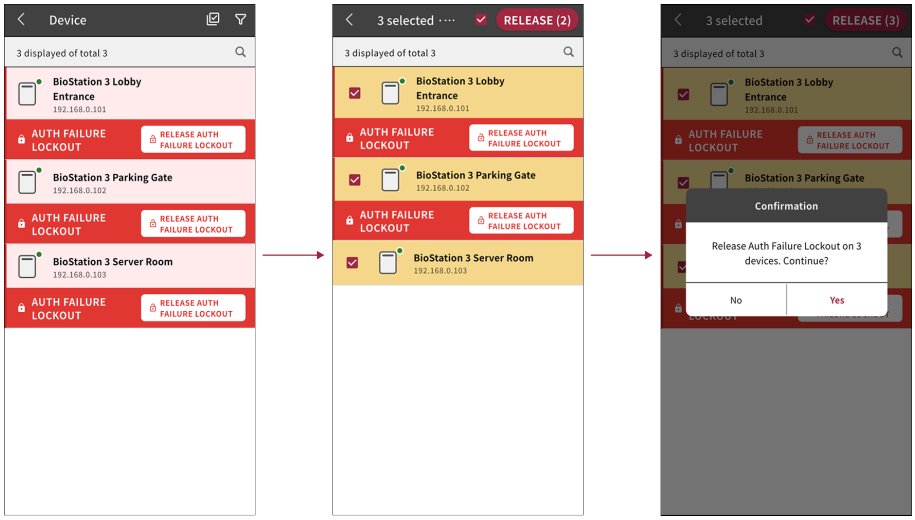
デバイス一覧で認証失敗ロック状態のデバイスを解除できます。



1. デバイス一覧で、**AUTH FAILURE LOCKOUT** ラベルが表示されたデバイスを確認してください。
2. 該当デバイスのロックを解除するには、**RELEASE AUTH FAILURE LOCKOUT** ボタンをタップしてください。
3. 確認メッセージが表示されたら、**Yes** をタップしてください。
4. ロック解除成功メッセージが表示されたら、**OK** をタップしてください。

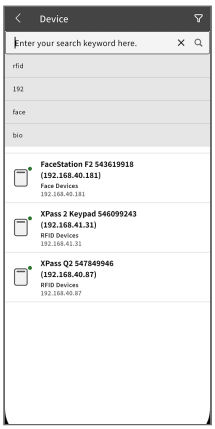
複数のデバイスのロック解除

AUTH FAILURE LOCKOUT ラベルが表示された複数のデバイスを同時にロック解除できます。



1. デバイス一覧の右上にある をタップしてください。
2. **AUTH FAILURE LOCKOUT** ラベルが表示されたデバイスを一台以上選択してください。
3. 右上の **RELEASE** ボタンをタップしてください。
4. 確認メッセージが表示されたら、**Yes** をタップしてください。
5. ロック解除成功メッセージが表示されたら、**OK** をタップしてください。

デバイス検索



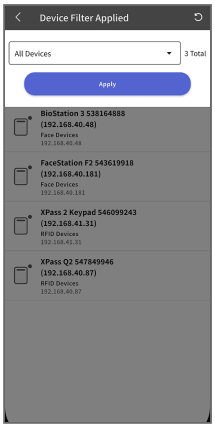
デバイス名、グループ、IPアドレスで検索できます。

1. デバイス一覧の上部にある をタップしてください。
2. 検索入力フィールドに検索語を入力します。デバイス名、グループ名、IPアドレスで検索できます。
3. 検索語の入力を完了したら、 をタップします。

検索結果に、検索語に一致するデバイスを表示します。

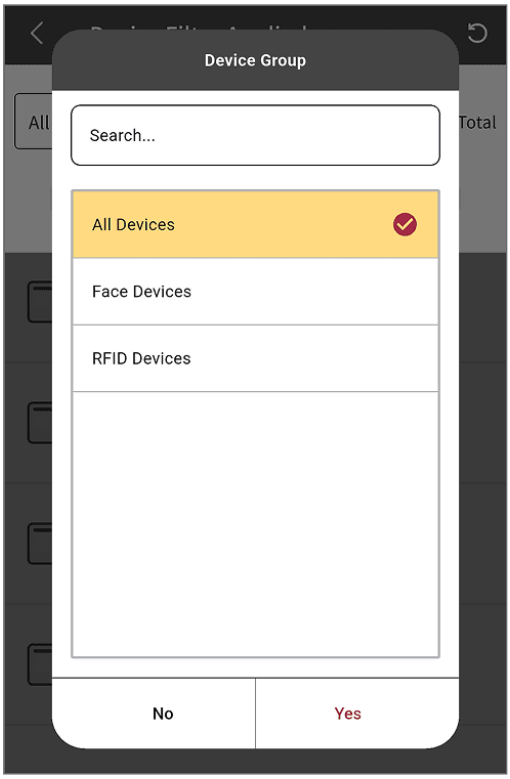
> **情報**
>
> - 検索入力フィールドの下には、最近の検索履歴が表示されます。最近の検索履歴をタップすると、その検索語で再度検索できます。
> - 検索入力フィールドを閉じるには をタップします。

デバイス一覧をフィルタリングする



デバイス一覧をデバイスグループでフィルタリングできます。

1. デバイス一覧の上部にある をタップしてください。
2. **All Devices**をタップしてください。
3. デバイスグループ一覧から目的のグループを選択します。



