CLUe

管理者ガイド

バージョン R_2026-09-28

日本語
JA 102.00

suprema
SECURITY & BIOMETRICS

目次

CLUe Webポータルの始め方 5

管理者レベルの理解 5

下位項目の追加 6

管理者の招待 7

サービスを設定する 9

顧客API連携 12

開始する前に 12

顧客社API連携 13

主な作業ワークフロー 14

設定ワークフロー 15

入力ルール要約 26

トラブルシューティング 27

ファームウェアを変更する 31

CLUe対応モードに切り替え 31

トラブルシューティング 33

デバイスを追加する 35

デバイス登録（ブランチ管理者） 35

デバイス割り当て 36

テストプレースの設定（ブランチ管理者） 39

デバイスのセルフ登録 41

対応デバイスおよびファームウェアバージョン 41

管理者準備段階 41

現場登録段階 43

参考 46

ドアの追加 47

ドア設定 47

スレーブ装置リレー使用 48

ファームウェアをアップグレードする 50

プレースへ移動 50

ファームウェアをアップグレードする 51

デバイス Webhook 設定 53

対応デバイス 53

主な利点 53

Webhook 設定 53

参考 46

監査ログを確認する 58

監査ログを照会する 58

詳細情報の確認 58

照会期間の設定 59

検索 59

モバイルアプリの使用方法 61

CLUeモバイルアプリの管理者招待 61

CLUeアプリのダウンロード 62

ログイン 63

CLUeアプリの主要機能 66

CLUe APIガイド 68

APIキーとは 68

APIキーの発行 68

CLUe APIの基本 69

API呼び出し制限 71

Dynamic QRコード連携 72

CLUe Dynamic QRコードとは 72

開始する前に 12

APIキーの発行 68

サービス設定 73

次のステップ 0

次のステップ 0

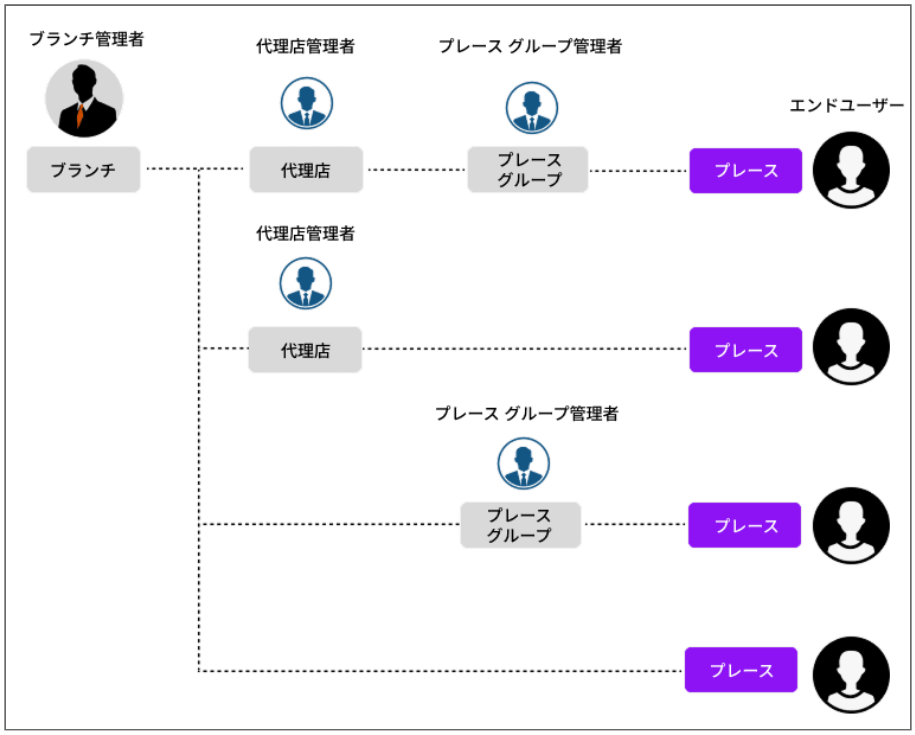
次のステップ 0

CLUe Webポータルの始め方

CLUe Webポータルを初めて使用する場合は、まず管理者権限の構造を理解してください。 このドキュメントでは、ブランチの下に代理店、プレース グループ、プレースを追加する方法を案内します。

管理者レベルの理解

CLUeは、複数の拠点で顧客サービスを運営する流通チャネル環境向けに設計された、3段階の階層構造を持つマルチテナントシステムです。



- **ブランチ管理者**(Branch Admin): ブランチ管理者は、**代理店/プレース グループ/プレース**を下位項目として作成できます。
- **代理店管理者**(Disti Admin): 代理店管理者は、**プレース グループ/プレース**を下位項目として作成できます。
- **プレース グループ管理者**(Place Group Admin): プレース グループ管理者は、**プレース**を下位項目として作成できます。

