BioStar X

管理者ガイド

バージョン 1.0.3

日本語

JA 102.00.BSX

suprema
SECURITY & BIOMETRICS

目次

概要 6

さらに強化された運用効率とセキュリティ 6

強力な拡張性と安定性の提供 6

開始する前に 7

対応デバイス 11

システム最小要件 13

はじめに 16

ネットワーク優先順位を確認する 16

簡単インストール 23

カスタムインストールを実行する 30

アップグレードする 38

マルチコミュニケーションサーバーをインストールする 46

ログインする 53

ライセンスキーを登録する 55

初期設定ガイド 58

サーバー管理 60

サーバーの起動と停止 60

サービス設定 61

メインサーバーのIPアドレスを変更する 64

ポートを変更する 67

データベースを変更する 68

補助データベースを追加する 70

BioStar Xサーバーのアンインストールとセキュリティ証明書の復元 78

ランチャー 85

ユーザー 86

ユーザーグループを管理する 86

ユーザー登録 90

ユーザー基本情報を入力 92

ユーザークレデンシャルを登録する 94

ユーザー権限を設定する 118

ユーザーの詳細設定 121

身分証明書のスキャンでユーザーを登録、編集する 122

ユーザーを閲覧する 126

ユーザー管理 131

アクセスグループを管理する 141

多要素認証でログインする 143

顔を一括登録する 145

顔マイグレーション 150

緊急開放権限を設定する 152

モニタリング 155

ドアをモニタリング 155

マップをモニタリングする 183

デバイスをモニタリングする 191

ビデオをモニタリングする 199

イベントをモニタリングする 206

データ 215

レポートを作成する 215

自動生成スケジュールを設定する 230

レポート保存パスを設定する 232

ダッシュボード 233

ウィジェットを追加 233

ウィジェットを編集する 239
ウィジェットを削除する 240

設定 241

デバイス管理 241
デバイス設定 264
イメージログを設定する 302
USB エージェントを設定する 306
デバイス接続管理を設定する 308
ドア管理 311
運用権限管理 324
長期間未入退室ユーザーへの対処 329
身分証明書スキャンを設定する 334
入退室制御設定 335
スケジュールを設定する 345
作業条件と動作を設定する 348
クイックアクションを使用する 350
イベントログの取得 353
アラームを設定する 355
クレデンシャル管理 356
ライセンスを有効化 379
監査トレイルを管理する 385
システム設定 394

高度な設定 426

エレベーター管理 426
高度な入退室制御設定 433
ビデオ設定 463
マップ管理 485
訪問者設定 500
ディレクトリ連携を設定する 504

リモートアクセスを設定する 516
仮想デバイスのイベントログを連携する 519

プラグイン 524

プラグイン (Plugins) とは？ 524
BioStar X提供プラグイン 524
主要な活用事例 524
プラグインの登録 524
プラグインの管理 526
勤怠管理を使用 527
訪問者の申請と管理 573

UI を確認 588

共通 UI を理解する 588
ユーザー 588
モニタリング 590
ダッシュボード 590
設定 591

ライセンス ポリシー 593

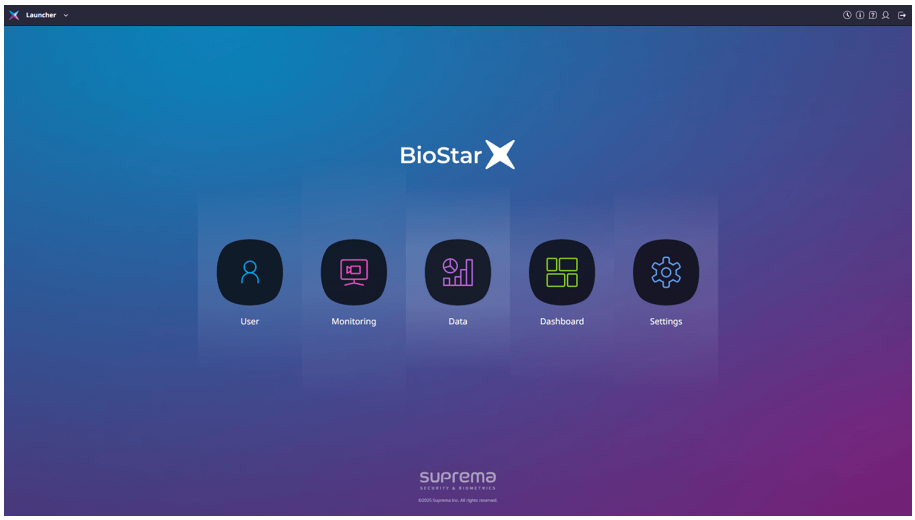
基本ライセンス 593
ライセンスアップグレード 594
機能追加オプション (Feature Add-ons) 594
高度な入退室管理（Advanced Access Control） 596
デバイスライセンス 596

付録 598

免責事項 598
著作権に関するお知らせ 599
オープンソースライセンス 599

概要

BioStar Xは、AIベースの入退室管理とインテリジェント映像解析を融合したSupremaの次世代統合セキュリティプラットフォームです。単なる入退室管理を超え、セキュリティ運用全体を効果的に統合管理できる革新的なプラットフォームです。



BioStar XはAIベースの入退室管理とインテリジェント映像解析を統合し、AI技術を活用してリアルタイムの入退室管理、映像モニタリング、異常行動検知を1つのプラットフォームで行えるよう設計されています。入退室管理だけでなく、侵入検知、徘徊検知、転倒検知など多彩なAIベースの映像解析機能を備えており、事前対応が可能です。

さらに、ピープルカウント、テイルゲーティング検知、ブラックリスト検出、行方不明者捜索機能により、大規模施設でもより精緻なセキュリティ監視を実現します。これらの機能は、学校、ショッピングモール、空港、病院などの多目的施設はもちろん、スマートビルでも有効に活用できます。

さらに強化された運用効率とセキュリティ

BioStar Xは、1つのプラットフォーム上であらゆるセキュリティ要素をリアルタイムに統合管理できるよう支援します。これにより、セキュリティ担当者は個別システムを別々に管理することなく、単一のインターフェースで効率的にモニタリングと制御を行えます。

さらに、統合運用方式はセキュリティ監視要員を最適化し、保守にかかるコストと時間を削減する効果をもたらします。個別のセキュリティシステムを追加する必要がなく、BioStar Xの柔軟な拡張性を活用すれば、必要な機能を簡単に追加でき、より安全で効率的なセキュリティ環境を構築できます。

強力な拡張性と安定性の提供

大企業や公共機関などのエンタープライズ環境では、セキュリティシステムの拡張性と安定性が不可欠です。 BioStar X は数万人以上のユーザー登録に対応し、多様なデバイスを接続しても安定した運用が可能です。

さらに、ユーザーに合わせたUI・UXを提供し、複雑なセキュリティ運用をより直感的に管理できるよう支援します。モニタリング画面のインターフェースレイアウトを自由に構成できるため、必要な情報を迅速かつ効果的に確認できます。

必須のセキュリティソリューション BioStar X

セキュリティ脅威が多様化し運用の複雑性が高まる現在、AIと統合セキュリティ技術を融合した BioStar X は、不可欠なセキュリティソリューションとしての地位を確立しています。強力なセキュリティと効率的な運用を同時に求める企業にとって、BioStar X

は最良の選択肢となると確信できます。

開始する前に

> **ヒント**
> BioStar X を開始する前に知っておくべき事項を案内します。 BioStar X は 64 ビットオペレーティングシステムをサポートします。インストールする前に、BioStar X をインストールする PC のシステム仕様を確認してください。

インストール前の注意事項

BioStar X をインストールする前に、次の事項を確認してからインストールを進めてください。

- BioStar X は 64 ビットオペレーティングシステムにのみインストールできます。
- MS SQL 2012 Express を使用する場合は サービス パック 3 をインストールしてください。
- MS SQL 2014 Express を使用する場合は サービス パック 2 をインストールしてください。
- MS SQL Server を使用する場合は、サーバーと各テーブルの `Collation` オプションを CI（大文字小文字を区別しない）に設定してください。
- 旧バージョンの BioStar X でデータベースをバックアップする際は、すべてのサービスを停止してから実行してください。また、AC データベースと TA データベースを同時にバックアップして復元しないと、TA データベースを使用できません。
- BioStar X データベースをバックアップする際は、*\Program Files\BioStar X\util* フォルダーの *enckey* ファイルと *\Program Files\BioStar X* フォルダーの *system.conf*、*setting.conf* ファイルも必ず一緒にバックアップしてください。これを行わないと、データベースが使用できなくなります。
- BioStar X が使用するポートの既定値については、サービス設定をご参照ください。他のプログラムが同じポートを占有している場合、BioStar X が正常に動作しない可能性があります。

データベースの確認

BioStar X をインストールする前に、ユーザーが独自に構成したデータベースを使用する場合は、以下の事項を確認してください。

MariaDB

1. *my.cnf* ファイルの `[mysql]` セクションの下にあるオプションを次のように変更してください。

   my.cnf

   ```
   character-set-server=utf8
   collation-server=utf8_unicode_ci
   max_connections = 600
   ```

2. *my.cnf* ファイルの `[mysql]` セクションの下に次のオプションを追加してください。

   my.cnf

```
log_bin_trust_function_creators = 1
group_concat_max_len = 102400
```

3. root 権限で MariaDB に接続し、次のコマンドを実行してください。

   SQL

```
GRANT SUPER ON . TO user_id@'localhost' IDENTIFIED BY "password";
GRANT SUPER ON . TO user_id@'%' IDENTIFIED BY "password";
```

MS SQL Server

> **情報**
>
> - すべてのデータベースとテーブルの `Collation` オプションを、大文字小文字を区別しない CI（Case-insensitive）に設定してください。
> - データベース名には、数字、英字（大文字小文字を区別）、特殊記号 `-` と `_` のみを使用できます。

ポート設定

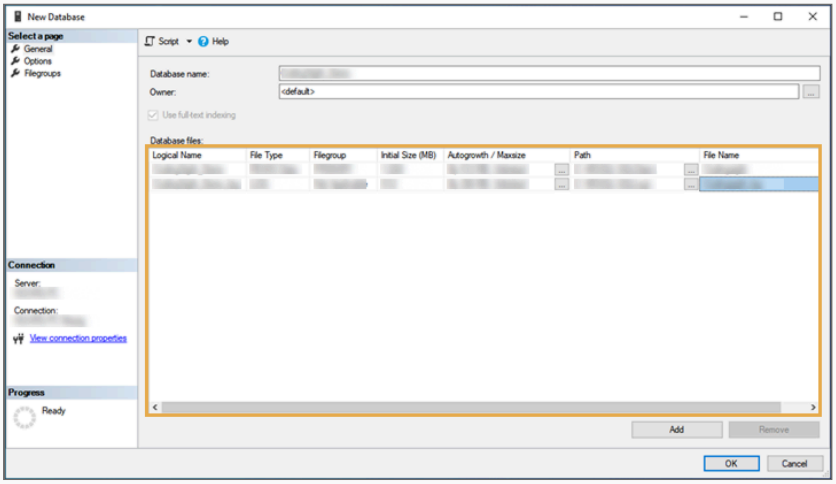
- **SQL Server 構成マネージャー** を起動し、**SQL EXPRESS に対するプロトコル** の **TCP/IP プロトコル** を使用したいポート番号に設定してください。
- 設定を適用するには、SQL Server サービスを再起動してください。

ユーザーとデータベースの作成

1. **SQL Server Management Studio** で **SQL Server 認証** を使用して **sa** アカウントでログインしてください。
2. **セキュリティ** を右クリックし、**新しいログイン** をクリックしてください。
3. **ログイン名** フィールドに任意の名前を入力し、**SQL Server 認証** を選択してください。
4. **パスワード** と **パスワード確認** フィールドに使用するパスワードを入力し、**パスワード ポリシーの適用を強制** を無効にしてください。
5. **OK** をクリックしてください。
6. **データベース** を右クリックし、**新しいデータベース** をクリックしてください。
7. **データベース名** フィールドに任意の名前を入力してください。
8. **所有者** フィールドに手順 3 で設定したログイン名を入力してください。

ヒント

データベース ファイル セクションで、以下の推奨値に設定します。**自動増加** はパーセンテージではなく固定サイズ (MB/GB) で設定し、あまりにも小さい単位で頻繁に増加しないよう注意してください。



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。

小規模組織 (10 GB 以下)

- データ：**初期サイズ** 1〜5 GB、**自動増加** 100〜512 MB
- ログ：**初期サイズ** 512 MB〜2 GB、**自動増加** 100〜512 MB
- TempDB：**初期サイズ** 512 MB〜1 GB

> *例：データ 2 GB (**自動増加** 256 MB) / ログ 1 GB (**自動増加** 128 MB) / TempDB 512 MB*

中規模組織 (10〜500 GB)

- データ：**初期サイズ** 10〜50 GB、**自動増加** 512 MB〜1 GB
- ログ：**初期サイズ** 5〜10 GB、**自動増加** 512 MB〜1 GB
- TempDB：**初期サイズ** 2〜8 GB

> *例：データ 20 GB (**自動増加** 1 GB) / ログ 5 GB (**自動増加** 512 MB) / TempDB 4 GB*

大規模組織 (500 GB 以上)

- データ：**初期サイズ** 100 GB 以上、**自動増加** 1〜4 GB
- ログ：**初期サイズ** 20〜100 GB、**自動増加** 1〜4 GB
- TempDB：**初期サイズ** 8〜32 GB

> *例：データ 100 GB (**自動増加** 2 GB) / ログ 50 GB (**自動増加** 2 GB) / TempDB 16 GB*

注意

- **自動増加** を極端に小さい単位で設定したり、**最大サイズ** を **無制限** に設定したりせず、予想される増加量に応じて適切に設定するか、モニタリングしてください。
- トランザクションが多い環境では、ログを定期的にバックアップしてログ ファイルのサイズが増加しないよう注意してください。

Windows 認証のデータベース設定

1 事前設定

Microsoft Windows Active Directory を使用する場合は、Windows 認証データベースを設定する前に、以下の事前設定を完了してください。

1. **SQL Server Management Studio** に管理者アカウントでログインしてください。
2. **セキュリティ** を右クリックし、**新しいログイン** をクリックしてください。
3. **Windows 認証** を選択して **検索** をクリックしてください。
4. **ユーザーまたはグループの選択** ウィンドウで [場所] をクリックし、Active Directory のパスを選択して **OK** をクリックしてください。
5. **選択するオブジェクト名を入力してください** フィールドにユーザー名を入力し、**名前の確認** > **OK** をクリックしてください。
6. **[ページの選択]** で **サーバー ロール** をクリックしてください。
7. **sysadmin** を選択して **OK** をクリックしてください。
8. **[ページの選択]** で **ユーザー マッピング** をクリックしてください。
9. **ac**、**master**、**ta**、**ve** を選択し、**既定のスキーマ** を **dbo** に設定してください。
10. **OK** をクリックして保存してください。

2 Active Directory アカウントで MS SQL Windows Authentication を使用するための設定

1. *services.msc* を実行してください。
2. SQL Server データベースの **プロパティ** > **ログオン** 画面で **アカウント指定** を選択し、ドメイン ユーザーでログインしてください。
3. Windows ファイアウォールに 1433 ポートを例外として追加してください。
4. SQL Server に空の **ac**、**ta**、**ve** データベースを **sysadmin** 権限で作成してください。
5. SQL Server でドメイン ユーザーが Windows Authentication を使用できるように設定し、**ac**、**ta**、**ve** データベースに **sysadmin** 以外のすべての権限を割り当てます。
6. ローカル コンピューターを除くすべてのサービスを *services.msc* で接続します。
7. ドメイン ユーザーをローカル サービス コンピューターの管理者に設定します。
8. MS SQL ODBC を接続します。

3 データベース設定

1. **SQL Server 構成マネージャー** を起動し、**SQL Native Client** 配下の **クライアント プロトコル** をクリックします。
2. **TCP/IP** を選択し、既定ポートを確認します。

3. **SQL Server ネットワーク構成** 配下の **SQL EXPRESS に対するプロトコル** をクリックします。
4. **TCP/IP** で ODBC ポートが既定ポートと同じに設定されていることを確認します。
5. **SQL Server Management Studio** に管理者アカウントで接続します。
6. **セキュリティ** > **ログイン** をクリックし、**NT AUTHORITY\SYSTEM** をダブルクリックします。
7. **[ページの選択]** で **サーバー ロール** をクリックしてください。
8. **public** と **sysadmin** を選択してチェックし、**OK** をクリックします。
9. **[ページの選択]** で **ユーザー マッピング** をクリックしてください。
10. **ac**、**ta**、**ve** データベースを選択し、**OK** をクリックして保存します。

次のステップ

BioStar X をインストールするためのシステム最小要件を確認します。
初めてインストールするユーザー向けの簡易インストール手順を案内します。
既にインストール済みのデータベースと連携するためのカスタムインストール手順を案内します。

対応デバイス

BioStar X プラットフォームが対応するデバイス一覧です。



BioStation 3 Max



XPass Q2



BioEntry W3



BioStation 2a



BioStation 3



X-Station 2



FaceStation F2



XPass 2



FaceLite



BioLite N2



XPass D2



BioEntry R2



BioEntry P2



FaceStation 2



BioEntry W2



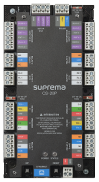
BioStation L2



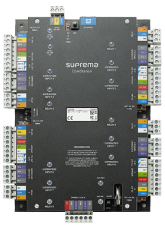
BioStation A2



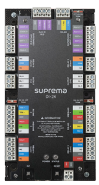
BioStation 2



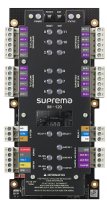
CoreStation 20



CoreStation



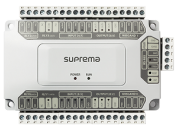
Door Interface



Input Module



Output Module



Door Module



Secure I/O 2

システム最小要件

BioStar X は、大規模エンタープライズ環境向けに、安定して拡張可能な統合セキュリティ管理ソリューションを提供します。システムはメインサーバーとマルチコミュニケーションサーバーで構成される分散アーキテクチャにより、最大千台以上のデバイスを効率的に管理できます。

メインサーバーはシステムの中核管理機能を担当し、マルチコミュニケーションサーバーはデバイス通信を専任することで負荷を分散し、パフォーマンスを最適化します。管理者はクライアント PC のウェブブラウザーからシステムにアクセスし、すべての管理業務を実行できます。以下のシステム要件を確認し、組織規模に合わせて最適な環境を構築してください。

> **情報**
> ライセンス構成および最適化の詳細については、Suprema グローバル技術サポートチーム までお問い合わせください。

メインサーバー

メインサーバーは **BioStar X** の中央管理システムがインストールされるサーバーです。ユーザーがウェブブラウザーで接続してシステムを管理し、ユーザー情報や入退室権限設定などのすべての業務を処理します。さらに、システム全体の状態を監視し、イベントログやアラームの管理を担当します。

項目		小規模組織	中規模組織	大規模組織
使用環境	デバイス数	1〜50 台	51〜100 台	101〜1,000 台
システム環境	オペレーティング システム	Windows 10、Windows 11、Windows Server 2016、Windows Server 2019、Windows Server 2022、Windows Server 2025		
	データベース	MariaDB 11.4.4、MS SQL Server 2012 SP3、MS SQL Server 2014 SP2、MS SQL Server 2016 SP1、MS SQL Server 2017、MS SQL Server 2019、MS SQL Server 2022		
	CPU	2.3 GHz 6 Core	2.3 GHz 8 Core	最小 2.3 GHz 推奨 4.0 GHz 16 Core
	RAM	16GB	32GB	最小 64GB 推奨 128GB
	SSD	512GB	512GB	1TB

項目	小規模組織	中規模組織	大規模組織
HDD	**Image Log** 機能を使用する場合、1,000万件のイメージログにつき 200GB が必要です		

情報

- **BioStar X** は 64 ビットのオペレーティングシステムにのみインストールできます。
- MS SQL Server のセキュア通信は TLS 1.2 をサポートします。
- MS SQL Server と **BioStar X** を異なる PC にインストールする場合、**BioStar X** がインストールされている PC に Microsoft OLE DB Driver for SQL Server をインストールする必要があります。
- 大規模組織では MS SQL Server データベースの導入を推奨します。
- データベースに MS SQL Server を使用し、**BioStar X T&A** を利用する場合は Microsoft ODBC Driver 17 for SQL Server が必要となるため、環境に適したドライバーをインストールしてください。
- Mac オペレーティングシステムで提供される Boot Camp の Windows 仮想環境はサポートしていません。
- Ethernet (TCP/IP) で接続できるデバイスの最大数は 1,000 台です。より多くのデバイスを接続するには、マルチコミュニケーションサーバーを追加してください。

SQL Server ライセンス要件

データベースに SQL Server を使用する場合、**BioStar X** を安定して運用するには、接続されるデバイス数に応じた適切な SQL Server ライセンスが必要です。各環境の推奨ライセンス構成を参考に、組織の規模とニーズに合ったライセンスを選択してください。

情報

SQL Server のライセンスの詳細については Microsoft SQL Server ライセンス を参照してください。

一般的な使用

組織	デバイス数	コア数
小規模組織	1〜50 台	4〜6
中規模組織	50 - 300 台	8〜12
大規模組織	300 - 1,000 台	16〜24

BioStar X API の使用

組織	デバイス数	コア数
小規模組織	1〜50 台	4〜6
中規模組織	50 - 300 台	8〜12

組織	デバイス数	コア数
大規模組織	300 - 1,000 台	16〜24

マルチコミュニケーションサーバー

マルチコミュニケーションサーバーは、入退室管理デバイスとの通信を専任で行うサーバーです。メインサーバーとは別に設置し、多数のデバイスを安定して管理できるよう支援します。一台のマルチコミュニケーションサーバーで最大 1,000 台のデバイスを接続でき、必要に応じて複数台のマルチコミュニケーションサーバーを追加することもできます。

項目		仕様
システム環境	オペレーティングシステム	Windows 10、Windows 11、Windows Server 2016、Windows Server 2019、Windows Server 2022、Windows Server 2025
	CPU	最小 2.3 GHz、推奨 4.0 GHz 16 Core
	RAM	最小 64GB、推奨 128GB
	SSD	1TB

情報

Ethernet (TCP/IP) で接続できるデバイスの最大数は 1,000 台です。

クライアント

クライアントは、管理者が Web ブラウザーを介して **BioStar X** にアクセスし、システムを運用する PC です。

項目		小規模組織	中規模組織	大規模組織
システム環境	CPU	2.5 GHz	2.5 GHz	最小 2.5 GHz
	RAM	16GB	32GB	最小 32GB
	GPU	VMS を使用する場合、最低でも NVIDIA GeForce RTX 4060		
	ウェブブラウザー	Google Chrome バージョン 100 以上		

情報

- **BioStar X** は Google Chrome に最適化されています。
- **BioStar X** のウェブインターフェースはモバイルブラウザーをサポートしていません。

はじめに

BioStar X を初めて使用するユーザー向けの必須設定ガイドです。インストール方法の選択からライセンス登録まで、BioStar X を成功裏に構築し運用するために必要な主要手順を段階的に案内します。

ネットワーク優先順位を確認する

BioStar X をインストールする前に、サーバーのネットワーク優先順位を確認して設定する方法を案内します。

必要なタイミング？

次のような場合にネットワーク優先順位の確認と設定が必要です。

- サーバーに 2 つ以上のネットワークアダプター (LAN カード) が搭載されている場合
- BioStar X サービスで特定のネットワークアダプターを使用する必要がある場合
- BioStar X のインストール後にネットワーク接続問題が発生しないように事前に防止したい場合

> **情報**
> 上記に該当しない場合、ネットワーク優先順位を変更する必要はありません。この手順をスキップし、BioStar X をインストールする。 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。

> **警告**
> BioStar X のインストール時、メトリック値が低い (優先順位が高い) ネットワークアダプターが自動的に選択されます。インストール後にこの設定を変更することは困難なため、**インストール前に必ずネットワーク優先順位を確認して調整する必要があります。**

ネットワーク優先順位を確認する

コマンドプロンプトで確認

1. **スタート** メニューで `cmd` を検索し、**コマンドプロンプト** を起動する。
2. 次のコマンドを入力する。

```
route print
```

3. 出力結果の **IPv4 Route Table** セクションで **Network Destination** が `0.0.0.0` の項目を探す。
4. **Metric** 列の値を確認する。**値が低いほど優先順位が高くなります。**

出力例：

```
IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0    192.168.120.1  192.168.120.141     306
          0.0.0.0          0.0.0.0     192.168.40.1  192.168.40.123      20
        127.0.0.0        255.0.0.0         On-link         127.0.0.1    331
        127.0.0.1  255.255.255.255         On-link         127.0.0.1    331
  127.255.255.255  255.255.255.255         On-link         127.0.0.1    331
     192.168.40.0    255.255.252.0         On-link     192.168.40.123    266
   192.168.40.123  255.255.255.255         On-link     192.168.40.123    266
   192.168.43.255  255.255.255.255         On-link     192.168.40.123    266
     192.168.56.0    255.255.255.0         On-link      192.168.56.1    281
```

上記の例では、`192.168.40.123` インターフェースがメトリック値 **20** でより高い優先順位を持ちます。

ネットワークアダプター情報を確認

各インターフェースがどのネットワークアダプターに対応しているかを確認する。

1. **コマンドプロンプト** で次のコマンドを入力する。

   ```
   ipconfig /all
   ```

2. 各ネットワークアダプターの **IPv4 アドレス** と先ほど確認した **Gateway** アドレスを照合し、どのアダプターかを特定する。

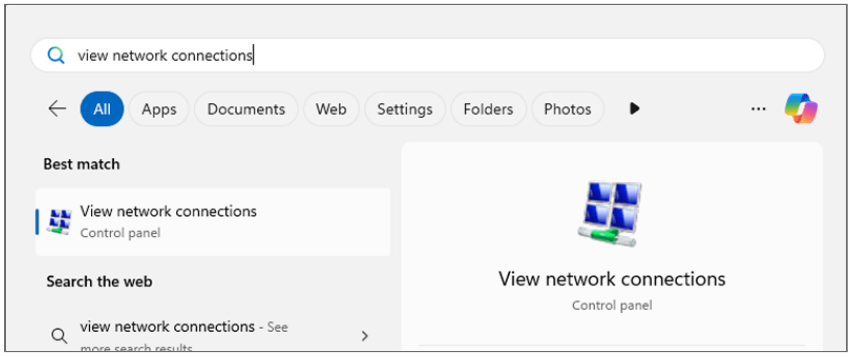
ネットワーク優先順位を変更する

目的のネットワークアダプターの優先順位を上げるには次の手順を実行する。

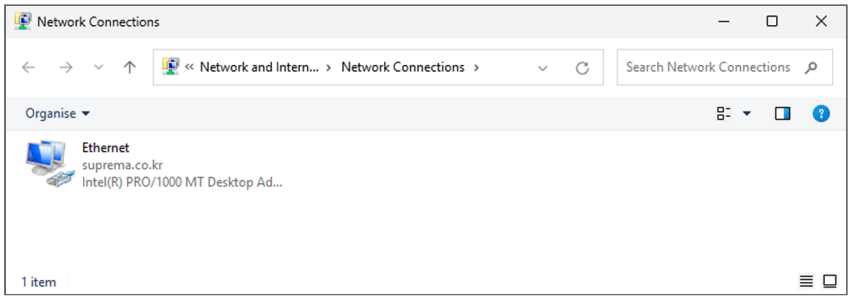
> **情報**
> 以下の手順は Windows 11 を基準としています。使用している Windows バージョンによってメニューの位置が異なる場合があります。

1 ネットワーク設定を開く

1. **スタート** メニューで **ネットワーク接続の表示** と入力する。

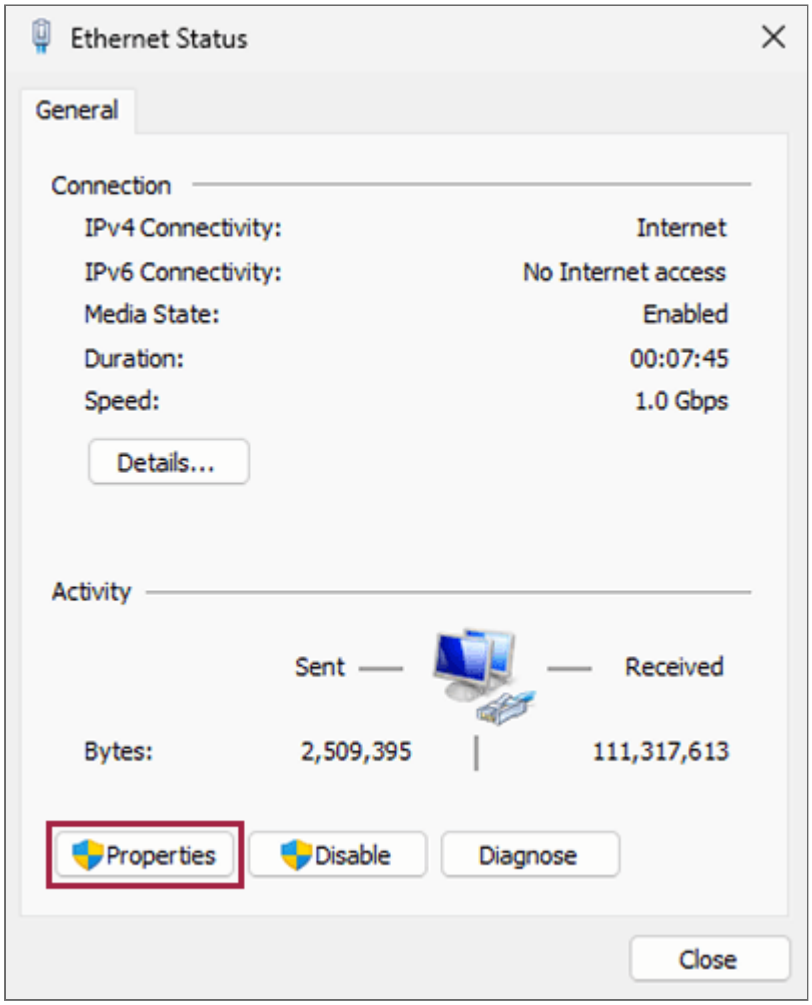


2. 検索結果で **ネットワーク接続の表示** をクリックする。
3. 一覧からインターネットに接続されているアダプターをダブルクリックする。

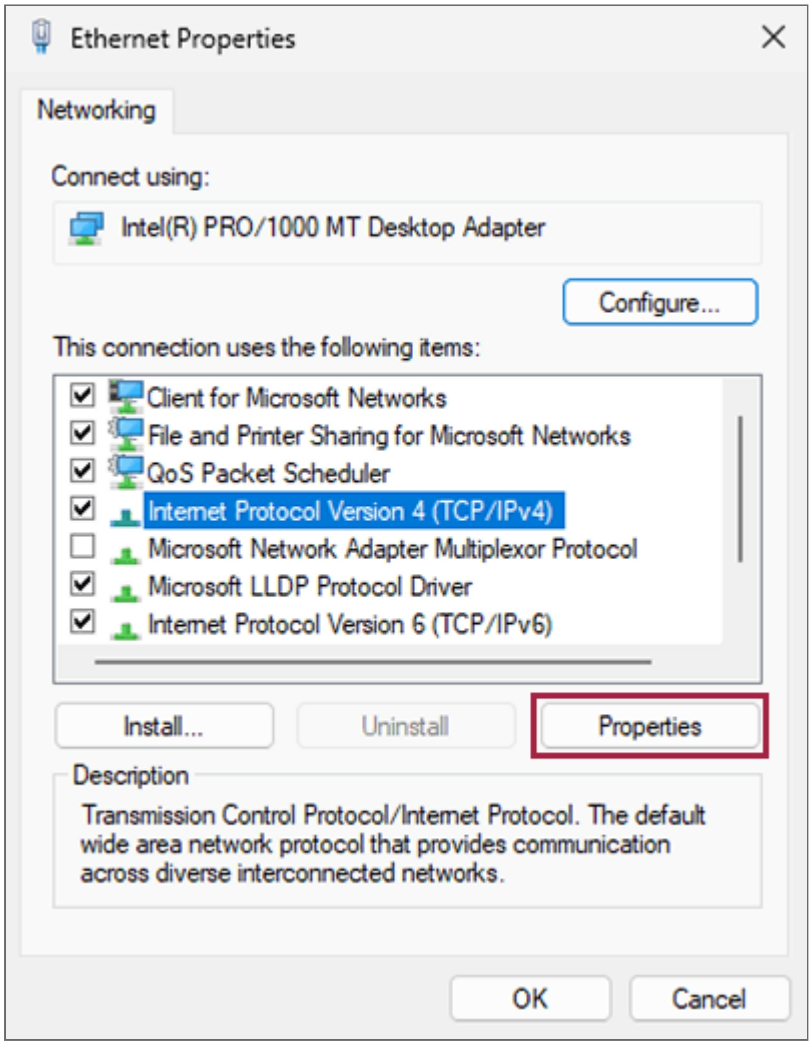


2 アダプターオプションを開く

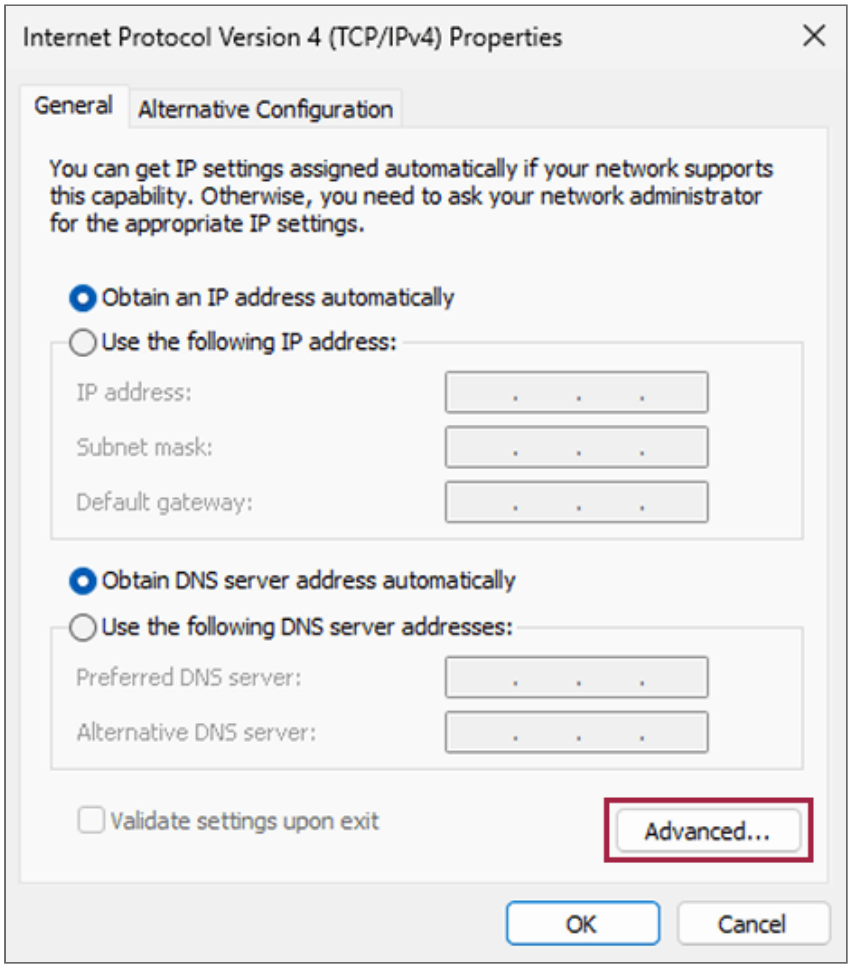
1. **イーサネットの状態** ウィンドウが表示されたら **プロパティ** をクリックする。



2. イーサネットのプロパティが表示されたら、一覧から **インターネット プロトコル バージョン 4 (TCP/IPv4)** を選択する。

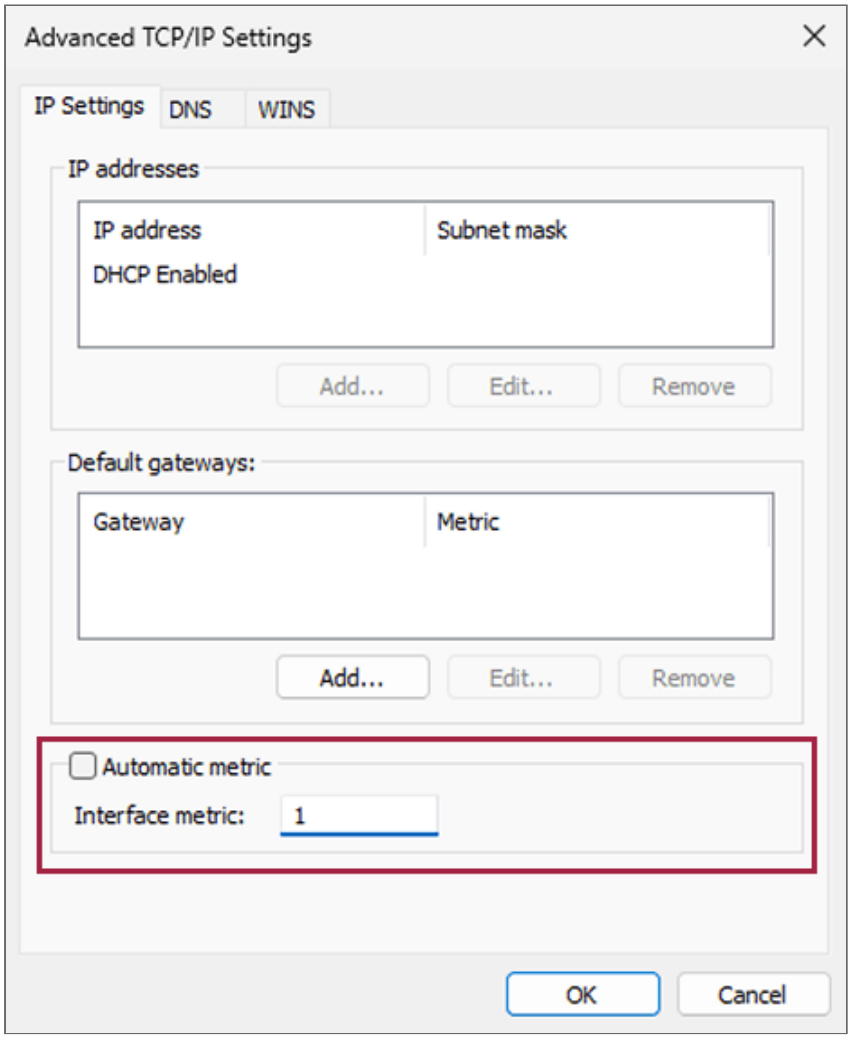


3. **プロパティ** をクリックする。
4. **インターネット プロトコル バージョン 4 (TCP/IPv4) のプロパティ** が表示されたら **詳細設定** をクリックする。



❸ メトリックを設定

1. **自動メトリック** のチェックを **外す**。



2. **インターフェイスメトリック** フィールドに希望する値を入力する。
   - 最高の優先順位にする場合は `1` を入力する。
   - 他のアダプターより高い優先順位にしたい場合、そのアダプターのメトリック値より小さい数値を入力する。
3. 設定を保存してすべてのウィンドウを閉じるには **OK** をクリックする。

> **情報**
> **インターフェイスメトリック** に入力できる値は `1` から `9999` まで。値が低いほど優先順位が高くなります。

4 設定を確認

1. **コマンドプロンプト** を再度開き、`route print` コマンドを実行する。
2. メトリック値が変更されたか確認する。

トラブルシューティング

- 設定が反映されない場合は、コンピューターを再起動するか、ネットワークアダプターを無効にしてから再度有効にする。
- ネットワーク接続が切れた場合は元の設定に戻し、**自動メトリック** オプションを再度有効にする。ネットワーク管理者に問

い合わせて正しい設定値を確認する。

> **情報**
> BioStar X のインストール後にネットワーク設定を変更する必要がある場合は、プログラムを完全に削除してから再インストールすることを推奨します。

次のステップ

初めてインストールするユーザー向けの簡易インストール手順を案内します。
既にインストール済みのデータベースと連携するためのカスタムインストール手順を案内します。

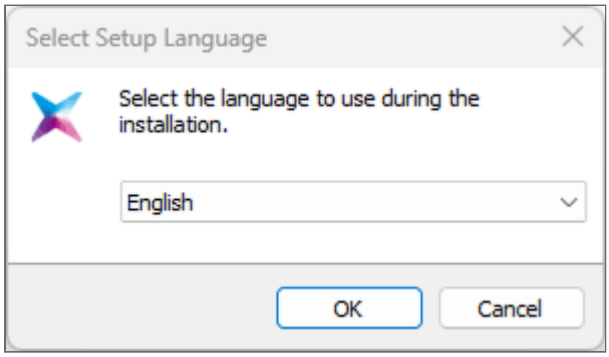
簡単インストール

簡易インストール 方式で BioStar X をインストールする手順を段階別に案内します。 **簡易インストール** は内蔵のMariaDBサーバーを自動でインストールし、データベースを作成して、別途データベース設定を行わずに迅速にインストールを完了できます。

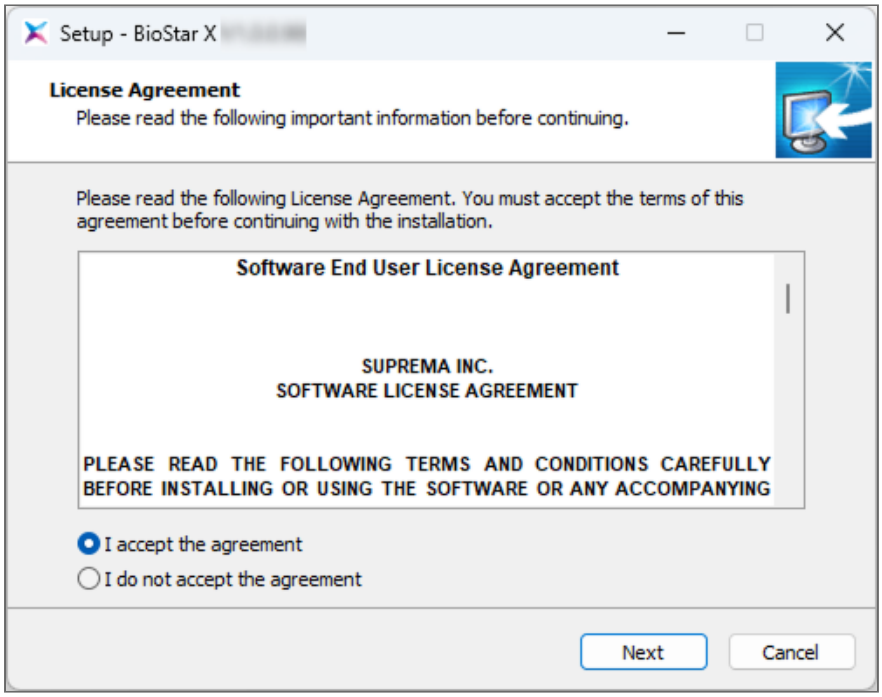
> **情報**
> 既にインストール済みのデータベースと連携させたい場合は、**カスタムインストール**での手順について、カスタムインストールを実行するを参照してください。

インストール案内

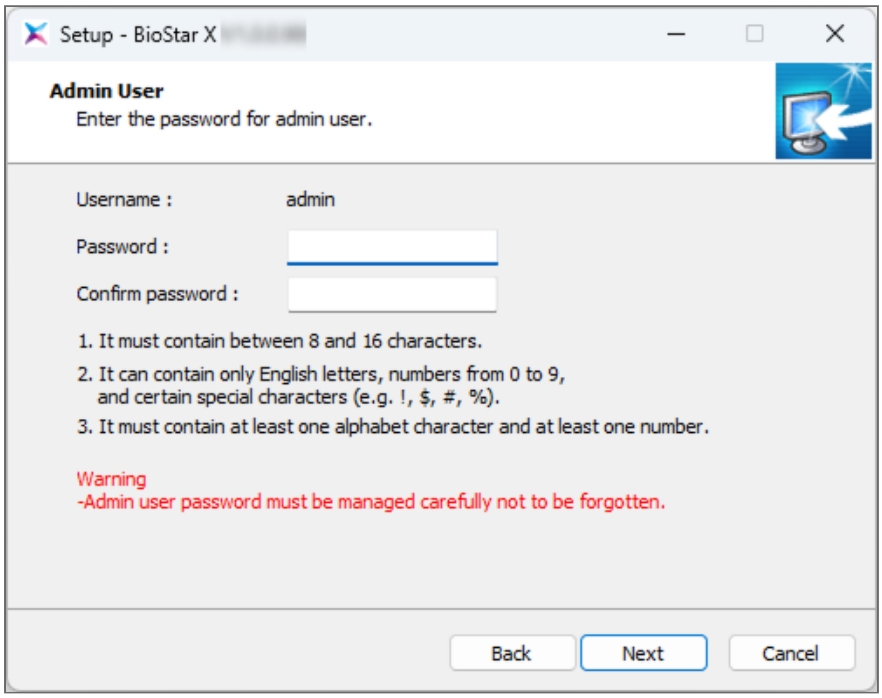
1. Suprema ダウンロードセンター にアクセスしてログイン後、インストールパッケージ (*BioStar X Setup.X.Y.Z.BB.exe*) をダウンロードしてください。
2. ダウンロードしたインストールファイルを実行してください。
3. 使用する言語を選択し、**OK** ボタンをクリックしてください。



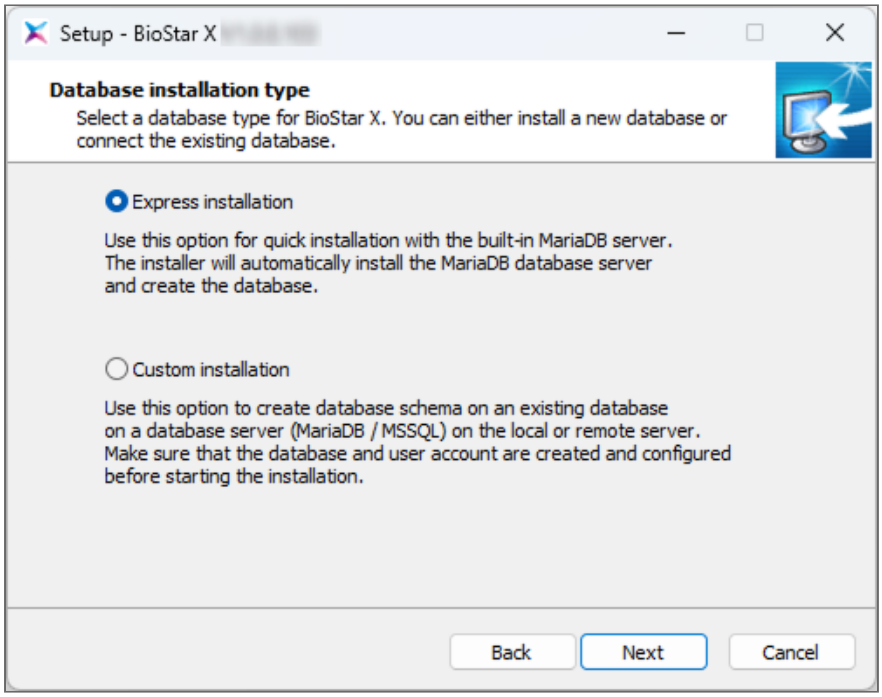
4. インストールを続行するには、**同意する** を選択し、**次へ** ボタンをクリックしてください。



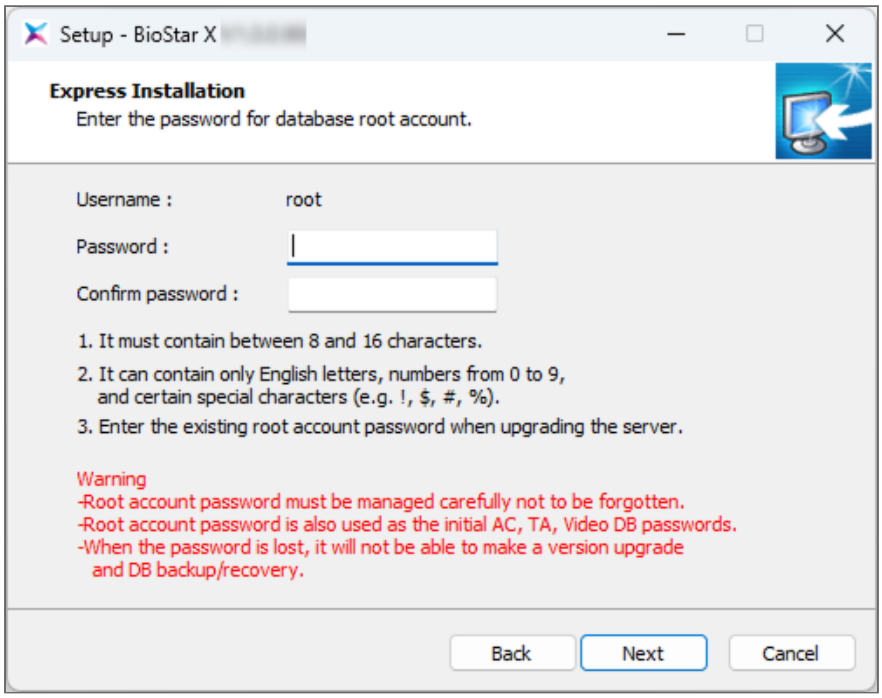
5. 管理者アカウントのパスワードを入力し、**次へ** ボタンをクリックしてください。



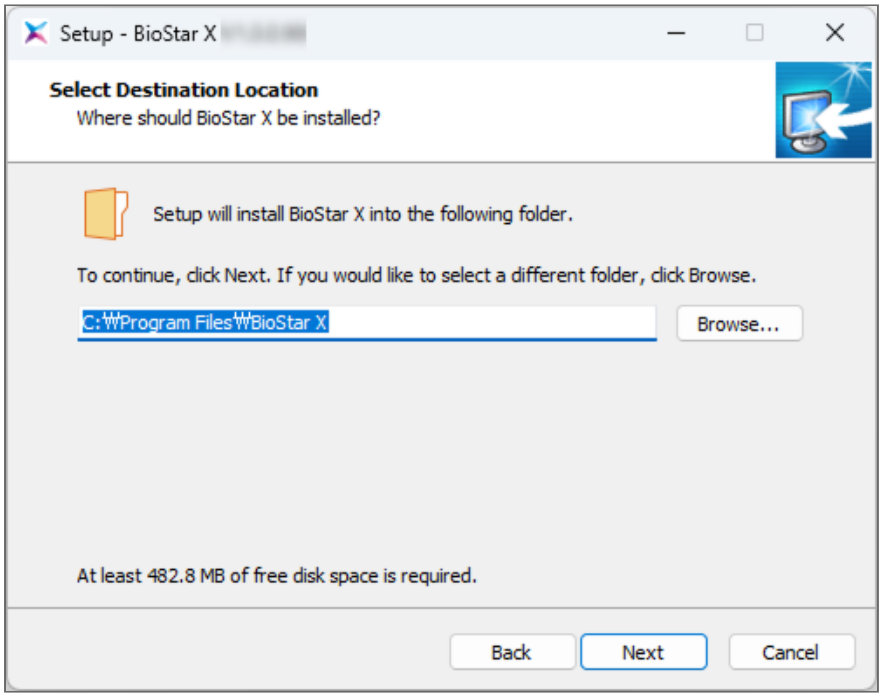
6. **簡易インストール** を選択し、**次へ** ボタンをクリックしてください。



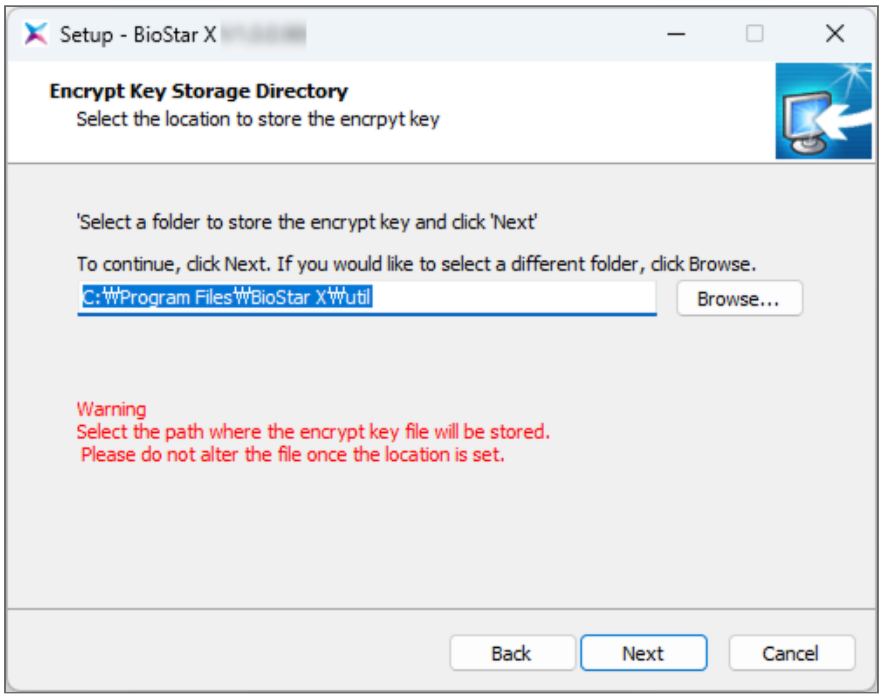
7. データベースの root アカウントのパスワードを入力し、**次へ** ボタンをクリックしてください。



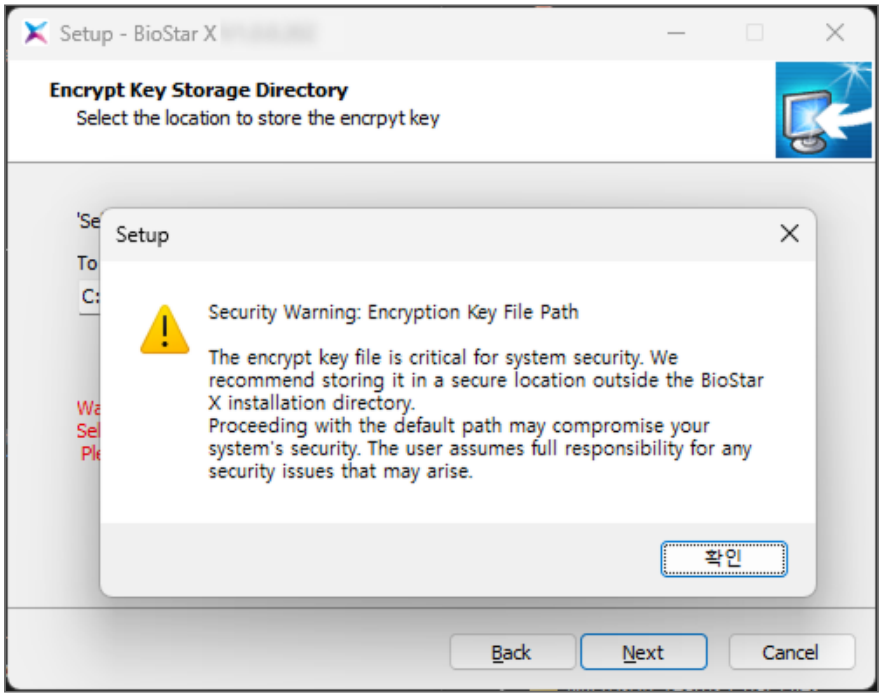
8. **BioStar X** をインストールするパスを設定し、**次へ** ボタンをクリックしてください。



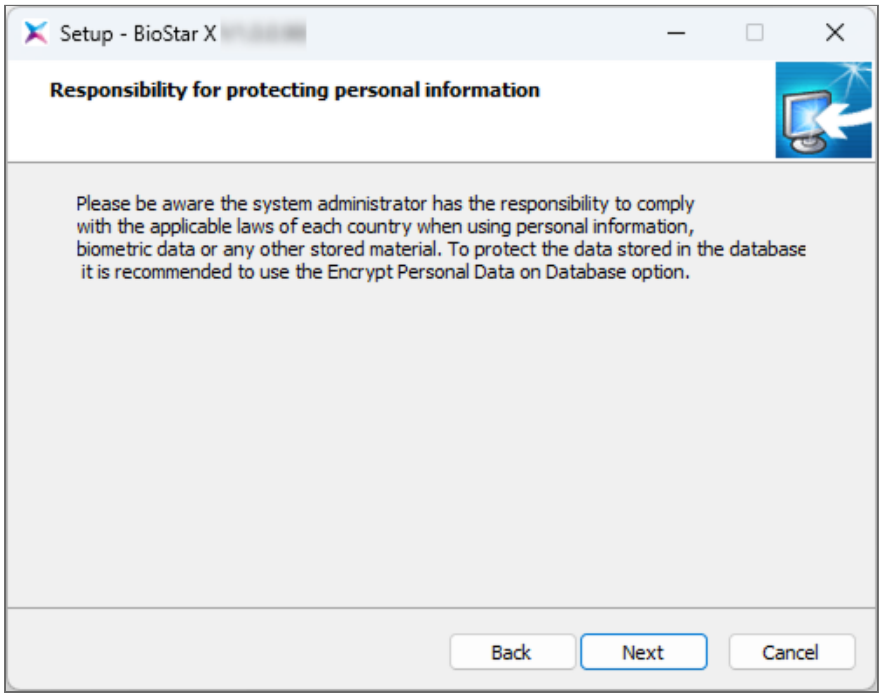
9. 暗号化キーを保存するパスを設定し、**次へ** ボタンをクリックしてください。



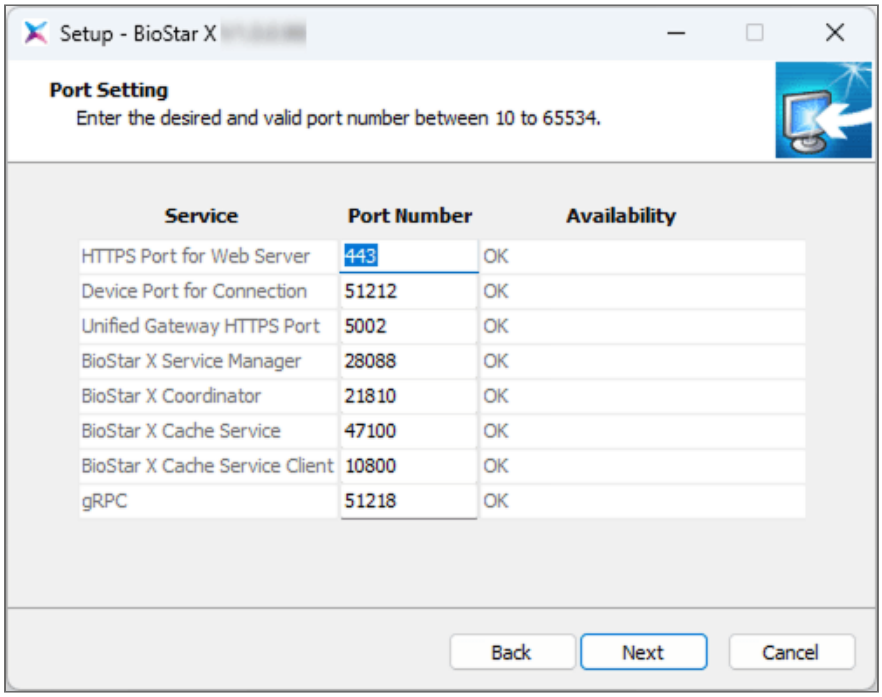
10. セキュリティ警告メッセージの内容を確認し、**OK** をクリックしてください。



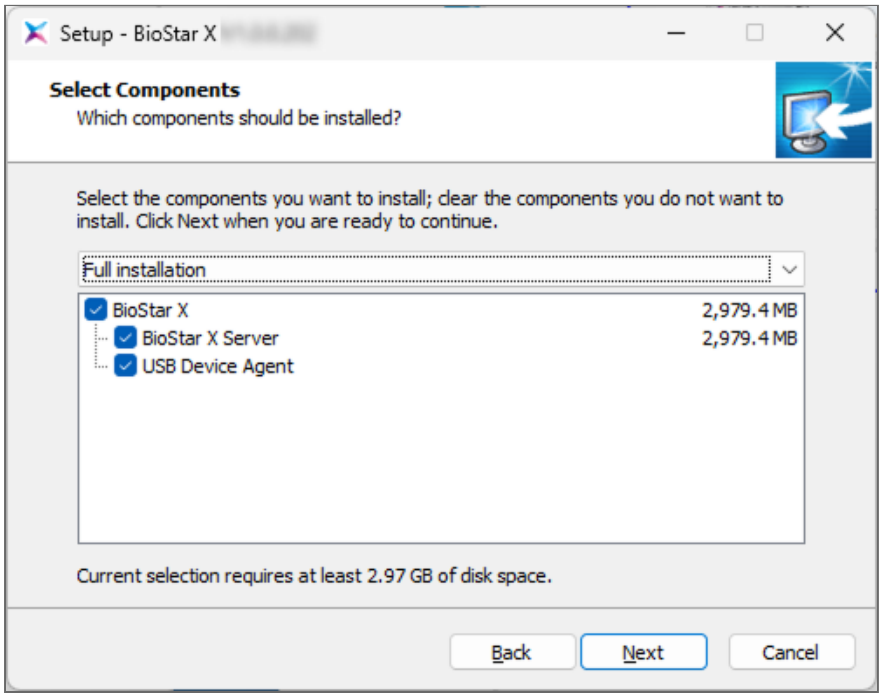
11. データベースに保存される個人情報の管理権限および責任に関する案内を読み、インストールを続行するには **次へ** ボタンをクリックしてください。



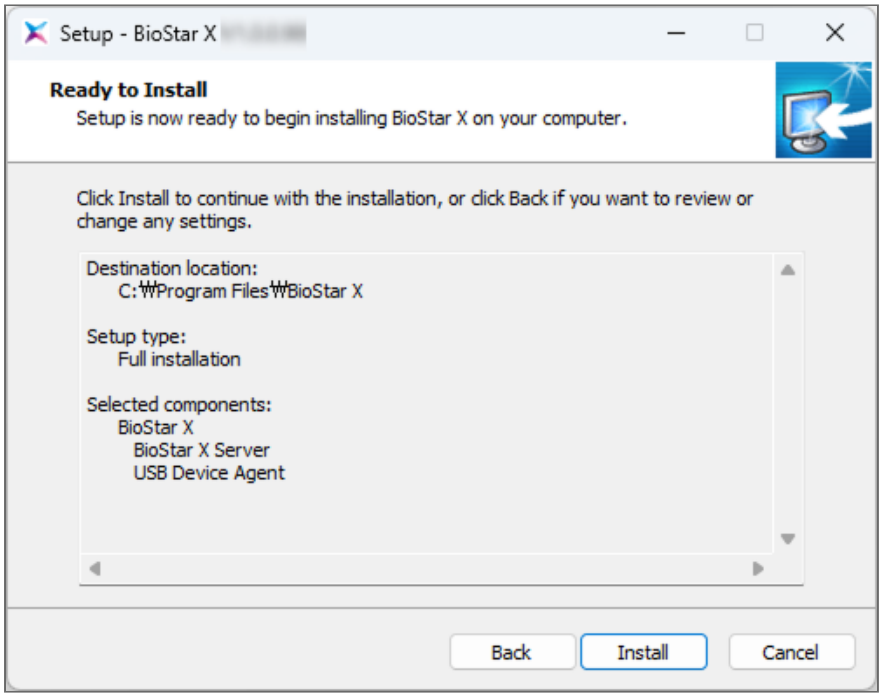
12. **BioStar X** の通信ポートを設定し、**次へ** ボタンをクリックしてください。



13. **BioStar X** のコンポーネントを選択し、**次へ** ボタンをクリックしてください。 **USB Device Agent** を選択すると、BioMini、BioMini Plus 2、BioMini Slim 2、DUALi DE-620 を使用するための USB Agent とドライバーが併せてインストールされます。



14. すべてのインストール準備が完了したら、**インストール** ボタンをクリックしてください。



15. 追加プログラムのインストール有無を選択し、終了 ボタンをクリックしてください。



16. インストール画面の指示に従って **USB Device Agent** のインストールを完了してください。

情報

- ダウンロードしたファイル名の `X.Y.Z` はバージョン情報、`BB` はビルド番号です。
- 管理者アカウントのパスワードは、**BioStar X** をインストールした後の初回ログイン時に使用します。
- データベースの root アカウントのパスワードは、AC、TA、Video DB の初期パスワードとして使用します。
- 暗号化キーの保存パスを変更できます。 パスを変更した後に暗号化キー ファイルを編集または別のパスに移動すると、システムエラーが発生する可能性があります。
- **BioStar X** をアンインストールすると、暗号化キー ファイルも同時に削除されます。
- 提供される USB Device Agent 証明書はローカルネットワークにのみ適用できます。
- 他のプログラムが 443 ポートを使用している場合、BioStar X Setting プログラムが自動的に起動し、ポート番号を変更できます。 ポート番号の変更については、ポートを変更するを参照してください。
- データベース設定の変更の詳細については、データベースを変更するを参照してください。

警告

- 管理者またはデータベースの root アカウントのパスワードを紛失しないよう注意してください。
- パスワードを紛失すると、バージョンアップグレードおよび DB のバックアップ/復元ができなくなる可能性があります。

次のステップ

Web ブラウザを起動して **BioStar X** にログインする方法を確認してください。
BioStar X のサーバー状態を確認し、停止または再起動する方法を確認してください。

カスタムインストールを実行する

本書では、**カスタムインストール** を使用して **BioStar X** をインストールする手順を段階的に説明します。 **カスタムインストール** は、ローカルサーバーまたはリモートサーバーに既にインストールされているデータベース（MariaDB、MS SQL Server）と連携してデータベーススキーマを作成します。インストールを開始する前に、連携するデータベースとユーザーアカウントをあらかじめ準備してください。

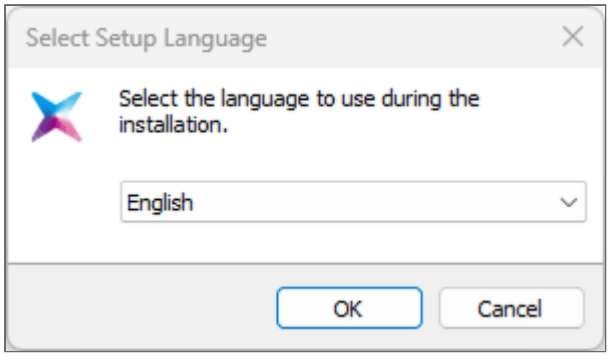
開始前

- **BioStar X** と連携して使用できるデータベースは次のとおりです。
  - MariaDB 11.4.4
  - MS SQL Server 2012 SP3
  - MS SQL Server 2014 SP2
  - MS SQL Server 2016 SP1

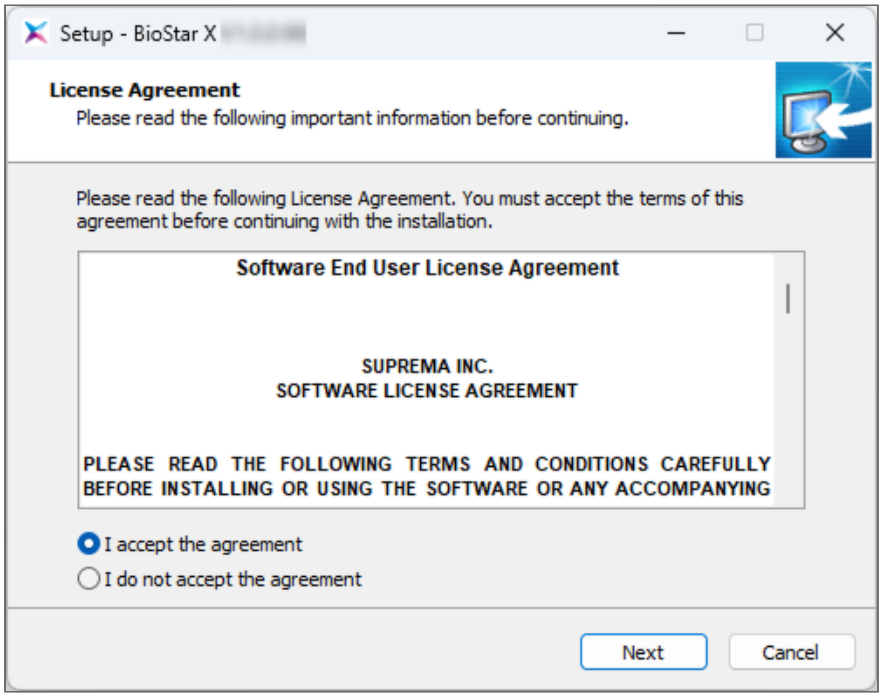
  - MS SQL Server 2017
  - MS SQL Server 2019
  - MS SQL Server 2022
- MS SQL Server のセキュア通信は TLS 1.2 をサポートします。
- MS SQL Server をデータベースとして設定し、テーブルの作成に失敗した場合は、*C:\Program Files\BioStar X\dbscript\mssql* にあるスクリプトを実行してテーブルを作成できます。
- インストールオプションで **カスタムインストール** を選択する場合、**AC DB name**、**TA DB name**、**VE DB name** を同じ名前に設定することはできません。
- Windows 認証を使用するには、Microsoft ODBC Driver 17 for SQL Server が必要です。まず、そのドライバーをインストールしてください。

インストール案内

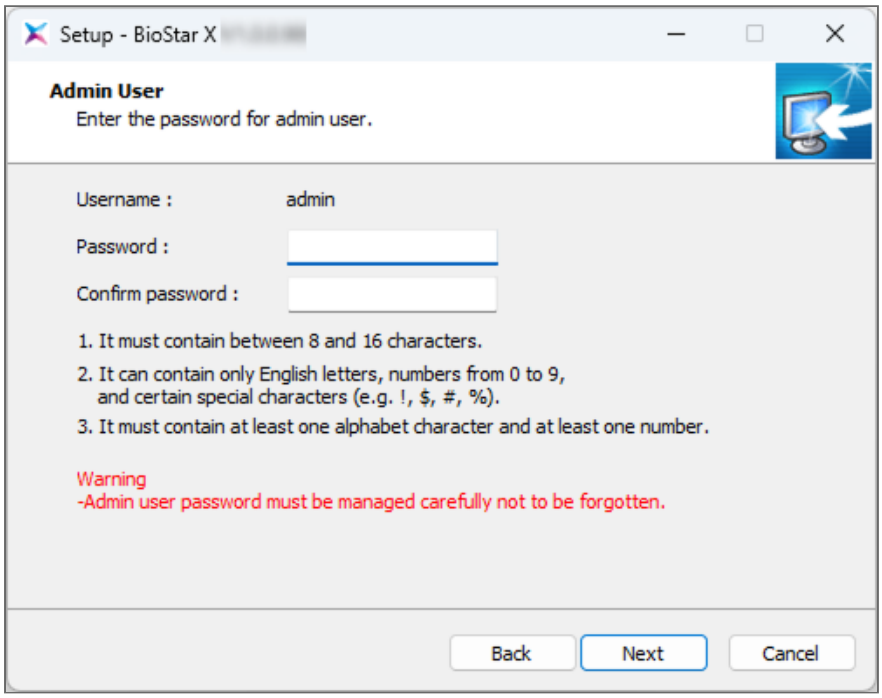
1. Suprema ダウンロードセンター にアクセスしてログイン後、インストールパッケージ (*BioStar X Setup.X.Y.Z.BB.exe*) をダウンロードしてください。
2. ダウンロードしたインストールファイルを実行してください。
3. 使用する言語を選択し、**OK** ボタンをクリックしてください。



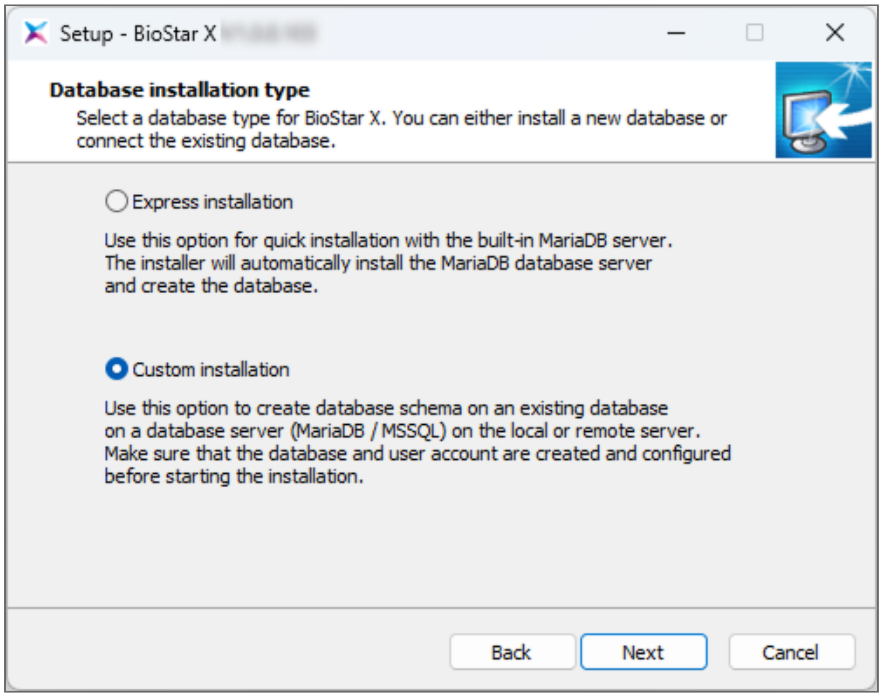
4. インストールを続行するには、**同意する** を選択し、**次へ** ボタンをクリックしてください。



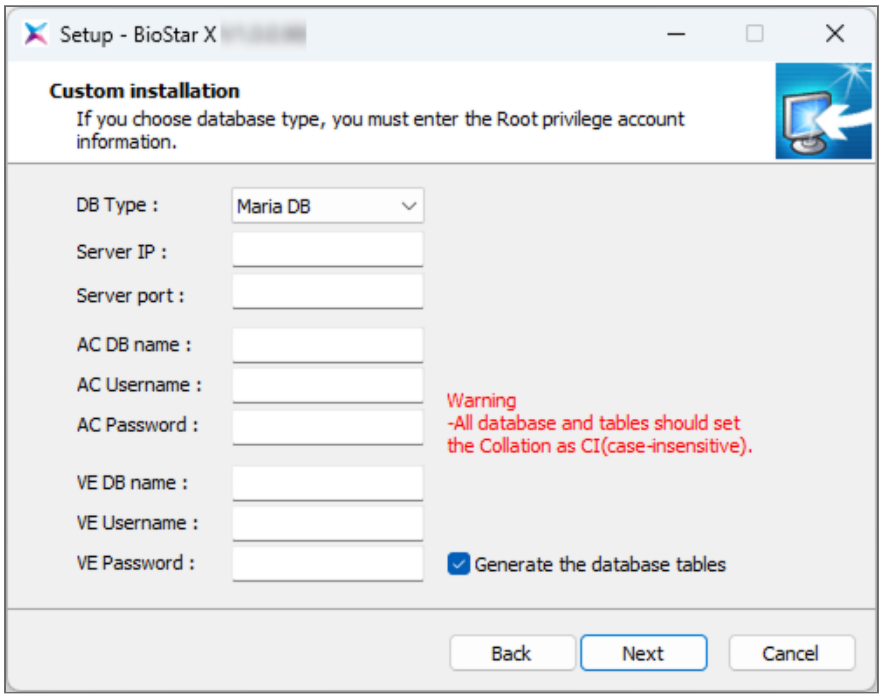
5. 管理者アカウントのパスワードを入力し、**次へ** ボタンをクリックしてください。



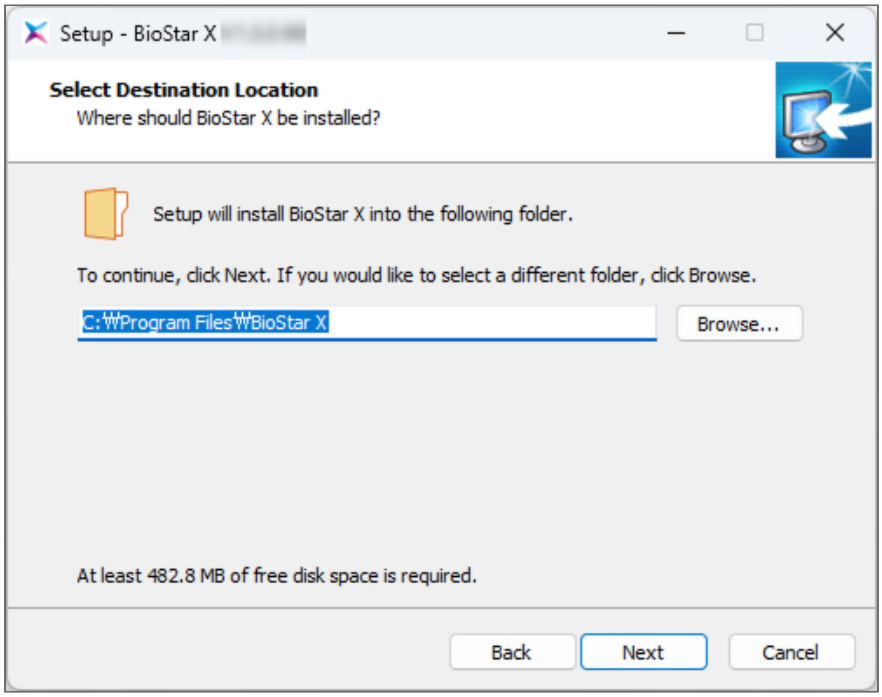
6. **カスタムインストール** を選択し、**次へ** ボタンをクリックしてください。



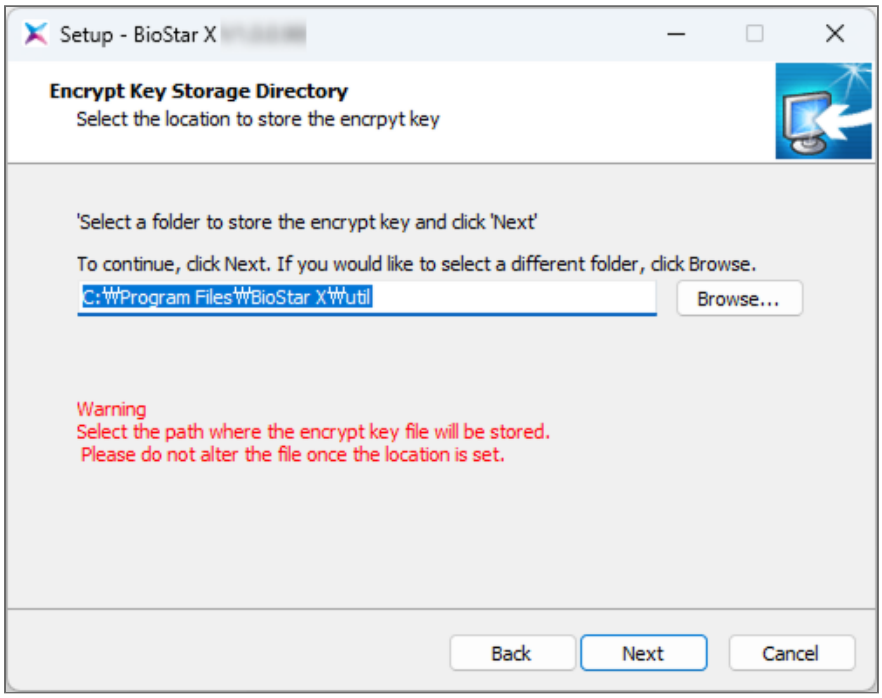
7. 既に構成済みのデータベースの詳細を入力し、**次へ** ボタンをクリックしてください。



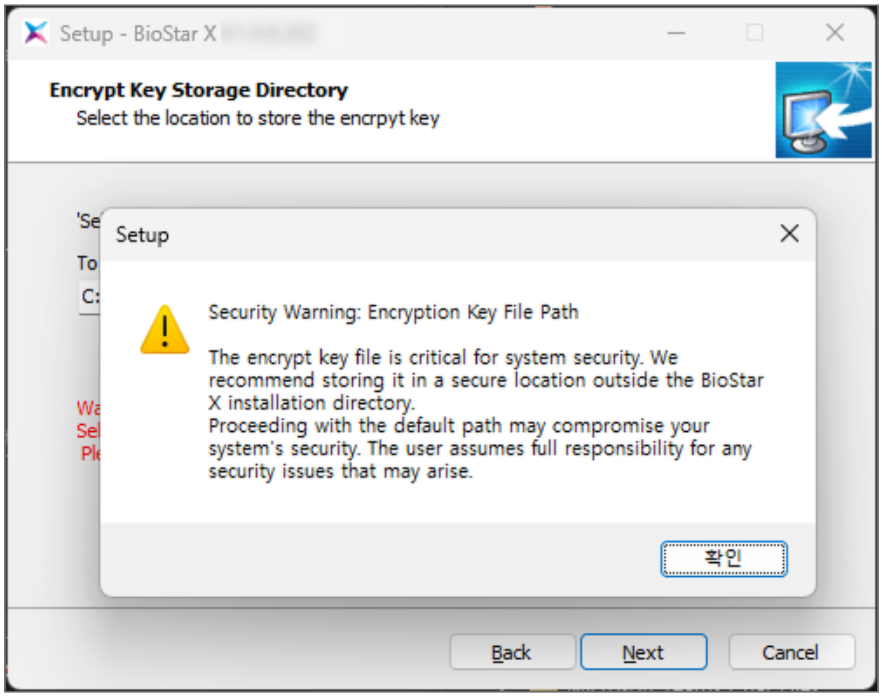
8. **BioStar X** をインストールするパスを設定し、**次へ** ボタンをクリックしてください。



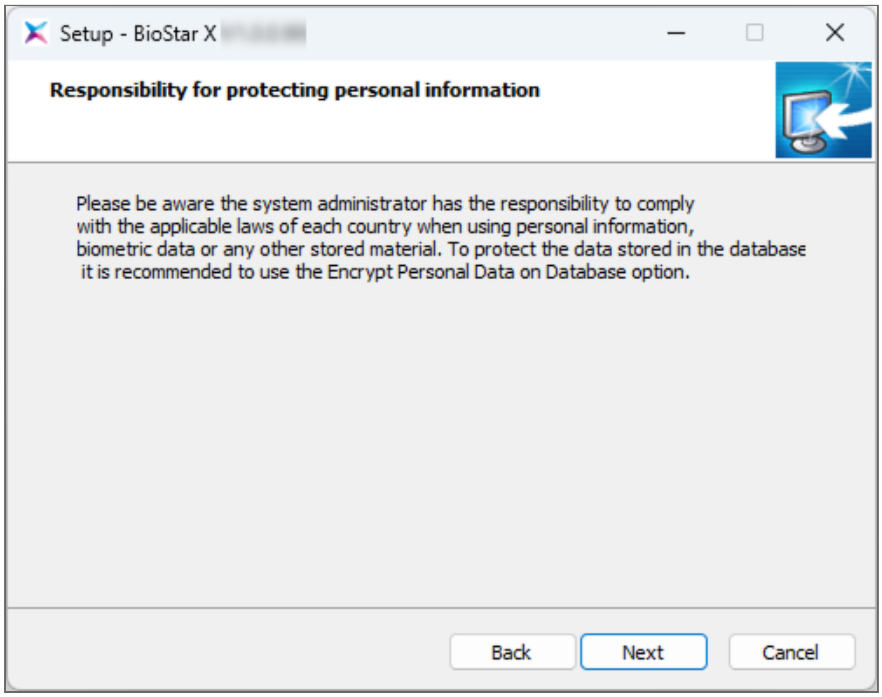
9. 暗号化キーを保存するパスを設定し、**次へ** ボタンをクリックしてください。



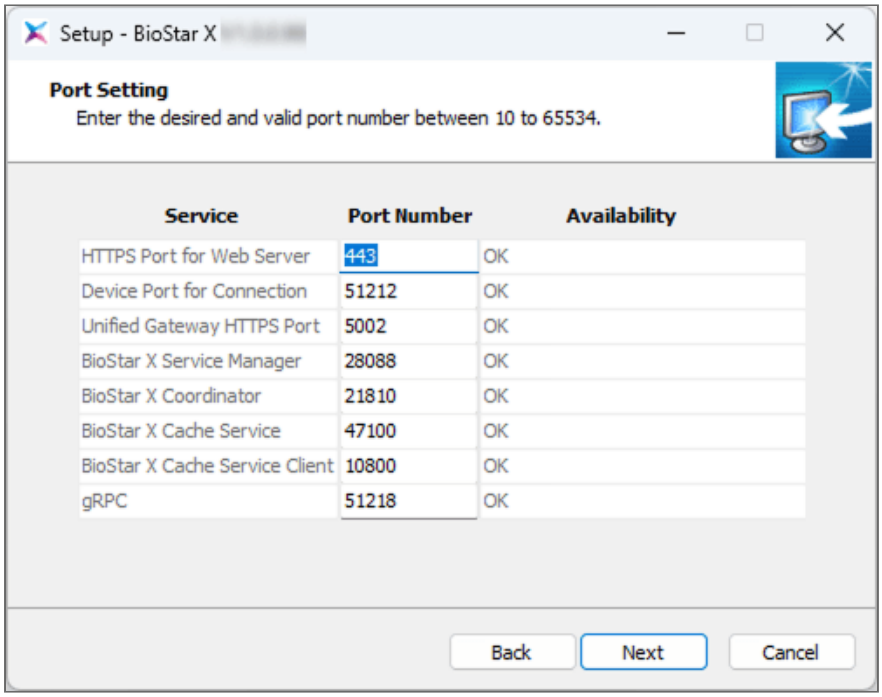
10. セキュリティ警告メッセージの内容を確認し、**OK** をクリックしてください。



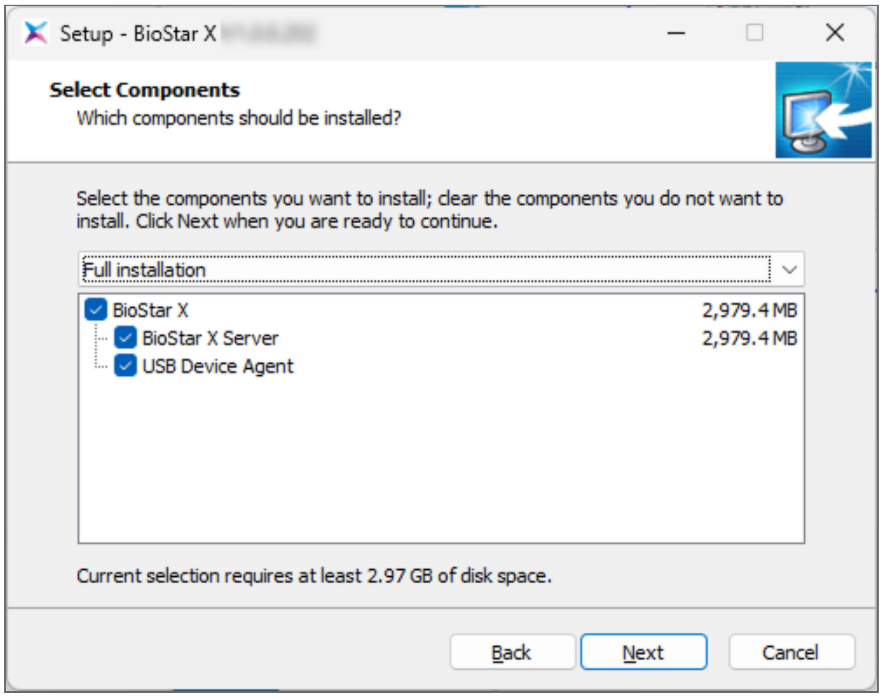
11. データベースに保存される個人情報の管理権限および責任に関する案内を読み、インストールを続行するには **次へ** ボタンをクリックしてください。



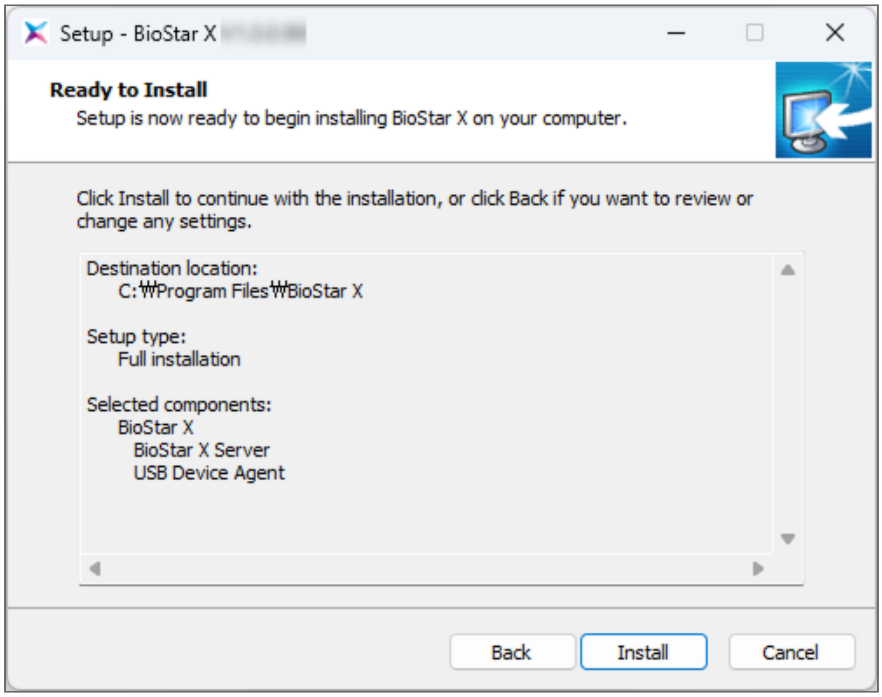
12. **BioStar X** の通信ポートを設定し、**次へ** ボタンをクリックしてください。



13. **BioStar X** のコンポーネントを選択し、**次へ** ボタンをクリックしてください。 **USB Device Agent** を選択すると、BioMini、BioMini Plus 2、BioMini Slim 2、DUALi DE-620 を使用するための USB Agent とドライバーが併せてインストールされます。



14. すべてのインストール準備が完了したら、**インストール** ボタンをクリックしてください。



15. 追加プログラムのインストール有無を選択し、終了 ボタンをクリックしてください。



16. インストール画面の指示に従って **USB Device Agent** のインストールを完了してください。

情報

- ダウンロードしたファイル名の `X.Y.Z` はバージョン情報、`BB` はビルド番号です。
- 管理者アカウントのパスワードは、**BioStar X** をインストールした後の初回ログイン時に使用します。
- データベースの root アカウントのパスワードは、AC、TA、Video DB の初期パスワードとして使用します。
- 暗号化キーの保存パスを変更できます。 パスを変更した後に暗号化キー ファイルを編集または別のパスに移動すると、システムエラーが発生する可能性があります。
- **BioStar X** をアンインストールすると、暗号化キー ファイルも同時に削除されます。
- 提供される USB Device Agent 証明書はローカルネットワークにのみ適用できます。
- 他のプログラムが 443 ポートを使用している場合、BioStar X Setting プログラムが自動的に起動し、ポート番号を変更できます。 ポート番号の変更については、ポートを変更するを参照してください。
- データベース設定の変更の詳細については、データベースを変更するを参照してください。

警告

- 管理者またはデータベースの root アカウントのパスワードを紛失しないよう注意してください。
- パスワードを紛失すると、バージョンアップグレードおよび DB のバックアップ/復元ができなくなる可能性があります。

次のステップ

Web ブラウザを起動して **BioStar X** にログインする方法を確認してください。
BioStar X のサーバー状態を確認し、停止または再起動する方法を確認してください。

アップグレードする

本ドキュメントでは、BioStar 2 を **BioStar X** にアップグレードする手順を段階的に案内します。アップグレードを開始する前に、システム要件と注意事項を確認してください。

開始前

BioStar 2 から **BioStar X** へアップグレードする前に、次の事項を確認してください。

情報

Important

最小要件

- アップグレードを進める前に、システム最小要件を参照してサーバーの仕様が要件を満たしているか確認してください。
- BioStar 2 v2.9.11 以上の環境であれば、**BioStar X** へアップグレードできます。
  - BioStar 2 v2.6.4 以下のバージョンを使用している場合、v2.9.11 まで段階的にアップグレードした後にアップグレードできます。 BioStar 2 を段階的にアップグレードする方法については、**BioStar 2 管理者ガイド**ご参照ください。
  - BioStar 2 v2.9.10 以下のバージョンではアップグレードできません。
- BioStar 2 に以下のデバイスが接続されている場合、**BioStar X** へのアップグレードはサポートされません。
  - XPass S2、XPass、BioEntry W、BioEntry Plus、BioLite Net

ライセンス

- **BioStar X** へアップグレードする前に、代理店に問い合わせて少なくとも 1 つの BioStar X ライセンスを準備してください。
- **BioStar X** へアップグレードすると、BioStar 2 とは異なるライセンスポリシーが適用されます。
- BioStar 2 AC ライセンスで Advanced 以上のグレードが有効な状態でアップグレードすると、以下のサービス機能および設定が削除されます。
  - グラフィックマップ (Graphic Map)
  - クラウド (Cloud)
- **BioStar X** でも BioStar 2 T&A サービスを使用するには、**BioStar X T&A** ライセンスを別途購入する必要があります。

警告

証明書の確認

BioStar 2 から BioStar X にアップグレードすると、`nginx\conf` パスと `nginx\cert` パスにある `biostar_cert.crt` ファイルが異なる場合があります。この状態でアップグレードすると、次の問題が発生します。

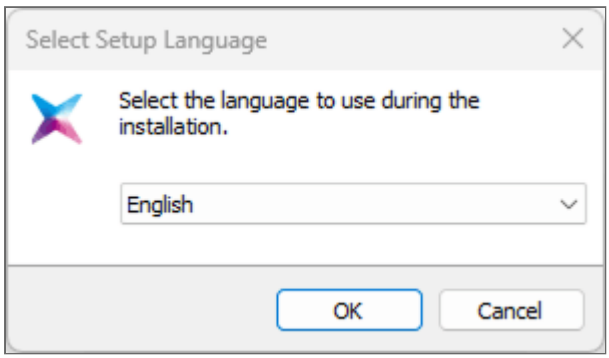
- 監査ログの一部が記録されません。
- ユーザーグループの作成、Wiegand の追加、ツリーの更新に失敗します。

BioStar X にアップグレードする前に証明書ファイルを一致させるには、次の手順に従ってください。

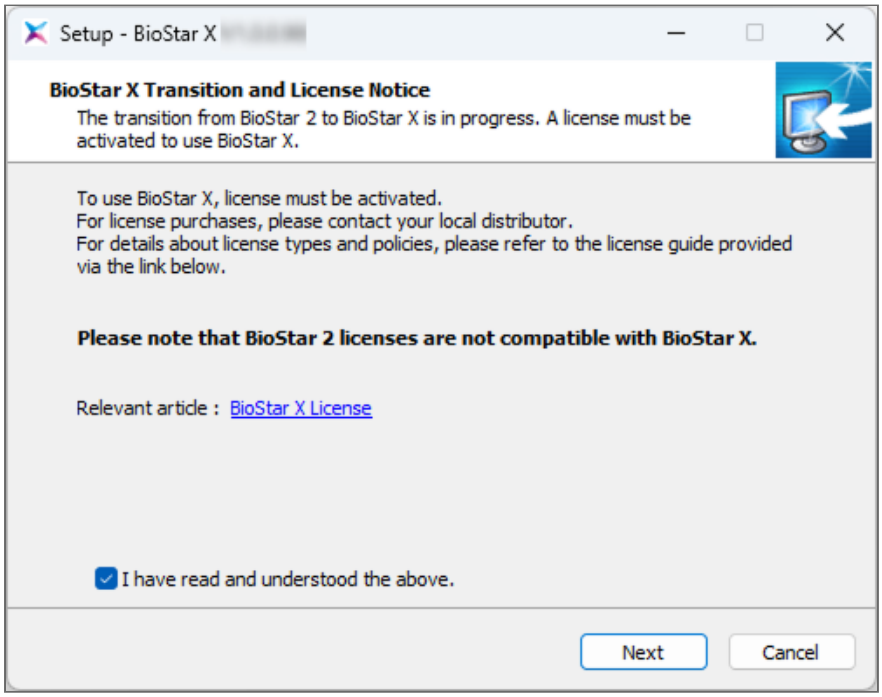
1. BioStar 2 サービスを停止してください。
2. `nginx\conf` パスの `biostar_cert.crt`、`biostar_cert.key` ファイルを `nginx\cert` パスに上書きしてください。
3. BioStar 2 サービスを再起動してください。

アップグレードインストール案内

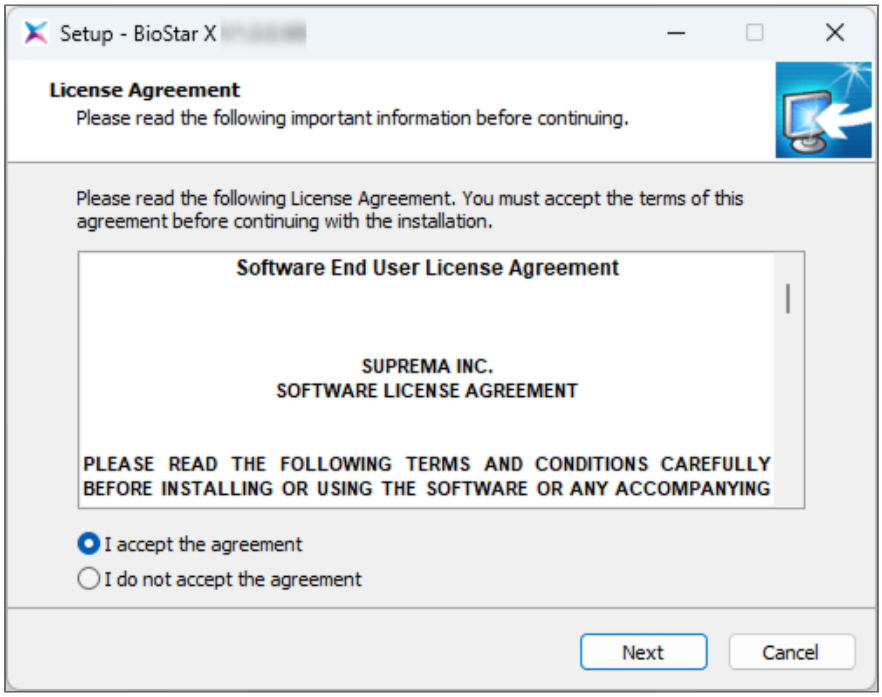
1. Suprema ダウンロードセンター にアクセスしてログイン後、インストールパッケージ (*BioStar X Setup.X.Y.Z.BB.exe*) をダウンロードしてください。
2. ダウンロードしたインストールファイルを実行してください。
3. 使用する言語を選択し、**OK** ボタンをクリックしてください。



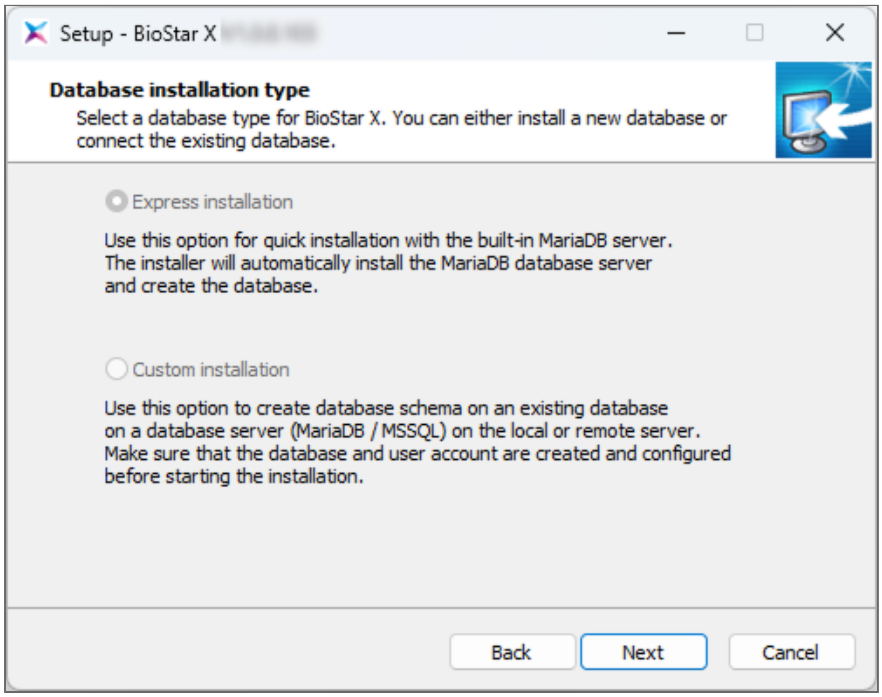
4. BioStar 2 から **BioStar X** に移行するというライセンスポリシーに同意してください。チェックボックスをクリックし、**次へ** ボタンを選択してください。



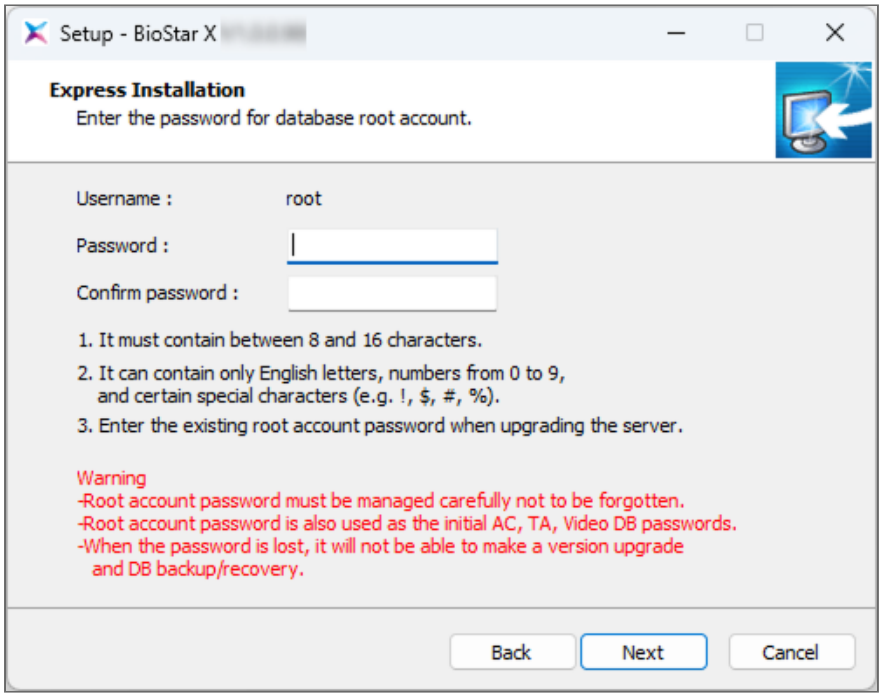
5. インストールを続行するには、**同意する** を選択し、**次へ** ボタンをクリックしてください。



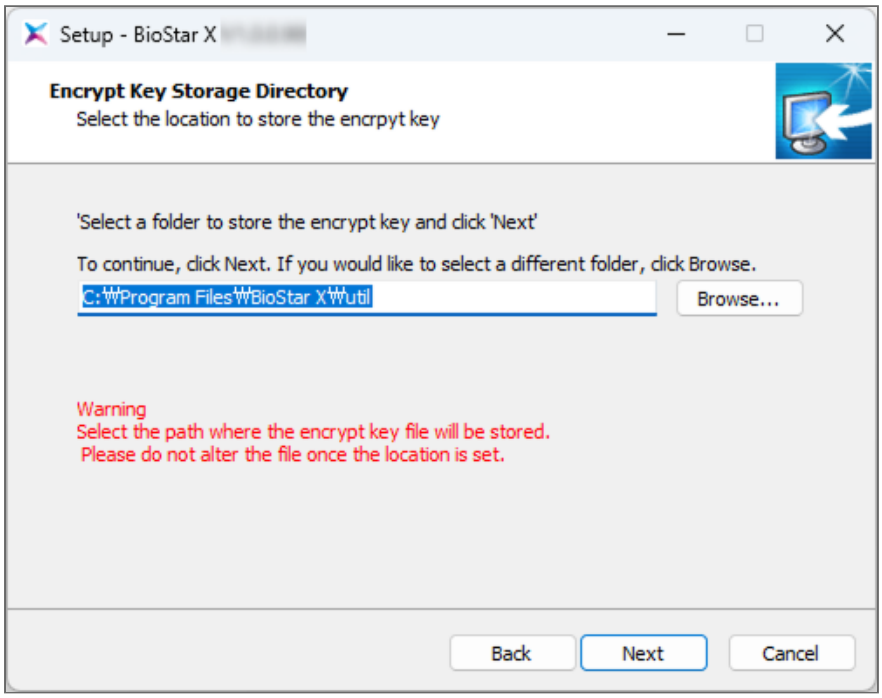
6. BioStar 2 からアップグレードする場合、既存のデータベースを接続してインストールを進めます。 **次へ** ボタンをクリックしてください。



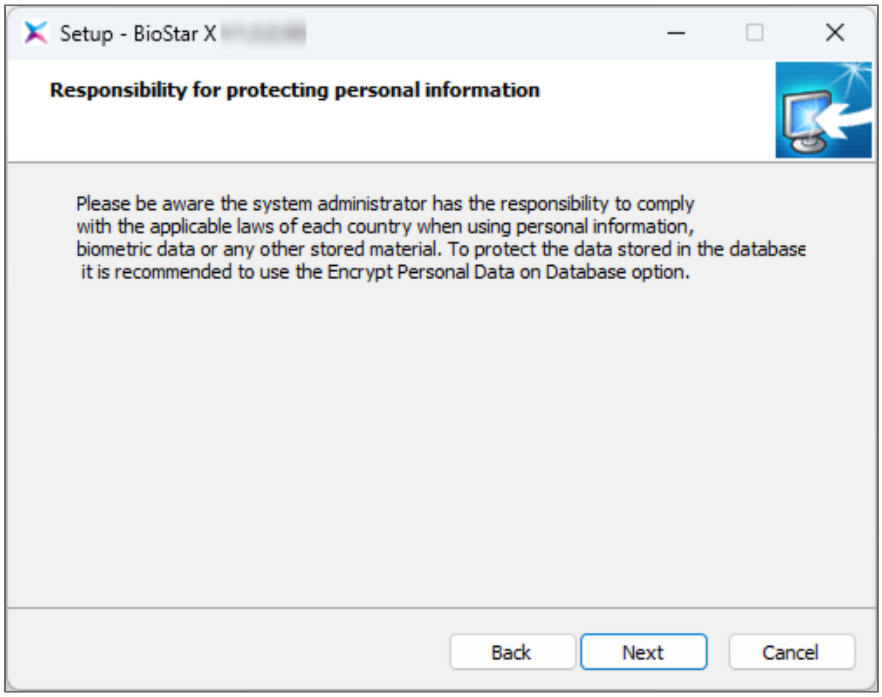
7. 既存のデータベースの root アカウントのパスワードを入力し、**次へ** ボタンをクリックしてください。



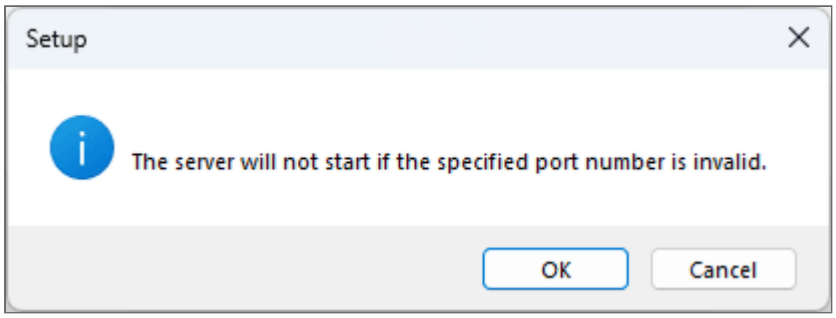
8. 暗号化キーを保存するパスを設定し、**次へ** ボタンをクリックしてください。



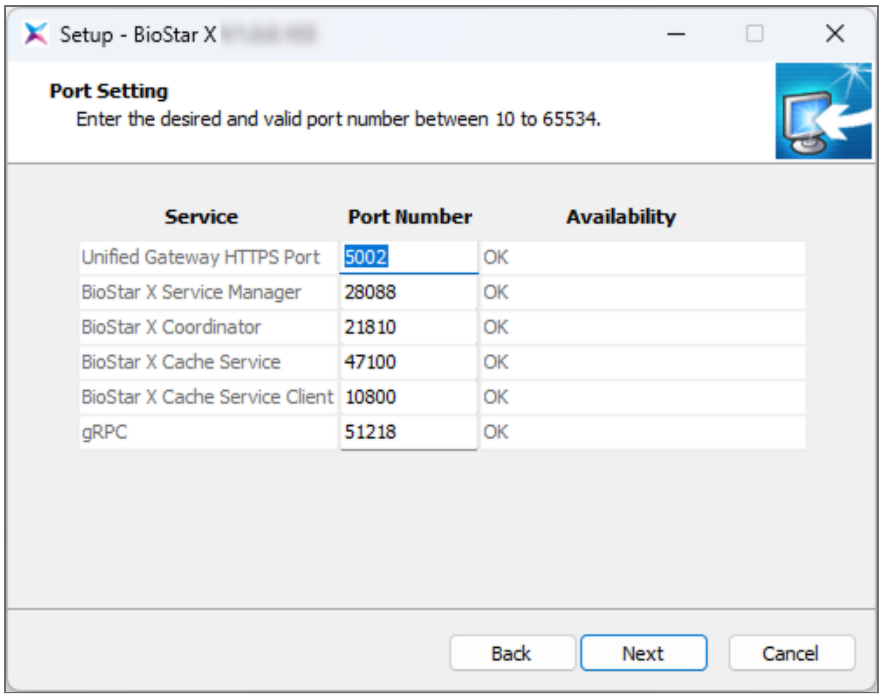
9. データベースに保存される個人情報の管理権限および責任に関する案内を読み、インストールを続行するには **次へ** ボタンをクリックしてください。



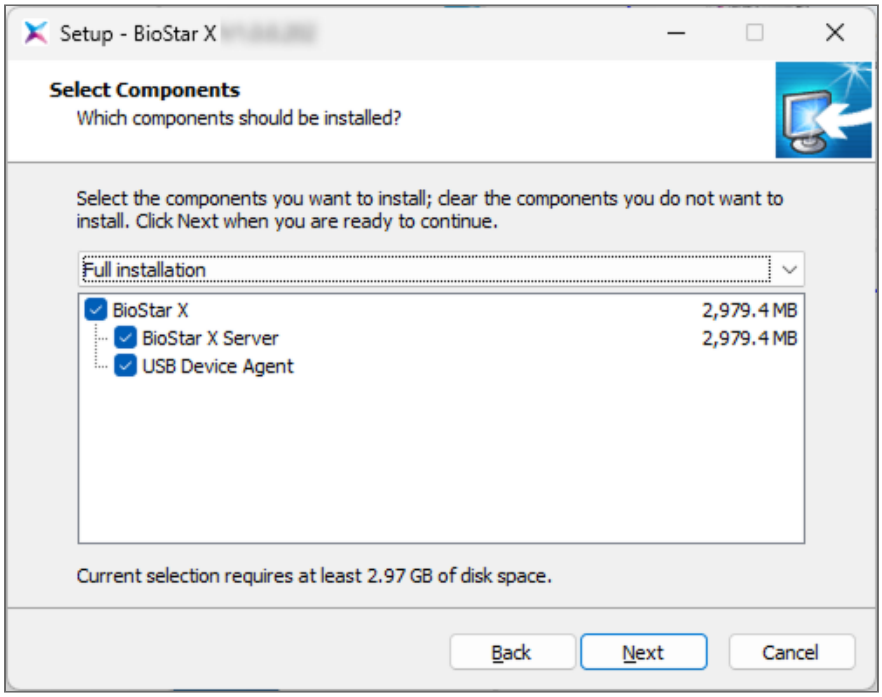
10. ポート番号に関するメッセージが表示されたら、**OK** をクリックしてください。



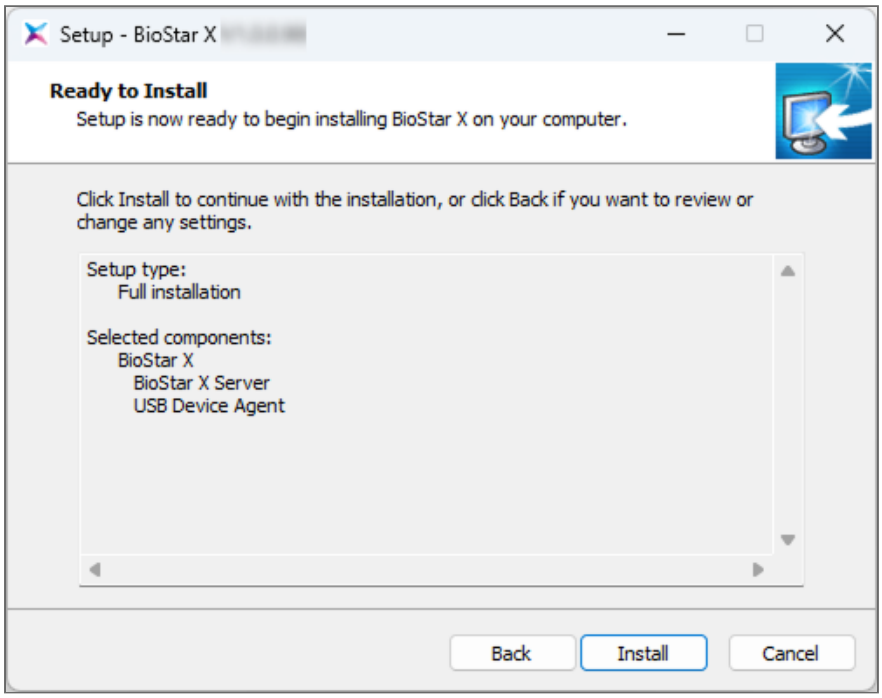
11. **BioStar X** の通信ポートを設定し、**次へ** ボタンをクリックしてください。



12. **BioStar X** のコンポーネントを選択し、**次へ** ボタンをクリックしてください。 **USB Device Agent** を選択すると、BioMini、BioMini Plus 2、BioMini Slim 2、DUALi DE-620 を使用するための USB Agent とドライバーが併せてインストールされます。



13. すべてのインストール準備が完了したら、**インストール** ボタンをクリックしてください。



14. 追加プログラムのインストール有無を選択し、終了 ボタンをクリックしてください。



15. インストール画面の指示に従って **USB Device Agent** のインストールを完了してください。

情報

- ダウンロードしたファイル名の X.Y.Z はバージョン情報、BB はビルド番号です。
- 管理者アカウントのパスワードは、**BioStar X** をインストールした後の初回ログイン時に使用します。
- データベースの root アカウントのパスワードは、AC、TA、Video DB の初期パスワードとして使用します。
- 暗号化キーの保存パスを変更できます。 パスを変更した後に暗号化キー ファイルを編集または別のパスに移動すると、システムエラーが発生する可能性があります。
- **BioStar X** をアンインストールすると、暗号化キー ファイルも同時に削除されます。
- 提供される USB Device Agent 証明書はローカルネットワークにのみ適用できます。
- 他のプログラムが 443 ポートを使用している場合、BioStar X Setting プログラムが自動的に起動し、ポート番号を変更できます。 ポート番号の変更については、ポートを変更するを参照してください。
- データベース設定の変更の詳細については、データベースを変更するを参照してください。

警告

- 管理者またはデータベースの root アカウントのパスワードを紛失しないよう注意してください。
- パスワードを紛失すると、バージョンアップグレードおよび DB のバックアップ/復元ができなくなる可能性があります。

次のステップ

Web ブラウザを起動して **BioStar X** にログインする方法を確認してください。
BioStar X のサーバー状態を確認し、停止または再起動する方法を確認してください。

マルチコミュニケーションサーバーをインストールする

本ドキュメントでは、**BioStar X** の **マルチコミュニケーション（Multi Communications）サーバー** のインストール方法を案内します。

マルチコミュニケーションサーバーは、入退室管理デバイスとの通信を専任で行うサーバーです。メインサーバーとは別に設置し、多数のデバイスを安定して管理できるよう支援します。一台のマルチコミュニケーションサーバーで最大 1,000 台のデバイスを接続でき、必要に応じて複数台のマルチコミュニケーションサーバーを追加することもできます。

> **情報**
> Ethernet (TCP/IP) で接続できるデバイスの最大数は 1,000 台です。

開始前

マルチコミュニケーションサーバーをインストールする前に、次の事項を確認します。

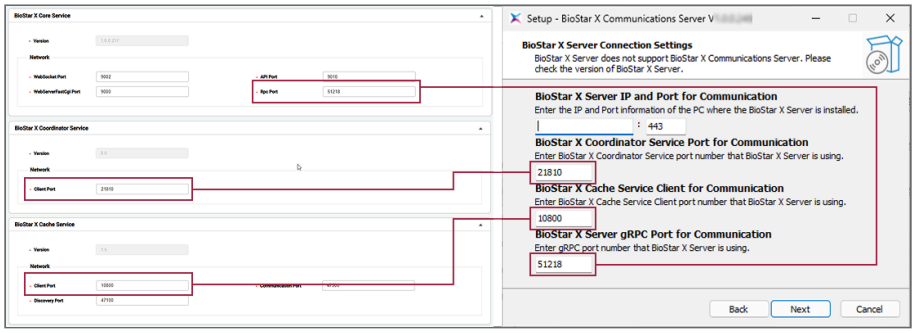
- マルチコミュニケーションサーバーは **BioStar X** サーバーと同じサーバーにインストールできません。
- マルチコミュニケーションサーバーは 64 ビットオペレーティングシステムにのみインストールできます。システムの最低要件の詳細については システム最小要件 をご参照ください。
- マルチコミュニケーションサーバーをインストールして接続するには、マルチコミュニケーションサーバーライセンスが必要です。ライセンスポリシーの詳細については、ライセンス ポリシーを参照してください。

インストール前の確認事項

マルチコミュニケーションサーバーをインストールする前に **BioStar X Service Manager** を実行し、インストール中に入力が必要な情報を確認します。

1. Windows で 開始 → **BioStar X** → **BioStar X Service Manager** をクリックします。
2. **BioStar X Service Manager** ウィンドウが表示されます。
3. **SERVICE SETTINGS** をクリックします。

以下に、マルチコミュニケーションサーバーのインストール時に入力が必要な情報を示します。各項目を確認して準備します。



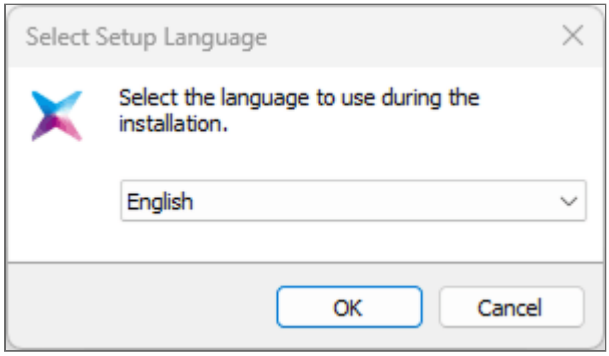
BioStar X Service Manager	マルチコミュニケーションサーバーインストール時の入力情報
BioStar X Core Service → **RPC Port**	BioStar X Server gRPC Port for Communication
BioStar X Coordinator Service → **Client Port**	BioStar X Coordinator Service Port for Communication
BioStar X Cache Service → **Client Port**	BioStar X Cache Service Client for Communication

> **情報**
> **SERVICE SETTINGS** の詳細については サービス設定 をご参照ください。

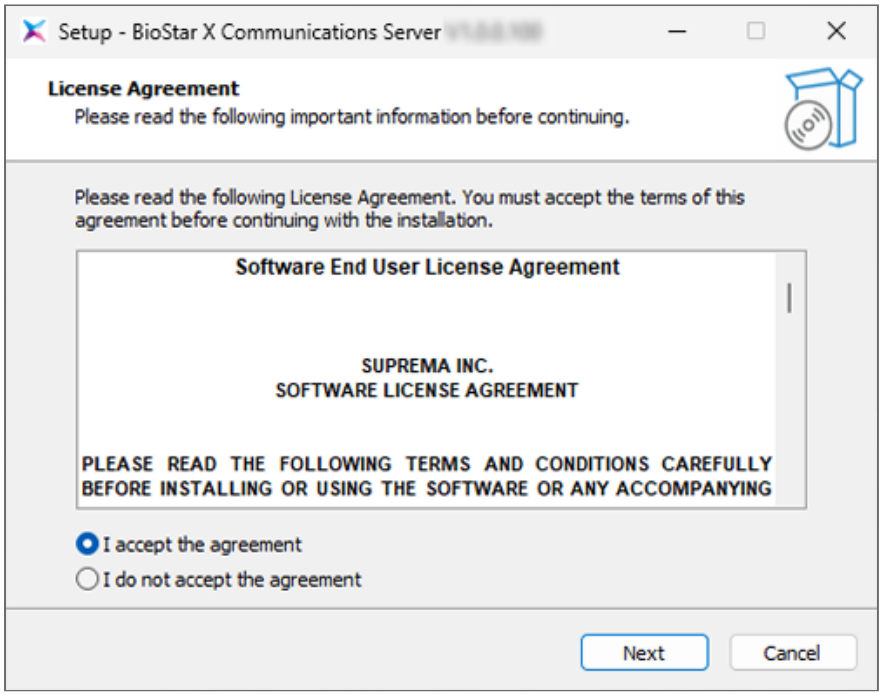
インストールガイド

マルチコミュニケーションサーバーをインストールするには、次の手順に従います。

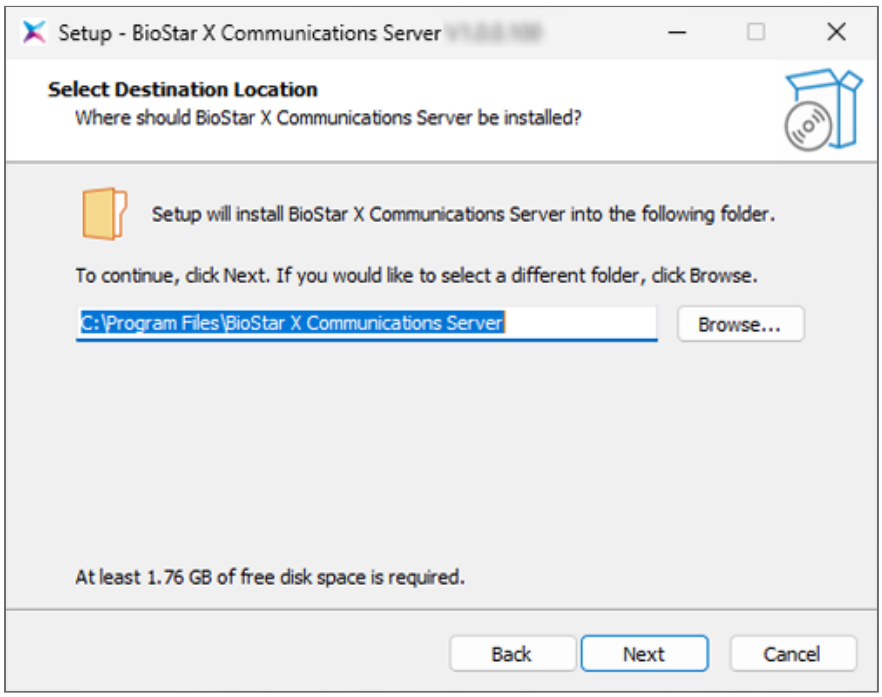
1. Suprema ダウンロードセンター にアクセスしてログインし、インストールパッケージ (*BioStar X Communications Server.X.Y.X.BB.exe*) をダウンロードします。
2. ダウンロードしたインストールファイルを実行してください。
3. 使用する言語を選択し、**OK** ボタンをクリックしてください。



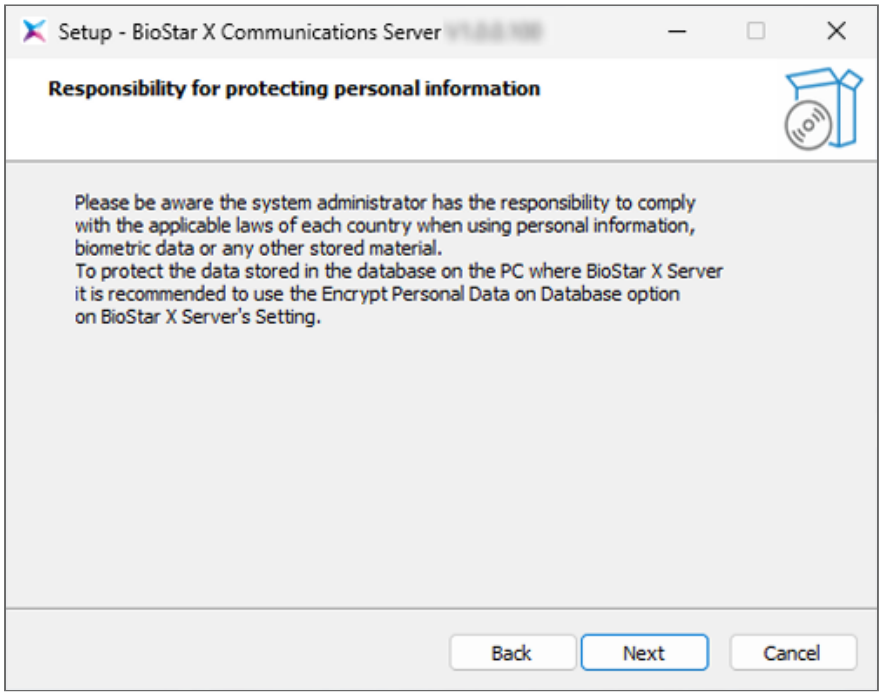
4. インストールを続行するには、**同意する** を選択し、**次へ** ボタンをクリックしてください。



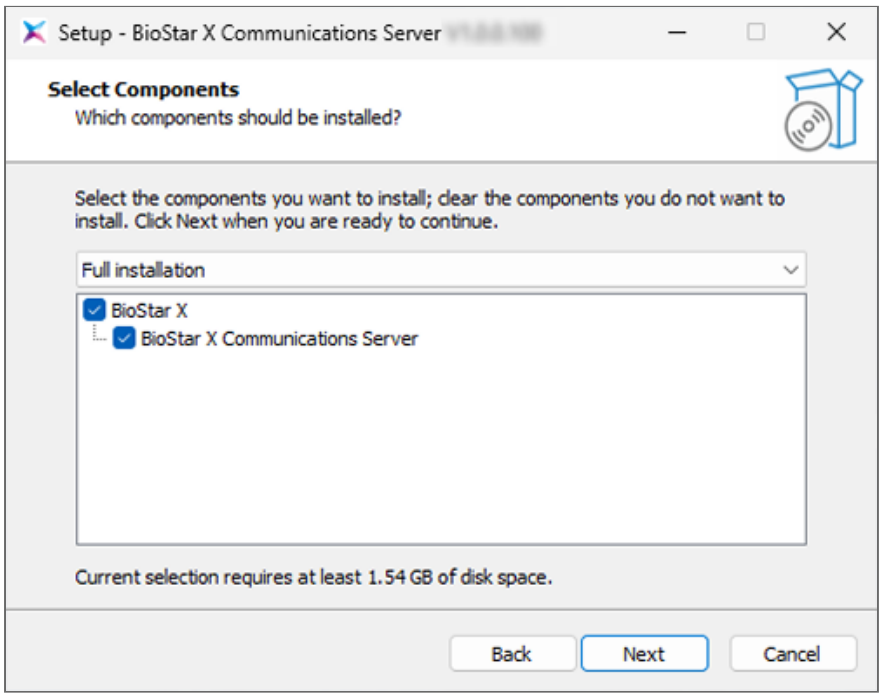
5. マルチコミュニケーションサーバーをインストールするパスを設定し、**次へ** をクリックします。



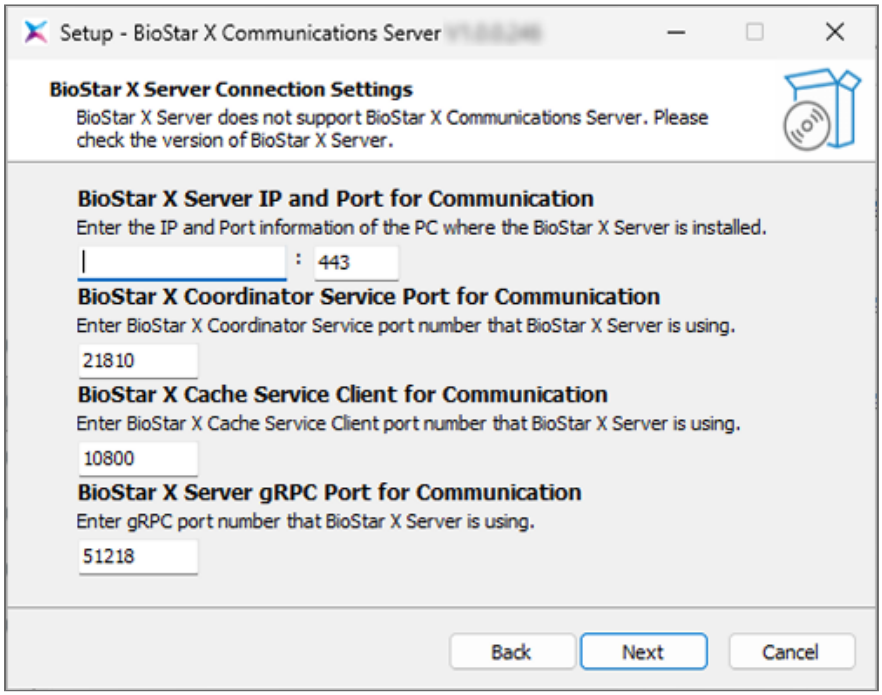
6. 個人情報に関する権限と責任の内容を確認し、インストールを続行するには **次へ** をクリックします。



7. マルチコミュニケーションサーバーのコンポーネントを選択し、**次へ** をクリックします。

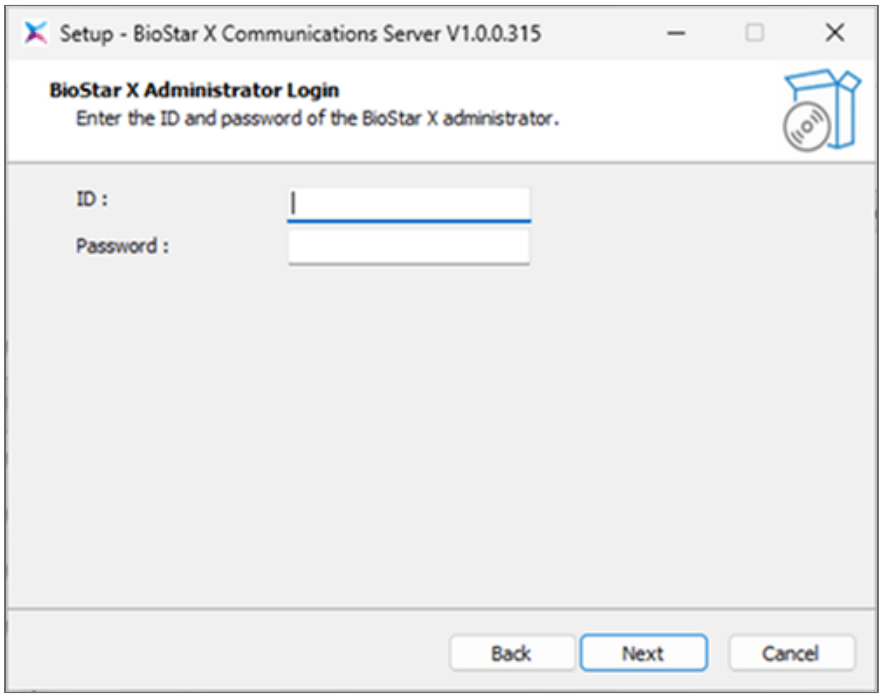


8. **BioStar X** サーバーの IP アドレスとポート番号を入力し、**BioStar X** サーバーと接続するために各項目を入力します。設定を完了し、**次へ** をクリックします。

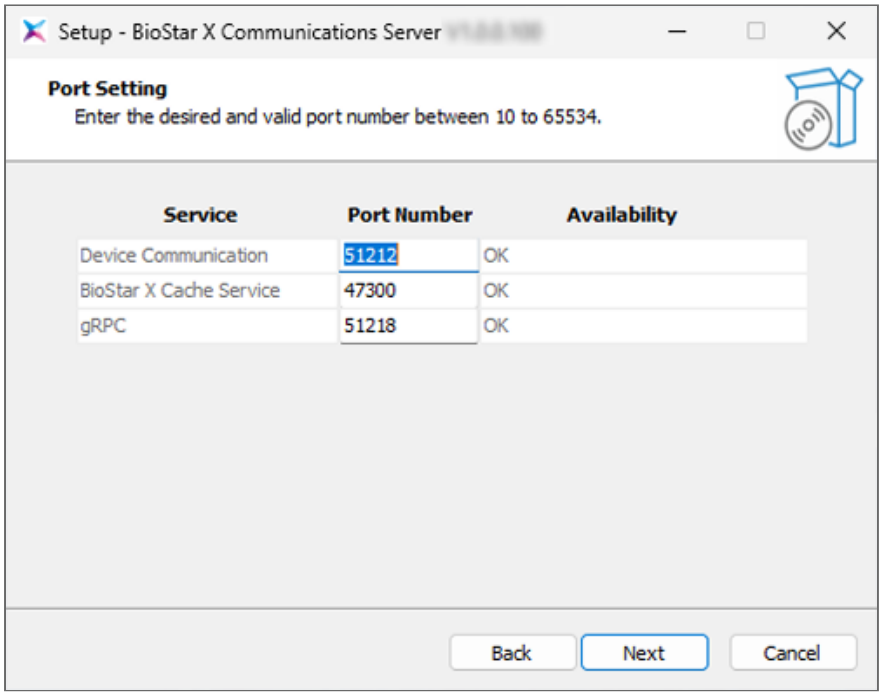


> 各入力項目の詳細については インストール前の確認事項 をご参照ください。

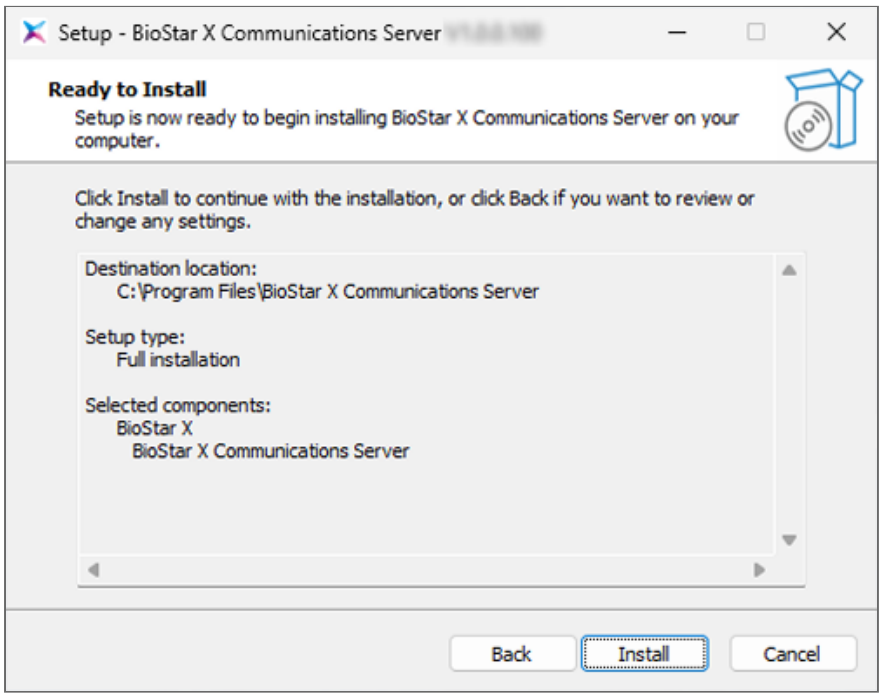
9. **BioStar X** の管理者 ID とパスワードを入力し、**次へ** ボタンをクリックします。



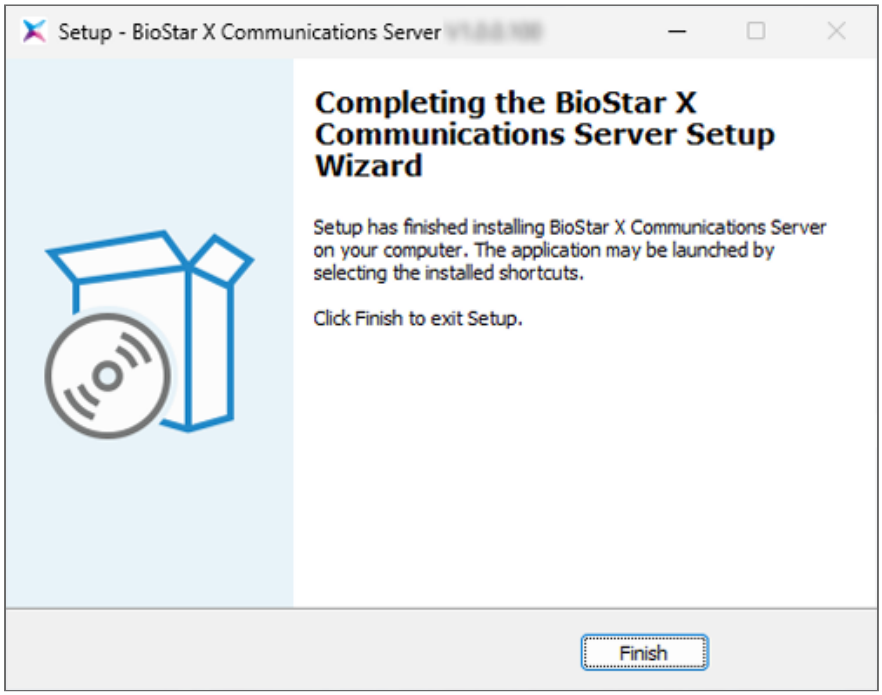
10. 通信用ポートを設定し、**次へ** をクリックします。



11. すべてのインストール準備が完了したら、**インストール** ボタンをクリックしてください。インストールを実行します。



12. インストール完了メッセージを確認し、**完了** をクリックします。

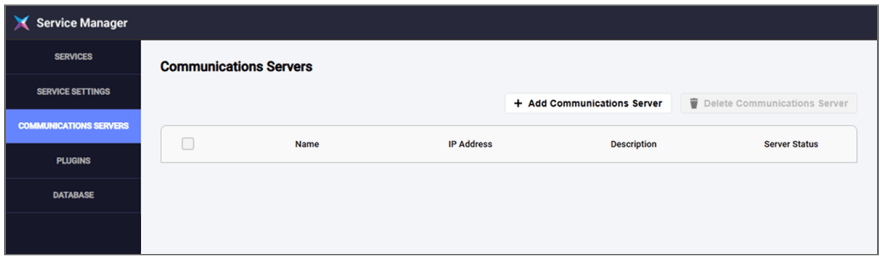


マルチコミュニケーションサーバーのインストールを完了します。インストールが完了したら、**BioStar X** メインサーバーでマルチコミュニケーションサーバーと接続されていることを確認します。

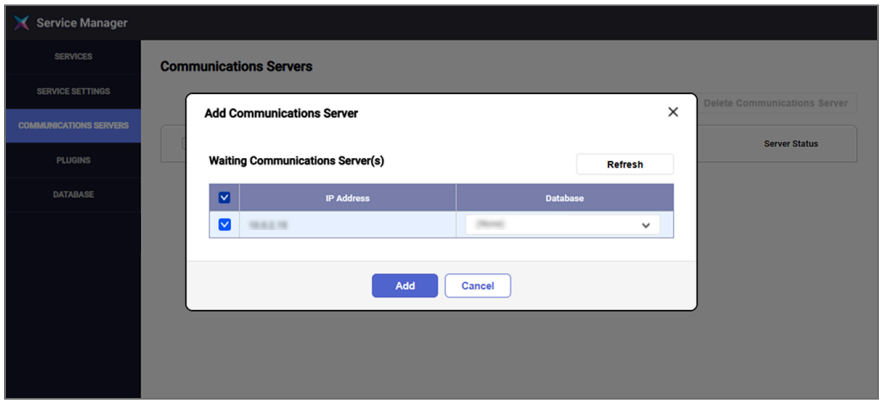
インストール後の確認事項

マルチコミュニケーションサーバーのインストールを完了したら、**BioStar X Service Manager** を使用してメインサーバーとマルチコミュニケーションサーバーを接続する必要があります。

1. Windows で 開始 → **BioStar X** → **BioStar X Service Manager** をクリックします。
2. **BioStar X Service Manager** ウィンドウが表示されます。
3. 画面左側のサイドバーで **COMMUNICATIONS** メニューをクリックします。

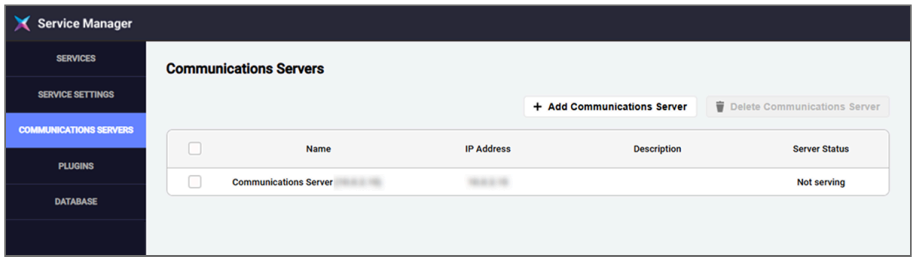


4. 画面右上の **Add Communication Server** ボタンをクリックします。
5. **Add Communication Server** ウィンドウが表示されたら、インストールしたマルチコミュニケーションサーバーの IP アドレスと一致する項目のチェックボックスをクリックし、**Database** 列で使用するデータベースを選択します。



6. **Add** をクリックします。

マルチコミュニケーションサーバー一覧で、追加したマルチコミュニケーションサーバーの **Server Status** 列が **Connected** 状態であることを確認します。



情報

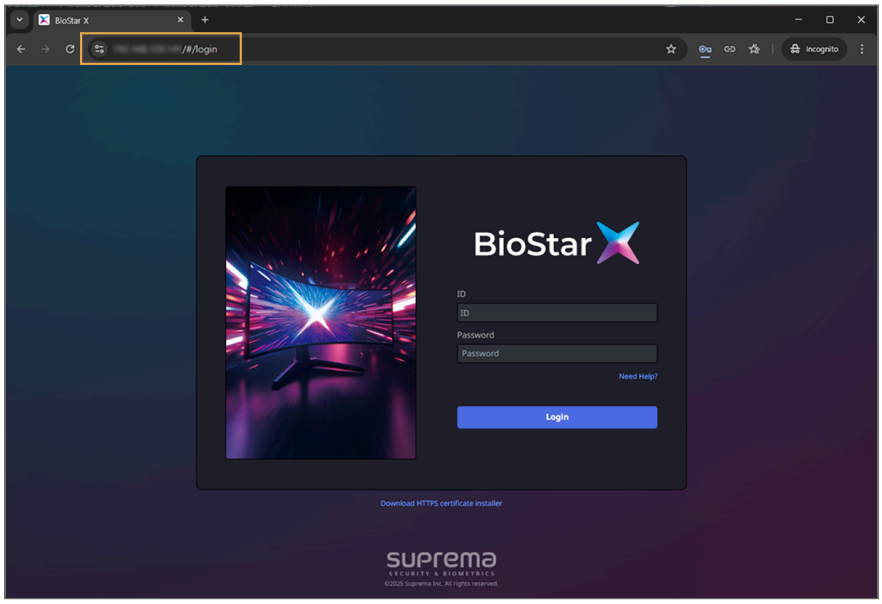
- **COMMUNICATIONS** メニューは、マルチ Communication サーバーライセンスを有効化したときに使用できます。ライセンスポリシーの詳細については、ライセンス ポリシーを参照してください。
- マルチコミュニケーションサーバーを削除するには、一覧で削除するサーバーのチェックボックスをクリックし、画面右上の **Delete Commnunication Server** ボタンをクリックします。
- マルチコミュニケーションサーバーを追加した場合、メインサーバーの負荷を軽減するために、マルチコミュニケーションサーバーと連携する補助データベースを追加できます。補助データベースの追加に関する詳細は 補助データベースを追加する をご参照ください。

ログインする

インストールパッケージを使用して **BioStar X** のインストールが完了したら、Webブラウザーから接続して正常に動作するか確認します。 **BioStar X** はWebベースのサービスを提供しており、いつでもどこでもアクセスできます。

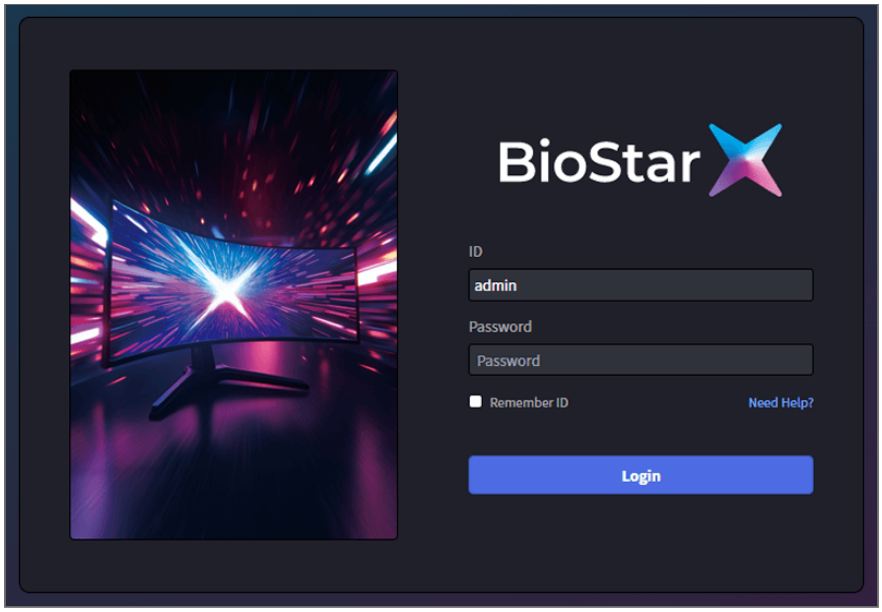
Webブラウザーでログインする

1. Windows で 開始 → **BioStar X** → **BioStar X** をクリックします。
2. Webブラウザーを通じて **BioStar X** に接続します。



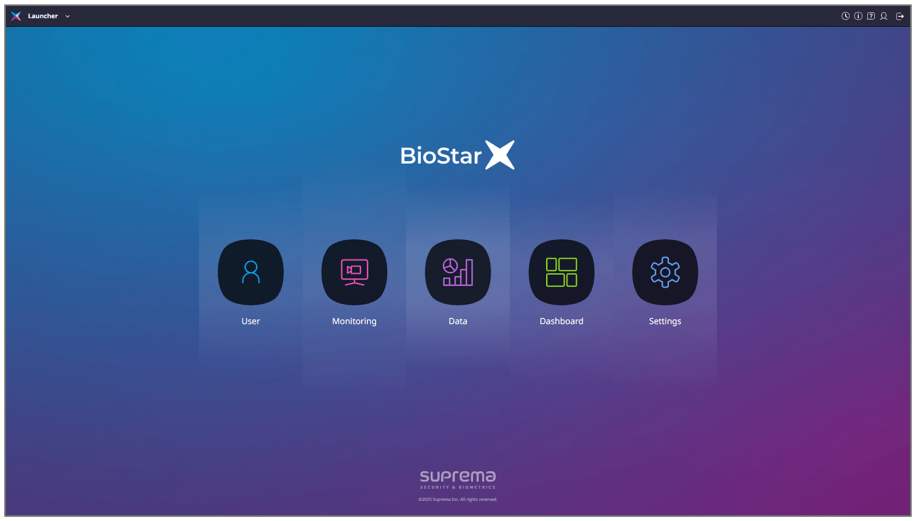
- Webブラウザーのアドレスバーで **BioStar X** の接続アドレスを確認します。
- **BioStar X** を別のPCにインストールした場合は、そのPCのIPアドレスを入力します。例：https://192.168.0.1
- 'localhost' を **BioStar X** の接続アドレスとして使用しないでください。
- **BioStar X** はUnified Gateway（統合ゲートウェイ）を介してすべてのリクエストを統合処理します。そのため、Webアクセスおよびapi呼び出しは統合ゲートウェイポート（デフォルト443）を通じて行われます。

3. ログイン画面が表示されたら、管理者アカウントでログインします。



- 管理者IDは **admin** です。
- Webブラウザーのアドレスバーに **安全ではありません** の警告が表示された場合は、HTTPS証明書をインストールする必要があります。証明書のインストールの詳細については HTTPS 証明書をインストールするを参照してください。

ログインすると **Launcher** 画面が表示されます。



情報

- Chrome 100 以降のバージョンのブラウザーの使用を推奨します。
- **BioStar X** をインストールしたPCの外部IPアドレスは次のリンクにアクセスして確認できます。
- **BioStar X** は **443** ポートをデフォルトで使用します。 **443** ポートを使用しているプログラムがある場合は終了してから、再度接続を試みてください。そのプログラムを終了できない場合は **BioStar X Service Manager** を実行してポート番号を変更します。詳細については、ポートを変更するを参照してください。

ライセンスキーを登録する

BioStar X ライセンスを購入した場合は、ライセンスキーを登録してより多くの機能を利用できます。

Settings → **License** → **BioStar X License** メニューに移動します。

ユーザーのネットワーク環境によって、**BioStar X License** を有効化する方法が異なります。案内に従ってネットワーク状態を確認し、ライセンスを有効化してください。

情報

- ライセンスを登録していない状態では、ユーザーの追加や出入口、デバイスの追加といった一部の機能が制限されます。
- **License** メニューの詳細は ライセンスを有効化 をご参照ください。
- 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。
- ライセンスのエラーコードを確認するには次のリンクを参照してください。

オンラインで登録する

情報

ライセンスキーには、数字とハイフン(`-`)のみ入力できます。 `1111-1111-1111-1111` 形式で、最大16文字の数字を入力する必要があります。

単一ライセンスの登録

インターネットに接続されたオンライン環境で **BioStar X** ライセンスをアクティベートするには、名前と受け取ったライセンスキーを入力し、**Activate** ボタンをクリックします。



複数ライセンスの登録

最大30件のライセンスを一度に追加できます。 ＋ **Add More License** ボタンをクリックします。ライセンスをすべて入力したら、**Activate** ボタンをクリックします。



- 入力欄が30件に達すると、＋ **Add More License** ボタンが無効になり、これ以上追加できません。
- 複数のライセンスキーをまとめてコピーして入力欄に貼り付けると、`1111-1111-1111-1111` 形式のキーだけを自動認識し、各入力欄に分割して追加します。
- 貼り付けたキーが30件を超えると、30件まで自動入力され、超過分は無視されます。

アクティベーションの進行状況

Activate ボタンをクリックすると、進行状況ポップアップが表示されます。アクティベーションが完了するまで、ページやポップアップを閉じないでください。

オフラインで登録する

閉鎖ネットワーク環境やインターネット接続が制限されたオフライン環境で **BioStar X** ライセンスをアクティベートするには、以下の手順に従ってください。

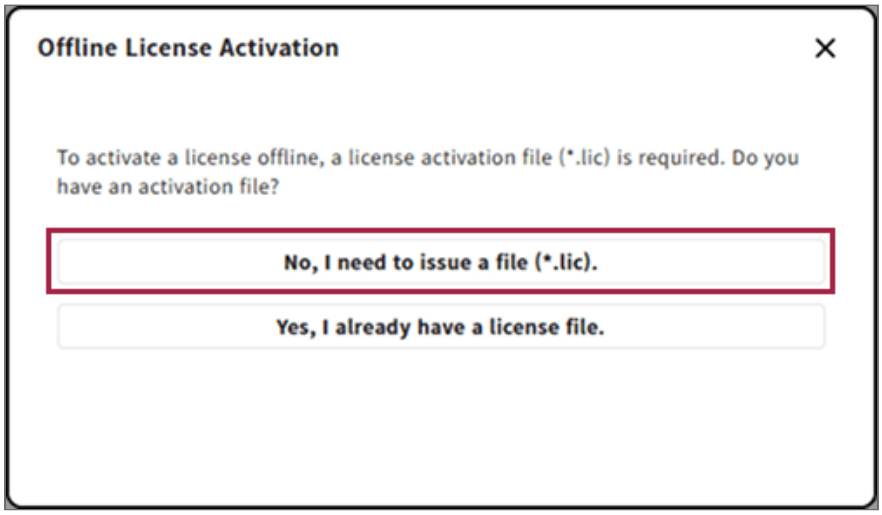
1. **License Activation** セクションで任意の登録管理者名とライセンスキーを入力します。

   - ライセンスキーには、数字とハイフン(`-`)のみ入力できます。 `1111-1111-1111-1111` 形式で、最大16文字の数字を入力する必要があります。
   - 登録管理者名とライセンスキーを覚えるか、メモしておいてください。
   - 複数のライセンスが必要な場合は、＋ **Add More License** ボタンをクリックして追加します。

2. **Offline Activation** ボタンをクリックします。

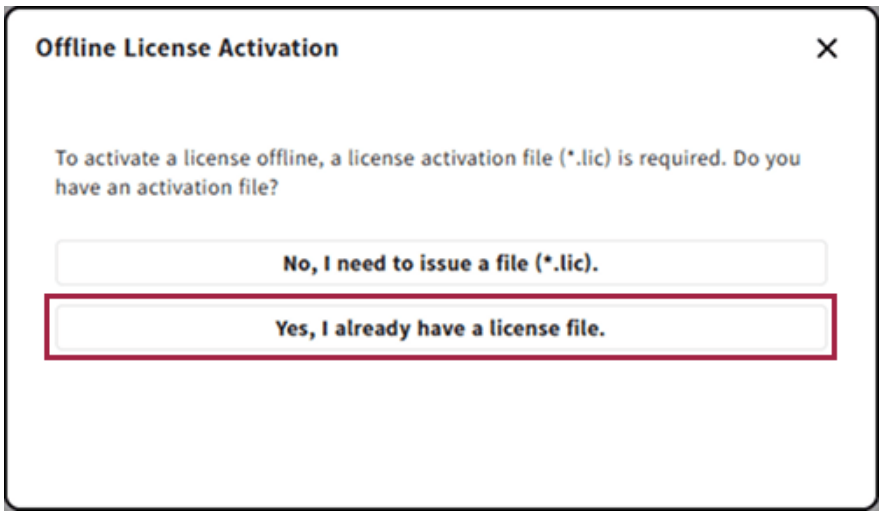


3. **Activate License Offline** ウィンドウが表示されたら、**No, I need to issue a file (*.lic).** ボタンをクリックします。



> すでに発行済みのライセンスファイルがある場合は、この画面で **Yes, I already have a license file.** ボタンをクリックしてから、手順9に進んでください。

4. 発行要求ファイル（*.req）が生成されたら、ローカルディスクへダウンロードしてください。
5. ダウンロードした発行要求ファイルを購入先へ送付し、オフライン有効化ファイル（*.lic）を要求してください。
6. オフラインアクティベーションファイルを受け取ったら、手順1で入力した登録管理者名とライセンスキーを **License Activation** セクションに入力します。
7. **Offline Activation** ボタンをクリックします。
8. **Activate License Offline** ウィンドウが表示されたら、**Yes, I already have a license file.** ボタンをクリックします。



9. ［ファイルを開く］ダイアログが開いたら、ローカルに保存したオフライン有効化ファイル(*.lic)または圧縮ファイル(*.zip)を選択してください。

> 複数のライセンスをリクエストした場合、圧縮ファイルを受け取ることがあります。

10. 進行状況のポップアップが開きます。アクティベーションが完了するまで、ページやポップアップを閉じないでください。

初期設定ガイド

初めて BioStar X をインストールした後、正常に運用するために必要な設定を段階的に案内します。各段階を順に実行し、効率的な入退室管理環境を構築してください。

1 デバイス登録

BioStar X に接続するデバイスを登録してください。デバイスごとに認証モードを個別に構成したり、それぞれのデバイスに管理者を設定できます。

また、デバイスで発生する各種イベント（認証失敗、強要指紋認証、アンチパスバック違反など）に応じた動作を設定できます。

- デバイスグループを管理する
- デバイスを登録する
- Wiegandデバイスを登録する
- スレーブ装置を登録する
- デバイス設定

> **情報**
> デバイスを登録するには、**デバイス マネージャー**以上の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 ポリシーをご参照ください。

2 ドアの登録と設定

デバイスが設置されているドアの情報を登録してください。リレー、アンチパスバック、二要素認証、アラームなどを設定できます。

- ドアグループを管理する
- ドアを登録する

3 アクセスレベル設定

アクセスレベルはドア情報とスケジュール情報を組み合わせて作成し、1 つのアクセスレベルに複数のドアとスケジュールを登録できます。

アクセスレベルを管理する

4 アクセスグループ設定

アクセスグループはアクセスレベル（ドア、スケジュール）とユーザー情報を組み合わせて作成し、1 つのアクセスグループに複数のアクセスレベルとユーザーを登録できます。

アクセスグループを管理する

5 ユーザー登録

ユーザー情報やクレデンシャルなど、入退室管理に使用する情報を登録してください。ユーザー情報はデバイスで直接登録することも、BioStar X で登録することもできます。さらに、デバイスで登録したユーザー情報を BioStar X に取り込んだり、BioStar X で登録したユーザー情報をデバイスに送信することもできます。

- ユーザーグループを管理する
- ユーザー管理
- ユーザー登録
- ユーザークレデンシャルを登録する

6 高度な入退室管理設定

アンチパスバック、火災警報などを設定でき、火災警報はローカルとグローバルを設定できます。

- 高度な入退室制御設定
- マップをモニタリングする

> **情報**
> **エッセンシャル**（Essential）以上のライセンスでのみ使用できます。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。

7 モニタリング

ドア、デバイス、イベントなど、さまざまなモニタリング機能を通じてリアルタイムで入退室管理システムを管理できます。

- ドアをモニタリング
- デバイスをモニタリングする
- イベントをモニタリングする

サーバー管理

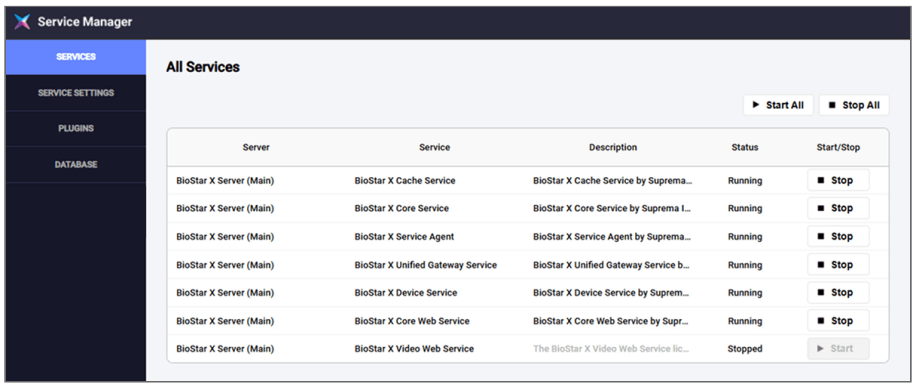
BioStar X をインストールした後、ユーザーはさまざまなサーバー管理機能を利用してシステムを効率的に運用できます。本書では、BioStar X のサーバー管理機能について説明します。

サーバーの起動と停止

BioStar X Service Manager を使用して BioStar X サーバーのサービスを管理する方法を確認します。個別のサービスを起動または停止できます。

BioStar X Service Manager

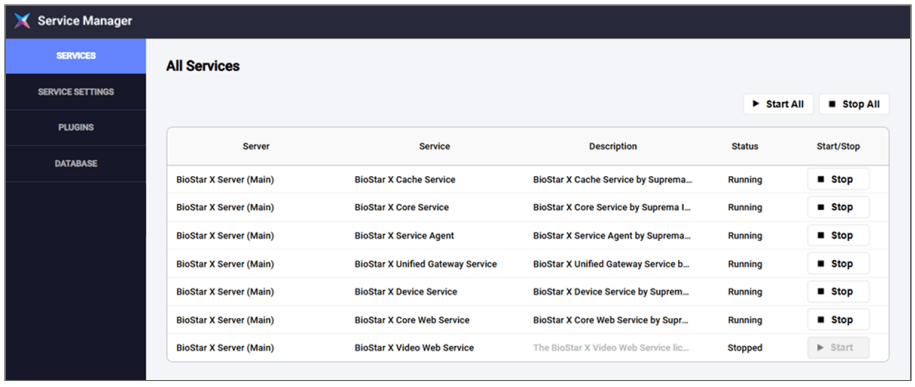
BioStar X サーバーの状態を管理できるツールを提供します。 Windows で 開始 → **BioStar X** → **BioStar X Service Manager** をクリックします。 **BioStar X Service Manager** ウィンドウが表示されます。



> **情報**
>
> **BioStar X** サーバーの時間設定を変更した場合は、**BioStar X Core Service** を停止して再起動してください。再起動しないと、**BioStar X** が動作しない可能性があります。

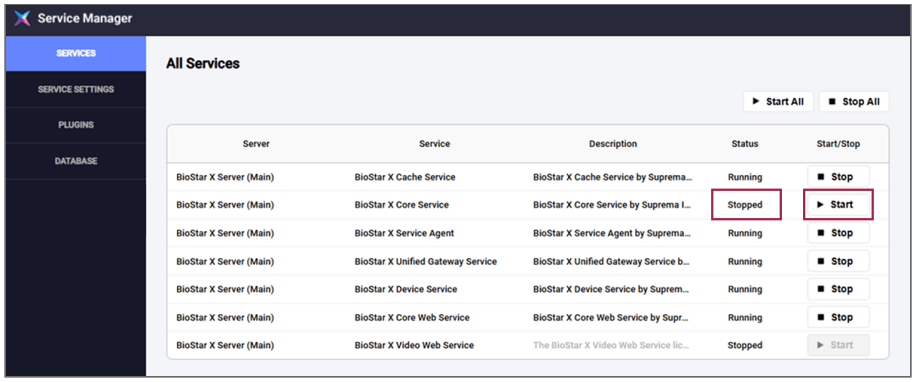
サービスを終了する

BioStar X を終了するには、**SERVICES** メニューで各サービスの **Stop** ボタンをクリックします。すべてのサービスを終了するには、画面右上にある **Stop All** ボタンをクリックしてください。



サーバーを起動する

BioStar X を再起動するには、**SERVICES** メニューの **Status** 列で **Stopped** 状態のサービスの **Start** ボタンをクリックします。すべてのサービスを再起動するには、画面右上の **Start All** ボタンをクリックしてください。



サービス設定

BioStar X Service Manager の **Service Settings** メニューでは、システムのコアサービスを構成して管理できます。各サービスは独立して設定され、ネットワークポートとバージョン情報を確認できます。

Service Settings は以下の主要サービスで構成されています。

- **BioStar X Core Web Service**：Web インターフェースサービス
- **BioStar X Core Service**：システムのコア機能および API 通信サービス
- **Unified Gateway Service**：リバースプロキシベースの統合ゲートウェイサービス
- **BioStar X Coordinator Service**：分散システムの構成情報管理およびサービス間同期
- **BioStar X Server (Main)**：メインサーバーサービス
- **BioStar X Cache Service**：データキャッシュとシステム性能の向上

設定変更が必要な状況

次のような状況でサービス設定を変更する必要があります。

- **ポート競合の解決**：他のアプリケーションが同じポートを使用して競合が発生した場合
- **セキュリティポリシーの遵守**：組織のネットワークセキュリティポリシーにより特定のポート範囲のみ許可されている場合
- **ファイアウォール設定**：企業のファイアウォールで許可されているポートに変更する必要がある場合
- **サーバー環境の変更**：サーバー IP アドレスやネットワーク構成を変更する場合
- **性能最適化**：トラフィック分散やロードバランシングのためにポートを分離する必要がある場合

設定変更方法

1. **BioStar X Service Manager** で **SERVICE SETTINGS** メニューをクリックします。
2. 変更するサービスのセクションに移動します。

3. 必要なポート番号やアドレスを修正します。
4. 変更を適用するには、画面右上の **Apply** ボタンをクリックします。

- サービス設定を変更した後、変更を反映させるには関連サービスを再起動してください。
- 一部のサービスではポートの変更に対応していない場合があります。

注意
ポート番号を変更する際は、他のサービスやアプリケーションと競合しないよう注意してください。

サービス構成

BioStar X Core Web Service

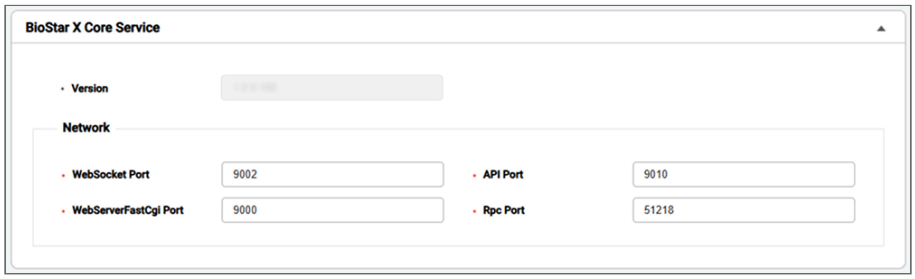
Web ベースのユーザーインターフェースを担当するサービスです。



- **HTTPS Port**：Web インターフェース接続ポート (デフォルト：5002)
- **WebServerThrift Port**：Thrift プロトコルベースの Web サーバー通信ポート (デフォルト：9310)

BioStar X Core Service

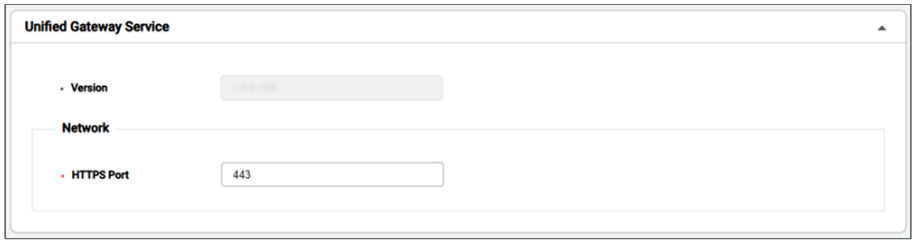
システムのコア機能と外部 API 通信を処理するメインサービスです。



- **WebSocket Port**：リアルタイムの双方向通信用 WebSocket ポート (デフォルト：9002)
- **API Port**：REST API 通信用ポート (デフォルト：9010)
- **WebServerFastCgi Port**：FastCGI プロトコルベースの Web サーバー通信ポート (デフォルト：9000)
- **Rpc Port**：RPC （リモートプロシージャコール）通信ポート (デフォルト：51218)

Unified Gateway Service

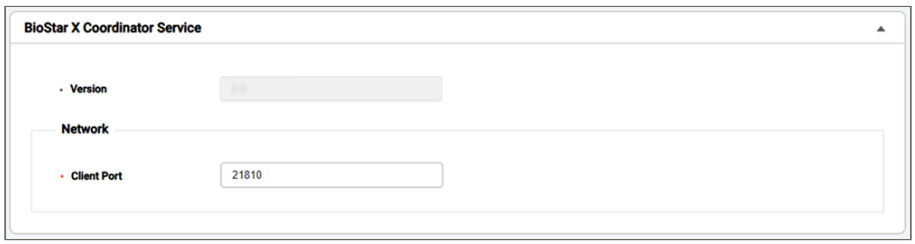
リバースプロキシ方式により **BioStar X** サーバーへのリクエストを効率的に処理し、iframe のセキュリティ脆弱性を改善し、SSL 証明書のエラーを最小化します。



- **HTTPS Port**：統合ゲートウェイ HTTPS 通信用ポート (デフォルト：443)

BioStar X Coordinator Service

分散システムの構成情報管理、サービス状態のモニタリング、およびサービス間同期を担当するサービスです。

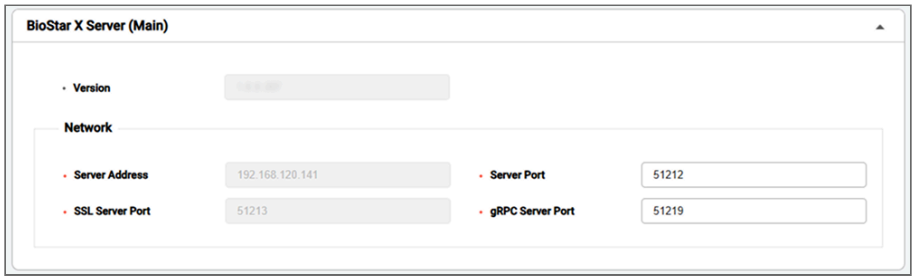


- **Client Port**：クライアント接続用通信ポート (デフォルト：21810)

> **情報**
>
> - **Client Port** の値を変更した場合は、**Windows Services**(*services.msc*) で **BioStar X Coordinator Service** を探して手動で再起動してください。
> - **BioStar X Coordinator Service** を再起動した後、**BioStar X Service Manager** → **SERVICES** メニューで全サービスを再起動します。
>
> 画面右上の **Stop All** ボタンをクリックします。すべてのサービスが停止した後、**Start All** ボタンが有効になったらクリックします。

BioStar X Server (Main)

システムのメインサーバーとして機能するコアサービスです。

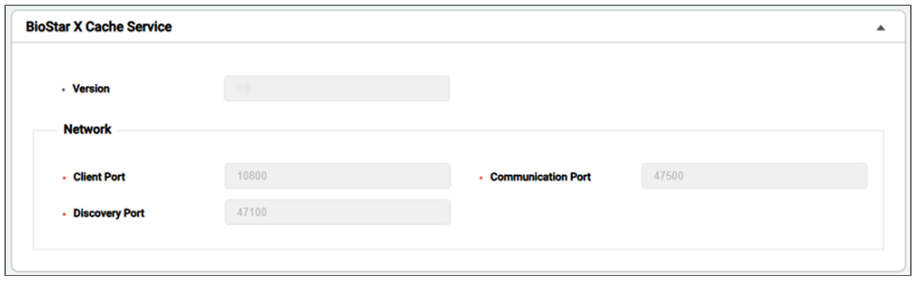


- **Server Address**：メインサーバーの IP アドレス
- **Server Port**：一般サーバー通信用ポート (デフォルト：51212)

- **SSL Server Port**：SSL セキュア通信ポート (デフォルト：51213)
- **gRPC Server Port**：gRPC プロトコルベースの高性能通信ポート (デフォルト：51219)

BioStar X Cache Service

頻繁に使用されるデータをメモリに保存し、システムのデータ処理速度と性能を向上させるサービスです。



- **Client Port**：キャッシュサービスのクライアント接続ポート (デフォルト：10800)
- **Communication Port**：キャッシュノード間内部通信ポート (デフォルト：47500)
- **Discovery Port**：分散キャッシュノード自動検出用ポート (デフォルト：47100)

次のステップ

BioStar X のデフォルトポート (443) を変更する手順をステップごとに確認しましょう。

メインサーバーのIPアドレスを変更する

サーバーのネットワーク環境が変更された場合や、初期設定後にIPアドレスを変更する必要がある場合は、このドキュメントを参照してください。 BioStar X メインサーバーのIPアドレスを安全に変更し、接続されているマルチコミュニケーションサーバーを再構成する方法を説明します。

> **情報**
> メインサーバーのIPアドレス変更機能は **BioStar X v1.0.2** 以降でサポートされています。

IPアドレスの変更

まず**BioStar X**をインストールしたサーバーでIPアドレスを変更してください。外部ネットワークに接続されているLANカードのIPアドレスを変更する必要があります。

> **情報**
> WindowsでのIPアドレスの変更の詳細については、Microsoft サポートをご確認ください。

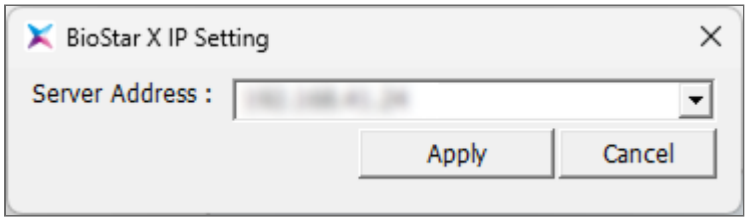
変更したIPアドレスの適用

次の手順に従って、**BioStar X**をインストールしたサーバーのIPアドレスを変更してください。

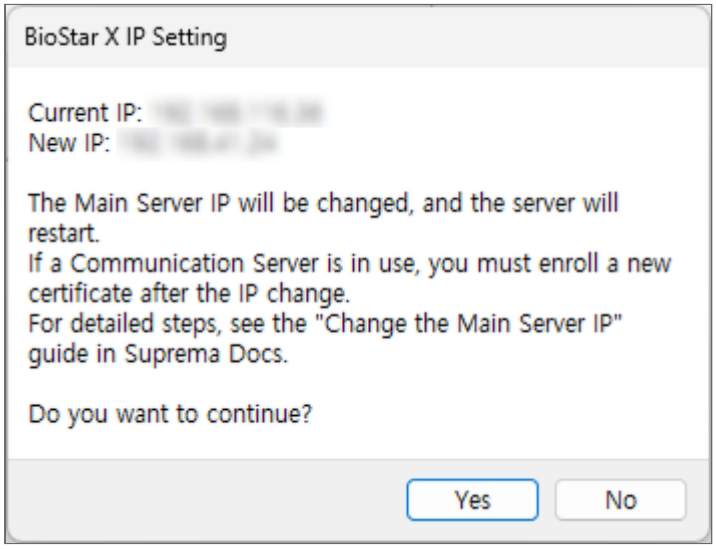
BioStar X IP Setting

BioStar X IP Setting ツールでIPアドレスを変更できます。

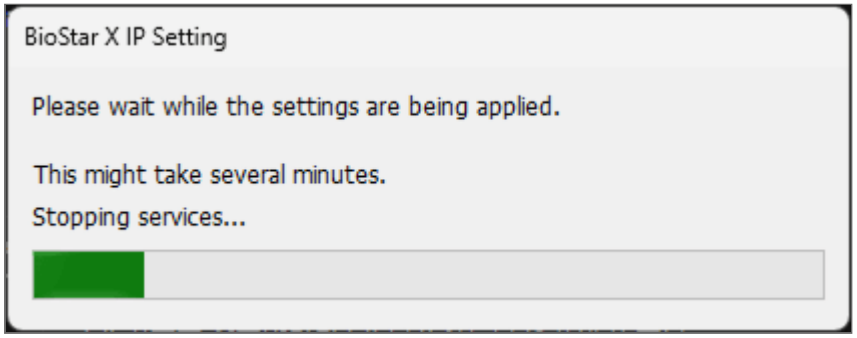
1. Windowsで 開始 → **BioStar X** → **BioStar X IP Setting** をクリックしてください。
2. **BioStar X IP Setting** ウィンドウが表示されたら、**Server Address** で変更するIPアドレスを選択してください。



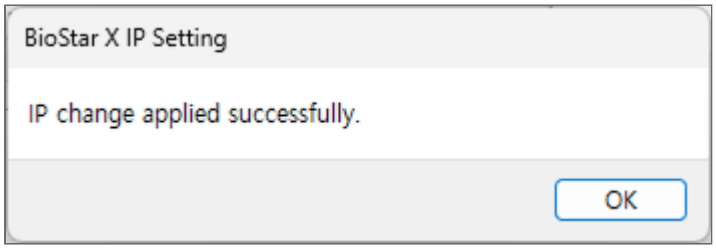
3. **Apply** をクリックしてください。
4. IPアドレス変更に関するメッセージウィンドウが表示されたら、内容を確認して **Yes** ボタンをクリックしてください。



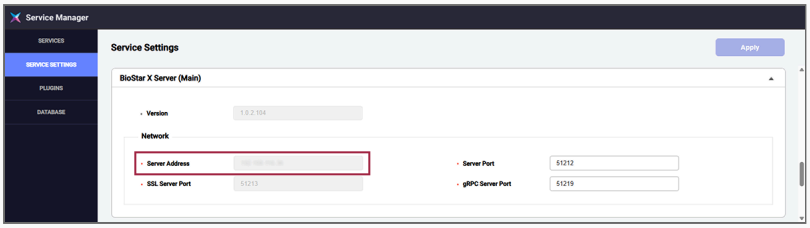
5. IPアドレス変更プロセスが完了するまで待ってください。完了すると成功メッセージウィンドウが表示されます。



6. **IP change applied successfully** メッセージウィンドウが表示されたら、**OK** をクリックしてください。



IPアドレスの変更が完了したら、すべてのサービスを再起動します。

> **情報**
>
> - 変更するIPアドレスは手動入力できず、**Server Address** に表示されているIPアドレスの中から選択できます。
> - 変更したIPアドレスは **BioStar X Service Manager** → **SERVICE SETTINGS** → **BioStar X Server (Main)** セクションの **Server Address** 項目で確認できます。
>
> 
>
>
> - デバイスが **Device** ▶ **Server Connection** オプションで BioStar X に登録されている場合は、各デバイスで管理者がサーバーのIPアドレスを変更後のIPアドレスに手動で更新する必要があります.

データベースサーバー設定の変更

データベースを **BioStar X** と同じサーバーに設置して運用している場合は、すべてのサービスを停止してから **BioStar X** の *system.conf* ファイルを編集してください. 外部データベースサーバーを使用している場合は、この手順をスキップしてください.