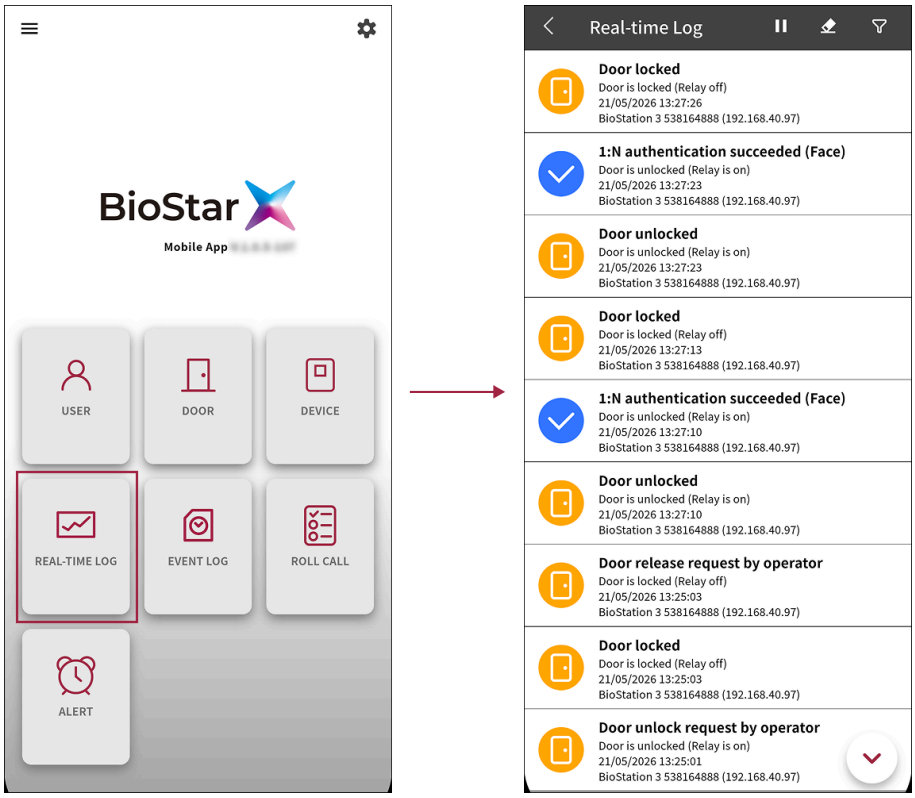
4. デバイスグループの選択を完了したら **Yes** をタップします。
5. 選択した条件でデバイス一覧をフィルタリングするには **Apply** をタップしてください。

一覧に、選択したデバイスグループに属するデバイスを表示します。

> **情報**
> フィルタリング条件を初期化するには、画面右上の → をタップします。

リアルタイムログモニタリング

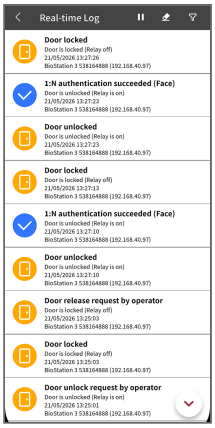
BioStar Xサーバーで発生するイベントをリアルタイムで確認してください。アプリのホーム画面で **REAL-TIME LOG** をタップしてください。



REAL-TIME LOG では、次のような状況で使用できます。

- 出勤時間帯の入場試行を監視
- 現在受信中のイベントをリアルタイムで確認

リアルタイムログの確認



アプリのホーム画面で **REAL-TIME LOG** をタップしてください。最初にリアルタイムログ(**Real-time Log**)画面を開くと、一覧は空です。

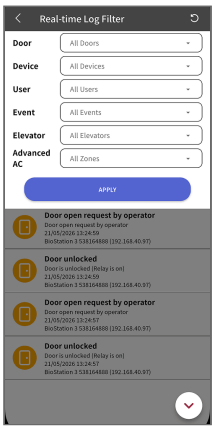
- 新しいイベントが発生すると、自動的に一覧へリアルタイムで追加されます。一覧の行数に制限はなく、新しいイベントは先頭に追加されます。
- リアルタイムイベントの受信を一時停止するには、画面右上の ⏸ をタップしてください。一時停止中は新しいイベントが一覧に追加されませんが、バックグラウンドでキューに追加されます。リアルタイムイベントの受信を再開するには、▶ をタップしてください。キューに追加されたイベントは、新しいイベントより先に一覧へ追加されます。
- リアルタイムログ一覧を消去するには、画面右上の をタップしてください。ログ一覧が消去され、新しいイベントが発生した時点からリアルタイムで追加されます。
- リアルタイムログ一覧をフィルタリングして、特定のイベント、ユーザー、ドア、またはデバイスなど、関連するログだけを表示できます。詳しくは 特定のログのみ表示 を

ご参照ください。

情報

- 別のメニューへ移動してから再び **Real-time Log** に戻ると、ログ一覧は空になり、新しいログが発生した時点からリアルタイムで追加されます。
- ログに表示される日付と時刻は、BioStar Xサーバーの環境設定に従います。BioStar Xの日付と時刻の表示形式設定の詳細は、基本設定を構成する をご参照ください。
- リアルタイムログ画面は、サイドメニュー(☰) → **Monitoring** → **Real-time Log** をタップして開くこともできます。

特定のログのみ表示



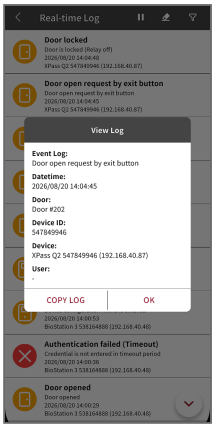
リアルタイムログ一覧では、特定のイベント、ユーザー、ドア、またはデバイスなど、関連するログだけを表示するようにフィルタリングできます。

1. 画面右上の をタップしてください。
2. 表示したいログだけに絞るには、下のフィルタ条件を組み合わせて設定してください。
   - **Door**: 特定のドア（例: 1階正面入口）
   - **Device**: 特定のデバイス（例: 特定の入退室制御デバイスで発生したイベント）
   - **User**: 特定のユーザー（例: VIPユーザーの入退室記録）
   - **Event**: 特定のイベント種別（例: 顔認証失敗、侵入警報アラームなど）
   - **Elevator**: 特定のエレベーター（例: 特定階のエレベーター）
   - **Advanced AC**: 特定の高度な入退室制御（例: アンチパスバック、火災警報、スケジュール開閉錠など）
3. 設定した条件でログ一覧をフィルタリングするには、**Apply** をタップしてください。

情報

- フィルタ条件を初期化するには、画面右上の → をタップしてください。
- エレベーターと高度な入退室管理は、**エッセンシャル**（Essential）以上のライセンスを有効化した場合に使用できます。ライセンスポリシーの詳細については、ライセンス ポリシーをご参照ください。