メールで顧客を招待し、招待された顧客はメールに含まれるリンクから登録した後、招待されたプレース グループにアクセスできます。

1つのブランチは複数の代理店を持て、1つの代理店も複数のプレース グループを持てます。 代理店管理者レベルでは、自分の代理店と下位項目のみを表示できます。

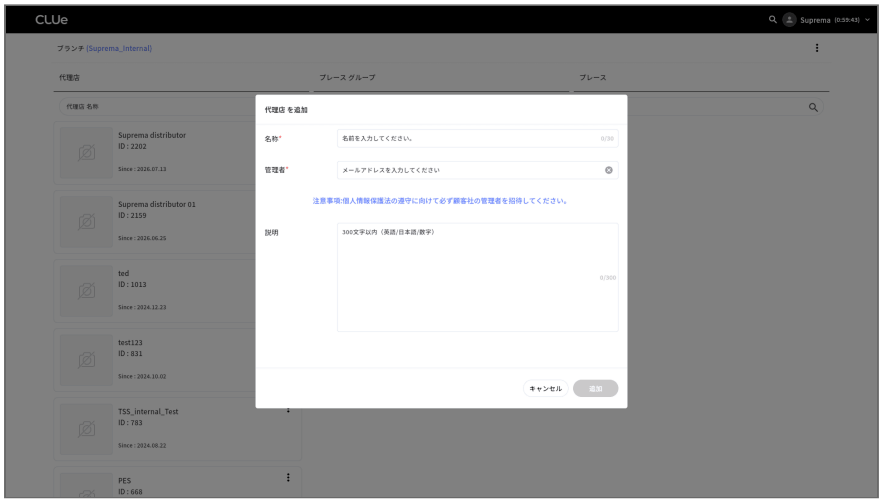
> **顧客や最終ユーザーはどの項目に該当しますか?**
>
> この階層構造では、**プレース グループ**(Place Group)が顧客またはサービス提供者に割り当てる項目です。 プレース グループは、複数のプレースを運営する顧客単位を表します。そのため、プレースを作成するときは、該当顧客の管理者メールアドレスを入力してください。

下位項目の追加

1. CLUe Webポータルにログインしてください。
2. ログインすると、招待されたブランチの一覧を確認できます。 目的のブランチを選択してください。
3. 選択したブランチの下位項目である代理店/プレース グループ/プレースの一覧が表示されたら、画面右上の ⋮ 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 **下位階層を追加** をクリックしてください。



5. **代理店 追加** のポップアップが表示されたら、各フィールドを入力します。



> **管理者メールアドレスを入力する理由**
>
> 既定では、最上位管理者は、デバイスやドア設定など、顧客の個人情報に関係しないメニューにのみアクセスできます。 顧客の個人情報にアクセスするには顧客の同意が必要なため、まず顧客管理者を招待してください。
>
> その後、個人情報へのアクセスが必要な場合は、顧客が最上位管理者を追加で招待できます。 招待された最上位管理者は、ユーザー、管理者、監視など、個人情報を含むメニューにアクセスできます。

6. すべての入力が完了したら、下部の **追加** ボタンをクリックしてください。
7. 項目を追加すると、自動的に **基本設定** ページに移動し、名前や写真を変更できます。



情報

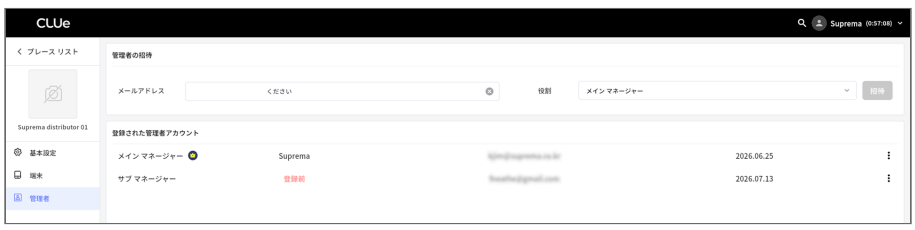
同様に、代理店、プレース グループ、プレースの一覧で ⋮ → **下位階層を追加** をクリックすると、下位項目を追加できます。

管理者の招待

管理者 メニューは表示されますが、顧客企業の同意がない限り、管理者情報は閲覧できません。 顧客企業(代理店またはプレースグループ管理者)が上位管理者を招待して初めて閲覧できます。



管理者 メニューでメールアドレスを入力すると、同じレベルの管理者を簡単に招待できます。 招待されたユーザーが登録を完了すると、同じレベルの管理者権限を持ちます。



情報

メイン マネージャー / **サブ マネージャー**: 機能上の違いはありません。 これは、少なくとも1人のメイン管理者を維持するためです。 ただし、サブ管理者はメイン管理者を削除できません。

サービスを設定する

プレース グループ単位で出入管理サービスの方式を設定します。 プレース グループで設定したサービス種類とクレデンシャルは下位のプレース全体に自動適用されるため、プレースごとに繰り返し設定する必要はありません。

CLUeは2つの出入管理サービス方式をサポートします。

- **お客様の確認**: 外部 API を通じてクライアントに出入承認を要求する方式です。
- **メンバーシップ管理**: 外部連携なしで CLUe が独立して出入を制御する方式です。