1. Windowsのサービス(service.msc)で**BioStar X**に関連するすべてのサービスを停止してください。
2. *C:\Program Files\BioStar X Server* フォルダーに移動してください.
3. *system.conf* ファイルをメモ帳などのテキストエディタで開いてください.
4. `database` に関する項目の `server_ip` 値を変更後のIPアドレスに修正してください.
5. *system.conf* ファイルを保存して閉じてください.
6. Windowsのサービス(service.msc)で**BioStar X**に関連するすべてのサービスを再起動してください。

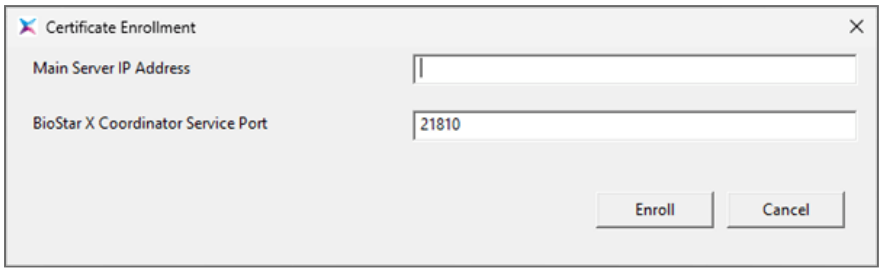
ウェブブラウザを開いて、変更後のIPアドレスに正常にアクセスできるか確認してください。

マルチコミュニケーションサーバーの更新

マルチコミュニケーションサーバーを別途インストールしている場合は、メインサーバーで変更したIPアドレスに合わせてマルチコミュニケーションサーバーの設定を変更してください。マルチコミュニケーションサーバーをインストールしたサーバー上で操作を行ってください。

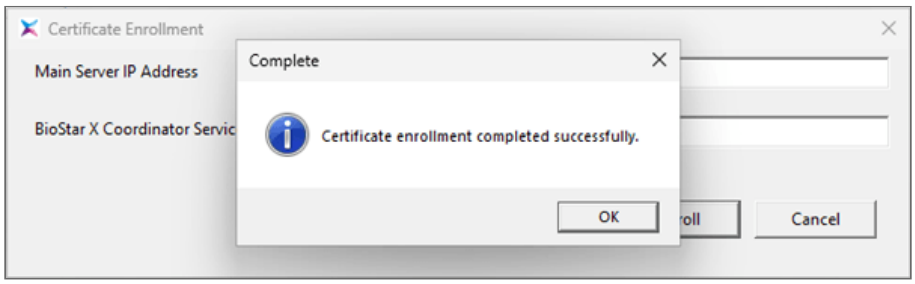
1. *C:\Program Files\BioStar X Communications Server* に移動してください。
2. *biostar-device-cert-enroll.exe* を実行してください。
3. **Certificate Enrollment** ウィンドウが表示されたら、**Main Server IP Address**の入力フィールドに変更したメインサーバー

のIPアドレスを入力してください。



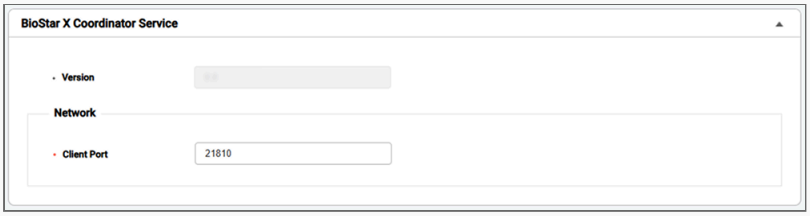
4. メインサーバーのポート番号が既定値(21810)と異なる場合は、**BioStar X Coordinator Service Port** フィールドに変更したポート番号を入力してください。
5. **Enroll** ボタンをクリックしてください。

メインサーバーのIPアドレス変更が完了すると、成功メッセージが表示されます。



情報

- マルチコミュニケーションサーバーをインストールしていない場合は、この手順をスキップしてください。
- BioStar Xをインストールしたメインサーバーのポート番号を変更した場合は、メインサーバーで **BioStar X Service Manager** を起動し、**SERVICE SETTINGS** → **BioStar X Coordinator Service** セクションの **Client Port** 値を確認してください。

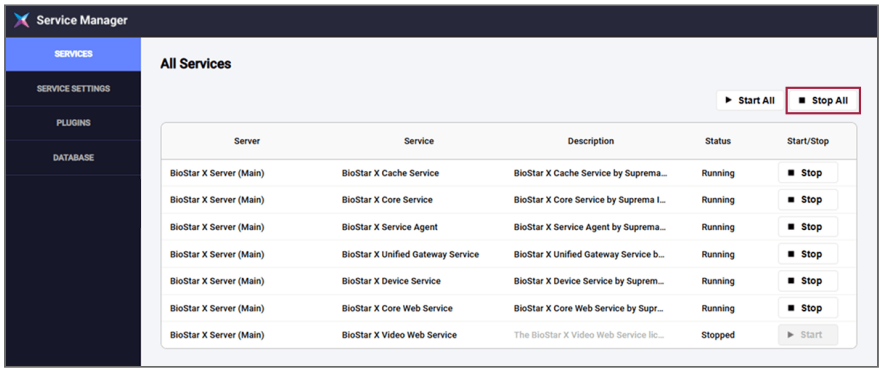


- マルチ通信サーバーのインストールの詳細についてはマルチコミュニケーションサーバーをインストールするをご参照ください。

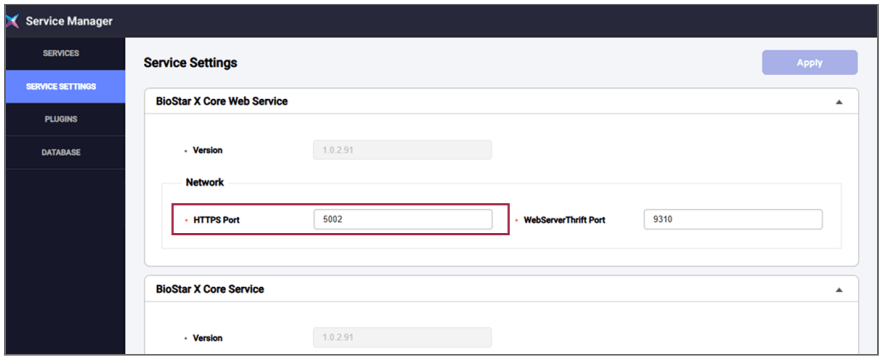
ポートを変更する

BioStar X の既定ポート (443) を使用できない場合にポートを変更する方法を説明します。

1. Windows で 開始 → **BioStar X** → **BioStar X Service Manager** をクリックします。
2. Web ブラウザーで **BioStar X Service Manager** ウィンドウが表示されたら、**SERVICES** メニューをクリックします。
3. すべてのサービスを終了するには、画面右上にある **Stop All** ボタンをクリックしてください。



4. 画面左のサイドバーで **SERVICE SETTINGS** をクリックします。
5. **Unified Gateway Service** セクションの **HTTPS Port** フィールドに変更するポート番号を入力します。



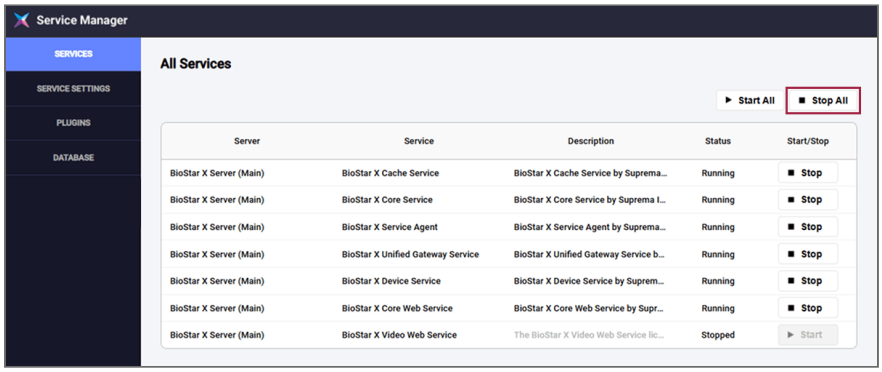
6. 画面右上の **Apply** をクリックします。
7. 確認メッセージが表示されたら **OK** をクリックします。
8. **SERVICES** に移動し、すべてのサービスで **Start** をクリックします。
9. ウェブブラウザーで **BioStar X** にアクセスします。

> **情報**
>
> - ポート番号を 450 に変更した場合は、アドレスバーに `https://{ip_address}:450` と入力します。
> - 一部のサービスではポートの変更に対応していない場合があります。

データベースを変更する

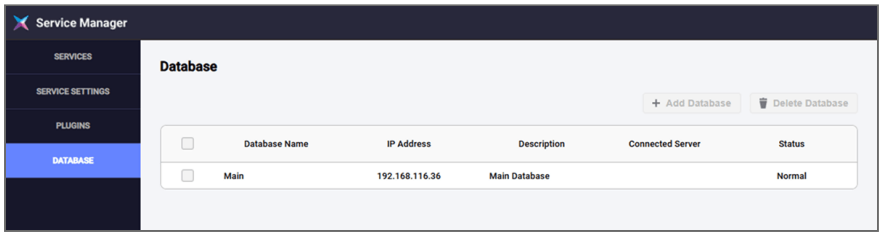
データベースの設定を変更できます。

1. Windows で 開始 → **BioStar X** → **BioStar X Service Manager** をクリックします。
2. Web ブラウザーで **BioStar X Service Manager** ウィンドウが表示されたら、**SERVICES** メニューをクリックします。
3. すべてのサービスで **Stop** ボタンをクリックします。

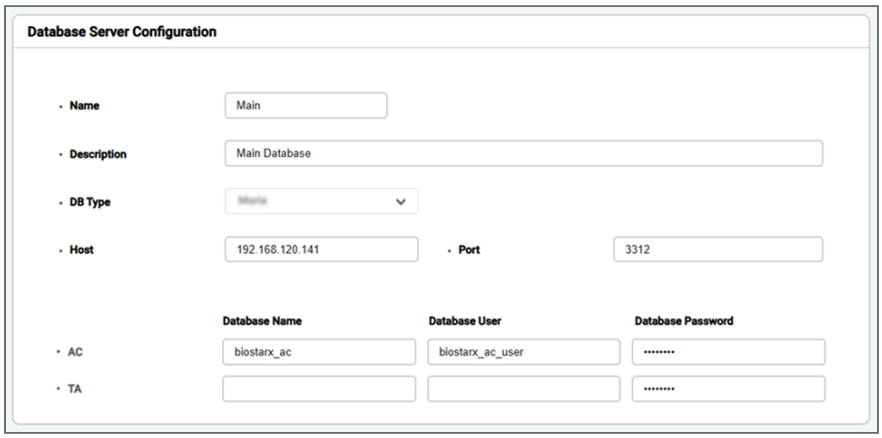


> すべてのサービスを一度に停止するには、**Stop All** ボタンをクリックします。

4. 画面左側のサイドバーで **DATABASE** メニューをクリックします。



5. データベース一覧から、設定を変更するデータベースを選択します。
6. **Database Server Configuration** セクションで以下の設定を変更できます。



- **Name**：データベース名を入力します。
- **Description**：データベースの説明を入力します。
- **DB Type**：データベースの種類を選択します。（MariaDB, MS SQL）
- **Host**：データベースサーバーのホスト名または IP アドレスを入力します。
- **Port**：データベースサーバーのポート番号を入力します。
- **AC** / **TA** / **Video**：AC、TA、Video データベースの名前、ユーザー、パスワードを入力します。

7. データベースが正常に接続されているか確認するには、画面右上の **Test Connection** ボタンをクリックします。
8. 設定を保存するには、画面右上の **Save** ボタンをクリックします。

補助データベースを追加する

マルチ通信サーバーを追加した際にメインサーバーの負荷を軽減するため、マルチ通信サーバーと連携する補助データベースを追加して接続する方法を説明します。

> **情報**
>
> - 補助データベースを追加するには **マルチ通信サーバー** 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。
> - マルチ通信サーバーのインストールの詳細についてはマルチコミュニケーションサーバーをインストールするをご参照ください。

開始する前に

MariaDB を使用する環境でデータベース間通信に IP アドレスではなくドメインまたはホスト名を使用する場合は、次の案内事項を必ず確認してください。

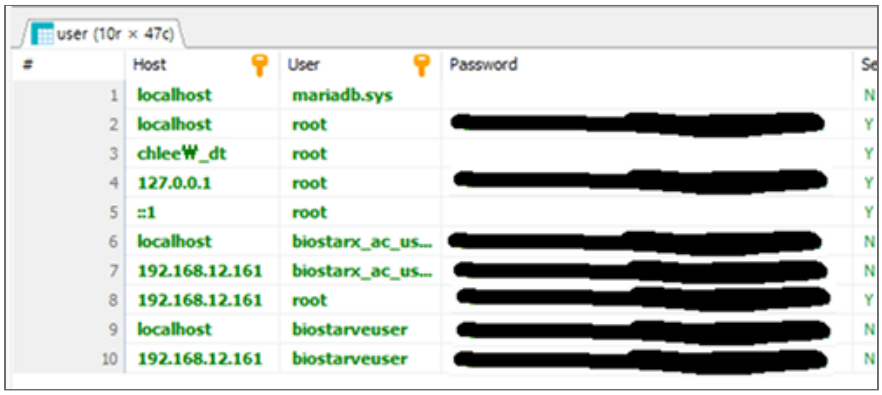
- IP アドレスを使用しない場合、`CREATE USER` または `GRANT` の登録ができない可能性があります。
- ドメインまたはホスト名で通信する場合は、必ず localhost に対してユーザーと権限が登録されていることを確認してください。
- BioStar X を簡易インストール方式でインストールした場合、root アカウントは localhost のみユーザーと権限が登録されているため、当該サーバーの IP アドレスまたは *127.0.0.1* で追加登録する必要があります。

登録方法

ホストが *127.0.0.1* でユーザーが root のアカウントにパスワードが設定されているか確認し、設定されていない場合は必ずパスワードを設定して権限を付与してください。

1. ホストが *127.0.0.1* でユーザーが root のアカウントにパスワードが設定されているか確認してください。

```
SELECT * FROM mysql.user;
```



空欄であればパスワードが設定されていないため、次の項目にあるクエリを実行してパスワードの追加と権限付与を必ず行ってください。

2. ホストが *127.0.0.1* でユーザーが root のアカウントにパスワードを設定し、権限を付与してください。

```
ALTER USER 'root'@'127.0.0.1' IDENTIFIED BY '<Main DB AC Schema Password>';
GRANT ALL PRIVILEGES ON *.* TO 'root'@'127.0.0.1';

CREATE USER '<Main DB AC User>'@'127.0.0.1' IDENTIFIED BY '<Main DB AC Schema Password>';
GRANT ALL PRIVILEGES ON *.* TO '<Main DB AC User>'@'127.0.0.1';
CREATE USER '<Main DB AC User>'@'::1' IDENTIFIED BY '<Main DB AC Schema Password>';
GRANT ALL PRIVILEGES ON *.* TO '<Main DB AC User>'@'::1';

CREATE USER '<Main DB TA User>'@'127.0.0.1' IDENTIFIED BY '<Main DB AC Schema Password>';
GRANT ALL PRIVILEGES ON *.* TO '<Main DB TA User>'@'127.0.0.1';
CREATE USER '<Main DB TA User>'@'::1' IDENTIFIED BY '<Main DB AC Schema Password>';
GRANT ALL PRIVILEGES ON *.* TO '<Main DB TA User>'@'::1';

CREATE USER '<Main DB VE User>'@'127.0.0.1' IDENTIFIED BY '<Main DB AC Schema Password>';
GRANT ALL PRIVILEGES ON *.* TO '<Main DB VE User>'@'127.0.0.1';
CREATE USER '<Main DB VE User>'@'::1' IDENTIFIED BY '<Main DB AC Schema Password>';
GRANT ALL PRIVILEGES ON *.* TO '<Main DB VE User>'@'::1';

FLUSH PRIVILEGES;
```

Example

```
ALTER USER 'root'@'127.0.0.1' IDENTIFIED BY 'admin1234!';
GRANT ALL PRIVILEGES ON *.* TO 'root'@'127.0.0.1';
FLUSH PRIVILEGES;
```

IP アドレスで通信を設定

以下の設定により、強制的に IP アドレスで通信するように設定できます。

1. **BioStar X** をインストールした後、次のパスに移動してください。

   > *C:\Program Files\BioStar X\ta\mariadb-11.4.4-winx64*

2. *my.cnf* ファイルを管理者権限で開き、[mysqld] セクションに `skip-name-resolve` オプションを追加してください。

```
[mysqld]
port = 3312
character-set-server=utf8
collation-server=utf8_unicode_ci
socket = /tmp/mysql.sock
skip-external-locking
key_buffer_size = 32M
max_allowed_packet = 64M
...
skip-name-resolve
```

3. MariaDB サービスを再起動してください。

補助データベースを追加

補助データベースを追加する方法を説明します。使用するデータベースの種類に応じて、MariaDB と SQL Server の 2 通りの方法があります。

MariaDB

1 メインデータベース

新しい補助データベースからメインデータベースへアクセスできるように、アカウントと権限を付与してください。

```
CREATE USER '<Main DB AC Schema User>'@'<Sub DB IP>' IDENTIFIED BY '<Main DB AC Schema Password>';

GRANT ALL PRIVILEGES ON <Main DB AC Schema>.* TO '<Main DB AC Schema User>'@'<Sub DB IP>';
FLUSH PRIVILEGES;
```

Example

```
CREATE USER 'biostarx_ac_user'@'192.168.12.42' IDENTIFIED BY 'password';

GRANT ALL PRIVILEGES ON biostar2_ac.* TO 'biostarx_ac_user'@'192.168.12.42';
FLUSH PRIVILEGES;
```

2 補助データベース

メインデータベースから新しい補助データベースへアクセスできるように、アカウントと権限を付与してください。

```
CREATE USER '<Sub DB AC Schema User>'@'<Main DB IP>' IDENTIFIED BY '<Sub DB AC Schema Password>';

GRANT ALL PRIVILEGES ON <Sub DB AC Schema>.* TO '<Sub DB AC Schema User>'@'<Main DB IP>';
FLUSH PRIVILEGES;
```

Example

```
CREATE USER 'biostarx_ac_user'@'192.168.12.161' IDENTIFIED BY 'password';

GRANT ALL PRIVILEGES ON biostar2_ac.* TO 'biostarx_ac_user'@'192.168.12.161';
FLUSH PRIVILEGES;
```

3 FederatedX 使用状況の確認

メインおよび補助データベースで以下のコマンドを実行し、FederatedX ストレージエンジンが有効になっているか確認してください。

```
SHOW ENGINES;
```

クエリ結果に `Engine : FEDERATED, Support : YES` と表示されれば、すでにインストールされています。 FederatedX ストレージエンジンがインストールされていない場合は、以下のクエリを実行してください。

```
INSTALL PLUGIN federated SONAME 'ha_federatedx';
```

> **情報**
> MariaDB をインストールしたパス配下の *lib/plugin* フォルダーに *ha_federatedx.dll* ファイルがあるか確認してください。通常、*C:\Program Files\MariaDB {version}\lib\plugin* パスに dll ファイルが存在します。

4 サーバーエイリアスの登録

補助データベースに作成される FederatedX テーブルがメインデータベースの元テーブルにアクセスできるように、サーバーエイリアス(alias)を登録してください。

```
CREATE SERVER 'default' FOREIGN DATA WRAPPER mysql OPTIONS (HOST '<Main DB IP>', PORT <Main DB PORT>, DATABASE '<Main DB AC Schema>', USER '<Main DB AC USER>', PASSWORD '<Main DB AC USER Password>');

-- 登録が正常に行われたことを確認
SELECT * FROM mysql.servers;
```

既に登録したサーバー名の Host、Port、DB、User、Password の情報を変更する必要がある場合は、`ALTER` 文で修正できます。一部の情報のみを変更することもできます。

```
ALTER SERVER 'default' OPTIONS (HOST '<Main DB IP>', PORT <Main DB PORT>, DATABASE '<Main DB AC Schema>', USER '<Main DB AC USER>', PASSWORD '<Main DB AC USER Password>');
```

Example

```
CREATE SERVER 'default' FOREIGN DATA WRAPPER mysql OPTIONS (HOST '192.168.12.161', PORT 3312, DATABASE 'biostar2_ac', USER 'biostarx_ac_user', PASSWORD 'password');

ALTER SERVER 'default' OPTIONS (HOST '192.168.12.161', PORT 3312, DATABASE 'biostar2_ac', USER 'biostarx_ac_usermt__fttid__', PASSWORD 'password');
```

5 テーブルリンクの設定

補助データベースに必要なテーブルは、以下の順序で進めてメインデータベースのテーブルを補助データベースにリンク設定してください。

- 以下はメインデータベースで `CREATE TABLE` 文を生成するクエリです。

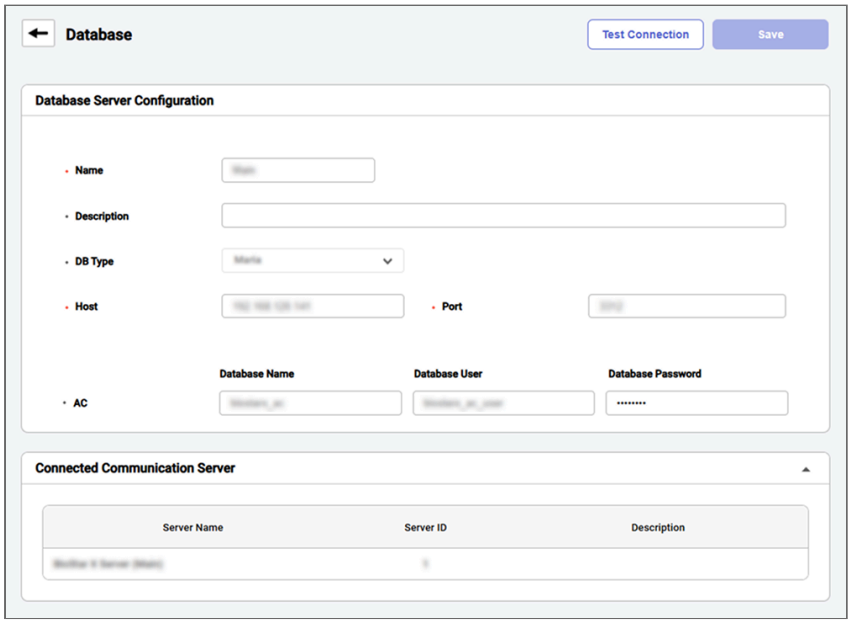
```
select
  concat(
     'CREATE TABLE IF NOT EXISTS <SubDB_AC_Database_Schema>.', table_name,
     ' ENGINE=FEDERATED ',
     'CONNECTION="default/', table_name, '";'
  ) as create_table_sql
from information_schema.TABLES
where TABLE_SCHEMA = '<MainDB_AC_Database_Schema>'
    AND TABLE_TYPE = 'BASE TABLE'
    AND NOT TABLE_NAME REGEXP '^t_lg[0-9]{6}$'
    AND NOT TABLE_NAME REGEXP '^t_almevt[0-9]{6}$'
    AND NOT TABLE_NAME REGEXP '^t_lgalmtrstrc[0-9]{6}$'
ORDER BY TABLE_NAME;
```

情報

FederatedX の特性上、`Table_type` は 'BASE TABLE' に設定することを推奨します。 `VIEW` タイプも可能ですが、推奨しません。

6 Service Manager 設定

1. **BioStar X Service Manager** を実行してください。 （開始 → **BioStar X** → **BioStar X Service Manager**）
2. 画面左側のサイドバーで **DATABASE** メニューをクリックします。
3. 画面右上の **+ Add Database** ボタンをクリックしてください。
4. データベース追加画面で各項目を入力してください。



- **Name**：データベース名を入力します。
- **Description**：データベースの説明を入力します。
- **DB Type**：データベースの種類を選択します。 （MariaDB, MS SQL）

- **Host**：データベースサーバーのホスト名または IP アドレスを入力します。
- **Port**：データベースサーバーのポート番号を入力します。
- **AC** / **TA**：AC、TA データベースの名前、ユーザー、パスワードを入力してください。

5. データベースが正常に接続されているか確認するには、画面右上の **Test Connection** ボタンをクリックします。
6. 設定を保存するには、画面右上の **Save** ボタンをクリックします。

SQL Server

1 メインデータベース権限付与

sysadmin 権限を持つアカウントでメインデータベースに以下の権限を付与してください。

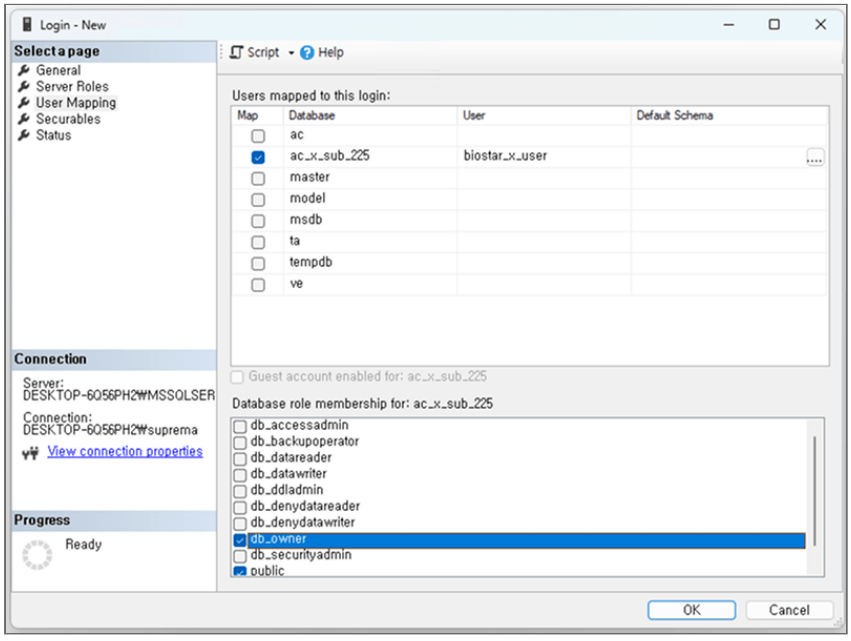
```
GRANT ALTER ANY LINKED SERVER TO [<MAIN DATABASE AC USER>];
GRANT ALTER ANY LOGIN TO [<MAIN DATABASE AC USER>];
```

Example

```
GRANT ALTER ANY LINKED SERVER TO [biostar_x_user];
GRANT ALTER ANY LOGIN TO [biostar_x_user];
```

2 補助データベース権限付与

1. sysadmin 権限を持つアカウントで補助データベースにテーブルおよびユーザーの User Mapping 接続が必要です。このとき `db_owner` ロールの追加が必要です。



2. 追加するデータベースに以下の権限を付与します。

```
GRANT ALTER ANY LINKED SERVER TO [<SUB DATABASE AC USER>];
GRANT ALTER ANY LOGIN TO [<SUB DATABASE AC USER>];
```

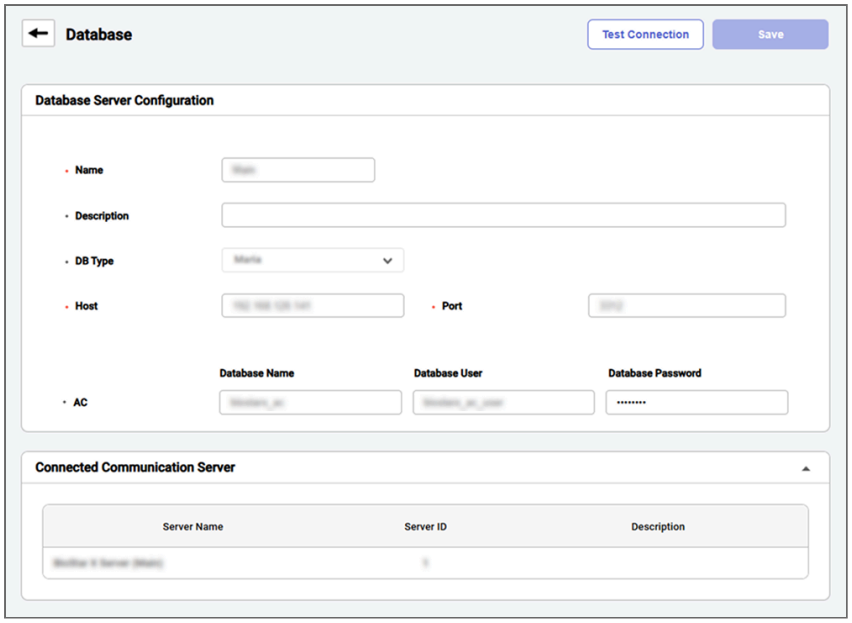
Example

```
GRANT ALTER ANY LINKED SERVER TO [biostar_x_user_sub];
GRANT ALTER ANY LOGIN TO [biostar_x_user_sub];
```

3 Service Manager 設定

BioStar X Service Manager で補助データベースを追加します。

1. BioStar X Service Manager を実行してください。（開始 → BioStar X → BioStar X Service Manager）
2. 画面左側のサイドバーで **DATABASE** メニューをクリックします。
3. 画面右上の **+ Add Database** ボタンをクリックしてください。
4. データベース追加画面で各項目を入力してください。



- **Name**：データベース名を入力します。
- **Description**：データベースの説明を入力します。
- **DB Type**：データベースの種類を選択します。（MariaDB, MS SQL）
- **Host**：データベースサーバーのホスト名または IP アドレスを入力します。
- **Port**：データベースサーバーのポート番号を入力します。
- **AC** / **TA**：AC、TA データベースの名前、ユーザー、パスワードを入力してください。

5. データベースが正常に接続されているか確認するには、画面右上の **Test Connection** ボタンをクリックします。
6. 設定を保存するには、画面右上の **Save** ボタンをクリックします。

情報

- 設定を完了すると、メインデータベースと補助データベースそれぞれに Linked Server 設定が自動で実行されます。
- データベース情報を修正する際も、Linked Server 設定は自動で更新されます。メインデータベースを修正すると、登録されているすべての補助データベースに対して Linked Server 設定が変更内容で反映されます。補助データベースを修正すると、メインデータベースとその補助データベースのみに変更内容が反映されます。

4 Linked Temp Table クエリの生成

メインデータベースで次のクエリを実行し、補助データベースに作成する Linked Temp Table 用クエリを生成します。

```
USE [<AC Schema>];
GO
DECLARE @LinkedServer  sysname = N'default';
DECLARE @SourceSchema  sysname = N'dbo';
DECLARE @TargetSchema  sysname = N'dbo';

SELECT
    'IF OBJECT_ID(N''' + QUOTENAME(@TargetSchema,'') + '.' + QUOTENAME(t.name,'') + ''', ''SN'') IS NOT NULL '
  + 'DROP SYNONYM ' + QUOTENAME(@TargetSchema) + '.' + QUOTENAME(t.name) + ';'
  + 'CREATE SYNONYM ' + QUOTENAME(@TargetSchema) + '.' + QUOTENAME(t.name)
  + ' FOR ' + QUOTENAME(@LinkedServer) + '.' + QUOTENAME(DB_NAME()) + '.' + QUOTENAME(s.name) + '.' + QUOTENAME(t.name) + ';'
  AS recreate_synonym_sql
FROM sys.tables AS t
JOIN sys.schemas AS s
  ON s.schema_id = t.schema_id
WHERE s.name = @SourceSchema
  AND t.is_ms_shipped = 0
  AND t.name NOT LIKE 't_lg[0-9][0-9][0-9][0-9][0-9]'
  AND t.name NOT LIKE 't_almevt[0-9][0-9][0-9][0-9][0-9]'
  AND t.name NOT LIKE 't_lgalmtrstrc[0-9][0-9][0-9][0-9][0-9]'
ORDER BY t.name;
```

Example

```
-- 例
USE [main_ac_x_215];
GO
DECLARE @LinkedServer  sysname = N'default';  -- Linked Server name set in the sub DB
DECLARE @SourceSchema  sysname = N'dbo';      -- Schema to target in the main DB
DECLARE @TargetSchema  sysname = N'dbo';      -- Schema to create synonyms in the sub DB (reflected in the output string)

SELECT
    'IF OBJECT_ID(N''' + QUOTENAME(@TargetSchema,'') + '.' + QUOTENAME(t.name,'') + ''', ''SN'') IS NOT NULL '
  + 'DROP SYNONYM ' + QUOTENAME(@TargetSchema) + '.' + QUOTENAME(t.name) + ';'
  + 'CREATE SYNONYM ' + QUOTENAME(@TargetSchema) + '.' + QUOTENAME(t.name)
  + ' FOR ' + QUOTENAME(@LinkedServer) + '.' + QUOTENAME(DB_NAME()) + '.' + QUOTENAME(s.name) + '.' + QUOTENAME(t.name) + ';'
  AS recreate_synonym_sql
FROM sys.tables AS t
JOIN sys.schemas AS s
  ON s.schema_id = t.schema_id
WHERE s.name = @SourceSchema
  AND t.is_ms_shipped = 0
  AND t.name NOT LIKE 't_lg[0-9][0-9][0-9][0-9][0-9][0-9]'
  AND t.name NOT LIKE 't_almevt[0-9][0-9][0-9][0-9][0-9][0-9]'
  AND t.name NOT LIKE 't_lgalmtrstrc[0-9][0-9][0-9][0-9][0-9][0-9]'
ORDER BY t.name;
```

5 補助データベースでクエリを実行

先ほど生成した `CREATE SYNONYM` クエリをすべてコピーします。追加する補助データベースサーバーに接続し、以下のようにクエリを作成して実行します。補助データベースの AC スキーマ内の Synonyms に保存されます。

```
use [<Sub DB AC Database>];

IF OBJECT_ID(N'[dbo].[T_ACSGR]', 'SN') IS NOT NULL DROP SYNONYM [dbo].[T_ACSGR];CREATE SYNONYM [dbo].[T_ACSGR] FOR
[default].[main_ac_x_215].[dbo].[T_ACSGR];
IF OBJECT_ID(N'[dbo].[T_ACSGRLVLS]', 'SN') IS NOT NULL DROP SYNONYM [dbo].[T_ACSGRLVLS];CREATE SYNONYM [dbo].[T_ACSGRLVLS]
FOR [default].[main_ac_x_215].[dbo].[T_ACSGRLVLS];
IF OBJECT_ID(N'[dbo].[T_ACSGRSENT]', 'SN') IS NOT NULL DROP SYNONYM [dbo].[T_ACSGRSENT];CREATE SYNONYM
[dbo].[T_ACSGRSENT] FOR [default].[main_ac_x_215].[dbo].[T_ACSGRSENT];
IF OBJECT_ID(N'[dbo].[T_ACSGRUSS]', 'SN') IS NOT NULL DROP SYNONYM [dbo].[T_ACSGRUSS];CREATE SYNONYM [dbo].[T_ACSGRUSS]
FOR [default].[main_ac_x_215].[dbo].[T_ACSGRUSS];
...
```

BioStar Xサーバーのアンインストールとセキュリティ証明書の復元

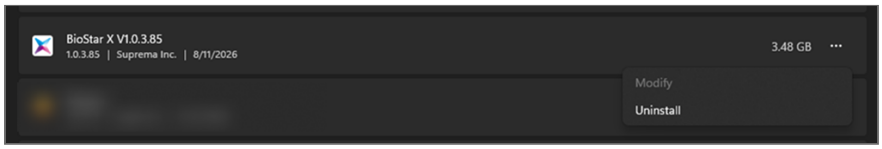
コンピューターから **BioStar X** サーバーをアンインストールする手順を説明します。 **Secure communication with device** オプションを使用していない場合、証明書のバックアップと復元を行わずにアンインストールを進めてください。

Secure communication with device オプションを使用している場合、**BioStar X** をアンインストールする前に、サーバーのセキュリティ証明書セット（ルートCA／サーバー証明書／キー）を必ずバックアップしてください。このバックアップは、同じサーバーを再インストールした後に既存デバイスを再接続する唯一の復元手段です。システムが提供する復元機能と異なり、データベースや設定は保持したままセキュア通信証明書のみを再利用する場合は、バックアップしたセキュア通信証明書の復元を参照してください。

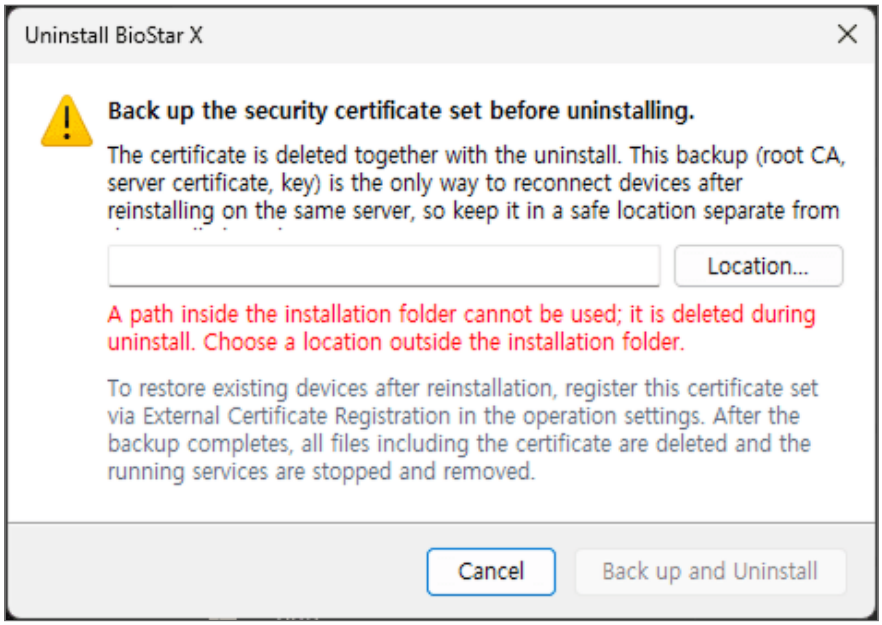
BioStar Xサーバーのアンインストール

> **注意**
> BioStar X をアンインストールすると、証明書を含むインストールファイルがすべて削除され、コンテンツ（ユーザー情報）も削除される場合があります。データベース、設定、キーなどを保持するには、アンインストールの前にシステムをバックアップするを参照し、先にシステムをバックアップしてください。

1. Windowsで **設定** → **アプリ** → **インストールされているアプリ** に移動してください。
2. 一覧で **BioStar X** を探し、••• ボタンをクリックして **アンインストール** を選択してください。

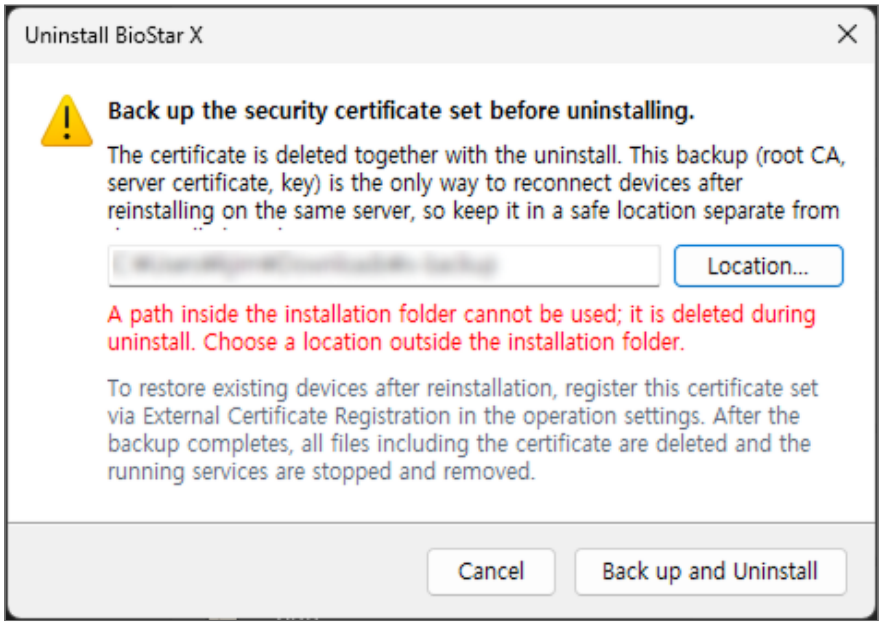


3. **Secure communication with device** オプションを使用している場合、証明書バックアップの案内ウィンドウが表示されます。**参照...** ボタンをクリックし、バックアップ先のパスを指定してください。このオプションを使用していない場合、証明書のバックアップ手順なしで手順7に進みます。

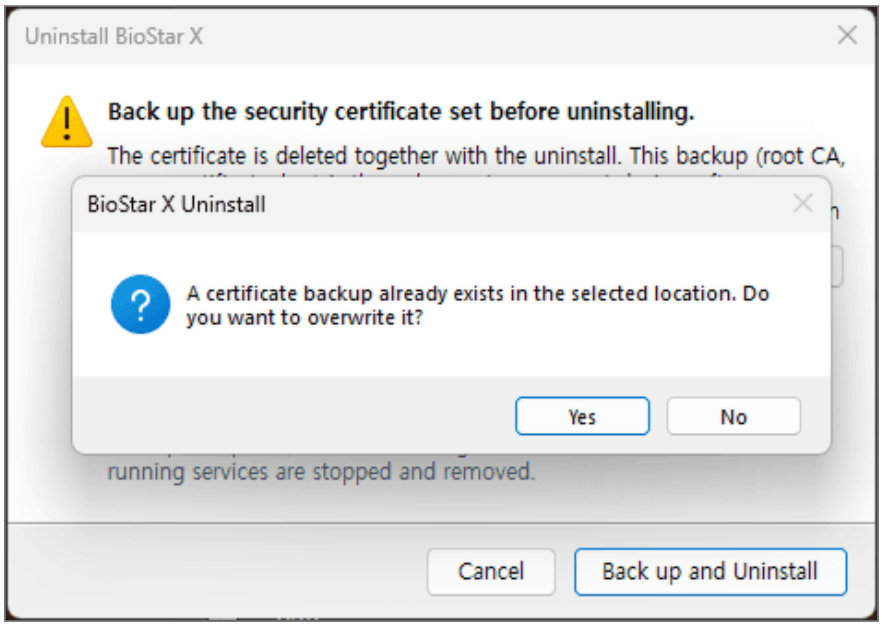


> **注意**
> BioStar X のインストールパスはバックアップ先として使用できません。アンインストール時に BioStar X のインストールフォルダーと一緒に削除されるためです。必ず BioStar X のインストールパス以外を指定してください。

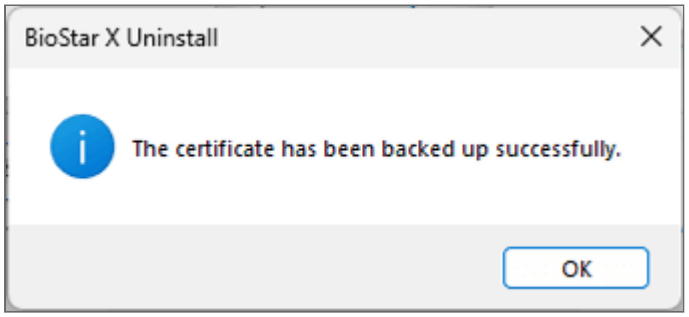
4. パスを指定し、**バックアップしてアンインストール** ボタンが有効になったらクリックしてください。



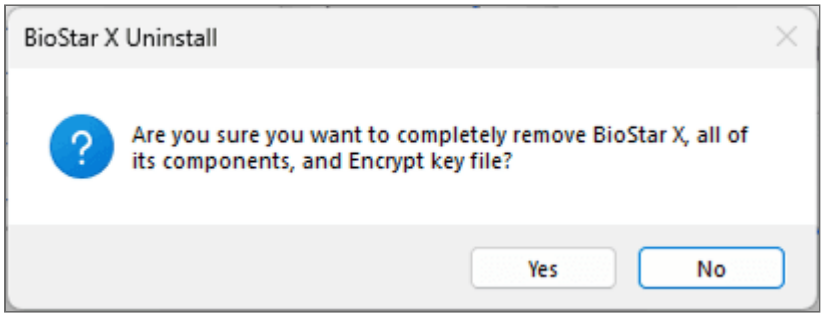
5. 指定した場所にすでに証明書のバックアップファイルがある場合、上書きするか確認するウィンドウが表示されます。既存のバックアップを上書きする場合は **はい**、別のパスを再指定する場合は **いいえ** をクリックしてください。



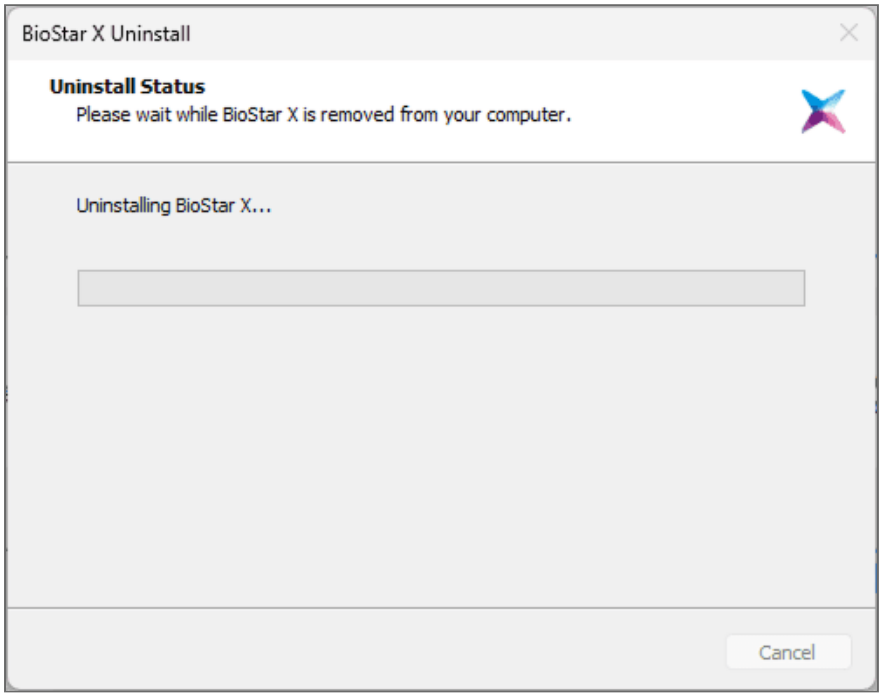
6. 証明書のバックアップが完了すると、案内ウィンドウが表示されます。 **OK** をクリックしてください。



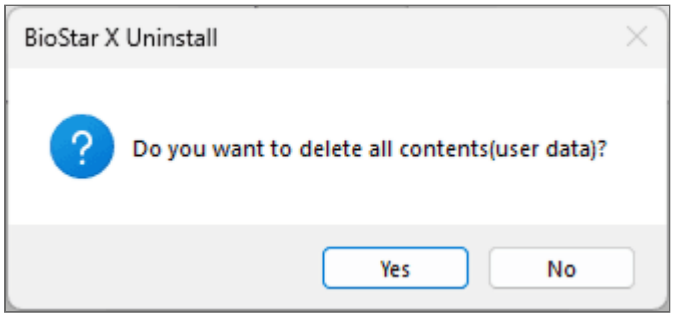
7. **BioStar X** と関連コンポーネントをすべてアンインストールするか確認するウィンドウが表示されたら、**はい** をクリックしてください。



8. アンインストールが完了するまで待ってください。

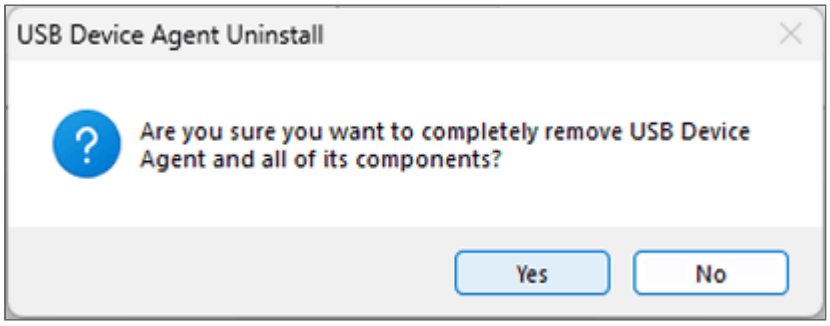


9. すべてのコンテンツ（ユーザー情報）を削除するか確認するウィンドウが表示されます。データベースに保存されたユーザー情報もすべて削除する場合は **はい** を、残す場合は **いいえ** をクリックしてください。



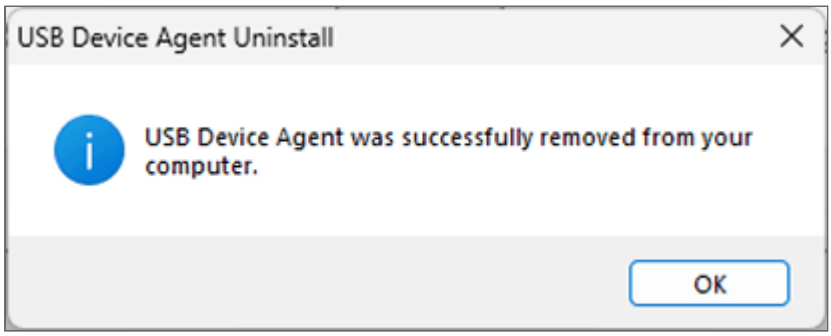
> **注意**
> **はい** をクリックすると、データベースに保存されたユーザー情報を含むすべてのデータが削除され、復元できません。データを保持する必要がある場合は **いいえ** をクリックするか、削除する前に システムをバックアップする を参照してシステムを先にバックアップしてください。

10. **USB Device Agent** がインストールされている場合、一緒に削除するか確認する画面が表示されます。**はい** をクリックしてください。

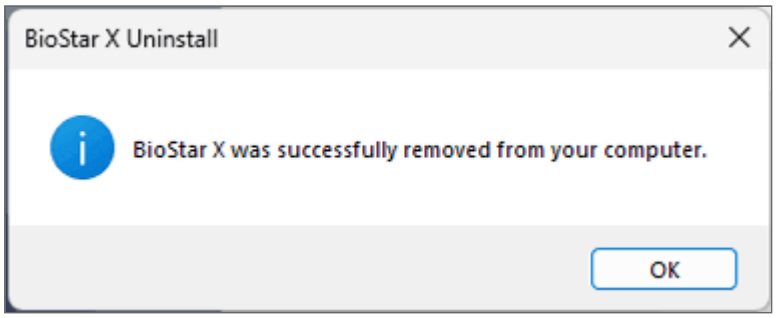


使用中のコンポーネントによっては、関連ドライバーの削除画面が追加で表示されることがあります。画面の指示に従って削除を完了してください。

11. コンポーネントの削除が完了すると、案内画面が表示されます。 **OK** をクリックしてください。



12. **BioStar X** の削除が完了すると、案内画面が表示されます。 **OK** をクリックしてください。



バックアップしたセキュア通信証明書の復元

Secure communication with device オプションを使用していたサーバーを再インストールした後、既存のデバイスを再接続するには、セキュア通信証明書を復元する必要があります。システム復元ツール は、データベースと設定を含むシステム全体を以前の状態に戻します。この手順は、システムを復元せずにセキュア通信証明書だけを再利用する場合に使用します。専用ツールを使わず、バックアップした証明書ファイルをインストールパスに直接復元する必要があります。

情報

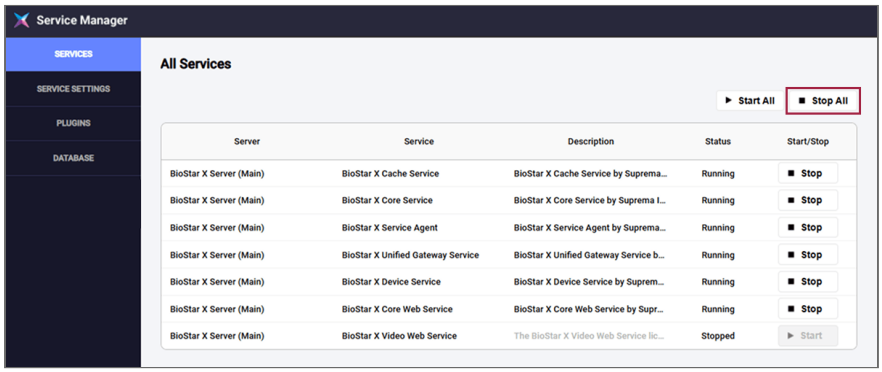
メインサーバーとマルチコミュニケーションサーバーで構成された環境では、各サーバーが個別のセキュア通信証明書を使用します。証明書を復元した後にマルチコミュニケーションサーバーをインストールして追加すると、マルチコミュニケーションサーバーの証明書が自動でコピーされるため、個別に復元する必要はありません。

1. **BioStar X** を新しくインストールしてください。インストール方法は 簡単インストール または カスタムインストールを実行する をご参照ください。

2. **BioStar X** のインストール完了後、Windows で 開始 → **BioStar X** → **BioStar X Service Manager** をクリックしてください。

3. Web ブラウザーで **BioStar X Service Manager** ウィンドウが表示されたら、**SERVICES** メニューをクリックします。

4. すべてのサービスを終了するには、画面右上にある **Stop All** ボタンをクリックしてください。



5. バックアップした証明書ファイル（ルート CA、サーバー証明書、キー）をすべて、**BioStar X** のインストールパス配下の *cert* フォルダーにコピーしてください。

   > *例: C:\Program Files\BioStar X\cert*

   > 新規インストール時に自動生成された証明書ファイルと名前が同じです。上書きするか確認する画面が表示されたら、**はい** をクリックして既存ファイルを上書きしてください。

6. **SERVICES** メニューで全サービスを再起動するには、**Start All** ボタンをクリックしてください。

7. マルチコミュニケーションサーバーを使用する場合は、別の環境にマルチコミュニケーションサーバーをインストールしてください。インストール方法は マルチコミュニケーションサーバーをインストールする をご参照ください。

8. メインサーバーの **BioStar X Service Manager** でマルチコミュニケーションサーバーを追加してください。追加方法は マルチコミュニケーションサーバーをインストールする をご参照ください。

マルチコミュニケーションサーバーを追加すると、メインサーバーの *cert* フォルダにあるセキュリティ証明書ファイルがマルチコミュニケーションサーバーに自動でコピーされます。

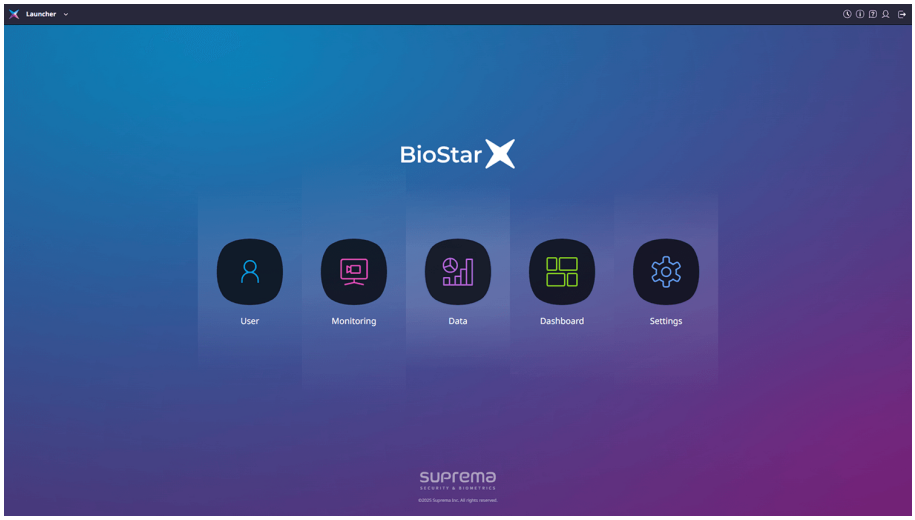
> **注意**
> 証明書を復元する前（手順4\~6の前）にマルチコミュニケーションサーバーを先にインストールして追加した場合、マルチコミュニケーションサーバーには復元前の証明書がすでにコピーされています。この場合、以下の手順に従ってマルチコミュニケーションサーバーの証明書も個別に交換してください。
>
> 1. マルチコミュニケーションサーバーをインストールした環境で **BioStar X Service Manager** を実行し、すべてのサービスを停止してください。
> 2. バックアップした証明書ファイルを、マルチコミュニケーションサーバーのインストールパス配下の *cert* フォルダに同じようにコピーしてください。
>
>   > *例: C:\Program Files\BioStar X Communications Server\cert*
>
> 3. メインサーバーとマルチコミュニケーションサーバーの両方で、**BioStar X Service Manager** を使用してすべてのサービスを再起動してください。

情報

- BioStar X Service Manager の使用方法の詳細については サーバーの起動と停止 をご参照ください。
- **Secure communication with device** オプションの詳細については、システムセキュリティを強化するをご参照ください。
- マルチコミュニケーションサーバーをインストールして接続するには、マルチコミュニケーションサーバー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。

ランチャー

Launcher ページは、ログイン後に最初に表示される **BioStar X** のスタートページであり、ユーザーが **BioStar X** の主要機能にアクセスするための中心的なハブとして機能します。このページは、ユーザーが **BioStar X** のすべての機能を簡単に探索して利用できるように設計されています。ランチャーページの UI 構成要素は次のとおりです。



Launcher ページでは、**User**、**Monitoring**、**Data**、**Dashboard**、**Settings** ページへのリンクが提供されます。

- **User**：ユーザーグループ管理、ユーザー管理、ユーザーテンプレート管理、入退室権限別ユーザー確認など、さまざまな機能を通じてユーザーを効率的に管理し、権限によってセキュリティを強化できます。詳細については、ユーザーを参照してください。
- **Monitoring**：ドア、デバイス、ビデオ、イベントを多様な方法で監視します。関連機能を制御し、リアルタイム映像で監視できます。詳細については、モニタリングを参照してください。
- **Data**：ユーザー情報や希望の条件のイベントを照会でき、レポートを一定の周期で生成できます。詳細については、データを参照してください。
- **Dashboard**：**BioStar X** が提供する多様なデータを利用して、ユーザーが選択したデータに基づくウィジェットを追加・配置し、希望のダッシュボードを構築できます。詳細については、ダッシュボードを参照してください。
- **Settings**：デバイスおよび入退室制御、ユーザーごとの権限、言語、時刻などの多様な設定を通じて、ユーザー環境に最適化された **BioStar X** を構成できます。詳細については、設定を参照してください。

情報

- 画面上部ヘッダー領域の詳細については、共通 UI を理解するを参照してください。
- 画面下部では、プラグインを追加してインストールした機能を利用できます。プラグイン機能を使用するには、プラグインライセンスが必要です。
  - プラグインの使用に関する詳細は、プラグインを参照してください。
  - 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。

ユーザー

BioStar X の主要機能の 1 つである User ページで利用できるさまざまな機能について説明します。このページでは、ユーザーグループ管理、ユーザー管理、ユーザーテンプレート管理、入退室権限別ユーザー確認など、多様な機能を活用してユーザーを効率的に管理し、権限によってセキュリティを強化する方法を紹介します。各機能を活用して BioStar X をさらに効果的に利用しましょう。

Launcher ページで User をクリックするか、画面左上のショートカットリストから User を選択します。

ユーザーグループを管理する

ユーザーグループは共通の属性と権限を共有できます。ユーザーがグループのメンバーになると、そのグループのすべての属性を自動で継承できます。ユーザーは 1 つのユーザーグループにのみ所属できます。

- 個々のユーザーごとに入退室権限を設定する代わりに、部署別または役割別のユーザーグループを作成して同一の権限を一括で適用できます。
- グループの入退室権限を修正すると、そのグループに属するすべてのユーザーに自動適用されるため、管理者の負担を軽減できます。組織変更や新規プロジェクト発生時に迅速に権限を調整できます。
- グループ別の権限設定によって不要な入退室を防ぎ、セキュリティを向上できます。
- 特定グループの入退室記録を個別に分析できるため、セキュリティ監査とログ管理が容易になります。
- ユーザーグループは入退室グレードと連携し、入退室制限時間や制限区域などの詳細ポリシーを適用できます。

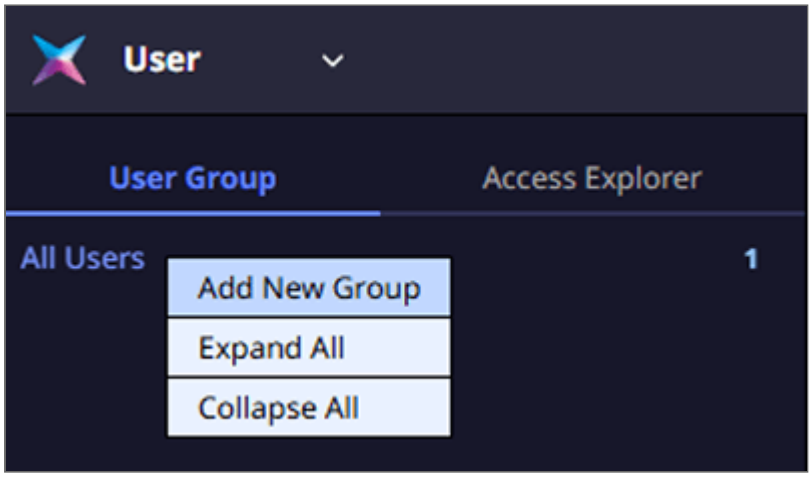
グループの追加

複数のユーザーを効率的に管理するためにグループを作成します。ユーザーが所属する組織などの名前で登録すると便利に管理できます。

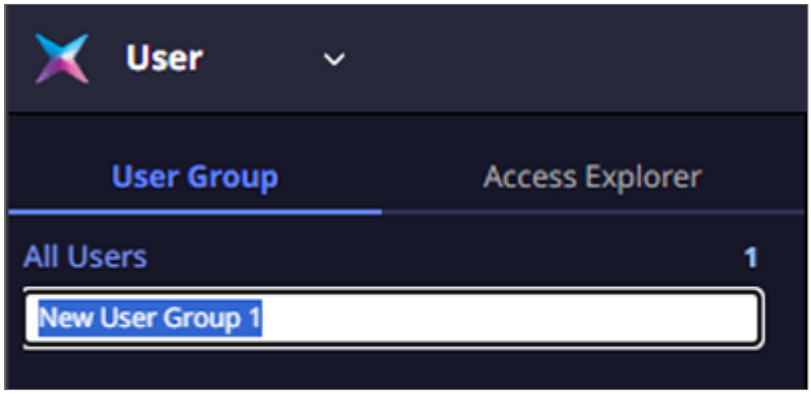
> **情報**
>
> - グループ名はユーザーが所属する組織または部署名で登録すると管理が容易です。
> - グループの下位グループは最大 8 階層まで順に作成できます。
> - ユーザーグループ名は最大 48 文字まで入力できます。
> - ユーザーグループ一覧でグループを選択すると、そのグループに属するユーザーだけをユーザー一覧に表示できます。

最上位グループの作成

1. Launcher ページで User をクリックします。
2. 画面左側サイドバーの User Group タブで All Users を選択し、右クリックします。

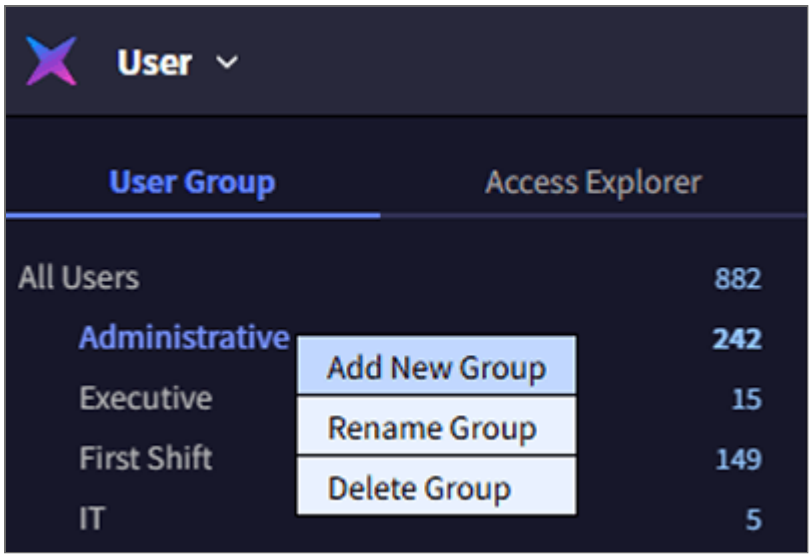


3. ポップアップメニューで **Add New Group** をクリックします。
4. グループが作成されたら、目的のグループ名を入力します。



下位グループの作成

1. 画面左側サイドバーの **User Group** タブで上位グループを選択し、右クリックします。



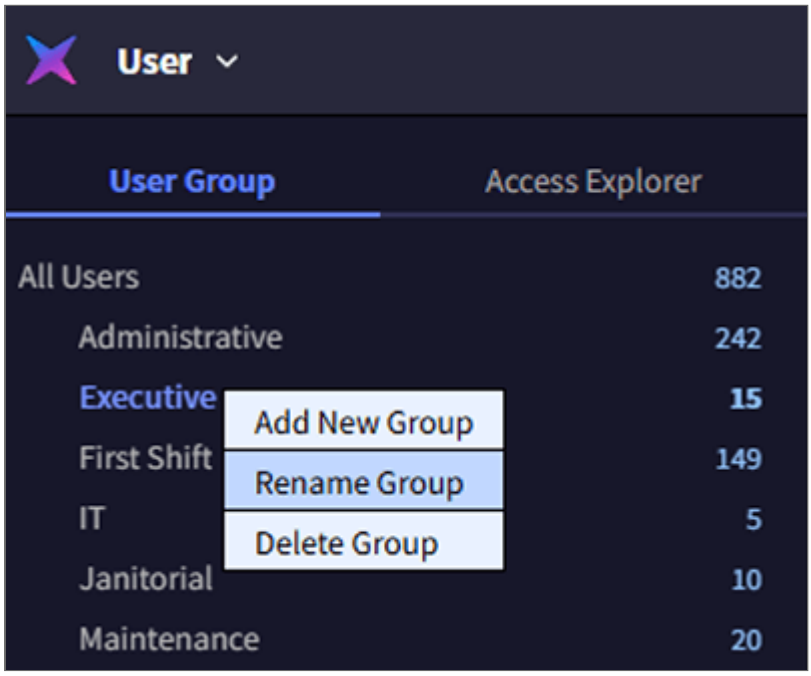
2. ポップアップメニューで **Add New Group** をクリックします。
3. グループが作成されたら、目的のグループ名を入力します。

> **情報**
>
> - 下位グループを作成する際は上位グループを選択する必要があり、最大 8 階層まで作成できます。
> - グループを別のグループへドラッグして移動すると、対象グループの下位グループとして設定できます。 **All Users** へグループを移動すると、最上位グループとして設定できます。

グループ名の変更

ユーザーが所属するグループの名前を変更できます。組織または部署名が変更された場合、グループ名も合わせて変更することを推奨します。

1. **Launcher** ページで **User** をクリックします。
2. 画面左側サイドバーの **User Group** 一覧で名前を変更するグループを選択し、右クリックします。



3. ポップアップメニューで **Rename Group** をクリックします。
4. 目的のグループ名に変更します。

User Group 一覧で変更内容を確認します。

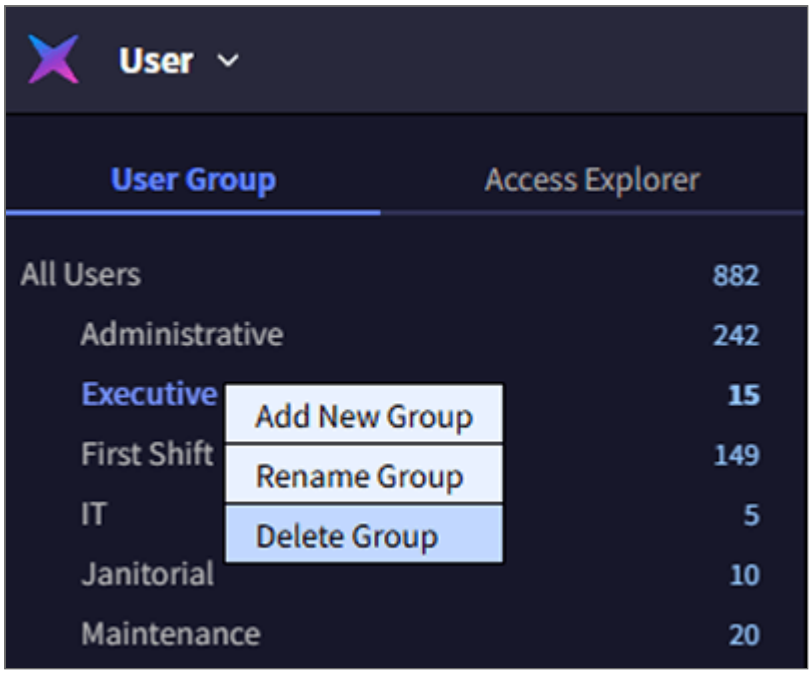
> **情報**
> ユーザーグループ名は最大 48 文字まで入力できます。

グループの削除

ユーザーが所属するグループを削除できます。

1. **Launcher** ページで **User** をクリックします。
2. 画面左側サイドバーの **User Group** 一覧で削除するグループを選択し、右クリックします。

3. ポップアップメニューで **Delete Group** をクリックします。

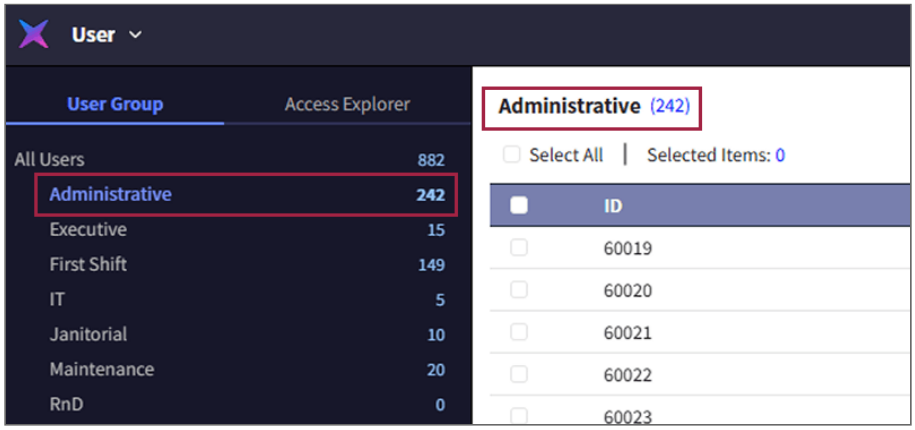


4. 確認メッセージが表示されたら、**Yes** ボタンをクリックします。

User Group 一覧で選択したグループが削除されたことを確認します。

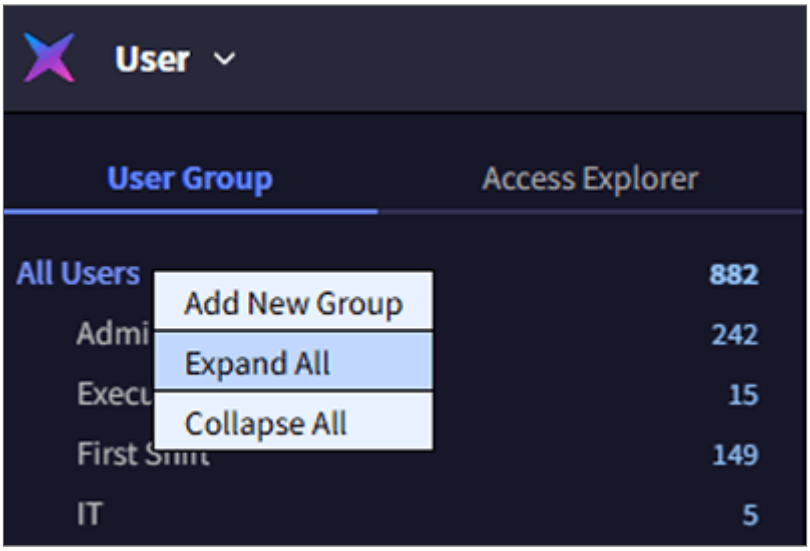
グループ別ユーザーの確認

ユーザーグループに所属するユーザーを確認できます。 **User** ページで、画面左側サイドバーから目的のユーザーグループを選択します。選択したユーザーグループのユーザーが一覧に表示されます。

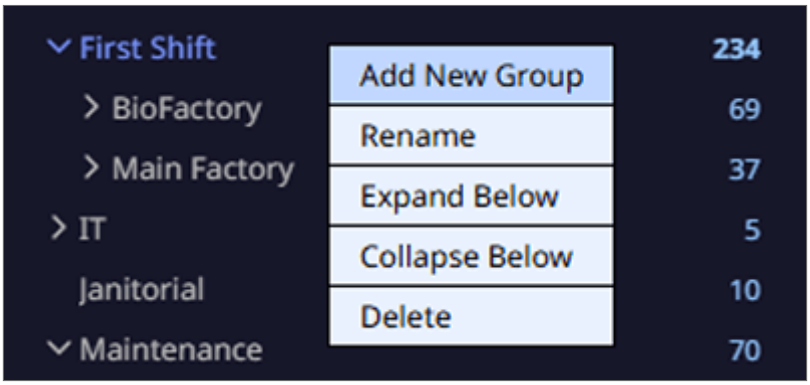


グループリストの展開/折りたたみ

ユーザーグループ一覧を展開または折りたたむことができます。 **User Group** タブで **All Users** を選択し、右クリックします。ポップアップメニューで **Expand All** または **Collapse All** をクリックします。



グループ内に下位グループがある場合は、その下位グループを展開または折りたたむことができます。上位グループを選択し、右クリックします。ポップアップメニューで **Expand Below** または **Collapse Below** をクリックします。



ユーザー登録

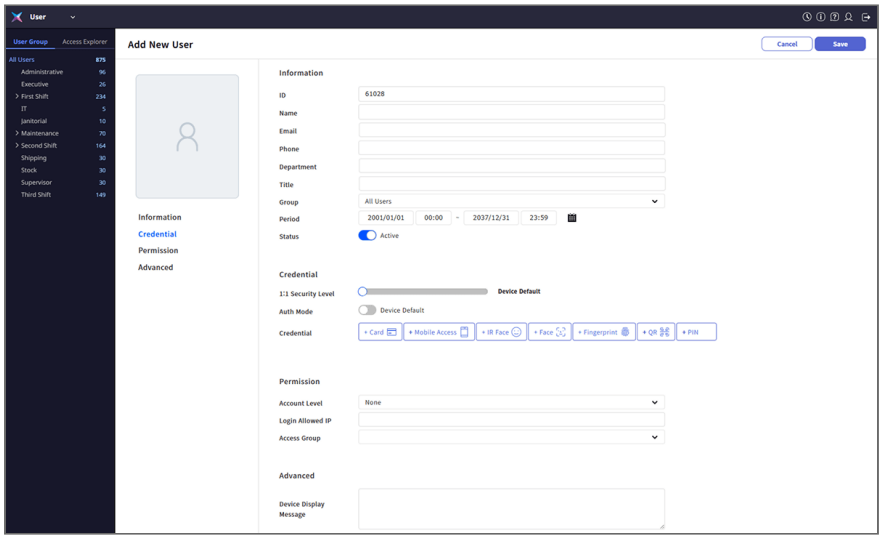
新規ユーザーを登録する方法について説明します。ユーザーの写真、氏名、メールアドレス、電話番号などの情報を入力し、ユーザーの入退室権限と生体情報を設定できます。

ユーザー情報の入力、入退室権限の設定、クレデンシャル登録の順に進めます。

1. **Launcher** ページで **User** をクリックします。
2. **User** ページ右上の **New User** ボタンをクリックします。



3. **Add New User** 画面でユーザー情報を入力します。



4. **Information** セクションでユーザーの基本情報を入力します。
5. **Credential** セクションでユーザーの生体認証情報を登録します。
6. **Permission** セクションでユーザーの **BioStar X** 運用権限と入退室権限を設定します。
7. **Advanced** セクションでユーザーが入退室する際にデバイスに表示するメッセージを入力できます。
8. すべての情報を入力し、画面右上の **Save** ボタンをクリックします。

ユーザー一覧で登録したユーザーを確認できます。各セクションの入力と設定の詳細は以下を参照してください。

Information セクションでユーザーの基本情報を入力します。各項目の詳細を確認できます。
Credential セクションでユーザークレデンシャルを登録し、入退室認証方式を設定します。
Permission セクションでユーザーの入退室権限の設定方法を確認します。
Advanced セクションでユーザー入退室時にデバイスに表示するメッセージを設定するか、Directory Service 連携時に当該ユーザーを同期対象から除外できます。
パスポートをスキャンしてユーザーを登録または修正する方法を確認してください。

情報

- 入退室権限と生体認証情報は任意項目です。基本情報を入力して保存した後で、修正または追加できます。
- ユーザー情報をカードテンプレートでカードに印刷するには、画面右上の **Print Card** ボタンをクリックします。詳細については、カードを印刷するご参照ください。
- ユーザー登録を取り消すには、画面右上の **Cancel** ボタンをクリックします。

ユーザー基本情報を入力

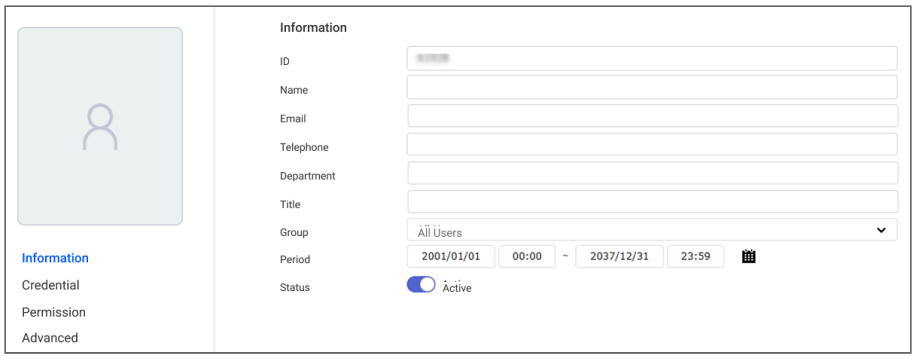
ユーザーの基本情報の入力方法について詳しく説明します。入力したユーザー情報は検索および管理に使用されます。ユーザー情報を明確に管理することで、組織のセキュリティポリシーや個人情報保護ポリシーの遵守に役立ちます。

- 氏名、部署、役職、グループなどの基本情報を体系的に入力すると、ユーザーを簡単に検索・分類・管理できます。
- ユーザーの所属、役職、グループ情報に応じて入退室権限を細分化して設定できます。
- ユーザーごとに活動履歴や入退室記録などを正確に追跡できるため、セキュリティおよび監査に有利です。

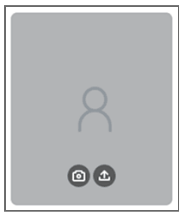
Launcher → **User** ページへ移動し、次の 2 つの方法でユーザー情報を入力できます。

- **新規ユーザー**：画面右上の **New User** をクリックします。 **New User** ウィンドウが表示されます。
- **既存ユーザー**：ユーザーリストでユーザーをダブルクリックします。 または、ユーザーをクリックすると画面右側に表示されるプレビュー画面で **See More** をクリックします。 ユーザー情報を編集できるウィンドウが表示されます。

Information セクションで設定できる項目は次のとおりです。各項目の説明を参照してユーザー情報を入力してください。



- **写真**：ユーザーの写真を登録してください。ウェブカメラで写真を撮影するか、PCから写真をアップロードできます。プロフィールにマウスを合わせると使用可能なツールが表示されます。



  - 📷：PC にウェブカメラが接続されている場合、ボタンをクリックして写真を撮影・登録できます。
  - ⬆：PC に保存されている画像ファイルをアップロードできます。

  詳細については 顔を登録する を参照してください。

- **ID**：ユーザーに付与する固有 ID を入力してください。
- **Name**：ユーザーの氏名を入力してください。
- **Email**：メールアドレスを入力してください。
- **Phone**：電話番号を入力してください。
- **Department**：ユーザーが所属する部署を入力してください。
- **Title**：ユーザーの役職を入力してください。
- **Group**：ユーザーのグループを選択してください。ユーザーグループの追加および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。
- **Period**：ユーザーアカウントの使用期間を設定してください。日付および時間フィールドをクリックして直接入力するか、📅 ボタンをクリックして希望の日付と時間を選択できます。

- **Status**：ユーザーアカウントを一時的に無効に設定できます。

入力した基本情報を保存するには、画面右上の **Save** ボタンをクリックしてください。

ユーザーIDおよび名前の入力ルール

- **ID** の値には空白を含めることはできません。
- **ID**にはマーク(.)を含められますが、マーク一つ(.)または二つ(..)だけでは入力できません。
- ユーザー名は特殊記号を含めて最大 48 文字まで入力できます。

  特殊記号： `~` `!` `@` `#` `$` `%` `^` `&` `(` `)` `-` `_` `=` `+` `[` `]` `{` `}` `;` `.` `'`
- ユーザーIDおよび名前には、次の文字を使用できません。 `₩` `/` `:` `*` `?` `"` `<` `>` `|` `` ` ``
- ユーザーIDには、アポストロフィー(')も使用できません。
- ユーザー名の先頭に `&@~` を連続して入力できません。ただし、 `&` 、 `@` 、 `~` はそれぞれ単独でユーザー名の先頭文字に使用できます。

情報

- **ID** は **Settings** → **System** → **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。詳細については、サーバーの詳細を設定するをご参照ください。
  - **Number**：1 ～ 4294967294 の数字で入力できます。
  - **Alphanumeric**：英字と数字を組み合わせて入力できます。
- モバイル入退室カードにユーザーの写真、部署、役職を表示するには、必ず写真を追加し、部署と役職を入力してください。
- 役職および部署名は特殊記号 `空白` `_` を含めて最大 64 文字まで入力できます。
- モバイル入退室カードを使用する場合、送信方法によってはメール送信時にユーザーのメールアドレスを必ず入力してください。
- 顔モバイル登録や BioStar X QR を使用するには、必ずユーザーのメールアドレスを入力してください。

ヒント

BioStar X が提供する基本入力フィールド以外に追加のユーザー情報を入力する場合は、**Custom User Field** 機能を使用してカスタムフィールドを追加できます。 **Custom User Field** は組織の要件に合わせてユーザー情報を拡張できる便利な機能です。

Custom User Field の追加方法の詳細については サーバーの詳細を設定する を参照してください。

次のステップ

Credential セクションでユーザークレデンシャルを登録し、入退室認証方式を設定します。
Permission セクションでユーザーの入退室権限の設定方法を確認します。
Advanced セクションでユーザー入退室時にデバイスに表示するメッセージを設定するか、Directory Service 連携時に当該ユーザーを同期対象から除外できます。
ユーザー情報を修正する方法を確認してください。

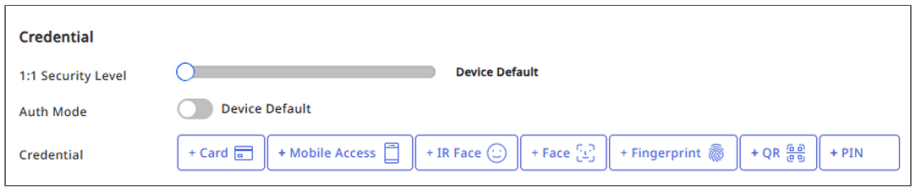
ユーザークレデンシャルを登録する

ユーザーのクレデンシャルを登録する方法を案内します。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。

Launcher → **User** ページに移動し、以下の二つの方法でクレデンシャルを登録、追加、変更できます。

- **新規ユーザー**：画面右上の **New User** をクリックします。 **New User** ウィンドウが表示されます。
- **既存ユーザー**：ユーザーリストでユーザーをダブルクリックします。 または、ユーザーをクリックすると画面右側に表示されるプレビュー画面で **See More** をクリックします。 ユーザー情報を編集できるウィンドウが表示されます。

Credential セクションで設定できる項目は以下のとおりです。各項目の説明を参考に適切なユーザー権限を設定します。



クレデンシャルを登録し、**1:1 Security Level** 項目で適切なセキュリティレベルを設定します。セキュリティレベルが高いほど認証率が低下したり本人拒否率（FRR）が高くなる可能性があります。

크리덴셜(**Credential**): 사용자의 신원을 확인하기 위한 데이터입니다. 일반적으로 디지털 서명, 스마트카드, 바이오 정보, 사용자 이름과 비밀번호 등이 있습니다.

情報

- モバイル入退カードはAirfobポータルと連携して初めて使用できます。 Airfobポータルとの連携およびモバイルアクセスカードの利用に関する詳しい情報は、モバイルアクセスカードを管理するをご参照ください。

クレデンシャルを登録する

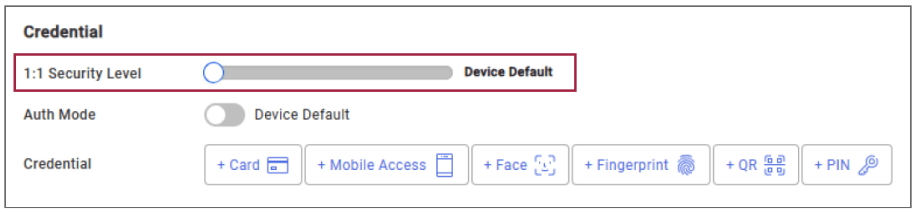
ユーザーのクレデンシャルを登録する方法は以下のとおりです。クレデンシャルは指紋、顔、カード、パスワードなどさまざまな形態で登録できます。

次のステップ

Permission セクションでユーザーの入退室権限の設定方法を確認します。
Advanced セクションでユーザー入退室時にデバイスに表示するメッセージを設定するか、Directory Service 連携時に当該ユーザーを同期対象から除外できます。
ユーザー情報を修正する方法を確認してください。

セキュリティレベルを設定する

デバイスで設定したバイオメトリクスの1:Nセキュリティレベルに関係なく、ユーザーごとに個別のセキュリティレベルを割り当てることができます。デバイスの1:Nセキュリティレベルを高く設定していて認証に頻繁に失敗するユーザーがいる場合は、**1:1 Security Level**を低く設定して認証失敗を緩和できます。



1:1 Security Level項目で、希望するレベルを設定します。設定可能な値は以下を参照してください。

- **Device Default**
- **Lowest**
- **Low**
- **Normal**
- **High**
- **Highest**

設定を保存するには、画面右上の**Save**をクリックします。

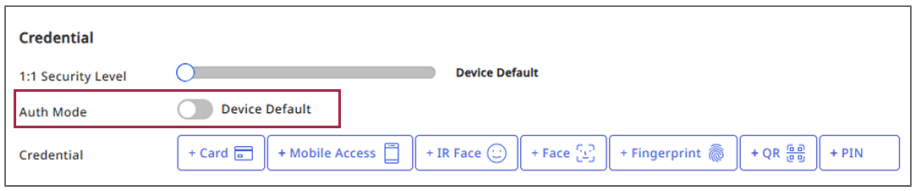
> **情報**
>
> - **Credential**セクションで**Private Auth Mode**項目を**Biometrics**に設定した場合、入力されたユーザーを特定できないため1:1セキュリティレベルを適用できません。カードやIDを含むユーザー特定が可能な認証モードを設定した場合にのみ、1:1セキュリティレベルを適用できます。**Private Auth Mode**の詳細については認証モードを設定するを参照してください。
> - 適切なセキュリティレベルを設定します。セキュリティレベルが高いほど、指紋認証率が低下したり、本人拒否率(FRR)が高くなったりする可能性があります。

認証モードを設定する

ユーザーごとに柔軟に認証方法を設定できます。デバイスで設定したデフォルトの認証方法を使用するか、各ユーザーに適した個別の認証モードを指定できます。また、顔と指紋を組み合わせた拡張認証モードによりセキュリティレベルを高めることができます。

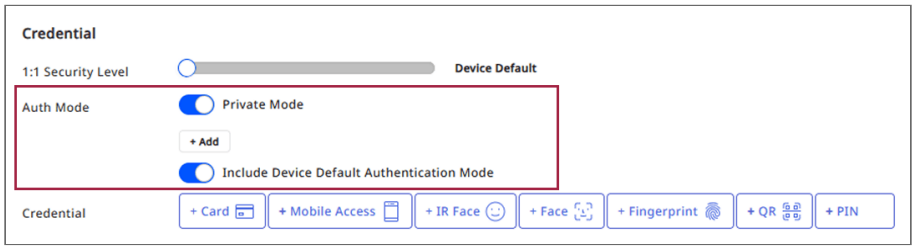
デバイスデフォルト

Auth Mode オプションを **Device Default** に設定すると、デバイスで設定した方式で認証できます。



個人認証モード

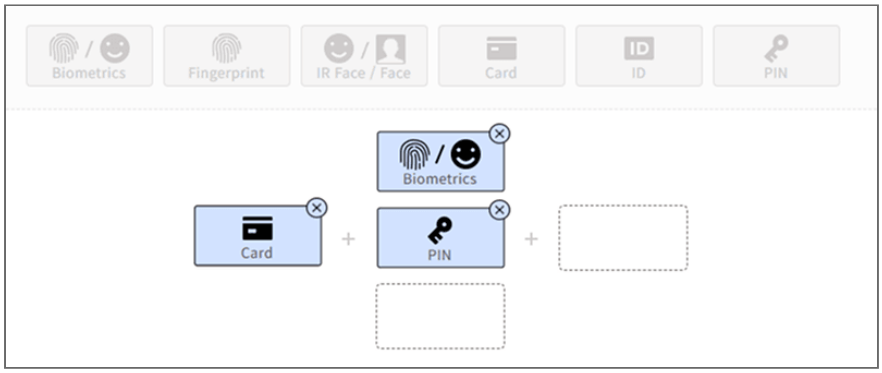
Auth Mode オプションを **Private Mode** に設定すると、ユーザーごとに認証方法を個別に設定できます。



+ Add をクリックすると、**Add New Auth Mode** ウィンドウが表示されます。希望する認証方法を設定します。



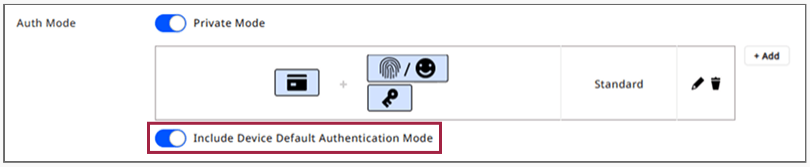
- **Extended Auth Mode**：拡張認証モードの使用可否を設定します。拡張認証モードを使用すると、顔と指紋を含む認証モードを組み合わせることができます。
- **Auth Mode**：使用する認証モードをドラッグ＆ドロップで設定します。



設定した認証モードを登録するには **Apply** をクリックします。

情報

- **Extended Auth Mode** オプションはBioStation 3 Max、BioEntry W3、BioStation 3、FaceStation F2の各モデルで利用できます。
- **Include Device Default Authentication Mode** に設定すると、デバイスで設定された認証モードと **BioStar X** で設定した個別認証モードの両方を使用できます。



- **Exclude Device Default Authentication Mode** に設定すると、**BioStar X** で設定した個別認証モードのみを使用できます。

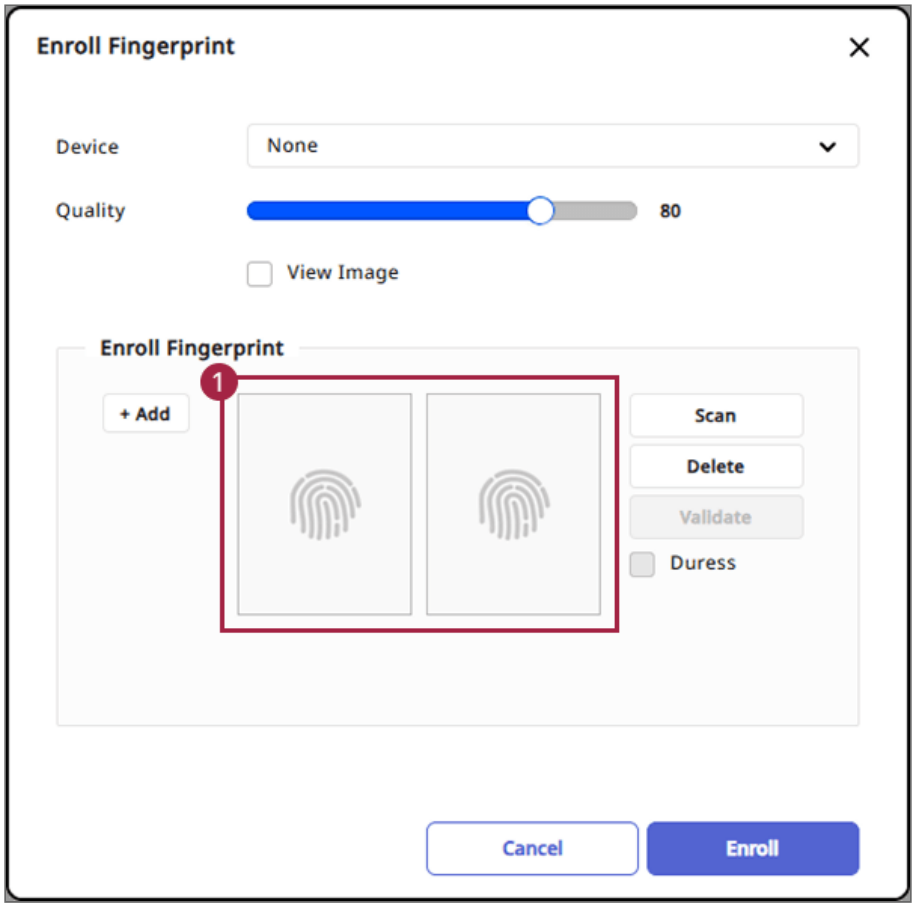
指紋を登録する

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。指紋は、指紋スキャナーが搭載されているデバイスでスキャンできます。

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。

Credential セクションで **+ Fingerprint** をクリックします。 **Enroll Fingerprint** ウィンドウが表示されたら各項目を設定し、**Enroll** をクリックします。



- **Device**：指紋を登録するデバイスを選択します。
- **Quality**：指紋登録の品質を調整できます。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。
- **View Image**：指紋をスキャンしたとき、元の画像を 1 エリアで確認できます。
- **+ Add**：指紋を追加するにはクリックします。指紋は最大 10 個まで登録できます。
- **Scan**：追加した指紋番号を選択してクリックします。指紋スキャナーまたはデバイスセンサーに指を当てて指紋をスキャンします。



- **Delete**：登録した指紋を削除できます。削除する指紋番号を選択してクリックします。
- **Validate**：既に登録されている指紋かどうかを確認できます。
- **Duress**：デュレス指紋として登録する場合は、このオプションを選択して指紋をスキャンします。誰かに脅迫されて強制的にドアを開けなければならない場合、その指紋を使用して通知を送信できます。

情報

- 日常の入退室で使用する指紋をデュレス指紋として使用しないでください。
- **View Image** オプションを有効にすると指紋画像を確認できますが、**BioStar X** サーバーには保存されません。
- 指紋認証率が低い場合は、指紋情報を削除して新しい指紋情報を登録します。
- 良質な指紋を取得するには、指紋センサーの表面を完全に覆うように指を当てます。人差し指または中指の指紋を登録します。



IRフェイスを登録する

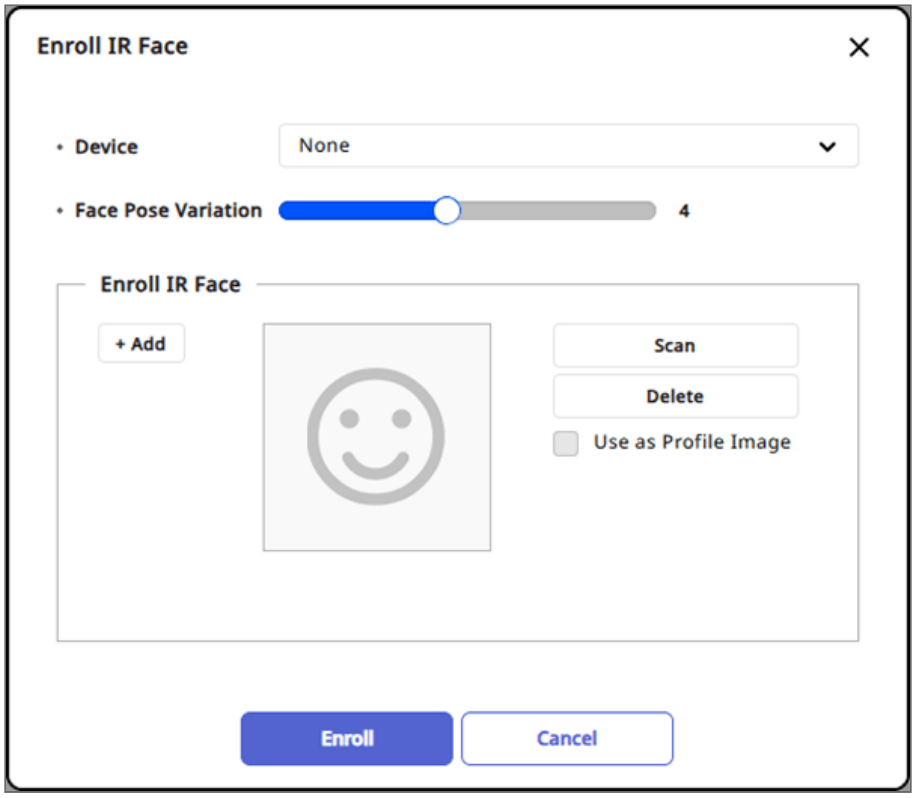
入退室の認証手段としてユーザーの顔を登録して使用できます。 IRフェイス登録は、ユーザーの顔を赤外線カメラで撮影して行う認証手段です。

IRフェイス登録時の注意事項

- 顔を登録する際は、装置と顔の距離を60～100 cmに保ってください。
- 表情を変えないように注意してください。
- マスク、帽子、アイマスクを着用しないでください。
- マスクを着用した顔を登録しないでください。 マスクを着用した顔と着用していない顔の両方を登録すると、誤認識率が高くなる可能性があります。
- 頭を上げたり下げたりしないでください。
- 濃い化粧をしないでください。
- 目を閉じないでください。
- 画面に両肩が収まるようにしてください。
- 動かず正面を向いて顔を登録してください。
- 2 人の顔が画面に同時に映らないように注意してください。 一度に 1 人ずつ登録してください。
- 画面の指示に従わないと、顔登録に時間がかかったり失敗したりすることがあります。

デバイスで登録

Credential セクションで **+ IR Face** をクリックします。 **Enroll IR Face** ウィンドウが表示されたら、各項目を設定して **Enroll** をクリックします。



- **Device**：IRフェイスを登録するデバイスを選択します。
- **Face Pose Variation**：IRフェイスを登録する際に顔の位置、角度、距離に対する感度を設定できます。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。
- **+ Add**：IRフェイスを登録するにはボタンをクリックします。 IRフェイスは最大5件まで追加できます。
- **Scan**：IRフェイスをスキャンするには追加した **N番目** ボタンをクリックします。デバイス画面の指示に従って顔をスキャンします。



- **Use as Profile Image**：登録したIRフェイス画像をプロフィール画像として使用するには、当該オプションのチェックボックスをクリックします。
- **Delete**：IRフェイスクレデンシャルを削除できます。削除する番号を選択してボタンをクリックします。

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
- 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。

顔を登録する

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。カメラで撮影したユーザーの顔情報は、モバイルデバイスで非対面で登録することもできます。

顔を登録する際の注意事項

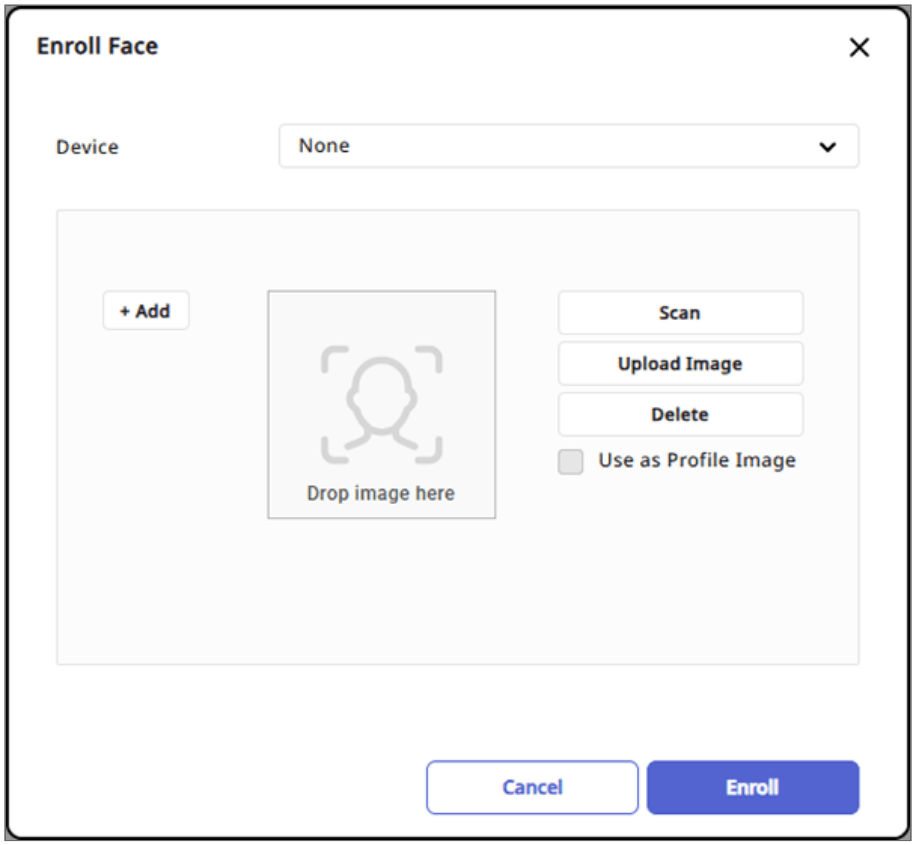
- 顔を登録する際は、装置と顔の距離を60〜100 cmに保ってください。
- 表情を変えないように注意してください。
- マスク、帽子、アイマスクを着用しないでください。
- マスクを着用した顔を登録しないでください。 マスクを着用した顔と着用していない顔の両方を登録すると、誤認識率が高くなる可能性があります。
- 頭を上げたり下げたりしないでください。
- 濃い化粧をしないでください。
- 目を閉じないでください。
- 画面に両肩が収まるようにしてください。
- 動かず正面を向いて顔を登録してください。
- 2 人の顔が画面に同時に映らないように注意してください。 一度に 1 人ずつ登録してください。
- 画面の指示に従わないと、顔登録に時間がかかったり失敗したりすることがあります。

情報

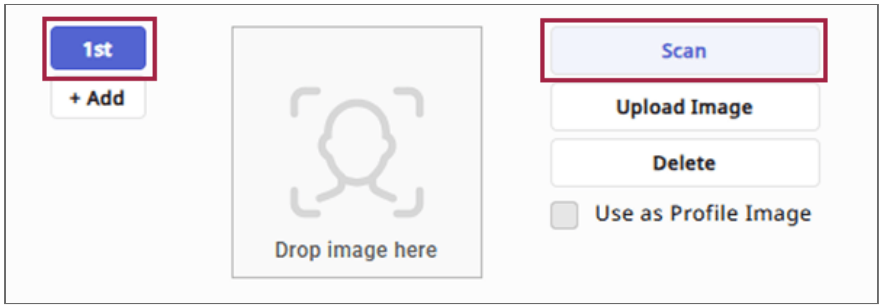
CSVファイルのインポート機能を使用して複数ユーザーの顔を一括登録したり、複数ユーザーにメールで顔登録リンクを送信してモバイルデバイスで直接顔を登録することもできます。詳細については顔を一括登録するをご参照ください。

デバイスで登録

Credential セクションで **+ Face** ボタンをクリックします。 **Enroll Face** ウィンドウが表示されたら、各項目を設定して **Enroll** をクリックします。



- **Device**：顔を登録するデバイスを選択します。
- **+ Add**：顔を登録するにはボタンをクリックします。最大2件の顔を追加できます。
- **Scan**：顔をスキャンするには追加した **N番目** ボタンをクリックします。デバイス画面の指示に従って顔をスキャンします。



- **Upload Image**：顔をスキャンせずに顔画像をアップロードして使用できます。

  – 対応する画像ファイルのサイズは最大10MBです。
  – 対応する画像ファイル形式はJPG、JPEG、PNGです。

- **Use as Profile Image**：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、当該オプションのチェックボックスをクリックします。
- **Delete**：顔クレデンシャルを削除できます。削除する番号を選択してボタンをクリックします。

情報

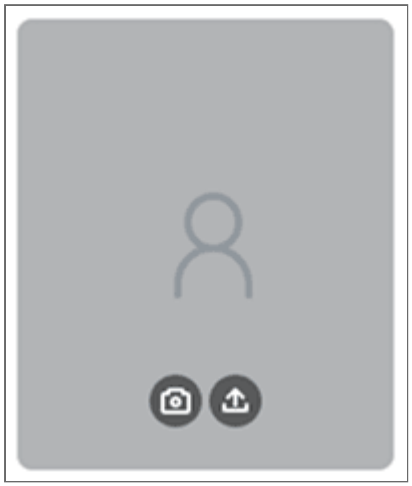
- 顔を登録できるデバイスは以下を参照してください。
  - BioStation 3 Max
  - BioEntry W3
  - BioStation 3
  - FaceStation F2
- 顔認証率が低い場合は顔情報を削除し、新しい顔情報を登録します。

ウェブカメラまたは写真画像で登録

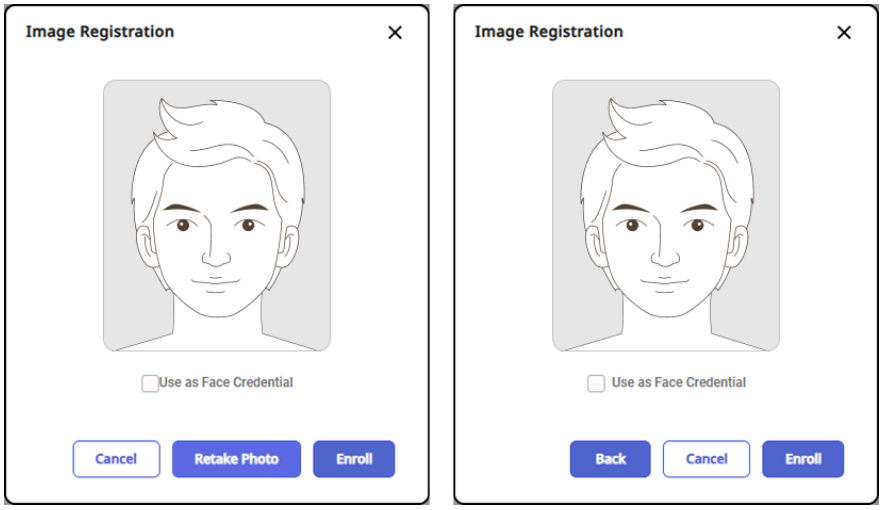
PCに接続したウェブカメラで写真を撮影し、その写真をユーザープロフィール画像として設定し、顔クレデンシャルとして登録できます。また、アップロードした写真を顔クレデンシャルとして登録できます。

1. PCにウェブカメラを接続します。
2. 画面右上のプロフィール画像領域にマウスを乗せると表示される ボタンをクリックします。

   PCに保存した画像をアップロードするには ボタンをクリックします。



3. **Image Registration** ウィンドウが表示されたら、**Take Photo** または **Upload Photo** ボタンをクリックします。
4. ウェブカメラで写真を撮影するとその写真が表示され、PCから写真をアップロードするとアップロードした写真が表示されます。



5. ウェブカメラで撮影した写真またはアップロードした写真を顔クレデンシャルとして登録するには、**Use as Face Credential** オプションのチェックボックスをクリックします。

6. 顔登録を完了するには **Enroll** ボタンをクリックします。

情報

- ウェブカメラを初めて使用する場合、ブラウザからカメラ使用許可を求めるポップアップが表示されます。ウェブカメラを使用するには、ブラウザのカメラ使用許可を許可する必要があります。
- ブラウザによってカメラ使用許可の手順が異なる場合があります。
- **Take Photo** ボタンをクリックしてから写真が撮影されるまでに数秒かかる場合があります。
- Google Chrome バージョン100以上の使用を推奨します。
- 写真をアップロードするための画像ファイルサイズは最大10MBです。
- 対応する画像ファイル形式はJPG、JPEG、PNGです。
- ウェブカメラで顔を撮影する際は次の事項に注意してください。
  - ウェブカメラと顔の距離が近すぎたり遠すぎたりしないようにします。
  - 動かず正面から顔を登録します。
  - 表情を変えないように注意してください。
  - マスク、帽子、アイマスクを着用しないでください。
  - 頭を上げたり下げたりしないでください。
  - 濃い化粧をしないでください。
  - 目を閉じないでください。
  - 両方の肩が写るようにします。
  - 二人の顔が同時に写らないように注意します。一度に一人ずつ撮影します。

入退室カードを登録する

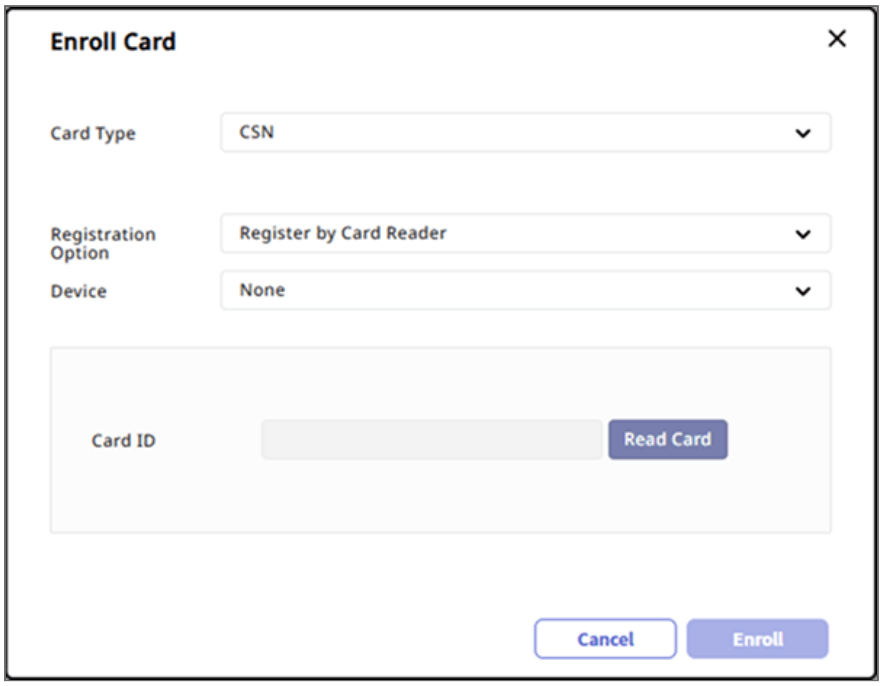
ユーザーにアクセスカードを登録する方法を案内します。 CSNカード、Wiegandカード、スマートカードの登録方法とカードの読み取り/フォーマット機能について説明します。デバイスがサポートするカードの種類については、該当デバイスのマニュアルを参照してください。

USB エージェントを使ったカード登録

カード種類	CSN	Wiegand	スマートカード
EM	✕	✕	✕
MIFARE	✓	✕	✓
DESFire	✓	✕	✓
FeliCa	✓	✕	✕
HID Prox	✕	✕	✕
HID iCLASS	✕	✕	✕

CSNカード

1. 「**Credential**」セクションで、**+ Card**をクリックします。
2. 「**Enroll Card**」ウィンドウが表示されたら、**Card Type** オプションで **CSN** を選択します。

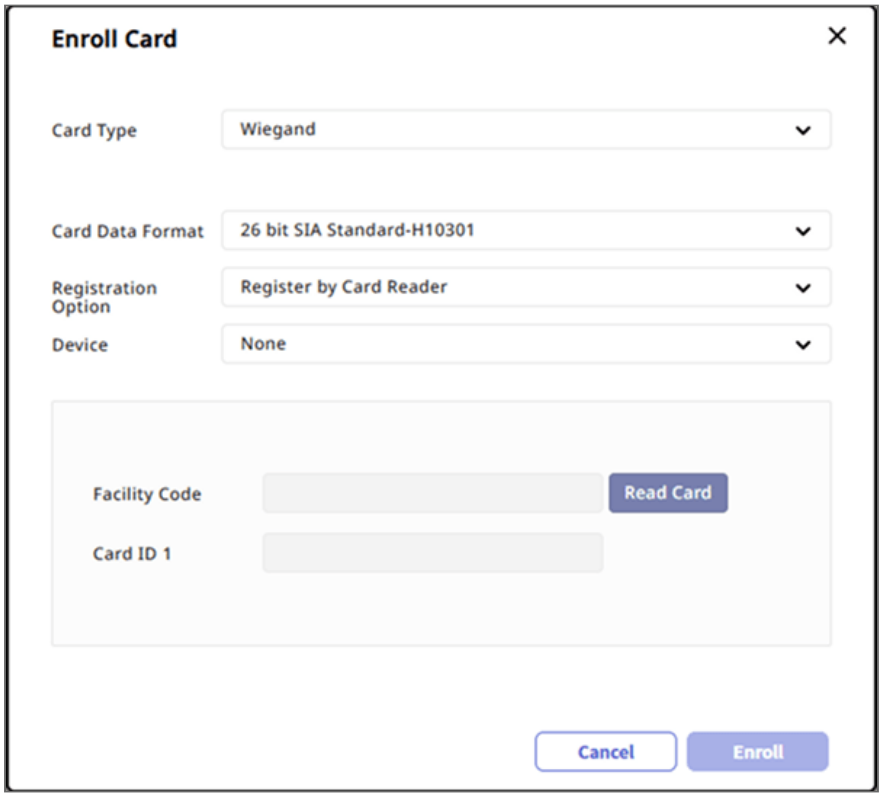


3. **Registration Option** オプションで、希望するカード登録方式を選択します。
   - **Register by Card Reader**：**Device** リストからカードをスキャンするデバイスを選択し、**Read Card** をクリックします。
   - **Assign Card**：リストからユーザーに割り当てるカードを選択します。入力フィールドで検索することもできます。
   - **Enter Manually**：カード番号を直接入力するか、**Use User ID** をクリックします。

4. **Enroll** ボタンをクリックします。

Wiegandカード

1. 「**Credential**」セクションで、**+ Card**をクリックします。
2. 「**Enroll Card**」ウィンドウが表示されたら、**Card Type** オプションで **Wiegand** を選択します。



3. **Card Data Format** オプションで、必要なフォーマットを選択します。
4. **Registration Option** オプションで、希望するカード登録方式を選択します。
   - **Register by Card Reader**：**Device** リストからカードをスキャンするデバイスを選択し、**Read Card** をクリックします。
   - **Assign Card**：リストからユーザーに割り当てるカードを選択します。入力フィールドで検索することもできます。
   - **Enter Manually**：施設コード (Facility Code) とカードIDを直接入力します。
5. **Enroll** ボタンをクリックします。

> **情報**
> **Card Data Format** オプションに目的のカードデータ形式がない場合はWiegand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

セキュアクレデンシャルカード、アクセスオンカード、カスタムスマートカードを登録できます。

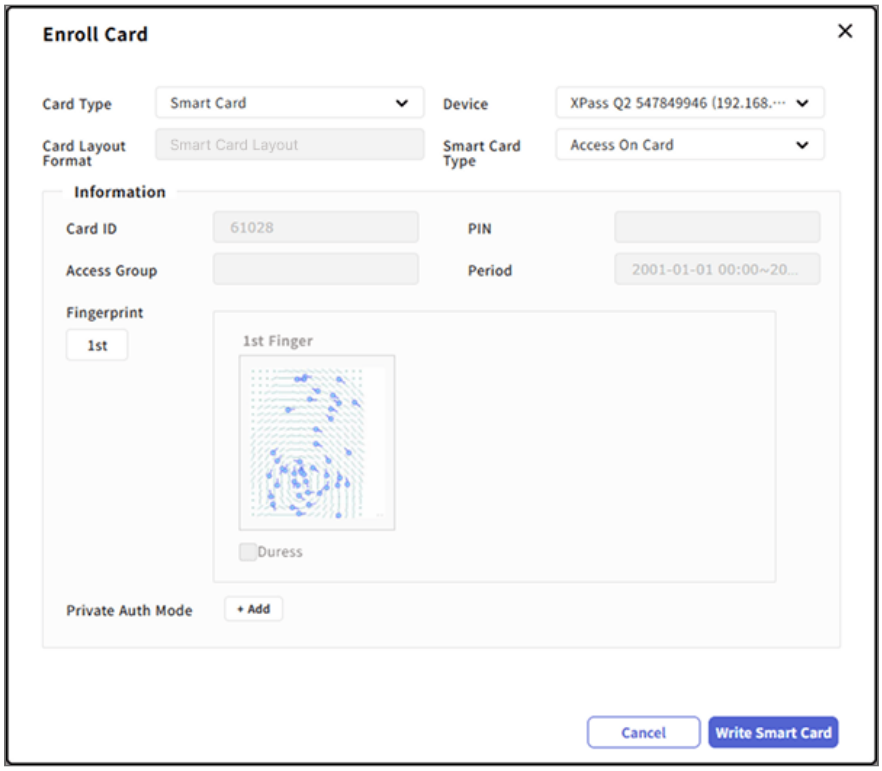
情報

- 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。カード形式の詳細については[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。
- 顔テンプレートを使用するには、**Settings** → **Credential** → **Card Format** メニューで新しいスマートカードを追加する際、**Layout** セクションで **Use Face Template** を選択します。詳細については[スマートカード形式を設定する]を参照してください。
- デバイスにスマートカードのレイアウトを設定するには[認証を設定する]を参照してください。
- スマートカードをフォーマットして情報を再書き込むには[カードの読み取り／フォーマット]を参照してください。

Access On Card

カード ID、PIN、アクセスグループ、期間、指紋テンプレート、顔テンプレート、個人認証モードを含むユーザー情報をカードに保存するには、**Access On Card**を選択してください。

1. 「**Credential**」セクションで、**+ Card**をクリックします。
2. 「**Enroll Card**」ウィンドウが表示されたら、**Card Type** オプションで **Smart Card** を選択します。
3. **Device** オプションで、カードを登録するデバイスを選択します。
4. デバイスを選択すると、**Card Layout Format** オプションに設定されているカードレイアウト形式が表示されます。
5. **Smart Card Type** オプションで **Access On Card** を選択してください。



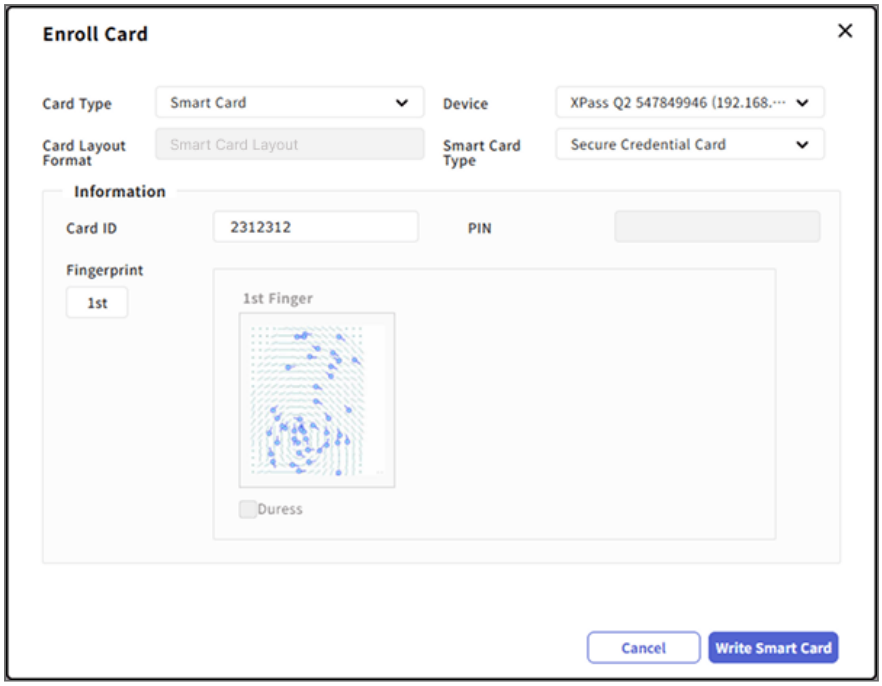
6. カードに登録する指紋テンプレートを選択します。指紋テンプレートがない場合は、この手順をスキップします。
7. **Write Smart Card** をクリックします。

> **情報**
> Access On Card ではカードIDを直接設定できません。

Secure Credential Card

カード ID、PIN、指紋テンプレート、顔テンプレートを含むユーザー情報をカードに保存するには、**Secure Credential Card**を選択してください。

1. 「**Credential**」セクションで、**+ Card**をクリックします。
2. 「**Enroll Card**」ウィンドウが表示されたら、**Card Type** オプションで **Smart Card** を選択します。
3. **Device** オプションで、カードを登録するデバイスを選択します。
4. デバイスを選択すると、**Card Layout Format** オプションに設定されているカードレイアウト形式が表示されます。
5. **Smart Card Type** オプションで **Secure Credential Card** を選択してください。



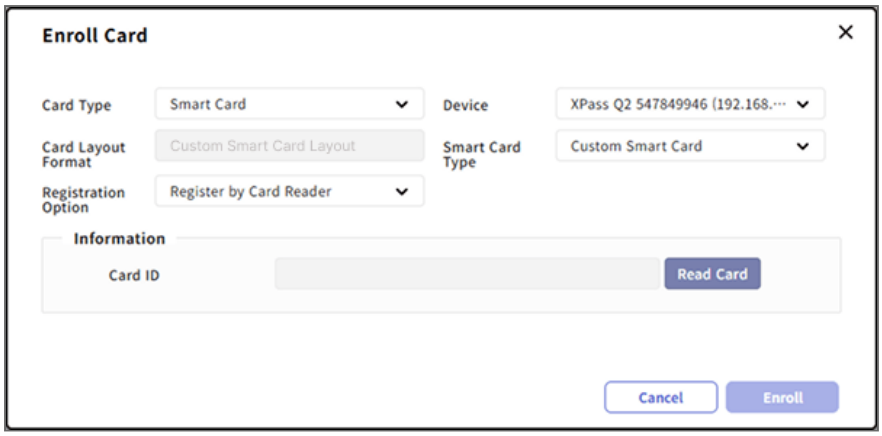
6. **Card ID** を直接入力します。
7. カードに登録する指紋テンプレートまたは顔テンプレートを選択します。テンプレートがない場合は、この手順をスキップします。
8. **Write Smart Card** をクリックします。

Custom Smart Card

サードパーティが発行したスマートカードを登録するには、**Custom Smart Card**を選択してください。

1. 「**Credential**」セクションで、**+ Card**をクリックします。
2. 「**Enroll Card**」ウィンドウが表示されたら、**Card Type** オプションで **Smart Card** を選択します。
3. **Device** オプションで、カードを登録するデバイスを選択します。
4. デバイスを選択すると、**Card Layout Format** オプションに設定されているカードレイアウト形式が表示されます。

5. **Smart Card Type** オプションで **Custom Smart Card** を選択してください。



6. **Registration Option** オプションで、希望するカード登録方式を選択します。
   - **Register by Card Reader**：**Device** リストからカードをスキャンするデバイスを選択し、**Read Card** をクリックします。
   - **Assign Card**：リストからユーザーに割り当てるカードを選択します。入力フィールドで検索することもできます。
   - **Enter Manually**：カード番号を10進数形式で直接入力してください。
7. **Enroll** ボタンをクリックします。

情報

カスタムスマートカードが使用できるデバイスとファームウェアバージョンは以下のリストを参照してください。

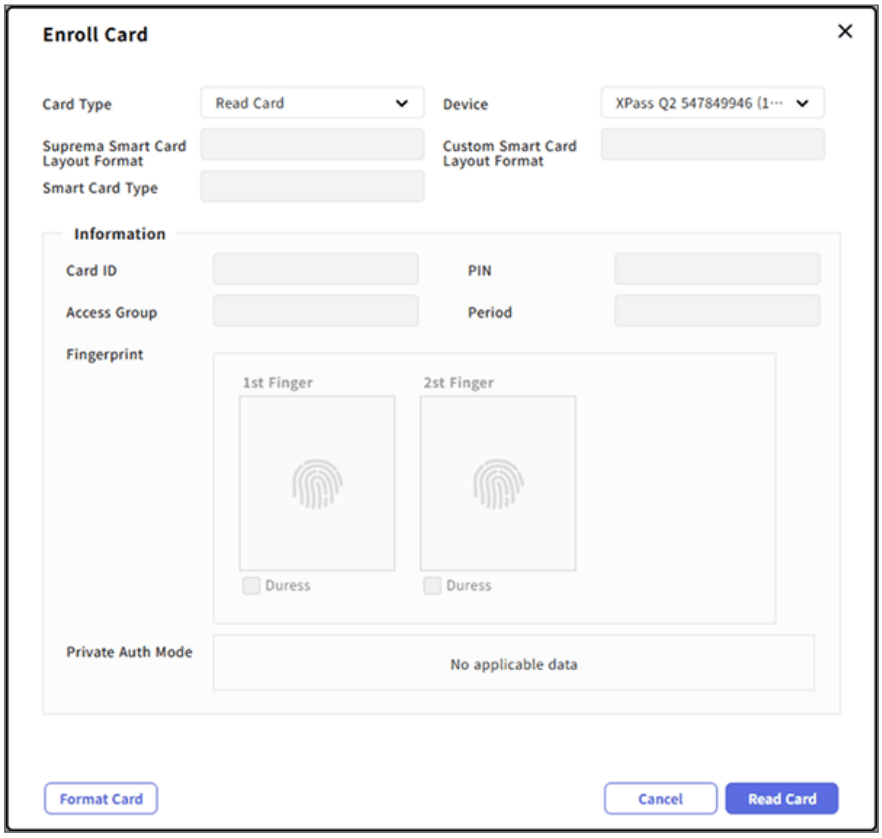
▼ カスタムスマートカード対応デバイスとファームウェアバージョンを表示

- BioStation 3 Maxのファームウェアバージョン1.0.0以降
- XPass Q2のファームウェアバージョン1.0.0以降
- BioEntry W3 ファームウェア 1.0.0 以上
- BioStation 2a ファームウェア 1.1.0 以上
- BioStation 3 ファームウェア 1.3.0 以上
- X-Station 2 ファームウェア 1.3.0 以上
- BioLite N2 ファームウェア 1.6.2 以上
- XPass D2 ファームウェア 1.7.1 以上
- BioEntry P2 ファームウェア 1.5.1 以上
- BioEntry W2 ファームウェア 1.8.0 以上

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**」セクションで、**+ Card**をクリックします。
2. 「**Enroll Card**」ウィンドウが表示されたら、**Card Type** オプションで **Read Card** を選択します。

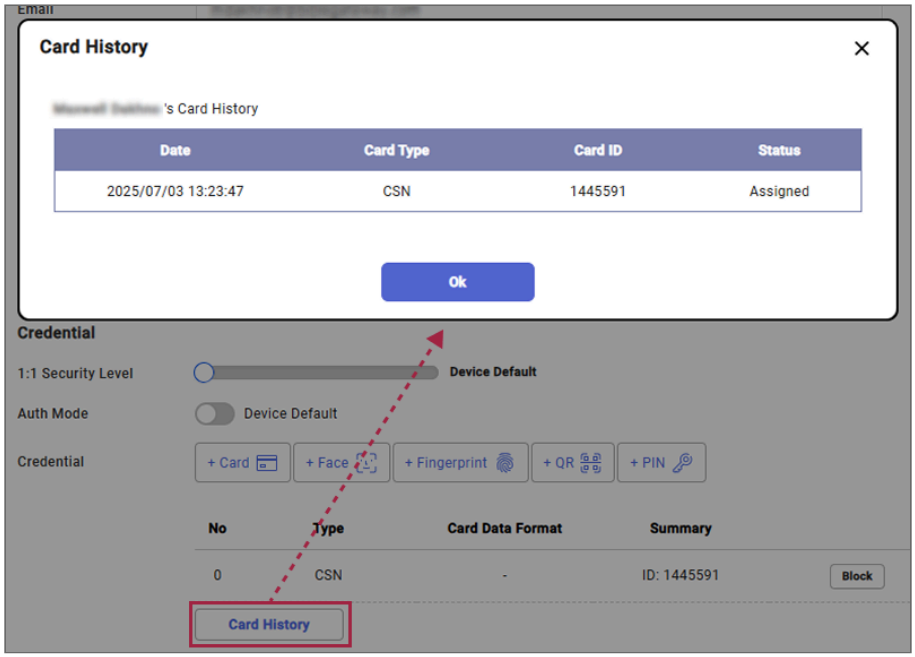


3. **Device** オプションで、スマートカードを読み取ることができるデバイスを選択します。
4. **Smart Card Type** を選択します。
5. **Read Card** をクリックします。
6. カード情報を確認し、**Format Card** をクリックします。

> **情報**
>
> - **Device** のデバイス一覧はスマートカードのレイアウトが設定されている場合にのみ表示されます。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。
> - カスタムスマートカードはフォーマットできません。

割り当てたカード情報の確認

ユーザーに割り当てられたカード情報を確認するには、**Credential** セクションの **Card History** ボタンをクリックします。カードを割り当てた日付、カードの種類、カードID、状態を確認できます。



モバイルアクセスカードを登録する

Suprema の Airfob Portal と連携してモバイルアクセスカードを使用すると、ユーザーにモバイルアクセスカードを発行できます。モバイルアクセスカードは、各ユーザーが個別に登録することも、CSV インポート機能を使用して多数のユーザーを一括登録することもできます。

Airfob Portal で設定したモバイルアクセスカード送信方法に応じて、ユーザーのメールアドレスを入力する必要があります。

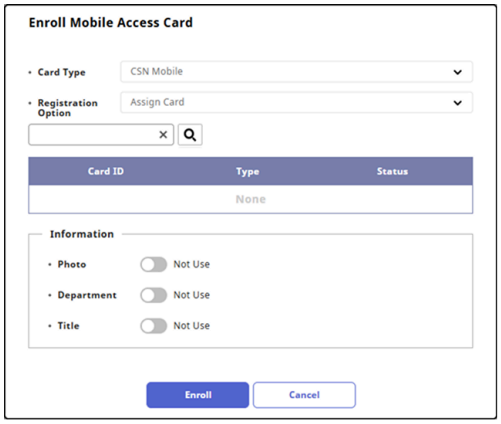
> **情報**
>
> - モバイルアクセスカードは **CSN モバイルカード** と **テンプレート・オン・モバイル** のいずれか一方のみ使用できます。
> - この機能を使用するには Airfob Portal と連携する必要があります。 Airfobポータルとの連携およびモバイルアクセスカードの利用に関する詳しい情報は、モバイルアクセスカードを管理するをご参照ください。

CSN モバイル

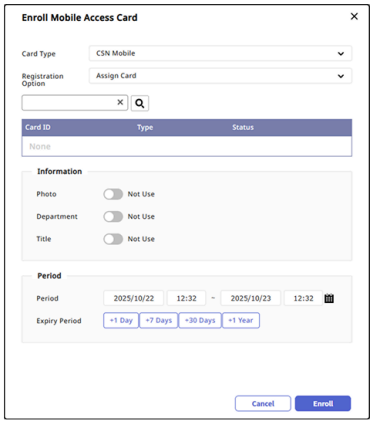
ユーザーに CSN モバイルアクセスカードを発行できます。

カード割り当て

1. **Credential** セクションで **Mobile Access** ボタンをクリックしてください。
2. **Enroll Mobile Access Card** ウィンドウが表示されたら、**Card Type** オプションで **CSN Mobile** を選択してください。
3. **Registration Option** オプションで **Assign Card** を選択してください。



Airfob portal site: Regular



Airfob portal site: Dynamic

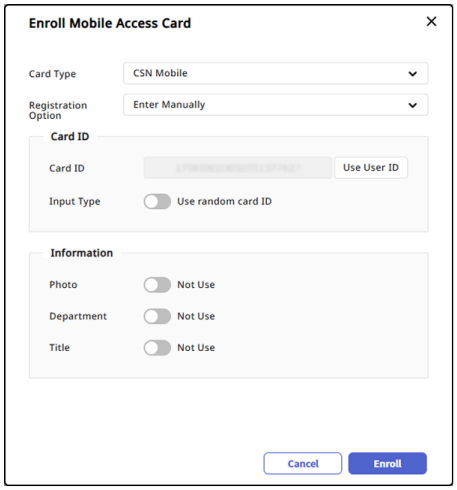
> **Period** 項目は、Airfobポータルでサイトを作成する際に**ダイナミック(Dynamic)**サイトとして設定すると有効になります。 ユーザーのモバイルアクセスカードの有効期限と利用期間を設定できます。 Airfobポータルの利用に関する詳細は次のリンクを参照してください。

4. カード一覧から割り当てたいカードを選択するか検索してください。
5. **Info** と **Period** を設定してください。
6. **Enroll** ボタンをクリックします。

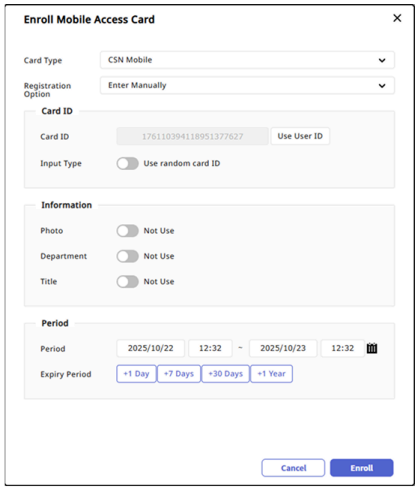
> **情報**
>
> - **Info** セクションで **Photo**、**Department**、**Title** オプションを有効にした場合、その情報をユーザーのモバイル入退室カードに表示できます。このとき表示される項目は、ユーザー情報に入力された内容に基づきます。ユーザー基本情報の入力について詳しくは、ユーザー基本情報を入力を参照してください。
> - ユーザー名にモバイルアクセスカードと互換性のない特殊文字が含まれている場合、発行を制限します。 `@` `-` `_` `+` `[` `]` `,` `.` のみ使用できます。
> - ユーザー名にシングルクォート(`'`)が含まれている場合、ユーザーを保存するとシングルクォートを削除した値がモバイル入退室カード発行システムに送信されるという案内が表示されます。この案内が表示される時点で、カードレコードはすでに作成されています。そのため、案内をキャンセルすると、エアポップポータルへの送信だけを中断し、該当カードは使用できない状態のまま残ります。この場合、システムは使用できないカードをユーザーに紐付けず、残りのユーザー情報のみ保存します。

直接入力

1. **Credential** セクションで **Mobile Access** ボタンをクリックしてください。
2. **Enroll Mobile Access Card** ウィンドウが表示されたら、**Card Type** オプションで **CSN Mobile** を選択してください。
3. **Registration Option** オプションで **Enter Manually** を選択します。



Airfob portal site: Regular



Airfob portal site: Dynamic

> **Period** 項目は、Airfobポータルでサイトを作成する際に**ダイナミック(Dynamic)**サイトとして設定すると有効になります。 ユーザーのモバイルアクセスカードの有効期限と利用期間を設定できます。 Airfobポータルの利用に関する詳細は次のリンクを参照してください。

4. **Input Type** オプションを選択します。
   - **Use random card ID**：カード ID を自動生成します。
   - **Use User ID**：ユーザー ID をカード ID として使用します。ユーザーIDが数字のみで構成されている場合にのみ使用できます。
   - **Enter manually**：カード ID を直接入力できます。
5. **Info** と **Period** を設定してください。
6. **Enroll** ボタンをクリックします。

> **情報**
>
> - **Info** セクションで **Photo**、**Department**、**Title** オプションを有効にした場合、その情報をユーザーのモバイル入退室カードに表示できます。このとき表示される項目は、ユーザー情報に入力された内容に基づきます。ユーザー基本情報の入力について詳しくは、ユーザー基本情報を入力を参照してください。
> - ユーザー名にモバイルアクセスカードと互換性のない特殊文字が含まれている場合、発行を制限します。 `@` `-` `_` `+` `[` `]` `,` `.` のみ使用できます。
> - ユーザー名にシングルクォート(`'`)が含まれている場合、ユーザーを保存するとシングルクォートを削除した値がモバイル入退室カード発行システムに送信されるという案内が表示されます。この案内が表示される時点で、カードレコードはすでに作成されています。そのため、案内をキャンセルすると、エアポップポータルへの送信だけを中断し、該当カードは使用できない状態のまま残ります。この場合、システムは使用できないカードをユーザーに紐付けず、残りのユーザー情報のみ保存します。
> - メールで送信したアクティベーションコードをユーザーが紛失または削除し、アクティベーションリンクを再発行する場合は **再送信** ボタンをクリックしてください。
> - CSN モバイルアプリケーションの詳細については次のリンクを参照してください。

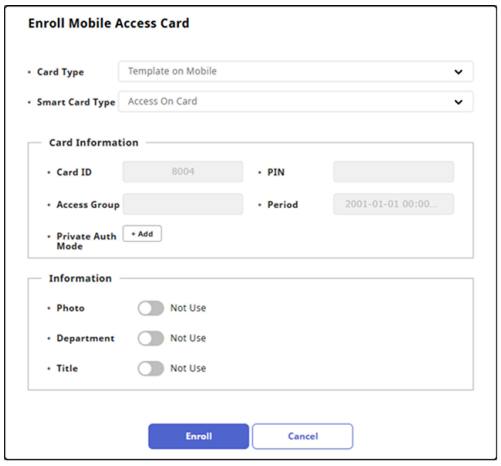
Template on Mobile

テンプレート・オン・モバイル は、ユーザーのバイオメトリックテンプレートをモバイルデバイスに保存するモバイルアクセスカ

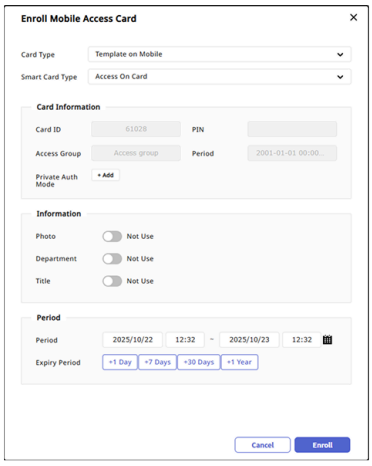
ードです。 **BioStar X** サーバー、Airfob Portal、およびデバイスにユーザーデータを保存しなくてもバイオメトリック認証が行えます。

この機能は、バイオメトリックをクレデンシャルとして使用したいが、プライバシー保護のためサーバーやデバイスに生体情報を保存できない環境で有用です。**テンプレート・オン・モバイル** の発行とバイオメトリックテンプレートの登録が別々に行われるため、ユーザーは管理者と対面せずに **テンプレート・オン・モバイル** 対応デバイスで直接顔を登録できます。

1. **Credential** セクションで **Mobile Access** ボタンをクリックしてください。
2. **Enroll Mobile Access Card** ウィンドウが表示されたら、**Card Type** オプションで **Template on Mobile** を選択してください。



Airfob portal site: Regular



Airfob portal site: Dynamic

> **Period** 項目は、Airfobポータルでサイトを作成する際に**ダイナミック(Dynamic)**サイトとして設定すると有効になります。 ユーザーのモバイルアクセスカードの有効期限と利用期間を設定できます。 Airfobポータルの利用に関する詳細は次のリンクを参照してください。

3. **Smart Card Type** オプションで希望のカードタイプを選択してください。
   - **Access On Card**：ユーザーの情報（カード ID、PIN、アクセスグループ、期間、個人認証モード）をカードに保存できます。
   - **Secure Credential Card**：セキュアクレデンシャルカードです。ユーザーのカード ID と PIN データをカードに保存できます。
4. **Info** と **Period** を設定してください。
5. **Enroll** ボタンをクリックします。

登録されたユーザーのメールアドレスに発行メールを送信します。メールのリンクから Airfob Pass アプリケーションをインストールし、モバイルデバイスで **テンプレート・オン・モバイル** の発行を完了すると使用できます。

> **ヒント**
> **テンプレート・オン・モバイル認証方法**
>
> ユーザーはテンプレート・オン・モバイルを発行したモバイルデバイスを装置にかざし、画面の案内に従って顔を認証してください。

情報

- **Info** セクションで **Photo**、**Department**、**Title** オプションを有効にした場合、その情報をユーザーのモバイル入退室カードに表示できます。このとき表示される項目は、ユーザー情報に入力された内容に基づきます。ユーザー基本情報の入力について詳しくは、ユーザー基本情報を入力を参照してください。
- ユーザー名にモバイルアクセスカードと互換性のない特殊文字が含まれている場合、発行を制限します。 `@` `-` `_` `+` `[` `]` `,` `.` のみ使用できます。
- ユーザー名にシングルクォート(')が含まれている場合、ユーザーを保存するとシングルクォートを削除した値がモバイル入退室カード発行システムに送信されるという案内が表示されます。この案内が表示される時点で、カードレコードはすでに作成されています。そのため、案内をキャンセルすると、エアポップポータルへの送信だけを中断し、該当カードは使用できない状態のまま残ります。この場合、システムは使用できないカードをユーザーに紐付けず、残りのユーザー情報のみ保存します。
- **テンプレート・オン・モバイル** が使用可能な装置とファームウェアバージョンについては以下の一覧を参照してください。
  - BioStation 3 Maxのファームウェアバージョン1.0.0以降
  - BioEntry W3 ファームウェア 1.0.0 以上
  - BioStation 3 ファームウェア 1.2.0 以上
  - FaceStation F2 ファームウェア 2.2.0 以上
- モバイルアクセスカードは **CSN モバイルカード** と **テンプレート・オン・モバイル** のいずれか一方のみ発行できます。

QR/バーコードを登録する

ユーザー認証手段として QR コードまたはバーコードを登録する方法を案内します。 **BioStar X** で直接生成した QR コードと外部で発行された QR/バーコードを登録できます。

情報

- スキャナーでQR/バーコード認証を利用できるデバイスは以下のとおりです。
  - X-Station 2 (XS2-QDPB, XS2-QAPB)
- カメラでQR/バーコード認証を利用できるデバイスは以下のとおりです。
  - BioStation 3 Maxのファームウェアバージョン1.0.0以降
  - XPass Q2のファームウェアバージョン1.0.0以降
  - BioStation 3 ファームウェア バージョン 1.1.0以降
  - X-Station 2 (XS2-ODPB, XS2-OAPB, XS2-DPB, XS2-APB) ファームウェア 1.2.0 以上
  - X-Station 2 (XS2-QDPB, XS2-QAPB) ファームウェア 1.4.1 以上
- カメラで QR/Barcode 認証を使用するには、別途デバイスライセンスが必要です。詳しくはデバイスライセンスをご覧ください。

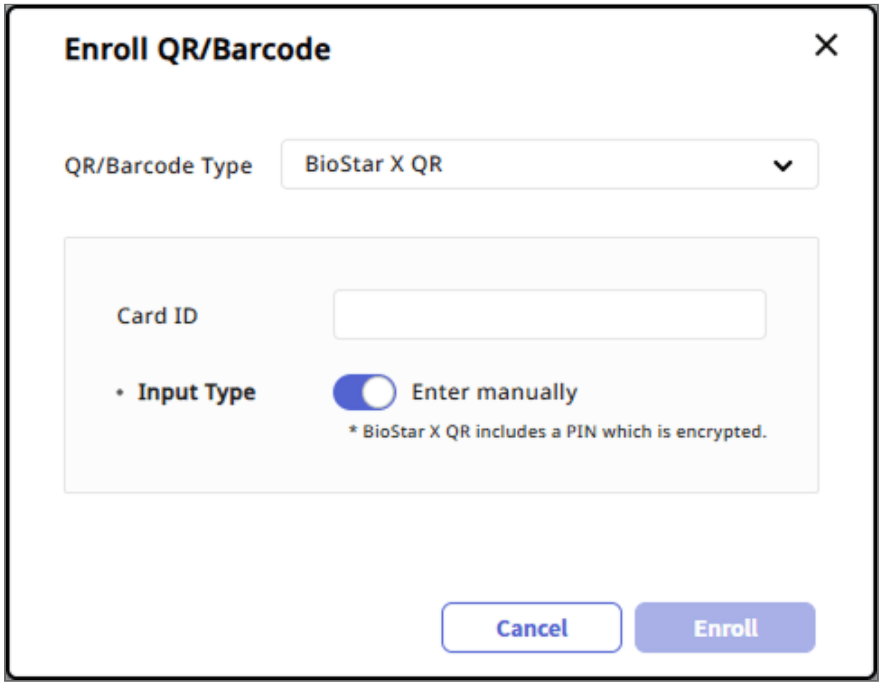
BioStar X QR

暗号化された PIN を含む QR コードをユーザーに発行して入退室を許可できます。

始める前に

- BioStar QR を使用する前に、SMTP 設定を含むメール情報の設定を完了してください。詳細については、メールを設定するご参照ください。
- BioStar QR を発行するには、必ずユーザー情報にメールアドレスを登録する必要があります。詳しくはユーザー基本情報を入力をご参照ください。

1. **Credential** セクションで **+ QR/Barcode** ボタンをクリックします。
2. **Enroll QR/Barcode** ウィンドウが表示されたら、**QR/Barcode Type** オプションで **BioStar QR** を選択します。



3. **Input Type** オプションを選択します。
   - **Use random card ID**：カード ID を自動生成します。
   - **Enter manually**：カード ID を直接入力します。
4. **Enroll** ボタンをクリックします。

その後、ユーザーが入退室認証を行う際に QR コードを発行し、ユーザー情報に登録されたメールアドレスへ送信します。ユーザーはメールに含まれる QR コードをデバイスでスキャンして入退室できます。

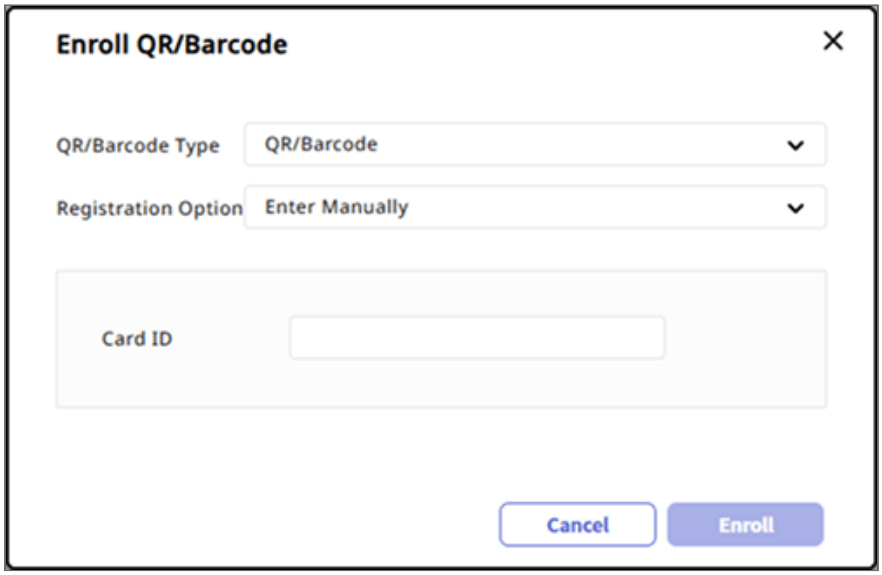
情報

重複したカード ID の生成を防ぐため、**Input Type** オプションで **Use random card ID** を設定することを推奨します。

QR/バーコード

外部の他の発行元で発行された QR/バーコードをユーザーに登録できます。

1. **Credential** セクションで **+ QR/Barcode** ボタンをクリックします。
2. **Enroll QR/Barcode** ウィンドウが表示されたら、**QR/Barcode Type** オプションで **QR/Barcode** を選択します。



3. **Registration Option** オプションで **Enter Manually** を選択します。
4. **Card ID** オプションに既に発行された QR/バーコード ID を直接入力します。
5. **Enroll** ボタンをクリックします。

> **情報**
> **Card ID** オプションには、英字、数字、特殊記号を含めて最大 32 文字まで入力できます。

PINを登録する

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を登録する方法を説明します。個々のユーザーにPINを登録することも、CSVインポートで多数のユーザーにPINを一括登録することもできます。

PIN登録

1. **Credential** セクションで **PIN** ボタンをクリックします。



2. 入力フィールドが有効になったら、パスワードを入力します。
3. **Confirm PIN** に同じパスワードを入力します。
4. **Enroll** ボタンをクリックします。

> **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。

CSVインポートでPINを登録

CSVインポート機能を使用すると、多数のユーザーを一度に登録できます。

1. インポートするCSVファイルに `pin` 列を追加します。
2. `pin` 列にユーザーのPINを入力し、CSVファイルを保存します。
3. **User** ページに移動します。
4. 画面右上の[•••]ボタンをクリックし、**Import** → **CSV** を選択します。
5. 画面の案内に従ってCSVファイルを選択し、インポートオプションを設定します。

> **情報**
>
> - 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。
> - CSVのインポート機能の詳細についてはユーザー情報のエクスポート/インポートをご参照ください。

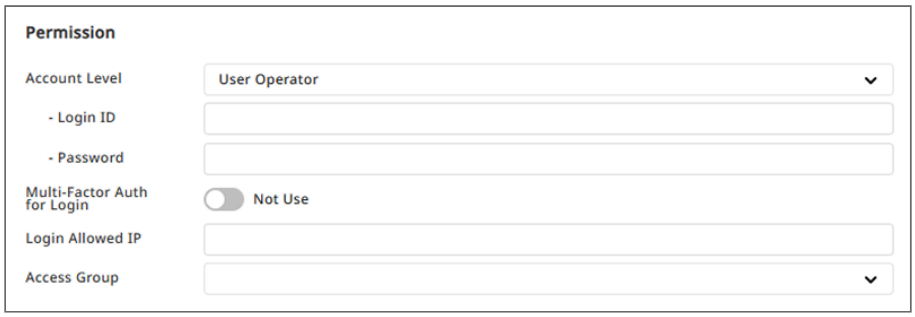
ユーザー権限を設定する

組織のセキュリティポリシーに応じて、ユーザーごとに **BioStar X** の運用権限と入退室権限を区別して設定できます。管理者グレードで主要メニューへのアクセスを制限し、入退室グループで物理的スペースへのアクセスを制御できます。さらに、IP アドレス制限と多要素認証によりセキュリティを強化できます。

Launcher → **User** ページに移動し、次の 2 つの方法で入退室権限を設定します。

- **新規ユーザー**：画面右上の **New User** をクリックします。 **New User** ウィンドウが表示されます。
- **既存ユーザー**：ユーザーリストでユーザーをダブルクリックします。 または、ユーザーをクリックすると画面右側に表示されるプレビュー画面で **See More** をクリックします。 ユーザー情報を編集できるウィンドウが表示されます。

Permission セクションで設定できる項目は次のとおりです。各項目の説明を参考に適切なユーザー権限を設定します。



管理者グレードを選択

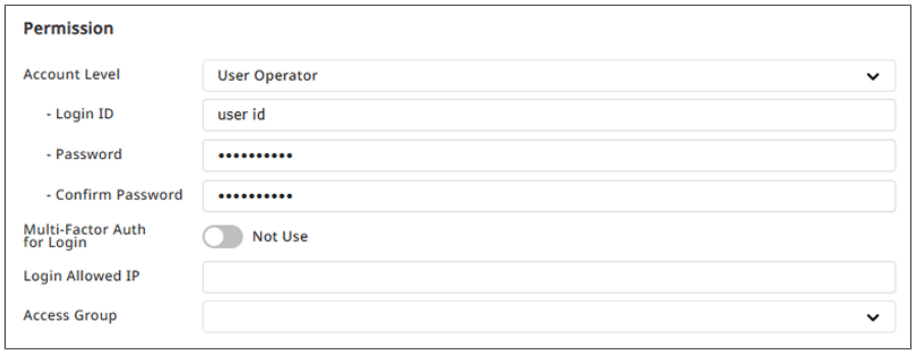
管理者グレードによってアクセスできるメニューが制限されます。 **Permission** セクションの **Account Level** 項目で、ユーザーの管理者グレードを選択します。ユーザーに割り当てられる管理者グレードは次の一覧を参照してください。

- **Administrator**：すべてのメニューを使用できる管理者権限レベルです。
- **User Operator**：**User** メニューに対する **読み取り**、**編集** 権限を持ちます。 **User** メニュー以外の設定グループに対する権限はありません。
- **Monitoring Operator**：**Monitoring** と **Data** メニューに対する **読み取り**、**編集** 権限を持ち、**Dashboard** メニューに対する **読み取り** 権限を持ちます。
- **T&A Operator**: **TIME ATTENDANCE** メニューの閲覧、編集権限を持ち、**User** メニューの閲覧権限を持ちます。
- **Visitor Operator**：**VISITOR** メニューで **読み取り**、**編集** 権限を持ちます。

> **情報**
>
> - 管理者権限レベルを設定しない場合は、**None** を選択してください。この場合、該当ユーザーは **BioStar X** にログインできません。
> - **Monitoring** メニューの **編集** 権限では、タブを追加したり、状態ツリー項目を制御したりできます。
> - **Data** メニューの **編集** 権限では、レポートの保存、レポートの自動スケジュール追加、設定へのアクセスができます。
> - 既定のユーザー権限以外の新しいユーザー権限を追加するには、カスタム権限を追加するを参照してください。
> - 既定のアカウントの権限は変更または削除できません。
> - **T&A Operator** および **Visitor Operator** 権限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。

ログイン ID とパスワードを設定

管理者グレードを選択したら、そのユーザーが **BioStar X** にログインする際に使用する ID とパスワードを設定する必要があります。



情報

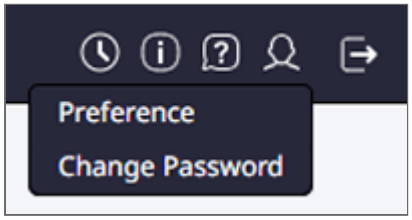
ID とパスワードを設定する際の注意事項

- IDは英字、数字、ピリオド(.)を組み合わせて8~32文字以内に設定してください。ただし、アポストロフィ(')は使用できません。
- パスワードポリシーの設定に関する詳細はシステムセキュリティを強化するを参照してください。
- セキュリティ上脆弱なパスワードは使用しないでください。
  - 連続した文字または数字（例：abcd、1234）
  - 一般的な単語またはパターン（例：qwerty、password）

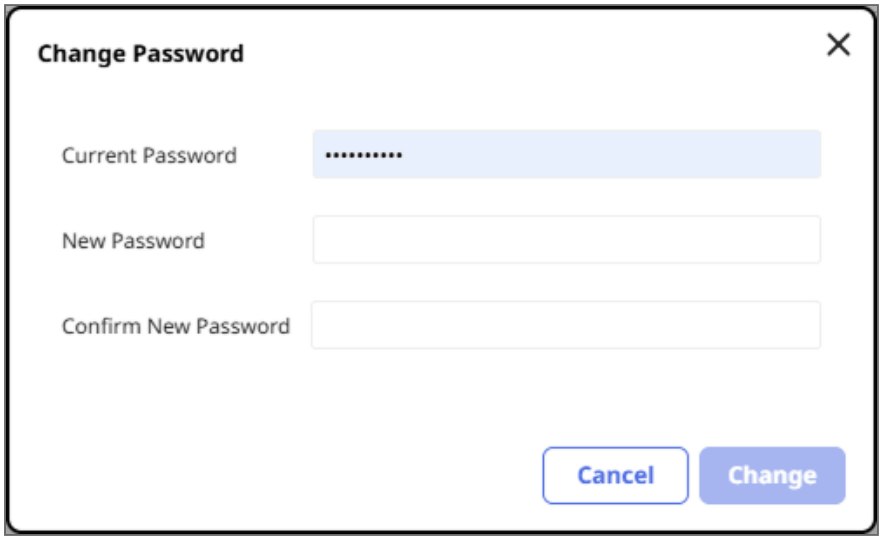
ログインユーザーのパスワード変更

ユーザーは BioStar X にログインした後、自分のパスワードを変更できます。

1. BioStar X にログインします。
2. 画面右上の ボタンをクリックします。



3. ドロップダウンメニューで **Change Password** をクリックします。
4. **Change Password** ウィンドウが表示されたら、現在のパスワードと新しいパスワードを入力します。



5. すべての項目を入力したら **Change** ボタンをクリックします。

多要素認証の設定

Multi-Factor Auth for Login を有効にすると、ユーザーは BioStar X にログインする際に指紋認証を追加してログインできます。

> **情報**
> 多要素認証の設定に関する詳細は多要素認証でログインするを参照してください。

ユーザーIPアドレスによるログイン設定

ユーザー IP アドレスを登録すると、アカウントに登録した IP 情報と一致する場合にのみ PC にログインできます。これによりセキュリティが向上します。 **Permission** セクションの **Login Allowed IP** 項目にユーザーの IP アドレスを入力します。

> **情報**
> - IP アドレスは xxx.xxx.xxx.xxx 形式で入力でき、各オクテットには 0〜255 の数値のみを入力できます。
> - IP アドレスを登録しない場合は、IP 情報に関係なく PC にログインできます。

入退室グループを選択

ユーザーの入退室グループを設定して、組織や部署ごとに入退室を制限できます。 **Permission** セクションの **Access Group** 項目で入退室グループを選択します。

> **情報**
> 入退室グループの追加および設定に関する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。

次のステップ

Advanced セクションでユーザー入退室時にデバイスに表示するメッセージを設定するか、Directory Service 連携時に当該ユーザーを同期対象から除外できます。
ユーザー情報を修正する方法を確認してください。

ユーザーの詳細設定

ユーザーの入退室時にデバイスに表示するメッセージを設定したり、Directory Service 連携時に当該ユーザーを同期対象から除外したりできます。この機能はユーザーを新規追加または編集する際に設定できます。

Launcher → **User** ページに移動し、次の 2 つの方法で入退室権限を設定します。

- **新規ユーザー**：画面右上の **New User** をクリックします。 **New User** ウィンドウが表示されます。
- **既存ユーザー**：ユーザーリストでユーザーをダブルクリックします。 または、ユーザーをクリックすると画面右側に表示されるプレビュー画面で **See More** をクリックします。 ユーザー情報を編集できるウィンドウが表示されます。

Advanced セクションで設定できる項目は次のとおりです。



- **Device Display Message**：ユーザーの入退室時にデバイスに表示するメッセージを入力できます。メッセージは最大128文字まで入力できます。
- **Exclude from Directory Integration**：Directory Service 連携時にそのユーザーを同期対象から除外できます。

> **情報**
>
> - **Exclude from Directory Integration** オプションは **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。
> - ディレクトリ連携設定の詳細はディレクトリ連携を設定するをご参照ください。

次のステップ

ユーザー情報を修正する方法を確認してください。

身分証明書のスキャンでユーザーを登録、編集する

ユーザー情報を一つずつ入力する代わりに、身分証明書をスキャンして氏名や写真などの情報を自動取得し、ユーザーを登録したり既存ユーザー情報を編集したりできます。

開始する前に

- 身分証明書をスキャンするには、DESKO スキャナーをクライアント PC に接続する必要があります。
- 身分証明書をスキャンしてユーザーを登録する前に、身分証明書から取得するデータを設定したか確認してください。身分証明書スキャンの設定に関する詳細は、身分証明書スキャンを設定するをご参照ください。

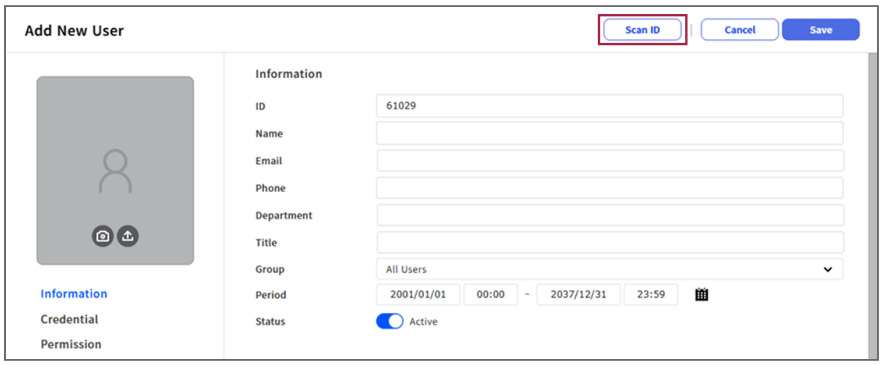
> **情報**
>
> **Scan ID** は現在、パスポートのスキャンのみをサポートしています。

身分証明書のスキャンでユーザーを登録する

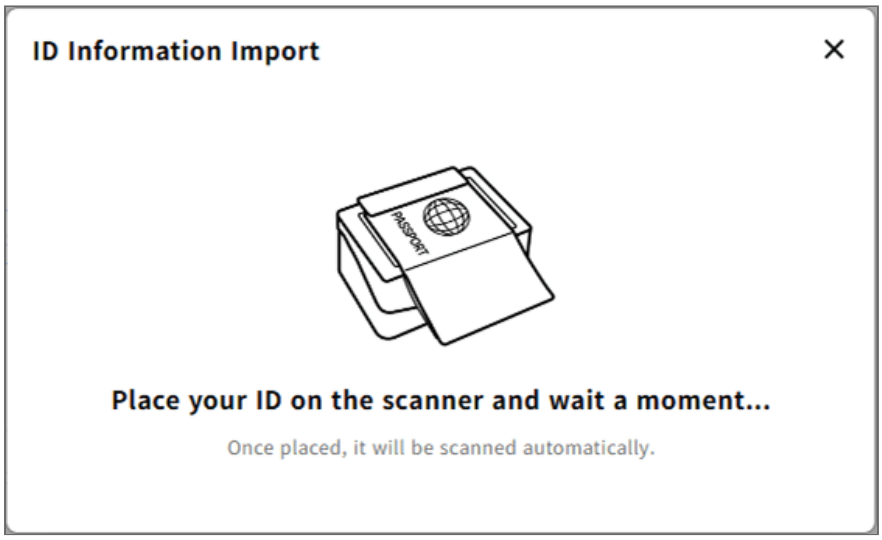
1. **Launcher** ページで **User** をクリックします。
2. **User** ページ右上の **New User** ボタンをクリックします。



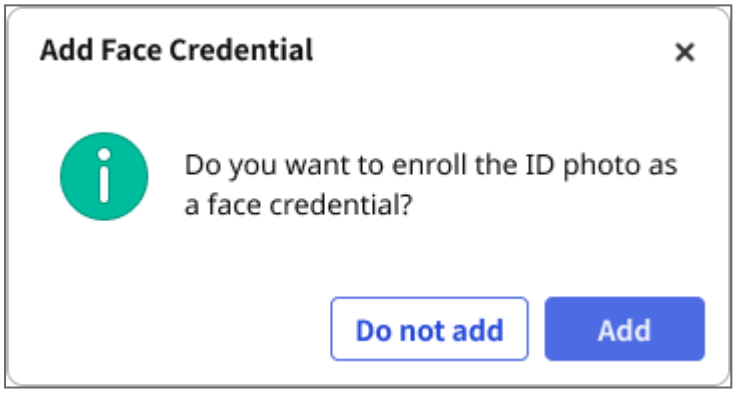
3. **Add New User**画面の右上にある**Scan ID**ボタンをクリックします。



4. **ID Information Import** ウィンドウが表示されたら、スキャナーに身分証明書を置きます。



5. 身分証明書のスキャン成功メッセージが表示されたら、身分証明書の写真を顔クレデンシャルとして登録するかどうかを選択します。

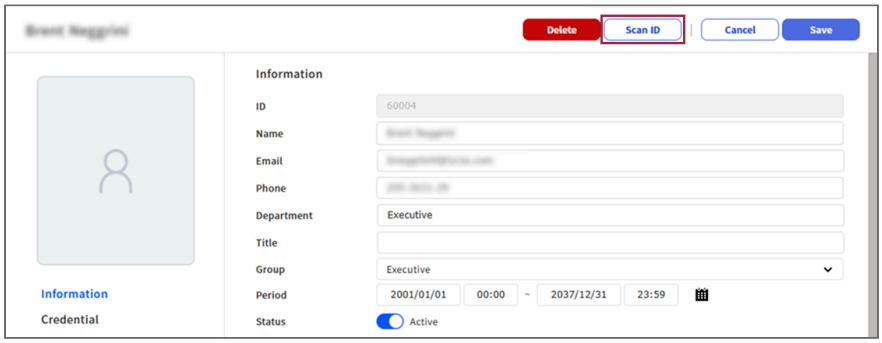


> このメッセージは、**Settings** → **Account** → **ID Scanning**で**Face Credential**オプションを**Require Confirmation**に設定すると表示されます。**Do Not Ask**オプションに設定すると、このメッセージは表示されず、すぐに顔クレデンシャルとして登録されます。

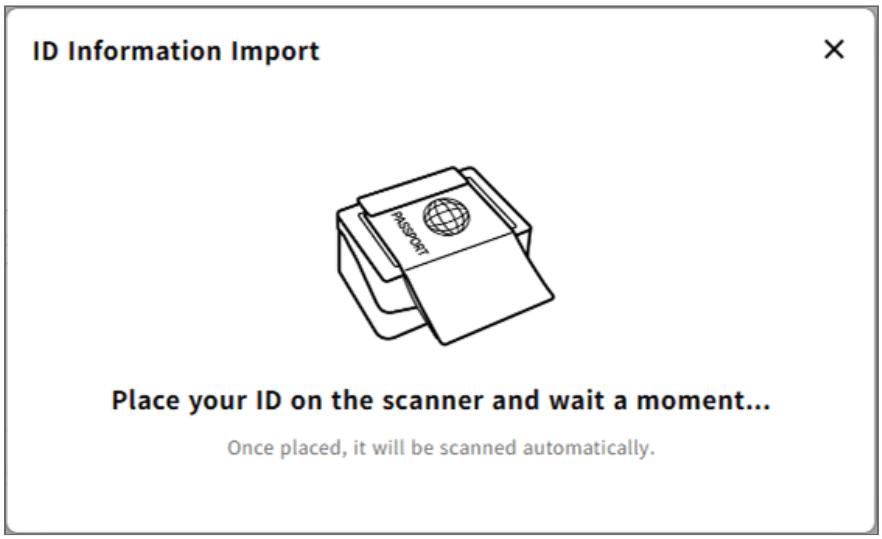
6. 身分証明書のスキャンで取得した情報を確認し、必要に応じて修正します。
7. ユーザーを保存するには、画面右上の **Save** をクリックします。

身分証明書のスキャンでユーザーを編集する

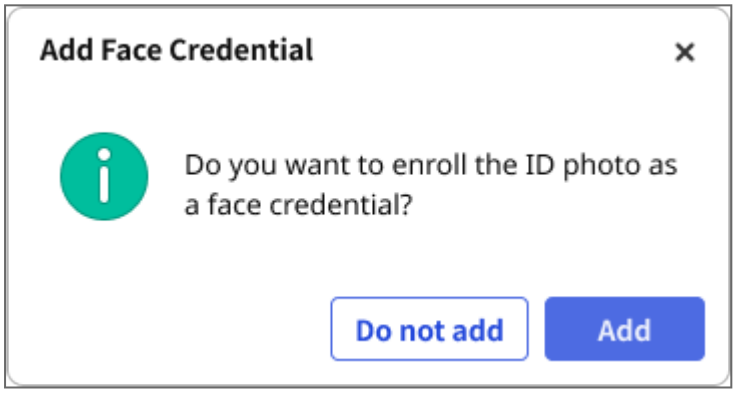
1. **Launcher** ページで **User** をクリックします。
2. ユーザーリストで、身分証明書のスキャンで編集するユーザーをダブルクリックします。
3. ユーザー情報修正画面の右上にある**Scan ID**ボタンをクリックします。



4. **ID Information Import** ウィンドウが表示されたら、スキャナーに身分証明書を置きます。



5. 身分証明書のスキャン成功メッセージが表示されたら、身分証明書の写真を顔クレデンシャルとして登録するかどうかを選択します。



> このメッセージは、**Settings** → **Account** → **ID Scanning**で**Face Credential**オプションを**Require Confirmation**に設定すると表示されます。**Do Not Ask**オプションに設定すると、このメッセージは表示されず、すぐに顔クレデンシャルとして登録されます。

6. 身分証明書のスキャンで取得した情報を確認し、必要に応じて修正します。
7. スキャンした情報でユーザー情報を修正するには、画面右上の**Save**ボタンをクリックしてください。

> **情報**
> 身分証明書のスキャンで編集するユーザーに顔クレデンシャルが2つ以上登録されている場合、最初に登録された顔クレデンシャルを上書きします。

エラーガイダンス

身分証明書のスキャン中に問題が発生すると、画面にメッセージが表示され、原因と対処方法を案内します。以下を参照してエラーを解決してください。

スキャン失敗

身分証明書をスキャナーに置き、自動認識する際に問題が発生すると、以下のいずれかのメッセージが表示されます。

原因	エラーメッセージ
身分証明書のセキュリティ要素（UV 模様など）の検証に失敗	**Invalid ID. Check the ID and try again.**
指定時間内に身分証明書を認識できない	**The ID was not scanned in time. Please try again.**
スキャン中に身分証明書が外れる、ページ認識に失敗するなど、その他のスキャンエラー	**Unable to scan the ID. Check the ID and scanner, then try again.**

上記のメッセージが表示されたら、画面に表示された**Retry**ボタンをクリックして再度スキャンしてください。身分証明書をスキャナーに正しく置いたか確認し、再試行してください。正常に認識されます。

> **情報**
> **Retry**ボタンをクリックすると、**Place your ID on the scanner and wait a moment...**の案内から自動認識を再度開始します。

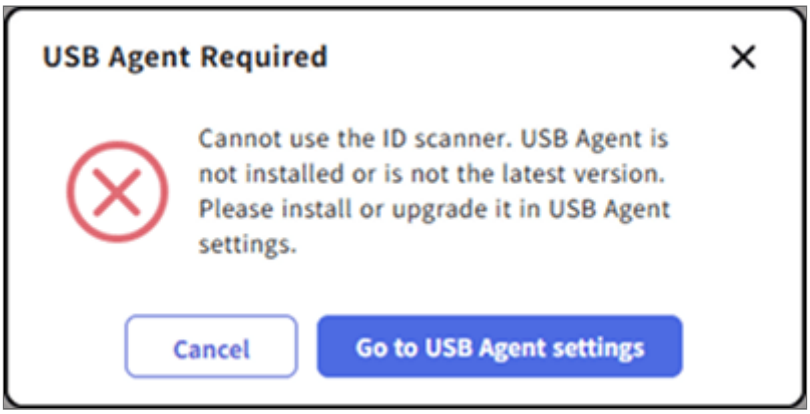
スキャナー接続エラー

スキャナーの接続に問題がある場合、以下のメッセージが表示されます。このエラーには再試行ボタンがないため、案内に従って問題を解決し、**Scan ID**ボタンを再度クリックして最初からスキャンしてください。

状況	エラーメッセージ	解決方法
スキャナーがクライアントPCに接続されていない	**The scanner is not connected. Please check the device connection and try again.**	身分証明書スキャナーとクライアント PC の接続状態を確認してください。

USB Agent を確認する

身分証明書スキャナーを使用するには、最新バージョンの USB Agent をインストールしておく必要があります。 USBエージェントがインストールされていないか、バージョンが古い場合、**Scan ID** ボタンをクリックすると、次のようなエラーウィンドウが表示されます。



- **Cancel**：エラーウィンドウを閉じ、スキャンしません。
- **Go to USB Agent settings**: **Settings** → **Device** → **USB Agent** 画面に移動します。移動した画面でUSB Agentを最新バージョンにアップグレードしてから、スキャンを再試行してください。

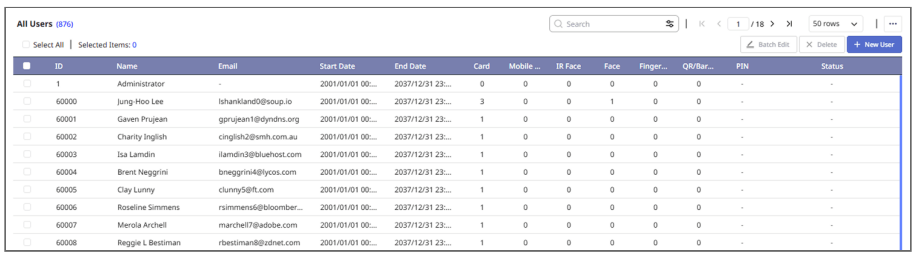
ユーザーを閲覧する

ユーザー一覧ページで登録済みユーザーを照会および管理する方法を説明します。一般検索と詳細検索を利用して目的のユーザーを素早く見つけられ、一覧の並べ替え、列設定、印刷などの機能を使用できます。

User ページにアクセスするには、**Launcher** ページで **User** をクリックするか、画面左上のショートカットリストから **User** を選択します。

ユーザー一覧を表示する

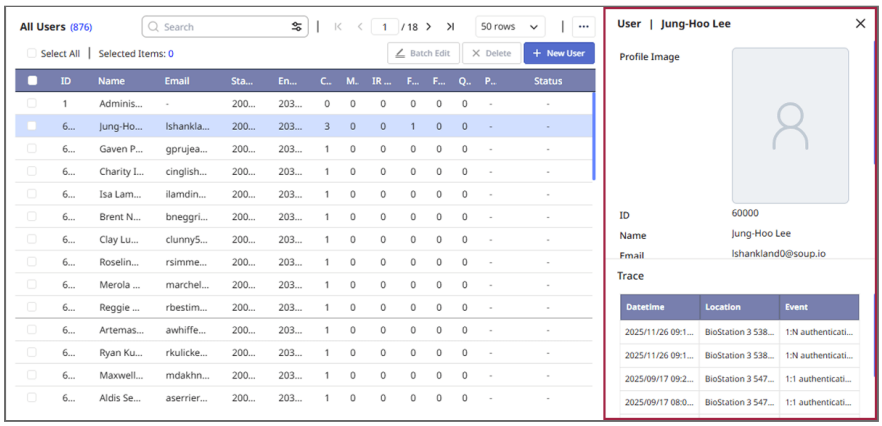
ユーザー一覧ページでは、ユーザーの基本情報と状態を確認でき、各ユーザーの詳細情報を閲覧または編集できます。



ユーザー一覧には登録済みユーザーがすべて表示され、各ユーザーのID、名前、メールアドレス、利用期間、登録済みクレデンシャル状況、状態を基本情報として確認できます。ユーザーはID順に一覧表示されます。

- 個別ユーザーの詳細情報を確認するには、ユーザー一覧で対象ユーザーをクリックします。ユーザーのプロフィール情報が画

面右側に表示されます。ユーザープロフィール情報で **See More** ボタンをクリックすると、ユーザーの詳細情報を編集できるページへ移動します。



- ユーザーの詳細情報を編集するには、ユーザー一覧で対象ユーザーをダブルクリックします。ユーザーの詳細情報を編集できるページへ移動します。

> **情報**
>
> - ユーザー情報の編集の詳細については ユーザー情報を編集 をご覧ください。
> - ユーザー一覧で列レイアウトを変更できます。列レイアウトの変更の詳細については ユーザーを閲覧する をご覧ください。

表示オプションを選択する

画面右上のツールボタンを使用して、ユーザー一覧の表示オプションを変更できます。

ユーザー一覧ページの移動

ユーザー一覧にはデフォルトで10人のユーザーが表示されます。画面上部のボタンをクリックして別のページへ移動できます。



- |< ：ユーザー一覧の最初のページへ移動します。
- < ：ユーザー一覧の前のページへ移動します。
- > ：ユーザー一覧の次のページへ移動します。
- >| ：ユーザー一覧の最後のページへ移動します。
- 指定ページへ移動するには、数値入力フィールドにページ番号を入力し、`Enter` キーを押します。

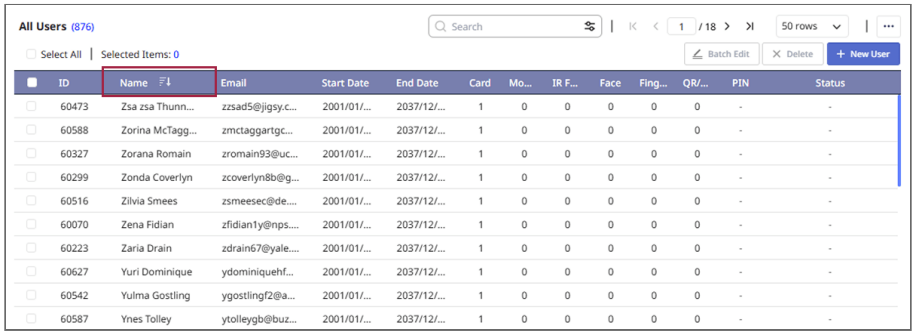
ユーザー一覧の表示件数を変更する

ユーザー一覧に表示されるユーザー数を変更できます。画面右上のリスト選択ボックスで表示件数を選択します。選択できるオプションは50件、100件、200件です。



ユーザー一覧の並べ替え

ユーザー一覧の並べ替え基準を変更できます。一覧上部の列ヘッダーをクリックすると、昇順または降順に並べ替えられます。例えば、**Name**列のヘッダーをクリックすると、ユーザー名を基準に昇順または降順で並べ替えられます。クリックした項目には昇順(⇡) または降順(⇣) のアイコンが表示されます。



> **情報**
> 列の種類によっては並べ替えできない項目があります。

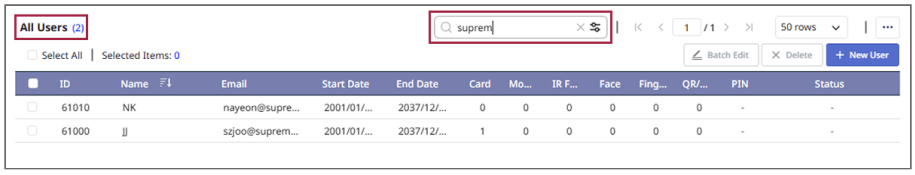
ユーザー検索

特定のユーザーを検索する方法を説明します。ユーザー一覧ページの検索機能を使って、目的のユーザーを素早く見つけることができます。

> **情報**
>
> - 検索に使用するキーワードでは大文字と小文字が区別されません。
> - ユーザーの基本情報が入力されている必要があります。ユーザーの基本情報の入力の詳細については ユーザー基本情報を入力 をご覧ください。

一般検索

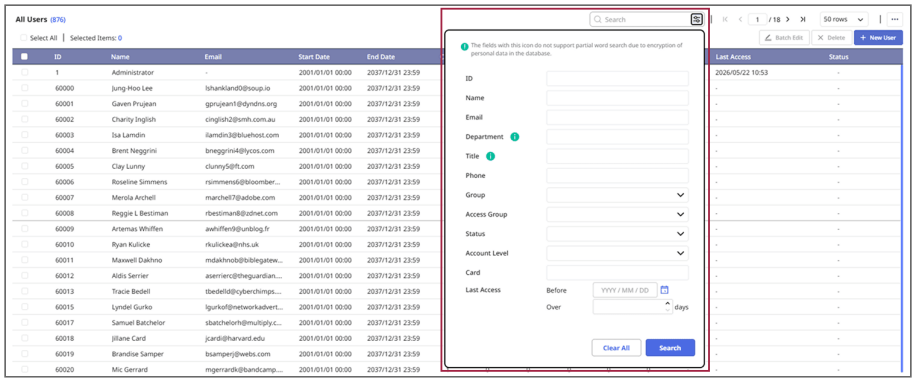
ユーザーのID、名前、メールアドレスを基準に検索できます。画面上部の検索入力フィールドにキーワードを入力し、`Enter` キーを押します。入力したキーワードと一致するユーザーが一覧に表示されます。一覧の最上部で検索結果の件数を確認できます。



高度な検索

ユーザーのID、名前、メールアドレス、電話番号などを指定して検索できます。

1. 画面上部の検索入力フィールド横にある ボタンをクリックします。
2. 詳細検索ウィンドウが開いたら、検索条件を入力し、**Search** ボタンをクリックします。



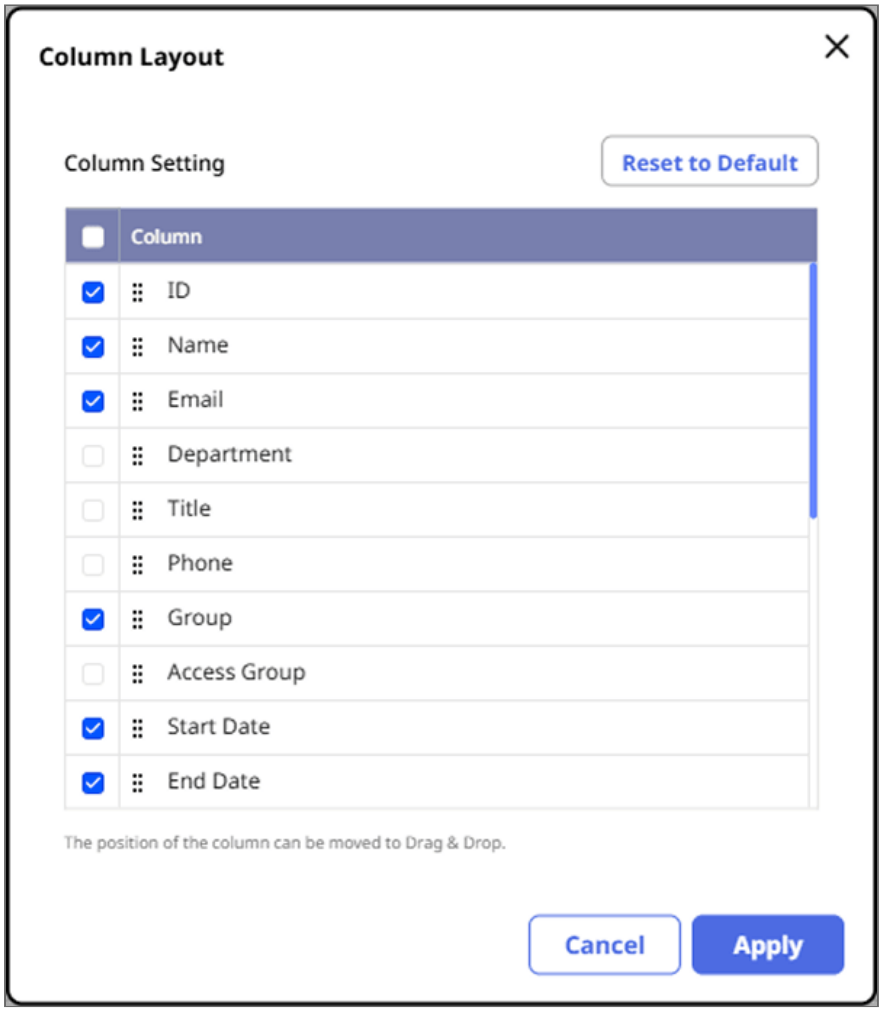
情報

- 入力フィールドのうち アイコンが表示されている項目は、個人情報DBの暗号化により完全一致でのみ検索できます。
- 詳細検索ウィンドウで入力条件をリセットするには、**Clear All** ボタンをクリックします。
- 詳細検索では **Custom User Field** の検索をサポートします。 **Custom User Field** の詳細については サーバーの詳細を設定する をご覧ください。

ユーザー一覧の列(Column)設定

ユーザー一覧で表示される列設定を変更できます。列設定で表示する列を選択したり、列の順序を変更したりできます。

1. ユーザー一覧画面右上の ボタンをクリックします。
2. **Column Layout** をクリックします。
3. **Column Layout** ウィンドウが表示されたら、必要な列を選択または選択解除します。



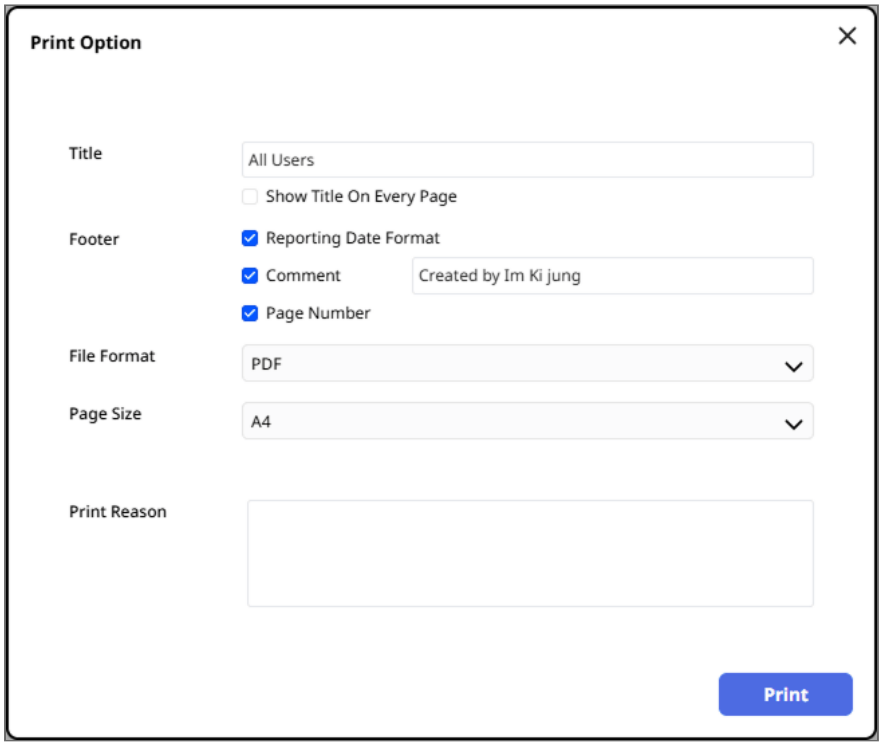
4. 列の順序を変更するには、目的の列をクリックしたままドラッグして位置を変更します。
5. 設定を保存するには、**Apply** ボタンをクリックします。

> **情報**
>
> - 列設定は各ユーザーアカウントごとに保存されます。
> - 列レイアウト設定を初期化するには、**Default Column** ボタンをクリックします。

ユーザー一覧を印刷

表示中のユーザー一覧をPDFまたはSVGファイルとして保存できます。

1. ユーザー一覧画面右上の ••• ボタンをクリックします。
2. **Print**をクリックします。
3. 「**Print Option**」ウィンドウが表示されたら、「**File Format**」オプションで目的のフォーマットを選択し、その他のオプションを設定します。



4. **Print Reason**(任意)を入力して **Print** ボタンをクリックします。

ブラウザーで開いたPDFまたはSVGファイルを印刷できます。

> **情報**
> **Print Reason** は必須入力項目ではありません。 **Print Reason** の記録は **Settings** → **Audit Trail** → **AC Audit Log** で確認できます。

ユーザー管理

登録済みユーザーを効果的に管理する方法を案内します。ユーザー情報の編集・削除、デバイスとのデータ同期、入退室履歴の追跡、ユーザーデータのエクスポート/インポートなど、ユーザー管理に必要な主要機能を段階的に説明します。

ユーザー情報を編集

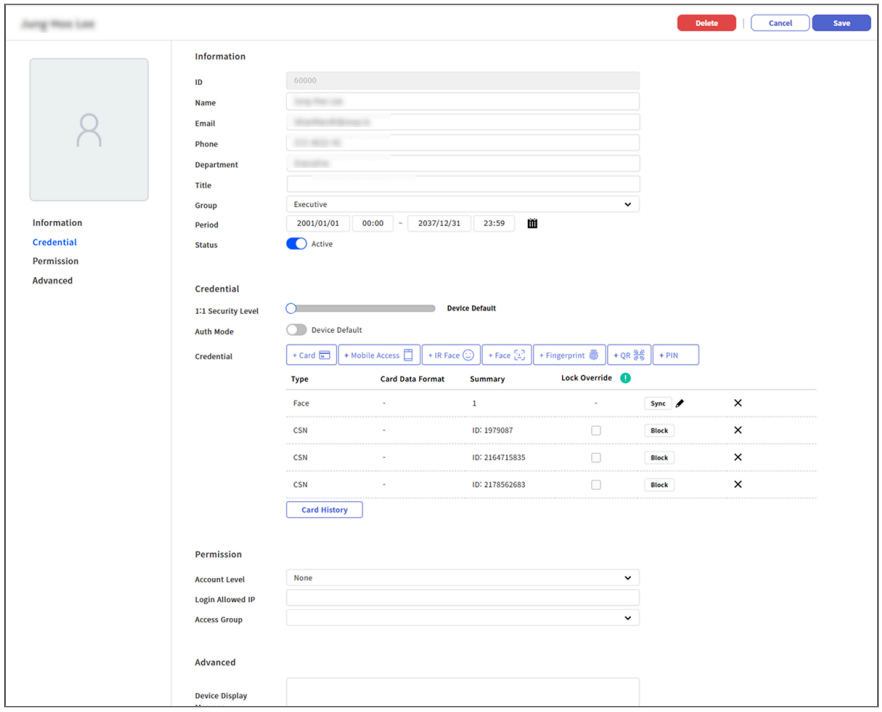
登録済みユーザーの情報を編集する方法を説明します。個別ユーザーの基本情報、アクセス権限、クレデンシャルを編集したり、複数ユーザーの情報を一括で編集します。

> **情報**
> 最初に作成されたIDが `1` のユーザーは、他の管理者が編集できません。該当アカウントでログインした本人のみが自分の情報を編集できます。

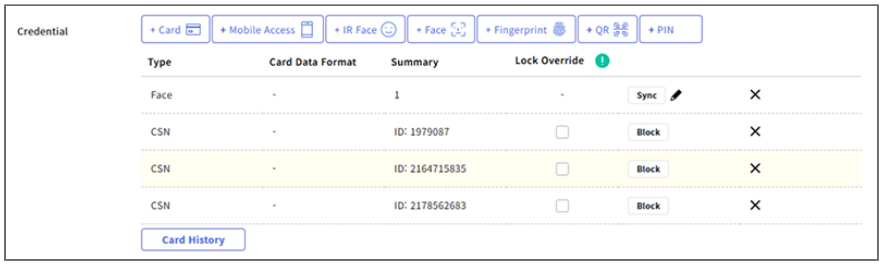
ユーザー情報を編集

1. **Launcher** ページで **User** をクリックします。
2. ユーザー一覧から編集するユーザーを選択します。

3. ユーザーをダブルクリックするか、画面右側にユーザープロフィール情報が表示されたら、**See More** をクリックします。
4. ユーザー情報を編集できるウィンドウが表示されます。



5. 必要な項目を編集します。
6. クレデンシャル項目を編集するには ✎ をクリックし、削除するには ✕ をクリックします。



7. 変更内容を保存するには、画面右上の**Save** をクリックします。

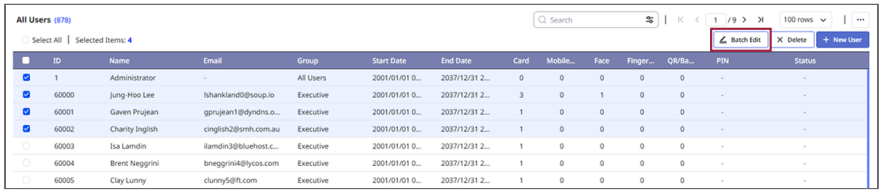
> **情報**
>
> - **Information** セクションの各項目の詳細については ユーザー基本情報を入力 を参照してください。
> - **Credential** セクションの各項目の詳細については ユーザークレデンシャルを登録する を参照してください。
> - **Permission** セクションの各項目の詳細については ユーザー権限を設定する を参照してください。
> - **Advanced** セクションでユーザーに関連する個人メッセージを入力します。

ユーザー情報を一括編集

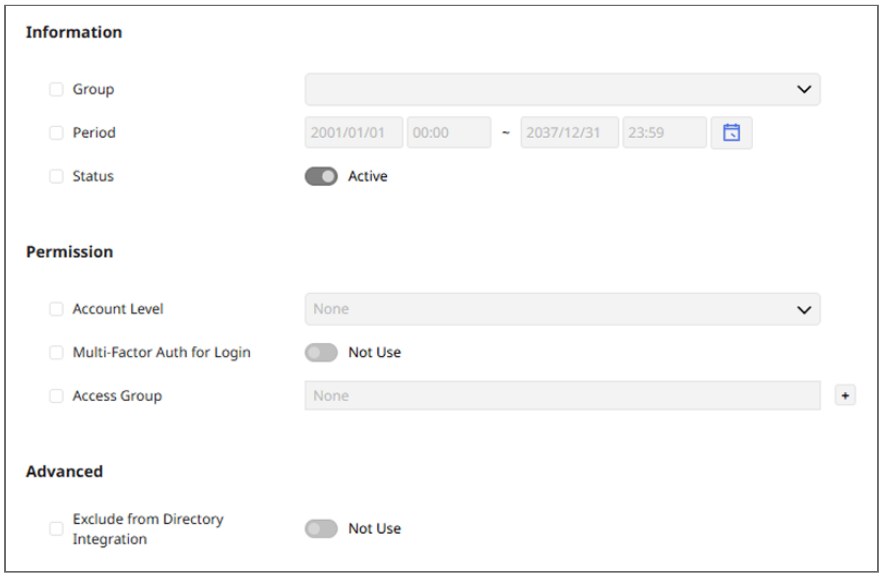
複数ユーザーの情報やアクセス権限を一度に編集します。この機能は多数のユーザーに同一のアクセス権限またはグループを設定する際に役立ちます。

1. **Launcher** ページで **User** をクリックします。

2. ユーザー一覧で編集するユーザーの最左列のチェックボックスをクリックします。 2人以上のユーザーを選択します。
3. 画面右上の **Batch Edit** ボタンをクリックします。



4. **Batch Edit** 画面が表示されたら、目的の項目のチェックボックスをクリックして編集します。



5. 編集内容を保存するには、画面右上の**Save** をクリックします。

> **情報**
>
> - ユーザーのID、名前、メールアドレス、電話番号、クレデンシャルなどの個人情報は一括編集できません。
> - 編集を取り消すには、画面右上の**Cancel** をクリックします。

次のステップ

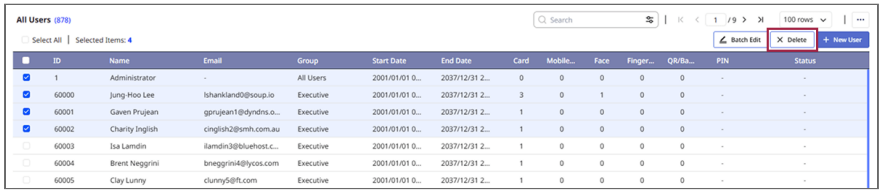
ユーザークレデンシャルを登録し、入退室認証方式を設定します。
ユーザーのアクセス権限を設定する方法を確認します。
ユーザー情報を変更したら、デバイスへ送信する必要があります。ユーザー情報をデバイスへ送信する方法を確認します。

ユーザーを削除する

退職、契約終了、セキュリティ違反などの理由で**BioStar X**に登録したユーザーを削除する場合は、次の手順に従って削除できます。

1. **Launcher** ページで **User** をクリックします。

2. ユーザー一覧で削除するユーザーの左端にある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. 画面右上の**Delete**をクリックします。



4. 確認メッセージが表示されたら**Delete**をクリックします。

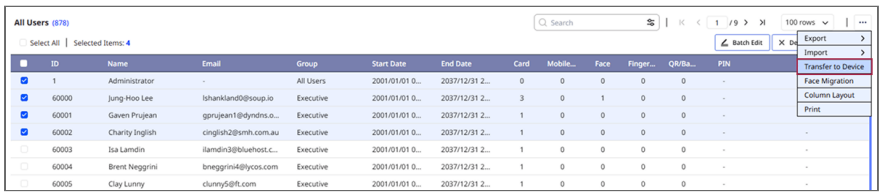
ユーザー一覧で選択したユーザーが削除されたことを確認します。

> **情報**
>
> - 1 のIDを持つユーザーは削除できません。
> - デバイスからユーザー情報を削除する方法の詳細については、デバイスに登録したユーザーを管理するを参照してください。

デバイスにユーザー情報を転送する

入退室管理のために **BioStar X** サーバーに登録したユーザー情報をデバイスへ転送する機能を提供します。デバイスへユーザー情報を転送すると、デバイスはユーザーデータを利用して入退室権限を判定し、オフライン環境でも認証を実行できます。

1. **Launcher** ページで **User** をクリックします。
2. ユーザーリストで、情報を転送するユーザーの一番左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. 画面右上の ••• ボタンを選択し、**Transfer to Device** をクリックします。



4. **Transfer to Device** ウィンドウが表示されたら、デバイス一覧でユーザー情報を転送するデバイスを選択します。



5. 同じ ID でも情報が異なる場合に **BioStar X** サーバーの内容で上書きするには、**Overwrite users with different information** オプションのチェックボックスをクリックします。

6. 転送するデバイスをすべて選択したら、**Apply** ボタンをクリックします。

選択したデバイスへユーザー情報を転送します。

> **情報**
>
> - 検索入力フィールドにキーワードを入力してデバイスを検索することもできます。
> - ユーザー情報を転送するには、デバイスが **BioStar X** サーバーに接続されている必要があります。
> - デバイスに既に登録されているユーザーの情報を変更した場合、変更内容をデバイスに反映するにはユーザー情報を再転送する必要があります。ユーザー情報をデバイスと同期する **Automatic User Synchronization** オプションを利用するには、サーバーの詳細を設定する を参照してください。
> - デバイスごとに登録できるユーザー数には制限があります。デバイスに登録できるユーザー数を確認します。

ユーザーの入退室履歴を追跡する

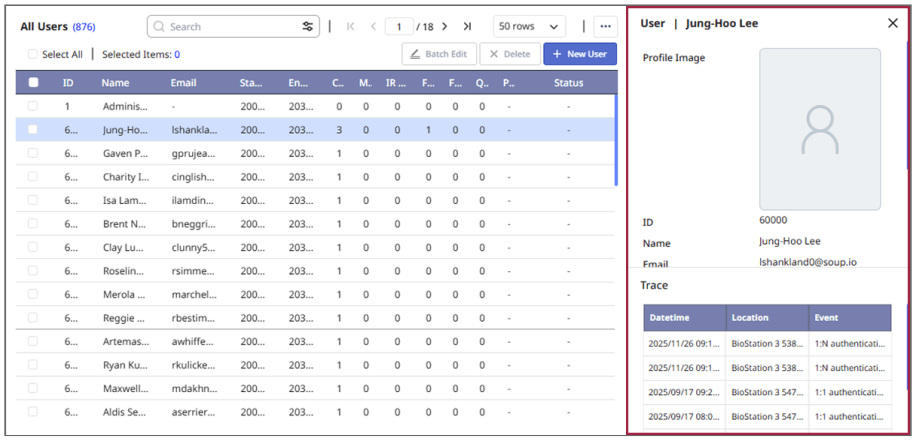
ユーザーの入退室履歴を追跡して確認することは、セキュリティを強化し運用効率を高めるうえで非常に重要です。入退室履歴を活用することで、セキュリティの脅威を防ぎ、運用を最適化できます。入退室権限のない場所や許可されていない時間帯に入退室を試みたユーザーを特定できます。これにより、セキュリティの脅威に迅速に対応できます。繰り返される認証失敗や異常な時間帯の入退室などの異常兆候を把握し、セキュリティの脅威を早期に発見できます。

次の手順に従ってユーザーの入退室履歴を確認できます。

1. **Launcher** ページで **User** をクリックします。

2. ユーザーリストで入退室履歴を確認するユーザーをクリックします。

3. 画面の右側に選択したユーザーのプロフィール情報が表示されます。



プレビュー画面の下部にある **Trace** セクションで、そのユーザーの入退室履歴を確認できます。

> **情報**
>
> - リアルタイムの入退室イベントは **Monitoring** ページで確認できます。詳しくは、イベントをモニタリングする をご参照ください。
> - 過去の入退室イベントは **Data** ページで確認できます。詳細については、データを参照してください。

ユーザー情報のエクスポート/インポート

ユーザー情報をエクスポートまたはインポートして、旧バージョンや別のサーバーのユーザー情報を利用します。

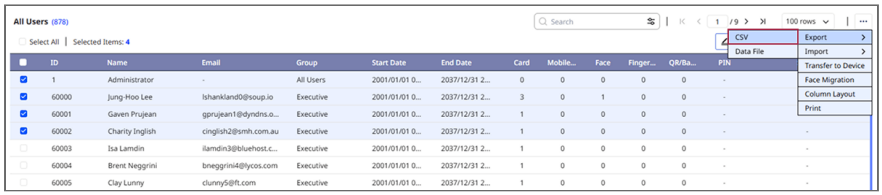
CSV エクスポート／インポート

選択したユーザー情報をCSVファイルに保存するか、保存済みのCSVファイルを読み込みます。 CSVファイルを使用して簡単にユーザー情報を移行します。

> **情報**
>
> - **BioStar X** に追加していないカスタムユーザーフィールドがある場合、CSVファイルを正しくインポートできません。カスタムユーザーフィールドの追加方法については、サーバーの詳細を設定する を参照してください。
> - 英語と韓国語以外の言語でユーザー情報を入力した場合は、CSVファイルをUTF-8で保存します。

CSV エクスポート

1. **Launcher** ページで **User** をクリックします。
2. ユーザーリストでCSVファイルに保存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. 画面右上の ••• をクリックし、**Export** → **CSV** を選択します。



4. **CSV Export** ウィンドウが表示されたら、**Export Reason**(任意)を入力し、**Download** ボタンをクリックします。



5. ローカルの任意のパスにCSVファイルを保存します。

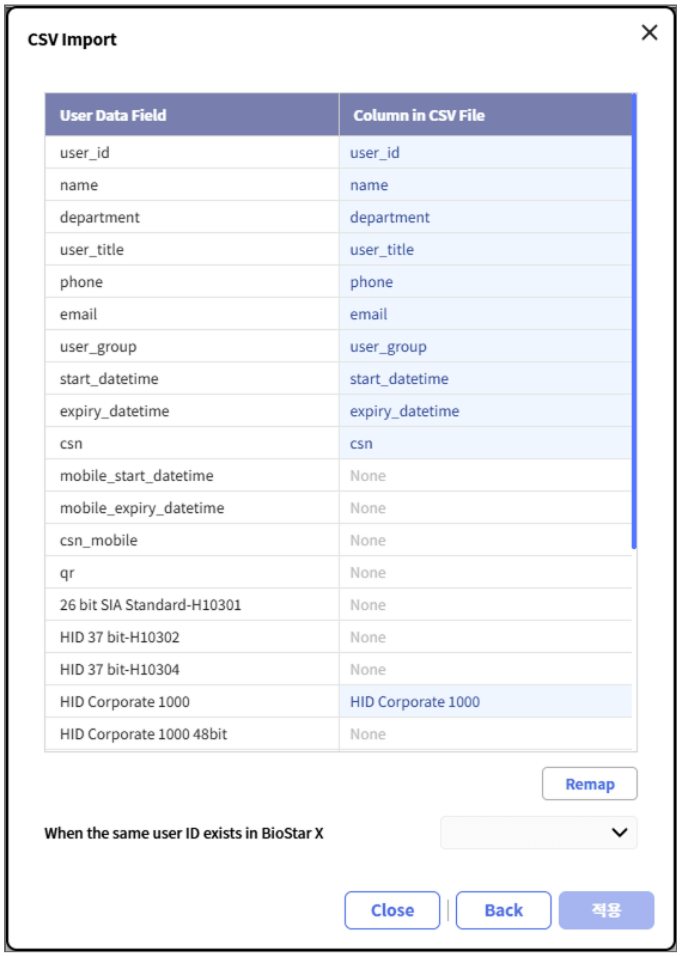
> **情報**
> **Export Reason** は必須入力項目ではありません。エクスポート理由は **Settings** → **Audit Trail** → **AC Audit Log** で確認できます。

CSV インポート

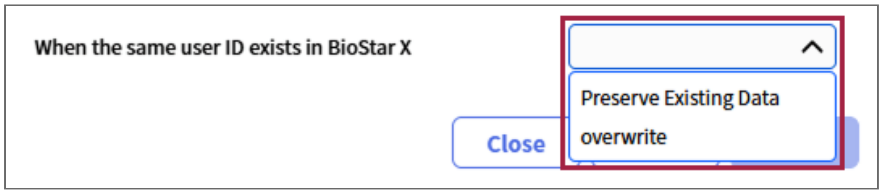
1. **Launcher** ページで **User** をクリックします。
2. 画面右上の[•••]ボタンをクリックし、**Import** → **CSV** を選択します。
3. ローカルに保存したCSVファイルを選択します。
4. **CSV Import** ウィンドウで **Start import at row** を設定し、**Next** をクリックします。



5. CSVファイルのユーザーデータフィールドと **BioStar X** のユーザーデータフィールドが自動でマッピングされて表示されます。 **Remap** をクリックすると、名前が同じフィールドが再マッピングされます。



6. **BioStar X** にすでにユーザーIDが登録されているユーザーデータを保持するか、CSVファイルの情報で上書きするかを選択し、**Apply** をクリックします。



CSVファイルの情報をインポート中にエラーが発生した場合、エラーが発生したCSVデータのみを再確認してアップロードできます。

情報

- CSVインポートでモバイルアクセスカードを発行します。レギュラーサイトを使用する場合、インポート完了後にAirfob Portalでモバイルアクセスカード1枚につき1クレジットが差し引かれます。モバイルアクセスカードを発行しない場合は、マッピングを解除します。
- CSVファイルに **BioStar X** に登録済みのユーザーに発行したモバイルアクセスカードと同一のデータが存在する場合は、データを保持するか上書きし、既存のモバイルアクセスカードを維持します。
- CSVファイルに **BioStar X** に登録済みのユーザーに発行したモバイルアクセスカードと異なるデータが存在する場合、データを保持すると既存のモバイルアクセスカードが維持され、上書きするとそのユーザーに新しいモバイルアクセスカードが発行されます。
- CSVインポートでモバイルアクセスカードを発行する際にダイナミックサイトを使用する場合は、`mobile_start_datetime` と `mobile_expiry_datetime` フィールドに必ず値を入力します。
- **BioStar X** QR はCSVインポートでは発行できません。
- CSVインポートでユーザーの顔を登録します。詳細については、顔を一括登録するを参照してください。
- CSVインポートでユーザーのPINを登録します。詳細については、PINを登録するを参照してください。
- 保存済みのCSVファイルに一致しない列を追加すると、**BioStar X** でファイルをインポートできません。
- ユーザー名の先頭が `&@~` で連続して始まる場合、該当ユーザーを CSV からインポートできません。
- 有効期限（失効日時）は 2037-12-31 23:59:59 まで設定できます。この日付を超える値を含む行はインポートに失敗します。
- エクスポートした CSV ファイルは、Excel などの表計算ソフトで直接開かないことを推奨します。ユーザー名が `=` 文字で始まる場合、プログラムが数式として認識し、実際の値と異なる表示になることがあります。

データファイル エクスポート／インポート

外部ストレージ(USB)にユーザー情報を保存し、**BioStar X** またはデバイスでインポートします。最大500,000人のユーザー情報をサーバーからデバイスへ、またはデバイス間で移行します。

情報

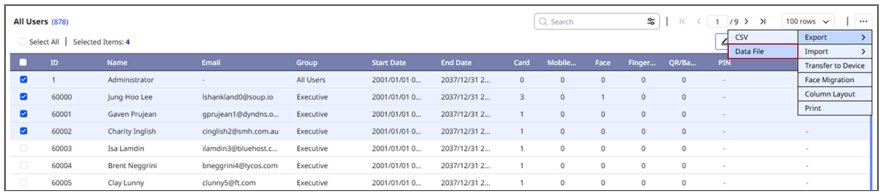
- 古いファームウェアバージョンを使用するデバイスからエクスポートしたデータは **BioStar X** にインポートできません。常に最新バージョンのファームウェアを使用してください。
- 異なる指紋テンプレート形式を使用する場合、データをインポートできません。例えば、Suprema指紋テンプレート形式を使用するデバイスからエクスポートしたデータは、ISO指紋テンプレート形式を使用するデバイスではインポートできません。
- ユーザーデータを取り込む際、**BioStar X** サーバーに登録されている指紋および顔クレデンシャルがすでに存在する場合、既存のデータは上書きされます。
- 古いファームウェアバージョンを使用するデバイスのデータはインポートできません。デバイスのファームウェアを互換バージョンにアップグレードします。

  ▼ 対応デバイスとファームウェアバージョンを表示

  - BioStation 2 ファームウェア 1.9.0 以上
  - BioStation A2 ファームウェア 1.8.0 以上
  - FaceStation 2 ファームウェア 1.4.0 以上
  - FaceStation F2 ファームウェア 2.2.0 以上
  - X-Station 2 ファームウェア 1.0.0 以上
  - BioStation 3 ファームウェア 1.3.1 以上
  - BioStation 2a ファームウェア 1.0.0 以上

データエクスポート

1. **Launcher** ページで **User** をクリックします。
2. ユーザーリストでエクスポート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. 画面右上の [•••] をクリックし、**Export** → **Data File** を選択します。



4. **Data File Export** ウィンドウで、データファイルを適用するデバイスを選択してください。



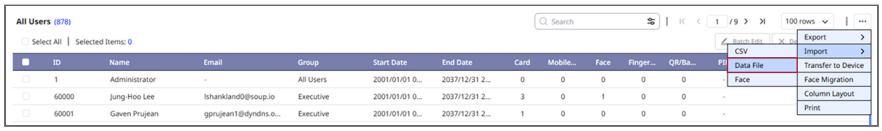
5. **Export Reason**(任意)を入力し、**Apply** ボタンをクリックします。
6. ローカルの任意のパスにデータファイルを保存します。

> **情報**
>
> - データファイルのエクスポートでは、ユーザー情報のうちプロフィール写真、ID、名前、有効期間、入退グループ、PIN、個人認証モード、クレデンシャル（顔、指紋、カード、モバイルカード、顔、QR/Barcode）、1:1セキュリティ等級情報をファイルとして保存します。
> - データファイルを適用するデバイスを正しく選択しないと、そのデバイスではデータファイルを認識できません。
> - **Export Reason** は必須入力項目ではありません。エクスポート理由は **Settings** → **Audit Trail** → **AC Audit Log** で確認できます。

> **注意**
>
> BioStar X からエクスポートしたファイルをデバイスにインポートするには、現在のデバイスが認識できるようにファイル名を以下のとおり変更する必要があります。ファイル名の形式は、今後のデバイスファームウェアのアップデートにより自動認識されるよう調整される予定です。
>
> ***BioStarX**_YYYYMMDD_HHMMSS.tgz* → ***BioStar2**_YYYYMMDD_HHMMSS.tgz*

データインポート

1. **Launcher** ページで **User** をクリックします。
2. 画面右上の [•••] をクリックし、**Import** → **Data File** を選択します。



3. ローカルに保存されているデータファイル（*.tgz*）を選択します。

データファイルのインポートに成功すると、画面にメッセージが表示されます。

アクセスグループを管理する

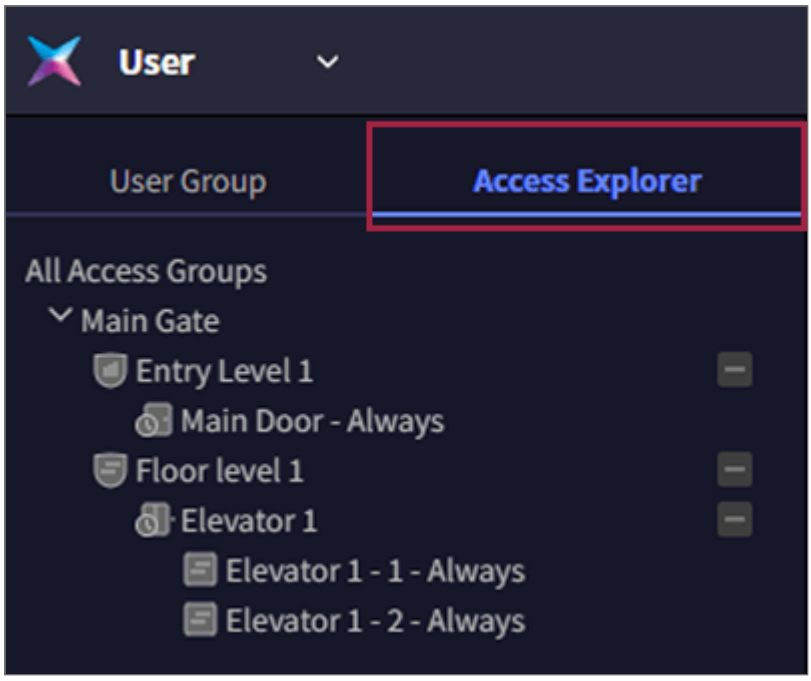
アクセスグループを基準にユーザーを検索および管理する方法を案内します。**Access Explorer**を使用して、アクセスグループごとに登録されたユーザーを確認し、ツリー構造でアクセス権限階層を探索できます。

> **情報**
>
> **Access Explorer**でアクセスグループに含まれるドアや階を確認するには、事前にアクセス制御機能を設定しておく必要があります。詳しくは 入退室制御設定 をご参照ください。

アクセスグループ別にユーザーを確認する

1. **Launcher** ページで **User** をクリックします。

2. ツリー構造メニューで**Access Explorer**タブをクリックします。



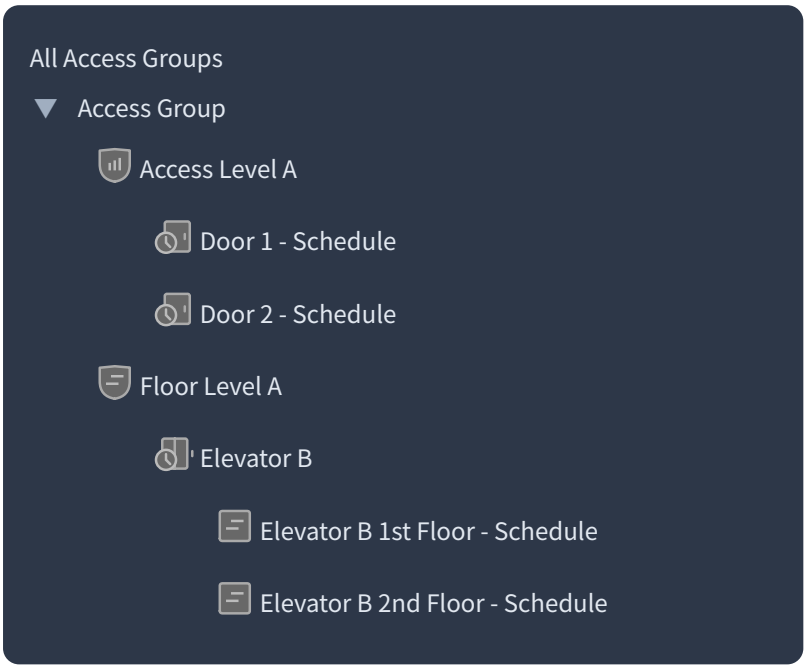
3. **All Access Groups**で目的のアクセス権限グループをクリックします。

選択したアクセス権限グループに属するユーザーをユーザーリストで確認できます。

> **情報**
>
> アクセスグループ配下のアクセスレベルまたは階レベルを展開または折りたたむには、＋ または － ボタンをクリックします。

ツリー構造を確認する

ツリー構造メニューは以下のような構成になっています。



- **アクセスグループ**はアクセスレベル、階レベル、ユーザーグループ、ユーザーを包含する上位階層です。**アクセスグループ**を通じてアクセス権限を管理できます。アクセスグループの作成の詳細は アクセスグループを管理する を参照してください。
- **アクセスレベル**はユーザーが入退室できる時間を設定し、その時間内にドアへのアクセス権限を付与します。アクセスレベルの作成の詳細は アクセスレベルを管理する を参照してください。
- **階レベル**を使用して、ユーザーがエレベーターでアクセスできる階を管理できます。フロアレベルの作成の詳細は フロアレベルを管理する を参照してください。
- **スケジュール**は入退室および休日スケジュールを設定し、アクセス制御と勤怠管理を効率的に運用する機能です。スケジュール登録の詳細は スケジュールを設定する を参照してください。
- **エレベーター**を登録し、エレベーターでアクセスできる階を管理できます。エレベーターの登録について詳しくは、エレベーターを登録する をご参照ください。

情報

エレベーター登録機能は**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。

多要素認証でログインする

BioStar X にログインする際、セキュリティを強化するために多要素認証機能を使用できます。 **Multi-Factor Auth for Login** 機能を有効にすると、ユーザー ID とパスワードの組み合わせに指紋スキャナーによる指紋認証ステップが追加されます。

情報

- **Multi-Factor Auth for Login** 機能を使用するユーザーは、指紋情報を登録し、ID とパスワード、権限レベルをすべて設定する必要があります。
- **Multi-Factor Auth for Login** 機能を使用するには、BioStar X クライアント PC に多要素認証ログインをサポートする指紋スキャナーを接続する必要があります。指紋スキャナーとしてサポートされるデバイスは以下の一覧を参照してください。
  - BioMini
  - BioMini Plus 2
  - BioMini Slim 2
- Directory Service アカウントで **Use for BioStar X Login** オプションを使用している場合、**Multi-Factor Auth for Login** 機能は使用できません。
- **Multi-Factor Auth for Login** を設定した管理者は、入退室管理以外の BioStar X サービス（勤怠管理およびビデオ）には初回認証できません。これらのサービスを使用するには、**Multi-Factor Auth for Login** 設定を解除してからログインしてください。その後、再度 **Multi-Factor Auth for Login** 設定を有効にできます。

注意

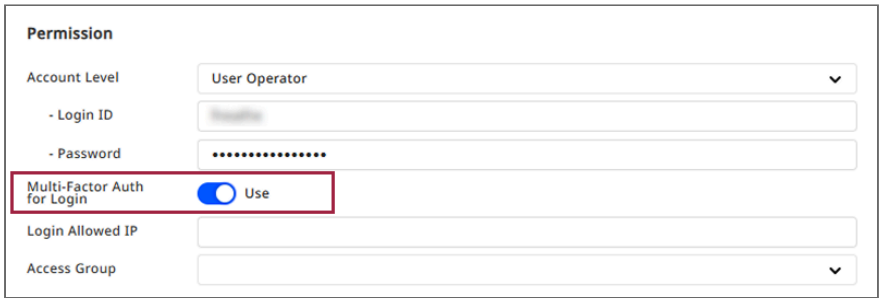
- 全体管理者（ID 1）のアカウントに多要素認証機能を設定した後に指紋認証が利用できなくなると、そのアカウントではログインできなくなるため注意してください。
- 指紋認証でログインできない場合は、Suprema グローバル技術サポートチーム までお問い合わせください。

多要素認証の設定

Multi-Factor Auth for Login を設定するには、次の手順に従ってください。

1. **Launcher** ページで **User** をクリックします。
2. ユーザー一覧で **Multi-Factor Auth for Login** を設定するユーザーをダブルクリックします。

   または、ユーザーを選択し、右側に表示されるプロファイルで **See More** ボタンをクリックします。
3. ユーザープレビュー画面が表示されたら、**Permission** セクションで **Multi-Factor Auth for Login** 項目を **Use** に設定します。



4. 画面右上の **Save** ボタンをクリックします。

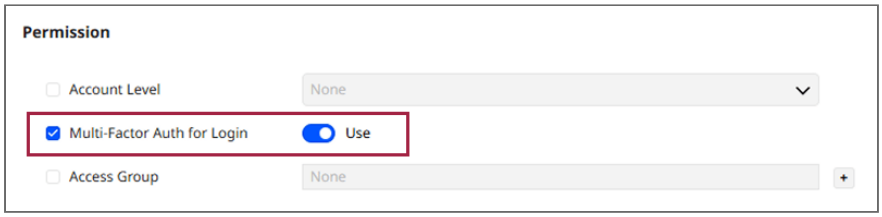
多要素認証の設定を完了します。

多要素認証の一括設定

> **始める前に**
>
> 多要素認証ログイン機能を使用するには、次の条件を満たす必要があります。
> - 当該ユーザーの指紋認証手段が登録されている必要があります。
> - **Operator**、**Login ID**、**Password** が設定されている必要があります。詳しくはユーザー権限を設定するをご覧ください。

一括編集機能を使用して、複数ユーザーに **Multi-Factor Auth for Login** 機能を適用できます。

1. **Launcher** ページで **User** をクリックします。
2. ユーザー一覧で多要素認証を設定するユーザーの最左列にあるチェックボックスをクリックします。
3. 画面右上の **Batch Edit** ボタンをクリックします。
4. 一括編集ウィンドウが表示されたら、**Permission** セクションで **Multi-Factor Auth for Login** オプションのチェックボックスを選択し、**Use** に設定します。



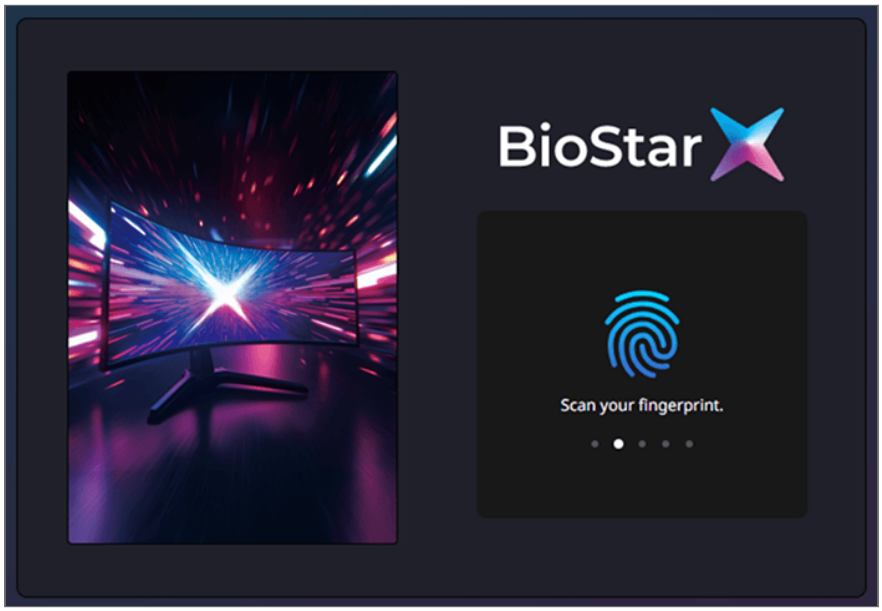
5. 画面右上の **Save** ボタンをクリックします。

選択した複数ユーザーの多要素認証設定を完了します。

> **情報**
> 選択したユーザーのうち、**Multi-Factor Auth for Login** 機能を有効にするための条件を満たしていないユーザーは、ポップアップメッセージの **Not applicable user(s)** リストで確認できます。設定に必要な条件を確認し、再試行してください。

多要素認証でログイン

1. Web ブラウザーで BioStar X のログイン画面にアクセスします。
2. ユーザー ID とパスワードを入力し、**Login** ボタンをクリックします。
3. 指紋入力画面が表示されたら、指紋スキャナーで指紋をスキャンします。



ログインを完了します。

> **情報**
> - 指紋スキャンの制限時間は 18 秒に固定されており、変更できません。
> - 最大 3 回まで連続して指紋をスキャンでき、3 回のスキャンで正しく読み取れない場合は認証失敗となります。
> - 認証に失敗した場合は、**Retry** ボタンをクリックして指紋認証を再試行します。最大 2 回まで再試行できます。再試行回数内で認証に失敗した場合、ログイン初期画面に戻ります。

顔を一括登録する

ユーザーの顔を一括登録する方法を説明します。 CSVファイルのインポート機能を使用するか、ユーザーIDと同じファイル名の顔写真を読み込み登録することで、複数のユーザーの顔を一度に登録できます。また、複数のユーザーにメールで顔登録リンクを送信し、モバイルデバイスで直接顔を登録させることもできます。

開始する前に

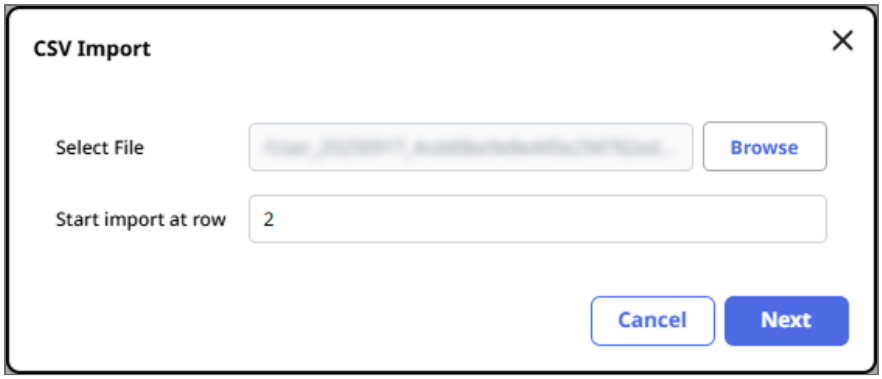
顔の一括登録を開始する前に、ユーザーの顔画像を準備してください。

- 顔画像ファイルはすべて同じフォルダーに保存しておく必要があります。顔画像ファイル名はユーザーIDと同じである必要があります。
- 対応する画像ファイルのサイズは最大10MBです。
- 対応する画像ファイル形式はJPG、JPEG、PNGです。

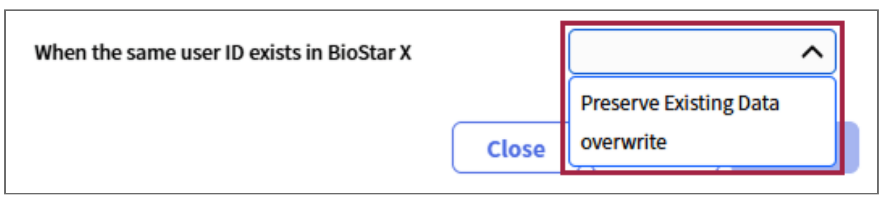
CSVファイルのインポートで登録

CSVインポート機能でユーザーの顔を一括登録できます。

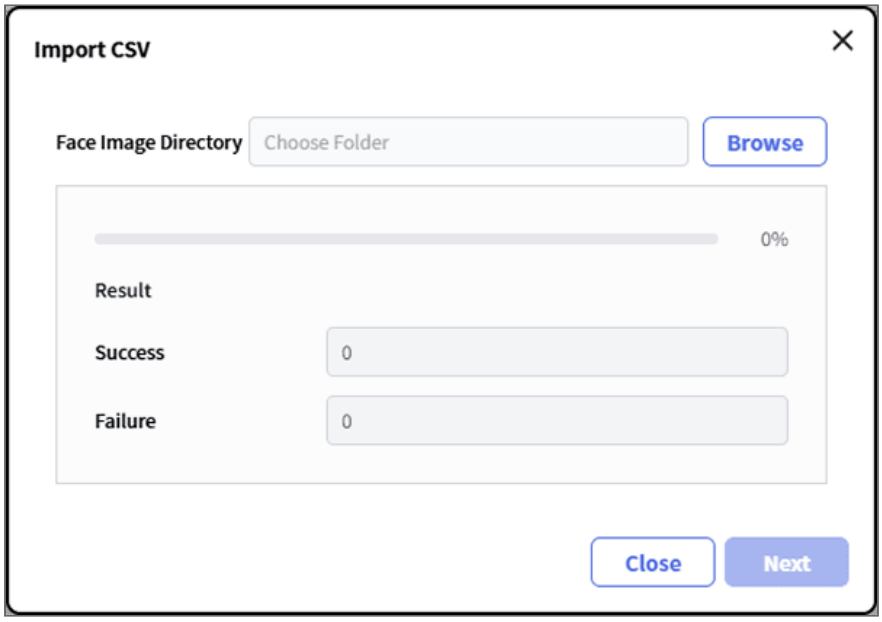
1. **Launcher** ページで **User** をクリックします。
2. ユーザー一覧で顔を登録するユーザーのチェックボックスをクリックしてください。 1 人以上のユーザーを選択できます。
3. 画面右上の ••• をクリックし、**Export** → **CSV** を選択します。
4. CSVエクスポートウィンドウが表示されたら、**Download** をクリックしてください。
5. ローカルの任意のパスにCSVファイルを保存します。
6. CSVファイルを開き、face_image_file1 、face_image_file2 列を追加してください。
7. 追加した列に顔画像ファイル名（拡張子を含む）を入力して保存してください。
8. 画面右上の ••• ボタンをクリックし、**Import** → **CSV** を選択します。
9. 編集したCSVファイルを選択してください。
10. CSVインポートウィンドウが表示されたら、**Start import at row** を設定し、**Next** をクリックしてください。



11. すでに **BioStar X** に登録されているユーザーデータを保持するか、CSVファイルの情報で上書きするかを選択し、**Apply** をクリックしてください。



12. **Face Image Directory** 項目で **Browse** をクリックしてください。



13. 顔画像が保存されているパスを選択し、**Upload** をクリックしてください。
14. CSVインポートを完了するには、**Next** をクリックしてください。

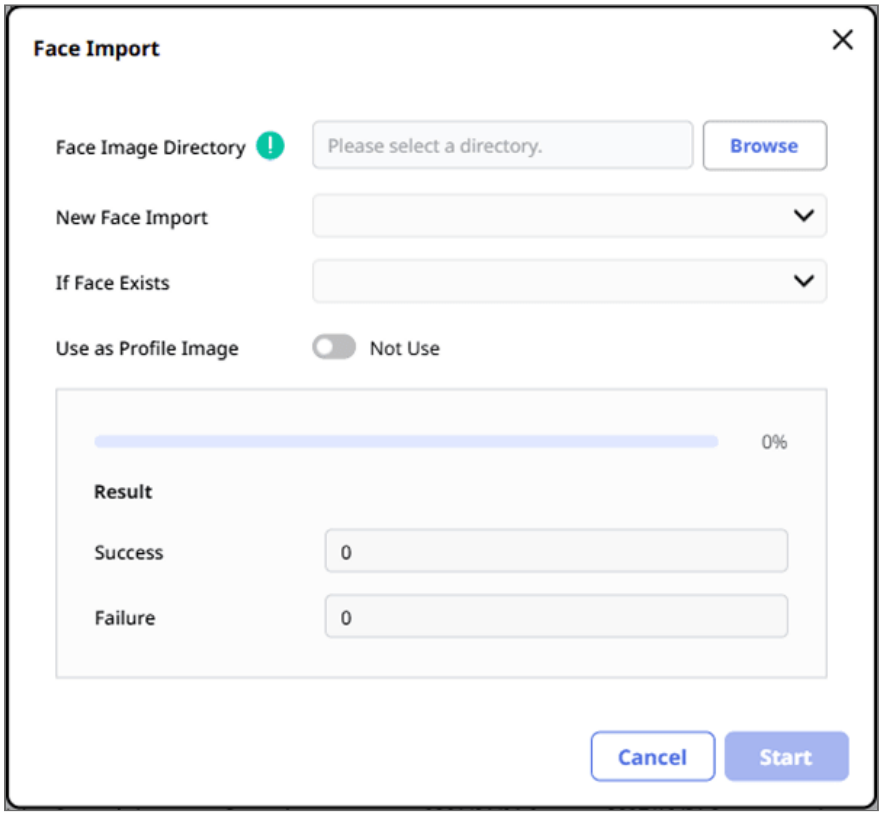
CSVファイルの情報をインポート中にエラーが発生した場合、エラーが発生したCSVデータのみを再確認してアップロードできます。

> **情報**
> インポートするCSVファイルと顔画像ファイルは同じパスに置くことを推奨します。

顔をインポート

ユーザーIDと一致するファイル名の顔写真を読み込み、顔認証用として登録できます。開始する前にユーザーの顔画像ファイルを準備してください。顔画像ファイル名はユーザーIDと同じである必要があります。

1. **Launcher** ページで **User** をクリックします。
2. 画面右上の [•••] をクリックし、**Import** → **Face** を選択してください。
3. **Face Import** ウィンドウが表示されたら、**Browse** をクリックしてください。



4. 顔画像が保存されているパスを選択してください。
5. **New Face Import** オプションで、顔画像をインポートする方法を選択してください。
   - **Import image files whose name matches user ID**：顔画像ファイル名とユーザーIDが一致する画像をインポートします。
   - **Import image files whose name matches user ID + Add new user by using file name as user ID**：登録済みのユーザーIDと顔画像ファイル名が一致する場合はその画像をインポートし、一致しない場合はファイル名をユーザーIDとして新規ユーザーを作成し、顔認証手段として登録します。
6. **If Face Exists** オプションで、**Preserve data** または **Overwrite** を選択してください。
   - **Preserve**：登録済みユーザーの顔画像を保持します。
   - **Overwrite**：登録済みユーザーの顔画像を新しい顔画像で上書きします。
7. インポートした顔画像をプロフィール画像として使用する場合は、**Use as Profile Image** オプションをクリックして有効にしてください。
8. **Start** をクリックしてください。