ログ詳細情報の確認



ログ項目をタップして、そのログの詳細情報を確認してください。

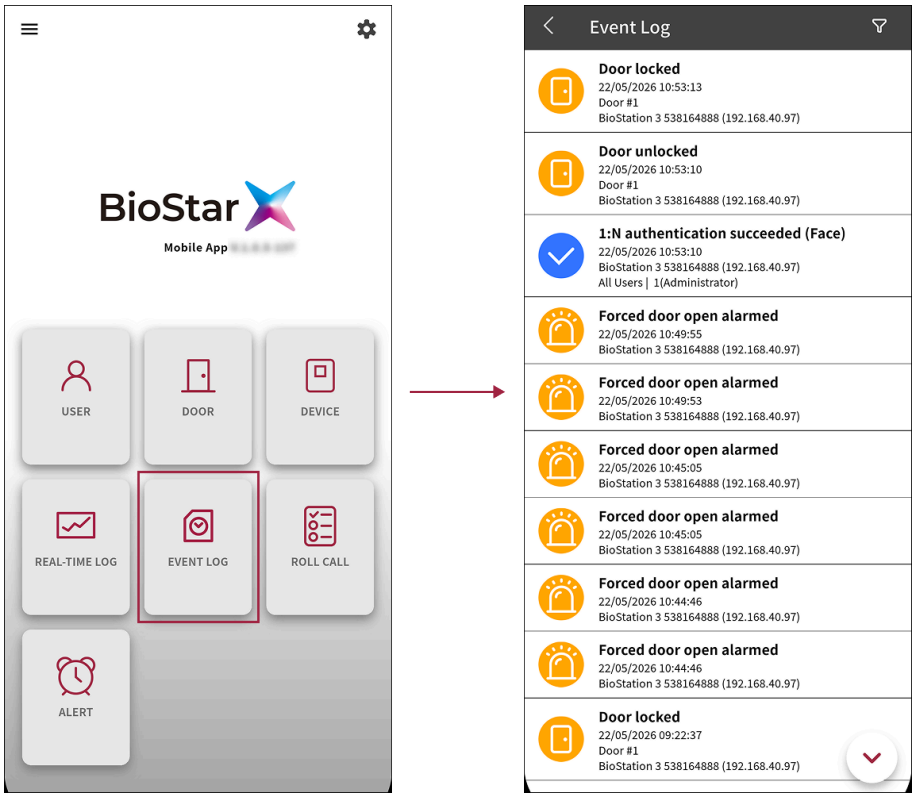
- **Event Log**: イベントの種類です。どの種類のイベントが発生したかを表示します。
- **Datetime**: イベントが発生した日付と時刻です。
- **Door**: イベントが発生したドアです。
- **Device ID**/**Device**: イベントが発生したデバイス ID とデバイス名です。
- **User**: イベントを発生させたユーザーです。たとえば、入退室認証イベントの場合、入室を試みたユーザーが表示されます。

詳細情報ポップアップ下部のボタンをタップして、次の操作を実行できます。

- イベント情報をクリップボードにコピーするには、**COPY LOG**をタップしてください。
- 詳細情報ポップアップを閉じるには、**OK** をタップしてください。

過去ログの照会

過去ログを照会して、特定の期間と場所で発生した入退室履歴を確認できます。ログをフィルタリングすると、条件に合うイベントを簡単に見つけられます。

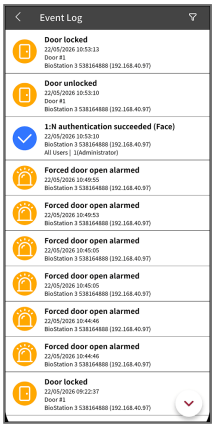


EVENT LOG 機能は、次のような状況で活用できます。

- 特定ユーザーの過去の入退室記録を確認
- 特定期間内のセキュリティイベント履歴を追跡
- 入退室管理の監査とレポート作成

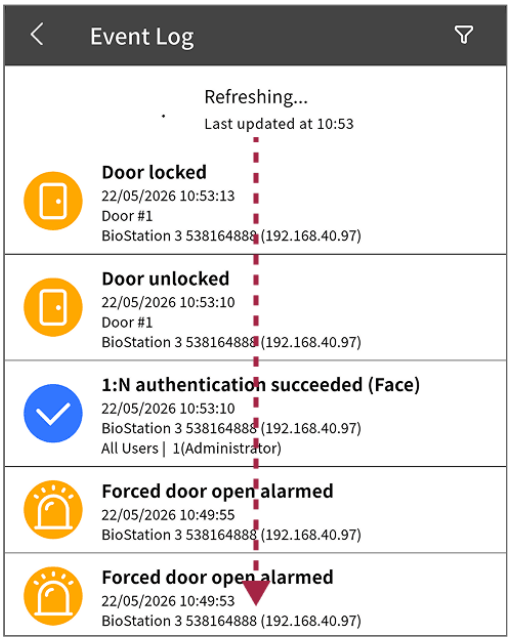
> **リアルタイムログとの違い**
> - **リアルタイムログ**: 現在発生しているイベントをすぐに監視できます。リアルタイムログは現在の状況を把握し、即時対応が必要な場合に役立ちます。
> - **過去ログ**: 特定期間のイベント履歴を検索して照会できます。

過去ログの照会



アプリのホーム画面で **EVENT LOG** をタップします。

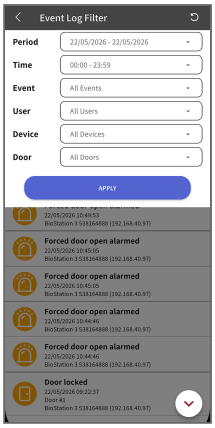
- 各ログには、イベントタイプ、発生時刻、出入口/デバイス、ユーザー情報が表示されます。
- ログ一覧を下に引いて更新すると、一覧が更新され、最新のログが表示されます。



情報

- ログに表示される日付と時刻は、BioStar Xサーバーの環境設定に従います。BioStar Xの日付と時刻の表示形式設定の詳細は、基本設定を構成する をご参照ください。
- イベントログ画面には、サイドメニュー（☰）→ **Monitoring** → **Event Log** をタップして移動することもできます。

特定のログのみを表示

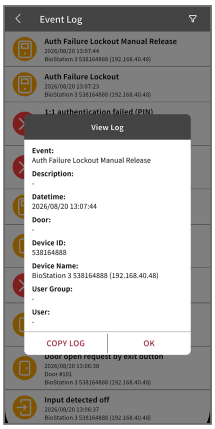


ログ一覧で、特定のイベント、ユーザー、出入口、またはデバイスなど、関連するログのみをフィルタリングして表示できます。

1. 画面右上の をタップしてください。
2. 表示したいログだけに絞るには、下のフィルタ条件を組み合わせて設定してください。
   - **Period**: イベント発生期間の設定
   - **Time**: イベント発生時刻の設定
   - **Event**: 特定のイベントタイプを選択（例: 顔認証失敗、侵入警報アラームなど）
   - **User**: 特定のユーザーを選択（例: VIPユーザーの入退室記録）
   - **Device**: 特定のデバイスを選択（例: 特定の入退室管理デバイスで発生したイベント）
   - **Door**: 特定の出入口を選択（例: 1階正面入口）
3. 設定した条件でログ一覧をフィルタリングするには、**Apply** をタップしてください。