プレース グループ設定の左サイドバーで **サービス設定** をクリックします。



お客様の確認 設定

お客様の確認 方式は、出入口を開く前に外部クライアント API を呼び出して出入承認の可否を決定します。 QR コードと顔認証をサポートします。

QR 方式

QR コードをスキャンすると、CLUe サーバーがクライアント API を呼び出し、出入許可の可否を直接受け取ります。 使用する QR コードの種類に応じて、次の 2 つの方式から 1 つを選択します。

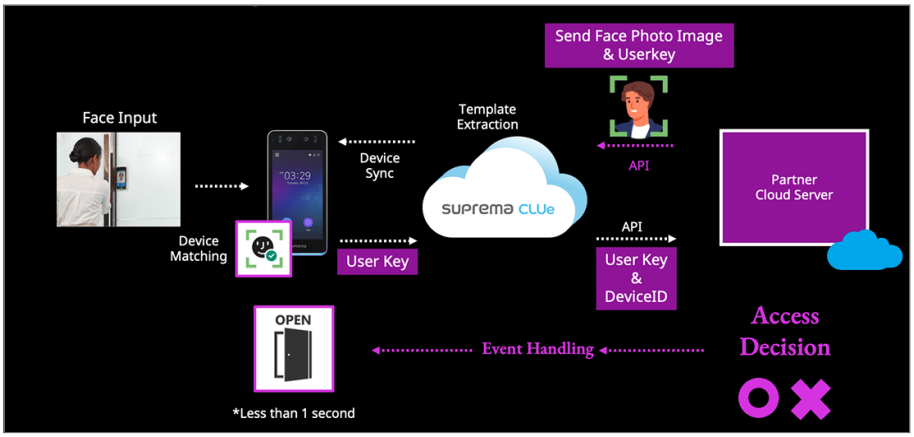
- **CLUe QR**: CLUe から直接発行する動的 QR コードです。
- **Customer QR**: 顧客が独自に QR コードを生成・運用する場合に選択します。



上記の画像は例示です。実際の画面とは異なる場合があります。

顔認証方式

顔認証を使用する場合は、画像のみを登録すると、CLUe サーバーがテンプレートを抽出してデバイスと同期します。 顔照合に成功すると、QR 方式と同様にクライアント API を通じて出入の可否を決定します。 顔ユーザー登録方法は CLUe API ドキュメントを参照してください。



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。

顧客確認コード設定

お客様の確認 方式を使用するには、CLUe サーバーが顧客またはパートナー API をどこで、どのように呼び出すかを、顧客確認コードとあわせて入力する必要があります。

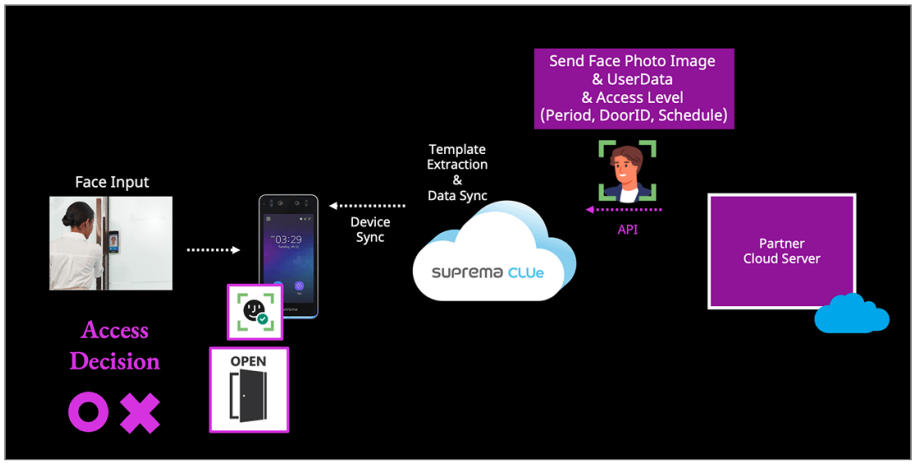


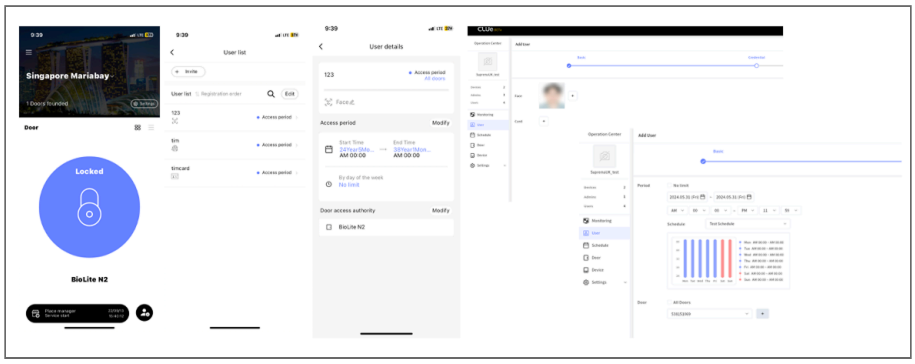
お客様の確認 コードは、Suprema CLUe チームがどのクライアントの API を呼び出すかを判断するために、事前にテストして開発したコード形式です。 このコードを入力すると、下位のプレースで追加設定なしに各認証方式に合う API を自動呼び出しし、指定した応答値を基に出入制御を実行します。