顔写真ファイルのインポート中にエラーが発生すると、エラーが発生した写真の一覧が表示されます。一覧を確認して再試行してください。

> **情報**
> 顔画像はユーザーIDごとに1枚のみインポートできます。

モバイルデバイスで顔を登録

ユーザーにメールで顔登録リンクを送信できます。ユーザーはモバイルデバイスでそのリンクにアクセスし、顔を直接登録できま

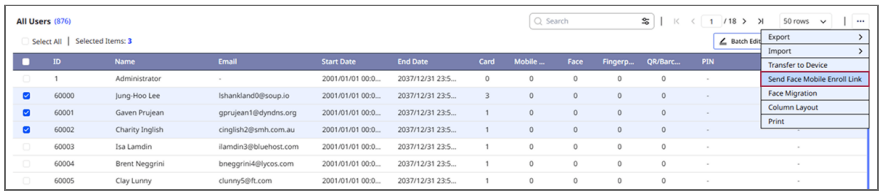
す。

開始する前に

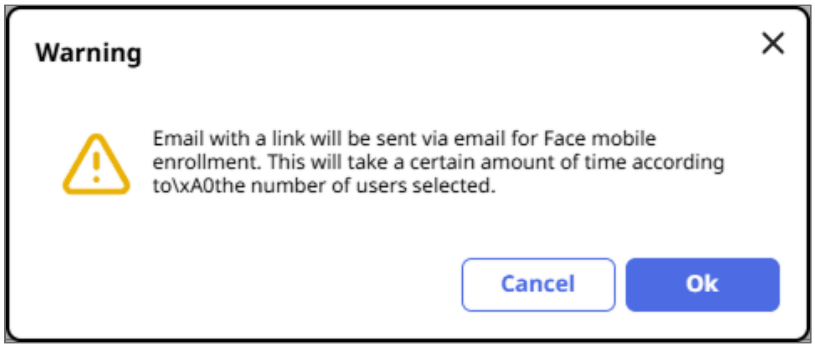
- モバイル顔登録機能を使用する前に、SMTP設定を含むメール情報設定を完了してください。 詳細については 次のドキュメント を参照してください。詳細については、メールを設定するご参照ください。
- モバイル顔登録機能は **Remote Access** 機能を有効にすると使用できます。 **Remote Access** の詳細については リモートアクセスを設定する をご参照ください。

顔登録リンクを送信

1. **Launcher** ページで **User** をクリックします。
2. ユーザー一覧で顔を登録するユーザーのチェックボックスをクリックしてください。 1 人以上のユーザーを選択できます。
3. 画面右上の ••• をクリックし、**Send Face Mobile Enroll Link** を選択してください。



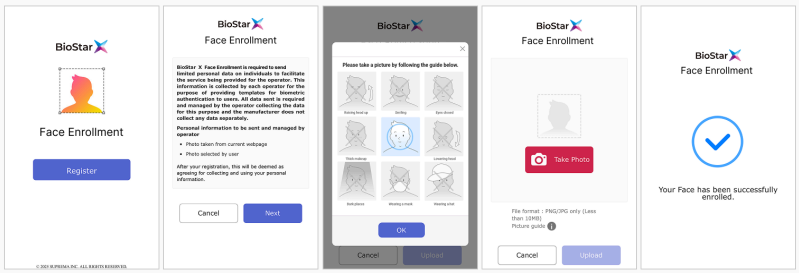
4. メッセージウィンドウが表示されたら、**Ok** をクリックしてください。



選択したユーザーのメールアドレスに顔登録リンクを送信します。ユーザーがアップロードを完了すると、ユーザー情報に顔情報が追加されます。

情報

- **Audit Trail** でメール送信の成否を確認できます。詳細については、監査トレイルを管理するご参照ください。
- 顔登録モバイルリンクからアクセスするページに表示される言語は、モバイル端末で使用しているブラウザーの言語設定に従います。
- ユーザーが受信した顔登録モバイルリンクにアクセスすると、以下のように顔登録サービスが起動します。画面の指示に従って進めてください。



- 対応する画像ファイルのサイズは最大10MBです。
- 対応する画像ファイル形式はJPG、JPEG、PNGです。
- 送信された顔登録モバイルリンクは24時間後に失効します。
- 顔写真のアップロードが完了し、モバイル顔登録に成功すると、登録成功のメッセージが表示されます。登録に失敗した場合は、登録失敗メッセージと失敗理由が表示され、ユーザーは別の写真を使用して顔登録を再試行できます。

顔マイグレーション

BioStar X の旧バージョンで登録した顔を最新のアルゴリズムにアップグレードして認識性能を向上できます。ユーザーを同期する際、顔画像を除いたテンプレートのみを送信するようプロトコルを改良し、同期に要する時間を大幅に短縮するとともに個人情報に関する問題の発生を防止できます。

開始する前に

顔マイグレーション機能を実行する前に、次の事項を確認してください。

顔マイグレーションとは？

BioStar X サーバーにすでに保存されているユーザーの画像から 2 種類の顔テンプレートを生成する機能です。ユーザー同期時に顔をテンプレートのみで同期するには、**Face Migration** を実行する必要があります。

対応デバイスおよびファームウェアバージョン

顔をテンプレートとして同期できるデバイスの一覧は以下を参照してください。

- BioStation 3 Max ファームウェア v1.0.0 以上
- BioEntry W3 ファームウェア v1.0.0 以上
- BioStation 3 ファームウェア v1.3.1 以上

- FaceStation F2 ファームウェア v2.2.0 以上

▼ FaceStation F2 v1.x.x ファームウェアのサポート終了案内

BioStar X は、ユーザーの顔をデバイスへ同期する際にテンプレートのみを送信するよう変更し、同期性能を最適化しました。そのため、デバイスでのみテンプレートを抽出できる FaceStation F2 v1.x.x ファームウェアのサポートは終了します。現在 FaceStation F2 の 1.x.x バージョンのファームウェアを使用している場合、**BioStar X** を利用するには FaceStation F2 を最新ファームウェアへアップグレードしてください。

最新ファームウェアは Suprema ダウンロードセンターからダウンロードできます。

顔テンプレートタイプに関する注意事項

BioStation 3 Max、BioEntry W3、BioStation 3、FaceStation F2 は、顔テンプレートの形式がそれぞれ異なります。

- **NPU タイプ**：BioStation 3 Max、BioEntry W3、BioStation 3
- **GPU タイプ**：FaceStation F2

- **顔テンプレートタイプが異なるデバイス間での同期所要時間**

  Face Migration を実行する前に、FaceStation F2 のみを接続して使用していた環境に BioStation 3 Max、BioEntry W3、BioStation 3 を追加して同期すると、テンプレート形式が異なるため画像から NPU タイプのテンプレートを抽出することになり、サーバーに登録されている顔の数によってはかなり時間がかかる場合があります。

- **BioStar X での顔登録を推奨**

  デバイスの **顔画像を保存** オプションを無効にした状態で顔を登録した場合、**BioStar X** にはテンプレートのみが同期されるため、顔テンプレートタイプが異なるデバイスへは同期できません。したがって、顔は **BioStar X** で登録することを推奨します。

デバイスに関する注意事項

BioStar X からエクスポートしたユーザーデータファイルには画像が含まれずテンプレートのみのため、旧ファームウェアを使用している FaceStation F2 および BioStation 3 へはユーザーデータファイルをインポートできません。

そのため、FaceStation F2 および BioStation 3 でデータファイルをエクスポートする場合は、以下のバージョン以上でのみエクスポートが可能です。

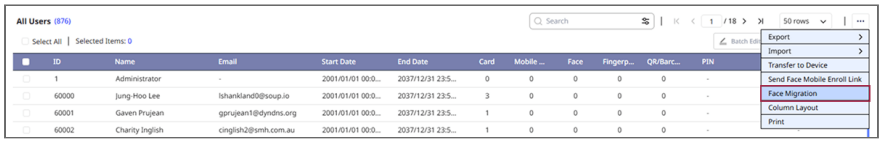
- FaceStation F2 ファームウェア v2.2.0 以上
- BioStation 3 ファームウェア v1.3.1 以上

注意

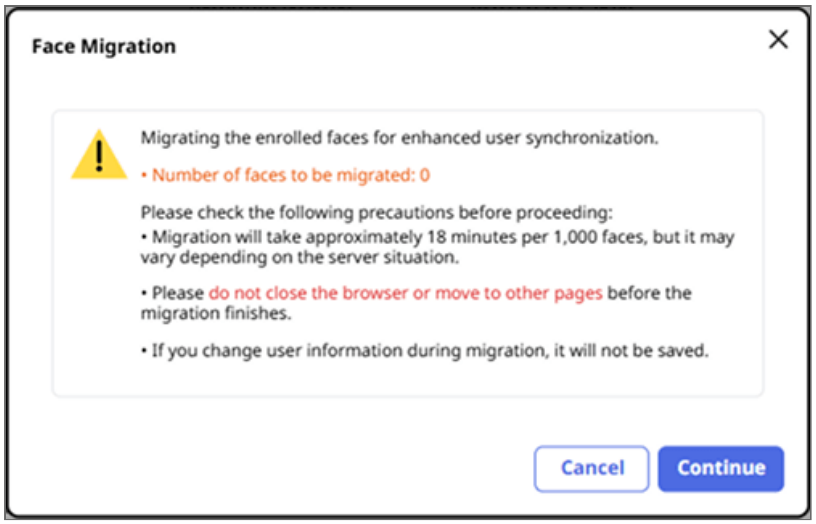
FaceStation F2、BioStation 3 を使用している場合は、最新バージョンのファームウェアへアップグレードすることを推奨します。最新ファームウェアは Suprema ダウンロードセンターからダウンロードできます。

マイグレーションを実行

1. **Launcher** ページで **User** をクリックします。
2. 画面右上の ••• ボタンを選択し、**Face Migration** ボタンをクリックしてください。



3. 警告ポップアップの内容を確認し、**Continue** をクリックしてください。



顔マイグレーションを実行します。顔マイグレーションが完了すると、総顔数、成功件数および失敗件数を確認できるポップアップが表示されます。

- マイグレーションが成功したら、デバイスにユーザー情報を同期して変更を適用してください。デバイスにユーザー情報を送信する方法の詳細については、デバイスにユーザー情報を転送する をご参照ください。
- 顔マイグレーションに失敗した場合、失敗したユーザーの一覧を CSV ファイルでダウンロードできます。マイグレーションに失敗した顔を一括削除するには、**Delete** ボタンをクリックしてください。

情報

- この機能は、ユーザー ID が 1 の管理者アカウントのみ使用できます。
- マイグレーションを実行中は、現在のページから離れないでください。
- ユーザーによっては、登録された顔画像のサイズが大きいほどテンプレート生成に時間がかかる場合があります。
- 顔 1,000 件の場合の所要時間は約 18 分で、サーバーの性能によって異なる場合があります。
- ユーザーの顔画像をサーバーに保存せず、テンプレートのみを保存する方法の詳細については、サーバーの詳細を設定する をご参照ください。

緊急開放権限を設定する

緊急時に特定のユーザーがすべてのドアにアクセスできるよう緊急開放権限を設定できます。緊急開放権限が設定されたカードでドアを開放すると、そのドアは開いたままになり誰でも通行できます。

開始する前に

緊急開放権限を設定する前に、まずカードクレデンシャルを追加する必要があります。カード認証情報の追加方法については、入退室カードを登録するをご参照ください。

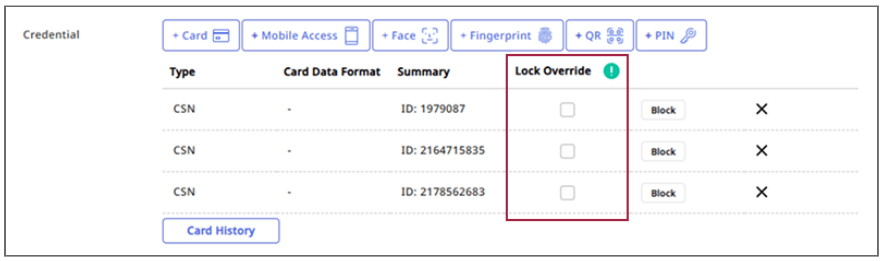
情報

- カードクレデンシャル以外のクレデンシャルはサポートしていません。
- スマートカード（AoC）、ToMモバイルアクセスカード（ToM AoC）を除くすべてのカードクレデンシャルをサポートします。
- デバイスによっては緊急開放機能をサポートしていない場合があります。サポートされるデバイスとファームウェアバージョンは以下を参照してください。
  - BioStation 3 Max ファームウェア v1.0.0 以上
  - XPass Q2 ファームウェア v1.0.0 以上
  - BioStation 3 ファームウェア v1.4.0 以降

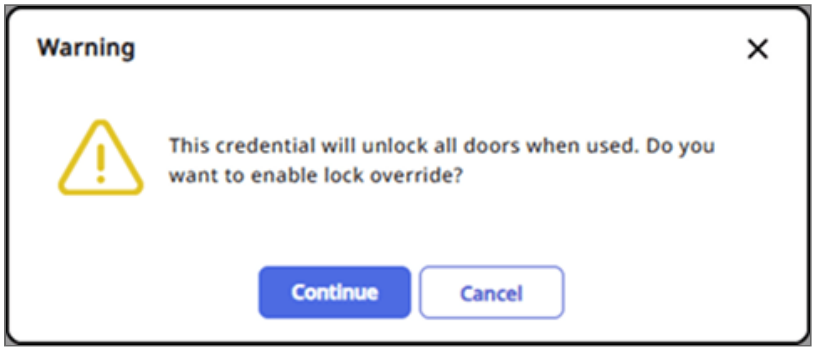
緊急開放権限を設定する

1. **Launcher** ページで **User** をクリックします。
2. ユーザーリストで緊急開放権限を設定するユーザーをダブルクリックします。

   または、ユーザーを選択し、右側に表示されるプロファイルで **See More** ボタンをクリックします。
3. ユーザー詳細画面が表示されたら、**Credential** セクションに移動します。
4. 緊急開放を許可するカードクレデンシャルの **Lock Override** 項目のチェックボックスをクリックします。



5. 警告メッセージが表示されたら内容を確認し、**Continue** をクリックします。



6. 画面右上の **Save** ボタンをクリックします。

緊急開放権限の設定が完了します。

注意

ユーザーは緊急開放権限が設定されたカードで全てのドアを開放できます。

情報

- 緊急開放権限を付与するカードクレデンシャルは1枚以上選択できます。
- 緊急開放権限を解除するには、選択したカードクレデンシャルの **Lock Override** 項目のチェックボックスを再度クリックします。

モニタリング

BioStar X の主要機能の 1 つである **Monitoring** ページで利用できる機能について案内します。

Launcher ページで **Monitoring** をクリックするか、画面左上のショートカットリストから **Monitoring** を選択してください。

ドアをモニタリング

ドア監視はセキュリティシステムの主要機能の一つで、ドアの状態をリアルタイムで確認および制御できます。本ドキュメントでは、ドアとエレベーター、高度なアクセス制御をモニタリングおよび制御する方法を案内します。これにより、効率的なセキュリティ管理と迅速な対応が可能になります。

状態を確認

ドア、エレベーター、高度入退室制御の状態をリアルタイムで監視し、セキュリティシステムを安定的に運用できます。**Monitoring** が提供するステータスアイコンでアラームと異常状態を一目で確認し、対応が必要なものだけをまとめて、即座に対応してください。

Launcher ページで **Monitoring** をクリックするか、画面左上のショートカットリストから **Monitoring** を選択してください。画面左のサイドバーにある **Door** タブで各項目の状態を確認します。

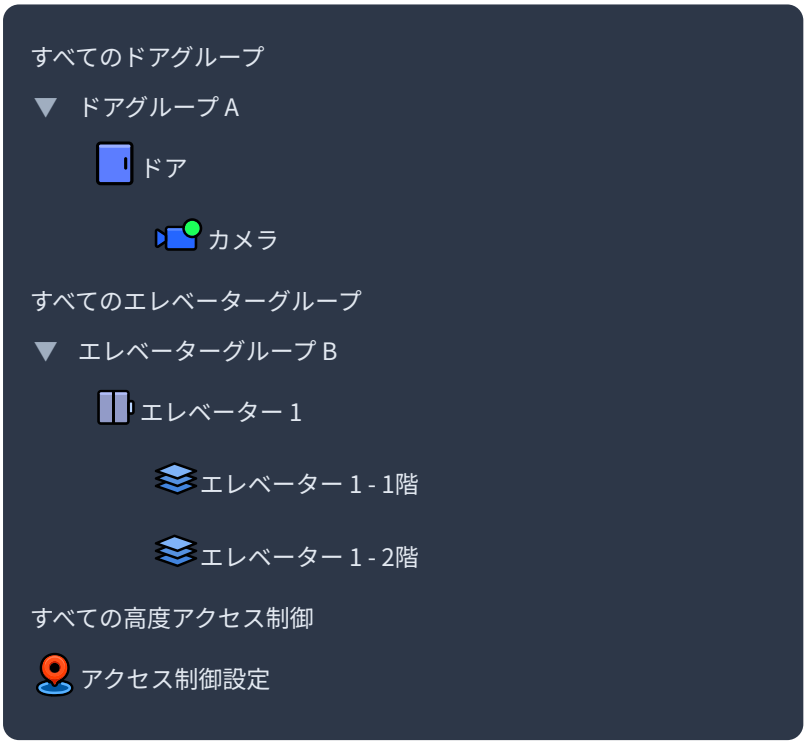
開始する前に

ドアに接続されたデバイスが正しく構成されているか確認してください。デバイスがネットワークに接続され、最新ファームウェアに更新されているか確認することが重要です。問題が発生した場合は、まずデバイスの電源状態とネットワーク接続を確認してください。

> **情報**
>
> - デバイスの追加・構成の詳細はデバイス管理をご覧ください。
> - ドアの追加・設定の詳細はドア管理をご覧ください。
> - ドアの状態をモニタリングまたは制御するには、**Log Upload** 機能を有効にする必要があります。この機能は、**Settings** → **System** → **Server** のメニュー経路にある **General** セクションで有効化してください。
> - VMSサーバーと連携してカメラをドアに紐付ける機能は、**エッセンシャル** (Essential) 以上のライセンス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。

ツリー構造を確認

画面左のサイドバーにある **Door** タブのツリーは次のような構成です。



情報

- デバイスの追加・構成の詳細はデバイス管理をご覧ください。
- ドアの追加・設定の詳細はドア管理をご覧ください。
- エレベーターの追加・設定の詳細はエレベーター管理をご覧ください。
- 高度なアクセス制御の設定の詳細は高度な入退室制御設定をご覧ください。
- ドアとカメラを連携する方法についてはビデオルールを設定するをご覧ください。

状態を確認

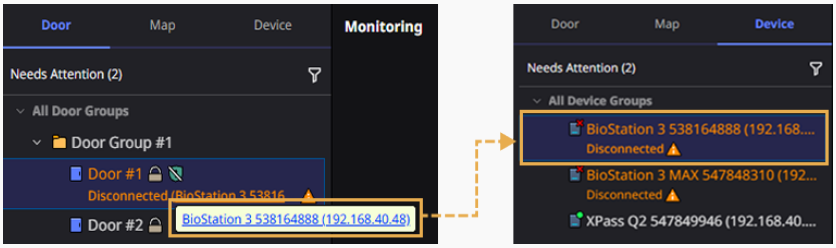
接続エラーとアラームを確認

ドアまたはエレベーターの状態を確認して、正常に動作しているか把握できます。各アイコンの状態は以下を参照してください。

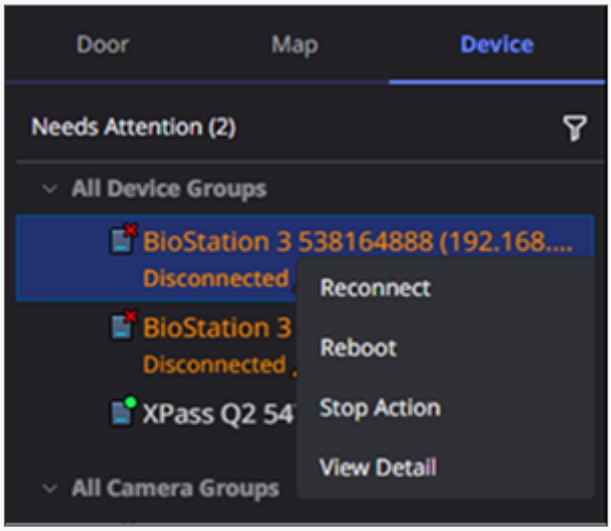
ステータスアイコン	説明
	デバイスの切断、マルチ通信サーバーエラー、同期エラーなどの異常状態を表示します。
	ドア、エレベーター、高度入退室制御、AI映像解析アラームが発生している状態を表示します。

ヒント

ステータスアイコンをクリックすると、ツールチップで詳細情報を確認できます。ツールチップに表示されたエラーメッセージのリンクをクリックすると、ドアまたはエレベーターに接続されたデバイスの一覧へ移動できます。



該当デバイスを右クリックし、**Reconnect** または **Reboot** オプションを選択してください。

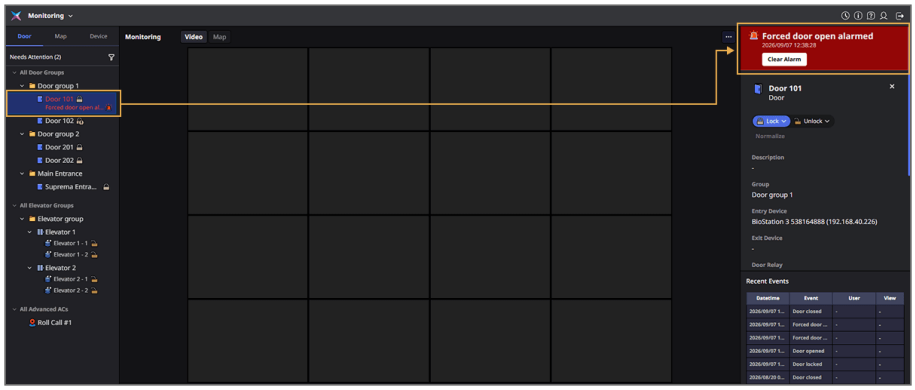


情報

- ドアまたはエレベーターで発生するアラームは、次の設定で構成できます。
  - ドアアラーム設定
  - エレベーターアラーム設定
  - 高度アクセス制御設定
- ビデオルールでドアとカメラを連携させてアラームを設定します。ビデオルールの設定の詳細はビデオルールを設定するをご覧ください。
- VMSサーバーと連携する際、映像に対するAIイベントアラームを設定すると、**BioStar X** にアラームを送信できます。詳細はVMSサーバーのマニュアルを参照してください。
- アラーム解除の詳細はイベントをモニタリングするをご覧ください。

プレビューパネルでアラームを確認

Door タブでアラーム( )アイコンが表示されたドア、エレベーター、または高度な入退室管理を選択し、画面右側のプレビューパネル上部でアラームを詳しく確認します。ドアとエレベーターは、異常( )状態がある場合も、パネル上部であわせて確認します。

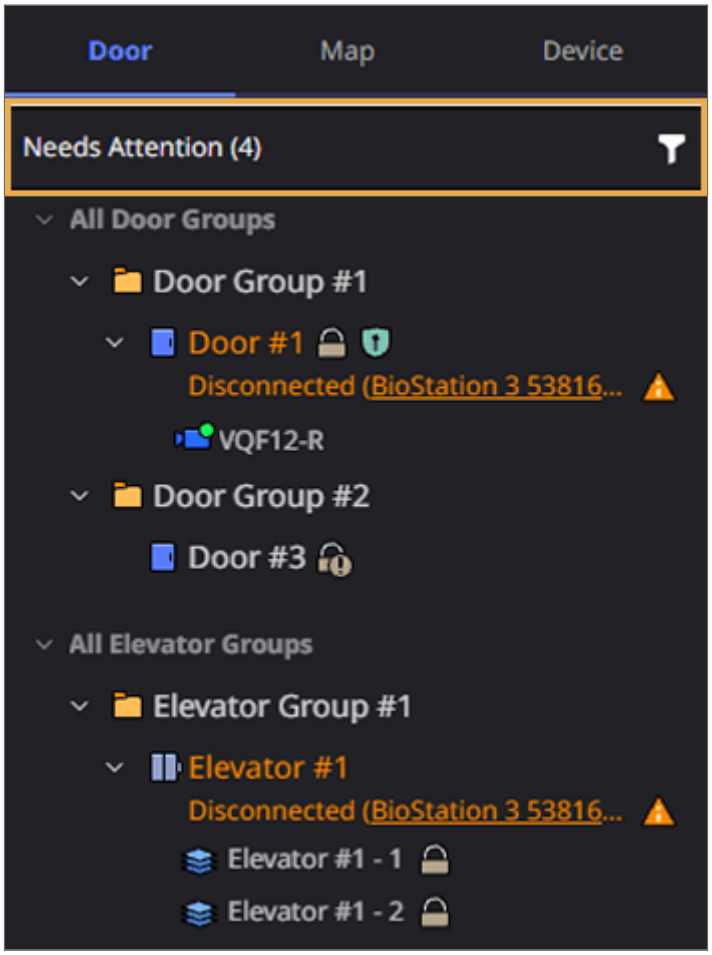


パネル上部のバナーは、アラーム名や発生時刻などの現在の状態情報を表示します。状況に応じた対応をすぐ実行できるボタンも提供します。

> **情報**
>
> - アラームが複数同時に発生しても、バナーには最新のアラーム1件だけが表示されます。
> - ドアまたはエレベーターでは、デバイスの接続が切れた状態で発生したアラームは、発生時刻を表示せず、アラームの種類のみ表示します。
> - バナーのボタンはアラームの種類によって異なります。ボタンをクリックして、アラームに応じた対応を実行してください。
> - アラームが表示されていても、ドアの施錠、解錠などの制御はそのまま利用できます。ドア制御の詳細については、出入ドアを制御するを参照してください。

注意が必要な対象をまとめて表示

管理者は、対応が必要なドアとエレベーターだけをまとめて確認できます。画面左のサイドバーの **Needs Attention** をクリックします。ドアとエレベーターの状態を確認し、問題が発生したデバイスに即座に対応できます。



> **情報**
> どの状態でドアとエレベーターが対応対象として表示されるかについては、対応対象の判定基準を参照してください。

対応対象の判定基準

ドア

ドアは、以下の条件のいずれかに該当すると、対応が必要な対象として表示されます。

ドアモードの変更

管理者、スケジュール、非常事態によりドアが施錠または解錠された状態を含みます。

理由	状態表示
管理者による手動操作	**Locked by Operator** / **Unlocked by Operator**
スケジュール	**Locked by Schedule** / **Unlocked by Schedule**
非常事態	**Locked by Emergency** / **Unlocked by Emergency**

アラーム

未解除のアラームが一つでもあると、対応対象として表示されます。強制開放、長時間開放、アンチパスバック関連のアラームは、異常状態ではなくアラームに分類します。

アラームの種類	説明
出入口ドアの強制開放	解錠せずに強制的に開いた状態
出入口ドアの長時間開放	設定した時間を超えて開いたままの状態
アンチパスバック（APB）アラーム	再入退室ルールに違反した状態
時間制限付きアンチパスバックアラーム	時間基準の再入退室ルールに違反した状態
緊急開放（Lock Override）アラーム	ロック状態（管理者によるロックまたはスケジュールロック）で、緊急開放（Lock Override）カード認証により解錠された状態
AI映像解析アラーム	テールゲーティング、徘徊、侵入、転倒、放置など、映像解析に基づくアラーム

異常状態

出入口ドアに接続された機器の接続状態を基準に判定します。

異常状態の種類	説明
接続切断	デバイスとのネットワーク接続が切断された状態
同期化エラー	接続はされているが、データ同期がずれている状態
マルチコミュニケーションサーバーエラー	デバイスが属するマルチコミュニケーションサーバーでエラーが発生した状態

情報

- **Needs Attention** フィルターには、上記の異常状態に加えて、機器ロック、認証の連続失敗によるロック（Auth Fail Lockout）状態も含まれます。
- アラームと異常状態が同時に発生すると、両方の状態アイコンが一緒に表示され、一方が他方を隠すことなく、同じ行ですべて確認できます。
- 下位機器で発生した異常状態は、上位の出入口ドアノードに集計して表示されます。フィルターをオンにしても、階層構造に沿って問題の発生箇所を確認できます。

エレベーター

エレベーターも出入口ドアと同じ条件で判定します。ただし、異常状態とアラーム条件には、次の違いがあります。

- **モード変更**: 出入口ドアと同じです。管理者、スケジュール、非常時により施錠または開放されると、対応対象として表示します。

- **異常状態**：出入扉と同じ基準を適用します。ただし、強制開放と長時間開放はエレベーターにない状態のため、判定対象から除外します。
- **アラーム**: エレベーターには、出入口とは異なる専用アラームがあります。以下を参照してください。

アラームの種類	説明
エレベーターアラーム発生	エレベーターでアラームが発生した状態
エレベーター入力アラーム	外部入力信号で発生したアラーム
エレベーター全階開放アラーム	全階が強制的に開放された状態

情報

- 階はエレベーターノード配下の独立したノードとして表示し、各階はロック()/開放()状態のみを持ちます。
- アラームと異常状態は、階ではなく上位のエレベーターノードに表示します。エレベーターを展開すると、対応が必要な階のみを表示し、正常な階は非表示にします。

高度なアクセス制御

高度入退室制御グループの項目（アンチパスバック、火災警報、侵入、招集、在室人数制限、インターロック）も、対応要否の判定に含まれます。ただし、ドアやエレベーターと異なり、モード変更や異常状態の条件は適用されません。解除されていないアラームが一つでもあると、対応対象として表示されます。

アラームの種類	説明
アンチパスバック（APB）アラーム	再入退室ルールに違反した状態
火災警報	火災を検知して発生したアラーム
スケジュールロックアラーム	スケジュールロックを設定した状態で発生したアラーム
侵入アラーム	侵入を検知して発生したアラーム
インターロックアラーム	インターロック規則に違反した状態
点呼招集アラーム	招集状況で発生したアラーム

情報

- 警備（Arm）状態と無効化された項目は、対応対象として表示されません。警備は正常に運用中の状態であり、無効化は意図的にオフにした状態であるためです。
- 各項目は高度入退室制御グループの直下に表示され、下位にドアは展開されません。対応が必要な項目だけがツリーに残り、対応対象がない場合は高度入退室制御グループ自体がツリーから除外されます。

ドアの状態を確認

ドアの閉状態、開状態、異常状態を確認できます。ドアの状態は以下をご参照ください。

ステータスアイコン	説明
	ドアが閉まっています。
	ドアが開いています。
	出入扉センサーが設定されていません。

ドアのロックを確認

ドアリレーの状態からドアのロック状態を確認できます。ドアリレーの状態は以下を参照してください。

ステータスアイコン	説明
	ドアが施錠されています。
	ドアを **Timed** または **Permanent** オプションで施錠した状態です。
	ドアが解錠されています。
	ドアを **Timed** または **Permanent** オプションで解錠した状態です。

> **情報**
> ドア制御オプションの詳細は 出入ドアを制御する をご参照ください。

カメラの状態を確認

カメラの状態を確認して、正常に動作しているか確認できます。カメラの状態は以下を参照してください。

ステータスアイコン	説明
	カメラが接続されています。
	カメラの電源がオフ、または接続が解除されています。

情報

- ドアと連動しているカメラが表示されない場合は、カメラグループの権限を確認してください。カスタム権限を持つ管理者がカメラグループの権限を設定していないと、カメラが表示されないことがあります。カメラグループの権限設定の詳細については カメラを設定するご参照ください。
- 出入口のドアとカメラを連動させるには、ビデオルールを追加する必要があります。詳しくはビデオルールを設定するをご覧ください。

セキュリティ状態を確認

ドアまたは高度アクセス制御設定の警備状態を確認します。

ステータスアイコン	説明
	警備状態です。
	警備が解除されています。

情報

警備状態は、ドアを警備に設定した場合にのみ表示されます。侵入アラーム設定の詳細は警備をご覧ください。

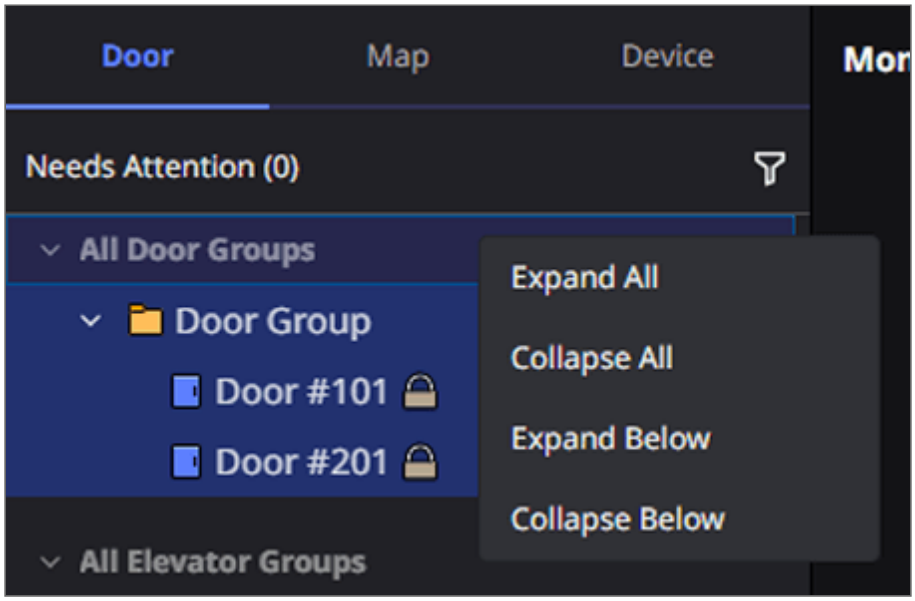
エレベーター状態を確認

エレベーター経由のフロアアクセス制御状態を確認します。

ステータスアイコン	説明
	エレベーター経由で当該フロアが施錠されています。
	エレベーター経由で当該フロアが解放されています。

グループリストの展開/折りたたみ

最上位グループまたはサブグループからリストを展開または折りたたむことができます。



最上位グループ

1. **Door** タブで **All Door Groups** または **All Elevator Groups**、**All Advanced ACs** を選択して右クリックしてください。
2. ポップアップメニューで **Expand All** または **Collapse All** を選択してください。

選択した最上位グループを基準にすべてのサブリストを展開または折りたたむことができます。

サブグループ

1. 各最上位グループのサブグループリストを展開または折りたたむには、サブグループを選択して右クリックしてください。
2. ポップアップメニューで **Expand Below** または **Collapse Below** を選択してください。

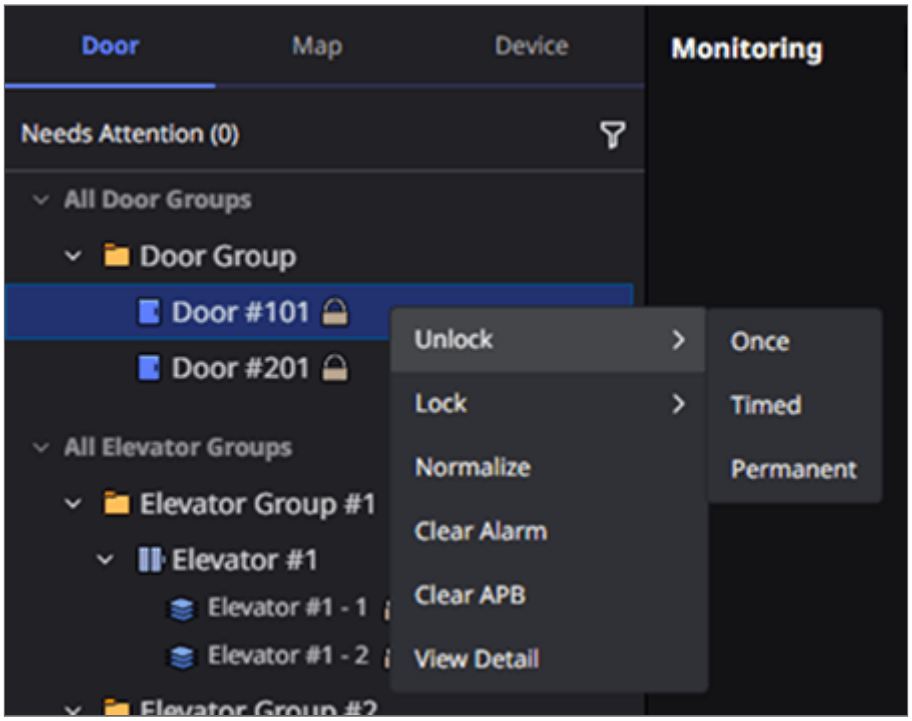
選択したサブグループのリストを展開または折りたたむことができます。

出入ドアを制御する

出入ドアを制御する方法を説明します。出入ドアを一定時間ロックしたり、出入ドアに接続されたカメラを確認したり、発生したアラームを解除できます。

- 出入ドアをリモートで制御して、出入を管理してください。特定時間、出入ドアを解放またはロック状態に設定できます。
- 出入ドアに接続されたカメラを通じてリアルタイムで出入状況をモニタリングできます。
- アンチパスバック 機能により、不正侵入をブロックし、入退室履歴を正確に管理できます。

Launcher ページで **Monitoring** をクリックするか、画面左上のショートカットリストから **Monitoring** を選択してください。制御したい出入ドアを選択し、右クリックしてください。ポップアップメニューで必要な機能を選択できます。

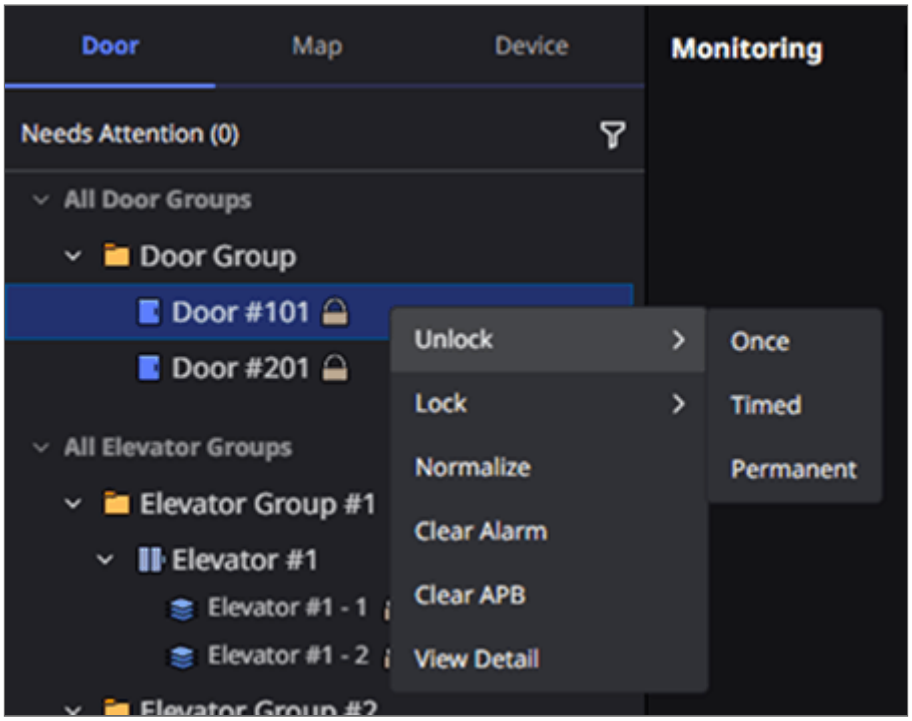


情報

- ドアの状態をモニタリングまたは制御するには、**Log Upload** 機能を有効にする必要があります。この機能は、**Settings** → **System** → **Server** のメニュー経路にある **General** セクションで有効化してください。
- **Open Video** オプションは、VMSと連携しており、ドアとカメラが連係されている必要があります。また、この機能は **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 ポリシーをご参照ください。
- 複数のドアをまとめて選択して制御する場合は、一括制御を参照してください。

ドア開放

開放状態のドアは誰でも出入りできます。ポップアップメニューで **Unlock** をクリックし、必要なオプションを選択してください。



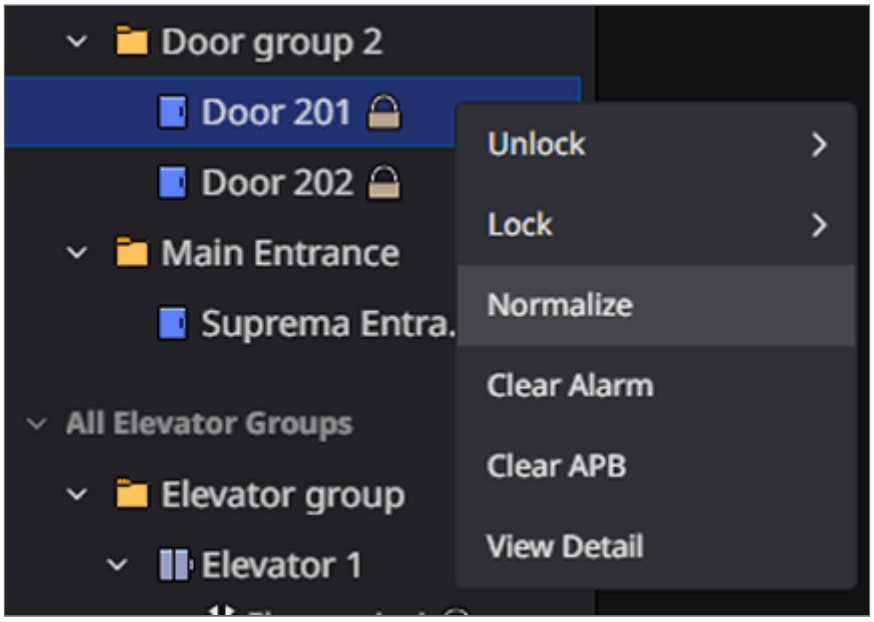
- **Once**：ドアを一度だけ開放します。
- **Timed**：一定時間ドアを開放します。希望する時間を秒（second）単位で入力してください。
- **Permanent**：時間に関係なくドアを開放します。

ドアを一時的に開放すると、ドアリレーアイコンが 状態から 状態に変わります。 **Timed** または **Permanent** オプションで開放すると、アイコンが 状態に変わります。

> **ヒント**
> 外部の来客時にドアを一時的に開放して、便利に出入りできます。ドアを開放した後は、必ず **Normalize** 状態に戻してください。

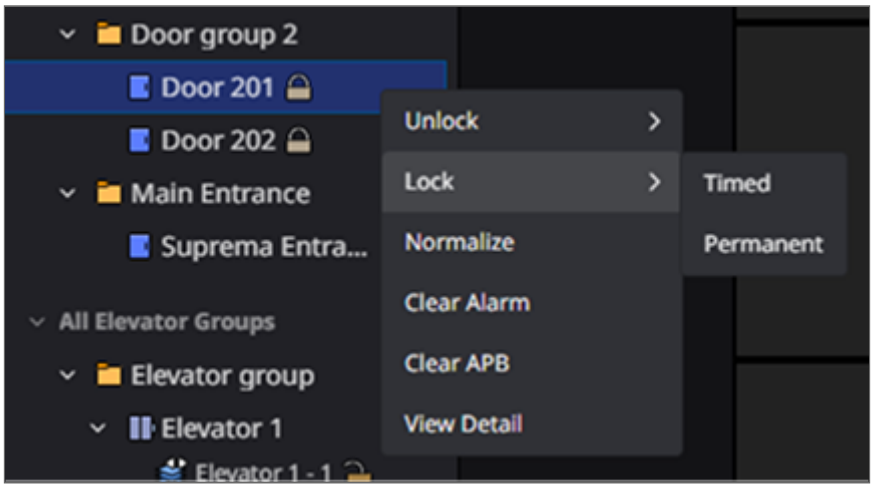
ドア解除

ドアを **Normalize** 状態にすると、許可されたユーザーだけが出入りできます。ポップアップメニューで **Normalize** をクリックしてください。



ドアロック

ドアを **Lock** 状態にすると、誰も出入りできません。ポップアップメニューで **Lock** をクリックし、必要なオプションを選択してください。

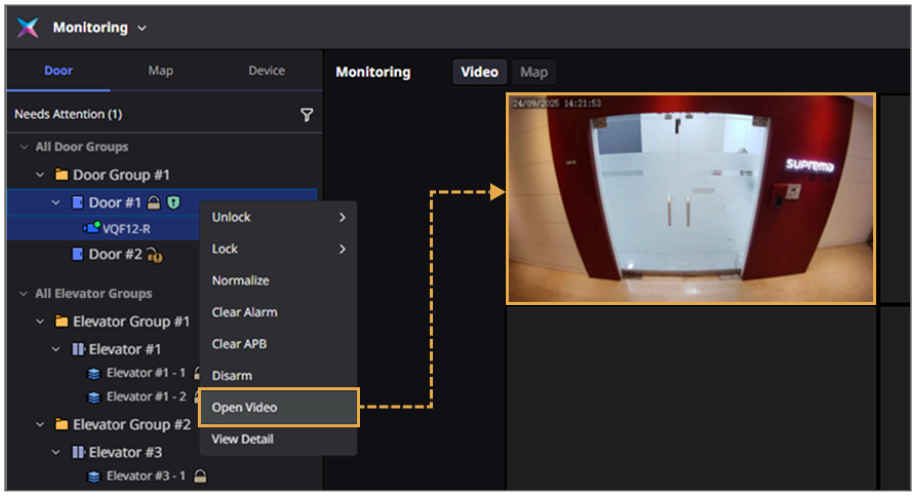


- **Timed**：一定時間ドアをロック状態にします。希望する時間を秒（second）単位で入力してください。
- **Permanent**：時間に関係なくドアをロック状態にします。

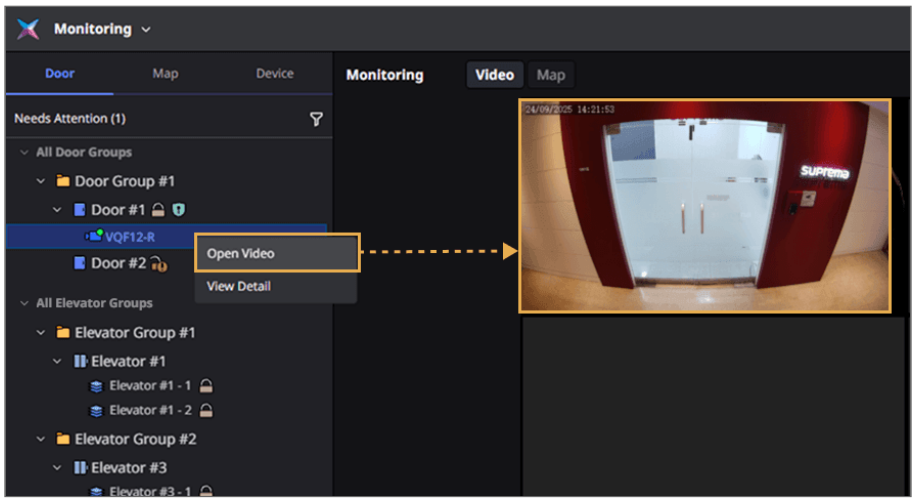
ドアを施錠状態に変更すると、ドアリレーアイコンが 状態に変わります。

ドアカメラ確認

ドアに接続されたカメラを確認できます。ポップアップメニューで **Open Video** をクリックしてください。 **Monitoring** セクションのビデオタイルに選択したカメラの映像を追加して再生できます。



また、目的のカメラを選択して右クリックしてください。ポップアップメニューで **Open Video** をクリックすると、選択したカメラの映像を追加して再生できます。

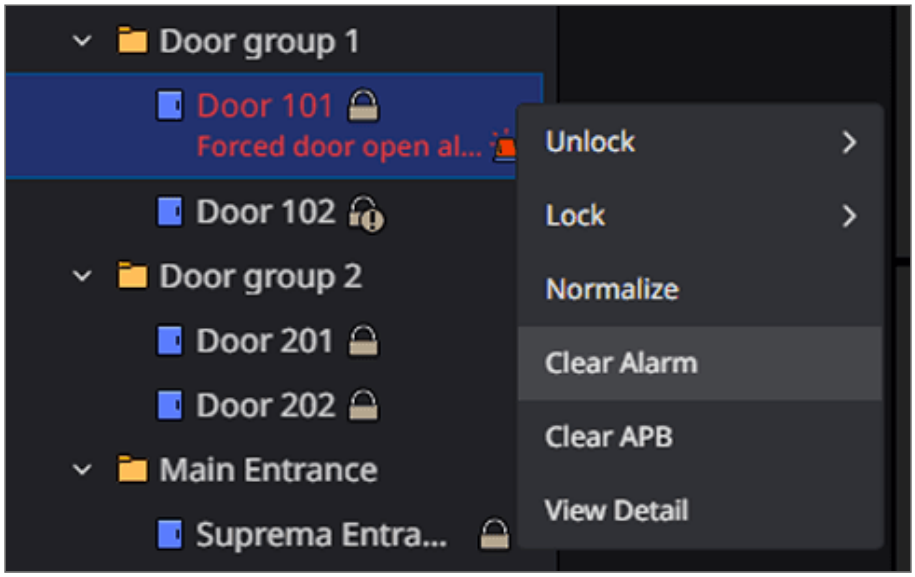


情報

- ドアに接続されているカメラが1台以上ある場合、最初に接続されたカメラがビデオタイルに表示されます。
- ビデオタイルは画面左上から順に追加され、現在の画面に追加スペースがない場合はエラーメッセージが表示されます。
- ビデオモニタリングの詳細については ビデオをモニタリングするご参照ください。
- ドアと連動しているカメラが表示されない場合は、カメラグループの権限を確認してください。カスタム権限を持つ管理者がカメラグループの権限を設定していないと、カメラが表示されないことがあります。カメラグループの権限設定の詳細については カメラを設定するご参照ください。
- この機能は **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。

アラーム解除

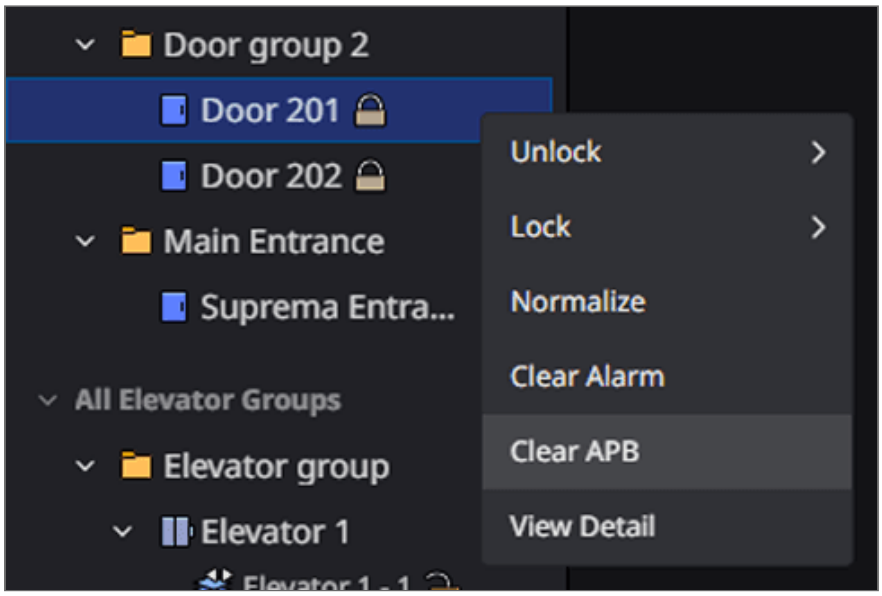
ドアで発生したアラームを解除できます。ポップアップメニューで **Clear Alarm** をクリックしてください。画面右上にアラームメッセージが表示されます。



APB解除

アンチパスバック違反が発生した場合、APBアラームを解除できます。

1. ポップアップメニューで **Clear APB** をクリックしてください。



2. **Clear APB** ウィンドウが表示されたら、全ユーザーの一覧を確認します。



3. アンチパスバックに違反したユーザーを選択し、**Apply** ボタンをクリックしてください。

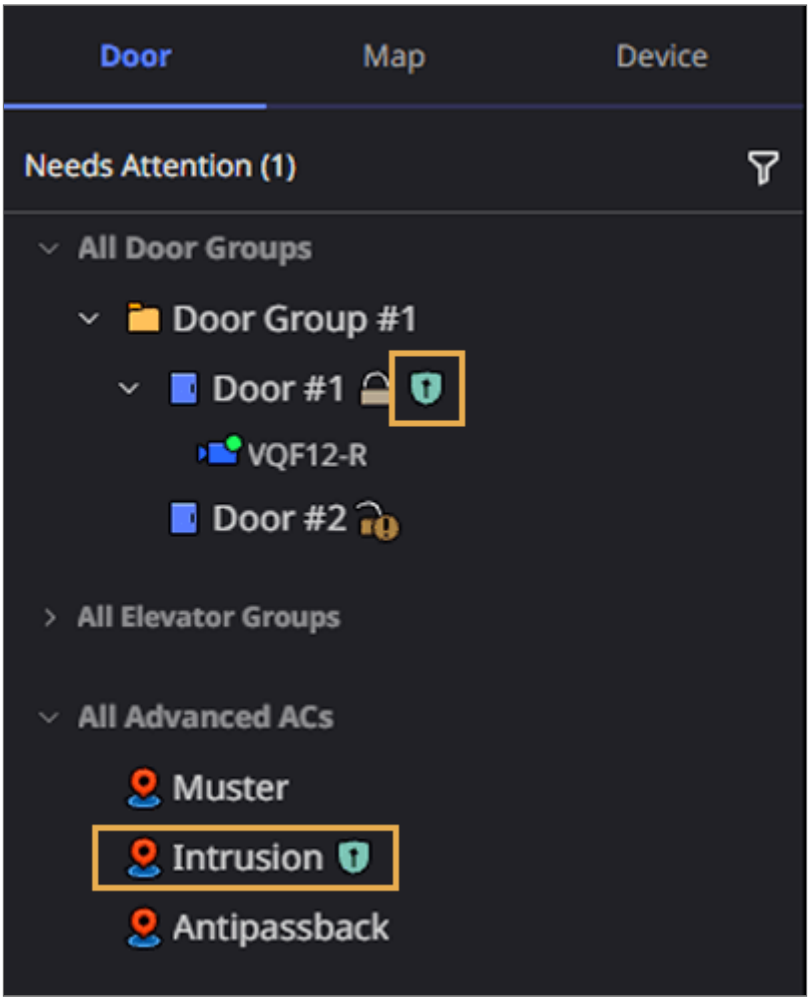
画面右上に完了メッセージが表示されます。

情報

- **안티패스백(Anti-Passback)**: 출입 통제를 위해 구조적인 방법으로서, 출입문 안쪽/바깥쪽에 출입 통제 장치를 설치하여 구역에 출입할 때 반드시 인증을 통해 출입해야 하는 기능입니다. 카드를 사용해 출입할 때 리더기에 카드를 인식하지 않고 앞 사람을 따라 입실했다면, 퇴실할 때 출입문이 열리지 않으며 **안티패스백** 이벤트가 발생합니다.
  안티패스백은 Hard APB와 Soft APB로 구분합니다. **안티패스백** 위반 시 Hard APB는 **안티패스백** 이벤트를 생성하고 출입할 수 없으며, Soft APB는 **안티패스백** 이벤트를 생성하고 출입은 가능합니다.
- 出入口に**アンチパスバック**を設定する方法の詳細については ドアを登録するご参照ください。

警備設定および解除

ドアが警備モードに設定されている場合、警備を有効化または解除します。ポップアップメニューで **Arm** または **Disarm** をクリックしてください。

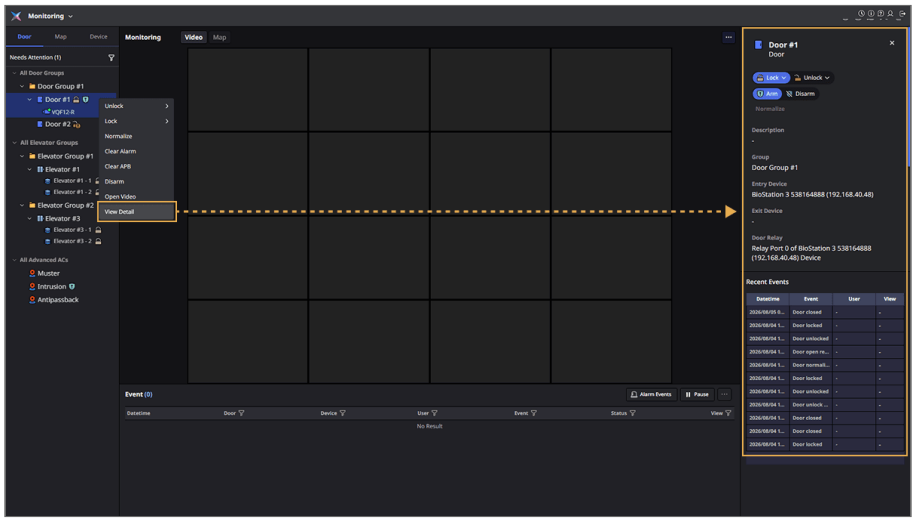


警備状態のドアでは、警備状態アイコンが から に変わります。このとき、該当するアクセス制御設定にも アイコンが適用されます。

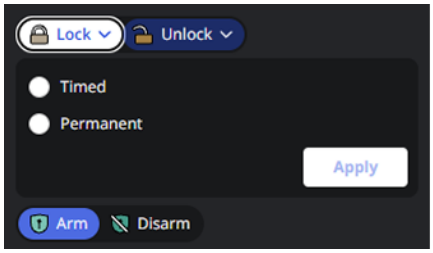
> **情報**
> この機能は、**エッセンシャル**（Essential）ライセンスで追加オプションを購入するか、**エンタープライズ**（Enterprise）ライセンス以上で利用できます。ライセンスポリシーの詳細については、ライセンス ポリシーをご参照ください。

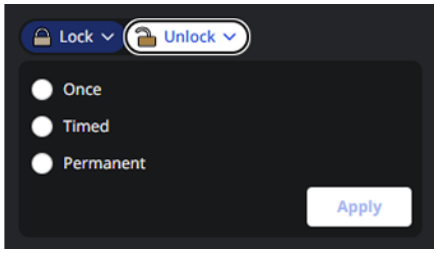
詳細情報確認

ドアの詳細情報とイベント発生履歴を確認できます。ポップアップメニューで **View Detail** をクリックしてください。画面右側に、ドア制御、ドアの詳細情報、イベント発生履歴を確認できるパネルが表示されます。



- **ドア制御**: ドアをロック、開放、警備、または警備解除の状態に変更できます。





- **Normalize**: 管理者がドアを手動で開放したり、ロック状態に変更した場合に使用できます。
- **ドアの詳細情報**：ドアの名前、位置、状態、接続されているサブデバイス情報などを確認できます。
- **Recent Events**：選択したドアで発生した最近のイベント一覧を確認できます。

> **情報**
> 出入口の詳細情報セクションの各項目については、 ドアを登録するご参照ください。

エレベーターを制御

エレベーターを制御する方法を案内します。提供されている機能を使用してエレベーターを制御したり、詳細情報を確認できます。

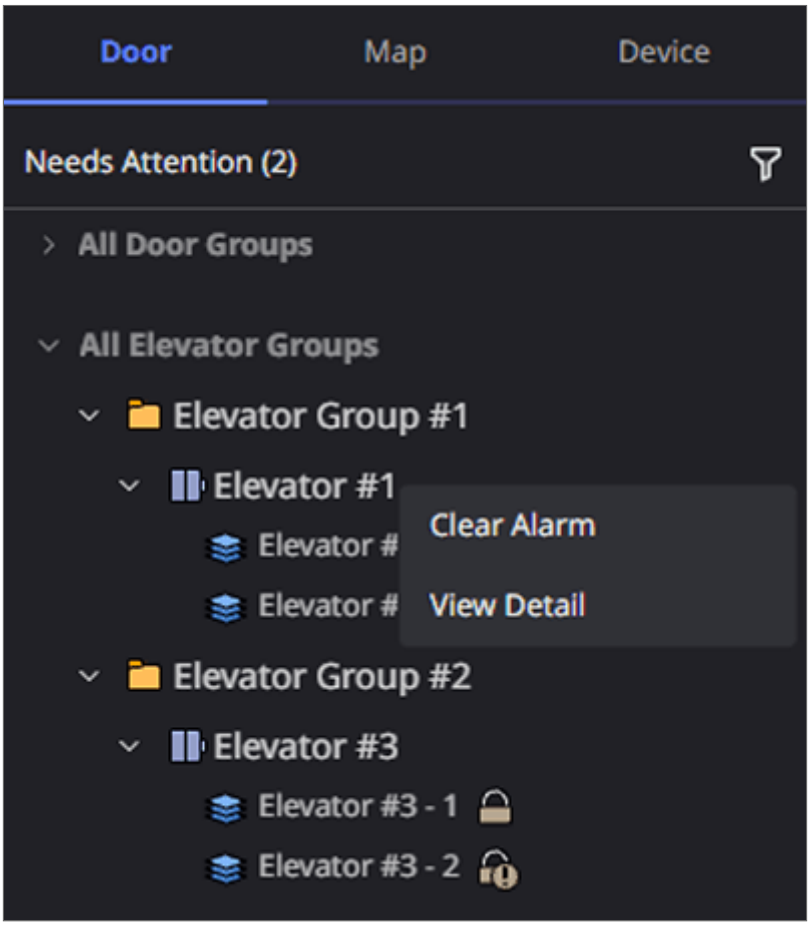
1. **Launcher** ページで **Monitoring** をクリックするか、画面左上のショートカットリストから **Monitoring** を選択してください。

2. 画面左側のサイドバーにある **Door** タブで **All Elevator Groups** に移動します。
3. 目的のグループのエレベーターを選択し、右クリックします。ポップアップメニューで必要な機能を選択できます。

> **情報**
>
> - エレベーターの設定およびグループ構成の詳細についてはエレベーター管理を参照してください。
> - 複数のエレベーターとフロアを一度に選択して制御するには、一括制御を参照してください。

エレベーターを制御

エレベーターで発生したアラームを解除したり、詳細情報を確認できます。

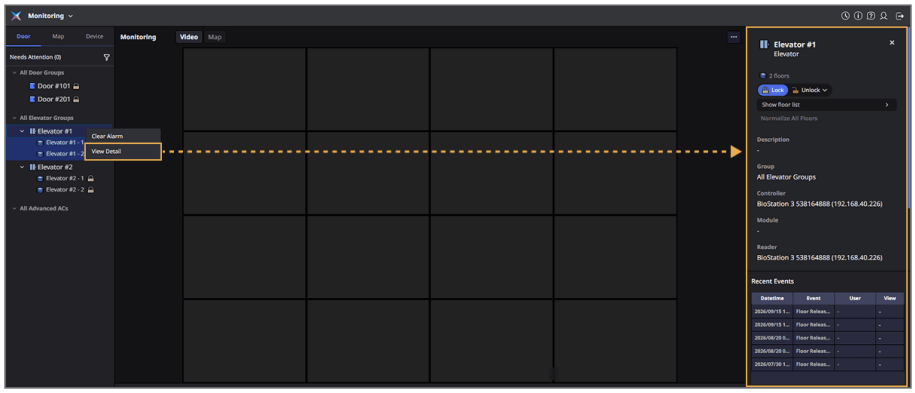


アラーム解除

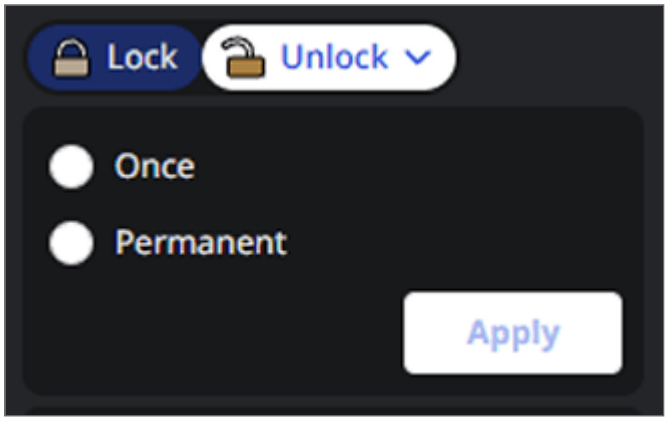
該当エレベーターで発生したアラームを解除できます。ポップアップメニューで **Clear Alarm** をクリックしてください。画面右上に完了メッセージが表示されます。

詳細情報確認

エレベーターの詳細情報とイベント履歴を確認できます。ポップアップメニューで **View Detail** をクリックしてください。画面右側にエレベーターの詳細情報とイベント履歴が表示されます。



- **エレベーター制御**: エレベーターをロック状態または解放状態に切り替えます。



- **Show floor list**：エレベーターに設定した階の一覧を確認します。

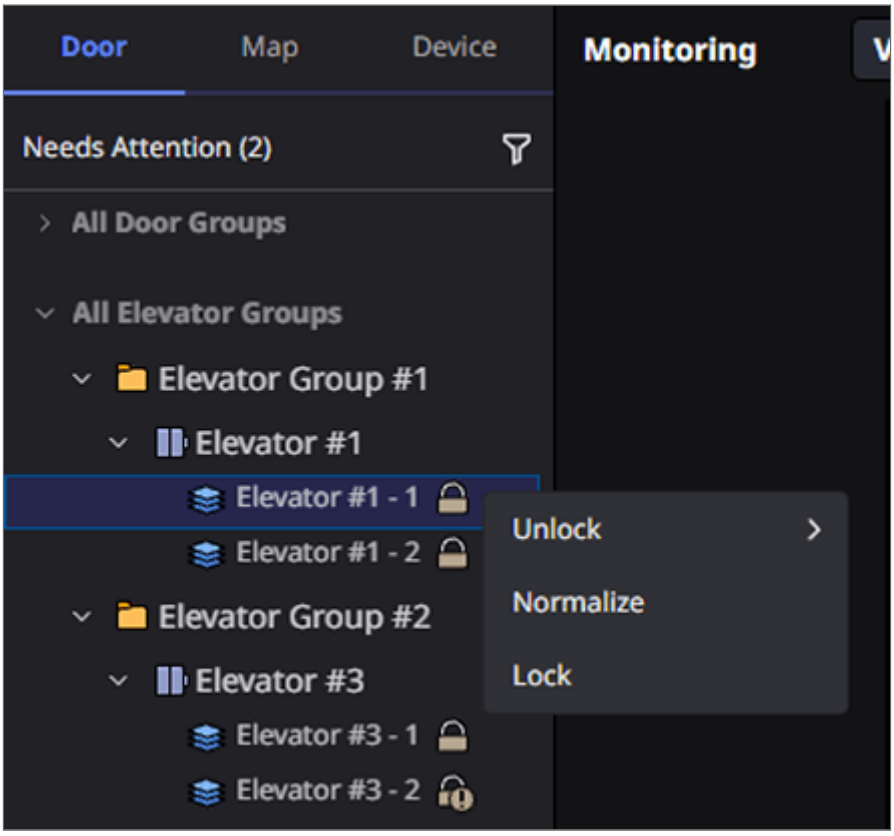


- **Normalize All Floors**: 管理者がすべてのフロアを手動で解放またはロック状態に変更した場合に使用します。
- **エレベーターの詳細情報**：エレベーターの名前、位置、状態などを確認できます。
- **Recent Events**：選択したエレベーターで発生した最近のイベント一覧を確認できます。

> **情報**
> エレベーターの詳細情報セクションにある各項目の説明についてはエレベーターを登録するを参照してください。

フロアアクセス制御

エレベーターで移動できる階を制御できます。エレベーターに設定されている階のリレーをクリックし、右クリックします。ポップアップメニューから目的の機能を選択します。



フロア解放

解放状態の階は誰でも出入りできます。ポップアップメニューで **Unlock** をクリックし、必要なオプションを選択してください。

- **Once**：一度だけ階を解放します。
- **Permanent**：時間に関係なく階を解放します。

> **ヒント**
> 外部の来客がある場合に、選択した階を一時的に解放して便利に出入りできます。階を解放した後は必ず **Normalize** 状態に戻します。

フロア解除

選択した階を **Normalize** 状態に変更すると、許可されたユーザーのみが出入りできます。ポップアップメニューで **Normalize** をクリックしてください。

フロアロック

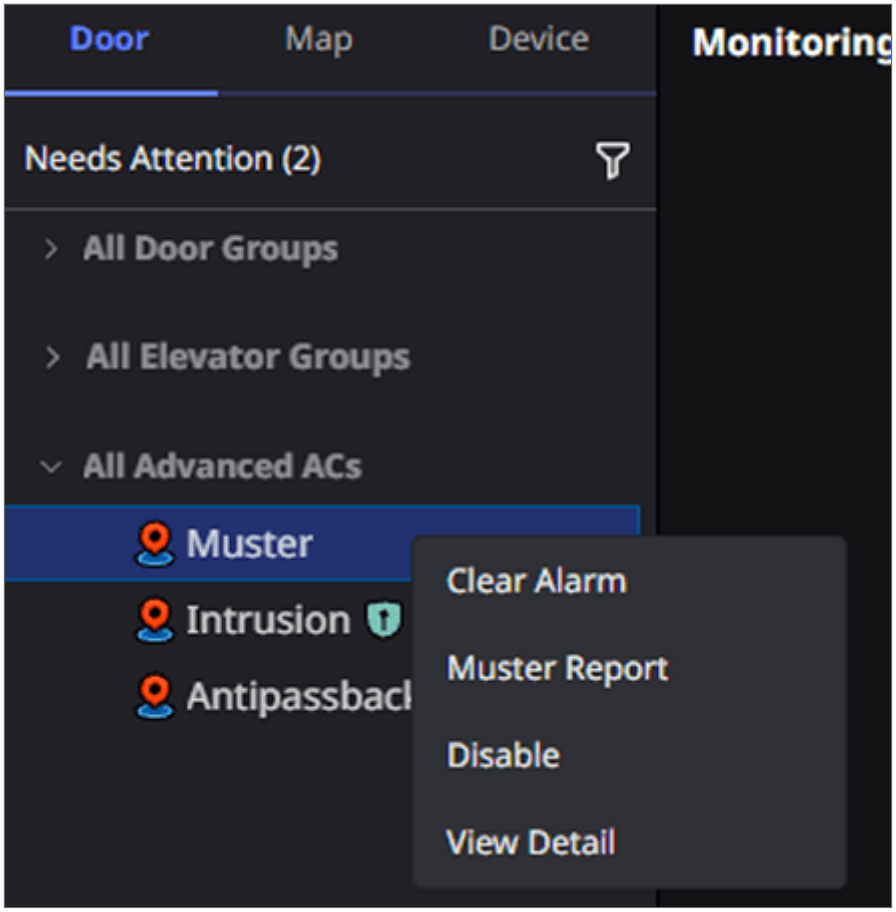
選択した階を **Lock** 状態に変更すると、誰も出入りできません。ポップアップメニューで **Lock** をクリックします。

高度アクセス制御を操作する

高度アクセス制御に設定されたドアまたはデバイスの操作方法を案内します。提供される機能により、問題発生時に迅速に対応し、効率的に管理できます。

1. **Launcher** ページで **Monitoring** をクリックするか、画面左上のショートカットリストから **Monitoring** を選択してください。

2. 画面左側のサイドバーで **Door** タブを開き、**All Advanced ACs** に移動します。
3. 設定された高度アクセス制御を選択し、右クリックします。ポップアップメニューで必要な機能を選択できます。



情報

- 高度アクセス制御の種類によって提供される機能が異なります。高度アクセス制御の種類は次のとおりです。
  - **アンチパスバック**
  - 火災警報
  - スケジュールロック/開放
  - 警備
  - インターロック
  - 点呼招集
  - 在室人数制限
  - 出席確認（Roll Call）
- 各高度アクセス制御機能の詳細については 高度な入退室制御設定 を参照してください。
- 複数の高度なアクセス制御の設定をまとめて選択して制御するには、一括制御をご覧ください。

APB 解除

アンチパスバックに設定されたドアまたはデバイスの APB アラームを解除できます。ポップアップメニューで **Clear APB** をクリックしてください。画面上部に完了メッセージが表示されます。

情報

- **Clear APB** 機能は **アンチパスバック** でのみ使用できます。
- **アンチパスバック**の設定の詳細は アンチパスバック を参照してください。
- **アンチパスバック**の詳細は 用語集 を参照してください。

アラーム解除

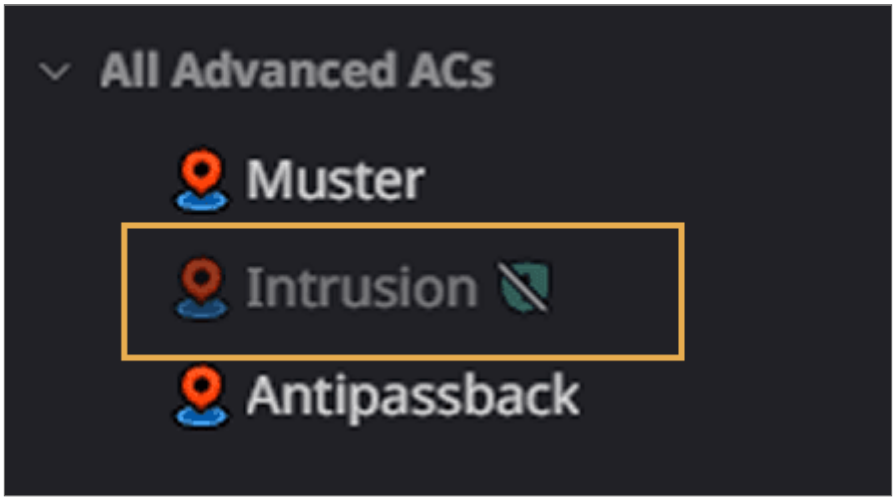
ドアまたはデバイスで発生したアラームを解除できます。ポップアップメニューで **Clear Alarm** をクリックしてください。画面上部に完了メッセージが表示されます。

情報

Clear Alarm は在室人数制限機能では使用できません。

有効化/無効化

高度アクセス制御機能を有効化するか、使用しない機能を無効化できます。無効化された高度アクセス制御は不透明表示に変わります。ポップアップメニューで **Enable** または **Disable** をクリックします。



警備/警備解除

ドアまたはデバイスの警備を設定または解除できます。ポップアップメニューで **Arm** または **Disarm** をクリックします。

情報

- **Arm** と **Disarm** は警備に設定された高度アクセス制御でのみ使用できます。
- 侵入アラーム設定の詳細は警備をご覧ください。

点呼招集レポートの確認

点呼招集に関するレポートを確認するには **Muster Report** をクリックします。新しいウィンドウが開くと、ユーザーリストと点呼招集機能に設定されたデバイスを通じて、ユーザーの入室・退室時刻や滞在時間超過の有無を確認できます。

情報

- **Muster Report** 機能は点呼招集でのみ使用できます。
- 点呼機能の詳細については 点呼招集 を参照してください。

在室人数制限のモニタリング

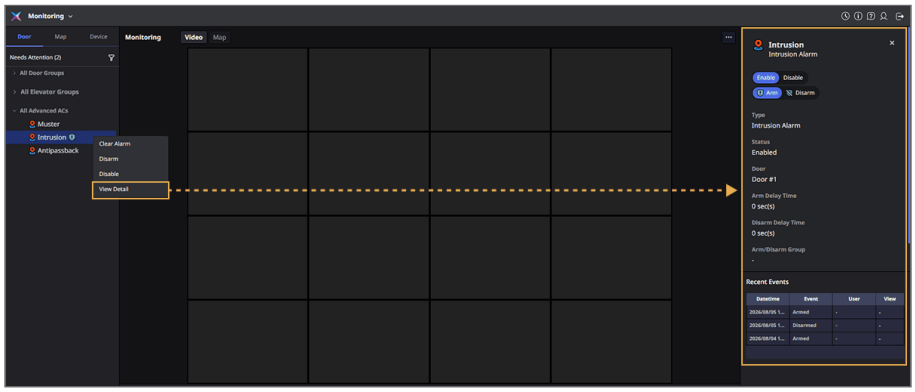
在室人数制限機能に設定されたデバイスの状態を確認できます。ポップアップメニューで **Occupancy Monitoring** をクリックします。新しいウィンドウが開いたら **Settings** → **Access Management** → **Advanced AC** メニューに移動します。 **Occupancy Limit** リストで状態を確認できます。

情報

- **Occupancy Monitoring** 機能は在室人数制限機能に設定された項目でのみ使用できます。
- 在室人数制限の設定の詳細は 在室人数制限 を参照してください。

詳細情報確認

高度アクセス制御の詳細情報とイベント発生履歴を確認できます。ポップアップメニューで **View Detail** をクリックしてください。画面右側のパネルに詳細情報とイベント発生履歴が表示されます。



- **高度なアクセス制御の制御:** 選択した高度なアクセス制御に対応する制御機能を使用します。
- **詳細情報**：高度アクセス制御機能の名前と状態、デバイス情報などを確認できます。
- **Recent Events**：選択した高度アクセス制御で発生した最近のイベント一覧を確認できます。

情報

高度アクセス制御の詳細情報セクションにある各項目の詳細については 高度な入退室制御設定 を参照してください。

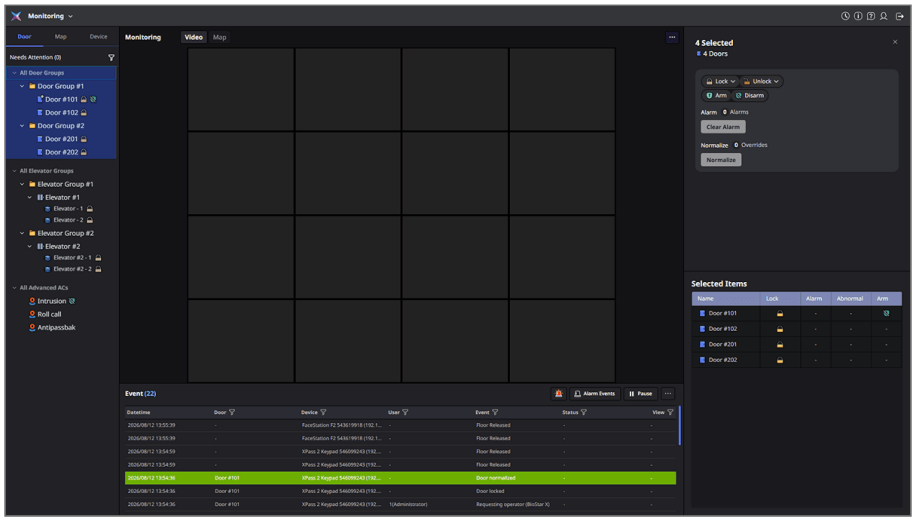
一括制御

複数の出入ドア、エレベーター、高度な入退室管理の設定を一度に選択し、解錠、施錠、アラーム解除などのコマンドをまとめて実行する方法を説明します。

- ステータスツリーで二つ以上の対象を選択すると、画面右側に一括制御パネルが表示されます。対象を個別に制御せず、一度にコマンドを実行します。

- 緊急時や複数の出入口を同時に制御する場合、迅速に対応します。
- 出入ドア、エレベーター（階）、高度な入退室管理の設定をそれぞれ一括選択して制御します。異なる種類を同時に選択すると制御できません。

Launcher ページで **Monitoring** をクリックするか、画面左上のショートカットリストから **Monitoring** を選択してください。画面左側のサイドバーのステータスツリーで、制御する対象を二つ以上選択すると、画面右側に一括制御パネルが表示されます。



> **情報**
>
> - カメラは一括制御の対象ではありません。ほかの対象と一緒に選択しても、選択リストから除外されます。
> - この文書では、複数の対象を一度に制御する方法を説明します。出入ドア、エレベーター、高度な入退室管理のいずれかを選択して制御する方法は、次の文書を参照してください。
>   - 出入ドアを制御する
>   - エレベーターを制御
>   - 高度アクセス制御を操作する

複数の対象の選択

画面左側のサイドバーにあるステータスツリーで、出入ドア、エレベーター、階、高度な入退室管理を選択する方法は次のとおりです。 Windows エクスプローラーで複数のファイルを選択する方法と同じです。

- **クリック**: 対象を一つだけ選択します。既存の選択は解除されます。
- Ctrl + **クリック**: クリックした対象を選択リストに追加または除外します。ほかの選択はそのまま残ります。
- Shift + **クリック**: 最後にクリックした対象から、今回クリックした対象までの表示範囲をすべて選択します。既存の選択はこの範囲に置き換わります。
- Ctrl + Shift + **クリック**: 既存の選択を保持したまま、範囲を追加で選択します。離れた複数の対象をまとめて選択するときに使用してください。
- **グループクリック**: グループ（📁）名をクリックすると、その配下のすべての出入ドア、エレベーター、階、高度な入退室管理設定が一度に選択されます。グループを展開または折りたたむには、グループ名の前の矢印(›)をクリックしてください。

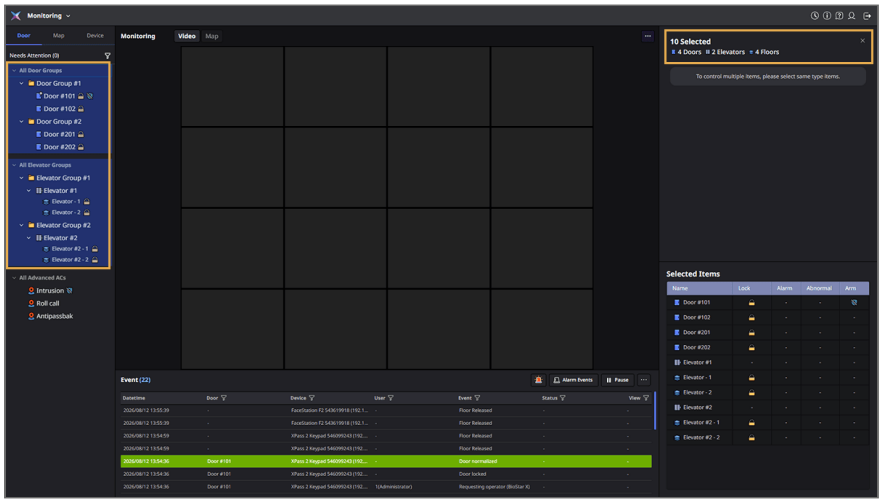
> **情報**
>
> 選択した対象がない、または一つだけの場合、一括制御パネルは開きません。項目を一つだけ残すと、その項目の詳細ビューが表示され、すべての選択を解除すると右側のパネルが消えます。

一括制御パネルの構成

画面左側のサイドバーにある状態ツリーで複数の対象を選択すると、画面右側に表示される一括制御パネルは次のように構成されます。

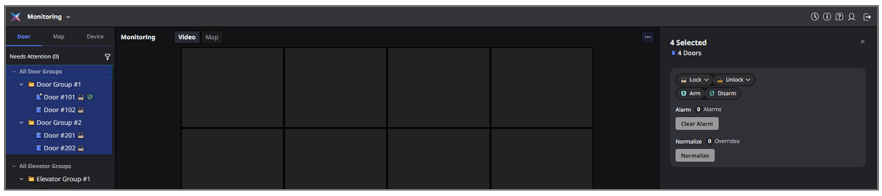
- **選択数と種類**：例として、ドア4つ、エレベーター2つ、4フロアを選択すると、次のように表示されます。

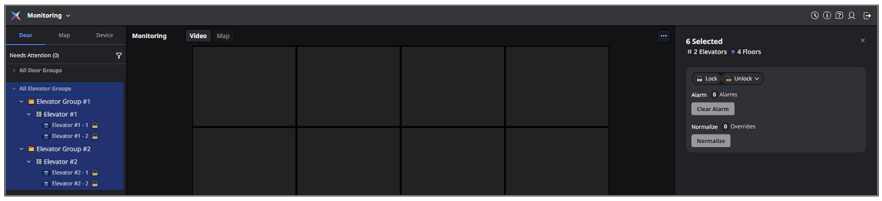
  > *10 Selected / 4 Doors 2 Elevators 4 Floors*



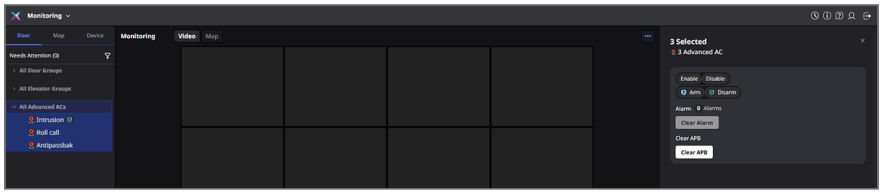
  > 異なる種類を同時に選択すると、制御機能は使用できません。

- **ドア/エレベーター制御**：ドアとエレベーターで使用できる制御機能が表示されます。

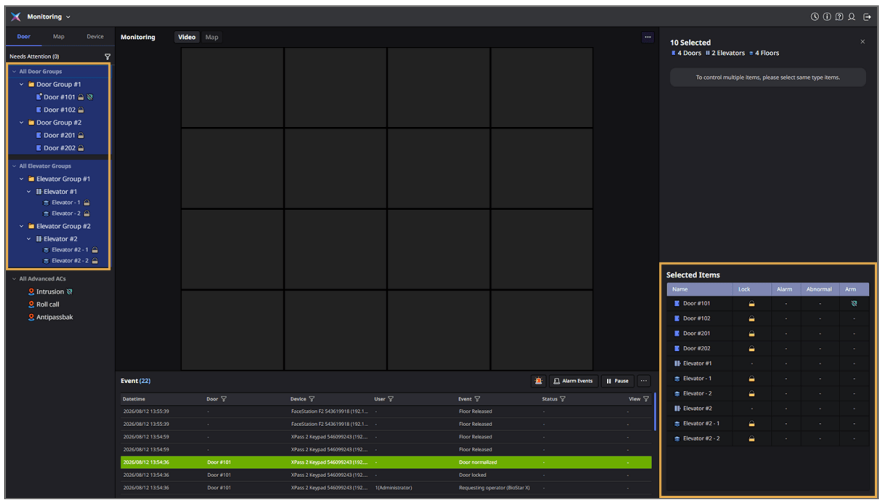




- **高度なアクセスコントロール制御**：高度なアクセスコントロールで使用できる制御機能が表示されます。

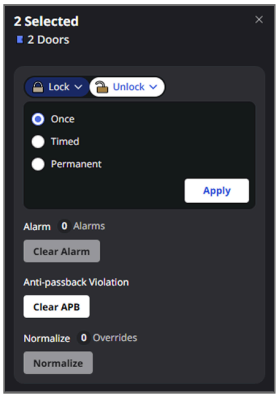


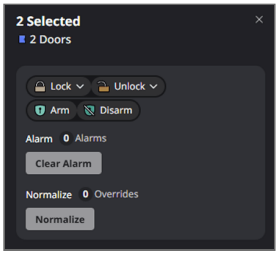
- **選択対象のサマリー表**：画面右側のパネル下部で、選択した各対象の名前と状態を確認できます。制御エリアとサマリー表の間の境界線を上下にドラッグすると、両エリアの高さを調整できます。選択対象が多い場合、境界線をドラッグしてサマリー表エリアを広げて確認してください。



ドアの一括制御

ドアのみを二つ以上選択すると、単一ドア制御と同じ基本制御と高度な制御を使用できます。





基本制御

- **Once**：開放状態で一度だけ適用します。
- **Timed**：入力した時間の間、施錠または開放状態を維持します。
- **Permanent**：時間に関係なく、施錠または開放状態にします。

必要なコマンドを選択して適用するには **Apply** ボタンをクリックしてください。

高度な制御

次のボタンは、下の条件に該当する対象が一つでもある場合に使用できます。

- **Clear Alarm**：選択したドアにアラームが発生している対象がある場合に使用できます。
- **Clear APB**: 選択したドアの中にアンチパスバックが設定されているものがある場合に使用できます。詳しくは 出入ドアを制御する をご参照ください。
- **Normalize**: 管理者が手動で開放または施錠したドアがある場合に使用します。スケジュールまたは非常事態によって変更された状態は含まれません。
- **Arm**/**Disarm**: 高度な入退室制御設定の一種である警備に設定されたドアがある場合にのみ表示されます。

情報

- **Clear Alarm**, **Normalize** ボタンをクリックすると、ポップアップウィンドウが開きます。解除するには、ポップアップウィンドウで **Clear Alarm** または **Normalize** ボタンをクリックする必要があります。一方、**Arm**/**Disarm** ボタンは、確認ウィンドウを表示せずに状態を切り替えます。
- 高度な入退室制御設定は、**エッセンシャル**（Essential）ライセンスで追加オプションを購入するか、**エンタープライズ**（Enterprise）ライセンス以上で利用できます。ライセンスポリシーの詳細については、ライセンス ポリシーをご参照ください。

エレベーターおよび階の一括制御

エレベーターを選択すると、設定済みのすべての階をまとめて制御できます。特定の階のみを制御するには、階を直接選択してください。

ドアとの違いは次のとおりです。

制御機能	ドア	エレベーター、階
Unlock	**Once**, **Timed**, **Permanent**	**Once**, **Permanent**
Lock	**Timed**, **Permanent**	**Permanent**
Normalize	対応	対応
Clear Alarm	対応	選択にエレベーターが含まれる場合は表示され、階のみを選択すると表示されません
Clear APB	対応	非対応

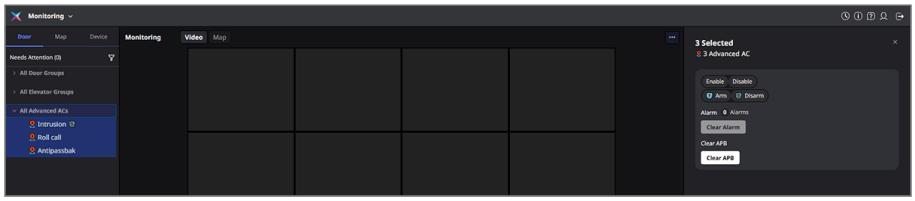
情報

エレベーターとその配下の階をまとめて選択し、開放または施錠すると、階ごとにコマンドが送信されず、エレベーター単位で一度だけ送信されます。

高度な入退室制御の一括制御

高度な入退室制御設定も複数選択して、一度に制御できます。二つ以上選択すると、右側の領域が一括制御パネルに切り替わります。選択、範囲、フィルターの動作は、ドアとエレベーターと同じです。

高度な入退室制御設定にはロックリレーや管理者による開放/施錠の概念がないため、ドア、エレベーターとは制御項目が異なります。選択した設定の種類に応じて、次の制御ボタンが表示されます。



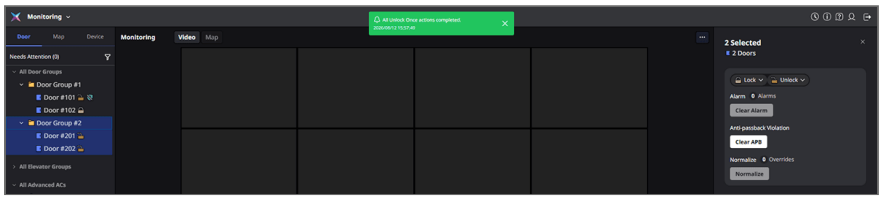
- **Enable**/**Disable**: すべての高度な入退室制御設定に共通で表示されます。

- **Arm/Disarm**: 選択した項目に警備設定がある場合にのみ表示されます。
- **Clear Alarm**: 選択した項目にアラームが発生する設定（アンチパスバック、火災警報、スケジュールロック、警備、インターロック、招集）がある場合にのみ表示されます。在室人数制限や人数点検など、アラームが発生しない設定のみを選択すると表示されません。
- **Clear APB**: 選択した項目にアンチパスバック設定がある場合にのみ表示されます。このボタンをクリックし、ユーザー選択画面でアンチパスバックに違反したユーザーのAPBアラームを解除します。詳しくは 高度アクセス制御を操作する をご参照ください。

> **情報**
>
> - **Lock**、**Unlock**、**Normalize** 機能は一括制御に含まれません。招集レポートの確認、在室人数の制限モニタリングなど、別画面へ移動する機能は一括制御パネルでは提供しません。これらの機能は、該当する設定を一つだけ選択した場合、詳細情報画面で使用できます。
> - 高度なアクセス制御の詳細は高度アクセス制御を操作するをご覧ください。

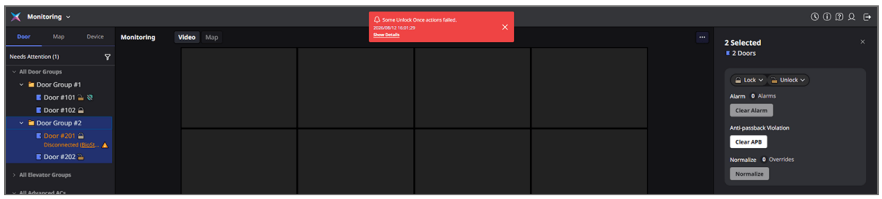
実行結果の確認

- 選択したすべての対象が成功すると、画面上部に成功メッセージが表示されます。



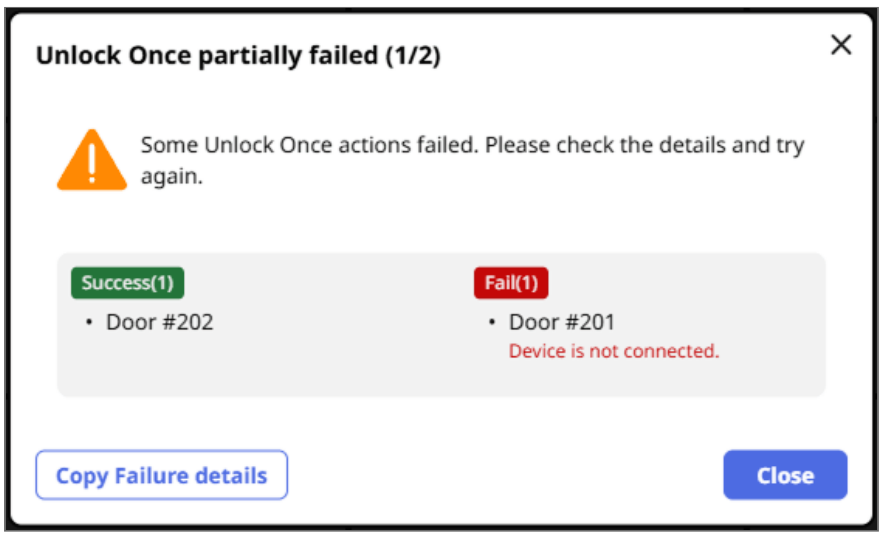
上記の画像は例示です。実際の画面とは異なる場合があります。

- 一つでも失敗すると、失敗メッセージとともに **Show Details** ボタンが表示されます。



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。

Show Detailsをクリックすると、**Success**、**Failure**、**Skipped**の三つのグループに区分された結果を確認できます。失敗した対象の名前と理由をクリップボードにコピーするには、**Copy Failure details**ボタンをクリックします。



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。

マップをモニタリングする

マップモニタリング機能を使用して、エリアおよびそのフロアごとのドアとカメラの状況をリアルタイムで確認し、制御する方法を説明します。マップモニタリングは Google マップと連携したビジュアルインターフェースを通じて、エリア (Area) とフロア (Floor) を簡単に探索し、ドア制御やカメラ映像再生などの多様な機能を利用できます。

Monitoring ページには、**Launcher** ページで **Monitoring** をクリックするか、画面左上のショートカットリストから **Monitoring** を選択してアクセスできます。

BioStar X では、1 つのエリアに複数の施設（Facility）を構成できます。各施設には複数のフロアを構成できます。 1 つのフロアでは、図面を基準にドアとカメラを設定してモニタリングできます。次の図を参照してください。



図のように構成した地域をGISマップと連携し、マップ上のエリア（Area）→ 施設（Facility）→ 階（Floor）の順に移動して、ドアとカメラを監視および制御します。この構造は、**Monitoring** ページのサイドバーでも同じように確認できます。

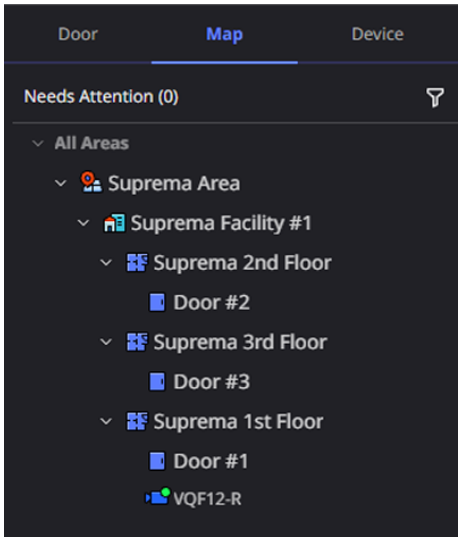
情報

- マップを構成する方法の詳細については**マップ管理**を参照してください。
- **Monitoring** エリアは、システムに登録されたデバイスカメラがない、またはマップ構成要素（エリア、施設、階）が登録されていない場合、有効になりません。
- GISと連動したマップモニタリング機能は、**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。

構成要素とオプション

マップツリーの構成要素

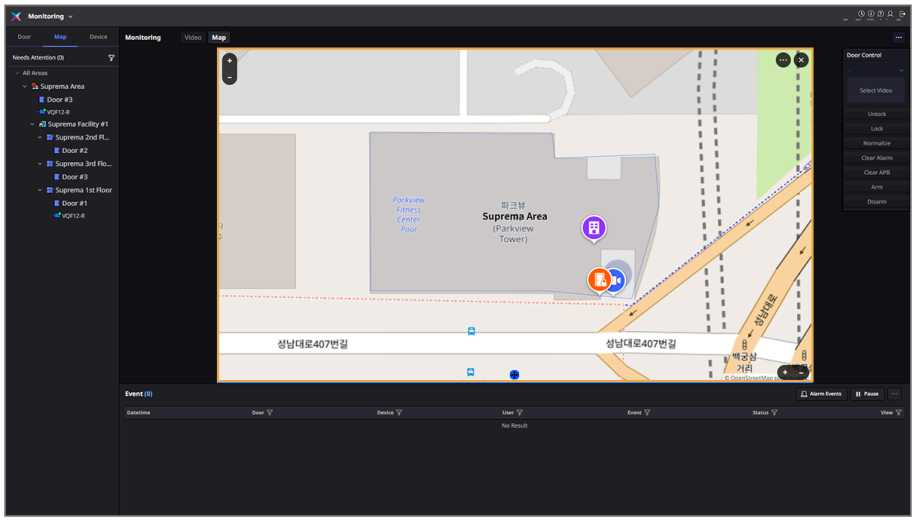
画面左のサイドバーにマップツリーの構成要素が表示されます。マップツリー上の各構成要素のアイコンで、エリア、施設、階、出入口、カメラを区別できます。



アイコン	名前
	エリア（Area）
	施設（Facility）
	階（Floor）
	ドア
	カメラ

マップエリアの構成要素

マップに表示される構成要素は、エリア（Area）、施設（Facility）、および施設に接続されたカメラです。施設からフロア（Floor）にアクセスできます。フロアではドアとカメラを確認できます。



構成要素	説明
	施設 (Facility)：マップに配置された施設をクリックすると、その施設に設定されているフロア（Floor）へ入ることができます。
	ドア：マップに配置されたドアをクリックすると、そのドアを制御できるポップアップメニューが表示されます。提供する機能の詳細については出入ドアを制御するを参照してください。
	カメラ：カメラをクリックすると、その施設またはフロアの映像を再生できます。
	カメラエラー：カメラが接続されていない、または電源がオフになっている場合に表示されます。

構成要素	説明
	**開いているドア**：フロア（Floor）に配置されたドアが開いている状態です。
	**施錠されたドア**：フロア（Floor）に配置されたドアが施錠されている状態です。

オプション

マップまたはフロアで提供されるオプションは次のとおりです。

機能	説明
	マップ左上または右下にあるボタンをクリックして拡大／縮小できます。また、マウスホイールでマップを拡大／縮小できます。
	フロアの右下にあるボタンをクリックすると、拡大／縮小できます。
	ボタンをクリックすると、追加機能を利用できます。
×	ビデオタイル上のマップまたはフロアを閉じるには、右上のボタンをクリックします。
	アイコンをクリックしたままドラッグすると、マップを別の位置へ移動できます。

> **情報**
>
> - マップ上でマウスをクリックしたままドラッグすると位置を移動できます。マウスホイールで拡大または縮小できます。
> - マップをダブルクリックすると全画面表示に拡大されます。もう一度ダブルクリックするか、`ESC` キーを押すと元のサイズに戻ります。

状態を確認する

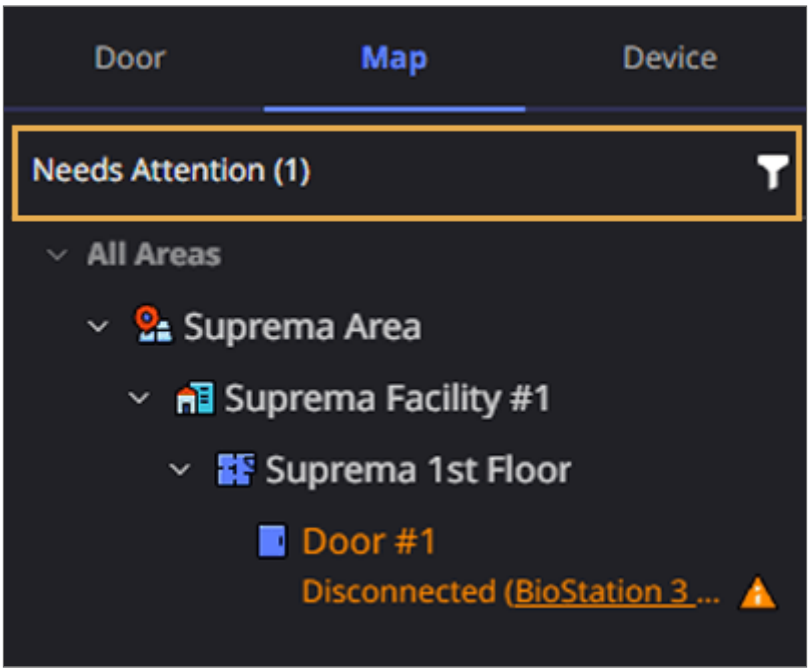
画面左のサイドバーで各施設またはフロアのドアとカメラの状態を確認できます。各アイコンの状態は以下を参照してください。

ステータスアイコン	説明
	マルチ通信サーバーでエラーが発生したか、接続が切断されています。
	ドアでアラームが発生している状態です。徘徊検知、侵入検知などが発生すると該当アイコンが表示されます。

ステータスアイコン	説明
	カメラが接続されています。
	カメラの電源がオフ、または接続が解除されています。

注意が必要な対象をまとめて表示

管理者は、対応が必要な対象だけをまとめて確認できます。画面左のサイドバーの **Needs Attention** をクリックします。エリア、施設、階の階層に配置されたドアの状態を確認し、問題が発生した対象に対応できます。



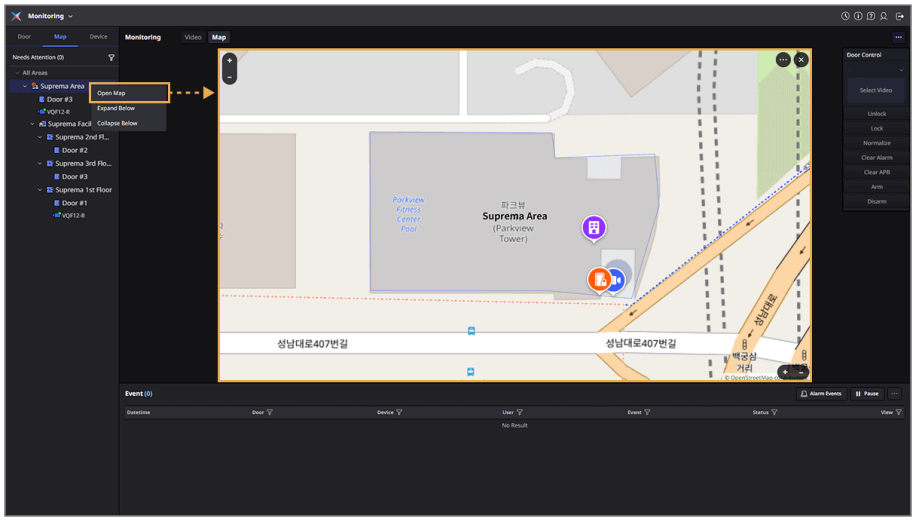
> **情報**
> ドアへの対応が必要かどうかの判定基準は、状態を確認を参照してください。

マップを開く

エリアが GIS マップと連携している場合、**Monitoring**セクションにマップを表示できます。

1. 画面左のサイドバーで、マップで確認する施設を選択します。
2. マウスの右ボタンをクリックします。
3. ポップアップメニューで **Open Map** をクリックします。

選択したエリアのマップが **Monitoring** セクションのビデオタイルに表示されます。

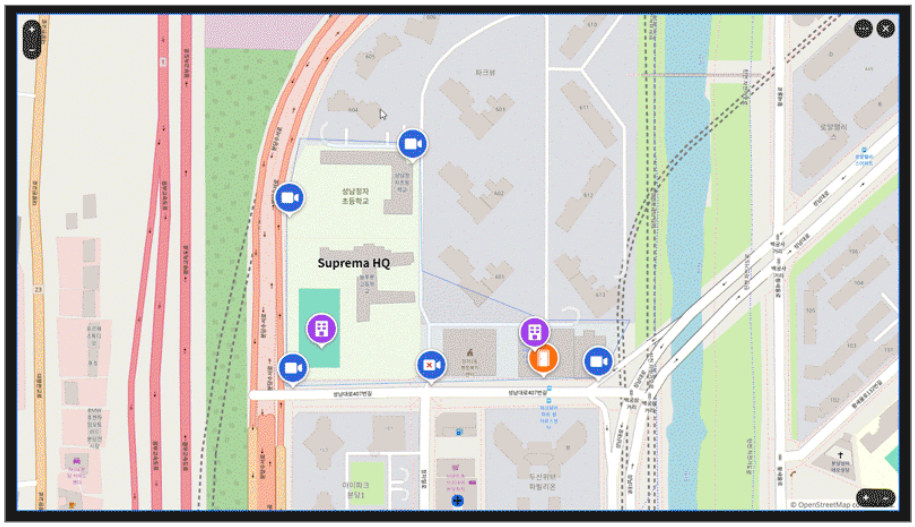


情報

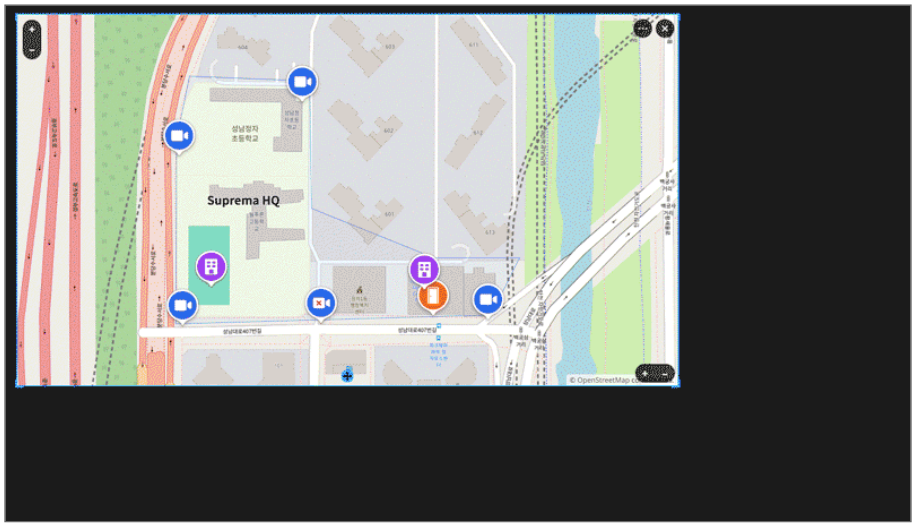
- 画面左のサイドバーで該当する施設をダブルクリックすると、その施設があるマップが開きます。
- 画像は例示用の画面です。実際の画面とは異なる場合があります。
- GISマップと連携してエリアを構成する方法の詳細についてはエリアを構成するを参照してください。

マップのサイズ調整と位置移動

マップのサイズを調整するには、地図上の空白部分をクリックします。各コーナーにサイズ調整用ハンドルが表示されます。ハンドルをクリックしたままドラッグして、目的のサイズに調整します。



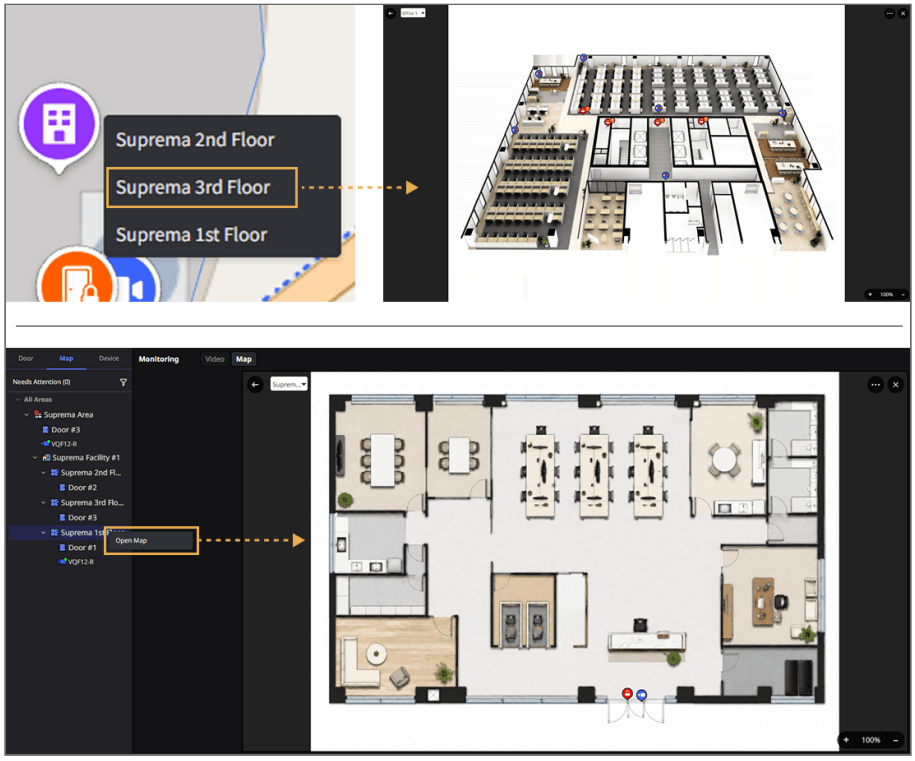
サイズを調整した後にマップを別の位置へ移動するには、マップ上のアイコンをクリックしたまま目的の位置へドラッグします。



フロアに入る

マップからフロアへ入るには、Facility をクリックします。ポップアップメニューにアクセス可能なフロアの一覧が表示されたら、目的のフロアを選択します。選択したフロアの図面、ドア、カメラを確認できます。

または、画面左のサイドバーでフロアをダブルクリックするか、右クリックしてポップアップメニューから**Open Map**をクリックします。



構成要素	説明
	**開いているドア**：フロア（Floor）に配置されたドアが開いている状態です。

構成要素	説明
	**施錠されたドア**：フロア（Floor）に配置されたドアが施錠されている状態です。
	**カメラ**：カメラをクリックすると、その施設またはフロアの映像を再生できます。

- ドアまたはカメラにマウスを合わせると、現在の状態が表示されます。

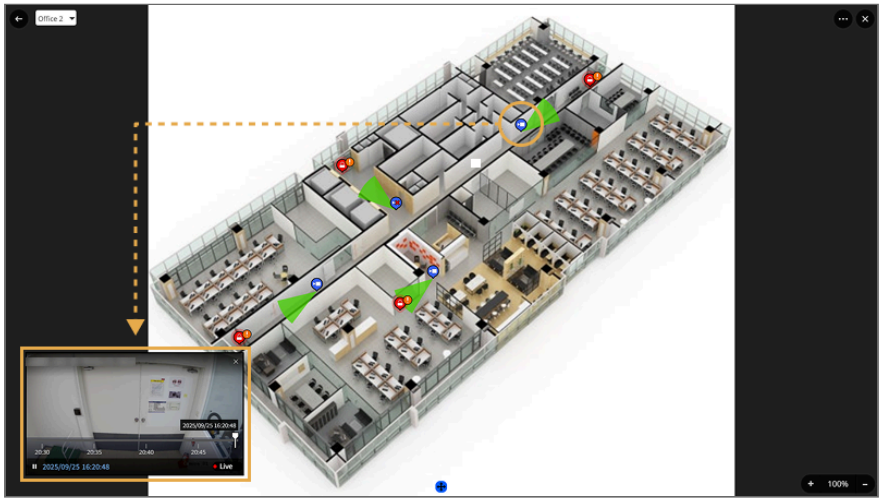




- ドアをクリックすると、そのドアを制御できるポップアップメニューが表示されます。提供する機能の詳細については出入ドアを制御するを参照してください。



- カメラをダブルクリックすると、ライブ映像を再生できます。



情報

- 施設が表示されるマップに戻るには、左上の←ボタンをクリックします。
- フロア(Floor)に出入口とカメラを設定する方法の詳細については フロアを構成するを参照してください。
- 映像の制御方法および映像に表示されるツールの詳細についてはビデオをモニタリングするを参照してください。
- 画像は例示用の画面です。実際の画面とは異なる場合があります。

別のフロアへ移動する

別のフロアへ移動するには、マップ左上の選択オプションをクリックし、一覧から移動したいフロアを選択します。

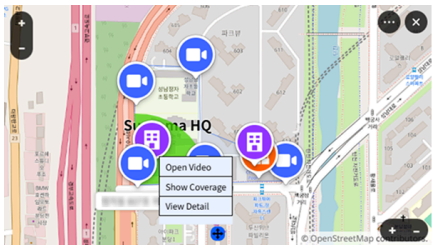


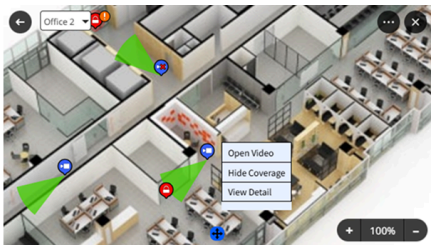
情報

- 施設が表示されるマップに戻るには、左上の←ボタンをクリックします。
- マップ左上のフロア選択オプションには、Facility に設定されているフロアのみが表示されます。そのフロアが Facility に設定されていない場合、リストに表示されません。施設にフロアを設定する方法の詳細については施設を構成を参照してください。

カメラを制御する

- マップまたはフロアでカメラを制御するには、カメラアイコンをクリックします。ポップアップメニューから目的の機能を選択します。

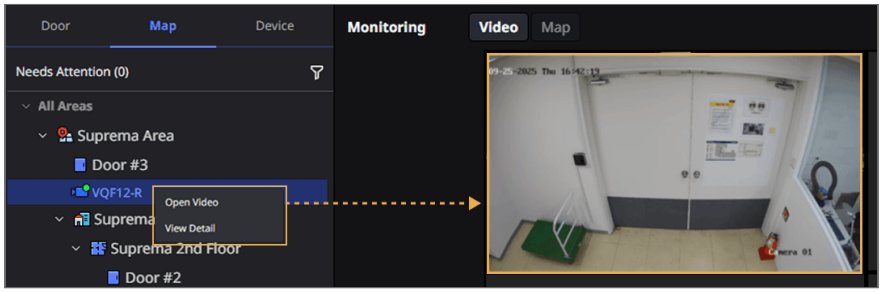




  - **Open Video**：カメラ映像をリアルタイムで確認できます。
  - **Show Coverage** / **Hide Coverage**：カメラの撮影範囲を表示または非表示にできます。

  - **View Detail**：カメラの詳細情報を確認できます。画面右のパネルにカメラの名前、グループ、ID、IPアドレスなどが表示されます。

- ビデオタイルにカメラ映像を配置して再生するには、画面左のサイドバーにある **Map** リストでカメラをダブルクリックします。またはマウスの右ボタンをクリックし、ポップアップメニューで **Open Video** をクリックします。



カメラの名前、グループなどの詳細情報を確認するには、ポップアップメニューで**View Detail**をクリックします。

情報

- ビデオタイルは画面左上から順に追加され、現在の画面に追加スペースがない場合はエラーメッセージが表示されます。
- 映像の制御方法および映像に表示されるツールの詳細についてはビデオをモニタリングするを参照してください。
- マップ上でカメラが表示されない場合は、カメラグループの権限を確認してください。カスタム権限を持つ管理者がカメラグループの権限を設定していないと、カメラが表示されないことがあります。カメラグループの権限設定の詳細については カメラを設定するご参照ください。

デバイスをモニタリングする

デバイスおよびカメラのモニタリング機能の使用方法を説明します。デバイスとカメラの状態をチェックし、詳細情報を確認し、カメラ映像をリアルタイム再生するなど、さまざまな機能を利用できます。さらに、最近発生したイベントを確認してデバイスとカメラの状態を効率的に管理する方法もご確認ください。

Monitoring ページには、**Launcher** ページで **Monitoring** をクリックするか、画面左上のショートカットリストから **Monitoring** を選択してアクセスできます。

デバイスおよびカメラの状態チェック

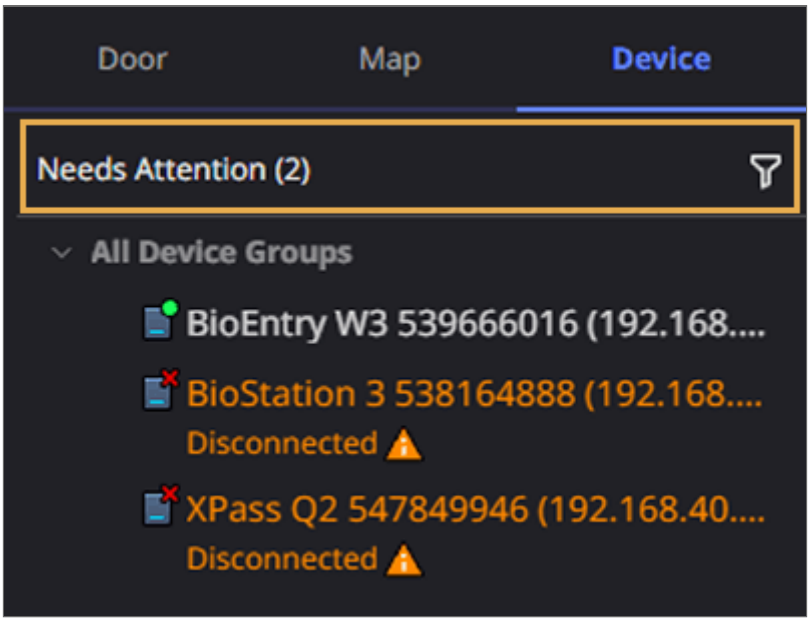
画面左側のサイドバーで**Device**タブをクリックします。すべてのデバイスとカメラの状態をチェックできます。デバイスとカメラの状態は以下を参照してください。

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。
	カメラが接続されています。

ステータスアイコン	説明
	カメラの電源がオフ、または接続が解除されています。

注意が必要なデバイスをまとめて表示

管理者は対応が必要なデバイスだけを一度にまとめて表示できます。画面左のサイドバーの **Needs Attention** をクリックします。デバイスの状態を確認し、問題が発生した対象に対応できます。



対応対象の判定基準

デバイスツリーで正常ではないデバイスを対応対象として判定します。

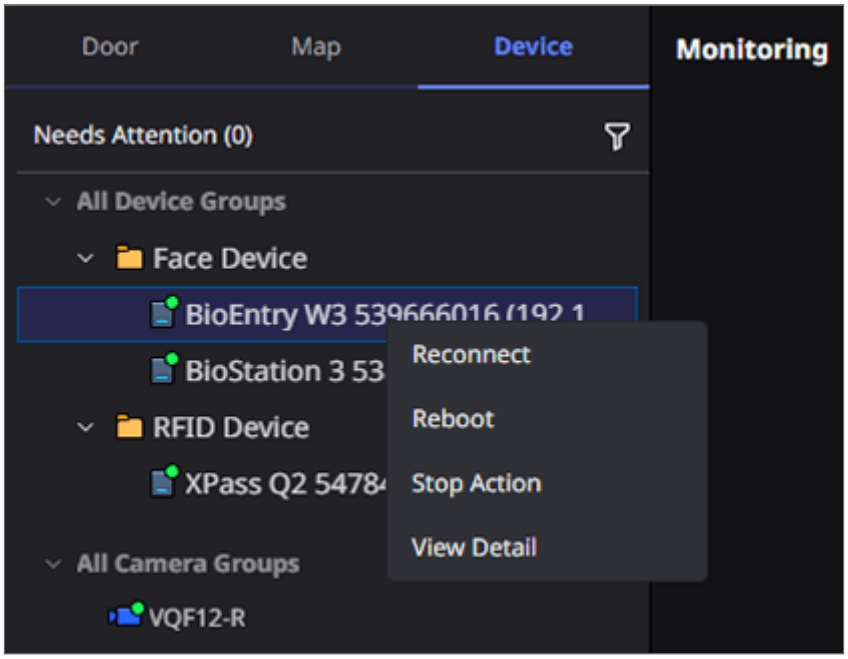
異常状態の種類	状態表示	説明
接続切断	**Disconnected**	デバイスとのネットワーク接続が切断された状態
同期化エラー	**Sync Error**	接続はされているが、データ同期がずれている状態
マルチコミュニケーションサーバーエラー	**Communications Server Error**	デバイスが属するマルチコミュニケーションサーバーでエラーが発生した状態
デバイスロック	**Device Locked**	作業条件と動作によりデバイスがロックされた状態
認証失敗ロック	**Auth Failure Lockout**	指定回数以上の認証失敗によりデバイスがロックされた状態

情報

- **Device Locked** 条件は 作業条件と動作を設定する で設定した作業条件および動作に基づいて決まります。この状態の確認と解除方法は デバイスロック解除 をご参照ください。
- **Auth Failure Lockout** 条件はデバイス設定で設定できます。詳しくは 認証を設定する をご参照ください。この状態の確認と解除方法は 認証失敗ロックアウト解除 をご参照ください。

デバイス制御

画面左側のサイドバーのデバイス一覧で目的のデバイスを選択し、右クリックします。ポップアップメニューで必要な機能を選択できます。



デバイスタイプによって表示される制御機能が異なる場合があります。

機器タイプ	制御機能
マスター デバイス、スレーブなしでサーバーに直接接続される基本デバイス	**Stop Action**、 **Reboot**、 **Unlock Device**、 **Release Auth Failure Lockout**、 **Reconnect**(サーバーからデバイスに接続する方式の場合のみ)
スレーブ デバイス	**Stop Action**、**Reboot**、**Unlock Device**、**Release Auth Failure Lockout**
OSDP 通信デバイス	**Unlock Device**, **Reconnect**(接続方式によって異なる)
Wiegand 機器	**Unlock Device**
拡張モジュール（Secure I/O 2、DM-20、OM-120、IM-120）	**Stop Action**
デバイスからサーバーへ接続する方式のデバイス	**Stop Action**、**Reboot**、**Unlock Device**、**Release Auth Failure Lockout**

機器タイプ	制御機能
ワイヤレスアンテナモジュール	なし

デバイス再接続

デバイスの接続状態に関係なく、ポップアップメニューで**Reconnect**をクリックしてください。接続が切れたデバイスは再接続を試みます。正常に接続されたデバイスは、設定を再送信し、異常状態を解消します。デバイスが再接続されると、ステータスアイコンが正常状態（ ）に変わります。

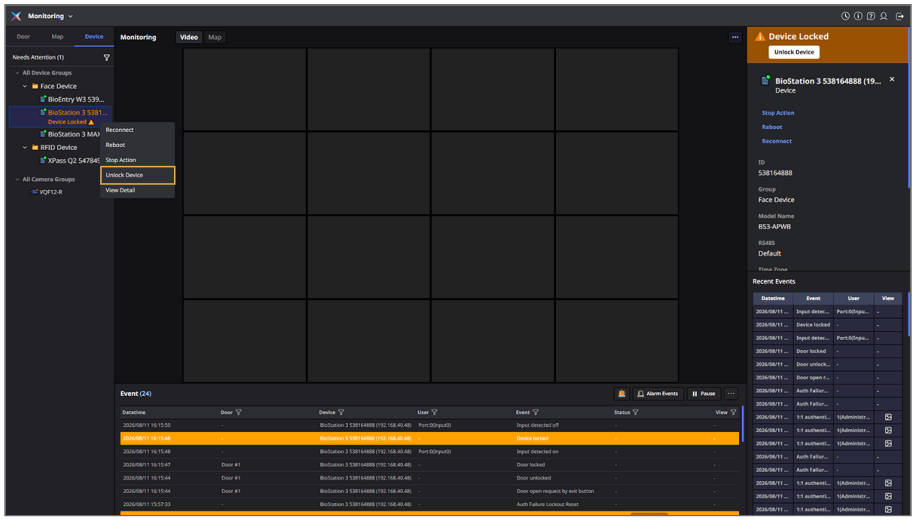
> **情報**
>
> **Reconnect**機能は、**Device ▶ Server Connection**オプションに設定したデバイスをサポートしません。デバイスの登録に関する詳細は、デバイスを登録するをご参照ください。

デバイス再起動

デバイスを再起動するには、ポップアップメニューで**Reboot**をクリックします。警告メッセージウィンドウが表示されたら、**Ok**ボタンをクリックしてください。

デバイスロック解除

管理者が設定した動作条件と動作によってデバイスがロックされると、画面左側のサイドバーでデバイス名の下に**Device Locked**状態が表示されます。デバイスを選択すると、画面右側のプレビューパネル上部にも同じバナーが表示されます。



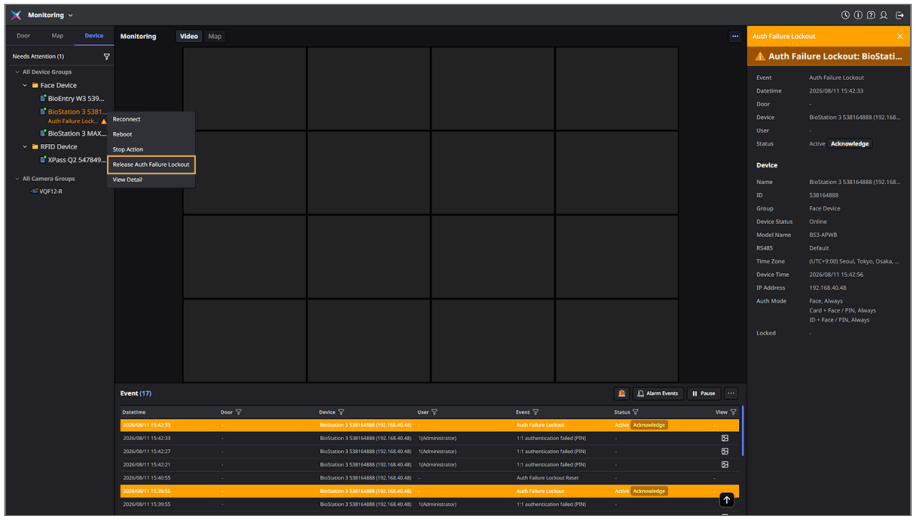
- デバイスがロック状態のときだけ、ポップアップメニューに**Unlock Device**が表示されます。ロック状態を解除するには、ロックされたデバイスを選択し、ポップアップメニューで**Unlock Device**をクリックします。
- ロックされたデバイスを選択し、画面右側のプレビューパネル上部に表示されるバナーで**Unlock Device**ボタンをクリックします。

> **情報**
>
> **Unlock Device**機能は、**Administrator**または**Monitoring Operator**権限を持つユーザーにだけ表示されます。

認証失敗ロックアウト解除

Auth Failure Lockoutオプションで設定した回数以上、認証に失敗するとデバイスがロック状態に切り替わります。デバイスがロックアウト状態になると、画面左側のサイドバーでデバイス名の下に**Auth Failure Lockout**状態が表示されます。デバイスを選択すると、画面右側のプレビューパネル上部にも同じバナーが表示され、イベント発生時刻とデバイス情報を確認できます。

デバイスが認証失敗ロックアウト状態のときだけ、ポップアップメニューに**Release Auth Failure Lockout**が表示されます。ロックされたデバイスを選択し、ポップアップメニューで**Release Auth Failure Lockout**をクリックしてください。



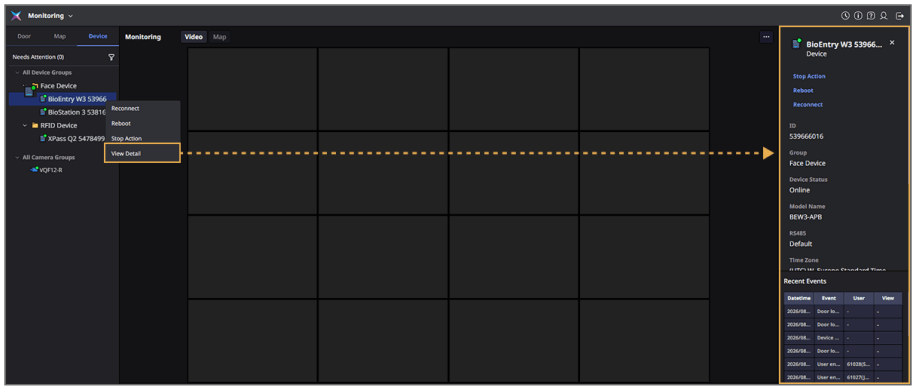
> **情報**
>
> - **Release Auth Failure Lockout**メニューは、**Administrator**または**Monitoring Operator**権限を持つユーザーにだけ表示されます。
> - 設定したロック時間（**1st Lockout Duration**/**2nd Lockout Duration**）が経過すると、デバイスが自動的にロックを解除します。この場合、追加の操作なしでロック状態が解除されます。ロック条件およびロック時間設定の詳細は認証を設定するを参照してください。

作業停止

デバイスで実行中のアラームベースおよびトリガーベースの動作をすべて停止するには、ポップアップメニューで**Stop Action**をクリックしてください。画面上部に作業停止成功のメッセージが表示されます。

デバイスの詳細表示

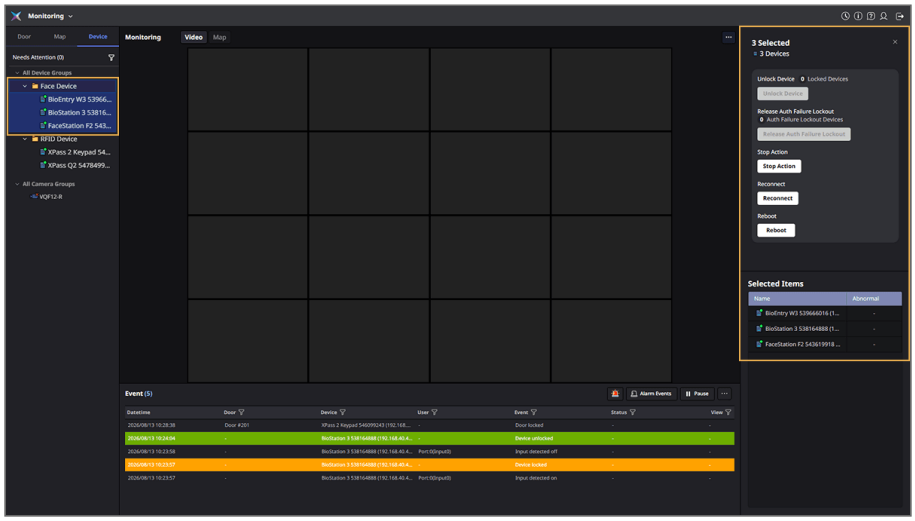
デバイスの詳細情報を確認するには、ポップアップメニューで**View Detail**をクリックします。またはデバイスをダブルクリックします。画面右側にデバイスの詳細情報が表示されます。



- **デバイス制御**：デバイスの動作を停止、再起動、再接続するなどの制御を実行できます。
- **デバイス詳細情報**：デバイスのIDとグループ、モデル名、起動時間、IPアドレスなどの情報を確認できます。
- **Recent Events**：選択したデバイスで発生した最近のイベント一覧を確認できます。

複数のデバイスを一括で制御する

複数のデバイスをまとめて選択し、再接続、再起動、ロック解除などのコマンドを一括で実行する方法を説明します。画面左のサイドバーにある **Device** タブでデバイスを二台以上選択すると、画面右に一括制御パネルが表示されます。



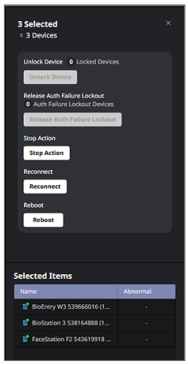
> **情報**
> カメラは一括制御の対象ではありません。カメラの制御方法については、カメラを制御するをご参照ください。

複数のデバイスを選択する

画面左のサイドバーにある**Device**タブでデバイスを選択する方法は次のとおりです。

- `Ctrl` **+ クリック**：クリックしたデバイスを選択リストに追加または除外します。ほかの選択はそのまま残ります。
- `Shift` **+ クリック**：最後にクリックしたデバイスから、今クリックしたデバイスまでの範囲を選択します。デバイスグループは範囲選択の対象外です。
- **グループ（🗀）をクリック**：グループ名をクリックすると、その下のすべてのデバイスが選択リストに追加されます。すでに選択したデバイスはそのままです。

> **情報**
>
> - 配下にデバイスがない空のグループだけを選択すると、画面右のパネルが閉じます。
> - デバイスを一台だけ選択するとデバイス詳細情報パネルが表示され、二台以上選択すると一括制御パネルに切り替わります。



一括制御パネルの構成

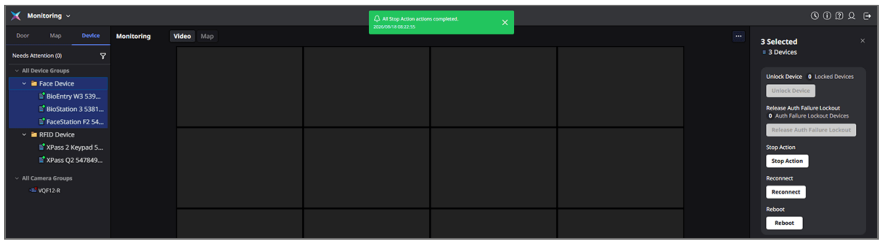
- **Unlock Device**, **Release Auth Failure Lockout**：選択したデバイスの中にロック、または認証失敗によるロックアウト状態のデバイスがある場合に有効になり、ボタンの横に対象デバイス数が表示されます。
- **Stop Action**, **Reconnect**, **Reboot**：対象デバイス数は表示せず、選択したデバイスの中に該当する制御をサポートするデバイスがある場合に有効になります。
- デバイス制御：**Unlock Device**、**Release Auth Failure Lockout**、**Stop Action**、**Reconnect**、**Reboot**の実行ボタンを使用できます。
- 区切り線：デバイス制御領域と**Selected Items**の間の境界線を上下にドラッグすると、両領域の高さ配分を調整できます。
- **Selected Items**: 選択したデバイスの接続状態、名前、異常状態を表示します。異常状態の種類は 対応対象の判定基準 をご参照ください。

各ボタンをクリックすると、確認ウィンドウを表示します。確認ウィンドウで **Cancel** をクリックすると、選択した操作を実行しません。選択した操作が表示されたボタンをクリックすると、選択したすべてのデバイスに対してその操作を実行します。

> **情報**
>
> 選択したデバイスの種類が混在している場合、各デバイスがサポートする制御をまとめて表示します。選択したデバイスのいずれでもサポートされていない制御のボタンは表示されません。サポートする制御が一つもない場合は、案内文と選択デバイス一覧表のみが表示されます。

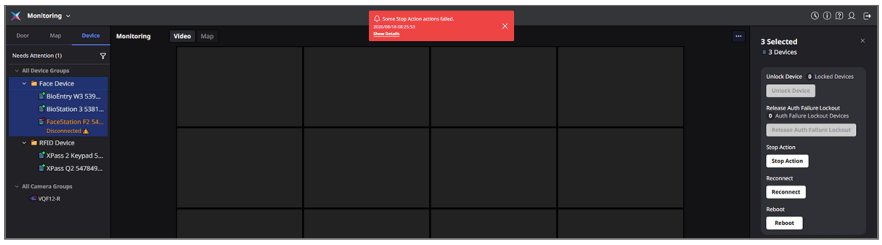
実行結果を確認する

- 選択したすべてのデバイスが成功した場合、成功メッセージのみを表示します。



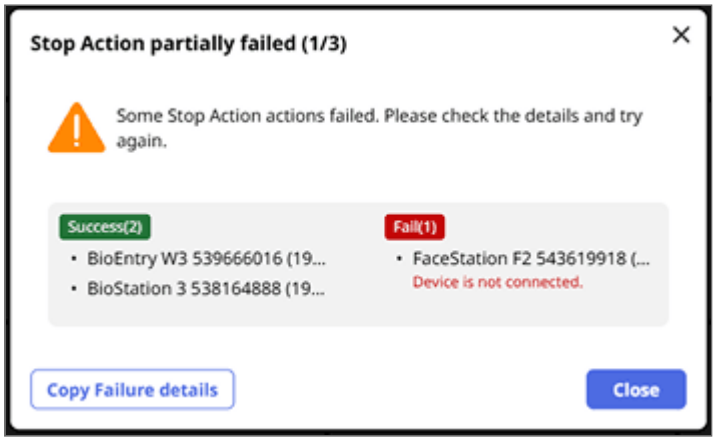
上記の画像は例示です。実際の画面とは異なる場合があります。

- 一台でも失敗した場合、失敗メッセージとともに **Show Details** ボタンが表示されます。



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。

Show Detailsをクリックすると、**Success**、**Failure**、**Skipped**の三つのグループに区分された結果を確認できます。失敗した対象の名前と理由をクリップボードにコピーするには、**Copy Failure details**ボタンをクリックします。



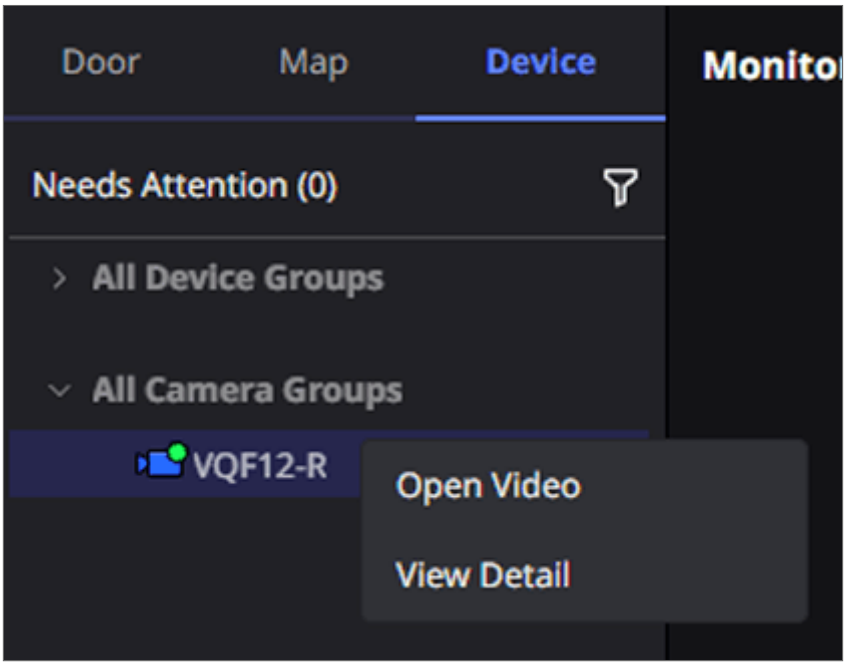
上記の画像は例示です。実際の画面とは異なる場合があります。

情報

- **Reconnect** ボタンは例外です。リクエストを受け付けると、常に成功メッセージのみを表示します。失敗の有無や詳細結果ウィンドウは提供しません。実際に接続できたかどうかは、ステータスツリーで確認してください。
- **Unlock Device** と **Release Auth Failure Lockout** はそれぞれ別に処理され、結果ウィンドウも別々に表示します。

カメラを制御する

画面左側のサイドバーのカメラ一覧で目的のカメラを選択し、右クリックします。ポップアップメニューで必要な機能を選択できます。



カメラ映像の再生

ビデオタイルにカメラ映像を配置してリアルタイムにモニタリングするには、ポップアップメニューで**Open Video**をクリックします。

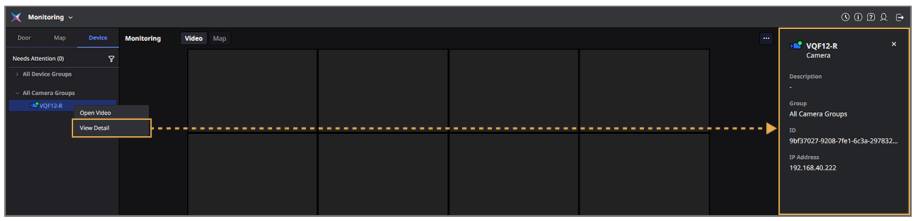
ビデオタイルにカメラ映像を追加する方法として、以下の方法もサポートしています。
- 画面左側のサイドバーのカメラ一覧で、映像を再生するカメラをダブルクリックします。
- カメラをビデオタイル領域にドラッグ＆ドロップして映像を追加することもできます。

情報

- ビデオタイルは画面左上から順に追加され、現在の画面に追加スペースがない場合はエラーメッセージが表示されます。
- 映像の制御方法や、映像上に表示されるツールの詳細については、ビデオをモニタリングするをご参照ください。
- **All Camera Groups**の一覧にカメラが表示されない場合は、カメラグループの権限を確認してください。カスタム権限を持つ管理者がカメラグループの権限を設定していないと、カメラが表示されないことがあります。カメラグループの権限設定の詳細については カメラを設定するご参照ください。

カメラの詳細表示

カメラの詳細情報を確認するには、ポップアップメニューで **View Detail** をクリックしてください。カメラのグループ、説明、ID、IP アドレスを確認できます。

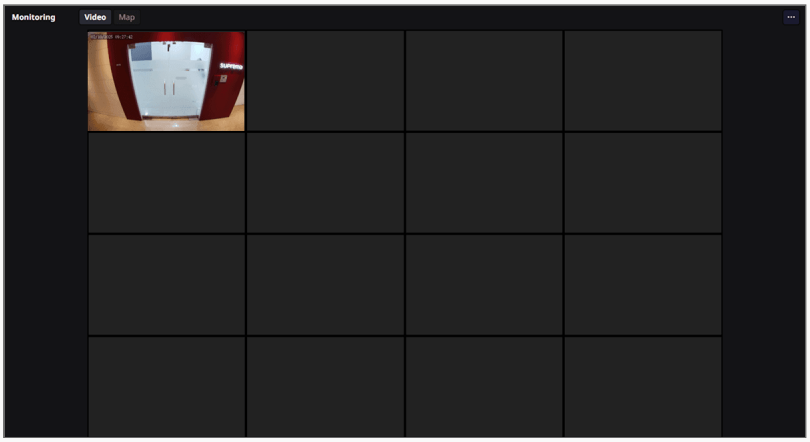


ビデオをモニタリングする

ビデオモニタリング機能を使用すると、ドア、エリア、デバイスに連携されたカメラ映像をリアルタイムで確認し、制御できます。本書では、ビデオタイルを使用してカメラ映像を追加し、サイズ変更、位置変更、全画面表示などのさまざまな操作を行う方法を説明します。さらに、アラーム状態の確認や解除といった管理機能によって、セキュリティ状況に迅速に対応できるよう支援します。

情報

- **ビデオタイル**は、画面中央に位置するカメラ映像表示エリアです。複数のカメラ映像を同時に配置してモニタリングできるインターフェースコンポーネントです。ユーザーはビデオタイルで映像のサイズを調整したり位置を変更し、必要に応じて映像を閉じたり全画面に切り替えたりできます。



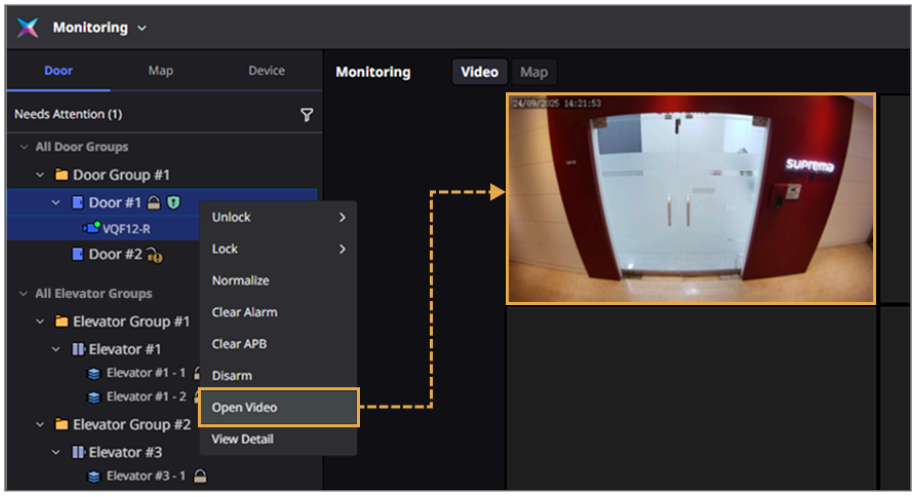
- **Monitoring** エリアは、システムに登録されたデバイスカメラがない、またはマップ構成要素（エリア、施設、階）が登録されていない場合、有効になりません。
- VMSと連携してカメラを追加・管理する方法については、ビデオ設定を参照してください。
- VMS の録画映像を再生するときにロードエラーが発生する場合は、VMS サーバーに証明書をインストールし、クライアント PC にも VMS サーバーの証明書をインストールする必要があります。詳細については次のドキュメントを参照してください。
  - VMS サーバーでの証明書インストール
  - クライアント PC での VMS サーバー証明書のインストール
- エリアと連動しているカメラが表示されない場合は、カメラグループの権限を確認してください。カスタム権限を持つ管理者がカメラグループの権限を設定していないと、カメラが表示されないことがあります。カメラグループの権限設定の詳細については カメラを設定するご参照ください。
- ビデオモニタリングは **エッセンシャル**(Essential) 以上のライセンス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。

映像を再生する

ビデオタイルにカメラ映像を追加してモニタリングできます。ビデオタイルは画面中央に配置され、複数のカメラ映像を同時にモニタリングできます。

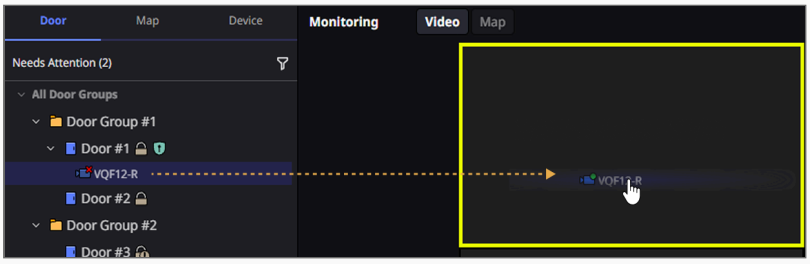
1. 画面左のサイドバーで **Door** または **Map**、**Device** タブから映像を確認するカメラデバイスを選択します。
2. マウスの右ボタンをクリックします。
3. ポップアップメニューで **Open Video** をクリックしてください。

選択したカメラの映像を画面中央のビデオタイルに配置できます。



情報

- サイドバーのリストからカメラを選択し、ビデオタイル領域へドラッグ＆ドロップして映像を追加することもできます。



- ビデオタイルは画面左上から順に追加され、現在の画面に追加スペースがない場合はエラーメッセージが表示されます。

映像を制御する

ビデオタイルに配置した映像はデフォルトでリアルタイム再生されます。再生ツールを使って映像を停止したり、過去の録画映像を確認できます。



1. カメラデバイスの名前です。
2. 映像を全画面(⛶)で再生したり、ビデオタイルから除外(×)したりできるボタンです。

3. 映像の再生位置を調整できるスライダーです。スライダーをドラッグして過去時点の映像を表示できます。
4. ▶ または ⏸ をクリックして動画を再生または一時停止します。
5. 現在の映像をリアルタイムで再生していることを示すアイコンです。過去の映像を再生中にリアルタイム映像へ戻すには、このアイコンをクリックしてください。

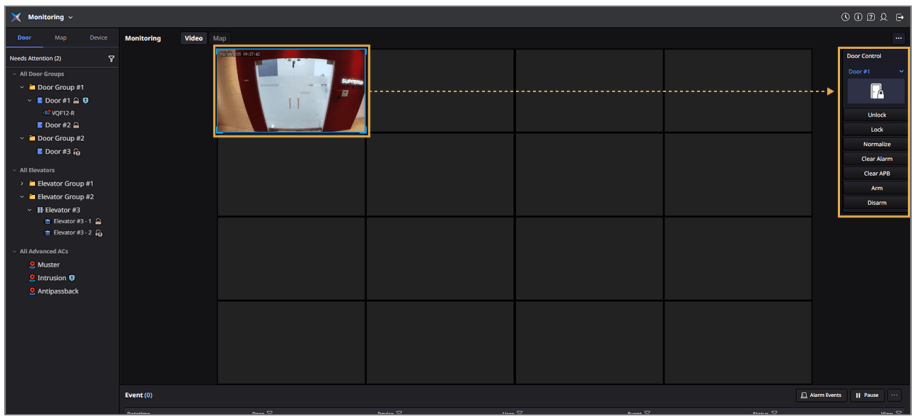
録画映像の再生状態の維持と失敗通知

Video タブから別の画面に移動した後（例：別のページに移動、**Map** タブに切り替え、更新）、再度 **Video** タブに戻ると、以前再生していた録画映像の状態を維持します。このとき、各ビデオタイルは配置順に映像を再読み込みします。

> **情報**
> 映像ごとに応答速度が異なるため、再生失敗が表示されるタイミングはタイルごとに異なる場合があります。ただし、再生に失敗するタイルは、タイル順で後ろ側から現れる傾向があります。

ドア制御ツール

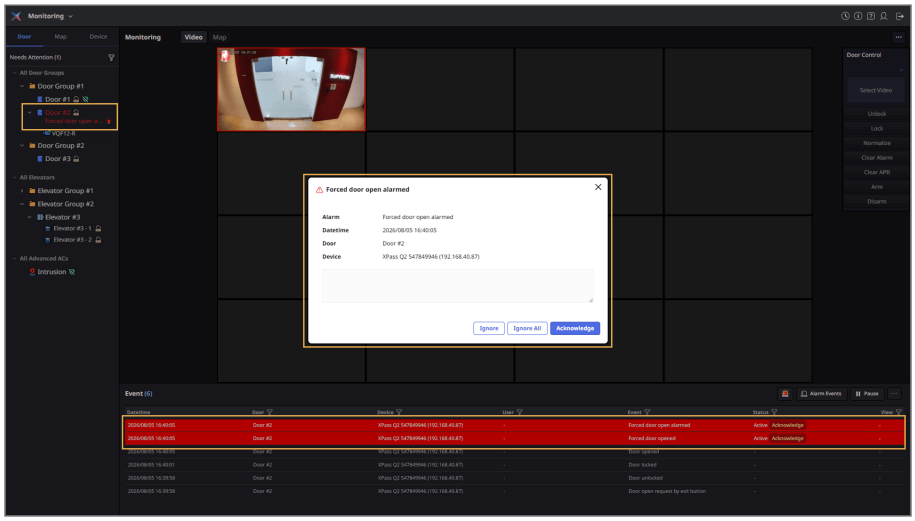
映像を追加した後、**Door Control** ツールを使用して追加操作を実行できます。ビデオタイルでドアに連携されたカメラを選択すると、ドアを制御できる **Door Control** ツールが有効になります。ドアの開放、ロック、解除、アラーム解除などの機能を利用できます。



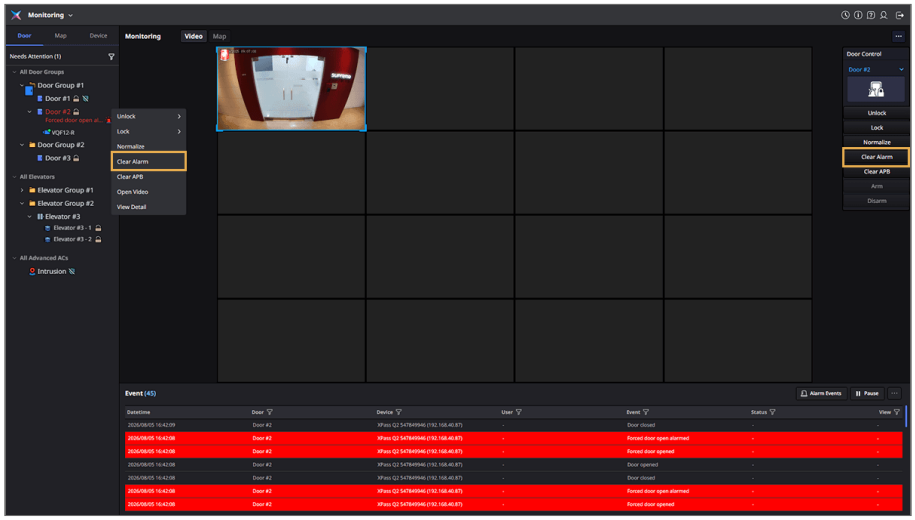
> **情報**
> - **Door Control** ツールは、右パネルに何も開かれていないときに使用できます。右パネルに詳細情報が開いている場合は、閉じてから使用してください。
> - この機能を使用するには、ドアにカメラが連携されている必要があります。出入口とカメラの連携の詳細については、ビデオルールを設定するを参照してください。
> - **Door Control** ツールで利用できる機能の詳細については、出入ドアを制御するを参照してください。

映像アラームを確認する

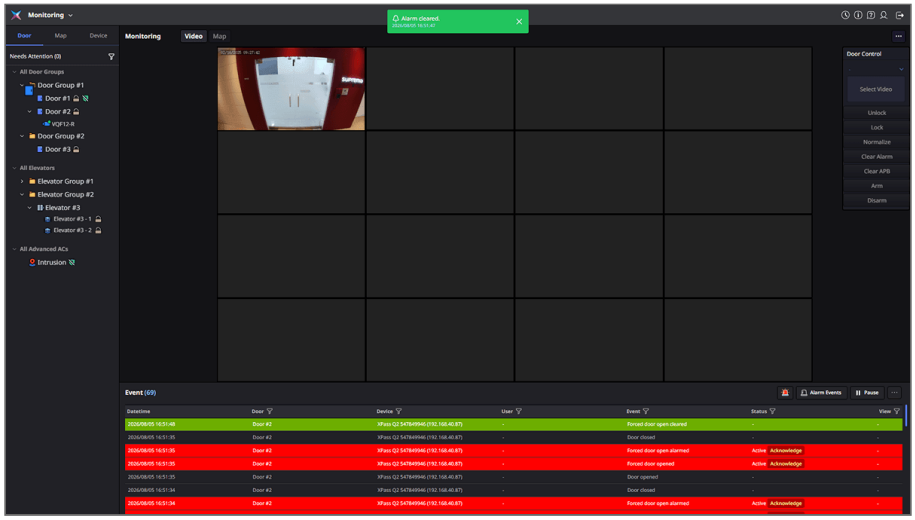
カメラと連携されたドアのいずれかがアラーム状態になると、映像にアラームアイコンが表示されます。連携されたドアのアラームをすべて解除すると、アラームアイコンが消えます。



ドアのアラームを解除するには、ドアリストで右クリックし、ポップアップメニューから **Clear Alarm** をクリックします。または **Door Control** ツールで **Clear Alarm** をクリックします。



画面上部に成功または失敗メッセージが表示されます。

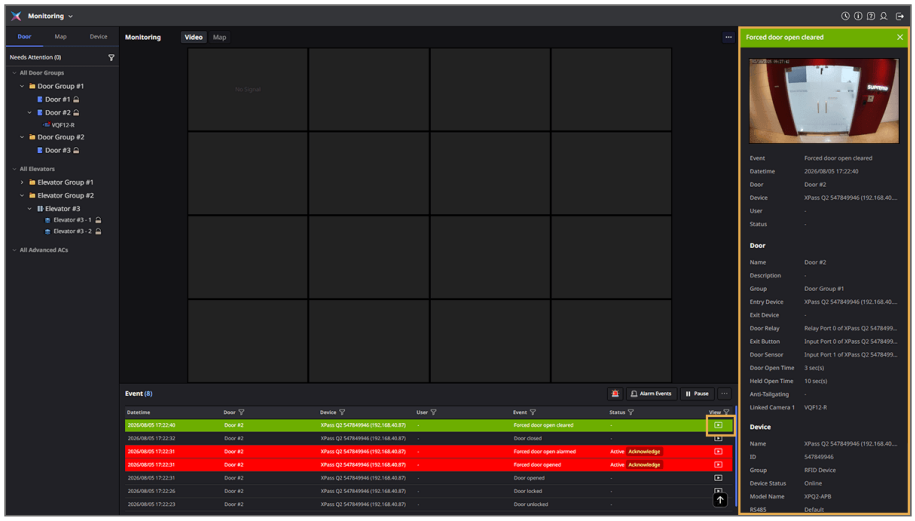


情報

画面下部の **Event** セクションの詳細については、イベントをモニタリングするを参照してください。

ビデオログを確認する

ルールで設定されたドアで特定のイベントが発生すると、**Event** セクションの該当イベント項目にビデオログ(▶)アイコンが表示されます。ビデオログアイコンが表示されたイベント項目をクリックすると、画面右側に詳細情報が表示されます。特定のイベントが発生した時刻の映像を確認できます。



情報

- ビデオログアイコンは、ドアにカメラが連携されている場合に表示されます。カメラと出入口の連携の詳細については、ビデオルールを設定するを参照してください。
- イベント設定ルールに基づき、最初に接続されたカメラを優先して再生します。映像をさらに大きな画面で再生するには、画面をダブルクリックします。
- ドアには最大4台のカメラを接続でき、映像下部のカメラボタンをクリックして目的のカメラ映像を再生できます。接続されているカメラが1台のみの場合、カメラボタンは表示されません。
- 画面下部の **Event** セクションの詳細については、イベントをモニタリングするを参照してください。

ビデオタイルのレイアウトを設定する

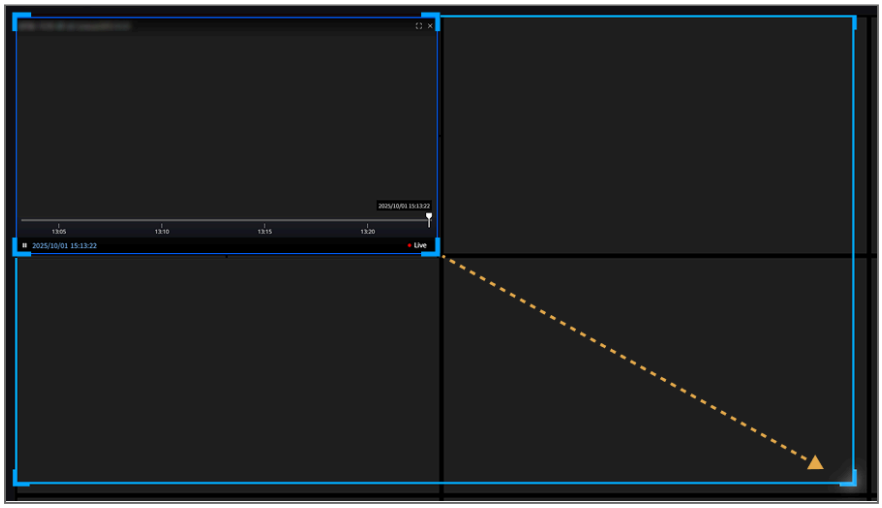
ビデオタイルに配置した映像は、サイズを変更したり任意の位置に移動したりできます。重要度に応じて映像のサイズを調整し、位置を変更してモニタリングします。

映像サイズを変更する

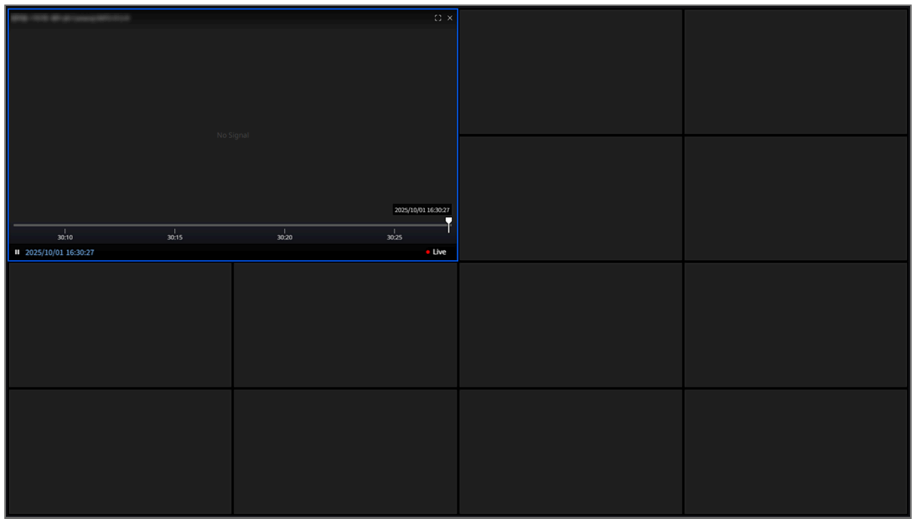
1. サイズを変更する映像をクリックすると、選択した映像のフレームがアクティブになります。



2. フレームの境界にカーソルを合わせると、サイズを調整できるカーソルに変わります。
3. 角をクリックして希望のサイズまでドラッグします。

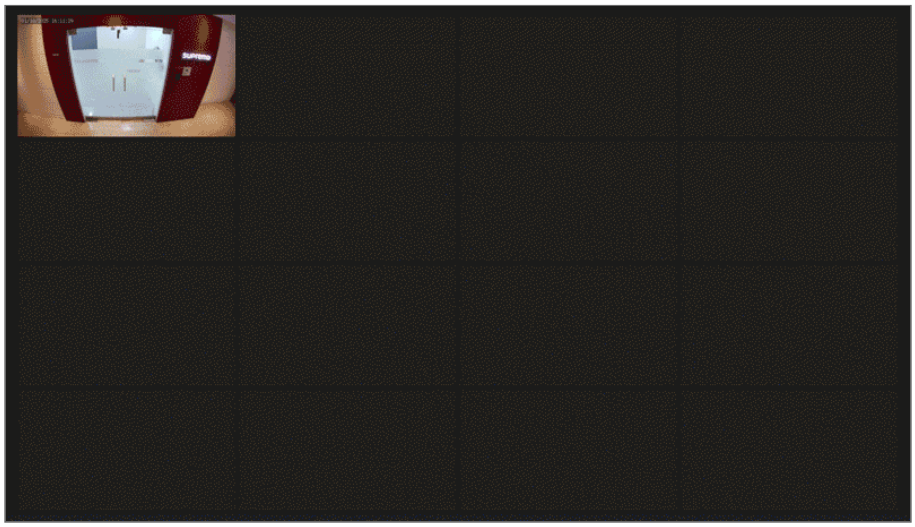


配置されたタイルのサイズに比例して映像のサイズを調整できます。逆に映像のサイズを縮小することもできます。



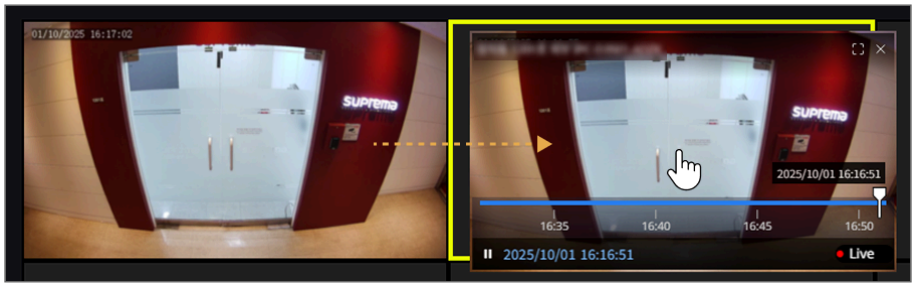
映像を拡大する

映像をビデオタイルの全体サイズに拡大するには、映像をダブルクリックします。映像がビデオタイルのサイズに拡大されます。

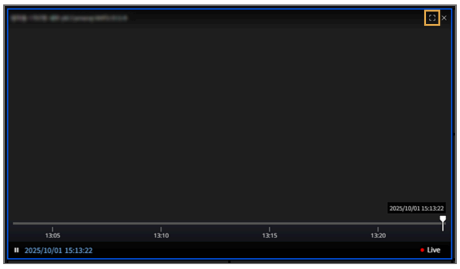


映像の位置を変更する

位置を変更する映像をクリックし、目的の位置へドラッグします。選択した映像の位置を変更できます。



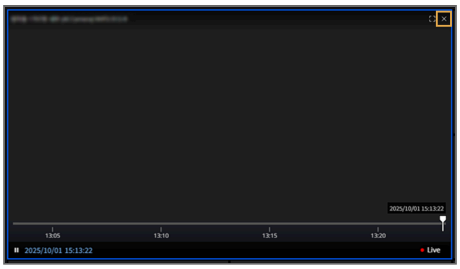
全画面で表示する



ビデオタイルに配置された映像を全画面で表示するには、映像右上の ⛶ ボタンをクリックします。

全画面表示を終了するには、画面右上の ⛶ ボタンをクリックしてください。またはキーボードの キーを押します。

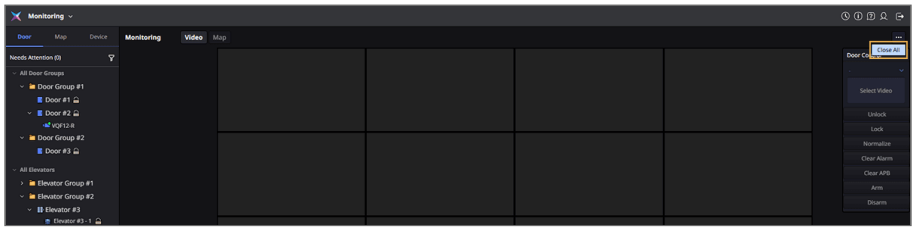
映像を閉じる



ビデオタイルに配置された映像を閉じるには、映像右上の ✕ ボタンをクリックします。

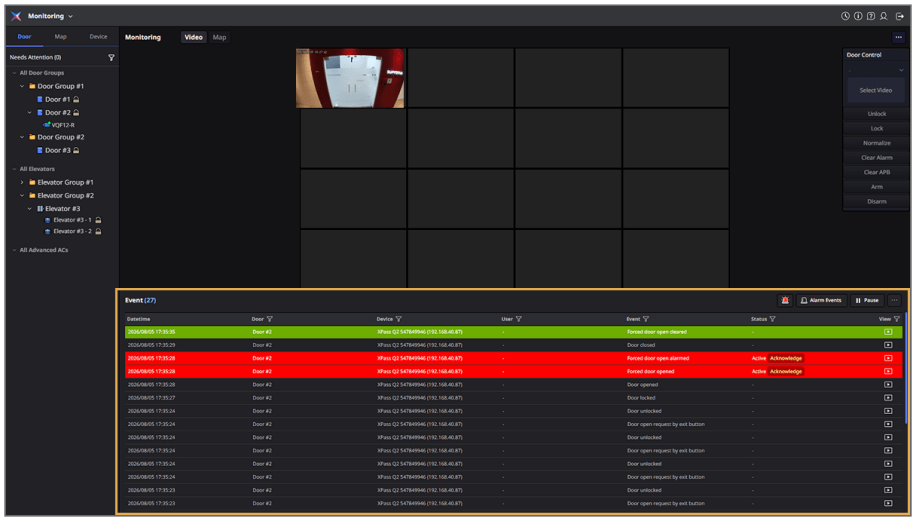
すべての映像を閉じる

ビデオタイルに配置したすべての映像を閉じるには、画面右上の ••• ボタンをクリックします。ポップアップメニューで **Close All** をクリックしてください。



イベントをモニタリングする

モニタリングページの画面下部にある **Event** セクションで、リアルタイムで発生するイベントを確認および管理できます。イベントの状態、アラームイベント処理、フィルタリング、色分けなど多様な機能により、イベントを効率的に管理できます。特に、ドア、デバイス、ユーザーに関連するイベントをリアルタイムでモニタリングし、必要な対応を迅速に行えます。



イベント一覧を確認する

Event セクションでは、発生したイベントをリアルタイムで確認できます。イベントには次の情報が含まれます。



- **Datetime**：イベントが発生した日時です。
- **Door**：イベントが発生したドアです。
- **Device**：イベントが発生したデバイスです。
- **User**：イベントを発生させたユーザーです。
- **Event**：イベントの詳細内容です。
- **Status**：イベントの状態です。アクティブなイベントの場合、**Active** 状態で表示されます。アラームイベントには **Acknowledge** ボタンが表示されます。 **Acknowledge** ボタンをクリックすると、該当イベントが解除されます。

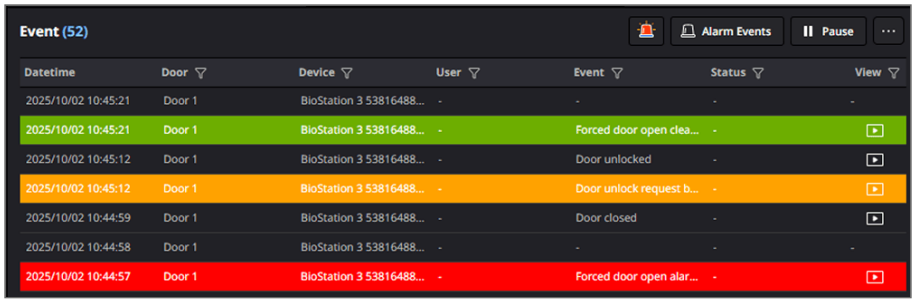


- **View**：イベントに扉に接続されたカメラの映像情報が含まれている場合、ビデオアイコン(▶)が表示されます。アイコンをクリックすると映像を確認できます。

> **情報**
>
> - 個別のイベントをクリックすると、画面右側に詳細情報が表示されます。詳細情報には、イベント発生日時とエリア、ドア、デバイス、ユーザーグループ、ユーザー、ポート、イベントの詳細が含まれます。
> - イベントにドアに接続されたカメラの映像または画像情報が含まれている場合、ビデオおよびイメージログも確認できます。

色によるイベント区分

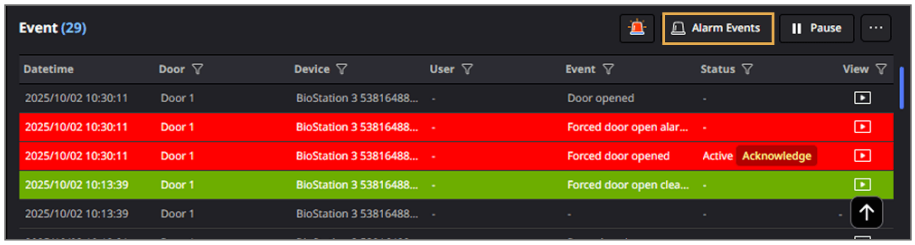
イベント一覧に表示されるイベントは色分けで区別できます。



- **色なし**：通常イベントです。
- オレンジ：注意イベントです。アクセスが許可されていないエリアにユーザーが入ろうとした場合や、ドアが開いたままの場合など、注意が必要なイベントです。
- 赤：アラームイベントです。システムで発生したイベントのうち、対応が必要な警告イベントです。
- 緑：解除されたアラームイベントです。

アラームイベントの確認

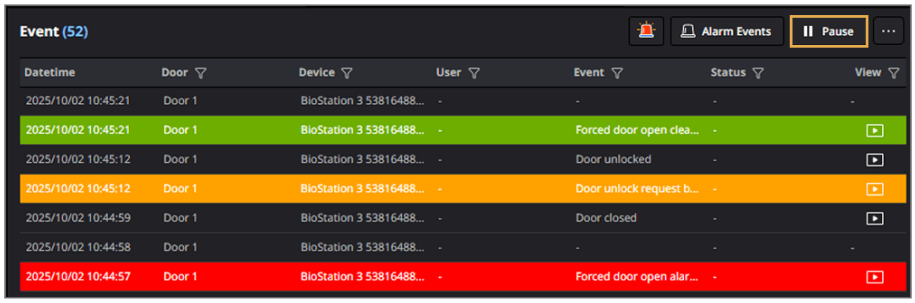
Event セクションの一覧でアラームイベントのみを確認できます。 **Event** セクション右上の **Alarm Events** ボタンをクリックします。イベント一覧にはアラームイベントのみが表示されます。アラームイベントは赤色で表示されます。



> **情報**
>
> **Event** セクション右上の **All Events** ボタンをクリックすると、アラームイベントを含むすべてのイベントを確認できます。

リアルタイムイベント

Event セクションのイベント一覧では、リアルタイムで発生するイベントを確認できます。リアルタイムイベントを停止するには、**Event** セクション右上の **Pause** ボタンをクリックします。 **Play** ボタンをクリックすると、リアルタイムイベントを再開します。

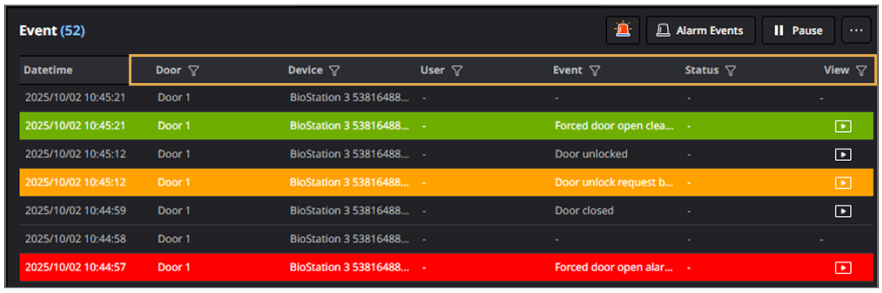


イベントのフィルタリング

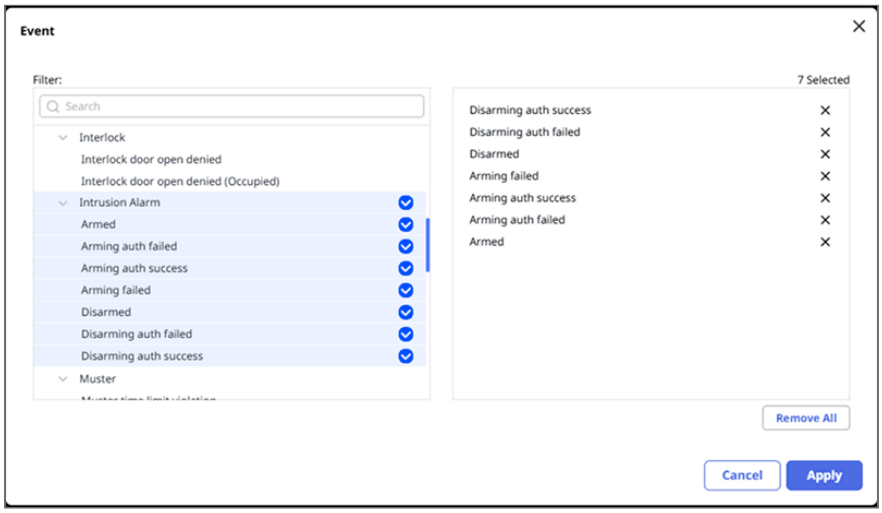
フィルター適用

ユーザーが希望する条件でイベント一覧をフィルタリングできます。これにより、目的の条件に合ったイベントを素早く確認できます。

1. **Event** セクション一覧の各ヘッダー列で ▽ アイコンをクリックします。



2. フィルターウィンドウが表示されたら、左側の一覧から目的の項目をクリックします。



- 上位の項目を選択すると、下位の項目をすべて選択できます。
- 選択した項目を解除するには、✕ ボタンをクリックしてください。すべての項目を解除するには **Remove All** ボタンをクリックします。

3. すべての設定が完了したら、**Apply** ボタンをクリックします。

イベント一覧には設定した条件のイベントのみが表示されます。

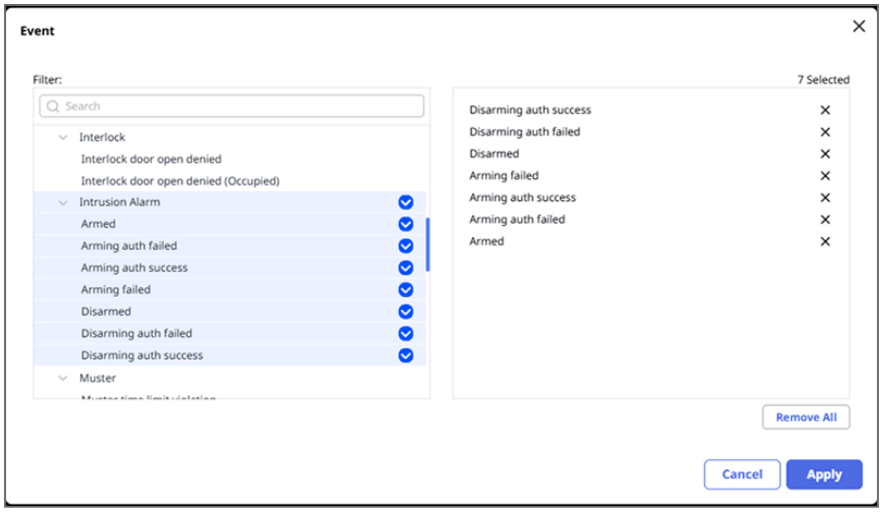
情報

- フィルターウィンドウの検索入力フィールドを使って目的の項目を素早く検索することもできます。
- 各ヘッダー列ごとに複数の条件を設定できます。 1つ以上の条件を設定すると、 AND 条件が適用されます。
- ヘッダー列ごとにフィルタリング可能な項目は異なる場合があります。
- フィルター条件を設定すると、ヘッダー列の ▼ アイコンの色が変わります。

フィルタリング解除

適用したフィルター条件を解除できます。

1. **Event** セクション一覧でフィルターが適用されているヘッダー列の ▼ アイコンをクリックしてください。
2. フィルターウィンドウが表示されたら、右側の一覧で解除したい項目の右側にある ✕ ボタンをクリックしてください。すべてのフィルターを解除するには、**Remove All** ボタンをクリックします。



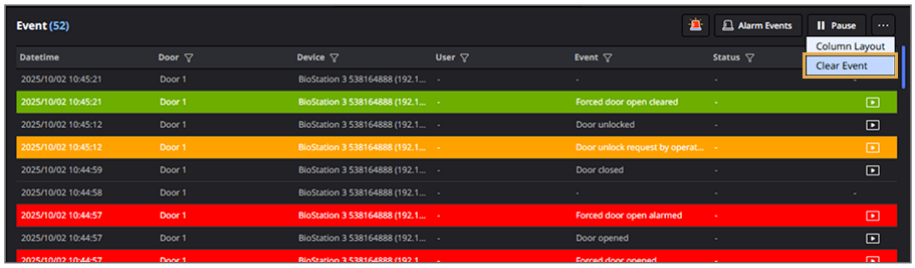
3. 解除する条件をすべて設定したら、**Apply** ボタンをクリックします。

情報

- フィルターウィンドウの検索入力フィールドを使って目的の項目を素早く検索することもできます。
- フィルター条件が解除されると、ヘッダー列のアイコンの色が元に戻ります。

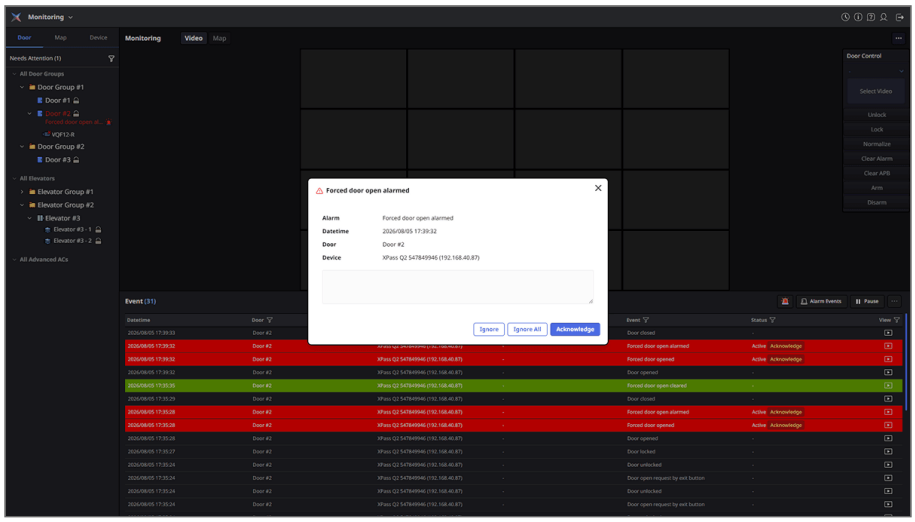
イベント一覧をクリア

Event セクションの一覧からイベントを削除できます。 **Event** セクション右上の ••• ボタンをクリックし、ポップアップメニューで **Clear Event** を選択します。イベント一覧に不要なイベントが大量に溜まっている場合は、**Clear Event** 機能を使用して整理できます。



アラームの確認および措置内容の記録

ドアの強制開放などのアラームイベントが発生すると、アラームメッセージウィンドウが表示されます。アラームメッセージウィンドウには、発生したアラームイベントの詳細が含まれます。このとき管理者は、発生したアラームイベントの認知状況と措置内容を記録できます。



情報

Ignore All ボタンは、アラームイベントが2件以上発生した場合にのみ表示されます。

アラームイベントへの措置内容の記録

メッセージ入力フィールドにアラームイベントへの措置内容を入力します。最大500文字まで入力できます。措置内容を入力して **Acknowledge** ボタンをクリックします。アラームイベントの認知状況と措置内容が記録されます。アラームメッセージウィンドウが閉じられます。



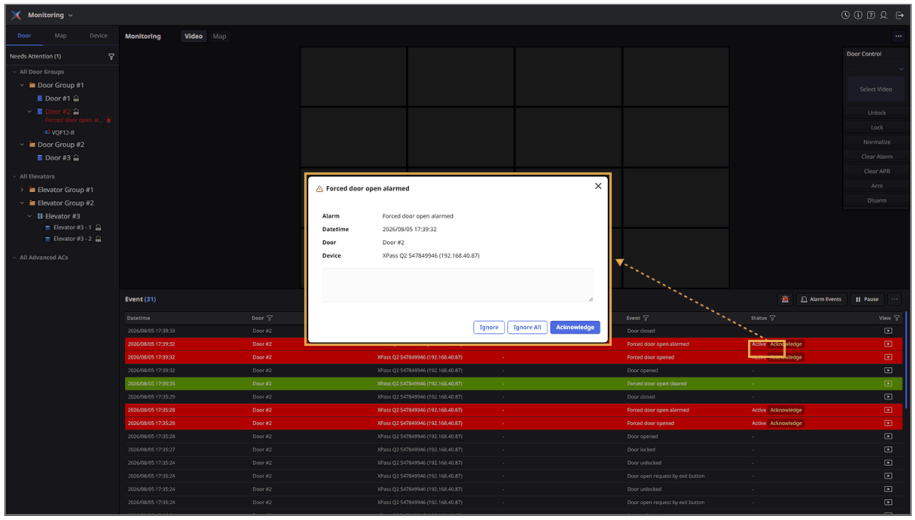
アラームイベントの認知保留

Ignore ボタンをクリックして、アラームイベントの認知を保留することもできます。対応事項を記録できます。アラームメッセージウィンドウが閉じられます。保留したアラームイベントはイベント一覧で **Active** 状態で表示され、**Acknowledge** ボタンを使用できます。



イベント一覧でアラームイベントを確認

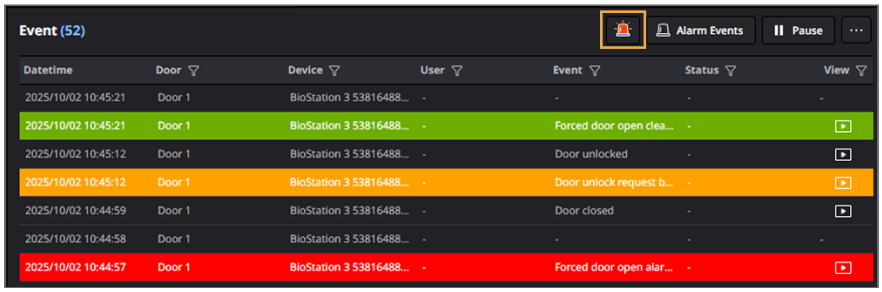
イベント一覧の **Status** 列に表示される **Acknowledge** ボタンをクリックすると、発生したアラームイベントの認知状況と措置内容を記録できます。入力を完了し、**Acknowledge** ボタンをクリックします。



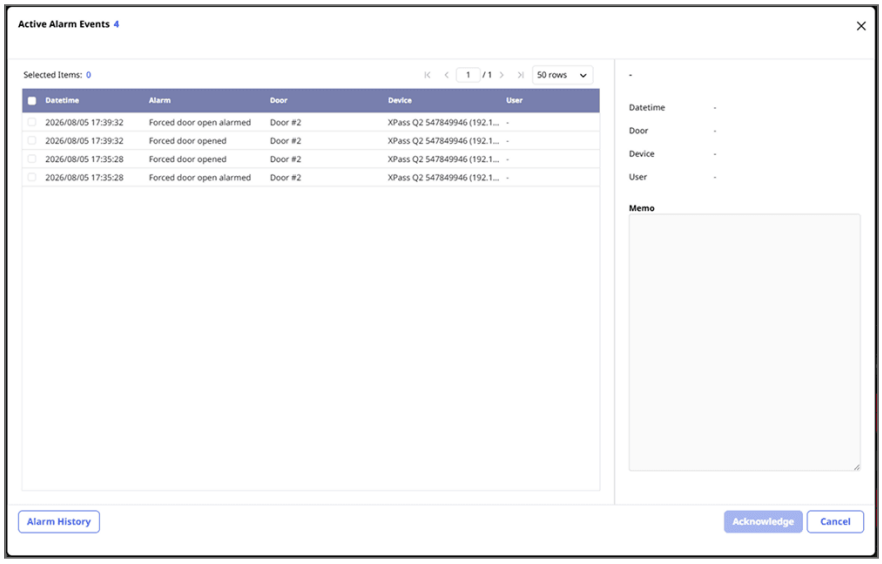
未確認のアラームイベントを表示する

まだ確認していないアラームイベントを一度に確認し、対応事項を記録できる機能を提供します。同じアラームイベントが複数発生した場合に有用です。

1. **Event** セクション右上の  ボタンをクリックします。



2. **Active Alarm Events** ウィンドウが表示されたら、左側の一覧で措置内容を記録するアラームイベントを選択します。すべてのイベントを選択するには、ヘッダー列一番左のチェックボックスをクリックします。



3. **Memo** 入力フィールドにアラームイベントへの措置内容を入力します。
4. **Acknowledge** ボタンをクリックします。

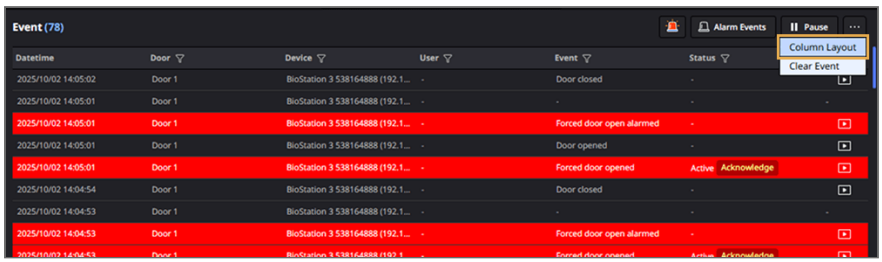
選択したイベントに対する対応事項を記録します。アラームイベントのポップアップウィンドウが閉じられます。

> **情報**
> アラームイベント一覧で1件以上のイベントを選択すると、**Acknowledge** ボタンが有効になります。

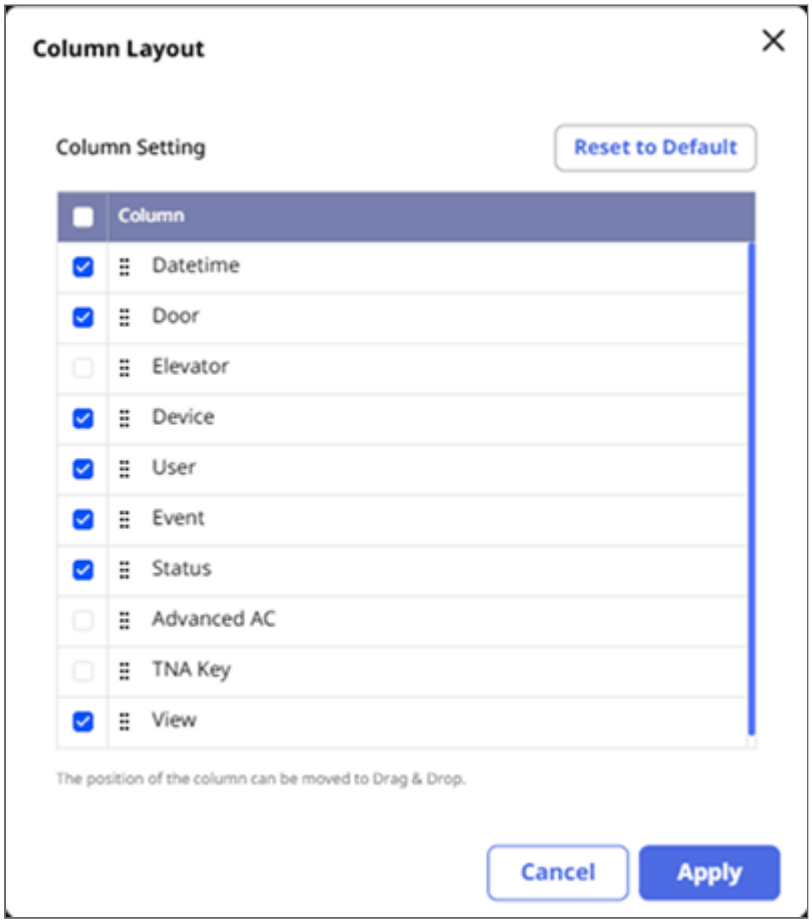
イベント一覧の列設定

イベント一覧で表示する列を追加したり、順序変更や非表示設定ができます。

1. **Event** セクション右上で ••• → **Column Layout** をクリックします。



2. **Column Layout** ウィンドウが表示されたら、表示する列のチェックボックスをクリックして追加または非表示設定ができます。ドラッグ＆ドロップで列の順序を変更することもできます。



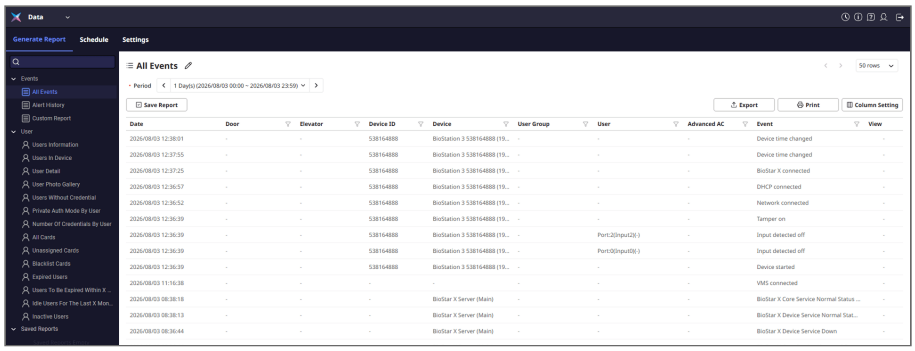
3. 列設定をすべて変更したら、**Apply** ボタンをクリックします。

> **情報**
> 列設定を初期化するには、**Default Column** をクリックします。

データ

Data メニューを使用すると、**BioStar X** に登録されたユーザー情報や希望条件のイベントを照会でき、レポートを一定周期で生成できます。必要に応じて希望のレポートを一定周期で自動生成でき、生成されたレポートは CSV または PDF ファイルとしてエクスポートするか印刷できます。

Launcher ページで **Data** をクリックするか、画面左上のショートカットリストから **Data** を選択してください。



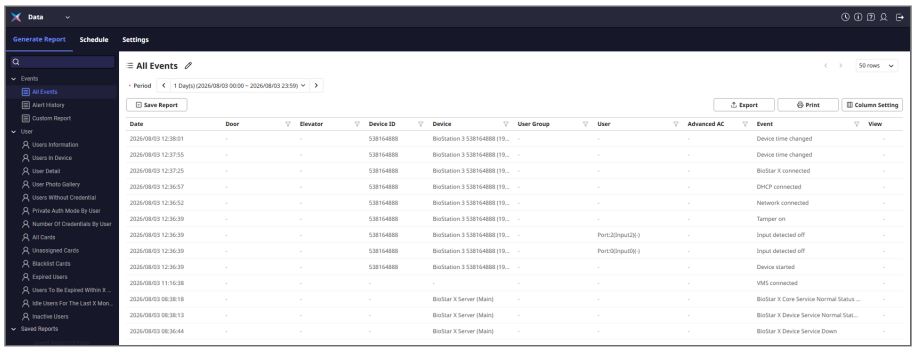
レポートを作成する

BioStar X で発生したすべてのイベントを閲覧することも、警報履歴のみを閲覧することもできます。ユーザーの条件に合わせてフィルタリングし、カスタムレポートを作成することもできます。

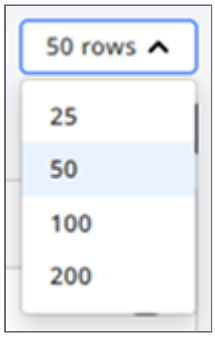
Launcher ページで **Data** をクリックするか、画面左上のショートカットリストから **Data** を選択してください。

すべてのイベントを閲覧

BioStar X で発生したすべてのイベントを閲覧できます。画面左側のサイドバーで **Events** → **All Events** をクリックします。

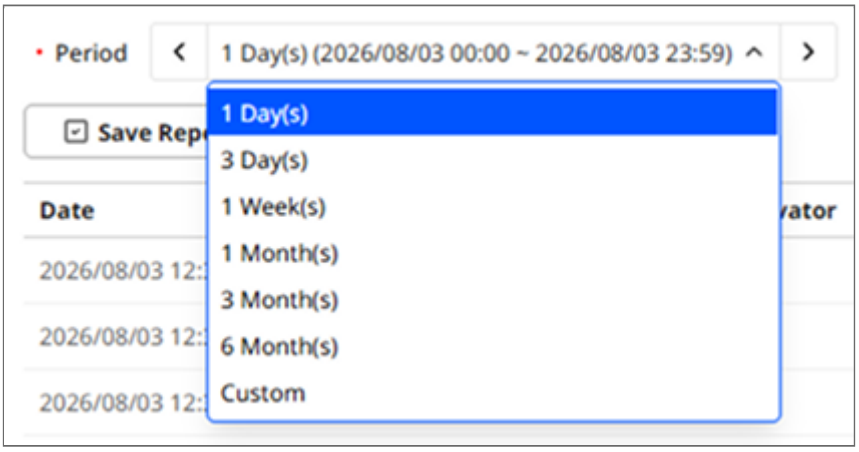


- 表示されたリストで前のページまたは次のページを確認するには、画面右上の ‹ または › ボタンをクリックしてください。
- リストに表示する行数を変更するには、画面右上のドロップダウンメニューをクリックし、希望の値を選択してください。最少で25行、最大で200行まで選択できます。

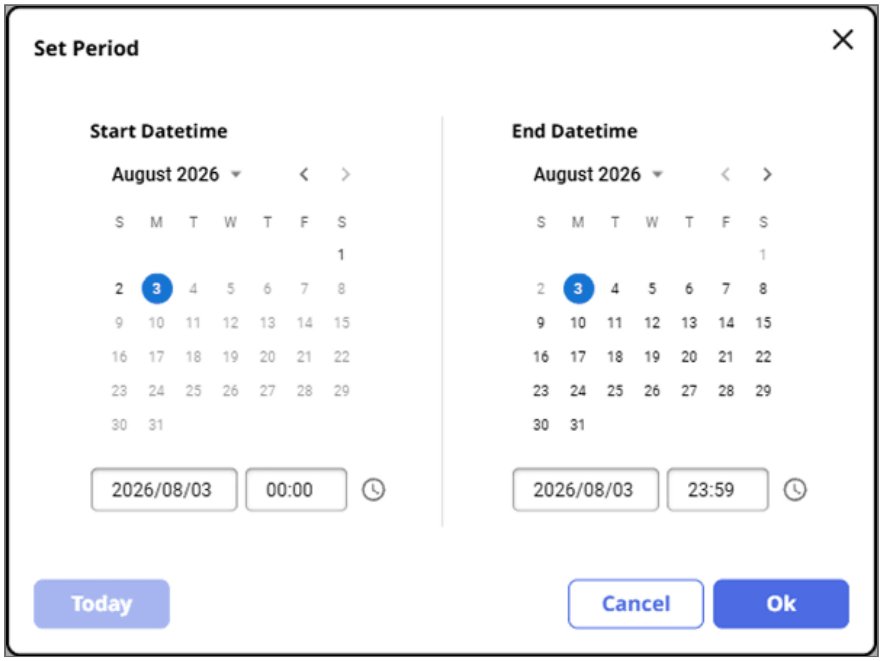


期間の設定

画面左上の **Period** で、希望する期間を設定できます。日付エリアをクリックしてください。



- 本日を基準に、1日から6か月までのあらかじめ定義された期間を選択できます。期間を選択すると、その期間に発生したイベントがリストに自動表示されます。
- **Custom** を選択して、期間を直接設定してください。期間選択ウィンドウが表示されたら、開始日、終了日、時間を設定し、**Ok** ボタンをクリックしてください。設定した期間に発生したイベントがリストに自動表示されます。

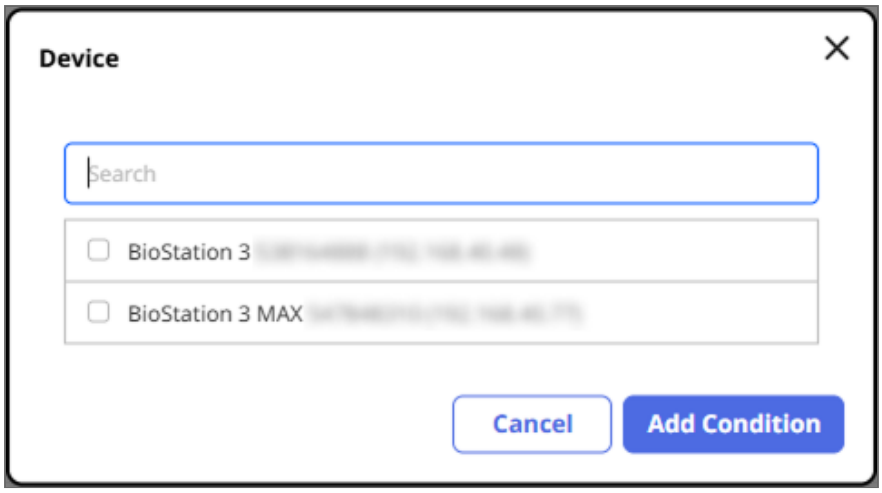


> **情報**
> 本日の日付を選択するには、**Today** ボタンをクリックしてください。

照会条件の設定

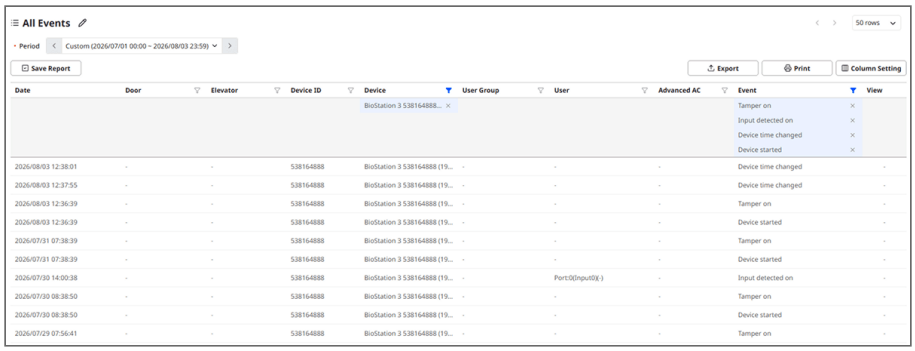
リストのヘッダーで条件を設定し、リストをフィルタリングできます。日付を除くすべての項目に条件を設定できます。

1. イベントリストのヘッダーで、対象列の ボタンをクリックしてください。
2. フィルター条件ウィンドウが表示されたら、必要な項目を選択してください。



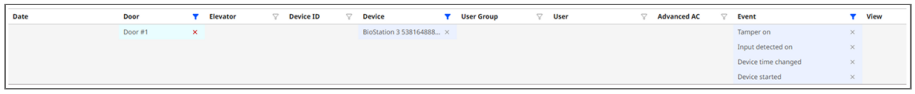
3. 選択が完了したら、**Add Condition** ボタンをクリックしてください。

選択した条件に一致するイベントのみがリストに表示されます。



照会条件の解除

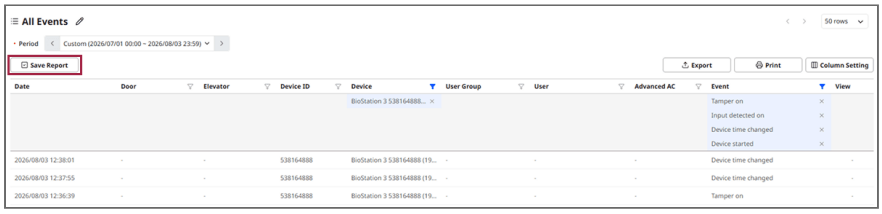
設定した照会条件を解除するには、ヘッダー下に表示されている条件の ✕ ボタンをクリックしてください。条件が解除され、すべてのイベントがリストに再表示されます。



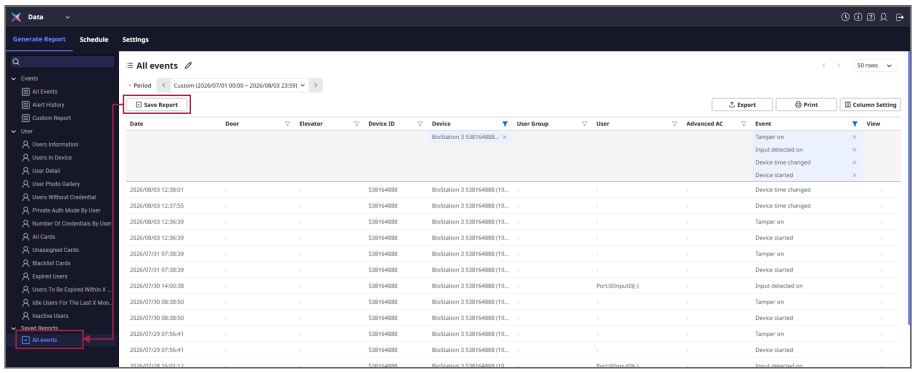
レポート保存

ユーザーが設定した照会期間と条件で、イベントをレポートとして保存できます。

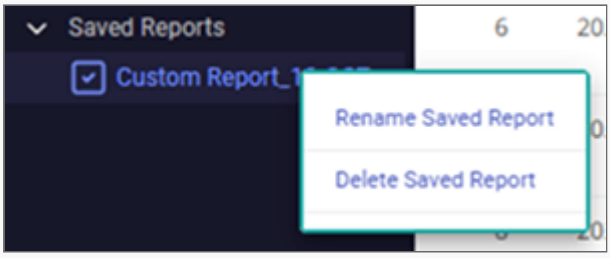
1. イベント一覧の左上にある **Save Report** ボタンをクリックしてください。



2. レポートテンプレートの保存成功メッセージが表示されたら、**Ok** ボタンをクリックしてください。
3. 画面左のサイドバーで **Saved Reports** の下に、保存したレポートが表示されます。



保存したレポートをテンプレートとして保存すると、後から同じ条件でレポートを作成する際に便利です。

> **情報**
>
> - 保存したレポートのタイトル、イベント項目、期間、フィルター条件を修正するには、レポート上部の ✎ ボタンをクリックしてください。
> - レポートタイトルは画面左のサイドバーの **Saved Reports** 配下でも変更できます。タイトルを変更するカスタムレポートを選択し、右クリックします。ポップアップメニューで **Rename Saved Report** を選択します。
>
> 
>
>
> - レポート管理の詳細については[レポート管理]を参照してください。

イベント映像を確認する

イベントリストで、特定のイベントが発生したデバイスにカメラが接続されている場合、そのイベントの **View** 列に ▶ アイコンが表示されます。アイコンをクリックすると、ポップアップウィンドウで該当イベント発生時点の映像を確認できます。



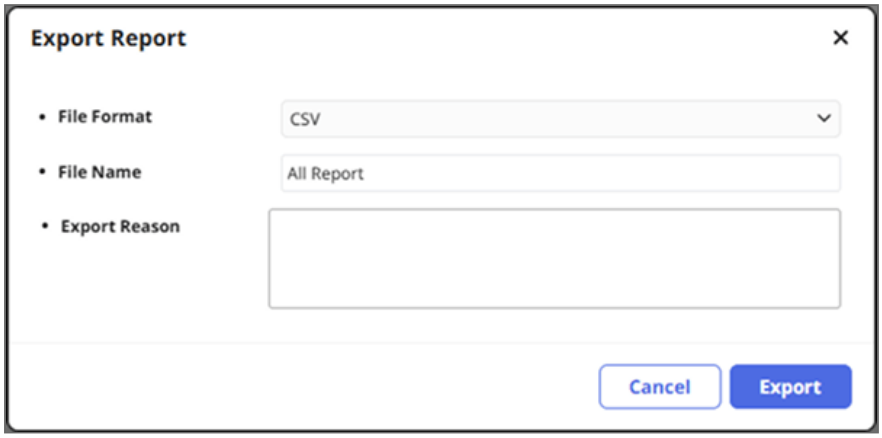
情報

- カメラルール設定で複数のカメラを連携している場合は、1台目のカメラ映像を再生します。カメラのルール設定の詳細については[ビデオルールを設定する]を参照してください。
- 出入口とカメラの連携の詳細については、[ビデオルールを設定する]を参照してください。
- この機能は **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。

CSV へのエクスポート

表示されたイベントリストを CSV ファイルとしてエクスポートできます。

1. 画面右上の **Export** ボタンをクリックします。
2. 「**Export Report**」ウィンドウが表示されたら、**File Format** で **CSV** を選択します。