> **情報**
> フィルタ条件を初期化するには、画面右上の → をタップしてください。

ログ詳細情報の確認



ログ一覧で希望するログをタップすると、そのログの詳細情報を確認できます。

- **Event**：発生したイベントの種類です。（例：入退室認証成功、入退室認証失敗、アラーム発生など）
- **Description**：イベントの説明です。
- **Datetime**: イベントが発生した日付と時刻です。
- **Door**: イベントが発生したドアです。
- **Device ID**/**Device Name**：イベントが発生したデバイスのIDと名前です。
- **User Group**：イベントを発生させたユーザーのグループ名です。
- **User**: イベントを発生させたユーザーです。

詳細情報ポップアップ下部のボタンをタップして、次の操作を実行できます。

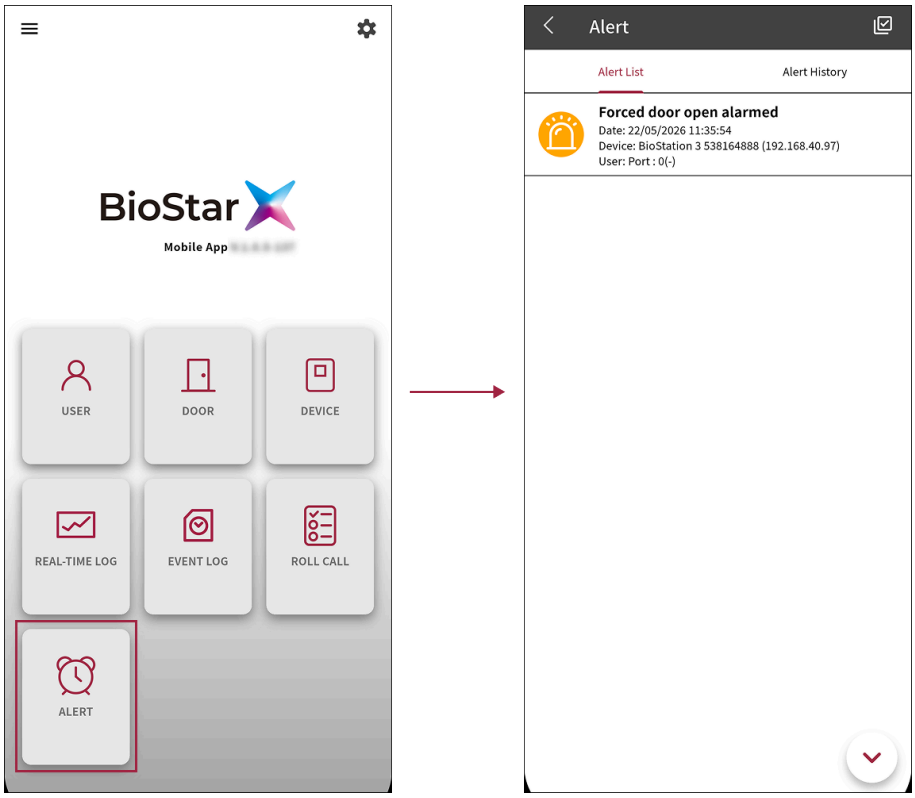
- イベント情報をクリップボードにコピーするには、**COPY LOG**をタップしてください。
- 詳細情報ポップアップを閉じるには、**OK** をタップしてください。

情報

イベントログが出入口関連イベントの場合、ログ詳細情報に出入口制御関連情報が追加で表示されます。

警報アラームの確認と解除

BioStar Xで発生した警報アラームを、モバイルアプリで確認し、必要に応じて解除できます。出入口の強制開放などの警報アラームイベントが発生したとき、アプリで警報アラームを確認し、対応内容を記録できます。



情報

- BioStar Xで警報アラームを確認し、解除する方法の詳細は、イベントをモニタリングするを参照してください。
- 警報アラーム一覧に表示される日付と時刻は、BioStar Xサーバーの環境設定に従います。 BioStar Xの日付と時刻の表示形式設定の詳細は、基本設定を構成する をご参照ください。

警報アラーム一覧 (Alert List)

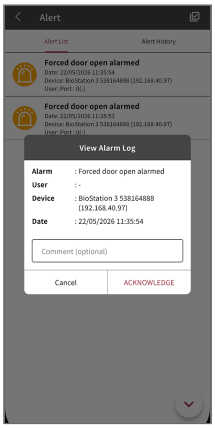


ホーム画面でALERTをタップします。警報アラーム一覧(Alert List)を確認できます。

警報アラーム一覧では、出入口の強制開放などの警報アラームイベントを新しい順で確認できます。新しい警報アラームイベントが発生すると、自動的に一覧へリアルタイムで追加されます。

情報

警報アラーム画面は、サイドメニュー(☰) → Alertをタップして開くこともできます。

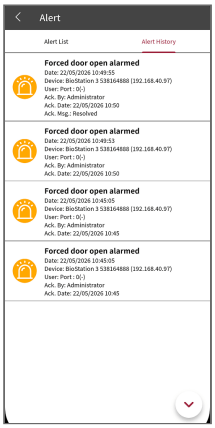


アラーム詳細情報の表示

警報アラーム一覧で特定のアラームをタップすると、そのアラームの詳細情報を確認できます。アラーム詳細情報には、発生したアラームイベントの種類、ユーザー、発生時刻、出入口/デバイスなどが表示されます。

- 警報アラームを確認し、対応内容などを記録するには、**Comment (optioinal)**フィールドに内容を入力します。入力した内容はBioStar Xサーバーに保存され、アラームイベントの詳細情報で確認できます。
- 対応内容を入力して警報アラームを解除するには、**ACKNOWLEDGE**をタップします。警報アラームが解除され、**Alert List**から該当アラームイベントが消えます。

警報アラーム履歴 (Alert History)



警報アラーム履歴では、確認済みの警報イベントを確認できます。各アラームイベントの種類、発生時刻、出入口/デバイス、ユーザーなどの情報を確認できます。確認済みのアラームイベントには、どのユーザーがいつ確認したかなどの情報も表示されます。