> **顧客確認コードの取得方法**
>
> 他のクライアントのコードが公開されないよう、CLUe チームで個別に管理します。 顧客確認コードの生成は API 仕様確認後に個別対応します。詳細は CLUe チームへ直接お問い合わせください。

メンバーシップ管理 設定

メンバーシップ管理 方式は、外部クライアントや第三者の介入なしで、CLUe システムが独立して出入制御を決定します。 Web ポータルやモバイルアプリケーションだけで CLUe を運用する場合にも適用できます。





メンバーシップ管理 設定を通じて、下位のプレースに適用するクレデンシャルを選択できます。



プレース グループと異なり、プレース設定を変更できますか?

はい、プレース設定ページで認証方式を設定できます。 ただし、出入方式を **メンバーシップ管理** から **お客様の確認** へ、またはその逆へ変更することはできません。 そのため、同じプレース グループの顧客で異なる出入方式が必要な場合は、用途に合わせて別のプレース グループを作成することを推奨します。

次のステップ

CLUe プレース グループで顧客企業（Vendor）API を登録し、クレデンシャルに連携して、顧客企業の出入判定ロジックを CLUe の出入制御と連携する方法を確認してください。

顧客API連携

顧客社API連携は、CLUeデバイスが認識したクレデンシャル（顔、指紋、RFカード、PIN、CLUe QR、カスタムQRなど）を顧客社が運用する外部APIに送信し、その応答に応じて入室を許可または拒否する入退室方式です。 この方式を使うと、入室権限、勤怠、訪問者管理などの顧客社固有のポリシーを、個別開発なしでCLUe入退室制御に直接反映できます。

CLUeはクレデンシャルを認識して顧客社APIへ送信する役割のみを担い、実際の入室許可可否は顧客社APIの応答で決まります。

開始する前に

対象

この文書は**プレース グループ管理者**と**プレース管理者**を対象にしています。

- **プレース グループ管理者**: 顧客社（Vendor）APIを登録、編集、削除し、クレデンシャルタイプとAPIをマッピングし、設定を下位プレースに適用します。
- **プレース管理者**: プレース グループから継承した設定を確認し、必要なときにプレース別の上書きを適用します。

> **情報**
> この文書は、**HTTPS**、**HTTPステータスコード**、**Webhook**（HTTP POST）、**JSON**、**JSONPath**に慣れたIT管理者を対象にしています。 顧客社API仕様（URL、認証ヘッダー、リクエスト/レスポンスJSON構造）は、事前に顧客担当者と相談してください。

事前準備

- このメニューにアクセスするには、対象のプレース グループ（またはプレース）に管理者として招待されている必要があります。
- 顧客社の認証用Webhook URL（**HTTPS必須**、**HTTP POST受信**）と必要な認証ヘッダー値を事前に準備してください。

主な用語

用語	説明
顧客社API連携（Customer API Integration）	ユーザーがデバイスにクレデンシャルを提示すると、クレデンシャルデータを顧客社（Vendor）が運用する外部APIへ送信して検証する入退室方式です。
クレデンシャル（Credential）	顔 / 指紋 / RFカード / ユーザーPIN / CLUe QR / カスタムQR
Webhook URL	CLUeからの認証リクエスト（HTTP **POST**、`Content-Type: application/json`）を受信するために、顧客社サーバーが公開するHTTPSエンドポイントです。
リクエストヘッダー（Request Header）	認証と権限付与のために、リクエストと一緒に送信するKey/Valueペアです。 （例: `Authorization` トークン）

用語	説明
自動フィールド	システムがリクエスト本文に自動で入力する値です。 必要なフィールドだけを選択してください。
手動フィールド	管理者がリクエスト本文に含めるために直接入力する固定値です。
判定基準（Judgment Criteria）	顧客社応答を入室許可または拒否として解釈するルールセット（statusCode、成功結果Key/Value、成功/失敗メッセージキー）です。 画面では **レスポンス解析** セクションとして表示されます。
判定モード（Judgment Mode）	判定基準を構成する要素です。 HTTP応答コードのみ使用 / 応答本文フィールドのみ使用 / 両方の組み合わせから1つを選択します。

顧客社API連携

顧客社API連携は、CLUeデバイスが認識したクレデンシャルデータを顧客社が運用するHTTPS APIへ送信し、その応答を基に入室の許可/拒否を判定する入退室方式です。 これにより、入室権限、勤怠、訪問者管理などの顧客社固有のポリシーをCLUe入退室制御に直接反映できます。

- 顔、指紋、RFカード、PIN、CLUe QR、カスタムQRなど、クレデンシャルタイプごとに異なる顧客社APIを連携できます。
- 登録を保存する前に、テスト呼び出しで連携動作を事前に確認できます。
- CLUeはクレデンシャルを識別して送信する役割のみを担い、実際の許可または拒否の判断は顧客社APIの応答で決まります。