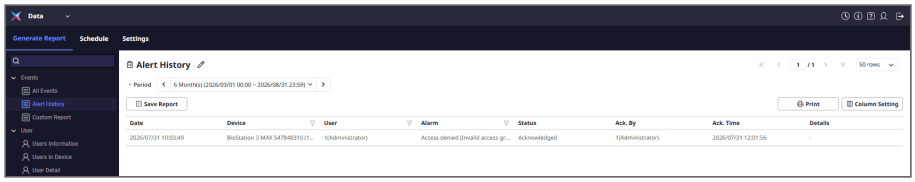


3. **File Name** で保存するファイル名を変更できます。
4. **Export Reason**(任意)を入力して **Export** ボタンをクリックします。
5. ローカルの任意のパスにCSVファイルを保存します。

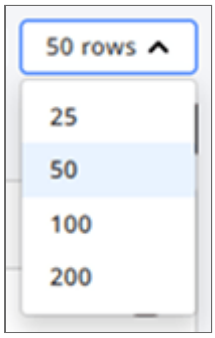
> **情報**
>
> **Export Reason**は必須入力項目ではありません。エクスポート理由は **Settings** → **Audit Trail** → **AC Audit Log** で確認できます。

警報履歴の閲覧

警報（アラーム）履歴のみを閲覧できます。画面左のサイドバーで **Events** → **Alert History** をクリックしてください。



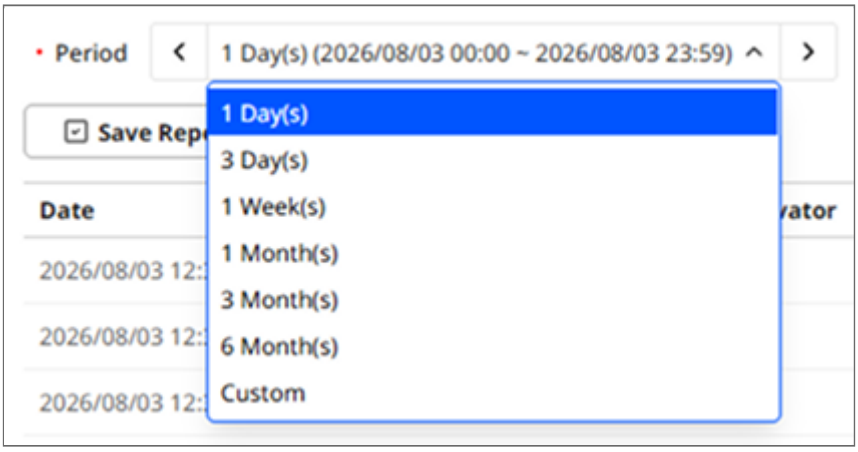
- 表示されたリストで前のページまたは次のページを確認するには、画面右上の ‹ または › ボタンをクリックしてください。
- 表示されたリストで最初のページまたは最後のページへ移動するには、画面右上の |‹ または ›| ボタンをクリックしてください。
- リストに表示する行数を変更するには、画面右上のドロップダウンメニューをクリックし、希望の値を選択してください。最少で25行、最大で200行まで選択できます。



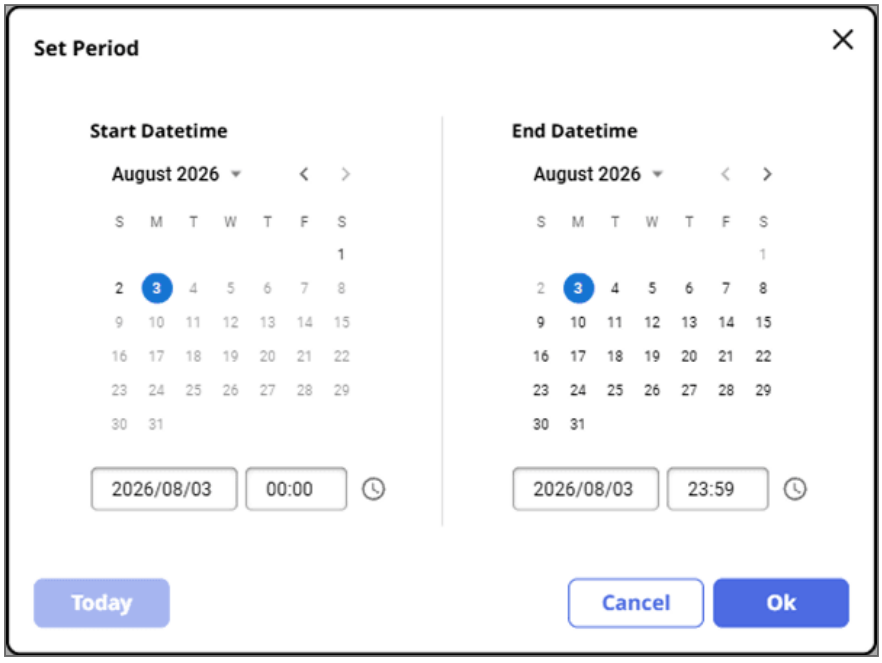
> **情報**
>
> イベントモニタリングにおける警報（アラーム）イベントの確認方法の詳細はイベントをモニタリングするを参照してください。

期間の設定

画面左上の **Period** で、希望する期間を設定できます。日付エリアをクリックしてください。



- 本日を基準に、1日から6か月までのあらかじめ定義された期間を選択できます。期間を選択すると、その期間に発生したイベントがリストに自動表示されます。
- **Custom** を選択して、期間を直接設定してください。期間選択ウィンドウが表示されたら、開始日、終了日、時間を設定し、**Ok** ボタンをクリックしてください。設定した期間に発生したイベントがリストに自動表示されます。

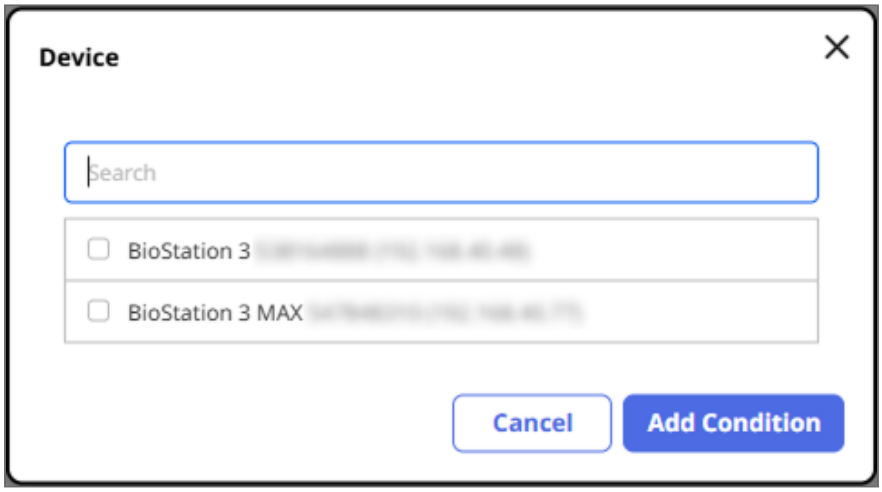


> **情報**
> 本日の日付を選択するには、**Today** ボタンをクリックしてください。

照会条件の設定

リストのヘッダーで条件を設定し、リストをフィルタリングできます。日付を除くすべての項目に条件を設定できます。

1. イベントリストのヘッダーで、対象列の ボタンをクリックしてください。
2. フィルター条件ウィンドウが表示されたら、必要な項目を選択してください。



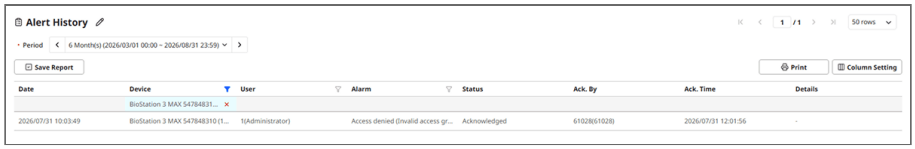
3. 選択が完了したら、**Add Condition** ボタンをクリックしてください。

選択した条件に一致するイベントのみがリストに表示されます。



照会条件の解除

設定した照会条件を解除するには、ヘッダー下に表示されている条件の ✕ ボタンをクリックしてください。条件が解除され、すべてのイベントがリストに再表示されます。



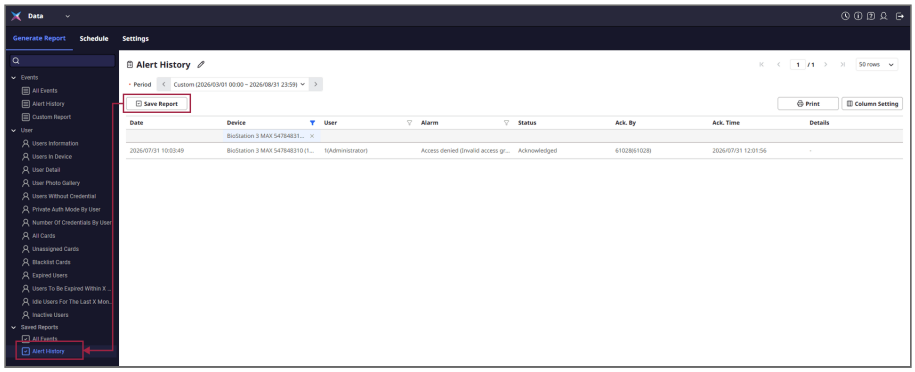
レポート保存

ユーザーが設定した照会期間と条件で、警報履歴をレポートとして保存できます。

1. 警報履歴一覧の左上にある **Save Report** ボタンをクリックしてください。



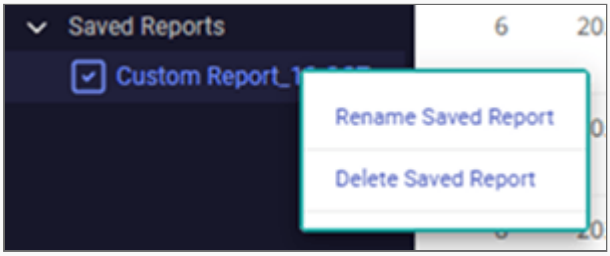
2. レポートテンプレートの保存成功メッセージが表示されたら、**Ok** ボタンをクリックしてください。
3. 画面左のサイドバーで **Saved Reports** の下に、保存したレポートが表示されます。



保存したレポートをテンプレートとして保存すると、後から同じ条件でレポートを作成する際に便利です。

情報

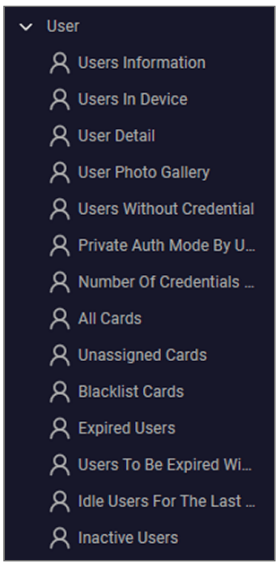
- 保存したレポートのタイトル、イベント項目、期間、フィルター条件を修正するには、レポート上部の ボタンをクリックしてください。
- レポートタイトルは画面左のサイドバーの **Saved Reports** 配下でも変更できます。タイトルを変更するカスタムレポートを選択し、右クリックします。ポップアップメニューで **Rename Saved Report** を選択します。



- レポート管理の詳細についてはレポート管理を参照してください。

ユーザーリポートの参照

ユーザー関連テンプレートを選択してレポートを作成できます。画面左のサイドバーの **User** 配下で、目的のテンプレートをクリックしてください。



- **Users Information**：ユーザーの詳細情報をリスト形式で閲覧できます。
- **Users In Device**：デバイスに登録されたユーザー情報を閲覧できます。
- **User Detail**：ユーザーの詳細情報をカード形式で閲覧できます。
- **User Photo Gallery**：ユーザープロフィール写真をギャラリー形式で閲覧できます。
- **Users Without Credential**：クレデンシャルを設定していないユーザーを閲覧できます。
- **Private Auth Mode By User**：ユーザーの個別認証モード設定情報を閲覧できます。
- **Number Of Credentials By User**：ユーザーに設定されているクレデンシャルの数を閲覧できます。
- **All Cards**：登録済みカードを基準にユーザーを検索できます。
- **Unassigned Cards**：ユーザーに割り当てられていないカードを検索できます。

- **Blacklist Cards**：使用停止されたカードを検索できます。
- **Expired Users**：有効期限が切れたユーザーを検索できます。
- **Users To Be Expired Within X Days**：N日以内に有効期限が切れるユーザーを検索できます。日数はレポート作成前に直接入力できます。
- **Idle users for the last N months**：直近Nか月間に入退室履歴がないユーザーを検索できます。月数はレポート作成前に直接入力できます。
- **Inactive Users**：無効化されたユーザーを検索できます。

> **情報**
>
> - 作成したレポートは **Saved Reports** 配下に保存できます。レポート左上の **Save Report** ボタンをクリックします。
> - レポート管理の詳細についてはレポート管理を参照してください。

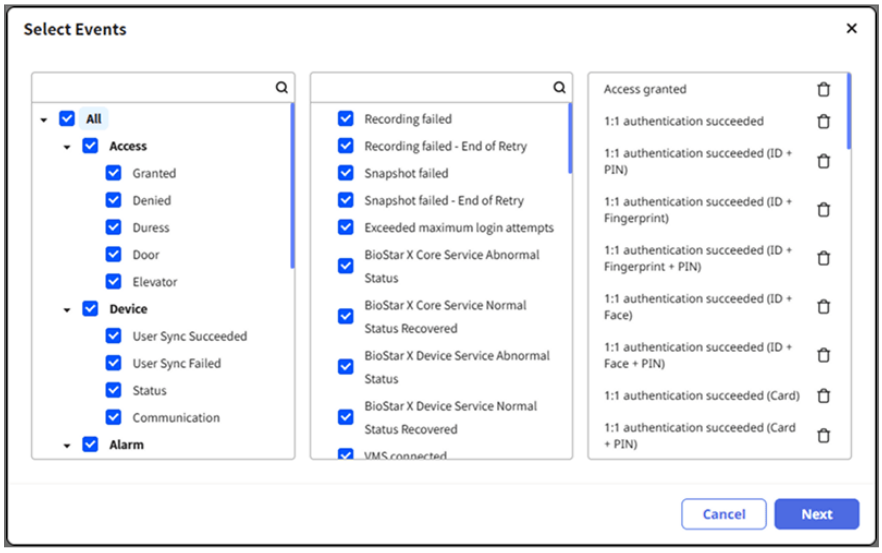
カスタムレポートの作成

必要な条件でフィルタリングしてカスタムレポートを作成できます。作成したレポートをテンプレートとして保存すると、後から同じ条件でレポートを作成する際に便利です。

1. 画面左のサイドバーで **Events** → **Custom Report** をクリックします。
2. **Select Events** ウィンドウで必要なイベントを選択します。

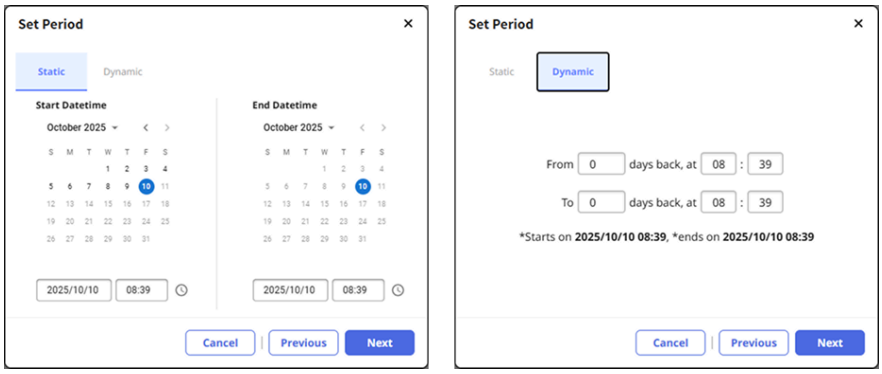


3. イベントの選択を終えたら、**Next** ボタンをクリックします。



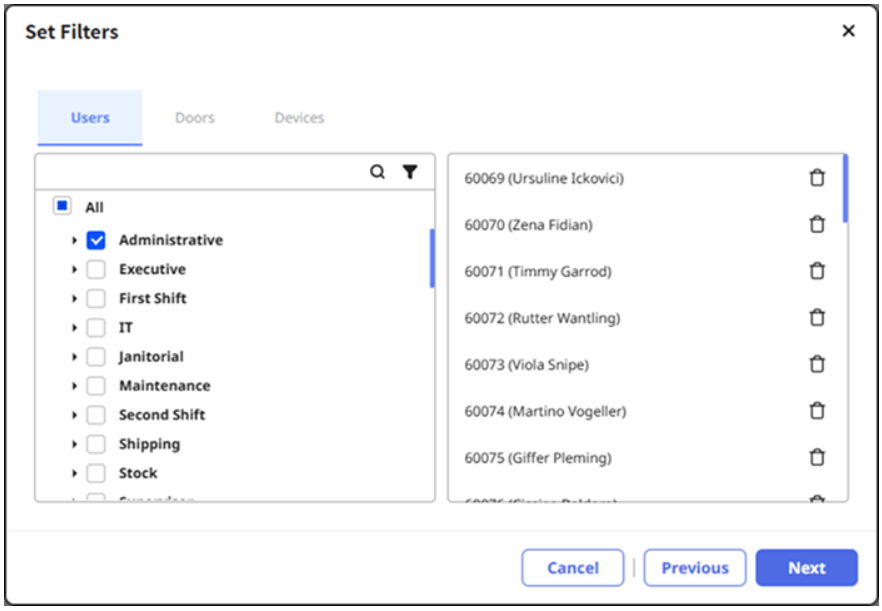
- 検索(🔍)入力フィールドで必要な項目を検索できます。
- 最右列のリストで 🗑 ボタンをクリックすると、選択した項目を除外できます。

4. 照会期間を設定し、**Next** ボタンをクリックします。



- **Static**：指定した日付と時刻を設定して照会期間を設定できます。
- **Dynamic**：本日を基準に開始日、終了日、時刻を設定できます。一定期間のレポートを繰り返し作成する際に便利です。

5. ユーザー、ドア、デバイスを基準にグループ別または個別で条件を設定できます。

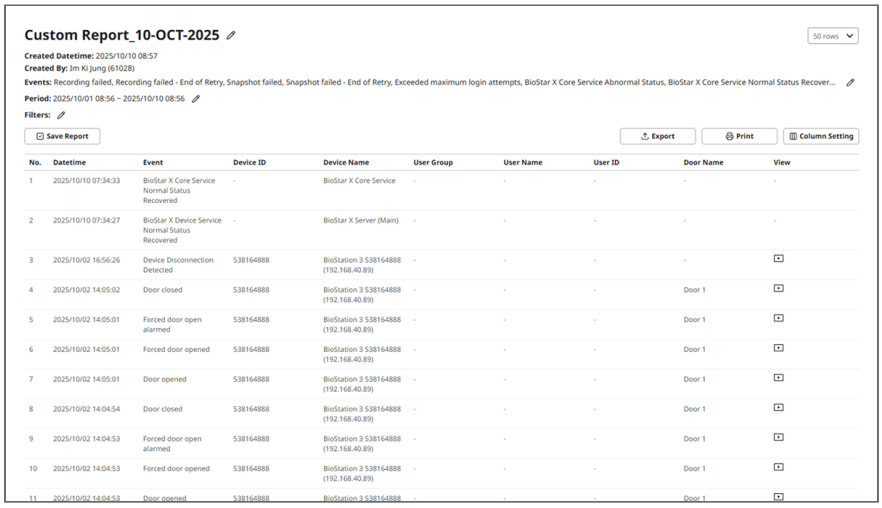


- 右側のリストで 🗑 ボタンをクリックすると、選択した項目を除外できます。

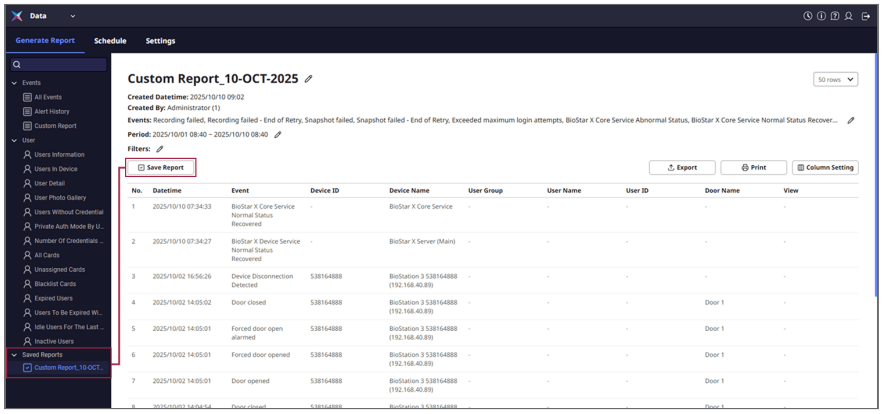
6. 必要な条件を選択し、**Next** ボタンをクリックします。
7. 列設定ウィンドウでレポートに表示するカラムを選択します。



8. カラムの選択を終えたら、**Generate** ボタンをクリックします。
9. 設定した条件でレポートを作成します。



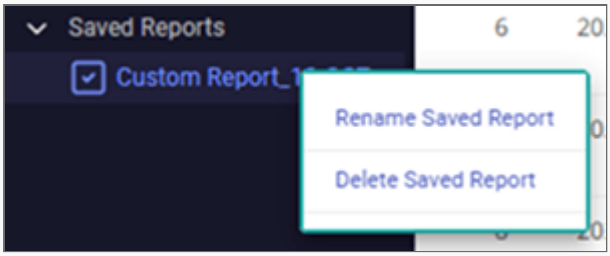
10. 作成したレポートをテンプレートとして保存するには、一覧の左上にある **Save Report** ボタンをクリックしてください。保存したレポートは画面左のサイドバーの **Saved Reports** 配下で確認できます。



保存したレポートをテンプレートとして保存すると、後から同じ条件でレポートを作成する際に便利です。

情報

- 保存したレポートのタイトル、イベント項目、期間、フィルター条件を修正するには、レポート上部の ✎ ボタンをクリックしてください。
- レポートタイトルは画面左のサイドバーの **Saved Reports** 配下でも変更できます。タイトルを変更するカスタムレポートを選択し、右クリックします。ポップアップメニューで **Rename Saved Report** を選択します。

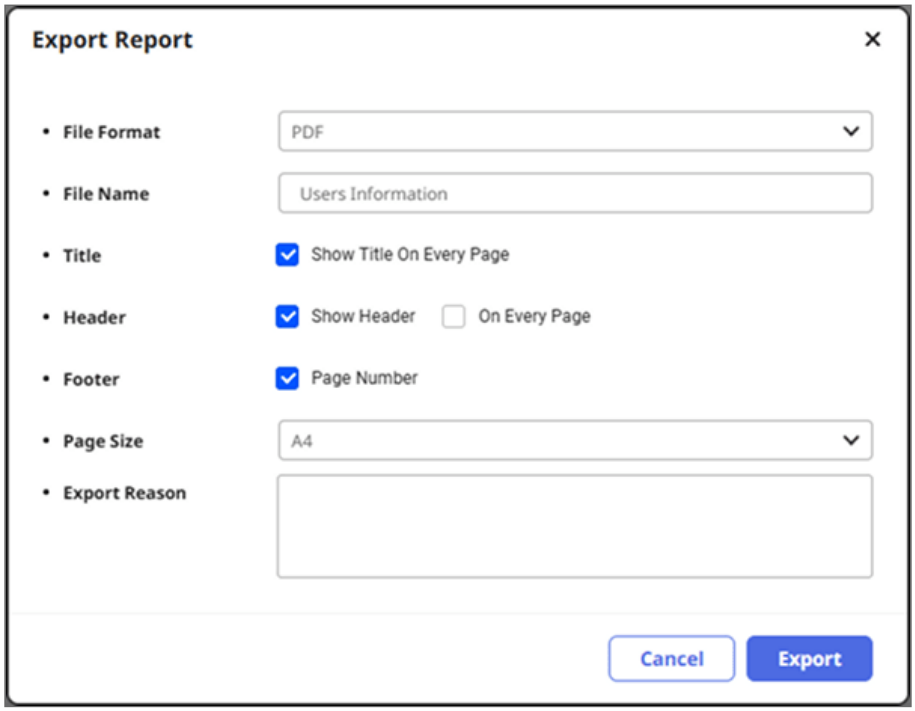


- レポート管理の詳細については[レポート管理]を参照してください。

レポート管理

レポートファイルの保存

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、**Export** ボタンをクリックします。 **Export Report** ウィンドウが表示されたら、各項目を設定して **Export** をクリックします。

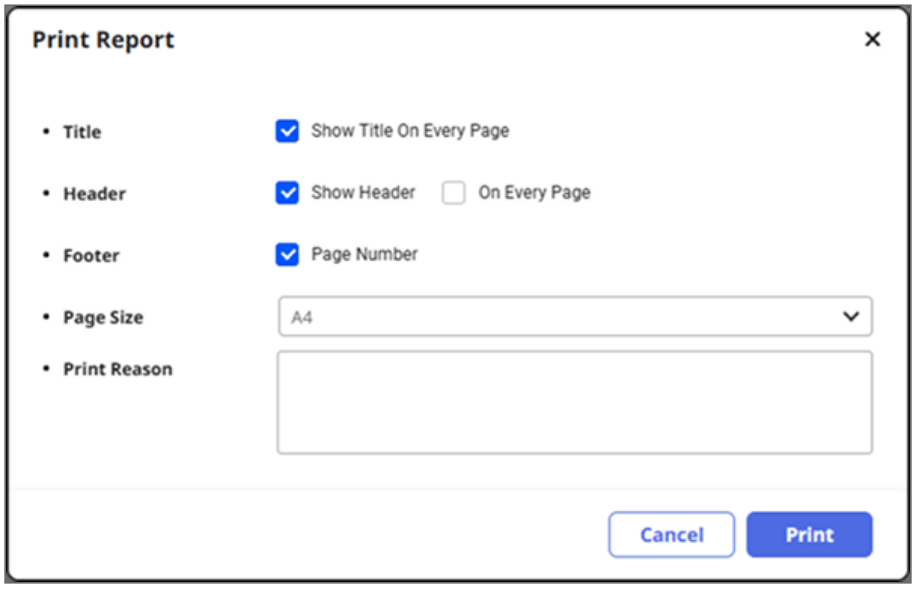


情報

Export Reasonは必須入力項目ではありません。エクスポート理由は **Settings** → **Audit Trail** → **AC Audit Log** で確認できます。

レポートの印刷

PCに接続されたプリンターでレポートを印刷するには、**Print** ボタンをクリックします。 **Print Report** ウィンドウが表示されたら、各項目を設定して **Print** をクリックします。

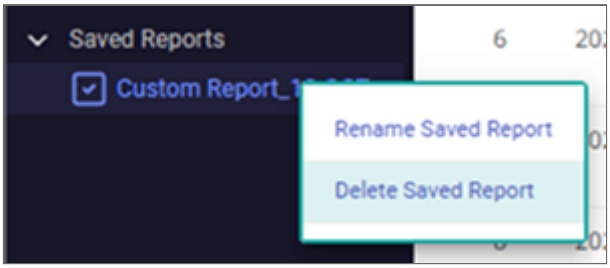


Webブラウザーの新しいタブで印刷プレビュー画面が表示されます。画面右上の印刷ボタンをクリックすると印刷を開始できます。

> **情報**
> **Print Reason** は必須入力項目ではありません。印刷理由は **Settings** → **Audit Trail** → **AC Audit Log** で確認できます。

レポートの削除

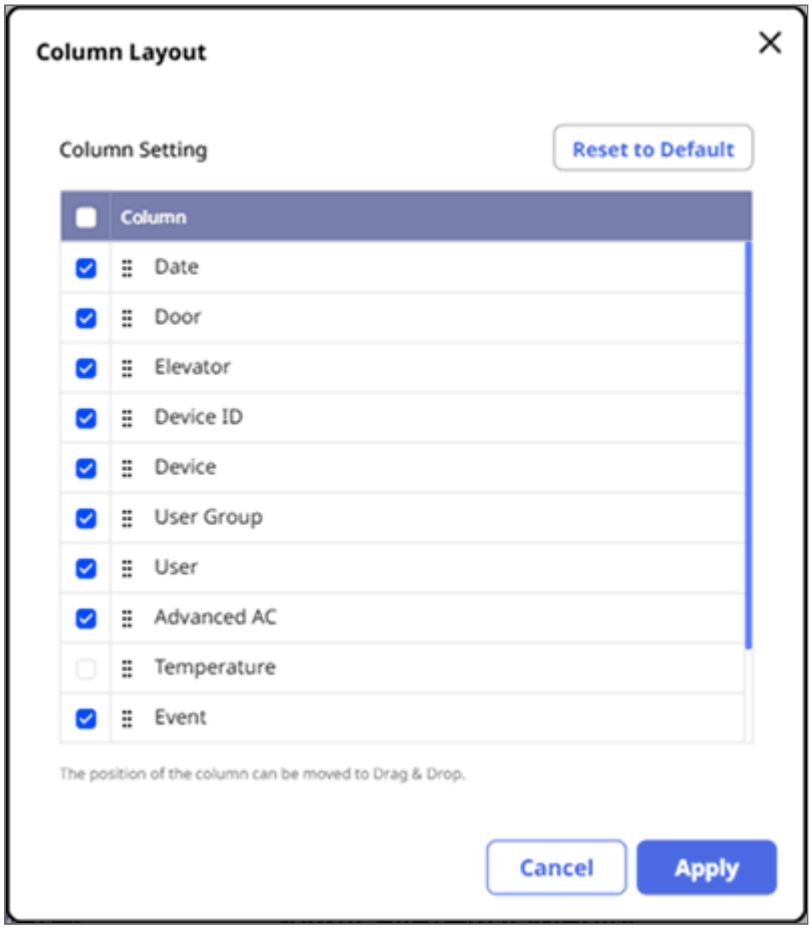
保存したレポートを削除するには、画面左のサイドバーの **Saved Reports** 配下で削除するレポートを選択し、右クリックします。ポップアップメニューで **Delete Saved Report** を選択します。



列設定

レポートに表示される列（カラム）設定を変更できます。列設定で表示する列を選択したり、列の順序を変更したりできます。

1. レポート右上の **Set Columns** ボタンをクリックします。
2. **Column Layout** ウィンドウが表示されたら、必要な列を選択または選択解除します。



3. 列の順序を変更するには、目的の列をクリックしたままドラッグして位置を変更します。
4. 設定を保存するには、**Apply** ボタンをクリックします。

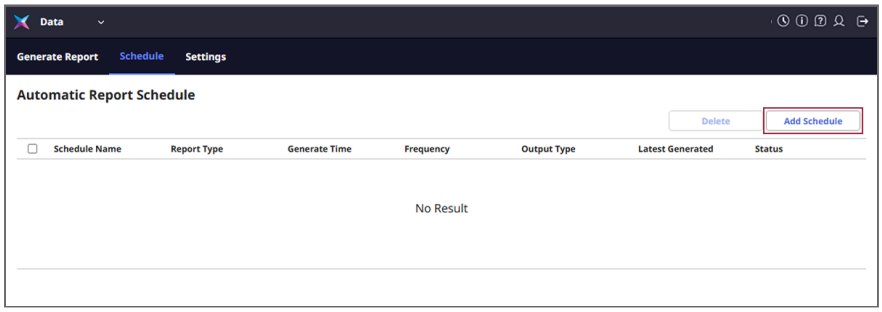
> **情報**
>
> - 列レイアウト設定を初期化するには、**Default Column** ボタンをクリックします。
> - 作成したレポートによって、選択または選択解除できる列が異なる場合があります。

自動生成スケジュールを設定する

変動期間で作成した**Custom Report**を自動生成するようスケジュールを設定します。

自動生成スケジュールを追加する

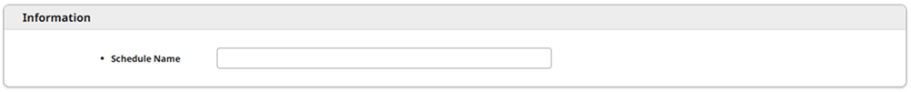
1. **Launcher** ページで **Data** をクリックするか、画面左上のショートカットリストから **Data** を選択してください。
2. **Schedule**タブをクリックします。
3. 画面右上の**Add Schedule**をクリックします。



4. **Add Automatic Report Schedule**画面が表示されたら、各項目を設定します。

情報を設定する

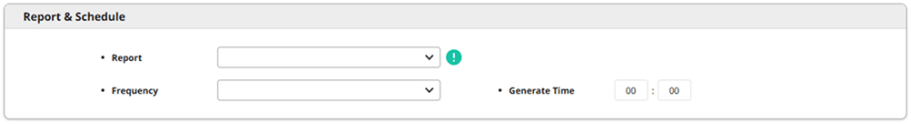
自動生成スケジュールの基本情報を設定します。



- **Schedule Name**：スケジュール名を入力します。

レポートとスケジュールを設定する

レポートごとの自動生成スケジュールを設定します。

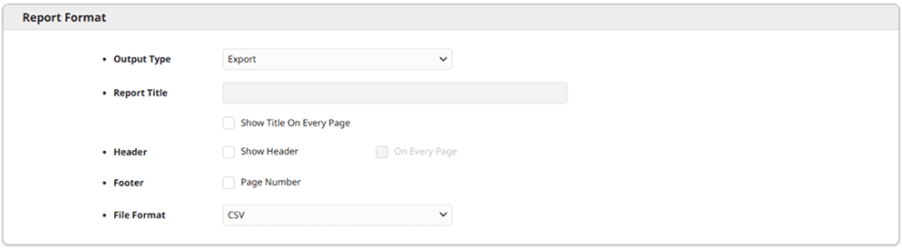


- **Report**：自動生成するカスタムレポートを選択します。変動期間に設定されたカスタムレポートのみ表示されます。
- **Frequency**：レポートを自動生成する周期を設定します。
- **Generate Time**：レポートを自動生成する時間を設定します。

> **情報**
> カスタムレポート作成の詳細については レポートを作成する を参照してください。

レポート形式を設定する

レポートごとの形式を設定します。



- **Output Type**：レポートの自動生成方式を設定します。
- **Report Title**：レポート名をすべてのページのタイトルとして表示するには、**Show Title On Every Page**を選択します。

- **Header**：**Show Header**を選択すると、レポート生成時にヘッダーを表示できます。ヘッダーをすべてのページに表示するには、**On Every Page**を選択します。

> **情報**
> レポートごとに生成されるヘッダーは異なる場合があります。

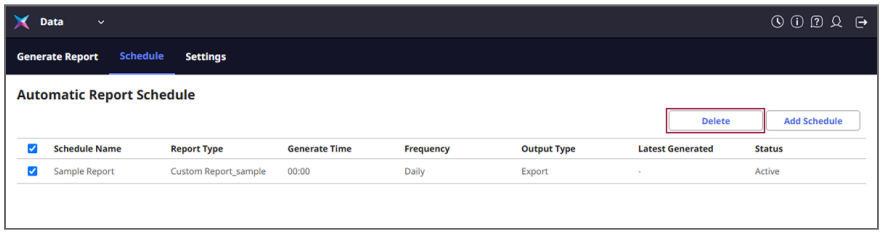
- **Footer**：ページ番号を表示するかどうかを設定します。
- **File Format**：レポートを出力するファイル形式を設定します。

3. 設定を保存するには、**Apply**をクリックします。

> **情報**
> すべての設定が完了したら、レポートを保存するパスを設定します。詳細については レポート保存パスを設定する を参照してください。

自動生成スケジュールを削除する

1. **Launcher** ページで **Data** をクリックするか、画面左上のショートカットリストから **Data** を選択してください。
2. **Schedule**タブをクリックします。
3. 自動スケジュール一覧で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。

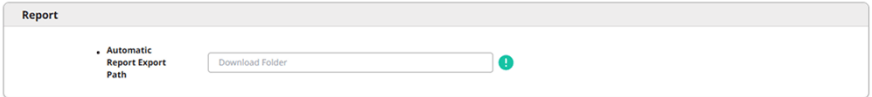


4. 画面右上の**Delete**をクリックします。

レポート保存パスを設定する

Scheduleを設定した場合は、レポート保存パスを設定します。

1. **Settings**をクリックします。
2. レポート保存パスを入力します。



- **Automatic Report Export Path**：指定したパスにレポートが保存されます。パスを入力しない場合、ユーザー PC の *Documents\BioStarX* フォルダーに自動保存されます。

3. 設定を保存するには、**Apply**をクリックします。

ダッシュボード

ダッシュボードは、ユーザーごとに必要な情報を選択してウィジェットを追加し、ウィジェットを自由に設定・配置して好みに合わせて構成できます。

> **情報**
>
> - 各ユーザーは個別にDashboardを構成できます。
> - Dashboardで確認できる情報は、Account Levelによって異なる場合があります。

ウィジェットを追加

BioStar X ダッシュボードは、ユーザーが希望する情報を自由に配置できるカスタムモニタリング画面です。さまざまなウィジェットを追加して、入退室管理システムの主要情報を業務環境に合わせて構成できます。

追加可能なウィジェットの種類は次のとおりです。

- **チャート**：入退室イベントデータを棒／線／円チャートで可視化
- **カウンター**：日次／週次イベント発生数を数値で表示
- **リアルタイムイベント**：BioStar X で発生するすべてのイベントをリアルタイムでモニタリング
- **リアルタイム出入モニタリング**：特定デバイスで認証に成功したユーザー情報をリアルタイム表示
- **システム使用状況**：ユーザー、デバイス、ドアなどの登録状況を数値で表示
- **ドア制御**：選択したドアの状態確認とリモート制御
- **テキスト**：お知らせやウィジェットタイトルなどのカスタムテキストを配置

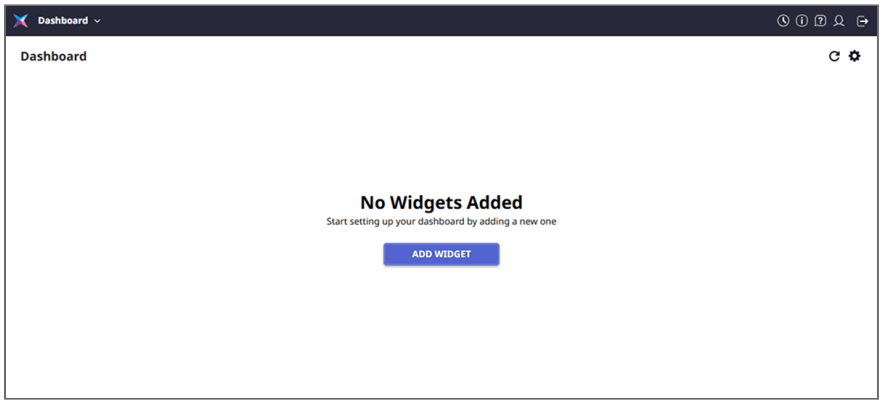
ダッシュボードに配置したウィジェットによって、次のようなメリットが得られます。

- **カスタム構成**：業務に必要な情報だけを選択し、一画面に配置
- **リアルタイムモニタリング**：入退室イベントとシステム状態を即時確認
- **直感的なビジュアル化**：チャートとカウンターによるデータの視覚的表現
- **効率的な管理**：モニタリングと制御機能を統合し、業務効率を向上

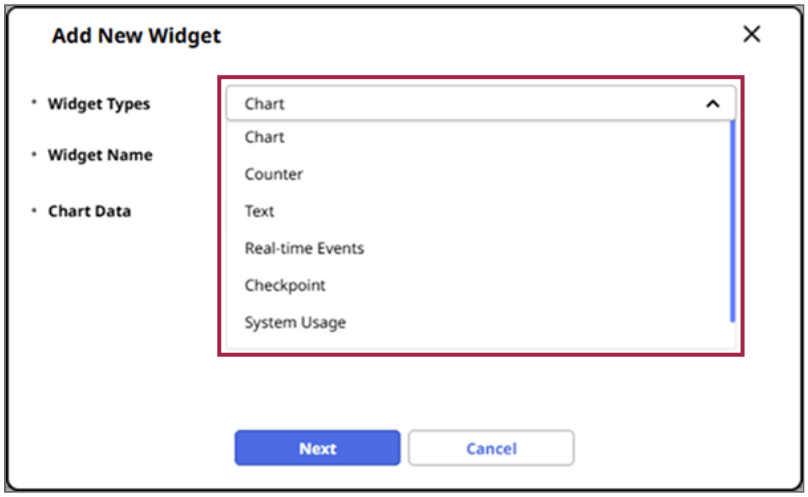
ウィジェットの追加

Dashboard にウィジェットを追加して、必要な情報を確認できます。

1. Launcher ページで Dashboard をクリックします。
2. Add Widget ボタンをクリックします。



3. **Add New Widget** ウィンドウが表示されたら、**Widget Type** から希望の項目を選択し、必須項目を入力または設定します。

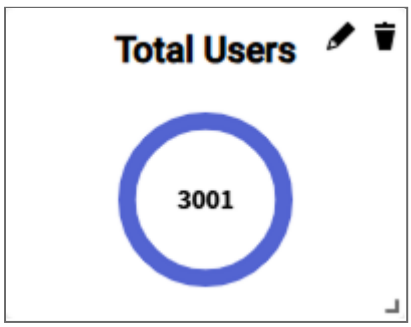


4. ウィジェットの設定を完了し、**Apply** ボタンをクリックします。
5. ウィジェット表示エリアにウィジェットが作成されたら、サイズを調整するか、希望の位置に配置します。
6. すべての設定が完了したら、画面右上の **Apply** ボタンをクリックします。

> **情報**
>
> 既にウィジェットが追加されている場合は、画面右上の ⚙ アイコンをクリックします。 **Dashboard Settings** モードに入ったら、**Add Widget** ボタンをクリックします。

ウィジェットの種類

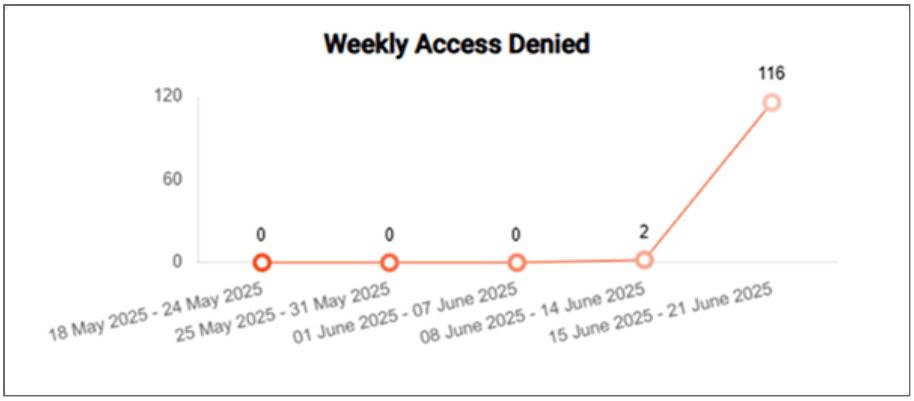
- ウィジェットごとにデフォルトサイズが異なり、デフォルト状態で最も見やすいよう最適化されています。
- すべてのウィジェットは右下をドラッグしてサイズを調整できます。



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。

チャート

任意のチャートデータを選択して発生したイベント数をチャートで表示できます。



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。

- **Chart Data**：日次または週次イベント一覧から希望のチャートデータを選択します。
  - **Daily Access Granted**、**Daily Access Denied**、**Daily Communication Issue**、**Daily APB Violation**、**Weekly Access Granted**、**Weekly Access Denied**、**Weekly Communication Issue**、**Weekly APB Violation**
- **Chart Type**：**Vertical Bar**、**Horizontal Bar**、**Line**、**Pie** の中から希望のタイプを選択します。
- **Color Schemes**：5 つのカラースキームから希望の色を選択します。

> **情報**
> **Color Schemes** を選択するときに表示されるチャートの値は実際の値ではなく、プレビュー用の仮の値です。

カウンター

任意のカウンターデータを選択して発生したイベント数を数値で表示できます。

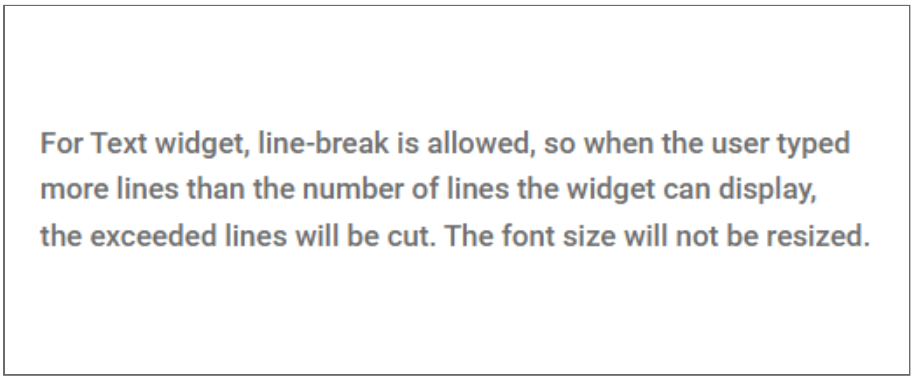


上記の画像は例示です。実際の画面とは異なる場合があります。

- **Counter Data**：日次または週次イベント一覧から希望のカウンターデータを選択します。
  - **Daily Access Granted**、**Daily Access Denied**、**Daily Communication Issue**、**Daily APB Violation**、**Weekly Access Granted**、**Weekly Access Denied**、**Weekly Communication Issue**、**Weekly APB Violation**

テキスト

Dashboard のウィジェット領域に、ユーザーが希望するテキストを入力して配置できます。作成後、必要な位置に配置してウィジェットのタイトルやお知らせなどに利用できます。

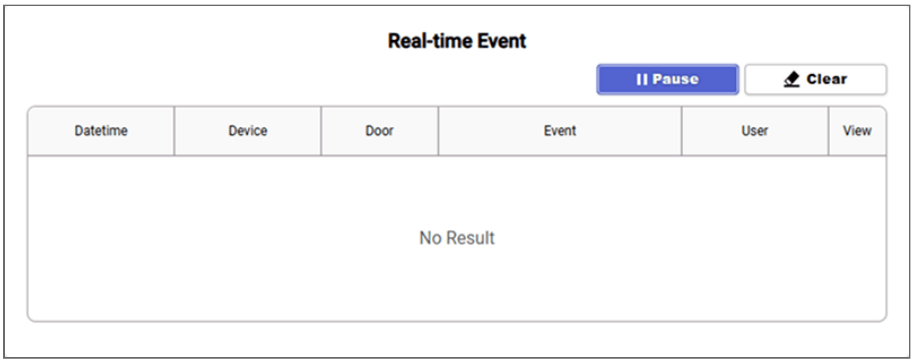


上記の画像は例示です。実際の画面とは異なる場合があります。

> **情報**
> **Text** ウィジェットを作成するときに **Remove Background** オプションを選択すると、背景に透明度が適用されます。

リアルタイムイベント

BioStar Xで発生するイベントをリアルタイムで表示します。特定のイベント、ユーザー、ドア、デバイスをフィルタリングしてイベントを確認できます。



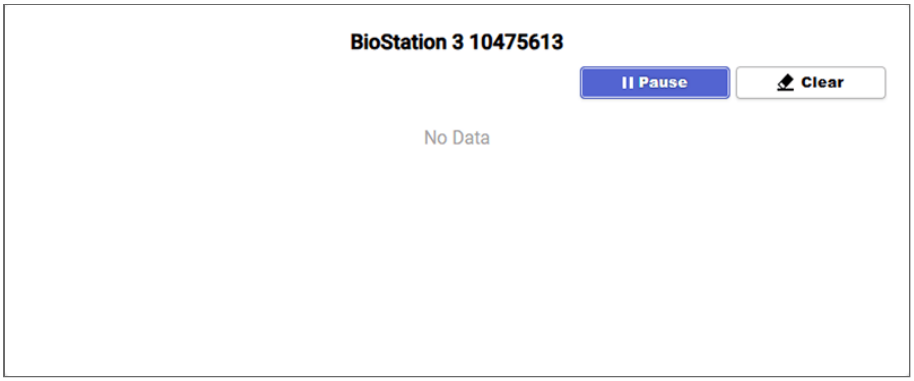
上記の画像は例示です。実際の画面とは異なる場合があります。

- **Pause**：リアルタイムイベントを停止できます。
- **Play**：停止したリアルタイムイベントを再開できます。
- **Clear**：認証履歴をすべて削除できます。

> **情報**
> 別のページに移動してから再度**Dashboard**に戻ると、リストがクリアされてイベントが再び記録されます。

リアルタイムアクセス監視

1 台のデバイスを選択すると、そのデバイスで認証に成功したユーザーのプロフィール写真と情報（**User**、**Date**、**Device**）をリアルタイムで表示します。



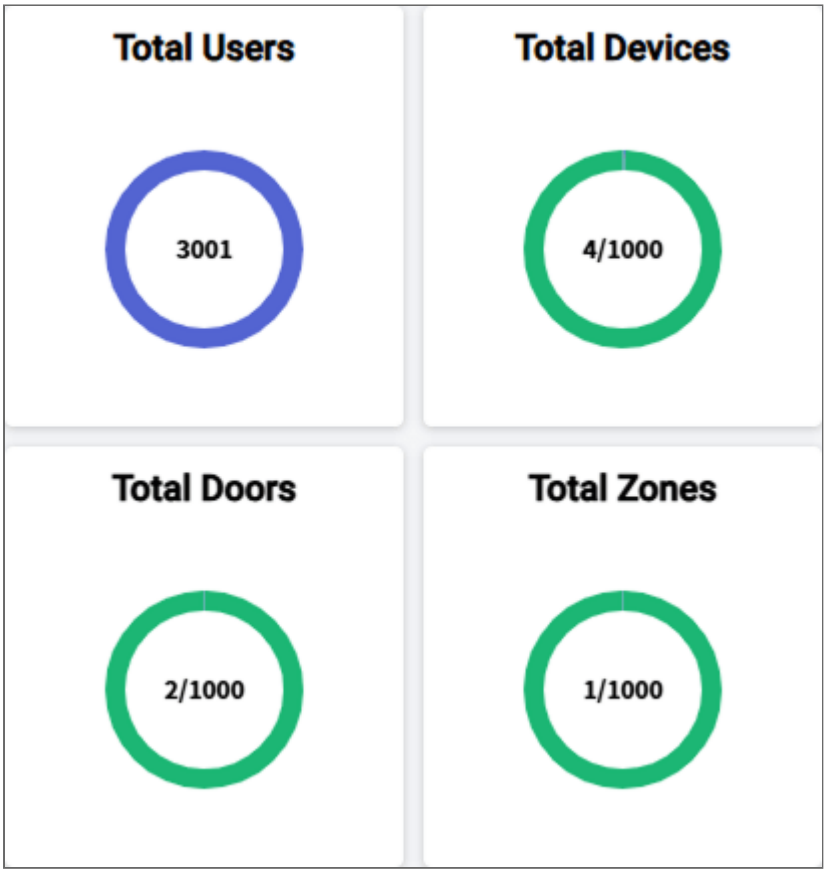
上記の画像は例示です。実際の画面とは異なる場合があります。

- **Pause**：リアルタイム出入モニタリングを停止できます。
- **Play**：停止したリアルタイム出入モニタリングを再開できます。
- **Clear**：認証履歴をすべて削除できます。

> **情報**
> **Checkpoint** には最大 5 名まで記録されます。

システム使用状況

BioStar X のさまざまな利用状況を数値で表示します。



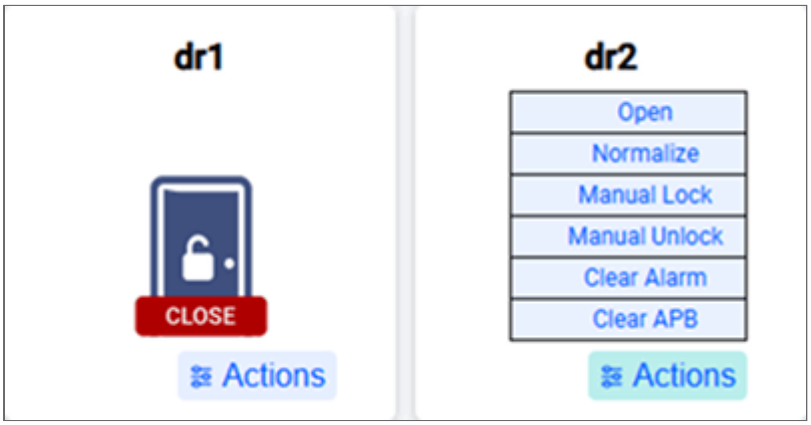
上記の画像は例示です。実際の画面とは異なる場合があります。

表示可能な **System Usage** は次のとおりです。

- **Total Users**、**Total Cards**、**Total Fingerprints**、**Total Faces**、**Total Faces**、**Total QR/Barcode**、**Total Mobile Access**、**Total Devices**、**Total Doors**、**Total Advanced ACs**、**Total Access Groups**、**Total User Groups**、**Total Device Groups**、**IR Face**

ドア制御

1 つのドアを選択して、そのドアの状態を確認および制御できます。



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。

Actions ボタンで制御できる項目は次のとおりです。

- **Open**、**Normalize**、**Manual Lock**、**Manual Unlock**、**Clear Alarm**、**Clear APB**

> **情報**
> **Door Control** ウィジェットの名前はドア名で自動設定され、変更できません。

ウィジェットデータの更新間隔の設定

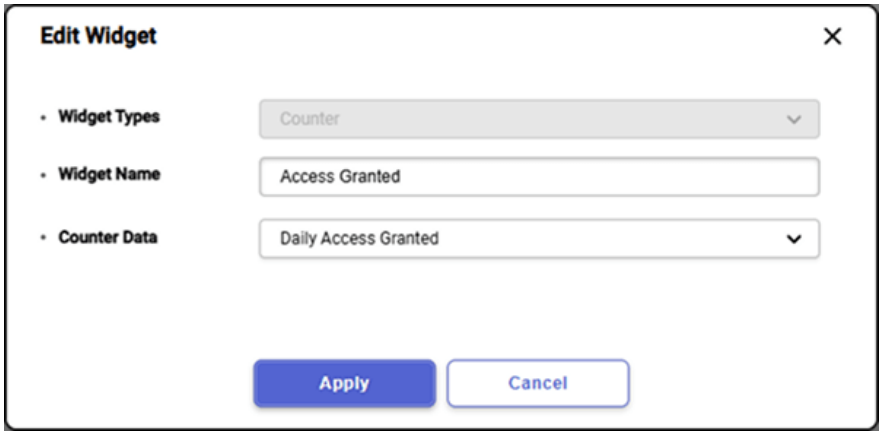
ダッシュボードに追加したウィジェットのデータ更新間隔を設定できます。

1. **Launcher** ページで **Dashboard** をクリックします。
2. 画面右上の ⚙ アイコンをクリックします。
3. **Dashboard Settings** モードに入ったら、画面下部の一般設定で**Auto Refresh Interval**を設定します。

ウィジェットを編集する

ダッシュボードに追加したウィジェットの編集方法を説明します。

1. **Launcher** ページで **Dashboard** をクリックします。
2. 画面右上の ⚙ アイコンをクリックします。
3. **Dashboard Settings**モードに入ったら、編集する**ウィジェット**の右上にある ✎ アイコンをクリックします。
4. **Edit Widget**ウィンドウが表示されたら、必要な項目を編集します。



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. 編集が完了したら、**Apply**ボタンをクリックします。
6. **Dashboard Settings**画面の右上にある**Apply**ボタンをクリックします。

ダッシュボード画面で変更内容が反映されていることを確認します。

> **情報**
> - **Edit Widget**では**Widget Types**を変更できません。
> - 定義済み項目を使用する**Text**、**System Usage**、**Door Control**では**Widget Name**を変更できません。

ウィジェットを削除する

ダッシュボードに追加されたウィジェットを削除する方法を説明します。

1. **Launcher** ページで **Dashboard** をクリックします。
2. 画面右上の ⚙ アイコンをクリックします。
3. **Dashboard Settings** モードに入ったら、削除したい **ウィジェット** の右上にある 🗑 ボタンをクリックします。
4. 削除確認ポップアップを確認し、**Yes** ボタンをクリックします。



5. **Dashboard Settings** 画面右上の **Apply** をクリックします。

ダッシュボード画面で変更内容が反映されていることを確認します。

設定

BioStar X の Settings ページで設定できるさまざまな機能を案内します。装置を追加し、権限、言語、日時、入退室カード管理など、ユーザー環境に合わせてカスタマイズするためのさまざまなオプションを確認できます。

Launcher ページで Settings をクリックするか、画面左上のショートカットリストから Settings を選択します。

> **情報**
> ユーザーの権限によって設定できる機能が異なる場合があります。特定の機能は管理者権限を持つユーザーのみが使用できます。ユーザー権限ごとにアクセス可能なメニューの詳細については ユーザー権限を設定する をご参照ください。

デバイス管理

デバイスの追加・削除・変更の管理方法を案内します。デバイスに登録されているユーザー情報を BioStar X サーバーに取り込む、またはリモートでファームウェアをアップグレードできます。

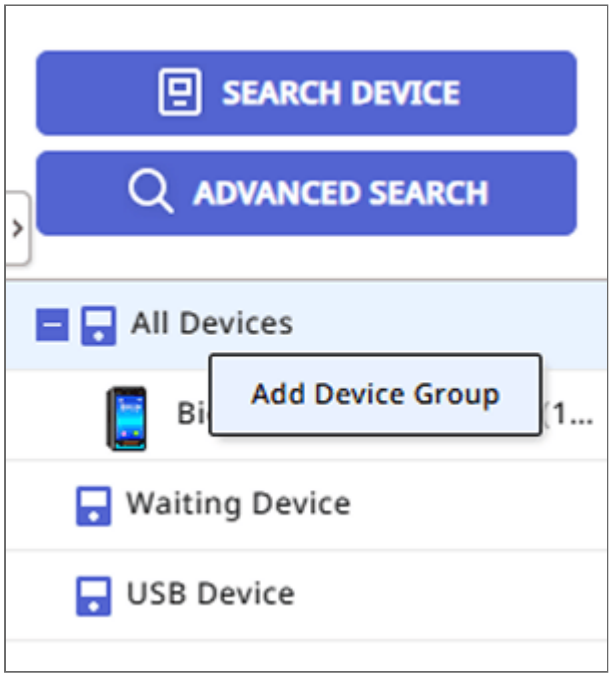
デバイスグループを管理する

複数のデバイスを効率的に管理できるデバイスグループ機能について説明します。デバイスグループを使用すると複数のデバイスを1つのグループにまとめて管理できるため、大規模システムでデバイス設定を一括適用したり監視したりする際に便利です。

> **ヒント**
> デバイスグループ名は、デバイスの設置場所や用途で指定すると管理がしやすくなります。例えば、「1階ドア」「2階オフィス」「会議室」などでグループを設定できます。

デバイスグループの作成

1. Launcherページで Settingsをクリックします。
2. 画面左のサイドバーで Device → Device をクリック。
3. デバイスリストで All Devices を右クリックします。

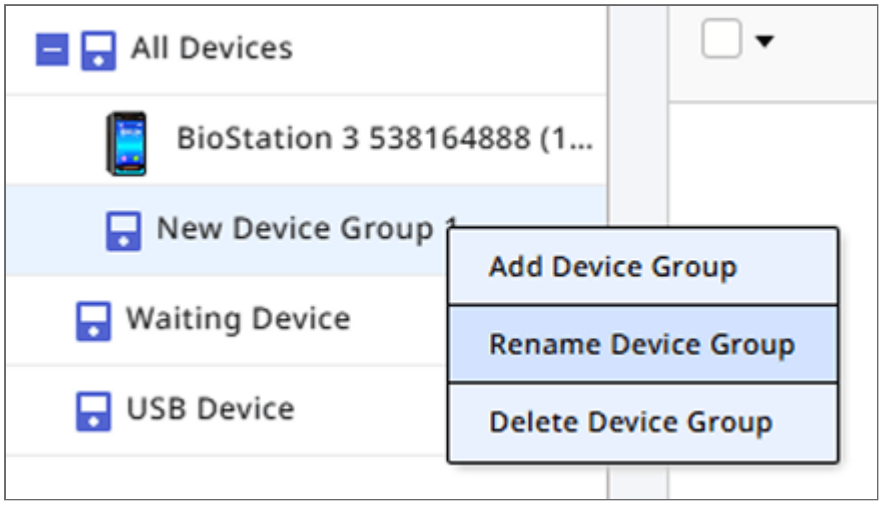


4. ポップアップメニューで **Add Device Group** をクリックします。
5. 希望するグループ名を入力します。

> **情報**
>
> - デバイスグループは最大8階層までサブグループを作成できます。
> - デバイスグループ名は最大48文字まで入力できます。
> - デバイスリストでデバイスグループを選択すると、そのグループに属するデバイスのみがリストに表示されます。

デバイスグループ名の変更

1. **Launcher**ページで**Settings**をクリックします。
2. 画面左のサイドバーで **Device** → **Device** をクリック。
3. デバイスリストの **All Devices** 配下で、名前を変更するデバイスグループを選択して右クリックします。



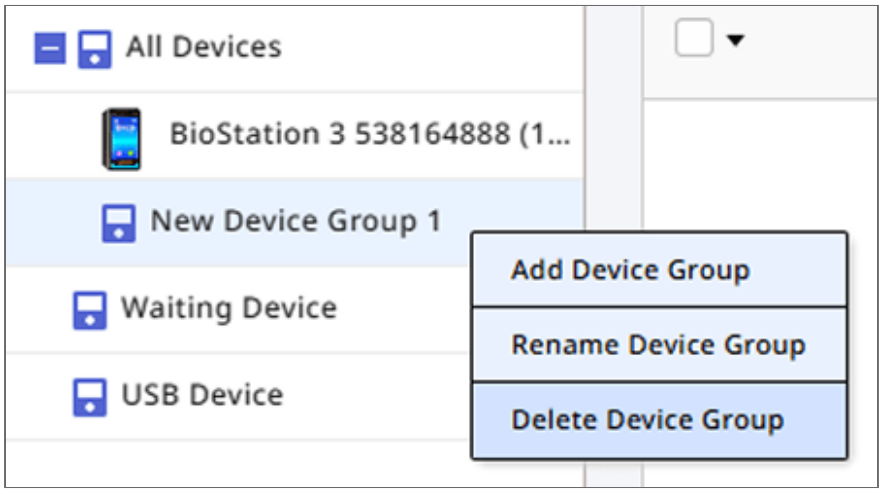
4. ポップアップメニューで **Rename Device Group** をクリックします。

5. 変更するグループ名を入力します。

> **情報**
> デバイスグループ名は最大48文字まで入力できます。

デバイスグループの削除

1. **Launcher**ページで**Settings**をクリックします。
2. 画面左のサイドバーで **Device** → **Device** をクリック。
3. デバイスリストの **All Devices** 配下で、削除するデバイスグループを選択して右クリックします。



4. ポップアップメニューで **Delete Device Group** をクリックします。

> **注意**
> デバイスグループを削除すると、そのグループに属するすべてのデバイスも削除されます。

デバイスを登録する

BioStar X にデバイスを登録する方法を説明します。デバイスを登録すると、**BioStar X** でそのデバイスの状態を監視して管理できます。デバイスを検索する前に、デバイスが正しく接続されていることを確認します。複数のデバイスをまとめて追加する場合は、各デバイスの設置場所、ID、IP アドレスなどを事前に把握しておくと便利です。

情報

- デバイスを新規登録するとき、デバイスのキー値をサーバーのデータ暗号化キー値に変更します。キーを変換すると、デバイス内のすべてのユーザーデータが削除されます。
- デバイスに保存されているすべての設定情報とユーザー情報を削除して再送信するには、**Delete Data & Sync Device** をクリックします。 **Delete Data & Sync Device** オプションは、デバイスリストでデバイスを選択し、••• ボタンをクリックすると表示されます。
- グループ内のすべてのデバイスを登録するには、**Waiting Device** グループ名を右クリックし、**Add All Waiting Devices** をクリックします。各デバイスを個別に登録する場合は、デバイス名を右クリックし、**Add Waiting Device** をクリックします。
- **BioStar X** とデバイスでユーザー ID タイプが異なる場合は、**BioStar X** のユーザー ID 設定に合わせてデバイス設定を変更します。
- **BioStar X** のユーザー ID タイプを英数字に設定すると、一部のデバイスが使用できなかったり制限が発生したりすることがあります。詳細については、サーバーの詳細を設定するをご参照ください。
- デバイスを登録して詳細を設定するには、デバイス設定をご参照ください。
- Ethernet (TCP/IP) で接続できるデバイスの最大数は 1,000 台です。
- デバイスを登録するには、**デバイス マネージャー**以上の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 ポリシーをご参照ください。

開始前に

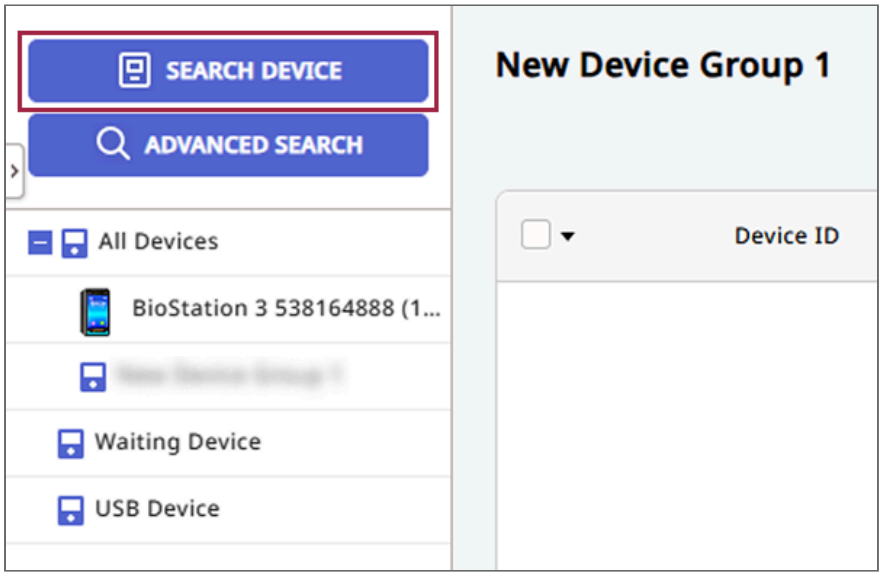
デバイスを登録する前に、次の事項を確認します。

- 入退室制御用の入室レベル、入室グループ、フロアレベルを設定します。詳しくは 入退室制御設定 をご参照ください。
- デバイスを効率的に管理するグループを作成します。詳細については、デバイスグループを管理するをご参照ください。

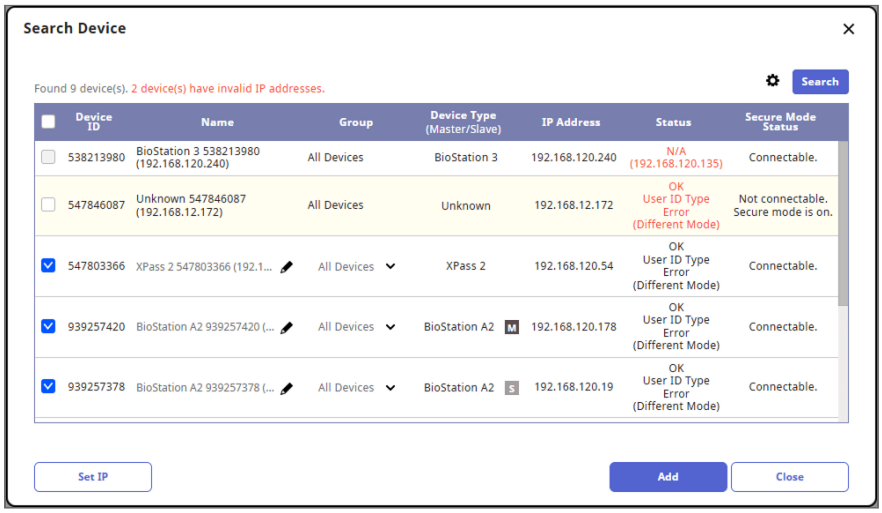
簡易登録

BioStar X と同じネットワーク上にあるデバイスを自動で検索して登録できます。

1. **Launcher**ページで**Settings**をクリックします。
2. 画面左のサイドバーで **Device** → **Device** をクリック。
3. デバイス一覧で **Search Device** をクリックします。

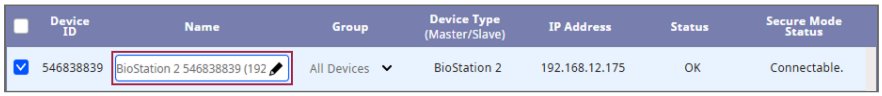


4. **Search Device** ウィンドウが表示されると、登録可能なすべてのデバイス一覧が表示されます。目的のデバイスが一覧にない場合は、右上の **Search** をクリックします。

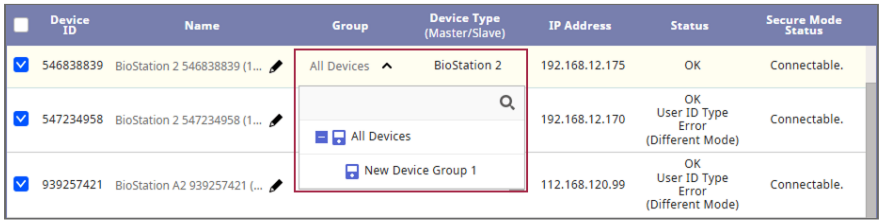


5. デバイス一覧で登録するデバイスを選択し、登録しないデバイスは選択を解除します。

6. 登録するデバイス名を変更するには、**Name** 列の ✎ をクリックして編集します。

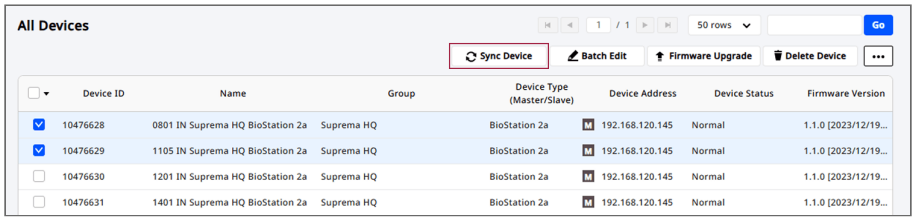


7. 登録するデバイスのグループを設定するには、**Group** 列で選択します。



8. 選択したデバイスの設定が完了したら、**Add** をクリックします。

追加したデバイスがデバイス一覧に表示されます。追加したデバイスを選択し、**Sync Device** をクリックします。

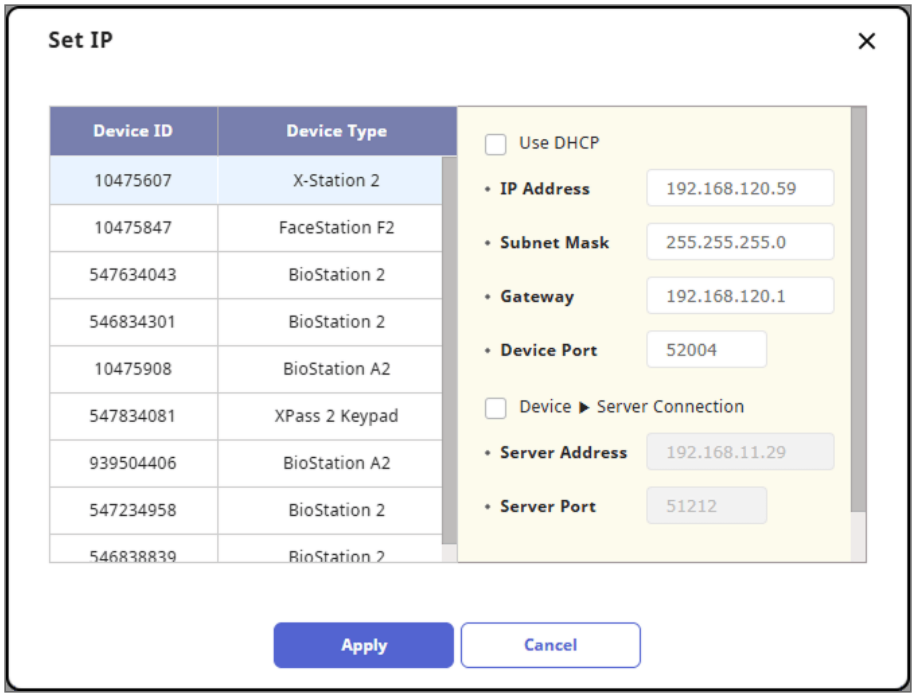


情報

IP アドレスを使用できない、または変更が必要なデバイスは、**Set IP** をクリックして変更できます。詳細については、IP アドレス設定をご参照ください。

IP アドレス設定

新規登録するデバイスの IP アドレスを変更できます。 **Search Device** ウィンドウ左下の **Set IP** をクリックします。 **Set IP** ウィンドウが表示されたら、デバイス一覧から IP アドレスを変更するデバイスを選択します。



- **Use DHCP**：デバイスが DHCP で IP アドレスを自動取得するように設定します。このオプションを選択すると、デバイスがネットワークに接続するたびに IP アドレスが変わる可能性があります。

  IP アドレス、サブネットマスク、ゲートウェイなどを手動入力する場合は、このオプションの選択を解除します。

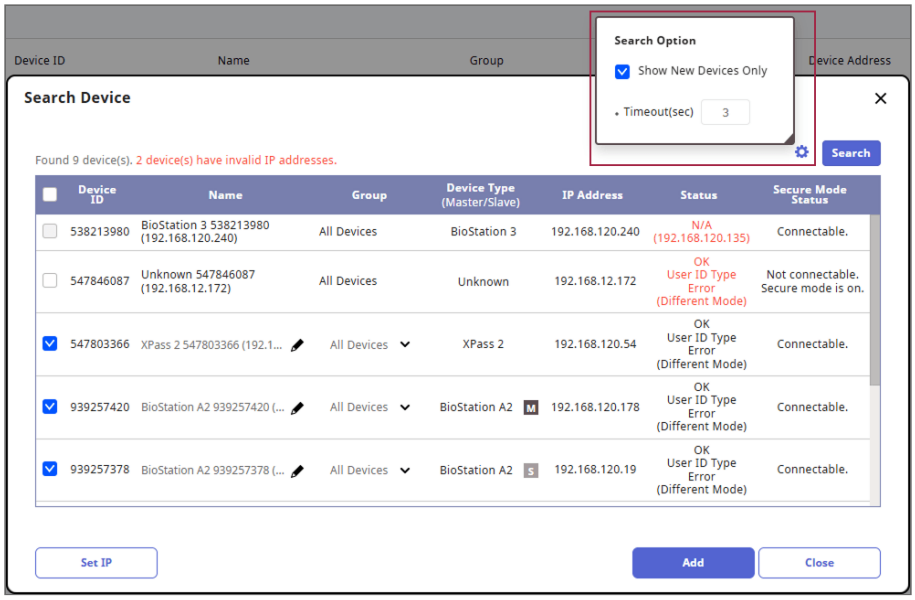
- **Device ▶ Server Connection**：デバイスから **BioStar X** サーバーへ接続するように設定する場合は、このオプションを選択します。 **BioStar X** をインストールしたサーバーの IP アドレスとポート番号を入力する必要があります。

情報

IP 設定を完了して変更を保存するには、**Apply** をクリックします。変更を取り消す場合は、**Cancel** をクリックします。

デバイス検索オプション

Search Device ウィンドウ右上の ⚙ をクリックすると、デバイス検索オプションを設定できます。

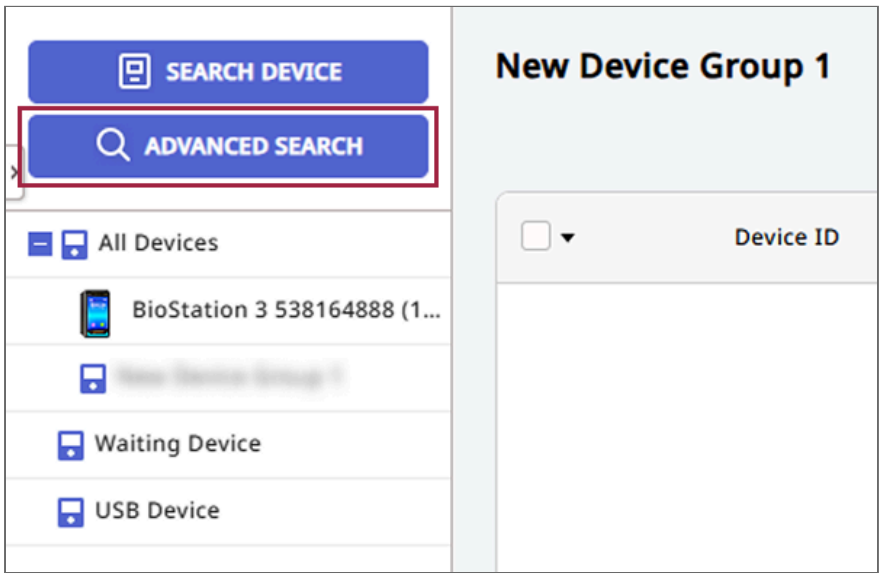


- **Show New Devices Only**：新しく検出されたデバイスのみを一覧に表示する場合は、このオプションを選択します。
- **Timeout(sec)**：一定時間応答しないデバイスを一覧から除外する場合は、所要時間を設定します。秒単位で設定でき、デフォルトは 3 秒です。

高度な検索

特定のデバイスの IP アドレスとポート番号を指定して登録できます。

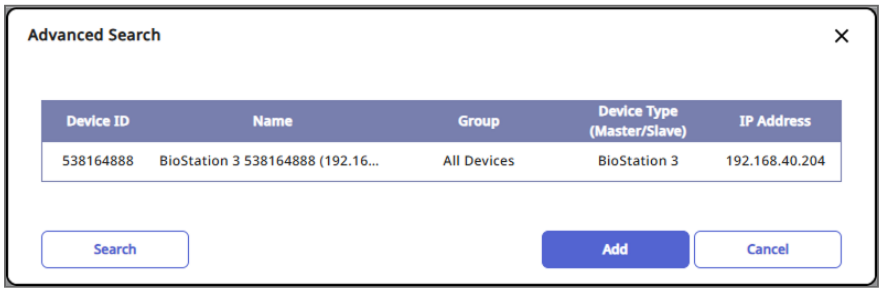
1. **Launcher**ページで**Settings**をクリックします。
2. 画面左のサイドバーで **Device** → **Device** をクリック。
3. デバイス一覧で **ADVANCED SEARCH** をクリックします。



4. **ADVANCED SEARCH** ウィンドウが表示されたら、登録するデバイスの IP アドレスとポート番号を入力します。



5. **Search** をクリックすると、入力した条件に一致するデバイスが一覧に表示されます。



6. デバイスを登録するには、**Add** をクリックします。

追加したデバイスがデバイス一覧に表示されます。追加したデバイスを選択し、**Sync Device** をクリックします。

待機中のデバイスの登録

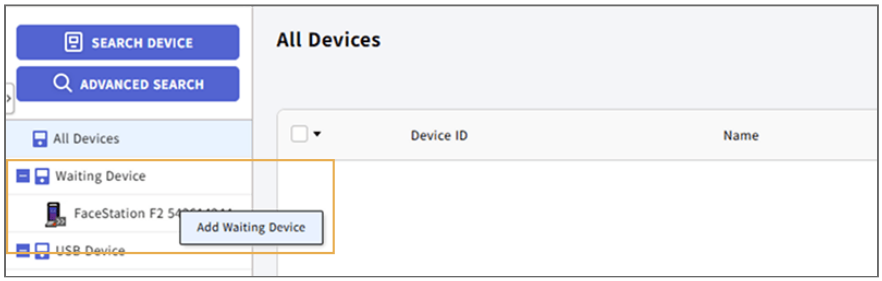
Device → Server オプションで設定したデバイスは、サーバーのIPアドレスとポート番号を使用して **BioStar X** サーバーへの接続を試みます。この方法で接続したデバイスは、アクティブデバイス一覧に自動で追加されません。デバイスは **Waiting Device** グループに表示され、権限のある管理者が手動で登録する必要があります。

1. デバイスの **Device → Server** オプションで **BioStar X** のIPアドレスとポート番号を設定します。
2. **Launcher**ページで**Settings**をクリックします。
3. 画面左のサイドバーで **Device → Device** をクリック。
4. **Waiting Device** グループに表示されたデバイスを確認します。



5. 個別のデバイスを登録するには、**Waiting Device** グループのデバイス名を右クリックします。

   Waiting Device グループのすべてのデバイスを登録するには、**Waiting Device** グループを右クリックします。



6. ポップアップメニューで **Add Waiting Device**(個別デバイス) または **Add All Waiting Devices**(すべてのデバイス) をクリックします。

Waiting Device グループのデバイスを登録すると、デバイスは **All Devices** 一覧に移動します。

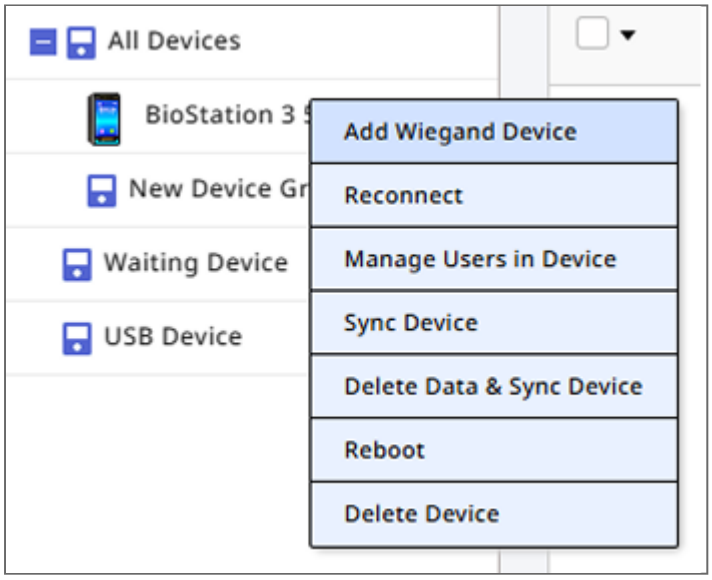
> **情報**
>
> - デバイスの **Device → Server** オプションは **SETTINGS** → **NETWORK** → **Server** で設定できます。メニューのパスはデバイスによって異なる場合があります。
> - **BioStar X** では、**Set IP** → **Device** ▶ **Server Connection** オプション(IP アドレス設定)でも設定できます。
> - システムは **Waiting Device** グループのデバイスを同期しません。システムは、デバイスを登録してデバイス同期が実行されるまで、ユーザーデータ、アクセスレベル、アクセスグループ、およびデバイス設定をそのデバイスに送信しません。

Wiegandデバイスを登録する

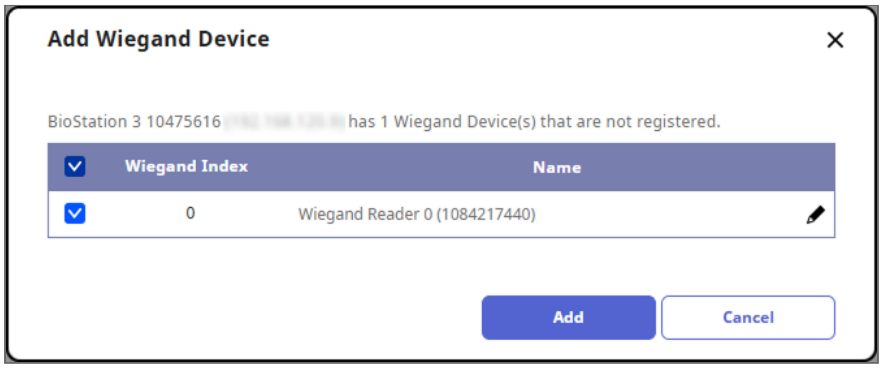
登録済みのマスターまたはスレーブデバイスにWiegandデバイスを追加する方法を説明します。

> **情報**
>
> - **마스터(Master) 장치**: RS-485로 연결한 장치 중 컨트롤러 역할을 수행하는 장치입니다. 슬레이브 장치를 주기적으로 모니터링하여 데이터를 처리합니다. 호스트(Host) 장치라고도 부릅니다.
> - **슬레이브(Slave) 장치**: RS-485로 연결한 장치 중 리더 또는 입출력 기능만 수행하는 장치입니다. 사용자 정보를 갖고 있지 않으며 마스터 장치에 의해 제어됩니다.
> - **Wiegand**: Wiegand는 두 개의 신호선(DATA0, DATA1)을 사용하여 데이터를 전송하는 통신 방식입니다. 주로 출입 통제 시스템에서 리더(Reader)와 컨트롤러 간의 통신에 사용되며, 간단한 구조와 낮은 비용으로 구현할 수 있습니다. 다만, 전송 거리가 짧고 데이터 전송 속도가 느린 한계가 있습니다.

1. **Launcher**ページで**Settings**をクリックします。
2. 画面左のサイドバーで **Device** → **Device** をクリック。
3. **All Devices** リストのマスターまたはスレーブデバイスを右クリックします。



4. ポップアップメニューで**Add Wiegand Device** をクリックします。
5. そのマスターデバイスに接続されているWiegandデバイスのリストが表示されたら、登録するデバイスを選択します。



6. **Add** をクリックします。
7. デバイス登録の確認メッセージが表示されたら、**Apply** をクリックします。

登録したWiegandデバイスが、選択したデバイスの下位に表示されます。



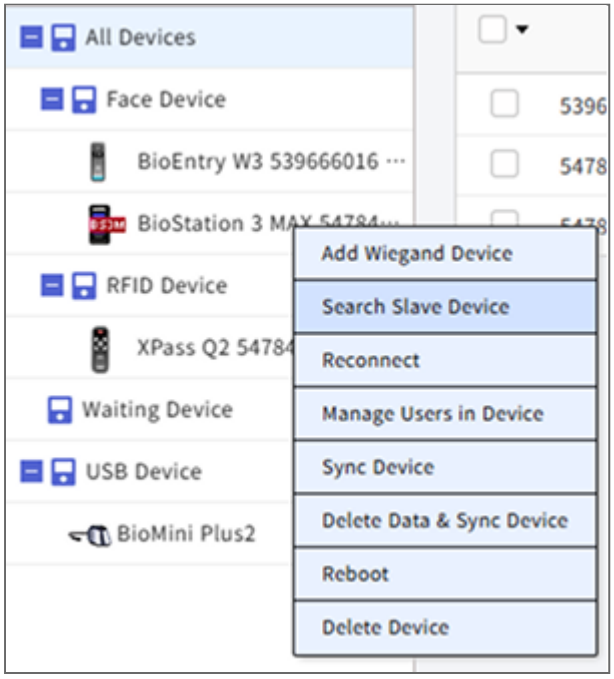
スレーブ装置を登録する

登録済みのマスター装置にスレーブ装置を追加して、アクセス制御システムのネットワークを簡単に拡張します。マスター装置とスレーブ装置はRS-485通信で接続します。装置だけでなくSecure I/O 2などの付属装置も接続して使用します。

1. **Launcher**ページで**Settings**をクリックします。

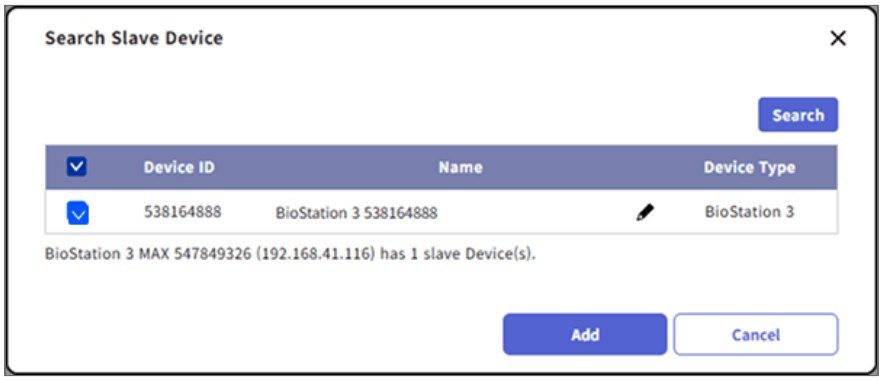
2. 画面左のサイドバーで **Device** → **Device** をクリック。

3. **All Devices** リストのマスターまたはスレーブデバイスを右クリックします。



4. ポップアップメニューで**Search Slave Device**をクリックします。

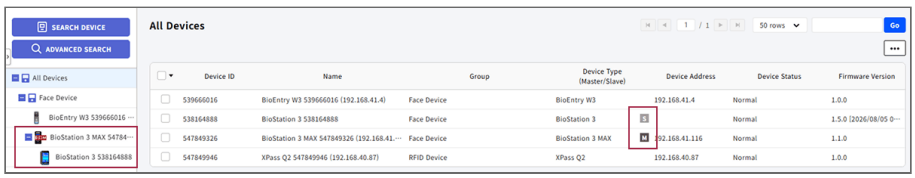
5. 該当マスター装置に接続されているスレーブ装置の一覧が表示されたら、登録する装置を選択します。目的の装置がない場合は、右上の**Search**ボタンをクリックします。



6. **Add** をクリックします。

7. デバイス登録の確認メッセージが表示されたら、**Ok** ボタンをクリックしてください。

選択した装置の下位に登録したスレーブ装置が表示されます。デバイスリストでは、マスターデバイスにはアイコン、スレーブデバイスにはアイコンが表示されます。



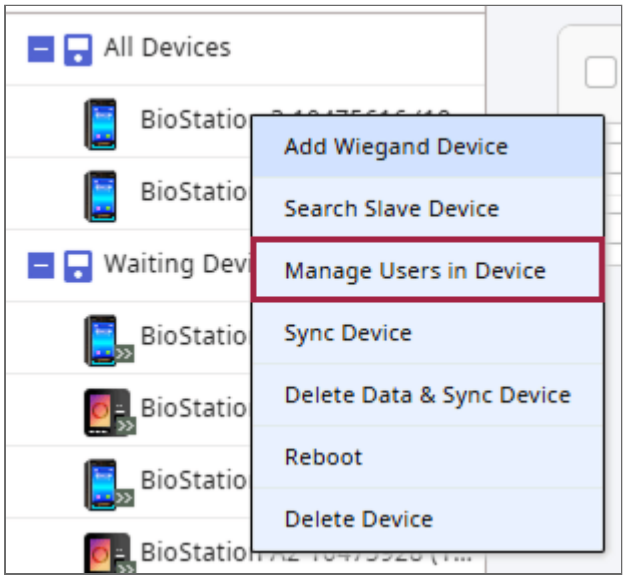
情報

- 指紋認証装置がマスター装置の場合、顔認証装置をスレーブ装置として追加できません。
- 顔認証装置がマスター装置で、別のスレーブ装置が既に追加されている場合、顔認証装置をスレーブ装置として追加できません。
- 顔認証装置がマスター装置で、顔認証装置をスレーブ装置として接続する場合、顔認証装置は1台のみスレーブ装置として追加できます。
- 顔認証装置がマスター装置で、顔認証装置をスレーブ装置として接続する場合、Secure I/O 2とDM-20をそれぞれ1台ずつ追加で接続できます。
- 接続可能なスレーブ装置の最大数は認証方法、ユーザー数、装置数によって変わり、スレーブ装置の数は認証速度に影響します。

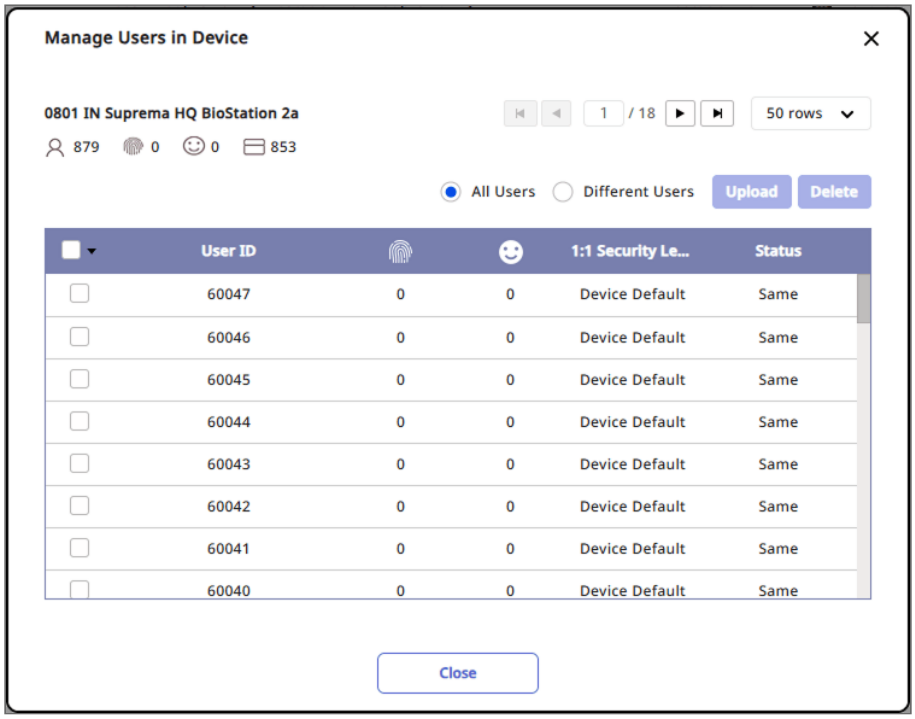
デバイスに登録したユーザーを管理する

デバイスに登録されているユーザー数、指紋数、顔情報数、カード数を確認できます。 **BioStar X** に未登録または既に登録済みのユーザー情報と比較し、**BioStar X** サーバーに送信または削除できます。

1. **Launcher**ページで**Settings**をクリックします。
2. 画面左のサイドバーで **Device** → **Device** をクリック。
3. **All Devices** リストでデバイスを選択し、右クリックしてください。
4. ポップアップメニューで **Manage Users in Device** をクリックしてください。



Manage Users in Device ウィンドウが表示されたら、デバイスに登録したユーザー情報と **BioStar X** に登録したユーザー情報を比較できます。



Status 列に表示される値を参照して、ユーザー情報をデバイスから削除するか **BioStar X** サーバーに送信するかを選択できます。**Status** 列の値は次のとおりです。

- **Same**：**BioStar X** サーバーに登録されている情報と同一のユーザー
- **Different**：**BioStar X** サーバーに登録されている情報と異なるユーザー
- **New User**：**BioStar X** サーバーに登録されていないユーザー

特定のユーザー情報をデバイスから削除するには、削除するユーザーを選択して **Delete** ボタンをクリックしてください。ユーザー情報を **BioStar X** サーバーに送信するには、**Upload** ボタンをクリックしてください。

> **情報**
>
> - **Manage Users in Device** 機能は 1 台のデバイスのみ選択して使用できます。
> - **Upload** ボタンをクリックしたとき、**BioStar X** サーバーに同じ ID を持つユーザーがいる場合は、デバイスの情報で更新できます。
> - 削除したユーザー情報はデバイスでのみ削除され、**BioStar X** サーバーには残ります。
> - デバイスの詳細設定については、デバイス設定をご参照ください。

ファームウェアをアップグレードする

BioStar Xと接続されたデバイスは、追加の接続や操作なしで簡単にファームウェアをアップグレードできます。デバイスのファームウェアを最新バージョンに保つことで、セキュリティ脆弱性を解消し、新機能を利用できます。

開始前に

デバイスのファームウェアをアップグレードする前に、新しいバージョンのファームウェアファイルをあらかじめ用意してください。ダウンロードしたファームウェアファイルを以下のパスに保存し、圧縮を解凍してください。「*firmware*」フォルダーがない場合は新規作成してください。

> *C:\Program Files\BioStar X\firmware*

情報

新しいバージョンのファームウェアファイルは、Suprema ダウンロードセンターでデバイスのモデル名を検索し、最新バージョンのファームウェアファイルをダウンロードしてください。

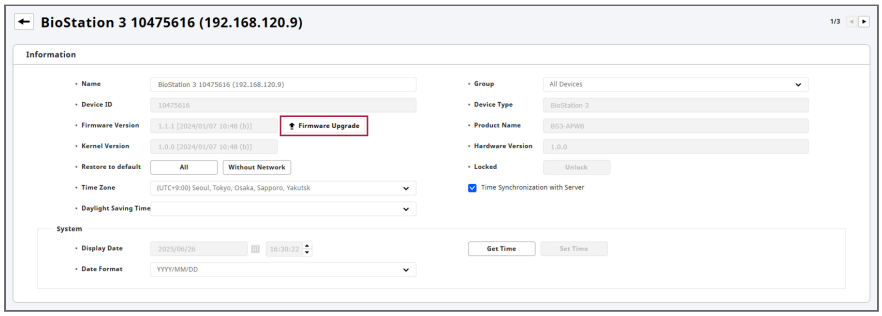
ファームウェアのアップグレード

注意

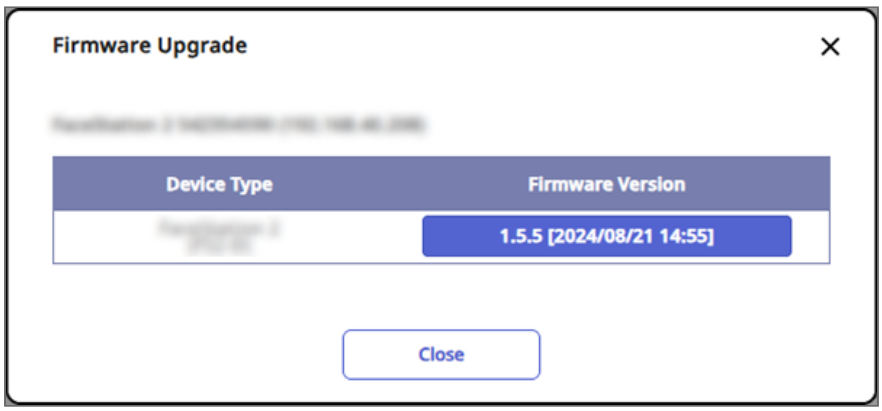
- ファームウェアのアップグレード前に、デバイスの電源供給またはネットワーク状態を必ず確認してください。特に、アップグレード中に電源供給が遮断されないよう注意してください。
- デバイスの種類とモードによっては、最大1時間以上かかる場合があります。また、アップグレード中はデバイスを使用できません。
- ファームウェアのアップグレード中は、デバイスの電源を切らないでください。アップグレードが完了すると、デバイスは自動的に再起動します。

1 台のデバイスのファームウェアアップグレード

1. **Launcher**ページで**Settings**をクリックします。
2. 画面左のサイドバーで **Device** → **Device** をクリック。
3. デバイスリストでファームウェアをアップグレードするデバイスをクリックします。
4. デバイス詳細画面の **Information** セクションで **Firmware Upgrade** をクリックします。



5. **Firmware Upgrade** ウィンドウが表示されたら、ファームウェアバージョンをクリックします。

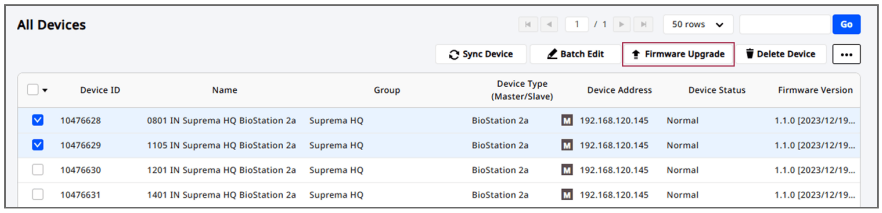


6. 警告メッセージウィンドウが表示されたら、**Continue** ボタンをクリックしてください。

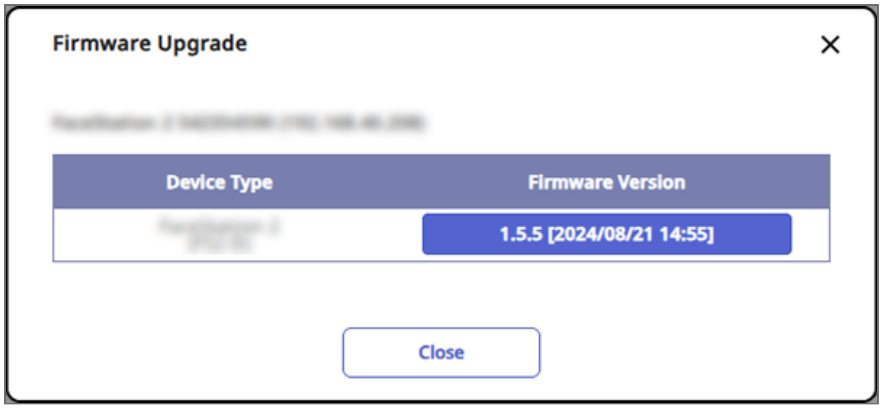
デバイスのファームウェアをアップグレードします。

複数デバイスのファームウェアアップグレード

1. **Launcher**ページで**Settings**をクリックします。
2. 画面左のサイドバーで **Device** → **Device** をクリック。
3. デバイスリストでファームウェアをアップグレードするデバイスの一番左にあるチェックボックスを選択します。複数のデバイスを選択できます。
4. デバイスリストの右上にある **Firmware Upgrade** をクリックします。



5. **Firmware Upgrade** ウィンドウが表示されたら、ファームウェアバージョンをクリックします。



6. 警告メッセージウィンドウが表示されたら、**Continue** ボタンをクリックしてください。

選択したデバイスのファームウェアをアップグレードします。

> **情報**
>
> - **Firmware Upgrade** はデバイスリストでデバイスを選択した後にのみ有効になります。
> - 同じ RS-485 モードを持つデバイスは、複数台を同時にアップグレードできます。たとえば、マスターデバイスはマスターデバイス同士で複数台を同時にアップグレードでき、スレーブデバイスはスレーブデバイス同士で複数台を同時にアップグレードできます。
> - マスターデバイスやマスターに接続されていないスレーブデバイスは、複数台を同時にアップグレードできます。
> - 同じマスターデバイスに接続されているスレーブデバイスは、複数台を同時にアップグレードできません。

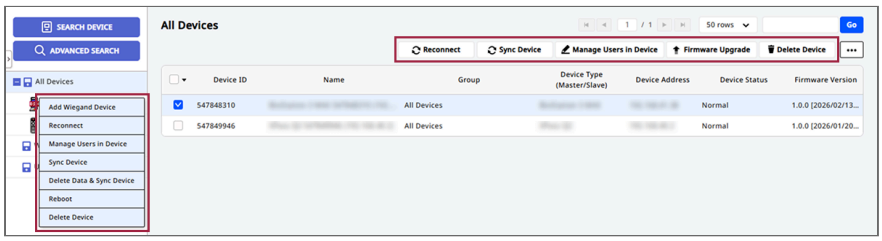
デバイス管理機能を利用する

BioStar X でデバイスのその他の機能を使用する方法を説明します。デバイスの再接続、同期、情報の一括編集、削除、設定のエクスポート/インポート機能を提供します。また、デバイス削除時にセキュア通信証明書も削除するオプションについても説明します。

個々のデバイスを管理する機能

一台のデバイスに対する管理機能の使い方は以下のとおりです。

1. **Launcher**ページで**Settings**をクリックします。
2. 画面左のサイドバーで **Device** → **Device** をクリック。
3. **All Devices** リストでデバイスを選択し、右クリックしてください。または、デバイス一覧で対象のデバイスのチェックボックスをクリックします。



4. ポップアップメニュー、またはデバイス一覧の上部から希望する機能を選択します。

提供される機能については、以下をご参照ください。提供される機能はデバイスによって異なる場合があります。

- **Reconnect**：選択したデバイスを再接続できます。デバイスを 1 台選択した場合に使用できます。通常、デバイスはネットワーク接続が復旧すると、別途操作しなくても自動的にオンライン状態へ戻ります。この機能は、ネットワーク復旧後もデバイスが自動的に再接続しない場合に使用します。

> **情報**
> この機能は **Device ▶ Server Connection** オプションで接続されたデバイスではサポートされません。デバイスの登録に関する詳細は、デバイスを登録するをご参照ください。

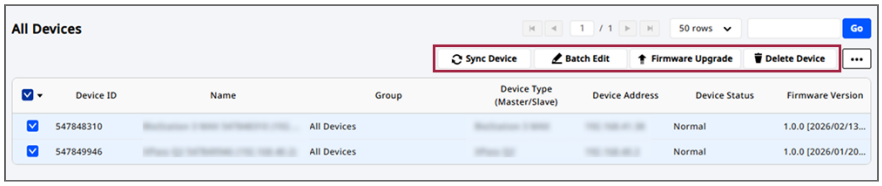
- **Sync Device**：登録したデバイスと **BioStar X** のすべてのユーザー情報を同期できます。 **BioStar X** のデータベース情報を基準にユーザー情報を同期し、デバイスのみに登録されているユーザー情報は削除します。ユーザー情報を **BioStar X** にアップロードするには **Manage Users in Device** 機能を使用します。
- **Delete Data & Sync Device**：デバイスに保存されているすべての設定情報およびユーザー情報を削除して再送できます。この機能はデバイス一覧でデバイスを選択し、[•••] ボタンをクリックして使用することもできます。
- **Manage Users in Device**：デバイスに登録されているユーザー情報を **BioStar X** にアップロードするか、デバイスから削除できます。詳細については、デバイスに登録したユーザーを管理するご参照ください。
- **Firmware Upgrade**：デバイスのファームウェアを簡単にアップグレードできます。詳細については、ファームウェアをアップグレードするをご参照ください。
- **Reboot**：選択したデバイスを再起動できます。この機能はデバイスが正常に動作しない場合に使用できます。
- **Delete Device**：選択したデバイスを一覧から削除できます。ドアまたは区画として設定されたデバイスは削除できません。詳しくは デバイスの削除 をご参照ください。

> **情報**
> - **Add Wiegand Device**の機能の詳細については、Wiegandデバイスを登録するをご参照ください。
> - **Search Slave Device**の機能の詳細については、スレーブ装置を登録するをご参照ください。

複数のデバイスの管理機能

一台以上のデバイスに対する管理機能の使い方は以下のとおりです。

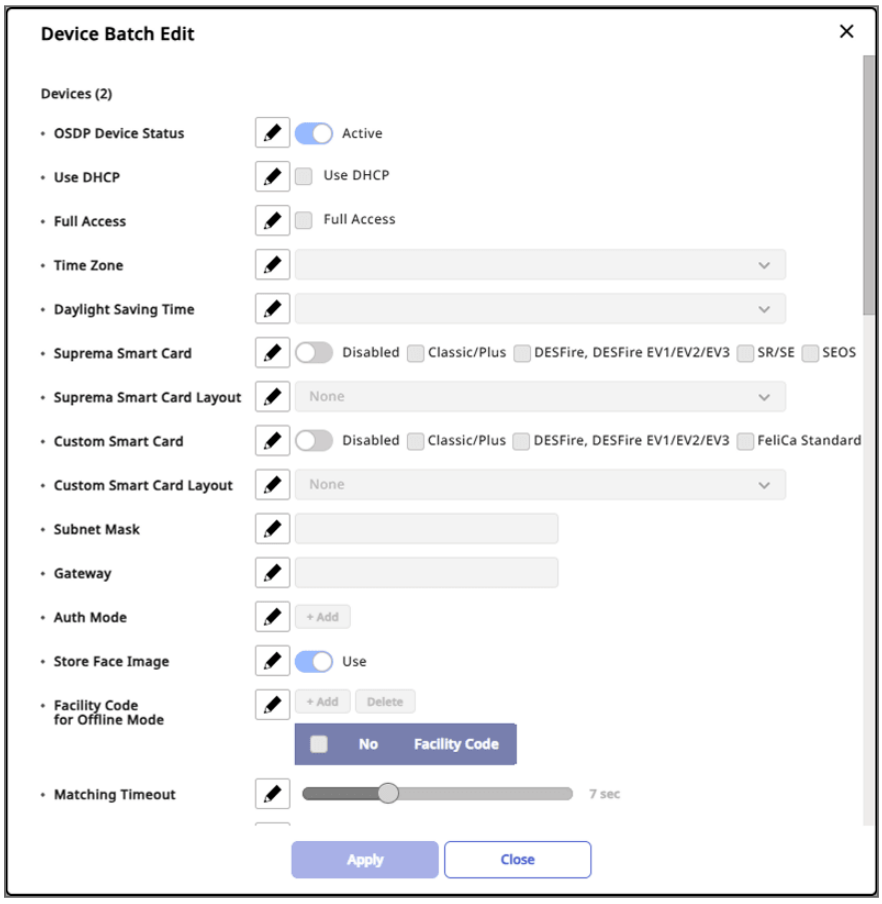
1. **Launcher**ページで**Settings**をクリックします。
2. 画面左のサイドバーで **Device** → **Device** をクリック。
3. デバイス一覧で対象のデバイスのチェックボックスをクリックします。 1 台以上のデバイスを選択できます。



4. デバイス一覧の上部から希望する機能を選択します。

提供される機能については、以下をご参照ください。提供される機能はデバイスによって異なる場合があります。

- **Sync Device**：登録したデバイスと **BioStar X** のすべてのユーザー情報を同期できます。 **BioStar X** のデータベース情報を基準にユーザー情報を同期し、デバイスのみに登録されているユーザー情報は削除します。
- **Batch Edit**：選択したデバイスの情報を一括編集できます。ボタンをクリックすると、**Device Batch Edit** ウィンドウが表示されます。



> **情報**
>
> - 選択したデバイスの種類によって、**Device Batch Edit** ウィンドウに表示される詳細項目が異なる場合があります。
> - マスターデバイスとスレーブデバイスを同時に選択して一括編集をクリックすると、**Authentication** と **Display/Sound** 項目の一部のみを変更できます。
> - **Auth Mode** は同一モデル名のデバイスを選択した場合にのみ一括編集できます。

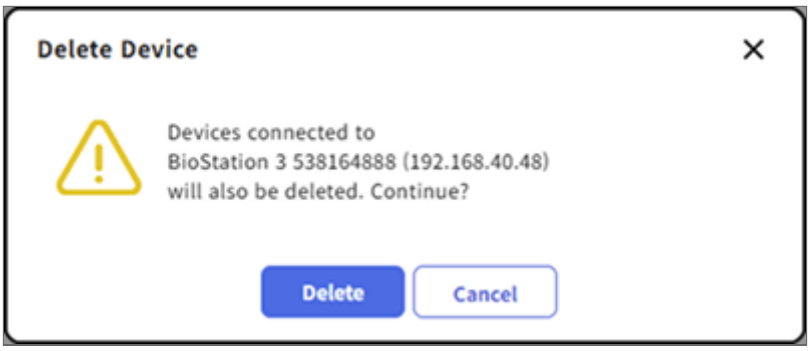
- **Firmware Upgrade**：デバイスのファームウェアを簡単にアップグレードできます。詳細については、ファームウェアをアップグレードするをご参照ください。
- **Delete Device**：選択したデバイスを一覧から削除できます。ドアまたは区画として設定されたデバイスは削除できません。詳しくは デバイスの削除 をご参照ください。

デバイスの削除

Delete Device 機能でデバイスを一覧から削除できます。削除時に表示されるオプションは、**Secure communication with device** オプションが有効か無効かによって異なります。

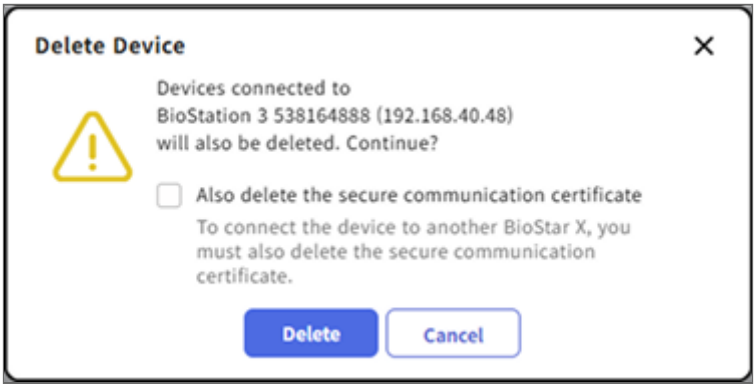
デバイスでセキュア通信を使用しない場合

Secure communication with device オプションが **Not Use** の場合、追加オプションなしで選択したデバイスを削除できます。



デバイスでセキュア通信を使用する場合

Secure communication with device オプションが **Use** の場合、**Delete Device** ダイアログに **Also delete the secure communication certificate** オプションが表示されます。



- **Also delete the secure communication certificate** オプションを選択しない場合（デフォルト）、証明書は削除せず、デバイスのみ削除します。

- **Also delete the secure communication certificate** オプションを選択すると、デバイスに保存されたセキュア通信証明書も削除します。削除したデバイスを別の **BioStar X** サーバーに接続する場合は、このオプションを使用します。

> **注意**
>
> **BioStar X** との接続が切れたデバイスは証明書を削除できません。このため、**Also delete the secure communication certificate** オプションを選択した状態ではデバイスを削除できません。デバイスを削除するには、オプションの選択を解除するか、デバイスを再接続してから再試行してください。

> **情報**
>
> - **Secure communication with device** オプションを使用している状態で、**Also delete the secure communication certificate** オプションを選択せずにデバイスを削除すると、デバイスに証明書が残ります。その後 **Secure communication with device** オプションを **Not Use** に変更し、そのデバイスを再度 **BioStar X** に登録すると、デバイスに証明書が残っているため接続できません。既定の証明書を使用している場合は、**Secure communication with device** オプションを再度 **Use** に変更してください。
> - 選択したデバイスがすべてスレーブデバイスであるか、セキュア通信に対応していない場合は、**Also delete the secure communication certificate** オプションなしでデバイスを削除できます。
> - **Also delete the secure communication certificate** オプションは、**Secure communication with device** オプションを有効にした場合のみ表示されます。詳しくは システムセキュリティを強化する をご参照ください。

デバイス設定のエクスポート/インポート

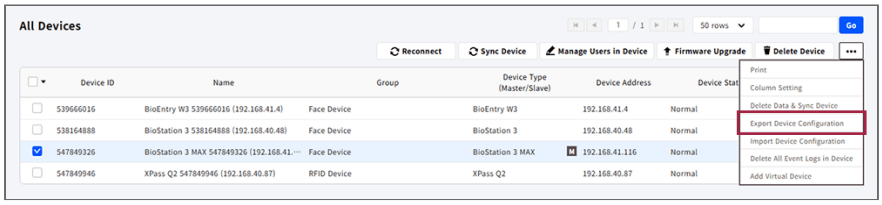
あるデバイスの設定をファイルにエクスポートした後、同じモデルの別のデバイスにそのままインポートして適用できます。複数のデバイスに同じ設定を繰り返し入力する代わりに、設定済みのデバイスから設定ファイルを作成し、他のデバイスに適用してください。

> **情報**
>
> - 同一モデルとは、デバイスの詳細モデル名とパート番号（例: XPD2-XXX の XXX 部分）まで、すべて一致するデバイスを指します。
> - デバイス設定のエクスポート/インポート機能は、デバイス設定へのフル権限を持つ管理者が使用できます。管理者権限の設定の詳細は 運用権限管理 をご参照ください。

デバイス設定のエクスポート

デバイス一台の設定をファイルとしてダウンロードする方法は以下のとおりです。

1. **Launcher**ページで**Settings**をクリックします。
2. 画面左のサイドバーで **Device** → **Device** をクリック。
3. デバイス一覧で、設定をエクスポートするデバイスのチェックボックスをクリックします。デバイスは一台のみ選択できます。
4. デバイス一覧の上部にある ••• → **Export Device Configuration** をクリックします。



5. ダウンロードウィンドウが表示されたら、設定ファイルをローカルに保存します。

注意

次のデバイスは設定をエクスポートできません。

- **BioStar X** との接続が切断された、または応答がタイムアウトしたデバイス
- 仮想デバイス（Virtual Device）
- RS-485 通信モードがないデバイス（例：Wiegand デバイス、IO モジュール、Door Interface、Door モジュール、Secure モジュール、OSDP Antenna/Reader）

情報

- デバイスを一台も選択しない、または二台以上選択した状態では、この機能を実行できません。
- システムはファイル名を、モデル名、デバイス ID、RS-485 通信モード（Master/Default/Slave）、エクスポート日の順に自動で指定します。日付は **Settings** → **System** → **Preferences** で指定した日付形式に従います。

  たとえば、モデル名が BS3-DB、デバイス ID が 538001234、シリアル通信モードが **Master**、エクスポート日が 2026年6月23日のデバイスは、`BS3-DB_538001234_Master_20260623.json` 形式のファイルとして保存されます。

エクスポートから除外される設定

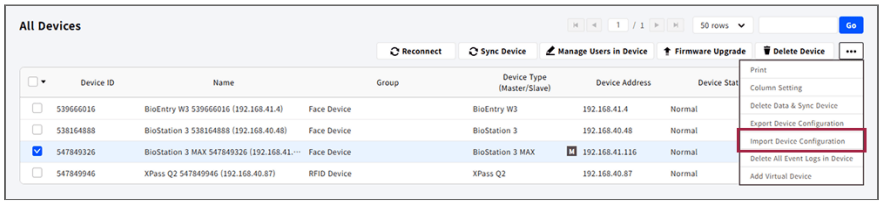
次の設定は、デバイスごとに固有であるか、デバイスにのみ保存されているか、認証情報などの機微情報に該当するため、エクスポートファイルに含めません。

- デバイス固有の設定: Name, Group、有線/無線ネットワーク設定、サーバー接続設定、OSDP 識別子、Trigger & Action
- デバイスにのみ保存され、他のデバイスへ移行できない設定: Display/Sound の言語リソース、ホーム画面、サウンド、シリアル通信の SCB キー、BioStation 3 Max に追加した映像設定
- 認証情報および機微情報: IP インターホンと RTSP のユーザー名とパスワード、Master Admin 設定、Two-step Authentication オプション

デバイス設定のインポート

エクスポートした設定ファイルを同じモデルのデバイス一台以上に適用する方法は以下のとおりです。

1. **Launcher**ページで**Settings**をクリックします。
2. 画面左のサイドバーで **Device** → **Device** をクリック。
3. デバイス一覧で、設定を適用するデバイスのチェックボックスをクリックします。一台以上のデバイスを選択できます。
4. デバイス一覧の上部にある ••• → **Import Device Configuration** をクリックします。



5. Web ブラウザの［開く］ウィンドウが表示されたら、ローカルに保存した設定ファイルを選択します。

6. デバイス設定のインポート結果メッセージが表示されたら内容を確認し、**Ok** ボタンをクリックします。

> **注意**
>
> システムは、別のサイトやサーバーで作成された設定ファイルも、出所の確認や警告なしに正規のファイルとして受け入れます。取り込むファイルが信頼できる出所で作成されたものか確認してください。

> **情報**
>
> デバイスを一台も選択していない場合、この機能は実行できません。

インポートを実行すると、システムは設定を適用する前に次の項目を順に確認します。いずれかの確認が条件を満たさない場合、設定を適用せず、理由を案内します。

- 選択したデバイスのモデル名（パート番号を含む）がすべて同じか
- 選択したデバイスとファイルのRS-485通信モードがすべて同じか
- ファイルに保存されたモデル名（パート番号を含む）が、選択したデバイスのモデル名（パート番号を含む）と同じか
- 選択したデバイスに仮想デバイス（Virtual Device）が含まれているか

確認に合格すると、システムはエクスポートから除外される設定を除く残りの設定を、選択したすべてのデバイスに適用します。

情報

- 特定の機能をサポートしないデバイスからエクスポートしたファイルをサポートするデバイスにインポートすると、その機能はオフで適用され、対象デバイスで事前にオンにしたオプションがオフになります。反対に、機能をサポートするデバイスからエクスポートしたファイルをサポートしないデバイスにインポートすると、その機能は適用されず、残りの設定のみ適用されます。どちらの場合もインポート失敗として扱わず、失敗リストにも含まれません。
- デバイスライセンスが必要な設定は、そのライセンスが適用されていないデバイスには適用されません。反対に、ライセンスが適用されていないデバイスからエクスポートしたファイルを、ライセンスが適用されているデバイスにインポートすると、その設定はオフの状態で適用され、対象デバイスで事前にオンにしていたオプションがオフになります。どちらの場合もインポート失敗として扱わず、失敗リストにも含まれません。
- すべてのデバイスに正常に適用すると、システムは成功メッセージを表示します。一部またはすべてのデバイスに適用できない場合、システムは失敗したデバイス数とともに、失敗リストをCSVファイルとしてダウンロードできる案内メッセージを表示します。このファイルには、失敗したデバイスのID、名前、失敗理由（デバイスとの接続切断、または入退室グループが設定されていて全入退室権限をオンにできない場合）が含まれます。

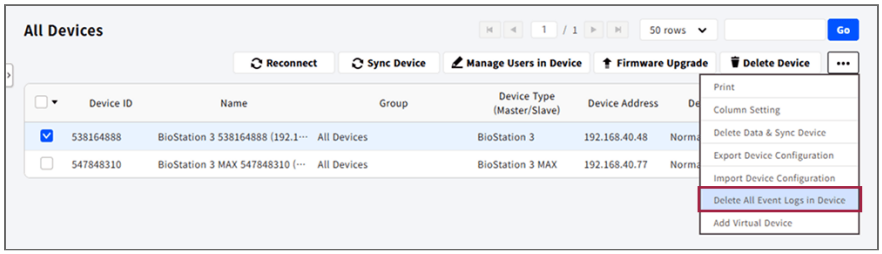
  > *例えば、2026年6月23日15時45分30秒に実行したインポートが失敗した場合、ファイル名は `Device_Template_Import_Error_20260623T154530.csv` 形式になります。*

- CoreStation デバイスも適用対象に含まれます。
- デバイス設定のエクスポートとインポートの作業履歴は **Settings** → **Audit Trail** → **AC Audit Log** で確認できます。

デバイス内のイベントログの削除

デバイスに保存されたイベントログを削除できます。

1. **Launcher**ページで**Settings**をクリックします。
2. 画面左のサイドバーで **Device** → **Device** をクリック。
3. デバイス一覧で対象のデバイスのチェックボックスをクリックします。 1 台以上のデバイスを選択できます。
4. デバイス一覧の上部にある ••• → **Delete All Event Logs in Device** ボタンをクリックします。



5. 警告メッセージが表示されたら内容を確認し、**Continue** ボタンをクリックします。

デバイスのイベントログ削除操作が完了すると、ポップアップメッセージが表示されます。対象デバイス数、成功したデバイス数、失敗したデバイス数を確認できます。

注意

デバイスから削除されたイベントログは復元できず、サーバーから再度デバイスへ送信することはできません。削除を実行する前に、イベントログがサーバーに保存されていることを確認してください。また、選択したデバイスにスレーブ、仮想デバイス、または Wiegand デバイスが含まれている場合、これらはログを保存しないため、ログ削除の対象外になります。

> **情報**
>
> - この機能は **Administrator Role** 権限を持つユーザーのみ利用できます。
> - デバイスのイベントログ削除履歴は **Settings** → **Audit Trail** → **AC Audit Log** で確認できます。

追加機能

デバイス一覧を印刷したり、列設定を変更したりするなど、追加機能を利用できます。

デバイス一覧を印刷する

デバイス一覧をPDFまたはSVG形式で保存して印刷できます。

1. **Launcher**ページで**Settings**をクリックします。
2. 画面左のサイドバーで **Device** → **Device** をクリック。
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. ポップアップメニューで **Print** をクリックしてください。
5. 「**Print Option**」ウィンドウが表示されたら、「**File Format**」オプションで目的のフォーマットを選択し、その他のオプションを設定します。



6. **Print** をクリックしてください。

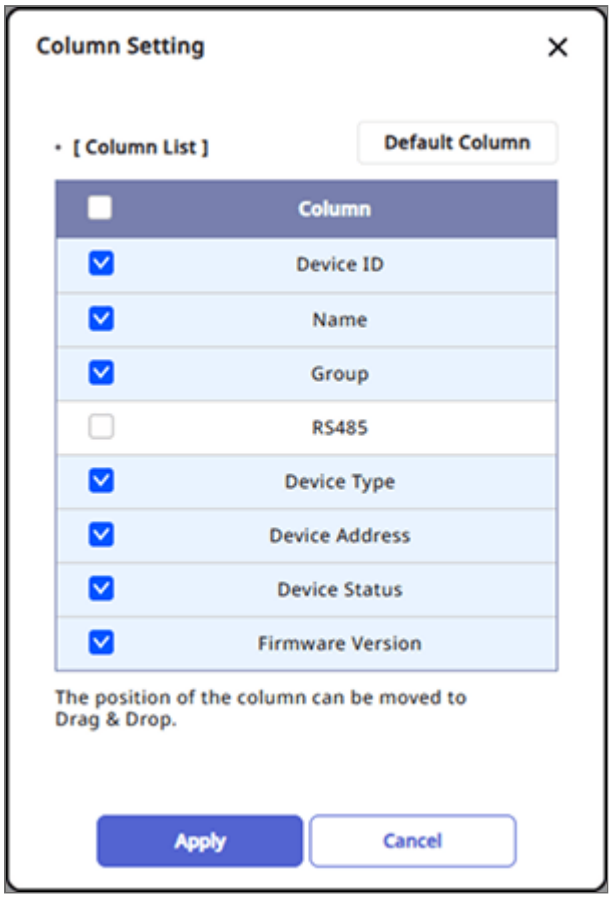
ブラウザーで開いたPDFまたはSVGファイルを印刷できます。

デバイス一覧の列(Column)の設定

デバイス一覧に表示される列(Column)の設定を変更できます。列設定で表示する列を選択したり、列の順序を変更したりできます。

1. **Launcher**ページで**Settings**をクリックします。
2. 画面左のサイドバーで **Device** → **Device** をクリック。
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. ポップアップメニューで **Column Setting** をクリックしてください。

5. **Column Setting** ウィンドウが表示されたら、必要な列を選択するか、選択を解除してください。



6. 列の順序を変更するには、目的の列をクリックしたままドラッグして位置を変更します。
7. 設定を保存するには、**Apply** をクリックします。

> **情報**
> 列設定を初期化するには、**Default Column** をクリックします。

デバイス設定

登録済みデバイスの詳細機能を設定および管理する方法を説明します。デバイスの情報、ネットワーク、認証、高度な設定などの詳細を設定できます。詳細は RS-485 の接続方式やデバイスの種類によって異なります。

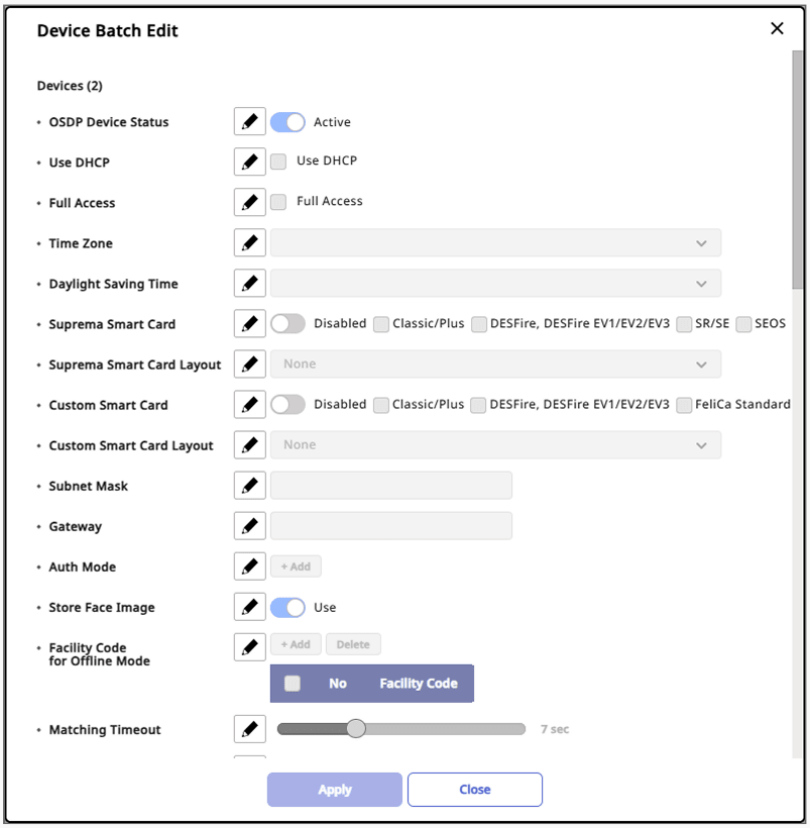
1. **Launcher**ページで**Settings**をクリックします。
2. 画面左のサイドバーで **Device** → **Device** をクリック。
3. デバイス一覧で詳細を設定したいデバイスをクリックします。
4. 各セクションの詳細項目を参照してデバイス情報を設定します。
   - **Information**：デバイス名、グループ、タイムゾーン、ハードウェアおよびファームウェアのバージョンを確認および変更できます。詳細については、基本情報を設定するご参照ください。
   - **Network**：デバイスの TCP/IP、RS-485、サーバー通信などのネットワークを設定できます。詳細については、ネットワークを設定するご参照ください。

- **Authentication**：デバイスのユーザー認証に関するオプションを設定できます。詳細については、認証を設定するご参照ください。
- **Advanced**：マスター管理者、デバイス管理者、画面/サウンド、動作条件および動作などを設定できます。詳細については、高度設定ご参照ください。
- **Thermal & Mask** / **Mask**：サーマルカメラおよびマスク使用に関する詳細項目を設定できます。詳しくは熱画像とマスクを設定するをご覧ください。
- **Intercom**：IP インターフォンの使用に関する詳細項目を設定できます。詳細については、IPインターホンを設定するを参照してください。
- **RTSP**：Real Time Streaming Protocol (RTSP) ストリーミング用の詳細項目を設定できます。詳細については、RTSPを設定するご参照ください。

5. すべての設定が完了したら、画面最下部の **Apply** ボタンをクリックします。

情報

- 複数のデバイス情報をまとめて編集することもできます。 2 台以上のデバイスを選択し、画面右上の **Batch Edit** をクリックします。

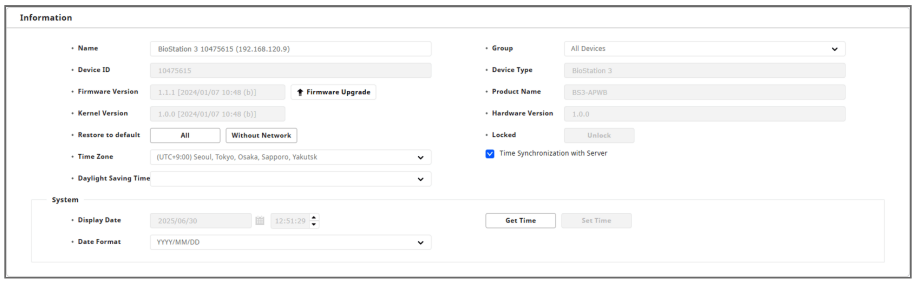


- 選択したデバイスの種類によって、**Device Batch Edit** ウィンドウに表示される詳細項目が異なる場合があります。
- マスターデバイスとスレーブデバイスを同時に選択して一括編集をクリックすると、**Authentication** と **Display/Sound** 項目の一部のみを変更できます。
- **Auth Mode** は同一モデル名のデバイスを選択した場合にのみ一括編集できます。

基本情報を設定する

「**Information**」セクションではデバイスの基本情報を設定できます。デバイスの名前とグループ、タイムゾーン、ハードウェアおよびファームウェアバージョンなどを確認できます。デバイスの名前とグループを変更したり、デバイスのファームウェアをア

ップグレードできます。



以下はデバイスに設定されている基本情報で、ユーザーが変更できない項目です。

- **Device ID**：デバイスのIDを確認できます。
- **Device Type**：デバイスの種類を確認できます。
- **Product Name**：デバイスのモデル名を確認できます。
- **Kernel Version**：デバイスのカーネルバージョンを確認できます。
- **Hardware Version**：デバイスのハードウェアバージョンを確認できます。

> **情報**
> ユーザーが任意で変更した内容がある場合は、**Apply** をクリックします。変更内容を保存しないとデバイスに反映されません。

デバイス名を変更する

既定のデバイス名を変更できます。「**Name**」項目に希望のデバイス名を入力します。デバイス名は最大48文字まで入力できます。デバイス名はデバイスリストでデバイスを識別するために使用します。

デバイスグループを変更する

デバイスが属するグループを変更できます。「**Group**」項目で希望のデバイスグループを選択します。

> **情報**
> 新しいデバイスグループの作成やグループ名の変更・削除の詳細はデバイスグループを管理するを参照してください。

ファームウェアをアップグレードする

デバイスのファームウェアバージョンを確認するには「**Firmware Version**」項目で確認できます。ファームウェアをアップグレードするには「**Firmware Upgrade**」ボタンをクリックします。

> **情報**
> デバイス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。

デバイスの日付と時刻を設定する

以下のオプションでデバイスの日付と時刻を設定できます。

- **Time Zone**：デバイスがあるタイムゾーンを選択できます。
- **Time Synchronization with Server**：デバイスの時刻をBioStar Xサーバーの時刻と同期できます。
- **Daylight Saving Time**：ユーザーが設定した夏時間をデバイスに適用できます。新しい夏時間を追加するにはサマータイムを設定するを参照してください。
- **Display Date**：デバイスの日付と時刻を手動で設定できます。日付と時刻を設定したら「**Set Time**」ボタンをクリックします。

  > この機能は「**Time Synchronization with Server**」オプションを選択していない場合に使用できます。

- **Date Format**：デバイスに表示される日付形式を選択できます。
- **Get Time**：デバイスに設定されている時刻を取得できます。

> **注意**
> 設定した日付と時刻はイベントログとリアルタイムログに記録されます。デバイスの日付と時刻が正確でないとログ記録が不正確になる可能性があります。

デバイスのロックを解除する

動作条件によりデバイスがロックされた場合、「**Locked**」項目の「**Unlock**」ボタンをクリックします。デバイスのロックを解除できます。

> **情報**
> 作業条件およびアクション設定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。

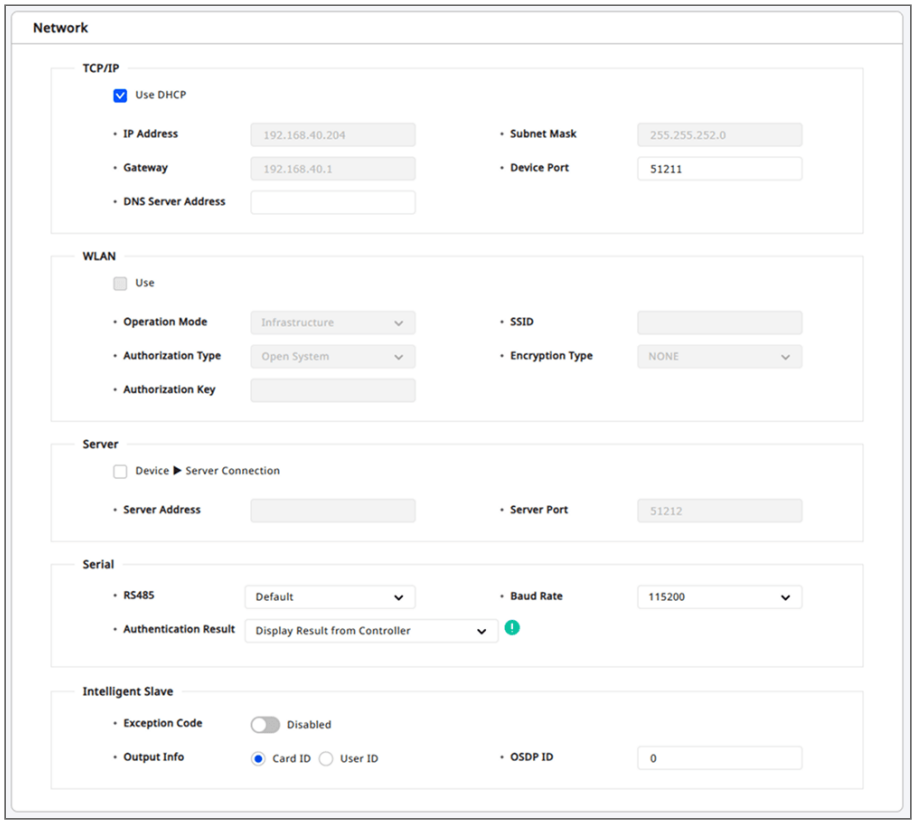
デバイスを初期化する

デバイスの設定を初期化するには「**Restore to default**」項目で以下のいずれかを選択します。

- **All**：デバイスのすべての設定を初期化します。
- **Without Network**：ネットワーク設定を保持し、それ以外を初期化します。

ネットワークを設定する

登録した装置のネットワーク設定を案内します。 **Network** セクションでは、装置のTCP/IP、RS-485、サーバー通信などのネットワークを設定できます。



情報

- デバイスの種類によって設定できるネットワークオプションが異なる場合があります。
- ユーザーが任意で変更した内容がある場合は、**Apply** をクリックします。変更内容を保存しないとデバイスに反映されません。

TCP/IP 設定

TCP/IP グループではデバイスの IP アドレスを設定できます。

情報

デバイスを登録する際のIPアドレス設定の詳細については、デバイスを登録するをご参照ください。

動的 IP 設定

装置を動的IPで使用するよう設定するには、**Use DHCP** オプションのチェックボックスをクリックします。デバイスが DHCP サーバーから IP アドレスを自動取得します。この場合、デバイスの IP アドレスが変更されることがあります。

固定 IP 設定

装置のIPアドレスを固定に設定するには、**Use DHCP** オプションのチェックボックスの選択を解除します。以下の詳細項目に装置のネットワーク情報を入力できます。

- **IP Address**：デバイスの IP アドレスを入力します。 IP アドレスは `xxx.xxx.xxx.xxx` 形式で入力でき、各オクテットには 0～255 の数値のみを入力できます。
- **Subnet Mask**：デバイスのサブネットマスクを入力します。

- **Gateway**：デバイスのゲートウェイアドレスを入力します。
- **Device Port**：デバイスのポート番号を入力します。
- **DNS Server Address**：デバイスの DNS サーバーアドレスを入力します。

▼ DNS サーバーアドレスを入力できるデバイスとファームウェアバージョンを表示

- BioStation 3 Maxのファームウェアバージョン1.0.0以降
- XPass Q2のファームウェアバージョン1.0.0以降
- BioEntry W3 ファームウェア 1.0.0 以上
- BioStation 3 ファームウェア 1.0.0 以上
- X-Station 2 ファームウェア 1.0.0 以上
- FaceStation F2 ファームウェア 1.0.0 以上
- XPass 2 ファームウェア 1.0.0 以上
- FaceLite ファームウェア 1.0.0 以上
- BioLite N2 ファームウェア 1.0.0 以上
- FaceStation 2 ファームウェア 1.0.0 以上
- BioStation L2 ファームウェア 1.0.0 以上
- BioStation A2 ファームウェア 1.0.0 以上
- BioStation 2 ファームウェア 1.2.0 以上

無線 LAN 設定

WLAN グループではデバイスの無線 LAN 設定をオンまたはオフにできます。詳細項目はデバイスで設定でき、詳細はデバイスのユーザーガイドを参照してください。

情報

無線 LAN 設定に対応するデバイスは以下を参照してください。

- BioStation 2
- BioStation A2
- FaceStation 2
- BioStation 3

サーバー通信設定

Server グループでは **BioStar X** サーバーとの通信方法を設定できます。

- **Device ▶ Server Connection**：このオプションを選択すると、デバイスで接続する **BioStar X** サーバーの IP アドレスとポート番号を入力できます。
- **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ます。
- **Server Port**：**BioStar X** サーバーのポート番号を入力します。

ヒント

この機能は **BioStar X** サーバーの IP アドレスが変更される際に便利です。 **BioStar X** サーバーの IP アドレスを変更する前に複数のデバイスでこのオプションを事前に設定しておくと、デバイスは自動的に変更後の IP アドレスへ接続します。

▼ Server Address にドメインを入力できるデバイスとファームウェアバージョンを表示

- BioStation 3 Maxのファームウェアバージョン1.0.0以降
- XPass Q2のファームウェアバージョン1.0.0以降
- BioEntry W3 ファームウェア 1.0.0 以上
- BioStation 3 ファームウェア 1.0.0 以上
- X-Station 2 ファームウェア 1.0.0 以上
- FaceStation F2 ファームウェア 1.0.0 以上
- XPass 2 ファームウェア 1.0.0 以上
- FaceLite ファームウェア 1.0.0 以上
- BioLite N2 ファームウェア 1.0.0 以上
- BioEntry P2 ファームウェア 1.0.0 以上
- FaceStation 2 ファームウェア 1.0.0 以上
- BioEntry W2 ファームウェア 1.0.0 以上
- BioStation L2 ファームウェア 1.0.0 以上
- BioStation A2 ファームウェア 1.0.0 以上
- BioStation 2 ファームウェア 1.2.0 以上

シリアル通信設定

Serial グループでは RS-485 通信方式で接続されたデバイスのモード、伝送速度、および表示する認証結果を設定できます。

- **RS485**：RS-485 モードを設定します。
- **Baud Rate**：RS-485 通信速度を設定します。
- **Authentication Result**：他社コントローラーと連携してデバイスを使用する際、デバイス画面に表示する認証結果を選択します。
  - **Display Result from Controller**：他社コントローラーの認証結果をデバイスに表示できます。
  - **Display Device Matching Result**：デバイスの認証結果を表示できます。

情報

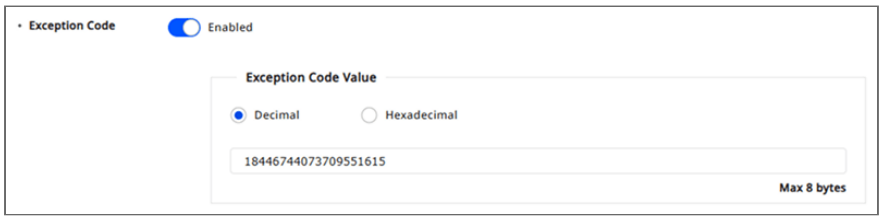
Authentication Result オプションは、**RS485** オプションで **Slave** または **Default** を選択した場合に有効になります。

インテリジェントスレーブ設定

Intelligent Slave グループでは、Suprema デバイスと他社コントローラーを組み合わせた環境でユーザーが指紋認証を行った

際、その認証結果を Open Supervised Device Protocol(OSDP) のカードデータとして送信し、多数の 1:1 または 1:N マッチングをサポートします。

- **Exception Code**：インテリジェントスレーブを使用する際に認証失敗などの例外が発生した場合、例外コードを10進数(0～18446744073709551615)または16進数(0～FFFFFFFFFFFFFFFF)形式で入力して正確なログを残せます。 16進数は数字または英字で入力できます。



- **Output Info**：認証が成功したときにカードIDまたはユーザーIDを出力できます。
- **OSDP ID**：装置のOSDPアドレスを入力してください。 0～126 の範囲の数字で入力できます。

> **情報**
>
> - **Exception Code**のデータサイズは最大8バイトまで入力できます。
> - **Intelligent Slave** オプションは、**RS485** オプションで **Default** を選択したときに有効になります。

▼ Intelligent Slave オプションをサポートするデバイスとファームウェアバージョンを表示

- BioStation 3 Maxのファームウェアバージョン1.0.0以降
- XPass Q2のファームウェアバージョン1.0.0以降
- BioEntry W3 ファームウェア 1.0.0 以上
- BioStation 3 ファームウェア 1.0.0 以上
- X-Station 2 ファームウェア 1.1.0 以上
- FaceStation F2 ファームウェア 1.1.2 以上
- XPass 2 ファームウェア 1.2.3 以上
- BioLite N2 ファームウェア 1.4.1 以上
- BioEntry P2 ファームウェア 1.4.1 以上
- BioEntry W2 ファームウェア 1.6.3 以上
- BioStation L2 ファームウェア 1.6.1 以上

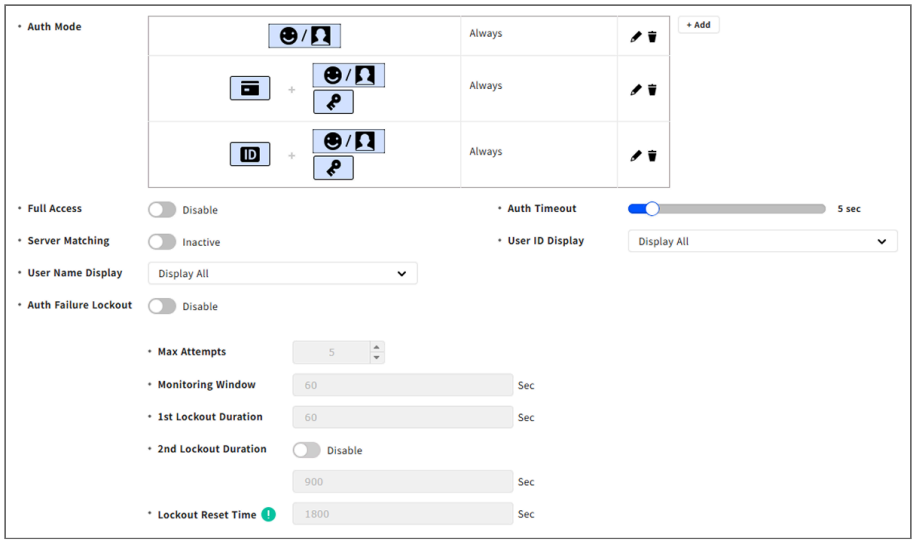
認証を設定する

デバイスのユーザー認証に関するさまざまな設定方法を案内します。 **Authentication** セクションでは、認証方式とデバイスがサポートする主要な認証オプションを段階的に確認します。設定を変更すると実際のデバイスに反映される点に留意し、各オプションの機能と注意事項を参照して環境に適した認証ポリシーを構成してください。

> **情報**
>
> - デバイスの種類によって設定できるネットワークオプションが異なる場合があります。
> - ユーザーが任意で変更した内容がある場合は、**Apply** をクリックします。変更内容を保存しないとデバイスに反映されません。

認証方法の設定

デバイスの認証モードと権限、サーバーマッチング、認証待機時間を設定できます。



- **Auth Mode**：1 つ以上のクレデンシャルを組み合わせてデバイスの認証モードを設定します。詳しくは認証モードを追加するをご覧ください。
  - 追加した認証モードを編集するには をクリックします。
  - をクリックして追加した認証モードを削除します。
- **Full Access**：デバイスに登録されたユーザーに出入グループ設定なしですべての出入権限を付与できます。

> **情報**
>
> このオプションを **Use** に設定すると、**Access Level** および **Floor Level** にデバイスを登録できません。

- **Auth Timeout**：**Auth Mode** オプションで複数のクレデンシャルを組み合わせて使用する場合、2 番目のクレデンシャルを認証するまでの待機時間です。指定した時間内にクレデンシャルを認証しない場合、認証に失敗します。
- **Server Matching**
  - **Active**：サーバーマッチング機能を有効にします。 **BioStar X**をインストールしたサーバーに保存されているユーザー情報を使用して認証を行うサーバーマッチング機能を設定してください。
  - **Inactive**：サーバーマッチング機能を無効にします。この場合、デバイスに登録されているユーザー情報で認証を行います。

> **▼ Server Matching 機能に対応するデバイスとファームウェアバージョンを表示**
> - BioStation 3 Maxのファームウェアバージョン1.0.0以降

  - XPass Q2のファームウェアバージョン1.0.0以降
  - BioEntry W3 ファームウェア 1.0.0 以上
  - BioStation 3 ファームウェア 1.0.0 以上
  - X-Station 2 ファームウェア 1.0.0 以上
  - FaceStation F2 ファームウェア 1.0.0 以上
  - XPass 2 ファームウェア 1.0.0 以上
  - BioLite N2 ファームウェア 1.0.0 以上
  - XPass D2 ファームウェア 1.0.0 以上
  - BioEntry P2 ファームウェア 1.0.0 以上
  - FaceStation 2 ファームウェア 1.4.0 以上
  - BioEntry W2 ファームウェア 1.0.0 以上
  - BioStation L2 ファームウェア 1.0.0 以上
  - BioStation A2 ファームウェア 1.0.0 以上
  - BioStation 2 ファームウェア 1.2.0 以上
  - CoreStation ファームウェア 1.0.0 以上
  - FaceLite はサーバーマッチング機能をサポートしていません。
  - BioStation 3、BioEntry W3、FaceStation F2 の各デバイスは顔認証のサーバーマッチング機能をサポートしていません。

- **Face Detection Level**：ユーザーが認証するときにデバイスに内蔵されたカメラで顔を検出するアルゴリズムレベルを設定してください。
  - **Normal**：腕の長さ程度の距離から顔を検出できます。
  - **High**：腕の長さより近づく必要があり、顔を検出できます。
  - **Not Use**：顔検出機能を使用しません。

> **情報**
> このオプションは BioStation A2 モデルでサポートされています。

- **User ID Display**：認証成功時にデバイスに表示されるユーザーIDを表示または非表示にできます。
  - **Display All** / **Mask All but First Letter** / **Hide All**
- **User Name Display**：認証成功時にデバイスに表示されるユーザー名を表示または非表示にできます。
  - **Display All** / **Mask All but First Letter** / **Hide All**
- **Auth Failure Lockout**：短時間に認証に繰り返し失敗すると、一定時間デバイスをロックして総当たり攻撃を遮断します。このオプションを **Enable** に設定すると、以下の項目を設定できます。デフォルトは **Disable** です。
  - **Max Attempts**：デバイスをロックするまでに許容する認証失敗回数を 3~15回の範囲で設定してください。デフォルトは5回です。
  - **Monitoring Window**：認証失敗回数を累積して計算する時間を 30~300秒の範囲で設定してください。デフォルトは60秒です。

- **1st Lockout Duration**：認証失敗回数が **Max Attempts** に達したときにデバイスをロックする時間を 30~900秒の範囲で設定してください。デフォルトは60秒です。値の入力が必須です。
- **2nd Lockout Duration**: 1次ロックが解除された後も認証失敗が繰り返される場合に適用する2次ロック時間です。このオプションを **Use** に設定すると、900~3,600秒の値を入力できます。デフォルトは900秒です。

  > このオプションを **Disable** に設定すると、2次ロックなしで1次ロックのみを繰り返し適用します。

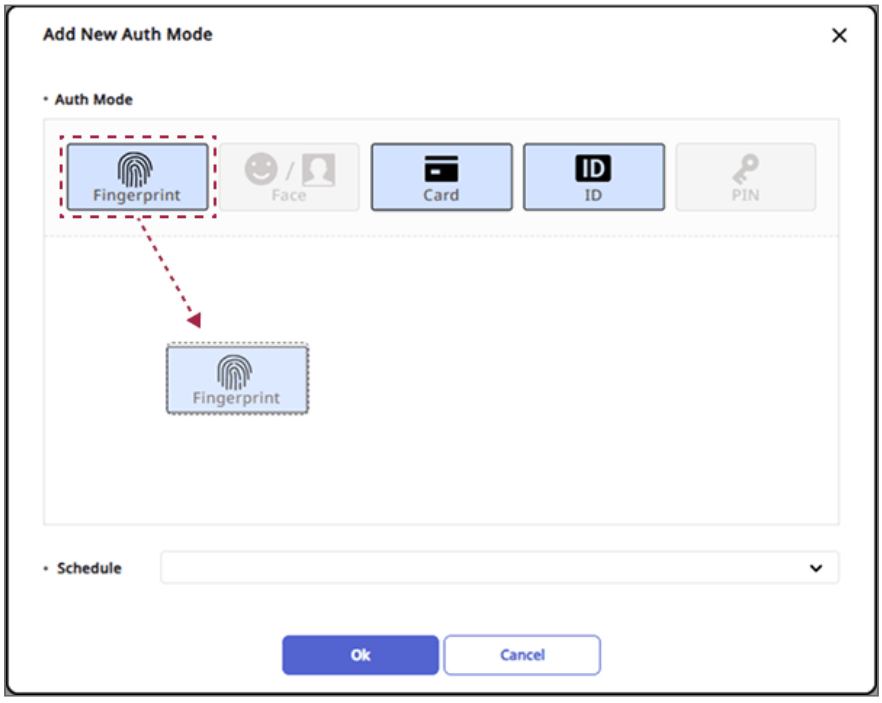
- **Lockout Reset Time**：最後の認証失敗後、この時間内に追加の失敗がなければ、累積失敗回数を初期化します。600~3,600秒の範囲で設定してください。デフォルトは1,800秒です。

> **情報**
>
> - デバイスが現在ロック状態の場合、**Auth Failure Lockout**を**Disable**に変更して保存すると、デバイスは直ちにロックを解除します。ただし、**2nd Lockout Duration**を**Disable**に変更して保存しても、デバイスはロックを解除しません。
> - **Auth Failure Lockout** オプションは BioStation 3 のファームウェア 1.5.0 以降でサポートされています。

認証モードを追加する

Auth Mode オプションでデバイスの認証モードを設定してください。指紋、ID、カード、PIN、顔などのクレデンシャルを組み合わせて認証モードを設定できます。

1. **Auth Mode** オプションで ＋ **Add** ボタンをクリックしてください。
2. **Add New Auth Mode** ウィンドウが表示されたら、希望する認証モードを中央エリアへドラッグしてください。



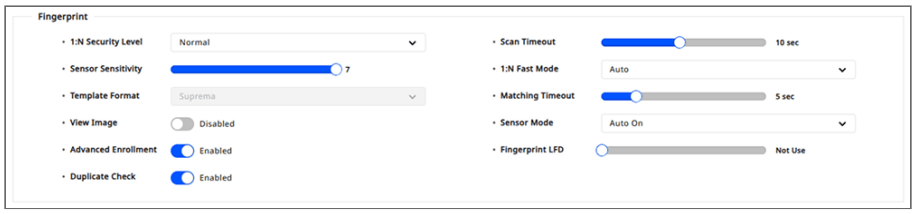
追加できる認証モードは最大5個までです。

3. **Schedule** オプションで希望の項目を選択してください。
4. すべての設定が完了したら、**Apply** ボタンをクリックしてください。

> **情報**
>
> **Schedule** オプションに希望のスケジュールがない場合は、＋ **Add New Schedule** をクリックしてください。新しいスケジュールを追加できます。スケジュール設定の詳細については、スケジュールを設定するをご参照ください。

指紋認証を設定する

Fingerprint グループでは、デバイスの指紋認証に関する詳細を設定できます。



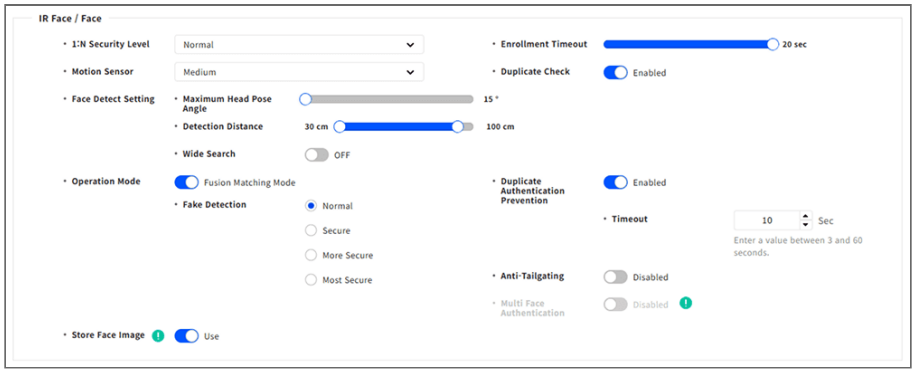
- **1:N Security Level**：指紋認証時に使用するセキュリティレベルを設定してください。セキュリティレベルを上げるほど、本人拒否率 (FRR) は高くなりますが、他人受入率 (FAR) は低くなります。
- **Scan Timeout**：指紋スキャンの待機時間を設定してください。設定した時間内に指紋をスキャンできない場合、認証は失敗します。
- **Sensor Sensitivity**：指紋センサーの感度を設定してください。より精密な指紋情報を取得するには、センサー感度を高く設定してください。
- **1:N Fast Mode**：指紋認証の速度を設定してください。 **Automatic** を選択すると、デバイスに登録されている指紋テンプレートの総数に応じて認証速度が設定されます。
- **Template Format**：設定されている指紋テンプレート形式を確認できます。
- **Matching Timeout**：指紋マッチングの待機時間を設定してください。設定した時間内に認証が完了しない場合、認証は失敗します。
- **View Image**：指紋認証時に画面に指紋画像を表示できます。
- **Sensor Mode**：指紋センサーの動作モードを設定してください。
  - **Auto On**：指紋センサーがユーザーの指を検知すると、センサーがオンになります。
  - **Always On**：指紋センサーが常にオンになっています。
- **Advanced Enrollment**：高品質の指紋情報を保存するために、スキャンした指紋の品質を検査できます。**Use**に設定すると、指紋品質が低い場合にユーザーへ通知し、正しくスキャンできるよう支援します。
- **Fingerprint LFD**：偽造指紋検出レベルを設定できます。偽造指紋検出レベルを高く設定すると、実際の指紋に対する拒否率も高くなる場合があります。
- **Duplicate Check**：指紋を登録する際に重複登録をチェックできます。

情報

- デバイスの種類によって設定できるオプションが異なる場合があります。
- 指紋認証設定で **Template Format** オプションを変更すると、以前に保存されたすべての指紋は使用できなくなります。ユーザーの指紋を登録する前に、必ず **Template Format** オプションでテンプレートを選択してください。
- **View Image** オプションは BioStation 3 Max (BS3M-ODB, BS3M-OAPB)、X-Station 2 (XS2-ODPB, XS2-OAPB)、FaceStation F2 (FSF2-ODB)、BioLite N2、BioStation L2、BioStation A2、BioStation 2 のモデルでサポートされています。
- **Fingerprint LFD** オプションは BioStation 3 Max (BS3M-ODB, BS3M-OAPB)、X-Station 2 (XS2-ODPB, XS2-OAPB)、FaceStation F2 (FSF2-ODB)、BioLite N2、BioStation L2、BioStation A2、BioEntry W2 のモデルでサポートされています。

顔認証の設定

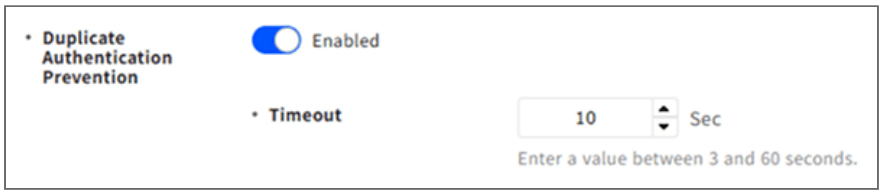
IR Face / Face または **Face** グループでは、デバイスの顔認証に関する詳細設定を行えます。



- **1:N Security Level**：顔を認証する際に使用するセキュリティレベルを設定します。セキュリティレベルを上げるほど、本人拒否率 (FRR) は高くなりますが、他人受入率 (FAR) は低くなります。
- **Enrollment Timeout**：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。
- **Motion Sensor**：デバイス周囲の動きを検知する感度を設定します。
- **Ambient Brightness**：デバイス周囲の明るさを検知して IR LED の強度を調整できます。
- **Enhanced fake face enrollment block**：偽造顔検出レベルを設定します。偽造顔検出レベルを高く設定すると、実際の顔に対する拒否率も高くなる場合があります。
- **Light Brightness**：デバイス照明の明るさを手動で調整できます。 **Normal** または **High** で明るさを設定するか、 **Not Use** を選択して照明をオフにできます。
- **Quick Enrollment**：クイック顔登録の使用有無を設定します。
  - **Enable**：顔登録手順をワンステップに設定します。
  - **Disabled**：顔登録手順を3段階に設定します。高品質の顔テンプレートを登録する場合は、**Disabled** に設定します。
- **Duplicate Check**：顔を登録する際に重複登録をチェックできます。
- **Face Detect Setting**：顔を認証する際の顔認識環境を設定します。
  - **Maximum Head Pose Angle**：許容される顔の最大回転角度を設定します。
  - **Detection Distance**：顔を認識する最小および最大距離を設定します。

  - **Wide Search**：カメラ映像全体で顔を認識する場合は **ON** に設定します。

- **Operation Mode**：顔を認証する際のデバイスの動作モードを設定します。
  - **Fusion Matching Mode**：ビジュアルと赤外線の両方でマッチングを行い、顔認証の精度を高めます。
  - **Fast Matching Mode**：デバイスの認証範囲内でユーザーが歩きながらでも顔認証を行えるよう、高速で認証を実行します。
- **Fake Detection**：写真などによる偽造顔を利用したユーザー認証を防止できます。 **Operation Mode** オプションを **Fusion Matching Mode** に設定すると有効になります。
- **Store Face Image**：顔の実際の画像と特徴情報のみを抽出したテンプレートを保存します。実際の画像を保存しない場合は、この設定を無効にしてください。
- **Duplicate Authentication Prevention**：同じユーザーの顔が短時間に再度検知された場合、重複して認証しないように設定してください。 **Enable** に設定すると、**Timeout** を 3~60秒の範囲で設定できます。



> この設定は、**Anti-Tailgating** と **Multi Face Authentication** のどちらを使用しても共通で適用されます。

- **Anti-Tailgating**：デバイスカメラの撮影範囲内で2人以上の顔を同時に検知すると、共連れと判断して認証を中断します。
- **Multi Face Authentication**：デバイスカメラの撮影範囲内にいる複数のユーザーの顔を順番に認証します。

> - このオプションを使用するには、別途デバイスライセンスが必要です。ライセンスがないデバイスでは、このオプションを使用に設定できません。詳しくはデバイスライセンスをご覧ください。
> - このオプションを **Use** に設定すると、デバイスに設定された **Auth Mode** に関係なく、顔認証専用で動作します。
> - このオプションを使用するデバイスでは、**T&A**および**Server Private Message**機能は使用できません。

情報

- デバイスの種類によって設定できるオプションが異なる場合があります。
- **Ambient Brightness**、**Enhanced fake face enrollment block**、**Quick Enrollment** の各オプションは FaceStation 2、FaceLite モデルでサポートされています。
- **Light Brightness** オプションは FaceStation F2 ファームウェア 1.1.0 以降のモデルでサポートされています。
- **Face Detect Setting**, **Operation Mode** オプションは BioStation 3 Max、BioStation 3、FaceStation F2 のモデルでサポートされています。
- **Anti-Tailgating** と **Multi Face Authentication** は同時に **Use** に設定できません。一方のオプションを **Use** に設定すると、もう一方のオプションは自動的に **Not Use** に切り替わります。
- **Duplicate Authentication Prevention** と **Multi Face Authentication** オプションを設定できるのはマスターデバイスのみです。 **Anti-Tailgating** オプションは、マスターデバイスとスレーブデバイスでそれぞれ設定できます。
- **Duplicate Authentication Prevention**、**Anti-Tailgating**、**Multi Face Authentication** オプションは、デバイスの種類およびファームウェアのバージョンによってサポート状況が異なる場合があります。
  - BioStation 3 ファームウェア バージョン 1.5.0以降

QR/バーコード設定

QR/Barcode グループでは、デバイスの QR/バーコード認証に関する詳細設定を行えます。



- **Use QR/Barcode through Camera** / **Use QR/Barcode**：デバイスのカメラでのQR/バーコード認証を使用するかどうかを設定します。
- **Camera Timeout** / **Scan Timeout**：カメラのスキャン待機時間を設定します。設定した時間内に QR/バーコードをスキャンしないと、認証に失敗します。
- **Use QR as Card**：ユーザーに発行した 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します。
- **Motion Sensor**：動きを検知してカメラのスキャンを開始する感度を設定します。
- **Use QR/Barcode through Scanner**：デバイスのスキャナーによるQR/バーコード認証の使用可否を設定します。
- **Scanner Timeout**：スキャン待機時間を設定します。設定した時間内に QR/バーコードをスキャンしないと、認証に失敗します。
- **LED Light**：QRコード認証時にデバイスのLED照明を使用するかどうかを設定します。

情報

- **Use QR/Barcode through Camera** オプションを使用するには、別途デバイスライセンスが必要です。詳しくはデバイスライセンスをご覧ください。
- **Use QR/Barcode through Camera**、**Camera Timeout**、**Use QR as Card**、**Motion Sensor** オプションに対応しているデバイスは以下のとおりです。
  - BioStation 3 Maxのファームウェアバージョン1.0.0以降
  - BioStation 3 ファームウェア バージョン 1.1.0以降
  - X-Station 2 (XS2-ODPB, XS2-OAPB, XS2-DPB, XS2-APB) ファームウェア 1.2.0 以上
  - X-Station 2 (XS2-QDPB, XS2-QAPB) ファームウェア 1.4.1 以上
- 以下のデバイスが **Use QR/Barcode through Scanner** および **Scanner Timeout** オプションに対応しています。
  - X-Station 2 (XS2-QDPB, XS2-QAPB)
- **Use QR/Barcode**、**Scan Timeout**、**LED Light** のオプションに対応しているデバイスは以下のとおりです。
  - XPass Q2のファームウェアバージョン1.0.0以降

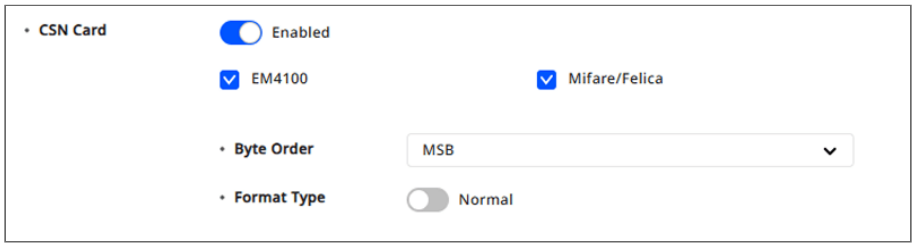
カード認証設定

Card Type グループでデバイスが使用するカードタイプを設定します。

情報
デバイスがサポートするカードタイプのみが **Card Type** グループに表示されます。

CSN Card

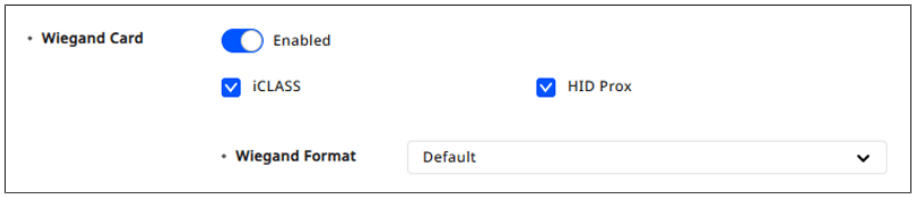
CSNカードとフォーマットの種類を選択し、バイト順序を設定します。



- **Byte Order**
  - **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。
- **Format Type**
  - **Normal**：カードのシリアル番号 (CSN) を変換せずにそのまま読み取って表示します。
  - **Wiegand**：ユーザーが定義した Wiegand 形式に従ってカードシリアル番号 (CSN) を変換して表示します。新しい Wiegand 形式を設定するには、Wiegandカード形式を設定するを参照してください。

Wiegand Card

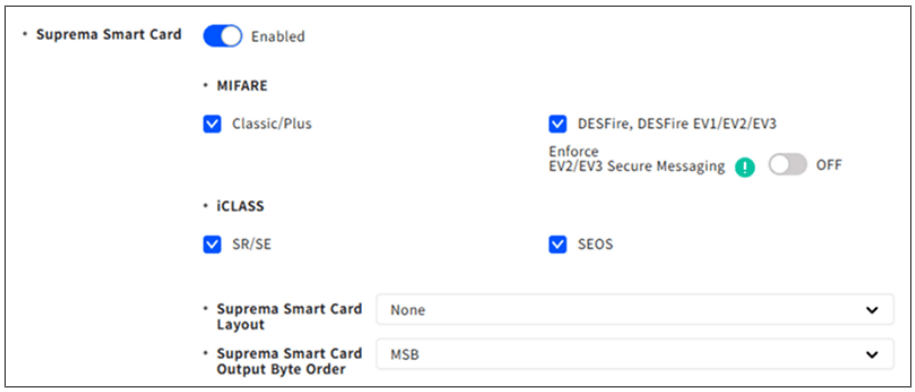
Wiegand カードの種類を選択し、Wiegand 形式を設定します。 **Wiegand Format** オプションで使用する Wiegand 形式を選択します。



> **情報**
> 新しい Wiegand 形式を設定するには、Wiegandカード形式を設定するを参照してください。

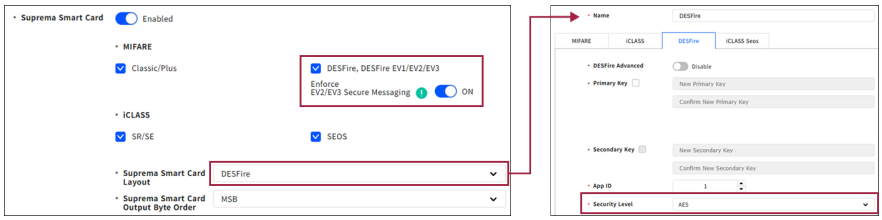
Suprema Smart Card

Suprema スマートカードの種類を選択し、カードレイアウトとバイト順序を設定します。



- **Enforce EV2/EV3 Secure Messaging**: このオプションを**ON**に設定すると、認証はEV2セキュアメッセージングに対応するカード（DESFire EV2/EV3）に限られます。デバイスは、EV2セキュアメッセージングに対応しないDESFire EV1カードの認証を拒否します。

  このオプションは、**DESFire, DESFire EV1/EV2/EV3**を選択し、選択した**Suprema Smart Card**の**Security Level**が**AES**の場合に有効になります。**Suprema Smart Card**を使用しない場合、このオプションは**OFF**状態で表示されます。

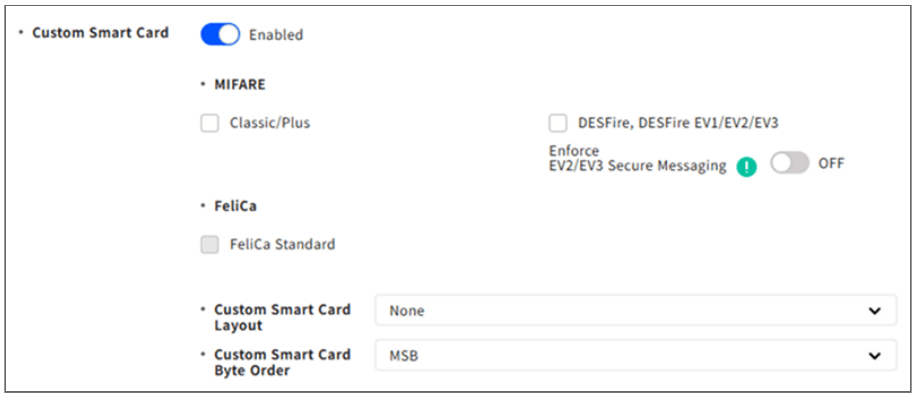


- **Suprema Smart Card**と**Custom Smart Card**は設定値を共有しています。どちらか一方でも使用中の場合、どちらかの値を変更すると確認メッセージが表示されます。メッセージウィンドウで **Ok** ボタンをクリックすると、二つのオプションが同時に変更されます。片方でスマートカードを使用していない場合、確認メッセージなしで値を変更できます。
- セキュアメッセージングは、DESFire EV2およびEV3カードでのみ使用できます。使用するには、DESFireを有効にし、カードレイアウトの暗号化の種類をAESに設定してください。
- デバイスがEV2セキュアメッセージング機能をサポートしない場合、**Enforce EV2/EV3 Secure Messaging**オプションは表示されません。
- 複数のデバイスを選択し、**Device Batch Edit**でこのオプションを設定することもできます。一括編集では、EV2セキュアメッセージングに対応しないデバイスを自動的に除外します。

- **Suprema Smart Card Layout**：Suprema スマートカードレイアウトを選択します。詳しくはスマートカード形式を設定するをご覧ください。
- **Suprema Smart Card Output Byte Order**
  - **MSB**：カードデータを大きいバイト単位から小さいバイト単位の順に処理します。
  - **LSB**：カードデータを小さいバイト単位から大きいバイト単位の順に処理します。

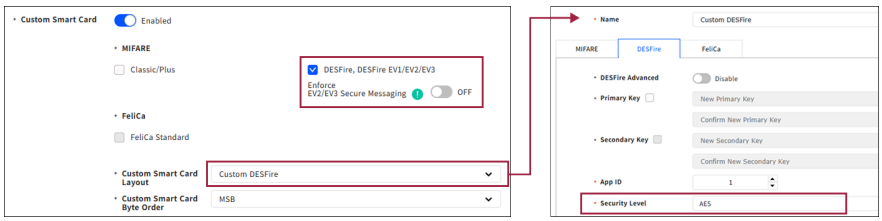
Custom Smart Card

他社が発行したカスタムスマートカードの種類を選択し、カードレイアウトとバイト順序を設定します。



- **Enforce EV2/EV3 Secure Messaging**: このオプションを**ON**に設定すると、認証はEV2セキュアメッセージングに対応するカード（DESFire EV2/EV3）に限られます。デバイスは、EV2セキュアメッセージングに対応しないDESFire EV1カードの認証を拒否します。

  このオプションは、**DESFire, DESFire EV1/EV2/EV3**を選択し、選択した**Custom Smart Card**の**Security Level**が**AES**の場合に有効になります。**Custom Smart Card**を使用しない場合、このオプションは**OFF**状態で表示されます。



- **Suprema Smart Card**と**Custom Smart Card**は設定値を共有しています。どちらか一方でも使用中の場合、どちらかの値を変更すると確認メッセージが表示されます。メッセージウィンドウで **Ok** ボタンをクリックすると、二つのオプションが同時に変更されます。片方でスマートカードを使用していない場合、確認メッセージなしで値を変更できます。
- セキュアメッセージングは、DESFire EV2およびEV3カードでのみ使用できます。使用するには、DESFireを有効にし、カードレイアウトの暗号化の種類をAESに設定してください。
- デバイスがEV2セキュアメッセージング機能をサポートしない場合、**Enforce EV2/EV3 Secure Messaging**オプションは表示されません。
- 複数のデバイスを選択し、**Device Batch Edit**でこのオプションを設定することもできます。一括編集では、EV2セキュアメッセージングに対応しないデバイスを自動的に除外します。

- **Custom Smart Card Layout**：カスタムスマートカードレイアウトを選択します。詳しくはスマートカード形式を設定するをご覧ください。
- **Custom Smart Card Byte Order**
  - **MSB**：カードデータを大きいバイト単位から小さいバイト単位の順に処理します。
  - **LSB**：カードデータを小さいバイト単位から大きいバイト単位の順に処理します。

▼ カスタムスマートカードをサポートするデバイスとファームウェアバージョンを表示

- BioStation 3 Max ファームウェア 1.3.0 以上
- XPass Q2のファームウェアバージョン1.0.0以降
- BioEntry W3 ファームウェア 1.0.0 以上
- BioStation 2a ファームウェア 1.1.0 以上
- BioStation 3 ファームウェア 1.3.0 以上
- X-Station 2 ファームウェア 1.3.0 以上
- BioLite N2 ファームウェア 1.6.2 以上
- XPass D2 ファームウェア 1.7.1 以上
- BioEntry P2 ファームウェア 1.5.1 以上
- BioEntry W2 ファームウェア 1.8.0 以上

CSN Mobile

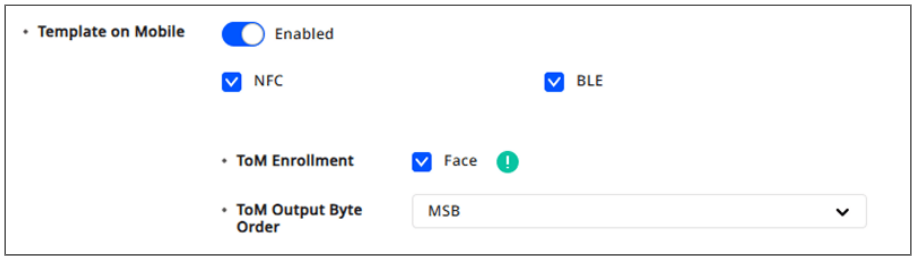
モバイルカードの認識方法を設定します。



- **NFC**：モバイル機器で NFC 通信を使用してモバイルカードを認識します。
- **BLE**：低電力 Bluetooth (Bluetooth Low Energy、BLE) 通信を使用してモバイルカードを認識します。

Template on Mobile

テンプレートオンモバイルの認識方法と、ユーザーがデバイスで直接登録するバイオメトリクスを指定し、バイト順序を設定します。



- **ToM Output Byte Order**
  - **MSB**：カードデータを大きいバイト単位から小さいバイト単位の順に処理します。
  - **LSB**：カードデータを小さいバイト単位から大きいバイト単位の順に処理します。

▼ テンプレートオンモバイルをサポートするデバイスとファームウェアバージョンを表示

- BioStation 3 Maxのファームウェアバージョン1.0.0以降
- BioEntry W3 ファームウェア 1.0.0 以上
- BioStation 3 ファームウェア 1.2.0 以上

PIN認証設定

PIN グループでは、デバイスのPIN認証に対して **Scramble Keypad** オプションをオンまたはオフに設定します。



情報

Scramble Keypad オプションは、LCD画面のユーザーインターフェースに対応するSuprema製品でのみ使用できます。

高度設定

Advanced セクションで設定できる項目について説明します。マスター管理者、管理権限管理、勤怠イベント、画面とサウンド、動作条件と動作、イメージログ、Wiegand、セキュリティタンパーなど、多彩な高度機能の設定方法と各オプションの意味を確認できます。環境に合わせた設定を適用し、デバイスを効率的に管理します。

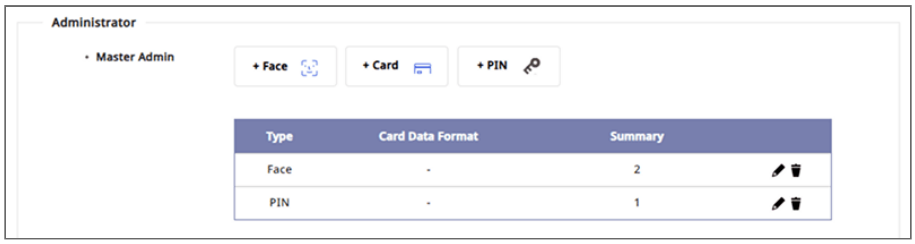
情報

- デバイスの種類によって設定できるネットワークオプションが異なる場合があります。
- ユーザーが任意で変更した内容がある場合は、**Apply** をクリックします。変更内容を保存しないとデバイスに反映されません。

マスター管理者の追加 CE 製品

Master Admin 機能は、デバイスのフル管理権限を強化し、セキュリティを向上させて不正アクセスや設定変更を防止するための機能です。新しいデバイスでは、この機能を使用して必ずマスター管理者を登録する必要があり、登録されたマスター管理者のみが管理メニューにアクセスして設定を変更できます。

Advanced → **Administrator** の **Master Admin** メニューで、必要な 2 種類のクレデンシャルを選択して登録します。



Master Admin に登録できるクレデンシャルは次のとおりです。

クレデンシャルの種類	登録可能数	詳細条件
カード	最大 4 件	CSN と Wiegand タイプのみ対応し、同一タイプ内で重複登録はできません。
顔	最大 2 件	同じアルゴリズムを搭載したデバイスでのみ登録できます。
指紋	最大 2 件	-
PIN	1 件	8 桁以上の数字を入力できます。

- 登録済みのクレデンシャルを変更するには、該当クレデンシャルの右側にある ✎ ボタンをクリックします。
- 登録済みのクレデンシャルを削除するには、該当クレデンシャルの右側にある 🗑 ボタンをクリックします。

注意

この機能は **LCD 画面によるユーザーインターフェースに対応する Suprema 製品**のうち、**CE 製品**でのみ使用できます。サポート対象のデバイスおよびファームウェアバージョンの詳細については、Master Admin セットアップガイドを参照してください。

登録条件

- 少なくとも 2 種類以上のクレデンシャルを登録する必要があります。
- マスター管理者に対応するファームウェアをアップグレードしたデバイスにも、同じ条件が適用されます。
- デバイスがサポートするすべてのクレデンシャルを認証手段として使用できます。

情報

- この機能は LCD 画面を使ったユーザーインターフェースに対応する Suprema 製品でのみ利用できます。
- ファームウェアをアップグレードした既存のデバイスでは、**BioStar X** のデバイス設定に **Master Admin** メニューが表示されません。
- **Master Admin** 設定を提供しないデバイスのうち一部（例：ファームウェアアップグレードで当該機能が追加されたデバイス）は、**Two-step Authentication** オプションで全管理者の権限を強化できます。デバイスの種類によっては、**Two-step Authentication** オプション自体が表示されない場合があります。
- マスター管理者のクレデンシャルはデバイス内に別途保存され、一般ユーザーの PIN とは独立して管理されます。そのため、ユーザーの PIN を変更または削除しても、マスター管理者のクレデンシャルには影響しません。

2段階認証の設定

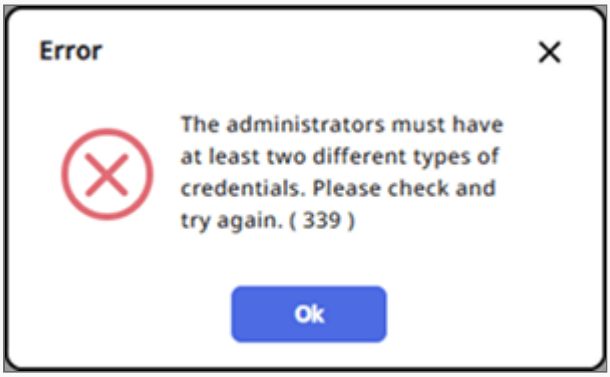
Master Adminをサポートしないグローバルデバイスでファームウェアをアップグレードした場合、**Two-step Authentication**オプションでフル管理者の権限を強化し、デバイスのセキュリティを向上させられます。



Two-step Authentication オプションを **Use** に設定すると、デバイスのフル管理者認証には2種類以上のクレデンシャルが必要になります。例として、カードとPINの両方を登録した場合、フル管理者の認証ではカードのスキャンとPINの入力の両方を行う必要があります。

情報

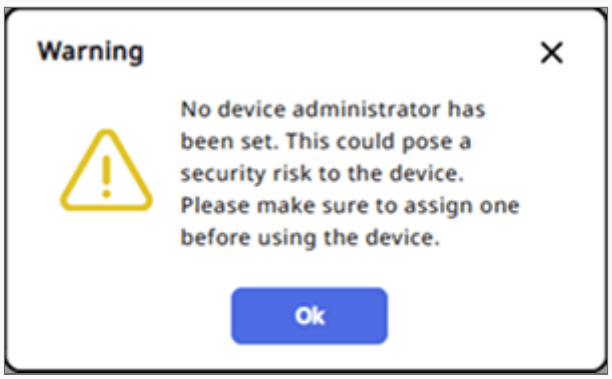
- すべての管理者に 2 種類以上のクレデンシャルが登録されていない場合、有効化に失敗し、エラーメッセージが表示されます。すべての管理者に 2 種類以上のクレデンシャルを登録してから、再試行してください。



- デバイスによっては、**Two-step Authentication** オプションが画面に表示されなくても、以前に有効化した設定が維持される場合があります。この場合、**BioStar X** で無効化できないため、Suprema グローバル技術サポートチームにお問い合わせください。

注意

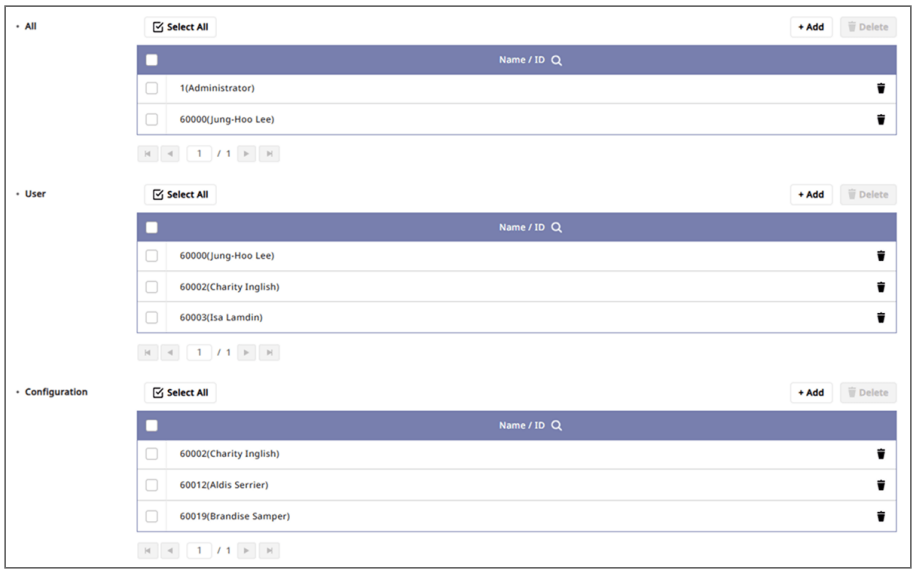
デバイスにフル管理者が設定されていない場合、次のようなポップアップメッセージが表示されます。 **Advanced** → **Administrator** で、すべての権限に管理者を追加してください。



> **警告**
>
> **Two-step Authentication** を有効にした後にすべての管理者のクレデンシャルを2種類未満に削除すると、**BioStar X** に接続できない状況下ではデバイスから管理者メニューにアクセスできなくなります。そのため、管理者クレデンシャルを削除する際は十分に注意してください。

管理者追加

Administrator グループでデバイス管理者を階級別に管理します。



権限レベル別の管理者を追加するには、**+ Add** をクリックしてください。ユーザー一覧が表示されたら、目的のユーザーを選択してください。ユーザー一覧で 🔍 をクリックすると、目的のユーザーを検索することもできます。

各階級の権限は以下を参照します。

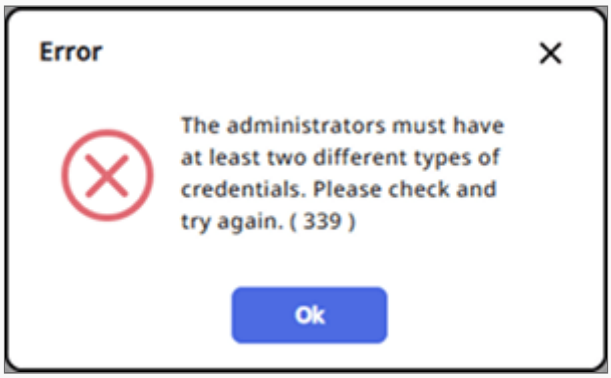
階級	ユーザー情報管理	デバイス設定
All	✔	✔
User	✔	✕
Configuration	✕	✔

情報

- 管理者を最大1,000人まで追加して管理します。追加できる管理者数はデバイスのファームウェアバージョンによって異なる場合があります。
- 登録済みユーザーを検索するには、**Name / ID** で 🔍 をクリックしてください。
- **デバイス設定**でデバイスの画面や音声、ネットワーク、RS-485 などの設定を変更します。
- 管理者を削除するには、該当管理者の右側にある 🗑 をクリックします。
- 各デバイスに設定された管理者は **BioStar X** の権限に影響しません。
- マスター管理者に対応するデバイス（**CE 製品**）で、デバイス管理者として登録したユーザーの PIN が 8 桁未満の場合、そのユーザーの PIN を 8 桁以上で再登録する必要があります。 PIN 登録の詳細については PINを登録するを参照してください。
- **Configuration** 権限が付与されたユーザーの PIN を 4 桁に変更するには、まずすべてのデバイスの管理者権限から除外してください。

注意

デバイス管理者に設定するユーザーに登録されているクレデンシャルが 2 種類未満の場合、エラーメッセージが表示されます。すべてのデバイス管理者に 2 種類以上のクレデンシャルを登録してから、再試行してください。



削除されたユーザーの管理者登録の処理

デバイスに登録されている管理者のうち **BioStar X** ですでに削除されたユーザーがいる場合、デバイス設定を保存するために画面最下部の **Apply** ボタンをクリックすると、次のポップアップが表示されます。

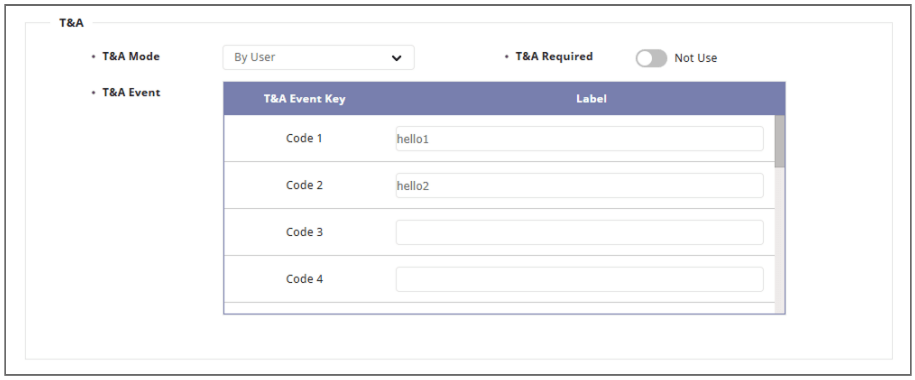


- **Yes**: 削除されたユーザーを管理者リストから削除して保存します。

- **No**: 保存をキャンセルします。

勤怠管理

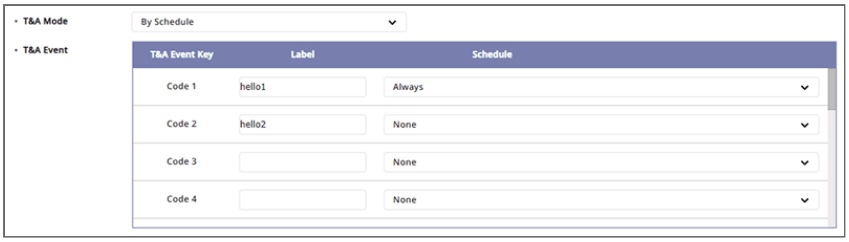
T&A グループでデバイスの勤怠イベント名を変更したり、勤怠モードを設定します。



- **T&A Mode**：勤怠イベントの登録方法を設定します。
  - **Not Use**：勤怠イベントを記録できません。
  - **By User**：ユーザーが認証時に希望する勤怠イベントを選択できます。
  - **By Schedule**：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。
  - **Last Choice**：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。
  - **Fixed**：選択した勤怠イベントのみを使用できます。固定で使用する勤怠イベントを選択します。
- **T&A Required**：ユーザーが認証する際に必ず勤怠イベントを登録するように設定します。

> このオプションは、**T&A Mode** オプションが **By User** に設定されている場合に使用できます。

- **T&A Event**：勤怠イベント名を修正したり、**T&A Mode** オプションを **By Schedule** に設定した際に使用するスケジュールを追加します。
  - **T&A Event Key**：勤怠登録に使用できるキーの一覧です。
  - **Label**：**T&A Event Key** に対応する勤怠イベント名を変更できます。
  - **Schedule**：**T&A Mode** オプションを **By Schedule** に設定した場合に自動で切り替えるスケジュールを設定します。



情報

- LCD 画面がないデバイスでは、勤怠モードを **Fixed** と **By Schedule** に設定でき、固定の勤怠イベントを登録するか、あらかじめ設定したスケジュールに応じて切り替わる勤怠イベントを登録できます。対応機種は XPass Q2、XPass 2、XPass D2、BioEntry P2、BioEntry W2 です。
- 新しいスケジュールの設定に関する詳細は、スケジュールを設定するをご参照ください。
- デバイスで **Multi Face Authentication** オプションを **Use** に設定すると、このデバイスは勤怠管理に使用できません。 **Multi Face Authentication** について詳しくは、認証を設定するを参照してください。

画面と音声の設定

デバイスの画面や音声に関する設定を変更します。デバイスによって設定できるオプションが異なる場合があります。

▼ XPass 2、XPass D2、BioEntry P2、BioEntry W2

- **Sound**：音声をオンまたはオフに切り替えます。
- **LED/Buzzer**：LED またはブザーを動作させるイベント項目を選択して設定します。
- **Keypad Backlight**：キーパッドバックライトをオンまたはオフに切り替えます。このオプションを有効にすると、キーパッド背面の照明が点灯します。暗い環境でもキーを簡単に識別できます。

Keypad Backlight オプションは XPass D2 ハードウェア V02M、ファームウェア 1.7.1 以降で使用できます。

▼ FaceLite、BioLite N2、BioStation L2、BioStation 2

- **Language**：デバイスの画面に表示する言語を設定します。デバイスに言語リソースファイルを送信するには、**Update Resource** をクリックします。
- **Device Volume**：デバイスで再生される基本音量を設定します。
- **Menu Timeout**：メニュー画面が待機画面に切り替わるまでの時間を設定します。
- **Theme**：デバイスのホーム画面スタイルを変更します。
- **Backlight Timeout**：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。
- **Message Timeout**：メッセージが自動で消えるまでの時間を設定します。
- **Voice Instruction**：通知音の代わりに音声ガイダンスを使用できます。
- **Background**：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。
  - **Logo**：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。 **Add** ボタンをクリックして、希望する画像を登録します。
  - **Notice**：管理者が入力した内容をホーム画面に表示できます。
  - **Slide Show**：ユーザーが登録した最大10枚の画像をスライドショーとしてホーム画面に表示できます。 **Add** ボタンをクリックして、希望する画像を登録します。

> – **Update** ボタンをクリックして、変更内容をデバイスにリアルタイムで反映します。
> – 壁紙の種類を変更した場合、**Update** ボタンをクリックしてもデバイスに適用されません。画面下部の **Apply** ボタンをクリックします。
> – **Notice**、**Slide Show** オプションは BioStation 2 モデルでサポートされています。

- **Sound**：デバイスの起動、認証成功、認証失敗イベント時に再生する効果音を設定します。サイズが500KB以下の **.wav* ファイルを選択します。 **Browse** ボタンをクリックします。

> **Update** ボタンをクリックして、変更内容をデバイスにリアルタイムで反映します。

▼ **BioStation 3 Max、BioStation 3、X-Station 2、FaceStation F2、FaceStation 2、BioStation A2**

- **Language**：デバイスの画面に表示する言語を設定します。デバイスに言語リソースファイルを送信するには、**Update Resource** をクリックします。
- **Device Volume**：デバイスで再生される基本音量を設定します。
- **Intercom Speaker Volume**：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される音量を設定します。
- **Intercom Microphone Volume**：IP インターホン機能を使用するときにデバイスへ入力される音量を設定します。
- **Menu Timeout**：メニュー画面が待機画面に切り替わるまでの時間を設定します。
- **Backlight Timeout**：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。
- **Message Timeout**：メッセージが自動で消えるまでの時間を設定します。
- **Server Private Message**：ユーザーが認証する際に画面に表示する個人メッセージの使用有無を設定できます。

> デバイスで **Multi Face Authentication** オプションを **Use** に設定すると、このオプションを使用できません。 **Multi Face Authentication** について詳しくは、認証を設定するを参照してください。

- **Voice Instruction**：通知音の代わりに音声ガイダンスを使用できます。
- **Home Screen**：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。
  - **Normal**：既定の画像をホーム画面に表示します。
  - **Logo**：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。 **Add** ボタンをクリックして、希望する画像を登録します。
  - **Notice**：管理者が入力した内容をホーム画面に表示できます。

> – **Update** ボタンをクリックして、変更内容をデバイスにリアルタイムで反映します。
> – 壁紙の種類を変更した場合、**Update** ボタンをクリックしてもデバイスに適用されません。画面下部の **Apply** ボタンをクリックします。
> – ホーム画面を **Logo** に設定し、**Slide Show** に設定すると、最大10枚の画像をスライドショーとしてホーム画面に表示できます。 **Add** ボタンをクリックして、希望する画像を登録します。

- **Sound**：デバイスの起動、認証成功、認証失敗イベント時に再生する効果音を設定します。サイズが500KB以下の **.wav* ファイルを選択します。 **Browse** ボタンをクリックします。

> **Update** ボタンをクリックして、変更内容をデバイスにリアルタイムで反映します。

- **Default Idle Screen**: デバイスを使用しない時間に画面に表示する待機画面を選択できます。
  - **Screen Saver**: スクリーンセーバーを待機画面として表示します。
  - **Home Screen**: **Home Screen** オプションで選択した内容を表示します。

> - このオプションは BioStation 3 Max、BioStation 3、X-Station 2、FaceStation F2、FaceStation 2 のモデルでサポートされています。
> - **Play Video** オプションの詳細は待機画面で動画を再生をご参照ください。

▼ XPass Q2

LED/Buzzer：LED またはブザーを動作させるイベント項目を選択して設定します。

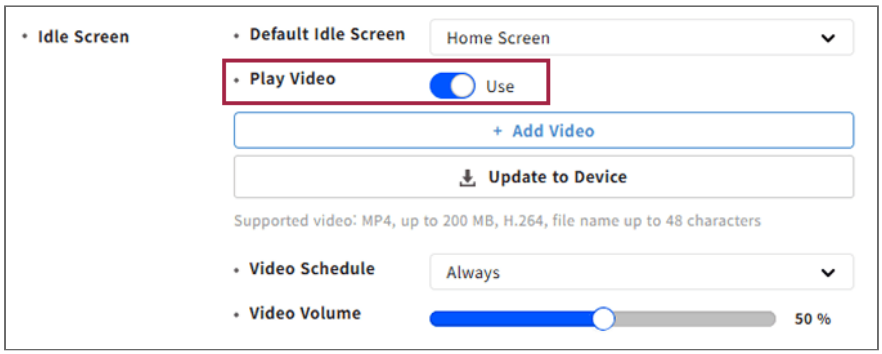
待機画面で動画を再生

> 待機画面で動画を再生する機能は、**BioStation 3 Max** のファームウェア 1.1.0 以降に対応しています。動画をデバイスに転送する前に準備してください。

動画の追加とデバイスへの転送

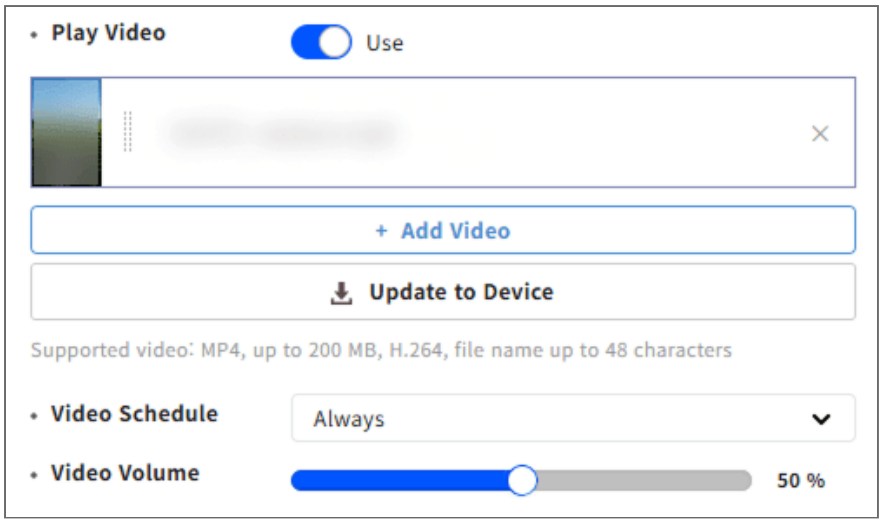
デバイスの待機画面で任意のコンテンツを再生するよう設定できます。

1. **Launcher**ページで**Settings**をクリックします。
2. 画面左のサイドバーで **Device** → **Device** をクリック。
3. デバイス一覧で BioStation 3 Max をクリックします。
4. **Advanced** → **Display/Sound** セクションに移動します。
5. **Idle Screen** → **Play Video** オプションを **Use** に設定します。



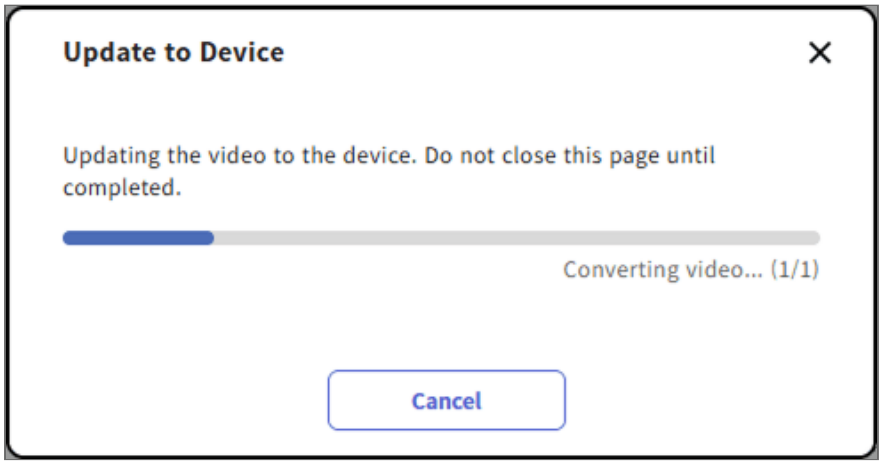
6. **Add Video** ボタンをクリックします。
7. ローカルに保存された動画を選択します。

8. 動画がアップロードされたら、**Video Schedule**と **Video Volume**を設定します。

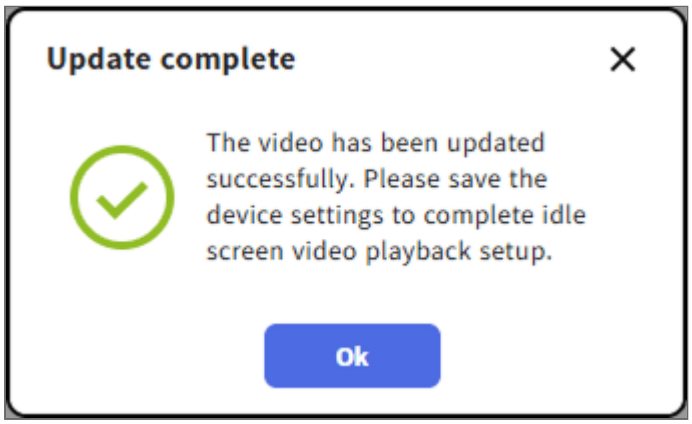


9. アップロードした動画をデバイスに転送するには、**Update to Device** ボタンをクリックします。

10. 更新の進行状況ポップアップが表示されます。アップロードが完了するまでページを閉じないでください。



11. アップロード完了メッセージが表示されたら、**Ok** ボタンをクリックします。



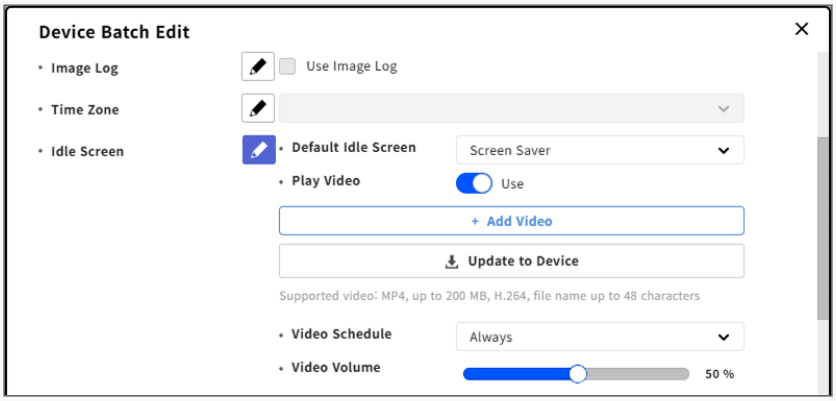
12. 変更内容を保存するには、画面最下部の **Apply** ボタンをクリックします。

情報

- 動画は、**Video Schedule** オプションで指定したスケジュールに従い、**Play Video** が **Use** に設定され、かつ動画が 1 件以上登録されている場合にのみ再生されます。この条件を満たさないスケジュールでは、**Default Idle Screen** で選択した画面が表示されます。
- 対応する動画ファイルのサイズは最大 200MB で、ファイル形式は MP4（H.264）です。
- 動画ファイル名の長さは最大 48 文字です。ファイル名にピリオド（`.`）、シングルクォーテーション（`'`）、バッククォート（`` ` ``）などの文字が含まれている場合、追加できません。
- 動画は最大 3 件まで追加できます。動画を 3 件まで追加すると、**Add Video** ボタンは無効になります。
- デバイスがスレーブとして接続されている場合（RS-485 で接続されている場合）、動画を追加、削除、または転送できません。
  - マスターデバイスが動画再生機能に対応している場合、スレーブ画面にはマスターデバイスに登録された動画リストが参照専用で表示されます。リストは確認のみです。追加、削除、転送、順序変更はマスターデバイスでのみ行います。
  - マスターデバイスが動画再生機能に対応していない場合、スレーブ画面には動画リストが表示されず、**Default Idle Screen** オプションのみ表示されます。

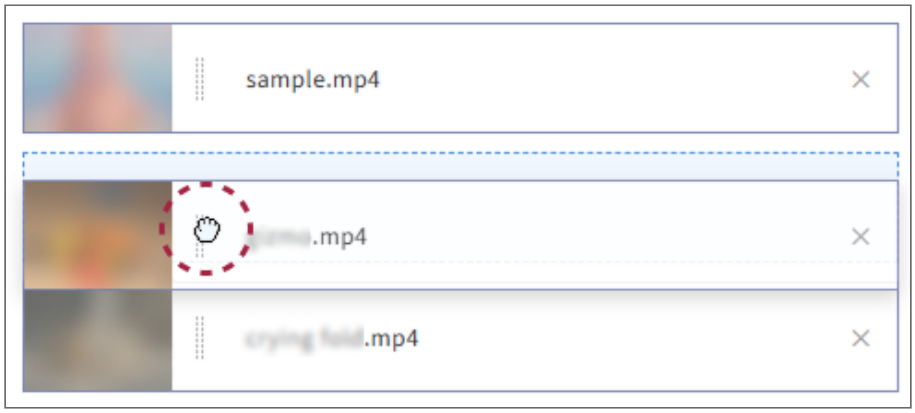
ヒント

Batch Edit 機能で、複数のデバイスに動画を一度に追加して転送できます。**Batch Edit**の機能の詳細については、デバイス管理機能を利用するをご参照ください。