出席確認（Roll Call）を開始する

出席確認（Roll Call）は、特定の時点と場所での入退室記録を基に人員リストをすばやく作成します。緊急時には、ユーザーがあらかじめ指定された場所の入室または退室デバイスで認証し、出席確認場所に到着したかどうかを把握できます。

緊急対応、安全確認、救助隊への情報提供などに使用できます。これにより、入退室記録を効率的に活用して人員状況を管理できます。

> **情報**
>
> - 出席確認を開始する前に、BioStar Xで出席確認設定を完了する必要があります。出席確認の設定方法の詳細は 出席確認（Roll Call） を参照してください。
> - 出席確認設定は **エッセンシャル**（Essential）ライセンス以上で追加オプションとして利用できます。ライセンスポリシーの詳細については、ライセンス ポリシーを参照してください。

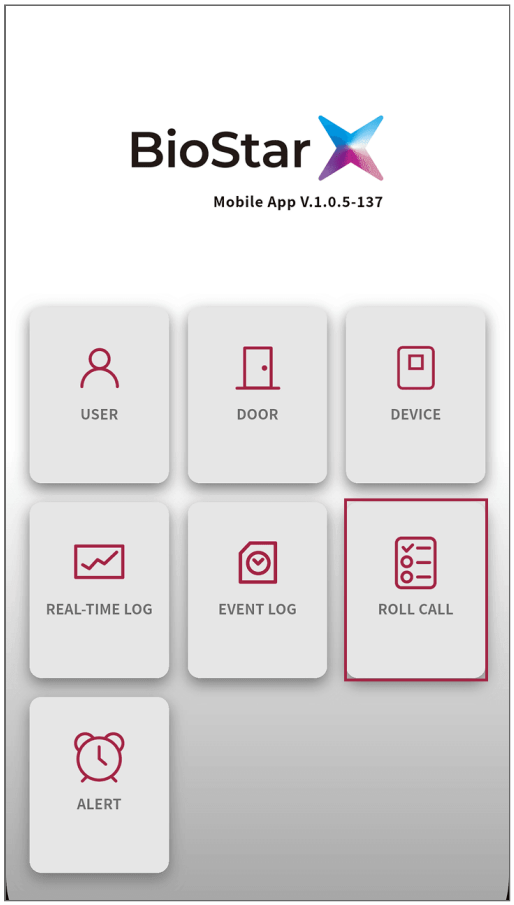
モバイルアプリで出席確認を使用する

出席確認機能は BioStar X モバイルアプリで利用できます。

出席確認を開始する

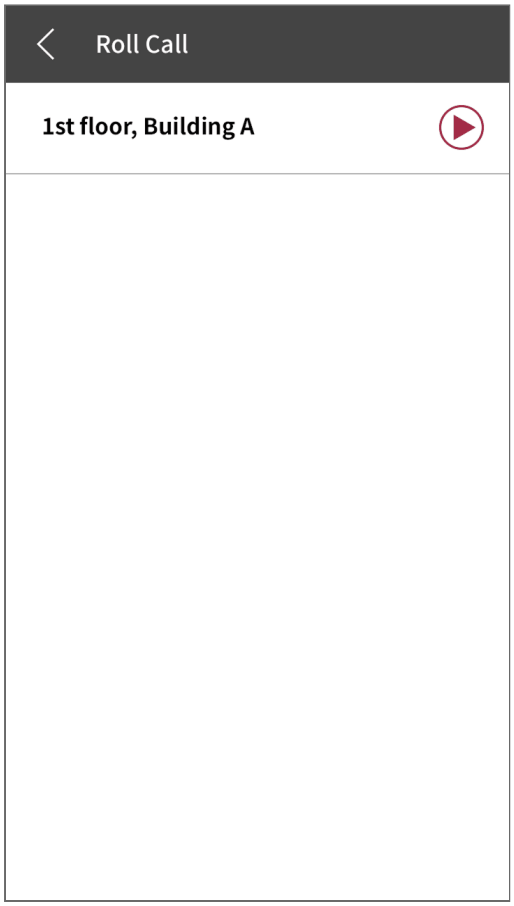
モバイルアプリで出席確認機能を開始するには、次の手順に従います。

1. モバイル端末で BioStar X モバイルアプリを起動します。
2. アプリのホーム画面で **ROLL CALL** をタップします。



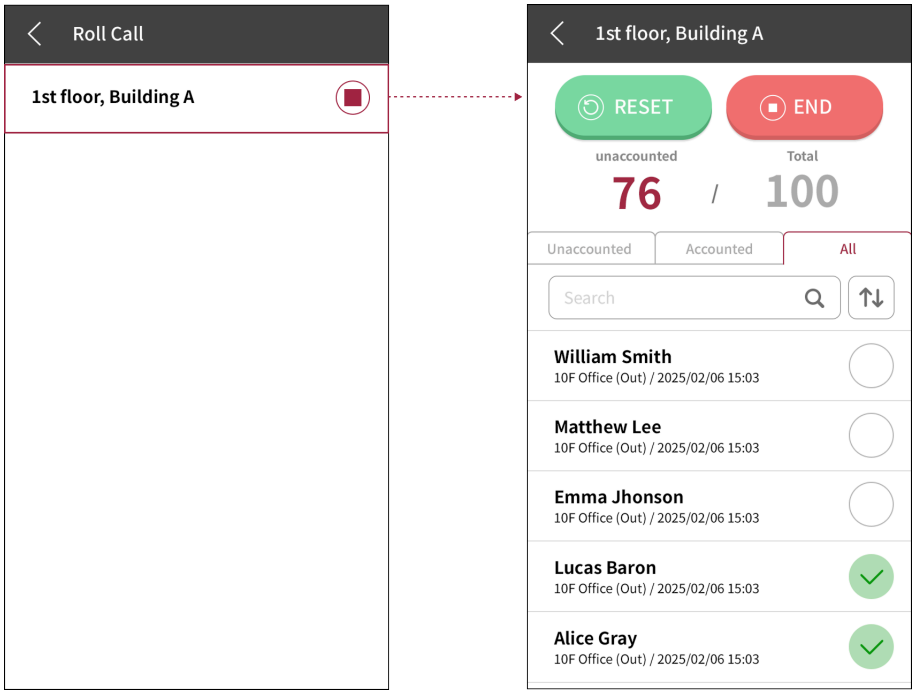
サイドメニューからも開けます。 ☰ → **Monitoring** → **Roll Call** をタップします。