対応クレデンシャル

- 顔
- 指紋
- RFカード
- ユーザーPIN
- CLUe QR
- カスタムQR

プレース グループとプレースの役割

レベル	役割	担当業務
プレース グループ	プレース グループ管理者	顧客社APIの登録/編集/削除、APIとクレデンシャルの連携
プレース	プレース管理者	継承した設定の確認、必要に応じたプレース別上書きの適用

適用ルール
- **プレース グループレベルで保存**: 同じ設定が、そのプレース グループのすべての下位プレースに即時適用されます。既存のプレース別上書きは、プレース グループ値で上書きされます。
- **プレースレベルで保存**: そのプレースにのみ適用されます。 他のプレースや上位のプレース グループには影響しません。

主な作業ワークフロー

顧客社API連携は、大きく2つのワークフロー（Workflow）で構成されます。 管理者が最初に行う**設定ワークフロー**と、ユーザーが実際に入室を試行したときに進行する**入室イベントワークフロー**です。

設定ワークフローの概要

管理者が実行するステップです。 各ステップは第4章から詳しく説明します。

1. （プレース グループ）入退室方式を選択してください。
   - **お客様の確認** または **混合 / 高度な方法**
   - 左サイドバーで **顧客先API連携** 項目が有効になります。
2. （プレース グループ）**顧客先API連携** でAPIを登録してください。

   基本情報 → カスタムヘッダー → 自動フィールド → 手動フィールド → テスト実行 → 応答パース設定 → 保存
3. （プレース グループ）登録したAPIを各クレデンシャルに連携してください。

   保存すると、同じ設定がすべての下位プレースに自動適用されます。
4. （オプション）プレース別の上書きを設定してください。

   選択したプレースにのみ適用されます。 既定値はプレース グループ設定をそのまま使用します。

入室イベントワークフローの概要

設定完了後、ユーザーが実際に入室を試行するときの処理順です。

1. ユーザーがデバイスにクレデンシャルを提示します。（顔 / 指紋 / RFカード / PIN / CLUe QR / カスタムQR）
2. デバイス → CLUeサーバーへ検証リクエストを送信します。
3. CLUeサーバー → 顧客社サーバーへ検証リクエストを送信します。

   登録済みWebhook URL、カスタムヘッダー、自動フィールド、手動フィールドを含みます
4. CLUeサーバーが顧客社応答を基に入室可否を判定します。

   設定した判定基準に従って、許可/拒否を決定します。
5. 結果をデバイスへ返します。

   応答にメッセージが含まれている場合、デバイス画面に表示されます。

設定ワークフロー

1段階 — 顧客社API連携を有効化

1. CLUe Webポータルにログインしてください。
2. プレース グループを選択してください。
3. 画面右上の ⋮ → **詳細設定** をクリックしてください。



4. 画面左側のサイドバーで **サービス設定** をクリックします。

> 初期状態では **アクセス方法** は **選択無し** に設定されています。 この状態では、どの設定も有効になりません。
>
> 
>

5. **アクセス方法** で **お客様の確認** を選択してください。
6. **確認対象** セクションが表示されます。



確認対象 セクションには、対応する6つのクレデンシャルがすべて表示されます。 その後、各クレデンシャルに登録した顧客社APIを連携できます。

7. 左サイドバーで **顧客先API連携** が有効になったらクリックしてください。

> **情報**
>
> - **顧客先API連携** は、**アクセス方法** が **お客様の確認** または **混合 / 高度な方法** に設定されているときに有効になります。
> - この段階では保存は不要です。 連携するAPIを登録するには、2段階 — 顧客社API登録を参照してください。

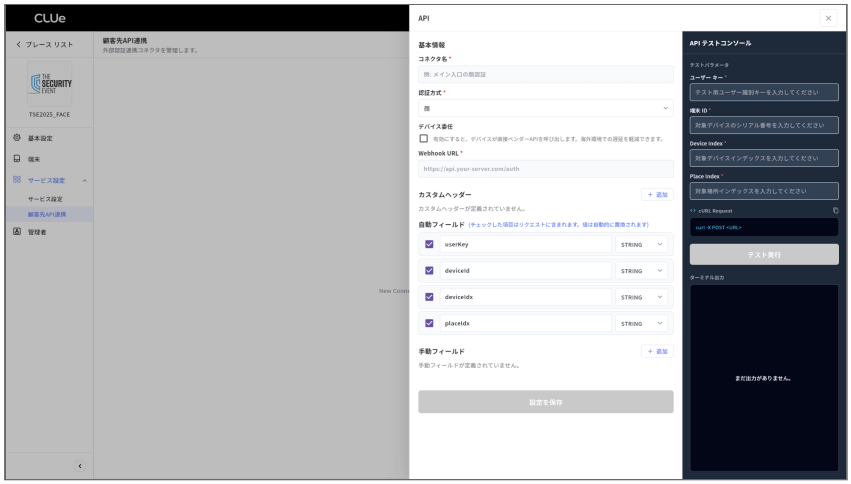
2段階 — 顧客社API登録

1 API追加

1. 画面右上の **API** ボタンをクリックしてください。



2. **API** パネルが表示されたら、必要な情報を入力してください。



2 基本情報入力

フィールド	説明	必須かどうか	入力ルール
コネクタ名	この連携を識別する名前を入力してください。	必須	最大64文字まで入力できます。
認証方式	このAPIを使用するクレデンシャルを選択してください。	必須	6つのタイプから1つを選択してください。