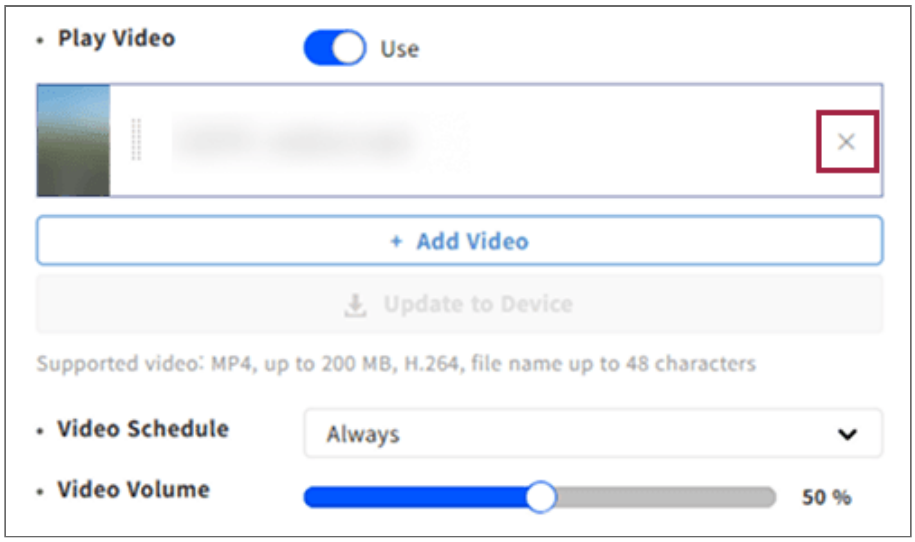
動画の再生順序の変更

動画サムネイルの右側領域をクリックしたままドラッグして、再生順序を変更してください。順序を変更した後、変更内容を保存するには、画面最下部の **Apply** をクリックします。



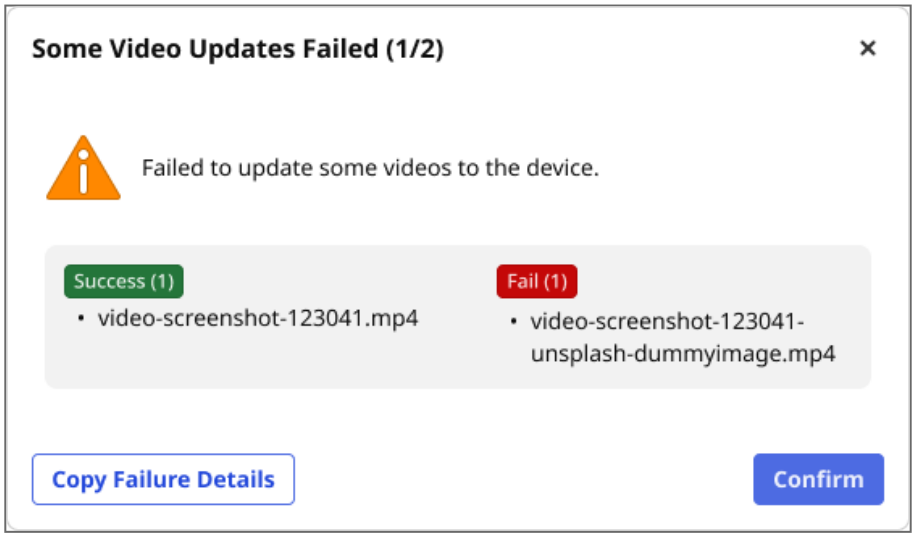
動画の削除

アップロードした動画を削除するには、**Idle Screen** → **Play Video** で、削除する動画の ✕ ボタンをクリックします。その後、**Update to Device** ボタンをクリックしてください。変更内容を保存するには、画面最下部の **Apply** ボタンをクリックします。



動画の転送失敗

動画のデバイスへの送信に失敗すると、ポップアップが失敗した動画名を表示します。



転送に失敗する主な原因は次のとおりです。

- デバイスの応答処理中にエラーが発生した場合
- 上記の理由に該当しないその他のエラーが発生した場合

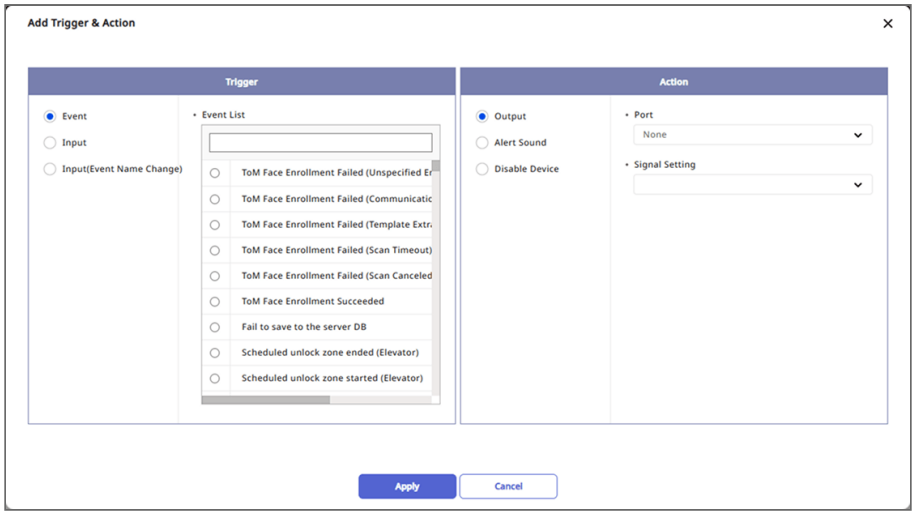
> **ヒント**
> **Batch Edit** 機能で複数のデバイスに動画を一括送信した際に、一部のデバイスだけ失敗した場合は、結果ポップアップで **Copy Failure Details** ボタンをクリックして、失敗したデバイスの一覧と理由をクリップボードにコピーします。

作業条件と動作の設定

Trigger & Action グループでは、各状況に応じた作業条件と動作を設定できます。例えば、認証に失敗したときにすべてのアラー

ムを鳴らす、または RS-485 接続が切断されたときにデバイスを使用できないように設定できます。

作業条件と動作は、イベントを選択して登録することも、ユーザーが任意の条件や動作を設定することもできます。 **Trigger & Action** グループの右側で ＋ **Add** ボタンをクリックします。



Trigger

あらかじめ設定されたイベントを選択するか、ユーザー定義の条件を追加できます。

- **Event**：あらかじめ設定されたイベントを選択します。
- **Input**：オプション内の各項目を選択してユーザー定義の条件を設定します。
- **Input(Event Name Change)**：オプション内の各項目を選択してユーザー定義の条件を設定します。入力に対する動作を伴わずに入力のみを検知するように設定できます。

> **情報**
>
> - **Trigger** を **Event** に設定した場合、イベントリストから 1 つのイベントしか選択できません。
> - **Input** または **Input(Event Name Change)** オプションを選択してカスタム条件を設定する際に希望するスケジュールがない場合は、**+ Add Schedule** をクリックします。スケジュール設定の詳細については、スケジュールを設定するをご参照ください。
> - **Input(Event Name Change)** オプションを選択してカスタム条件を設定する際に目的のイベント名がない場合は、**Add Event Name** をクリックします。該当イベントが発生すると、イベントログおよびリアルタイムログに設定したイベント名が表示されます。
> - イベント名は最大 64 文字まで入力できます。

Action

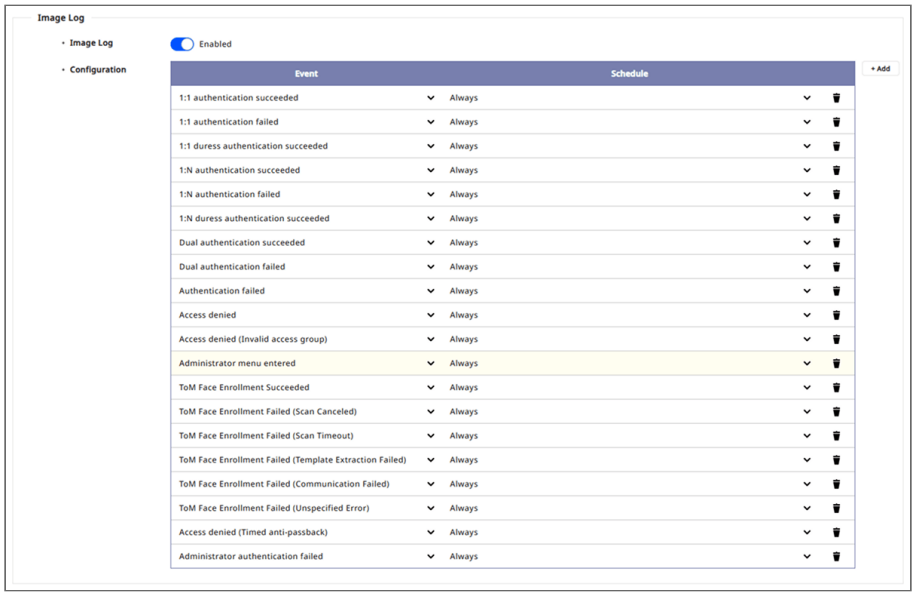
あらかじめ設定された動作を選択するか、ユーザー定義の動作を追加できます。

> **情報**
>
> - **Output** オプションを選択してカスタム動作を設定する際に目的の信号設定がない場合は、**+ Add Signal** をクリックして設定します。
> - **Trigger** を **Input(Event Name Change)** に選択した場合、**Action** を **Port None** に設定できます。

イメージログ設定

Image Log グループでは、デバイスで使用するイメージログイベントとスケジュールを設定できます。

1. **Image Log** オプションを **Use** に設定します。
2. **Configuration** で **+ Add** をクリックし、必要なイベントとスケジュールを設定します。



> **情報**
>
> - この機能はBioStation 3 Max、BioStation 3、X-Station 2、FaceStation F2、FaceStation 2、BioStation A2の各モデルで利用できます。
> - イメージログの基本設定の詳細については、イメージログを設定するを参照してください。

Wiegand 設定

Wiegand グループでは、Wiegand デバイスの入出力に関する詳細項目を設定できます。



- **Input/Output**：入出力モードを選択します。
- **Pulse Width(µs)**：Wiegand 信号のパルス幅を設定します。
- **Wiegand Input Format**：デバイスに指定する Wiegand フォーマットを変更します。
- **Pulse Interval(µs)**：Wiegand 信号のパルス間隔を設定します。
- **Output Mode**：Wiegand 信号の出力モードを設定します。
  - **Normal**：設定済みの Wiegand フォーマットでカードをスキャンします。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。
  - **Bypass**：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。

- **Output info**：認証時にデバイスへ出力する情報を選択します。

> **情報**
> Wiegand形式の設定の詳細については、Wiegandカード形式を設定するをご参照ください。

セキュリティタンパー設定

デバイスでタンパーイベントが発生した場合に、デバイスに保存されているすべてのユーザー情報、全ログ、およびセキュリティキーを削除するよう設定できます。 **Secure Tamper** 機能を有効にするには、**On** に設定します。



アナログインターホン設定

アナログインターホンの使用可否を設定できます。デバイスに接続されたインターホンを使用するには、**Interphone** グループで **Use** をクリックします。

> **情報**
> この機能は BioStation 2 モデルのみ対応しています。

カメラ設定

カメラの周波数を設定できます。蛍光灯を使用する環境で周波数を誤って設定すると、画像がちらつく場合があります。 **Camera** グループで地域に合わせた周波数を設定します。

> **情報**
>
> - この機能は、ファームウェア 2.1.4 以降の FaceStation F2 モデルおよび BioStation A2 モデルでサポートされます。
> - カメラの周波数は地域によって異なります。米国では 60 Hz が一般的で、多くの他地域では 50 Hz が使用されています。地域に適したカメラ周波数については代理店にお問い合わせください。

熱画像とマスクを設定する

Thermal & Mask または **Mask** セクションで熱画像カメラとマスクの使用に関する詳細項目を設定します。

- 熱画像カメラをSupremaの顔認証デバイスと連携して出入口を通過するユーザーの体温を測定し、基準温度を超えたユーザーのアクセスを制限します。
- マスクを検出し、マスク未着用のユーザーのアクセスを制限します。

情報

- **Thermal Camera** 設定機能はFaceStation 2とFaceStation F2モデルでサポートします。対応する熱画像カメラは以下を参照してください。
  - TCM10-FS2
  - TCM10-FSF2
- **Mask Detection** 設定機能はFaceStation F2、BioStation 3、BioEntry W3、BioStation 3 Maxに対応しています。
- ユーザーが任意で変更した内容がある場合は、**Apply** をクリックします。変更内容を保存しないとデバイスに反映されません。

マスク設定

Mask Configuration グループではマスク検出の使用可否を設定します。

- **Mask Detection**：マスク検出の使用可否を選択します。
  - **Use (Deny access when failed to detect mask)**：マスクを着用していないユーザーは認証が拒否され、マスク未着用イベントログが記録されます。
  - **Use (Allow access after leaving log when failed to detect mask)**：マスクを着用していないユーザーも認証できますが、マスク未着用イベントログが記録されます。
  - **Not Use**：マスク検出機能を使用しません。
- **Mask Detect Level**：マスク検出感度を選択します。

情報

Mask Check Mode オプションの詳細はサーマルおよびマスク確認方式をご参照ください。

熱画像カメラ設定

Thermal Camera グループでは熱画像カメラの使用可否と詳細項目を設定します。

- **Thermal Camera Use**：熱画像カメラの使用可否を設定します。
  - **Use (Deny access when exceeded threshold temperature)**：基準温度を超えたユーザーは認証が拒否され、基準温度超過イベントログが記録されます。
  - **Use (Allow access after leaving log when exceeded threshold temperature)** 基準温度を超えたユーザーも認証できますが、温度超過イベントログが記録されます。
- **Celsius/Fahrenheit**：温度表示単位を設定します。
- **Threshold Temp. (°C)** / **Threshold Temp. (°F)**：アクセスを制限する基準温度の下限と上限を設定します。

  表面温度が**Low**値より低い場合、または**High**値より高い場合、**Thermal Camera Use** オプションに従ってアクセスを制限します。 1°C～45°Cの範囲で設定でき、**Low**値は**High**値より高く設定できません。
- **Save Temp. Data**：ユーザーの温度ログの保存可否を設定します。
  - **Enabled**：認証成功の有無とユーザーの温度値をログに保存します。

  - **Disable**：認証成功の有無のみをログに保存します。

- **Temp. Fail Sound**：基準温度超過による認証失敗時の通知可否を設定します。
- **Show Infrared Image**：デバイス画面に赤外線映像を表示するかどうかを設定します。
- **Camera Configuration**：熱画像カメラの詳細オプションを設定します。
  - **Temp. Correction (℃)**：使用環境に応じて温度を一定値だけ高くまたは低く測定するよう補正できます。例えば、温度が常に0.1℃高く測定される環境では、温度補正値を-0.1℃に設定します。
  - **Distance(cm)**：ユーザーと熱画像カメラ間の距離を設定します。
  - **Emissivity**：赤外線放射率を設定します。
  - **Dynamic ROI**：周囲に他の照明がある場合、熱画像カメラが自動で照明ではなくユーザーの温度を測定するように設定できます。
  - **ROI X(%)** / **ROI Y(%)** / **ROI Width(%)** / **ROI Height(%)**：**Dynamic ROI** オプションを **Disable** に設定した場合、ROI（関心領域）を手動で設定できます。 ROI の位置とサイズを調整し、熱画像カメラが温度を測定する領域を手動で設定します。

情報

- **Threshold Temp.** オプションの**Low**値および**High**値の設定は、以下のファームウェアバージョン以降でサポートします。
  - FaceStation 2 ファームウェア 1.4.2 以上
  - FaceStation F2 ファームウェア 1.0.2 以上
- 最適な性能を得るために、**Camera Configuration** のサブオプションはデフォルト設定のまま使用することを推奨します。デバイスごとの各オプションのデフォルト値は以下を参照してください。

項目	FaceStation 2	FaceStation F2
Distance(cm)	100	100
Emissivity	0.98	0.98
ROI X(%)	47	30
ROI Y(%)	45	25
ROI Width(%)	15	50
ROI Height(%)	10	55

サーマルおよびマスク確認方式

Thermal & Mask Check Mode または **Mask Check Mode** グループでは、**Mask Detection** または **Thermal Camera Use** オプションを **Use** に設定することで、デバイスの用途に応じた確認方式を選択できます。

- **Check after authentication**：認証後にユーザーのマスク着用有無を確認するか体温を測定します。

- **Check before authentication**：ユーザーのマスク着用有無を確認するか体温を測定してから認証を実行します。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。
- **Check without authentication**：マスク着用有無の確認または体温測定の用途にのみデバイスを使用できます。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。

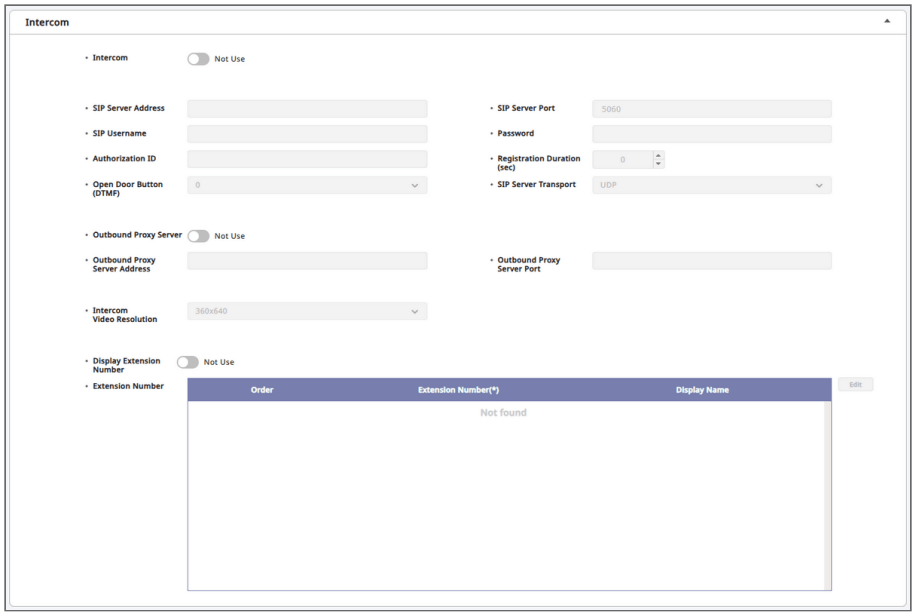
IPインターホンを設定する

この**Intercom**セクションでは、IPインターホンの詳細項目を設定できます。

> **情報**
>
> - この機能はBioStation 3 Max、BioStation 3、FaceStation 2、BioStation A2の各モデルで利用できます。
> - ユーザーが任意で変更した内容がある場合は、**Apply** をクリックします。変更内容を保存しないとデバイスに反映されません。

IPインターホンの設定

各オプションを設定して、デバイスを**Session Initiation Protocol**（SIP）サーバーに登録してください。



- **Intercom**：デバイスをIPインターホンとして使用するには**Enabled**に設定してください。
- **SIP Server Address**：SIPサーバーのアドレスを入力してください。
- **SIP Server Port**：SIPサーバーのポートを入力してください。デフォルトは5060です。
- **SIP Username**：SIPアカウントのユーザー名を入力してください。
- **Password**：SIPアカウントのパスワードを入力してください。
- **Authorization ID**：SIPアカウントの認証IDを入力してください。
- **Registration Duration (sec)**：登録維持時間を秒単位で入力してください。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。
- **Open Door Button (DTMF)**：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。

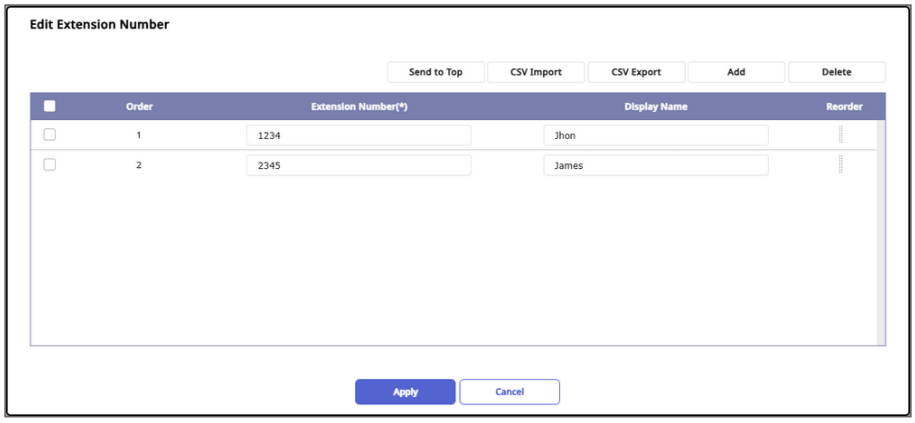
- **SIP Server Transport**：IPインターホンのSIPサーバー設定の際にSIPトランスポート方式を選択してください。
- **Outbound Proxy Server**：別の（アウトバウンド）プロキシサーバー経由でSIPサービスを使用する場合は**Enabled**に設定してください。
  - **Outbound Proxy Server Address**：アウトバウンドプロキシサーバーのアドレスを入力してください。
  - **Outbound Proxy Server Port**：アウトバウンドプロキシサーバーのポートを入力してください。
- **Intercom Video Resolution**：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。デフォルトは**360 x 640**です。
- **Display Extension Number**：デバイスで内線番号を表示しないようにするには**Disable**に設定してください。内線番号を表示しない場合、発信画面で受信者を識別できません。
- **Extension Number**：最大128件の内線番号を登録できます。内線番号を追加または編集するには**Edit**ボタンをクリックしてください。詳細については内線番号の編集をご参照ください。

情報

- **SIP Username**と**Authorization ID**オプションでは数字、英字（大文字・小文字区別）、特殊記号のみ入力できます。
- **Registration Duration (sec)**オプションは60秒から600秒の範囲で設定できます。
- **SIP Server Transport**と**Intercom Video Resolution**オプションはBioStation 3ファームウェア1.3.0以上でサポートされています。
- Session Initiation Protocol（SIP）は、インターネット電話やビデオ会議など、さまざまなマルチメディア通信のためのインターネットプロトコルベースの通信プロトコルです。 SIPサーバーはこれらの通信を管理し、接続を確立する役割を担います。

内線番号の編集

Edit Extension Numberウィンドウで提供される機能について説明します。



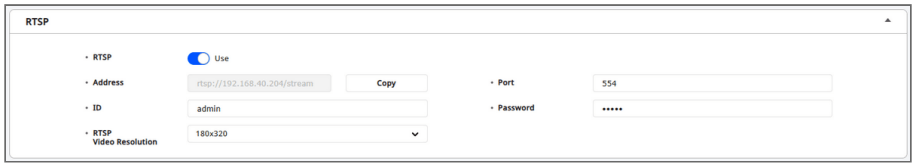
- **Send to Top**：選択した内線番号をリストの最上段へ移動できます。
- **CSV Import**：内線番号を保存したCSVファイルを読み込めます。
- **CSV Export**：保存されている内線番号をCSVファイルにエクスポートできます。
- **Add**：内線番号を追加します。
- **Delete**：内線番号を削除します。

- **Reorder**：内線番号をドラッグして順序を変更します。

> **情報**
>
> - FaceStation 2とBioStation A2モデルでは、内線番号を最大16件まで保存できます。
> - サポート上限を超える数の内線番号が含まれるCSVファイルは読み込めません。
> - 内線番号には数字、英字（大文字・小文字区別）、特殊記号のみ入力できます。

RTSP を設定する

RTSPセクションでは、**Real Time Streaming Protocol**(RTSP) ストリーミング用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。

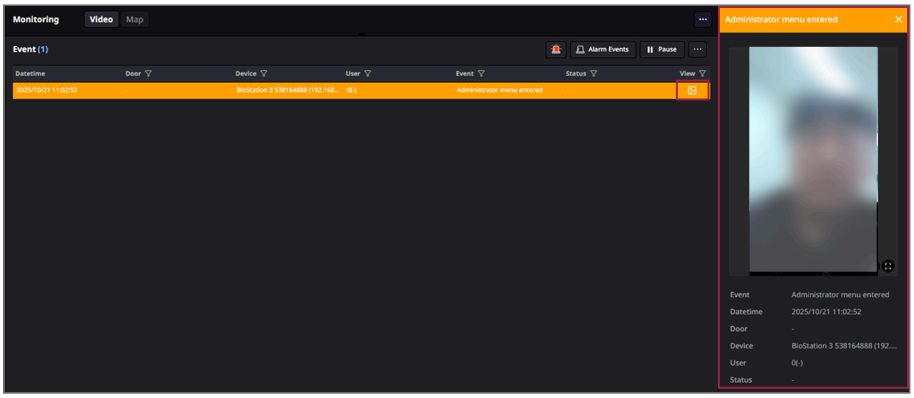


- **RTSP**：RTSP ストリーミングを使用するには、**Enabled**に設定します。
- **Address**：RTSP サーバーアドレスは固定されています。 RTSP アドレスをコピーするには、**Copy**をクリックします。
- **Port**：RTSP ポートを設定します。
- **ID**：RTSP サーバーの ID を入力します。
- **Password**：RTSP サーバーのパスワードを入力します。
- **RTSP Video Resolution**：RTSP 使用時に出力される映像の解像度を選択します。デフォルトは **180 x 320** です。

> **情報**
>
> - この機能はBioStation 3 Max、BioStation 3、BioEntry W3モデルに対応しています。
> - **RTSP Video Resolution** オプションは BioStation 3 のファームウェア 1.3.0 以降でサポートされています。
> - ユーザーが任意で変更した内容がある場合は、**Apply** をクリックします。変更内容を保存しないとデバイスに反映されません。

イメージログを設定する

Image Log は、カメラ付きデバイスで発生したイベントを画像として確認できる機能です。ドアを通過するユーザーの顔画像やイベント発生時の状況をデバイスのカメラで記録できます。記録された画像は **Monitoring** ページのリアルタイムイベントで確認できます。



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。

イメージログを設定すると、**Event** リストにそのイベントのイメージログが生成されます。イベント項目の最右端で をクリックします。右側パネルで、そのイベントが発生したときに撮影された画像を確認できます。

情報

- この機能はBioStation 3 Max、BioStation 3、X-Station 2、FaceStation F2、FaceStation 2、BioStation A2の各モデルで利用できます。
- **Monitoring** ページでイベントログを確認する方法の詳細については、イベントをモニタリングするをご参照ください。

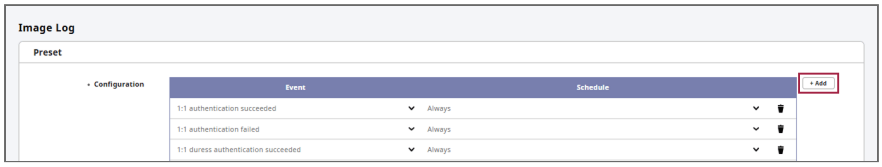
注意

Settings → **Device** → **Image Log** メニューで設定した内容はデバイスに反映されません。各デバイスで **Image Log** オプションを有効にする必要があります。詳しくは 高度設定 をご参照ください。

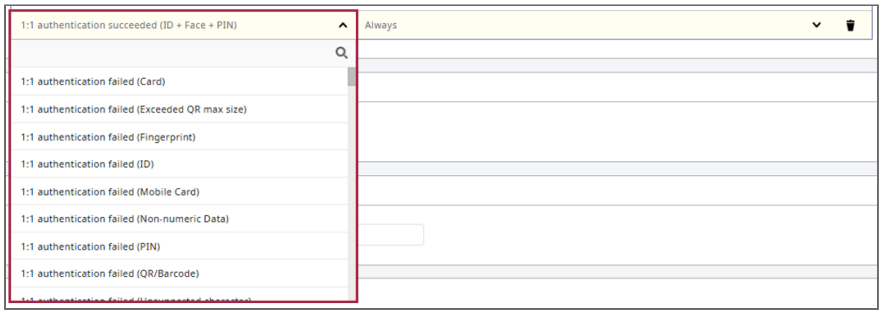
基本設定を追加

デバイスで **Image Log** オプションを有効にしたときに適用される基本設定を設定してください。画像ログを生成するイベントとスケジュールを設定してください。イベントおよびスケジュール条件に一致するとイメージログが生成されます。

1. **Launcher**ページで**Settings**をクリックします。
2. 画面左のサイドバーで **Device** → **Image Log** をクリックします。
3. **Preset** セクションの右側で **+ Add** をクリックします。



4. リスト下部にイベントが追加されたら、対象イベントの をクリックし、目的の項目を選択します。



5. 該当イベントのスケジュールで ⌄ をクリックし、目的の項目を選択します。



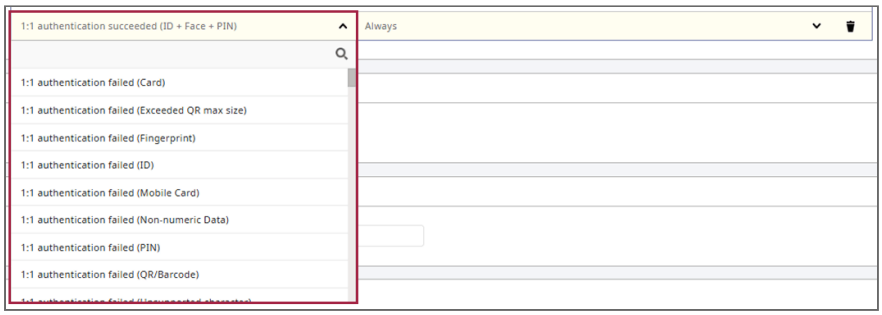
6. 設定を保存するには、画面最下部の **Apply** をクリックします。

> **情報**
> 目的のスケジュールがない場合は、**+ Add Schedule** をクリックして追加します。スケジュール設定の詳細については、スケジュールを設定するをご参照ください。

基本設定を変更

既に設定済みのイメージログのイベントとスケジュールを変更できます。

1. **Launcher**ページで**Settings**をクリックします。
2. 画面左のサイドバーで **Device** → **Image Log** をクリックします。
3. **Preset** セクションのリストで変更するイベントの ⌄ をクリックし、目的の項目を選択します。



4. 該当イベントのスケジュールで ⌄ をクリックし、目的の項目を選択します。



5. 設定を保存するには、画面最下部の **Apply** をクリックします。

情報

- 目的のスケジュールがない場合は、**+ Add Schedule** をクリックして追加します。スケジュール設定の詳細については、スケジュールを設定するをご参照ください。
- 変更した基本設定は、新しく追加したデバイスにのみ適用されます。すでに **Image Log** オプションを有効にしているデバイスには反映されないため、該当デバイスの設定で追加する必要があります。

基本設定を削除

既に設定済みのイメージログのイベントとスケジュールを削除できます。

1. **Launcher**ページで**Settings**をクリックします。
2. 画面左のサイドバーで **Device** → **Image Log** をクリックします。
3. **Preset** セクションのリストで削除するイベントの 🗑 をクリックします。



4. 設定を保存するには、画面最下部の **Apply** をクリックします。

Delete Option

イメージログファイルが保存スペースを占有し続けないように、**BioStar X** サーバーで削除オプションを設定できます。設定したファイルサイズまたは期間を超えたイメージログは自動で削除されます。

1. **Launcher**ページで**Settings**をクリックします。
2. 画面左のサイドバーで **Device** → **Image Log** をクリックします。
3. **Delete Option** セクションでイメージログの削除条件を設定します。



- **Delete Option**：ファイルサイズ単位（**MB**/**GB**）または期間単位（**Day**/**Week**/**Month**）を選択します。
- **Amount of Image Log**：**Delete Option** で設定した条件の単位を設定します。
- **Delete Cycle**：イメージログを削除する周期を選択します。

4. 設定を保存するには、画面最下部の **Apply** をクリックします。

Storage Path Settings

イメージログを保存するパスを設定できます。

1. **Launcher**ページで**Settings**をクリックします。

2. 画面左のサイドバーで **Device** → **Image Log** をクリックします。
3. **Storage Path Settings** セクションの **Image Log File Path** 入力フィールドにイメージログを保存するパスを入力します。



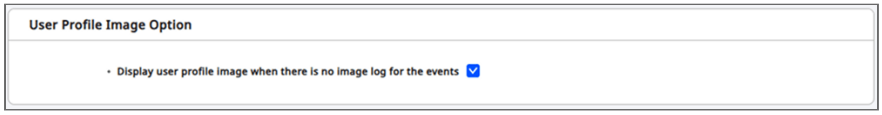
4. 設定を保存するには、画面最下部の **Apply** をクリックします。

> **情報**
>
> - 保存パスは自動生成されないため、イメージログを保存するパスをあらかじめ作成しておく必要があります。
> - たとえば、`.\imagelog\` と入力すると、BioStar X をインストールしたパス配下にイメージログを保存します。
>
> *C:\Program Files\BioStar X\imagelog*

User Profile Image Option

イメージログを撮影できないデバイスでイベントログやリアルタイムログをモニタリングする際に、ユーザープロフィール写真を表示するように設定できます。

1. **Launcher**ページで**Settings**をクリックします。
2. 画面左のサイドバーで **Device** → **Image Log** をクリックします。
3. **User Profile Image Option** セクションの **Display user profile image when there is no image log for the events** 項目のチェックボックスをクリックします。



4. 設定を保存するには、画面最下部の **Apply** をクリックします。

> **情報**
>
> - このオプションが有効な場合、イメージログが発生するとユーザープロフィール写真ではなく撮影されたイメージログを表示します。
> - **Monitoring** ページでイベントログを確認する方法の詳細については、イベントをモニタリングするをご参照ください。

USB エージェントを設定する

クライアント PC から **BioStar X** に接続した際に、USB 指紋登録デバイスとカード登録デバイスを利用できるようにサポートします。そのためには、USB Device Agent をインストールする必要があります。本書では、USB Device Agent のインストールと設定方法を案内します。

USB Device Agent をインストールする

クライアント PC から **BioStar X** に接続して USB 指紋登録デバイスおよびカード登録デバイスを使用するには、USB Device Agent をインストールする必要があります。

1. **Launcher**ページで**Settings**をクリックします。
2. 画面左のサイドバーで **Device** → **USB Agent** をクリックします。
3. **USB Device Agent** セクションで **Download** ボタンをクリックします。



4. ダウンロードしたファイルを実行し、画面の案内に従ってインストールを完了します。

> **情報**
> Windows で **ユーザー アカウント制御** が有効になっている場合、USB Agent は自動実行できません。ユーザー アカウント制御をオフにするか、管理者権限で直接実行します。

USB カードデバイスのバイト順序を設定する

USB カードデバイスのバイト順序を設定できます。

1. **Launcher**ページで**Settings**をクリックします。
2. 画面左のサイドバーで **Device** → **USB Agent** をクリックします。
3. **Byte Order of USB Card Device** セクションで **Byte Order** オプションを設定します。



- **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。

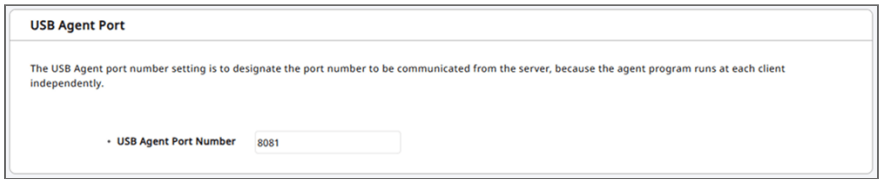
4. すべての設定が完了したら、画面最下部の **Apply** ボタンをクリックします。

> **情報**
> **Byte Order** オプションは CSN カードにのみ適用できます。

USB Agent ポートを設定する

USB Agent が使用するポートを設定できます。

1. **Launcher**ページで**Settings**をクリックします。
2. 画面左のサイドバーで **Device** → **USB Agent** をクリックします。
3. **USB Agent Port** セクションの **USB Agent Port Number** 入力フィールドにポート番号を入力します。



4. すべての設定が完了したら、画面最下部の **Apply** ボタンをクリックします。

> **情報**
> USB Agent はクライアントごとに動作するプログラムであり、ポート番号の設定はサーバーがそのポート番号で通信するためのものです。

デバイス接続管理を設定する

BioStar X の **Device Connection Manager** は、企業や大型ビルで多数のデバイスを効率的に管理するために作られた機能です。従来は1台のサーバーで最大1,000台のデバイスしか接続できませんでしたが、現在は **Communication** サーバーを複数のコンピューターにインストールすることで、最大3,000台のネットワークデバイスを管理できます。

> **情報**
> - この機能は **Device Manager** ライセンスを有効化すると利用できます。ライセンスポリシーの詳細については、ライセンス ポリシーをご参照ください。
> - マルチコミュニケーションサーバーの仕様とインストールの詳細については次のドキュメントを参照してください。
> - システム最小要件
> - マルチコミュニケーションサーバーをインストールする

主な機能

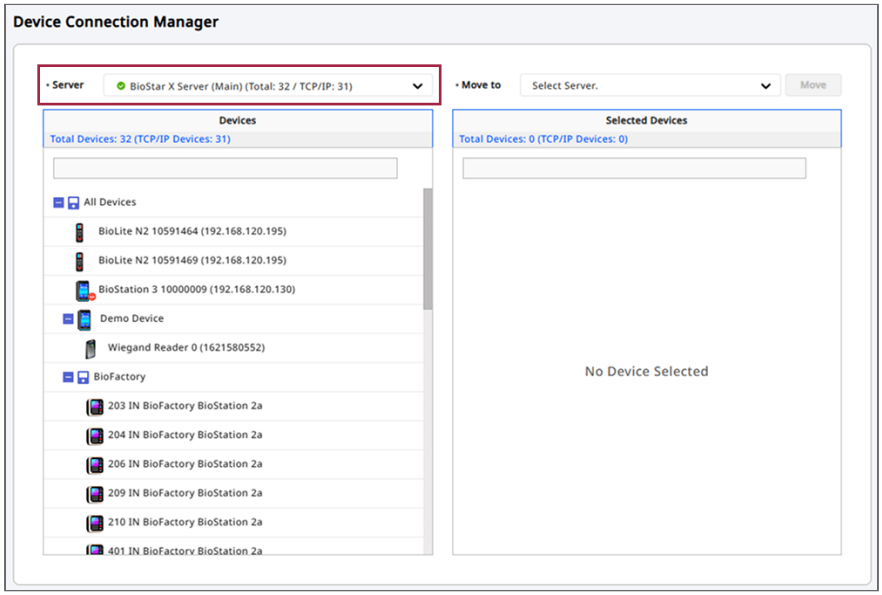
- **サーバー拡張**：メインコンピューター以外の追加コンピューターに通信サーバーをインストールし、より多くのデバイスを接続できます。
- **複数サーバー運用**：最大3台のサーバーを併用して合計3,000台のデバイスをサポートします。
- **便利なデバイス管理**：新しいデバイスを追加する際に接続先サーバーを選択でき、既存デバイスを別のサーバーへ移動することもできます。
- **大規模環境サポート**：大規模な事業所や建物で必要とされる多数のデバイスを安定して運用できます。

マルチコミュニケーションサーバーは、BioStar X の統合サーバーからデバイス接続機能のみを分離した専用サービスです。デバイスとの安定した通信に特化し、システム全体のパフォーマンスを向上させます。

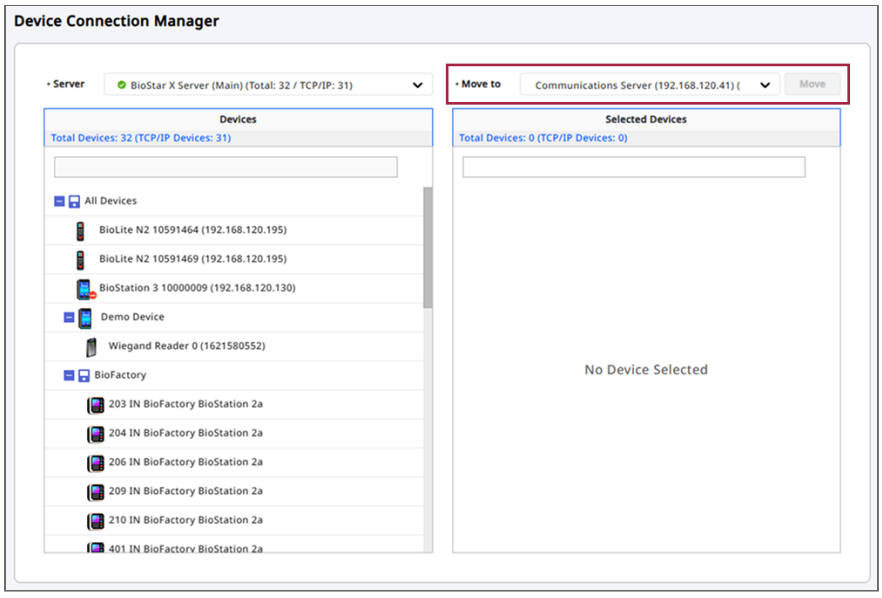
別のサーバーへデバイスを移動する

メインサーバーまたは別のマルチコミュニケーションサーバーに登録されているデバイスを、別のマルチコミュニケーションサーバーへ移動できます。この機能により、デバイスの接続状態を維持したままサーバー間でデバイスを移動できます。

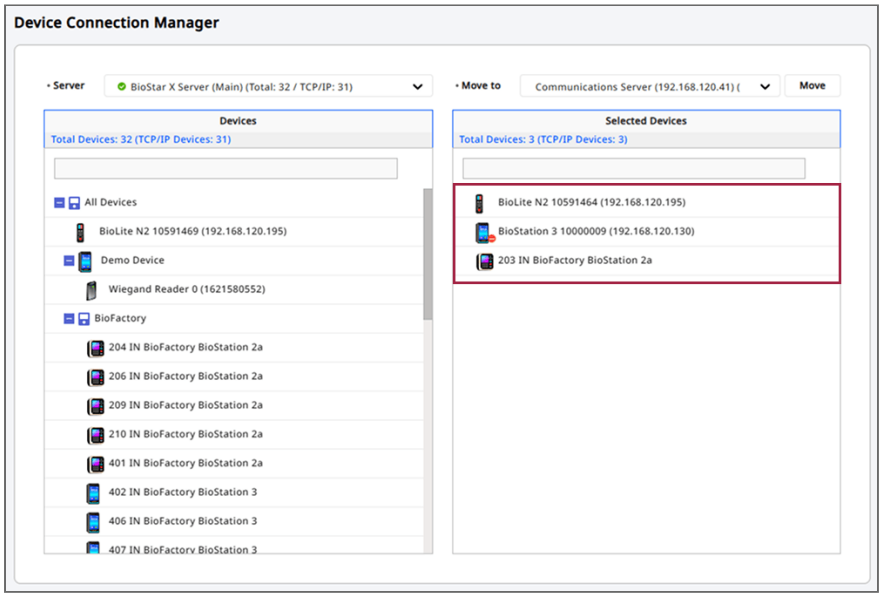
1. **Launcher**ページで**Settings**をクリックします。
2. 画面左側のサイドバーで **Device** → **Device Connection Manager** をクリックします。
3. 左側の **Server** 項目で、移動したいデバイスが登録されているサーバーを選択します。



4. 右側の **Move to** 項目で、デバイスを移動する宛先サーバーを選択します。

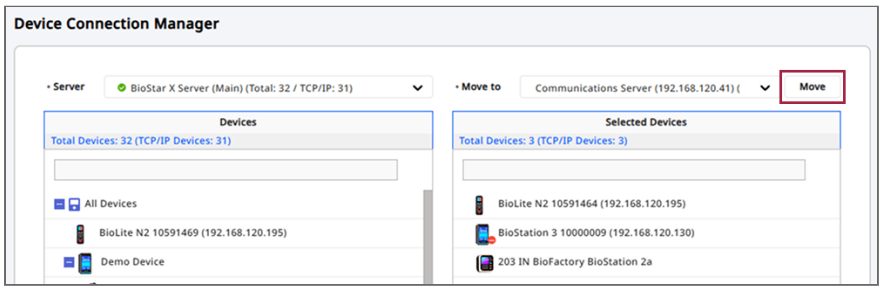


5. デバイス一覧から移動するデバイスを選択します。複数のデバイスを選択できます。



特定のデバイスを検索するには、上部の入力フィールドにキーワードを入力します。デバイス名やシリアル番号で検索できます。

6. デバイスを宛先サーバーへ移動するには、**Move** ボタンをクリックします。



7. メッセージウィンドウで移動するデバイス総数、TCP/IP 接続デバイス数、移動先サーバーの名前と IP アドレスを確認します。

8. **Yes** ボタンをクリックします。

移動が完了すると、メッセージウィンドウで移動されたデバイス総数、TCP/IP 接続デバイス数、移動先サーバーの名前と IP アドレスを確認できます。

移動に失敗したデバイスがある場合、メッセージウィンドウで失敗したデバイス数と TCP/IP 接続デバイス数を確認できます。移動に失敗したデバイスの一覧と失敗理由を CSV ファイルで確認するには、**Download** ボタンをクリックします。

情報

- 接続された拡張サーバーがない場合、画面右側の **Move to** は表示されません。
- サーバーを選択すると、そのサーバーに登録されている Wiegand や RS-485 接続デバイスを含むすべてのデバイスを確認できます。
- デバイスまたはデバイスグループを選択すると、デバイスに接続された子デバイスやグループに含まれるデバイスも一緒に移動します。
- TCP/IP 通信で接続していないデバイスは移動できません。

ドア管理

登録済みデバイスが設置されている扉の情報を設定および管理する方法を案内します。デバイスのリレー、二要素認証、アンチパスバック、強制扉開放、長時間扉開放に対するアラームなどの情報を設定でき、設定した扉情報はアクセスレベルの構成要素として使用されます。

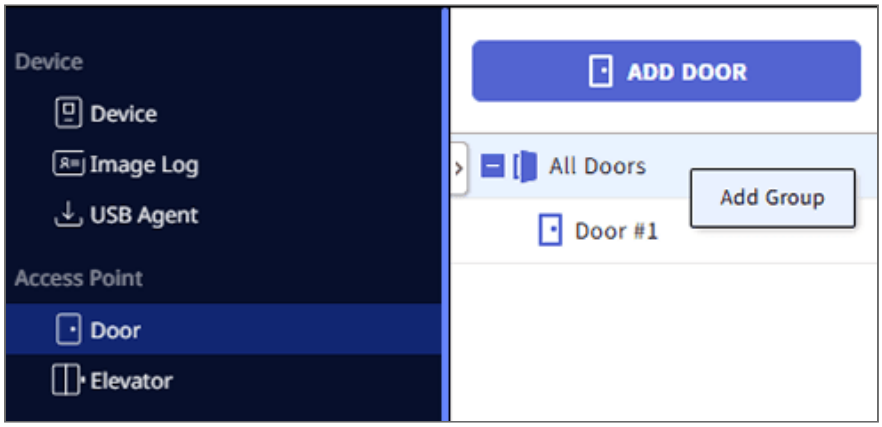
ドアグループを管理する

複数のドアを簡単に管理できるよう、グループ設定方法を案内します。ドアグループは、複数のドアを 1 つのグループにまとめて管理できる機能です。グループを設定すると、ドアを一括設定できます。

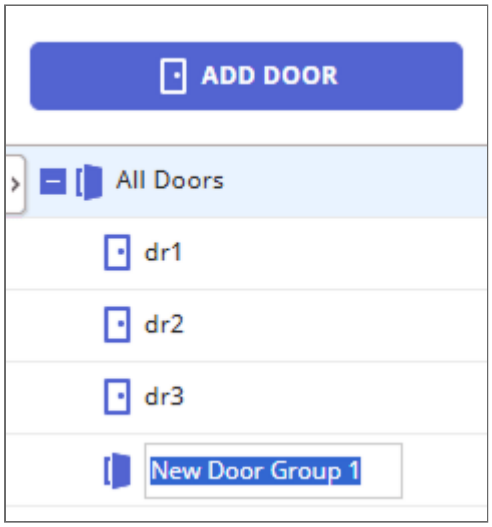
> **ヒント**
> ドアの位置やオフィス名などでグループ名を登録すると、管理が便利です。

ドアグループを追加

1. **Launcher**ページで**Settings**をクリックします。
2. 画面左側のサイドバーで **Access Point** → **Door** をクリックしてください。
3. ドア一覧で **All Doors** を選択し、右クリックします。



4. ポップアップメニューで **Add Group** をクリックします。

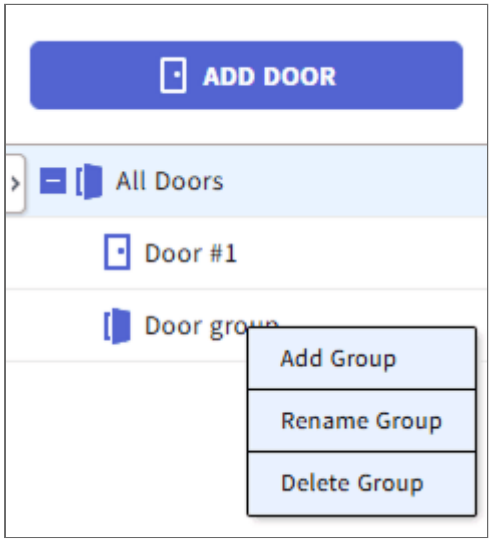


5. 希望するグループ名を入力します。

> **情報**
>
> - ドアグループは最大 8 階層まで作成できます。
> - ドアグループ名は最大 48 文字まで入力できます。

ドアグループ名を変更

1. **Launcher**ページで**Settings**をクリックします。
2. 画面左側のサイドバーで **Access Point** → **Door** をクリックしてください。
3. ドア一覧で名前を変更するグループを選択し、右クリックします。

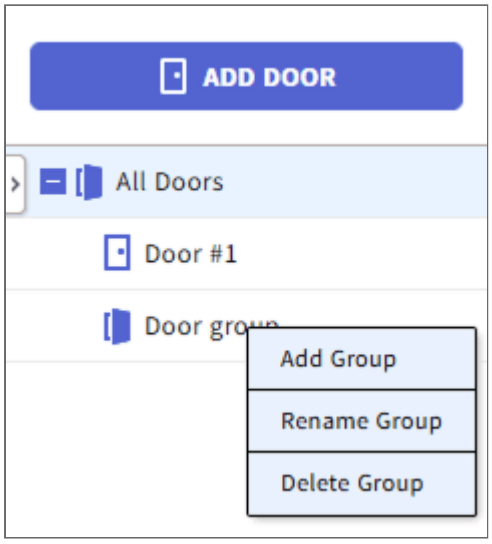


4. ポップアップメニューで **Rename Group** をクリックします。
5. 変更するグループ名を入力します。

> **情報**
> ドアグループ名は最大 48 文字まで入力できます。

ドアグループを削除

1. **Launcher**ページで**Settings**をクリックします。
2. 画面左側のサイドバーで **Access Point** → **Door** をクリックしてください。
3. ドア一覧で削除するグループを選択し、右クリックします。



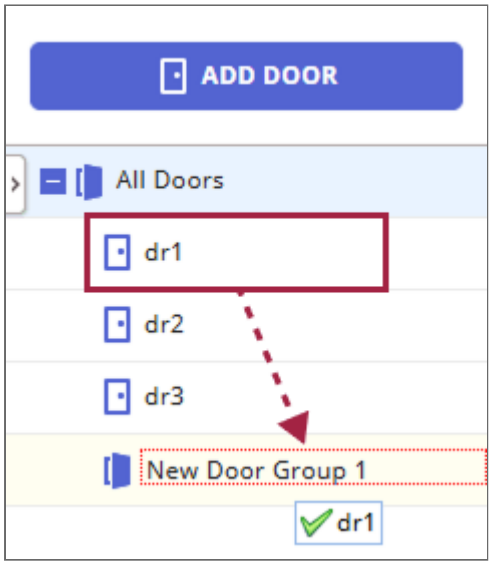
4. ポップアップメニューで **Delete Group** をクリックします。

> **注意**
> ドアグループを削除すると、グループに含まれるすべてのドアが削除されます。グループ内のドアを削除したくない場合は、まずドアを別のグループに移動してからグループを削除してください。

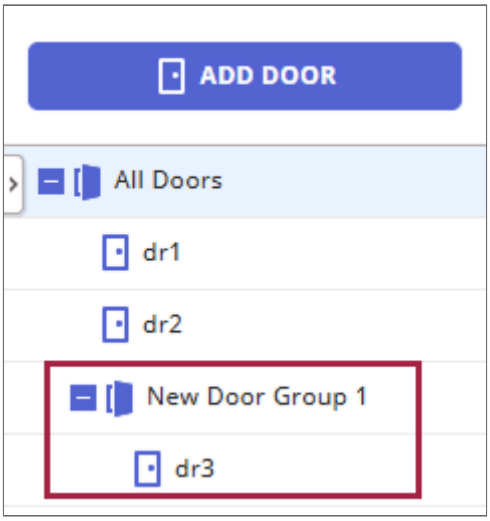
グループにドアを追加

ドア一覧からグループに追加する

1. **Launcher**ページで**Settings**をクリックします。
2. 画面左側のサイドバーで **Access Point** → **Door** をクリックしてください。
3. ドア一覧でグループに追加するドアを選択し、目的のグループにドラッグします。

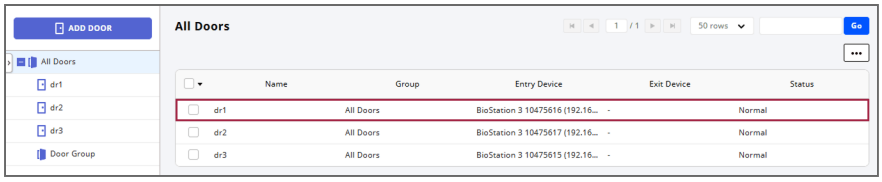


選択したドアがグループに移動します。

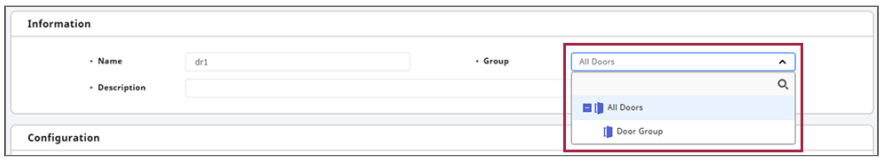


ドア情報からグループに追加する

1. **Launcher**ページで**Settings**をクリックします。
2. 画面左側のサイドバーで **Access Point** → **Door** をクリックしてください。
3. 画面右側のドア一覧で、グループに追加するドアをクリックします。



4. ドア情報の編集画面が表示されたら、**Information** セクションの **Group** オプションをクリックします。



5. 目的のグループを選択します。

6. 画面最下部にある **Apply** をクリックします。

ドアを登録する

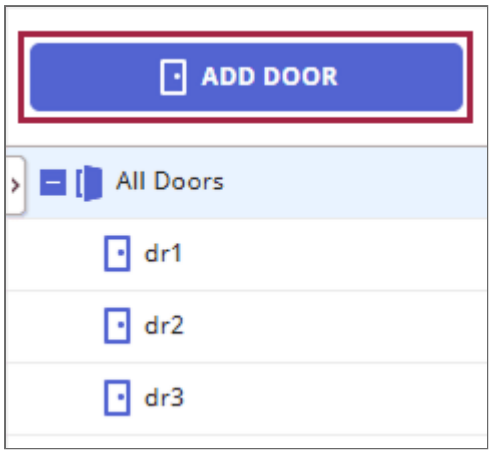
ドアを登録して設定する手順を案内します。ドアごとに入室・退室デバイスを接続し、アンチパスバックや二重認証などのセキュリティ機能を設定することで、体系的な入退室管理環境を構築できます。さらに、ドアの状態に基づくアラーム設定によりセキュリティ事故を事前に防止できます。

開始前に

- ドアを登録する前に、入退室管理用の入室レベル、入室グループ、フロアレベルを設定してください。詳しくは 入退室制御設定 をご参照ください。
- ドアを登録する前にデバイスを登録してください。デバイス登録の詳細は、以下のドキュメントを参照してください。
  - デバイスを登録する
  - Wiegandデバイスを登録する
  - スレーブ装置を登録する

ドア登録

1. **Launcher**ページで**Settings**をクリックします。
2. 画面左側のサイドバーで **Access Point** → **Door** をクリックしてください。
3. **ADD DOOR** ボタンをクリックします。



4. **Add New Door** 画面が表示されたら、各セクション項目を順に設定してください。
   - **Information**：ドアの基本情報を設定します。詳しくは 基本情報の設定 をご参照ください。
   - **Configuration**：ドアに接続されたデバイス、入室および退室ボタン、ドアセンサーを設定します。詳しくは ドア設定 をご参照ください。
   - **Option**：追加オプションを設定してください。詳しくは 追加オプションの設定 をご参照ください。
   - **Anti PassBack**：入退室履歴を管理しセキュリティを強化するアンチパスバック機能を設定します。詳しくは アンチパスバック設定 をご参照ください。
   - **Timed Anti PassBack**：アンチパスバック機能の初期化時間を設定できます。詳しくは 時間制限アンチパスバック設定 をご参照ください。

- **Alarm**：アンチパスバック違反が発生した際に警報を鳴らしたりデバイスを使用不可にする設定ができます。詳しくは アラーム設定 をご参照ください。

5. すべての設定が完了したら、画面最下部の **Apply** ボタンをクリックします。

基本情報の設定

Information セクションでは、ドアの名前、グループ、説明を入力または変更できます。

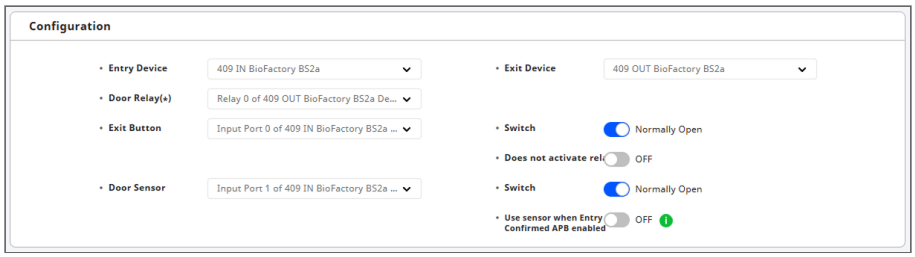


- **Name**：ドア名を入力します。管理を容易にするために識別しやすい名前を入力してください。
- **Group**：ドアグループを選択します。
- **Description**：ドアに関する簡単な説明を入力します。

> **情報**
>
> - ドア名は最大48文字まで入力できます。
> - ドアグループ登録の詳細は ドアグループを管理する をご参照ください。

ドア設定

Configuration セクションでは、ドアに接続されたデバイスや退室ボタン、ドア配線などを設定できます。



- **Entry Device**：入室時に使用するデバイスを選択します。デバイスが一覧にない場合は、先にデバイスを登録してください。
- **Door Relay**：ドアロックとして動作するリレーを選択します。
- **Exit Button**：退室ボタンとして使用するポートを選択します。
  - **Switch**：**N/C**(Normally Closed) または **N/O**(Normally Open) に設定できます。
  - **Does not activate relay**：退室ボタン入力時にドア解錠要求ログは生成されますが、リレーは動作しないように設定できます。
- **Door Sensor**：ドア状態を確認する際に使用するポートを選択します。 **None** に設定すると、**Alarm** セクションは使用できません。
  - **Switch**：**N/C**(Normally Closed) または **N/O**(Normally Open) に設定できます。
  - **Use sensor when Entry Confirmed APB enabled**：**Entry Confirmed APB** オプション使用時にドアセンサーの使用有無を設定できます。

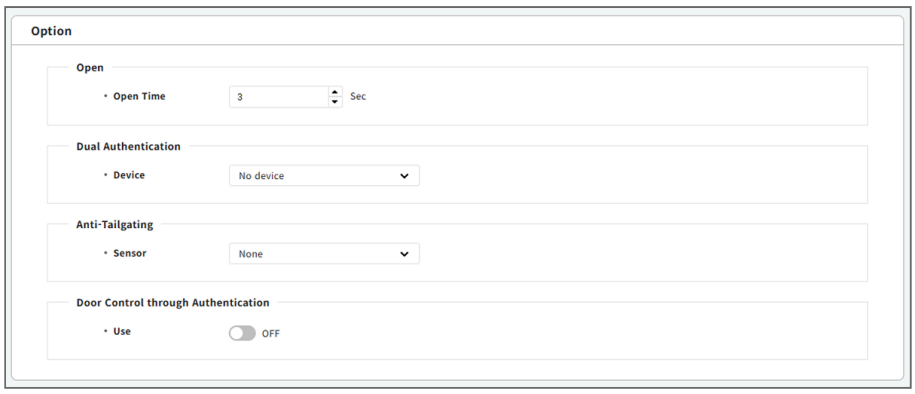
> **Timed Anti PassBack** が有効になっている場合、**Use sensor when Entry Confirmed APB enabled** オプションは使用できません。

- **Exit Device**：退室時に使用するデバイスを選択します。

> **情報**
>
> - **Entry Device** でワイヤレスドアロックを選択した場合、**Exit Device** でもワイヤレスドアロックを選択する必要があります。
> - **Entry Device** でワイヤレスドアロックを選択した場合、**Door Relay** オプションは使用できません。
> - CoreStationモデルは入室デバイスや退室デバイスとして使用できません。

追加オプションの設定

Option セクションでは、ドアに関する追加オプションを設定できます。



- **Open**：ドア解錠に関するオプションを設定します。
  - **Open Time**：認証完了後に出入口が開いたままになる時間を設定します。この時間を過ぎると、ドアは自動的にロックされます。
  - **Lock when door is closed**：ドアセンサーがドアの閉鎖を検知すると、ドアが施錠されます。 **Use Automatic Door** を **On** に設定すると使用できません。
  - **Use Automatic Door**：自動ドアをドアとして使用する場合、ドアセンサーの状態に関係なくリレーを動作させることができます。 **Lock when door is closed** を **On** に設定すると使用できません。

> **Open Time** は使用するドアロック装置の種類によって異なる場合があります。

- **Dual Authentication**：2人（一般ユーザーと管理者）がクレデンシャルを認証してドアを解錠するよう設定できます。
  - **Device**：二重認証を使用するデバイスを選択してください。二重認証を使用しない場合は**None**を選択してください。
  - **Schedule**：二重認証を適用するスケジュールを選択してください。目的のスケジュールがない場合は、**+ Add Schedule** をクリックして追加します。

- **Approval Type**：管理者認証の順序を設定してください。
  - **None**：認証グループに関係なく、2人の認証が必要です。
  - **Last**：一般ユーザーが認証し、設定した認証グループに属するユーザーが認証する必要があります。
- **Approval Group**：管理者が所属するグループを設定します。このオプションは、**Approval Type** を **Last** に選択した場合に使用できます。
- **Timeout**：1回目の認証後から2回目の認証までの待機時間を設定します。設定した時間内に2回目の認証が完了しない場合、階ボタンは有効になりません。

> - 在室人数制限設定に構成されているデバイスのデュアル認証を変更するには、次のメニューで設定を編集します。 **Settings** → **Access Management** → **Advanced AC** → **Occupancy Limit**
>
>   **Occupancy Limit** の設定について詳しくは 高度な入退室制御設定 をご参照ください。
> - スケジュール設定の詳細については、スケジュールを設定するをご参照ください。

- **Anti-Tailgating**：認証されていない人物が認証済みの人物に続いて入退室するテイルゲーティングを検知するよう設定できます。
  - **Sensor**：テイルゲーティングを検知するセンサーを選択してください。
- **Door Control through Authentication**: 権限のあるユーザーがダブルバッジ（Double Badge）すると、ドアが常時開放状態に切り替わるように設定します。詳しくは 認証による出入口制御を設定する をご参照ください。

> 新しいドアを追加する画面では、ドアがまだアクセスグループに含まれていないため、この設定は使用できません。ドアを保存してアクセスグループに追加した後、ドア情報の編集画面で設定してください。

アンチパスバック設定

アンチパスバックは入退室履歴を管理し、セキュリティを強化するために使用します。利用者が入室後にカードを他の利用者へ渡す悪用事例を防止でき、権限を持つ利用者に続いて外部者が入室した場合に退出できないように阻止できます。

以下を参考にして、**Anti PassBack** セクションで設定を完了してください。

- **Type**：アンチパスバックの種類を選択してください。
  - **None**：アンチパスバック機能を使用しません。
  - **Soft APB**：アンチパスバック違反時でも入退室は可能ですが、アラームを鳴らすか **BioStar X** にログを生成します。
  - **Hard APB**：アンチパスバック違反時には入退室できず、アラームを鳴らすか **BioStar X** にログを生成します。
- **Reset Time**：アンチパスバック機能が初期化されるまでの時間を設定してください。最大で7日（10080分）まで設定でき、0に設定すると初期化されません。

情報

- 入室デバイスと退室デバイスの両方が設置されている場合に使用でき、**Configuration** セクションで **Exit Device** オプションを **None** に設定すると使用できません。退室デバイスの設定方法については ドア設定 をご参照ください。
- **Anti PassBack** セクションを有効にするには、RS-485で接続されたマスター装置とスレーブ装置が必要です。
- **Timed Anti PassBack** セクションが有効になっている場合、**Anti PassBack** は使用できません。

時間制限アンチパスバック設定

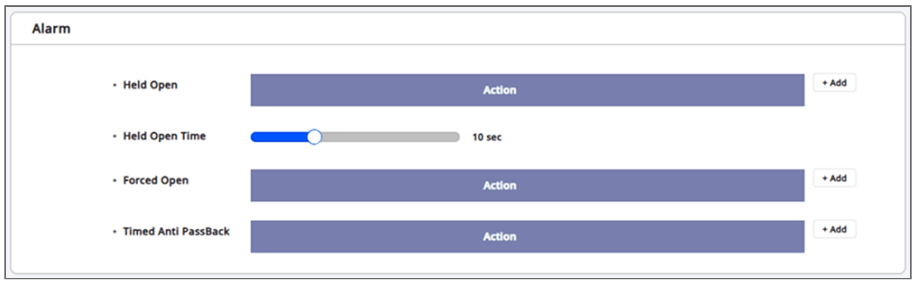
ユーザーが入退室認証後に同じデバイスで再度認証を試みると、アンチパスバック機能が作動して即時の再認証はできません。**Timed Anti PassBack** セクションでは、アンチパスバック機能の初期化時間を設定してユーザーの頻繁な入室を効果的に制限できます。



- **Timed APB**：時間制限アンチパスバック機能を使用するデバイスを選択してください。
- **Reset Time**：アンチパスバック機能が初期化されるまでの時間を設定してください。入力単位は分（min）で、デフォルトは10分です。最大で60分まで設定できます。
- **Bypass Group**：時間制限アンチパスバックの制限を受けず常に通行できる入退室グループを選択できます。

アラーム設定

Alarm セクションでは、ドアが強制的に開けられた場合、開いたまま放置された場合、またはアンチパスバック違反が発生した場合にアラームを鳴らすかデバイスの使用をブロックできます。アラームを追加する項目で **+ Add** ボタンをクリックしてください。



- **Held Open**：ドアが開いたまま放置されたときのアラーム動作を設定してください。
- **Held Open Time**：ドアが長時間開いている場合にアラームを鳴らす時間を設定してください。ドアが開いたままで許容される最大時間を設定してください。
- **Forced Open**：ドアが強制的に開けられたときのアラーム動作を設定してください。
- **Anti PassBack** / **Timed Anti PassBack**：アンチパスバックまたは時間制限アンチパスバック違反が発生したときのアラーム動作を設定してください。

情報

Anti PassBack オプションは、退室デバイスが登録されている場合にのみ設定できます。

出入口情報を編集

登録済みの出入口の設定情報を編集する方法を説明します。個別のドアの詳細設定を変更するか、複数のドアを選択して共通項目を一括編集できます。

一つの出入口情報を編集

1. **Launcher**ページで**Settings**をクリックします。
2. 画面左側のサイドバーで **Access Point** → **Door** をクリックしてください。
3. 出入口リストで編集する出入口をクリックします。
4. 各セクションの詳細項目を編集します。
5. すべての設定が完了したら、画面最下部の **Apply** ボタンをクリックします。

> **情報**
>
> - 出入口情報の編集画面の各セクションの詳細は、ドアを登録するをご覧ください。
> - 出入口を出入口グループに含めた後、**Door Control through Authentication** 機能を設定します。詳しくは 認証による出入口制御を設定する をご参照ください。

複数の出入口を一括編集

1. **Launcher**ページで**Settings**をクリックします。
2. 画面左側のサイドバーで **Access Point** → **Door** をクリックしてください。
3. ドアリストで編集するドアのチェックボックスをクリックします。 2つ以上のドアを選択します。
4. 画面右上にある**Batch Edit**をクリックします。
5. **Batch Edit**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。



- **Open Time**：認証完了後に出入口が開いたままになる時間を設定します。この時間を過ぎると、ドアは自動的にロックされます。

6. 設定が完了したら**Apply**をクリックします。

> **情報**
>
> **Batch Edit**は、出入口リストで2つ以上の出入口を選択すると有効になります。

認証による出入口制御を設定する

認証による出入口制御は、指定ユーザーが対応デバイスで同じカードを連続して二回認証（ダブルバッジ、Double Badge）すると、該当する出入口を常時開放状態に切り替える機能です。常時開放状態で再度ダブルバッジするか、許可されたスケジュールが終了すると、出入口は元のモードに自動で戻ります。

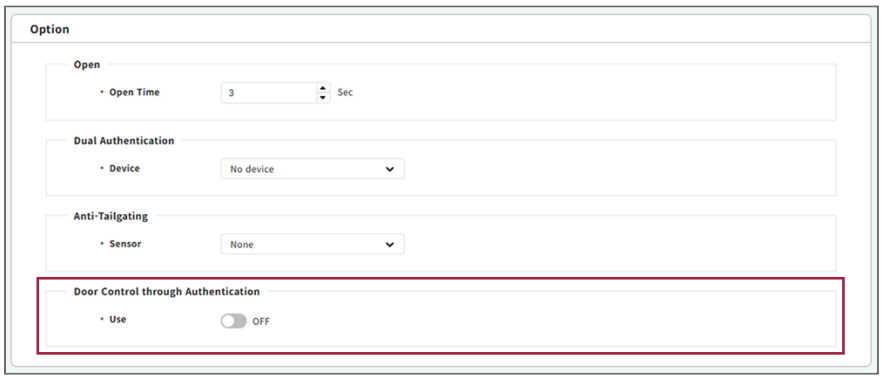
開始前に

- 出入口を出入グループに含める必要があります。新しい出入口の追加画面では、まだ出入グループに含まれていないため、この機能を使用できません。出入口を保存した後に出入グループへ追加し、出入口情報の編集画面でこの機能を設定してください。出入グループの設定については、入退室制御設定ご参照ください。
- 出入口の登録と情報の編集の詳細については、次の文書を参照してください。
  - ドアを登録する
  - 出入口情報を編集

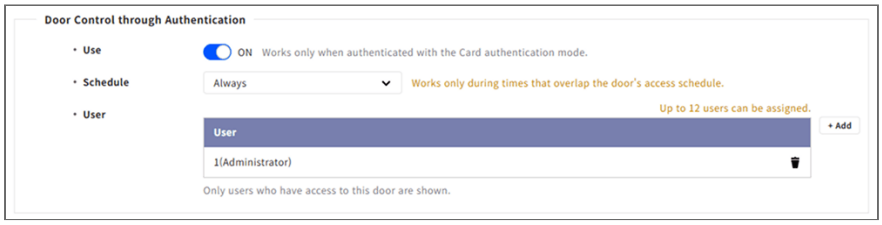
> **情報**
>
> - 認証による出入口制御は、次のデバイスとファームウェア バージョン以降で利用できます。この機能は、対応デバイスで構成された出入口で利用できます。
>   - XPass 2 ファームウェア 1.5.3 以上
>   - FaceStation F2 ファームウェア 2.3.0 以上
> - カード系クレデンシャル（CSN、Wiegand、スマートカード、モバイルカードの CSN/ToM）でのみ動作します。テンプレートクレデンシャルや指紋、顔などの生体認証は対象外です。通常の出入口認証として処理します。
> - 認証による出入口制御は、デバイスの認証モードがカード認証モードの場合にのみ動作します。 **BioStar X**はデバイスの認証モードを確認しないため、機能を使用する前にデバイスの認証モードを直接確認してください。
> - デバイスは、最初の認証と次の認証の間隔が3秒以内の場合にのみ、ダブルバッジとして認識されます。認証間隔が3秒を超えると、デバイスは二度の認証をそれぞれ個別の入退室認証として処理します。

認証による出入口制御を設定する

1. **Launcher**ページで**Settings**をクリックします。
2. 画面左側のサイドバーで **Access Point** → **Door** をクリックしてください。
3. 出入口リストで設定する出入口をクリックします。
4. **Option** セクションで **Door Control through Authentication** 項目へ移動します。

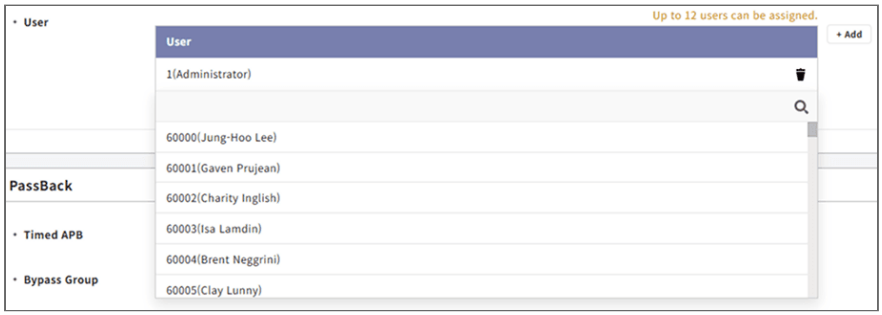


5. **Use** オプションを **ON** に設定してください。



6. **Schedule** で、この機能を適用するスケジュールを選択してください。デフォルトは **Always** です。適用するスケジュールがない場合は、先にスケジュールを追加してください。

7. ダブルバッジで出入口を制御できるユーザーを追加するには、**+ Add** ボタンをクリックし、**User** リストで選択してください。



- **User** 一覧には、該当ドアの入退室権限を持つユーザーのみを表示します。 **Settings** → **Access Management** → **Access Control**で入退室グループとアクセスレベルを確認してください。
- ユーザーは最大12人まで指定できます。
- ユーザーを検索するには、🔍 ボタンをクリックしてください。
- ユーザーグループ単位では指定できず、個別ユーザーのみ選択できます。

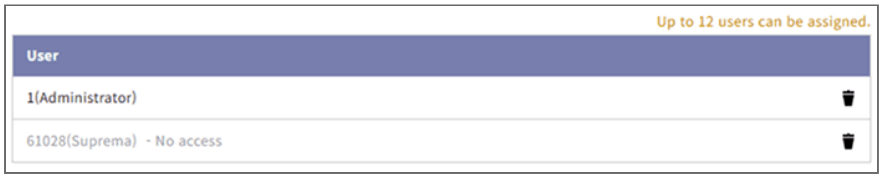
8. すべての設定が完了したら、画面最下部の **Apply** ボタンをクリックします。

情報

- スケジュール追加の詳細は スケジュールを設定するを参照してください。
- 入退室グループとアクセスレベル設定の詳細は 入退室制御設定を参照してください。

注意事項

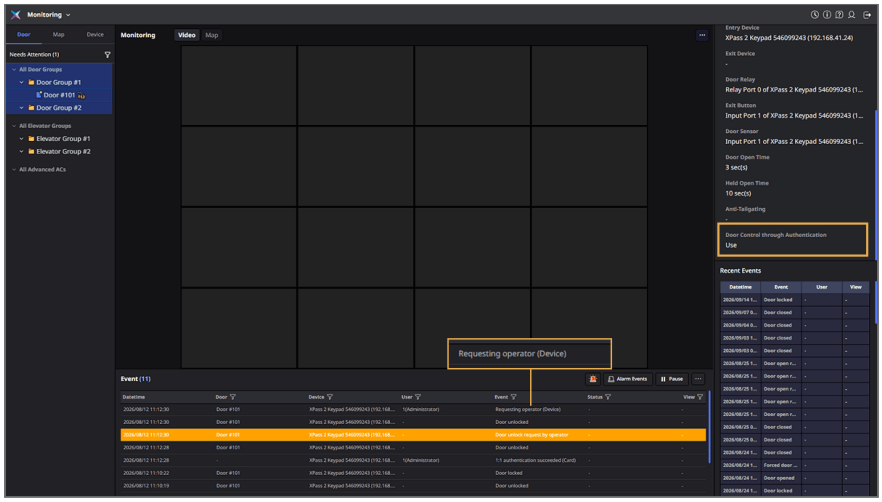
- 認証によるドア制御を使用中のドアは、入室デバイスまたは退室デバイスを非対応モデルに変更できません。デバイスを変更する前に、**Door Control through Authentication** オプションを **OFF** に設定してください。
- 制御権限ユーザーとして指定されたユーザーが、入退室グループの変更などで該当ドアの入退室権限を失うと、一覧では **No access** 状態として区別して表示します。この状態では保存できません。入退室権限を再付与するか、一覧から削除してください。



- 制御権限ユーザーを誰も指定していない状態では保存できません。
- 指定したスケジュールが削除されると、**Schedule** フィールドに **Deleted Schedule** と表示します。この状態では保存できません。別のスケジュールを選択してください。
- アンチパスバック違反が発生すると入室を拒否するハード（Hard）モードでは、認証による扉制御は動作しません。入室を許可するソフト（Soft）モードでは動作します。
- 火災警報、スケジュールロック、スケジュール開放など他の高度な入退室管理機能が適用されている場合、適用済みの高度な入退室管理機能が優先されます。

関連情報

- 認証によるドア制御の状態は、**Monitoring** 画面のドアプレビューパネルで確認できます。認証によるドア制御で発生した記録は、**Event** 一覧で **Requesting operator** として表示します。ドアモニタリングの詳細については、ドアをモニタリングを参照してください。

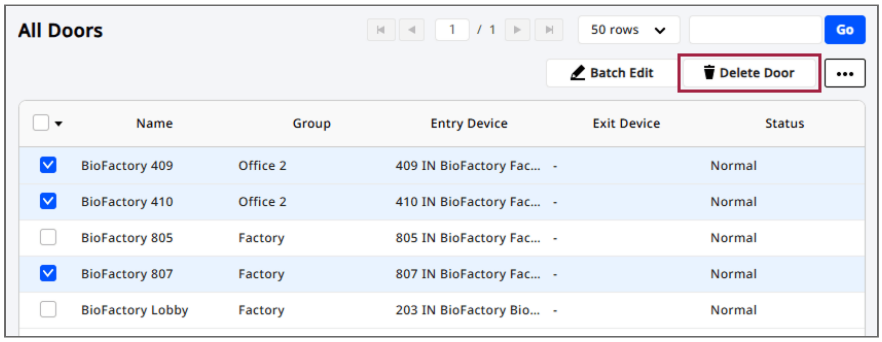


- 設定変更履歴は監査証跡に記録します。詳しくは 入退室管理の監査ログを確認する をご参照ください。

ドアを削除する

登録されたドアを削除する方法を説明します。

1. **Launcher**ページで**Settings**をクリックします。
2. 画面左側のサイドバーで **Access Point** → **Door** をクリックしてください。
3. ドア一覧で、削除したいドアのチェックボックスをクリックします。
4. 画面右上の **Delete Door** ボタンをクリックします。



5. 確認メッセージが表示されたら、**Yes** ボタンをクリックします。

選択したドアが削除されます。削除したドアは復元できません。

> **情報**
> ドアー覧で1つ以上のドアを選択すると、**Delete Door** ボタンが有効になります。

運用権限管理

登録したユーザーに運用権限を付与し、カスタム権限を追加して設定する方法を案内します。運用権限は、ユーザーが Biostar X で実行できる作業を制御する機能です。**カスタム権限** は、基本の運用権限に加えて追加の権限を設定できる機能です。

権限の種類を確認する

Launcherページで**Settings**をクリックします。画面左のサイドバーで **Account** → **Account** をクリックします。権限制に応じてデフォルトで提供されるアカウントを参照する。

- **Administrator**：すべてのメニューを使用できる管理者権限レベルです。
- **User Operator**：**User** メニューに対する **読み取り**、**編集** 権限を持ちます。 **User** メニュー以外の設定グループに対する権限はありません。
- **Monitoring Operator**：**Monitoring** と **Data** メニューに対する **読み取り**、**編集** 権限を持ち、**Dashboard** メニューに対する **読み取り** 権限を持ちます。
- **T&A Operator**: **TIME ATTENDANCE** メニューの閲覧、編集権限を持ち、**User** メニューの閲覧権限を持ちます。
- **Visitor Operator**：**VISITOR** メニューで **読み取り**、**編集** 権限を持ちます。

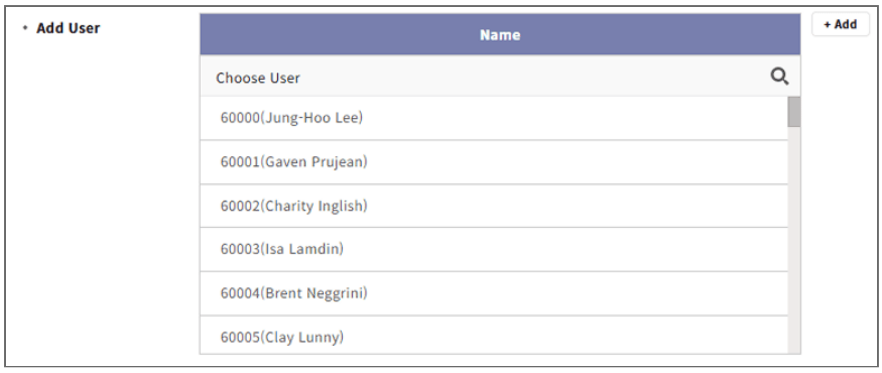
> **情報**
> - **Monitoring** メニューの **編集** 権限では、タブを追加したり、状態ツリー項目を制御したりできます。
> - **Data** メニューの **編集** 権限では、レポートの保存、レポートの自動スケジュール追加、設定へのアクセスができます。
> - 既定のユーザー権限以外の新しいユーザー権限を追加するには、カスタム権限を追加するを参照してください。
> - 既定のアカウントの権限は変更または削除できません。
> - **T&A Operator** および **Visitor Operator** 権限レベルには別途ライセンスが必要です。ライセンス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。

ユーザーに運用権限を付与する

一般ユーザーに運用権限を付与する方法を案内します。

1. **Launcher**ページで**Settings**をクリックします。
2. 画面左のサイドバーで **Account** → **Account** をクリックします。
3. アカウント一覧で目的の項目をクリックする。

4. **Add User** オプションで **+ Add** をクリックする。



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。

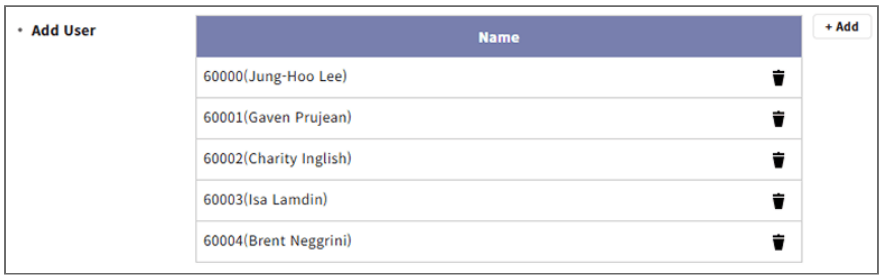
5. ユーザー一覧で運用権限を付与するユーザーを選択する。
6. 目的のユーザーをすべて選択したら、画面下部の **Apply** をクリックする。

> **情報**
>
> - ユーザーが多くて探しにくい場合は 🔍 をクリックして目的のユーザーを検索し、選択できる。
> - 運用権限はユーザー情報の追加や変更時にも付与できる。詳しくは[ユーザー権限を設定する]をご覧ください。
> - ユーザー情報を追加または変更する際に権限をすでに設定している場合、**Add User** オプションに追加されている。

運用権限を除外する

ユーザーに付与した運用権限を除外する方法を案内します。

1. **Launcher**ページで**Settings**をクリックします。
2. 画面左のサイドバーで **Account** → **Account** をクリックします。
3. アカウント一覧で目的のアカウント種類をクリックする。
4. **Add User** オプションで運用から除外するユーザーの 🗑 をクリックする。

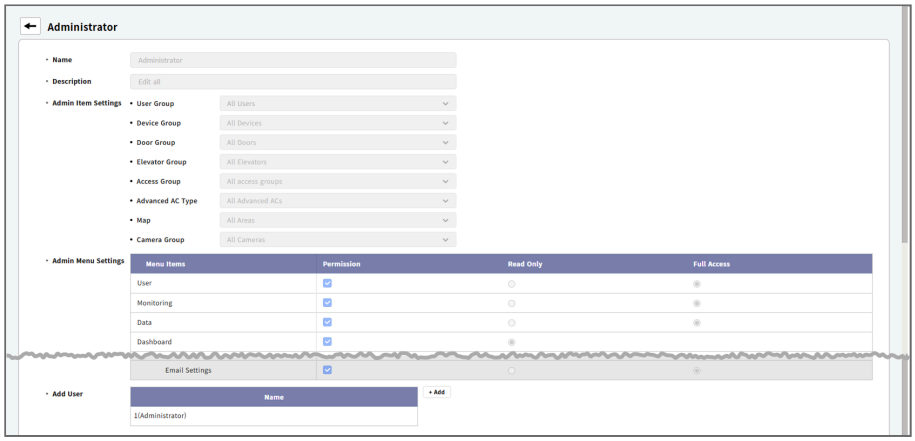


上記の画像は例示です。実際の画面とは異なる場合があります。

5. 設定を保存するには、画面最下部の **Apply** をクリックします。

運用権限の詳細を確認する

Account メニューのアカウント一覧でアカウントをクリックすると、そのアカウントの運用権限の詳細を確認できる。



- **Name**：選択した運用権限の名前。
- **Description**：権限の簡単な説明を確認できる。
- **Admin Item Settings**：アイテム別に権限が付与されているグループを確認できる。
- **Admin Menu Settings**：メニューにアクセスできる権限を確認できる。
  - **Read Only**：該当メニューの項目を追加、編集、削除できる権限を付与します。
  - **Full Access**：該当メニューへアクセスし、設定内容を確認のみできる権限を付与します。
- **Add User**：権限が付与されているユーザーを確認できる。

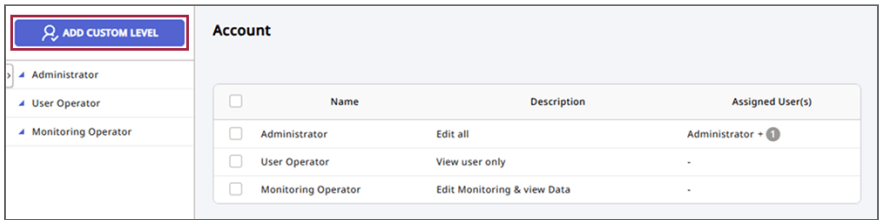
> **情報**
> 特定のユーザーに権限を付与する方法はユーザーに運用権限を付与するを参照してください。

カスタム権限を追加する

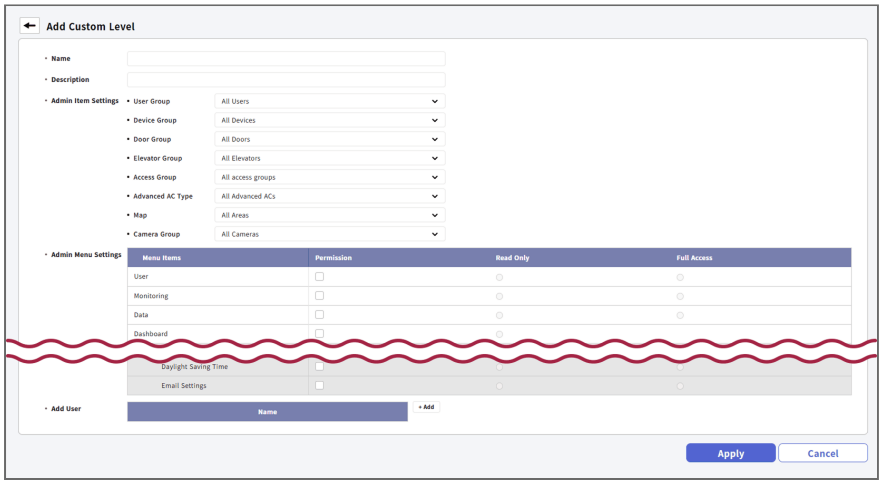
ユーザーが希望する権限レベルを追加する方法を説明します。カスタム権限は、基本の運用権限に加えて追加の権限を設定できるユーザー向けの機能です。

カスタム権限の追加

1. **Launcher**ページで**Settings**をクリックします。
2. 画面左のサイドバーで **Account** → **Account** をクリックします。
3. **Add Custom Level** をクリックします。



4. 新しく作成する権限の名前と説明を入力します。

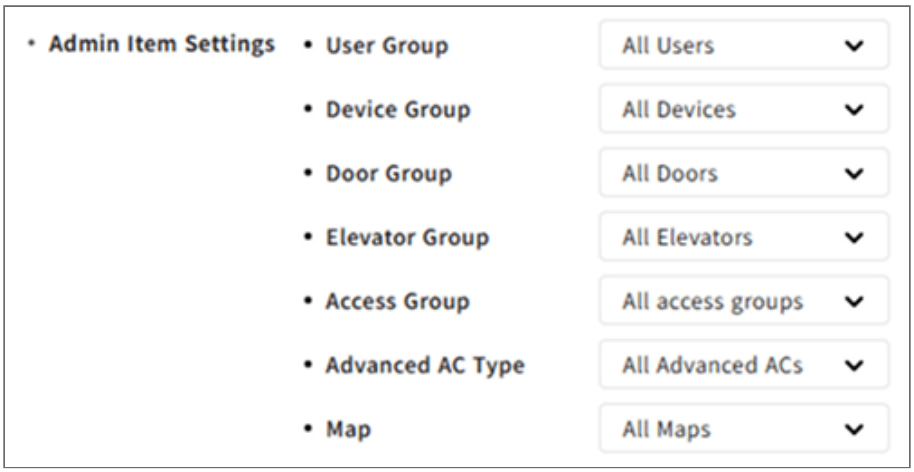


5. 残りの各項目を入力または選択します。
6. 設定を保存するには、画面最下部の **Apply** をクリックします。

> **情報**
>
> - **Admin Menu Settings** で設定できる項目は、有効化されているライセンスの種類によって異なる場合があります。
> - **Admin Item Settings**については、detailSettingをご参照ください。
> - **Admin Menu Settings**については、menuSettingをご参照ください。
> - **Add User**については、addUserをご参照ください。

Admin Item Settings

アイテムの詳細な権限を設定します。各メニューに対して編集権限および閲覧権限を付与するグループを選択できます。アイテム詳細権限は **User Group**、**Device Group**、**Door Group**、**Access Group** に対して設定でき、各メニューで既に作成されているグループ情報を基に設定できます。

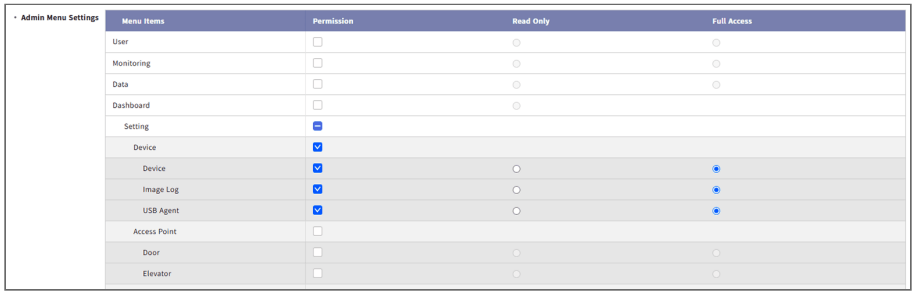


情報

- 目的のグループがない場合は、該当メニューに移動して新しいグループを追加します。グループの追加の詳細については、次のドキュメントを参照してください。
  - ユーザーグループを管理する
  - デバイスグループを管理する
  - ドアグループを管理する
  - エレベーターグループを管理する
  - アクセスグループを管理する
- **Map** 権限は **エッセンシャル**（Essential）ライセンス以上で利用できます。ライセンスポリシーの詳細については、ライセンス ポリシーをご参照ください。
- **Elevator Group**、**Advanced AC Type**、**Camera Group** 権限は **エッセンシャル**（Essential）ライセンス以上で、追加オプションにより利用できます。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。

Admin Menu Settings

個別メニューに対して **Read Only** または **Full Access** を選択できます。メニューごとに異なる権限を設定できます。権限を付与するメニューの **Permission** チェックボックスをクリックし、**Read Only** または **Full Access** を選択します。



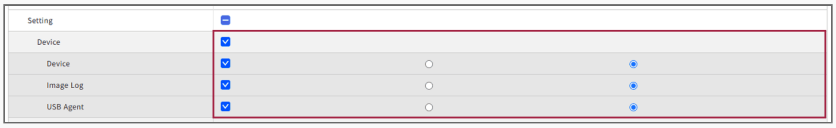
- **Read Only**：該当メニューへアクセスし、設定内容を確認のみできる権限を付与します。
- **Full Access**：該当メニューの項目を追加、編集、削除できる権限を付与します。

情報

- **Monitoring** メニューの **Full Access** は、タブを追加したり、状態ツリーの項目を制御したりできます。
- **Data** メニューの **Full Access** は、レポートを保存し、自動レポートのスケジュールを追加し、設定にアクセスできます。
- **Dashboard** メニューでは、**Read Only** 権限だけでも新しいダッシュボードとウィジェットを作成できます。
- **Menu Items** 一覧にないメニューは、権限に関係なくアクセスできます。

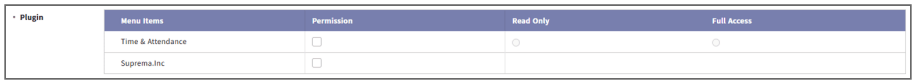
ヒント

上位メニューの権限をクリックすると、下位のすべてのメニューの権限が有効になります。



プラグイン

プラグインを追加した場合、プラグイン権限を設定できます。プラグイン権限がないユーザーは該当プラグインにアクセスできず、初期画面やランチャーに表示されません。

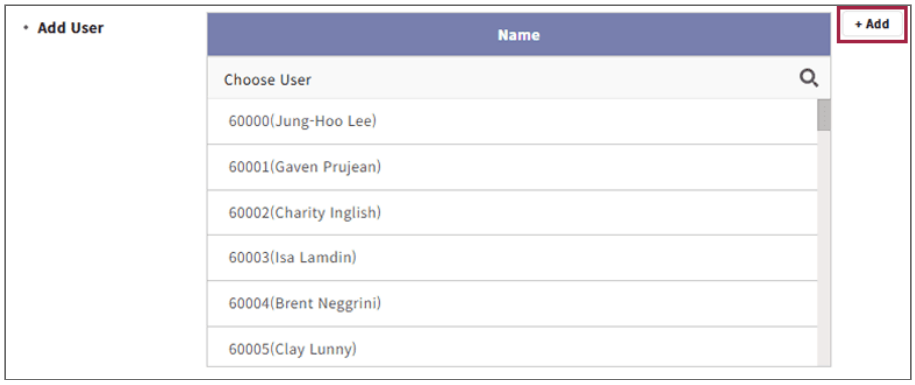


情報

- プラグイン機能を使用するには、プラグイン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。
- **Time & Attendance** プラグインにのみ **Read Only** または **Full Access** を適用できます。

Add User

権限を付与するユーザー情報を追加または確認できます。ユーザーを追加するには **+ Add** をクリックします。ユーザー一覧から権限を付与するユーザーを選択します。



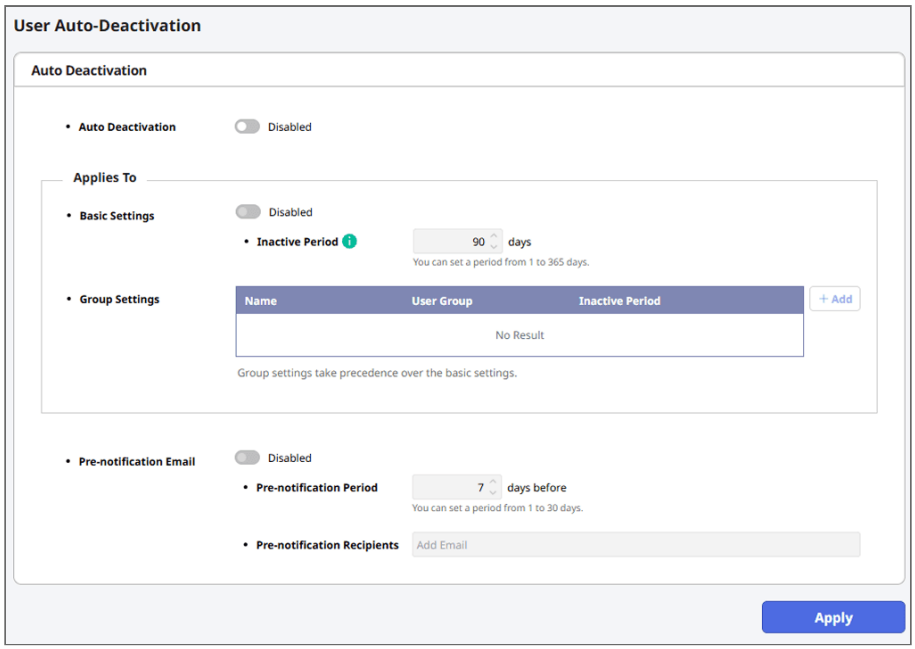
情報

ユーザー一覧でユーザーの をクリックすると、そのユーザーは権限から除外されます。

長期間未入退室ユーザーへの対処

退職や休職などで長期間入退室しないユーザーのクレデンシャルを残すと、なりすましや不正入退室などのセキュリティ脅威につながる可能性があります。自動無効化機能を使用すると、最終入退室以降に一定期間が経過したユーザーを自動で無効化します。管理者は手動で毎回整理せずに、ユーザーアカウントを安全に管理できます。自動で無効化する前に、指定した受信者へ事前通知メールを送信します。事前に確認したり、例外処理したりする時間を確保できます。

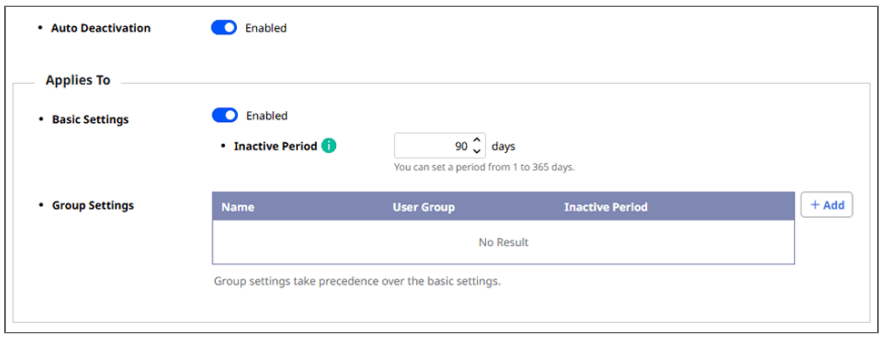
Launcherページで**Settings**をクリックします。画面左のサイドバーで **Account** → **User Auto-Deactivation** をクリック。



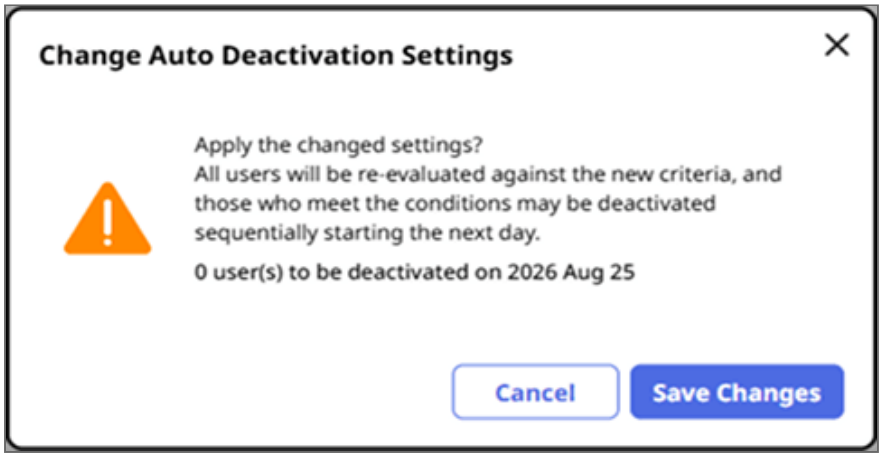
> **情報**
>
> **Account** → **User Auto-Deactivation** メニューには、当該メニューの権限を持つ管理者のみアクセスできます。特定のメニュー権限を管理者に付与する方法は、運用権限管理 を参照してください。

自動無効化の設定

1. **Auto Deactivation** オプションでトグルボタンをクリックして有効化してください。
2. **Applies To** セクションで、自動無効化の適用対象を設定してください。



   - すべてのユーザーに同一基準を適用する場合は、**Basic Settings** オプションでトグルボタンをクリックして有効化し、**Inactive Period** を入力してください。設定範囲は 1 日から 365 日です。
   - 特定のユーザーグループに異なる基準を適用する場合は、**Group Settings** を追加してください。追加方法は グループ別に異なる基準を適用 を参照してください。
3. 設定が完了したら、画面最下部の **Apply** ボタンをクリックしてください。
4. 確認画面が表示されたら、次回の自動処理予定日と無効化予定ユーザー数を確認し、**Save Changes** ボタンをクリックしてください。



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。

情報

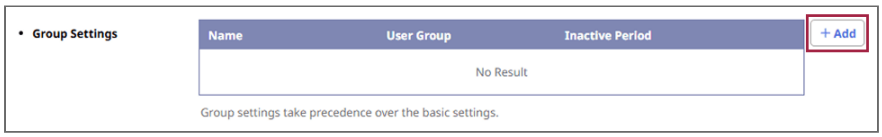
- ユーザーが自動で無効化される前に、指定した受信者へメールで事前通知するには、**Pre-notification Email** で設定します。詳細については、事前通知メールの設定をご参照ください。
- **Auto Deactivation** オプションを有効化しても、**Basic Settings** オプションは自動で有効になりません。 **Group Settings** のみでポリシーを構成する場合は、**Basic Settings** オプションを無効のままにしてください。
- 自動無効化は、最後に入退室認証した時刻を基準に判定します。入退室履歴がないユーザー、またはユーザー登録前の入退室履歴のみがあるユーザーは、無効化の対象外です。
- あるユーザーが **Basic Settings** と **Group Settings** の両方に該当する場合、**Group Settings** の **Inactive Period** が優先して適用されます。 2 つ以上の **Group Settings** に属する場合、そのうち最も短い **Inactive Period** が適用されます。
- 自動無効化は毎日1回（真夜中）実行されます。設定を変更してもすぐには反映されず、次回の処理時点から適用されます。すでに送信された事前通知のスケジュールには影響しません。
- **Auto Deactivation** オプションを無効にすると、確認メッセージを表示せずにすぐ保存されます。

グループ別に異なる基準を適用

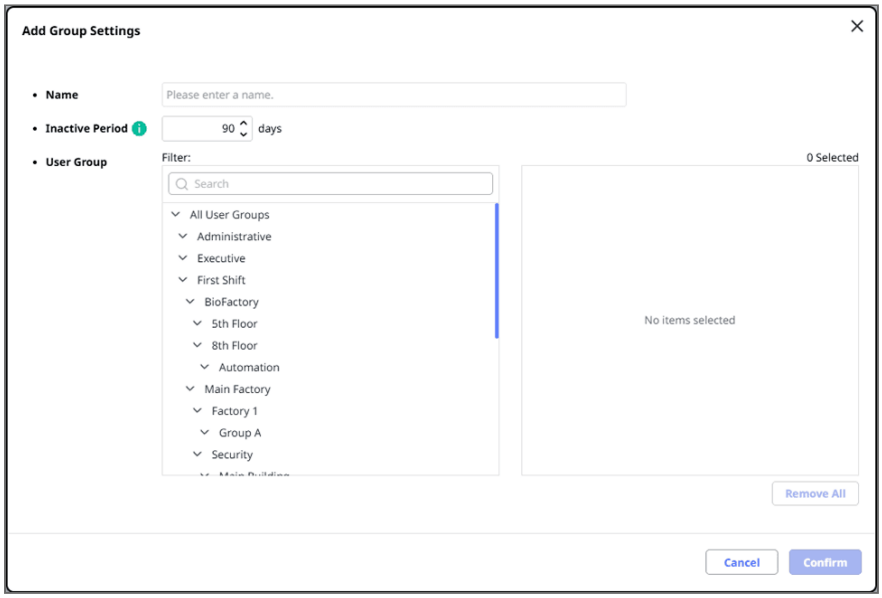
特定のユーザーグループには、**Basic Settings** と異なる **Inactive Period** を適用できます。

グループ設定を追加

1. **Group Settings** リストの右側にある **+ Add** ボタンをクリックします。



2. **Add Group Settings** ウィンドウが表示されたら、各項目を設定します。

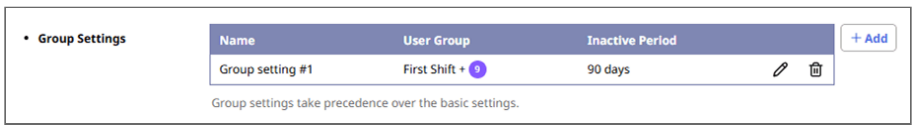


- **Name**: 他のグループ設定と重複しない名前を入力します。大文字と小文字、前後の空白は区別しません。
- **Inactive Period**: 最小 1 日から最大 365 日まで設定できます。
- **User Group**：適用するユーザーグループを選択します。グループを選択すると、下位のユーザーグループも一緒に選択されます。

3. ユーザーグループの選択を終えたら、**Confirm** ボタンをクリックします。
4. 変更を保存するには、画面の一番下にある **Apply** ボタンをクリックします。
5. 確認画面が表示されたら、次回の自動処理予定日と無効化予定ユーザー数を確認し、**Save Changes** ボタンをクリックしてください。

> **情報**
>
> - **User Group** では、管理者の権限範囲外のユーザーグループは選択できないよう無効で表示されます。リストからは非表示になりません。このグループは展開でき、下位グループのうち権限範囲内のグループは選択できます。
> - 管理者権限が **すべてのユーザー** に設定された管理者、またはスーパー管理者は、ユーザーグループの選択に制限がありません。管理者権限の詳細については 運用権限管理 をご覧ください。

グループ設定を編集または削除



- 編集するには、**Group Settings** リストで対象行の ボタンをクリックし、値を変更してから **Confirm** ボタンをクリックします。
- 削除するには、対象行の ボタンをクリックします。確認メッセージが表示されたら **Delete** ボタンをクリックします。

修正または削除した内容を保存するには、画面最下部の **Apply** ボタンをクリックしてください。確認画面が表示されたら、次回の自動処理予定日と無効化予定ユーザー数を確認し、**Save Changes** ボタンをクリックしてください。

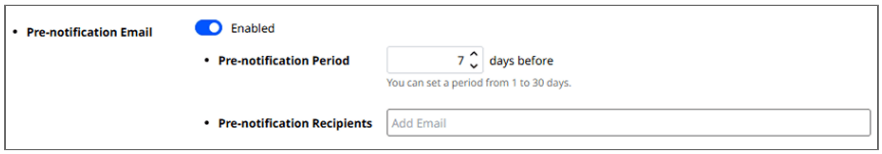
情報

- **Group Settings** に管理者の権限範囲外のユーザーグループが含まれている場合、リストには表示され続けますが、編集と削除はできません。
- **Group Settings**は**Basic Settings**より優先します。
- **Group Settings** を削除しても、すでに無効化されたユーザーは復元されません。削除後、該当ユーザーに適用可能な別の設定（**Basic Settings** など）がある場合、その設定に切り替わります。

事前通知メールの設定

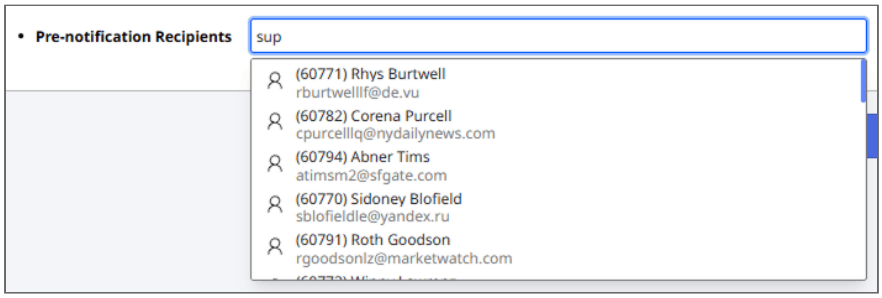
ユーザーが自動的に無効化される前に、指定した受信者へメールで事前通知できます。

1. **Pre-notification Email** オプションでトグルボタンをクリックして有効にしてください。



2. **Pre-notification Period** を入力してください。入力した期間だけ、自動無効化の通知メールを送信します。最小 1 日から最大 30 日まで設定できます。

3. **Pre-notification Recipients** 入力フィールドで名前、ID、メールでユーザーを検索して選択するか、メールアドレスを直接入力して Enter キーを押してください。



4. 設定が完了したら、画面最下部の **Apply** ボタンをクリックしてください。

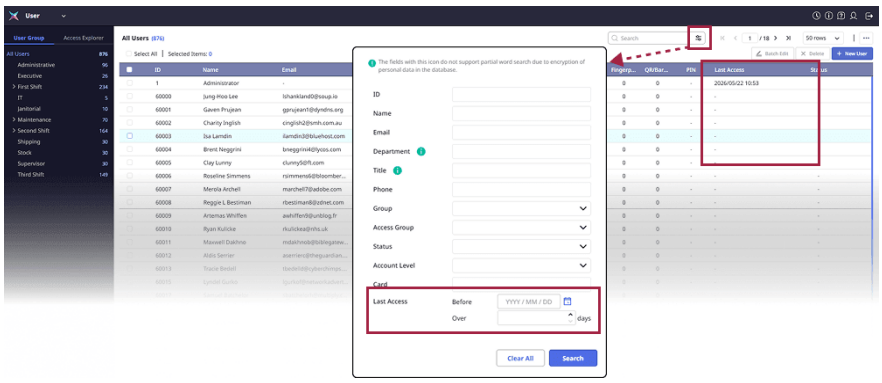
5. 確認画面が表示されたら、次回の自動処理予定日と無効化予定ユーザー数を確認し、**Save Changes** ボタンをクリックしてください。

情報

- 事前通知メールを使用するには、SMTP 設定を完了しておく必要があります。詳細については、メールを設定するご参照ください。
- **Pre-notification Period** は、**Basic Settings** とすべての **Group Settings** の未入退室期間より短く設定する必要があります。
- **BioStar X** に登録されていないメールアドレスも受信者に追加できます。
- 無効化予定のユーザーには、ユーザー別の個別メールではなく、毎日1回、統合メールとして送信されます。
- **Basic Settings** が無効で **Group Settings** もない状態で **Pre-notification Email** だけを有効にすると、適用対象がないためメールは送信されません。

関連情報

- 長期未入退室ユーザーは、ユーザーリストの **Last Access** 列、または詳細検索で確認できます。詳しくは ユーザーを閲覧する をご参照ください。

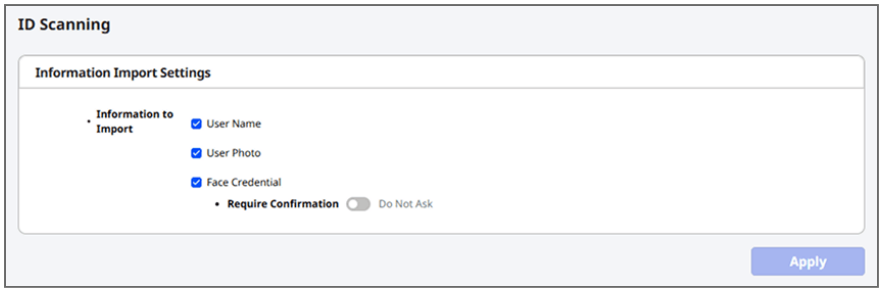


- 自動および手動で無効化されたユーザーの履歴は、**Inactive Users** レポートで確認できます。詳しくは レポートを作成する をご参照ください。

身分証明書スキャンを設定する

身分証明書スキャンでユーザーを登録する前に、スキャン時に取得するユーザー名、プロフィール画像、顔クレデンシャルの登録方式を事前に設定してください。本ドキュメントでは身分証明書スキャンの設定方法を案内します。

1. **Launcher**ページで**Settings**をクリックします。
2. 画面左のサイドバーで **Account** → **ID Scanning** をクリックします。



3. 身分証明書をスキャンする際に取得するデータを選択してください。
   - **User Name**：身分証明書に記載された氏名を取得します。
   - **User Photo**：身分証明書に記載されたプロフィール画像を取得します。
   - **Face Credential**：身分証明書に記載された顔画像を顔クレデンシャルとして登録します。
     - **Require Confirmation**：身分証明書に記載された顔画像を顔クレデンシャルとして登録する際、毎回確認します。
     - **Do Not Ask**：身分証明書に記載された顔画像を顔クレデンシャルとして登録する際、確認せずに登録します。
4. 設定を保存するには、**Apply** をクリックします。

情報

- **User Photo** オプションが選択されていない場合、**Face Credential** オプションは選択できません。
- 身分証明書をスキャンしてユーザーを登録または修正する方法の詳細については、身分証明書のスキャンでユーザーを登録、編集するを参照してください。

入退室制御設定

アクセス制御システムの設定方法を説明します。ドアと入退室時間を設定してアクセスレベルを作成し、アクセスレベルとユーザーグループ情報を用いてアクセスグループを設定できます。設定したアクセスグループはアクセス制御の構成に使用します。

アクセスレベルを管理する

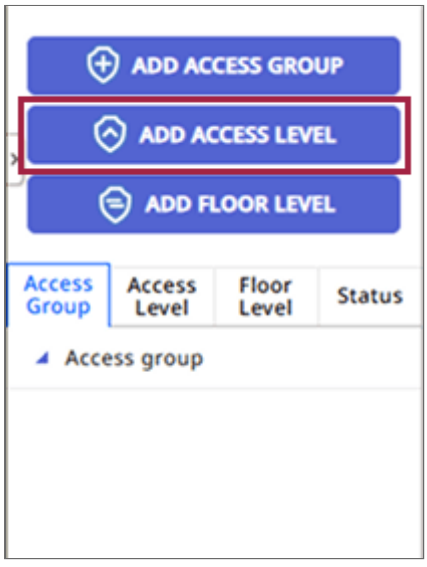
アクセスレベルとは、ユーザーが通行できる時間を設定し、その時間内にドアを出入りできる権限です。アクセスレベルはアクセスグループを設定するうえでの主要要素です。

開始前に

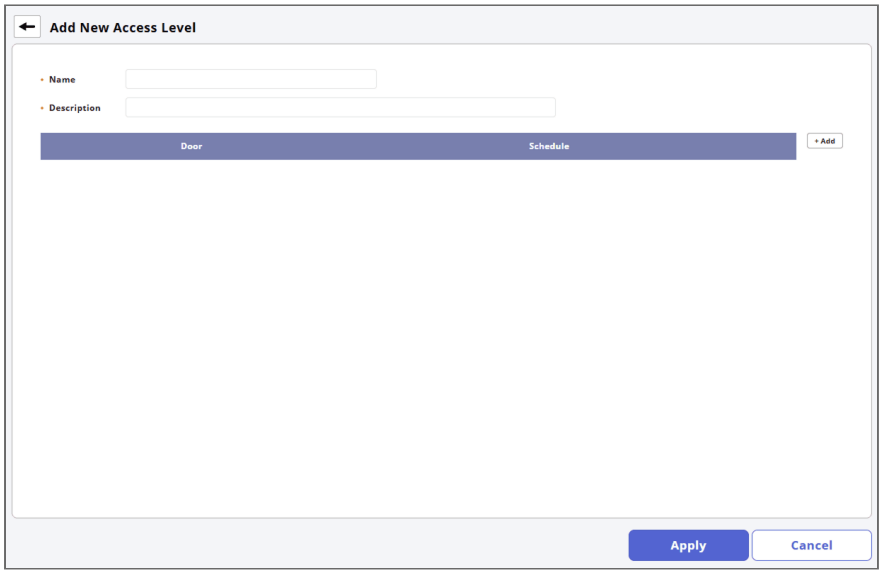
- アクセスレベルを登録する前にドアを設定します。出入口の登録の詳細については、ドアを登録するを参照してください。
- スケジュール設定で、アクセスレベルに適用する時間をあらかじめ定義できます。スケジュール設定の詳細については、スケジュールを設定するをご参照ください。

アクセスレベルの登録

1. **Launcher**ページで**Settings**をクリックします。
2. 画面左のサイドバーで **Access Management** → **Access Control** をクリック。
3. **ADD ACCESS LEVEL** をクリックします。



4. **Add New Access Level** 画面で **Name** と **Description** を入力します。

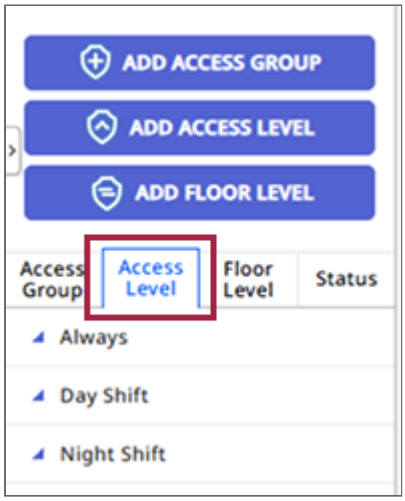


5. **Door** 項目で、アクセスレベルに適用するドアを選択します。
6. **Schedule** 項目で、アクセスレベルに適用するスケジュールを選択します。
7. 画面下部の **Apply** をクリックしてアクセスレベルを登録します。

> **情報**
>
> - アクセスレベルはアクセスグループごとに最大128件まで登録できます。
> - **Door** と **Schedule** 項目で 🔍 をクリックして、目的のドアとスケジュールを検索します。
> - **Door** と **Schedule** 項目で追加した項目を削除するには 🗑 をクリックします。
> - 目的のドアが見つからない場合は、新しいドアを登録します。出入口の登録の詳細については、ドアを登録するを参照してください。
> - 目的のスケジュールがない場合は、**+ Add Schedule** をクリックして追加します。スケジュール設定の詳細については、スケジュールを設定するをご参照ください。

アクセスレベルの修正

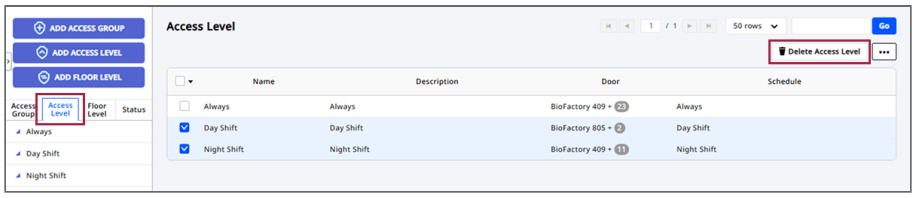
1. **Launcher**ページで**Settings**をクリックします。
2. 画面左のサイドバーで **Access Management** → **Access Control** をクリックします。
3. **Access Level** タブをクリックします。



4. アクセスレベルリストで編集するアクセスレベルをクリックします。
5. 必要な項目を編集します。
6. 編集が完了したら、画面下部の **Apply** をクリックします。

アクセスレベルの削除

1. **Launcher**ページで**Settings**をクリックします。
2. 画面左のサイドバーで **Access Management** → **Access Control** をクリックします。
3. **Access Level** タブをクリックします。
4. アクセスレベルリストで削除するアクセスレベルのチェックボックスをクリックします。
5. 画面右上の **Delete Access Level** をクリックします。



アクセスグループを管理する

入退室レベルとユーザーグループ情報を用いてアクセスグループを設定する方法を説明します。アクセスグループはドアの入退室権限を設定する重要な要素です。アクセスグループを設定すると、ユーザーのドア入退室権限を管理できます。

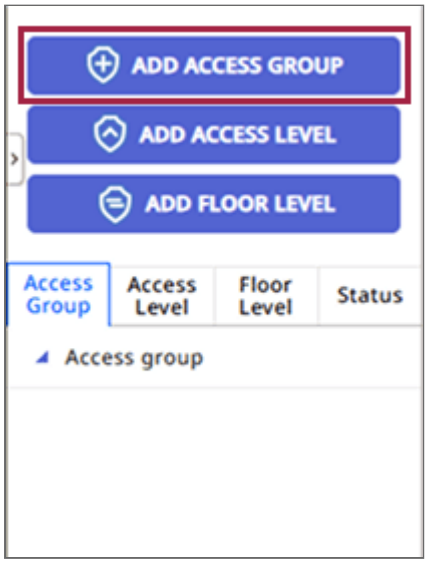
開始前に

アクセスグループを登録する前に、次の事項を確認してから進めてください。

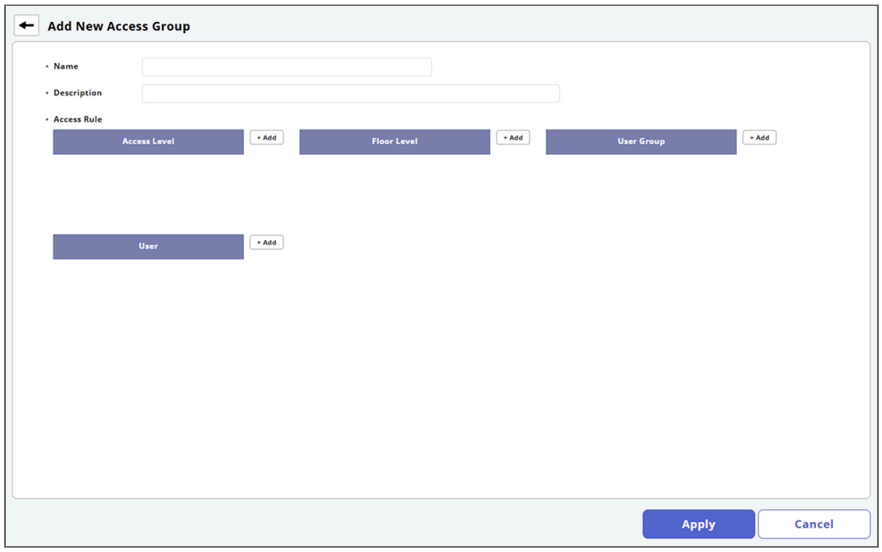
- 入退室レベルを設定します。入退室レベルの登録について詳しくは、アクセスレベルを管理するをご参照ください。
- フロアレベルを設定します。フロアレベルの登録に関する詳細はフロアレベルを管理するをご参照ください。
- ユーザーグループを設定します。ユーザーグループの登録に関する詳細はユーザーグループを管理するをご参照ください。

アクセスグループを登録する

1. **Launcher**ページで**Settings**をクリックします。
2. 画面左のサイドバーで **Access Management** → **Access Control** をクリックします。
3. **ADD ACCESS GROUP** をクリックします。



4. **Add New Access Group** 画面で、**Name** と **Description** を入力します。



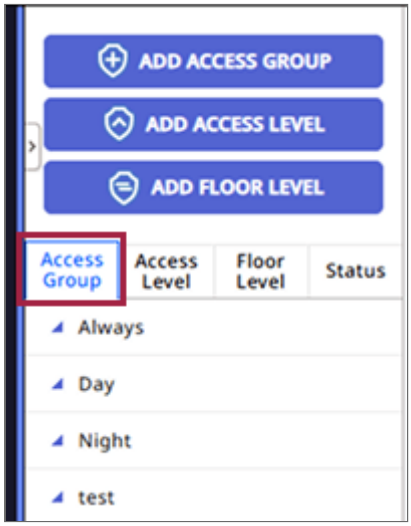
5. **Access Level** 項目で **+ Add** をクリックし、アクセスグループに適用する入退室レベルを選択します。
6. **Floor Level** 項目で **+ Add** をクリックし、アクセスグループに適用するフロアレベルを選択します。
7. **User Group** 項目で **+ Add** をクリックし、アクセスグループに適用するユーザーグループを選択します。
8. **User** 項目で **+ Add** をクリックし、アクセスグループに追加するユーザーを選択します。
9. アクセスグループを登録するには、画面下部の **Apply** をクリックします。

情報

- 必要な入退室レベルがない場合は、新しい入退室レベルを登録する必要があります。入退室レベルの登録について詳しくは、アクセスレベルを管理するをご参照ください。
- 必要なフロアレベルがない場合は、新しいフロアレベルを登録する必要があります。フロアレベルの登録に関する詳細はフロアレベルを管理するをご参照ください。
- 追加した項目を削除するには をクリックします。
- 項目を検索するには をクリックします。

アクセスグループを編集する

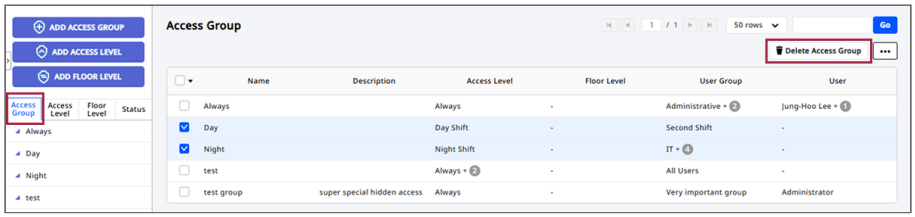
1. **Launcher**ページで**Settings**をクリックします。
2. 画面左のサイドバーで **Access Management** → **Access Control** をクリックします。
3. **Access Group** タブをクリックします。



4. アクセスグループ一覧で、編集するアクセスグループをクリックします。
5. 必要な項目を編集します。
6. 編集が完了したら、画面下部の **Apply** をクリックします。

アクセスグループを削除する

1. **Launcher**ページで**Settings**をクリックします。
2. 画面左のサイドバーで **Access Management** → **Access Control** をクリックします。
3. **Access Group** タブをクリックします。
4. アクセスグループ一覧で、削除するアクセスグループのチェックボックスをクリックします。
5. 画面右上の **Delete Access Group** をクリックします。



フロアレベルを管理する

設定済みのエレベーターとフロア情報を使用してフロアレベルを設定する方法を案内します。フロアレベルはアクセスグループに適用できる重要な要素です。フロアレベルを設定すると、ユーザーがエレベーターでアクセスできるフロアを管理できます。

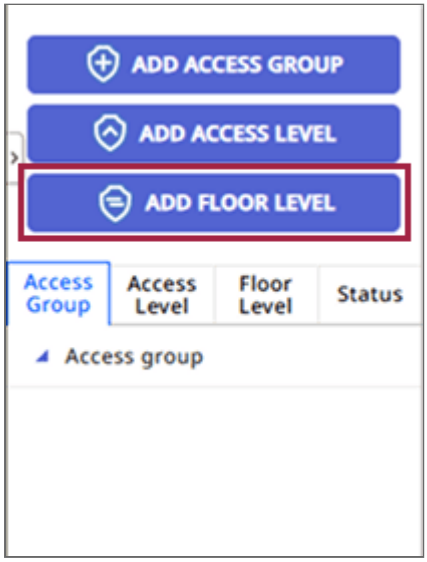
> **情報**
> フロアレベルに関連する機能は**エッセンシャル**(Essential)ライセンス以上で追加オプションとして利用できます。ライセンスポリシーの詳細については、ライセンス ポリシーをご参照ください。

開始前に

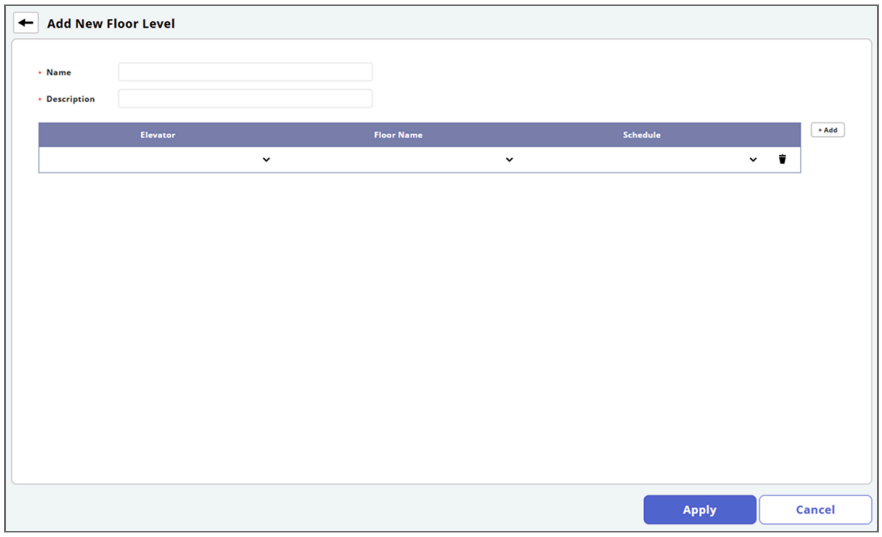
- フロアレベルを登録する前にエレベーターを設定する必要があります。エレベーターの登録について詳しくは、エレベーターを登録するをご参照ください。
- スケジュール設定によって、フロアレベルに適用する時間を事前に定義できます。スケジュール設定の詳細については、スケジュールを設定するをご参照ください。

フロアレベルを登録する

1. **Launcher**ページで**Settings**をクリックします。
2. 画面左のサイドバーで **Access Management** → **Access Control** をクリック。
3. **ADD FLOOR LEVEL** をクリックします。



4. **Add New Floor Level** 画面で、**Name** と **Description** を入力します。

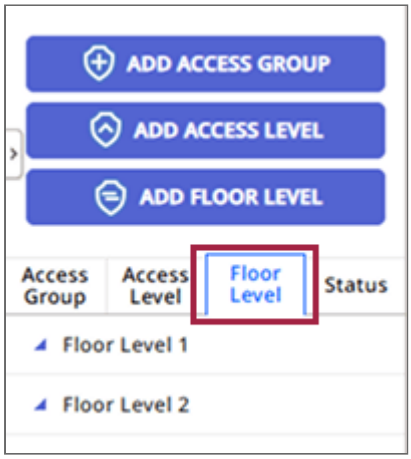


5. **Elevator** 項目でフロアレベルに適用するエレベーターを選択します。
6. **Floor Name** 項目でフロアレベルに適用するフロアを選択します。
7. **Schedule** 項目でフロアレベルに適用するスケジュールを選択します。
8. フロアレベルを登録するには、画面最下部にある **Apply** をクリックします。

> **情報**
>
> - 必要な入退室レベルがない場合は、新しい入退室レベルを登録する必要があります。入退室レベルの登録について詳しくは、アクセスレベルを管理するをご参照ください。
> - 目的のエレベーターがない場合は、新しいエレベーターを登録する必要があります。エレベーターの登録について詳しくは、エレベーターを登録するをご参照ください。
> - 目的のスケジュールがない場合は、**+ Add Schedule** をクリックして追加します。スケジュール設定の詳細については、スケジュールを設定するをご参照ください。
> - 追加した項目を削除するには をクリックします。
> - 項目を検索するには をクリックします。

フロアレベルを編集

1. **Launcher**ページで**Settings**をクリックします。
2. 画面左のサイドバーで **Access Management** → **Access Control** をクリックします。
3. **Floor Level** タブをクリックします。



4. フロアレベル一覧で編集するフロアレベルをクリックします。
5. 必要な項目を編集します。
6. 編集が完了したら、画面下部の **Apply** をクリックします。

フロアレベルを削除

1. **Launcher**ページで**Settings**をクリックします。
2. 画面左のサイドバーで **Access Management** → **Access Control** をクリックします。
3. **Floor Level** タブをクリックします。
4. フロアレベル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。
5. 画面右上の **Delete Floor Level** をクリックします。

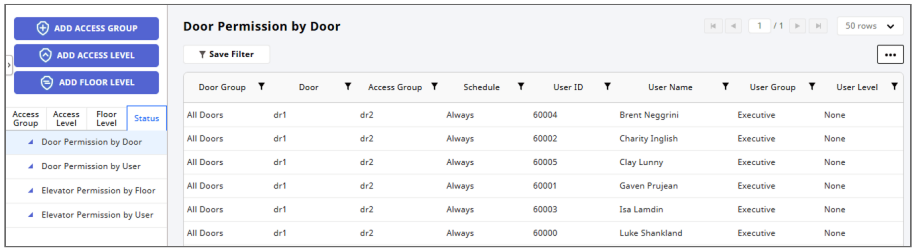


アクセス権限ステータスを確認する

ユーザーが通行できるドアの一覧を確認する方法を案内します。アクセス権限ステータスを確認すると、ユーザーが通行できるドアとそのドアに対する権限を管理できます。フィルター機能を使用して必要な結果を並べ替えたり、リストをCSVファイルとして保存したりできます。

アクセス権限ステータスの確認

アクセス権限はドアまたはフロア、ユーザーを基準に表示できます。



1. **Launcher**ページで**Settings**をクリックします。

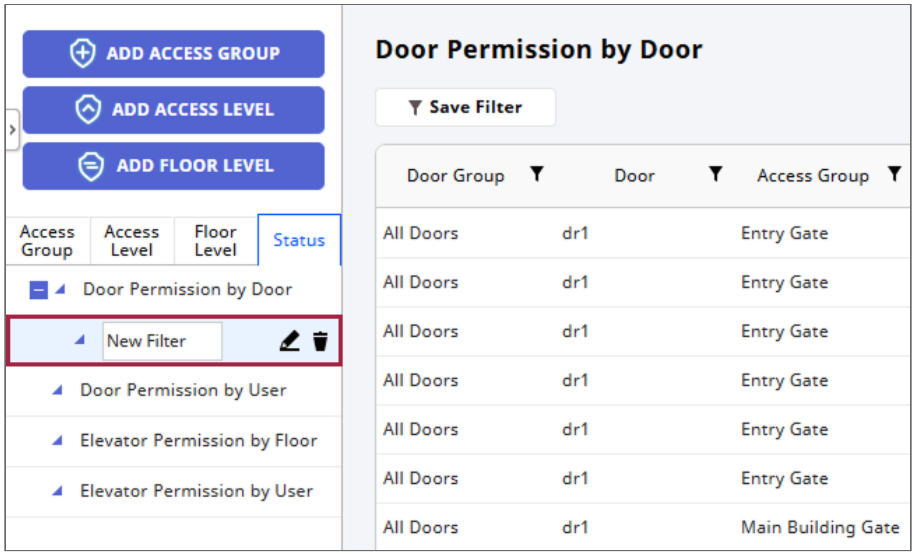
2. 画面左のサイドバーで **Access Management** → **Access Control** をクリック。
3. **Status** タブをクリックします。
4. **Status** タブの下にあるステータスリストで目的の項目をクリックします。
   - **Door Permission by Door**
   - **Door Permission by User**
   - **Elevator Permission by Floor**
   - **Elevator Permission by User**

選択した項目のアクセス権限ステータスを確認できます。

フィルターの保存

必要な結果を並べ替えるには、アクセス権限リストテーブルのヘッダーで ▼ ボタンをクリックします。フィルター条件を追加できます。

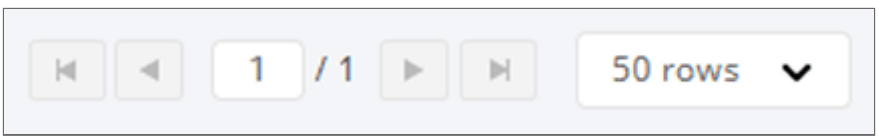
フィルターを設定した後は、フィルターを保存できます。 **Save Filter** ボタンをクリックします。保存したフィルターは、**Status** タブ下のステータスリストで確認できます。



- フィルター名を変更するには ✎ アイコンをクリックします。
- フィルターを削除するには 🗑 アイコンをクリックします。

一覧ページをナビゲートする

ページを移動したり、1ページに表示する一覧の件数を設定できます。 画面右上のページ移動ツールを使用します。



- ⏮：最初のページに移動します。
- ◀：前のページに移動します。
- ▶：次のページに移動します。

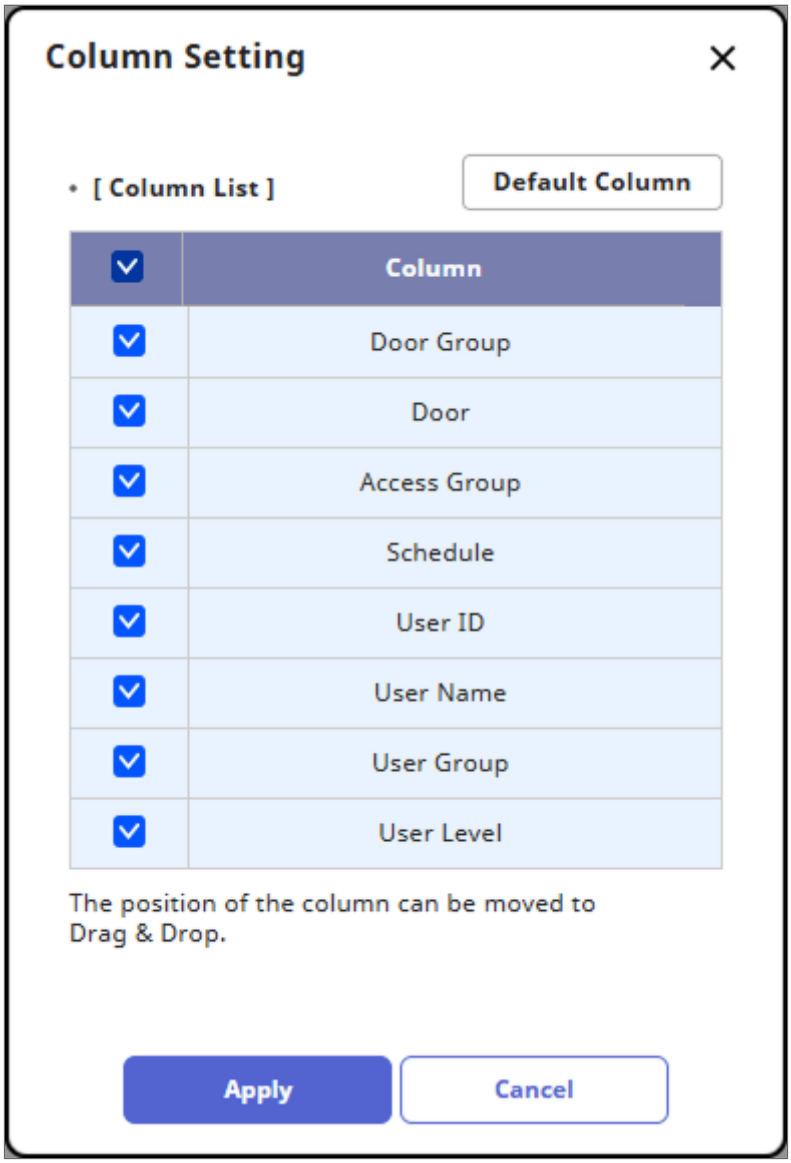
- ▶|：最後のページに移動します。
- 目的のページに移動するには、数字入力フィールドにページ番号を入力します。
- 1ページに表示する一覧の件数を設定するには、行選択ボックスをクリックします。

CSV へのエクスポート

現在表示されているアクセス権限ステータスリストをCSVファイルにエクスポートできます。画面右上の ••• ボタンをクリックし、**CSV Export** を選択します。

列設定

現在表示しているアクセス権限ステータステーブルで、必要な列を非表示または表示できます。画面右上の ••• ボタンをクリックし、**Column Setting** を選択します。



- **Column List** で表示する列を選択します。選択した列がリストテーブルに表示されます。選択しなかった列はリストテーブルで非表示になります。
- 設定を初期化するには **Default Column** ボタンをクリックします。

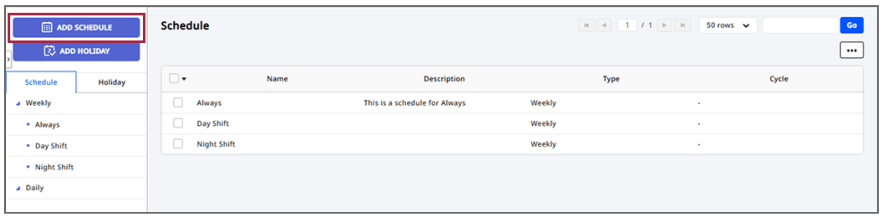
すべての設定が完了したら **Apply** ボタンをクリックします。

スケジュールを設定する

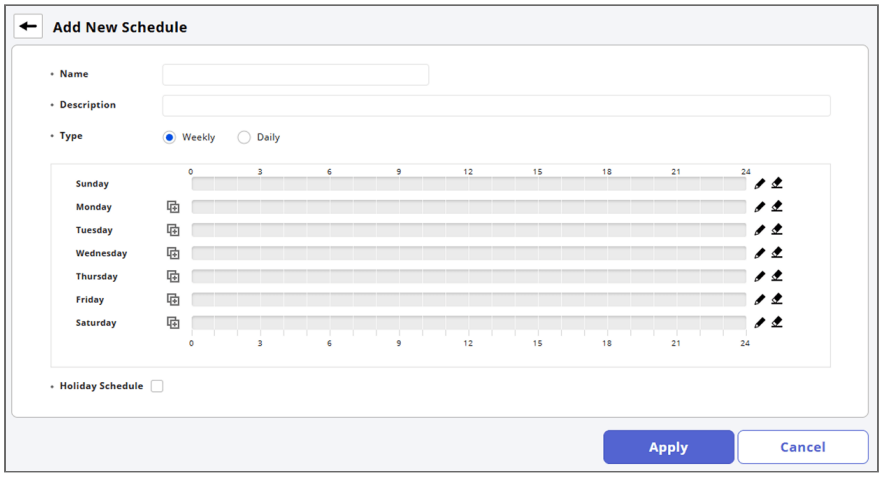
入退室および休日スケジュールを設定し、アクセス制御と勤怠管理を効率的に運用する方法を案内します。スケジュールはアクセス制御に適用できる重要な要素で、ユーザーの入退室時間と休日を管理できます。

スケジュール登録

1. **Launcher**ページで**Settings**をクリックします。
2. 画面左側のサイドバーで **Access Management** → **Schedule** をクリックしてください。
3. 画面左上の **ADD SCHEDULE** をクリックします。



4. **Add New Schedule** 画面で各項目を入力または設定します。

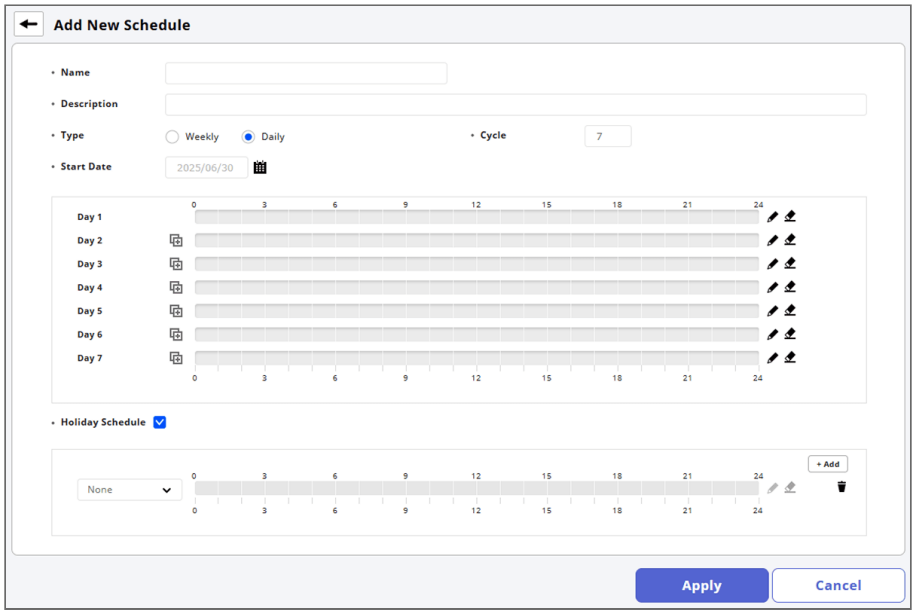


5. すべての設定が完了したら、画面下部の **Apply** をクリックします。

> **情報**
> **Add New Schedule** 画面の各項目の詳細については 新規スケジュール追加オプションの案内 を参照してください。

新規スケジュール追加オプションの案内

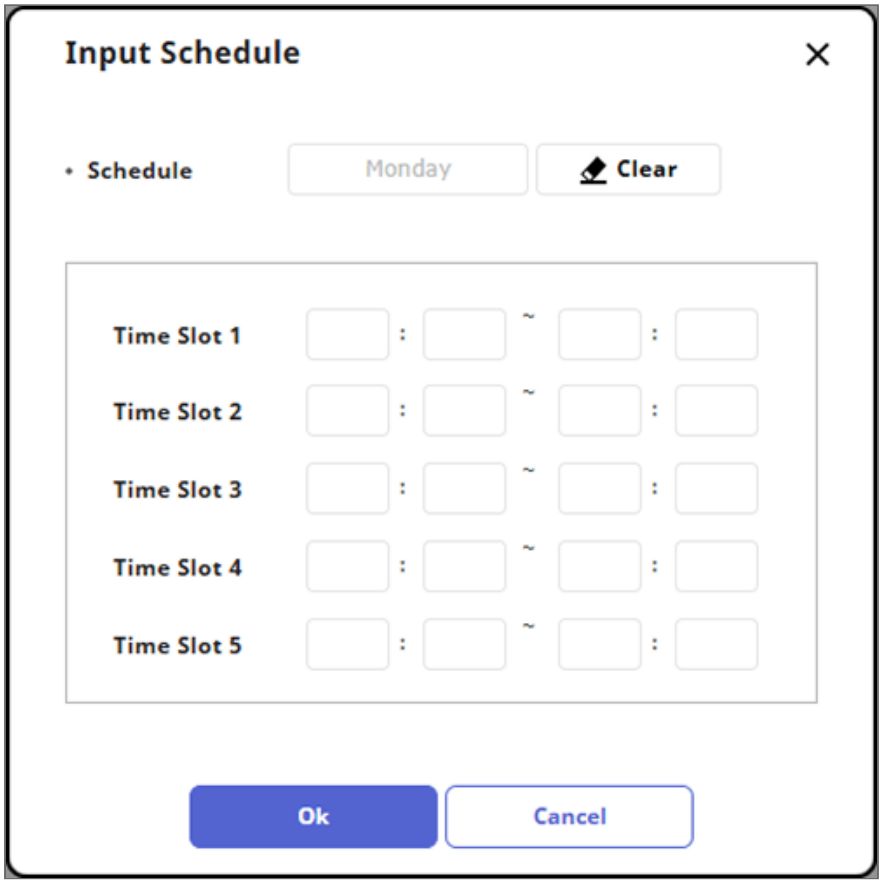
Add New Schedule 画面で設定できる各項目について説明します。



- **Name**：スケジュール名を入力します。
- **Description**：スケジュールの簡単な説明を入力します。
- **Type**：週単位または日単位のスケジュールを選択します。 **Daily** を選択すると、**Cycle** と **Start Date** を選択できます。



- 中央エリアの **Time segment** をクリックして、希望の時間を設定します。設定が完了したら、**Apply** をクリックします。



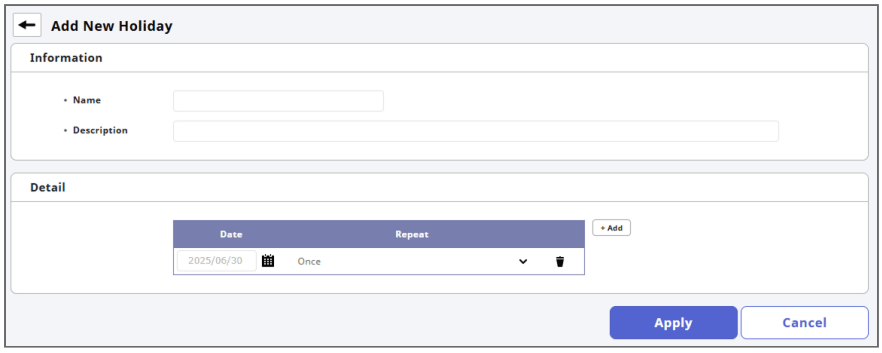
  - 曜日別・日別の時間スロットは最大5個まで設定できます。

  - スケジュールを設定して をクリックすると、直上の時間スロットをコピーできます。
  - 時間スロットを編集するには をクリックします。設定済みの時間スロットを削除するには をクリックします。
- **Holiday Schedule**：休日スケジュールを適用するかどうかを選択します。項目を選択すると詳細設定を適用できます。
  - **None** セレクトボックスで、事前に設定した休日を選択できます。休日を追加するには **+ Add** をクリックし、休日を設定します。
  - **休日時間スロット**：時間スロットをクリックして、休日に適用する時間スロットを設定します。

> **情報**
>
> - 時間スロットを編集するには をクリックします。設定済みの時間スロットを削除するには をクリックします。
> - 追加した休日を削除するには をクリックします。
> - 休日スケジュールの追加の詳細については 休日スケジュール追加 を参照してください。

休日スケジュール追加

1. **Launcher**ページで**Settings**をクリックします。
2. 画面左側のサイドバーで **Access Management** → **Schedule** をクリックしてください。
3. 画面左上の **ADD HOLIDAY** をクリックします。
4. **Add New Holiday** 画面で **Name** と **Description** を入力します。



5. **Detail** セクションで **+ Add** をクリックします。
6. をクリックして日付を選択し、繰り返し回数と期間を設定します。
7. 設定した休日スケジュールを登録するには **Apply** をクリックします。

> **情報**
>
> 休日スケジュールを削除するには をクリックします。

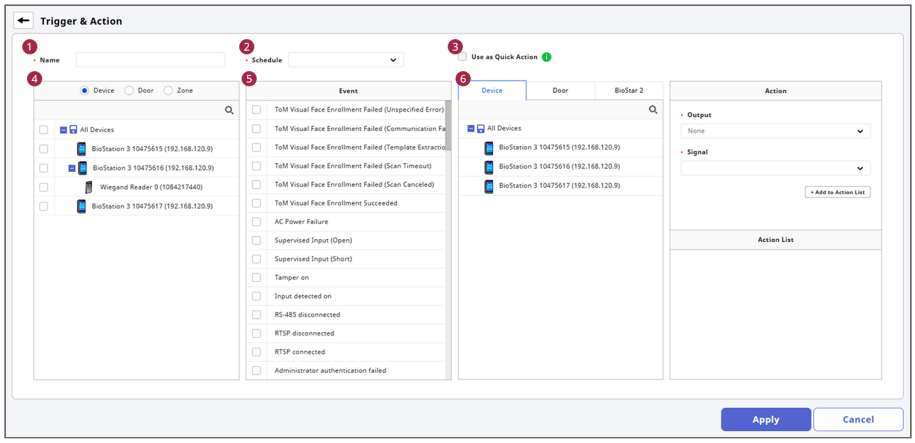
作業条件と動作を設定する

デバイス、ドア、ゾーンで特定のイベントが発生した際に、ユーザーが希望する動作をデバイスまたは BioStar X が実行するように設定できます。

1. **Launcher**ページで**Settings**をクリックします。
2. 画面左のサイドバーで **Access Management** → **Trigger & Action** をクリックします。
3. 画面左上の **Access Management** → **ADD TRIGGER & ACTION** ボタンをクリックします。



画面の案内に従って詳細項目を設定します。



1 名前の入力

Name：作業条件と動作の名前を入力します。

2 スケジュール設定

Schedule：作業条件と動作が適用されるスケジュールを設定します。

> **情報**
>
> - **Input** を選択してユーザー定義条件を設定する際、希望するスケジュールがない場合は **+ Add Schedule** をクリックして設定します。
> - スケジュール設定の詳細については、スケジュールを設定するをご参照ください。

3 クイックアクションとして使用する

Quick Action を設定すると、**BioStar X** のメイン画面で **Quick Action** から複数のドアを一度に制御できます。 **Use as Quick Action** チェックボックスをクリックします。

> **情報**
>
> - この機能は、**Schedule** オプションが **Always** のときのみ使用できます。
> - **Quick Action** は **Settings** → **Access Management** → **Quick Action** で設定できます。**Quick Action**の詳細については、クイックアクションを使用する を参照してください。

4 デバイス、ドア、高度入退室制御の選択

イベントシグナルを送信する項目を選択します。各デバイスは複数選択でき、**BioStar X** との接続が切れても独立して動作します。

> **情報**
>
> **Advanced AC** 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 ポリシーをご参照ください。

5 作業条件イベントの設定

条件イベントを設定します。 1 つ以上のイベントを選択する必要があります。

> **情報**
>
> 前の手順 で選択したオプションに応じて、それぞれ異なるイベントリストが有効になります。

6 動作設定

動作を実行するデバイスを選択します。動作を実行するデバイス、ドア、**BioStar X** の動作を選択できます。

Action セクションでは、選択した条件イベントが発生した際に送信するシグナルを設定できます。ログをメールで受信するには、**BioStar X** で設定できます。

> **情報**
>
> - **Device**、**Door**、**BioStar X** タブをクリックすると、動作セクションの内容が変わります。
> - メールサーバー情報を設定するには、**BioStar X** タブで ⚙ アイコンをクリックします。 **SMTP Option** ウィンドウが表示されたら、メールサーバー情報を入力し、**Apply** をクリックします。詳細については、メールを設定するご参照ください。
> - メールサーバー情報の詳細については、システム管理者にお問い合わせください。

すべての設定が完了したら、**Apply** ボタンをクリックしてください。

クイックアクションを使用する

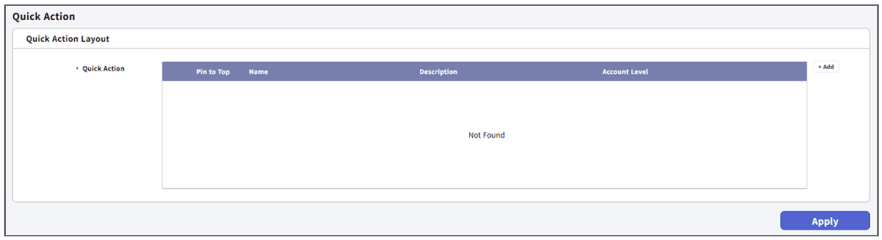
クイックアクションは、緊急時に複雑な制御手順を自動化する機能です。あらかじめ定義した複数のデバイスの動作を1つのボタンで即時に実行し、迅速に対応できます。

Quick Action メニューでクイックアクションボタンを追加すると、**BioStar X** のメイン画面からクイックアクションボタンをクリックして複数のドアを一括で制御できます。

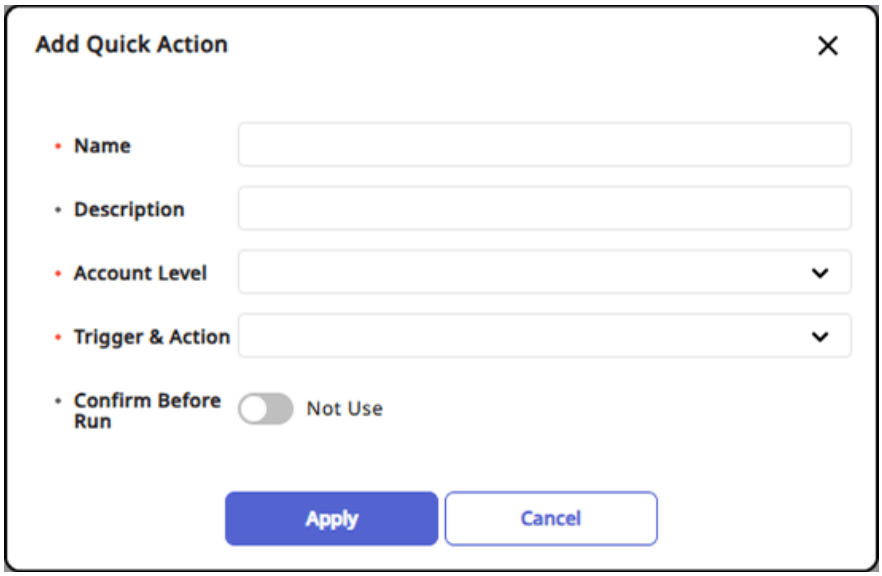
> **情報**
> クイックアクションとして使用する**Quick Action**を追加する方法については、作業条件と動作を設定するをご参照ください。

クイックアクションボタンを追加

1. **Launcher**ページで**Settings**をクリックします。
2. 画面左のサイドバーで **Access Management** → **Quick Action** をクリックしてください。



3. **Quick Action Layout** セクションで**+ Add**ボタンをクリックします。
4. **Add Quick Action** ウィンドウが表示されたら、各項目を入力して設定します。



- **Account Level**：追加するクイックアクションを実行できる**Account Level**を選択します。複数選択できます。
- **Trigger & Action**：実行する**Trigger & Action**を選択します。複数選択できます。

- **Confirm Before Run**：このオプションを有効にすると、**Quick Action** ボタンを押したときに実行の確認ポップアップが表示されます。

5. 設定を保存するには、**Apply**ボタンをクリックします。
6. 画面右下の **Apply** ボタンをクリックします。

BioStar X 画面の右上ヘッダーエリアに、追加した**Quick Action**ボタンが生成されます。作成した**Quick Action**ボタンをクリックして、**Quick Action**で設定したとおりに動作するか確認してください。

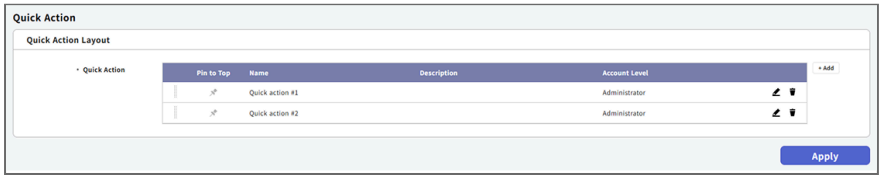


情報

- **Quick Action** ボタンは画面上部のヘッダーエリアに最大4個まで追加できます。どのページでも使用できるよう固定されています。
- ユーザーに設定された**Account Level**によって、使用できる**Quick Action**ボタンが異なる場合があります。

クイックアクションボタンを編集する

1. **Launcher**ページで**Settings**をクリックします。
2. 画面左のサイドバーで **Access Management** → **Quick Action** をクリックしてください。
3. 編集するクイックアクションボタンの右側にある ボタンをクリックします。



4. 編集用のポップアップが表示されたら、必要な項目を修正し**Apply**ボタンをクリックします。
5. 変更を保存するには、画面右下の**Apply**ボタンをクリックします。

クイックアクションの順序を変更

1. **Launcher**ページで**Settings**をクリックします。
2. 画面左のサイドバーで **Access Management** → **Quick Action** をクリックしてください。
3. クイックアクション一覧で、順序を移動する項目の最も左の列をクリックしたまま、目的の位置にドラッグしてください。



4. 変更した順序を保存するには、画面右下の **Apply** ボタンをクリックしてください。

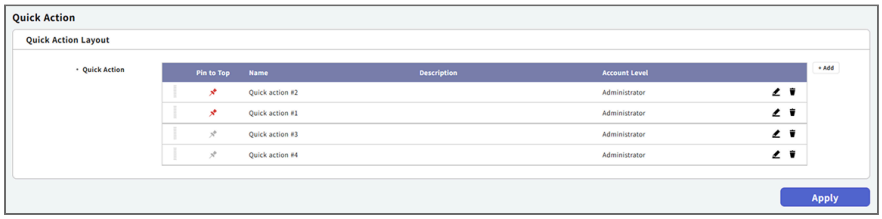
画面右上のクイックアクション一覧で、変更後の順序を確認できます。



ヘッダー領域にボタンを固定

すぐに実行する必要があるクイックアクション項目を、画面のヘッダー領域に配置できます。

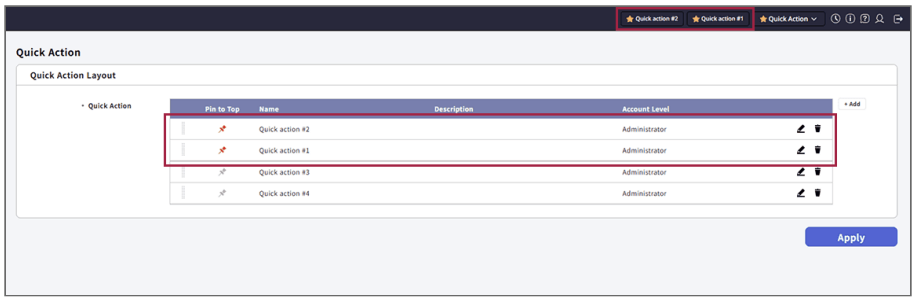
1. **Launcher**ページで**Settings**をクリックします。
2. 画面左のサイドバーで **Access Management** → **Quick Action** をクリックしてください。
3. ヘッダー領域に配置するには、**Pin to Top**( )をクリックしてください。



> 最も左の列をクリックしたまま目的の位置にドラッグして順序を変更するか、**Pin to Top**を解除してください。

4. ヘッダー領域に固定する項目をすべて選択したら、画面右下の **Apply** ボタンをクリックしてください。

画面右上の **Quick Action** ボタンの左側で、固定されたクイックアクションを確認できます。

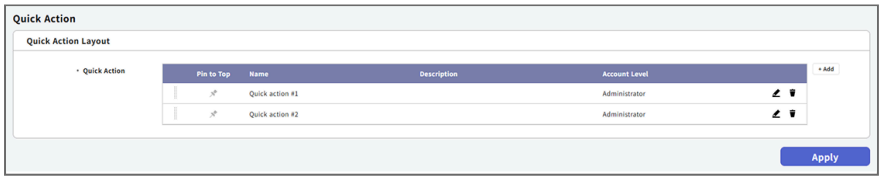


情報

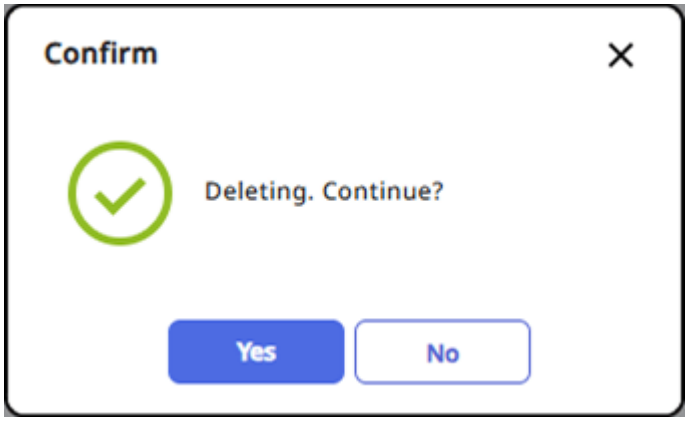
- 最大4個のクイックアクションをヘッダー領域に固定できます。すでに4個を固定している場合、クイックアクションを追加で固定できません。別の項目を解除してから、再度お試しください。
- Webブラウザのウィンドウ幅が狭くなると、ヘッダーの個別ボタンはすべて非表示になります。固定したクイックアクション項目は、ピン( )アイコンと一緒にQuick Actionボタンのドロップダウン一覧で確認できます。
- 登録済みのクイックアクションをすべてヘッダーに固定すると、Quick Action ボタンが表示されません。一部の項目を解除すると、ボタンが再び表示されます。

クイックアクションボタンを削除する

1. Launcherページで**Settings**をクリックします。
2. 画面左のサイドバーで **Access Management** → **Quick Action** をクリックしてください。
3. 削除するクイックアクションボタンの右側にある ボタンをクリックします。



4. 削除確認ポップアップを確認し、**Yes**をクリックします。



5. 削除内容を反映するには、画面右下の**Apply**をクリックします。

イベントログの取得

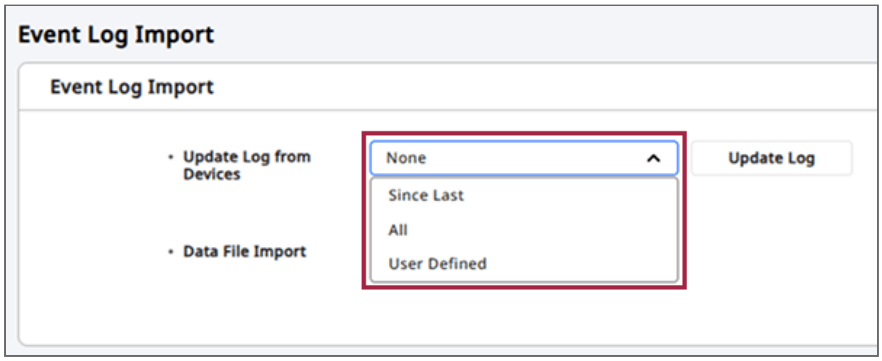
デバイスのログを BioStar X サーバーにインポートしてイベントを確認できます。この機能は、**Server** で **Log Upload** オプションを **Manual** に設定した場合に使用できます。

情報

Log Upload オプションの詳細については、サーバーの詳細を設定するをご参照ください。

手動で取得

1. **Launcher**ページで**Settings**をクリックします。
2. 画面左のサイドバーで **Event** → **Event Log Import** をクリックします。
3. **Update Log from Devices** でログを取得する期間を選択します。



- **Since Last**：最後に **BioStar X** サーバーに保存されたログの日付以降のログを取得します。
- **All**：デバイスのすべてのログを取得します。
- **User Defined**：ログを取得する開始日と終了日を選択できます。

4. ログを取得するには、**Update Log** をクリックします。

外部ストレージから取得

外部ストレージ（USB）に保存されたイベントログを **BioStar X** にインポートできます。

1. **Launcher**ページで**Settings**をクリックします。
2. 画面左のサイドバーで **Event** → **Event Log Import** をクリックします。
3. **Data File Import** で **Browse** をクリックします。



4. ローカルに保存されているデータファイル（*.tgz*）を選択します。

データファイルのインポートに成功すると、画面にメッセージが表示されます。

情報

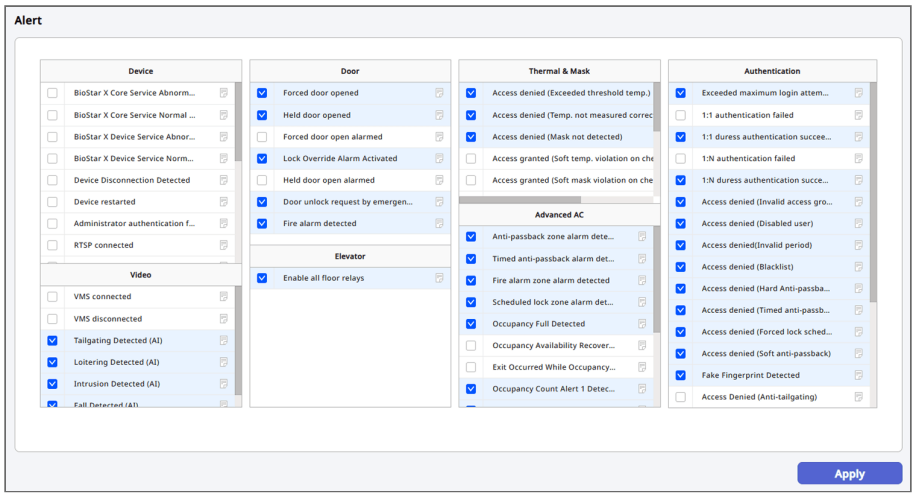
- 古いファームウェアバージョンのデバイスからエクスポートされたデータは **BioStar X** へインポートできません。常に最新バージョンのファームウェアを使用してください。
- BioStation 3 Max、BioStation 3、X-Station 2、FaceStation F2、FaceLite、FaceStation 2、BioStation A2、BioStation 2からエクスポートされたデータファイルのみインポートできます。
- **BioStar X** システムで設定したドア、エレベーター、ゾーンのイベントログ以外の場合、一部の情報が空欄で表示されることがあります。

アラームを設定する

デバイス、ドア、ゾーンでイベントが発生した場合に画面に表示するアラームの種類とメッセージを設定します。また、アラームが発生したときにアップロードしたサウンドファイルを再生するように設定します。

アラームを設定する

1. **Launcher**ページで**Settings**をクリックします。
2. 画面左のサイドバーで**Event** → **Alert**をクリックします。
3. 各カテゴリーのイベント一覧で画面に表示するイベントを選択します。
4. すべての設定が完了したら、**Apply** ボタンをクリックしてください。



アラームメッセージを編集する

イベント一覧で ボタンをクリックしてアラームメッセージを編集します。 **Alert Message** ウィンドウが表示されたら、各項目を設定して **Apply** をクリックします。



- **Name**：アラームメッセージの名前を変更します。
- **Message**：画面に表示するメッセージを入力します。
- **Sound Name**：イベント発生時に再生するサウンドファイルをアップロードしている場合は、一覧から選択します。
- **Play Options**：サウンドファイルを選択した場合は再生回数を選択します。

> **情報**
> 再生するサウンドファイルがない場合は、基本設定を構成するをご参照のうえ、ファイルをアップロードしてください。

クレデンシャル管理

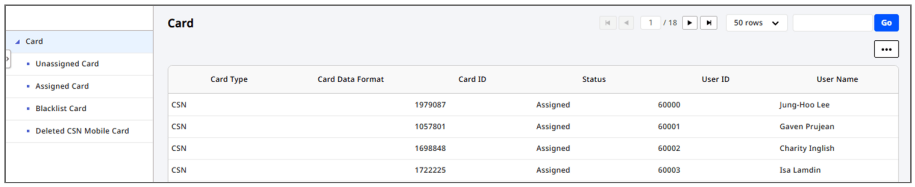
入退室認証に使用するクレデンシャルの管理方法を案内します。カードの発行状況、保有ユーザー、ブラックリストの確認方法と、Wiegand形式およびスマートカード形式の設定方法を説明します。このほか、cardPressoと連携したカード印刷、エアフォブポータル（Airfob Portal）と連携したモバイル入退室カード管理、IRフェイスのグループマッチング設定方法も説明します。

カードを管理する

カードの発行状態を確認し、Wiegandカードデータ形式を変更し、CSNモバイルカードの削除履歴を管理できます。

カード管理

1. **Launcher**ページで**Settings**をクリックします。
2. 画面左側のサイドバーで **Credential** → **Card** をクリックします。
3. カード一覧画面で登録済みカードを確認できます。



画面左側の発行状態をクリックすると、カード発行状態別にフィルターできます。カード発行状態は次のとおりです。

- **Unassigned Card**：ユーザーに割り当てられていないカードです。
- **Assigned Card**：特定ユーザーに割り当てられているカードです。カード一覧で割り当てられたユーザーのIDと名前を確認できます。
- **Blacklist Card**：ブラックリスト登録されたカードです。該当カード所持者は入退室認証できません。
- **Deleted CSN Mobile Card**：削除されたモバイル入退室カードです。

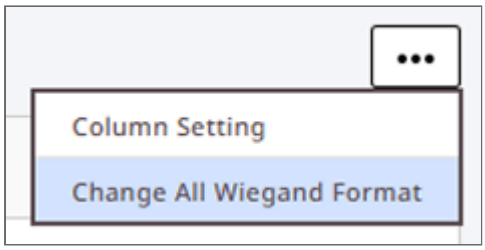
> **情報**
> ユーザーのカードをブロックした場合は、**Blacklist Card** リストでカード情報を確認できます。ブロックを解除するには、対象のカードを選択して **Unblocked** をクリックします。

Wiegandカードデータ形式の変更

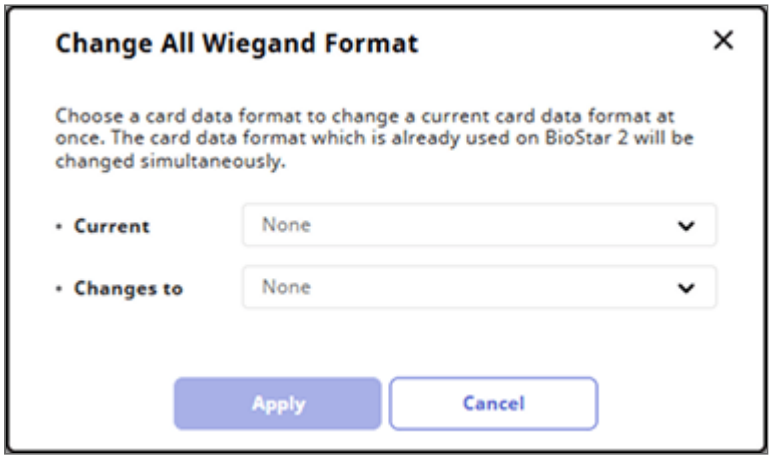
使用中のWiegandカードデータ形式を一括で変更できます。

> **注意**
> すでにユーザーに割り当てられているカードのデータ形式も変更されるため注意してください。

1. **Launcher**ページで**Settings**をクリックします。
2. 画面左側のサイドバーで **Credential** → **Card** をクリックします。
3. カード一覧の右上にある ••• ボタンをクリックし、**Change All Wiegand Format** を選択します。



4. **Change All Wiegand Format** ウィンドウが表示されたら、変更したいカードデータ形式を **Current** リストから選択します。



5. 変更先のカードデータ形式を **Changes to** リストから選択します。
6. カードデータ形式を変更するには、**Apply** ボタンをクリックします。

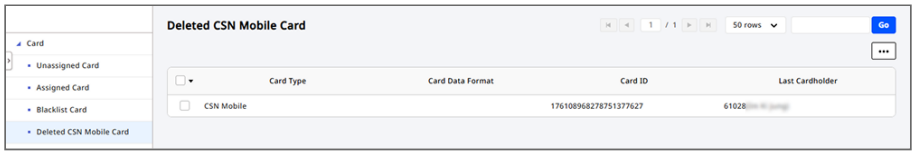
CSNモバイルカード削除時の管理指針

BioStar X に Airfobポータルレギュラーサイトを連携して CSN モバイルカードを使用している場合、カード所持者がカードを削除しても、同じカードIDを他のユーザーに発行できる状態になっていました。しかし、同じカードIDを他のユーザーに発行すると、既存のカード所持者も引き続き入退室が可能になる問題が発生します。

この問題を解決するために、CSNモバイルカードを削除した後に削除履歴を管理できる機能を提供します。

削除された CSN モバイルカードの個別管理

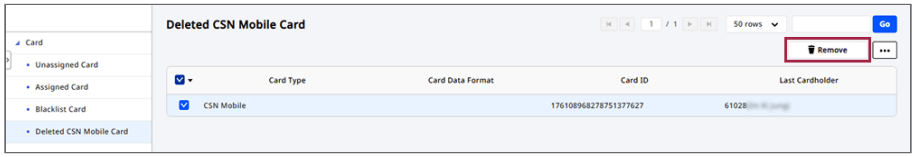
削除された CSN モバイルカードは **Settings** → **Credential** → **Card** の **Deleted CSN Mobile Card** リストに記録されます。リストでは **Card Type**、**Card Data Format**、**Card ID**、**Last Cardholder** を確認できます。



削除されたカードIDの再発行防止

削除履歴がある CSN モバイルカードを他のユーザーに発行しようとすると、処理は失敗します。

削除されたカードIDでカードを発行する場合は、**Deleted CSN Mobile Card** リストから該当する CSN モバイルカードを除外した後にのみ発行できます。



情報

Deleted CSN Mobile Card リストに含まれている CSN モバイルカードは **Unassigned Card** リストからは削除できません。

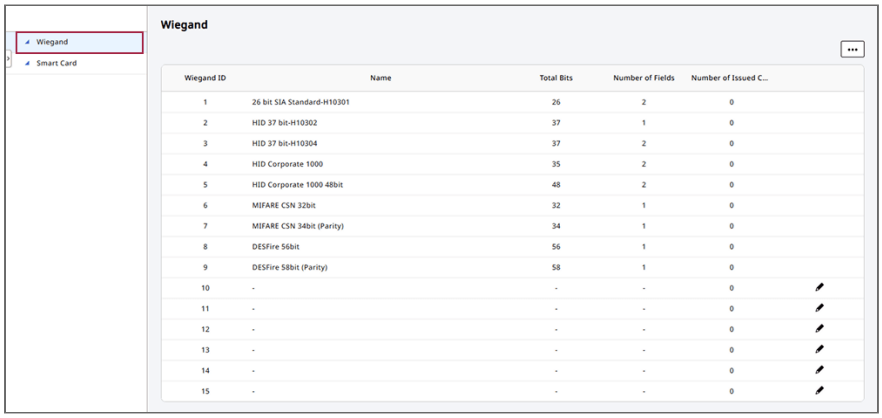
Unassigned Card リストからカードを削除するには、まず **Deleted CSN Mobile Card** リストからカードを除外してから再試行してください。

Wiegandカード形式を設定する

カードデータを読み取る形式を設定できます。設定したWiegand形式でカードデータが処理されます。

Wiegandカード形式の設定

1. **Launcher**ページで**Settings**をクリックします。
2. 画面左のサイドバーで**Credential** → **Card Format** をクリックしてください。
3. 画面左のカード形式リストで**Wiegand** をクリックしてください。

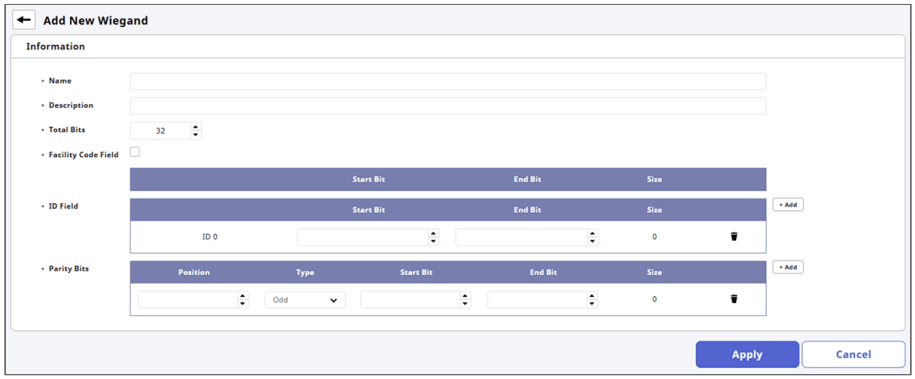


4. Wiegand形式リストで名前が指定されていない項目の ボタンをクリックしてください。
5. **Add New Wiegand** 画面が表示されたら、各項目を設定してください。詳細については設定オプションの案内をご参照ください。
6. 設定したWiegand形式を追加するには、**Apply** ボタンをクリックしてください。

> **情報**
>
> - Wiegand形式は最大15個まで使用できます。
> - あらかじめ定義された形式は修正または削除できません。

設定オプションの案内

Wiegandカード形式を追加または修正する際は、以下の項目を参考にビット構成を設定してください。



- **Name**：Wiegand形式の名前を入力してください。

- **Description**：Wiegand形式の簡単な説明を入力してください。
- **Total Bits**：総ビット数を入力してください。
- **Facility Code Field**：識別コードの使用有無を設定できます。識別コードを使用する場合はチェックボックスをクリックし、**Start Bit** と **End Bit** を入力してください。
- **ID Field**：使用するIDの**Start Bit** と **End Bit** を入力してください。 **+ Add** ボタンをクリックするとIDフィールドを追加できます。
- **Parity Bits**：**+ Add** ボタンをクリックしてパリティビット数を入力してください。使用するパリティビットの位置と開始ビット、終了ビットを入力してください。

> **情報**
> パリティビットを追加するには、**Total Bits** オプションを入力する必要があります。

スマートカード形式を設定する

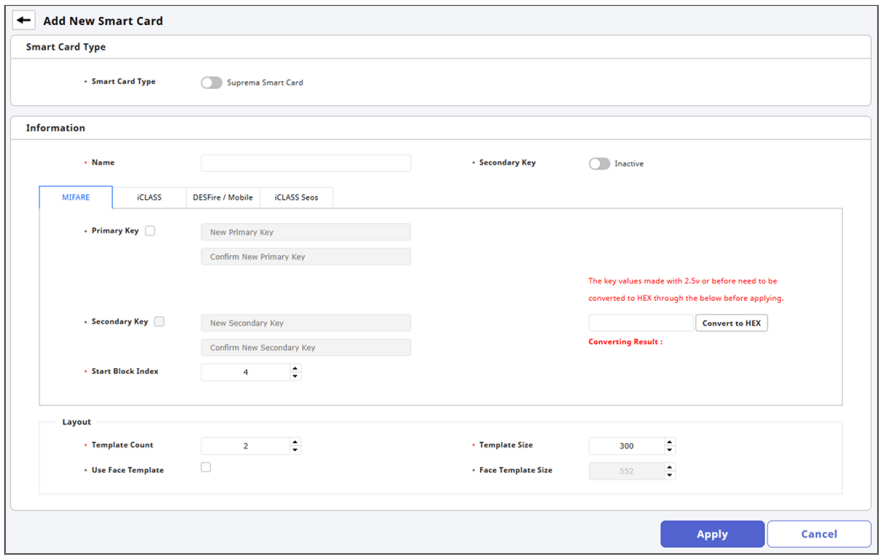
MIFARE、iCLASS、DESFire、iCLASS Seos などのスマートカードのレイアウトを設定できます。

スマートカードを追加

1. **Launcher**ページで**Settings**をクリックします。
2. 画面左のサイドバーで**Credential** → **Card Format** をクリックしてください。
3. 画面左側のカード形式リストで **Smart Card** をクリックします。



4. 画面左上の **Add Smart Card** をクリックします。
5. **Add New Smart Card** 画面が表示されたら、各項目を設定します。詳細については、スマートカードの種類ご参照ください。

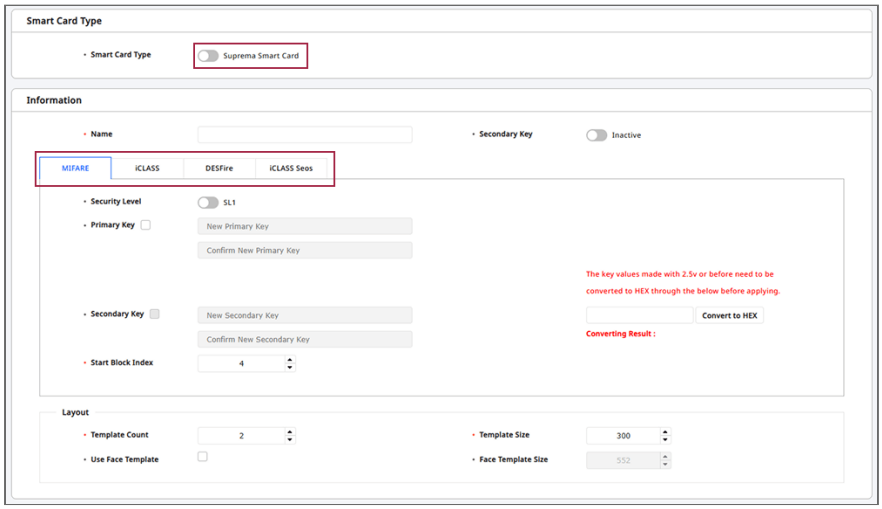


6. すべての設定が完了したら、**Apply** をクリックします。

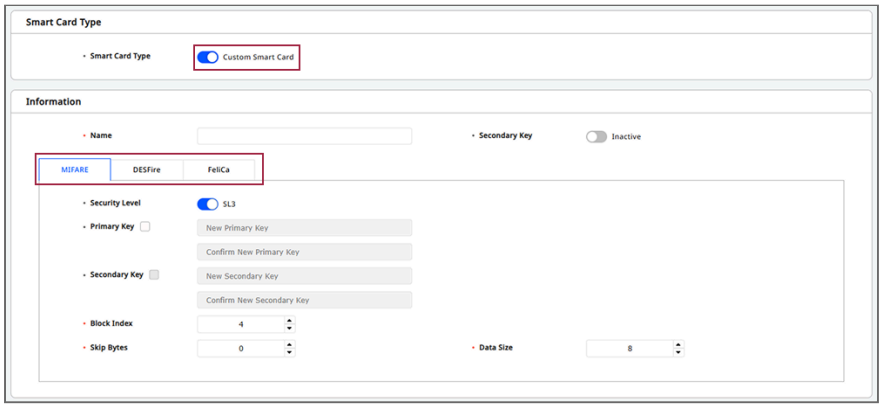
スマートカードの種類

Smart Card Type オプションで、希望するスマートカードの種類を設定できます。

- **Suprema Smart Card**



- **Custom Smart Card**

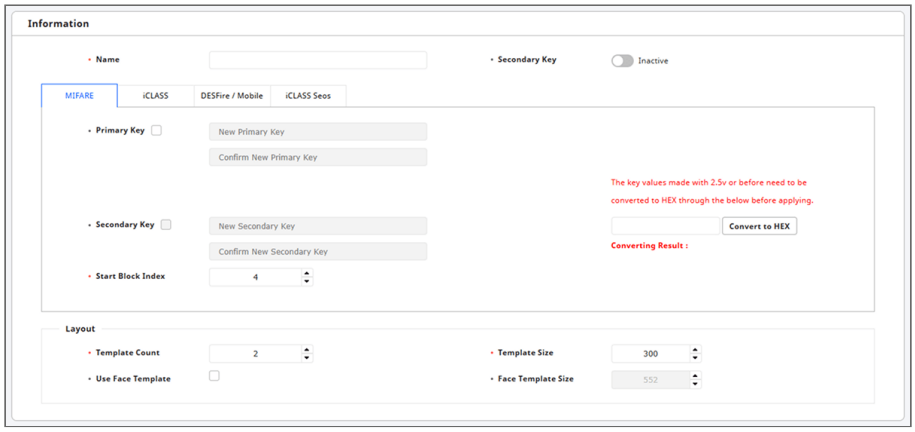


情報

- カスタムスマートカードは MIFARE、DESFire、FeliCa のみをサポートします。
- FeliCa は BioStation 3 ファームウェア 1.3.0 以降でのみサポートされます。

設定オプションの案内

Info セクションでカードレイアウトを設定します。

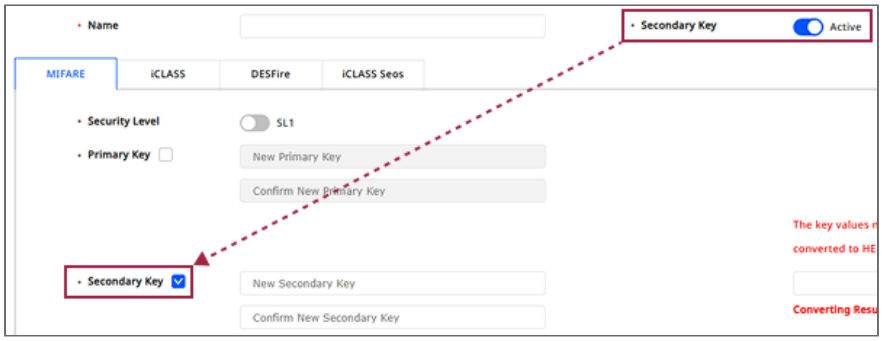


情報

- **Primary Key** と **Secondary Key** は 16 進数のみをサポートします。画面右側のフィールドにキー値を入力し、**Convert to HEX** をクリックします。変換された値をサイトキーとして使用します。
- **Convert to HEX** は、**Smart Card Type** オプションが **Suprema Smart Card** の場合にのみ使用できます。

基本情報の設定

- **Name**：スマートカード名を入力します。
- **Secondary Key**：補助サイトキーの使用有無を設定できます。 **Active** に設定すると、補助サイトキーを設定できます。補助サイトキーを設定すると、カードの基本サイトキーが一致しない場合に補助サイトキーを使用して認証を行います。



スマートカード設定

スマートカードの構造を設定できます。

Suprema スマートカード

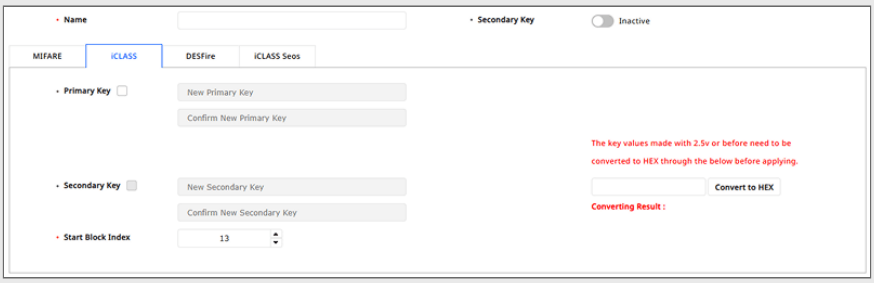
Primary Key と **Secondary Key** は 16 進数のみをサポートします。各入力フィールドにキー値を入力した後、**Convert to HEX** をクリックします。変換された値をサイトキーとして使用します。

▼ MIFARE



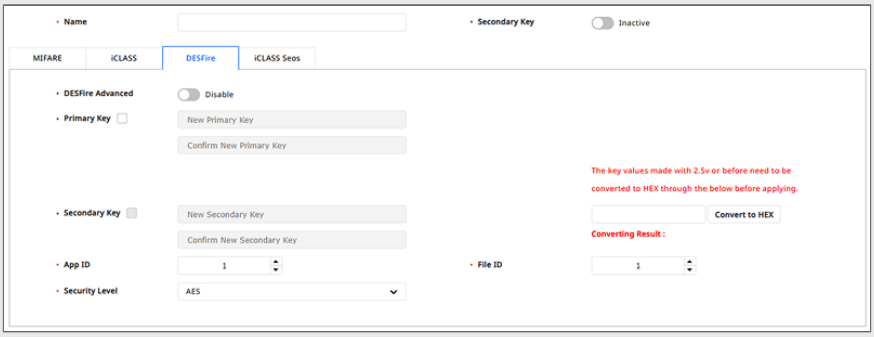
- **Security Level**：暗号化タイプを**SL1** または **SL3** に設定します。
- **Primary Key**：スマートカードとカードリーダー間の通信を暗号化するキーです。
- **Secondary Key**：カードのプライマリサイトキーが一致しない場合に使用して認証を実行します。補助サイトキーを入力するには、セクション上部の**Secondary Key**オプションを有効にします。
- **Start Block Index**：各テンプレートを保存する開始ブロックを選択します。このブロックはユーザー情報を保存するブロックのインデックスです。既にスマートカードを使用している場合は、保存可能なブロックを設定します。

▼ iCLASS



- **Primary Key**：スマートカードとカードリーダー間の通信を暗号化するキーです。
- **Secondary Key**：カードのプライマリサイトキーが一致しない場合に使用して認証を実行します。補助サイトキーを入力するには、セクション上部の**Secondary Key**オプションを有効にします。
- **Start Block Index**：各テンプレートを保存する開始ブロックを選択します。このブロックはユーザー情報を保存するブロックのインデックスです。既にスマートカードを使用している場合は、保存可能なブロックを設定します。

▼ DESFire



- **DESFire Advanced**：サードパーティが発行したDESFireカードを使用します。 DESFireのみ設定します。
- **Primary Key**：スマートカードとカードリーダー間の通信を暗号化するキーです。
- **Secondary Key**：カードのプライマリサイトキーが一致しない場合に使用して認証を実行します。補助サイトキーを入力するには、セクション上部の**Secondary Key**オプションを有効にします。
- **App ID**：アプリケーションIDを設定します。**File ID**を含む一種のディレクトリとして機能します。
- **File ID**：ファイルIDを設定します。
- **Security Level**：暗号化タイプを**DES/3DES** または **AES** に設定します。

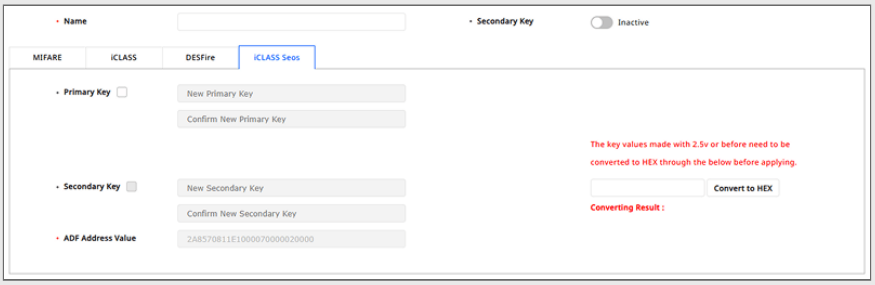
情報

暗号化タイプがAESで保存されているカードレイアウトをDES/3DESに変更すると、次の警告ポップアップが表示されます。

> ***Changing the Encryption Type to DES/3DES makes Enforce EV2/EV3 Secure Messaging unavailable on devices that use this card layout.***

Okボタンをクリックすると、変更内容を保存し、このカードレイアウトを使用するデバイスのEnforce EV2/EV3 Secure Messagingオプションを自動的にオフにします。 Enforce EV2/EV3 Secure Messaging オプションの詳細については、認証を設定するをご参照ください。

▼ iClass Seos



- Primary Key：スマートカードとカードリーダー間の通信を暗号化するキーです。
- Secondary Key：カードのプライマリサイトキーが一致しない場合に使用して認証を実行します。補助サイトキーを入力するには、セクション上部のSecondary Keyオプションを有効にします。
- ADF Address Value：デジタル資格情報が保存されるADFアドレスです。

レイアウト

ユーザー情報、顔情報、指紋情報が記録されるレイアウトを編集できます。

- Template Count：レイアウトに含める指紋テンプレート数を設定します。
- Template Size：指紋テンプレートが使用するバイト数を設定します。
- Use Face Template：顔テンプレートの使用有無を選択できます。
- Face Template Size：顔テンプレートが使用するバイト数を設定します。

情報

Use Face Template は BioStation 3 Max、BioEntry W3、BioStation 3、FaceStation F2 で使用できます。

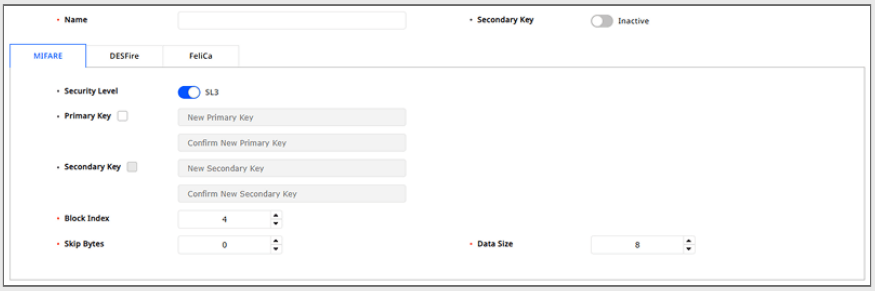
カスタムスマートカード

カスタムスマートカードは MIFARE、DESFire、FeliCa のみをサポートします。

情報

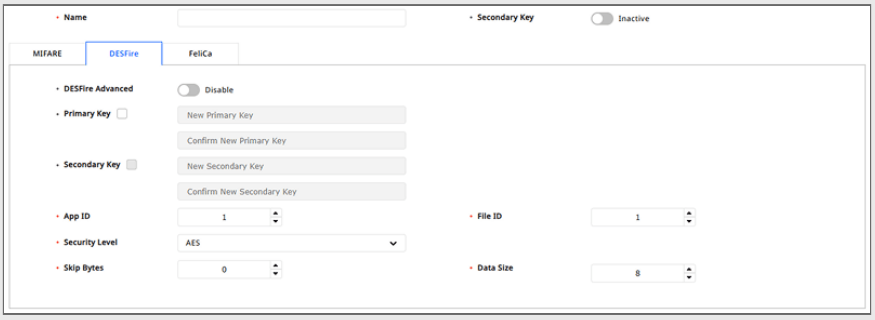
FeliCa は BioStation 3 ファームウェア 1.3.0 以降でのみサポートされます。

▼ MIFARE



- **Security Level**：暗号化タイプを**SL1** または **SL3** に設定します。
- **Primary Key**：スマートカードとカードリーダー間の通信を暗号化するキーです。
- **Secondary Key**：カードのプライマリサイトキーが一致しない場合に使用して認証を実行します。補助サイトキーを入力するには、セクション上部の**Secondary Key**オプションを有効にします。
- **Block Index**：各テンプレートを保存する開始ブロックを選択します。このブロックはユーザー情報を保存するブロックのインデックスです。既にスマートカードを使用している場合は、保存可能なブロックを設定します。
- **Skip Bytes**：カード番号を読み取る開始位置を設定します。
- **Data Size**：（設定した**Primary Key** と **Secondary Key** がカードの設定値と一致する場合）読み取るカードのデータサイズを設定します。

▼ DesFire



- **DESFire Advanced**：サードパーティが発行したDESFireカードを使用します。 DESFireのみ設定します。
- **Primary Key**：スマートカードとカードリーダー間の通信を暗号化するキーです。
- **Secondary Key**：カードのプライマリサイトキーが一致しない場合に使用して認証を実行します。補助サイトキーを入力するには、セクション上部の**Secondary Key**オプションを有効にします。
- **App ID**：アプリケーションIDを設定します。**File ID**を含む一種のディレクトリとして機能します。
- **File ID**：ファイルIDを設定します。
- **Security Level**：暗号化タイプを**DES/3DES** または **AES** に設定します。

情報

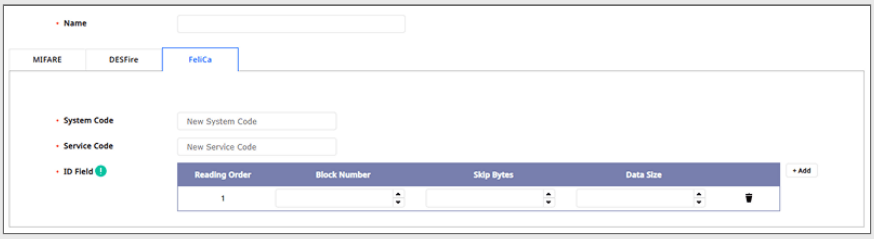
暗号化タイプが**AES**で保存されているカードレイアウトを**DES/3DES**に変更すると、次の警告ポップアップが表示されます。

> ***Changing the Encryption Type to DES/3DES makes Enforce EV2/EV3 Secure Messaging unavailable on devices that use this card layout.***

Okボタンをクリックすると、変更内容を保存し、このカードレイアウトを使用するデバイスの**Enforce EV2/EV3 Secure Messaging**オプションを自動的にオフにします。 **Enforce EV2/EV3 Secure Messaging** オプションの詳細については、認証を設定するをご参照ください。

- **Skip Bytes**：カード番号を読み取る開始位置を設定します。
- **Data Size**：（設定した**Primary Key** と **Secondary Key** がカードの設定値と一致する場合）読み取るカードのデータサイズを設定します。

▼ **Felica**



- **System Code**：FeliCaカードを読み取るためのシステムコードを16進数で最大4桁入力します。
- **Service Code**：FeliCaカードを読み取るためのサービスコードを16進数で最大4桁入力します。
- **ID Field**：カードの特定領域を読み取れるように設定します。 **+ Add** ボタンをクリックして、読み取り対象の最大8ブロックを設定します。

  Block Number：カードを読み取るブロックを設定します。 （0 ～ 150）

カードを印刷する

BioStar X と cardPresso を連携させて、ユーザーが希望するデザインのカードを印刷できます。 cardPresso はカードのデザインと印刷のための専門ソフトウェアです。 cardPresso を使用すると、さまざまなカードテンプレートを作成し、ユーザー情報をカードに合わせて配置できます。

開始する前に

BioStar X のカードプリンタ機能を使用するには、cardPresso をインストールして **BioStar X** と接続する必要があります。
cardPresso の Web 印刷サーバー機能を使用するには、cardPresso XXL edition のライセンスが必要です。

情報

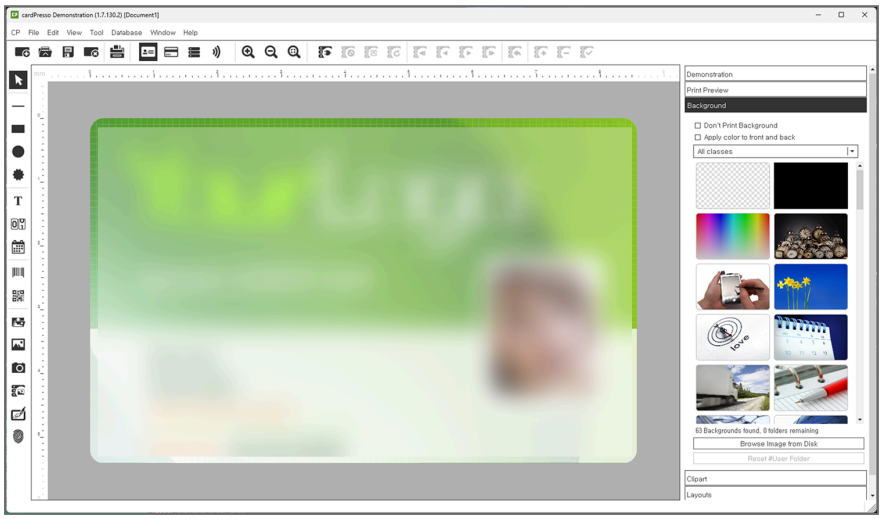
- ライセンスの種類について詳しくは、cardPresso Editions ページを参照してください。
- Web 印刷サーバー機能は Windows オペレーティングシステムでのみサポートされています。

cardPresso のインストールと設定

cardPresso をインストールして Web 印刷サーバーを設定するには、以下の手順に従ってください。

> インストールバージョンによってメニュー経路や画面が異なる場合があります。

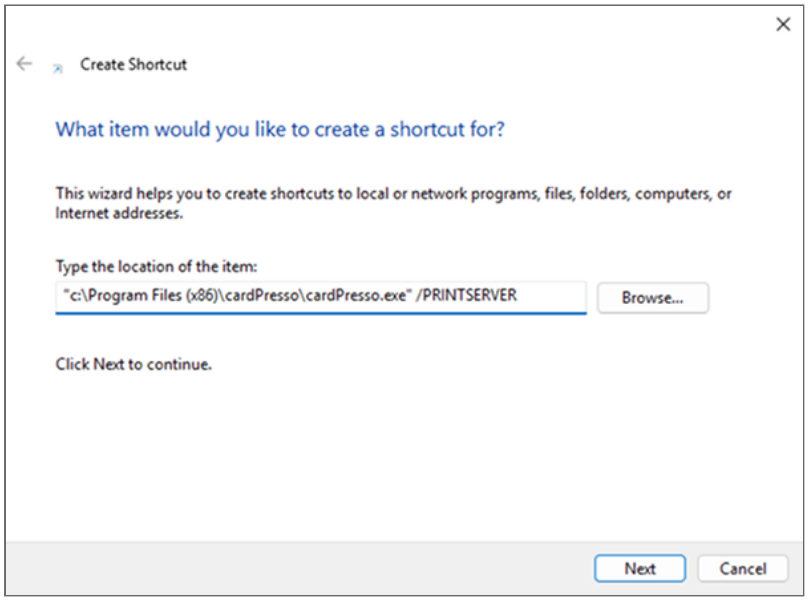
1. Web 印刷サーバーとして運用する PC の OS に対応した最新バージョンの cardPresso を cardPresso Download からダウンロードしてください。
2. プログラムをインストールして、cardPresso で発行したライセンスを有効化します。
3. cardPresso を起動し、カードテンプレートを作成してください。



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。

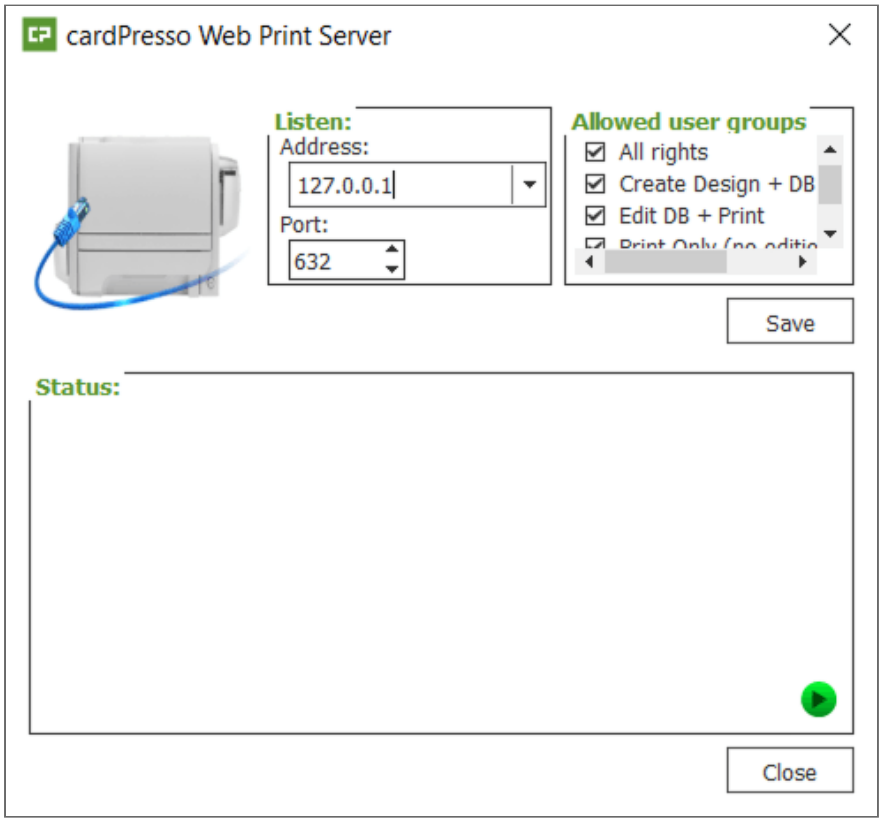
4. 作成したカードテンプレートを **BioStar X** をインストールしたサーバーの任意のパスに保存してください。(例：*C:\template\example.card*)
5. cardPresso をインストールした PC のデスクトップで右クリックし、ポップアップメニューから **New ** → **Shortcut** をクリックしてください。
6. ［**項目の場所を入力**］フィールドに以下のように入力し、［**次へ**］ボタンをクリックしてください。

```
"C:\Program Files (x86)\cardPresso\cardPresso.exe" /PRINTSERVER
```