3. Roll Call リストで出席確認を実行する項目の ▶ をタップします。



4. 確認メッセージが表示されたら、**Yes** をタップします。

出席確認が開始され、進行中の出席確認項目をタップすると出席確認状況を確認できます。



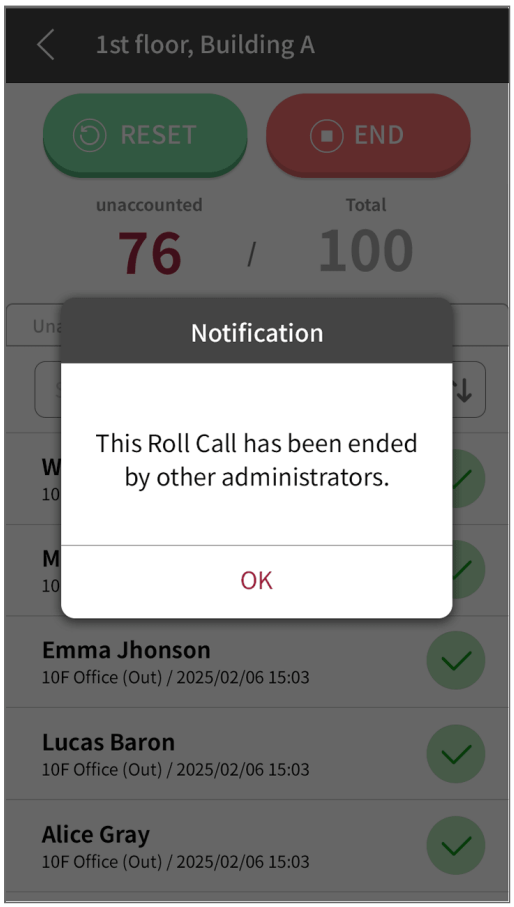
進行中の出席確認を制御する

- 入室済みのユーザーには アイコンが表示されます。すべてのユーザーが入室すると、出席確認終了メッセージが表示されます。出席確認を終了するには **Yes** をタップします。

- 管理者は手動でユーザーの入室または状態を変更できます。ユーザーリストで状態を変更するユーザーの一番右にある丸いボタンを長押しします。



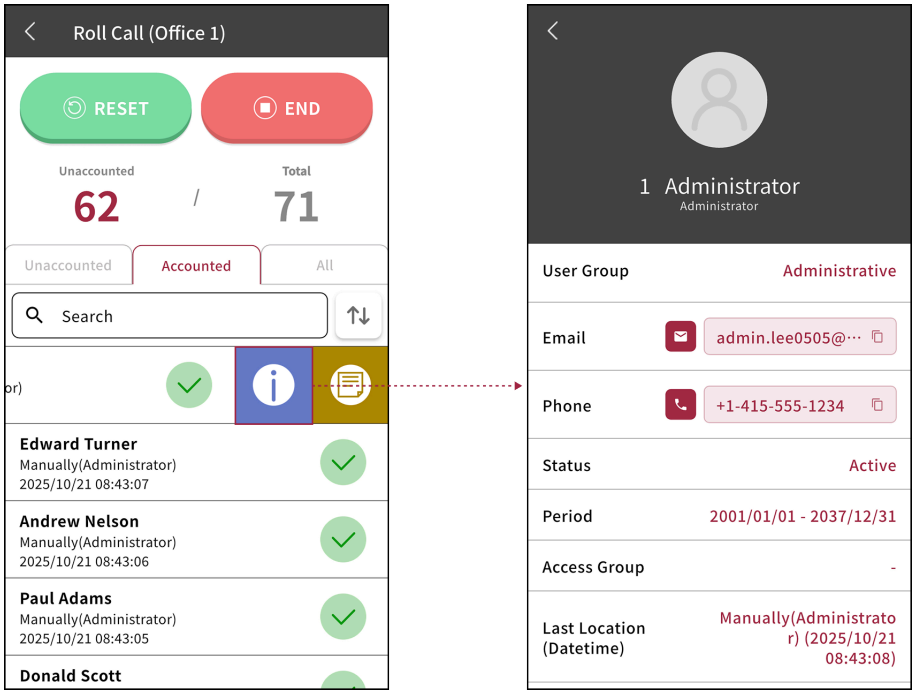
- 出席確認を初期化するには **Reset** をタップします。これまでのすべての変更が削除され、出席確認を最初から再開できます。
- 別の管理者によって出席確認が終了すると、通知メッセージが表示されます。



出席確認中のユーザー情報確認

モバイルアプリで、出席確認中に各ユーザーの情報を確認できます。ユーザーに緊急連絡を取れる連絡先情報や、ユーザーの最終位置などの詳細を確認できます。

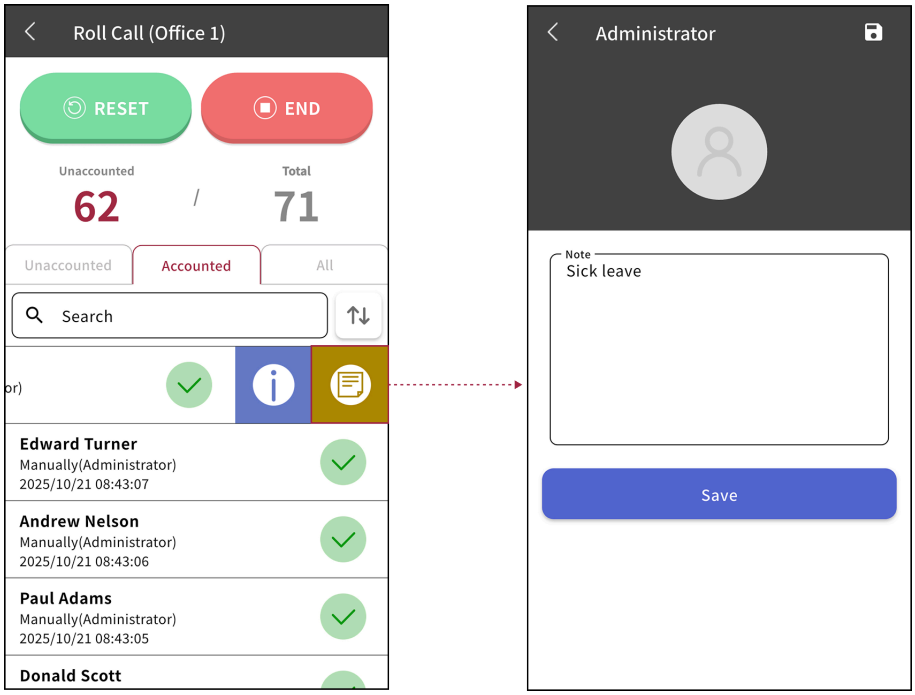
出席確認中に詳細を確認するユーザー項目を左にスワイプします。その後、ⓘをタップします。