フィールド	説明	必須かどうか	入力ルール
Webhook URL	顧客社Webhook URLです。	必須	`https://` で始まる必要があり、最大512文字です。 `http://` URLは保存できません。

> **情報**
> **認証方式** は一度設定すると変更できません。 他のクレデンシャルタイプで使うには、新しいAPIを登録してください。

3 リクエスト仕様

CLUeは、登録したURLに**HTTP POST**、`Content-Type: application/json` リクエストのみ送信します。 顧客社APIはこの形式のリクエストを受信できる必要があり、`GET`、`PUT` など他のメソッドのみを許可するエンドポイントは使用できません。

4 応答仕様

顧客社APIは応答ヘッダーに `Content-Type: application/json` を含め、応答本文をJSON形式で返す必要があります。 HTMLエラーページ、プレーンテキスト、XMLなどのJSON以外の応答はCLUeがパースできないため、テストと実際の入室検証の両方が失敗します。

Example response body

```
{
  "valid": true,
  "message": "Access granted."
}
```

上の例では、判定基準の `Key` を `$.valid`、`Value` を `true`（`BOOLEAN`）に設定して成功条件を定義し、**成功メッセージJSONPath** を `$.message` に設定して成功メッセージを表示できます。 実際のキー名と構造は、顧客社API仕様に合わせてください。

> **登録制限**
>
> クレデンシャルタイプごとに最大**3件**のAPIを登録できます。 つまり、顔、指紋、RFカード、PIN、CLUe QR、カスタムQRの6タイプを合わせて、プレース グループごとに最大18件のAPIを登録できます。 すでに3件登録されているクレデンシャルタイプには、追加登録できません。 各クレデンシャルで実際に使用するAPIは、3段階 — 各クレデンシャルへのAPI割り当てで選択します。

5 カスタムヘッダー追加

顧客社APIで**Authentication/Authorization headers**を要求する場合は、カスタムヘッダーを追加してください。

> *例:* `Authorization` *トークン、APIキー*



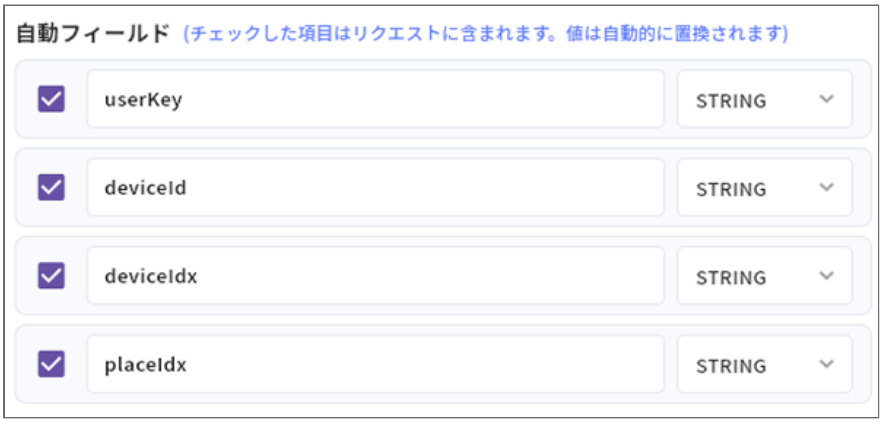
フィールド	説明
ヘッダー名	ヘッダー名（例: `Authorization`）を入力してください。 重複した名前は許可されません。
ヘッダー値	ヘッダー値を入力してください。

- カスタムヘッダーは最大**10件**まで追加できます。
- 顧客社APIが公開エンドポイントである場合や、別途ヘッダーが不要な場合は、このセクションを空のままにしてください。
- 行を挿入するには **追加** ボタンをクリックし、削除するには ✕ ボタンをクリックしてください。

> **固定ヘッダーは設定できません**
>
> `Content-Type` と `Accept` はカスタムヘッダーとして追加できません。 CLUeが内部的に `Content-Type: application/json` と `Accept: application/json` を固定値で送信するため、管理者が別途指定する必要はありません。 この名前でヘッダーを追加しようとしても保存されません。 顧客社APIは、この2つのヘッダーを前提に設計してください。

6 自動フィールド選択

自動フィールドは、システムがリクエスト本文に**自動で入力する値**です。 使用できる自動フィールドは、クレデンシャルタイプによって異なります。 各フィールドの値の位置は `{{...}}` **プレースホルダー**で表示され、リクエスト時に実際のデバイス/ユーザー値に置き換えられます。