インストール環境によって cardPresso がインストールされているパスが異なる場合があります。 cardPresso のインストールパスを確認した後、上記のパスを適切に修正してください。

7. ショートカット名を入力し、［完了］ボタンをクリックしてください。
8. デスクトップに作成した cardPresso Web 印刷サーバーのショートカットアイコンをダブルクリックして起動してください。
9. cardPresso Web 印刷サーバーのウィンドウが表示されたら、**設定** アイコンをクリックしてください。

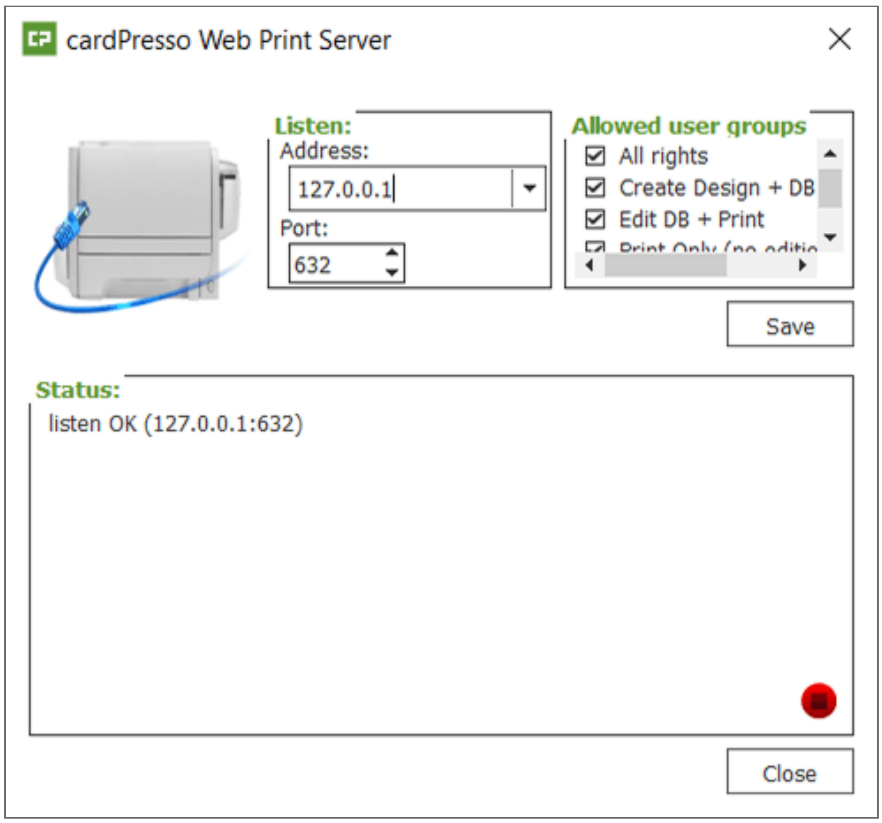


- **アドレス**：Web 印刷サーバーとして動作する PC の IP アドレスを入力します。
- **ポート**：cardPresso が印刷ジョブを受信するために使用するポート番号です。

- **許可されたユーザーグループ**：Web 印刷サーバーへアクセスできるユーザーグループを選択します。

10. 設定が完了したら **保存** をクリックします。

11. 右下にある  をクリックしてサービスを開始します。正しく設定されると、アイコンが  に変わり、**listen OK** メッセージが表示されます。

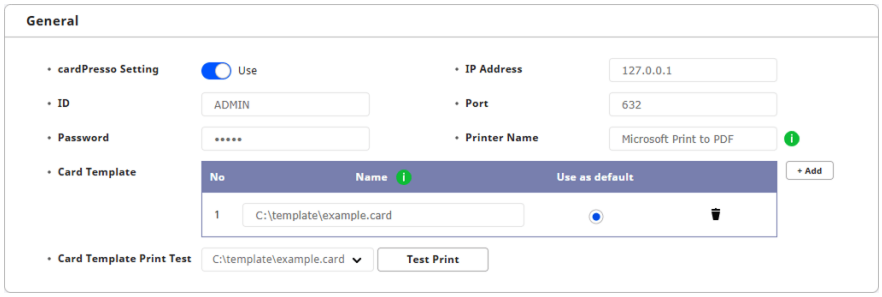


> カードの印刷が完了するまでウィンドウを閉じないでください。

cardPresso を BioStar X に接続する

BioStar X に cardPresso を接続するには、以下のように設定してください。

1. **Launcher**ページで**Settings**をクリックします。
2. 画面左側のサイドバーで **Credential** → **Card Printer** をクリックしてください。
3. **cardPresso Setting** を **Use** に設定してから各項目を入力します。



- **ID**：cardPresso のログイン ID を入力します。(デフォルト：ADMIN)

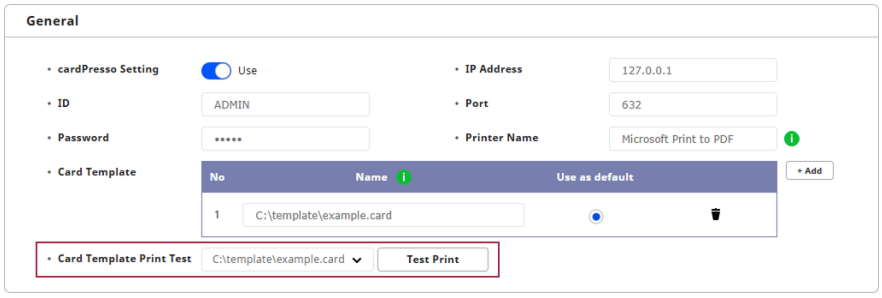
- **Password**：cardPresso のログインパスワードを入力します。(デフォルト：admin)
- **IP Address**：Web 印刷サーバーとして動作する PC の IP アドレスを入力します。
- **Port**：cardPresso が印刷ジョブを受信するために使用するポート番号です。
- **Printer Name**：カードプリンターとして使用するプリンター名を入力します。 Windows の **コントロール パネル** → **デバイスとプリンター** で確認できます。
- **Card Template**：**+ Add** をクリックして **Card Template** を追加できます。 **Name** 項目に、カードテンプレートのファイル名と拡張子を含むフルパスを入力してください。
  - カードテンプレートのファイル名には英数字と記号を使用できます。
  - カードテンプレートは最大 20 個までサポートします。
  - パス例：C:\template\example.card
- **Card Template Print Test**：カードテンプレートのテスト印刷ができます。

4. 設定が完了したら **Apply** をクリックしてください。

カードテンプレートをテスト印刷する

Administrator 情報を含むカードテンプレートをテスト印刷できます。

1. **Launcher**ページで**Settings**をクリックします。
2. 画面左側のサイドバーで **Credential** → **Card Printer** をクリックしてください。
3. 印刷するカードテンプレートを選択し、**Test Print** ボタンをクリックしてください。

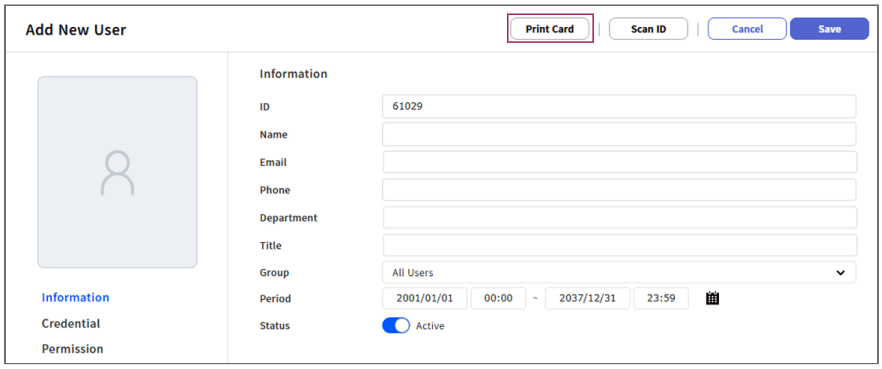


4. Administrator 情報を含むカードテンプレートが印刷されます。

ユーザー別カードテンプレートを印刷する

ユーザーごとの情報を含むカードテンプレートでカードを印刷できます。

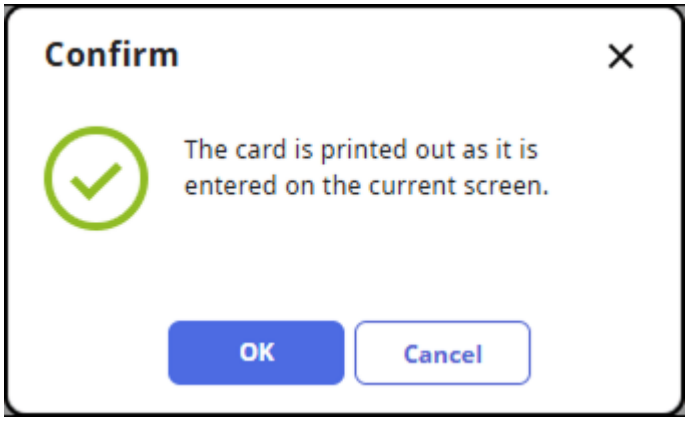
1. **Launcher** ページで **User** をクリックします。
2. 画面右上の **New User** ボタンをクリックします。 **New User** ウィンドウが表示されます。
3. フォームに入力し、**Print Card** ボタンをクリックしてください。
   - ユーザー情報には英字、数字、特殊記号を入力できます。



4. 印刷するカードテンプレートを選択し、**Print** ボタンをクリックしてください。



5. カードを印刷するかどうかを確認するポップアップが表示されたら、**OK** ボタンをクリックしてください。

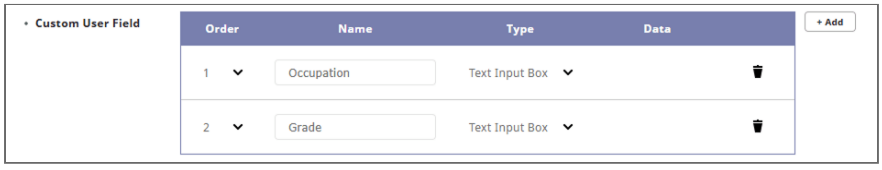


新しいユーザーが作成され、ユーザー情報を含むカードテンプレートでカードが印刷されます。

カスタムユーザーフィールドを追加する

カスタムユーザーフィールドを追加したカードテンプレートでカードを印刷できます。

1. **Launcher**ページで**Settings**をクリックします。
2. 画面左側のサイドバーで **System** → **Server** をクリックしてください。
3. **User/Device Management** セクションの **Custom User Field** 項目で **+ Add** ボタンをクリックし、**Name** を入力して **Type** を選択してください。追加した **Custom User Field** の順序に従ってカードテンプレートの属性 **ID** が決定されます。

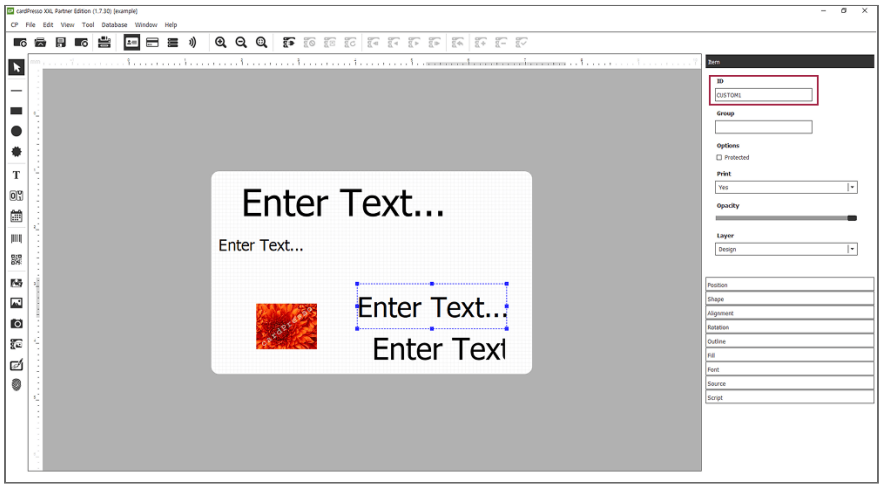


BioStar X の属性 ID では、順序 1 は CUSTOM1 に相当します。 BioStar X の属性IDに関する詳しい情報は、カードテンプレー

ト属性 IDご参照ください。

4. 設定が完了したら、画面最下部の **Apply** ボタンをクリックしてください。

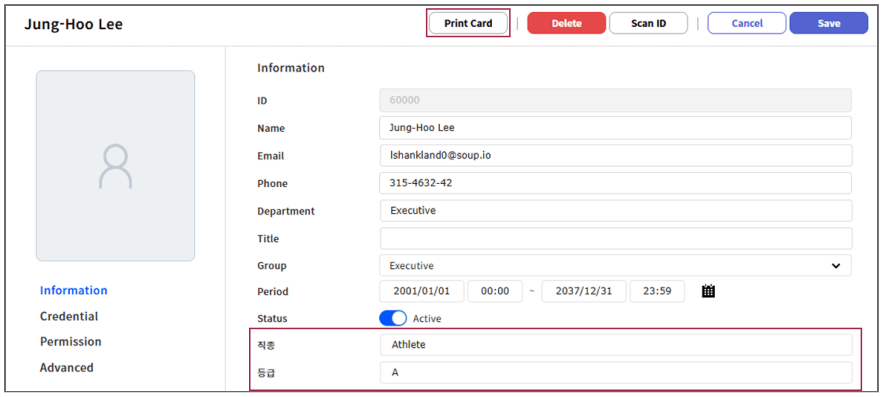
5. cardPresso で **ファイル → テンプレートを開く** をクリックしてカードテンプレートファイルを開いてください。新しい属性を追加し、BioStar X の属性 ID の順序に合わせた **XML 項目 ID 名** として **ID** を入力してください。



6. 設定が完了したら **ファイル → 保存** をクリックしてください。

7. **BioStar X** に戻り、**User** ページでカードテンプレートを適用するユーザーを選択してください。

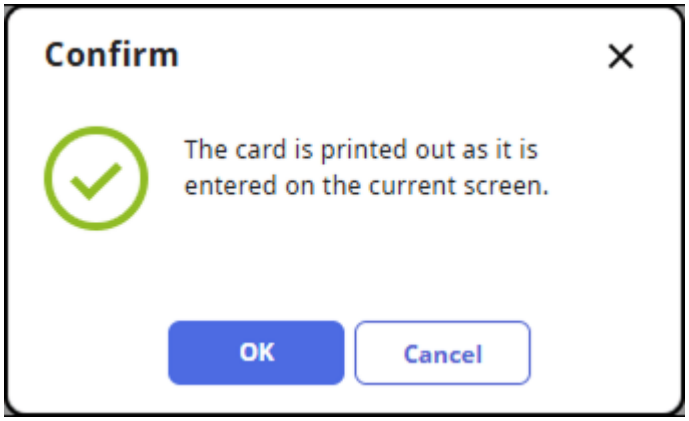
8. 追加したカスタムユーザーフィールド項目を確認できます。該当フォームに入力し、**Print Card** ボタンをクリックしてください。



9. 印刷するカードテンプレートを選択し、**Print** ボタンをクリックしてください。



10. カードを印刷するかどうかを確認するポップアップが表示されたら、**OK** ボタンをクリックしてください。



ユーザー情報が保存され、カスタムユーザーフィールドを追加したカードテンプレートでカードが印刷されます。

カードテンプレート属性 ID

BioStar X でサポートされる属性 ID は次のとおりです。カードテンプレートを作成するときは、属性 ID を適切な **XML 項目 ID 名**として入力します。

番号	BioStar X ユーザーデータ	XML 項目 ID 名
1	User ID	ID
2	User Name	NAME
3	Email	EMAIL
4	部署	DEPARTMENT
5	電話番号	TELEPHONE
6	ユーザーグループ	GROUP
7	プロフィール写真	PHOTO
8	カスタムフィールド 1	CUSTOM1
9	カスタムフィールド 2	CUSTOM2
10	カスタムフィールド 3	CUSTOM3
11	カスタムフィールド 4	CUSTOM4
12	カスタムフィールド 5	CUSTOM5
13	カスタムフィールド 6	CUSTOM6
14	カスタムフィールド 7	CUSTOM7
15	カスタムフィールド 8	CUSTOM8

番号	BioStar X ユーザーデータ	XML 項目 ID 名
16	カスタムフィールド 9	CUSTOM9
17	カスタムフィールド 10	CUSTOM10

モバイルアクセスカードを管理する

Airfob Portalを連携して、**BioStar X**でユーザーのモバイルアクセスカードを発行または削除できます。

ユーザーはAirfob Portalに登録したり別途モバイルアクセスカードを登録したりしなくても、メールで受け取ったリンクからモバイルアクセスカードを発行できます。

情報

- モバイルアクセスカードでは、**CSN Mobile**カードと**テンプレート オン モバイル**のいずれか一方のみ使用できます。
- **CSN Mobile**カードを使用できるデバイスとファームウェアバージョンについては、以下を参照してください。

  ▼ CSN Mobileカード対応デバイスおよびファームウェアバージョンを表示

  - BioStation 3 Maxのファームウェアバージョン1.0.0以降
  - XPass Q2のファームウェアバージョン1.0.0以降
  - BioEntry W3 ファームウェア 1.0.0 以上
  - BioStation 3 ファームウェア 1.0.0 以上
  - X-Station 2 ファームウェア 1.0.0 以上
  - FaceStation F2 ファームウェア 1.0.0 以上
  - XPass 2 ファームウェア 1.1.0 以上
  - FaceLite ファームウェア 1.2.0 以上
  - BioLite N2 ファームウェア 1.3.0 以上
  - XPass D2(Rev 2) ファームウェア 1.4.0 以上
  - FaceStation 2 ファームウェア 1.4.0 以上
  - BioEntry W2(Rev 2) ファームウェア 1.6.0 以上
  - BioStation A2 ファームウェア 1.8.0 以上 (NFC 対応モデル)
  - BioStation 2 ファームウェア 1.9.0 以上 (NFC 対応モデル)
- **テンプレート オン モバイル**を使用できるデバイスとファームウェアバージョンについては、以下を参照してください。
  - BioStation 3 Maxのファームウェアバージョン1.0.0以降
  - BioEntry W3 ファームウェア 1.0.0 以上
  - BioStation 3 ファームウェア 1.2.0 以上

Supremaモバイルアクセスカードを使用するには、Airfob Portalに登録してサイトを作成する必要があります。 Airfob Portalに登録した後、**BioStar X**でモバイルアクセスカードを管理できます。

1 Airfob Portalの登録とサイトの作成

Airfob Portalでモバイルアクセスカードと登録デバイスを設定し、サイトとクレジットを管理できます。

1. Airfob Portalにアクセスします。
2. **開始**をクリックして会員登録およびサイト作成を行ってください。
3. メール入力フィールドにAirfob Portal管理者のメールアドレスを入力し、**開始**をクリックします。入力したメールアドレスに認証コードが送信されます。
4. 認証コード入力欄にメールで受け取った認証コードを入力し、**確認**をクリックしてください。

   > 認証コードは6桁の数字です。

5. 個人情報ポリシーと利用規約を確認し、**同意**をクリックしてください。
6. Airfob Portalで使用するパスワードとニックネームを設定し、**アカウント作成**をクリックします。アカウント作成が完了します。
7. アカウント作成が完了したら、**ログイン**をクリックしてください。
8. メールアドレスとパスワードを入力し、**ログイン**をクリックしてください。
9. **サイト作成**をクリックしてサイトを開設してください。

   > **サイト**はモバイルアクセスカードを使用する組織または会社を指します。

10. サイト名と国を設定し、**次へ**をクリックしてください。
11. サイトの種類を選択してください。

    > サイトの種類に応じて、カードタイプを **ダイナミック** または **レギュラー** に選択できます。
    > - **ダイナミック**：デバイスおよび使用期間に応じてクレジットを差し引くタイプで、カード発行後も回収、停止、再発行、有効期限の設定などの管理が可能です。 そのため、フィットネスクラブや自習室などの会員制施設、またはシェアオフィスで利用できます。
    > - **レギュラー**：発行したカード数に応じてクレジットを差し引くタイプで、管理者が **BioStar X** でカードを削除するまで永久に使用できます。 そのため、一般企業や団体で社員証や入館証として利用できます。

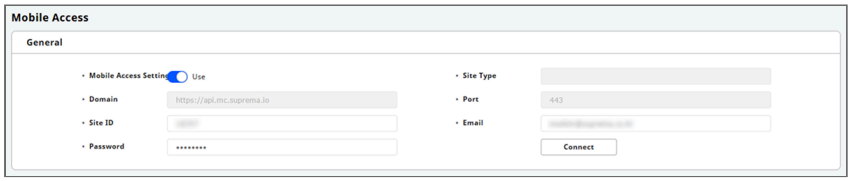
12. **作成**をクリックしてください。サイトの作成が完了します。
13. サイト名をクリックして、そのサイトのAirfob Portalにアクセスします。

> **情報**
> Airfob Portalの利用の詳細は次のリンクを参照します。

2 BioStar Xでモバイルアクセスカードを設定する

モバイルアクセスカードの利用可否を設定し、Airfob Portal連携に関する設定を管理できます。また、モバイルアクセスカードを使用するデバイスを登録できます。

1. **Launcher**ページで**Settings**をクリックします。
2. 画面左のサイドバーで**Credential** → **Mobile Access**をクリックします。
3. 各項目を設定してください。



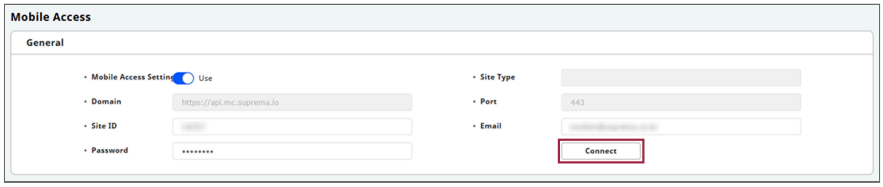
- **Mobile Access Setting**：モバイルアクセスカードの使用有無を設定できます。**Use**に設定すると、ユーザーにモバイルアクセスカードを発行できます。
- **Site ID**：Airfob Portalで作成したサイトIDを入力します。サイトIDはAirfob Portalの**設定**(Settings) → **サイト**(Site)メニューで確認できます。
- **Email**：モバイルアクセスカード管理者アカウントのメールアドレスを入力してください。
- **Password**：モバイルアクセスカード管理者アカウントのパスワードを入力してください。

4. すべての設定が完了したら、**Connect**をクリックします。

> **情報**
>
> **BioStar X**でモバイルアクセスカードを使用する前に、Airfob Portalへの登録と初期設定を完了します。詳細については、Airfob Portalの登録とサイトの作成ご参照ください。

3 デバイスの登録

Airfob Passアプリケーションまたは**BioStar X**で、モバイルアクセスカードを使用するデバイスを直接登録できます。

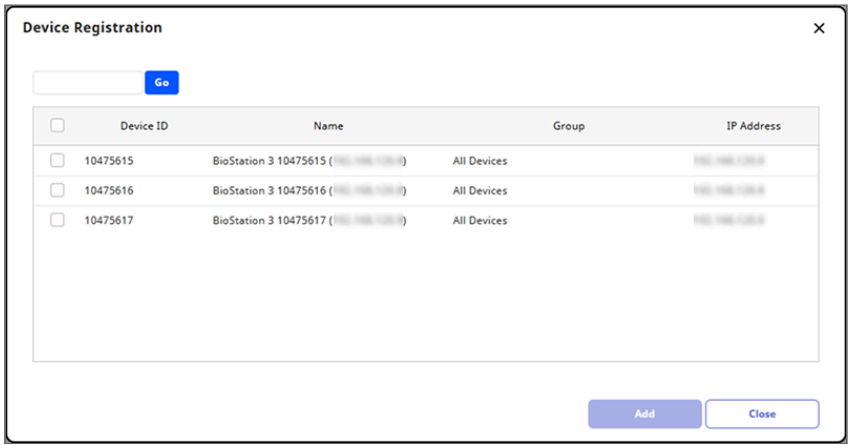


Airfob Portalとの連携設定を完了したら、**Connect**をクリックします。 **Device Registration** オプションを利用できます。

1. モバイルアクセスカードを使用するデバイスを追加するには、**+ Add** ボタンをクリックしてください。



2. **Device Registration**ウィンドウのデバイス一覧で、モバイルアクセスカードを使用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. すべてのデバイスを選択したら、**Add** ボタンをクリックしてください。

デバイス一覧で追加されたデバイスを確認できます。

- モバイルアクセスカード証明書を再送信するには、🔄ボタンをクリックしてください。
- 登録済みデバイスを削除するには、🗑ボタンをクリックしてください。

情報

- モバイルアクセスカードを使用できるデバイスとファームウェアバージョンについては、以下を参照してください。

  ▼ モバイルアクセスカードを使用できるデバイスおよびファームウェアバージョンを表示

  - BioStation 3 Maxのファームウェアバージョン1.0.0以降
  - XPass Q2のファームウェアバージョン1.0.0以降
  - BioEntry W3 ファームウェア 1.0.0 以上
  - BioStation 3 ファームウェア 1.0.0 以上
  - X-Station 2 ファームウェア 1.0.0 以上
  - FaceStation F2 ファームウェア 1.0.0 以上
  - XPass 2 ファームウェア 1.1.0 以上
  - FaceLite ファームウェア 1.2.0 以上
  - BioLite N2 ファームウェア 1.3.0 以上
  - XPass D2(Rev 2) ファームウェア 1.4.0 以上
  - FaceStation 2 ファームウェア 1.4.0 以上
  - BioEntry W2(Rev 2) ファームウェア 1.6.0 以上
  - BioStation A2 ファームウェア 1.8.0 以上 (NFC 対応モデル)
  - BioStation 2 ファームウェア 1.9.0 以上 (NFC 対応モデル)

- Airfob Passアプリケーションを使用してデバイスを登録することもできます。
- 登録済みデバイスを削除すると、デバイスに送信されたモバイルアクセスカード証明書が削除されます。

4 モバイルアクセスカード発行

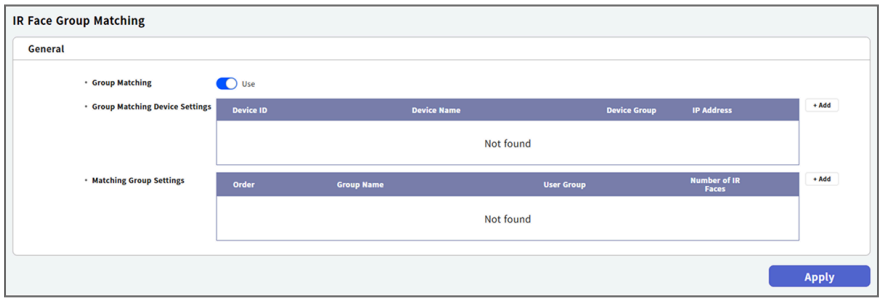
BioStar Xに登録されたユーザーにモバイルアクセスカードを発行できます。ユーザーにモバイルアクセスカードを発行するには、カード送付方法に応じたユーザー情報を必ず入力する必要があります。詳細については次のドキュメントを参照してください。

- ユーザー登録
- モバイルアクセスカードを登録する

IRフェイスグループマッチングを設定する

IR Face Group Matching は、ユーザーグループを基にマッチンググループを設定してユーザーを認証する機能です。この機能を使用すると、特定のユーザーグループに属するユーザーだけがIRフェイス認証を通じて入退室できます。

1. **Launcher**ページで**Settings**をクリックします。
2. 画面左側のサイドバーで **Credential** → **IR Face Group Matching** をクリックします。
3. **Group Matching** オプションを **Use** に変更します。



4. **Group Matching Device Settings** で **+ Add** ボタンをクリックします。
5. **Group Matching Device Settings** ウィンドウが表示されたら、目的のデバイスを選択し、**Add** ボタンをクリックします。

> FaceStation 2モデルのみ選択できます。

6. **Matching Group Settings** で **+ Add** ボタンをクリックします。
7. **Group Name** と **User Group** 項目を設定します。
8. 設定を保存するには、画面右下の **Apply** ボタンをクリックしてください。

情報

- 最大で10個のマッチンググループを作成できます。
- グループごとに最大3,000件のIRフェイステンプレートを含めることができます。
- 1つのマッチンググループに複数のユーザーグループを設定できます。
- マッチンググループ全体のIRフェイステンプレート数は5,000件を超えられません。
- ユーザーグループに含まれるIRフェイステンプレートが3,000件を超える場合、マッチンググループとして設定できません。
- この機能はFaceStation 2モデルのみ対応しています。
- グループマッチング機能を無効化するには、既に設定されているデバイスとグループ設定をすべて削除する必要があります。

ライセンスを有効化

BioStar X ライセンスおよびデバイス ライセンスの有効化方法を説明します。

BioStar Xライセンス

購入した **BioStar X** ライセンスを登録できます。

ユーザーのネットワーク環境によって、**BioStar X License** を登録する方法が異なります。案内に従ってネットワーク状態を確認し、ライセンスを有効化してください。

1. **Launcher**ページで**Settings**をクリックします。
2. 画面左のサイドバーで **License** → **BioStar X License** をクリックします。

情報

- 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。
- ライセンスのエラーコードを確認するには次のリンクを参照してください。

オンラインで登録する

情報

ライセンスキーには、数字とハイフン(`-`)のみ入力できます。 `1111-1111-1111-1111` 形式で、最大16文字の数字を入力する必要があります。

単一ライセンスの登録

インターネットに接続されたオンライン環境で **BioStar X** ライセンスをアクティベートするには、名前と受け取ったライセンスキーを入力し、**Activate** ボタンをクリックします。



複数ライセンスの登録

最大30件のライセンスを一度に追加できます。 ＋ **Add More License** ボタンをクリックします。ライセンスをすべて入力したら、**Activate** ボタンをクリックします。



- 入力欄が30件に達すると、＋ **Add More License** ボタンが無効になり、これ以上追加できません。
- 複数のライセンスキーをまとめてコピーして入力欄に貼り付けると、`1111-1111-1111-1111` 形式のキーだけを自動認識し、各入力欄に分割して追加します。
- 貼り付けたキーが30件を超えると、30件まで自動入力され、超過分は無視されます。

アクティベーションの進行状況

Activate ボタンをクリックすると、進行状況ポップアップが表示されます。アクティベーションが完了するまで、ページやポップアップを閉じないでください。

オフラインで登録する

閉鎖ネットワーク環境やインターネット接続が制限されたオフライン環境で **BioStar X** ライセンスをアクティベートするには、以下の手順に従ってください。

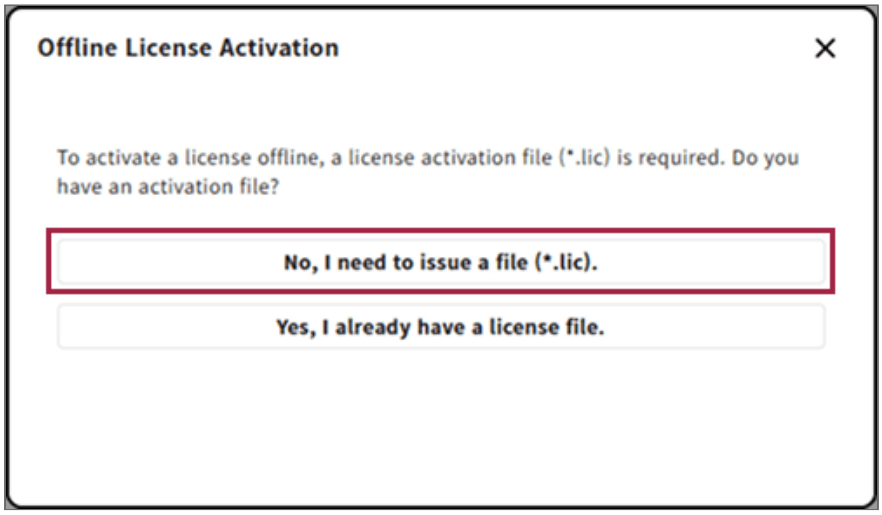
1. **License Activation** セクションで任意の登録管理者名とライセンスキーを入力します。

   - ライセンスキーには、数字とハイフン(`-`)のみ入力できます。 `1111-1111-1111-1111` 形式で、最大16文字の数字を入力する必要があります。
   - 登録管理者名とライセンスキーを覚えるか、メモしておいてください。
   - 複数のライセンスが必要な場合は、＋ **Add More License** ボタンをクリックして追加します。

2. **Offline Activation** ボタンをクリックします。

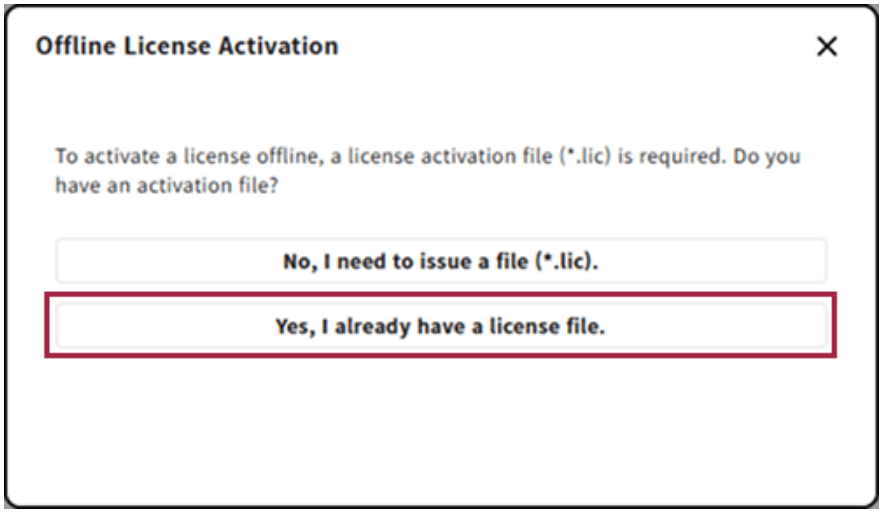


3. **Activate License Offline** ウィンドウが表示されたら、**No, I need to issue a file (*.lic).** ボタンをクリックします。



> すでに発行済みのライセンスファイルがある場合は、この画面で **Yes, I already have a license file.** ボタンをクリックしてから、手順9に進んでください。

4. 発行要求ファイル（*.req）が生成されたら、ローカルディスクへダウンロードしてください。
5. ダウンロードした発行要求ファイルを購入先へ送付し、オフライン有効化ファイル（*.lic）を要求してください。
6. オフラインアクティベーションファイルを受け取ったら、手順1で入力した登録管理者名とライセンスキーを **License Activation** セクションに入力します。
7. **Offline Activation** ボタンをクリックします。
8. **Activate License Offline** ウィンドウが表示されたら、**Yes, I already have a license file.** ボタンをクリックします。



9. ［ファイルを開く］ダイアログが開いたら、ローカルに保存したオフライン有効化ファイル(*.lic)または圧縮ファイル(*.zip)を選択してください。

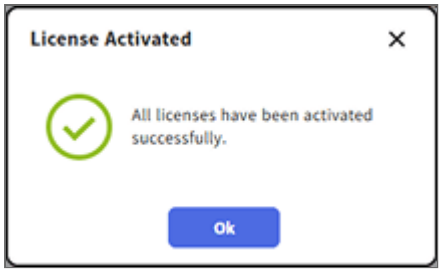
> 複数のライセンスをリクエストした場合、圧縮ファイルを受け取ることがあります。

10. 進行状況のポップアップが開きます。アクティベーションが完了するまで、ページやポップアップを閉じないでください。

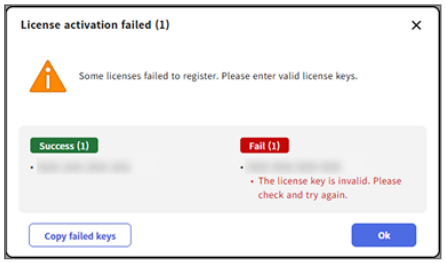
ライセンス有効化結果の確認

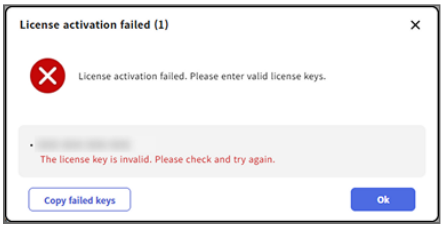
入力したライセンスキーの有効化結果に応じて、次の案内を表示します。

- 入力したすべてのライセンスキーが有効な場合、成功メッセージを表示します。



- 一部のキーだけ有効化に成功した場合、またはすべてのキーが失敗した場合、キーごとの成功・失敗と失敗理由を確認できます。成功したキーの入力欄を初期化し、失敗したキーは再入力できるよう入力欄に残します。





- インターネットに接続できず、すべてのキーが失敗した場合、インターネット接続を確認してから再試行するよう案内し、**Offline Activation** ボタンを表示します。閉域ネットワーク環境の場合、このボタンをクリックしてオフラインで登録してください。

> **情報**
> 失敗したキーをコピーするには、**Copy failed keys** ボタンをクリックしてください。

有効化済みライセンスの確認

登録した **BioStar X** ライセンス情報は、**Activated License**で確認できます。



デバイスライセンス

Suprema が発行した **Device License** を有効化して、ライセンスに対応する特定の機能を利用してください。

Device License では **BioStar X** と USB メモリを使用してデバイスのライセンスを有効化できます。

> **情報**
>
> - デバイスライセンスを発行するには、購入先にお問い合わせください。
> - デバイスライセンス 1 つにつき、1 つの機能を使用できます。
> - 1 つのデバイスライセンスファイルに複数のデバイスライセンスを含めることができます。（最大 100 個まで対応）
> - デバイスライセンスファイルは暗号化されているため、任意に変更できません。
> - デバイスライセンスはデバイスIDを基準に発行されます。 不正な方法でデバイスIDを変更した場合、ライセンスの保証サービスは提供されません。
> - ライセンスのエラーコードを確認するには次のリンクを参照してください。

開始前に

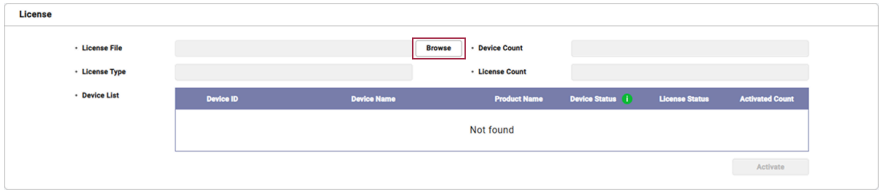
デバイスライセンスを有効化する前に次の項目を確認してください。

- 有効なデバイスライセンスファイルを準備してください。デバイスライセンスファイルについては購入先にお問い合わせください。
- 対象デバイスが **BioStar X** に登録されていることを確認してください。デバイス登録の詳細については、デバイスを登録するをご参照ください。

デバイスライセンスの適用

1. **Launcher**ページで**Settings**をクリックします。

2. 画面左のサイドバーで **License** → **Device License** をクリックします。
3. **Browse** ボタンをクリックします。



4. デバイスライセンスが保存されているパスからデバイスライセンスファイルを読み込みます。
5. 読み込んだライセンスに対応する情報が **License Type**、**Device Count**、**Device List** 項目に表示されます。



6. **Device List** を確認し、デバイスライセンスを有効化するには **Activate** ボタンをクリックします。

> **情報**
> ライセンスの有効化に失敗すると、エラーメッセージが表示されます。ライセンスの有効化を再試行してください。

デバイスライセンス情報

デバイスライセンスファイルを読み込むと、次の情報が表示されます。

- **License Type**：デバイスライセンスファイルに含まれるライセンスの種類を確認できます。
  - **Camera QR**

    「**Camera QR**」を利用できるデバイスは次のとおりです。
    - BioStation 3 Maxのファームウェアバージョン1.0.0以降
    - XPass Q2のファームウェアバージョン1.0.0以降
    - X-Station 2 (XS2-ODPB, XS2-OAPB, XS2-DPB, XS2-APB) ファームウェア 1.2.0 以上
    - X-Station 2 (XS2-QDPB, XS2-QAPB) ファームウェア 1.4.1 以上
    - BioStation 3 ファームウェア バージョン 1.1.0以降

  - **Multi Face Authentication**

    Multi Face Authentication ライセンスを使用できるデバイスは次のとおりです。
    - BioStation 3 ファームウェア バージョン 1.5.0以降

    このライセンスを有効にしたデバイスで **Multi Face Authentication** オプションを設定する方法は 認証を設定する を参照してください。

- ワイヤレスドアロック

  > - 対応する OSDP アンテナとワイヤレスドアロックは以下のとおりです。
  >   - U&Z OSDP アンテナ：CX8936
  >   - U&Z ワイヤレスドアロック：CX217x（ハンドル）、CX212x（ノブ）
  > - 接続予定のワイヤレスドアロックの台数分、最大 12 台までデバイスライセンスを発行できます。
  > - デバイスライセンスで接続できるワイヤレスドアロックの最大台数は 12 台です。複数のデバイスライセンスを有効化しても 12 台を超えることはできません。

- **Device Count**：デバイスライセンスファイルに含まれるデバイス数を確認できます。
- **License Count**：デバイスライセンスで有効化できるワイヤレスドアロックの台数を確認できます。
- **Device List**：デバイスライセンスファイルに含まれるデバイスの詳細情報を確認できます。
  - **Device ID**：デバイスを識別する固有 ID です。
  - **Device Name**：デバイスの名前です。
  - **Product Name**：デバイスのモデル名です。
  - **Device Status**：デバイスの現在の状態です。 **Normal** の状態のデバイスのみライセンスを有効化できます。
    - **Normal**、**Disconnected**、**Not Supported**、**Unregistered**

    > デバイスがライセンスの機能をサポートしていないモデル、またはファームウェアバージョンが低い場合、**Device Status** は **Not Supported** と表示されます。その機能をサポートするモデルとファームウェアバージョンを確認してください。

  - **License Status**：ライセンスの有効化状況です。 **Not Activated** の状態のデバイスのみライセンスを有効化できます。
    - **Not Activated**、**Activated**、**N/A**
  - **Activated Count**：ワイヤレスドアロックの接続状況です。

> **情報**
>
> - **License Count**、**Activated Count** 項目は、ワイヤレスドアロックのデバイスライセンスを読み込んだ場合にのみ値が表示されます。

監査トレイルを管理する

Audit Trail 機能は、システムで発生するすべてのアクティビティを記録して追跡します。ユーザーのログイン／ログアウト、設定変更、システム管理作業などのすべてのアクティビティが記録され、セキュリティ監査やシステム監視に活用できます。

画面左側のサイドバーの **Audit Trail** グループには、次のメニューが含まれます。

- **AC Audit Log**: ユーザー、デバイス、ドアなど、入退室管理に関連するすべての作成・変更・削除・照会・エクスポート・インポート・運用アクティビティを記録します。

- **Audit Settings**: 監査ログの保管期間と照会履歴を記録するかどうかを設定します。

> **情報**
>
> **T&A Audit Log** について詳しくは、勤怠監査ログを照会するを参照してください。 **T&A Audit Log** メニューを使用するには、勤怠管理（T&A）ライセンスを有効化する必要があります。

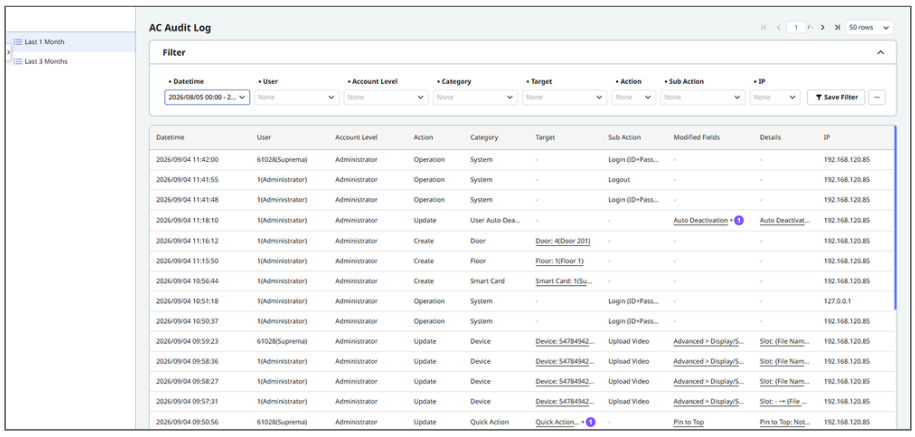
入退室管理の監査ログを確認する

AC Audit Log 機能は、ユーザー、デバイス、扉など入退室管理に関連する、作成、修正、削除、照会、エクスポート、インポート、運用のすべてのアクティビティを記録します。各記録は、いつ、誰が、何を、どのように変更したかを併せて示すため、セキュリティ監査やトラブルシューティングに活用できます。

- **セキュリティ監査**：不正アクセスの試みや権限乱用を検出できます。
- **トラブルシューティング**：システムエラーが発生した時点や設定変更履歴を追跡できます。
- **コンプライアンス**：個人情報の照会履歴を含むアクセス記録を保管し、監査レポートを作成できます。

入退室管理の監査ログを確認する

1. **Launcher**ページで**Settings**をクリックします。
2. 画面左のサイドバーで **Audit Trail** → **AC Audit Log**をクリックします。
3. 監査ログの一覧が画面に表示されます。



> **情報**
>
> - 保管期間などの監査ログポリシーを変更するには、監査設定を管理するを参照してください。
> - バージョン1.0.3にアップグレードした後、新たに作成される監査ログは、**Settings** → **System** → **Security** メニューの **Encrypt Personal Data on Database** オプションに関係なく、暗号化して保存します。
> - BioStar 2 から **BioStar X** にアップグレードした後、監査ログの一部が記録されない場合は アップグレードする を参照してください。

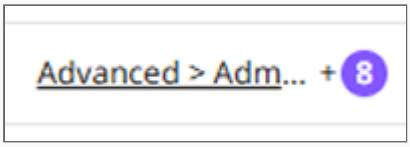
テーブル構成

監査ログ一覧テーブルは10列で構成され、現在の検索条件に該当する記録を **Datetime** の新しい順に表示します。

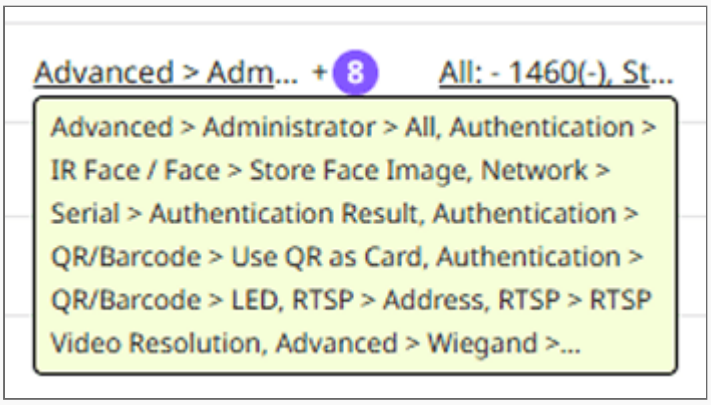
列	説明
Datetime	イベントが発生した日時です。
User	イベントを実行したユーザーです。 **id(名前)** 形式で表示されます。
Account Level	イベントを実行したユーザーの管理者レベルです。
Action	実行された操作の種類です。**Create**、**Update**、**Delete**、**Read**、**Export**、**Import**、**Operation** のいずれかに分類されます。
Category	イベント対象のドメイン分類です（例：ユーザー、デバイス、扉）。
Target	操作が適用された対象です。**タイプ: id(名前)** 形式で表示されます。
Sub Action	ログイン方式、アラーム解除のように、詳細な操作名がある場合のみ表示されます。
Modified Fields	変更または照会されたフィールド名です。
Details	動作別の詳細情報です。（例：変更値、理由、照会条件など）
IP	ユーザーが接続したIPアドレスです。システムが自動で発行した記録は**127.0.0.1**と表示されます。

情報

- **Target**と**Modified Fields**の値が2件以上の場合、最初の項目のみ表示し、残りは右側に残件数バッジ（例：+208）としてまとめて表示します。残件数が1,000件以上の場合は**+999**と表記し、正確な合計件数は詳細ポップアップのタイトルで確認できます。バッジをクリックすると、そのセルの詳細ポップアップが開きます。

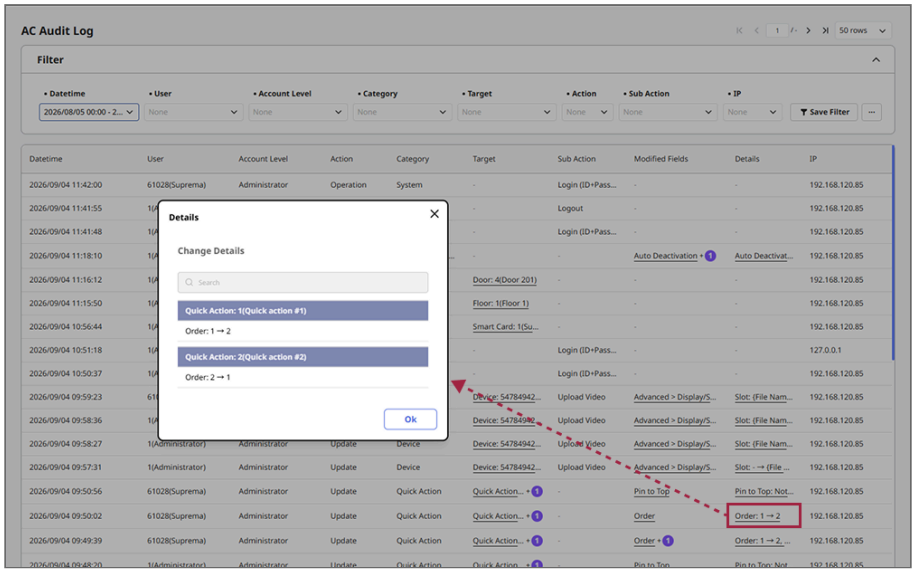


- セルの値が長い場合は一行で省略して表示します。マウスを合わせると値全体をツールチップに表示し、ツールチップからはみ出す部分は ... で省略して表示します。



詳細情報の確認

値がある**Target**、**Modified Fields**、**Details**列は下線が付き、クリックできます。該当列の値をクリックすると、動作に応じた詳細ポップアップが開きます。ポップアップを閉じるには**OK**ボタンまたは ✕ ボタンをクリックしてください。

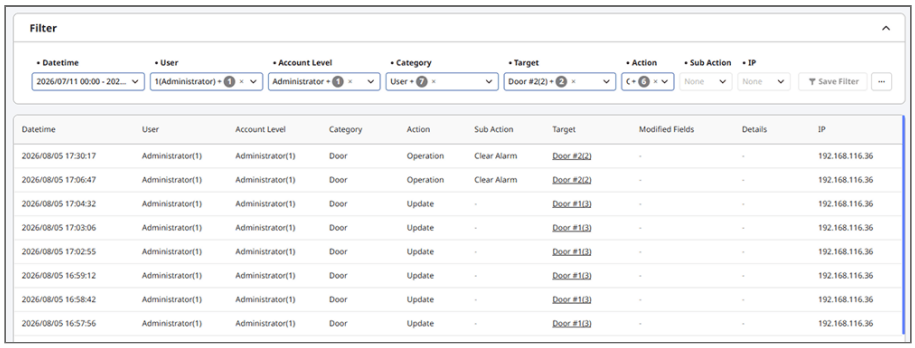


ポップアップ上部の**Search**入力フィールドに検索語を入力すると、一致する項目だけを強調表示するかフィルタリングします。対象ポップアップでは、検索時にグループとグループ別件数も更新されますが、タイトルの全体件数は検索に関係なく変わりません。

フィルターで記録を絞り込む

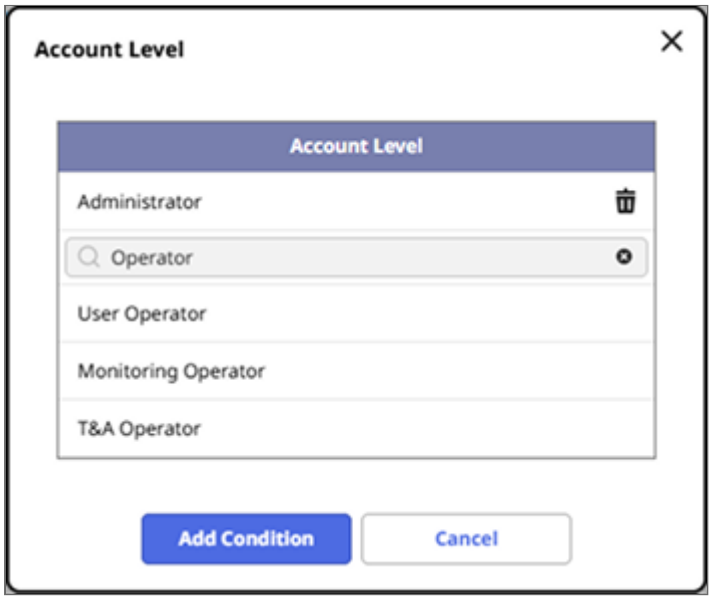
Filterセクションのフィルターを組み合わせ、目的の記録を絞り込んで探してください。同一フィルター内で複数の値を選択する

と OR で、異なるフィルターを併用すると AND で結合されます。

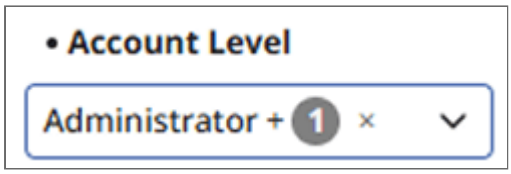


フィルター	動作方式
Datetime	開始・終了の日時を指定します。照会期間に長さ制限はありません。
User	検索語を入力し、Enterキーを押して一致するユーザーを探してください。最初に開くと一覧は空です。
Account Level	検索語を入力し、Enterキーを押して一致する管理者レベルを探してください。
Category	検索可能なチェックボックス一覧から、分類を一つ以上選択してください。
Target	検索語を入力し、Enterキーを押して一致する対象を探してください。
Action	チェックボックス一覧から動作を一つ以上選択してください。
Sub Action	検索可能なリストから詳細操作を選択してください。
IP	検索語を入力し、Enter キーを押して一致する IP を検索します。

- 適用したフィルターがない場合、現在の日付から30日前までの記録を既定で表示します。
- 各フィルターポップアップで値を選択し、**Add Condition** ボタンをクリックすると、検索にすぐ反映されます。 **Cancel** をクリックすると、選択を取り消してポップアップを閉じます。



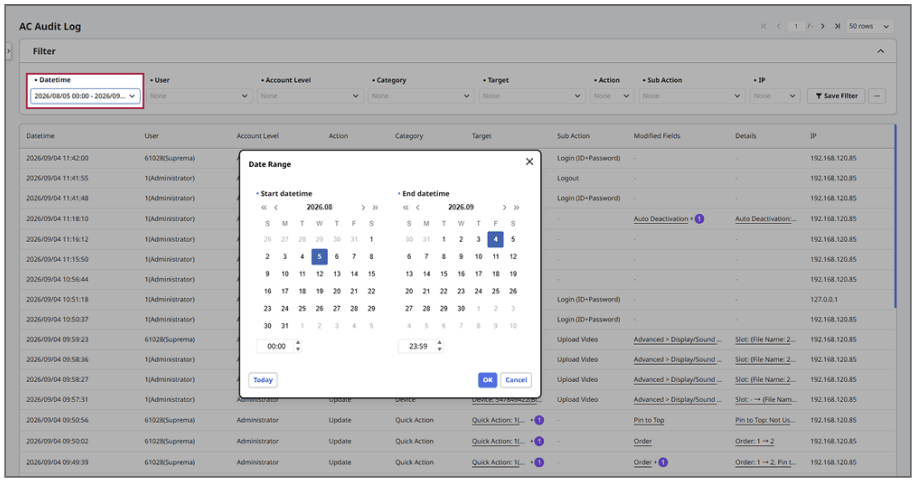
- 適用したフィルターは、先頭の条件と追加件数で要約して表示されます。 ✕ ボタンをクリックすると、該当フィルターのみ解除されます。値を選択していないフィルターは **None** と表示されます。



> **情報**
>
> **User**、**Account Level**、**Target**、**IP** フィルターは、検索語を入力すると結果が表示されます。部分一致に対応しているため、名前やIDの一部だけを入力しても検索できます。削除した対象も **Deleted** と表示して検索します。

照会期間の指定

Datetime をクリックすると、**Date Range** ポップアップが開きます。

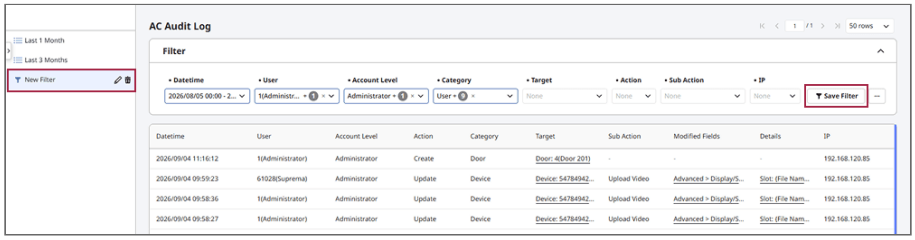


1. **Start datetime** と **End datetime** の日時をそれぞれ指定します。 **Today** をクリックすると、今日の日付へ移動します。
2. 照会期間を適用するには、**OK** ボタンをクリックします。

フィルターの保存

よく使う検索条件は **Saved Filters** に保存し、再度読み込めます。

1. 希望する条件でフィルターを設定します。
2. **Filter** セクションの **Save Filter** ボタンをクリックします。
3. 画面左のフィルターリストに **New Filter** が追加されます。



- フィルター名を変更するには ✎ ボタンをクリックし、新しい名前を入力して Enter キーを押します。

- フィルターを削除するには 🗑 ボタンをクリックします。

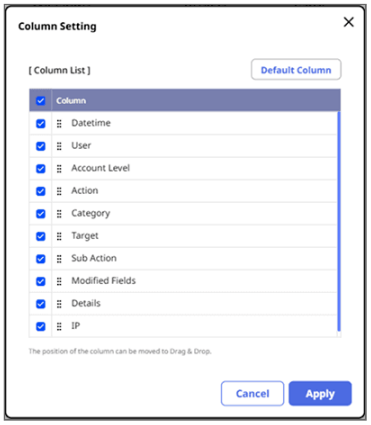
> **情報**
> 保存できるフィルターは最大20件です。保存したフィルターはブラウザーに保存されるため、別のPCやブラウザーでは表示されません。

ページナビゲーション

ページを移動したり、1ページに表示する一覧の件数を設定できます。

- ⏮：最初のページへ移動します。
- ‹：前のページへ移動します。
- ›：次のページへ移動します。
- ⏭：最後のページへ移動します。
- 50 rows ：一ページに表示するリスト数を選択します。

列設定



監査ログテーブルの列の位置を変更したり、非表示にしたりできます。
Filter セクション右側の ••• → **Column Setting** をクリックしてください。

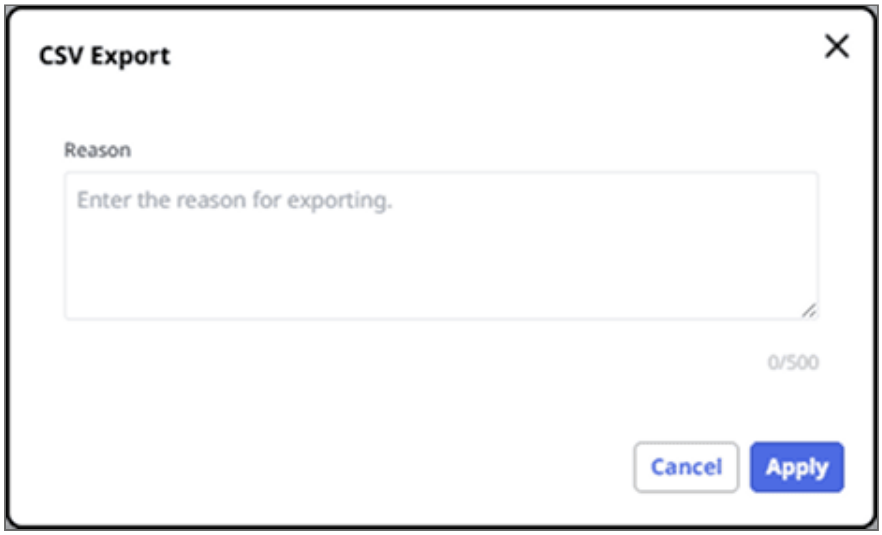
- **[Column List]** で非表示にする項目のチェックボックスの選択を解除してください。
- 列の順序を変更するには、目的の項目をドラッグしてください。
- 列設定を初期化するには、**Default Column** をクリックしてください。

設定を保存するには、**Apply** ボタンをクリックします。

CSV へのエクスポート

監査ログをCSVファイルにエクスポートし、外部分析ツールで活用してください。

1. **Filter** セクションで必要に応じてフィルターを設定してください。
2. セクション右側の ••• → **CSV Export** をクリックしてください。
3. **CSV Export** ウィンドウが表示されたら、**Export Reason**(任意)を入力し、**Apply** ボタンをクリックします。



エクスポートしたCSVファイルは、各レコードにつき一行で10列すべてを含み、すべての値は引用符で囲んで表記されます。対象が複数の値はバーティカルバー(|)で区切ります(例: **User: 7(Kim)|User: 8(Lee)**)。また、**Details** の値は省略せず、すべての対象とすべてのフィールドを含みます。

> **注意**
> CSV ファイルは、スプレッドシートが数式として解釈できる値を元のまま含みます。ダウンロードした CSV ファイルをスプレッドシートで直ちに開かず、必要に応じてテキストのインポート機能で開いてください。

> **ヒント**
> フィルターを設定した場合、フィルタリングされた結果だけをCSVファイルにエクスポートします。

BioStar 2 の記録を確認

以前のバージョン(BioStar 2)で残した記録も、同じテーブルでまとめて照会できます。 BioStar 2 の記録は次のように表示されます。

- **User** と **Target** は **名前(id)** 形式(空白の変形を含む)で、元の形のまま保持します。
- **Modified Fields** は常にハイフン(-)で表示します。
- 提供されるフィルターでBioStar 2 の記録も同様に検索できます。**User** と **Target** は名前とIDの両方に一致します。

> **情報**
> レガシー記録には、サポートしない検索条件が含まれる場合があります。保存したフィルターを読み込むときに一部の条件を除外すると、システムが案内メッセージを表示します。

監査設定を管理する

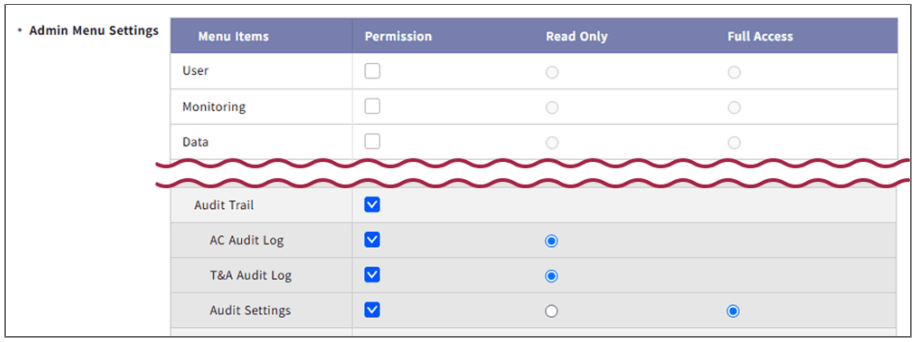
監査ログは時間とともに蓄積するため、保存容量と個人情報保護の観点から保管期間を管理する必要があります。**Audit Settings** で **AC Audit Log** 記録の保管期間と参照履歴を記録するかどうかを設定してください。

> **情報**
> 勤怠管理（T&A）の監査ログの保管ポリシーは別のドキュメントで説明します。

権限の説明

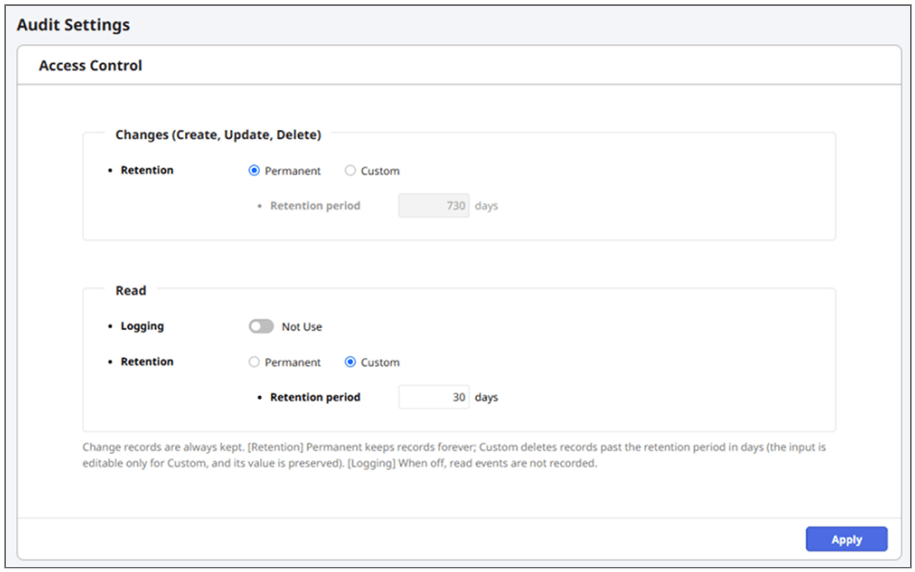
Administrator は **Audit Settings** メニューで常に参照および変更できます。カスタム権限管理者は、**Admin Menu Settings**で**Audit Settings**メニュー項目を**Read Only**に適用すると参照のみ行えます。**Full Access**に適用すると参照と変更の両方を行えます。

> ***Settings*** → ***Account*** → ***Account*** → ***Add Custom Level***



監査設定を開く

1. **Launcher**ページで**Settings**をクリックします。
2. 画面左側のサイドバーで **Audit Trail** → **Audit Settings** をクリックしてください。



保管ポリシーの設定

Access Control セクションは次の二つのグループで構成されます。

- **Changes (Create, Update, Delete)**：作成、修正、削除の記録です。システムは常に記録するため、オン/オフを切り替えられません。
- **Read**：参照記録です。記録するかどうかを設定します。

> **情報**
>
> - **Retention period** は、最小1日から最大2,147,483,647までの整数で入力してください。
> - **Access Control** セクションの設定変更は、**AC Audit Log** で監査記録として確認してください。

変更記録

Changes (Create, Update, Delete) グループは常に記録されるため、**Retention** を選択してください。

- **Permanent**：自動削除せず、記録を永久に保管します。
- **Custom**：規制や社内ポリシーにより保管期間を制限する必要がある場合は、このオプションを選択してください。**Retention period** 入力欄が有効になったら、保管期間を日単位で入力してください。

参照記録

Read グループでは、参照記録を残すかどうかを設定します。

- **Logging**：参照記録を残すには **Use** に設定してください。不要な場合は **Not Use** に設定してください。
- **Retention**：保管方法を選択してください。
  - **Permanent**：参照記録を自動削除せず、永久に保管します。
  - **Custom**：**Retention period** 入力欄が有効になります。保管期間を日単位で入力してください。

> **情報**
>
> **Logging** を **Not Use** に設定すると、参照イベント自体を記録しません。その後 **Use** に設定しても、以前の期間の記録は参照できません。

設定を保存

Changes (Create, Update, Delete) と **Read** の設定が完了したら、**Access Control** セクション下部の **Apply** ボタンをクリックしてください。二つのグループの設定値をまとめて保存します。

自動削除の動作方法

Custom で設定した保管期間を超えた記録は、ユーザー操作に関係なく、サーバーが毎日午前1時に実行するジョブで自動削除します。判定と削除は同じジョブで一度に行われ、この判定は一日一回だけ行います。

> *たとえば、**Read** の記録に **Custom** 方式で30日を適用した場合、午前1時のジョブ実行時点を基準に30日を超えた記録を、そのジョブで直ちに削除します。保管期間を超えた直後の記録でも、ジョブは一日に一度だけ実行されるため、その時点を過ぎると次の日の午前1時のジョブで削除されます。*

Retention を **Permanent** に設定すると自動削除ジョブが実行されず、記録が永久に残ります。

システム設定

BioStar X システムを安定して運用するための設定方法を案内します。サーバーの基本情報とHTTPS証明書を設定し、システムのバックアップと復元でデータを保護し、パスワードポリシーと暗号化でセキュリティを強化します。このほか、夏時間、メール通知、言語、タイムゾーンなどの基本環境も設定します。

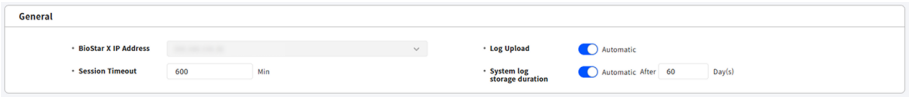
サーバーの詳細を設定する

BioStar X サーバーの基本情報、ユーザーおよびデバイス管理、サーバーマッチング、システムログレベル、顔画像保存の設定を変更できます。

1. Launcherページで**Settings**をクリックします。
2. 画面左のサイドバーで **System** → **Server** をクリック。
3. 各セクションで必要な項目を設定してください。
   - **General**：IP アドレス、ポート番号、セッションタイムアウト、イベントログのアップロード方法、ログ保存期間を設定できます。
   - **User/Device Management**：ユーザーおよびデバイス管理設定を変更できます。
   - **System Log Level Settings**：システムログレベル設定を変更できます。
   - **Expert Settings**：顔の実画像とテンプレートを両方保存するか、実画像を保存せずテンプレートのみ保存するかを設定できます。
4. 設定を保存するには、画面右下の **Apply** ボタンをクリックしてください。

基本情報を設定する

General セクションでは、**BioStar X** の基本情報を確認または設定できます。

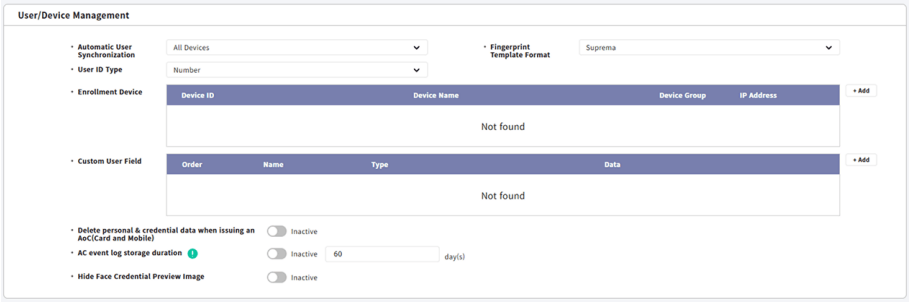


- **BioStar X IP Address**：サーバー IP アドレスを確認できます。
- **Log Upload**：イベントログのアップロード方法を選択できます。サーバーとリアルタイム通信が困難な場合は、**Manual**に設定してください。
- **System log storage duration**：ログ保存期間は1～120まで設定できます。
- **Session Timeout**：セッションのタイムアウト時間を設定できます。 **BioStar X** にログインした後、設定した時間操作がないと自動でログアウトします。

> **情報**
> **Log Upload** オプションを **Automatic** に設定すると、サーバーと装置間の接続が切断され、再接続時に装置に保存されたイベントログがサーバーに自動アップロードされます。

ユーザーおよびデバイス管理

User/Device Management セクションでは、ユーザーとデバイス間の同期および認証方法を設定できます。



Automatic User Synchronization

Automatic User Synchronization オプションでは、サーバーとデバイス間でユーザー情報を同期する方法を選択できます。同期にはユーザーに割り当てられたアクセスレベルとアクセスグループも含まれるため、**BioStar X**サーバーでアクセスレベルまたはアクセスグループを変更すると、システムはその変更を関連デバイスに自動的に適用します。

- **All Devices**：ユーザー情報がサーバーとデバイス間で自動的に同期されます。
- **All Devices(Including user update from device)**：サーバーのユーザー情報がサーバーに登録されたすべてのデバイスと同期されます。ただし、デバイスで修正したユーザー情報はサーバーに同期されず、デバイスで追加したユーザー情報のみがサーバーに同期されます。
- **Specific Devices(Only devices belonging to the access group)**：変更があるアクセスグループに属するデバイスのみがサーバーと自動同期されます。

> **情報**
>
> - **Specific Devices(Only devices belonging to the access group)** オプションを選択すると、デバイスに保存されているユーザーのうちアクセスグループに属していないユーザーはサーバーで管理できません。このオプションを使用するには、**Settings** → **Device** → **Device** メニューで各デバイスを選択し、**Delete Data & Sync Device** をクリックして同期を実行します。 **Delete Data & Sync Device** 機能の詳細については デバイス管理機能を利用する を参照してください。
> - **Specific Devices(Only devices belonging to the access group)** オプションを選択しても、以下のように特別な目的で指定されたアクセスグループの場合、デバイスのアクセスグループに関係なく同期されます。
>   - デバイスおよびエレベーターで設定された二要素認証アクセスグループ
>   - アンチパスバック設定の常時通過グループ
>   - スケジュール施錠設定の常時通過グループ
>   - スケジュール解放設定の解放認証入退室グループ
>   - 警備設定の警備/解除グループ
> - **Specific Devices(Only devices belonging to the access group)** オプションを選択しても、デバイス管理者に指定されたユーザーはアクセスグループに関係なく同期されます。

Fingerprint Template Format

Fingerprint Template Format オプションでは、指紋テンプレート形式を選択できます。次の項目から選択します。

- **SUPREMA**：Suprema指紋テンプレート形式です。 Supremaデバイスで指紋を登録する際に使用します。
- **ISO**：ISO国際指紋テンプレート形式です。
- **ANSI378**：米国規格協会（ANSI）が定義した指紋テンプレート形式です。

情報
デバイスにユーザーの指紋テンプレートが残っている場合、別の形式に変更できません。

User ID Type

User ID Type オプションでは、ユーザーIDの種類を **Number** または **Alphanumeric** に設定できます。 **BioStar X** サーバーに登録されているデバイス一覧を確認し、互換性のある設定値を選択します。

▼ User ID Type を変更できるデバイスとファームウェアバージョンを表示

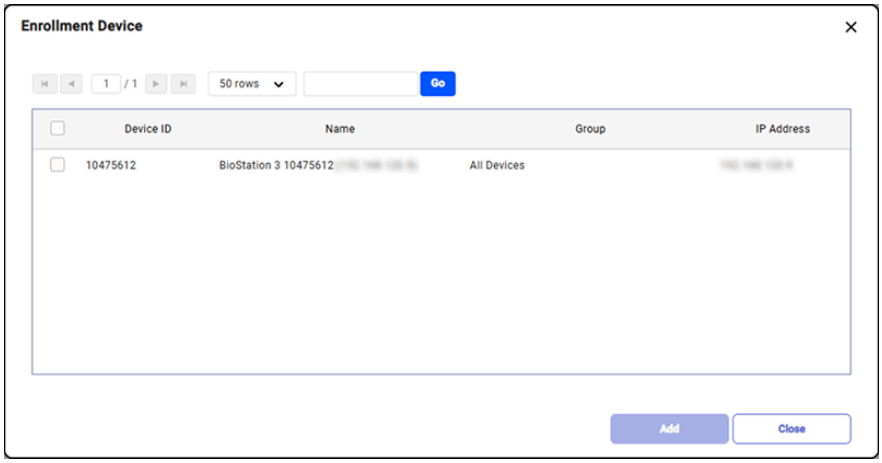
- BioStation 3 Maxのファームウェアバージョン1.0.0以降
- XPass Q2のファームウェアバージョン1.0.0以降
- BioStation 3 ファームウェア 1.0.0 以上
- X-Station 2 ファームウェア 1.0.0 以上
- XPass 2 ファームウェア 1.0.0 以上
- FaceLite ファームウェア 1.0.0 以上
- BioLite N2 ファームウェア 1.0.0 以上
- XPass D2 ファームウェア 1.0.0 以上
- BioEntry R2 ファームウェア 1.0.0 以上
- BioEntry P2 ファームウェア 1.0.0 以上
- FaceStation 2 ファームウェア 1.0.0 以上
- BioEntry W2 ファームウェア 1.1.0 以上
- BioStation L2 ファームウェア 1.2.0 以上
- BioStation A2 ファームウェア 1.3.0 以上
- BioStation 2 ファームウェア 1.4.0 以上
- CoreStation ファームウェア 1.0.0 以上

情報
Alphanumeric から **Number** へ変更する場合、**BioStar X** に登録されているすべてのユーザー情報を削除する必要があります。

Enrollment Device

指紋や顔、カードを登録する際によく使用するデバイスを **Enrollment Device** オプションに追加し、便利に利用できます。

1. デバイスを追加するには、**+ Add** ボタンをクリックします。
2. **Enrollment Device** ウィンドウが表示されたら、一覧で目的のデバイスのチェックボックスをクリックします。



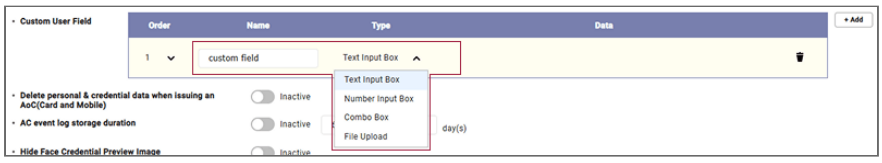
3. 選択したデバイスを追加するには、**Add** ボタンをクリックします。
4. 追加したデバイス設定を保存するには、画面右下の **Apply** ボタンをクリックします。

> **情報**
>
> - 登録デバイスが多く一覧から見つけにくい場合は、検索入力フィールドにキーワードを入力してデバイスを検索します。デバイスID、デバイス名、デバイスグループ、IPアドレスを入力できます。
> - ユーザー情報を登録する際の指紋または顔、カードクレデンシャル登録の詳細は次のドキュメントを参照してください。
>   - 指紋を登録する
>   - 顔を登録する
>   - 入退室カードを登録する
>   - モバイルアクセスカードを登録する

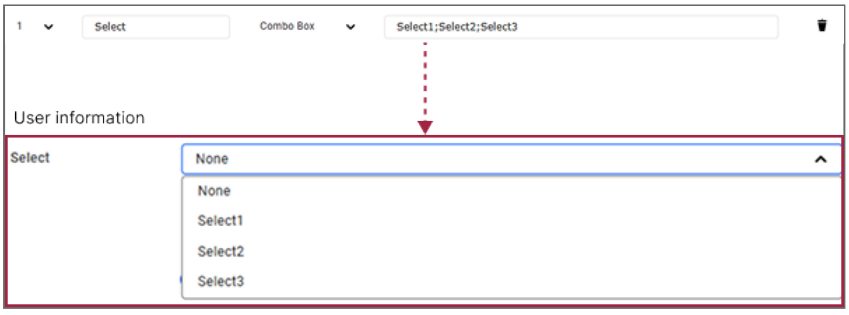
Custom User Field

Custom User Field オプションでは、ユーザーの付加情報を入力するフィールドを追加できます。追加したフィールドはユーザー情報画面に表示されます。

1. カスタムユーザーフィールドを追加するには、**+ Add** ボタンをクリックします。
2. カスタムユーザーフィールドの名前を入力し、タイプで希望の項目を選択します。



- **Number Input Box**：0 から 4294962795 まで入力でき、文字は入力できません。
- **Text Input Box**：最大 32 文字の数字および文字を入力できます。
- **Combo Box**：最大 20 個のサブ項目を 32 文字で追加でき、各項目はセミコロン（;）で区切ります。(例：選択1;選択2;選択3)



- **File Upload**：ファイルアップロード用のフィールドを追加できます。

  - 最大ファイルサイズは1MBです。
  - ファイル名は最小1文字から最大120文字まで可能です。
  - ファイル名の制約：ファイル名には英数字、アンダースコア(`_`)、ハイフン(`-`)を使用し、拡張子の区切りにはドット(`.`)を使用します。
  - 許可されるファイルの拡張子に制限はありません。アップロードされたファイルは暗号化されたうえでデータベースに保存されます。

3. 追加したカスタムユーザーフィールドを保存するには、画面右下の **Apply** ボタンをクリックします。

情報

- カスタムユーザーフィールドの順序を変更するには、**Order** 列の数字を変更します。該当フィールドの位置が変更されます。
- カスタムユーザーフィールドを修正した後、画面右下の **Apply** ボタンをクリックします。
- カスタムユーザーフィールドを削除するには、 ボタンをクリックします。削除したフィールドは復元できません。
- ユーザー情報の登録・編集の詳細については ユーザー を参照してください。
- カスタムユーザーフィールドを追加したユーザー情報をカードに印刷できます。詳細については カードを印刷する を参照してください。

AoCカード設定

ユーザーのクレデンシャルをカードに保存するAoC（Access on Card）を発行する際に、**BioStar X** サーバーから個人情報とクレデンシャル情報を削除するには、**Delete personal & credential data when issuing an AoC(Card and Mobile)** オプションを有効にします。

情報

▼ NFCモバイルカードをサポートするデバイスを表示

- モバイルデバイスのOS：Android 7.0 以上
- BioStar X Mobile
- BioStation 3 Max
- XPass Q2
- XPass 2
- FaceLite
- BioLite N2
- XPass D2
- BioEntry R2
- BioEntry P2
- FaceStation 2
- BioEntry W2
- BioStation L2：BSL2-OM
- BioStation A2：BSA2-OMPW、BSA2-OIPW
- BioStation 2：BS2-OMPW、BS2-OIPW

▼ BLEモバイルカードをサポートするデバイスを表示

- モバイルデバイスのOS：Android 7.0 以上 / iOS 13.0 以上
- BioStar X Mobile
- BioStation 3 Max
- XPass Q2
- XPass 2
- FaceLite：FL-DB
- BioLite N2
- XPass D2
- FaceStation 2：FS2-AWB

- **Mobile Access Card**と**Mobile Access**は同時に使用できません。

その他

- **AC event log storage duration**：出入管理イベントログを保存する期間を設定します。

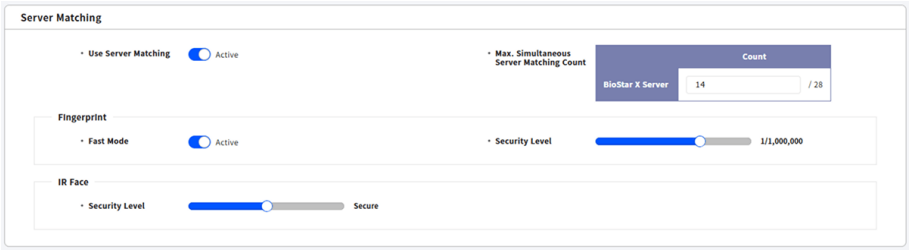
情報

入退室管理イベントログの保存期間の設定は、サーバーログにのみ適用されます。デバイスイベントログには、この設定が適用されません。デバイスイベントログを削除する場合は、**Settings** → **Device** → **Device** メニューでデバイスイベントログを個別に削除してください。

- **Hide Face Credential Preview Image**：ユーザーのプライバシーを保護するため、顔クレデンシャルを登録する際にプレビュー画像を非表示にできます。このオプションを有効にすると、ユーザーの顔クレデンシャルを登録する際にプレビュー画面が表示されません。

サーバーマッチングを設定する

Server Matching セクションでは、ユーザー情報をデバイスで認証せず **BioStar X** で認証できるサーバーマッチング機能を設定できます。



- **Use Server Matching**：サーバーマッチングの使用可否を設定できます。
- **Max. Simultaneous Server Matching Count**：同時にマッチングできる最大サーバーマッチング数を設定できます。

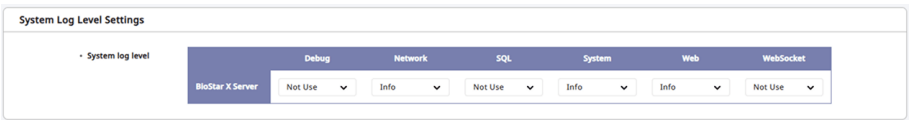
> このオプションは、**BioStar X** をインストールしているサーバー PC の CPU 性能によって異なる場合があります。

- **Fingerprint**
  - **Fast Mode**：指紋マッチング速度を調整できます。
  - **Security Level**：指紋に対するサーバーマッチングのセキュリティレベルを設定できます。セキュリティレベルが高いほど本人拒否率（FRR）が増加します。
- **IR Face**
  - **Security Level**：IRフェイスに対するサーバーマッチングのセキュリティレベルを設定できます。セキュリティレベルが高いほど本人拒否率（FRR）が増加します。

> **情報**
>
> **Server Matching** 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 ポリシーをご参照ください。

システムログレベルの設定

System Log Level Settings セクションでは、データベースに保存されるシステムログのレベルを設定できます。



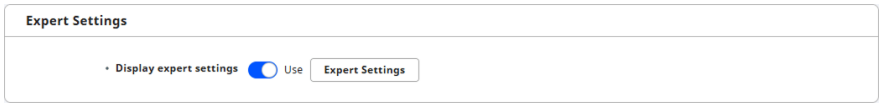
システムログはあらかじめ定義されたカテゴリーで管理され、ログレベルは **Trace**、**Debug**、**Info**、**Warning**、**Error**に分類されます。上位レベルには下位レベルのログがすべて含まれます。例えば、システムログレベルを **Trace** に選択すると、下位レベルである **Debug**、**Info**、**Warning**、**Error** のログもすべて含めて保存されます。

顔画像の保存

顔をクレデンシャルとして登録する際に、実際の画像とテンプレートの両方を保存するか、実際の画像は保存せずテンプレートのみ保存するかを設定できます。

> **使用前に**
>
> **Display expert settings** オプションを有効にする前に、**Server** メニューで行った変更がある場合は、先に変更内容を保存する必要があります。画面右下の **Apply** ボタンをクリックします。

1. **Expert Settings** セクションで **Display expert settings** オプションを **Use** に設定します。



2. **Expert Settings** ボタンをクリックします。
3. **Expert Settings** 画面に進み、**Store Face Image** オプションを設定します。



   - **Use**：既定値です。顔クレデンシャルの実際の画像とテンプレートを両方保存します。
   - **Not Use**：顔クレデンシャルの実際の画像は保存せず、テンプレートのみ保存します。このオプションを選択したら表示される警告ポップアップをよく読み、設定してください。

4. **Apply** をクリックして設定を保存します。

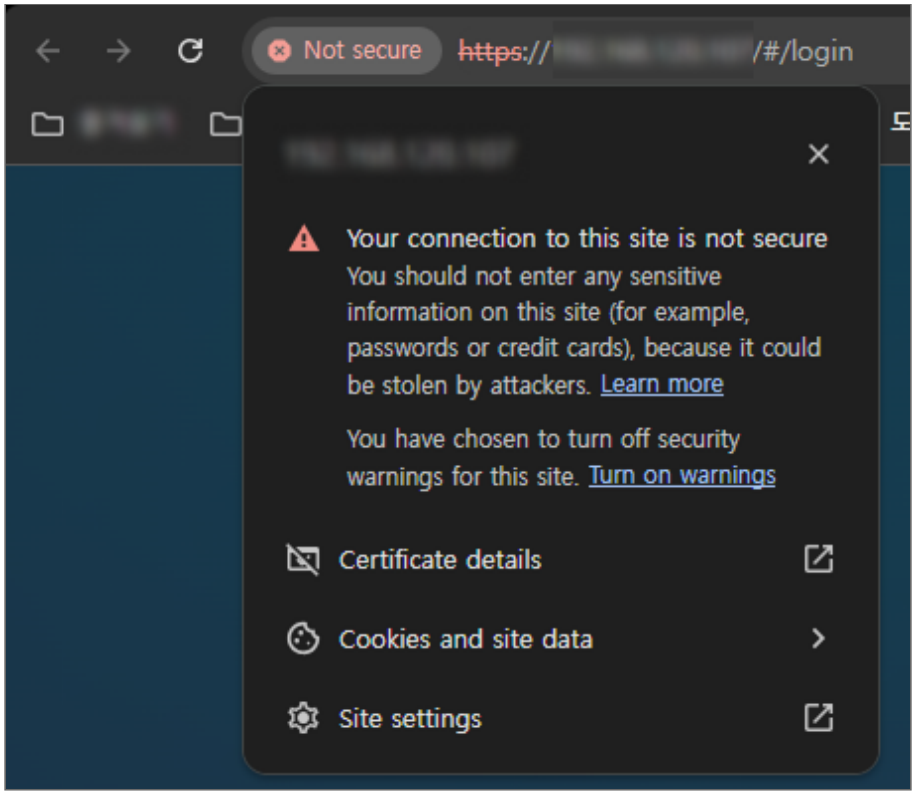
> **注意**
>
> **Store Face Image オプションを無効にする際の注意事項**
>
> - この機能を無効にすると、保存されている顔画像はすべて削除され、今後登録される顔画像も画像を除いたテンプレートのみ保存されます。
> - 登録済みの顔画像が2種類のテンプレートを持っていない場合、この機能を無効にできません。 **Face Migration** 機能の詳細については 顔マイグレーション を参照してください。
> - この機能を無効にした後、**Data File Import** で無効な顔画像テンプレートが含まれている場合、データファイルをインポートできません。問題を解決するには、この機能を一時的に有効にしてからデータファイルをインポートしてください。

HTTPS 証明書をインストールする

BioStar X を HTTPS で接続するには、**BioStar X** をインストールしたサーバーの IP アドレスを登録して証明書をインストールする必要があります。

証明書のインストールが必要な場合

BioStar X に HTTPS 証明書がインストールされていない状態で接続すると、Web ブラウザーに次のようなセキュリティ警告が表示されます。

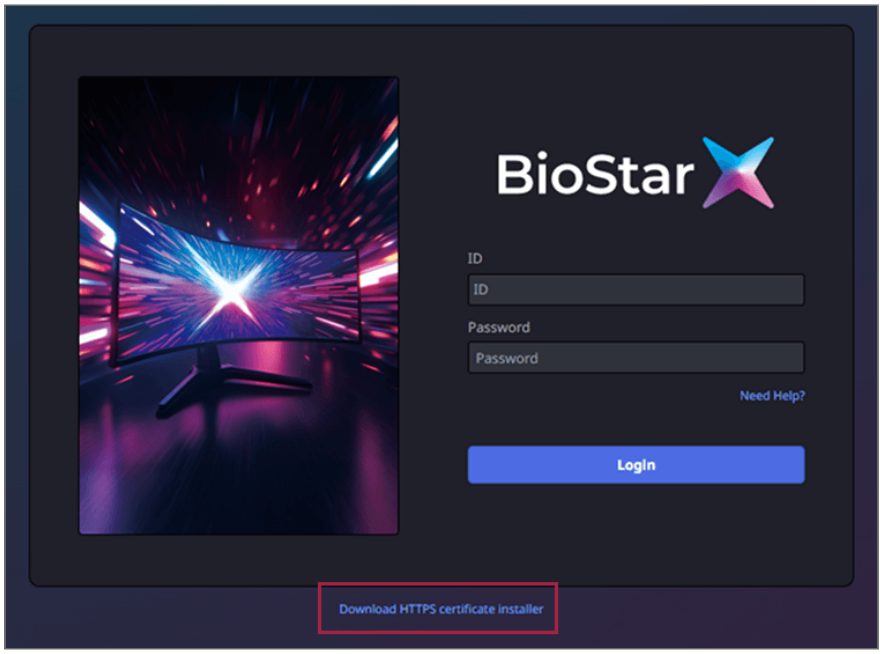


これは、ブラウザーがサーバーの身元を確認できないために表示される警告です。証明書をインストールすると、ブラウザーが **BioStar X** サーバーを信頼し、警告なしで安全な HTTPS 接続を利用できます。

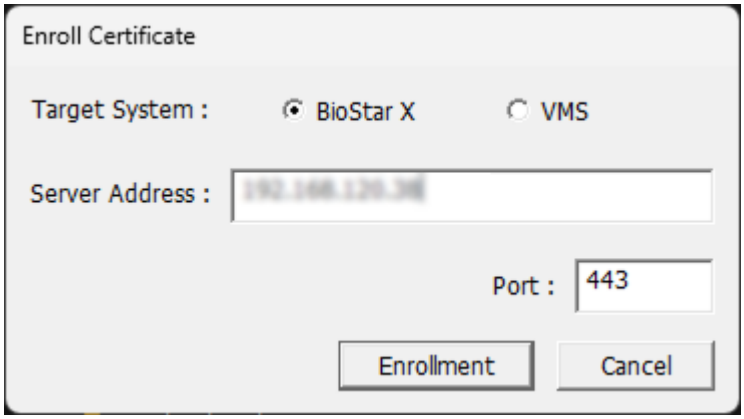
証明書のインストール

適切にネットワーク接続するため、**BioStar X** を使用する前に証明書をインストールします。

1. **BioStar X** のログインページにアクセスします。
2. 画面下部の **Download HTTPS certificate installer** リンクをクリックします。



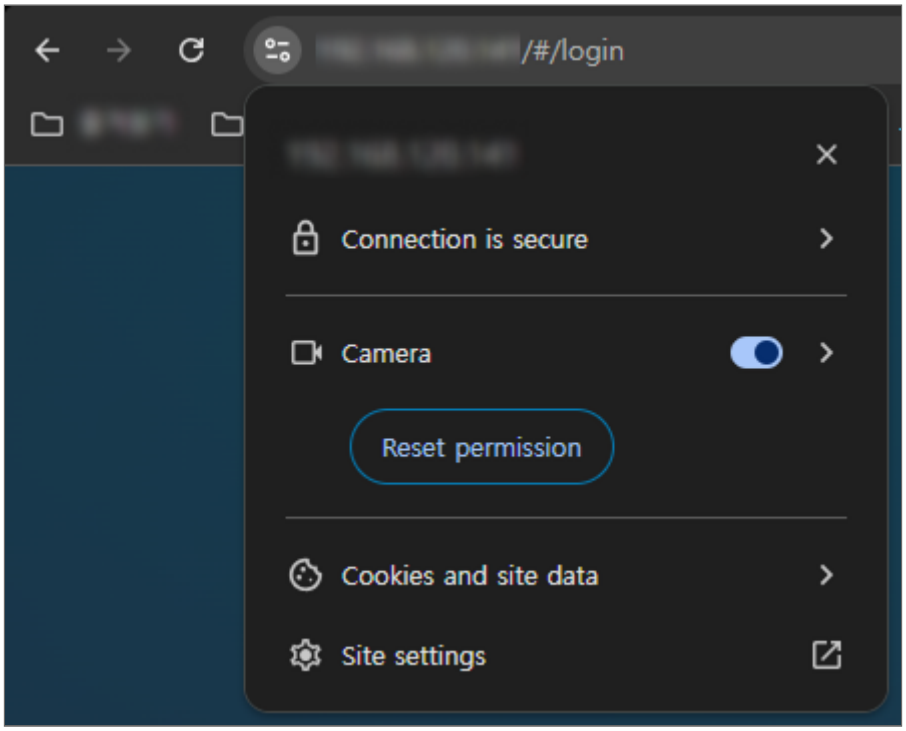
3. *cert-register.zip* ファイルをローカルに保存します。
4. ダウンロードしたファイルを解凍し、*cert-register.exe* ファイルを実行します。 **Enroll Certificate** プログラムが起動します。
5. **Target System** で **BioStar X** を選択し、**BioStar X** がインストールされている PC の IP アドレスを **Server Address** に入力して **Enrollment** ボタンをクリックします。



> **BioStar X** のデフォルトポート番号は 443 です。ポート番号を変更した場合は **Port** に変更後のポート番号を入力します。

6. セキュリティ警告メッセージを確認し、**はい** をクリックします。

Web ブラウザーを再起動し、登録した IP アドレスを入力して **BioStar X** ページへ移動します。アドレスバー左側のアイコンをクリックすると **この接続は安全です** のメッセージが表示されます。

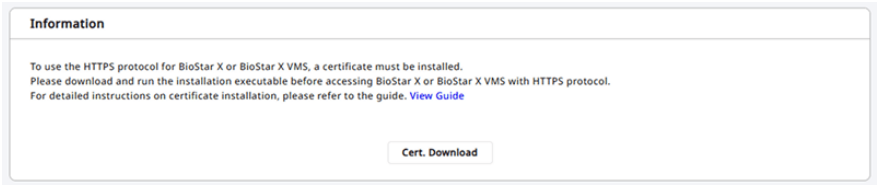


情報

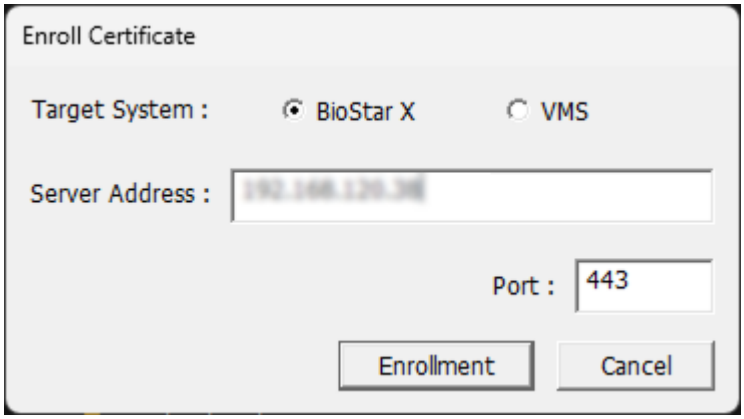
Enroll Certificate で入力する IP アドレスは **BioStar X** に設定されている IP アドレスと同一でなければなりません。
Settings → **System** → **Server** のメニューにある **BioStar X IP Address** で確認できます。

サーバー設定で証明書をインストール

1. **Launcher**ページで**Settings**をクリックします。
2. 画面左のサイドバーで **System** → **HTTPS** をクリック。
3. **Cert. Download** をクリックします。



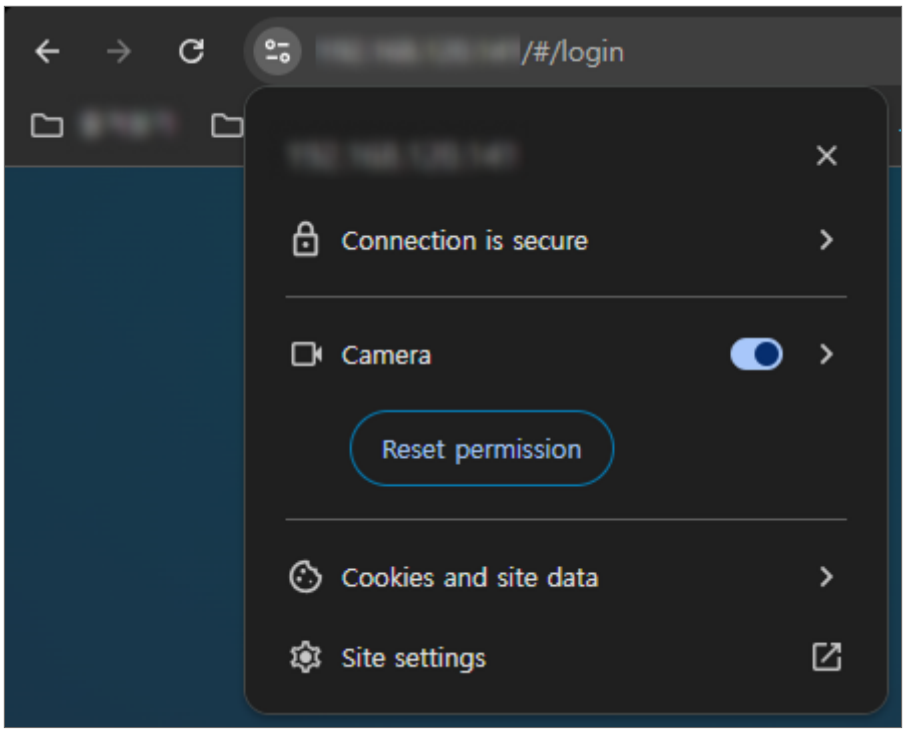
4. *cert-register.zip* ファイルをローカルに保存します。
5. ダウンロードしたファイルを解凍し、*cert-register.exe* ファイルを実行します。 **Enroll Certificate** プログラムが起動します。
6. **Target System** で **BioStar X** を選択し、**BioStar X** がインストールされている PC の IP アドレスを **Server Address** に入力して **Enrollment** ボタンをクリックします。



> **BioStar X** のデフォルトポート番号は 443 です。ポート番号を変更した場合は **Port** に変更後のポート番号を入力します。

7. セキュリティ警告メッセージを確認し、**はい** をクリックします。

Web ブラウザーを再起動し、登録した IP アドレスを入力して **BioStar X** ページへ移動します。アドレスバー左側のアイコンをクリックすると **この接続は安全です** のメッセージが表示されます。



VMS サーバーの証明書をインストールする

次のような状況が発生した場合、VMS サーバーにインストールされている証明書をクライアント PC にインストールして問題を解決できます。

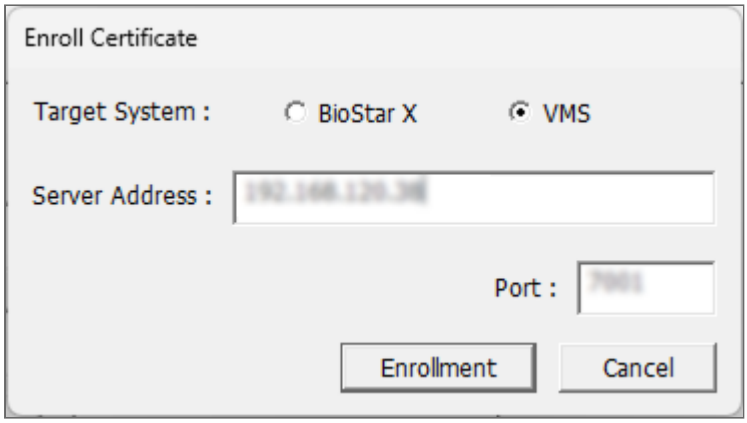
- ブラウザーで **Video Management System** (VMS) にアクセスした際に「安全ではありません」と警告が表示される場合
- **Monitoring** ページでライブ映像は再生されるが録画映像が再生されない場合
- VMS サーバーと **BioStar X** を同じサーバーにインストールする場合

情報

- VMSサーバーに証明書をインストールする方法は、VMS と連携するをご参照ください。
- VMS サーバーと連携する機能は、追加オプションを別途購入することで利用できます。ライセンスポリシーの詳細については、ライセンス ポリシーをご参照ください。

クライアント PC に証明書をインストールする

1. **BioStar X** をインストールしたクライアント PC のログイン画面、または **Settings** → **System** → **HTTPS** から HTTPS 証明書インストーラ (*cert-register.zip*) をダウンロードします。
2. ダウンロードしたファイルを解凍し、*cert-register.exe* ファイルを実行します。 **Enroll Certificate** プログラムが起動します。
3. **Target System** で **VMS** を選択し、次の情報を入力します。



   - **Server Address**：VMS サーバーの IP アドレス
   - **Port**：VMS サーバーのポート番号
4. **Enrollment** ボタンをクリックします。
5. セキュリティ警告メッセージを確認し、**はい** をクリックします。

Web ブラウザーを再起動し、**Monitoring** ページで VMS サーバーの録画映像が正常に再生されるか確認します。

システムをバックアップする

BioStar X のデータベース、各種設定、キーなどの主要情報をバックアップできます。バックアップファイルには、暗号化キー（enc key）や画像ログのパスなど、ユーザーが設定した項目も含まれます。 **System Backup** 機能は、サーバーデータの損失を防止したり、新しい PC へ移行する際に使用します。

サポートされるバックアップ方式は次のとおりです。

- **手動バックアップ**：ユーザーが手動でバックアップファイルを作成します。
- **自動バックアップ**：システムが設定された周期でバックアップファイルを自動生成します。

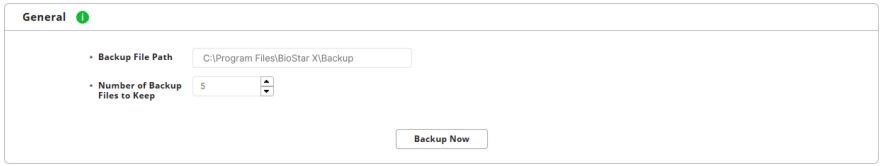
情報

- 以前の PC でバックアップした **BioStar X** のバックアップファイルを使用して新しい PC で **BioStar X** を復元する場合、ライセンスの再発行が必要です。
- SQL Server データベースと **BioStar X** が別々のサーバーにインストールされている場合、**BioStar X** のシステムバックアップと復元は使用できません。
- システムの復元の詳細については、システムを復元するを参照してください。

手動バックアップ

ユーザーがバックアップファイルを直接作成できます。

1. **Launcher**ページで**Settings**をクリックします。
2. 画面左のサイドバーで **System** → **System Backup** をクリックします。
3. **General** セクションで、バックアップファイルの保存パスと最大バックアップ数を設定します。



   - **Backup File Path**：バックアップファイルの保存パスを入力します。保存パスには、既に作成済みのディレクトリパスを入力します。
   - **Number of Backup Files to Keep**：最大バックアップ数を設定します。
4. **Backup Now** をクリックしてバックアップファイルを作成します。
5. 警告メッセージが表示されたら内容を確認し、**Continue** ボタンをクリックしてください。

バックアップファイルは **Backup File Path** オプションで指定したパスに *zip* 形式で保存されます。ファイル名は `BioStar_X_Backup_YYYYMMDD_HHMMSS.zip` 形式で生成されます。ここで `YYYYMMDD` はバックアップ日、`HHMMSS` はバックアップ時刻を示します。

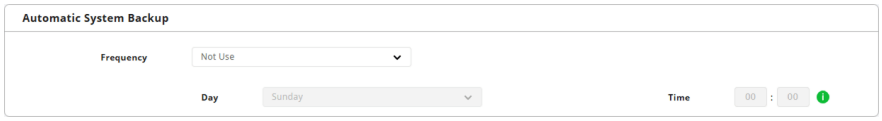
情報

- 最大バックアップ数を超えると、最も古いバックアップファイルから自動的に削除されます。
- **Number of Backup Files to Keep** には 1 ～ 100 の数値のみ入力できます。

自動バックアップの設定

自動バックアップを設定すると、システムが設定した周期でバックアップファイルを作成します。

1. **Launcher**ページで**Settings**をクリックします。
2. 画面左のサイドバーで **System** → **System Backup** をクリックします。
3. **Automatic System Backup** セクションで **Frequency** オプションを選択します。



- **Daily**：毎日自動バックアップします。 **Time** オプションでバックアップ時刻を設定します。
- **Weekly**：毎週自動バックアップします。 **Day** オプションで自動バックアップする曜日を設定し、**Time** オプションでバックアップ時刻を設定します。
- **Monthly**：毎月自動バックアップします。 **Date** オプションで自動バックアップする日付を設定し、**Time** オプションでバックアップ時刻を設定します。

4. **Apply** をクリックして設定を保存します。

自動バックアップを設定すると、定期的にバックアップが実行されます。自動バックアップの実行中に失敗が発生した場合、イベントログおよび監査トレースに失敗履歴が記録されます。失敗原因の詳細はログファイルで確認できます。

バックアップファイルは **General** セクションの **Backup File Path** オプションで指定したパスに *zip* 形式で保存されます。ファイル名は `BioStar_X_Backup_YYYYMMDD_HHMMSS.zip` 形式で生成されます。ここで `YYYYMMDD` はバックアップ日、`HHMMSS` はバックアップ時刻を示します。

> **情報**
>
> - 自動バックアップの頻度を **Monthly** に設定し、日付を 29、30、31 日に指定すると、その日付が存在しない月には自動バックアップを実行しません。
> - 時刻は **Preferences** で設定した標準タイムゾーンを基準にします。標準タイムゾーンの設定の詳細については、基本設定を構成するを参照してください。

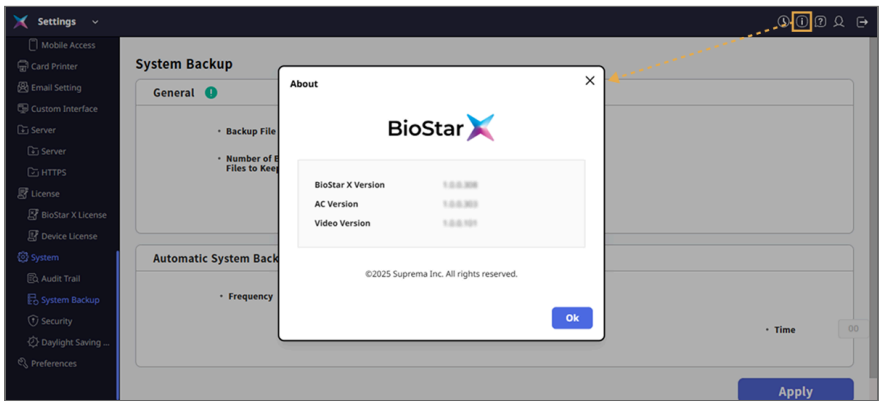
システムを復元する

BioStar X で問題が発生した場合や以前の状態に戻す必要がある場合は、システムバックアップファイルを使用して復元できる。復元機能を使用すると、データベース、各種設定、ライセンス情報などをバックアップ時点の状態に復元できます。

開始する前に

システム復元を開始する前に次の項目を確認してください。

- バックアップ時点の **BioStar X** バージョンと現在のバージョンが異なる場合、復元を実行できない。 **BioStar X** のバージョンを確認するには、画面右上の ⓘ をクリックする。



- バックアップ時点の **BioStar X** バージョンを確認するには、バックアップファイルを展開し、*sysbackup.conf* の `biostarVersion` を確認する。

- SQL Server データベースと **BioStar X** が別々のサーバーにインストールされている場合、**BioStar X** のシステムバックアップと復元は使用できません。
- 復元対象サーバーの IP アドレスがバックアップサーバーと異なる場合：
  - **BioStar X v1.0.2 以上**: 復元時に復元先の IP アドレスを検出し、既存の証明書の代わりに新しい IP アドレスに基づいて証明書を自動的に再発行します。証明書を再発行した後、当該証明書を使用する関連サービスは自動的に再接続されるため、追加の作業は不要です。
  - **BioStar X v1.0.1 以下**: 復元に失敗する可能性があります。復元を実行する前にサーバーの IP アドレスを確認してください。
- 暗号化キーやイメージログのパスが変更されていても、復元時は復元対象の **BioStar X** の現在の設定パスに従います。別途パス設定を指定していない場合は、復元対象の **BioStar X** の既定のパスが使用されます。
- 復元を実行する際、現在のデータは自動的にバックアップされるため、復元が失敗しても実行前の状態に戻せます。

> **情報**
> システムバックアップの作成については、システムをバックアップするを参照してください。

システム復元

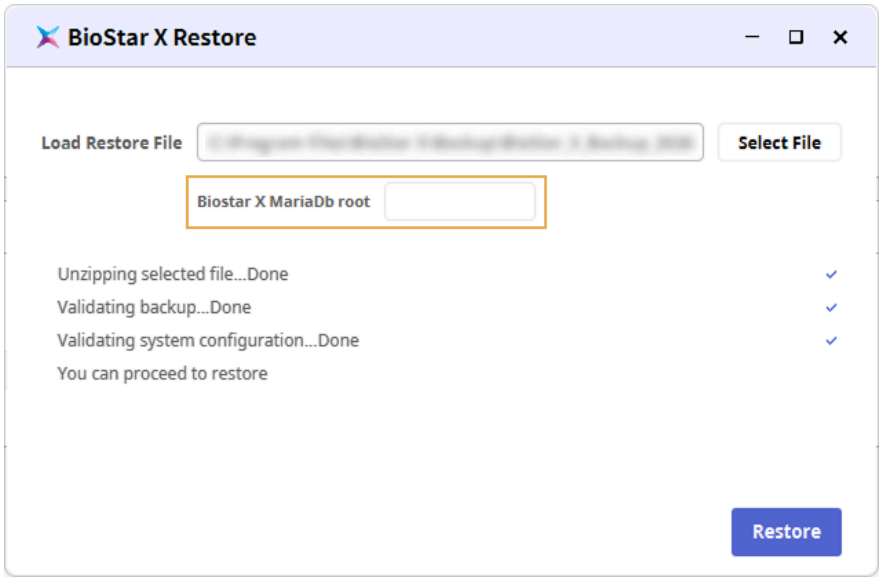
1. Windows で 開始 → **BioStar X** → **BioStar X Restore** を実行する。

   > *プログラムパス：C:\Program Files\BioStar X\biostar-restore.exe*

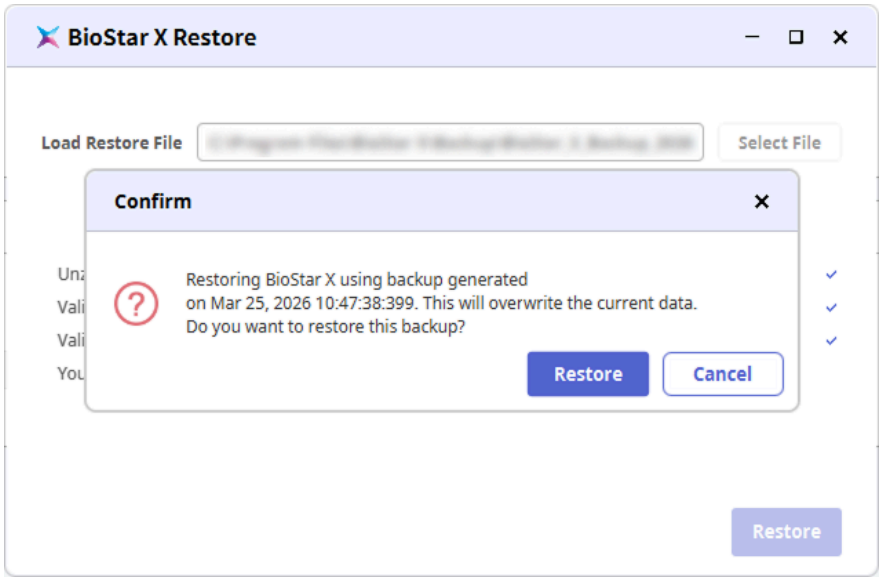
2. **Select File** をクリックし、復元するバックアップファイルを選択する。



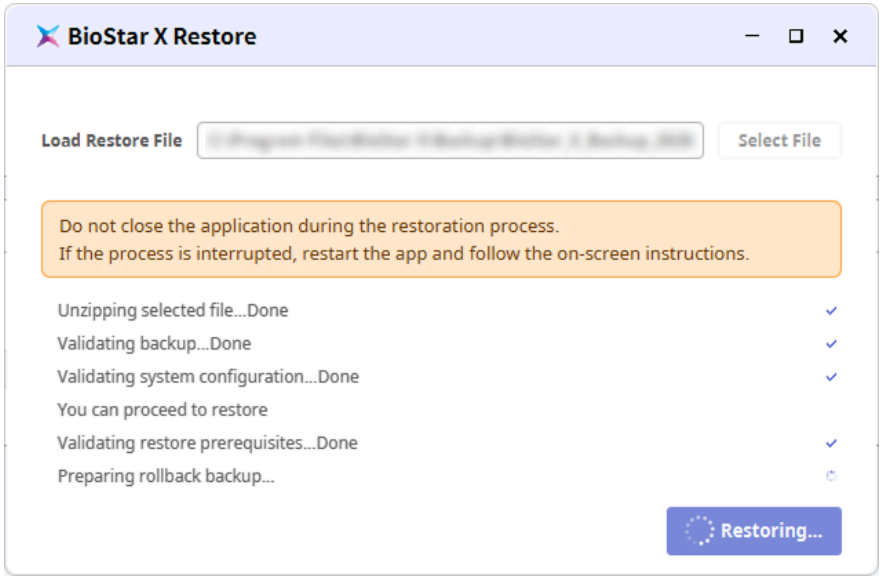
3. 復元を開始するには **Restore** をクリックする。
4. バックアップファイルの有効性を検証します。
5. 「**You can proceed to restore**」メッセージが表示されたら、データベースのパスワードを入力し、**Restore** ボタンをクリックしてください。



6. 確認メッセージが表示されたら、復元を続行するには **Restore** ボタンをクリックしてください。

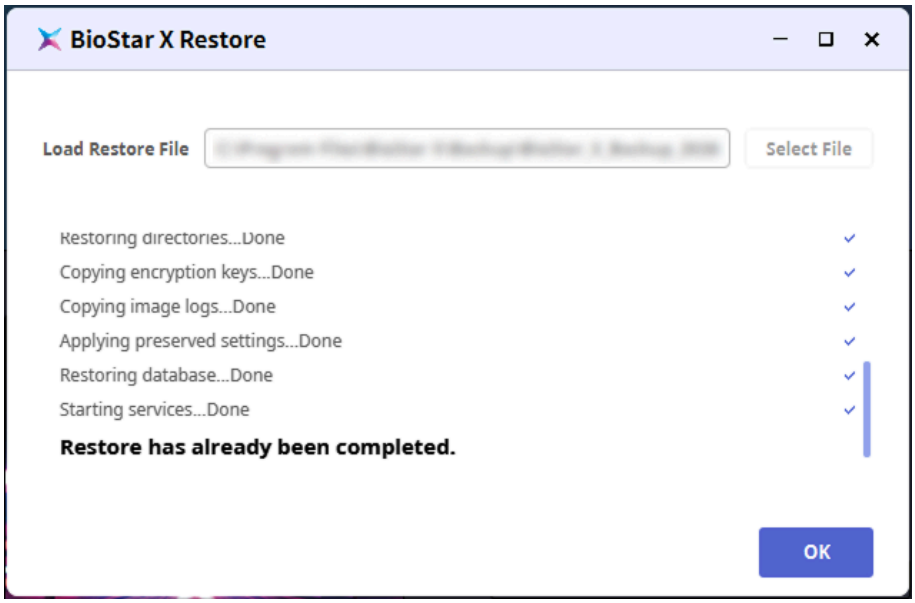


7. 復元の進行状況を確認できるメッセージが表示されます。復元処理が完了するまでお待ちください。



「**Restore has already been completed**」メッセージが表示されたら、復元は完了しています。 **BioStar X** に接続し、復元され

たデータを確認する。



情報

- 復元中にPCが異常終了した場合は、**BioStar X Restore** を再実行して復元を再試行してください。
- 復元対象サーバーの IP アドレスがバックアップサーバーと異なり、かつマルチコミュニケーションサーバーが接続されている場合は、証明書を再発行する必要があります。マルチコミュニケーションサーバーで証明書を再発行する方法については、メインサーバーのIPアドレスを変更するを参照してください。

システムセキュリティを強化する

組織のセキュリティポリシーに合わせて **BioStar X** のセキュリティ設定を構成します。パスワードポリシー、個人情報の暗号化、デバイス間通信のセキュリティ、同時接続制御などを選択的に設定できます。

情報

システムセキュリティを強化する前に、組織のセキュリティポリシーおよび規程を確認してください。

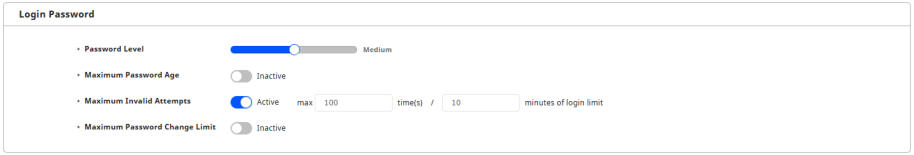
システムセキュリティを使用する

1. **Launcher**ページで**Settings**をクリックします。
2. 画面左のサイドバーで **System** → **Security** をクリックします。
3. セキュリティに関する各項目を設定します。
   - **Login Password**：ログインパスワードに関するセキュリティレベルを設定します。詳細については、パスワードポリシーの設定ご参照ください。
   - **Advanced Security Settings**：個人情報とデバイス間通信のセキュリティを強化できます。詳細については、高度なセキュリティ設定ご参照ください。
   - **Session Security**：セッションセキュリティを強化できます。詳細については、同時接続制御ご参照ください。
4. 設定を保存するには、画面右下の **Apply** をクリックします。

> **情報**
> **Advanced Security Settings** メニューは、ID が 1 の初期管理者アカウントのみ使用できます。

パスワードポリシーの設定

Login Password セクションでは、ログインパスワードに関するセキュリティレベルを設定します。組織のセキュリティ要件に合わせてパスワードポリシーを設定します。



パスワードの複雑性の設定

ユーザーパスワードの複雑性を設定できます。 **Password Level** オプションのスライダーを調整してセキュリティレベルを設定します。

- **Low**：最大 32 文字まで入力できます。
- **Medium**：パスワードを設定する際は、8〜32 文字の英字（大文字または小文字）と数字を組み合わせる必要があります。
- **Strong**：パスワードを設定する際は、10〜32 文字の英字（大文字と小文字、少なくとも 1 文字の大文字を含む）と数字、記号を組み合わせる必要があります。

パスワード変更周期の設定

パスワードの使用期間を制限するには、**Maximum Password Age** オプションでトグルボタンをクリックして **Active** 状態に切り替えます。ユーザーは設定した期間ごとにパスワードを変更する必要があります。パスワード変更周期を超えると、ログイン時にパスワード変更要求メッセージが表示されます。

> **情報**
> 1 日から 180 日まで設定できます。

ログイン失敗制限の設定

パスワード入力失敗の許容回数とログイン制限時間を設定できます。 **Maximum Invalid Attempts** オプションで設定した回数を超えてパスワードを誤入力すると、制限時間中はログインできません。

> **情報**
> このオプションはデフォルトで有効になっており、100 回失敗すると 10 分間ログインが制限されます。必要に応じて値を調整するか、無効化できます。

パスワード変更回数制限の設定

ユーザーが 1 日にパスワードを変更できる回数を制限するには、**Maximum Password Change Limit** オプションでトグルボタンをクリックして **Active** 状態に切り替えます。ユーザーは設定した回数だけパスワードを変更できます。

> **情報**
> 最大 10 回まで設定できます。

高度なセキュリティ設定

Advanced Security Settings セクションでは、個人情報とデバイス間通信のセキュリティを強化できます。



> **情報**
> **Advanced Security Settings** セクションは、初回の管理者アカウントでログインした場合にのみ有効になります。

個人情報保護の強化

機微な個人情報を暗号化してデータ漏えいのリスクを最小化するには、以下のオプションを設定してください。

- **Encrypt Personal Data on Database**
  - **Use**：クレデンシャルデータを含むユーザーの個人情報を暗号化して保存します。
  - **Not Use**：ユーザーの個人情報を暗号化せずに保存します。既に暗号化されているデータは復号して保存し、新しいデータは暗号化しません。
- **Personal Data Encryption Key**：データベースに保存された情報を暗号化または復号してユーザーの個人情報を安全に保護するために使用します。「**Change**」ボタンをクリックして、新しい暗号化キー値を設定してください。暗号化キーを変更すると、既に暗号化されているデータを再暗号化します。

情報

- 個人情報 DB の暗号化または復号処理の実行中にサーバーを強制的に起動しないでください。ログイン失敗やデータ破損などのエラーが発生する可能性があります。データベースのサイズとサーバーの性能によっては時間がかかる場合があります。

  ▼ 個人情報暗号化項目を表示

  - プロフィール画像
  - ユーザーID
  - 名前
  - 電話番号
  - ユーザーIP
  - 送信者および受信者のメール情報
  - ログインID
  - ログインパスワード
  - 顔テンプレート
  - 指紋テンプレート
  - カードID
  - スマートカードレイアウトキー
  - ユーザーおよび訪問者に関するカスタム情報
  - イメージログファイル

- **Personal Data Encryption Key** は英数字と記号を使用して 32 文字で入力できます。
- 1.0.3バージョンにアップグレードした後、新しく作成される監査ログは、**Encrypt Personal Data on Database** オプションの設定に関係なく、暗号化して保存します。

デバイス間通信のセキュリティ設定

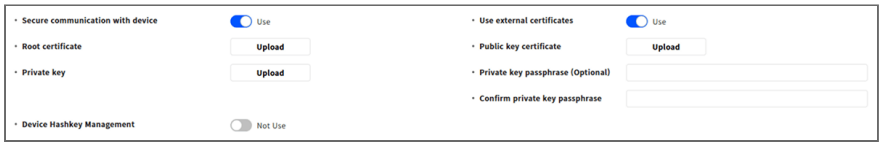
BioStar X サーバーとアクセス制御デバイス間の通信を証明書で保護して、セキュリティを強化してください。新規にインストールした **BioStar X** システムでは、**Secure communication with device** オプションはデフォルトで **Use** に設定されており、追加の有効化操作は不要です。既存システムをアップグレードすると、以前の設定を維持し、既存のセキュリティ証明書もそのまま再利用して、登録済みのデバイスを追加操作なしで再接続します。

- **Secure communication with device**：**BioStar X** サーバーとアクセス制御デバイス間の通信を証明書で保護します。このオプションが **Use** の場合、サーバーが自動で証明書を生成してデバイスに送信し、その後すべての通信が暗号化されます。デバイスはこの証明書を使用して、**BioStar X** サーバーとデータを送受信するときにセキュアチャネルを使用します。

  外部証明書を使用するには、**Use external certificates** オプションを **Use** に設定し、以下の項目を登録してください。

  - **Root certificate**、**Public key certificate**、**Private key** ファイルをそれぞれアップロードしてください。
  - 秘密鍵にパスフレーズが設定されている場合は、**Private key passphrase (Optional)** と **Confirm private key passphrase** に同じ値を入力してください。(オプション)

外部証明書ではなく、サーバーを削除する際にバックアップしたセキュリティ証明書を復元するには、**BioStar X** のインストールパスに直接コピーしてください。セキュリティ証明書のバックアップと復元方法については BioStar Xサーバーのアンインストールとセキュリティ証明書の復元をご参照ください。



- **Device Hashkey Management**：デバイスに適用するハッシュキーは管理者が直接管理します。このオプションを **Use** に設定すると、**Device Hashkey** の値を確認し、変更できます。「**Change**」ボタンをクリックし、新しいハッシュキーの値を設定してください。

注意

Device Hashkey Management オプションを有効化する前に、以下を必ず確認してください。

- 有効化すると、セキュリティ強化のため、デバイスはタンパー（Tamper）イベント発生時にユーザー、ログ、暗号化キーの値を削除します。注意してください。
- Administrator Role アカウント以外のユーザーにログインパスワードまたはPINが設定されている場合、ハッシュキー値を適用できません。ログインパスワードまたはPINを削除してから、再試行してください。パスワードとPINは、セキュリティ要件を満たすために復号できない方式で暗号化されるためです。
- デバイスのハッシュキーを変更すると、デバイスに設定されたマスター管理者PIN情報が削除されます。クレデンシャルを削除するとデバイスマネージャーメニューにアクセスできなくなる場合があるため、十分に注意してください。
- **Encrypt Personal Data on Database**と**Device Hashkey Management**は同時に使用できません。二つのオプションのいずれかを［使用しない］に切り替えてから、残りのオプションを設定してください。

情報

- **BioStar X** は、**Secure communication with device** オプションを **Not Use** に変更しても、サーバーが生成した既定の証明書を削除しません。オプションを再び **Use** に変更すると、既存の証明書をそのまま再利用し、証明書がない場合のみ新規に生成します。そのため、**Use** → **Not Use** → **Use** の順に変更しても同じ証明書が維持され、以前に登録したデバイスを追加の操作なしで再接続できます。ただし、外部証明書を使用中に **Not Use** に変更すると、サーバーが登録済みの外部証明書（ルート証明書、公開鍵証明書、秘密鍵）と秘密鍵パスワードを削除します。
- システムは、登録済みのすべてのデバイスとマルチコミュニケーションサーバーがサーバーに接続されている場合にのみ、**Secure communication with device** オプションと **Use external certificates** オプションの変更を許可します。接続が切れたデバイスがある、またはマルチコミュニケーションサーバーが接続されていない場合、システムは変更を拒否し、エラーメッセージを表示します。デバイスまたはマルチコミュニケーションサーバーを再接続してから再試行してください。使用しなくなったデバイスはデバイスリストから削除し、再試行してください。
- 以前は正常に接続されていたデバイスが証明書の不一致で接続に失敗すると、**BioStar X**はこれをシステムログに記録します。デバイスが突然接続できなくなった場合は、システムログで原因を確認した後、デバイスを工場出荷時設定に初期化するか、以前にエクスポートした証明書セットを**Use external certificates**オプションで再登録して復旧してください。ただし、サーバーを削除してから再インストールした場合は、BioStar Xサーバーのアンインストールとセキュリティ証明書の復元をご参照ください。
- サーバーを削除する際に証明書をバックアップする方法は、BioStar Xサーバーのアンインストールとセキュリティ証明書の復元をご参照ください。

▼ **Secure communication with device 機能対応デバイスとファームウェアバージョンを表示**

- BioStation 3 Maxのファームウェアバージョン1.0.0以降
- XPass Q2のファームウェアバージョン1.0.0以降
- BioStation 3 ファームウェア 1.0.0 以上
- BioStation 2a ファームウェア 1.0.0 以上
- X-Station 2 ファームウェア 1.0.0 以上
- XPass 2 ファームウェア 1.0.0 以上
- FaceLite ファームウェア 1.0.0 以上
- BioLite N2 ファームウェア 1.0.0 以上
- BioEntry P2 ファームウェア 1.1.0 以降
- FaceStation 2 ファームウェア 1.1.0 以降
- BioEntry W2 ファームウェア 1.2.0 以降
- BioStation L2 ファームウェア 1.3.0 以降
- BioStation A2 ファームウェア 1.5.0 以降
- BioStation 2 ファームウェア 1.6.0 以降
- CoreStation ファームウェア 1.1.0 以降

同時接続制御

Session Security セクションでは、セキュリティを強化するために同一アカウントの重複ログインを制限できます。**Simultaneous Connection Allow** オプションを **Inactive** に設定してください。同一アカウントで同時接続が試行されると、既に接続しているユーザーはログアウトされます。



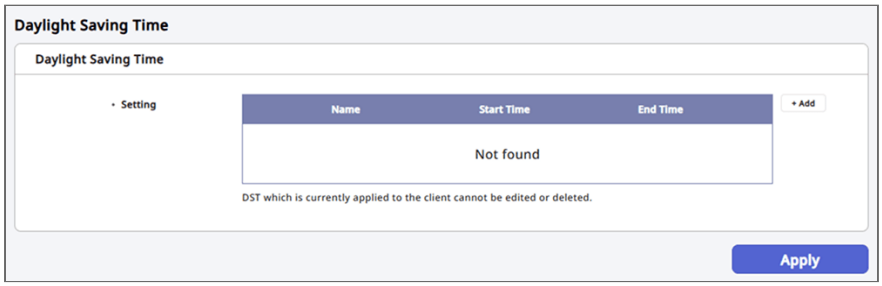
サマータイムを設定する

サマータイム（Daylight Saving Time、DST）を設定すると、現地の法定時間に合わせてシステム時刻を自動調整できます。これにより、入退室記録の正確性を保証し、他のシステムとの時刻同期の問題を防止できます。

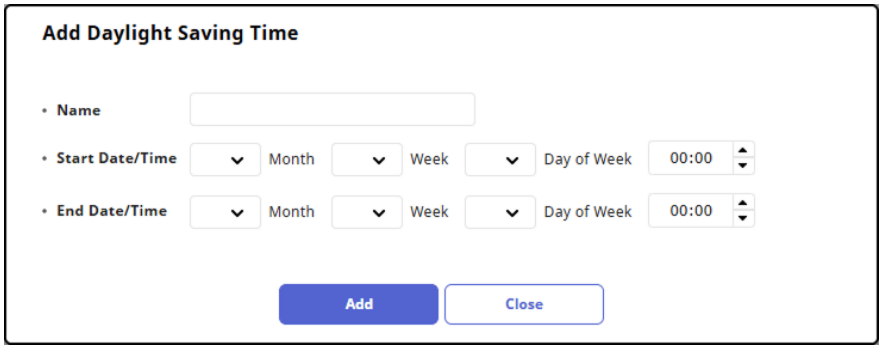
> **情報**
> 次のような場合にサマータイムを設定してください。
> - サマータイムを採用している国や地域でシステムを運用する場合
> - 勤怠管理システムと連携し、正確な入退室時刻を記録する必要がある場合
> - 複数のタイムゾーンにわたって運用される統合セキュリティシステムを管理する場合

サマータイムを追加

1. **Launcher**ページで**Settings**をクリックします。
2. 画面左のサイドバーで **System** → **Daylight Saving Time** をクリックします。
3. **+ Add** ボタンをクリックします。



4. 各項目を設定し、**Add** ボタンをクリックします。



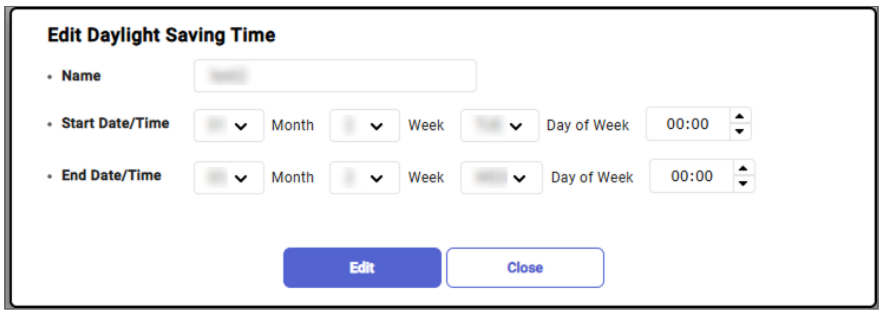
5. 追加した設定を保存するには、画面右下の **Apply** ボタンをクリックします。

> **情報**
> - 使用中のサマータイム設定は編集または削除できません。使用中のサマータイム設定は **Settings** → **System** → **Preferences** メニューで確認できます。
> - 追加した夏時間の設定をシステムに適用する方法の詳細については、基本設定を構成するをご参照ください。

サマータイムを編集

> **情報**
> 現在使用中の設定は編集できません。編集するには、まず **Settings** → **System** → **Preferences** メニューの **Language / Time Zone** セクションで選択を解除してください。

1. **Launcher**ページで**Settings**をクリックします。
2. 画面左のサイドバーで **System** → **Daylight Saving Time** をクリックします。
3. サマータイム一覧で編集する項目の ボタンをクリックします。
4. **Edit Daylight Saving Time** ウィンドウが表示されたら、必要な項目を編集します。



5. 編集が完了したら、**Edit** ボタンをクリックします。
6. 編集した設定を保存するには、画面右下の **Apply** ボタンをクリックします。

> **情報**
> 夏時間の設定をシステムに適用する方法の詳細については、基本設定を構成するをご参照ください。

サマータイムを削除

使用していないサマータイム設定を削除します。

1. **Launcher**ページで**Settings**をクリックします。
2. 画面左のサイドバーで **System** → **Daylight Saving Time** をクリックします。
3. サマータイム一覧で削除する項目の ボタンをクリックします。
4. 確認メッセージが表示されたら、**Yes** ボタンをクリックします。
5. 削除した設定を保存するには、画面右下の **Apply** ボタンをクリックします。

メールを設定する

ユーザーに顔登録用モバイルリンクを送信したりQR/バーコードを発行するメールの件名、会社名、会社ロゴ、連絡先などの情報を設定できます。

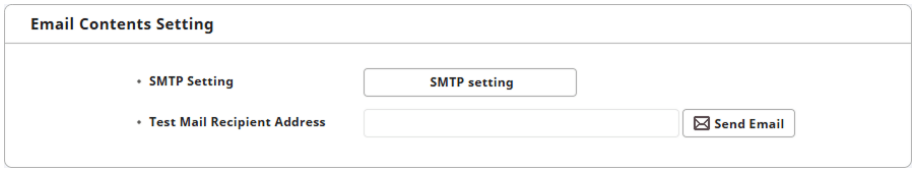
情報

- ユーザーに顔登録用モバイルリンクを送信したりQR/バーコードを発行するには、ユーザー情報にメールアドレスが登録されている必要があります。ユーザー情報の詳細については、ユーザー基本情報を入力をご参照ください。
- **顔認証**を利用できるデバイスは以下のとおりです。
  - FaceStation F2、BioStation 3、BioEntry W3、BioStation 3 Max
- **スキャナーでQR/バーコード認証**を利用できるデバイスは以下のとおりです。
  - X-Station 2 (XS2-QDPB, XS2-QAPB)
- **カメラでQR/バーコード認証**を利用できるデバイスは以下のとおりです。
  - BioStation 3 Maxのファームウェアバージョン1.0.0以降
  - BioStation 3 ファームウェア バージョン 1.1.0以降
  - X-Station 2 (XS2-ODPB, XS2-OAPB, XS2-DPB, XS2-APB) ファームウェア 1.2.0 以上
  - X-Station 2 (XS2-QDPB, XS2-QAPB) ファームウェア 1.4.1 以上
- **カメラでQR/バーコード認証**を利用するには、別途デバイスライセンスが必要です。デバイスライセンスの詳細については、デバイスライセンスをご参照ください。

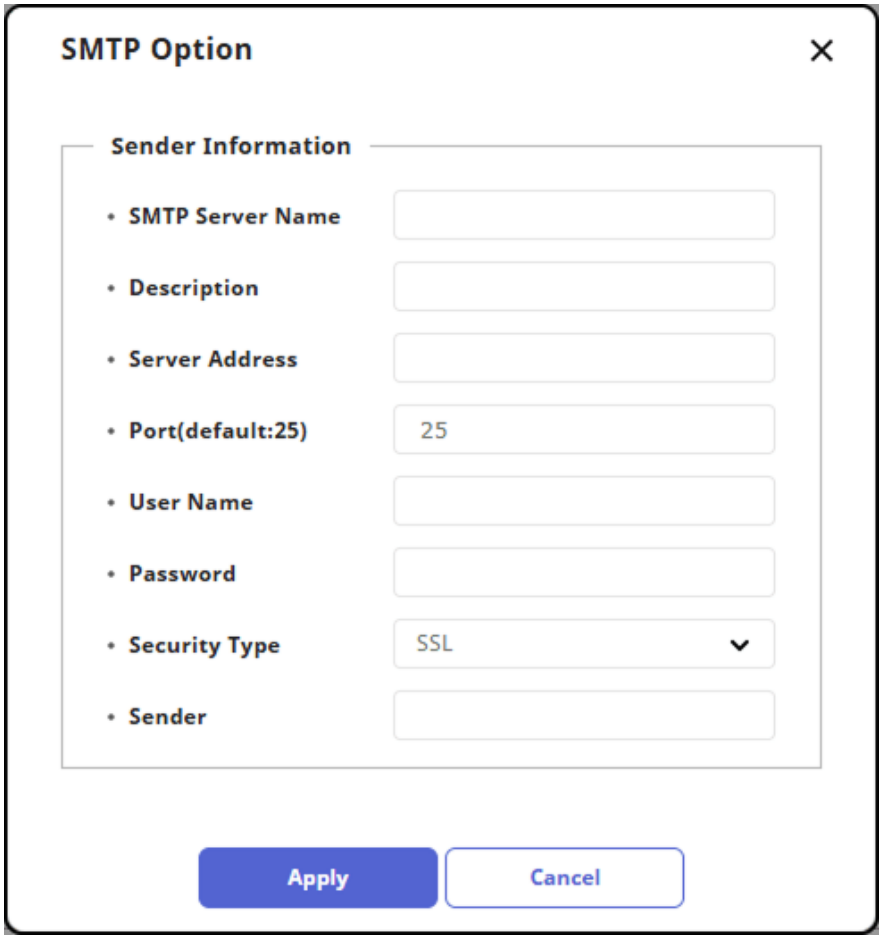
1. **Launcher**ページで**Settings**をクリックします。
2. 画面左側のサイドバーで **System** → **Email Settings** をクリックしてください。
3. 各項目を設定してください。
4. **Apply** をクリックして設定を保存します。

メールコンテンツを設定する

メール送信用のSMTPサーバー情報を入力してください。



- **SMTP Setting**：メール送信のためにシンプルメールトランスファープロトコル（SMTP）を設定してください。**SMTP setting**ボタンをクリックすると、**SMTP Setting**設定ウィンドウが表示されます。



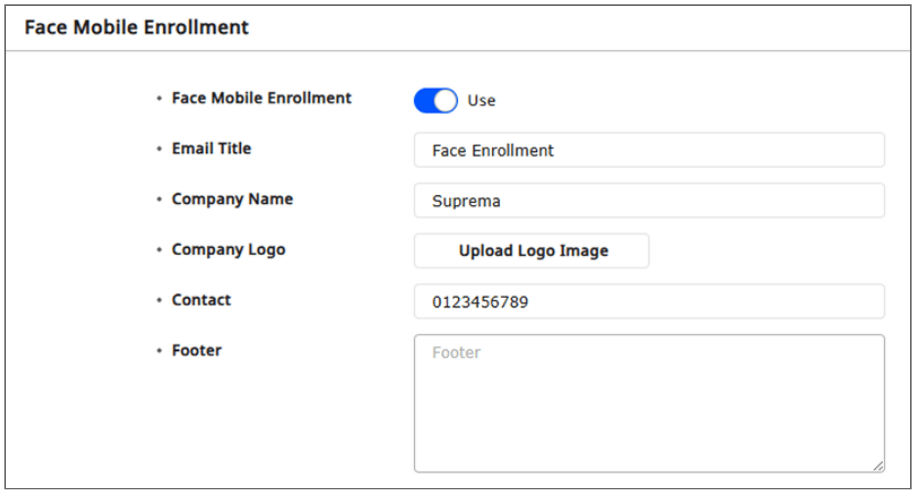
- **SMTP Server Name**：SMTP サーバー名を入力します。
- **Description**：SMTP の説明を入力します。
- **Server Address**：SMTP サーバーアドレスを入力します。 SMTP サーバーアドレスは `smtp.{email-service-provider}.com` のような形式で、SMTP サーバーとして使用するメールの設定画面で確認できます。
- **Port(default:25)**：SMTP サーバーのポート番号を入力します。 SMTP サービスプロバイダーのメール設定画面で確認できます。
- **User Name**：SMTP サービスのアカウントを入力します。
- **Password**：SMTP サービスのアカウントパスワードを入力します。
- **Security Type**：セキュリティタイプを選択します。
- **Sender**：送信元のメールアドレスを入力します。

> **情報**
>
> - SMTP の詳細についてはシステム管理者にお問い合わせください。
> - SMTP サーバーを 2 段階認証が設定されたメールアカウントで使用する場合、そのアカウントのパスワードを変更するときは次の点に注意してください。
>   - 2 段階認証を設定すると、SMTP パスワードにはそのメールアカウントのパスワードではなく、2 段階認証で生成されたアプリパスワードが使用されます。
>   - このとき、そのメールアカウントのパスワードが変更されるとアプリパスワードは自動的に削除され、SMTP パスワードは使用できなくなります。
>   - そのメールアカウントのパスワードを変更した場合は、アプリパスワードを再生成してから SMTP パスワードを再設定します。

- **Test Mail Recipient Address**：SMTP設定に問題がないか確認するには、受信するメールアドレスを入力してから**Send Email**ボタンをクリックしてください。

顔登録モバイルリンクを設定する

メールでユーザーに顔登録モバイルリンクを送信するには、**Use**に設定してください。



- **Email Title**：顔登録モバイルリンクを送信するメールの件名を入力してください。
- **Company Name**：会社名を入力してください。
- **Company Logo**：会社のロゴ画像をアップロードしてください。

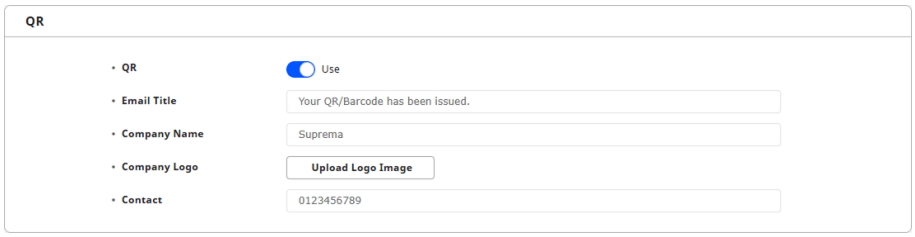
> **情報**
>
> - サポートされている画像ファイル形式はGIF、JPG、JPEG、JPE、JFIF、PNGです。
> - サポートされている画像ファイルのサイズは最大5MBです。

- **Contact**：担当者の連絡先を入力してください。
- **Footer**：法的通知文など、顔登録を行うユーザーに通知する内容を入力してください。顔登録モバイルリンク送信メールの下部に表示されます。

> **情報**
> フッターには最大5,000文字まで入力できます。

QR/バーコード発行を設定する

メールでユーザーにQR/バーコードを発行するには、**Use**に設定してください。



- **Email Title**：QR/バーコードを送信するメールの件名を入力してください。
- **Company Name**：会社名を入力してください。
- **Company Logo**：会社のロゴ画像をアップロードしてください。

> **情報**
> - サポートされている画像ファイル形式はGIF、JPG、JPEG、JPE、JFIF、PNGです。
> - サポートされている画像ファイルのサイズは最大5MBです。

- **Contact**：担当者の連絡先を入力してください。

基本設定を構成する

BioStar X を効率的に使用するためには、使用環境に合った基本設定が必要です。以下のような状況で必要な設定方法を案内します。

- 新規インストールした **BioStar X** の初期設定
- ユーザーが好む言語への変更
- 現地タイムゾーンに合わせた時刻設定
- イベント通知音のカスタマイズ

基本設定にアクセス

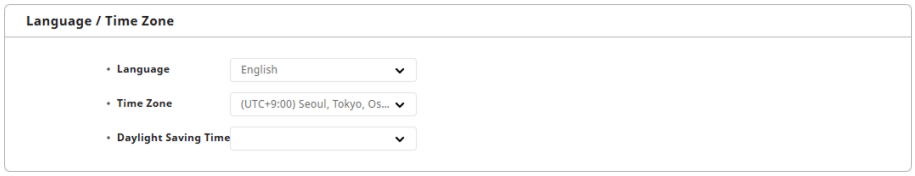
1. **Launcher**ページで**Settings**をクリックします。
2. 画面左側のサイドバーで **System** → **Preferences** をクリックしてください。
3. 各セクションで必要なオプションを設定します。
   - **Language / Time Zone**：インターフェース言語とタイムゾーン、サマータイム
   - **Date/Time**：日付と時刻の形式

- **Sound**：イベント通知音

4. すべての設定を完了したら、画面右下の **Apply** ボタンをクリックします。

言語とタイムゾーンの設定

BioStar X のインターフェース言語、タイムゾーン、サマータイム規則を設定できます。



- **Language**：使用するインターフェース言語を選択します。
- **Time Zone**：現在の場所に合わせたタイムゾーンを選択します。
- **Daylight Saving Time**：BioStar X サーバーに適用するサマータイム規則を選択します。必要な項目がない場合は、サマータイムを設定するを参照して追加してください。

設定を保存するには、画面右下の **Apply** ボタンをクリックしてください。

日付と時刻の表示形式の設定

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。



- **Date Format**：日付形式を変更できます。
  - **mm/dd/yyyy**：01/31/2025
  - **yyyy/mm/dd**：2025/01/31
  - **dd/mm/yyyy**：31/01/2025
- **Time Format**：時間形式を変更できます。
  - **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

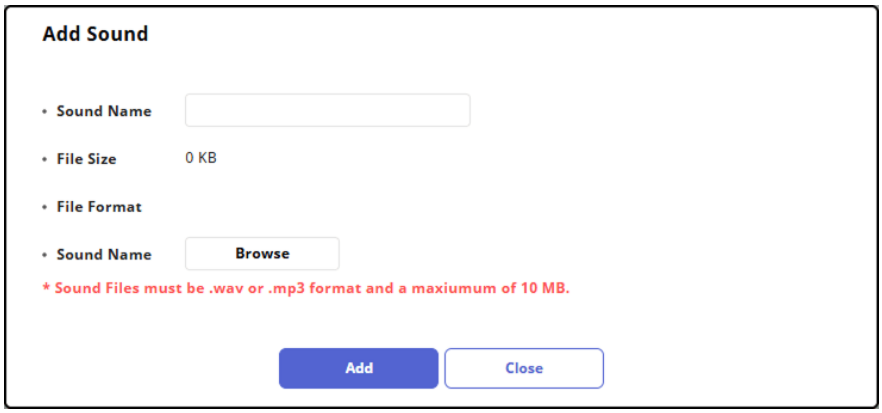
設定を保存するには、画面右下の **Apply** ボタンをクリックしてください。

イベント通知音の設定

イベント発生時に使用するサウンドファイルをアップロードできます。



1. **+ Add** をクリックします。
2. **Add Sound** ウィンドウが表示されたら、**Browse** をクリックします。



3. アップロードする *.wav* または *.mp3* ファイルを選択し、**開く** をクリックします。
4. サウンドファイルをアップロードするには、**Add** ボタンをクリックします。

設定を保存するには、画面右下の **Apply** ボタンをクリックしてください。

情報

- サウンドファイルは *.wav* または *.mp3* 形式のみアップロードできます。
- アップロードできる最大ファイルサイズは10MBです。
- イベント発生時にアップロードしたサウンドファイルを適用する方法は、アラームを設定するをご参照ください。

高度な設定

エッセンシャル（Essential）ライセンスで追加オプションを購入するか、**エンタープライズ**（Enterprise）ライセンス以上で利用できる高度な設定機能を案内します。

エレベーター管理

エレベーターのグループ登録および管理方法を案内します。エレベーターに関する入退室制御設定によって特定フロアへのアクセス権限を制御できます。これにより、セキュリティと利便性を強化できます。

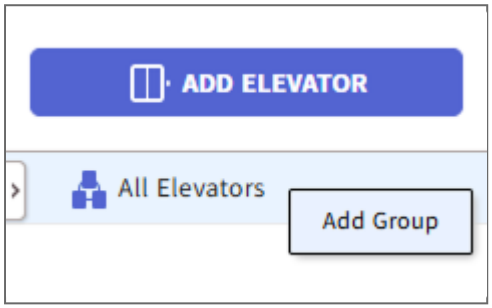
エレベーターグループを管理する

複数のエレベーターを簡単に管理できるように、グループ設定方法を説明します。エレベーターグループは、複数のエレベーターを 1 つのグループにまとめて管理できる機能です。グループを設定すると、エレベーターを一括設定できます。

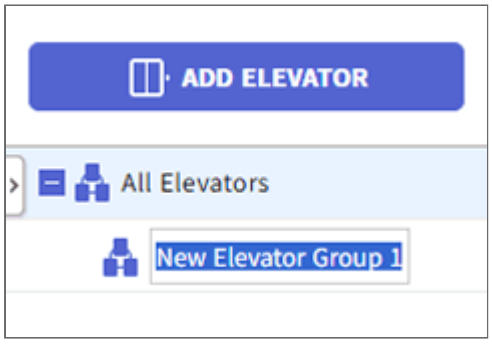
> **ヒント**
> エレベーターの設置場所をグループ名として登録すると、管理が便利です。

エレベーターグループを追加する

1. **Launcher**ページで**Settings**をクリックします。
2. 画面左のサイドバーで **Access Point** → **Elevator** をクリックします。
3. エレベーターリストで **All Elevators** を選択し、右クリックします。



4. ポップアップメニューで **Add Group** をクリックします。
5. 希望するグループ名を入力します。

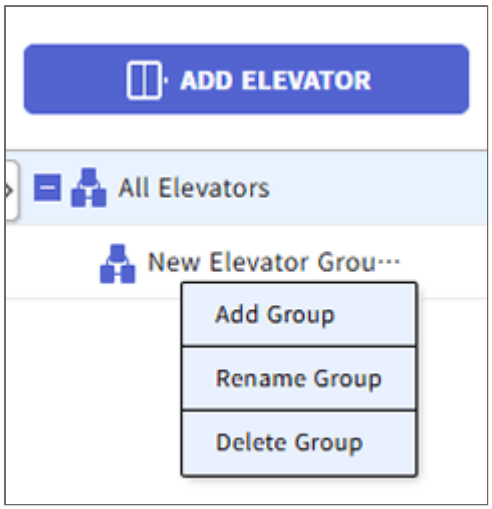


情報

- エレベーターグループは最大 8 段階まで作成できます。
- エレベーターグループ名は最大 48 文字まで入力できます。

エレベーターグループ名を変更する

1. **Launcher**ページで**Settings**をクリックします。
2. 画面左のサイドバーで **Access Point** → **Elevator** をクリックします。
3. エレベーターリストで名前を変更するグループを選択し、右クリックします。



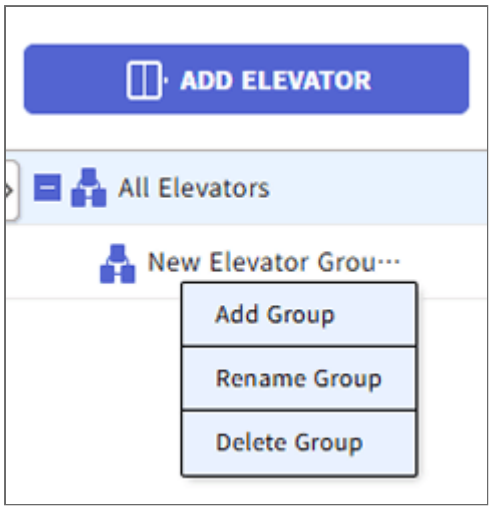
4. ポップアップメニューで **Rename Group** をクリックします。
5. 変更するグループ名を入力します。

情報
エレベーターグループ名は最大 48 文字まで入力できます。

エレベーターグループを削除する

1. **Launcher**ページで**Settings**をクリックします。
2. 画面左のサイドバーで **Access Point** → **Elevator** をクリックします。

3. エレベーターリストで削除するグループを選択し、右クリックします。



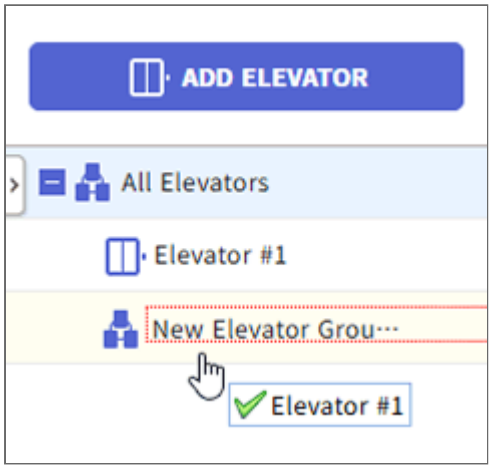
4. ポップアップメニューで **Delete Group** をクリックします。

> **注意**
> エレベーターグループを削除すると、そのグループに含まれるすべてのエレベーターも削除されます。グループに含まれるエレベーターを削除したくない場合は、先にエレベーターを別のグループへ移動してから、グループを削除してください。

グループにエレベーターを追加する

エレベーターリストからグループに追加する

1. **Launcher**ページで**Settings**をクリックします。
2. 画面左のサイドバーで **Access Point** → **Elevator** をクリックします。
3. エレベーターリストでグループに追加するエレベーターを選択し、目的のグループへドラッグします。



選択したエレベーターがグループへ移動します。

エレベーター情報からグループに追加する

1. **Launcher**ページで**Settings**をクリックします。

2. 画面左のサイドバーで **Access Point** → **Elevator** をクリックします。
3. 画面右側のエレベーターリストで、グループに追加するエレベーターをクリックします。
4. エレベーター情報の編集画面が表示されたら、**Information** セクションの **Group** オプションをクリックします。



5. 目的のグループを選択します。
6. 画面最下部にある **Apply** をクリックします。

エレベーターを登録する

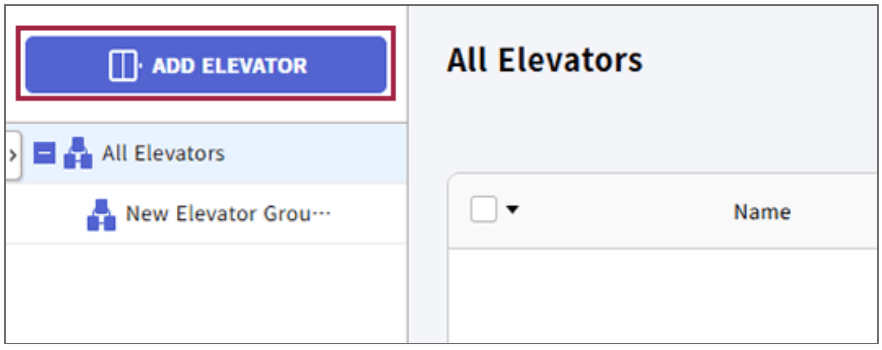
エレベーターを登録して設定する方法を案内します。エレベーターは階制御に使用され、ドアとともに入退室制御システムを構成します。エレベーターを登録すると、特定の階への入室権限を制御できます。

開始前に

- エレベーターを登録する前に、アクセス制御用のアクセスレベル、アクセスグループ、階レベルを設定してください。詳しくは 入退室制御設定 をご参照ください。
- エレベーターを登録する前に、デバイスを登録してください。デバイス登録の詳細は、以下のドキュメントを参照してください。
  - デバイスを登録する
  - Wiegandデバイスを登録する
  - スレーブ装置を登録する

エレベーターの登録

1. **Launcher**ページで**Settings**をクリックします。
2. 画面左のサイドバーで **Access Point** → **Elevator** をクリックします。
3. 画面左上の **ADD ELEVATOR** ボタンをクリックします。



4. **Add New Elevator** 画面が表示されたら、各セクション項目を順に設定してください。
   - **Information**：エレベーターの基本情報を設定してください。詳しくは 基本情報の設定 をご参照ください。
   - **Detail**：エレベーターの詳細情報を設定してください。詳細については、詳細情報の設定ご参照ください。

- **Option**：追加オプションを設定してください。詳しくは 追加オプションの設定 をご参照ください。
- **Alarm**：アンチパスバック違反が発生した際に警報を鳴らしたりデバイスを使用不可にする設定ができます。詳しくは アラーム設定 をご参照ください。

5. すべての設定が完了したら、画面最下部の **Apply** ボタンをクリックします。

基本情報の設定

Information セクションでは、エレベーターの名前・グループ・説明を入力または変更できます。

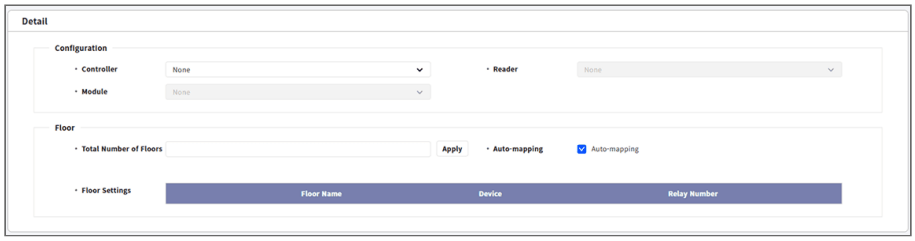


- **Name**：エレベーターの名前を入力してください。エレベーターの位置を特定できる名前を入力すると、より便利に管理できます。
- **Group**：エレベーターグループを選択してください。
- **Description**：エレベーターに関する簡単な説明を入力してください。

> **情報**
>
> - エレベーター名は最大48文字まで入力できます。
> - エレベーターグループの登録に関する詳細は、エレベーターグループを管理するをご参照ください。

詳細情報の設定

Detail セクションでは、エレベーターの詳細情報を設定できます。エレベーターに接続するデバイスと階情報を設定してください。



- **Controller**：エレベーターのアクセス権限を制御するデバイスを選択してください。
- **Reader**：認証に使用するデバイスを選択してください。
- **Module**：エレベーターボタンリレーを制御するデバイスを選択してください。
- **Total Number of Floors**：エレベーターで移動可能な総階数を入力してください。最大192階まで入力できます。
- **Auto-mapping**：自動マッピングの使用有無を選択してください。自動マッピングを使用すると、リレー番号が順番に割り当てられます。
- **Floor Settings**：階名と階を制御するリレー番号を設定してください。

情報

- **Controller** オプションでは、マスターデバイスのみ選択できます。
- **Reader** オプションでは、マスター、スレーブ、Wiegand デバイスのみ選択でき、最大4台まで選択できます。

  OM-120モデルはリーダーとして設定できません。
- **Module** オプションでは、OM-120、DM-20、IM-120、SIO2モデルのみ選択できます。

追加オプションの設定

Option セクションでは、エレベーターの追加オプションを設定できます。



- **Relay Control**：階ボタンリレーに関するオプションを設定してください。
  - **Open Time**：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てください。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。
- **Dual Authentication**：2人（一般ユーザーと管理者）がクレデンシャルを認証して階ボタンを有効にするよう設定できます。
  - **Device**：二重認証を使用するデバイスを選択してください。二重認証を使用しない場合は**None**を選択してください。
  - **Schedule**：二重認証を適用するスケジュールを選択してください。目的のスケジュールがない場合は、**+ Add Schedule** をクリックして追加します。
  - **Approval Type**：管理者認証の順序を設定してください。
  - **None**：認証グループに関係なく、2人の認証が必要です。
  - **Last**：一般ユーザーが認証し、設定した認証グループに属するユーザーが認証する必要があります。
  - **Approval Group**：管理者が所属するグループを設定します。このオプションは、**Approval Type** を **Last** に選択した場合に使用できます。
  - **Timeout**：1回目の認証後から2回目の認証までの待機時間を設定します。設定した時間内に2回目の認証が完了しない場合、階ボタンは有効になりません。

  情報

  - 在室人数制限設定に構成されているデバイスのデュアル認証を変更するには、次のメニューで設定を編集します。 **Settings** → **Access Management** → **Advanced AC** → **Occupancy Limit**

  Occupancy Limit の設定について詳しくは 高度な入退室制御設定 をご参照ください。

  - スケジュール設定の詳細については、スケジュールを設定するをご参照ください。
- **Tamper**：タンパー信号を出力するポートを設定します。

アラーム設定

Alarm セクションでは、タンパー入力を検知した場合や別途の入力信号を検知した場合に実行する動作を設定できます。作業条件と動作を追加するには、**+ Add** ボタンをクリックします。



- **Trigger**：タンパー入力の検知または別途の入力信号の検知を設定します。
- **Action**：設定した動作条件に応じて実行する動作を設定します。エレベーターの全階ボタンを有効化するか、特定の信号を出力できます。

エレベーター情報を編集する

登録済みエレベーターの設定情報を編集する方法を案内します。個別エレベーターの詳細設定を変更するか、複数のエレベーターを選択して共通項目を一括編集します。

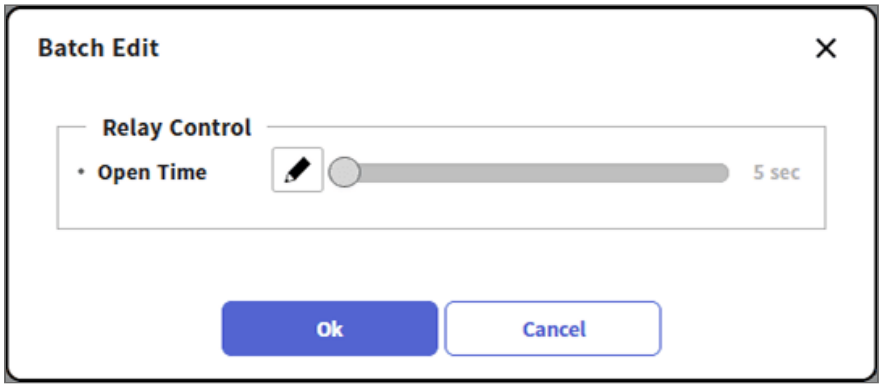
一台のエレベーター情報を修正する

1. **Launcher**ページで**Settings**をクリックします。
2. 画面左のサイドバーで **Access Point** → **Elevator** をクリックします。
3. エレベーター一覧で編集対象のエレベーターをクリックします。
4. 各セクションの詳細項目を編集します。
5. すべての設定が完了したら、画面最下部の **Apply** ボタンをクリックします。

> **情報**
> エレベーター情報の編集画面にある各セクションの詳細については、エレベーターを登録する をご参照ください。

複数のエレベーター情報を一括編集する

1. **Launcher**ページで**Settings**をクリックします。
2. 画面左のサイドバーで **Access Point** → **Elevator** をクリックします。
3. エレベーター一覧で編集対象のエレベーターのチェックボックスをクリックします。 2台以上のエレベーターを選択します。
4. 画面右上にある**Batch Edit**をクリックします。
5. **Batch Edit**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。



6. 設定が完了したらApplyをクリックします。

> **情報**
>
> - Batch Edit ボタンは、エレベーター一覧で2台以上のエレベーターを選択すると有効になります。
> - 一括編集では Open Time オプションのみ変更できます。

エレベーターを削除する

登録済みのエレベーターを削除する方法を説明します。

1. Launcherページで Settingsをクリックします。
2. 画面左のサイドバーで Access Point → Elevator をクリックします。
3. エレベーター一覧で、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。
4. 画面右上の Delete Elevator ボタンをクリックします。

選択したエレベーーターが削除されます。削除したエレベーターは復元できません。

> **情報**
>
> Delete Elevator ボタンは、エレベーター一覧で一台以上のエレベーターを選択すると有効になります。

高度な入退室制御設定

高度な入退室制御設定で入退室を制御します。セキュリティ要件と運用環境に応じて、さまざまな高度な入退室制御機能を設定します。アンチパスバックで不正な再入室を防止し、火災や侵入などの緊急事態に対応し、スケジュールに基づいてドアを自動制御し、特定エリアの人数を制限してモニタリングします。

アンチパスバック

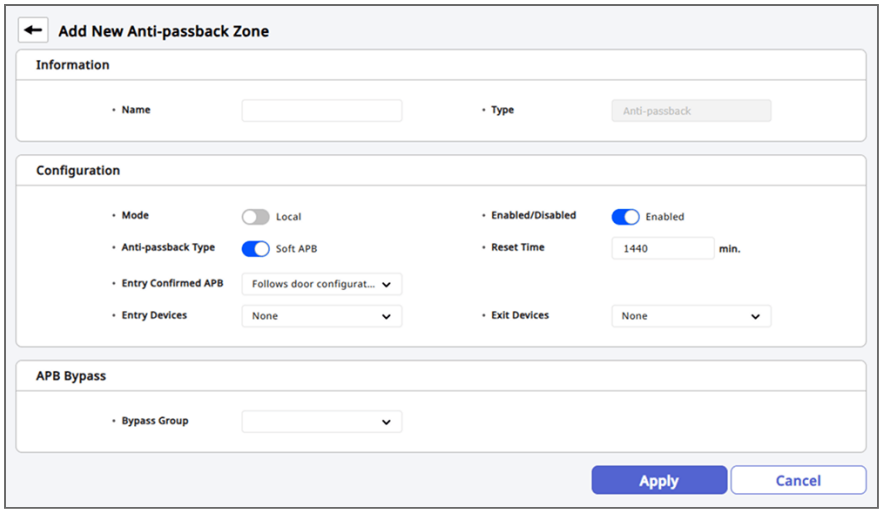
アンチパスバックは、ドアまたはデバイスを基準に作成されたアンチパスバックよりも高度な機能を提供します。アンチパスバックを設定することで、ユーザーが入室および退室する際に指定されたドアとデバイスを使用するよう強制できます。これにより、不正な再入室を防止し、セキュリティを強化できます。

情報

안티패스백(Anti-Passback): 출입 통제를 위해 구조적인 방법으로서, 출입문 안쪽/바깥쪽에 출입 통제 장치를 설치하여 구역에 출입할 때 반드시 인증을 통해 출입해야 하는 기능입니다. 카드를 사용해 출입할 때 리더기에 카드를 인식하지 않고 앞 사람을 따라 입실했다면, 퇴실할 때 출입문이 열리지 않으며 **안티패스백** 이벤트가 발생합니다.
안티패스백은 Hard APB와 Soft APB로 구분합니다. **안티패스백** 위반 시 Hard APB는 **안티패스백** 이벤트를 생성하고 출입할 수 없으며, Soft APB는 **안티패스백** 이벤트를 생성하고 출입은 가능합니다.

アンチパスバック登録

1. **Launcher**ページで**Settings**をクリックします。
2. 画面左のサイドバーで **Access Management** → **Advanced AC**をクリックしてください。
3. **ADD ADVANCED AC** ボタンをクリックします。
4. **Anti-passback** を選択し、**Apply** をクリックします。
5. **Info** セクションで追加するアンチパスバック機能の名前を入力します。



6. **Settings** セクションでアンチパスバック機能の詳細項目を設定します。詳細については設定オプションの案内をご参照ください。
7. **Alarm** セクションでアンチパスバック違反が発生したときに実行する動作を設定します。
8. **APB Bypass** セクションでアンチパスバックをバイパスして通過できるアクセスグループを選択します。このグループに属するユーザーはアンチパスバックをバイパスできます。
9. すべての設定が完了したら、画面下部の **Apply** ボタンをクリックします。

情報

Alarm セクションは、**Entry Devices** と **Exit Devices** の双方を設定して初めて使用できます。

設定オプションの案内

アンチパスバック設定の詳細項目は以下のとおりです。

- **Mode**：適用範囲を設定します。

  - **Local**：入室装置と RS-485 で接続されたデバイスで設定できます。
  - **Global**：BioStar X に登録されているすべてのデバイスに設定できます。
- **Enabled/Disabled**：設定を有効化または一時的に無効化できます。
- **Anti-passback Type**：アンチパスバックの種類を選択します。
  - **Hard APB**：アンチパスバックイベントを生成し、入退室できません。
  - **Soft APB**：アンチパスバックイベントを生成し、入退室できます。
- **Reset Time**：アンチパスバック規則に違反したユーザーに再び入退室を許可するまでの待機時間を設定します。アラーム発生後、設定した時間が経過すると該当ユーザーの入退室を自動で許可します。
  - 1 分から 10080 分（7日）の範囲で設定できます。
  - 0 分に設定するとアラームは自動で解除されず、管理者が手動で解除するまで入退室できません。
- **Entry Confirmed APB**：アンチパスバック規則を適用する範囲を設定します。
  - **ON**：入室装置と退室装置が構成されたドアの実際の動作に従ってアンチパスバック規則が適用されます。
  - **OFF**：ドアの動作に関係なく、ユーザーの認証に基づいて規則が適用されます。
  - **Follows door configuration**：当該ドアで入退室ベースの APB を使用する場合、センサー使用オプションの設定に従ってアンチパスバック規則が適用されます。
- **Entry Devices**：入室時に使用するデバイスを選択します。登録済みデバイスの一覧から選択できます。
- **Exit Devices**：退室時に使用するデバイスを選択します。登録済みデバイスの一覧から選択できます。
- **Network Failure Action**：BioStar X とアンチパスバックが設定されたデバイスとの通信が切断されたときのドア動作を設定します。この機能は **Mode** オプションを **Global** に設定した場合に使用できます。
  - **Open by auth**：ユーザーが正常に認証されるとドアが開きます。
  - **Open by auth & record APB log**：アンチパスバック違反アラームが発生し、ドアが開きます。
  - **Door locked & record APB log**：アンチパスバック違反アラームが発生し、ドアは開きません。

> **情報**
> デバイス登録の詳細は、以下のドキュメントを参照してください。
> - デバイスを登録する
> - Wiegandデバイスを登録する
> - スレーブ装置を登録する

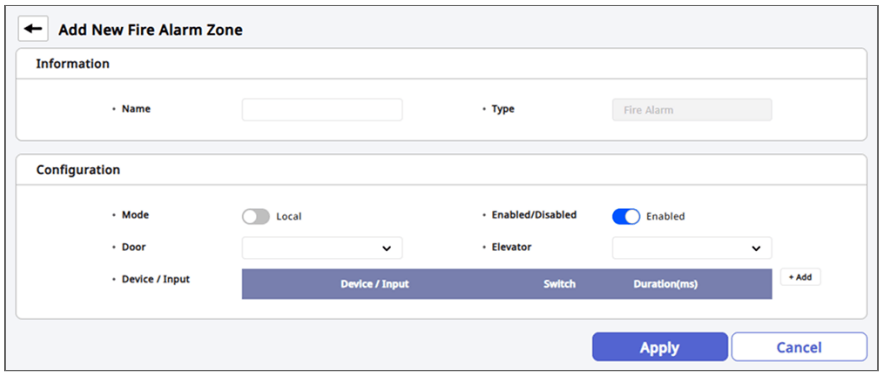
火災警報

火災警報の設定方法を案内します。火災警報は、火災発生時にすべてのドアまたはエレベーターを開放または施錠するように設定する機能です。

火災警報の登録

1. **Launcher**ページで**Settings**をクリックします。

2. 画面左のサイドバーで **Access Management** → **Advanced AC**をクリックしてください。
3. **ADD ADVANCED AC** ボタンをクリックします。
4. **Fire Alarm** を選択し、**Apply** をクリックします。
5. **Info** セクションで、追加する火災警報の名前を入力します。



6. **Settings** セクションで、火災警報の詳細項目を設定します。詳細については設定オプションの案内をご参照ください。
7. **Alarm** セクションで、火災警報が発生したときに実行する動作を設定します。
8. すべての設定が完了したら、画面下部の **Apply** ボタンをクリックします。

> **情報**
> **Alarm**セクションは、**Door**を設定すると使用できます。

設定オプションの案内

火災警報設定の詳細項目は次のとおりです。

- **Mode**：適用範囲を設定します。
  - **Local**：入室デバイスと RS-485 で接続されたデバイスのみ設定できます。
  - **Global**：BioStar X に登録されているすべてのデバイスに設定できます。
- **Enabled/Disabled**：設定を有効化または一時的に無効化できます。
- **Door**：火災警報ルールを適用するドアを選択します。
- **Elevator**：火災警報ルールを適用するエレベーターを選択します。
- **Device / Input**：**+ Add** をクリックし、火災警報信号を発生させるデバイスを設定します。

情報

- **Mode** オプションを **Local** に設定すると、ドアまたはエレベーターのいずれか一方にのみ火災警報機能を設定できます。
- **Mode** オプションを **Global** に設定すると、ドアとエレベーターの両方に同時に火災警報機能を設定できます。
- デバイス登録の詳細は、以下のドキュメントを参照してください。
  - デバイスを登録する
  - Wiegandデバイスを登録する
  - スレーブ装置を登録する

スケジュールロック

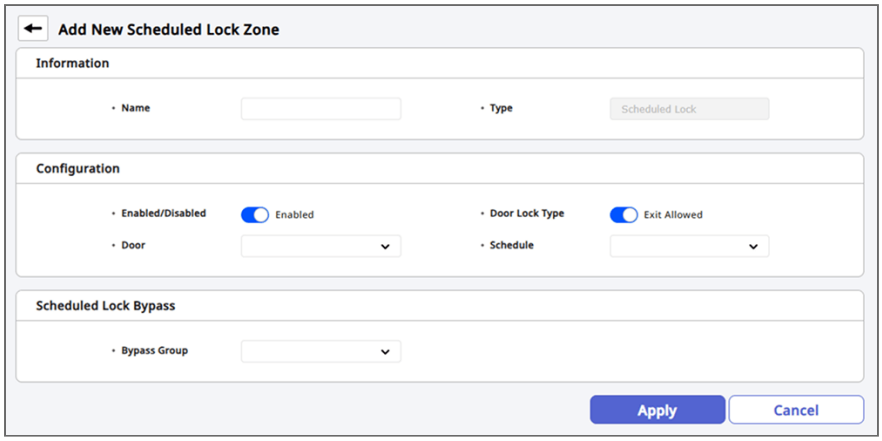
スケジュールロックの設定方法を案内します。スケジュールロックは特定の時間にドアをロックする機能を提供します。この機能は入退室制御を強化し、特定の時間帯に入退室を制限するのに役立ちます。

情報

スケジュールロックの設定は**Local**モードのみ対応しています。

スケジュールロックの登録

1. **Launcher**ページで**Settings**をクリックします。
2. 画面左のサイドバーで **Access Management** → **Advanced AC**をクリックしてください。
3. **ADD ADVANCED AC** ボタンをクリックします。
4. **Scheduled Lock** を選択し、**Apply** をクリックします。
5. **Info**セクションで追加するスケジュールロック機能の名前を入力します。



6. **Settings**セクションでスケジュールロック機能の詳細項目を設定します。詳細については設定オプションの案内をご参照ください。
7. **Alarm**セクションでスケジュールロック違反発生時に実行する動作を設定します。
8. **Scheduled Lock Bypass**セクションでスケジュールロックをバイパスできる入退室グループを選択します。このグループに属するユーザーはスケジュールロックをバイパスできます。

9. すべての設定が完了したら、画面下部の **Apply** ボタンをクリックします。

> **情報**
> **Alarm**セクションは、**Door**を設定すると使用できます。

設定オプションの案内

スケジュールロック設定の詳細項目は次のとおりです。

- **Enabled/Disabled**：設定を有効化または一時的に無効化できます。
- **Door Lock Type**：入室デバイスのみをロックするか、入室デバイスと退室デバイスの両方をロックするように設定できます。
- **Door**：スケジュールロック規則を適用するドアを選択します。
- **Schedule**：スケジュールを選択します。目的のスケジュールがない場合は、**+ Add Schedule** をクリックして追加します。

> **情報**
> - **Local**モードでは、複数のドアを選択してスケジュールロック機能を構成できます。
> - スケジュール設定の詳細については、スケジュールを設定するをご参照ください。

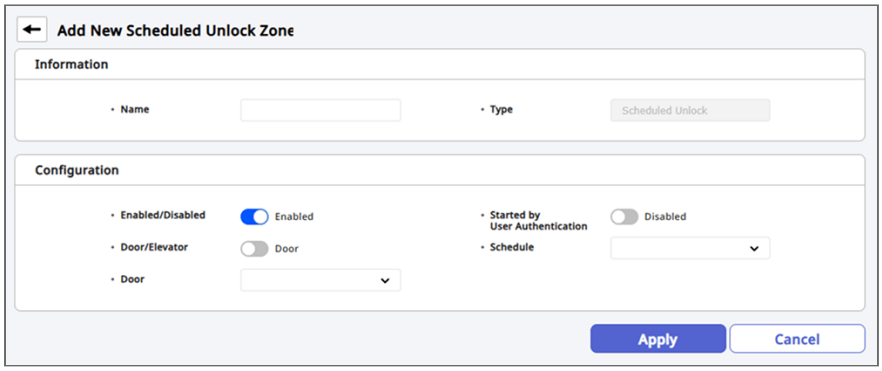
スケジュール開放

スケジュール開放の設定方法を説明します。スケジュール開放は、特定の時間にドアを開放する機能を提供します。この機能はアクセス制御を強化し、特定の時間帯にアクセスを許可するのに役立ちます。

> **情報**
> スケジュール開放は **Local** モードのみをサポートします。

スケジュール解錠登録

1. **Launcher**ページで**Settings**をクリックします。
2. 画面左のサイドバーで **Access Management** → **Advanced AC**をクリックしてください。
3. **ADD ADVANCED AC** ボタンをクリックします。
4. **Scheduled Unlock** を選択し、**Apply** ボタンをクリックします。
5. **Info** セクションで、追加するスケジュール開放機能の名前を入力します。



6. **Settings** セクションで、スケジュール開放機能の詳細項目を設定します。詳細については設定オプションの案内をご参照ください。

7. **Scheduled Unlock Authentication** セクションで、スケジュール開放を開始できるユーザーを含むアクセスグループを選択できます。

8. すべての設定が完了したら、画面下部の **Apply** ボタンをクリックします。

設定オプションの案内

スケジュール開放を設定するための詳細項目は以下のとおりです。

- **Enabled/Disabled**：設定を有効化または一時的に無効化できます。
- **Started by User Authentication**：**Enabled** に設定すると、**Scheduled Unlock Authentication** セクションが表示されます。 **Access Group** で選択したユーザーグループのユーザーが指定されたスケジュールに合わせて認証すると、スケジュール開放が開始されます。
- **Door/Elevator**：スケジュール開放機能を適用するドアまたはエレベーターを選択します。
  - **Door** を選択すると、ドア一覧が有効になります。スケジュール開放機能を適用するドアを選択します。複数のドアを選択できます。
  - **Elevator** を選択すると、エレベーター一覧が有効になります。スケジュール開放機能を適用するエレベーターを選択します。複数のエレベーターを選択できます。

> **Door/Elevator** オプションは、エレベーターが登録されている場合に表示されます。エレベーターが登録されていない場合は、**Door** オプションのみが表示されます。エレベーターの登録について詳しくは、エレベーターを登録するをご参照ください。

- **Schedule**：スケジュールを選択します。目的のスケジュールがない場合は、**+ Add Schedule** をクリックして追加します。
- **Floor**：選択したエレベーターの階を選択できます。

> **情報**
>
> - **Local** モードでは、複数のドアを選択してスケジュール開放機能を構成できます。
> - すでに別のスケジュール開放設定に含まれているエレベーターを選択した場合、同じ階を重複して設定することはできません。
> - スケジュール設定の詳細については、スケジュールを設定するをご参照ください。

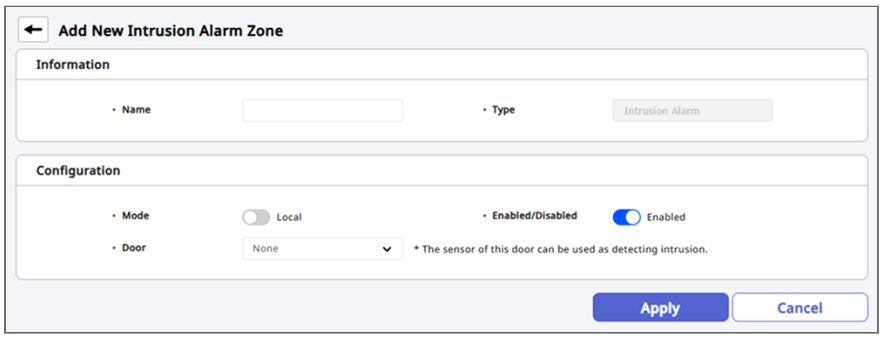
警備

警備設定の方法を案内します。警備機能は、侵入を検知した際にドアをロックしたりアラームを発生させたりする機能を提供します。

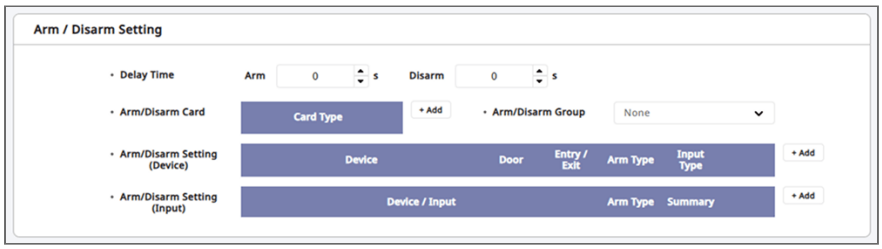
> **情報**
> **경비 구역:** 경비 개시 후 허가받지 않은 사람이 침입을 시도하면 경고음을 출력하거나 릴레이 신호를 출력하도록 설정한 구역입니다. 주로 업무 종료 이후 경비를 개시하며, 경비 개시 이후 출입을 시도하면 설정된 알람이나 신호를 출력합니다.