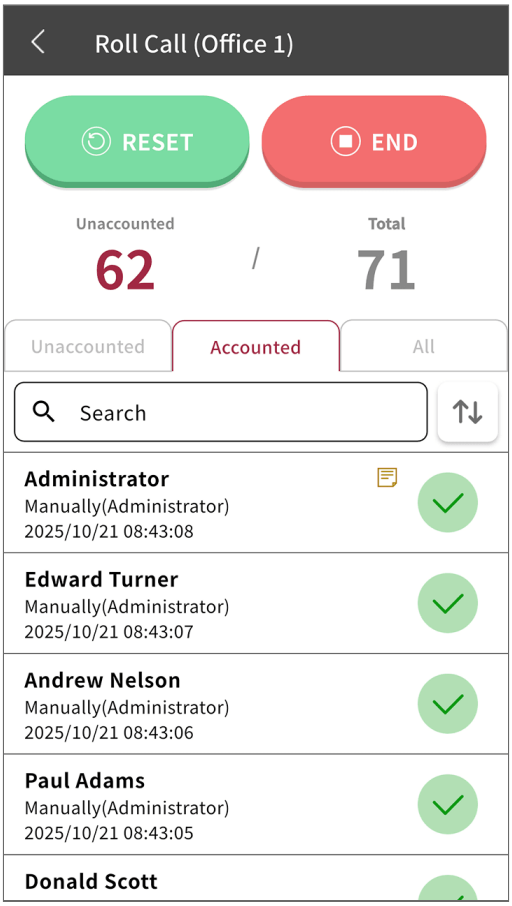
出席確認中にユーザーへメモを残す

モバイルアプリで出席確認中に特定のユーザーが入室していない場合、そのユーザーにメモを残すことができます。

出席確認中にメモを入力するユーザー項目を左へスワイプしてください。その後、をタップします。メモ入力画面で内容を入力してから **Save** をタップします。



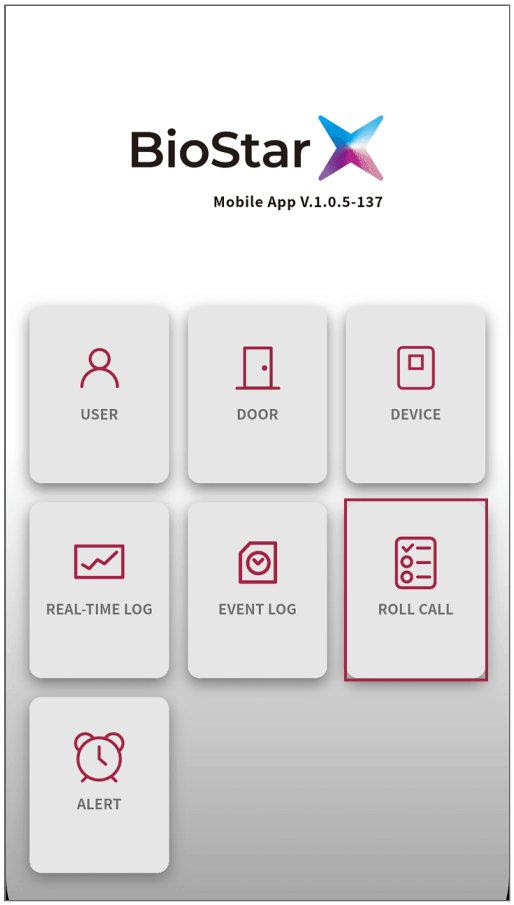
メモを入力したユーザーには、出席確認リストでアイコンが表示されます。



出席確認の詳細を確認

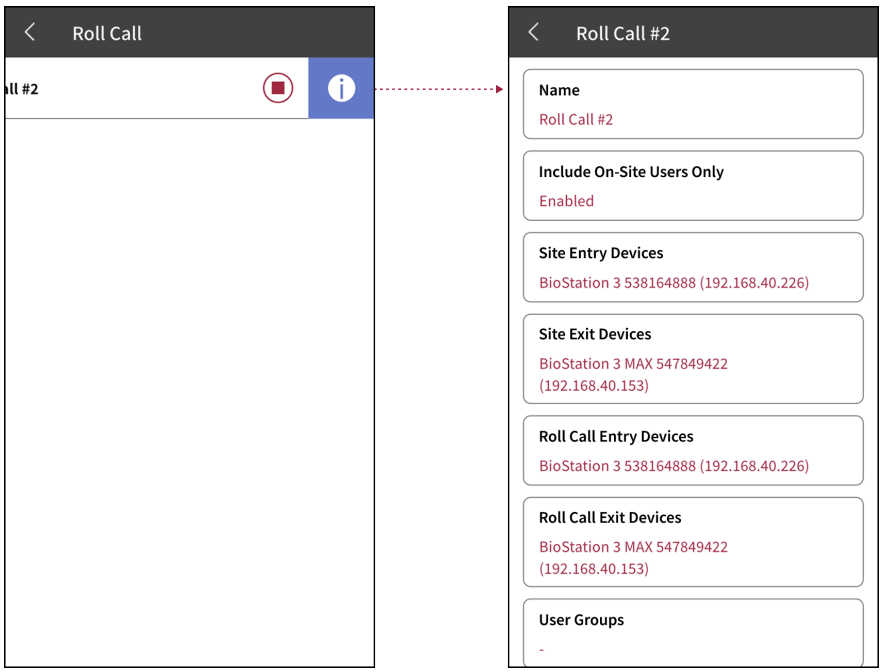
モバイルアプリで出席確認設定の詳細を確認できます。

1. モバイル端末で BioStar X モバイルアプリを起動します。
2. アプリのホーム画面で **ROLL CALL** をタップします。



サイドメニューからも開けます。 ☰ → **Monitoring** → **Roll Call** をタップします。

3. 一覧で詳細を確認する項目を左へスワイプし、ⓘ をタップします。

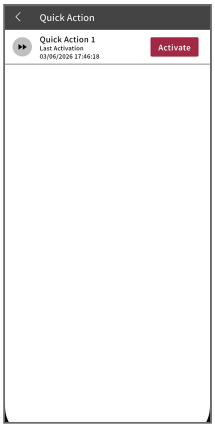


クイックアクションを使用する

クイックアクションは、緊急時に複雑な制御手順を自動化する機能です。あらかじめ定義した複数のデバイスの動作を1つのボタンで即時に実行し、迅速に対応できます。

> **情報**
>
> - **クイックアクション**機能の詳細は、クイックアクションを使用するを参照してください。
> - モバイルアプリでは、クイックアクション機能を実行したり、クイックアクション項目の詳細情報を確認したりできます。クイックアクションを作成または編集するには、BioStar X Webインターフェースにログインして設定します。