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。

基本キー	プレースホルダー（値の位置）	使用可能対象	実際の値
deviceId	{{DEVICE_SERIAL}}	すべてのクレデンシャルタイプ	要求したデバイスのシリアル番号
userKey	{{USER_KEY}}	顔 / 指紋 / CLUe QR	CLUeが管理するユーザー識別子
rfCard	{{CARD_NUMBER}}	RFカード	提示したカード番号
uniquePin	{{UNIQUE_PIN}}	ユーザーPIN	入力したPIN値
qrCode	{{QR_CODE}}	カスタムQR	QRペイロード

フィールド選択ルール

- 各フィールド左側のチェックボックスで、**リクエストに含めるかどうかを決定**します。
- すべてを選択する必要はありません。 顧客社APIが判定に実際に必要とする値だけを選択してください。 不要なデータを減らすと、問題の診断が容易になります。
- キー（フィールド名）は編集できます。 顧客社APIが要求する名前（例: `userKey → employeeId`）に合わせて変更してください。 値の位置のプレースホルダーはシステムで固定されるため、変更できません。
- 各フィールドのデータ形式（例: `STRING`）は、フィールド右側に表示されます。

情報

- 5つ以外のプレースホルダーは追加できません。 顧客社APIが追加値を要求する場合は、手動フィールド追加を参照して固定値を追加するか、顧客社と相談してデバイスシリアル番号やユーザーキーから顧客社側で派生させるようにしてください。
- 自動フィールドと手動フィールドを合わせて、リクエスト本文に最大**10件**のフィールドを含められます。 自動フィールドを多く選択するほど、使用できる手動フィールド数は減ります。

7 手動フィールド追加

顧客社APIが固定値をリクエストに含めるよう要求する場合は、手動フィールドを追加してください。



フィールド	説明
フィールド名	フィールド名は一意である必要があり、自動フィールド名とも異なる必要があります。
フィールドタイプ	`STRING`、`NUMBER`、`BOOLEAN` から選択してください。
値	このフィールドの値を入力してください。 選択したタイプに応じて、適切なJSONデータ型に変換されます。 例: `NUMBER: 123`、`STRING: \"123\"`、`BOOLEAN: true/false`

- 自動フィールドと手動フィールドを合わせて、最大**10件**まで含められます。
- 追加された手動フィールドがない場合は、**手動フィールドが定義されていません。** メッセージが表示されます。
- 行を挿入するには **追加** ボタンをクリックし、削除するには  ボタンをクリックしてください。

8 APIテスト実行

基本情報、カスタムヘッダー、自動フィールド、手動フィールドを完了したら、判定基準（judgment criteria）を構成する前にテストを実行してください。 テストで得た実際の応答（response）は、判定基準の構成（応答パース設定）に必要です。

API パネル右側の **API テストコンソール** を使用してください。

9 テストパラメーター

テストコンソールに表示される入力フィールドは、クレデンシャルタイプによって異なります。 **端末 ID**（デバイスシリアル番号）はすべてのタイプで必須です。残りの入力値は、該当クレデンシャルタイプで使う値を顧客社が管理する形式のまま入力してください。

認証方式	入力する値	対応するプレースホルダー
すべてのタイプ	**端末 ID** — 9~12桁の数字、デバイスシリアル番号	`{{DEVICE_SERIAL}}`
顔 / 指紋 / CLUe QR	**ユーザー キー** — 1~64文字、CLUeが管理するユーザー識別子	`{{USER_KEY}}`
RFカード	顧客社が管理する**カード番号**	`{{CARD_NUMBER}}`
ユーザーPIN	顧客社が管理する**ユーザーPIN**	`{{UNIQUE_PIN}}`
カスタムQR	顧客社が管理する**QRペイロード**	`{{QR_CODE}}`

テストコンソールに入力した値は、自動フィールドのプレースホルダーを置き換え、実際のリクエスト本文として送信されます。 テストでは、顧客社データベースに実際に存在する値を入力し、許可と拒否の応答の両方を確認してください。 実運用環境では、デバイスが認識した値が自動で代入されます。