警備登録

1. **Launcher**ページで**Settings**をクリックします。
2. 画面左のサイドバーで **Access Management** → **Advanced AC**をクリックしてください。
3. **ADD ADVANCED AC** ボタンをクリックします。
4. **Intrusion Alarm** を選択し、**Apply** をクリックします。
5. **Info** セクションで追加する警備設定の名前を入力します。



6. **Settings** セクションで警備設定の詳細項目を設定します。詳細については設定オプションの案内をご参照ください。
7. **Arm / Disarm Setting** セクションで警備開始と解除の認証設定を追加します。詳しくは警備開始または解除の設定をご参照ください。



> **Arm / Disarm Setting** セクションは、**Info** セクションでドアを選択したときに表示されます。

8. **Intrusion Setting** セクションで侵入検知信号を設定します。詳しくは侵入検知設定をご参照ください。



9. **Alarm** セクションで特定のイベントが発生したときに実行する動作を設定します。
10. すべての設定が完了したら、画面下部の **Apply** ボタンをクリックします。

> **情報**
> **Arm / Disarm Setting** と **Intrusion Setting**、**Alarm** セクションは、**Settings** セクションで **Door** オプションを設定すると使用できます。

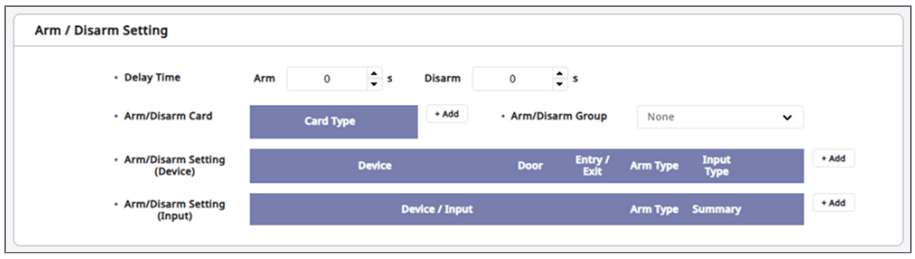
設定オプションの案内

警備設定のための詳細項目は以下のとおりです。

- **Mode**：適用範囲を設定します。警備設定は **Local** モードのみをサポートし、入室デバイスと RS-485 で接続されたデバイスでのみ設定できます。
- **Enabled/Disabled**：設定を有効化または一時的に無効化できます。
- **Door**：警備機能を適用するドアを選択します。

警備開始または解除の設定

警備開始と解除の認証設定を追加できます。

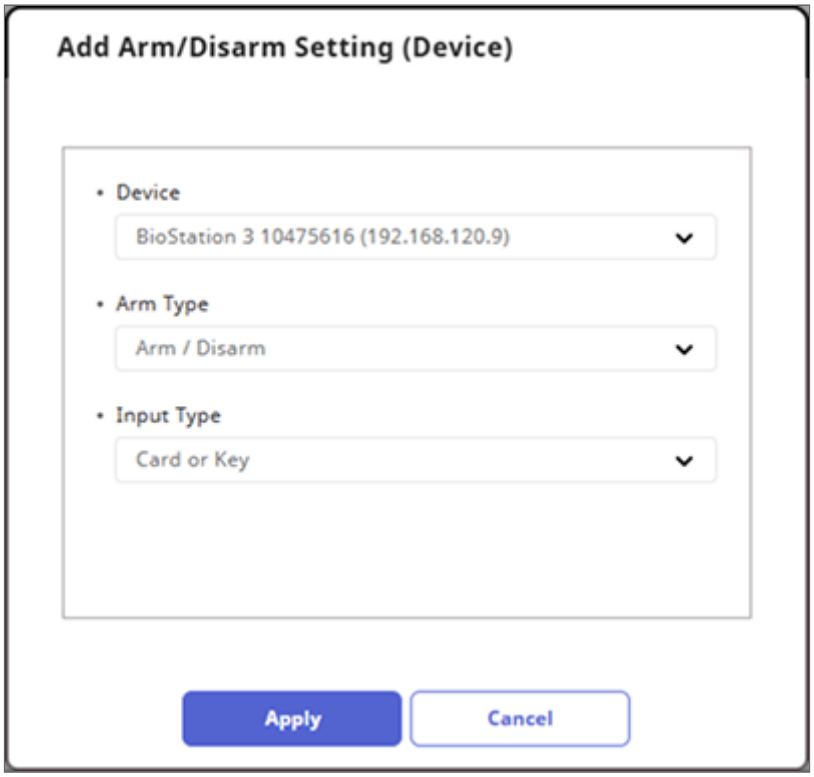


- **Delay Time**：警備開始または警備解除までの遅延時間を設定できます。つまり、開始は認証後から警備開始までの遅延時間であり、解除は侵入検知後からアラームが発生するまでの遅延時間です。
- **Arm/Disarm Card**：警備開始または解除の権限を付与したカードを追加できます。警備/解除カードは最大128枚まで登録できます。
- **Arm/Disarm Group**：警備開始または解除の権限を付与したグループを選択できます。警備/解除グループは最大128件まで登録できます。
- **Arm/Disarm Setting**：デバイスによる警備開始/解除または入力信号による警備開始/解除を設定できます。 **+ Add** をクリックし、各項目を設定します。

デバイスによる警備開始/解除の追加

「**Arm/Disarm Setting**」（**Device**）オプションで **+ Add** をクリックします。警備機能を制御するデバイスを選択し、**Arm Type** を選択します。

Input Type では、**Card**、**Key**、**Card or Key** を選択できます。 LCD画面のないデバイスは、入力種別として **Card** のみ使用できます。



入力信号による警備開始/解除の追加

「**Arm/Disarm Setting**」（**Input**）オプションで **+ Add** をクリックします。警備機能を制御するデバイスを選択します。 **Port** をクリックし、選択したデバイスの入力ポートを選択します。

Arm Type を選択した後、スイッチの種類と信号の持続時間を設定します。



侵入検知設定

侵入検知信号を設定できます。 **+ Add** をクリックし、以下のように設定すると、BioStation 3 デバイスの0番入力ポートに接続された N/O センサーが100(ms) の間信号を送信した場合に侵入を検知したと判断します。



インターロック

インターロックは、セキュリティが重要なエリアで使用される出入管理方式です。 2枚以上のドアがある場所でインターロックを設定すると、次のように動作します。

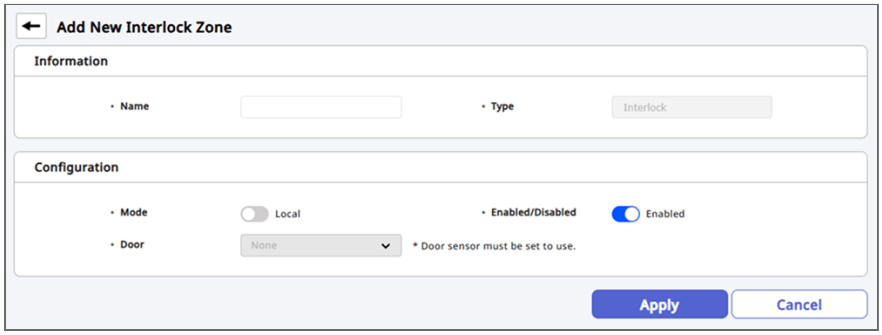
- ドアセンサーとリレーを使用して各ドアの状態をリアルタイムで監視します。
- 1つのドアが開いている、または解錠されている場合、他のすべてのドアは自動的に施錠されます。
- ユーザーがその場所に滞在している間は追加の出入りをブロックするよう設定します。

この方法により複数のドアが同時に開くことを防ぎ、セキュリティを強化します。

> **情報**
>
> - 1つのインターロック設定には最大4枚のドアを含めることができます。
> - CoreStationに接続されているデバイスで構成されたドアのみインターロックを設定できます。
> - インターロックに割り当てられたデバイスは、他のインターロック設定では使用できません。
> - インターロックに指定されたドアは、火災警報設定を除き他の設定では使用できません。

インターロックを追加

1. **Launcher**ページで**Settings**をクリックします。
2. 画面左のサイドバーで **Access Management** → **Advanced AC**をクリックしてください。
3. **ADD ADVANCED AC** ボタンをクリックします。
4. **Interlock** を選択し、**Apply** をクリックします。
5. **Info** セクションで、追加するインターロック設定の名前を入力します。



6. **Settings** セクションでインターロック設定の詳細項目を設定します。詳細については設定オプションの案内をご参照ください。
7. **Option** セクションで、ユーザーが滞在している間は出入りできないように設定します。
8. **Alarm** セクションで、インターロック設定で特定のイベントが発生した際に実行する動作を設定します。

> **情報**
> **Option** および **Alarm** セクションは、**Settings** セクションで **Door** を設定してから使用できます。

設定オプションの案内

インターロック設定の詳細項目は以下のとおりです。

- **Mode**：適用範囲を設定します。インターロック設定は **Local** モードのみをサポートし、CoreStationにRS-485で接続されたデバイスでのみ設定できます。
- **Enabled/Disabled**：設定を有効化または一時的に無効化できます。
- **Door**：インターロックに指定するドアを選択します。少なくとも2つ以上のドアを選択する必要があり、ドアセンサーが接続されているドアのみ追加できます。

点呼招集

点呼招集は、緊急事態発生時の効果的な人員管理と安全確保のために必須の設定です。この機能により、管理者は特定の場所を点呼招集地点として指定し、緊急時にユーザーが集まる場所を事前に定義できます。

点呼招集設定は次の目的で活用します。

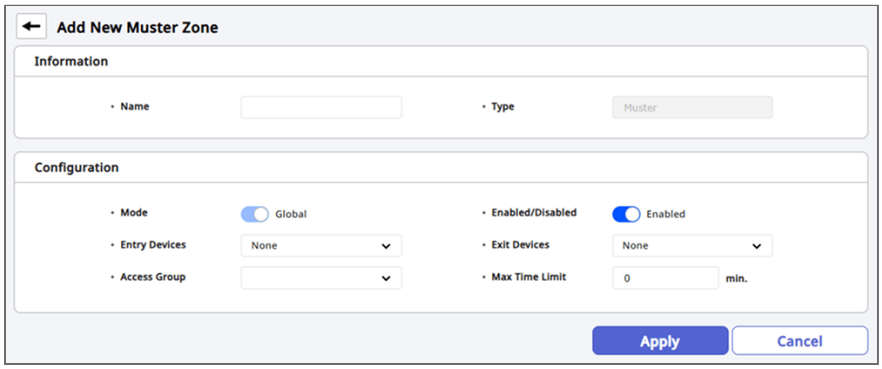
- **緊急対応**：火災や地震などの緊急時にユーザーが安全に集まれる場所を指定
- **人数モニタリング**：特定の場所内の現在の人数と入退室者リストをリアルタイムで確認

- **長時間滞在検知**：設定時間を超えて特定の場所に滞在するユーザーを検知し、管理者に通知を送信
- **セキュリティ強化**：機密性の高い場所への入退室を継続的にモニタリングしてセキュリティレベルを向上

このような機能により、管理者はより体系的で効率的なセキュリティ管理体制を構築できます。

点呼招集の登録

1. **Launcher**ページで**Settings**をクリックします。
2. 画面左のサイドバーで **Access Management** → **Advanced AC**をクリックしてください。
3. **ADD ADVANCED AC** ボタンをクリックします。
4. **Muster** を選択し、**Apply** ボタンをクリックします。
5. **Info** セクションで、追加する点呼招集設定の名前を入力します。



6. **Settings** セクションで、点呼招集設定の詳細項目を設定します。詳細については設定オプションの案内をご参照ください。
7. **Alarm** セクションで、点呼招集設定で特定のイベントが発生したときに実行する動作を設定します。
8. すべての設定が完了したら、画面下部の **Apply** ボタンをクリックします。

> **情報**
> **Alarm** セクションは、**Entry Devices** と **Exit Devices** の双方を設定して初めて使用できます。

設定オプションの案内

点呼招集設定の詳細項目は以下のとおりです。

- **Mode**：適用範囲を確認できます。点呼招集設定は **Global** モードのみをサポートし、**BioStar X** に登録されているすべてのデバイスで設定できます。
- **Enabled/Disabled**：設定を有効化または一時的に無効化できます。
- **Entry Devices**：入室時に使用するデバイスを選択します。登録済みデバイスの一覧から選択できます。
- **Exit Devices**：退室時に使用するデバイスを選択します。登録済みデバイスの一覧から選択できます。
- **Access Group**：点呼招集場所に滞在するユーザーが属する入退室グループを設定します。最大16個の入退室グループを設定できます。
- **Max Time Limit**：点呼招集場所に滞在できる最大時間を設定できます。最大4320分まで設定でき、指定時間を超えてユーザーが点呼招集場所に滞在した場合にアラームが発生します。

情報

デバイス登録の詳細は、以下のドキュメントを参照してください。

- デバイスを登録する
- Wiegandデバイスを登録する
- スレーブ装置を登録する

在室人数制限

在室人数制限は、空間の安全性と効率性を確保するための重要な入退室制御機能です。この機能により管理者は場所ごとに同時に入室できる最大人数をあらかじめ設定し、混雑を防ぎ、より体系的な空間管理を実現できます。

在室人数制限設定の主な活用分野は次のとおりです。

- **安全管理**：火災安全規定や建物の収容限度に基づく最大人数制限で安全事故を防止
- **空間効率**：会議室、実験室、作業場などの適正人数を維持して業務環境を最適化
- **感染症対策**：ソーシャルディスタンスや密度制限が必要な状況での人数管理
- **リアルタイムモニタリング**：場所ごとの現在の在室人数と入退室状況をリアルタイムで確認
- **自動警報**：設定した人数に達すると管理者へ即時通知を送り、迅速に対応可能

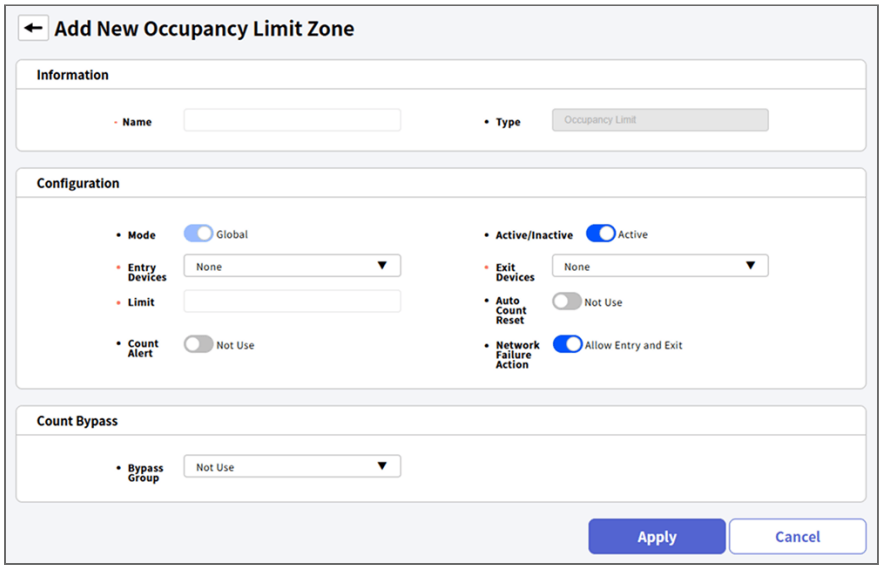
これらの機能を活用すると、管理者は各空間の特性に合わせたカスタム人数管理ポリシーを策定し、安全かつ効率的な施設運用を確保できます。

情報

- 在室人数制限設定は最大100件まで追加できます。
- 在室人数制限設定に構成できるデバイスとファームウェアバージョンは以下のとおりです。
  - FaceStation F2 ファームウェア 1.1.0 以上
  - FaceStation 2 ファームウェア 1.5.0 以上

在室人数制限の登録

1. **Launcher**ページで**Settings**をクリックします。
2. 画面左のサイドバーで **Access Management** → **Advanced AC**をクリックしてください。
3. **ADD ADVANCED AC** ボタンをクリックします。
4. **Occupancy Limit** を選択し、**Apply** をクリックします。
5. **Info** セクションで、追加する在室人数制限設定の名前を入力します。



6. **Configuration** セクションで在室人数制限設定の詳細項目を設定します。詳細については設定オプションの案内をご参照ください。

7. **Count Bypass** セクションで、在室人数制限を常にバイパスできる入退室グループを選択できます。詳細については常時通過人数の設定をご参照ください。

8. すべての設定が完了したら、画面下部の **Apply** ボタンをクリックします。

> **情報**
> **Name** は最大48文字まで入力でき、他の設定と同じ名前にはできません。

設定オプションの案内

在室人数制限設定の詳細項目は以下のとおりです。

- **Mode**：適用範囲を確認できます。在室人数制限設定は **Global** モードのみをサポートし、**BioStar X** に登録されているすべてのデバイスで設定できます。
- **Active/Inactive**：設定を有効化または一時的に無効化できます。
- **Entry Devices**：入室時に使用するデバイスを選択します。登録済みデバイスの一覧から選択できます。
- **Exit Devices**：退室時に使用するデバイスを選択します。登録済みデバイスの一覧から選択できます。
- **Limit**：入室を制限する人数を入力します。入室人数が設定した上限に達した場合、入室が制限されます。 0から10,000までの数値を入力でき、0に設定すると人数制限なしで入退室できます。
- **Auto Count Reset**：保存された在室人数を自動で初期化する時間を設定します。毎日設定した時間に在室人数および常時通過人数が初期化されます。
- **Count Alert**：入室人数が設定上限に達する前に、あらかじめ管理者へアラームを送信するかイベントログに記録できます。在室人数の事前警報を有効にすると、**Alert 1** 入力フィールドが有効になります。 **Alert 2** を設定するには、＋ をクリックします。
- **Network Failure Action**：設定されたデバイスでネットワーク障害が発生した際の入退室許可可否を設定できます。入退室許可に設定すると、デバイスがネットワーク切断された場合に入室制限が停止し、実際の入室人数が上限を超えてもユーザーは入室できます。

情報

- 同じデバイスを **Entry Devices** と **Exit Devices** に同時に設定することはできません。
- **Entry Devices** と **Exit Devices** は最大 128 台まで選択できます。
- **Dual Authentication**を出入口のドアで設定したデバイスは、**Entry Devices**または**Exit Devices**に設定できません。
- **Auto Count Reset** オプションの時間は、実際にその場所がある地域の標準タイムゾーンを考慮して設定してください。例として、UTC+1:00 の地域にある **BioStar X** サーバーで在室人数の自動初期化時刻を 00:00 に設定すると、UTC+2:00 の地域にある **BioStar X** クライアントでは 01:00 に自動初期化されます。
- **Count Alert** は最大 2 件まで設定でき、制限値より小さい数字のみ入力できます。 **Alert 1** と **Alert 2** は同じ値に設定できません。
- デバイス登録の詳細は、以下のドキュメントを参照してください。
  - デバイスを登録する
  - Wiegandデバイスを登録する
  - スレーブ装置を登録する

常時通過人数の設定

在室人数制限を常に通過できる入退室グループを選択できます。常時通過グループに属するユーザーは在室人数に関係なく入退室でき、在室人数としてカウントされません。実際に在室している常時通過人数は、在室人数制限設定リストの常時通過人数列で確認できます。

情報

- デバイスをサーマルカメラと接続して使用する場合、**Thermal & Mask Check Mode** を **Check without authentication** に設定すると、常時通過人数を設定しても動作しません。
- **Bypass Group** は最大 16 件まで設定できます。

リストの状況確認

在室人数制限設定のリストを確認できます。各設定の状態と在室人数を確認し、必要に応じて設定を変更できます。

- **Name**：名前を確認できます。
- **Status**：状態を確認できます。
  - **Normal**：現在の在室人数が、**Limit**、**Count Alert**(**Alert 1**、**Alert 2**) で設定した人数より少ない状態です。ユーザーは該当場所に入室できます。
  - **Count Alert**：在室人数が **Alert 1** または **Alert 2** で設定した人数に到達した状態です。
  - **Full**：在室人数が制限で設定した人数に到達した状態です。これ以上の入室は制限されます。
- **Count/Limit**：定員に対する現在の入室人数を確認できます。また、ネットワーク障害などの特殊な状況で在室人数と実際の人数が一致しない場合、管理者は ＋ または ー をクリックするか、在室人数をクリックして直接修正できます。
- **Count Bypass**：現在入室している常時通過人数に含まれるユーザー数を確認できます。
- **Device Status**：設定したデバイスの状態を確認できます。

  - **Normal**：設定されたすべてのデバイスのネットワークが正常に動作している状態です。
  - **Network Failure**：1 台以上のデバイスでネットワーク障害が発生しています。
- **Full Screen**：在室人数制限設定の状況をフルスクリーンで確認できます。

> **情報**
> **Limit** を設定した場合、在室人数は最大 50,000 まで入力できます。 **Limit** を設定しない場合、最大 999,999 まで入力できます。最大入力値を超える数字は入力できず、実際の在室人数が最大入力値を超える場合、超過分はデータベースに保存されません。

在室人数を初期化する

在室人数および常時通過人数を初期化できます。在室人数を初期化すると、ユーザーの入退室情報はすべて削除され、ネットワークの状態によって在室人数が不正確になる可能性があります。

1. **Launcher**ページで**Settings**をクリックします。
2. 画面左のサイドバーで **Access Management** → **Advanced AC**をクリックしてください。
3. リストで **Occupancy Limit** をクリックします。
4. 在室人数制限設定リストから初期化する設定のチェックボックスをクリックします。
5. 画面右上の **Reset Count** をクリックします。
6. 確認メッセージが表示されたら、**Apply** をクリックします。

有効化/無効化

無効化された在室人数制限設定を有効化するか、有効化された設定を無効化できます。設定を無効化すると、**Current Occupancy** と **Bypass Count** が初期化されます。

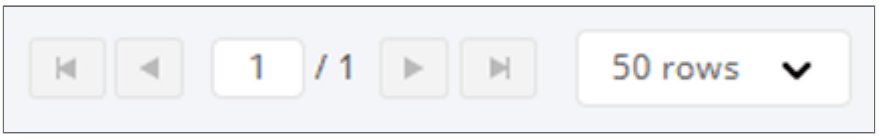
1. **Launcher**ページで**Settings**をクリックします。
2. 画面左のサイドバーで **Access Management** → **Advanced AC**をクリックしてください。
3. リストで **Occupancy Limit** をクリックします。
4. 在室人数制限設定リストから有効化または無効化する項目のチェックボックスをクリックします。
5. 画面右上の **Activate** または **Deactivate** をクリックします。

削除

1. **Launcher**ページで**Settings**をクリックします。
2. 画面左のサイドバーで **Access Management** → **Advanced AC**をクリックしてください。
3. リストで **Occupancy Limit** をクリックします。
4. 在室人数制限設定リストから削除する項目のチェックボックスをクリックします。
5. 画面右上の **Delete** をクリックします。
6. 確認メッセージが表示されたら、**Apply** をクリックします。

一覧ページをナビゲートする

ページを移動したり、1ページに表示する一覧の件数を設定できます。 画面右上のページ移動ツールを使用します。



- ⏮：最初のページに移動します。
- ◀：前のページに移動します。
- ▶：次のページに移動します。
- ⏭：最後のページに移動します。
- 目的のページに移動するには、数字入力フィールドにページ番号を入力します。
- 1ページに表示する一覧の件数を設定するには、行選択ボックスをクリックします。

出席確認（Roll Call）

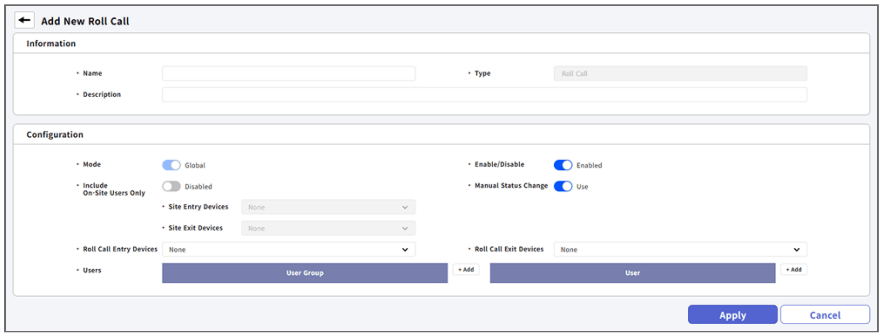
出席確認（Roll Call）は、特定の時点と場所での入退室記録を基に人員リストをすばやく作成します。緊急時には、ユーザーがあらかじめ指定された場所の入室または退室デバイスで認証し、出席確認場所に到着したかどうかを把握できます。

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。

出席確認の登録

1. **Launcher**ページで**Settings**をクリックします。
2. 画面左のサイドバーで **Access Management** → **Advanced AC**をクリックしてください。
3. **ADD ADVANCED AC** ボタンをクリックします。
4. **Roll Call** を選択し、**Apply** ボタンをクリックします。
5. **Info** セクションで追加する出席確認設定の名前と説明を入力します。

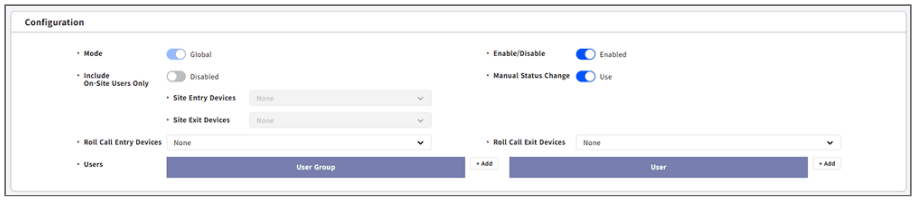


6. **Configuration** セクションで詳細項目を設定します。詳細については設定オプションの案内をご参照ください。
7. すべての設定が完了したら、画面下部の **Apply** ボタンをクリックします。

> **情報**
> **Name** は最大48文字まで入力でき、他の設定と同じ名前にはできません。

設定オプションの案内

出席確認設定の詳細項目は以下のとおりです。



- **Mode**：適用範囲を確認できます。出席確認設定は **Global** モードのみサポートしており、**BioStar X** に登録されているすべてのデバイスで設定できます。
- **Enabled/Disabled**：設定を有効化または一時的に無効化できます。
- **Include On-Site Users Only**：**Use** に設定すると、出席確認の開始時点で **現場入室デバイスで最後に認証したユーザー** のみを確認対象として固定します。既定値は **Not Use** です。この場合、設定された全ユーザー（ユーザーグループ + 個別ユーザー）が確認対象です。

  > システムは、各ユーザーの直近 7 日以内の現場入室または退室デバイスの認証履歴に基づき、ユーザーが現場にいるか判断します。出席確認の開始時点を基準に、最も新しい認証が現場入室デバイスで発生した場合は現場にいると判断し、現場退室デバイスで発生した場合は現場を離れたと判断します。直近 7 日以内に認証履歴がないユーザーは、現場にいないものとみなし、対象から除外されます。
  >
  > 対象者リストは人員点検を開始する時点で一度だけ確定され、点検中にユーザーが現場に入室または退室してもリストは変更されません。

  Include On-Site Users Only を **Use** に設定した場合、次のオプションを利用できます。

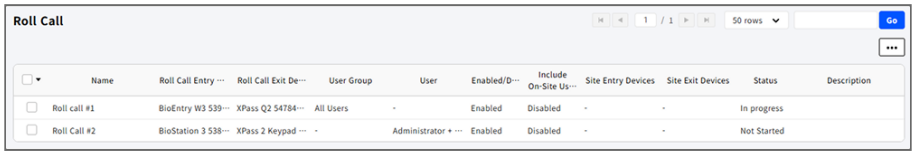
  - **Site Entry Devices**：現場入室認証に使用するデバイスを選択してください。
  - **Site Exit Devices**：現場退室認証に使用するデバイスを選択してください。
- **Manual Status Change**：手動で状態を変更できるように設定できます。
- **Roll Call Entry Devices**：入室時に使用するデバイスを選択してください。 デバイスが一覧にない場合は、先にデバイスを登録してください。登録済みデバイスの一覧から選択できます。
- **Roll Call Exit Devices**：退室時に使用するデバイスを選択してください。登録済みデバイスの一覧から選択できます。
- **Users**：入室可能なユーザーグループまたは個別ユーザーを選択できます。

情報

- 同じデバイスを **Roll Call Entry Devices** と **Roll Call Exit Devices** に同時に設定することはできません。
- **Roll Call Entry Devices** と **Roll Call Exit Devices** は最大 10 個まで選択できます。
- デバイス登録の詳細は、以下のドキュメントを参照してください。
  - デバイスを登録する
  - Wiegandデバイスを登録する
  - スレーブ装置を登録する

リスト状況の確認

出席確認リストで、各設定の詳細情報と状態を確認できます。

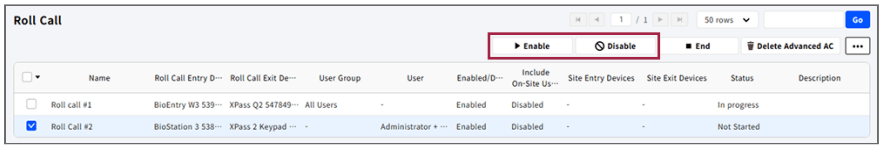


- **Name**：名前を確認できます。
- **Roll Call Entry Devices** / **Roll Call Exit Devices**：設定されたデバイスを確認できます。
- **User Group** / **Users**：設定された対象者を確認できます。
- **Enabled/Disabled**：有効状態を確認できます。
- **Include On-Site Users Only**：使用の有無を確認できます。
- **Site Entry Devices** / **Site Exit Devices**：設定された現場入室または退室デバイスを確認できます。
- **Status**：出席確認の進行状態（**Not Started**、**In progress** など）を確認できます。
- **Description**：登録された説明を確認できます。

有効化/無効化

無効化された出席確認設定を有効化したり、有効化されている設定を無効化できます。

1. **Launcher**ページで**Settings**をクリックします。
2. 画面左のサイドバーで **Access Management** → **Advanced AC**をクリックしてください。
3. 一覧で **Roll Call** をクリックします。
4. 出席確認設定リストの中から有効化または無効化する項目のチェックボックスをクリックします。

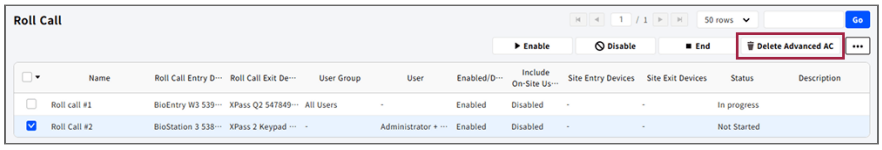


5. 画面右上の **Enable** または **Disable** ボタンをクリックします。

> **情報**
>
> - **Disable**を選択すると確認メッセージが表示されます。 **Yes** または **No**を選択します。
> - 進行中の出席確認は無効化できません。確認して再試行してください。

削除

1. **Launcher**ページで**Settings**をクリックします。
2. 画面左のサイドバーで **Access Management** → **Advanced AC**をクリックしてください。
3. 一覧で **Roll Call** をクリックします。
4. 出席確認設定リストの中から削除する項目のチェックボックスをクリックします。

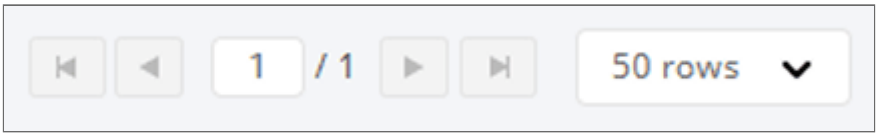


5. 画面右上の **Delete Advanced AC** ボタンをクリックします。
6. 警告メッセージが表示されたら **Continue** ボタンをクリックします。

> **情報**
>
> 進行中の出席確認は削除できません。出席確認を終了してから再試行してください。

一覧ページをナビゲートする

ページを移動したり、1ページに表示する一覧の件数を設定できます。 画面右上のページ移動ツールを使用します。



- ⏮：最初のページに移動します。
- ◀：前のページに移動します。
- ▶：次のページに移動します。
- ⏭：最後のページに移動します。
- 目的のページに移動するには、数字入力フィールドにページ番号を入力します。
- 1ページに表示する一覧の件数を設定するには、行選択ボックスをクリックします。

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。

情報

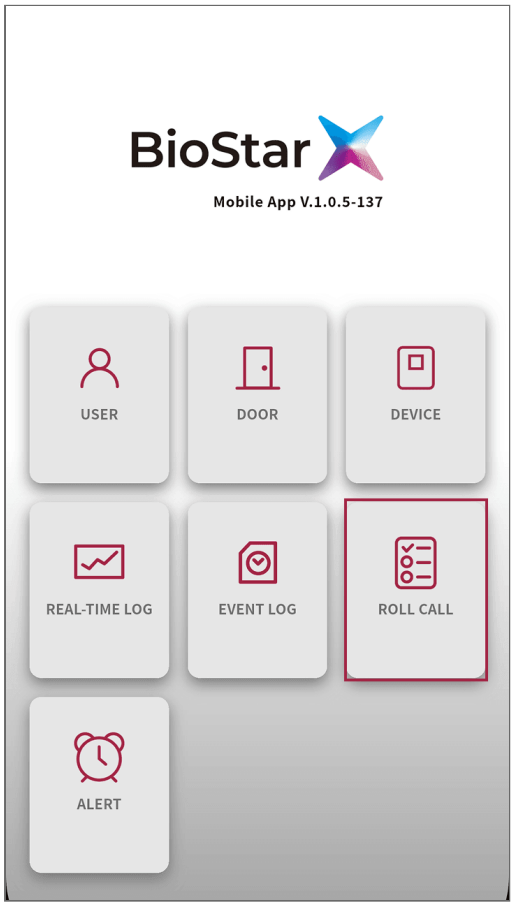
BioStar X モバイルアプリは次のリンクからインストールできます。

- iOS：Apple App Store
- Android：Google Play'

出席確認を開始する

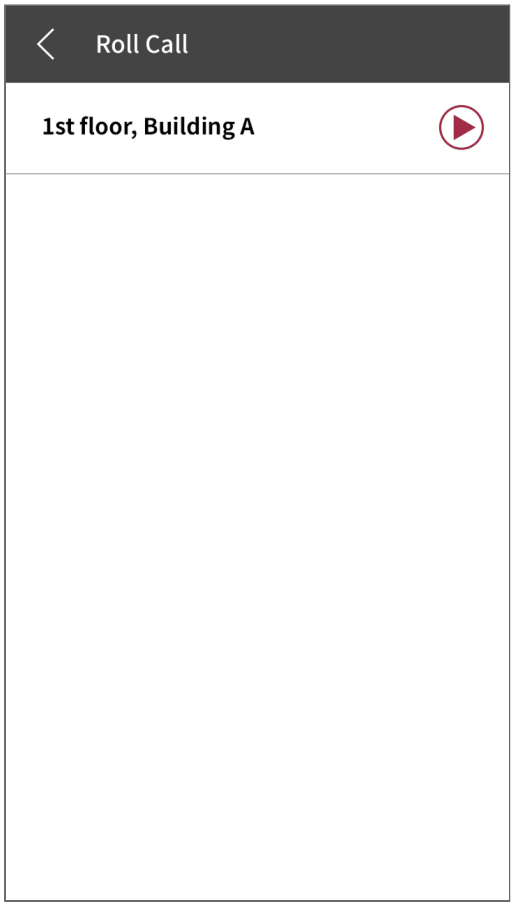
モバイルアプリで出席確認機能を開始するには、次の手順に従います。

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。



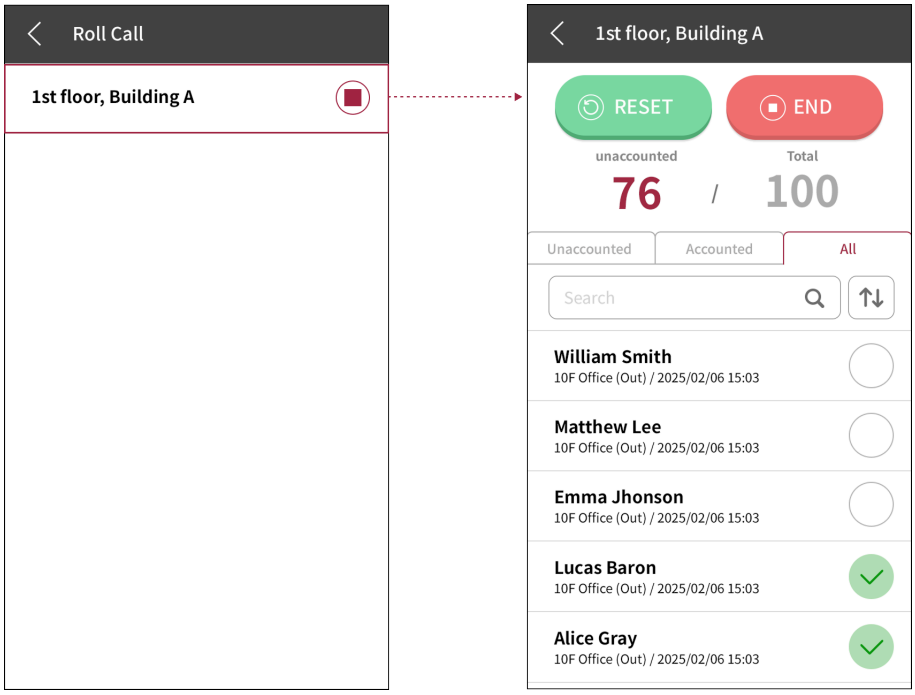
サイドメニューからも開けます。 ☰ → **Monitoring** → **Roll Call** をタップします。

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。



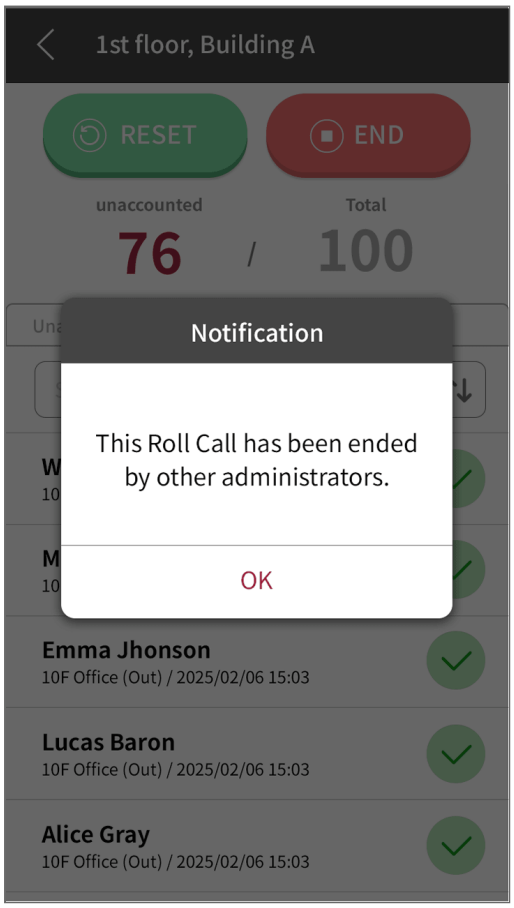
進行中の出席確認を制御する

- 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。

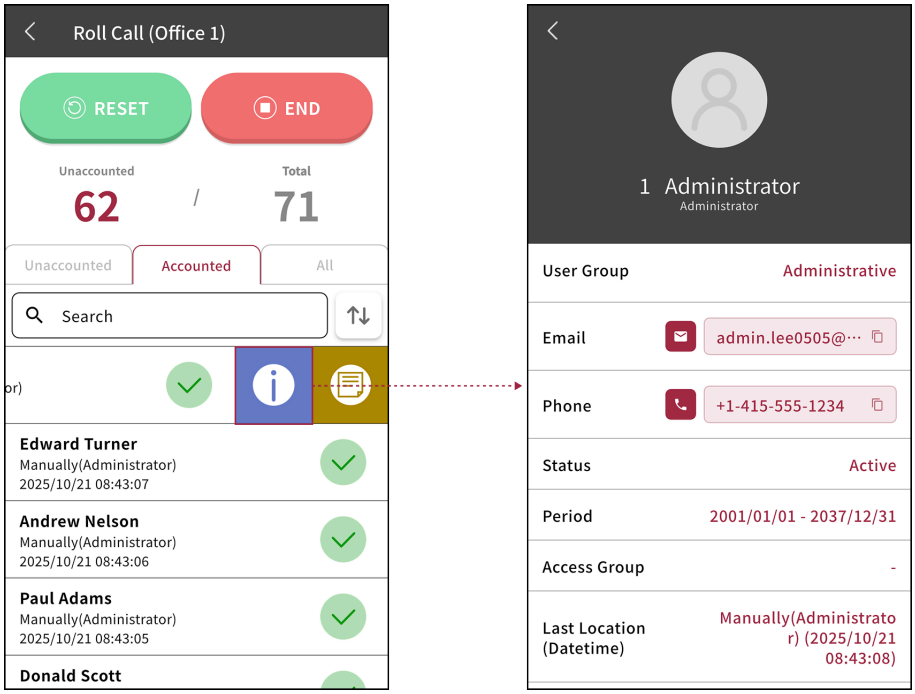


- 出席確認を完了した後、**Data** → **Generate Report** → **Roll Call** で関連レポートを確認できます。詳しくは出席確認レポートを確認を参照してください。

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。

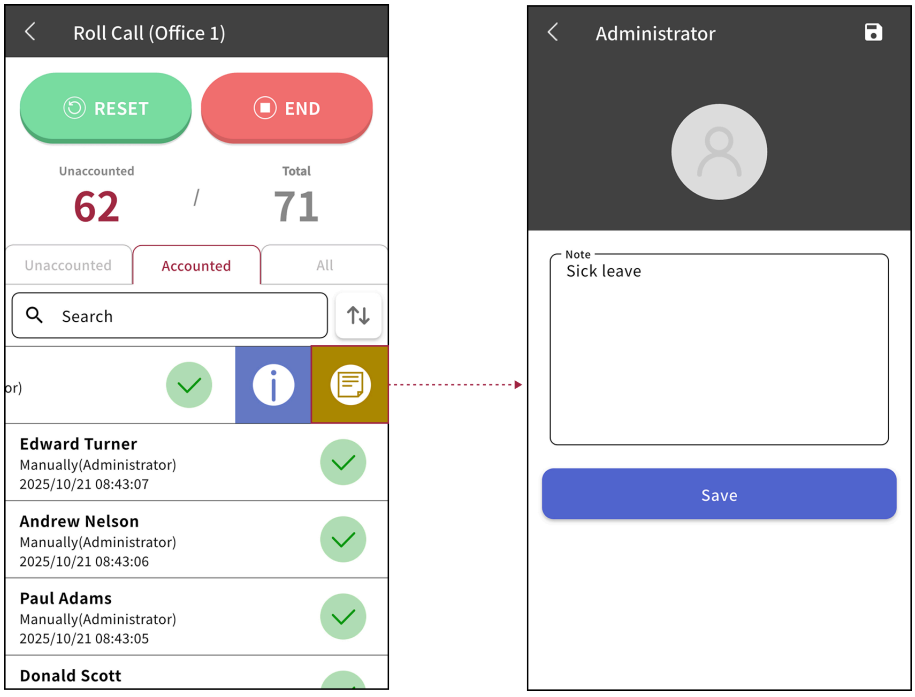
出席確認中に詳細を確認するユーザー項目を左にスワイプします。その後、ⓘをタップします。



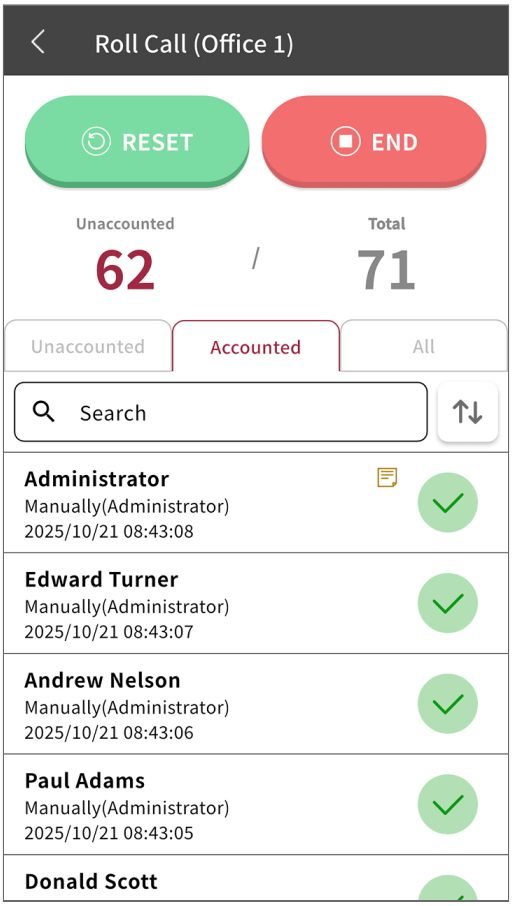
出席確認中にユーザーへメモを残す

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。



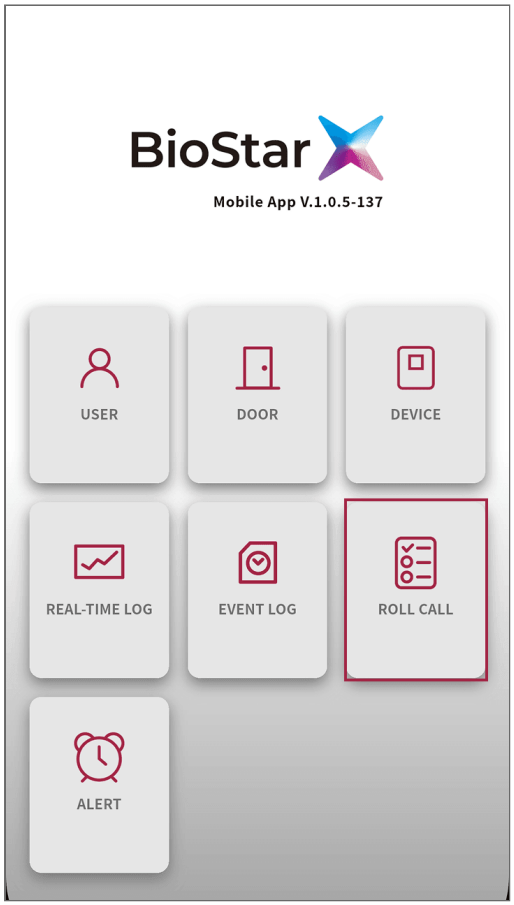
メモを入力したユーザーには、出席確認リストでアイコンが表示されます。



出席確認の詳細を確認

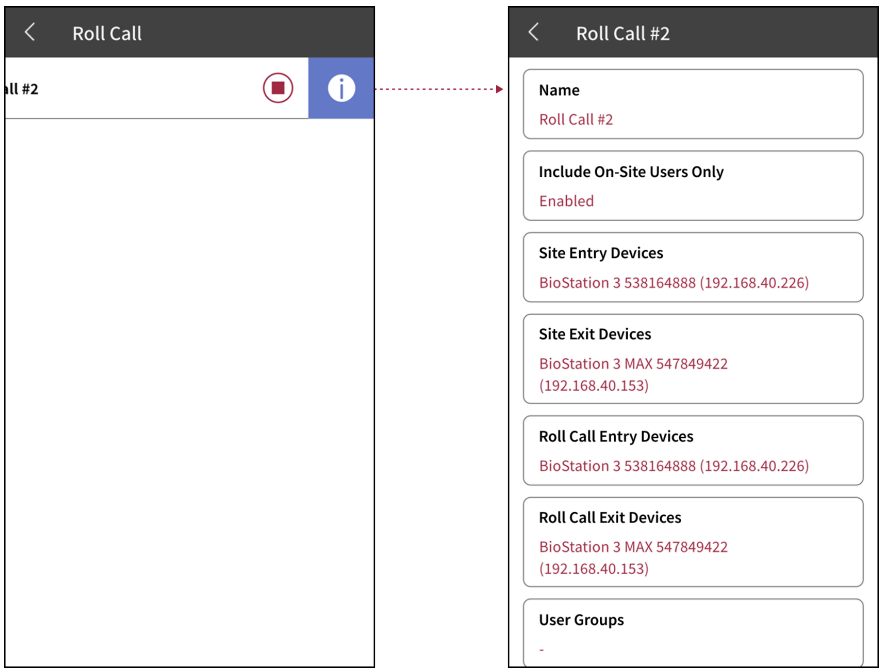
モバイルアプリで出席確認設定の詳細を確認できます。

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。

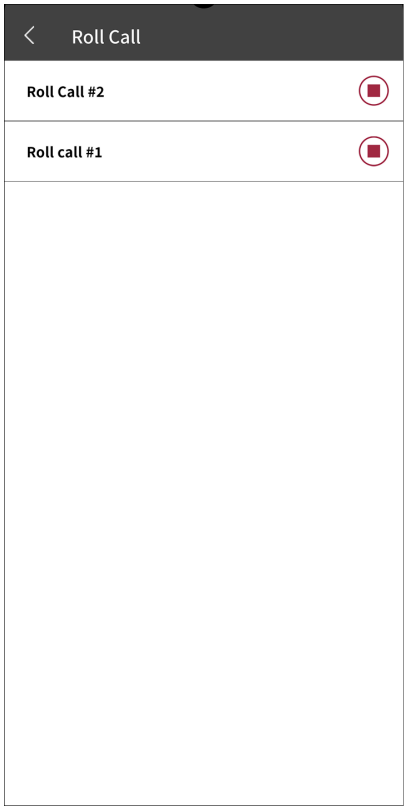


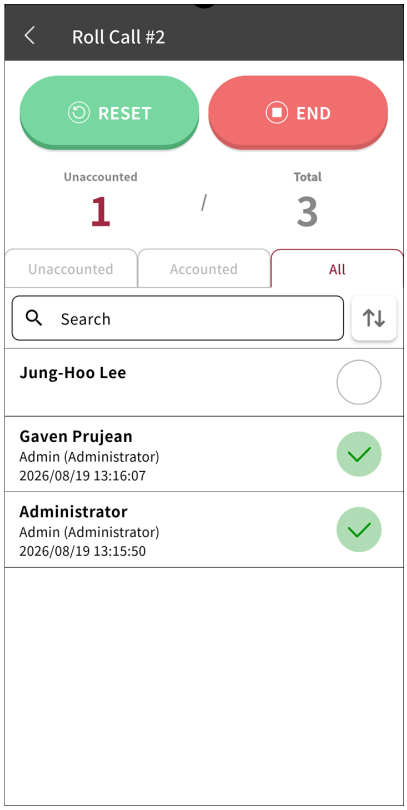
出席確認の終了

進行中の出席確認は **BioStar X** モバイルアプリとWebの両方で終了できます。

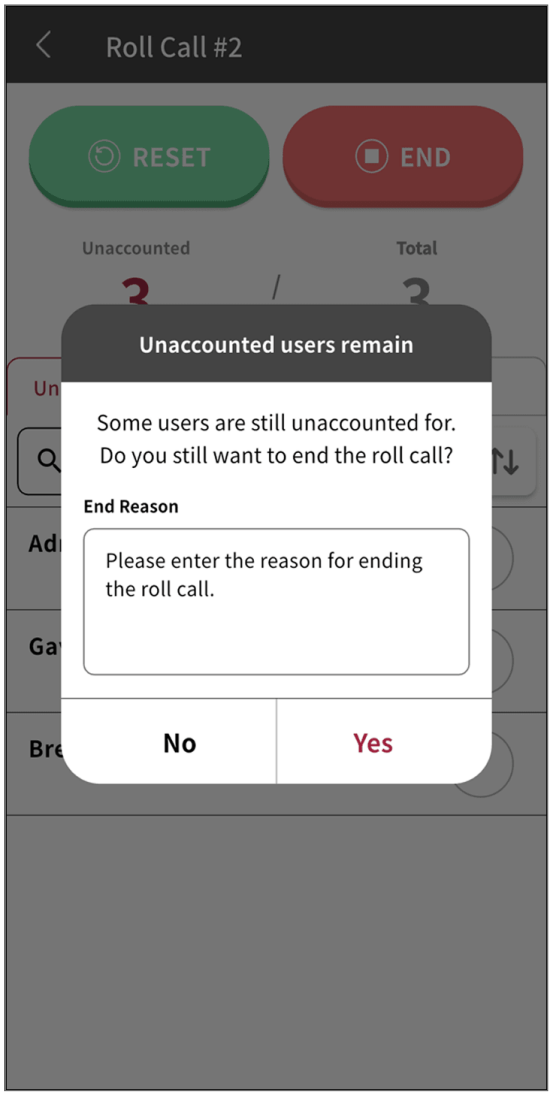
モバイルアプリで終了

1. 出席確認を終了するには、出席確認リスト画面で ⏹ ボタンをタップするか、出席確認状況画面で **END** ボタンをタップします。



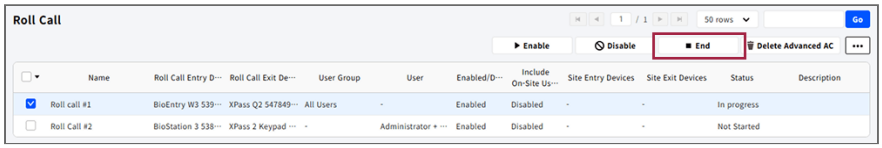


2. 未確認のユーザーが残っている場合、システムが警告ポップアップを表示します。出席確認を終了するには、終了理由を入力し、**Yes** ボタンをタップします。



Webで終了

1. **Launcher**ページで**Settings**をクリックします。
2. 画面左のサイドバーで **Access Management** → **Advanced AC**をクリックしてください。
3. 一覧で **Roll Call** をクリックします。
4. 出席確認リストで、終了する出席確認のチェックボックスをクリックします。



5. 画面右上の**End**ボタンをクリックしてください。
6. 確認メッセージが表示されたら、**Yes** ボタンをクリックします。

未確認のユーザーがいない出席確認は、すぐに終了します。未確認のユーザーが残っている出席確認では、**Unaccounted Users** リストと **End Reason** 入力欄があるダイアログが表示されます。出席確認を終了するには、理由を入力し、**End Roll Call** ボタンをクリックしてください。



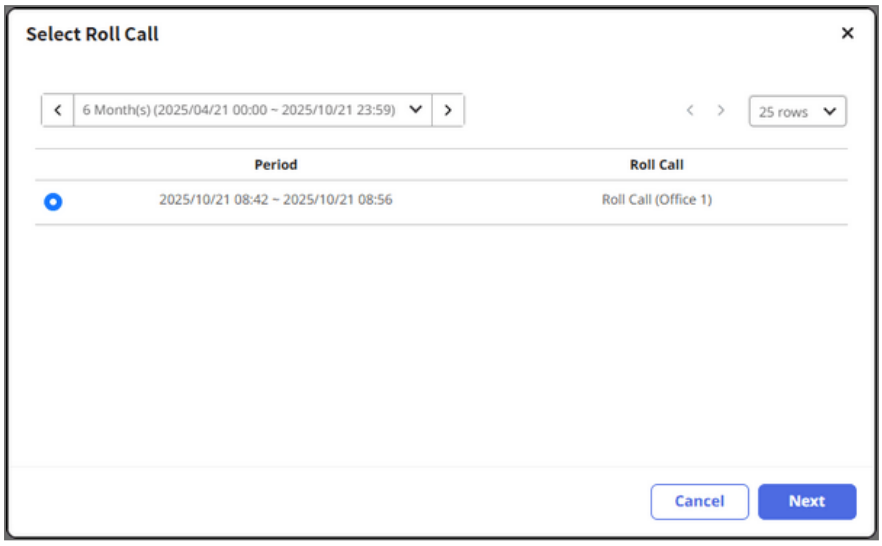
情報

- **End Reason**：最大 500 文字まで入力できます。
- 複数の出席確認項目を同時に選択して終了する場合、いずれかに未確認のユーザーが残っていると終了できません。出席確認項目を個別に選択して終了してください。

出席確認レポートを確認

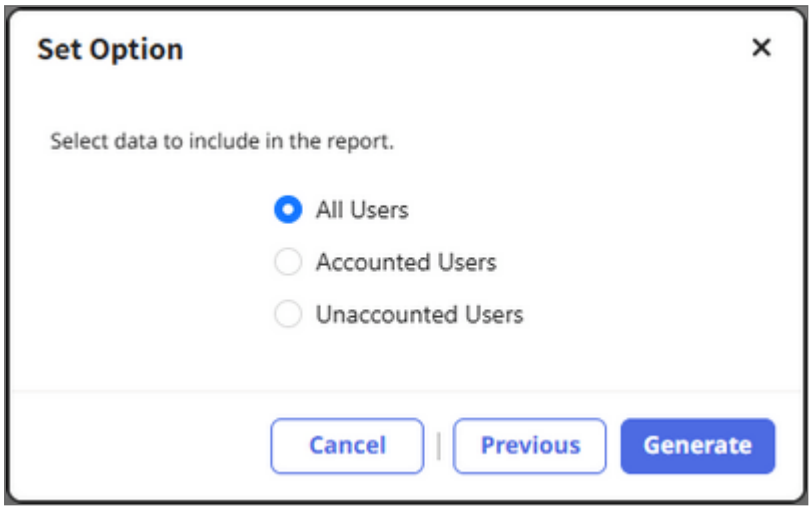
出席確認レポートを確認するには、次の手順に従ってください。

1. **Launcher** ページで **Data** をクリックしてください。
2. 画面左のサイドバーで **Events** → **Roll Call** をクリックしてください。
3. **Select Roll Call** ウィンドウが表示されたら、レポートで確認する出席確認項目を選択し、**Next** ボタンをクリックしてください。

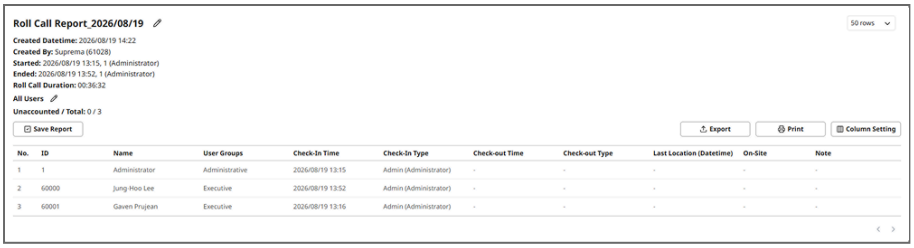


> 目的の出席確認項目が表示されない場合は、画面上部の期間を調整してください。

4. オプション設定ウィンドウでレポートに含めるデータを選択し、**Generate** ボタンをクリックしてください。

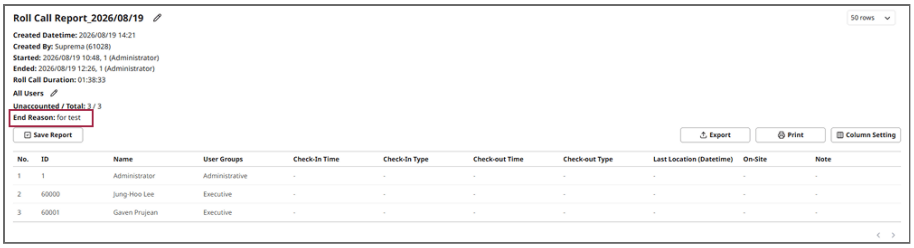


レポートを生成します。レポートでは、各ユーザーの情報や入室時間、退室時間、最後の場所、メモ内容などを確認できます。



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。

未確認のユーザーが残っている出席確認レポートでは、**End Reason**を確認できます。



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。

ビデオ設定

BioStar X のビデオ設定機能により、入退室管理と映像セキュリティを統合管理できます。**Video Management System**（VMS）と連携し、リアルタイム映像モニタリング、イベント連動録画、自動ブックマーク生成などの強力なセキュリティ管理機能を利用します。

> **情報**
>
> ビデオ設定機能は **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。

ビデオ設定の概要

ビデオ設定は次の 3 段階で構成されます。

1 VMS サーバーを連携する

VMS サーバーと **BioStar X** の接続を設定し、証明書を構成します。統合ビデオセキュリティ管理システムを構築するための必須ステップです。詳細については、VMS と連携するをご参照ください。

2 カメラを設定する

VMS に接続されているカメラの中から必要なカメラを選択し、効率的な管理のためにグループを構成します。詳細については、カメラを設定するをご参照ください。

3 ルールを設定する

入退室イベントと映像を連携するルールを作成し、自動ブックマークやイベント記録などの高度な機能を活用します。詳しくはビデオルールを設定するをご覧ください。

主な機能

- **統合モニタリング**：入退室管理と映像セキュリティを単一インターフェースで管理できます。
- **自動イベント記録**：入退室イベント発生時に関連映像を自動で記録し、タグを生成します。
- **効率的な検索**：ブックマークとイベントタグによる素早い映像検索と証拠収集が可能です。
- **リアルタイム対応**：セキュリティ事象発生時に関連カメラ映像を即時に確認できます。

VMS と連携する

Video Management System (VMS) は、複数のカメラ映像を統合管理し、録画と再生を行う映像管理システムです。 BioStar X と VMS を連携すると、入退室制御と映像セキュリティを 1 つのプラットフォームで統合管理できます。

VMSと連携すると、以下の機能が利用できます。

- **リアルタイムモニタリング**：出入口に接続されたカメラのライブ映像を確認できます。
- **統合イベント管理**：入退室イベントと映像を関連付けてセキュリティ状況を把握できます。
- **効率的な証拠収集**：特定の時点の録画映像を迅速に検索して再生できます。
- **ブックマーク機能**：重要なイベント時点に映像タグを追加し、簡単に検索および確認できます。

開始する前に

Video Management System (VMS) と連携する前に、次の項目を確認してください。

- VMS 連携機能は **エセンシャル** (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。
- VMS サーバーが正しくインストールおよび構成されていることを確認してください。 VMS サーバーが **BioStar X** とオンライ

ンで接続できる状態である必要があります。

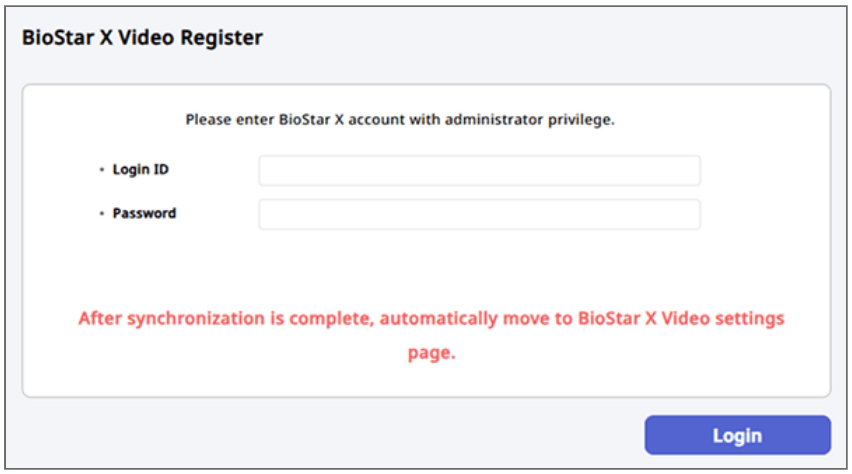
- **BioStar X** と互換性のある VMS を使用してください。 BioStar X VMS または **Nx Witness v5.1.5**、**v6.x.x** 系列の VMS を利用できます。
- VMS サーバーの IP アドレス、ポート番号、管理者アカウント情報を準備してください。これらの情報は **BioStar X** が VMS サーバーに接続する際に必要です。

VMS サーバー連携設定

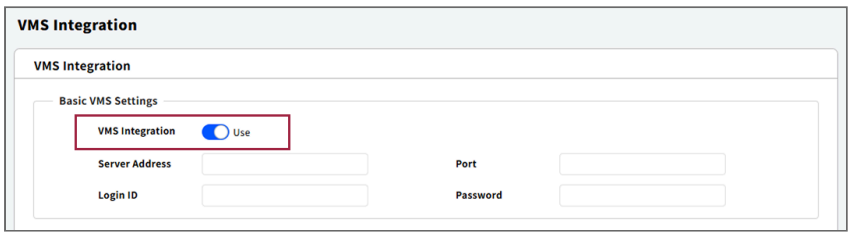
VMS サーバーと **BioStar X** を連携するには、次の手順に従ってください。

1 VMS 連携を有効化する

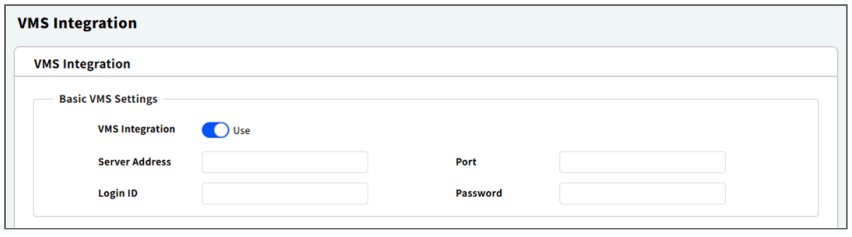
1. **Launcher**ページで**Settings**をクリックします。
2. 画面左のサイドバーで **Video** → **VMS Integration** をクリックしてください。
3. 初めてアクセスする場合は **BioStar X** の管理者アカウントでログインする必要があります。



4. **VMS Integration** オプションを **Use** に設定してください。



5. VMS サーバー情報を入力してください。



- **Server Address**：VMS サーバーの IP アドレスを入力してください。

- **Port**：VMS サーバーのポート番号を入力してください。
- **Login ID**：VMS サーバーの管理者アカウント ID を入力してください。
- **Password**：VMS サーバーの管理者アカウントのパスワードを入力してください。

6. VMS サーバー情報をすべて入力したら、画面右下の **Apply** ボタンをクリックしてください。

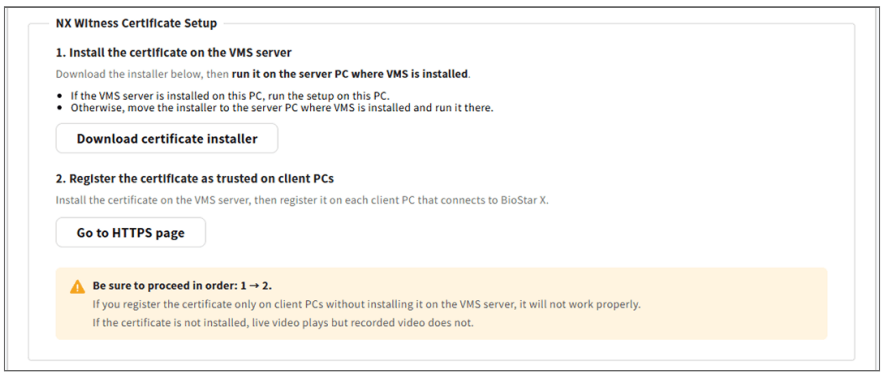
> **情報**
>
> - VMS サーバーとの連携に失敗してエラーメッセージが表示された場合は、サーバーアドレスや管理者アカウント情報などを再確認してください。 VMS サーバーがオンライン状態にあるか、ファイアウォール設定によってネットワーク接続がブロックされていないかを確認することも必要です。
> - **VMS Event/Bookmark** セクションの設定の詳細については、VMS イベントとブックマークの設定 を参照してください。

2 VMS サーバーに証明書をインストールする

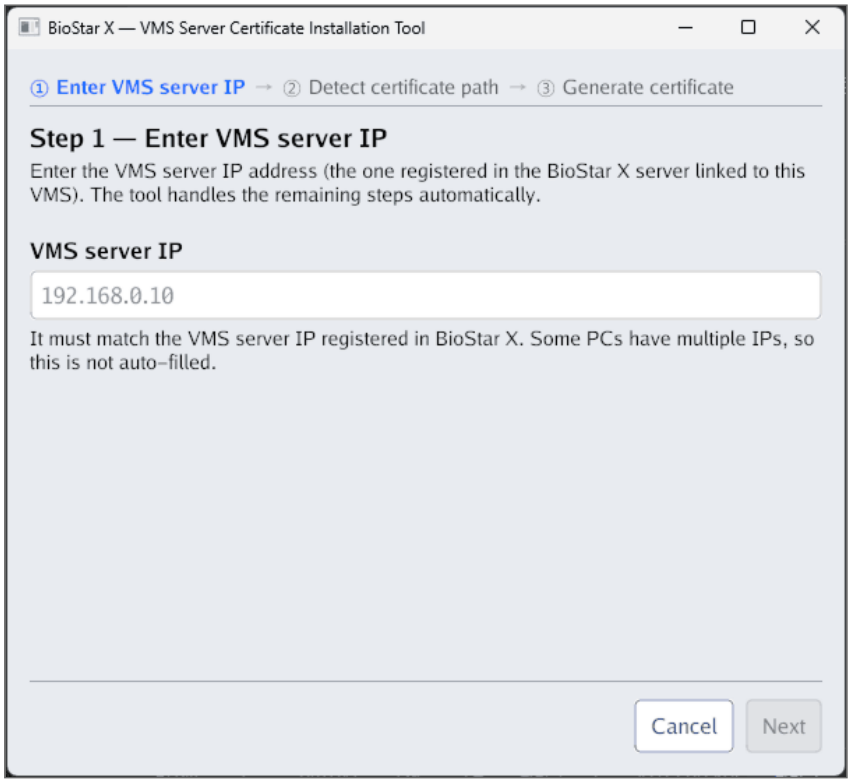
VMS サーバーの録画映像を再生するには、HTTPS プロトコルを使用する必要があります。一般的なSSL証明書はドメイン名を基に発行されるため、VMSサーバーにIPアドレスでアクセスする環境では有効ではありません。そのため、VMSサーバーのIPアドレスを含む証明書を別途作成する必要があります。

> **情報**
>
> VMSサーバーと **BioStar X** を同じサーバーにインストールする場合でも、別々のサーバーにインストールする場合でも、証明書をインストールする必要があります。

VMS Integration オプションを **Use** に設定すると、**NX Witness Certificate Setup** セクションが有効になります。

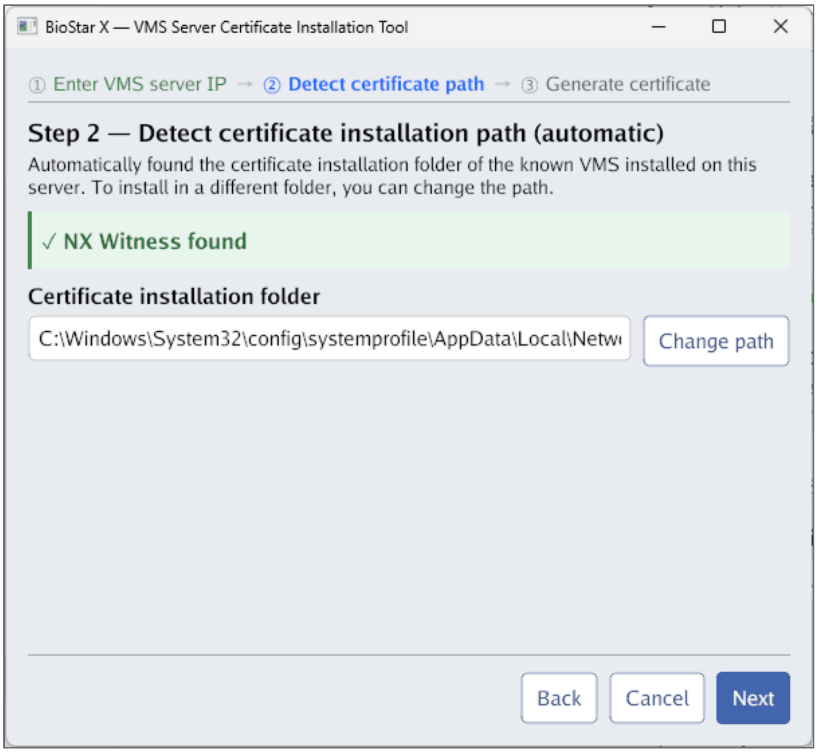


1. 証明書インストーラをダウンロードするには、VMS がインストールされたサーバーで **Download certificate installer** ボタンをクリックしてください。
2. ダウンロードした *vmsCertMaker.exe* ファイルを実行してください。
3. **VMS server IP** 入力フィールドに IP アドレスを入力してください。

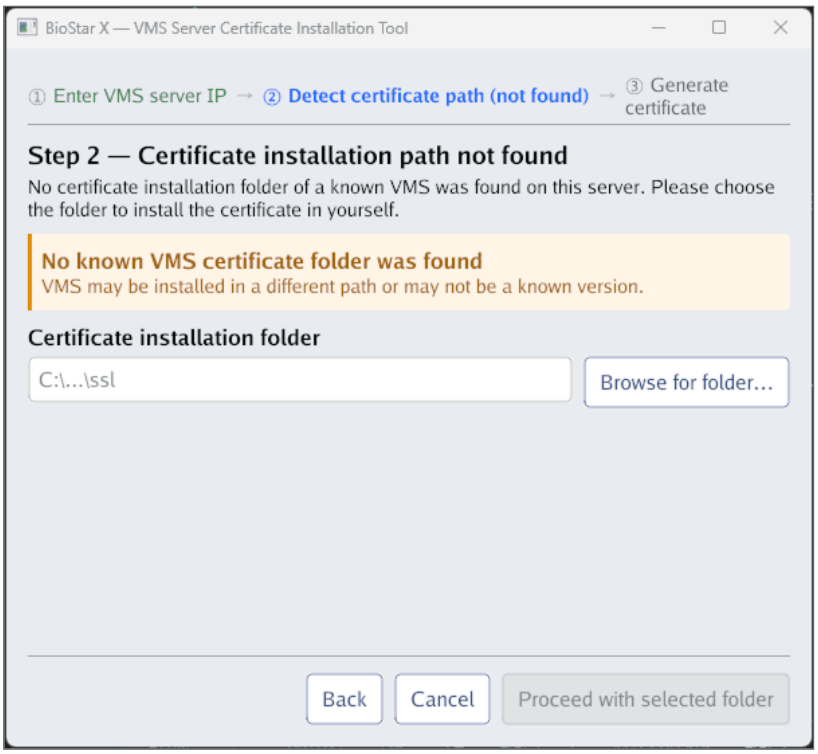


> IPv4 アドレス形式で入力してください。例: 192.168.0.10

4. 正しい形式の IP アドレスを入力すると、**Next** ボタンが有効になります。 **Next** ボタンをクリックします。
5. VMS の証明書インストール先を選択してください。
   - 互換性のある VMS では、インストール先を自動で検出します。

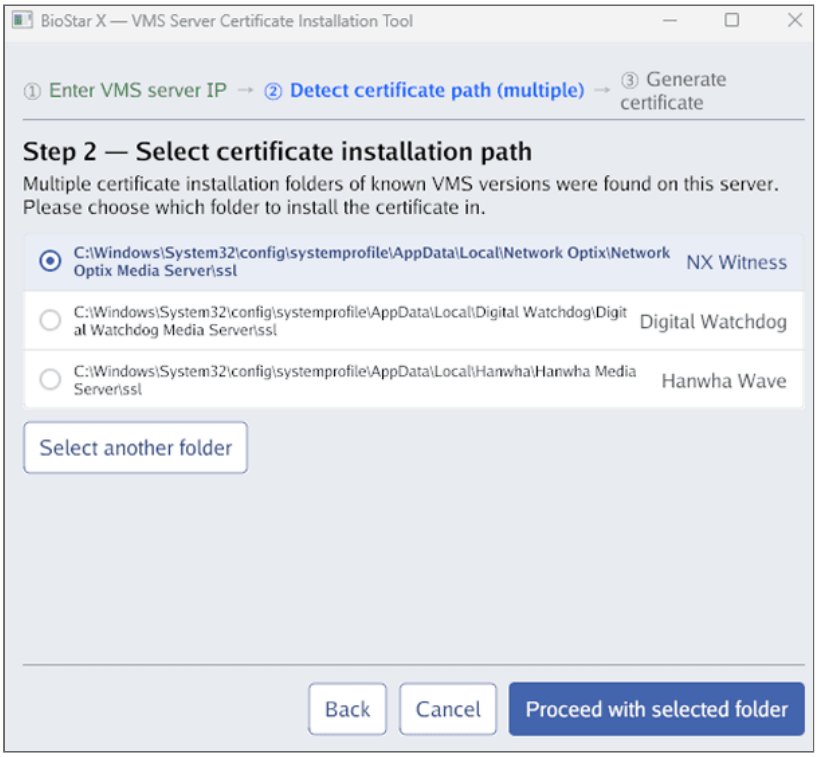


- インストール先を自動検出できない場合は、**Browse for folder** ボタンをクリックし、証明書インストール先を手動で選択してください。



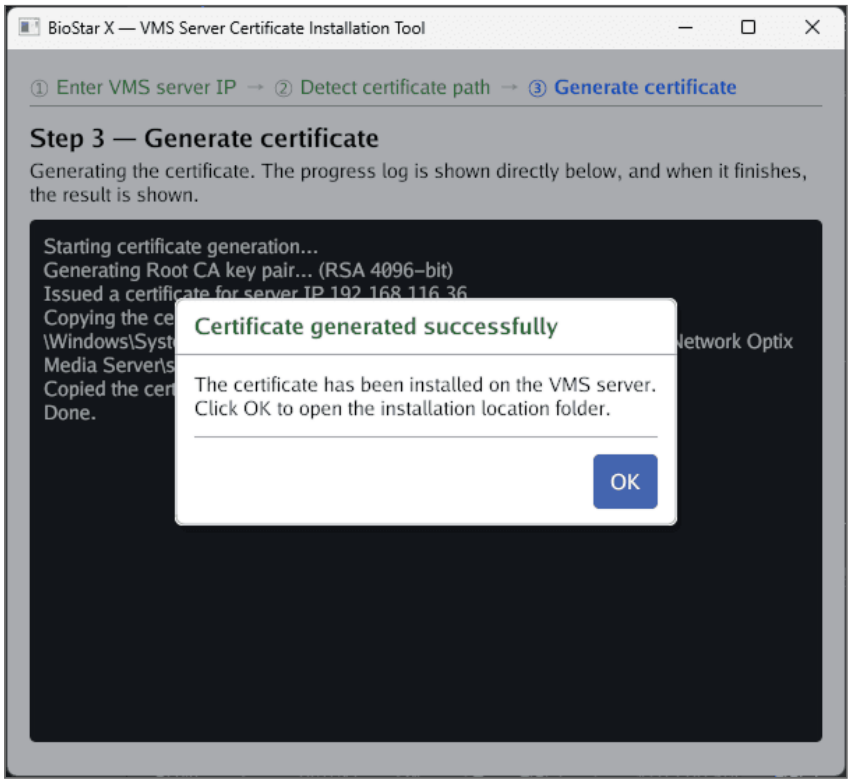
> 使用する VMS によって、証明書のインストール先が異なる場合があります。下記の例をご参照ください。
>
> - **BioStar 2 VMS**：*C:\Windows\System32\config\systemprofile\AppData\Local\Suprema Inc\Suprema Inc. Media Server\ssl*
> - **Digital Watchdog**：*C:\Windows\System32\config\systemprofile\AppData\Local\Digital Watchdog\Digital Watchdog Media Server\ssl*
> - **Hanwha Wave**：*C:\Windows\System32\config\systemprofile\AppData\Local\Hanwha\Hanwha Media Server\ssl*
> - **NX**：*C:\Windows\System32\config\systemprofile\AppData\Local\Network Optix\Network Optix Media Server\ssl*

- VMS 証明書のパスが複数ある場合、すべてのパスが表示されます。 **Select another folder** ボタンをクリックし、目的のパスを選択してください。



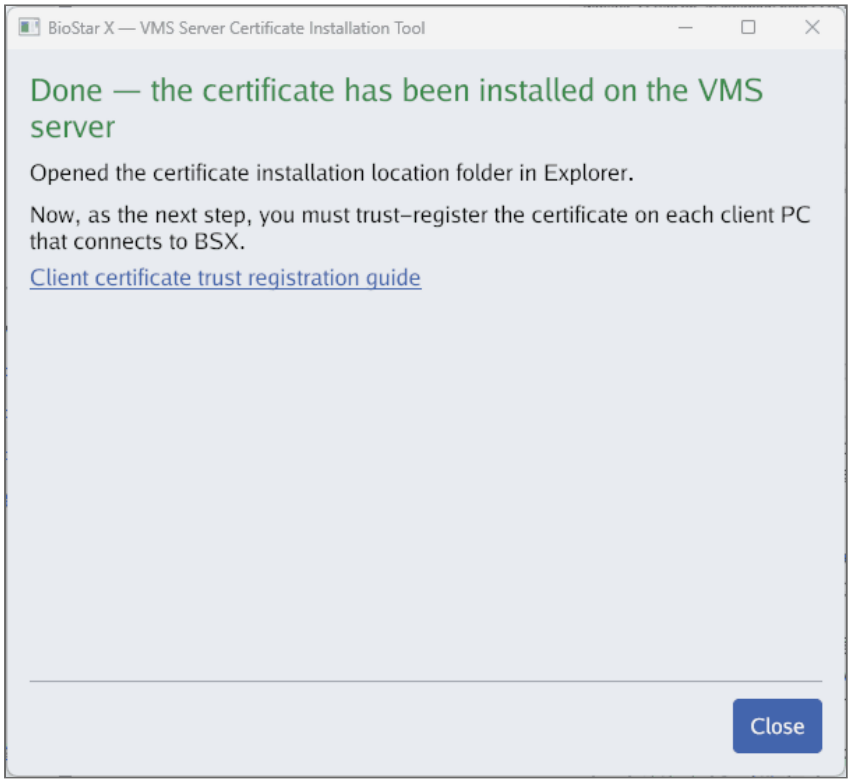
6. **Next** または **Proceed with selected folder** ボタンをクリックしてください。

7. 証明書の生成が完了すると、**Certificate generated successfully** メッセージウィンドウが表示されます。



8. **OK** ボタンをクリックすると、証明書をインストールしたパスが表示されます。証明書ファイル(*cert.pem*)が生成されたことを確認してください。

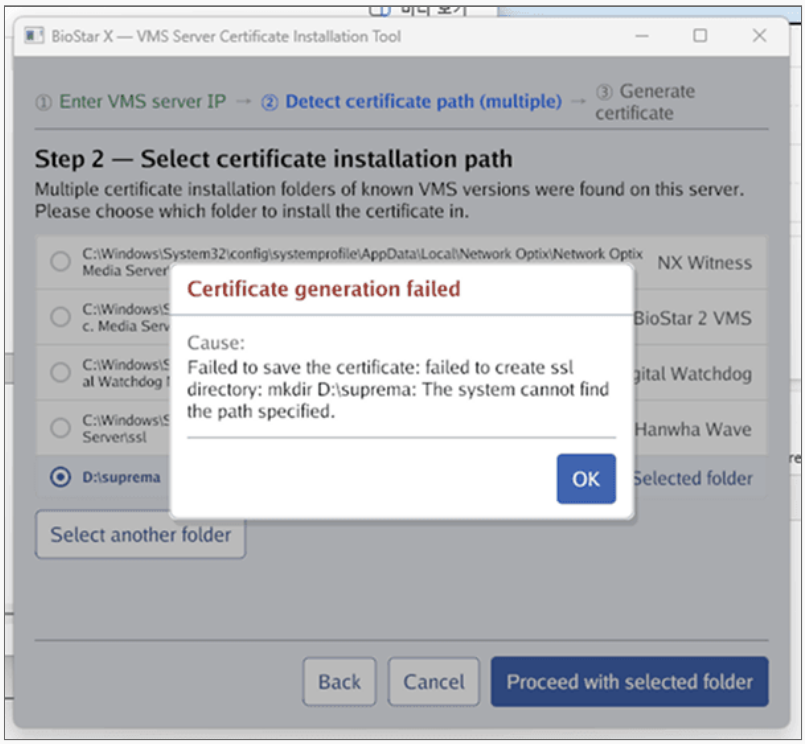
9. 証明書のインストールが完了したら、**Close** ボタンをクリックしてください。



10. VMS サーバーを再起動してください。

情報

証明書のインストールに失敗すると、失敗理由がメッセージに表示されます。メッセージの内容を確認し、必要な対応を行ってください。



3 クライアント PC に証明書をインストールする

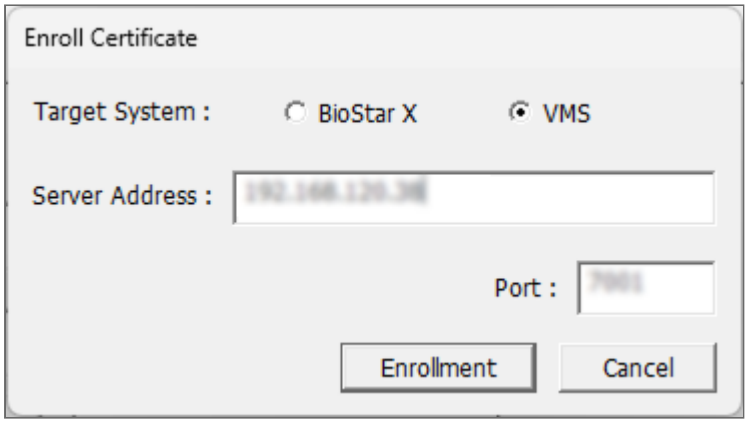
次のような状況が発生した場合、VMS サーバーにインストールされている証明書をクライアント PC にインストールして問題を解決できます。

- ブラウザーで **Video Management System** (VMS) にアクセスした際に「安全ではありません」と警告が表示される場合
- **Monitoring** ページでライブ映像は再生されるが録画映像が再生されない場合

> **注意**
> VMS サーバーに証明書をインストールせず、クライアント PC のみに登録すると、正常に動作しません。

---

1. ウェブブラウザーで **BioStar X** にアクセスします。
2. ログイン画面、または **Settings** → **System** → **HTTPS** から HTTPS 証明書インストーラ (*cert-register.zip*) をダウンロードしてください。
3. ダウンロードしたファイルを解凍し、*cert-register.exe* ファイルを実行します。 **Enroll Certificate** ウィンドウが表示されます。
4. **Target System** で **VMS** を選択し、次の情報を入力します。



   - **Server Address**：VMS サーバーの IP アドレス
   - **Port**：VMS サーバーのポート番号（デフォルト：7001）
5. **Enrollment** ボタンをクリックします。
6. セキュリティ警告メッセージを確認し、**はい** をクリックします。

Web ブラウザーを再起動し、**Monitoring** ページで VMS サーバーの録画映像が正常に再生されるか確認します。

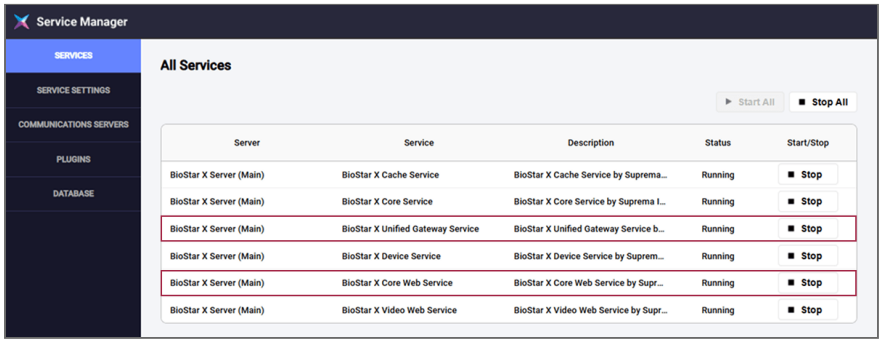
4 カメラの確認と設定

VMS サーバーと正常に連携できた場合、**Video** → **Video** メニューで接続されているカメラを確認できます。詳細については、カメラを設定するをご参照ください。

トラブルシューティング

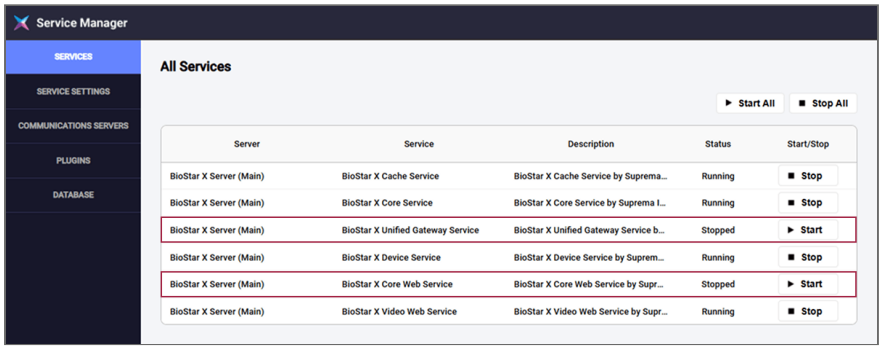
VMSサーバーと初回連携後に正常に動作しない場合は、次の手順に従って手動でサービスを再起動してください。

1. Windows で 開始 → **BioStar X** → **BioStar X Service Manager** をクリックします。
2. **All Services** リストで下記サービスの **Stop** ボタンをクリックしてサービスを停止してください。



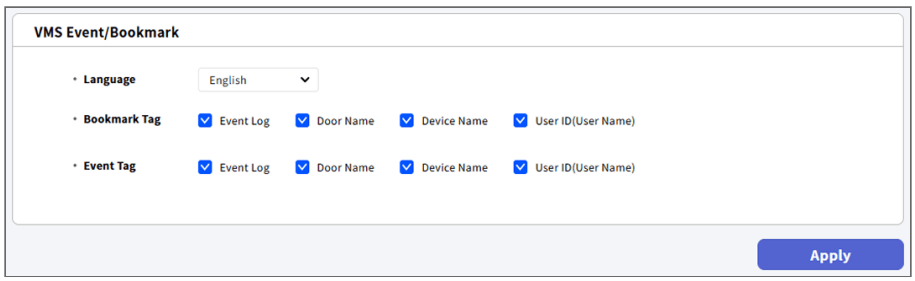
- **BioStar X Unified Gateway Service**
- **BioStar X Core Web Service**

3. 停止を要求したサービスの状態が **Pending** から **Stopped** に変わったら、**Start** ボタンをクリックしてサービスを再起動してください。



VMS イベントとブックマークの設定

連携したVMSサーバーにブックマークタグとイベントタグの情報を送信できます。このとき、イベントログ、ドア名、デバイス名、ユーザーIDも併せて送信するかどうかを選択できます。必要なオプションを選択し、画面右下の **Apply** をクリックしてください。



- **Language**：VMSサーバーに送信するイベントタグおよびブックマークタグの言語を選択します。韓国語または英語を選択できます。
- **Bookmark Tag**：ブックマークタグは、VMSサーバーに保存された映像にラベルと名前を付け、簡単に検索・確認できる機能です。ブックマークタグで送信する情報を選択します。
- **Event Tag**：ある時点で発生したイベントをVMSサーバーに送信して記録できます。イベントタグで送信する情報を選択しま

す。

情報

- VMSのブックマーク機能の詳細は次のリンクを参照してください。
- VMSのイベント機能の詳細は次のリンクを参照してください。
- ブックマークタグとイベントタグに次の文字が含まれている場合、VMS サーバーに送信する際に自動的に削除されます。
  - イベントタグ：`\` `'` `,` `#` `%` `=` `&` `<` `>`
  - ブックマークタグ：`<` `'`

VMSサーバー連携の解除

連携したVMSサーバーとの接続を解除するには、次の手順に従ってください。 VMS連携を解除すると、ビデオ設定、登録済みカメラ、ルールがすべて削除されます。

1. **Launcher**ページで**Settings**をクリックします。
2. 画面左のサイドバーで **Video** → **VMS Integration** をクリックしてください。
3. **VMS Integration** オプションを **Not Use** に設定します。
4. 画面右下の **Apply** をクリックしてください。
5. メッセージウィンドウの内容を確認し、**Yes** をクリックしてください。

カメラを設定する

VMS連携を完了した後、BioStar Xで使用するカメラを選択して設定します。適切なカメラ設定により、次のセキュリティ管理機能を利用できます。

- **選択的モニタリング**：VMSのすべてのカメラの中から必要なカメラだけを**BioStar X**に追加できます。
- **効率的な管理**：カメラをグループ別に構成し、場所や用途に応じて体系的に管理できます。

情報

- VMSサーバーとの連携方法については、VMS と連携するをご参照ください。
- カメラを追加したりグループを作成したりするには、カメラグループの権限が必要です。カメラグループの権限設定の詳細については、カメラグループの権限設定をご参照ください。

カメラの設定と管理

VMS連携後、**Settings** → **Video** → **Video** メニューでカメラを設定および管理できます。

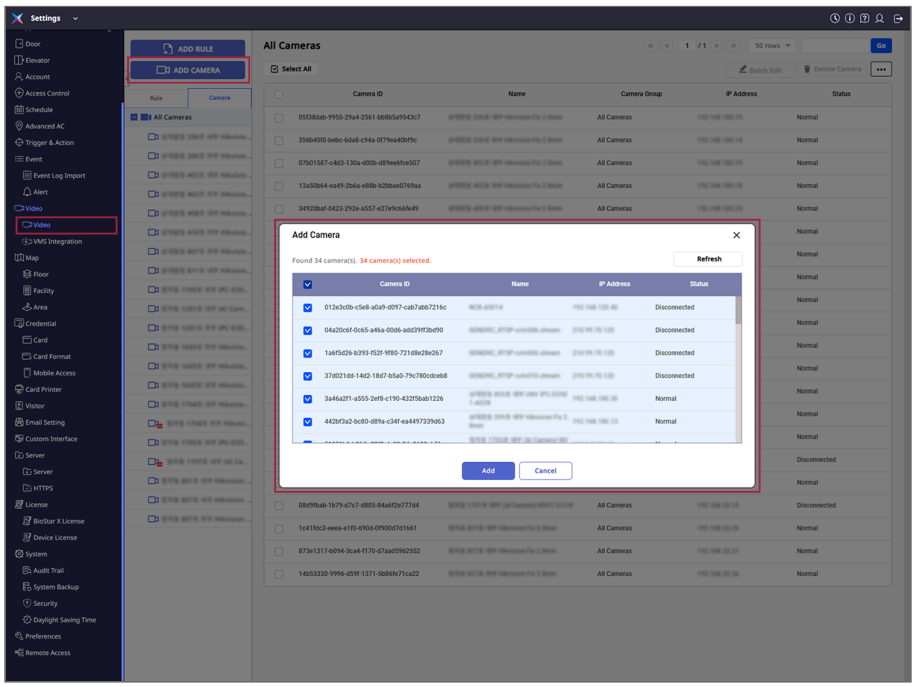
カメラの追加

VMSと連携している場合、VMSサーバーに接続されたカメラを**BioStar X**に追加し、**Monitoring** ページでライブ映像と録画映像を再生できます。

1. **Launcher**ページで**Settings**をクリックします。
2. 画面左のサイドバーで **Video** → **Video** をクリックします。
3. **ADD CAMERA** ボタンをクリックします。
4. **Add Camera** ウィンドウが表示されたら、一覧から除外するカメラを選択します。

   目的のカメラが表示されない場合は、**Refresh** ボタンをクリックしてカメラ一覧を更新します。
5. カメラをすべて選択したら、画面右下の**Add** ボタンをクリックします。

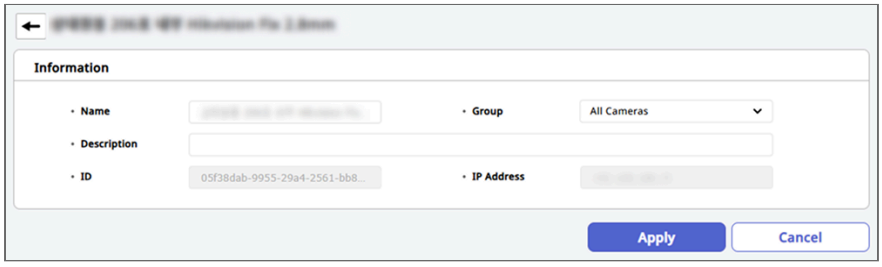
カメラ一覧で追加したカメラを確認できます。



カメラ情報の編集

追加したカメラの情報を編集できます。カメラ名、グループ、説明などを変更できます。

1. **Launcher**ページで**Settings**をクリックします。
2. 画面左のサイドバーで **Video** → **Video** をクリックします。
3. 画面左上の**Camera** タブをクリックします。
4. 一覧から編集するカメラをクリックします。
5. カメラ情報が表示されたら、必要な項目を編集します。



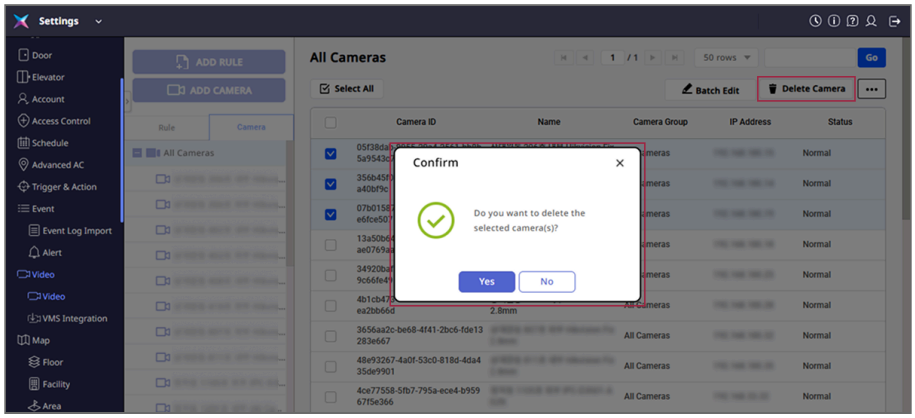
6. 編集が完了したら、画面右下の**Apply** ボタンをクリックします。

> **情報**
> カメラIDとIPアドレスは編集できません。

カメラの削除

追加したカメラを削除できます。

1. **Launcher**ページで**Settings**をクリックします。
2. 画面左のサイドバーで **Video** → **Video** をクリックします。
3. 一覧で削除するカメラの左端にあるチェックボックスをクリックします。 1台以上のカメラを選択できます。
4. 画面右上の **Delete Camera** ボタンをクリックします。
5. メッセージを確認し、**Yes** ボタンをクリックします。



> **情報**
> 削除対象のカメラがいずれかのルールに含まれている場合、カメラを削除できません。そのカメラをルールから削除してから再試行します。ルールの作成および管理の詳細については、ビデオルールを設定するをご参照ください。

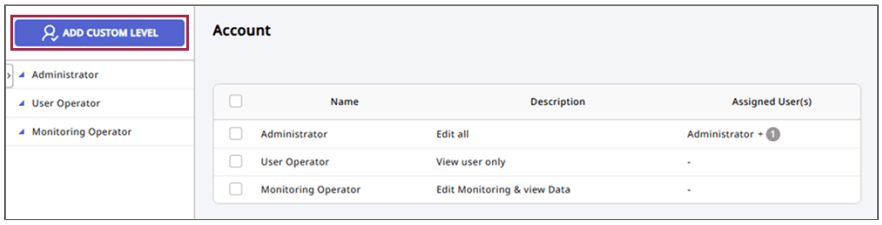
カメラグループの設定と管理

複数のカメラをグループ化して、場所や用途に応じて体系的に管理できます。カメラグループの作成と管理の手順は以下のとおりです。

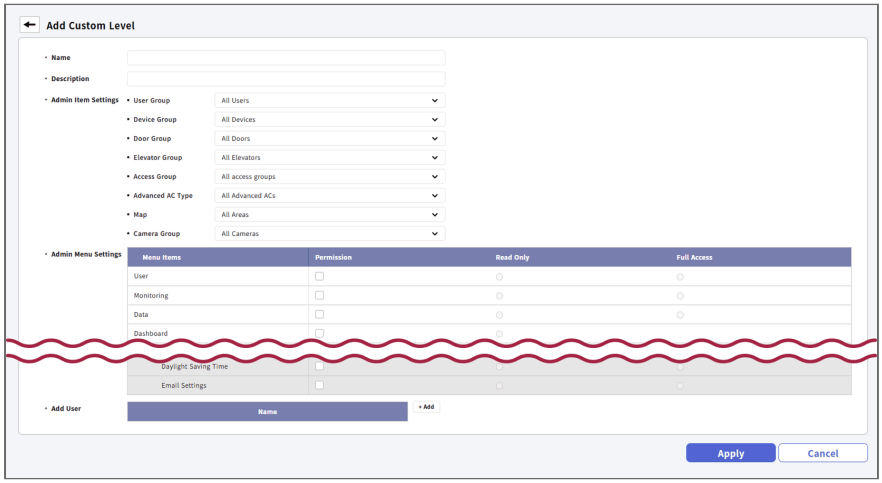
カメラグループの権限設定

管理者がカメラを追加したりグループを作成したりするには、カメラグループの権限が必要です。全体管理者、ユーザー管理者、監視管理者はすべてのカメラグループに対する権限を持っています。個別の権限設定が必要な場合は、カスタム権限を追加して、カメラグループの権限を設定できます。

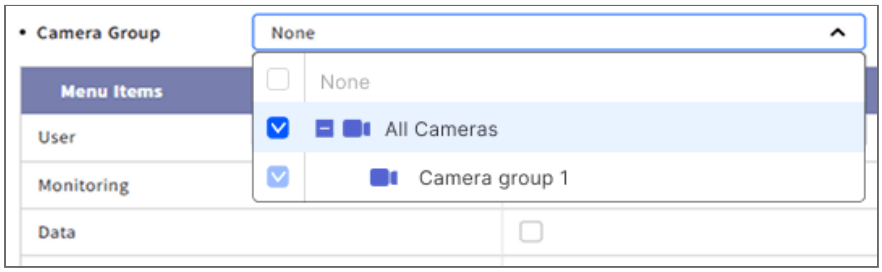
1. **Launcher**ページで**Settings**をクリックします。
2. 画面左のサイドバーで **Account** → **Account** をクリックします。
3. **Add Custom Level** をクリックします。



4. 新しく作成する権限の名前と説明を入力します。



5. **Admin Item Settings** の **Camera Group** 項目で権限を割り当てるカメラグループを選択します。



   - すべてのカメラグループに対する権限を付与するには、**All Cameras** を選択します。
   - 個別のカメラグループに対して権限を付与するには、カメラグループ一覧から目的のグループを選択します。一つ以上のグループを選択できます。

6. **Add User** で **+ Add** ボタンをクリックし、権限を付与するユーザーを選択します。
7. 設定を保存するには、画面最下部の **Apply** をクリックします。

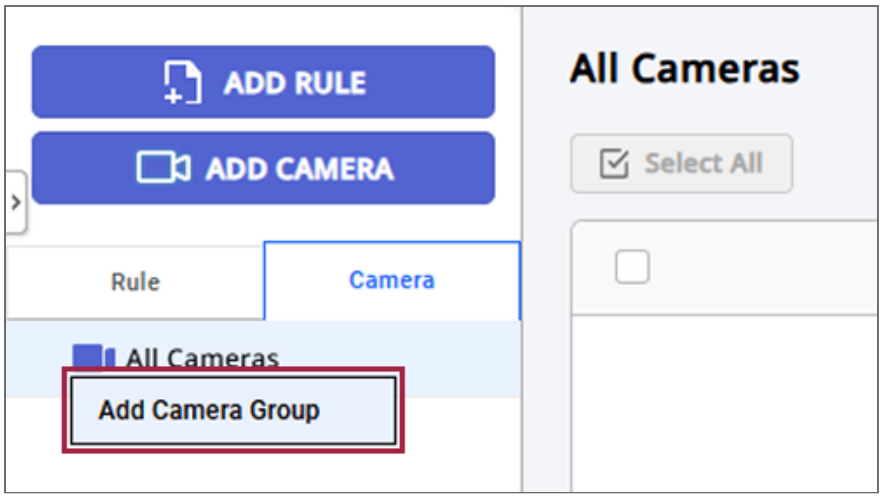
> **情報**
> 特定のカメラグループに対する権限がない場合、そのグループに属するカメラを閲覧できません。

カメラグループの追加

カメラグループを追加し、複数のカメラをグループ化して管理できます。

1. **Launcher**ページで**Settings**をクリックします。
2. 画面左のサイドバーで **Video** → **Video** をクリックします。
3. 画面左上の**Camera** タブをクリックします。

4. **All Cameras** 項目を選択し、右クリックします。



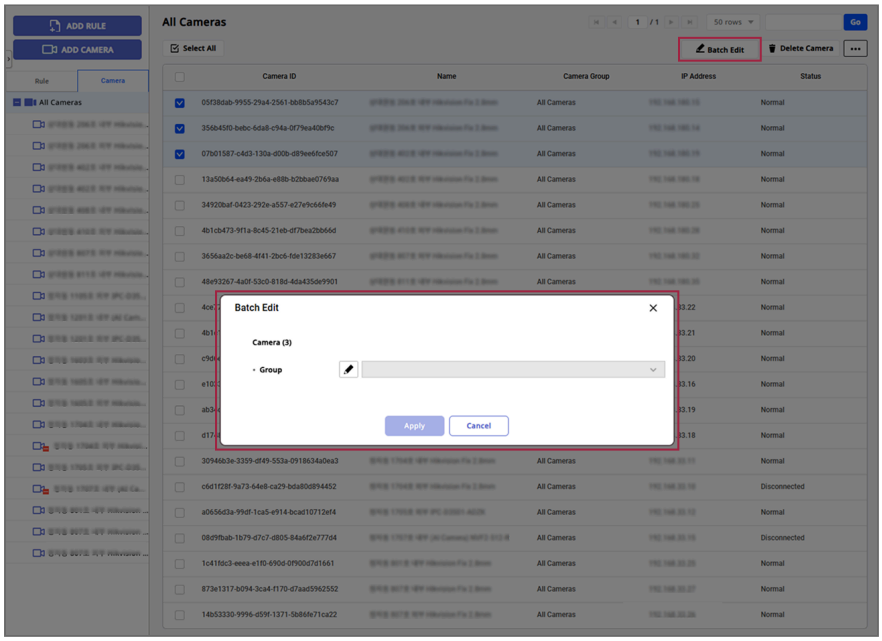
5. ポップアップメニューで**Add Camera Group** をクリックします。
6. 希望するグループ名を入力し、`Enter` キーを押します。

> **情報**
>
> - カメラグループは8階層までのサブグループを作成できます。
> - カメラグループ名は最大48文字まで入力できます。
> - カメラ一覧でグループを選択すると、そのグループに属するカメラだけが表示されます。

グループへの複数カメラの追加

作成したグループに1台以上のカメラを追加できます。

1. **Launcher**ページで**Settings**をクリックします。
2. 画面左のサイドバーで **Video** → **Video** をクリックします。
3. 一覧でグループに追加するカメラの左端にあるチェックボックスをクリックします。 1台以上のカメラを選択できます。
4. 1台以上を選択すると、画面右上の **Batch Edit** ボタンが有効になります。 **Batch Edit** ボタンをクリックします。



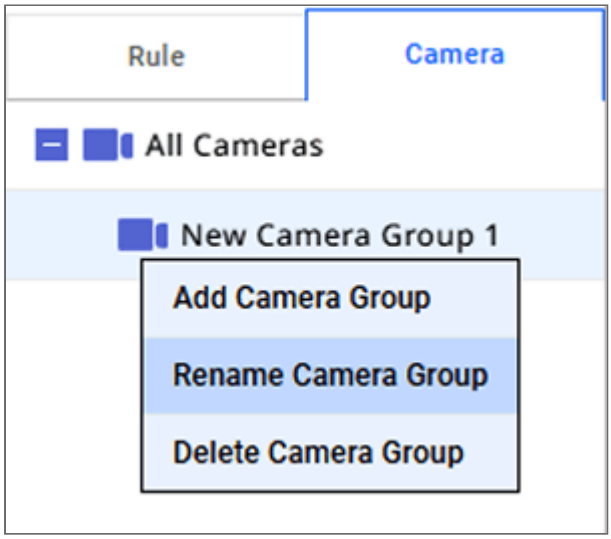
5. **Batch Edit** ウィンドウが表示されたら、**Group** 項目の ✎ ボタンをクリックします。
6. グループ一覧から目的のグループを選択します。
7. **Apply** ボタンをクリックします。

> **情報**
> **Camera** タブの一覧から項目を選択し、ドラッグ＆ドロップでもカメラをグループに追加できます。



カメラグループ名の編集

1. **Launcher**ページで**Settings**をクリックします。
2. 画面左のサイドバーで **Video** → **Video** をクリックします。
3. **Camera** タブをクリックします。
4. 名前を変更するグループを選択し、右クリックします。
5. ポップアップメニューで**Rename Camera Group** をクリックします。



6. 希望するグループ名を入力し、Enter キーを押します。

カメラグループの削除

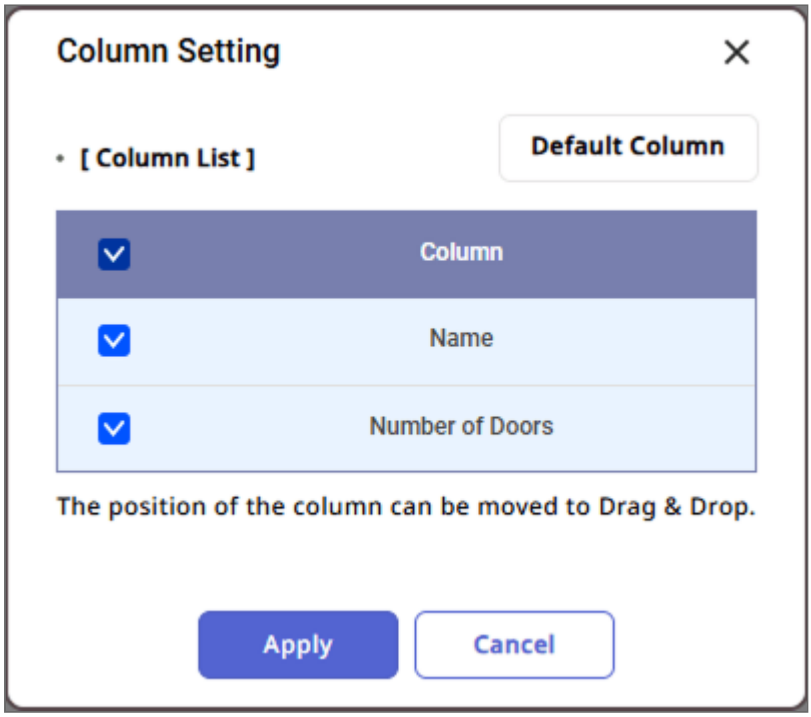
1. **Launcher**ページで**Settings**をクリックします。
2. 画面左のサイドバーで **Video** → **Video** をクリックします。
3. **Camera** タブをクリックします。
4. 名前を変更するグループを選択し、右クリックします。
5. ポップアップメニューで**Delete Camera Group** をクリックします。
6. 警告メッセージを確認し、**Yes** ボタンをクリックします。

> **情報**
> カメラグループにカメラが含まれている場合、グループを削除できません。グループ内のカメラを別のグループへ移動するか、グループから削除してから再試行します。

リスト列を設定する

リストで表示する列を追加、順序を変更、または非表示に設定できます。

1. **Launcher**ページで**Settings**をクリックします。
2. 画面左のサイドバーで **Video** → **Video** をクリックします。
3. **All Cameras** リストの右上で••• → **Column Setting** をクリックします。
4. **Column Setting** ウィンドウが表示されたら、表示する列のチェックボックスをクリックして追加または非表示設定ができます。ドラッグ＆ドロップで列の順序を変更することもできます。



5. 列設定をすべて変更したら、**Ok** ボタンをクリックします。

> **情報**
> 列設定を初期化するには、**Default Column** をクリックします。

ビデオルールを設定する

ルールは、カメラとドアで発生したイベントを組み合わせ、VMSサーバーにイベントおよびブックマーク形式で送信するための設定です。適切にビデオルールを設定することで、次のようなセキュリティ管理機能を活用できます。

- **自動ブックマーク生成**：特定の入退室イベントが発生した際に自動でブックマークを作成し、重要な映像を簡単に検索できます。
- **効率的なモニタリング**：ドアに接続されたカメラ映像をリアルタイムで監視し、イベント発生時に即座に確認できます。
- **統合イベント管理**：入退室イベントと映像を連携し、セキュリティ状況を総合的に把握できます。

> **情報**
> - ビデオルール機能は、**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。
> - 出入口のドアとカメラを連携する際には、そのカメラが所属するグループの権限が必要です。カメラグループの権限設定の詳細については カメラを設定するご参照ください。

ルール追加

1. **Launcher**ページで**Settings**をクリックします。
2. 画面左のサイドバーで **Video** → **Video** をクリックします。

3. 画面左上の **ADD RULE** ボタンをクリックします。

Add New Rule 画面が表示されたら、以下の案内に従ってルールを設定します。画面下部の **Apply** ボタンをクリックして、すべての設定を完了し保存します。

ルール情報の入力

Information セクションで、新しいルールの名前と説明を入力します。



> **情報**
> **Description** 項目は任意です。ルールの用途や特徴を把握しやすいように、簡単な説明を入力してください。

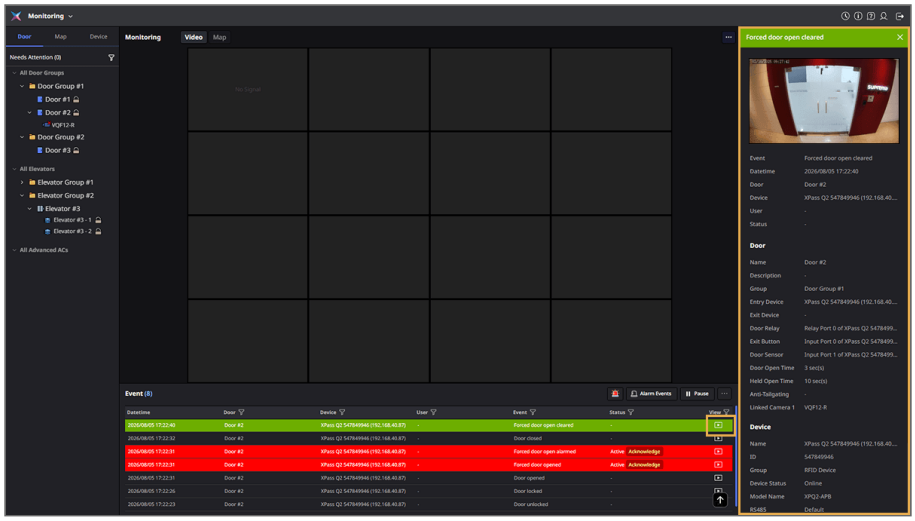
ビデオログ設定

Video Log は、特定のイベント発生前後の映像を自動で記録する機能です。イベント発生前後の状況を把握できるよう、指定した時間の映像を保存します。



- **Video Log**：現在のルールで Video Log 機能を使用するかどうかを設定します。
  - **Enabled**：イベント発生時に前後の映像を自動で記録します。
  - **Disabled**：Video Log 機能を無効にします。
- **Video Log Length**：イベント発生時刻を基準に、10秒前後の映像を記録する範囲を設定します。最大で60秒まで設定できます。

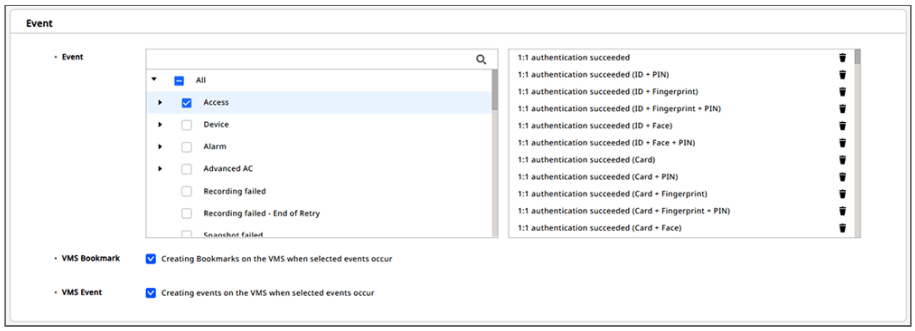
Video Log オプションを有効にすると、モニタリング画面のイベントパネルのイベント項目にビデオログ（▶）アイコンが表示されます。ビデオログアイコンが表示されたイベント項目をクリックすると、画面右側に詳細情報が表示されます。特定のイベントが発生した時刻の映像を確認できます。



> **情報**
>
> **Video Log Length** で設定した範囲が長いほど、多くの保存容量が必要になる場合があります。システム性能と保存容量を考慮して、適切な長さを設定してください。

VMSに記録するイベントの設定

Event セクションでは、VMSサーバーに記録するイベントを選択し、ブックマークまたはイベント送信の有無を設定できます。



- **Event**：VMSサーバーへ送信するイベントタイプを選択します。左側のイベントリストで目的のイベントを選択すると、右側のリストに追加されます。
- **VMS Bookmark**：イベントリストで選択したイベントが発生した際に、VMSサーバーにブックマークを作成するかどうかを設定できます。
- **VMS Event**：イベントリストで選択したイベントが発生した際に、VMSサーバーにイベント記録を作成するかどうかを設定できます。

> **情報**
>
> - イベントの選択は必須ではありません。
> - 左側のイベントリスト上部の検索フィールドを使用して、目的のイベントを素早く検索できます。
> - 右側のリストからイベントを削除するには、🗑 ボタンをクリックします。
> - ブックマークおよびイベントをVMSサーバーに送信する際、メッセージの言語を設定できます。詳しくはVMS と連携するをご参照ください。

ドアとカメラの連携

Door-Camera Linkage セクションでは、ドアとカメラを連携し、ドアでイベントが発生した際に接続されたカメラの映像と共にVMSサーバーへ送信できます。これにより、入退室イベントに関連する映像を容易に確認できます。



1. 右上の **+ Add** ボタンをクリックします。

2. **Add Linkage** ウィンドウが表示されたら、ドアを選択し、そのドアに関連付けるカメラを選択します。



3. ドアとカメラをすべて選択したら、**Add** ボタンをクリックします。

リストでドアに連携されたカメラを確認できます。



情報

- カメラグループの権限を持たない管理者は、特定のカメラグループに属するカメラを表示または選択できません。カメラグループの権限設定の詳細については カメラを設定するご参照ください。
- 1つのドアには最大4台のカメラを追加できます。
- 1つのルールに含まれたドアは、他のルールでは使用できません。
- カメラを複数のドアに制限なく連携でき、既に他のドアと連携されているカメラも再利用できます。
- ドアとカメラの連携ルールを削除するには、リストで削除したい項目のチェックボックスをクリックし、右上の **Delete** ボタンをクリックします。
- ドアと連携されたカメラは、**Monitoring** ページのドアリストでドアのサブツリーとして確認できます。詳しくは状態を確認をご参照ください。
- 画面下部の **Apply** ボタンをクリックして、すべての設定を完了し保存します。

ルールの編集

1. **Launcher**ページで**Settings**をクリックします。
2. 画面左のサイドバーで **Video** → **Video** をクリックします。
3. **All Rules** リストで編集したいルールをクリックします。
4. ルール編集画面が表示されたら、必要な項目を修正します。
5. 編集したルールを保存するには、画面右下の **Apply** ボタンをクリックします。

情報

ルール編集画面の各セクションの詳細についてはルール追加をご参照ください。

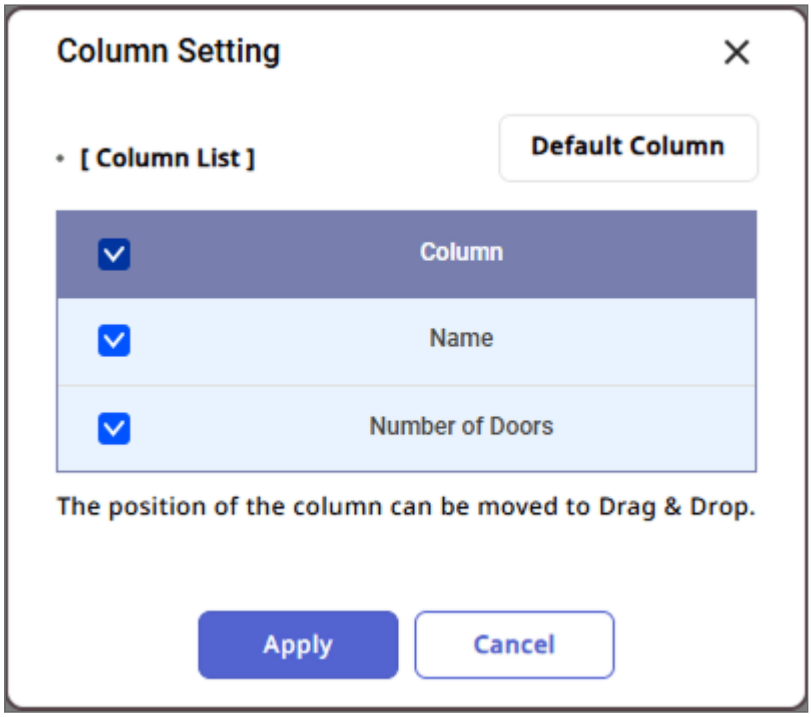
ルールの削除

1. **Launcher**ページで**Settings**をクリックします。
2. 画面左のサイドバーで **Video** → **Video** をクリックします。
3. **All Rules** リストで削除したいルールのチェックボックスをクリックします。 1つ以上のルールを選択できます。
4. 画面右上にある **Delete Rule** ボタンをクリックします。
5. メッセージを確認し、**Yes** ボタンをクリックします。

リスト列を設定する

リストで表示する列を追加、順序を変更、または非表示に設定できます。

1. **Launcher**ページで**Settings**をクリックします。
2. 画面左のサイドバーで **Video** → **Video** をクリックします。
3. **All Rules** リストの右上で ••• → **Column Setting** をクリックします。
4. **Column Setting** ウィンドウが表示されたら、表示する列のチェックボックスをクリックして追加または非表示設定ができます。ドラッグ＆ドロップで列の順序を変更することもできます。



5. 列設定をすべて変更したら、**Ok** ボタンをクリックします。

> **情報**
> 列設定を初期化するには、**Default Column** をクリックします。

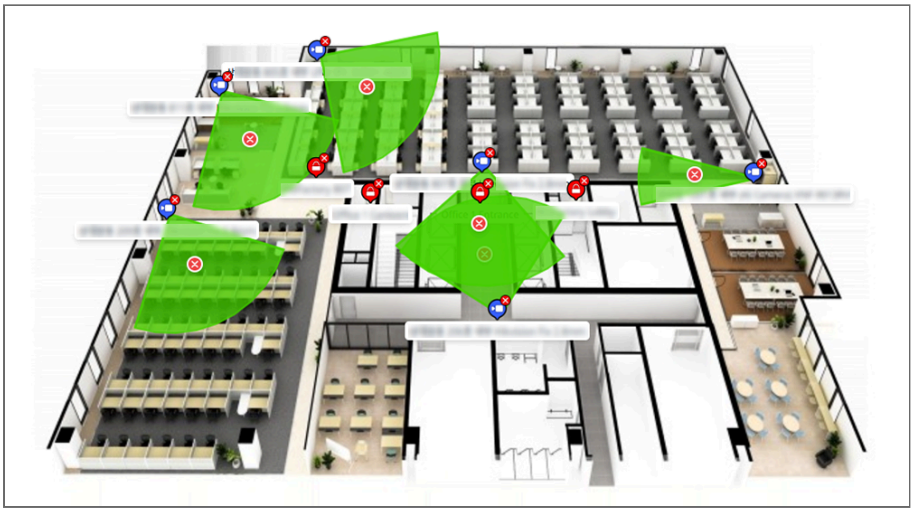
マップ管理

マップ設定機能は、マップと連携してフロア、施設、エリアを設定および管理する機能です。この機能を使用すると、**Monitoring** ページでエリア、施設、フロアごとに区分されたマップを確認できます。

> **情報**
> マップモニタリングの詳細については、マップをモニタリングするを参照してください。

フロアを構成する

区域と設備を構成する前にフロアを構成してください。該当フロアの配置図を画像としてアップロードし、ドアとカメラを配置して視覚的に管理できます。フロアを構成すると、**Monitoring** ページで該当フロアのドアとカメラを確認できます。



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。

> **情報**
>
> - フロアを構成する前に、先に出入口を登録してください。出入口の登録の詳細については、ドアを登録するを参照してください。
> - マップモニタリングの詳細については、マップをモニタリングするを参照してください。
> - フロアの追加および設定機能は、**エッセンシャル**（Essential）ライセンス以上で利用できます。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。

フロアを追加

フロアの配置図または3D鳥瞰図画像をアップロードしてフロアを追加し、出入口とカメラを配置できます。

1. **Launcher**ページで**Settings**をクリックします。
2. 画面左のサイドバーで **Map** → **Floor** をクリックします。
3. フロア一覧画面の右上で **New Floor** ボタンをクリックします。

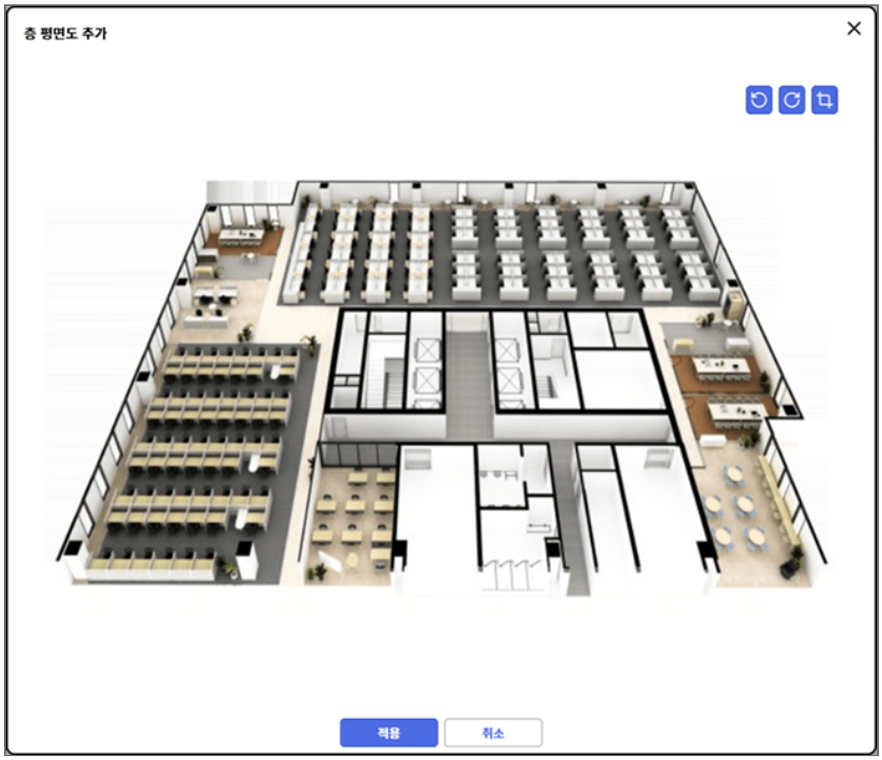


4. **Add New Floor** 画面の **Information** セクションで、追加するフロアの名前と説明を入力します。

5. **Floor Configuration** セクションの **Floor Plan** ボタンをクリックするか、アップロードする画像をドラッグしてアップロードします。

> 対応する画像ファイル形式はPNG、JPEG、JPGです。

6. **Add Floor Plan** ウィンドウでアップロードした画像を確認し、設定を進めます。

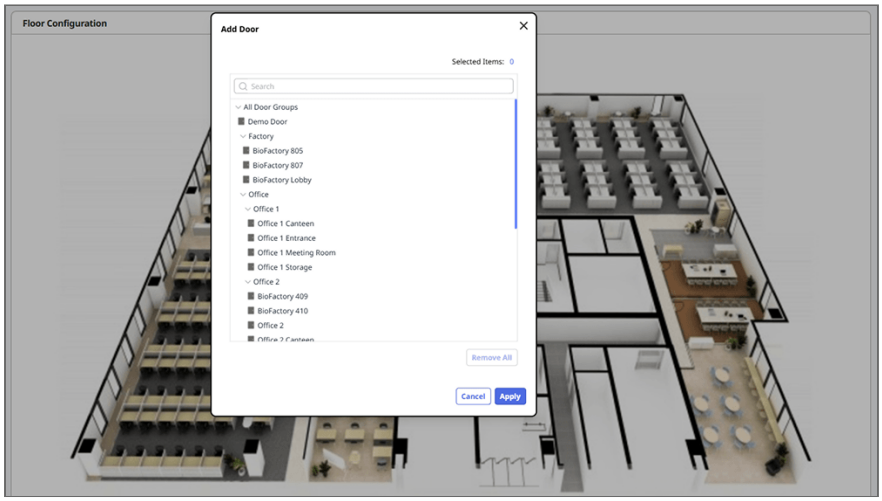


- 画像を回転するには、↺ または ↻ ボタンをクリックします。
- 画像を切り取るには、⌗ ボタンをクリックします。

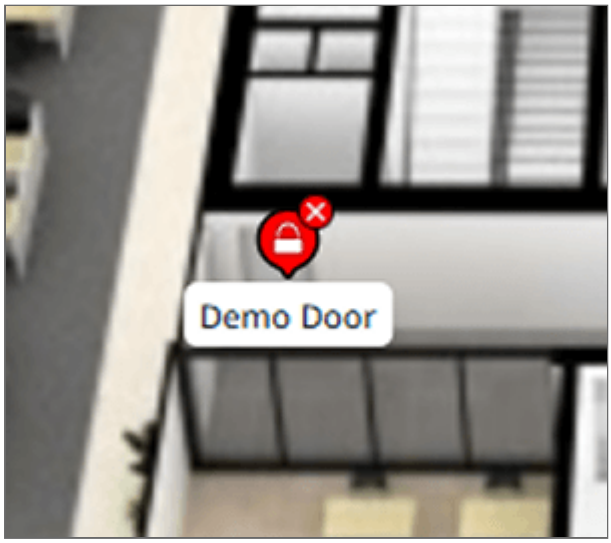
7. 画像の設定を完了したら、**Apply** ボタンをクリックします。

8. **Floor Configuration** セクションにアップロードした画像に出入口を追加するには、画像の任意の位置で右クリックし、**Add Door** を選択します。

9. **Add Door** ウィンドウが表示されたら、登録済みの出入口のいずれかを選択します。

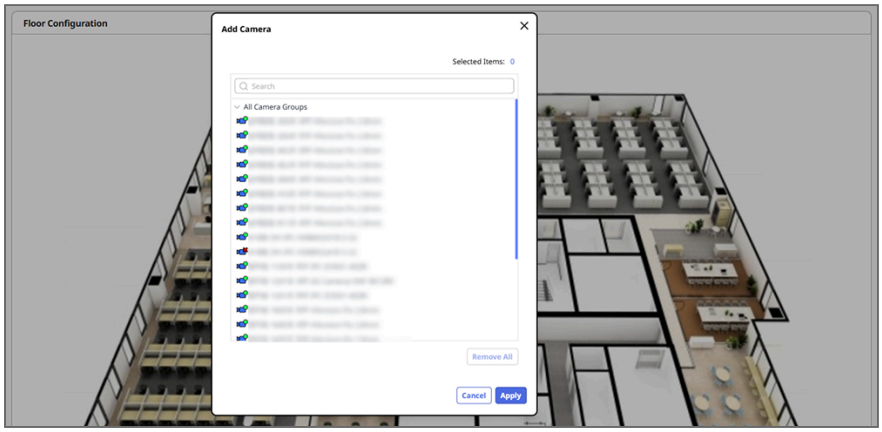


10. 出入口を画像に配置するには、**Apply** ボタンをクリックします。



11. アップロードした画像にカメラを追加するには、画像の任意の位置で右クリックし、**Add Camera** を選択します。

12. **Add Camera** ウィンドウが表示されたら、登録済みのカメラのいずれかを選択します。



13. カメラを画像に配置するには、**Apply** ボタンをクリックします。



14. 実際のフロアに配置されている出入口とカメラを追加で配置してください。
15. すべての設定を完了し、設定したフロアを保存するには、**Apply** ボタンをクリックします。

> **情報**
>
> - フロアに配置された出入口とカメラの位置を変更するには、該当する出入口またはカメラをクリックしたまま、目的の位置へドラッグします。
> - フロアに配置された出入口とカメラのアイコンおよび状態の詳細については、マップをモニタリングするを参照してください。

フロア構成を編集

ドアとカメラを追加したフロアの配置図を編集できます。フロアの配置図を編集すると、ドアとカメラの位置を変更または削除できます。

1. **Launcher**ページで**Settings**をクリックします。
2. 画面左のサイドバーで **Map** → **Floor** をクリックします。
3. フロア一覧で編集するフロアをクリックします。

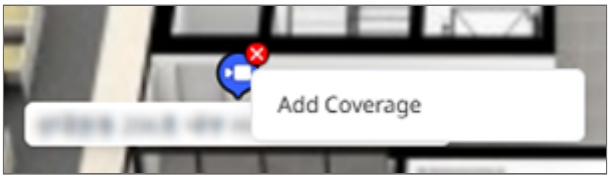
すべての設定を完了し、設定したフロアを保存するには、**Apply** ボタンをクリックします。

出入口／カメラを削除

フロア画像で削除したいドアまたはカメラの アイコンをクリックします。該当するドアまたはカメラを削除できます。

カメラ撮影範囲の設定

フロア画像で撮影範囲を設定するカメラを右クリックします。ポップアップメニューで **Add Coverage** をクリックします。



- 撮影範囲を変更するには、緑色の領域へマウスポインターを移動します。マウスポインターが十字形に変わったら、マウスを押したまま目的の位置へドラッグします。



- 撮影範囲を調整するには、範囲の端をクリックしたまま希望のサイズにドラッグします。

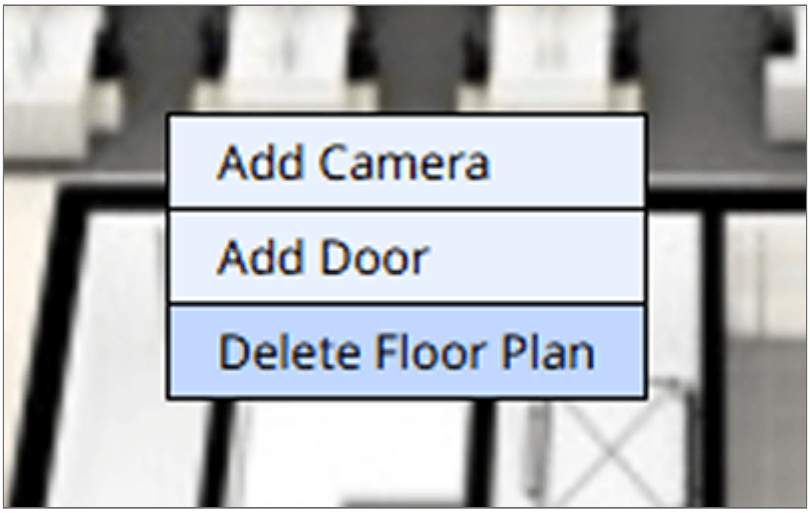


- 撮影範囲を削除するには ⊗ アイコンをクリックします。

> **注意**
> ユーザーが設定した内容はセキュリティ管理の利便性のための機能であり、実際のカメラ撮影範囲を反映しません。

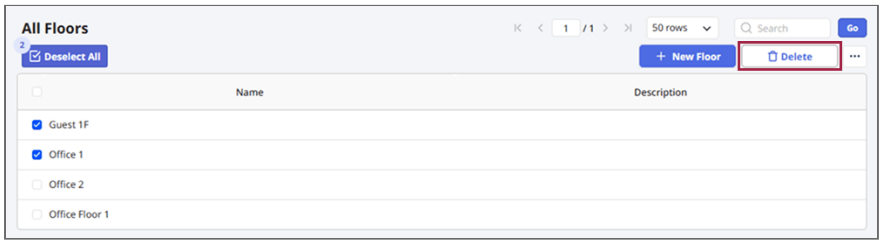
フロア画像を削除

フロア画像を削除するには、フロア画像上で右クリックし、ポップアップメニューから **Delete Floor Plan** を選択します。



フロアを削除

1. **Launcher**ページで**Settings**をクリックします。
2. 画面左のサイドバーで **Map** → **Floor** をクリックします。
3. フロアー覧で削除するフロアのチェックボックスをクリックします。 1つ以上のフロアを選択できます。

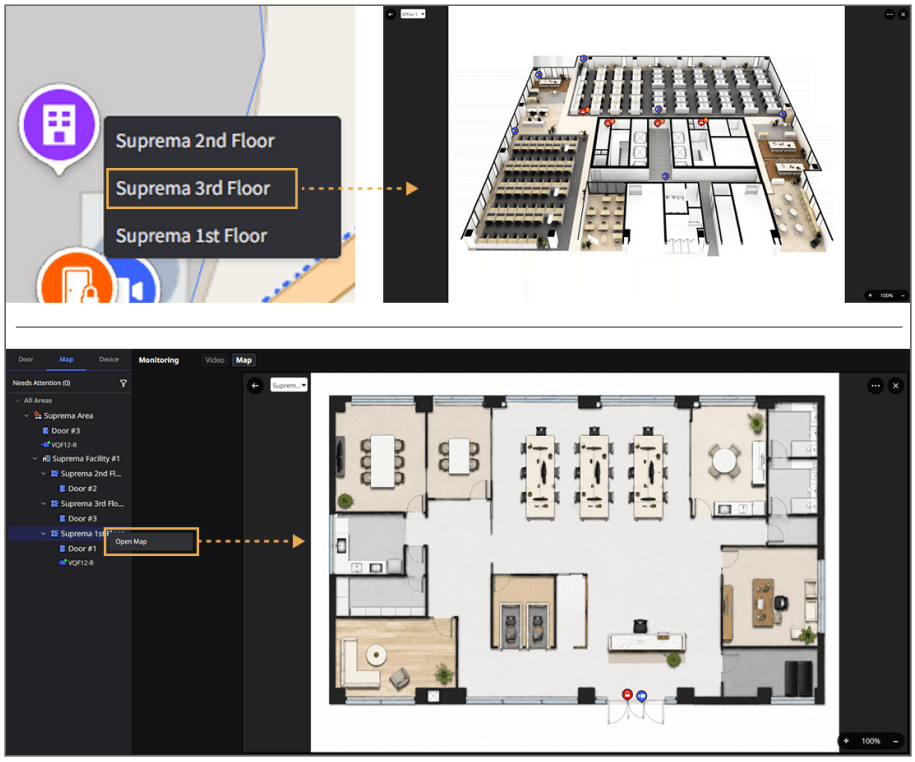


4. 画面右上の**Delete**をクリックします。

フロアー覧で選択したフロアが削除されます。選択したフロアは復元できません。

施設を構成

施設 (Facility) を構成し、階を配置します。階を順番に配置して、実際の施設の構造を表現できます。施設を構成すると、**Monitoring** ページで地図上に配置された施設を選択し、各階に入り監視できるようになります。



情報

- 施設を構成する前に階を先に登録します。階の登録の詳細については、フロアを構成するをご参照ください。
- マップモニタリングの詳細については、マップをモニタリングするを参照してください。
- 施設の追加および設定機能は、**エッセンシャル**（Essential）ライセンス以上で利用できます。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。

施設を追加

施設に階を追加して構造を設計するには、次の手順に従います。

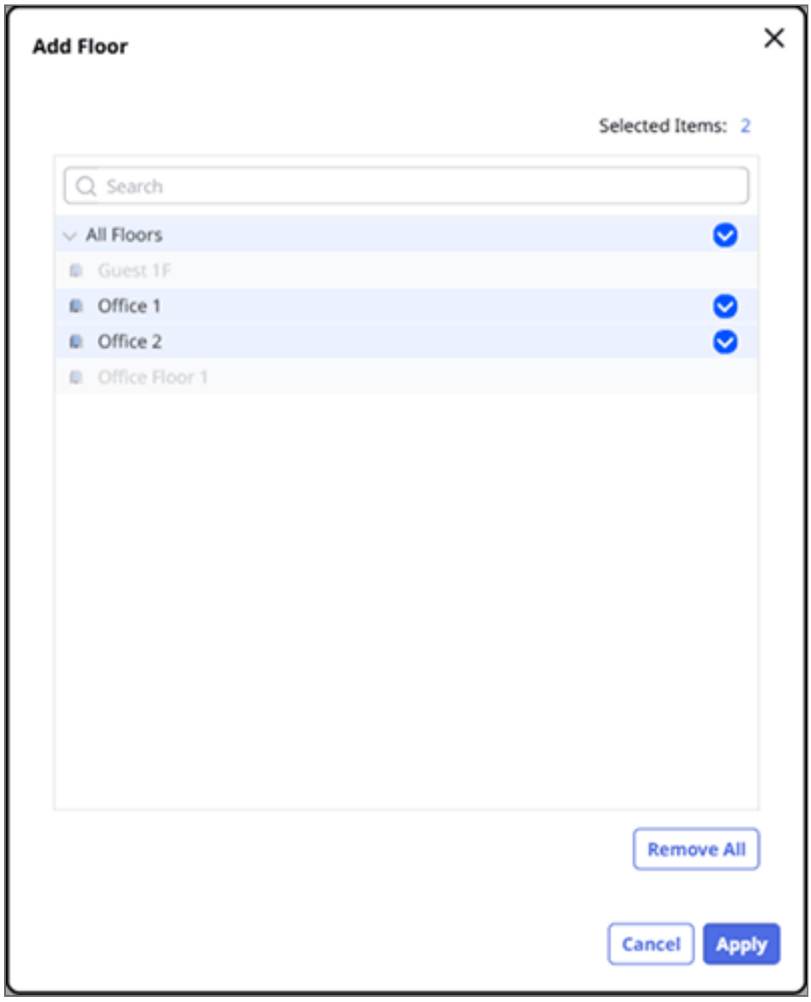
1. **Launcher**ページで**Settings**をクリックします。
2. 画面左のサイドバーで **Map** → **Facility** をクリックします。
3. 施設一覧画面の右上にある **New Facility** ボタンをクリックします。



4. **Add New Facility** 画面の **Information** セクションで、追加する施設の名前と説明を入力します。
5. **Facility Configuration** で **Add** ボタンをクリックします。



6. **Add Floor** ウィンドウが表示されたら、階の一覧から追加する階を選択します。



- 入力フィールドにキーワードを入力して階を検索することもできます。
- すべての階を選択するには、**All Floors** を選択します。

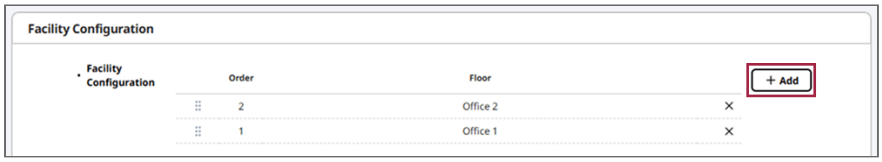
7. 階をすべて選択したら、**Apply** ボタンをクリックします。
8. 追加した階を出入口一覧で確認し、順序を変更する場合は、**Order** 列の ⠿ アイコンをドラッグして順序を変更します。
9. 施設の構成を完了して保存するには、画面右下の **Apply** ボタンをクリックします。

施設を編集

既存の施設に階を追加

既存の施設に階を追加できます。

1. **Launcher**ページで**Settings**をクリックします。
2. 画面左のサイドバーで **Map** → **Facility** をクリックします。
3. 施設一覧で階を追加する施設を選択します。
4. **Facility Configuration** で **Add** ボタンをクリックします。



5. **Add Floor** ウィンドウが表示されたら、追加する階のチェックボックスをクリックして階を選択します。
6. 階をすべて選択したら、**Apply** ボタンをクリックします。
7. 追加した階を出入口一覧で確認し、順序を変更する場合は、**Order** 列の ⠿ アイコンをドラッグして順序を変更します。
8. 施設の構成を完了して保存するには、画面右下の **Apply** ボタンをクリックします。

施設の階を削除

既存の施設から階を削除できます。

1. **Launcher**ページで**Settings**をクリックします。
2. 画面左のサイドバーで **Map** → **Facility** をクリックします。
3. 施設一覧で階を削除する施設を選択します。
4. **Facility Configuration** で、削除する階の ✕ ボタンをクリックします。
5. 階の削除を完了して保存するには、画面右下の **Apply** ボタンをクリックします。

施設を削除

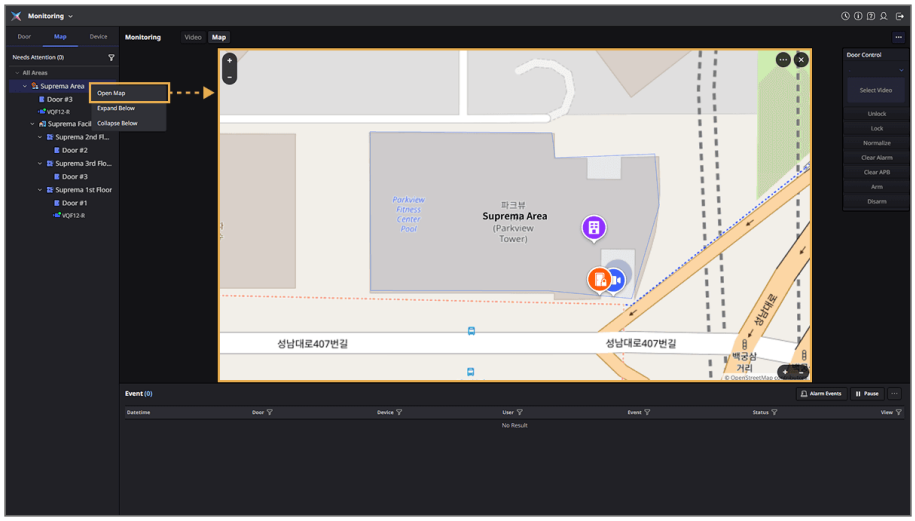
1. **Launcher**ページで**Settings**をクリックします。
2. 画面左のサイドバーで **Map** → **Facility** をクリックします。
3. 施設一覧で削除する施設のチェックボックスをクリックします。



4. 画面右上の**Delete**をクリックします。
5. 確認メッセージが表示されたら、**Yes** ボタンをクリックします。

エリアを構成する

フロアと施設の構成を完了すると、エリアを構成できます。管理しているセキュリティエリアをマップで管理・確認できます。エリアを構成すると、**Monitoring** ページから当該エリアの施設およびフロアに入り、モニタリングできます。



情報

- エリアを構成する前にフロアと施設を登録してください。フロアと施設の登録の詳細は次のドキュメントを参照してください。
  - フロアを構成する
  - 施設を構成
- マップモニタリングの詳細については、マップをモニタリングするを参照してください。
- エリア追加および設定機能は **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。

エリアを追加

現在管理しているセキュリティエリアをマップで設定および管理できます。

1. **Launcher**ページで**Settings**をクリックします。
2. 画面左のサイドバーで **Map** → **Area** をクリックします。
3. エリア一覧画面の右上にある **New Area** をクリックします。



4. **Add New Area** 画面の **Information** セクションで、追加するエリアの名前と説明を入力します。
5. **Area Configuration** セクションのマップで追加するエリアの位置を設定します。
6. マップ上で右クリックし、**Set Area** を選択します。

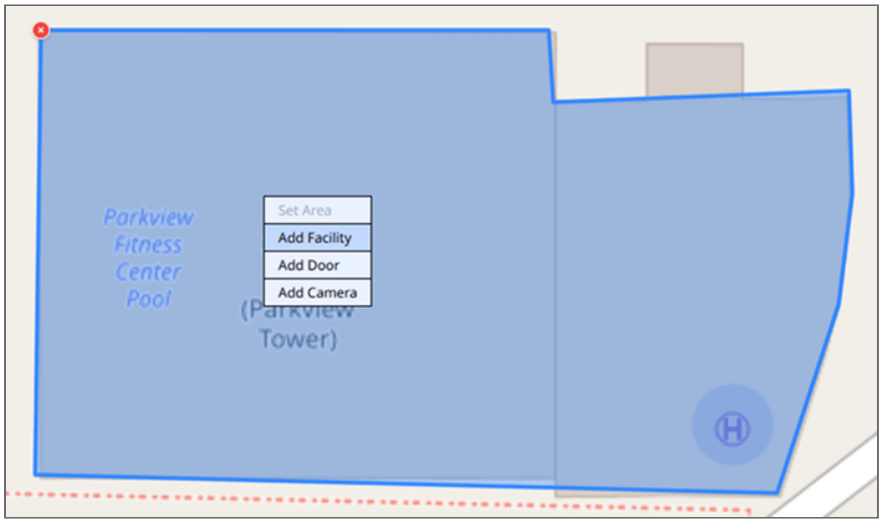


7. 希望する形状でエリアを設定します。クリックで開始し、ドラッグしてエリアを設定できます。



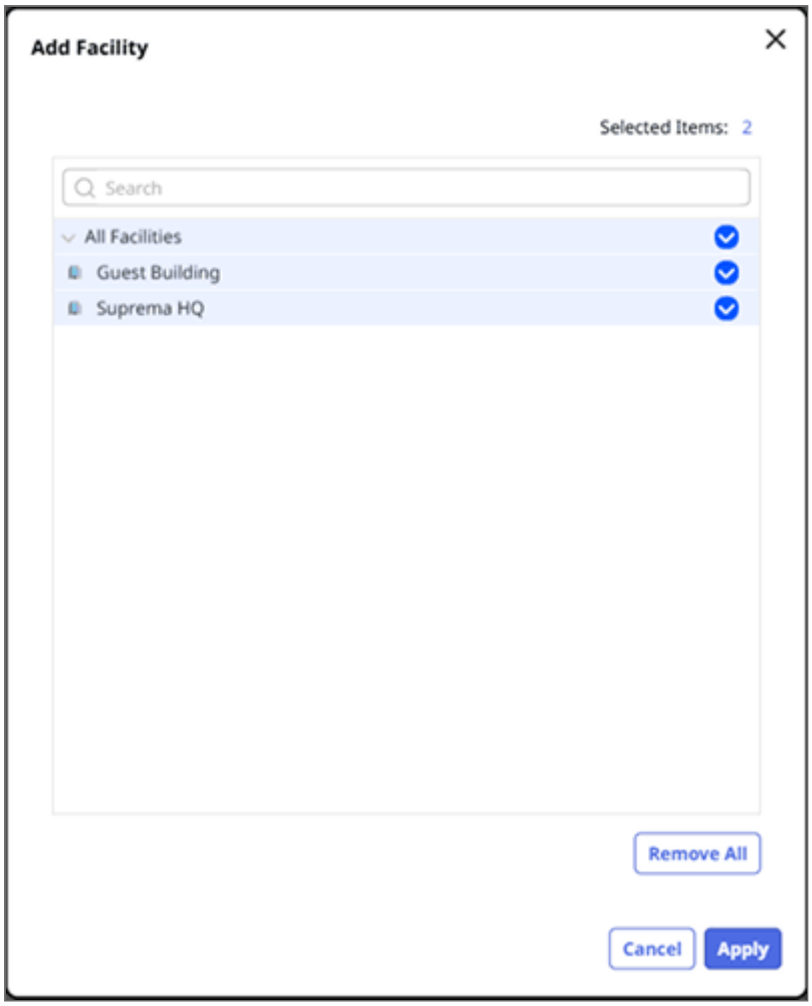
> エリアを再設定するには、設定済みのエリアを削除する必要があります。当該エリアを削除するには をクリックします。

8. 設定したエリアに施設を追加するには、右クリックして **Add Facility** を選択します。



エリアを追加する際は、少なくとも1つの施設またはドア・カメラを設定する必要があります。
- ドアを追加するには、右クリックして **Add Door** を選択します。
- カメラを追加するには、右クリックして **Add Camera** を選択します。

9. **Add Facility** ウィンドウが表示されたら、追加する施設を選択し、**Apply** をクリックします。



> ドアまたはカメラを追加する場合も同様に、**Add Door** または **Add Camera** ウィンドウが表示されます。追加する項目を選択し、**Apply** をクリックします。

10. エリア設定が完了したら、画面右下の **Apply** をクリックします。

> **情報**
>
> - マップ左上の入力フィールドで目的の位置を検索できます。現在位置に戻るには をクリックします。
>
> 
>
>
> - エリア追加時、マップでは1つの多角形でエリアを設定できます。エリアを設定する際は、開始点と終点を必ず同じ位置にしてください。エリアを設定した後に形状を変更することはできません。エリアを変更するには、エリアを削除して再度追加する必要があります。
> - 追加した施設・ドア・カメラの位置は、マップ上でドラッグ＆ドロップして変更できます。

エリアを編集

既存のエリアを削除して再設定するか、施設・ドア・カメラを追加または削除できます。

エリアを再設定

マップでエリアを再設定するには、既存のエリアを削除してから再度追加する必要があります。

1. **Launcher**ページで**Settings**をクリックします。
2. 画面左のサイドバーで **Map** → **Area** をクリックします。
3. エリア一覧で再設定するエリアを選択します。
4. **Area Configuration** セクションのマップで既存エリアの左上にある をクリックします。



5. マップ上で右クリックし、ポップアップメニューから **Set Area** を選択します。
6. 希望する形状でエリアを設定し保存するには、画面右下の **Apply** をクリックします。

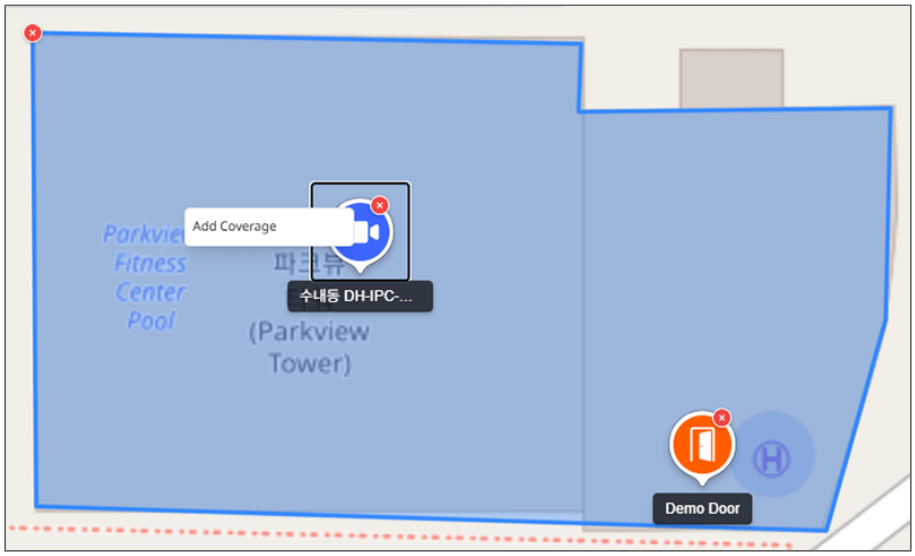
施設/ドア/カメラの削除

マップで削除したい施設・ドア・カメラをクリックします。 アイコンが表示されます。アイコンをクリックすると、選択した施設を削除できます。

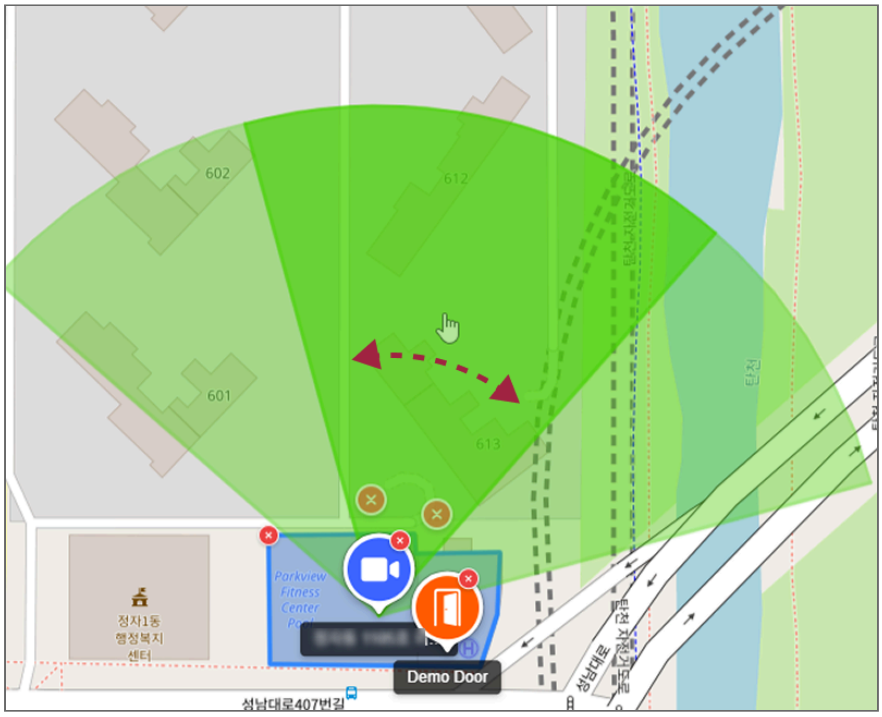


カメラ撮影範囲の設定

マップでカメラの撮影範囲を設定できます。カメラが配置されたアイコンを右クリックし、**Add Coverage** を選択します。



- 撮影範囲を変更するには、緑色領域の撮影範囲をクリックしたまま希望の方向へドラッグします。



- 撮影範囲を調整するには、範囲の端をクリックしたまま希望のサイズにドラッグします。



- 撮影範囲を削除するには ⊗ アイコンをクリックします。

> **注意**
> ユーザーが設定した内容はセキュリティ管理の利便性のための機能であり、実際のカメラ撮影範囲を反映しません。

エリアを削除

1. **Launcher**ページで**Settings**をクリックします。

2. 画面左のサイドバーで **Map** → **Area** をクリックします。
3. エリア一覧で削除するエリアのチェックボックスをクリックします。



4. 画面右上の**Delete**をクリックします。
5. 確認メッセージが表示されたら、**Yes** ボタンをクリックします。

訪問者設定

訪問者を管理するために訪問先と訪問PCを構成でき、訪問者向けの入退館規約と案内文を設定できます。さらに、カスタム訪問者フィールドを使用して訪問者に求める情報を直接追加することもできます。

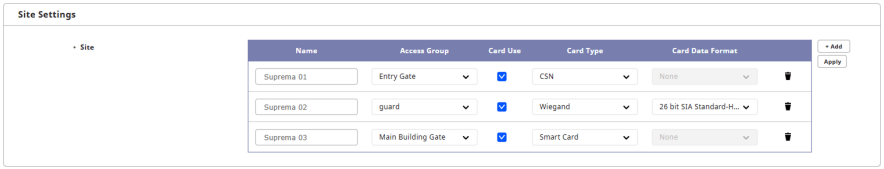
> **情報**
>
> - **Visitor** 設定は、**エッセンシャル** (Essential) ライセンス以上で追加オプションとして利用できます。ライセンスポリシーの詳細については、ライセンス ポリシーを参照してください。
> - **Visitor** メニューを使用するには、**Automatic User Synchronization** または **Use Server Matching** オプションを有効にする必要があります。詳細については、サーバーの詳細を設定するご参照ください。

訪問設定

1. **Launcher**ページで**Settings**をクリックします。
2. 画面左のサイドバーで **Visitor** → **Visitor**をクリックします。
3. 次の案内に従って訪問者設定を構成してください。

1 訪問先設定

各訪問先の訪問申請用または訪問者管理用PCで使用する入退館グループとカード使用の有無を設定できます。カードを使用する場合は、カード種類とデータ形式も設定できます。



- **Name**：訪問先の名前を入力できます。

> **情報**
>
> – 訪問先名は最大48文字まで入力できます。

- **Access Group**：訪問者に割り当てる入退館グループを選択できます。

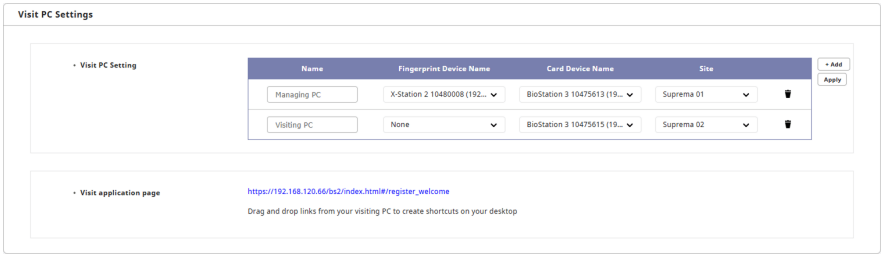
> **情報**
> 訪問者用の入退室グループをあらかじめ設定しておくと、管理が容易になります。出入グループの設定については、アクセスグループを管理するご参照ください。

- **Card Use**：カードを使用するかどうかを選択できます。
- **Card Type**：訪問先で使用するカードの種類を選択できます。カードの種類は、**Card Use** を設定した場合にのみ有効になります。
- **Card Data Format**：カードデータを読み取る形式を設定できます。 **Card Data Format** は、**Card Type** を **Wiegand** に設定した場合にのみ有効になります。

訪問先設定を保存するには、**Apply** をクリックしてください。

2 訪問PC設定

訪問申請用または訪問者管理用PCを設定できます。



- **Name**：訪問申請用または訪問者管理用PCの名前を設定できます。
- **Fingerprint Device Name**：訪問者が指紋認証で入退館する場合、指紋を登録するデバイスを選択します。
- **Card Device Name**：訪問者がカード認証で入退館する場合、カードを発行するデバイスを選択します。カードデバイス名は、カード使用を選択した訪問先を設定した場合にのみ有効になります。
- **Site**：該当の訪問PCで訪問を管理する訪問先を選択します。

訪問PC設定を保存するには **Apply** をクリックします。

> **情報**
> - 訪問PC名は最大48文字まで入力できます。
> - 指紋デバイスとカードデバイスを同時に使用でき、それぞれ1台ずつ選択できます。
> - 訪問先はPCごとに1つだけ選択できます。

3 訪問PC選択

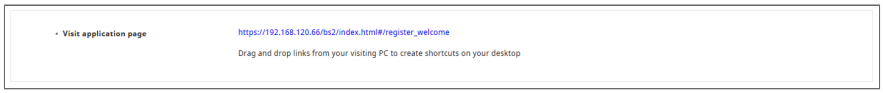
Visit PC Setting で設定したPCを選択し、使用中のPCに割り当てることができます。



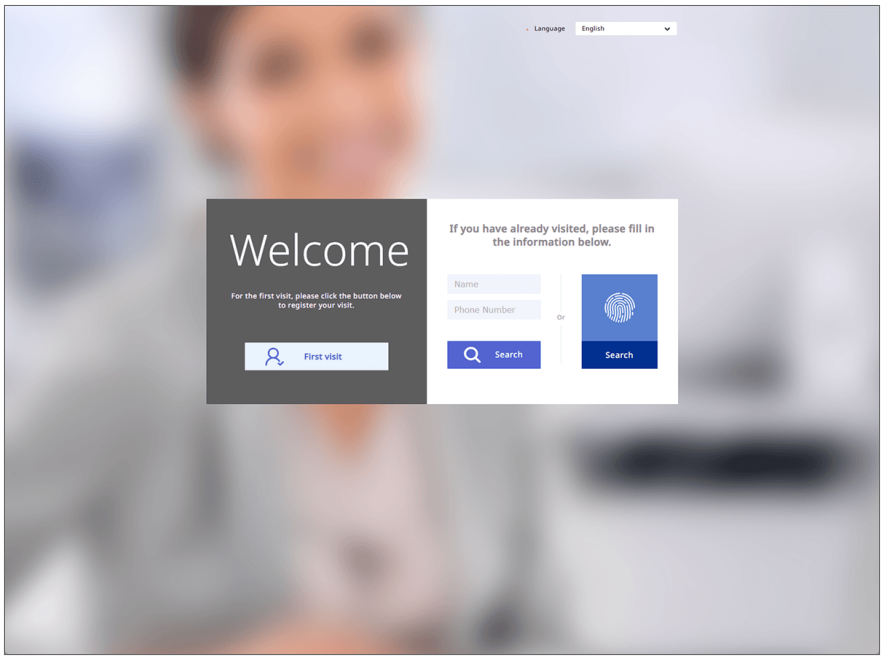
設定を保存するには **Apply** をクリックします。

4 訪問者申請ページショートカット

訪問申請用PCのデスクトップに訪問申請ページへのショートカットアイコンを作成できます。 **Visit application page** 項目のURLをデスクトップにドラッグしてください。

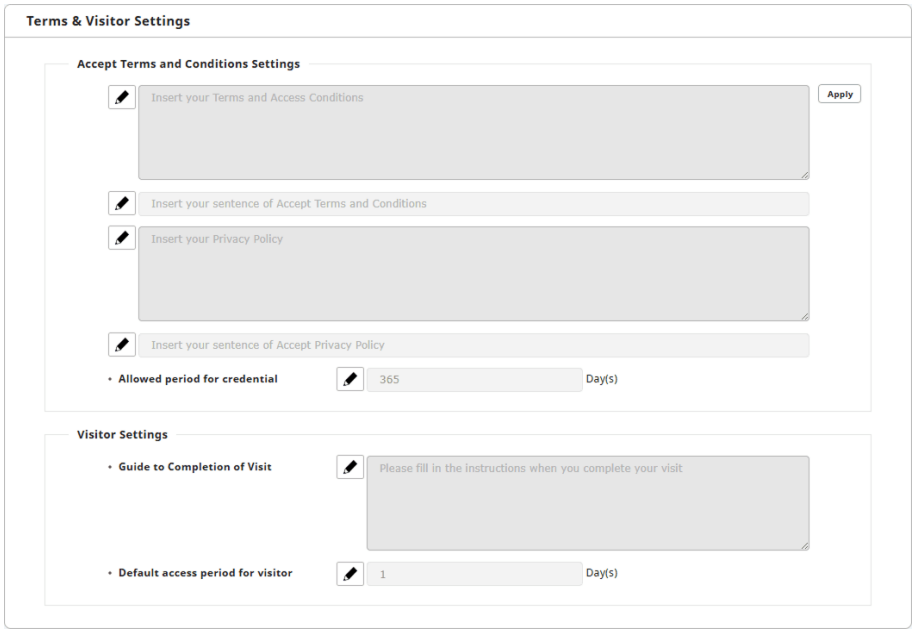


Webブラウザーでそのurlにアクセスすると、訪問申請ページを確認できます。



利用規約 & 訪問者設定

訪問者入退館規約、個人情報取扱方針、案内文など、訪問者に関する主要設定を管理できます。



- **入退館利用規約**：入退館に関する利用規約と規約同意文を入力できます。 ✎ をクリックして入力フィールドを有効化し、利用規約と規約同意文を入力します。

  > **情報**
  >
  > - 入退館規約は最大65,535文字まで入力できます。
  > - 規約同意文は最大64文字まで入力できます。

- **個人情報取扱方針**：訪問者が訪問時に提供した個人情報の取扱方針とその方針への同意文を入力できます。 ✎ をクリックして入力フィールドを有効化し、個人情報取扱方針とその方針への同意文を入力します。

  > **情報**
  >
  > - 個人情報取扱方針は最大65,535文字まで入力できます。
  > - 個人情報取扱方針への同意文は最大64文字まで入力できます。

- **Allowed period for credential**：訪問者が訪問時に提供した個人情報の保管期間を設定できます。 ✎ をクリックして入力フィールドを有効化し、個人情報の保管期間を日単位で入力します。

  > **情報**
  >
  > - 個人および機微情報の保管期間が満了した訪問者リストは **Visitor** メニューで削除できます。

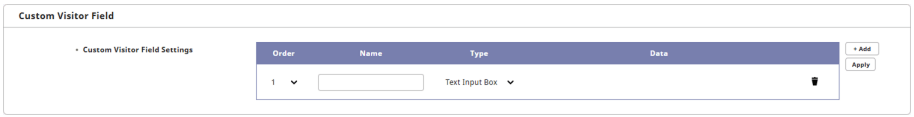
- **Guide to Completion of Visit**：訪問申請完了時にポップアップ画面で表示する案内文を入力できます。 ✎ をクリックして入力フィールドを有効化し、案内文を入力します。

> **情報**
>
> - 訪問申請完了時の案内文は最大65,535文字まで入力できます。
> - 案内文を入力しない場合、訪問申請完了時に案内文のポップアップ画面は表示されません。

- **Default access period for visitor**：訪問者の入退館許可期間を設定できます。 をクリックして入力フィールドを有効化し、訪問者のデフォルト入退館許可期間を日単位で入力します。

カスタム訪問者フィールド設定

訪問者の追加情報を入力するフィールドを追加でき、追加されたフィールドは訪問申請画面に表示されます。



- **Order**：ユーザー定義で追加した入力フィールドの順序を設定できます。
- **Name**：ユーザー定義で追加した入力フィールドの名前を設定できます。
- **Type**：文字入力ボックス、数値入力ボックス、選択ボックスを選択できます。
- **Data**：選択ボックスのリストに表示する選択肢を入力します。各項目はセミコロン(;)で区切ります。データは、**Type** を **Combo Box** に設定した場合にのみ有効になります。

設定を保存するには、**Apply** をクリックしてください。

> **情報**
>
> - **Text Input Box** で追加したカスタム訪問者フィールドには数字と文字を入力できます。
> - **Number Input Box** で追加したカスタム訪問者フィールドには数字のみ入力でき、文字は入力できません。
> - **Combo Box** で追加したカスタム訪問者フィールドでは、訪問者が項目を選択できます。カスタム訪問者フィールドを設定するときは、データに **Option 1; Option 2; Option 3; Option 4** を入力してください。

ディレクトリ連携を設定する

Microsoft Entra ID（以下 **Entra ID**）または **アクティブ ディレクトリ**（Active Directory）と **BioStar X** を連携し、ユーザーを同期・管理する方法を案内します。

Entra ID または **Active Directory** と連携すると、以下の便利な機能を利用できます。これにより、セキュリティと利便性を向上できます。

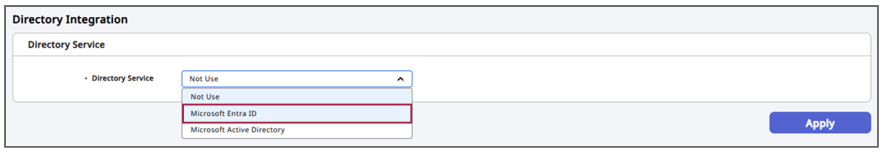
- **Entra ID** が提供するシングル サインオン（SSO）機能を使用して、**Entra ID** アカウントで **BioStar X** にログインできます。
- **Active Directory** が提供する Lightweight Directory Access Protocol（LDAP）認証を使用して **BioStar X** にログインできます。
- **Entra ID** または **Active Directory** で構成したユーザーおよびグループを **BioStar X** と同期できます。
- **Entra ID** または **Active Directory** で使用される役職・部署・グループなどのユーザー情報を **BioStar X** のカスタムフィールドにマッピングできます。

> **情報**
>
> Entra ID または Active Directory 設定機能は、**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。

ディレクトリ連携の設定

Entra ID

1. BioStar X に管理者 ID でログインします。
2. **Launcher**ページで**Settings**をクリックします。
3. 画面左のサイドバーで **System** → **Directory Integration** をクリックします。
4. **Directory Service** 項目で **Microsoft Entra ID** を選択します。



5. 以下の案内に従って各項目を設定します。

> **情報**
>
> Entra IDと連携するには、**System** → **Server** メニューで**User ID Type**項目を**Alphanumeric**に設定する必要があります。

1 Directory Server

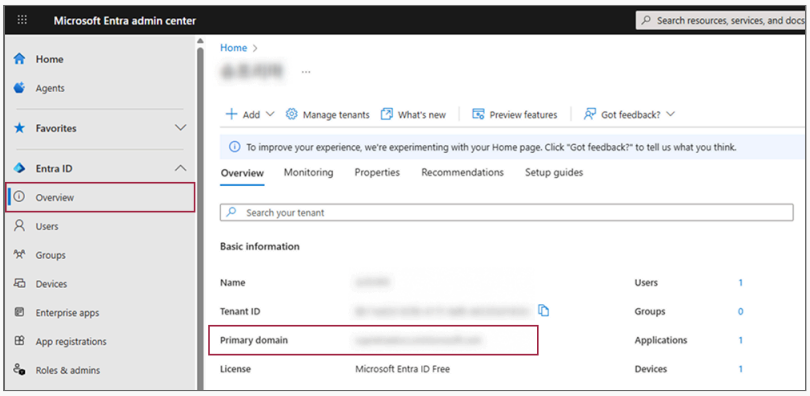
Directory Server セクションで **Entra ID** のサーバー情報を入力し、**Connect** ボタンをクリックします。



- **Client ID**：**Entra ID** で登録したアプリケーションの **クライアント ID**（Client ID）を入力します。
- **Client Secret**：**Entra ID** で登録したアプリケーションの **証明書とシークレット**（Certificates & secrets）に追加した **クライアント シークレット**（Client secrets）を入力します。
- **Primary Domain**：**Entra ID** で組織を作成するときに入力した既定のドメイン名を入力します。

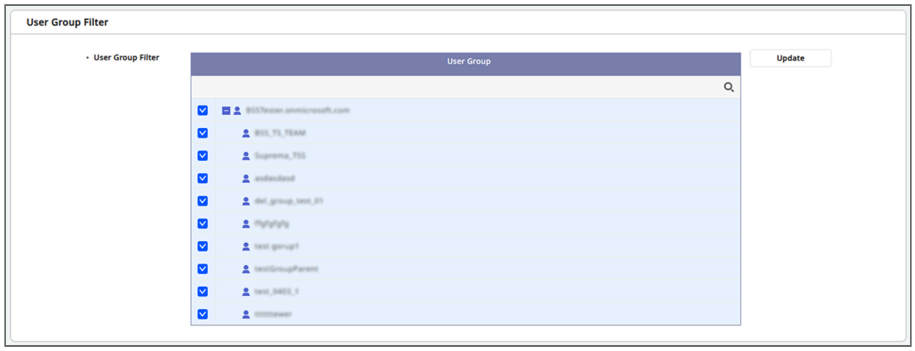
情報

- Entra ID でアプリケーションを登録する方法は 以下のリンク を参照してください。
- Entra ID で 証明書とシークレット を設定する方法は 以下のリンク を参照してください。
- テナント ID は Entra ID で登録したアプリケーションの 概要（Overview）で確認できます。
- **Primary Domain** の情報は Entra ID の 概要 (Overview) で確認できます。



1 User Group Filter

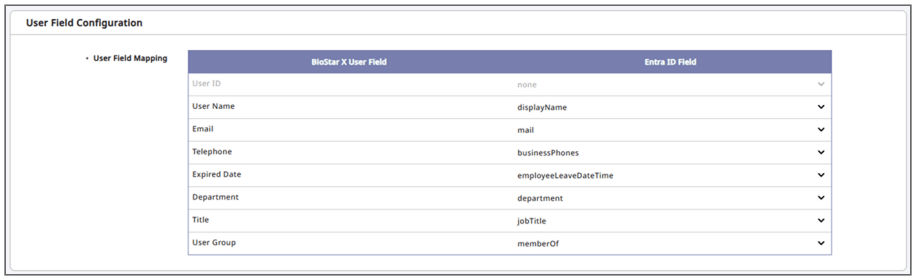
Directory Server セクションで設定を完了し、**Connect** ボタンをクリックすると、**User Group Filter** セクションでからユーザー グループ情報を取得します。 **BioStar X** に同期しないユーザー グループを選択解除します。



- **Update**：ユーザー グループ情報を再読み込みするにはクリックします。
- 🔍 ボタンをクリックして目的のユーザー グループを検索できます。

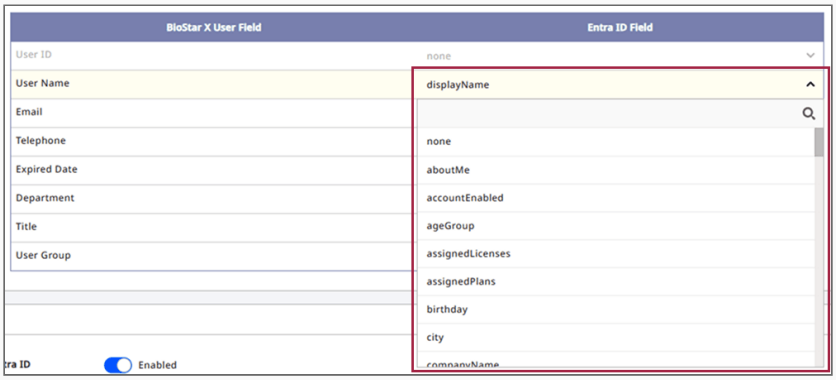
1 User Field Configuration

BioStar X のユーザーフィールドにマッピングする フィールドを設定できます。 **User Field Configuration** セクションで、BioStar X のユーザーフィールドとして使用する のフィールドを選択します。



情報

BioStar Xの各ユーザーフィールドは、のユーザー情報と一致する項目にマッピングできるようデフォルト設定されています。デフォルト設定されたフィールド値ではなく別のフィールド値を選択するには、**Entra ID Field** 列の項目をクリックして、目的のフィールド値を選択します。

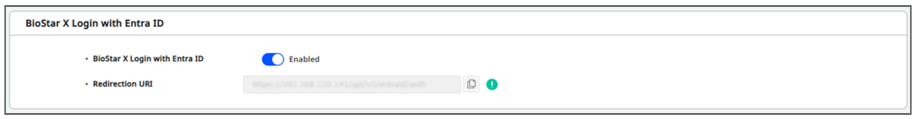


注意

Entra ID と連携する場合、**User ID** フィールドはマッピングできません。 **User ID** は BioStar X が自動生成して適用します。

1 BioStar X Login with Entra ID

Entra ID SSO で BioStar X にログインできるようにするには、**BioStar X Login with Entra ID** 項目を **Enabled** に変更します。



Redirection URI 項目のリダイレクト URL をコピー（）し、Entra ID ポータルの SSO リダイレクト設定に貼り付けます。ユーザーが Entra ID でのログインに成功すると、このアドレスへリダイレクトされます。

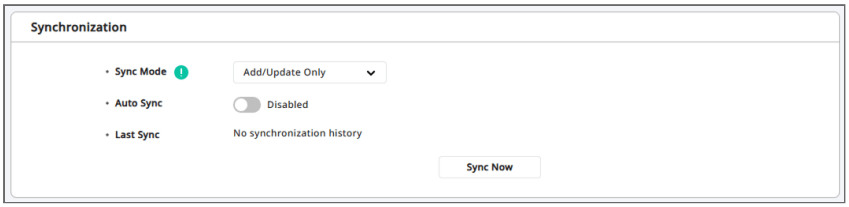
情報

- Entra ID にアプリケーションを登録し、リダイレクト URI を追加する方法については次のリンクを参照してください。
  - Microsoft Entra ID へのアプリケーション登録
  - アプリにリダイレクト URI を追加
- リダイレクト URL は Entra ID で登録したアプリケーションの 概要（Overview）で確認できます。

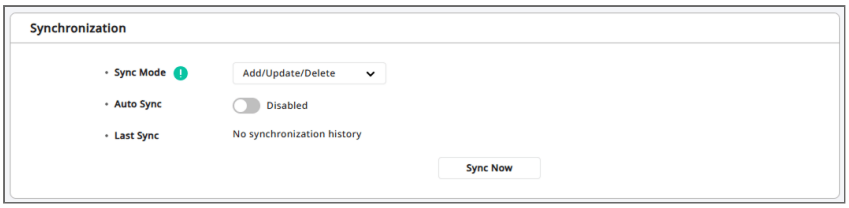
1 Synchronization

で変更されたユーザー情報を同期する機能です。

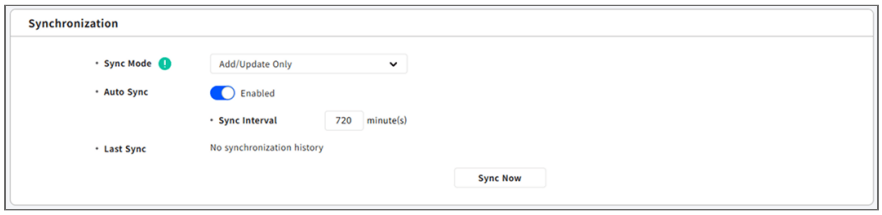
- **Sync Mode**：希望する同期モードを選択してください。
  - **Add/Update Only**：連携先のディレクトリサービスからユーザーを同期する際、BioStar Xに存在しないユーザーを追加し、情報が変更されたユーザーを更新します。ただし、次のユーザーは削除せずに保持します。
    - BioStar X にのみ登録されているユーザー
    - から削除されたユーザー



  - **Add/Update/Delete**：BioStar X のユーザー情報を連携先のディレクトリサービスと完全に一致するように同期します。BioStar X にのみ登録されているユーザーおよびから削除されたユーザーをすべて含めて同期するため、双方のデータが一致して管理されます。



- **Auto Sync**：自動同期の間隔を設定できます。**Sync Interval**に設定した間隔で自動的に同期されます。分単位で入力できます。最小設定値は 30 分、最大設定値は 10,080 分（7 日）です。



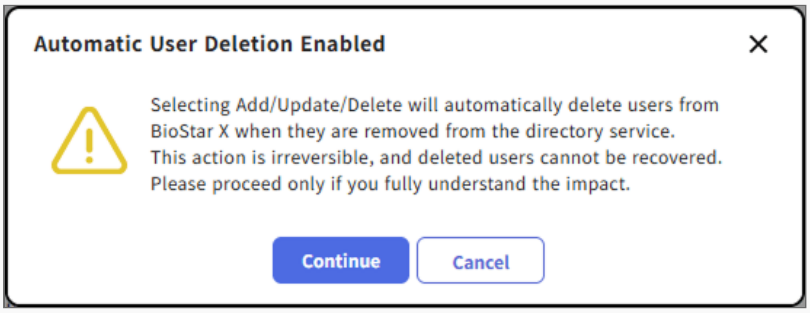
- **Last Sync**：直近の同期日時を確認できます。

注意

- **Add/Update Only** モード使用時、同名のユーザーグループがある場合は削除せずに保持します。
- **Add/Update/Delete** モードでは：
  - **同名のグループが既に存在する場合**：グループは新たに作成されず、既存グループの情報を保持します。ただし、該当グループに所属するユーザーはディレクトリサービスの最新情報を反映させるため、一旦すべて削除してから再度追加します。ただし、該当グループ内の同名ユーザーは維持されます。
  - **BioStar Xで作成されたユーザー**：BioStar X 上で直接作成したユーザーはディレクトリサービスとは連携されていません。同期時にこれらのユーザーの情報をディレクトリサービスと紐付けるように更新します。
  - **制限事項**：同期後に同名のグループが既に存在する場合、当該グループの情報と所属ユーザーが正常に同期されない可能性があります。
- ディレクトリ連携を設定した状態で **BioStar X v1.0.2** にアップグレードした場合、同期モードは **Add/Update/Delete** に既定で設定されます。

情報

- **Sync Now** ボタンをクリックするたびに、選択した同期モードでディレクトリサービスとユーザー情報を同期します。
- **Add/Update/Delete** モードを選択すると警告メッセージが表示されます。メッセージを確認して続行する場合は **Continue** ボタンを、キャンセルする場合は **Cancel** ボタンをクリックします。



- 同期機能で連携する際に、特定のユーザーを同期対象から除外する方法については、ディレクトリ連携の除外を参照してください。
- 同期するユーザーIDまたはユーザー名に、**BioStar X**で許可されていない文字が含まれる場合は、その文字だけを除いた値で登録します。ただし、ユーザーIDのピリオド(.)、ユーザー名のピリオド(.)およびアポストロフィ(')は除外対象ではないため、元のまま保持します。使用できない文字の詳細は、ユーザーIDおよび名前の入力規則を参照してください。

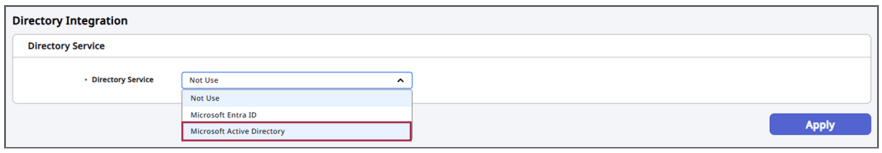
1 設定を保存

Directory Integration の設定をすべて完了したら、画面最下部の **Apply** ボタンをクリックして保存します。設定結果を確認するには、設定結果の確認を参照してください。

Active Directory

1. **BioStar X** に管理者 ID でログインします。
2. **Launcher**ページで**Settings**をクリックします。
3. 画面左のサイドバーで **System** → **Directory Integration** をクリックします。

4. **Directory Service** 項目で **Microsoft Active Directory** を選択します。



5. 以下の案内に従って各項目を設定します。

> **情報**
>
> - Active Directory は Windows Server 2008 R2 以降のシステム環境で使用できます。
> - Active Directoryと連携するには、**System** → **Server**メニューで**User ID Type**項目を**Alphanumeric**に設定してください。

1 Directory Server

Directory Server セクションで **Active Directory** のサーバー情報を入力し、**Connect** ボタンをクリックします。



- **Server Address**：Windows Active Directory サーバーのアドレスを入力します。
- **User Name**：Windows Active Directory のログイン ID を入力します。
- **Password**：Windows Active Directory のログインパスワードを入力します。
- **Base Domain Name**：Windows Active Directory の既定ドメイン名を入力します。既定ドメイン名は下記の手順で確認できます。

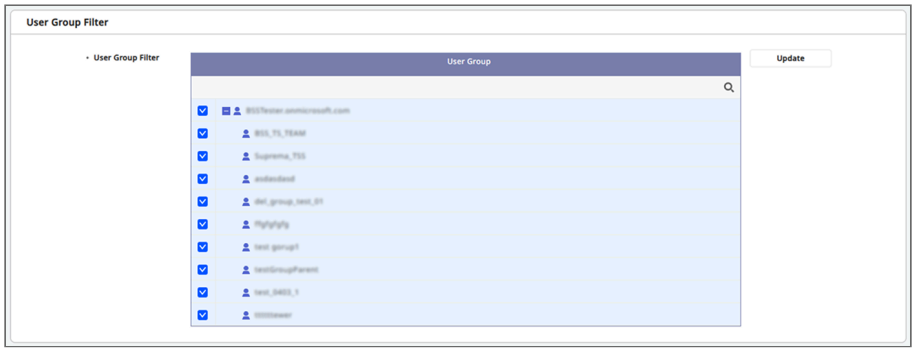
  1. **Active Directory 管理センター** を起動します。
  2. ユーザーデータが保存されているノード（Node）を右クリックし、**プロパティ** を選択します。
  3. **プロパティ** ウィンドウで **拡張** を選択し、**属性エディター** をクリックします。
  4. **distinguishedName** の値を確認します。

- **Secure Transfer**：Windows Active Directory サーバーと通信するときに暗号化を使用できます。 Active Directory 証明書サービスをインストールし、**Keystore Password**を設定するには、Active Directory の暗号化設定を参照してください。

  - **Keystore Password**：Windows Active Directory サーバーの暗号化キー ストアのパスワードを入力します。 **Secure Transfer** 項目を **Enabled** に設定すると入力できます。

1 User Group Filter

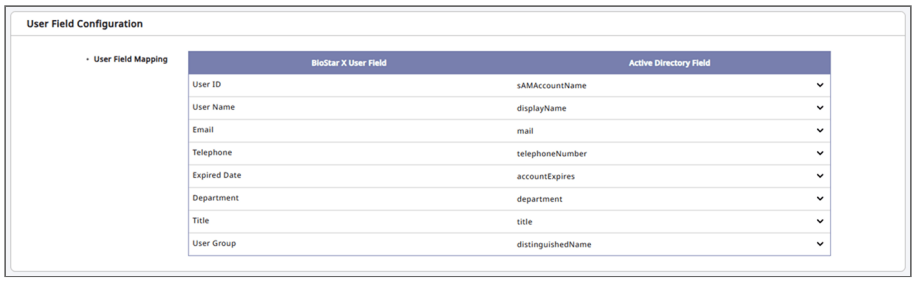
Directory Server セクションで設定を完了し、**Connect** ボタンをクリックすると、**User Group Filter** セクションでからユーザーグループ情報を取得します。 **BioStar X** に同期しないユーザー グループを選択解除します。

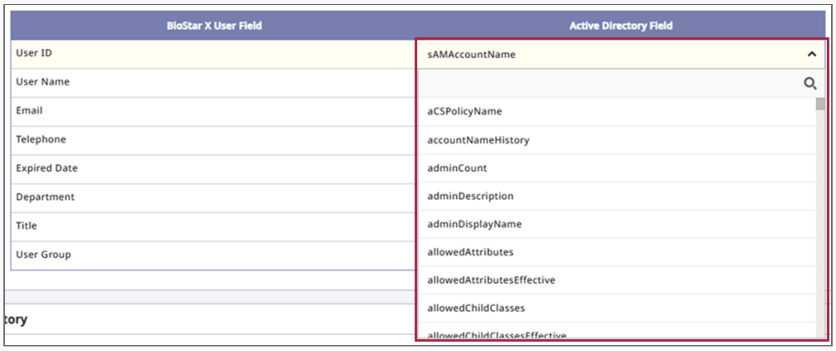


- **Update**：ユーザー グループ情報を再読み込みするにはクリックします。
- 🔍 ボタンをクリックして目的のユーザー グループを検索できます。

1 User Field Configuration

BioStar X のユーザーフィールドにマッピングする フィールドを設定できます。 **User Field Configuration** セクションで、BioStar X のユーザーフィールドとして使用する のフィールドを選択します。



> **情報**
>
> **BioStar X**の各ユーザーフィールドは、のユーザー情報と一致する項目にマッピングできるようデフォルト設定されています。デフォルト設定されたフィールド値ではなく別のフィールド値を選択するには、**Active Directory Field** 列の項目をクリックして、目的のフィールド値を選択します。
>
> 
>

1 BioStar X Login with Active Directory

Active Directory サーバーのユーザー ID でログインできるようにするには、**BioStar X Login with Active Directory** 項目を **Enabled** に変更します。 Active Directory サーバーの `sAMAccountName` フィールドの値が **BioStar X** のログイン ID にマッピングされます。

注意

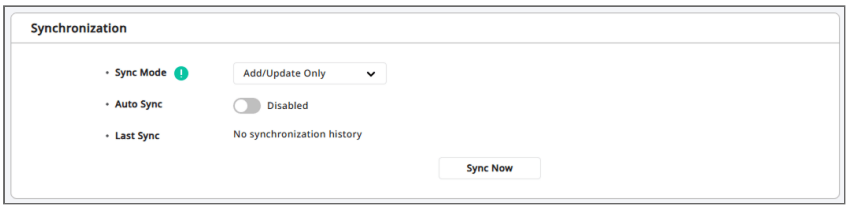
sAMAccountName フィールドには特殊文字を含めることはできません。 BioStar X のログイン ID ポリシーに合致しない場合、ログインに失敗することがあります。



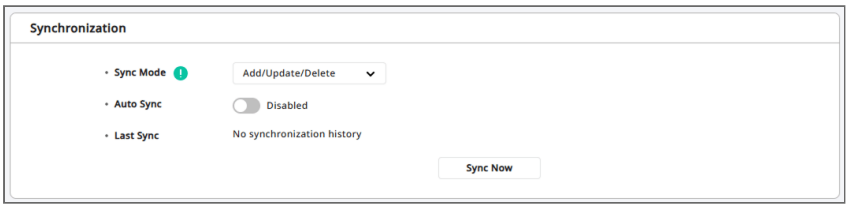
1 Synchronization

で変更されたユーザー情報を同期する機能です。

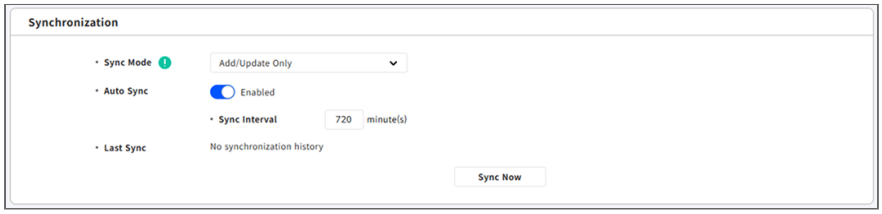
- **Sync Mode**：希望する同期モードを選択してください。
  - **Add/Update Only**：連携先のディレクトリサービスからユーザーを同期する際、BioStar Xに存在しないユーザーを追加し、情報が変更されたユーザーを更新します。ただし、次のユーザーは削除せずに保持します。
    - BioStar X にのみ登録されているユーザー
    - から削除されたユーザー



  - **Add/Update/Delete**：BioStar X のユーザー情報を連携先のディレクトリサービスと完全に一致するように同期します。BioStar X にのみ登録されているユーザーおよびから削除されたユーザーをすべて含めて同期するため、双方のデータが一致して管理されます。



- **Auto Sync**：自動同期の間隔を設定できます。**Sync Interval**に設定した間隔で自動的に同期されます。分単位で入力できます。最小設定値は 30 分、最大設定値は 10,080 分（7 日）です。



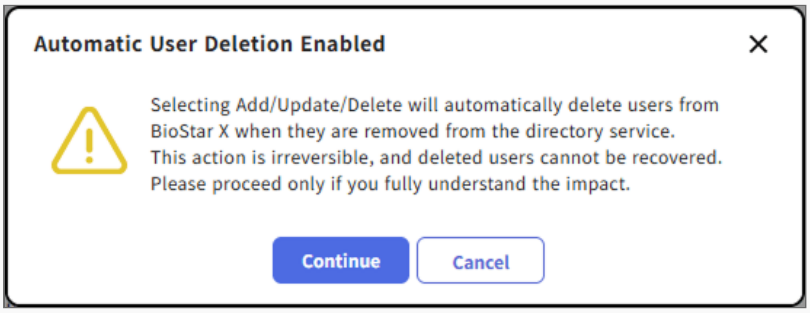
- **Last Sync**：直近の同期日時を確認できます。

注意

- **Add/Update Only** モードでは、同名のユーザーグループと同一のユーザーID(User ID)は削除せずに保持します。
- **Add/Update/Delete** モードでは：
  - **同名のグループが既に存在する場合**：グループは新たに作成されず、既存グループの情報を保持します。ただし、該当グループに所属するユーザーはディレクトリサービスの最新情報を反映させるため、一旦すべて削除してから再度追加します。ただし、該当グループ内の同名ユーザーは維持されます。
  - **BioStar Xで作成されたユーザー**：BioStar X 上で直接作成したユーザーはディレクトリサービスとは連携されていません。同期時にこれらのユーザーの情報をディレクトリサービスと紐付けるように更新します。
  - **制限事項**：同期後に同名のグループが既に存在する場合、当該グループの情報と所属ユーザーが正常に同期されない可能性があります。
- ディレクトリ連携を設定した状態で **BioStar X v1.0.2** にアップグレードした場合、同期モードは **Add/Update/Delete** に既定で設定されます。

情報

- **Sync Now** ボタンをクリックするたびに、選択した同期モードでディレクトリサービスとユーザー情報を同期します。
- **Add/Update/Delete** モードを選択すると警告メッセージが表示されます。メッセージを確認して続行する場合は **Continue** ボタンを、キャンセルする場合は **Cancel** ボタンをクリックします。



- 同期機能で連携する際に、特定のユーザーを同期対象から除外する方法については、ディレクトリ連携の除外を参照してください。
- 同期するユーザーIDまたはユーザー名に、**BioStar X**で許可されていない文字が含まれる場合は、その文字だけを除いた値で登録します。ただし、ユーザーIDのピリオド(`.`)、ユーザー名のピリオド(`.`)およびアポストロフィ(`'`)は除外対象ではないため、元のまま保持します。使用できない文字の詳細は、ユーザーIDおよび名前の入力規則を参照してください。

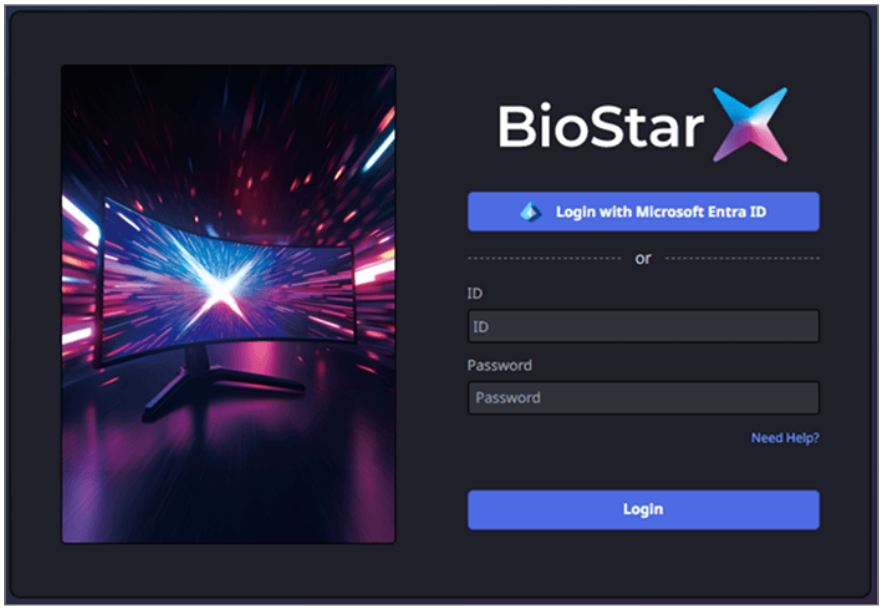
1 設定を保存

Directory Integration の設定をすべて完了したら、画面最下部の **Apply** ボタンをクリックして保存します。設定結果を確認するには、設定結果の確認を参照してください。

設定結果の確認

Entra ID または **Active Directory** との連携設定を完了したら、画面下部の **Apply** ボタンをクリックします。以下の項目を参考に同期された設定を確認します。

- **User** メニューで同期されたユーザーの一覧を確認します。
- Entra ID または Active Directory のログイン設定を完了した後、BioStar X にログインするときに **Login with Microsoft Entra ID** ボタンが表示されます。



サポートされない文字の処理

Entra IDまたはActive Directoryのユーザー IDまたはユーザー名にBioStar Xでサポートされない文字が含まれる場合、システムはサポートされない文字のみを削除した値でユーザーを同期します。

> *例えば、ディレクトリサービスのユーザーIDが `john/doe` で、ユーザー名が `John<Doe>` の場合、**BioStar X**にはそれぞれ `johndoe`、`JohnDoe` として登録します。*

情報

- ユーザー名のピリオド(`.`)とアポストロフィ(`'`)はサポートされない文字から除外され、ディレクトリサービスの値のまま登録します。

  > *例: `O'Brien`、`John.Doe` → ディレクトリサービスの値のまま登録*

- ユーザーIDのピリオド(`.`)はサポートされない文字から除外され、ディレクトリサービスの値のまま登録します。ただし、アポストロフィ(`'`)はユーザーIDで使用できないため、削除した値で登録します。

  > *ディレクトリサービスのユーザーIDの例：*
  >
  > - `O'Brien` → `OBrien` *として登録*
  > - `john.doe` → `john.doe` *のまま登録*

- ユーザーIDおよび名前の入力規則について詳しくは、ユーザー基本情報を入力を参照してください。

ディレクトリ連携の除外

Directory Integration 機能を使用して Entra ID または Active Directory と連携する場合、ディレクトリサービスに存在しないユーザーは BioStar X から削除されることがあります。削除したくないユーザーがいる場合、次の方法で連携から除外できます。

1. BioStar X に管理者 ID でログインします。

2. **User** メニューに移動します。
3. **All Users** 一覧で連携から除外するユーザーをクリックします。
4. 選択したユーザーの詳細画面が表示されたら、**Advanced** セクションで**Exclude from Directory Integration**オプションを有効にしてください。



5. **Apply** ボタンをクリックします。

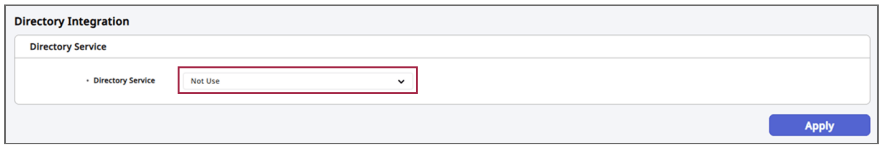
選択したユーザーは **Directory Integration** 機能を使用するときに連携から除外されます。

> **情報**
> 次に該当するユーザーは、自動的に連携から除外されます。
> - ユーザー名の先頭が `&@~` の連続で始まる場合
> - ユーザーIDまたはユーザー名の値が空の場合
> - ユーザーID（最大32文字）またはユーザー名（最大48文字）の長さ制限を超える場合
> - ユーザーIDが `admin` のように、システムで予約された値と同じ場合
> - ユーザーIDがピリオドが一つ（`.`）または二つ（`..`）の場合

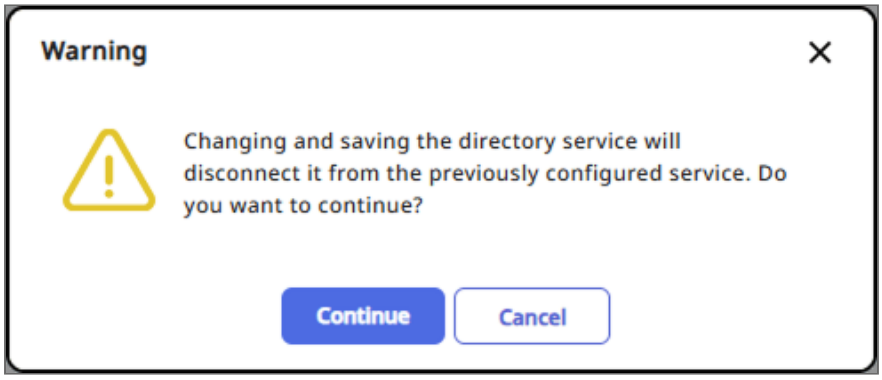
ディレクトリ連携の解除

Directory Service 機能を無効にする場合、次の手順に従います。

1. **BioStar X** に管理者 ID でログインします。
2. **System** → **Directory Integration** をクリックします。
3. **Directory Service** 項目で **Not Use** を選択します。



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



5. 画面下部の **Apply** ボタンをクリックします。

> **注意**
>
> **Directory Service** 機能を **Not Use** に設定すると、**BioStar X** で **Entra ID** または **Active Directory** と連携しているすべての設定が解除されます。連携されたユーザーおよびグループ情報は削除されませんが、以降は同期されません。連携を解除する前に必ず確認してください。

リモートアクセスを設定する

リモートアクセス（Remote Access）は、ngrok サービスを通じて外部ネットワークから内部ネットワークへ安全に接続できる機能です。この機能を使用すると、ファイアウォール設定やポートフォワーディングを行わなくても、遠隔地から **BioStar X** サーバーに接続できます。

> **情報**
>
> - リモートアクセス（Remote Access）機能は、追加オプションで利用できます。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。リモートアクセスライセンスは年額のサブスクリプションです。
> - リモートアクセスライセンスを購入すると、Suprema はリモートアクセスライセンスを発行し、リモートアクセス利用用の ngrok Suprema サイトの bot アカウントとエンドポイントを作成して、ライセンス文書をユーザーに提供します。

> **注意**
>
> - リモートアクセス（Remote Access）機能は、サードパーティサービスである ngrok のトンネリングサービスを通じて提供されます。機能を使用する前に必ず Remote Access 機能使用同意 規約を確認してください。
> - BioStar X は単に ngrok API を呼び出して接続をサポートするだけであり、インターネット接続のセキュリティ、安全性、継続性は ngrok サービスに完全に依存します。したがって、本機能の使用中に発生し得るセキュリティ事故、データ損失、システム侵害などについて、Suprema は一切の責任を負いません。

いつ使用しますか？

次のような状況でリモートアクセス機能を使用してください。

- 外部ネットワークから社内の **BioStar X** サーバーに接続する必要がある場合
- ファイアウォールや NAT 環境により直接接続が困難な場合

- 複雑なネットワーク設定なしで簡単にリモート接続を構成したい場合
- 一時的に外部接続の権限を提供する必要がある場合

リモートアクセスの設定

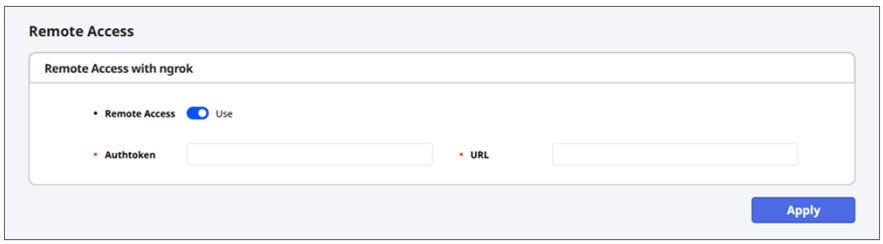
1 リモートアクセスライセンスの有効化

1. BioStar X 管理者 ID でログインします。
2. **Launcher**ページで**Settings**をクリックします。
3. 画面左のサイドバーで **License** → **BioStar X License** をクリックします。
4. Suprema から提供されたリモートアクセスライセンスキーと管理者名を入力し、**Activate** ボタンをクリックします。

> **情報**
> ライセンス登録の詳細については、BioStar Xライセンスをご参照ください。

2 リモートアクセスの有効化

1. BioStar X 管理者 ID でログインします。
2. **Launcher**ページで**Settings**をクリックします。
3. 画面左のサイドバーで **System** → **Remote Access** をクリック。
4. **Remote Access with ngrok** セクションで **Remote Access** オプションを **Use** に変更します。



3 ngrok 設定情報の入力

Suprema から提供された ngrok の設定情報を入力します。

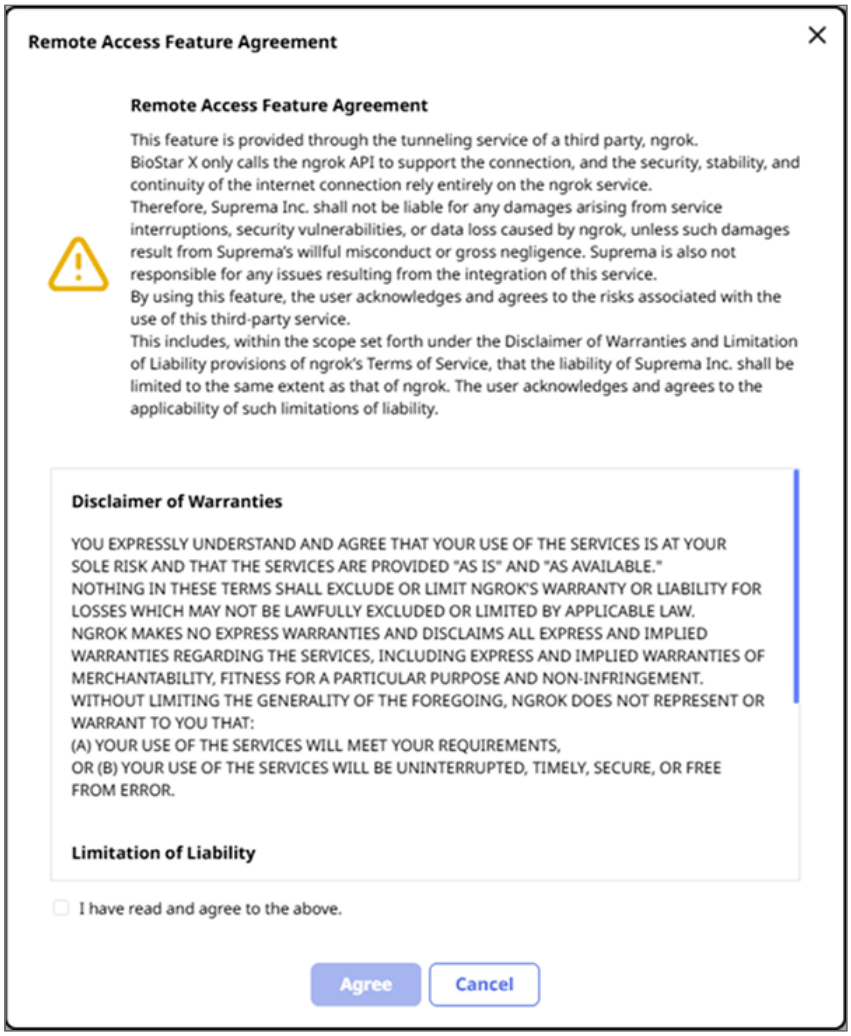
- **Authtoken**：Authtoken を入力します。
- **URL**：エンドポイント URL を入力します。 URL は `your-name.bsx.ngrok.app` 形式です。 URL は `https://subdomain.bsx.ngrok.app` 形式です。

情報

サブドメイン（subdomain）は以下のルールに従います。ルールに従っていないサブドメインは使用できません。

- 英字（A-Z、a-z）、数字（0-9）、ハイフン（-）のみ使用できます。
- 特殊文字や空白は使用できません。

1. すべての情報を入力したら、**Apply** ボタンをクリックします。
2. **Remote Access Feature Agreement**ウィンドウが表示されたら、内容を確認してください。



3. 利用規約に同意するチェックボックスをオンにして、**Agree** ボタンをクリックしてください。

エンドポイント URL への接続

設定を完了したら、**URL** 項目に入力したエンドポイント URL から外部ネットワークで **BioStar X** サーバーに接続できるか確認します。

情報

- エンドポイント URL にアクセスすると、**Settings** → **Audit Trail** → **AC Audit Log** で接続履歴を確認できます。

  例: [Remote Access] 192.168.1.100

- 外部ネットワークからエンドポイント URL で接続できない場合は、ライセンスを発行した販売店または代理店にお問い合わせください。

仮想デバイスのイベントログを連携する

仮想デバイス機能を使用すると、勤怠管理機能を連携する際にモバイルアプリや他社サービスで発生した出勤・退勤などのイベントを BioStar X に直接記録できます。実際の物理デバイスがなくてもイベントログを体系的に管理できるため、外部システムとの連携に役立ちます。

いつ使用しますか？

次のような場合に仮想デバイスのイベントログ連携機能を使用してください。

- 外部勤怠管理システムのイベントを BioStar X で統合管理する必要がある場合
- モバイルアプリや外部システムで発生した入退記録（Punch Log）を BioStar X に直接保存する必要がある場合（データベース連携なしで出勤／退勤イベントを記録）
- 他社アプリケーションやサービスから BioStar X API を通じて直接イベントを送信する必要がある場合

開始する前に

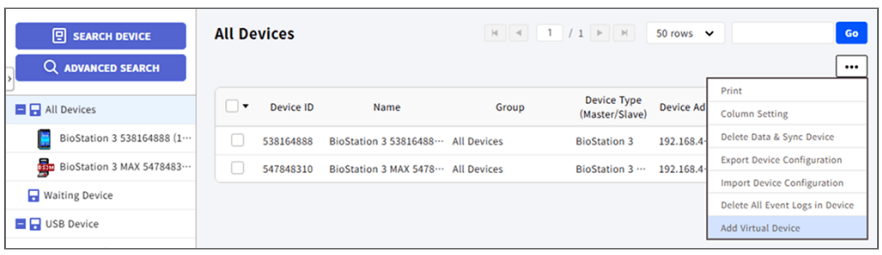
「イベントログ API」ライセンスが有効になっている必要があります。ライセンスポリシーの詳細については、ライセンス ポリシーを参照してください。

情報

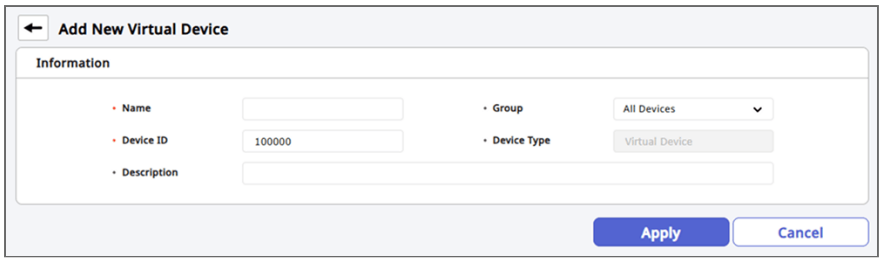
ライセンスの適用に関する詳細は、BioStar Xライセンスを参照してください。

仮想デバイスを登録する

1. **Launcher**ページで**Settings**をクリックします。
2. 画面左のサイドバーで **Device** → **Device** をクリック。
3. デバイス一覧で画面右上の ••• ボタンをクリックし、**Add Virtual Device** を選択します。



4. **Add Virtual Device** 画面が表示されたら設定情報を入力します。



   - **Name**：仮想デバイスの名前を入力します。
   - **Group**：仮想デバイスを割り当てるグループを選択します。
   - **Device ID**：仮想デバイスの固有 ID を入力します。既存のデバイス ID と重複しない範囲で指定する必要があります。
   - **Description**：仮想デバイスに関する説明を入力します。

5. 仮想デバイスを登録するには、画面右下の **Apply** ボタンをクリックします。

> **情報**
>
> - **Device ID** は 100000～999999 の範囲で指定できます。既存の Suprema デバイス ID と重複しない範囲で指定する必要があります。
> - 既に作成された **Device ID** の値は変更できません。

デバイスグループを管理する

仮想デバイスも通常のデバイスと同様にデバイスグループ機能を使用できます。

- 既存のデバイスと同じグループに配置できます。
- グループ権限があれば、そのグループ内の仮想デバイスにも権限を付与できます。

> **情報**
>
> デバイスグループの詳細については、デバイスグループを管理するを参照してください。

仮想デバイスの制限事項

- 仮想デバイスは次のメニューにのみ表示されます。
  - **Settings** → **Device** → **Device**
  - **Monitoring** メニューのすべてのイベントログ閲覧およびイベントログプレビュー
  - **Data** メニューのイベントログ閲覧
- 仮想デバイスは、ドアおよび **Advanced AC** で入退室制御機能を使用できません。
- **T&A** 用のデバイスとして指定できません。
- **Monitoring** メニューのサイドバーにはデバイス一覧として表示されません。

- デバイス制御機能は使用できません。
- 「マルチコミュニケーションサーバー」ライセンスのデバイス数には含まれません。

API でイベントログを記録する

対応イベントタイプ

次のイベントタイプのみ記録できます。

- **入退室許可** (Access granted：`4088`)
- **入退室拒否** (Access denied：`6400`)

API パラメーター

イベントログを記録するときは、次のパラメーターを指定する必要があります。

パラメーター	説明	必須かどうか
`dev_id`	登録済みの仮想デバイス ID のみ許可	必須
`evt`	Access Granted または Access Denied	必須
`datetime`	イベント発生時刻	必須
`user_id`	ユーザーID	必須
`tna_key`	指定された値のみ入力可能	任意

Request example

```
{
  "packet_device_id" : 100003, // required
  "is_virtual_device" : "true", // required
  "events":[ //4088 access granted, 6400 access denied
    {
      "dev_id": 100003, // required
      "evt": 6400, // required
      "datetime": "2025-08-21T14:12:00Z", // required
      "user_id": "2", // required
      "tna_key": "1"
    },
    {
      "dev_id": 100003,
      "evt": 6400,
      "datetime": "2025-08-21T14:13:01Z",
      "user_id": "2",
      "tna_key": "1"
    }
  ]
}
```

Response example

```
{
  "Response": {
    "code": "0",
    "link": "https://support.supremainc.com/en/support/home",
    "message": "Success"
  }
}
```

情報

- 単一 API 呼び出しで 1 つの仮想デバイスに対して複数のイベントログを一度に記録できます。
- API の利用に関する詳細はBioStar X APIを参照してください。

イベントログを照会する

仮想デバイスで記録したイベントログはメニューで照会できます。

- **Monitoring**：すべてのイベントの照会とフィルター、イベントプレビュー
- **Data**：すべてのイベントの照会とフィルター

情報

- **Monitoring** メニューでのイベント照会の詳細は、イベントをモニタリングするを参照してください。
- **Data** メニューに関する詳細は、レポートを作成するを参照してください。

監査トレイル

イベントログを記録すると、次の例のように監査トレイルが記録されます。

```
Access Granted, 2025/08/05 03:37:49, 12階出入口 外部, Administrator(1)
```

情報

- イベントを一括して記録しても、イベントごとに個別の監査トレイル項目が生成されます。
- **Audit Trail** について詳しくは、監査トレイルを管理するを参照してください。

トラブルシューティング

Add Virtual Device ボタンが表示されない場合

「イベントログ API」ライセンスが有効になっているか確認してください。

API 呼び出しが失敗する場合

- 「イベントログ API」ライセンスが有効になっているか確認してください。
- 登録されているデバイス ID が仮想デバイスであることを確認してください。
- API パラメーター形式が正しいか確認してください。

イベントが照会されない場合

- 記録したデバイスが正しい仮想デバイス ID であることを確認してください。
- イベントフィルターで該当の仮想デバイスが選択されているか確認してください。
- イベント記録時にエラーが発生していないか監査トレースを確認してください。

プラグイン

プラグイン (Plugins) とは？

BioStar X プラグイン (Plugins) は、**BioStar X** プラットフォームの拡張機能であり、顧客の特別な要件や既存システムとの連携のために追加機能を提供します。

> **情報**
>
> - プラグイン機能を使用するには、プラグイン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 ポリシーをご参照ください。
> - プラグイン開発の詳細については、BioStar X プラグイン開発者ガイドをご参照ください。

BioStar X提供プラグイン

ライセンス追加オプションで使用可能なプラグインの一覧です。

- 勤怠管理を使用
- 訪問者の申請と管理

> **情報**
> 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。

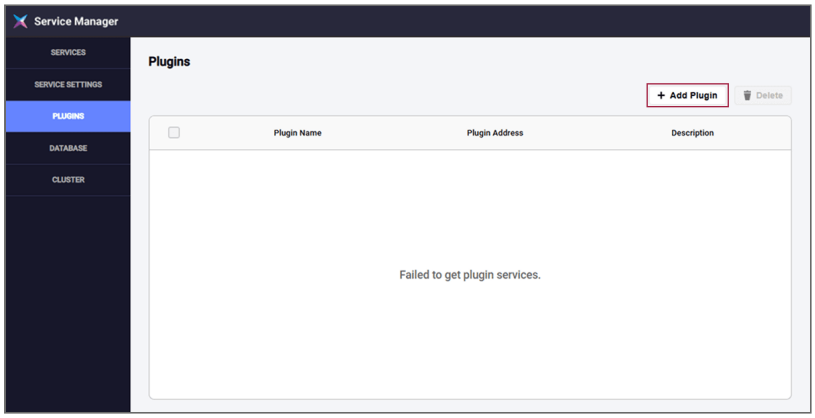
主要な活用事例

BioStar X のプラグインシステムを使用して、さまざまな外部システムと連携できます。代表的な活用事例は次のとおりです。

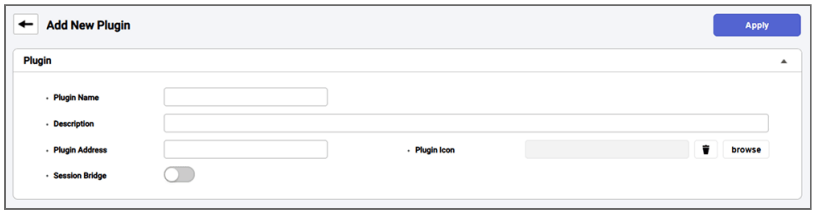
- **勤怠管理システム**：外部 T&A（Time & Attendance）ソリューションとの連携
- **来訪者管理システム**：別途の来訪者登録・管理システムとの連携
- **レポートソリューション**：カスタムレポートの作成および分析ツールとの連携
- **他社システム連携**：ERP、HRM など既存業務システムとのデータ連携

プラグインの登録

1. Windows で 開始 → **BioStar X** → **BioStar X Service Manager** をクリックします。
2. 画面左側のサイドメニューで**PLUGINS**をクリックします。
3. 画面右上の**Add Plugin**ボタンをクリックします。

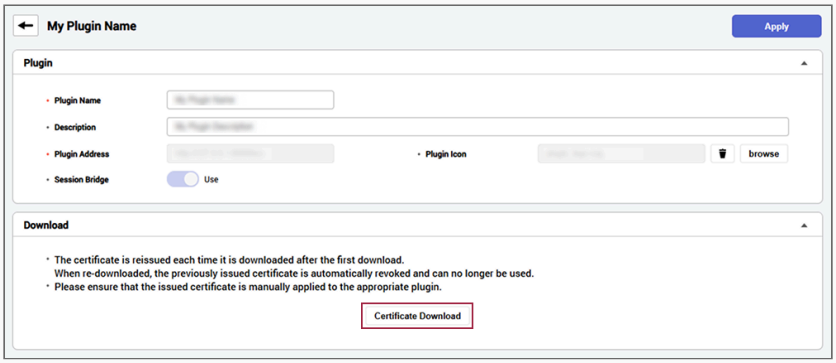


4. **Add New Plugin**画面でプラグイン情報を入力します。



5. プラグイン情報を入力し、登録を完了するには**Apply**ボタンをクリックします。

> **情報**
>
> **Session Bridge**を有効にした場合、画面下部から証明書をダウンロードできます。証明書は**BioStar X**とプラグイン間のセキュア通信に必要です。証明書を紛失した場合は再度ダウンロードできます。このとき既存の証明書は無効になります。



プラグイン情報の入力

- **Plugin Name**：プラグイン名を入力します。最大48文字まで入力できます。既に登録されているプラグインと同じ名前は使用できません。
- **Description**：プラグインの説明を入力します。最大500文字まで入力できます。
- **Plugin Address**：プラグインのアドレスを入力します。 `http://` または `https://` で始まる有効なURLである必要があり、既に登録されているプラグインと同じアドレスは使用できません。
- **Plugin Icon**：プラグインのアイコンをアップロードします。
  - 対応フォーマットはJPEG、PNG、SVG、GIFです。
  - ファイルサイズの上限は1MBで、0KBの空ファイルはアップロードできません。

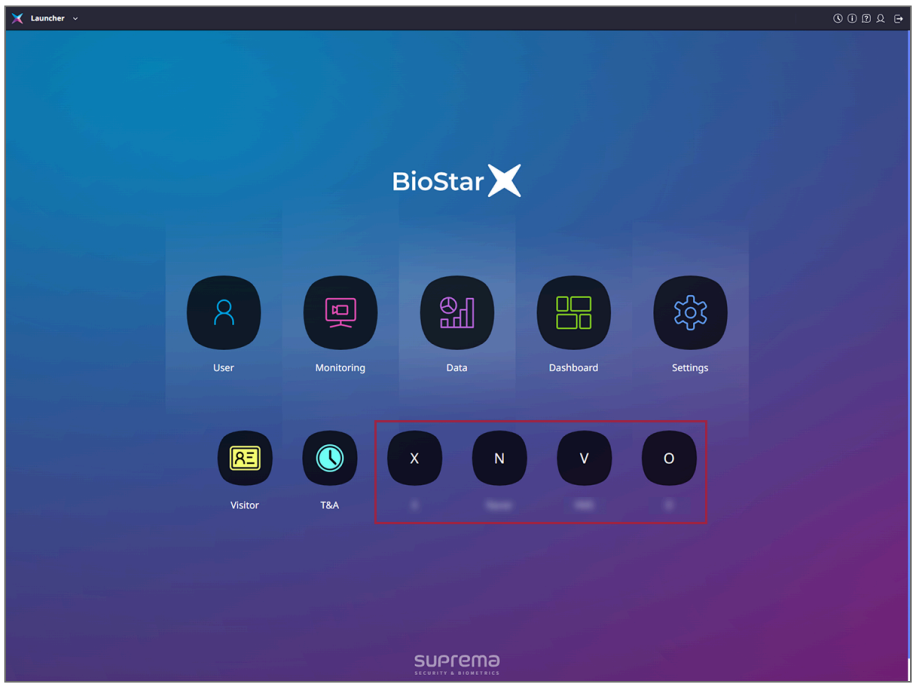
  - アップロードされた画像は104×104ピクセルに自動リサイズされます。

- **Session Bridge**：セッションブリッジを使用する場合は有効にします。この機能を使用すると、BioStar Xユーザーの権限が自動継承され、プラグインにアクセスする際に別途ログインする必要がありません。

> **情報**
>
> - アイコンをアップロードしない場合は、プラグイン名の先頭文字を使ってアイコンが自動生成されます。アップロードしたアイコンは ボタンをクリックして削除でき、削除すると自動生成アイコンに切り替わります。
> - **Session Bridge**を有効にすると無効化できず、セキュリティ上の理由からプラグインアドレスを変更できません。

ランチャー画面で確認

BioStar XのLauncher画面で追加したプラグインを確認できます。



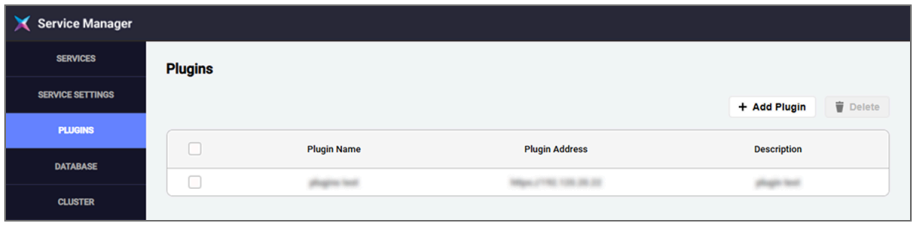
プラグインの管理

「BioStar X Service Manager」でインストールしたプラグインを管理できます。

Windows で 開始 → BioStar X → BioStar X Service Manager をクリックします。 「BioStar X Service Manager」画面のサイトメニューでPLUGINSをクリックします。

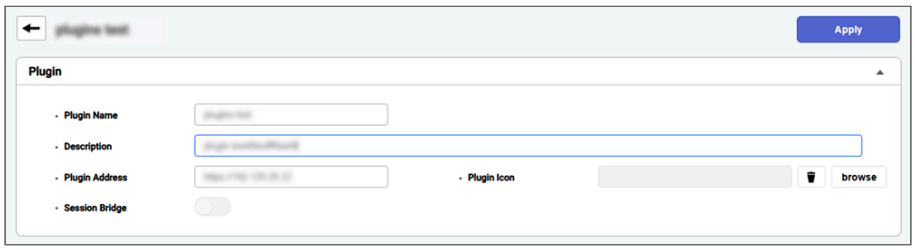
プラグイン一覧の確認

ユーザーが登録したすべてのプラグインを確認できます。



プラグインの編集

プラグイン一覧から編集するプラグインをクリックします。プラグイン情報の編集画面が表示されます。 **Plugin Name**（プラグイン名）、**Description**（説明）、**Plugin Icon**（アイコン）を編集できます。



> **情報**
> **Session Bridge**が有効な状態では、**Plugin Address**は編集できません。

プラグインの削除

1. プラグイン一覧で削除するプラグインの一番左のチェックボックスをクリックして選択します。
2. 画面右上の **Delete**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 **OK** をクリックします。

> **情報**
> - 勤怠管理ライセンスを適用して追加された勤怠管理 (T&A) プラグインは削除できません。
> - 勤怠管理プラグインは追加オプションで利用できます。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。

勤怠管理を使用

勤怠管理ルールを設定し、デバイスで記録された勤務データを確認するかレポートとして出力します。 T&A 機能はプラグイン形式で提供され、別途ライセンスが必要です。

> **情報**
> T&A機能は追加オプションで利用できます。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。

開始する前に

T&A 機能を使用するにはライセンスを適用し、別途インストーラーをダウンロードしてインストールする必要があります。

ライセンス適用

T&A ライセンスの適用手順を案内します。 **BioStar X** の購入先から T&A ライセンスを購入した後、次の手順に従ってライセンスを適用してください。

1. **BioStar X** の管理者アカウントでログインしてください。
2. **Launcher**ページで**Settings**をクリックします。
3. 画面左のサイドバーで **License** → **BioStar X License** をクリックします。
4. **License Activation**で、**Activated by**と**License Key**の項目を順に入力します。



5. **Activate** ボタンをクリックします。

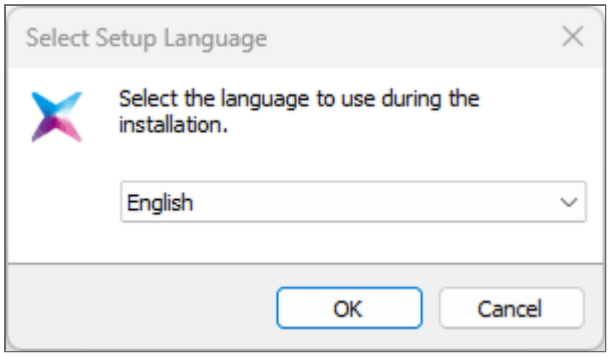
登録したライセンスは **Activated License** で確認できます。

> **情報**
> インターネット接続が制限されているオフライン環境や閉域ネットワーク環境でライセンスを有効化するには、BioStar Xライセンスを参照してください。