クイックアクションの実行



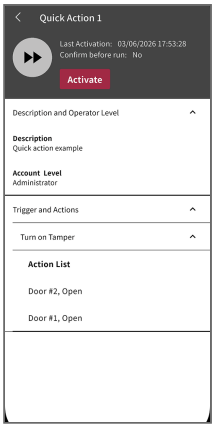
BioStar X Webインターフェースでクイックアクションを作成すると、モバイルアプリで使用できます。

1. アプリのホーム画面で**QUICK ACTION**をタップします。
2. クイックアクション一覧で、実行するクイックアクション項目の**Activate**ボタンをタップします。

クイックアクションが正常に実行されると、成功メッセージが表示されます。

> **情報**
>
> - クイックアクション設定によっては、実行確認のポップアップが表示される場合があります。
> - 各クイックアクション項目には、最近の実行日時が表示されます。

クイックアクションの詳細



クイックアクション項目に設定された詳細情報を確認するには、クイックアクション一覧で項目をタップします。

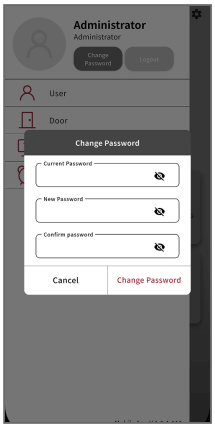
- **Last Activation**: クイックアクションが最後に実行された日時です。
- **Confirm before run**: クイックアクションの実行確認ポップアップが表示されるかどうかを示します。
- **Activate**: クイックアクションを実行するボタンです。
- **Description and Operator Level**: クイックアクションの説明と、実行権限が必要な管理者レベルです。
- **Trigger and Actions**: クイックアクションの実行時に制御するドアと、ドアに適用する

動作です。

> **情報**
> 作業条件と動作の詳細は、作業条件と動作を設定するを参照してください。

アカウントのパスワードを変更する

BioStar Xモバイルアプリでアカウントのパスワードを変更できます。アカウントのセキュリティを強化するため、パスワードを定期的に変更してください。



1. アプリのホーム画面で、画面左上の ☰ をタップします。
2. サイドメニューで **Change Password** をタップします。
3. **Current Password** 入力欄に現在のパスワードを入力します。
4. 新しいパスワードを **New Password**、**Confirm password** 入力欄に順に入力します。
5. パスワードの変更を完了するには、**Change Password** をタップします。

付録

製品に含まれる法的通知事項を掲載しています。

免責事項

- このウェブサイトは、Suprema製品に関する情報を提供します。
- このウェブサイトは、Supremaの製品使用および販売契約に含まれるSuprema製品にのみ使用できます。 このウェブサイトは、明示的、黙示的、禁反言の原則、またはその他いかなる方法によっても、知的財産権に対するライセンスを付与しません。
- お客様とSupremaとの契約に明示されている場合を除き、Supremaは一切の責任を負わず、特定目的への適合性、商品性、非侵害に関するあらゆる明示的または黙示的保証を否認します。
- 保証が無効となるのは、次の場合です。Suprema製品が 1) 誤って設置される、またはハードウェアのシリアル番号、保証情報、品質保証ステッカーが変更または除去された場合、2) Supremaが許可した方法以外で使用された場合、3) SupremaまたはSupremaが承認した以外の者によって変更、改造、修理された場合、4) 不適切な環境で運用または保守された場合。
- Suprema製品は、製品の故障が負傷や死亡事故につながる可能性のある医療、救命、生命維持などの用途向けに設計されていません。 お客様がこのような用途でSuprema製品を購入または使用する場合、これに起因する負傷または死亡によって発生するすべての請求、費用、損失、支出および合理的な弁護士費用から、SupremaおよびそのメンバーⅠ、子会社、関連会社、供給業者を免責するものとします。 製品の設計または製造にSupremaの過失があると主張される場合でも同様です。
- Supremaは、信頼性、機能または設計を向上させるため、予告なくいつでも仕様および製品説明を変更する権利を有します。
- 個人情報は、製品使用時に認証メッセージおよびその他の関連情報の形でSuprema製品に保存されることがあります。 Supremaは、Supremaが直接制御できない、または関連契約に明示されたSuprema製品に保存される個人情報を含むいかなる情報についても責任を負いません。 個人情報を含む保存された情報を使用する場合、製品ユーザーは関連法（例：GDPR）を遵守し、適切に取り扱いおよび処理する責任があります。
- お客様は、いかなる機能の欠如や特性、または"reserved"や"undefined"と表示された説明に依存してはなりません。 Supremaは後日これを定義することができ、後日行われた変更が現行内容と矛盾した場合でも、Supremaは責任を負いません。
- 本サイトに明示的に記載されている場合を除き、Supremaは法律で許容される最大範囲で"現状のまま"販売されます。
- 製品を注文する前に、最寄りのSuprema営業所または代理店に問い合わせ、最新の仕様を確認してください。

著作権に関するお知らせ

本ウェブサイトの著作権は Suprema に帰属します。 その他の製品名、商標、登録商標に関する権利は、それぞれの所有者である個人または団体に帰属します。

オープンソースライセンス

本製品にはオープンソースソフトウェアが含まれています。 GPL、LGPL、MPL などソースコード配布を必要とするオープンソースライセンスが適用されるソースコードは、Suprema グローバル技術サポートチーム にご請求いただくことで入手できます。

本製品のソースコードは、製品最終出荷日から 3 年間、Suprema グローバル技術サポートチームへご依頼いただくことで入手可能です。

ソースコードをその他の物理媒体で受け取る場合、料金が発生することがあります。本提案は、この情報を受け取ったすべての方に有効です。

この製品に含まれるオープンソースソフトウェアに関する必須通知事項とライセンスは、⚙ → **License**で確認できます。

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。