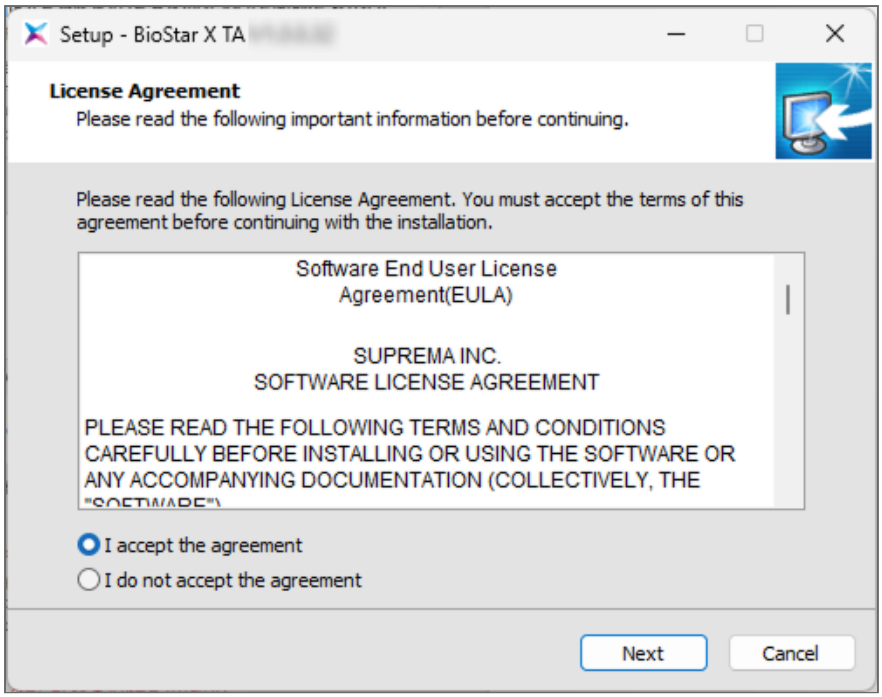
プラグインのインストール

T&A 機能を使用するには別途インストーラーをダウンロードしてインストールする必要があります。次の手順に従ってプラグインをインストールしてください。

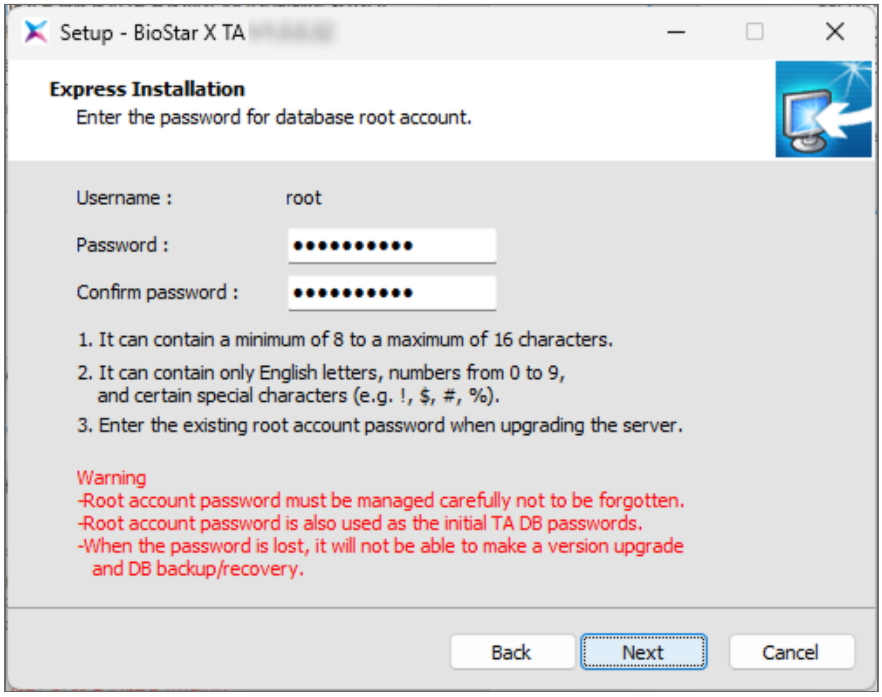
1. Supremaダウンロードセンター にアクセスし、T&A プラグインのインストールファイル(*BioStar X TA.X.Y.Z.BB.exe*) をダウンロードしてください。
2. インストーラを実行し、案内に従ってインストールを完了してください。
3. ダウンロードしたインストールファイルを実行してください。
4. 使用する言語を選択し、**OK** ボタンをクリックしてください。



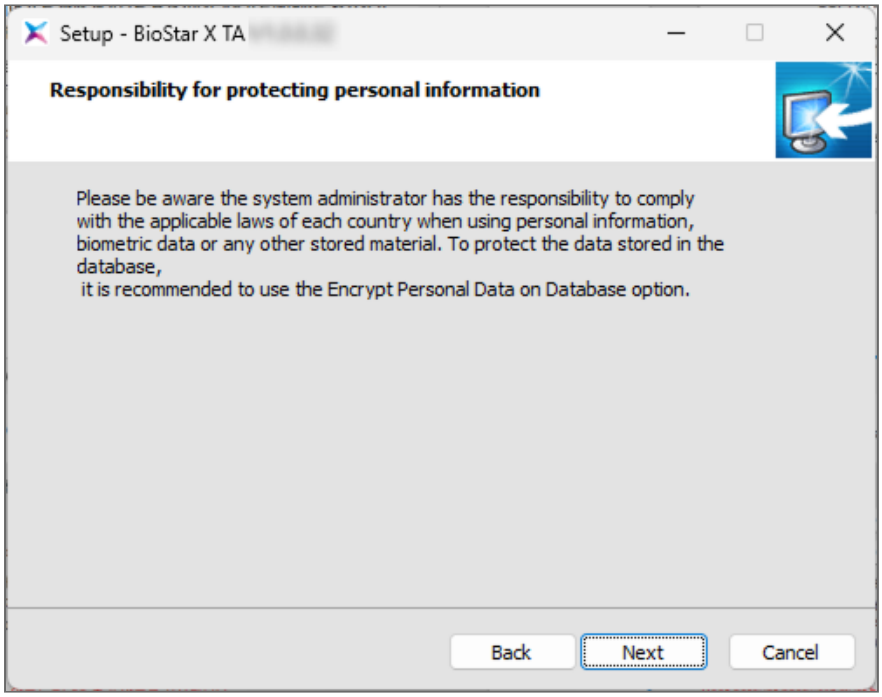
5. インストールを続行するには、**同意する** を選択し、**次へ** ボタンをクリックしてください。



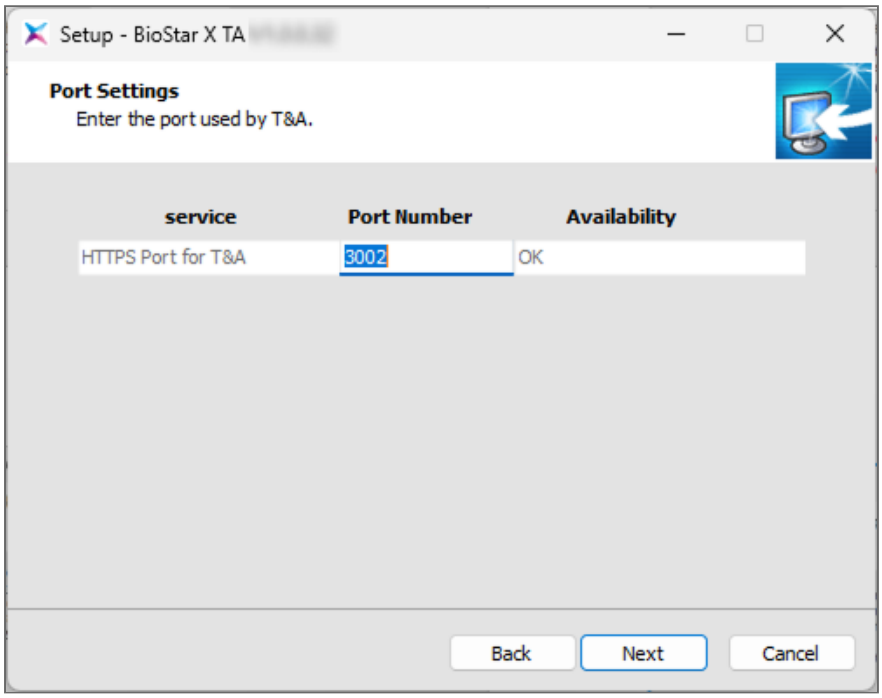
6. データベースの root アカウントのパスワードを入力し、**次へ** ボタンをクリックしてください。



7. データベースに保存される個人情報の管理権限および責任に関する案内を読み、インストールを続行するには **次へ** ボタンをクリックしてください。

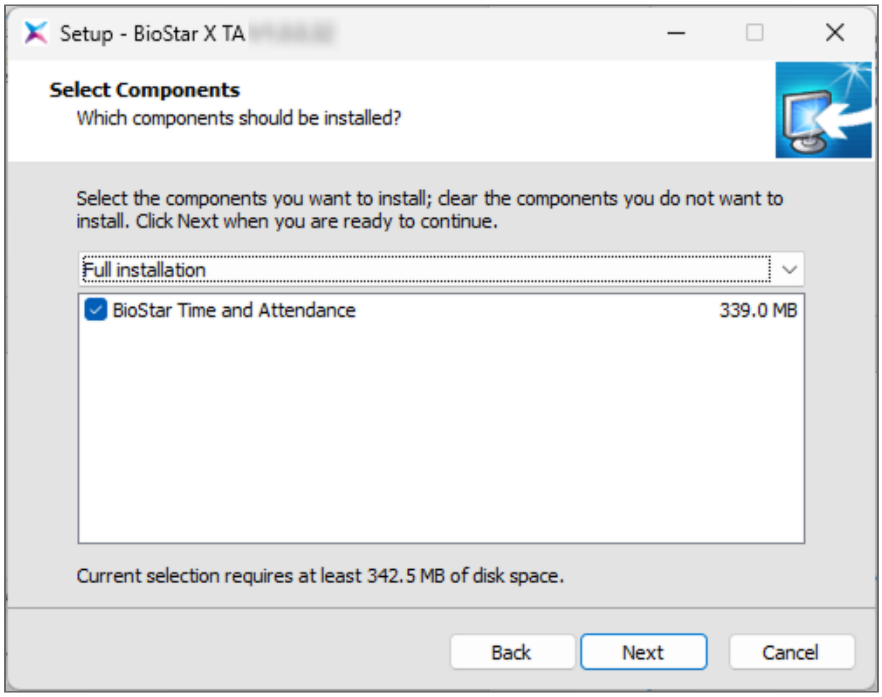


8. **BioStar X** と通信するポートを設定し、**次へ** をクリックしてください。

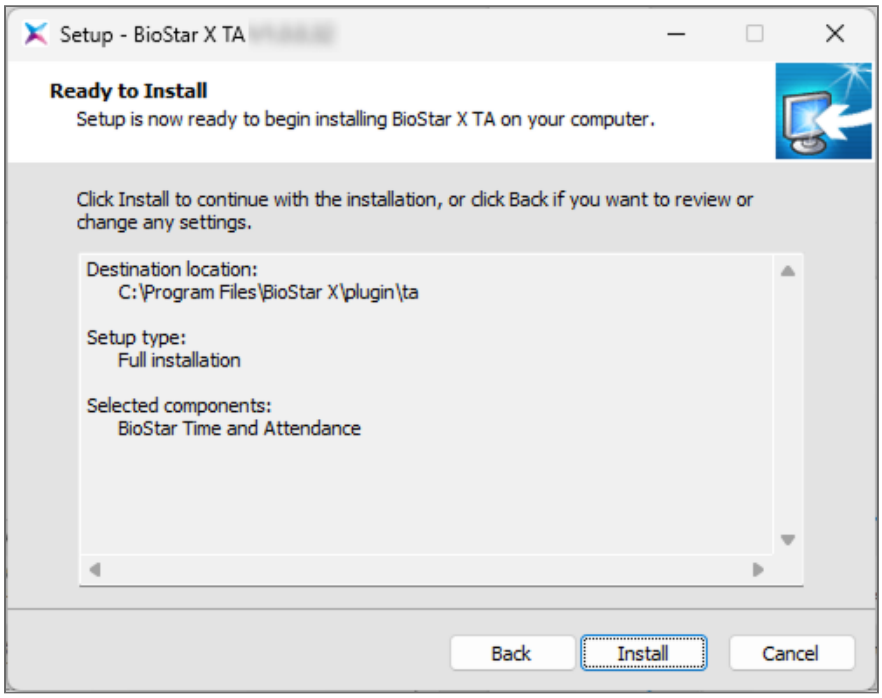


> ポート番号はデフォルト値（3002）を使用するか、別のポート番号に変更できます。ポート番号を変更した場合は、ファイアウォールでそのポートが開放されていることを確認してください。

9. インストールコンポーネントを選択し、**次へ** をクリックしてください。



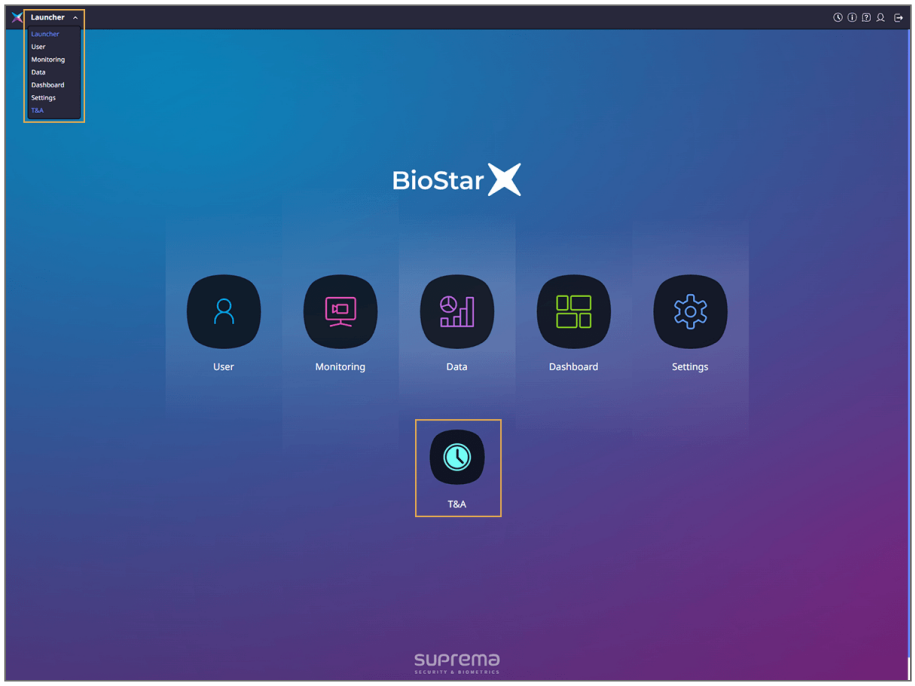
10. すべてのインストール準備が完了したら、**インストール** ボタンをクリックしてください。



> **情報**
>
> - ダウンロードしたファイル名の `X.Y.Z` はバージョン情報、`BB` はビルド番号です。
> - データベースのルート（root）アカウントのパスワードには、**BioStar X** をインストールしたときに設定したパスワードを使用してください。

T&A メニュー

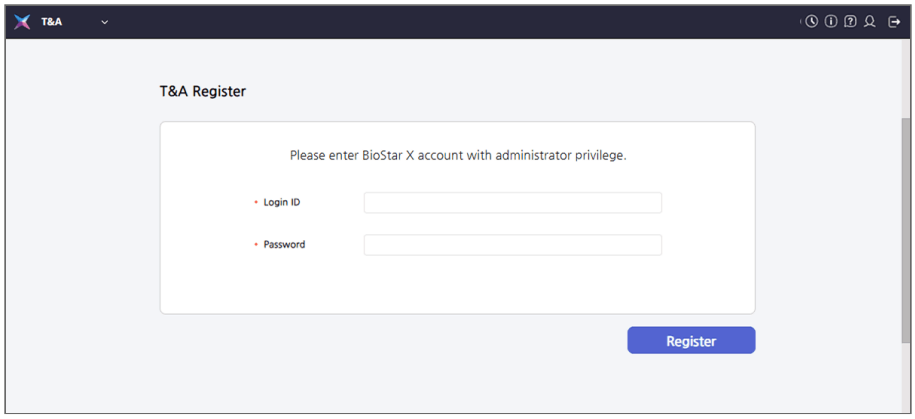
T&A ライセンスとプラグインのインストールが完了すると、**Launcher** ページに **T&A** メニューが追加されます。



Launcher ページで **T&A** アイコンをクリックするか、画面左上のショートカットリストから **T&A** を選択してください。

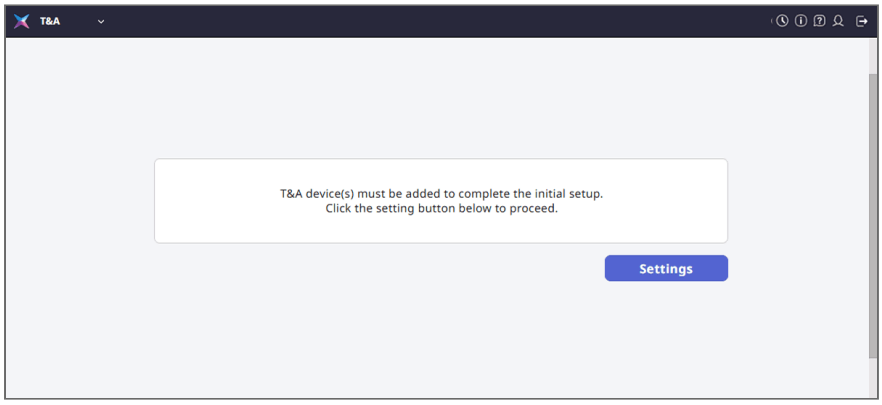
T&A ログイン

T&A 機能に初めてアクセスすると、専用のログイン画面が表示されます。 **BioStar X** の管理者アカウントでログインしてください。一度管理者アカウントで T&A 機能にログインすると、その後は追加のログインなしで T&A 機能を使用できます。

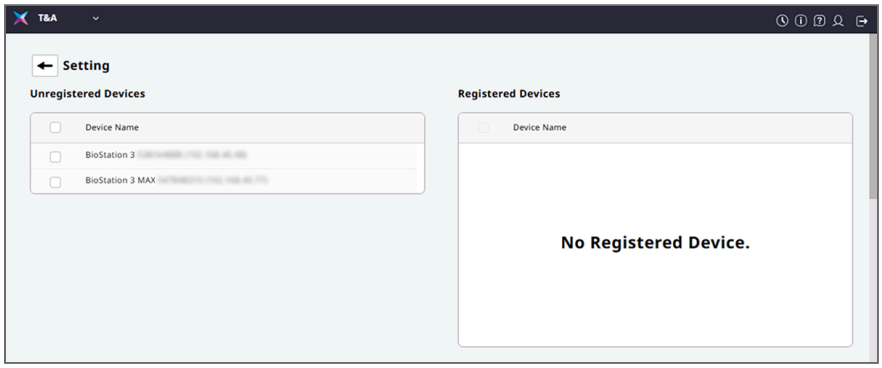


初期設定

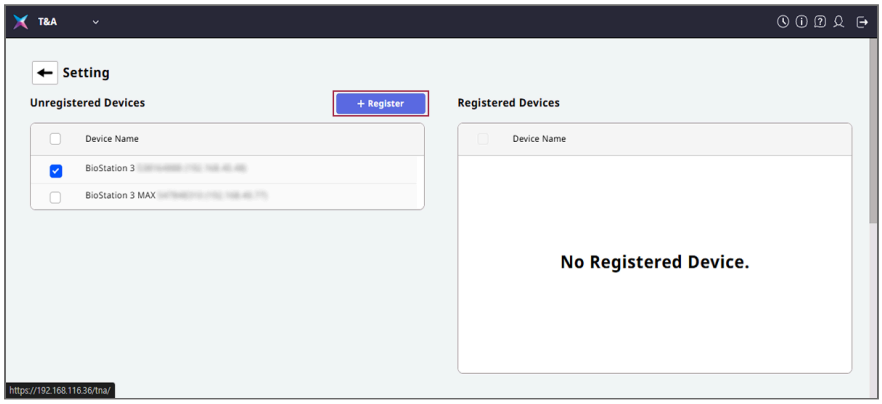
1. T&A 機能に初めてログインしたら、初期設定のために勤怠管理用デバイスを追加する必要があります。画面で **Settings** をクリックしてください。



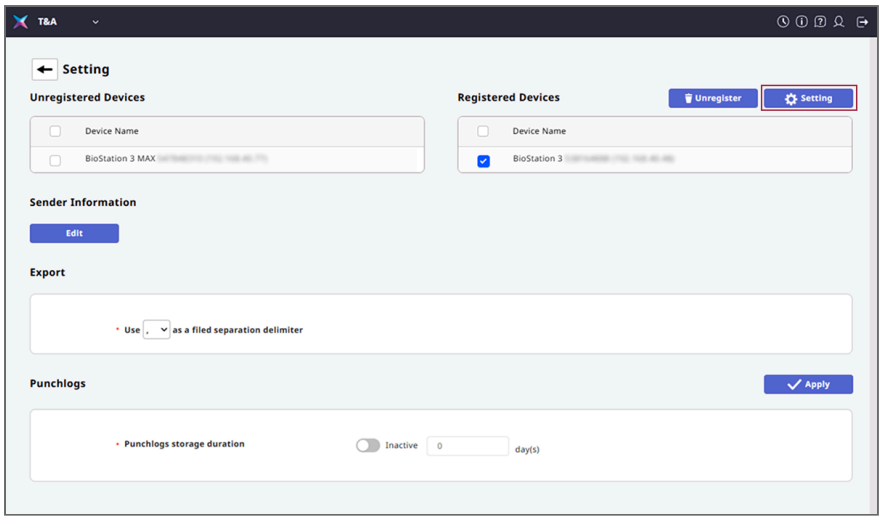
2. デバイスリストから勤怠管理に使用するデバイスを選択してください。



3. 有効になった ＋ **Register** をクリックしてください。



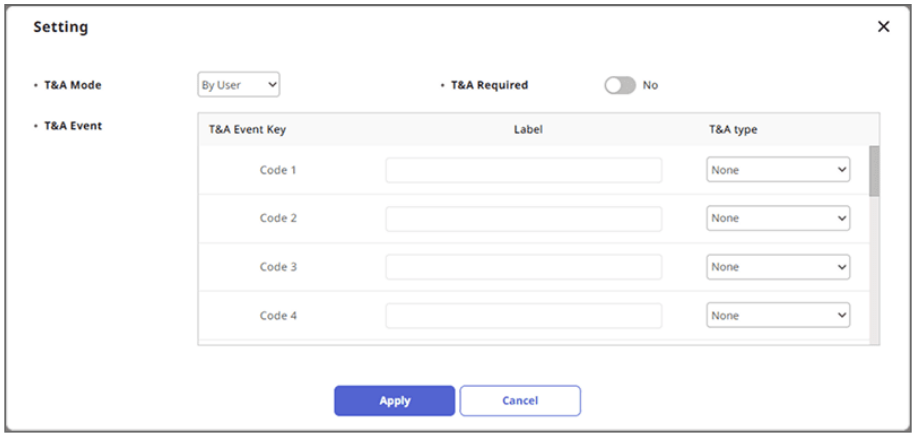
4. 選択したデバイスが **Registered Devices** リストに表示されたら、**Setting** をクリックしてください。



5. **Setting** ウィンドウが表示されたら、勤怠管理の基本設定を完了してください。

勤怠モード設定

勤怠モードと勤怠イベントの設定を行ってください。



- **T&A Mode**：勤怠イベントの登録方法を選択してください。
  - **By User**：認証時にユーザーが勤怠イベントを選択できます。
  - **By Schedule**：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。
  - **Last Choice**：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。
  - **Fixed**：選択した勤怠イベントのみを使用できます。
  - **Not Use**：勤怠イベントを記録しません。
- **T&A Required**：認証時に必ず勤怠イベントを登録するように設定できます。 **T&A Mode** を **By User** に設定した場合に使用できます。
- **T&A Event**：勤怠イベントの名前を変更するか、**T&A Mode** を **By Schedule** に設定した場合に使用されるスケジュールを追加できます。
  - **T&A Event Key**：勤怠登録に使用できるキーの一覧です。
  - **Label**：勤怠キーに応じて勤怠イベント名を変更できます。
  - **Schedule**：**T&A Mode** を **By Schedule** に設定した場合に自動で切り替わるスケジュールを設定できます。スケジュール設定の詳細については、スケジュールを設定するをご参照ください。

情報

- LCD 画面をサポートしないデバイスは、**T&A Mode** を **By Schedule** または **Fixed** に設定できます。固定された勤怠イベントを登録するか、あらかじめ設定されたスケジュールに従って変更される勤怠イベントを登録できます。
- 次の機種が**By Schedule**と**Fixed**モードに対応しています：XPass Q2、XPass 2、XPass D2、BioEntry W3、BioEntry P2、BioEntry W2。
- **Setting** メニューの詳細については、勤怠管理を設定するをご参照ください。

勤務規則を設定する

勤務スケジュールを時間・日・週単位で設定し、勤怠管理規則を構成する方法を案内します。

勤務規則を初めて登録する場合は、次の順序で設定します。

1 Time Code

勤怠記録管理、残業、欠勤に関する時間規則を設定できます。時間当たりの重み付けを設定でき、ひと目でわかるように色を指定して表示できます。

Time Codeの設定の詳細については、時間ルールを設定するを参照してください。

2 Shift

1日（24時間）単位の勤務規則を設定できます。勤務規則には、時間別の時間規則設定、1日の開始時間設定、時間の丸め規則などが含まれます。

Shiftの設定の詳細については、日次勤務規則を設定するを参照してください。

3 Schedule Template

設定された 1 日単位の勤務規則で週次勤務規則を設定します。週別または日別で週次勤務規則を設定します。

Schedule Templateの設定の詳細については、週次勤務規則を設定するを参照してください。

4 Rule

日次勤務規則に残業時間規則を追加していない場合に便利に使用できます。日次勤務規則で設定する残業は開始時刻と終了時刻を持ちますが、**Rule** は所定勤務時間を超えた合計時間を計算します。**Rule**は日別/週別/月別の総残業時間を管理する際に便利に使用でき、**Rule**を設定すると、勤務規則に追加された残業時間規則の代わりに適用されます。

Ruleの設定の詳細については、その他の勤務規則を設定するを参照してください。

5 勤務スケジュール

前のステップで設定した勤務スケジュールを適用する期間、ユーザー、その他の勤務規則、休暇日程を設定できます。

Scheduleの設定の詳細については、勤務スケジュールを設定するを参照してください。

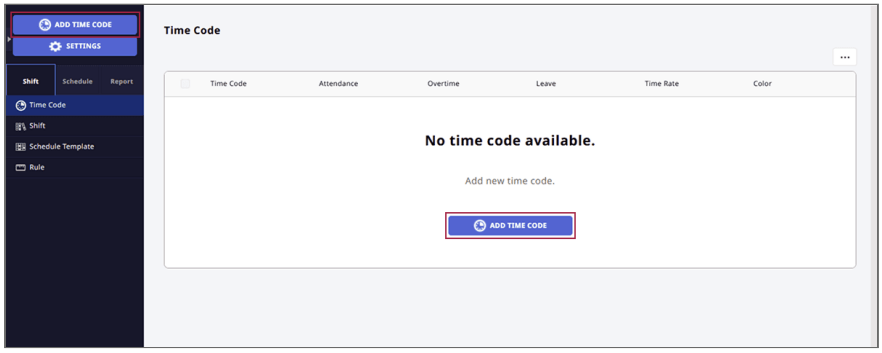
時間ルールを設定する

勤務時間の計算に使用する Time Code の設定方法を案内します。通常勤務用の時間ルール、残業用の時間ルール、不在用の時間ルールを設定できます。各 Time Code は時間当たりの重みを個別に設定して使用できます。

ADD TIME CODE

1. **Launcher** ページで **T&A** をクリックします。

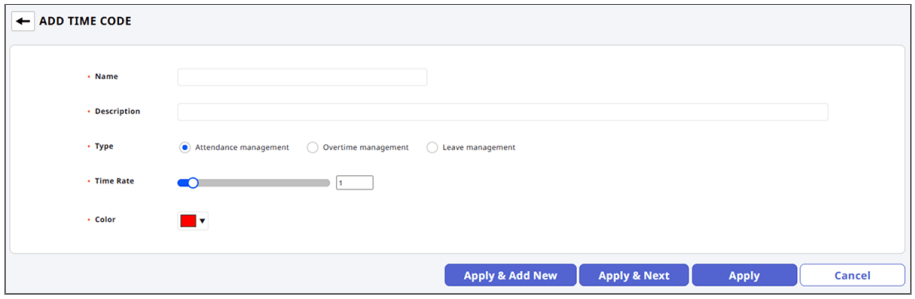
2. 画面左のサイドバーで **Shift** → **Time Code** をクリックします。
3. **ADD TIME CODE** ボタンをクリックします。



4. **ADD TIME CODE** 画面が表示されたら、各項目を設定します。

> **情報**
>
> - 設定を保存するには、画面下部の **Apply** をクリックします。
> - 続けて Shift を追加する場合は、**Apply & Next** ボタンをクリックします。
> - 設定を保存した後に別の **Time Code** を追加する場合は、**Apply & Add New** ボタンをクリックします。

設定オプションガイド



- **Name**：Time Code の名前を入力します。
- **Description**：Time Code の説明を入力します。
- **Type**：Time Code の種類を選択します。
  - **Attendance management**：通常勤務に使用する Time Code として設定します。
  - **Overtime management**：残業に使用する Time Code として設定します。
  - **Leave management**：外出、外勤、出張、休暇などに使用する Time Code として設定します。
- **Time Rate**：Time Code に応じた時間当たりの重みを設定します。 **1** は基本の重みで、**2** に設定すると、設定された Time Code が適用される際に勤務時間が時間当たり2倍で計算されます。
- **Color**：Time Code を区別する色を設定します。

次のステップ

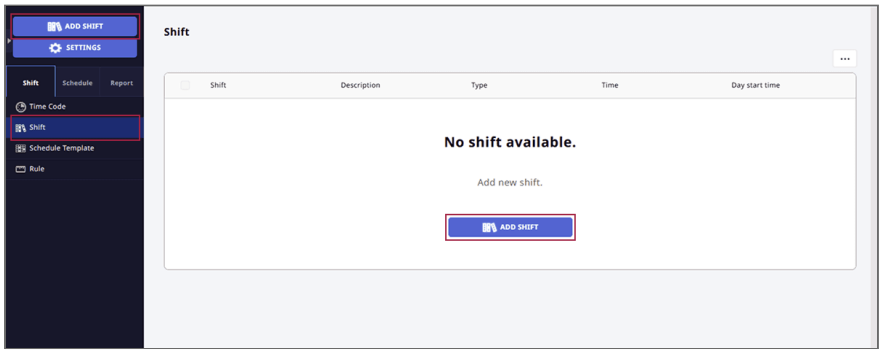
1日（24時間）単位の勤務規則を設定できます。勤務規則には、時間別の時間規則設定、1日の開始時間設定、時間の丸め規則などが含まれます。

日次勤務規則を設定する

24時間を基準に、時刻に応じて異なる時間規則を適用して勤務規則を作成します。固定勤務、フレックスタイム勤務、フローティング勤務を選択し、1日の開始時刻や時間の丸め規則などを設定します。

ADD SHIFT

1. **Launcher** ページで **T&A** をクリックします。
2. 画面左のサイドバーで **Shift** → **Shift** をクリックします。
3. **ADD SHIFT** をクリックします。



4. **ADD SHIFT** 画面が表示されたら、各項目を設定します。

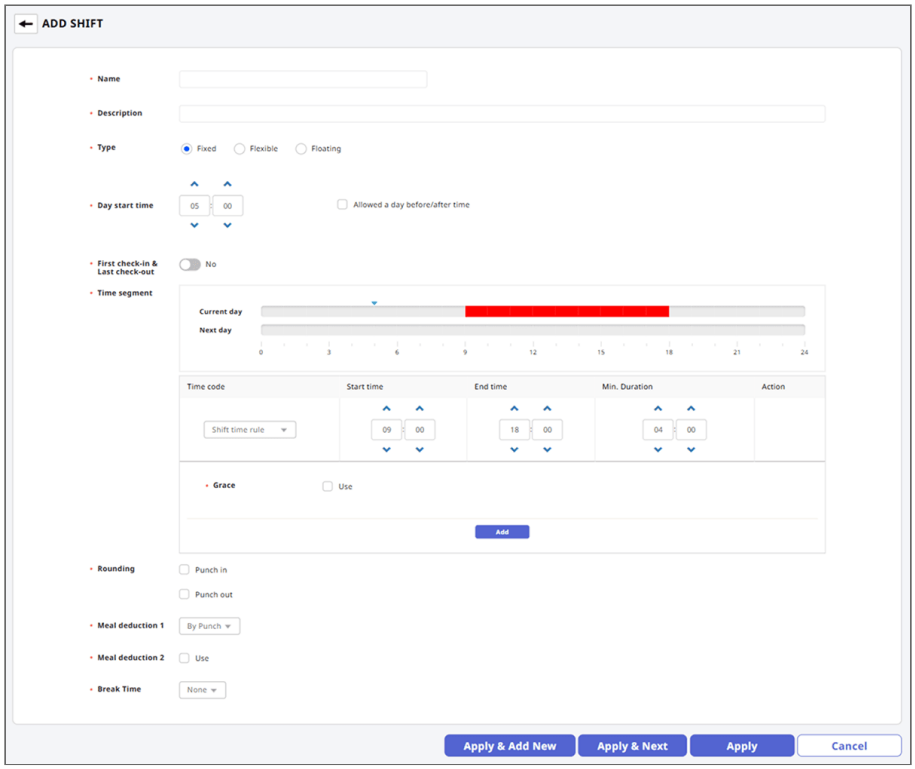
> **情報**
>
> - 設定を保存するには、画面下部の **Apply** をクリックします。
> - 週次勤務規則を続けて追加するには、**Apply & Next** をクリックします。
> - 設定を保存した後に別の **Shift** を追加するには、**Apply & Add New** をクリックします。

設定オプションガイド

勤務規則の種類に応じて、**Fixed**、**Flexible**、**Floating** のいずれかを選択します。選択した勤務規則の種類によって設定オプションが異なる場合があります。

Fixed

定められた時刻に出勤と退勤を行う勤務規則です。 Shift の名前と説明を入力し、**Type** で **Fixed** を選択します。



- **Day start time**：1日の勤務開始時刻を設定します。

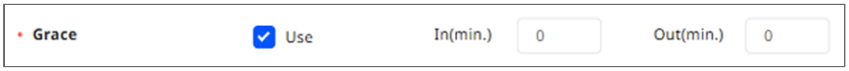
  Allowed a day before/after timeを使用すると、設定した1日の開始時刻を基準に24時間を超える勤務時間に対する勤務ルールを設定できます。最大で6時間まで設定できます。



- **First check-in & Last check-out**：このオプションを有効にすると、ユーザーが最初に認証した時刻を出勤時刻として記録し、最後に認証した時刻を退勤時刻として記録します。

> **情報**
>
> このオプションを有効にする場合、ユーザーの休憩時間を記録するために**Break by Punch**を設定する必要があります。

- **Time segment**：**Time code**列で勤怠記録を設定した項目を選択してから、**Start time**、**End time**、**Min. Duration**を設定します。
  - **Grace**：設定した時刻より遅く出勤したり早く退勤した場合でも通常勤務として認める猶予時間を設定します。



- **Rounding**：出勤と退勤の時刻を自動で丸めることができます。出勤と退勤それぞれについて単位と基準を設定します。



  - **Unit(min)**：設定された開始時刻より早いまたは遅い出勤イベントが登録された場合に、その時刻を丸めるルールを設定できます。

- **Point(min)**：設定された終了時刻より早いまたは遅い退勤イベントが登録された場合に、その時刻を丸めるルールを設定できます。

> **ヒント**
> たとえば、出勤時刻が09:00に設定され、**Unit(min)**が15分、**Point(min)**が8分に設定されている場合、次のように丸められます。
> - 09:07 出勤 → 09:00 に切り捨て（基準 8 分未満）
> - 09:08 出勤 → 09:15 に切り上げ（基準 8 分以上）

> **情報**
> **Rounding** ルールは **Grace** より先に適用されます。

- **Meal deduction 1** / **Meal deduction 2**：1日の勤務時間から食事時間を控除するように設定できます。
  - **By Punch**：固定の食事控除時間を設定せず、勤怠登録デバイスに記録された時間に基づいて控除するように設定できます。
  - **Auto**：**Deduction time**と**Minimal hours before deduction**を設定して、食事時間を自動で控除するように設定できます。
  - **Fixed**：**Start time**と**End time**を設定して、固定時間を控除するように設定できます。

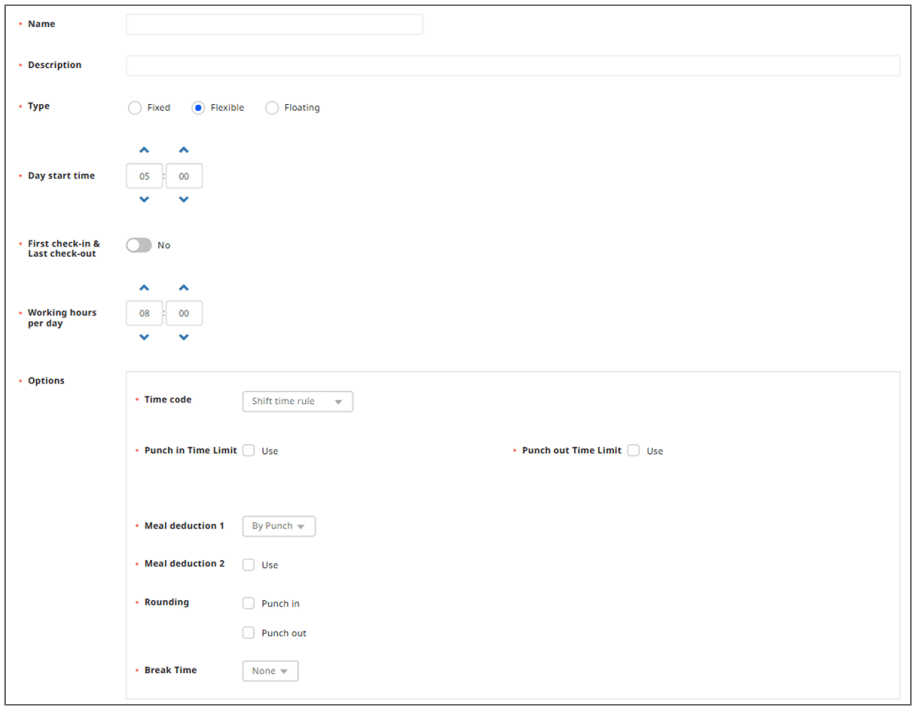
> **情報**
> - **Meal deduction 2**を使用すると、1日の勤務時間から2回の食事時間を控除できます。
> - **Auto**または**Fixed**を食事控除の種類として使用する場合、**Meal deduction 1**と**Meal deduction 2**は同じ種類にのみ設定できます。

- **Break Time**：休憩時間を設定できます。
  - **By Punch**：固定の休憩時間を設定せず、勤怠登録デバイスに記録された時間に従うように設定できます。このオプションを有効にすると、**Max. allowed break time(min.)**を設定できます。
  - **Fixed**：**Start time**と**End time**を設定して、固定時間をユーザーの休憩時間として設定できます。

> **情報**
> - **Attendance management** に設定された時間規則は、Shift に 1 つだけ追加できます。
> - **Overtime management** に設定された時間規則では、**Start time**、**End time**、**Min. Duration**、**Rounding** を設定できます。

フレックスタイム勤務

1日の勤務時間を設定し、1日の開始時刻を基準に出勤および退勤時刻を柔軟に調整する勤務規則です。 Shift の名前と説明を入力し、**Type** で **Flexible** を選択します。



- **Day start time**：1日の勤務開始時刻を設定します。
- **First check-in & Last check-out**：このオプションを有効にすると、ユーザーが最初に認証した時刻を出勤時刻として記録し、最後に認証した時刻を退勤時刻として記録します。

> **情報**
> このオプションを有効にする場合、ユーザーの休憩時間を記録するために**Break by Punch**を設定する必要があります。

- **Working hours
per day**：1日の総勤務時間を設定します。
- **Time code**：勤怠記録を設定した項目を選択します。
- **Punch in Time Limit** / **Punch out Time Limit**：ユーザーが出勤および退勤時刻を認証できる時間範囲を設定できます。



- **Meal deduction 1** / **Meal deduction 2**：1日の勤務時間から食事時間を控除するように設定できます。
  - **By Punch**：固定の食事控除時間を設定せず、勤怠登録デバイスに記録された時間に基づいて控除するように設定できます。
  - **Auto**：**Deduction time**と**Minimal hours before deduction**を設定して、食事時間を自動で控除するように設定できます。
  - **Fixed**：**Start time**と**End time**を設定して、固定時間を控除するように設定できます。

> **情報**
>
> - **Meal deduction 2**を使用すると、1日の勤務時間から2回の食事時間を控除できます。
> - **Auto**または**Fixed**を食事控除の種類として使用する場合、**Meal deduction 1**と**Meal deduction 2**は同じ種類にのみ設定できます。

- **Rounding**：出勤と退勤の時刻を自動で丸めることができます。出勤と退勤それぞれについて単位と基準を設定します。



  - **Unit(min)**：設定された開始時刻より早いまたは遅い出勤イベントが登録された場合に、その時刻を丸めるルールを設定できます。
  - **Point(min)**：設定された終了時刻より早いまたは遅い退勤イベントが登録された場合に、その時刻を丸めるルールを設定できます。

> **ヒント**
>
> たとえば、出勤時刻が09:00に設定され、**Unit(min)**が15分、**Point(min)**が8分に設定されている場合、次のように丸められます。
>
> - 09:07 出勤 → 09:00 に切り捨て（基準 8 分未満）
> - 09:08 出勤 → 09:15 に切り上げ（基準 8 分以上）

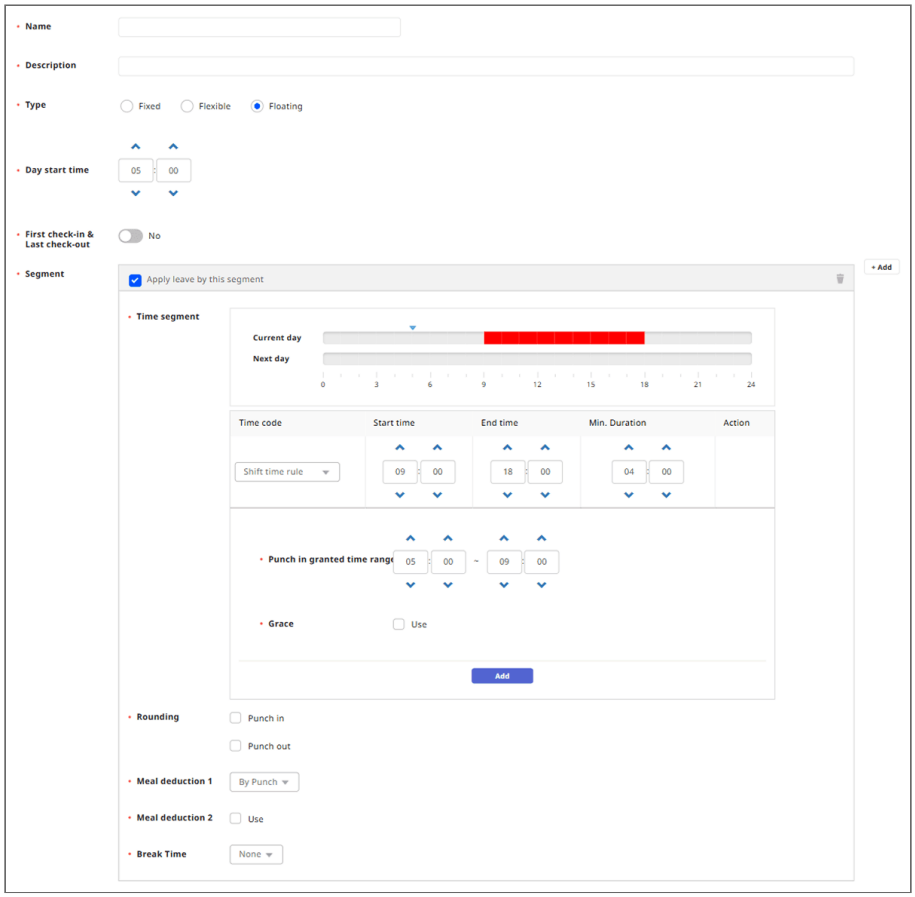
> **情報**
>
> **Rounding** ルールは **Grace** より先に適用されます。

- **Break Time**：休憩時間を設定できます。
  - **By Punch**：固定の休憩時間を設定せず、勤怠登録デバイスに記録された時間に従うように設定できます。このオプションを有効にすると、**Max. allowed break time(min.)**を設定できます。
  - **Fixed**：**Start time**と**End time**を設定して、固定時間をユーザーの休憩時間として設定できます。

> **情報**
>
> **Overtime management** に設定された時間規則は追加できません。

フローティング勤務

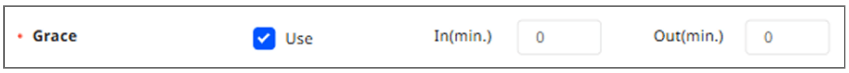
出勤と退勤時刻を自由に設定できる勤務規則です。 Shift の名前と説明を入力し、**Type** で **Floating** を選択します。



- **Day start time**：1日の勤務開始時刻を設定します。
- **First check-in & Last check-out**：このオプションを有効にすると、ユーザーが最初に認証した時刻を出勤時刻として記録し、最後に認証した時刻を退勤時刻として記録します。

> **情報**
> このオプションを有効にする場合、ユーザーの休憩時間を記録するために**Break by Punch**を設定する必要があります。

- **Time segment**：**Time code**列で勤怠記録を設定した項目を選択してから、**Start time**、**End time**、**Min. Duration**を設定します。
  - **Punch in granted time range**：設定された出勤・退勤時刻より早く出勤したり遅く退勤した場合に、通常勤務として認める時間範囲を設定します。
  - **Grace**：設定した時刻より遅く出勤したり早く退勤した場合でも通常勤務として認める猶予時間を設定します。



- **Rounding**：出勤と退勤の時刻を自動で丸めることができます。出勤と退勤それぞれについて単位と基準を設定します。



  - **Unit(min)**：設定された開始時刻より早いまたは遅い出勤イベントが登録された場合に、その時刻を丸めるルールを設定できます。

- **Point(min)**：設定された終了時刻より早いまたは遅い退勤イベントが登録された場合に、その時刻を丸めるルールを設定できます。

> **ヒント**
> たとえば、出勤時刻が09:00に設定され、**Unit(min)**が15分、**Point(min)**が8分に設定されている場合、次のように丸められます。
>
> - 09:07 出勤 → 09:00 に切り捨て（基準 8 分未満）
> - 09:08 出勤 → 09:15 に切り上げ（基準 8 分以上）

> **情報**
> **Rounding** ルールは **Grace** より先に適用されます。

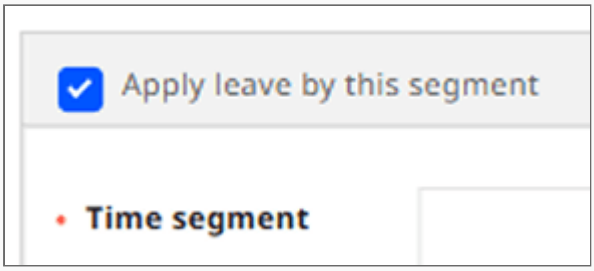
- **Meal deduction 1** / **Meal deduction 2**：1日の勤務時間から食事時間を控除するように設定できます。
  - **By Punch**：固定の食事控除時間を設定せず、勤怠登録デバイスに記録された時間に基づいて控除するように設定できます。
  - **Auto**：**Deduction time**と**Minimal hours before deduction**を設定して、食事時間を自動で控除するように設定できます。
  - **Fixed**：**Start time**と**End time**を設定して、固定時間を控除するように設定できます。

> **情報**
>
> - **Meal deduction 2**を使用すると、1日の勤務時間から2回の食事時間を控除できます。
> - **Auto**または**Fixed**を食事控除の種類として使用する場合、**Meal deduction 1**と**Meal deduction 2**は同じ種類にのみ設定できます。

- **Break Time**：休憩時間を設定できます。
  - **By Punch**：固定の休憩時間を設定せず、勤怠登録デバイスに記録された時間に従うように設定できます。このオプションを有効にすると、**Max. allowed break time(min.)**を設定できます。
  - **Fixed**：**Start time**と**End time**を設定して、固定時間をユーザーの休憩時間として設定できます。

情報

- 勤務組は最大 5 つの時間スロットで構成できます。 **+ Add** をクリックして時間スロットを追加します。
- 不在を設定する際は、**Apply leave by this segment** オプションを選択する必要があります。 **Apply leave by this segment** は勤務組で構成した時間スロットから選択できます。



- **Overtime management** に設定された時間規則では、**Start time**、**End time**、**Min. Duration**、**Rounding** を設定できます。

次のステップ

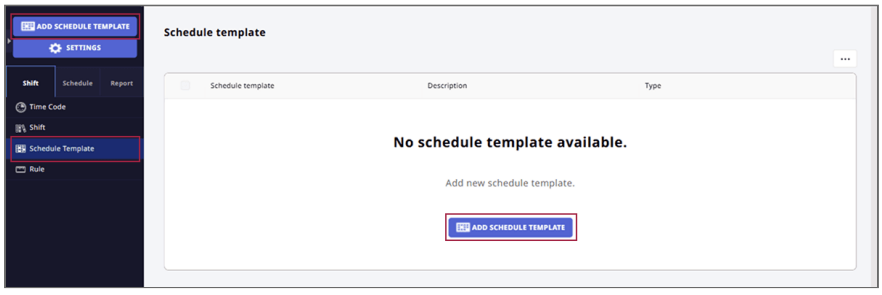
設定された 1 日単位の勤務規則で週次勤務規則を設定します。週別または日別で週次勤務規則を設定します。

週次勤務規則を設定する

設定した Shift を基に、週単位の勤務規則を作成する方法を案内します。

ADD SCHEDULE TEMPLATE

1. **Launcher** ページで **T&A** をクリックします。
2. 画面左側のサイドバーで **Shift** → **Schedule Template** をクリックします。
3. **ADD SCHEDULE TEMPLATE** ボタンをクリックします。

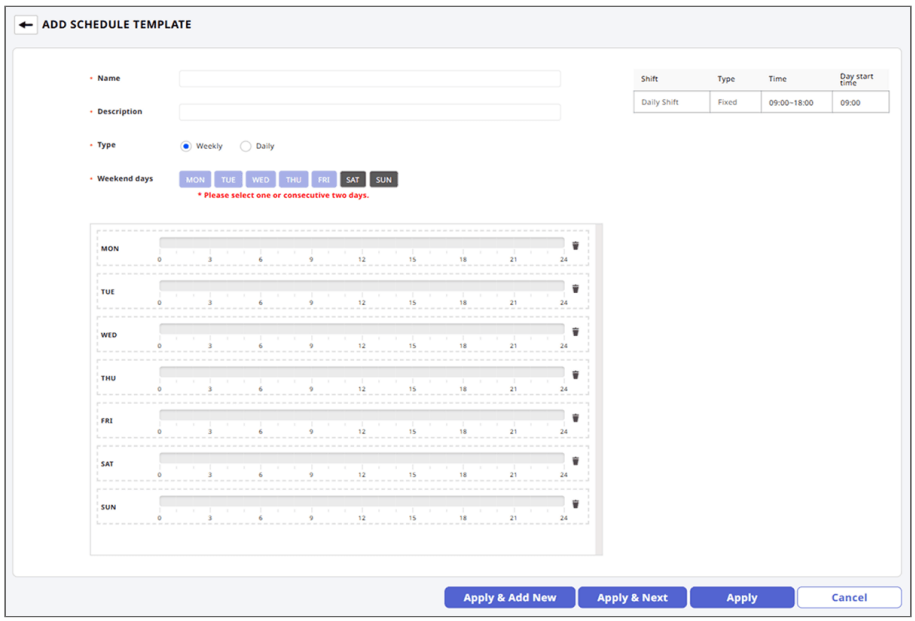


4. **ADD SCHEDULE TEMPLATE** 画面が表示されたら各項目を設定します。

情報

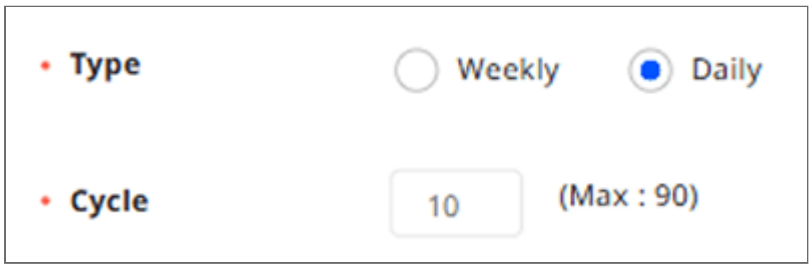
- 設定を保存するには、画面下部の **Apply** をクリックします。
- 続けて勤務スケジュールを追加する場合は、**Apply & Next**ボタンをクリックします。
- 設定を保存した後、別の **Schedule Template** を追加する場合は **Apply & Add New** ボタンをクリックします。

設定オプションガイド



- **Name**：Schedule Template の名前を入力します。
- **Description**：Schedule Template の説明を入力します。
- **Type**：Schedule Template を **Weekly** または **Daily** 日別で設定できます。

  Daily を選択すると、繰り返し使用期間（**Cycle**）を設定できます。



- **Weekend days**：週末として指定する曜日を設定します。
- **Shift**：設定された Shift の一覧を確認できます。
- 週別/日別スケジュール：設定した Shift をドラッグ＆ドロップで設定します。



情報

- 月曜日から日曜日まで全てに適用する場合は、**Copy All** ボタンをクリックします。
- 適用した Shift を解除するには、🗑 ボタンをクリックします。
- **Allowed a day before/after time** を設定した Shift を適用する場合、前日の超過許容時間を前日勤務規則の開始時刻より24時間以上前に設定することはできません。

次のステップ

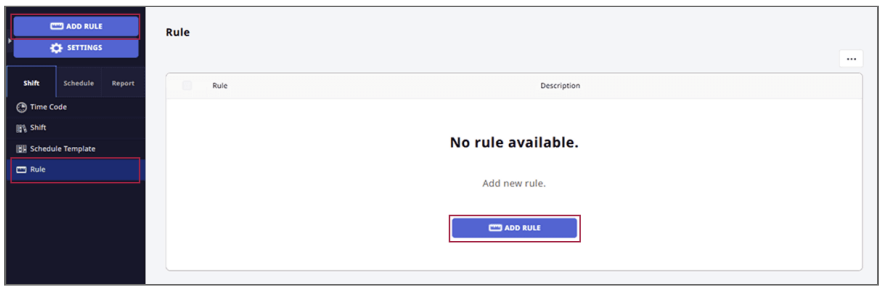
日次勤務規則に残業時間規則を追加適用して柔軟な勤務規則を作成する方法を案内します。

その他の勤務規則を設定する

Shiftで残業時間規則を追加していない場合に便利に使用できます。Shiftで設定する残業は開始時刻と終了時刻を持ちますが、Ruleは所定勤務時間を超える合計時間を計算します。Ruleを設定します。 日次、週次、月次単位で適用する残業規則を設定できます。Ruleを設定すると、Shiftに追加された残業時間規則の代わりに適用されます。

ADD RULE

1. **Launcher** ページで **T&A** をクリックします。
2. 画面左側のサイドバーで**Shift** → **Rule**をクリックします。
3. **ADD RULE**ボタンをクリックします。



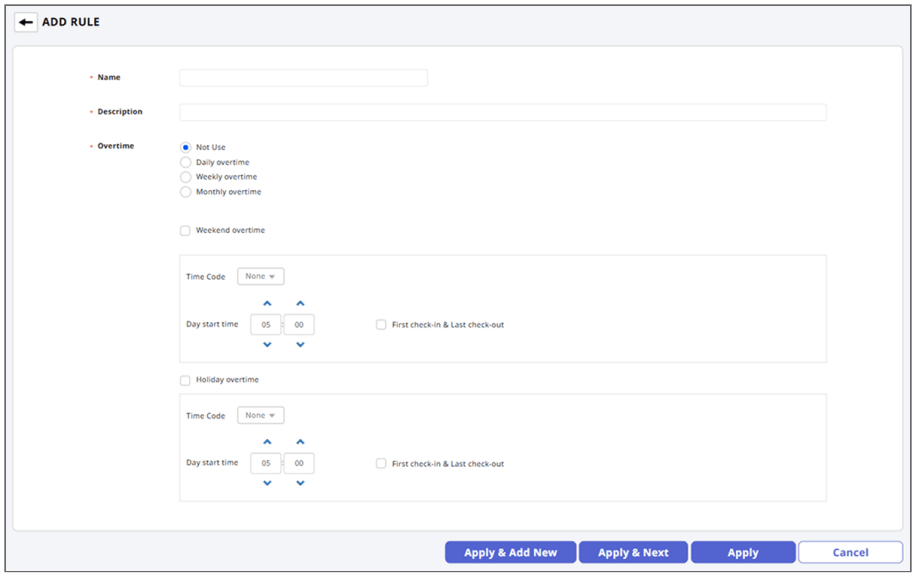
4. **ADD RULE**画面が表示されたら、各項目を設定します。

情報

- 設定を保存するには、画面下部の **Apply** をクリックします。
- 続けて勤務スケジュールを追加する場合は、**Apply & Next**ボタンをクリックします。
- 設定を保存した後、別の**Rule**を追加する場合は、**Apply & Add New**ボタンをクリックします。

設定オプションガイド

Ruleを設定します。日次、週次、月次単位で適用する残業規則を設定できます。



- **Name**：Ruleの名前を入力します。
- **Description**：Ruleの説明を入力します。
- **Overtime**：日次、週次、月次単位で所定勤務時間後に適用する残業規則を選択します。一定時間後に別の残業規則を適用できます。最大残業時間を設定して、従業員が働ける残業時間を制限することもできます。

ヒント

以下のように設定すると、所定勤務時間が午前8時から午後5時の場合、午後5時から午後11時までは**Overtime(1.5)**規則が適用され、午後11時から午前2時までは**Overtime(2)**規則が適用されます。また、1日に働ける最大残業時間が9時間に制限され、午前2時まで働いた記録のみを使用して1日の給与を計算します。



情報

総勤務時間には休憩時間や食事時間は含まれません。

- **Weekend overtime** / **Holiday overtime**：週末または休日に適用する勤務規則を設定します。
  - **Time Code**：適用するTime Codeを選択します。
  - **Day start time**：勤務開始時刻を設定します。
  - **First check-in & Last check-out**：最初にユーザーが認証した時刻を出勤時刻として記録し、最後にユーザーが認証した時刻を退勤時刻として記録します。

次のステップ

期間、ユーザー、その他の勤務規則、休暇日程を構成して勤務スケジュールを設定する方法を案内します。

勤務スケジュールを設定する

設定済みの Shift、Rule、期間、休日をユーザーに割り当てて勤務スケジュールを作成できます。

作成した勤務スケジュールには、臨時スケジュールや個人休暇も追加できます。

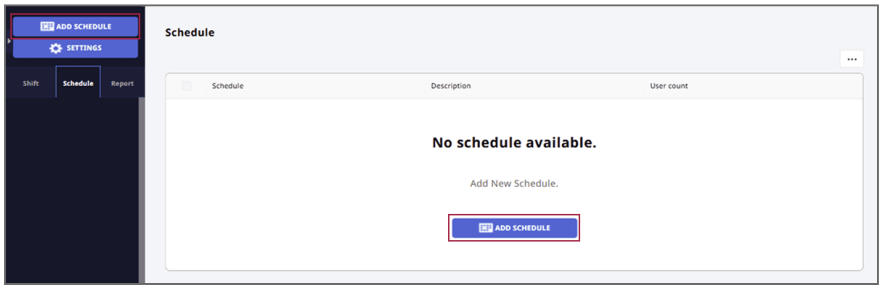
> **情報**
> スケジュールを作成する前に、使用する Time Code、Shift、Shift、休日が正しく作成されているか確認してください。
> - 勤務ルール設定の詳細については、次のドキュメントを参照してください。
>   - 時間ルールを設定する
>   - 日次勤務規則を設定する
>   - 週次勤務規則を設定する
>   - その他の勤務規則を設定する
> - 祝日設定の詳細はスケジュールを設定するをご参照ください。

勤務スケジュール

勤務スケジュールを追加する

以下の手順に従って、登録したユーザーの勤務スケジュールを追加してください。

1. **Launcher** ページで **T&A** をクリックします。
2. 画面左のサイドバーで **Schedule** タブをクリックします。
3. **ADD SCHEDULE** ボタンをクリックします。

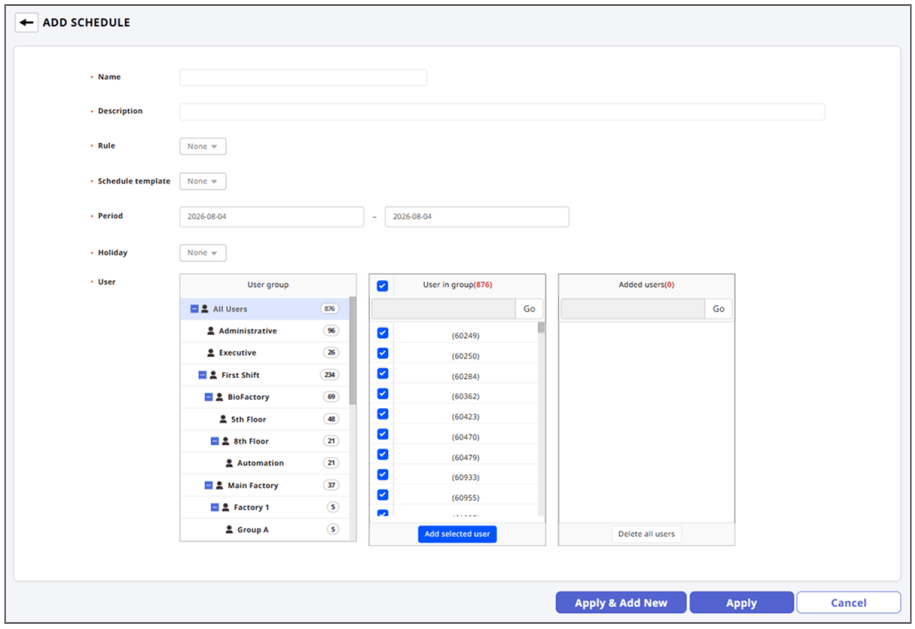


4. **ADD SCHEDULE** 画面が表示されたら、各項目を設定します。

> **情報**
>
> - 設定を保存するには、画面下部の **Apply** をクリックします。
> - 設定を保存後、別の **Schedule** を追加するには、**Apply & Add New** ボタンをクリックします。

設定オプションガイド

勤務スケジュールの設定オプションを説明します。



- **Name**：勤務スケジュールの名前を入力します。
- **Description**：勤務スケジュールの説明を入力します。
- **Rule**：設定した Rule を選択します。 Rule を設定すると、Shift で設定した残業時間ルールは適用されません。使用しない場合は **None** を選択します。

> **情報**
>
> 希望する Rule がない場合は、追加できます。詳細はその他の勤務規則を設定するをご参照ください。

- **Schedule template**：設定した Schedule template を選択します。一度設定した Schedule template は編集できません。

> **情報**
> 希望する Schedule template がない場合は、追加できます。詳細は週次勤務規則を設定するをご参照ください。

- **Period**：勤怠イベントを収集する期間を設定します。

> **情報**
> 開始日は一度設定すると後で変更できません。終了日は後で変更できますが、設定された日付より前に変更すると、変更された期間分の不在イベントが削除されます。

- **Holiday**：設定した休暇スケジュールを選択します。使用しない場合は **None** を選択します。

> **情報**
> 希望する休暇スケジュールがない場合は、追加できます。祝日設定の詳細はスケジュールを設定するをご参照ください。

- **User**：ルールを適用するユーザーを追加します。

> **情報**
> すべての勤務スケジュールに含まれるユーザー数は、登録済みの勤怠管理ライセンスがサポートする最大ユーザー数を超えることはできません。ライセンスごとの最大ユーザー数については ライセンス ポリシー を参照してください。

勤務スケジュールを編集する

登録済みの勤務スケジュールを編集する方法を案内します。

1. **Launcher** ページで **T&A** をクリックします。
2. 画面左のサイドバーで **Schedule** タブをクリックします。
3. **Schedule** リストで編集する項目をクリックします。または画面左のサイドバーで、編集する項目の ✎ ボタンをクリックします。
4. 対象項目を編集し、**Apply** ボタンをクリックします。

勤務スケジュールを削除する

登録済みの勤務スケジュールを削除する方法を案内します。

1. **Launcher** ページで **T&A** をクリックします。
2. 画面左のサイドバーで **Schedule** タブをクリックします。
3. **Schedule** リストで削除する項目のチェックボックスをクリックします。



4. 画面右上の **Delete schedule** ボタンをクリックします。または画面左のサイドバーで、削除する項目の 🗑 ボタンをクリックします。

5. 確認メッセージが表示されたら、**Yes** ボタンをクリックします。

臨時スケジュールを追加する

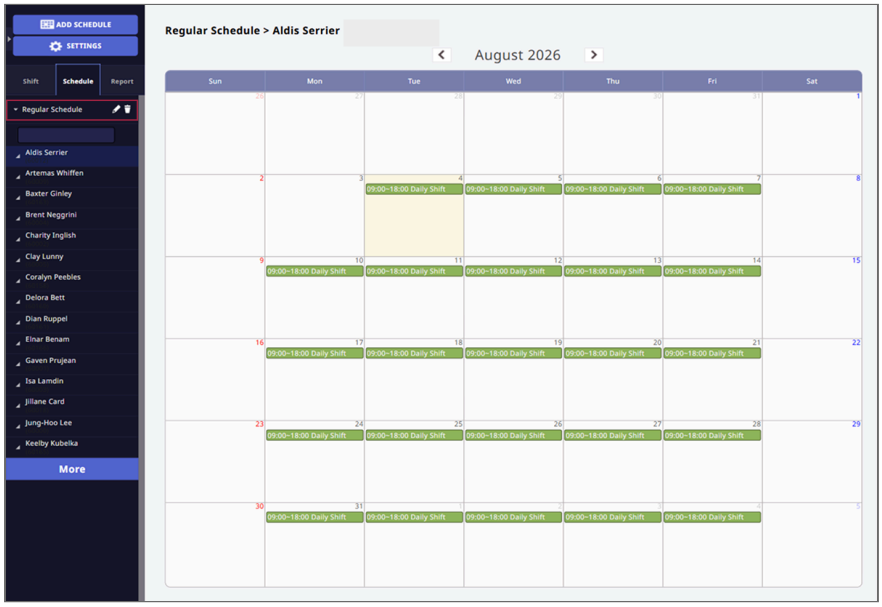
既に登録されているスケジュールがある場合、ユーザーに一時的に別の勤務ルールを適用できます。

1. **Launcher** ページで **T&A** をクリックします。

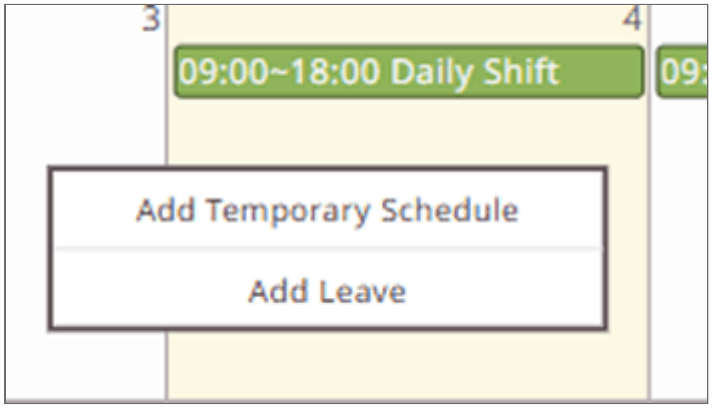
2. 画面左のサイドバーで **Schedule** タブをクリックします。

3. 画面左のリストで目的のスケジュールの ▶ ボタンをクリックしてください。

4. スケジュールに割り当てられたユーザーリストが表示され、臨時スケジュールを適用するユーザーを選択するとカレンダーが表示されます。

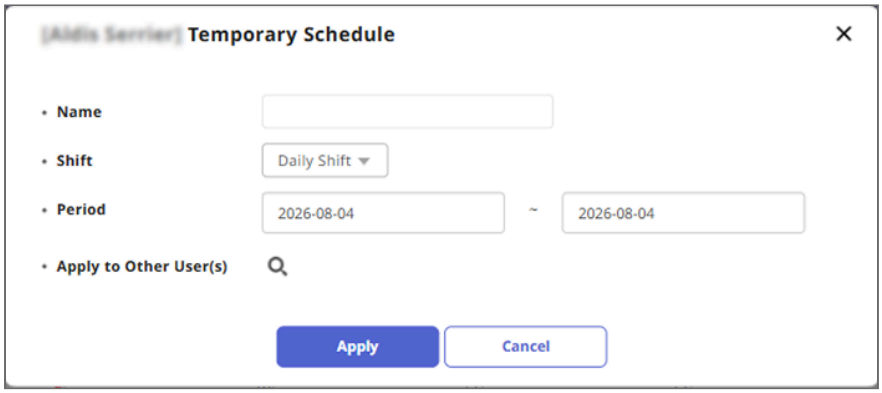


5. カレンダーで臨時スケジュールを追加する日付をクリックします。



6. ポップアップメニューで **Add Temporary Schedule** をクリックします。

7. **Add Temporary Schedule** 設定ウィンドウが表示されたら、各項目を設定します。



他のユーザーにも同じ勤務スケジュールを適用する場合は、🔍 ボタンをクリックしてユーザーを選択します。

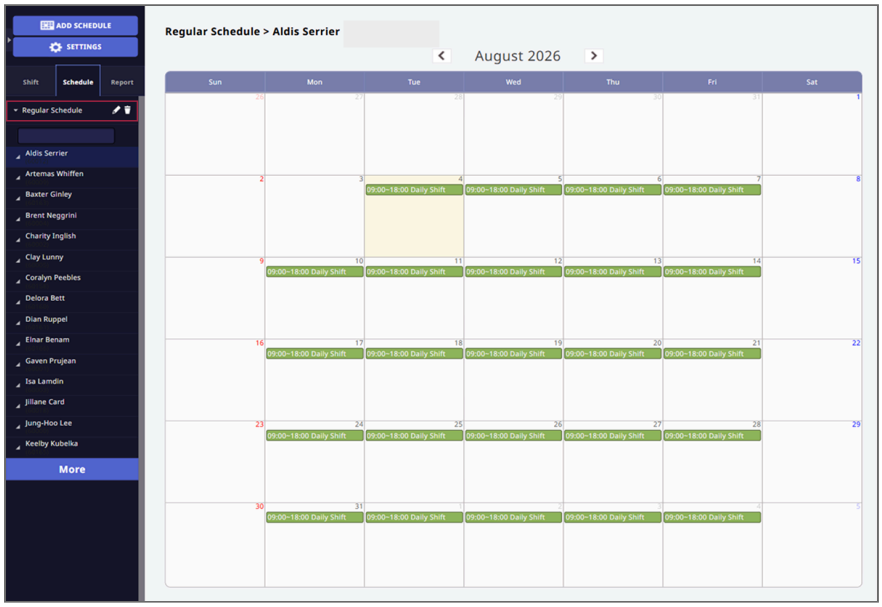
8. 設定した勤務ルールを適用するには、**Apply** ボタンをクリックします。

> **情報**
> ユーザーに適用した臨時スケジュールを削除するには、カレンダーで設定された臨時スケジュールをクリックします。確認メッセージが表示されたら、**Yes** ボタンをクリックします。

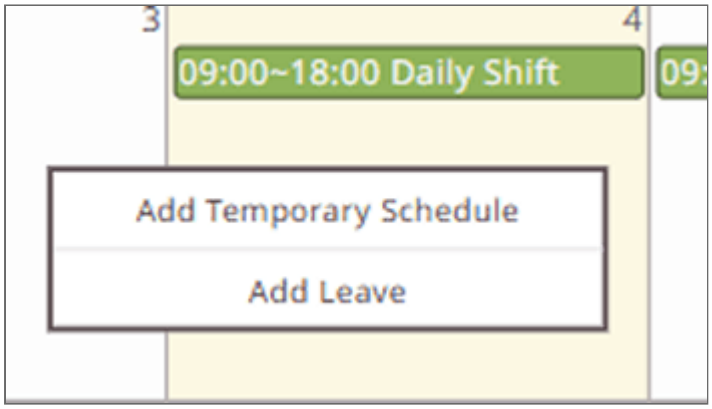
不在の追加および削除

ユーザーの不在スケジュールを追加できます。

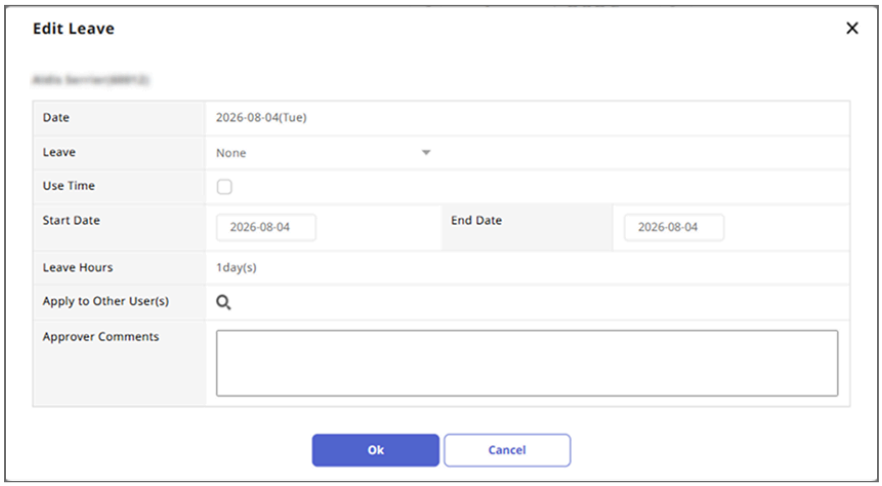
1. **Launcher** ページで **T&A** をクリックします。
2. 画面左のサイドバーで **Schedule** タブをクリックします。
3. 画面左のリストで目的のスケジュールの ▶ ボタンをクリックしてください。
4. スケジュールに割り当てられているユーザーの一覧が表示され、不在スケジュールを適用するユーザーを選択するとカレンダーが表示されます。



5. カレンダーでユーザーの不在スケジュールを追加する日付をクリックします。



6. ポップアップメニューで **Add Leave** をクリックします。
7. **Edit Leave** 設定ウィンドウが表示されたら、各項目を設定します。

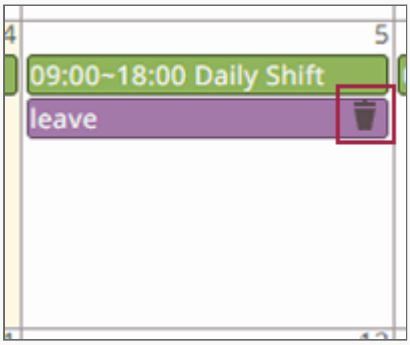


他のユーザーにも同じ不在スケジュールを適用する場合は、🔍 ボタンをクリックしてユーザーを選択します。

8. 設定した不在スケジュールを適用するには、**Apply** ボタンをクリックします。

情報

- 必要な不在管理時間ルールがない場合は、追加できます。時間ルールの追加の詳細は時間ルールを設定するをご参照ください。
- ユーザーに適用した不在スケジュールを削除するには、カレンダーで設定済みの不在スケジュールの 🗑 ボタンをクリックします。確認メッセージが表示されたら、**Yes** ボタンをクリックします。



勤怠記録を確認する

システムで収集したユーザーの勤怠イベントから勤怠レポートを生成でき、タイムレコードを編集したり、CSV ファイルまたは PDF ファイルにエクスポートしたりできます。

あらかじめ設定されている 7 つのレポートフィルターを利用して簡単に使うことができ、管理者がフィルターを直接設定することもできます。

開始する前に

多言語レポートを使用する前に

BioStar X では韓国語と英語を基本サポートしています。多言語レポートを使用するには、次の案内に従って希望の言語を設定してください。

1. 次のパスに移動します。 *C:\Program Files\BioStar X\plugin\ta\dist\setup\report_fonts*
2. 使用する言語名でフォルダーを作成します。言語名は ISO 639-1 規格を参照してください。例として、スペイン語を使用する場合はフォルダー名を "es" にします。
3. 作成したフォルダーにフォントをコピーして貼り付けます。 TrueType フォントは 1 つのみサポートされます。

レポートを更新する前に

BioStar X は標準データベースとして MariaDB を使用します。 MS SQL Server データベースを使用する場合は、以下の事項を先に確認してください。

BioStar X を MS SQL Server データベースと併用すると、登録ユーザー数が多い場合、レポートを更新するたびに PC のメモリ使用量が蓄積されることがあります。 MS SQL Server データベースの最大サーバーメモリを再設定してください。

1. **Microsoft SQL Server Management Studio** を実行します。
2. オブジェクトエクスプローラーで **BioStar X** のデータベースを右クリックします。
3. ポップアップメニューで **プロパティ** をクリックします。
4. **メモリ** をクリックし、**最大サーバーメモリ** 項目の値を下げます。

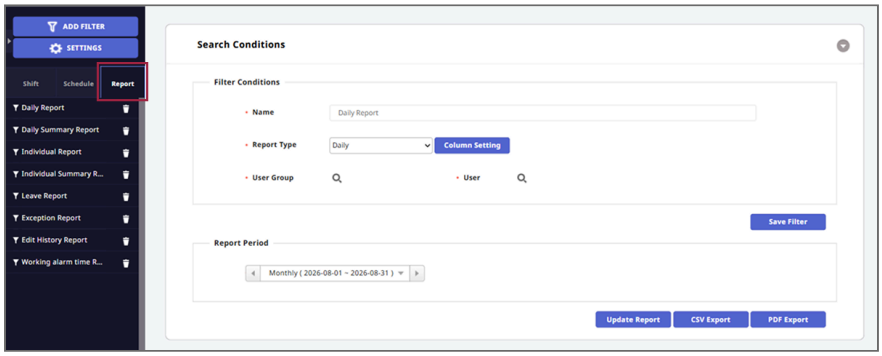
> **情報**
> **BioStar X** をインストールする際の MariaDB および MS SQL Server の設定に関する詳細は、カスタムインストールを実行するを参照してください。

勤怠記録の確認

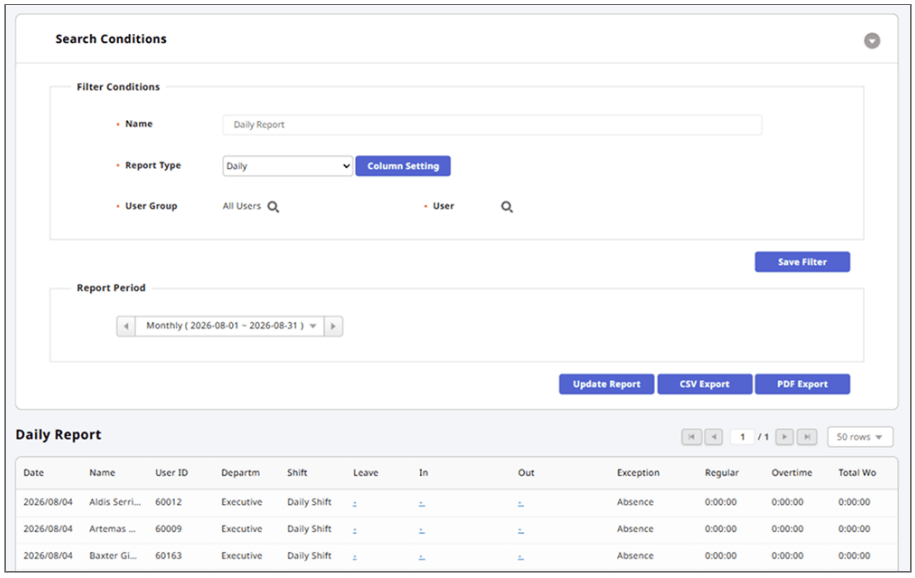
勤怠レポートを作成する

登録されたユーザーの勤怠記録レポートを生成する方法を説明します。

1. **Launcher** ページで **T&A** をクリックします。
2. 画面左のサイドバーで **Report** タブをクリックします。

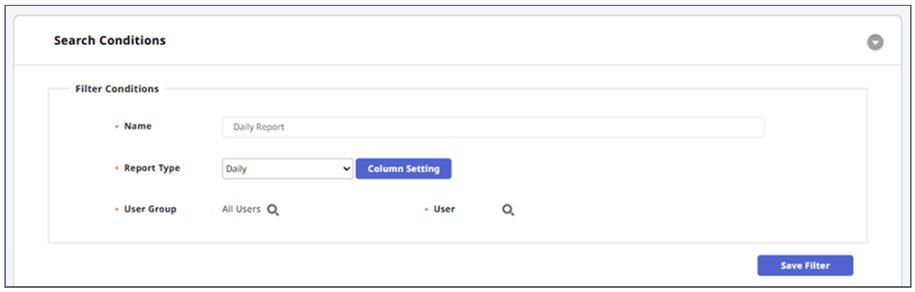


3. 画面左のサイドバーで目的のレポートフィルター項目をクリックします。
4. **User Group** または **User** 項目で 🔍 ボタンをクリックし、グループまたはユーザーを指定します。
5. レポートを生成するには **Update Report** ボタンをクリックします。
6. 画面下部にレポート一覧が表示されたら、目的の項目をクリックして詳細を確認できます。

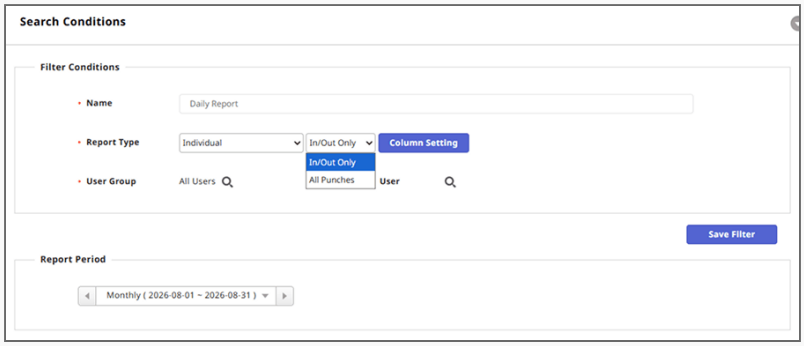


フィルター条件の設定

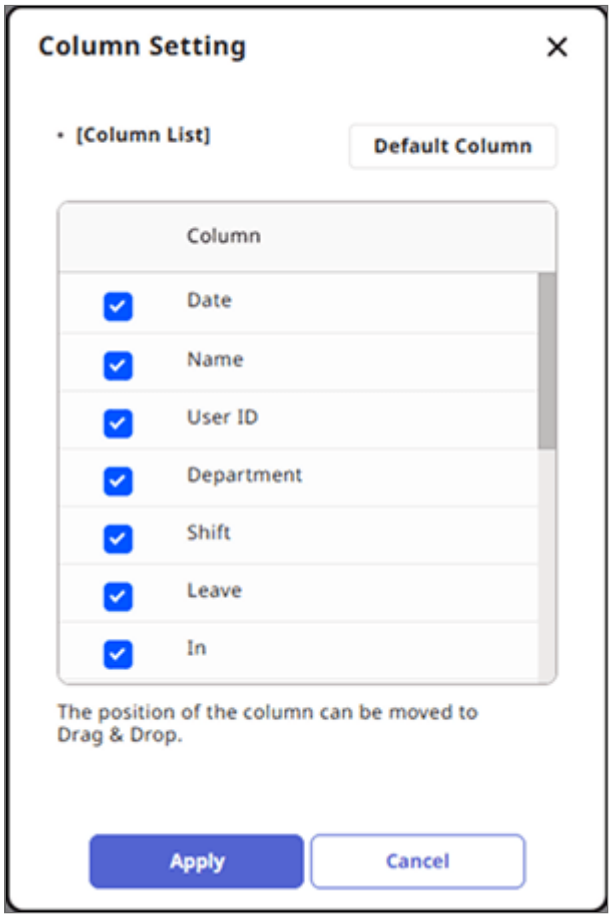
フィルター条件を設定して新しい勤怠記録レポートを生成できます。



- **Name**：レポート名を入力します。
- **Report Type**：希望するレポート種類を選択します。提供されているレポート種類は次のとおりです。
  - **Daily**、**Daily Summary**、**Individual**、**Individual Summary**、**Leave**、**Exception**、**Modified Punch Log History**、**Working alarm time**

> **情報**
> **Report Type** を **Individual** に選択すると、ユーザーの入退室記録の出力有無を設定できます。
>
> 
>
>
> - **In/Out Only**：レポートにはユーザーの出勤および退勤記録のみを出力します。
> - **All Punches**：レポートにはユーザーのすべての入退室記録を出力します。

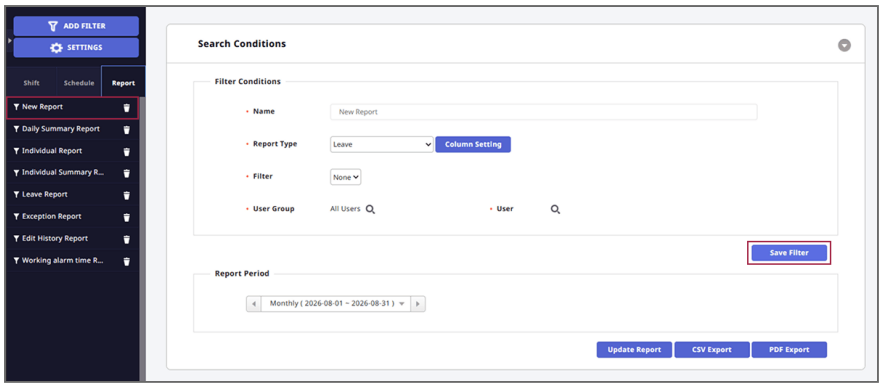
- **Column Setting**：レポートテーブルの列順を変更したり非表示にしたりできます。



> **情報**
> 列順を変更した後に既定設定へ戻すには **Default Column** ボタンをクリックします。

- **Filter**：**Report Type** を **Leave** または **Exception** に設定した場合のみ有効になり、不在記録または例外記録の詳細条件を選択できます。
- **User Group** / **User**：レポートを生成するユーザーグループまたはユーザーを選択します。

- **Save Filter**：設定した勤怠レポートをフィルターとして保存できます。



レポート期間の設定

レポート期間の設定方法を説明します。



レポート期間を **Daily**、**Weekly**、**Monthly** に設定できます。特定期間のレポートを生成するには **Custom** を選択します。

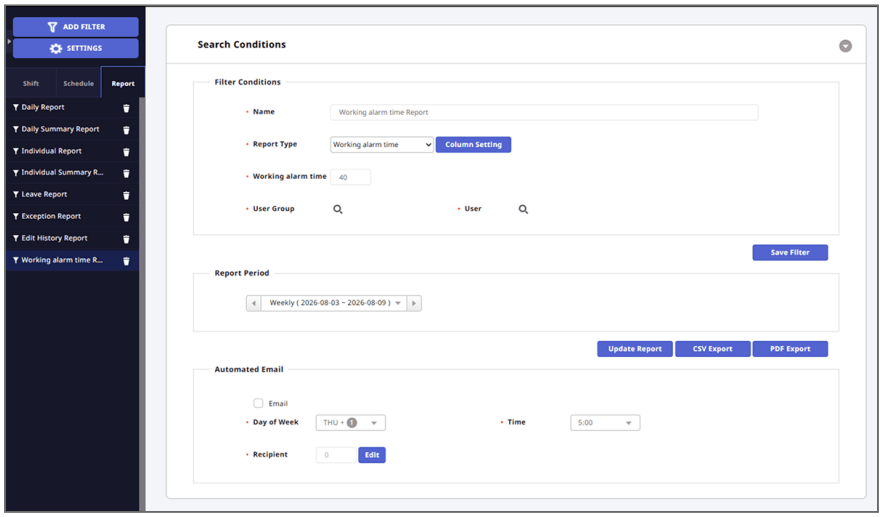
レポートのエクスポート

- **CSV Export**：生成したレポートを CSV ファイルとして保存できます。
- **PDF Export**：生成したレポートを PDF ファイルとして保存できます。

警告勤務時間レポートを作成する

指定された勤務時間に到達したユーザーの勤怠レポートを生成したり、メールで管理者に通知したりできます。警告勤務時間レポートは週単位で生成されます。

1. **Launcher** ページで **T&A** をクリックします。
2. 画面左のサイドバーで **Report** タブをクリックします。
3. 画面左サイドバーのフィルター一覧で **Working alarm time Report** をクリックします。



4. **Filter Conditions** と **Report Period** の各項目を設定します。

5. レポートを生成するには **Update Report** ボタンをクリックします。

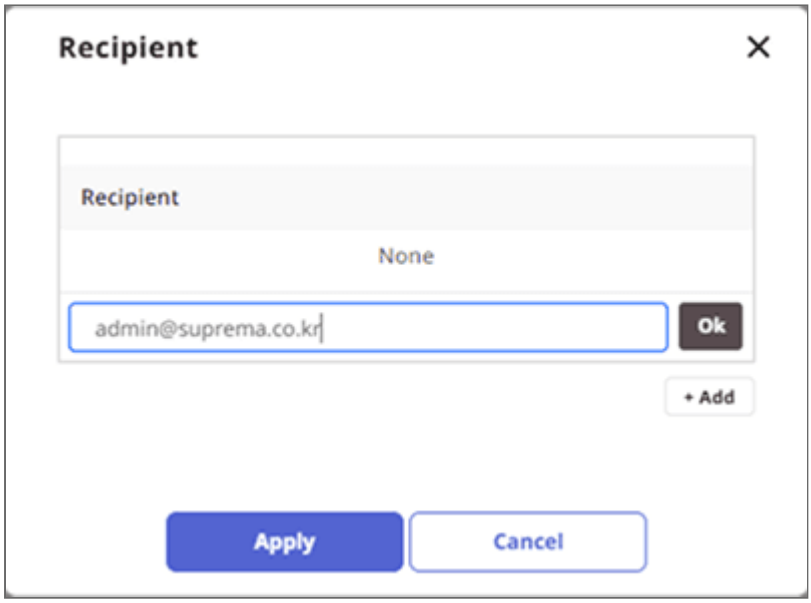
> **情報**
> 指定された勤務時間に達したユーザーの通知を管理者へメールで送信するには **Automated Email** を設定します。詳細については、メールの自動送信設定ご参照ください。

メールの自動送信設定

指定された勤務時間に達したユーザーに関する警告メールを自動で管理者へ送信できます。



- **Email**：管理者へメールを自動送信する場合は、チェックボックスをクリックします。
- **Day of Week**：管理者へメールを送信する曜日を選択します。
- **Time**：管理者へメールを送信する時間を設定します。
- **Recipient**：メールを受信する管理者を指定できます。 **Edit** ボタンをクリックすると、**Recipient** ポップアップが表示されます。メールアドレスを入力します。 1人以上の管理者を指定できます。



情報

- **Automated Email** 機能を設定するには、フィルター条件を設定してからフィルターを保存する必要があります。
- 自動送信メールの送信者情報は、画面左のサイドバーの **Setting**(⚙) → **Sender Information** で設定できます。詳細については、勤怠管理を設定するご参照ください。

勤怠記録を修正する

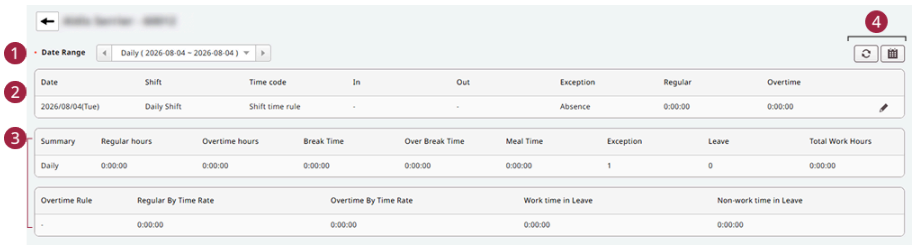
生成されたレポートのテーブルをクリックすると勤怠記録を修正できます。

情報

- 勤怠記録を修正するには、先にレポートを生成する必要があります。レポート作成の詳細については、勤怠記録を確認するをご覧ください。
- 勤怠スケジュールが登録されていないユーザーの出退勤記録は修正できません。

1. 生成されたレポート一覧で、修正する記録をクリックします。
2. 必要に応じて勤怠記録を修正するか、不在を追加します。

一覧で修正する



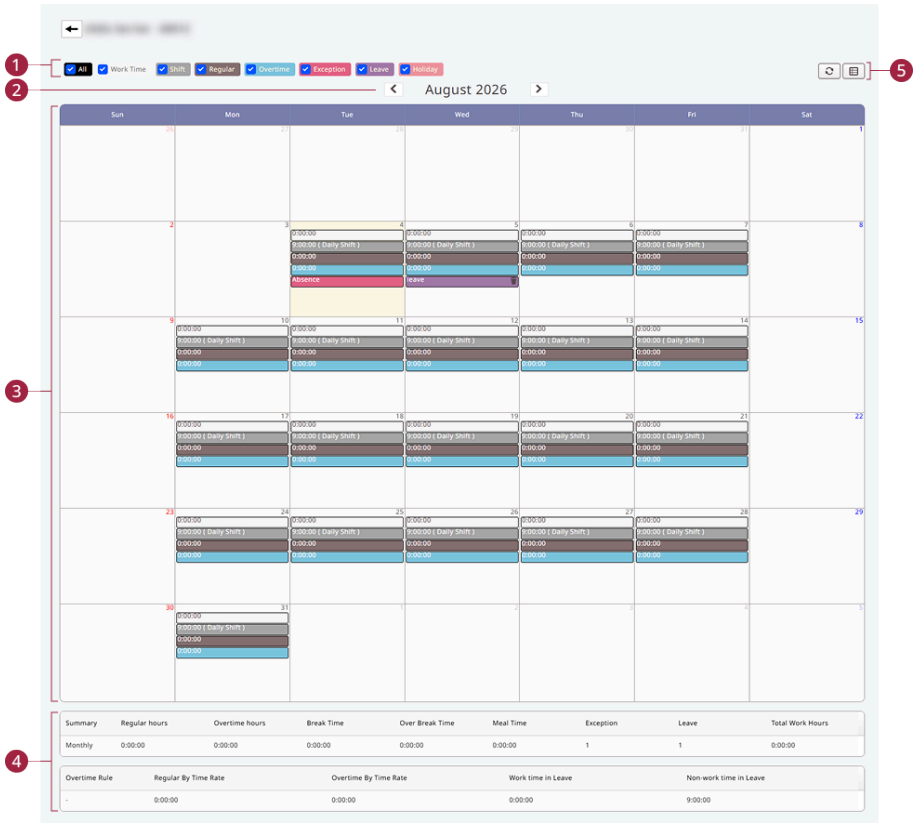
1. **Date Range**：一覧に表示する勤怠記録の期間を設定できます。
2. **日別勤怠記録**：日別の勤怠記録を確認できます。

- 出勤／退勤時間をクリックすると勤怠記録を追加・修正・削除できます。出勤／退勤時間をクリックしてから✎ボタンをクリックすると、既に登録されている勤怠記録を修正できます。変更内容を保存するには**Apply**ボタンをクリックします。
- 不在を追加するには✎ボタンをクリックします。休暇を追加するには、不在として設定された時間ルールが必要です。追加したユーザー不在の🗑をクリックすると削除できます。

3. **勤怠記録サマリー**：設定した期間の勤怠記録を確認できます。
4. **更新 / カレンダー表示**
   - 🔄：勤怠記録一覧を更新します。
   - 📅：勤怠記録をカレンダー形式で確認できます。

> **情報**
> 時間ルールの作成の詳細については、時間ルールを設定するをご覧ください。

カレンダーで修正する



1. **イベント種別**：イベント種別を選択してカレンダーに表示または非表示にできます。
2. **月**：前月または翌月に移動するには ‹ または › ボタンをクリックします。
3. **日別勤怠記録**：日別の勤怠記録を確認できます。
   - 勤務時間（白色）をクリックすると勤怠記録を追加・修正・削除できます。✎ボタンをクリックすると、既に登録されている勤怠記録を修正できます。変更内容を保存するには**Apply**ボタンをクリックします。
   - 勤務ルール（灰色）をクリックするとユーザー不在管理を追加できます。ユーザー不在を追加するには、不在として

設定された時間ルールが必要です。追加したユーザー不在の🗑をクリックすると削除できます。

4. **勤怠記録サマリー**：月別の勤怠記録を確認できます。
5. **更新 / 一覧表示**
   - 🔄：勤怠記録一覧を更新します。
   - ▦：勤怠記録を一覧形式で確認できます。

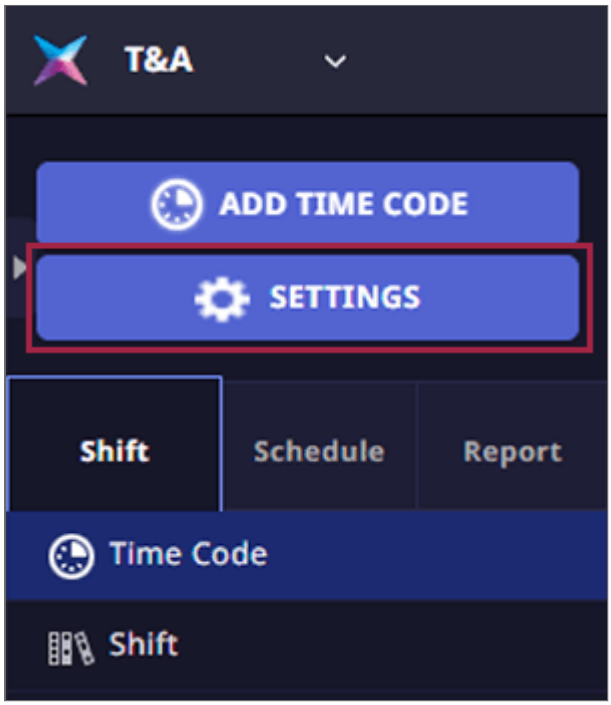
> **情報**
> 時間ルールの作成の詳細については、時間ルールを設定するをご覧ください。

勤怠管理を設定する

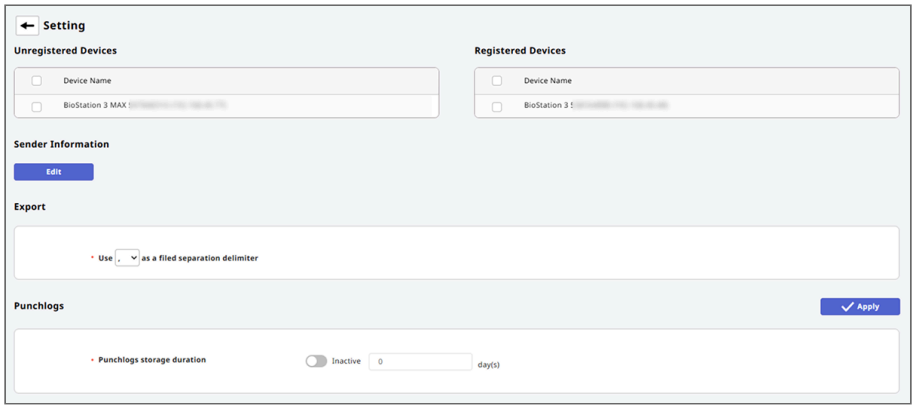
勤怠管理に使用する端末を登録したり、通知メール送信用の送信者情報を設定できます。 CSV エクスポートで勤怠レポートを出力する際に、ドキュメントの区切り文字を設定することもできます。

勤怠管理設定に移動

1. **Launcher** ページで **T&A** をクリックします。
2. 画面左のサイドバーで ⚙ **Settings** ボタンをクリックします。



3. 各項目を設定してください。



勤怠管理設定項目

Unregistered Devices

勤怠管理に使用できる端末の一覧です。端末を勤怠管理用に登録するには、対象端末を選択して **Register** ボタンをクリックします。



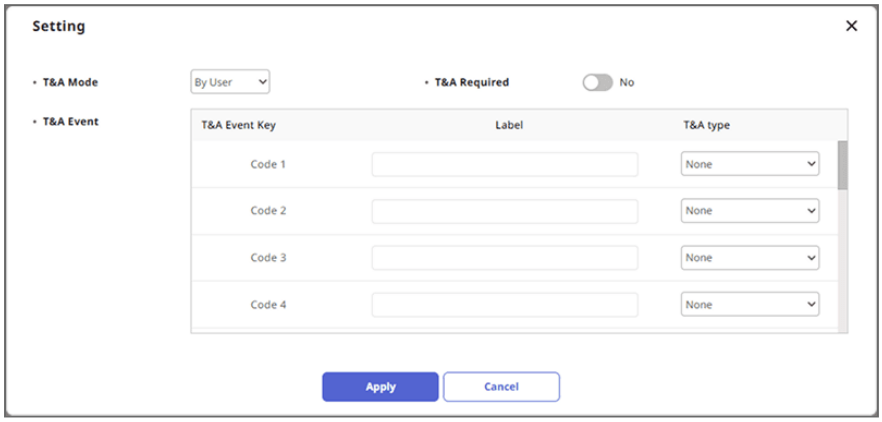
Registered Devices

現在使用中の勤怠管理端末の一覧です。

- 登録を解除するには、対象端末を選択して **Unregister** ボタンをクリックします。



- 登録済み端末の勤怠設定を編集するには、**Setting** ボタンをクリックします。勤怠設定の詳細については高度設定をご参照ください。



T&A type は、**T&A Event Key** と勤怠イベント種別をマッピングする設定です。勤怠イベントの種類は次のとおりです。

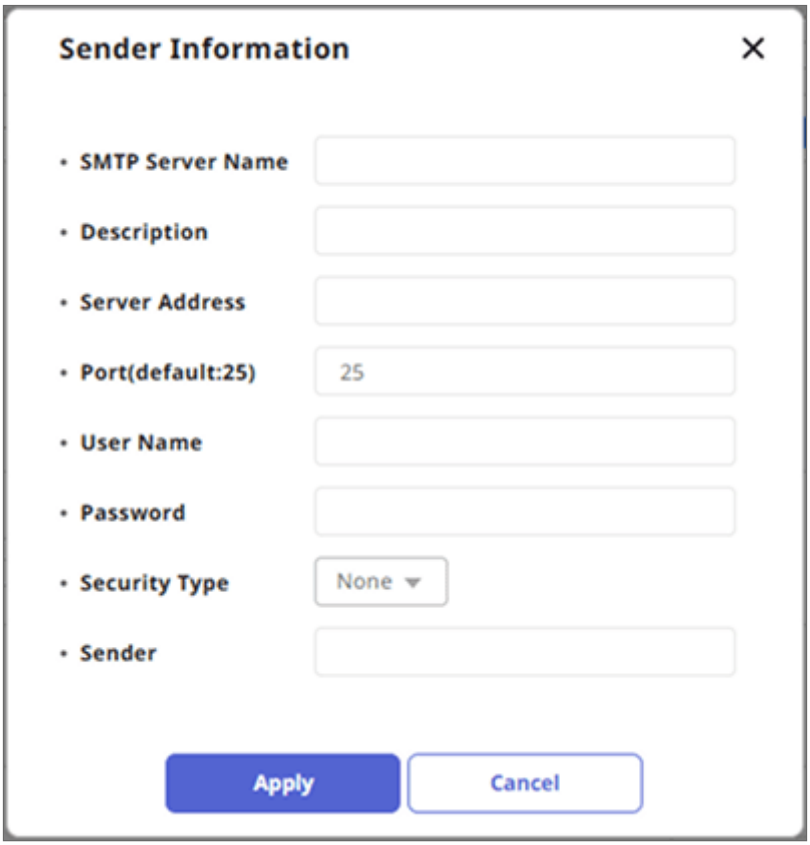
  - **Check In**

- **Check Out**
- **Break Start**
- **Break End**
- **Meal Time Start**
- **Meal Time End**

> **情報**
>
> - 端末が接続されている状態でのみ、端末の勤怠設定を編集できます。
> - **Settings** → **Device** → **Device** メニューで登録した端末を削除すると、システムは登録済みの勤怠管理端末も自動的に削除します。
> - 端末で **Multi Face Authentication** オプションを **Use** に設定すると、勤怠管理に使用できません。 **Multi Face Authentication** について詳しくは、認証を設定するを参照してください。

Sender Information

通知メールを送信する際に使用する送信者情報を設定できます。 **Edit** ボタンをクリックします。



- **SMTP Server Name**：SMTP サーバー名を入力します。
- **Description**：SMTP の説明を入力します。
- **Server Address**：SMTP サーバーアドレスを入力します。 SMTP サーバーアドレスは `smtp.{email-service-provider}.com` のような形式で、SMTP サーバーとして使用するメールの設定画面で確認できます。
- **Port(default:25)**：SMTP サーバーのポート番号を入力します。 SMTP サービスプロバイダーのメール設定画面で確認できます。

- **User Name**：SMTP サービスのアカウントを入力します。
- **Password**：SMTP サービスのアカウントパスワードを入力します。
- **Security Type**：セキュリティタイプを選択します。
- **Sender**：送信元のメールアドレスを入力します。

> **情報**
>
> - SMTP の詳細についてはシステム管理者にお問い合わせください。
> - SMTP サーバーを 2 段階認証が設定されたメールアカウントで使用する場合、そのアカウントのパスワードを変更するときは次の点に注意してください。
>   - 2 段階認証を設定すると、SMTP パスワードにはそのメールアカウントのパスワードではなく、2 段階認証で生成されたアプリパスワードが使用されます。
>   - このとき、そのメールアカウントのパスワードが変更されるとアプリパスワードは自動的に削除され、SMTP パスワードは使用できなくなります。
>   - そのメールアカウントのパスワードを変更した場合は、アプリパスワードを再生成してから SMTP パスワードを再設定します。

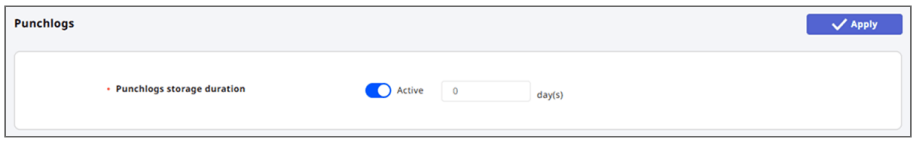
Export

CSV Export 機能で勤怠レポートを出力する際に、ドキュメントの区切り文字を選択できます。



Punchlogs

勤怠記録を保存する期間を設定できます。 **Punchlogs storage duration** オプションを **Active** に設定し、期間を入力します。設定を保存するには、**Apply** をクリックします。



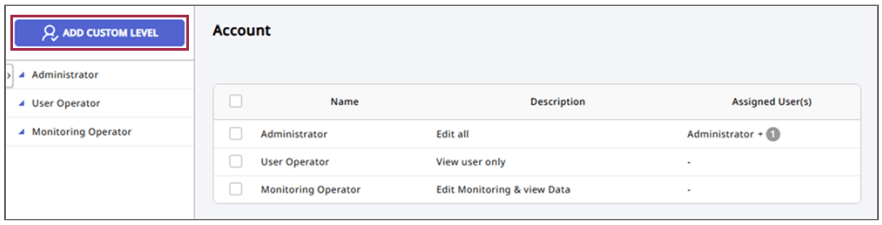
勤怠監査ログを照会する

T&A Audit Log 機能は、勤務・スケジュール・レポートなど、勤怠管理に関するすべての操作を記録します。各記録は、いつ、誰が、何を、どのように変更したかを併せて示すため、セキュリティ監査やトラブルシューティングに活用できます。

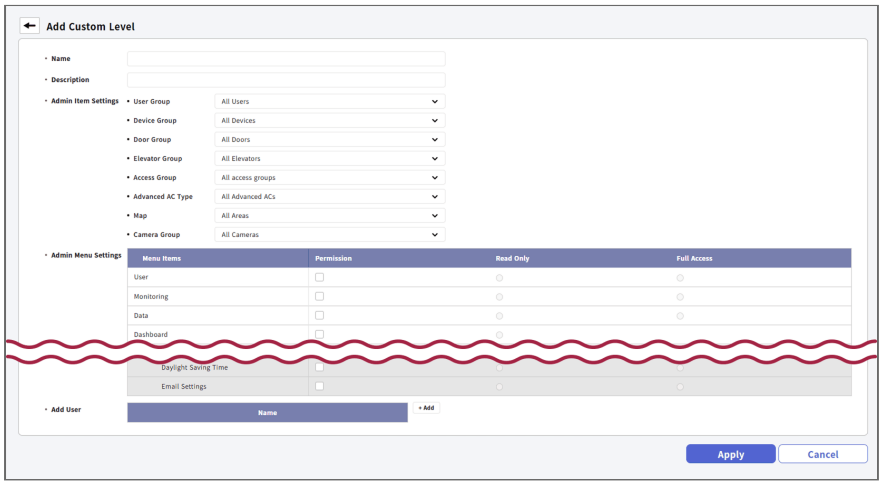
> **情報**
>
> **T&A Audit Log** メニューは、勤怠管理（T&A）ライセンスが有効で、運用管理者にこのメニュー権限がある場合に利用できます。勤怠管理プラグインのインストール時に既定で作成される **T&A Operator** アカウントにはこの権限がないため、カスタム権限を追加して設定します。

勤怠監査権限の追加

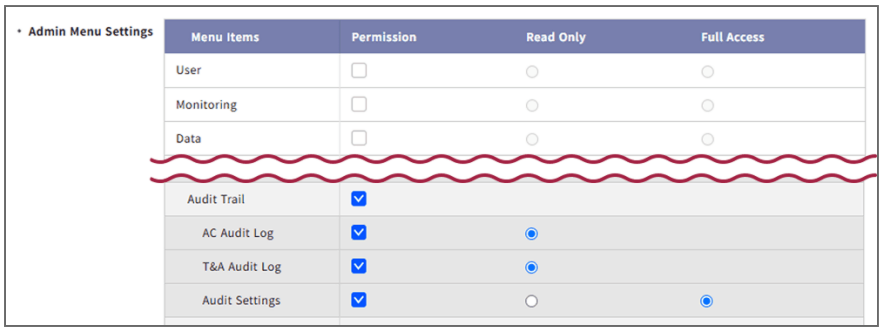
1. **Launcher**ページで**Settings**をクリックします。
2. 画面左のサイドバーで **Account** → **Account** をクリックします。
3. **Add Custom Level** をクリックします。



4. 勤怠監査ログを照会するための権限名と説明を入力します。



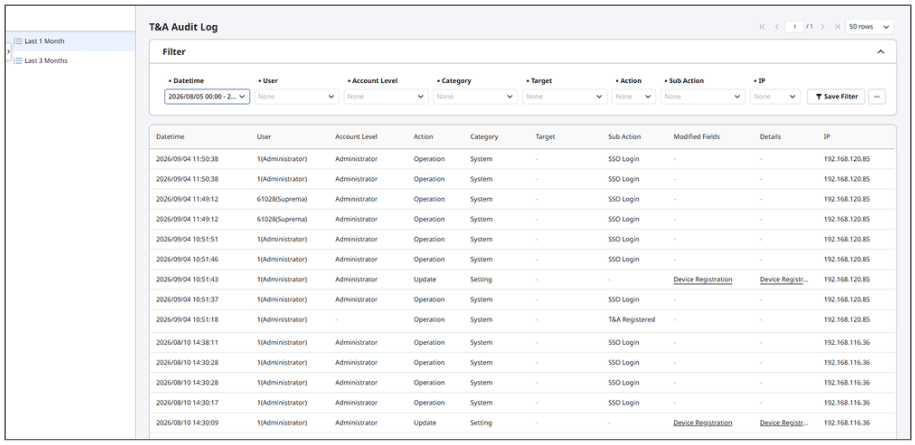
5. **Admin Menu Settings** で **Audit Trail** メニュー配下の **T&A Audit Log** と **Audit Settings** に権限を設定します。



6. **Add User** で **+ Add** ボタンをクリックし、ユーザーグループまたはユーザーを選択します。
7. カスタム権限を保存するには、画面最下部の **Apply** をクリックします。

勤怠監査ログの確認

1. **Launcher**ページで**Settings**をクリックします。
2. 画面左のサイドバーで **Audit Trail** → **T&A Audit Log** をクリックします。
3. 勤怠関連の監査ログ一覧が画面に表示されます。



情報

- 保存期間などの監査ログポリシーを変更する場合は、勤怠監査を設定するを参照してください。
- バージョン1.0.3にアップグレードした後、新たに作成される監査ログは、**Settings** → **System** → **Security** メニューの **Encrypt Personal Data on Database** オプションに関係なく、暗号化して保存します。
- BioStar 2 から **BioStar X** にアップグレードした後、監査ログの一部が記録されない場合は アップグレードする を参照してください。

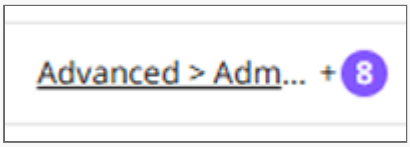
テーブルの構成

監査ログ一覧テーブルは10列で構成され、現在の検索条件に該当する記録を **Datetime** の新しい順に表示します。

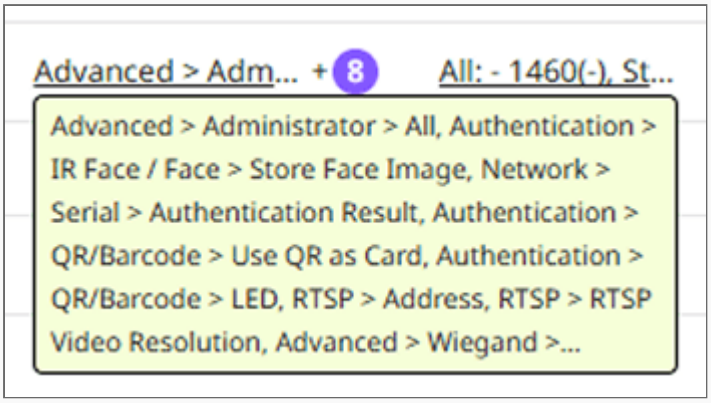
列	説明
Datetime	イベントが発生した日時です。
User	イベントを実行したユーザーです。 **id(名前)** 形式で表示されます。
Account Level	イベントを実行したユーザーの管理者レベルです。システムが自動で実行した操作は空欄にします。
Action	実行された操作の種類です。**Create**、**Update**、**Delete**、**Read**、**Export**、**Operation** のいずれかに分類されます。
Category	イベント対象のドメイン分類です。 (**Shift**, **Schedule**, **Report**, **T&A Audit Log**, **Setting**, **System**)
Target	操作が適用された対象です。**タイプ: id(名前)** 形式で表示されます。
Sub Action	**Operation**、**Read**、**Export** の操作でのみ表示される詳細操作名です。
Modified Fields	変更または照会されたフィールド名です。 **Operation** は常に空欄にします。
Details	動作別の詳細情報です。（変更値、照会条件、フィールドスナップショットなど）
IP	ユーザーが接続したIPアドレスです。システムが自動で発行した記録は**127.0.0.1**と表示されます。

情報

- **Action** が **Update** の記録は、常に対象を1件のみ示します。複数の対象を一度に変更する一括編集は勤怠管理にないため、対象が複数件としてまとめて表示されません。
- **User**、**Target**、**Change Details** に表示される名称は、その記録が発生した時点の値をそのまま保持します。その後に名称が変わったり対象が削除されたりしても、過去記録の表示名は変わりません。
- **Target**と**Modified Fields**の値が2件以上の場合、最初の項目のみ表示し、残りは右側に残件数バッジ（例：+208）としてまとめて表示します。残件数が1,000件以上の場合は**+999**と表記し、正確な合計件数は詳細ポップアップのタイトルで確認できます。バッジをクリックすると、そのセルの詳細ポップアップが開きます。

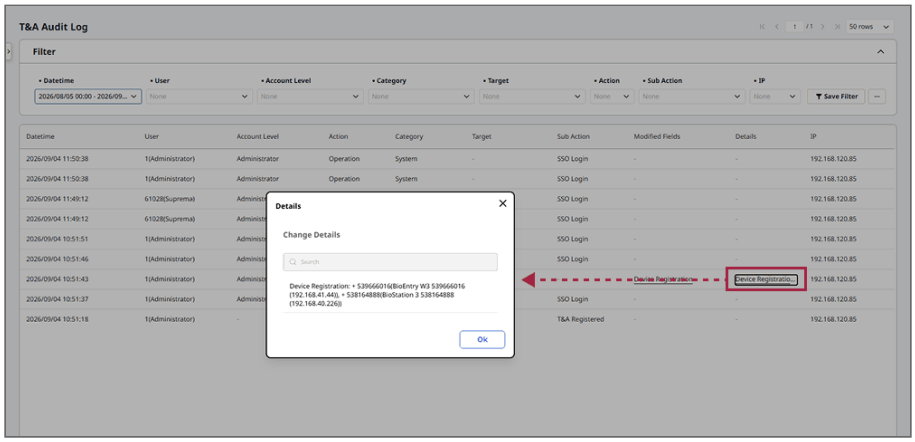


- セルの値が長い場合は一行で省略して表示します。マウスを合わせると値全体をツールチップに表示し、ツールチップからはみ出す部分は ... で省略して表示します。



詳細情報の確認

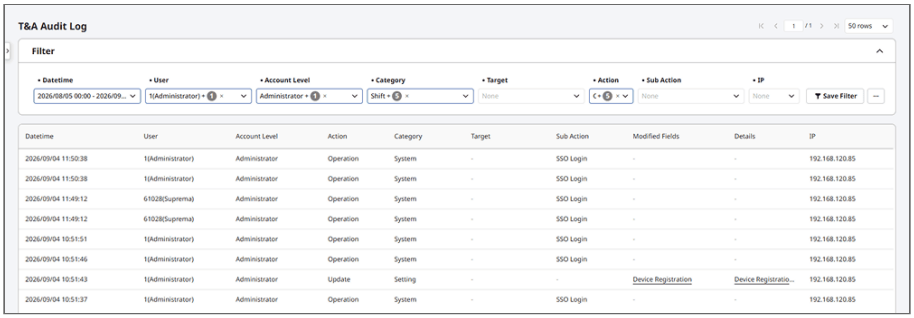
値が入っている **Target**、**Modified Fields**、**Details** のセルには下線が付き、クリックできます。セルをクリックすると、該当行の操作に応じた詳細ポップアップが開きます。**OK** ボタンまたは ✕ ボタンで閉じます。



ポップアップ上部の**Search**入力フィールドに検索語を入力すると、一致する項目だけを強調表示するかフィルタリングします。対象ポップアップでは、検索時にグループとグループ別件数も更新されますが、タイトルの全体件数は検索に関係なく変わりません。

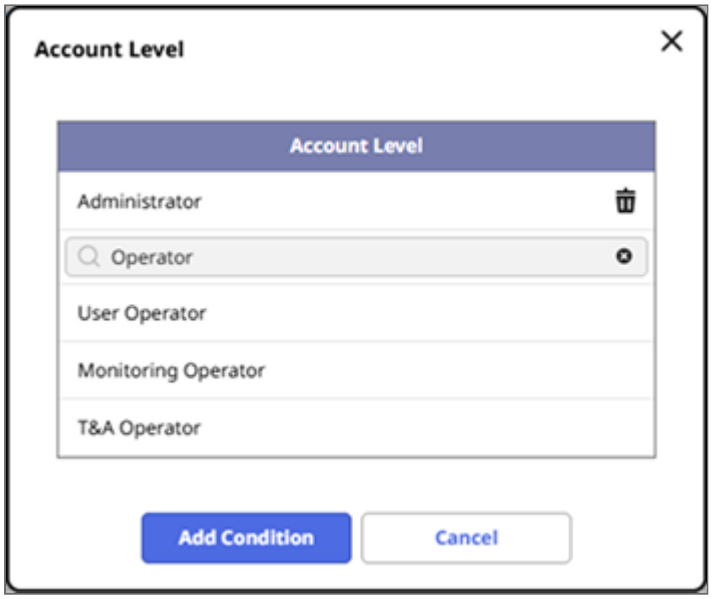
フィルターで記録を絞り込む

Filterセクションのフィルターを組み合わせ、目的の記録を絞り込んで探してください。同一フィルター内で複数の値を選択すると OR で、異なるフィルターを併用すると AND で結合されます。

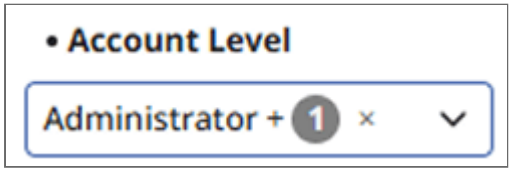


フィルター	動作方式
Datetime	開始・終了の日時を指定します。照会期間に長さ制限はありません。
User	検索語を入力し、Enter キーを押して一致するユーザーを探してください。最初に開くと一覧は空です。
Account Level	検索語を入力し、Enter キーを押して一致する管理者レベルを探してください。
Category	検索可能なチェックボックス一覧から、分類を一つ以上選択してください。
Target	検索語を入力し、Enter キーを押して一致する対象を探してください。
Action	チェックボックス一覧から動作を一つ以上選択してください。
Sub Action	検索可能なリストから詳細操作を選択してください。
IP	検索語を入力し、Enter キーを押して一致する IP を検索します。

- 適用したフィルターがない場合、現在の日付から30日前までの記録を既定で表示します。
- 各フィルターポップアップで値を選択し、**Add Condition** ボタンをクリックすると、検索にすぐ反映されます。 **Cancel** をクリックすると、選択を取り消してポップアップを閉じます。



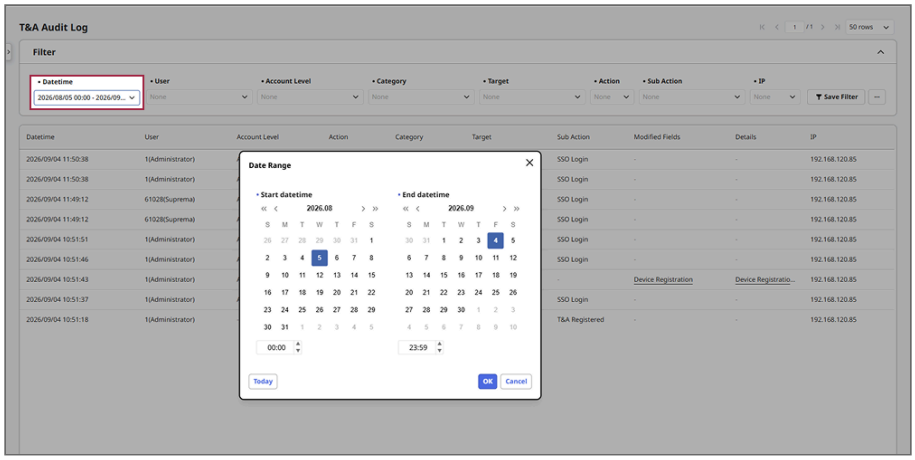
- 適用したフィルターは、先頭の条件と追加件数で要約して表示されます。 ✕ をクリックすると、そのフィルターだけを解除します。値を選択していないフィルターは **None** と表示されます。



> **情報**
> **User**、**Account Level**、**Target**、**IP** フィルターは、検索語を入力すると結果が表示されます。部分一致に対応しているため、名前やIDの一部だけを入力しても検索できます。削除した対象も **Deleted** と表示して検索します。

照会期間の指定

Datetime をクリックすると、**Date Range** ポップアップが開きます。

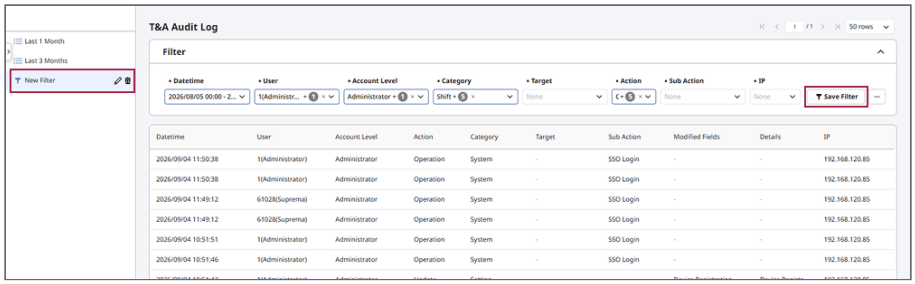


1. **Start datetime** と **End datetime** の日時をそれぞれ指定します。 **Today** をクリックすると、今日の日付へ移動します。
2. 照会期間を適用するには、**OK** ボタンをクリックします。

フィルターの保存

よく使う検索条件は **Saved Filters** に保存し、再度読み込めます。

1. 希望する条件でフィルターを設定します。
2. **Filter** セクションの **Save Filter** ボタンをクリックします。
3. 画面左のフィルターリストに **New Filter** が追加されます。



- フィルター名を変更するには ✎ ボタンをクリックし、新しい名前を入力して Enter キーを押します。
- フィルターを削除するには 🗑 ボタンをクリックします。

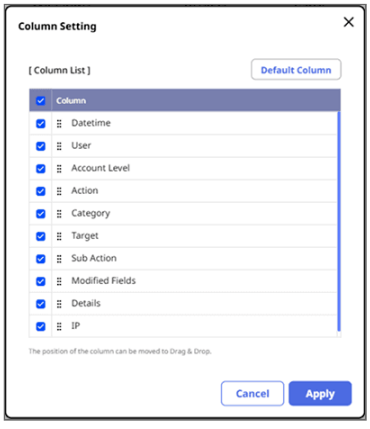
> **情報**
> 保存できるフィルターは最大20件です。保存したフィルターはブラウザーに保存されるため、別のPCやブラウザーでは表示されません。

連鎖削除で残る追加記録

勤務スケジュールを変更または削除すると、システムはそのスケジュールを使用していたユーザーの一時スケジュールと不在も削除する場合があります。この場合、システムは勤務スケジュール自体の変更または削除記録とは別に、実際に削除された一時スケジュールと不在ごとに追加記録を残します。

- 連鎖して削除された項目がない場合、追加記録も残りません。
- **Target** は、原因となった勤務スケジュール 1 件と、実際に項目が削除されたユーザーだけを含みます。スケジュールに属するユーザー全員ではありません。
- **Details** は削除件数を表示します。勤務スケジュールを削除した場合は、削除対象期間も表示します。

列設定



監査ログテーブルの列の位置を変更したり、非表示にしたりできます。**Filter** セクション右側の ••• → **Column Setting** をクリックしてください。

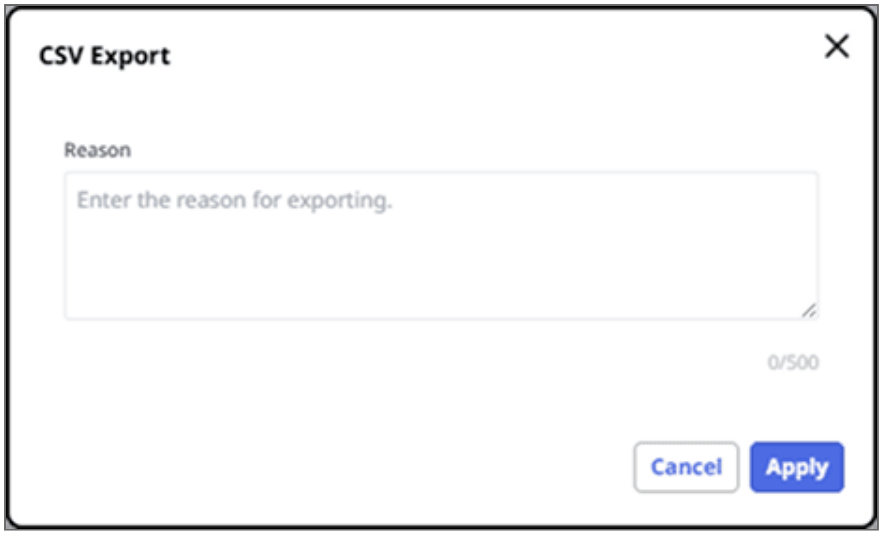
- **[Column List]** で非表示にする項目のチェックボックスの選択を解除してください。
- 列の順序を変更するには、目的の項目をドラッグしてください。
- 列設定を初期化するには、**Default Column** をクリックしてください。

設定を保存するには、**Apply** ボタンをクリックします。

CSV へのエクスポート

監査ログをCSVファイルにエクスポートし、外部分析ツールで活用してください。

1. **Filter** セクションで必要に応じてフィルターを設定してください。
2. セクション右側の ••• → **CSV Export** をクリックしてください。
3. **CSV Export** ウィンドウが表示されたら、**Export Reason**(任意)を入力し、**Apply** ボタンをクリックします。



エクスポートしたCSVファイルは、レコードごとに一行で10列すべてを含み、値にカンマが含まれるセルのみを引用符で囲みます。 **Target** と **Modified Fields** のように複数の値が入るセルは、縦棒(|)で区切ります（例: **Schedule: 7(Team Schedule)| User: 12(Robert)**）。 **Action** が **Update** の記録では、**Details** は省略せず全フィールドを含みます。

> **注意**
> CSV ファイルは、スプレッドシートが数式として解釈できる値を元のまま含みます。ダウンロードした CSV ファイルをスプレッドシートで直ちに開かず、必要に応じてテキストのインポート機能で開いてください。

> **ヒント**
> フィルターを設定した場合、フィルタリングされた結果だけをCSVファイルにエクスポートします。

勤怠監査を設定する

監査ログは時間とともに蓄積するため、保存容量と個人情報保護の観点から保管期間を管理する必要があります。**Audit Settings** で **T&A Audit Log** 記録の保管期間と閲覧履歴を記録するかどうかを設定してください。

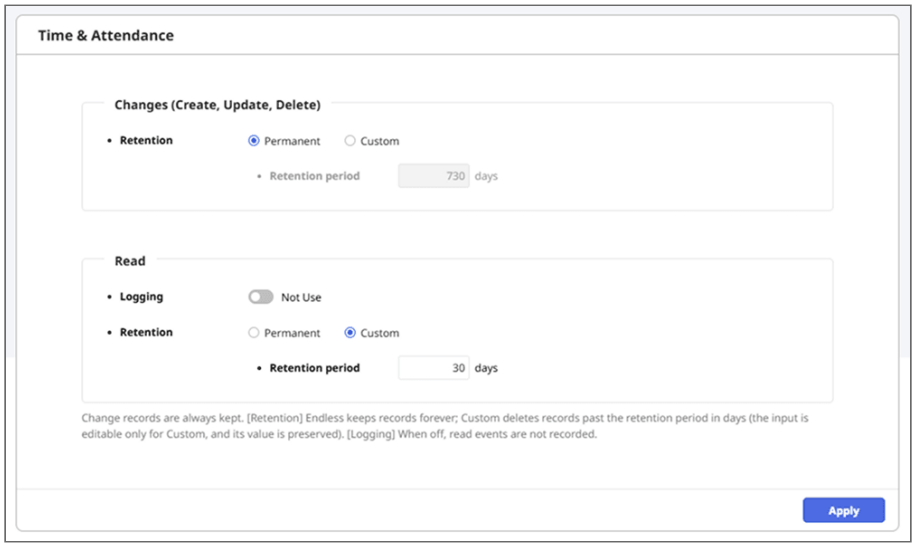
権限の説明

Administrator は **Audit Settings** メニューで常に参照および変更できます。カスタム権限管理者は、**Admin Menu Settings**で **Audit Settings**メニュー項目を**Read Only**に適用すると参照のみ行えます。**Full Access**に適用すると参照と変更の両方を行えます。

> **情報**
>
> - 勤怠管理プラグインをインストールすると既定で作成される勤怠管理者アカウントには、この権限がありません。必要に応じて、別途権限を付与してください。
> - 勤怠監査権限の追加について詳しくは 勤怠監査ログを照会する を参照してください。

監査設定を開く

1. **Launcher**ページで**Settings**をクリックします。
2. 画面左側のサイドバーで **Audit Trail** → **Audit Settings** をクリックしてください。
3. 画面を下にスクロールして **Time & Attendance** セクションに移動してください。



保管ポリシーの設定

Time & Attendance セクションは次の二つのグループで構成されます。

- **Changes (Create, Update, Delete)**：作成、修正、削除の記録です。システムは常に記録するため、オン/オフを切り替えられません。
- **Read**：参照記録です。記録するかどうかを設定します。

> **情報**
>
> - **Retention period** は、最小1日から最大2,147,483,647までの整数で入力してください。
> - **Time & Attendance** セクションの設定変更は、**T&A Audit Log** で **Update** 記録として確認してください。

変更記録

Changes (Create, Update, Delete) グループは常に記録されるため、**Retention** を選択してください。

- **Permanent**：自動削除せず、記録を永久に保管します。
- **Custom**：規制や社内ポリシーにより保管期間を制限する必要がある場合は、このオプションを選択してください。**Retention period** 入力欄が有効になったら、保管期間を日単位で入力してください。

参照記録

Read グループでは、参照記録を残すかどうかを設定します。

- **Logging**：参照記録を残すには **Use** に設定してください。不要な場合は **Not Use** に設定してください。
- **Retention**：保管方法を選択してください。
  - **Permanent**：参照記録を自動削除せず、永久に保管します。
  - **Custom**：**Retention period** 入力欄が有効になります。保管期間を日単位で入力してください。

> **情報**
> **Logging** を **Not Use** に設定すると、参照イベント自体を記録しません。その後 **Use** に設定しても、以前の期間の記録は参照できません。

設定を保存

Changes (Create, Update, Delete) と **Read** の設定が完了したら、**Time & Attendance** セクション下部の **Apply** ボタンをクリックしてください。二つのグループの設定値をまとめて保存します。

自動削除の動作方法

Custom で設定した保管期間を超えた記録は、ユーザー操作に関係なく、サーバーが毎日午前1時に実行するジョブで自動削除します。判定と削除は同じジョブで一度に行われ、この判定は一日一回だけ行います。

> *たとえば、**Read** の記録に **Custom** 方式で30日を適用した場合、午前1時のジョブ実行時点を基準に30日を超えた記録を、そのジョブで直ちに削除します。保管期間を超えた直後の記録でも、ジョブは一日に一度だけ実行されるため、その時点を過ぎると次の日の午前1時のジョブで削除されます。*

Retention を **Permanent** に設定すると自動削除ジョブが実行されず、記録が永久に残ります。

訪問者の申請と管理

Visitor 機能を使用すると、訪問申請用PCで訪問申請ページを作成し、訪問者管理用PCで訪問者の入退室を管理できます。

> **情報**
> - **Visitor** 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として使用できます。ライセンスポリシーの詳細については、ライセンス ポリシーを参照してください。
> - 訪問者機能はライセンスで有効化した後、設定方法の詳細については 訪問者設定 をご参照ください。

訪問者ライセンスの適用

訪問者ライセンスの適用方法を案内します。 **BioStar X** の購入先から Visitor ライセンスを購入した後、次の手順に従ってライセンスを適用してください。

1. **BioStar X** の管理者アカウントでログインしてください。
2. **Launcher**ページで**Settings**をクリックします。

3. 画面左のサイドバーで **License** → **BioStar X License** をクリックします。
4. **License Activation**で、**Activated by**と**License Key**の項目を順に入力します。



5. **Activate** ボタンをクリックします。

登録したライセンスは **Activated License** で確認できます。

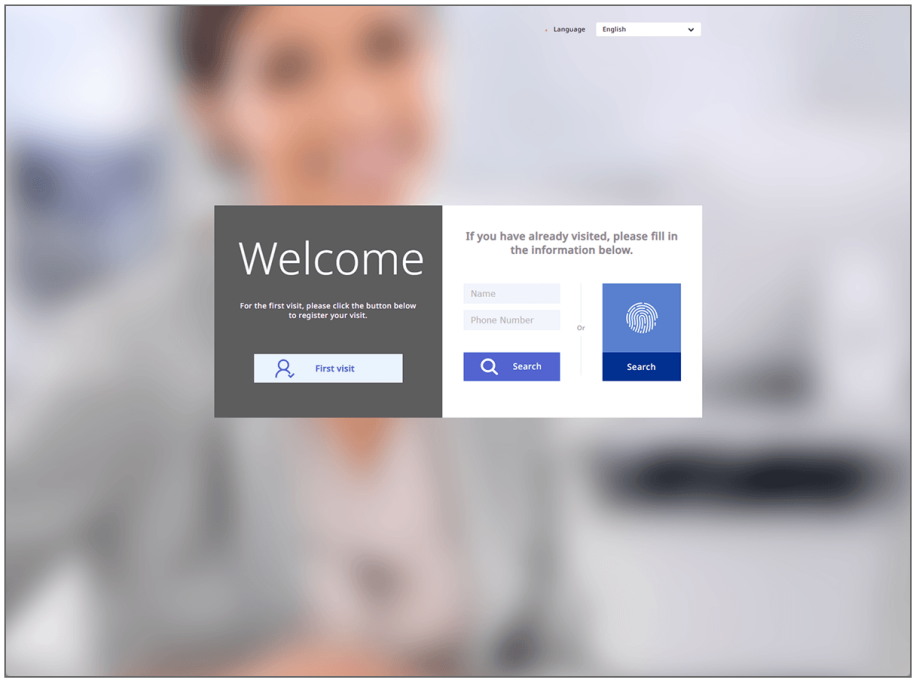
> **情報**
> インターネット接続が制限されているオフライン環境や閉域ネットワーク環境でライセンスを有効化するには、BioStar Xライセンスを参照してください。

> **ヒント**
> 訪問者ライセンスを適用すると、**Settings** → **Visitor** メニューが有効になり、画面左上のショートカットリストに **Visitor** 管理ページへ移動できるリンクが追加されます。

訪問申請ページの設定

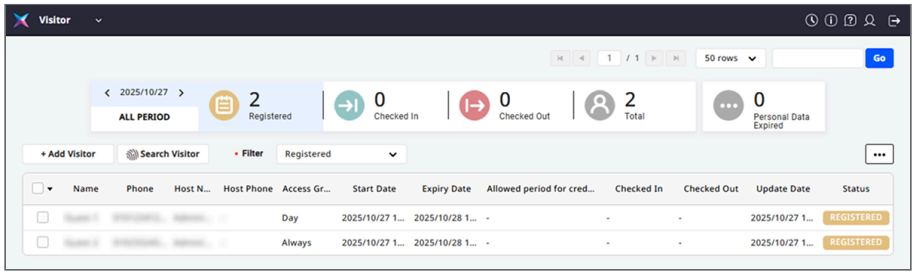
訪問申請ページは、先に訪問者設定を行った後に使用できます。訪問申請ページの設定方法の詳細については 訪問者設定 をご参照ください。

訪問申請ページには専用の訪問申請用PCからアクセスでき、訪問者が入退室を申請できます。訪問申請の詳細については 訪問を申請する をご参照ください。



訪問者入退室管理

訪問申請履歴を確認し、訪問者の入退室を管理できます。訪問者の入退室管理の詳細については 来訪申請を管理する をご参照ください。



訪問を申請する

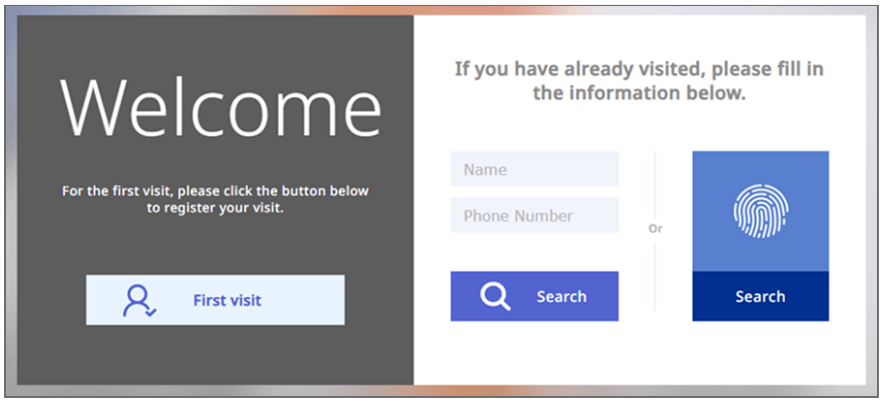
社内ユーザーではない外部訪問者が訪問申請用PCを使用して入退室を申請する方法を説明します。

> **情報**
>
> - 訪問申請用PCは別途構成する必要があり、訪問者設定を先に行う必要があります。訪問者設定の詳細については訪問者設定をご参照ください。
> - 訪問申請用PCに訪問申請ページのショートカットアイコンがない場合は、訪問者設定を参照してショートカットアイコンを作成してください。

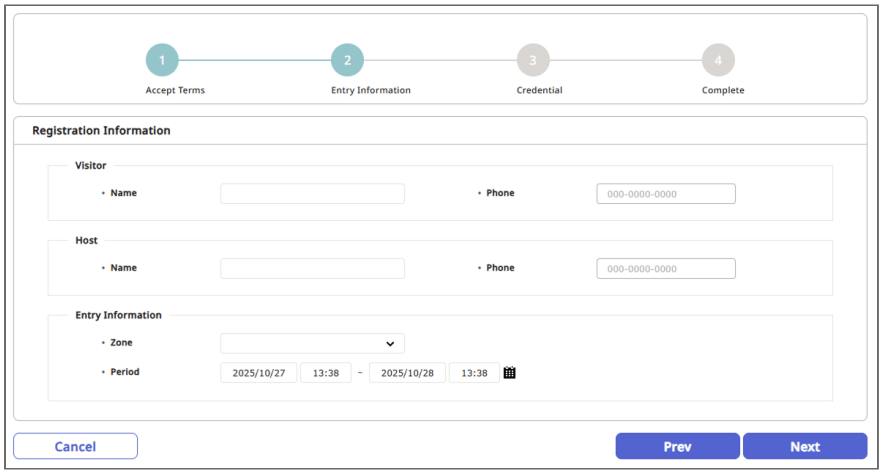
新規訪問申請

初めて訪問する訪問者が訪問申請用PCで入退室を申請する方法を説明します。

1. 訪問申請用PCで訪問申請ページを開いてください。訪問申請ページのURLアドレスは `https://{biostar_x_server_ip}/#/register-welcome` 形式です。

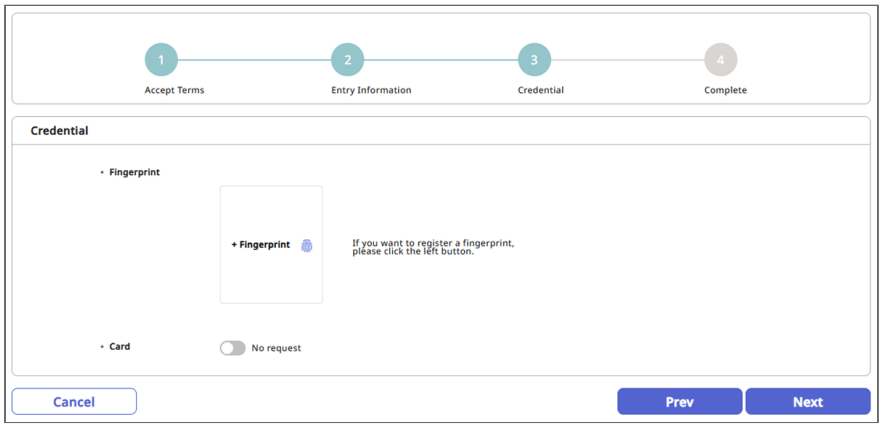


2. 画面中央の **First visit** をクリックしてください。
3. 訪問先の入退室に関する約款および個人情報取扱方針への同意を完了したら、画面右下の **Next** ボタンをクリックしてください。
4. 訪問申請に必要な情報を入力してください。



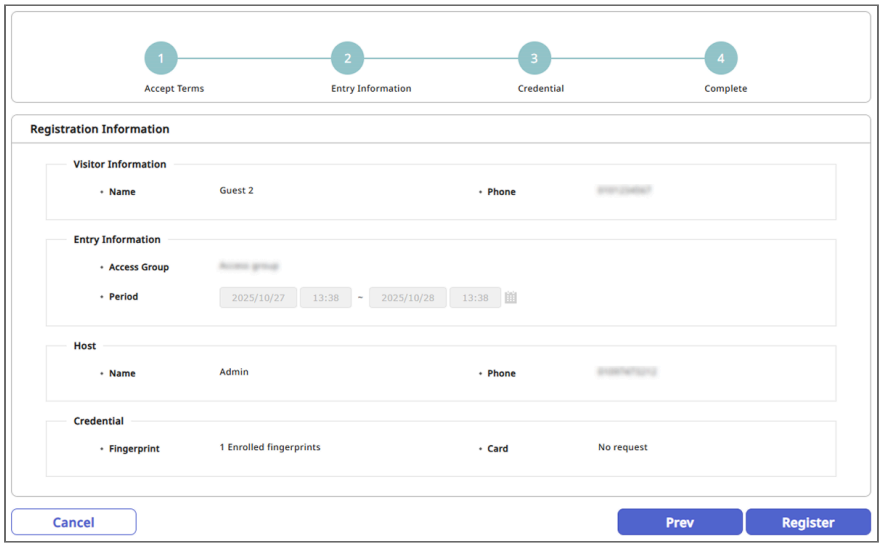
- **Visitor**：訪問者の名前と電話番号を入力してください。
- **Host**：訪問先担当者の名前と電話番号を入力してください。
- **Entry Information**：入退室エリアと訪問期間を設定してください。

5. 情報入力が完了したら、画面右下の **Next** ボタンをクリックしてください。
6. 入退室手段を設定してください。



- **Fingerprint**：指紋認証を使用する場合は **+ Fingerprint** ボタンをクリックして指紋を登録してください。
- **Card**：カード認証を使用する場合は **Request** に設定した後、管理者からカードを発行してもらってください。

7. 設定が完了したら、画面右下の **Next** ボタンをクリックしてください。
8. 申請したすべての情報を確認したら、画面右下の **Register** ボタンをクリックしてください。



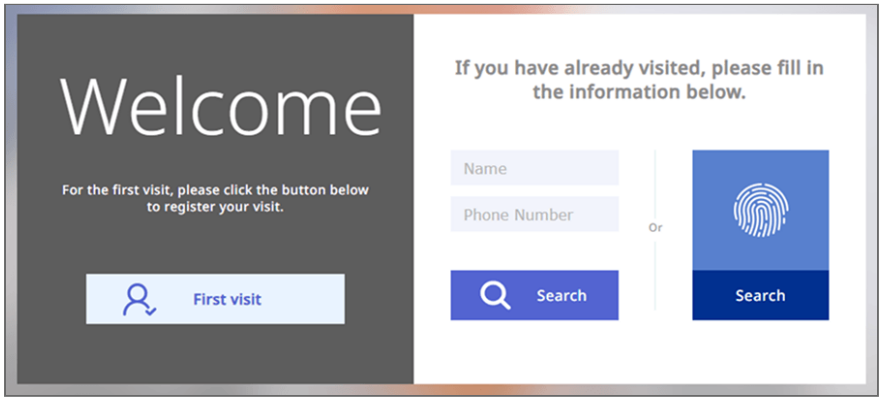
情報

- 訪問先の入退室に関する約款および個人情報の取扱方針の作成については、訪問者設定をご参照ください。
- 名前は最大48文字まで入力できます。
- 訪問者情報の入力にカスタムフィールドを追加するには、訪問者設定を参照してください。
- 訪問PCに割り当てた訪問先の入退室グループのみ選択できます。詳細については 訪問者設定 を参照してください。
- アクセスグループの詳細については、アクセスグループを管理するをご参照ください。
- 前の段階に戻って訪問情報を修正する場合は **Prev** ボタンをクリックしてください。
- 指紋をスキャンするには、訪問申請用PCに指紋登録デバイスが接続されている必要があります。

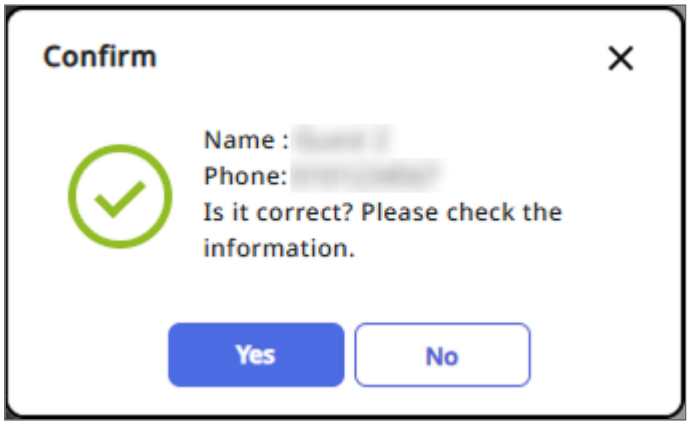
既存情報で訪問申請

訪問先に指紋が登録されている場合は、指紋を検索して既存の訪問情報を使用して訪問を申請できます。

1. 訪問申請用PCで訪問申請ページを開いてください。訪問申請ページのURLアドレスは `https://{biostar_x_server_ip}/#/register-welcome` 形式です。



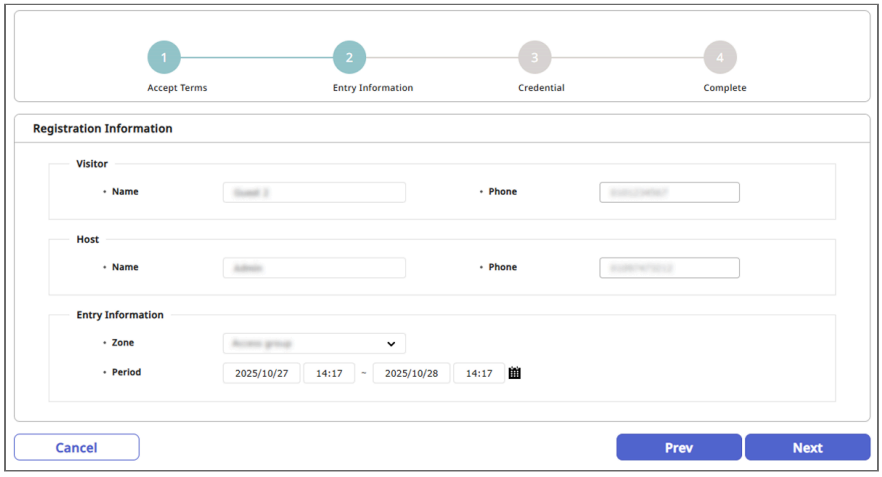
2. 画面中央の指紋アイコン下にある **Search** をクリックしてください。
3. 指紋スキャナデバイスで指紋をスキャンしてください。スキャンした指紋を使用して登録済みユーザーを検索します。
4. 以前に指紋を登録した訪問者と一致する指紋がある場合、確認メッセージが表示されます。



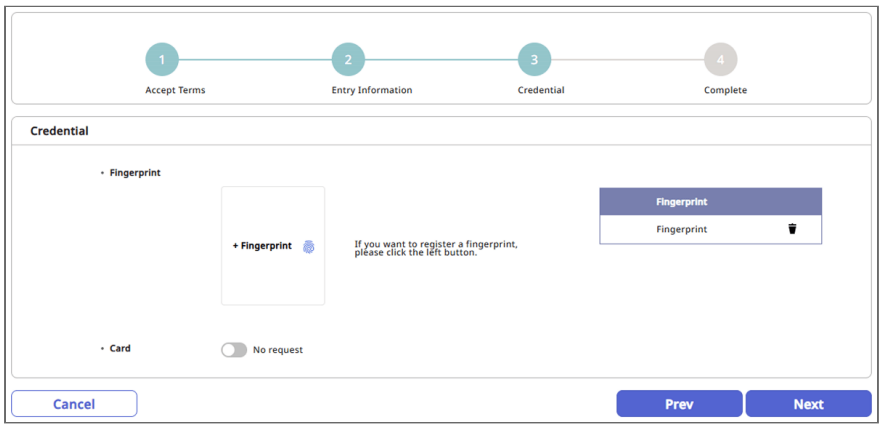
5. 検索された訪問者で正しければ **Yes** ボタンをクリックしてください。

6. 訪問先の入退室に関する約款および個人情報取扱方針への同意を完了したら、画面右下の **Next** ボタンをクリックしてください。

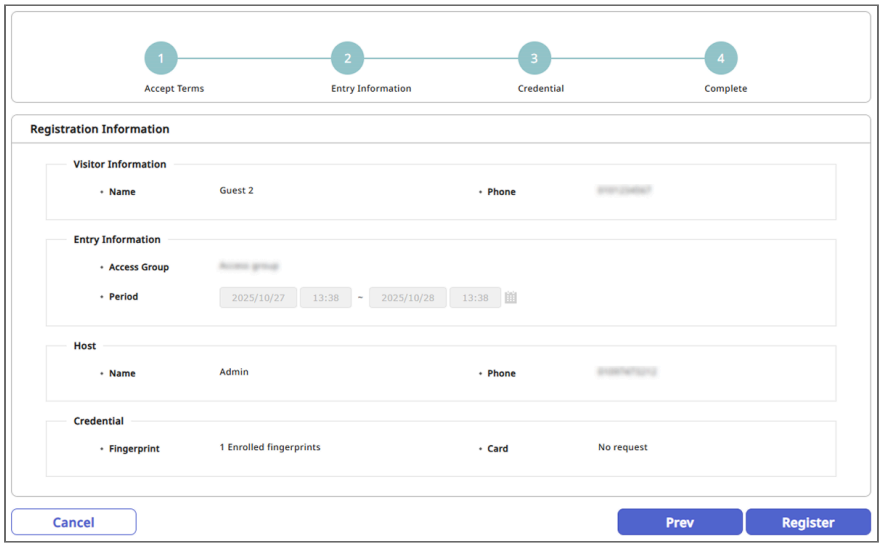
7. 前回訪問時に設定した訪問情報を確認してください。既存情報を修正する場合は各項目を修正した後、画面右下の **Next** ボタンをクリックしてください。



8. 前回訪問時に設定した入退室手段を確認してください。既存の入退室手段を変更する場合は、変更する項目を修正した後、画面右下の **Next** ボタンをクリックしてください。



9. 申請したすべての情報を確認したら、画面右下の **Register** ボタンをクリックしてください。



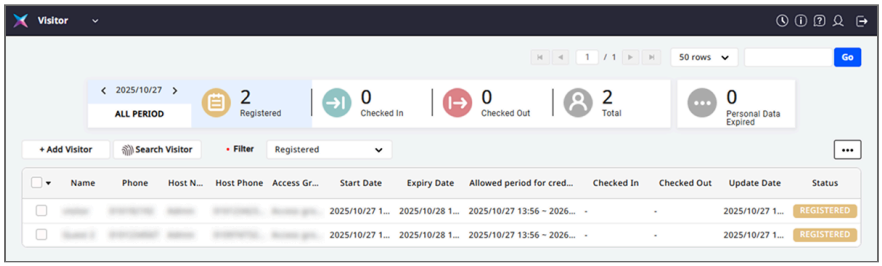
来訪申請を管理する

来訪申請を承認または修正できます。管理者が直接来訪者を追加または削除することもできます。

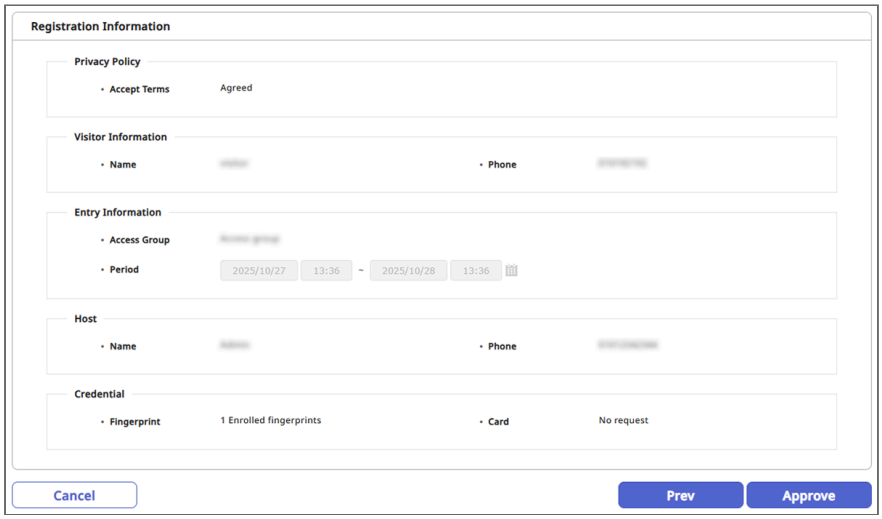
来訪承認

来訪申請履歴を確認し、来訪者の入退室を承認する方法を説明します。

1. **Launcher** ページで **Visitor** をクリックします。
2. 来訪者一覧で、承認する来訪者をクリックします。



3. 来訪者の来訪情報を確認して修正が必要な項目を修正した後、**Edit** をクリックします。
4. 画面右下の **Check in** をクリックします。
5. **Registration Information** の内容を確認し、来訪を承認するには、画面右下の **Approve** をクリックします。

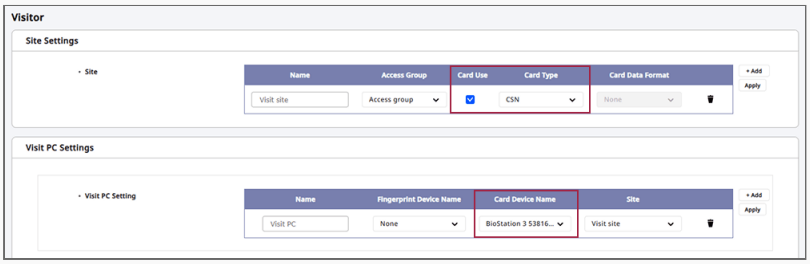


情報

- 来訪申請時に来訪者入退室利用規約に同意していない申請者の場合、**Approve** は無効化されます。 **View terms** をクリックして来訪者に入退室利用規約を提示し、規約への同意を取得します。来訪者が入退室利用規約に同意しない場合、来訪が制限されます。



- 来訪PCにカード登録デバイスが設定されている場合、**Approve and register card** が有効になります。来訪を承認して入退室カードを発行するには、**Approve and register card** をクリックします。詳細については 承認とカード登録 を参照してください。
- 来訪PCでカード利用を設定するには、**Settings** → **Visitor** メニューで以下の最小設定が必要です。詳細については 訪問者設定 を参照してください。

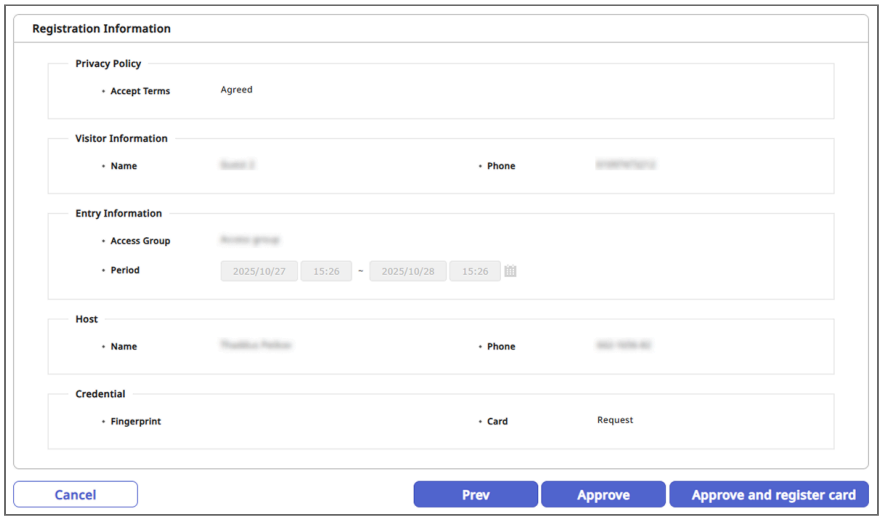


  - **Site Settings** → **Card Use** / **Card Type**
  - **Visit PC Visit PC Setting** → **Card Device Name**

承認とカード登録

来訪申請を承認して入退室カードを発行する方法を説明します。

1. **Registration Information** 画面で、画面右下の **Approve and register card** をクリックします。

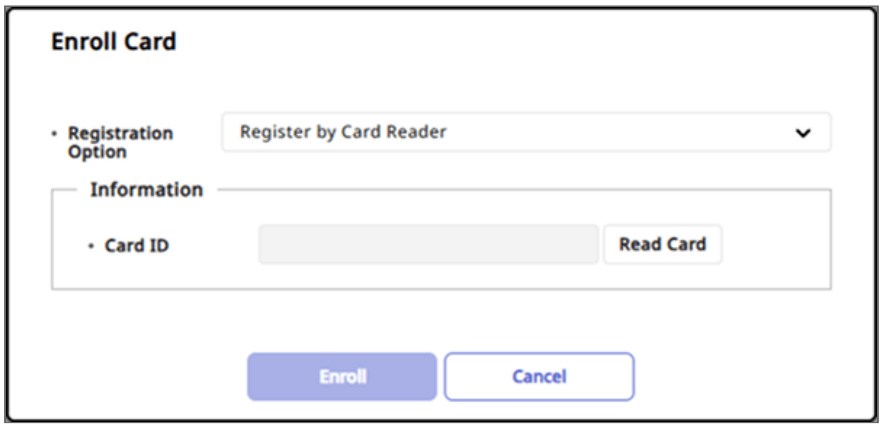


2. カード登録ウィンドウが表示されたら、希望する登録方法を選択します。
   - **Register by Card Reader**
   - **Enter Manually**

Register by Card Reader

来訪PCに接続されたデバイスでカード情報をスキャンして登録できます。

1. **Registration Option** を **Register by Card Reader** に選択します。

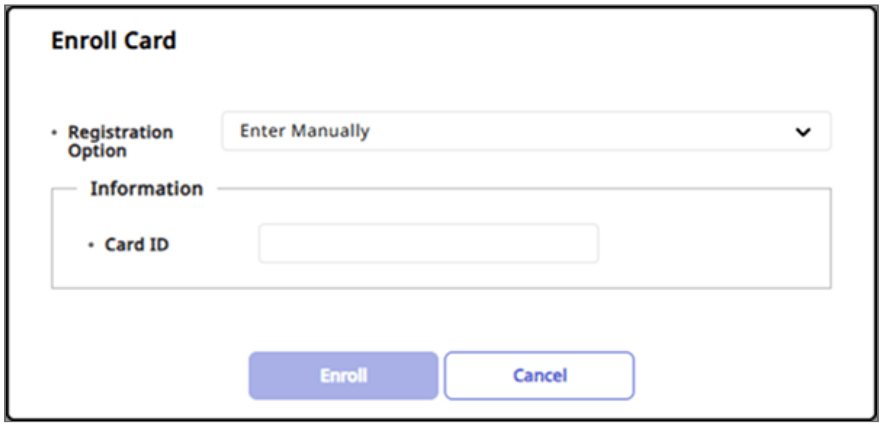


2. 登録するカードをデバイスにスキャンするには、**Read Card** をクリックします。
3. カードを登録するには、**Enroll** をクリックします。

Enter Manually

カード番号を直接入力して登録できます。

1. **Registration Option** を **Enter Manually** に選択します。

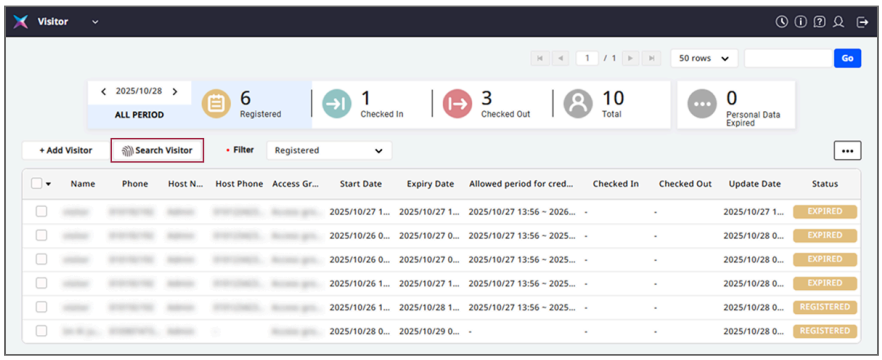


2. **Card ID** を直接入力します。
3. カードを登録するには、**Enroll** をクリックします。

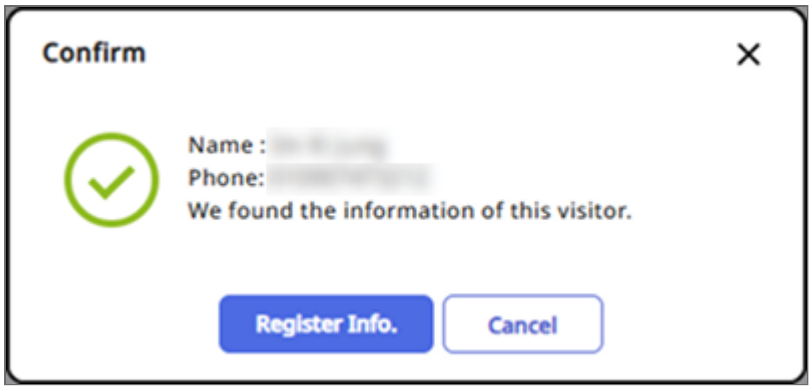
指紋検索による来訪者承認

指紋を登録済みの来訪者を指紋で検索し、承認できます。

1. **Launcher** ページで **Visitor** をクリックします。
2. 来訪申請一覧で左上の **Search Visitor** をクリックします。



3. 指紋スキャナに来訪者の指紋をスキャンします。
4. 指紋と一致する来訪者が検索されると、確認メッセージが表示されます。 **Register Info.** をクリックします。

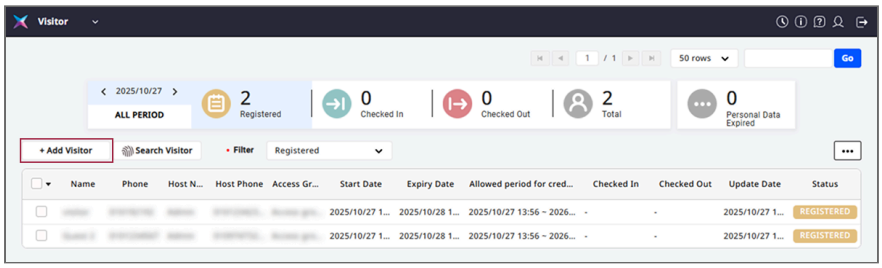


5. 来訪者の来訪情報を確認して修正が必要な項目を修正した後、**Edit** をクリックします。
6. 画面右下の **Check in** をクリックします。
7. **Registration Information** の内容を確認し、来訪を承認するには、画面右下の **Approve** をクリックします。

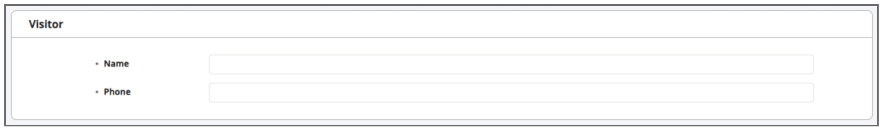
来訪者追加

管理者が直接来訪者を追加する方法を説明します。

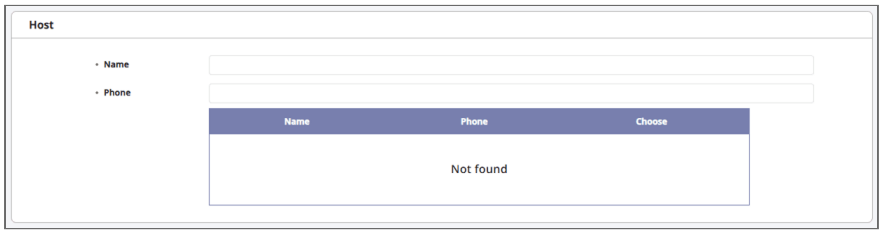
1. **Launcher** ページで **Visitor** をクリックします。
2. 来訪者一覧で左上の ＋ **Add Visitor** をクリックします。



3. **Visitor** セクションで来訪者の氏名と電話番号を入力します。

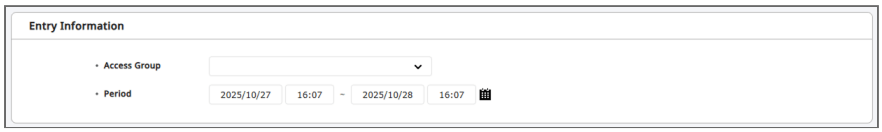


4. **Host** セクションで訪問先担当者の氏名と電話番号を入力します。



> 氏名または電話番号を入力すると、一致するユーザーの一覧が表示されます。希望するユーザーを指定するには、**Choose** をクリックします。

5. **Entry Information** セクションで入退室グループと訪問期間を設定します。



> 訪問PCに割り当てた訪問先の入退室グループのみ選択できます。詳細については 訪問者設定 を参照してください。

6. **Credential** セクションで入退室手段を設定します。



- **Card**：カード認証を使用する場合は **Request** に設定します。

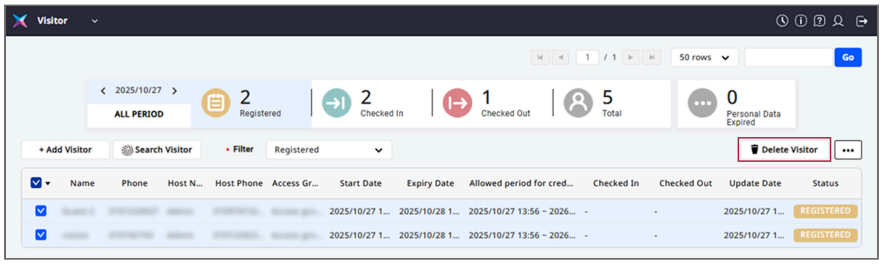
- **Fingerprint**：指紋認証を使用する場合は、**+ Fingerprint** をクリックして来訪者の指紋を登録します。

7. 来訪者追加を完了するには、画面右下の **Register** をクリックします。

> **情報**
>
> - 名前は最大48文字まで入力できます。
> - 訪問者情報の入力にカスタムフィールドを追加するには、訪問者設定を参照してください。

来訪者削除

1. **Launcher** ページで **Visitor** をクリックします。
2. 来訪申請一覧で削除する来訪者のチェックボックスをクリックします。



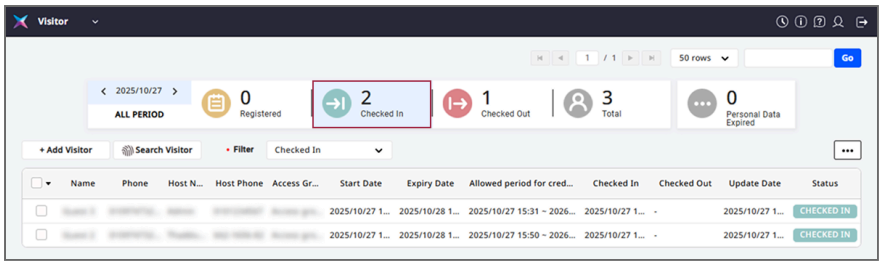
3. 画面右上の **Delete Visitor** をクリックします。
4. 確認メッセージが表示されたら、**Yes** ボタンをクリックします。

> **情報**
>
> - **Delete Visitor** は、来訪者のチェックボックスをクリックすると有効になります。
> - 来訪者は来訪申請一覧からのみ削除できます。

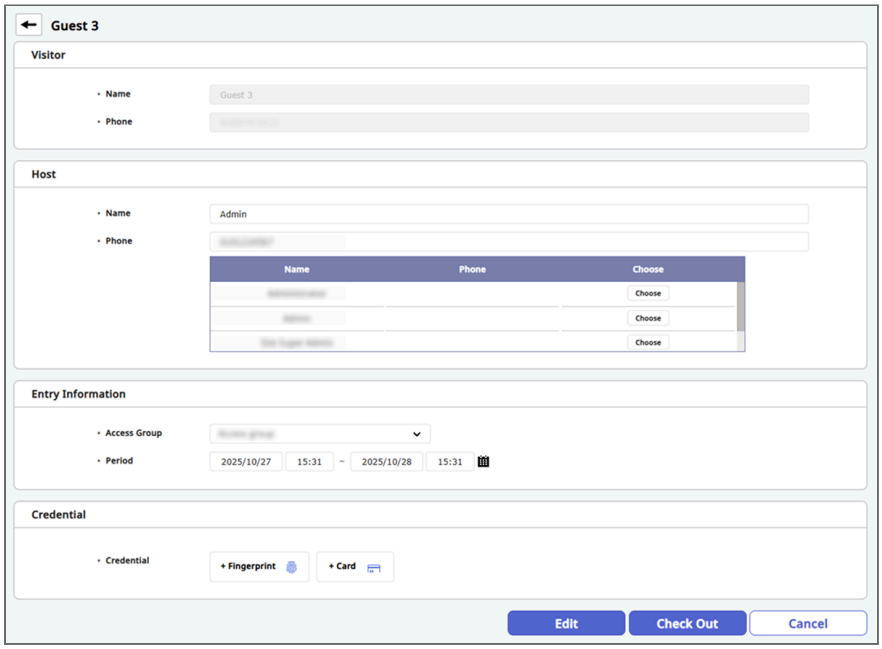
チェックイン訪問者を管理する

チェックイン状態の訪問者を確認し、訪問情報を編集するかチェックアウトできます。

1. **Launcher** ページで **Visitor** をクリックします。
2. 画面上部の **Check in** タブをクリックします。



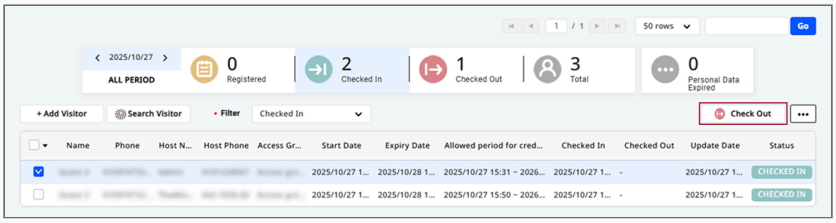
3. 訪問者リストで、編集またはチェックアウトする訪問者をクリックします。
4. 訪問者の訪問申請情報を確認します。



- 個別項目を編集して保存するには、画面右下の **Edit** ボタンをクリックします。
- チェックアウト処理を行うには、画面右下の **Check Out** ボタンをクリックします。

情報

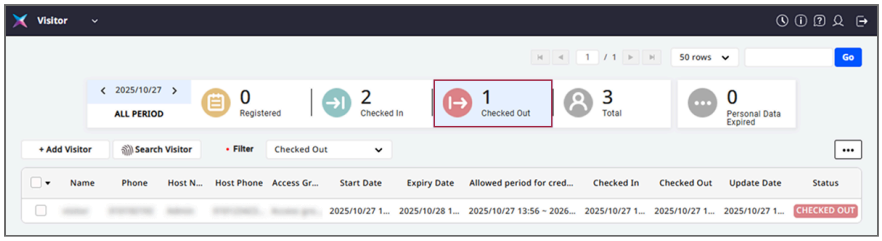
Check in リストから訪問者を選択してチェックアウトすることもできます。リストでチェックアウトする訪問者のチェックボックスをクリックし、画面右上の **Check Out** ボタンをクリックします。



チェックアウト訪問者を管理する

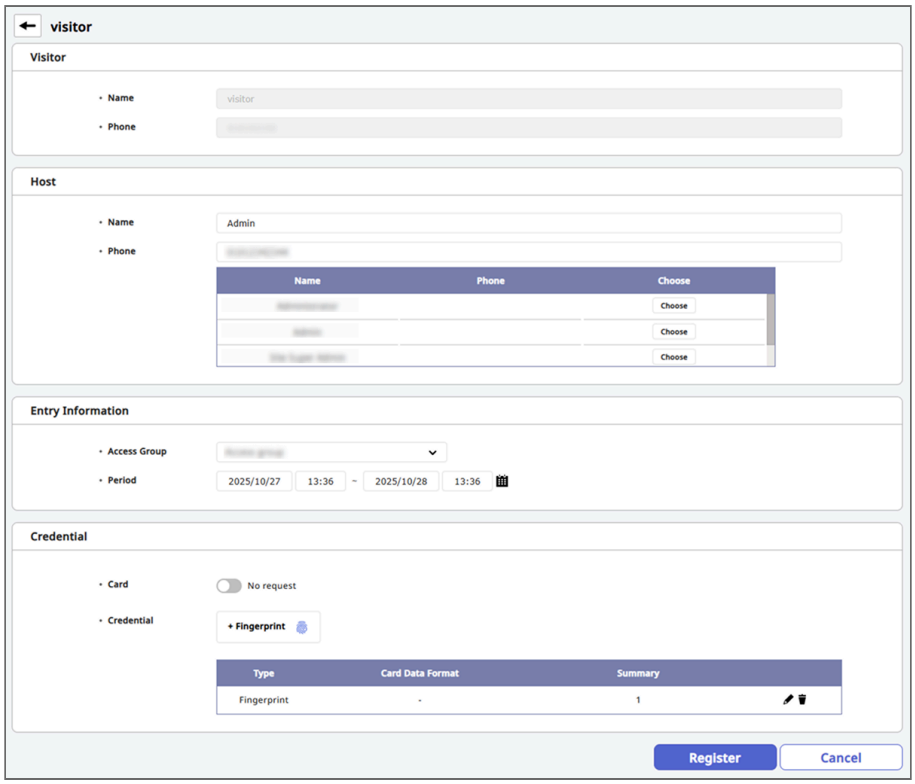
チェックアウト状態の訪問者を確認し、該当の訪問申請情報を利用して再訪問を登録できます。

1. **Launcher** ページで **Visitor** をクリックします。
2. 画面上部の **Check out** タブをクリックします。



3. 訪問者リストで再登録する訪問者をクリックします。
4. 画面右下の **Edit** ボタンをクリックします。

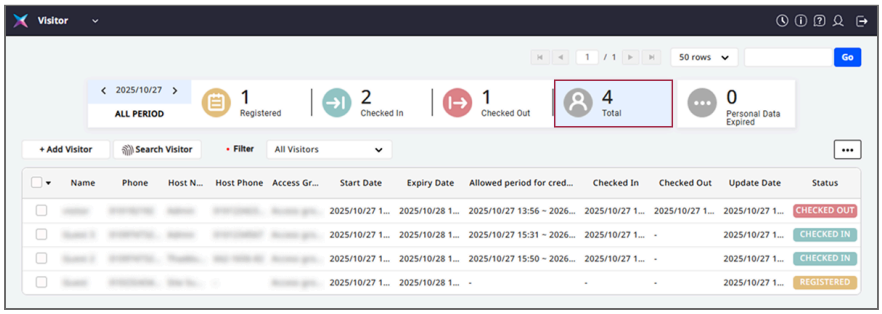
5. 修正が必要な項目がある場合は個別に修正した後、**Enroll** ボタンをクリックします。



再登録した訪問者が訪問申請リストに追加されます。画面上部の **Register** タブをクリックして確認します。

すべての訪問者を管理する

1. **Launcher** ページで **Visitor** をクリックします。
2. 画面上部の **Total** タブをクリックします。



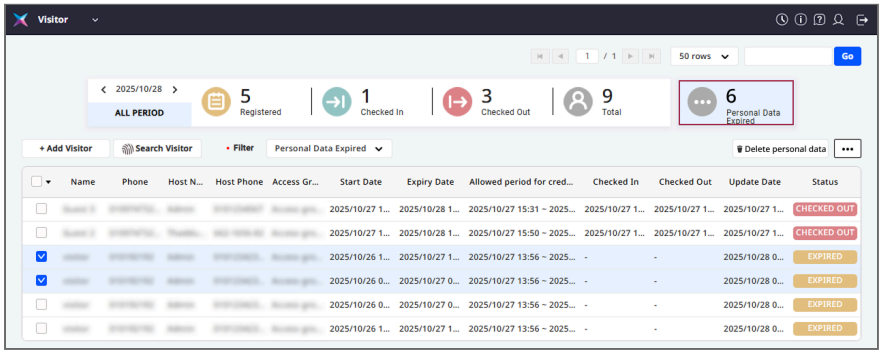
情報

- すべての訪問者リストで訪問申請を承認したり、訪問者を追加したりできます。詳細については、訪問を申請する ご参照ください。
- すべての訪問者リストでチェックインまたはチェックアウト状態の訪問者を管理できます。詳細については次のドキュメントを参照してください。
  - チェックイン訪問者を管理する
  - チェックアウト訪問者を管理する

個人情報の保存期限が切れた訪問者を削除する

個人情報の保存期間が過ぎた訪問者情報を削除します。

1. **Launcher** ページで **Visitor** をクリックします。
2. 画面上部の **Personal Data Expired** タブをクリックします。
3. 個人情報の保存期間を超過した訪問者リストが表示されたら、削除する訪問者のチェックボックスをクリックします。 1人以上選択します。



4. 訪問者リストの右上にある **Delete personal data** をクリックします。
5. 確認メッセージが表示されたら、**Yes** ボタンをクリックします。

> **情報**
>
> - 個人情報の期限切れ訪問者一覧を確認できるのは、**Administrator** 権限を持つユーザーのみです。ユーザー権限の詳細については ユーザー登録 をご覧ください。
> - 個人情報の保存期間の設定について詳しくは 訪問者設定 をご覧ください。

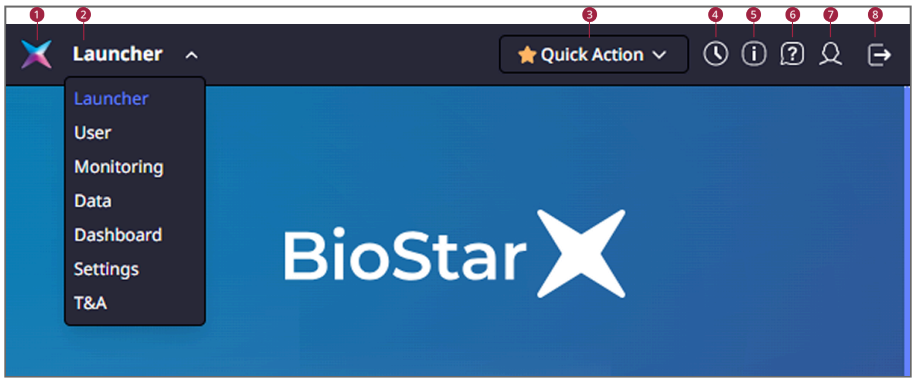
UI を確認

BioStar Xの各ページのUIを確認し、使用方法を案内します。 BioStar Xは多様な機能を提供しており、各機能にはユーザーインターフェース（UI）を通じて簡単にアクセスできます。各ページのユーザーインターフェースを確認することで、BioStar Xの機能をより簡単に理解して活用できます。以下は、BioStar Xの主要ページとそのUI構成要素の説明です。

共通 UI を理解する

BioStar X のユーザーインターフェース（User Interface、以下 UI）は、ユーザーがシステムを簡単に操作・利用できるように設計されています。本ドキュメントでは、**BioStar X** の共通 UI 構成要素について説明します。このドキュメントを通じて **BioStar X** の UI を理解し、システムをより効率的に利用できます。

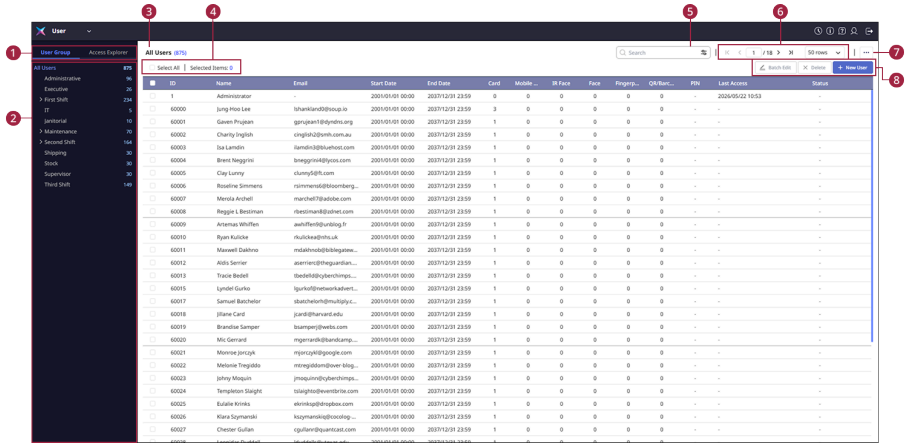
画面のヘッダー領域はすべてのページで共通で、**BioStar X** のさまざまな機能へアクセスできるリンクボタンを提供します。



1. **BioStar X ロゴ**：ユーザーが **BioStar X** の **Launcher** ページに戻るためのリンクボタンです。
2. **ショートカット**：**BioStar X** が提供する主要ページへ移動できるリンクを提供します。
3. **Quick Action**：サーバーユーザーが設定した **アクション**（Action）機能を実行できます。ボタンをクリックするとアクション一覧が表示されます。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。
4. **サーバー時刻**：稼働中の **BioStar X** サーバーの時刻を確認できます。ボタンにマウスを乗せると現在のサーバー時刻が表示されます。
5. **情報**：インストールされている **BioStar X** のバージョン情報を確認できます。
6. **ヘルプ**：**BioStar X** のヘルプページへ移動するリンクボタンです。
7. **アカウント**: **Preferences** メニューへ移動したり、現在ログインしているユーザーのパスワードを変更できます。
   - **Preferences**メニューの詳細は基本設定を構成するを参照してください。
   - 現在ログインしているユーザーのパスワード変更については、ユーザー権限を設定するを参照してください。
8. **ログアウト**：現在ログインしているユーザーのセッションを終了してログアウトできます。

ユーザー

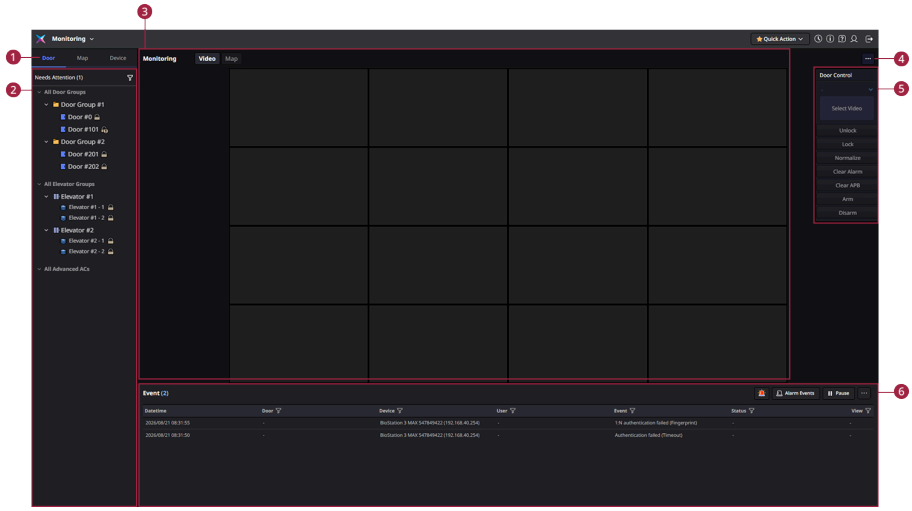
User ページの **User** メニューでは、ユーザーグループ管理、ユーザー管理、アクセス権別のユーザー確認など、さまざまな機能によりユーザーを効率的に管理し、権限によってセキュリティを強化できます。 **User** ページの UI 構成要素は次のとおりです。



1. ユーザーグループまたはアクセスグループを確認できます。
   - **User Group** について詳しくは、ユーザーグループを管理するを参照してください。
   - **Access Explorer** について詳しくは、アクセスグループを管理するを参照してください。
2. ユーザーグループまたはアクセスグループをツリー構造で確認できます。ツリーを展開または折りたたみ、各グループをクリックしてそのグループに属するユーザーを確認できます。
3. サイドメニューで選択したユーザーグループのユーザー数を確認できます。
4. ユーザー一覧に表示されているすべてのユーザーを選択するには、**Select All** ボタンをクリックします。選択したユーザーの数は **Selected Items** に表示されます。
5. キーワードを入力してユーザーを検索できます。詳しくは ユーザーを閲覧する をご参照ください。
6. 画面右上のページ移動ボタンをクリックして、次または前のユーザーリストを確認できます。また、移動したいページを指定することもできます。詳しくは ユーザーを閲覧する をご参照ください。
7. [•••] ボタンをクリックすると、ユーザーに関連するさまざまな機能を使用できます。
   - **Export**：ユーザー一覧を CSV ファイルまたは Data ファイル形式で保存できます。詳しくは ユーザー情報のエクスポート/インポート をご参照ください。
   - **Import**：ユーザー一覧を CSV ファイルまたは Data ファイル形式で読み込んだり、顔認証情報を取り込んだりできます。詳しくは ユーザー情報のエクスポート/インポート をご参照ください。
   - **Transfer to Device**：登録したユーザー情報をデバイスへ送信する機能です。詳しくは デバイスにユーザー情報を転送する をご参照ください。
   - **Face Migration**：**BioStar X** の以前のバージョンで登録した顔データを最新アルゴリズムにアップグレードし、認証性能を向上できます。詳しくは 顔マイグレーション をご参照ください。
   - **Column Layout**：ユーザー一覧で列ヘッダー項目を変更できます。詳しくは ユーザーを閲覧する をご参照ください。
   - **Print**：ユーザー一覧を印刷できます。
8. ユーザーの登録、一括編集、削除機能を利用できます。
   - **Batch Edit**：複数ユーザーの情報やアクセス権を一度に修正できます。詳しくは ユーザー情報を編集 をご参照ください。
   - **Delete**：選択したユーザーを削除できます。詳しくは ユーザーを削除する をご参照ください。
   - **New User**：新しいユーザーを登録できます。詳しくは ユーザー登録 をご参照ください。

モニタリング

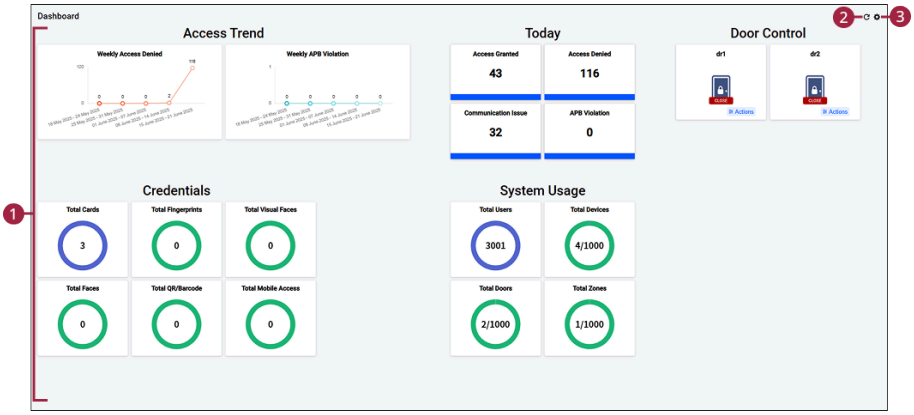
Monitoring ページのユーザーインターフェース (User Interface) を案内します。 **Monitoring** ページでは、扉、マップ、デバイスを基準にセキュリティ状態をリアルタイムでモニタリングできます。また、リアルタイムで発生するイベントを確認し、必要な対応を行えます。 **Monitoring** ページの UI コンポーネントは次のとおりです。



1. 検索入力フィールドにキーワードを入力して、デバイス、扉、カメラなど必要な項目を検索できます。
2. **Door**、**Map**、**Device** をグループ単位のツリー構造リストで確認し、モニタリングできます。
   - **Door** の監視について詳しくは、ドアをモニタリング をご参照ください。
   - **Map** の監視について詳しくは、マップをモニタリングする をご参照ください。
   - **Device** の監視について詳しくは、デバイスをモニタリングする をご参照ください。
3. **ビデオタイル** では、扉、カメラ、エリアなどのリアルタイム映像またはマップを確認できます。複数カメラの映像を同時に配置してモニタリングできます。
   - カメラ映像の監視について詳しくは、ビデオをモニタリングする をご参照ください。
   - マップモニタリングの詳細については、マップをモニタリングするを参照してください。
4. ••• ボタンをクリックすると、ビデオタイルのすべての要素を閉じる **Close All** 機能が使用可能になります。
5. **コントロールパネル** では、選択した扉またはデバイスの機能を制御できます。詳しくは、出入ドアを制御する をご参照ください。
6. **イベントリスト** では、リアルタイムで発生するイベントを時系列で確認できます。イベントごとに詳細情報、状態、関連ユーザーおよびデバイス情報を確認し、必要に応じてすぐに対処できます。詳しくは、イベントをモニタリングする をご参照ください。

ダッシュボード

Dashboard ページのユーザーインターフェース(User Interface)について説明します。



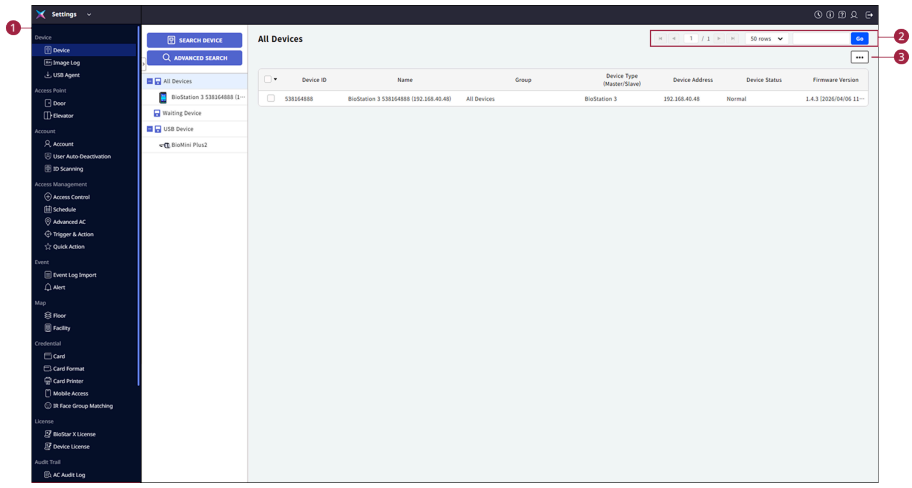
上記の画像は例示です。実際の画面とは異なる場合があります。

1. **ウィジェット表示エリア**：ユーザーが追加したウィジェットが表示されるエリアです。
   - 各ウィジェットのサイズは、ウィジェットごとに制限された範囲内で自由に調整できます。
   - ウィジェットは空いている領域にのみ配置でき、ウィジェット同士を重ねることはできません。
2. **再読み込み**：ダッシュボードページを再読み込みして、編集したウィジェットのデータを更新します。

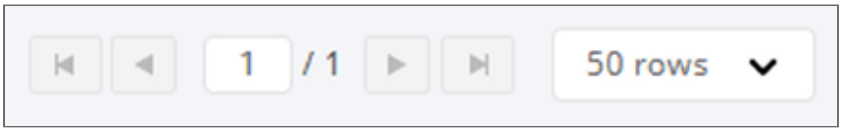
   Dashboard Settings の **Auto Refresh Interval** で再読み込み間隔を設定できます。
3. **Dashboard Settings**：新しいウィジェットを追加するか、追加済みウィジェットのデータと外観を設定できます。

設定

Settings ページでは、**BioStar X** のさまざまな設定を管理できます。このページの UI コンポーネントは次のとおりです。



1. **Settings** メニューから提供されるさまざまな設定メニューを確認できます。詳細については、設定を参照してください。
2. ページリストをナビゲートできるツールです。ページを移動したり、任意のページへジャンプできます。



- ：最初のページに移動します。

- ◀：前のページに移動します。
- ▶：次のページに移動します。
- ▶|：最後のページに移動します。
- 目的のページに移動するには、数字入力フィールドにページ番号を入力します。
- 1ページに表示する一覧の件数を設定するには、行選択ボックスをクリックします。

> **情報**
> 設定メニューによっては対応していない場合があります。

3. ••• ボタンをクリックすると追加機能を使用できます。

> **情報**
> 設定メニューによってサポートされる機能は異なる場合があります。

ライセンス ポリシー

BioStar X は **BioStar 2** の後継バージョンとして開発された次世代入退室管理ソフトウェアです。強化されたシステム アーキテクチャと拡張された機能、そしてより柔軟なライセンス モデルにより、現在および将来のさまざまな導入環境をサポートします。

BioStar X は **スターター**から **エリート**まで、合計 5 つの拡張可能なライセンス グレードを提供しており、小規模事業所から大規模企業環境まで、ニーズに合わせて選択できます。モジュール構造で設計されているため、ビデオ連携、モバイルアクセス、マルチサーバーサポートなどのさまざまなオプション機能を追加できます。

複雑なライセンス要件の解決に役立つ **BioStar X ライセンス計算機** をお試しください。このツールは、必要に応じたライセンスタイプと数量の決定を支援します。

基本ライセンス

基本ライセンス は、システムを有効化して運用するために必須のコンポーネントです。このライセンスは、追加機能やアップグレードを適用するための基盤となります。

	デバイスマネージャー(Device Manager)	スターター(Starter)	エッセンシャル(Essential)	アドバンス(Advanced)	エンタープライズ(Enterprise)	エリート(Elite)
最大ドア数	0	5	32	128	500	2000
最大ユーザー数	200	100	1,000	50,000	100,000	500,000
最大管理者数	1	1	10	20	40	100
最大接続 IP デバイス数	1,000	1,000	1,000	1,000	1,000	1,000
マップ(Maps)	✕	✕	✔	✔	✔	✔
ビデオ (Video)	✕	✕	アドオン	アドオン	アドオン	アドオン
高度な入退室管理 *(アンチパスバック、火災警報、侵入警報、点呼、在室人数制限、エレベーター、インターロック)*	✕	✕	アドオン	アドオン	✔	✔

	デバイスマネージャー(Device Manager)	スターター(Starter)	エッセンシャル(Essential)	アドバンス(Advanced)	エンタープライズ(Enterprise)	エリート(Elite)
ライセンスアップグレード *（ドア/ユーザー/管理者）*	ユーザーおよび管理者のみ対象	✕	アドオン	アドオン	アドオン	アドオン

- **デバイスマネージャー** ライセンスは、サードパーティーのソフトウェアまたはシステムを使用するお客様が BioStar X を通じて Suprema デバイスを効率的に管理する際に必要なライセンスです。
- **最大管理者数** は、システムにアクセス権を付与されたユーザー数を指します。
- 最大接続 IP デバイス数が 1,000 台以上の場合、**マルチコミュニケーション** サーバーの使用を推奨します。

ライセンスアップグレード

ライセンスアップグレードは **エッセンシャル**、**アドバンス**、**エンタープライズ**、**エリート** グレードのライセンス保有者に提供されます。**デバイスマネージャー** ライセンスの保有者は、ユーザー (User) と管理者 (Operator) のアップグレードのみ購入できます。

	数
ドア	32
ユーザー	5,000
管理者	10

機能追加オプション (Feature Add-ons)

以下の項目は個別に購入でき、**エッセンシャル**、**アドバンス**、**エンタープライズ**、**エリート**ライセンスグレードに追加できます。

機能	ライセンス種類	備考
マルチコミュニケーションサーバー Init	基本ライセンス	マルチコミュニケーションサーバーが1台含まれています。最大1,000台のIP機器をサポートします。
マルチコミュニケーションサーバー Add-on	追加サーバー	マルチコミュニケーションサーバーを1台追加する際に必要です。ライセンスごとにIP機器を1,000台ずつ追加できます。

機能	ライセンス種類	備考
GIS マップ	システム	GIS マップを利用してエリア（Area）や施設（Facility）、階（Floor）を設定できます。
ビデオ	カメラ	サードパーティ製のVMSと連携する際に必要です。システムごとに1,000台のカメラと連携できます。
サーバーマッチング	ID、カード、指紋、IR フェイス	デバイスに保存された ID、カード、指紋、IR フェイス情報をサーバーデータベースに保存されたクレデンシャルと照合するサーバーマッチング方式です。
訪問者	システム	管理者およびオペレーターは訪問者の出入りを追跡または制御できます。
ディレクトリ連携	システム	中央集権的なユーザー管理のためにディレクトリサービスとの統合をサポートしています。
出席確認(Roll Call)	システム	-

VMS に接続されているすべてのカメラを **BioStar X** と必ずしも連携する必要はありません。例えば、VMS が 32 台のカメラをサポートしていても、ユーザーは実際に **BioStar X** と連携させる特定のカメラ分だけライセンスを購入すればよく、すべてのカメラ分のライセンスを購入する必要はありません。

以下の項目は個別に購入でき、基本ライセンスに関係なく追加できます。

機能	ライセンス種類	備考
モバイルアプリ	システム	-
イベントログ API	システム	システムは外部 API を通じてイベントログを受信して記録できます。これにより、他社のアプリケーションやサービスが集中ロギングとレポートのために入退室管理システムにイベントデータを直接追加できます。
リモートアクセス	システム（年間決済）	外部ネットワークから **BioStar X** サーバーへ接続できるセキュアトンネル機能を提供します。外部ネットワークから **BioStar X** モバイルおよび API へのアクセスのゲートウェイとしても機能します。 **Send Face Mobile Enroll Link** 機能の使用に必要です。
BioStar X プラグイン	システム	外部プラグインの統合をサポートします。システムあたり最大 10 個のカスタムプラグインを利用できます。詳細については、プラグインご参照ください。
勤怠管理 (T&A)	Standard	最大 500 ユーザーをサポートします。
	Enterprise	ユーザー数に制限はありません。

情報

勤怠管理 (T&A) のユーザー数は基本ライセンスの制限に従い、勤怠管理 エディションで許可されている最大ユーザー数まで利用できます。（例: Standard エディションの場合、ユーザー 500 名）

高度な入退室管理（Advanced Access Control）

高度な入退室管理は次の7つの個別機能で構成され、必要な機能だけを選択して個別に購入できます。**エッセンシャル**、**アドバンス**ライセンスグレードでは追加オプションとして購入でき、**エンタープライズ**、**エリート**ライセンスグレードでは7つの機能がすべて標準で含まれます。

機能	ライセンス種類	備考
アンチパスバック（Anti-passback）	システム	-
火災警報（Fire Alarm）	システム	-
侵入警報（Intrusion Alarm）	システム	-
点呼（Muster）	システム	-
在室人数制限（Occupancy Limit）	システム	-
エレベーター（Elevator）	システム	-
インターロック（Interlock）	システム	-

- スケジュールロック（Scheduled Lock）とスケジュールアンロック（Scheduled Unlock）はライセンスが不要な基本の入退室管理機能で、上記7つの機能とは別に常に使用できます。
- すでに高度な入退室管理パッケージを購入している場合、引き続き同様に使用できます。新規購入からは、7つの機能を個別に選んで購入できます。

デバイスライセンス

デバイスライセンスは個別に購入でき、基本ライセンスに関係なく追加できます。デバイスライセンスはシリアル番号（S/N）を基準に発行されます。ライセンスが必要なデバイスでのみ、その機能を有効にできます。

機能	ライセンス種類	対応モデル	備考
カメラ QR	デバイス	BioStation 3 Max, XPass Q2, BioStation 3, X-Station 2	-
Multi Face Authentication	デバイス	BioStation 3	-

機能	ライセンス種類	対応モデル	備考
ワイヤレスロック	デバイス	CoreStation 40	-

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。

本製品に含まれるオープンソースソフトウェアの必須告知事項とライセンスについては、以下のリンク を参照してください。

ffmpeg

BioStar X には、動画ファイルの変換と情報の確認のために ffmpeg(https://ffmpeg.org) が含まれています。 *ffmpeg.exe* と *ffprobe.exe* のコマンドラインバイナリを提供しており、どちらのバイナリも下記の ffmpeg ソース tarball からビルドされます。 ffprobe は別のコンポーネントではなく、ffmpeg プロジェクトに含まれるツールです。

- Component: ffmpeg (ffmpeg.exe, ffprobe.exe)
- Version: 8.1
- License: GNU Lesser General Public License v2.1

  全文：COPYING.LGPLv2.1 を参照
- Source code: ffmpeg-8.1.tar.xz
- Upstream URL: ffmpeg-8.1.tar.xz
- SHA-256: b072aed6871998cce9b36e7774033105ca29e33632be5b6347f3206898e0756a

Build configuration:

```
./configure \
  --arch=x86_64 \
  --target-os=mingw64 \
  --disable-gpl \
  --disable-nonfree \
  --disable-libx264 \
  --disable-libx265 \
  --disable-libxvid \
  --enable-mediafoundation \
  --enable-libmp3lame \
  --disable-doc \
  --disable-debug \
  --enable-small \
  --pkg-config-flags=--static \
  --extra-ldflags="-static"
```

修正点: なし。アップストリームのソース tarball を変更せずそのまま使用してビルドしました。

BioStar X が使用するエンコーダーは次のとおりです。

- h264_mf (H.264 via Windows Media Foundation)
- libmp3lame (MP3 audio, LGPL)

libmp3lame

BioStar X は MP3 オーディオのエンコードに libmp3lame を使用します。

- Component: libmp3lame (LAME MP3 Encoder)
- Version: 3.100
- License: GNU Lesser General Public License v2.1

  全文：COPYING.LGPLv2.1 を参照 (ffmpeg と同じ LGPL v2.1 版)
- Source code: lame-3.100.tar.gz
- Upstream URL: lame-3.100.tar.gz
- SHA-256: ddfe36cab873794038ae2c1210557ad34857a4b6bdc515785d1da9e175b1da1e

修正点: なし。アップストリームのソース tarball を変更せずそのまま使用し、ビルド時に `--enable-libmp3lame` オプションで *ffmpeg.exe* と *ffprobe.exe* に静的にリンクしました。

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。