10 テスト実行

1. コンソール下部の **テスト実行** ボタンをクリックしてください。

2. テスト実行中は進行表示が出ます。
3. 結果を受け取ると、リクエスト/レスポンス内容が **ターミナル出力** コンソール領域に表示されます。

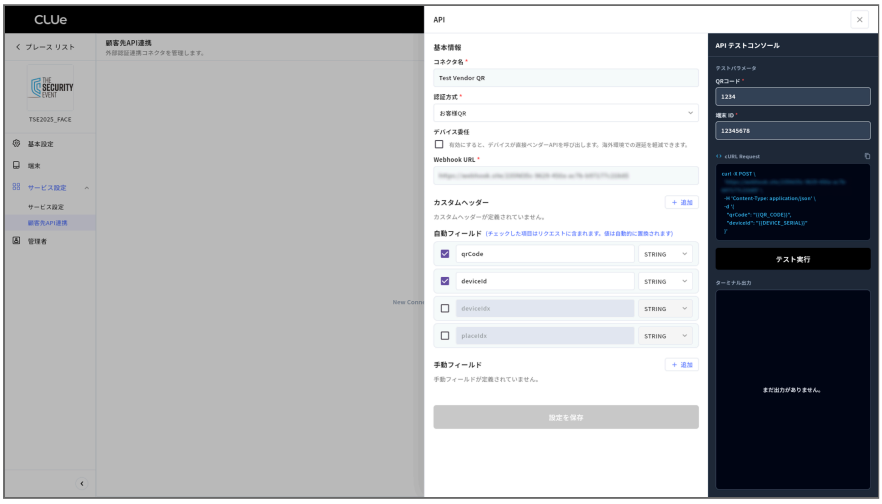
実行中にパネルを閉じるか、前のステップへ移動するとテストは中断されます。

応答を正常に受信したら、次のステップに進み、応答内容を基に判定基準（judgment criteria）を構成してください。 URL、ヘッダー、フィールド設定の問題で応答を受信できなかった場合は、該当入力値を確認してから再度テストしてください。

> **保存前の必須条件**
>
> **設定を保存** ボタンは、少なくとも1回テストに成功すると有効になります。 ここでの成功とは、顧客社サーバーから何らかのHTTP応答（4xx、5xxを含む）を受信したことを意味します。 ネットワークエラーで応答を受信できなかった場合は保存できません。

11 テスト失敗例 — 応答本文がJSONではない場合

顧客社サーバーが応答を返しても、本文がJSON形式でないか、応答ヘッダーの `Content-Type` が `application/json` でない場合は、テストコンソールにエラーと失敗ログが表示され、**設定を保存** ボタンは有効になりません。



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。

応答仕様を参照し、顧客担当者と一緒にAPIが次の2条件を両方満たすか確認してください。

- 応答ヘッダーに `Content-Type: application/json` が含まれているか
- 応答本文が有効なJSONか（HTMLエラーページ、プレーンテキスト、XMLなどではないか）

12 応答パース設定

受信した応答を基に、この段階でどの応答を入室許可（成功）として解釈するかを定義します。 設定した基準に一致する応答は入室許可として、それ以外はすべて入室拒否として処理します。

判定モードは、入力したフィールドに応じて自動で決まります。 **statusCode** と **成功結果 JSONPath** の少なくとも1つは必ず入力する必要があり、両方空のままでは保存できません。



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。

#	モード	入力	成功基準
1	応答コード検証	**statusCode** のみ	HTTPステータスコードが一覧の値のいずれかと一致すると成功します。
2	応答本文検証	**成功結果 JSONPath** のみ	HTTP応答コードに関係なく、本文の `Key = Value` 条件を満たすと成功します。 条件を満たせば、4xx/5xx応答でも許可されます。
3	結合検証	両方	ステータスコードが一致し、同時に本文条件も満たすと成功します。 ステータスコードが一致しない場合は、本文を評価しません。

statusCode（モード1、3で使用）

- 100〜399の範囲の整数のみ指定できます。 `4xx`、`5xx` コードは成功として指定できません。
- 最大3件まで指定でき、重複値は許可されません。
- 複数値を指定した場合は、いずれか1つでも一致すれば成功（例: `200`、`201`）として処理します。

成功結果 JSONPath（モード2、3で使用）

- 成功応答を識別する `Key`、`Value`、データ形式（`BOOLEAN`、`STRING`、`NUMBER`）を入力します。
- 成功キー条件は1件だけ設定できます。
- この条件に一致しない応答は入室拒否として処理されます。

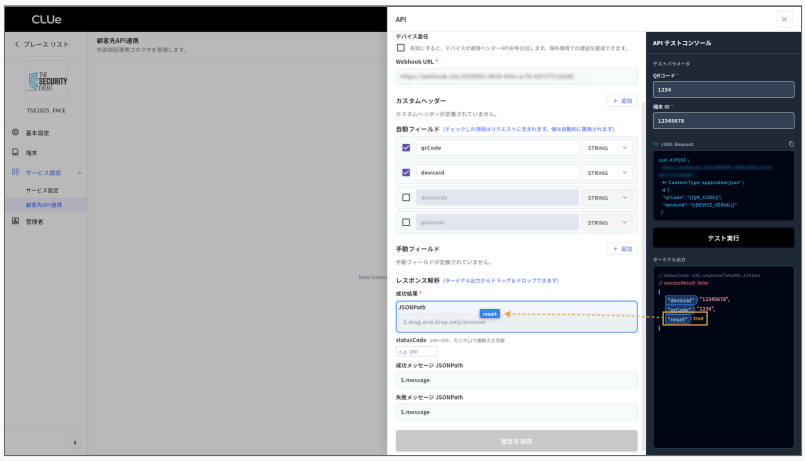
成功メッセージ JSONPath / 失敗メッセージ JSONPath（オプション）

- 認証成功/失敗時に、それぞれデバイス画面に表示する文字列を抽出するキーを指定します。 通常は `$.message` を使用します。
- 指定しなくても保存できます。 空のままにすると、許可/拒否のみ判定し、デバイス画面にメッセージは表示されません。
- 成功と失敗で異なるキーを指定できます。
- 指定したキーの値は必ず文字列である必要があり、デバイス画面サイズを考慮して長すぎないようにしてください。

ヒント

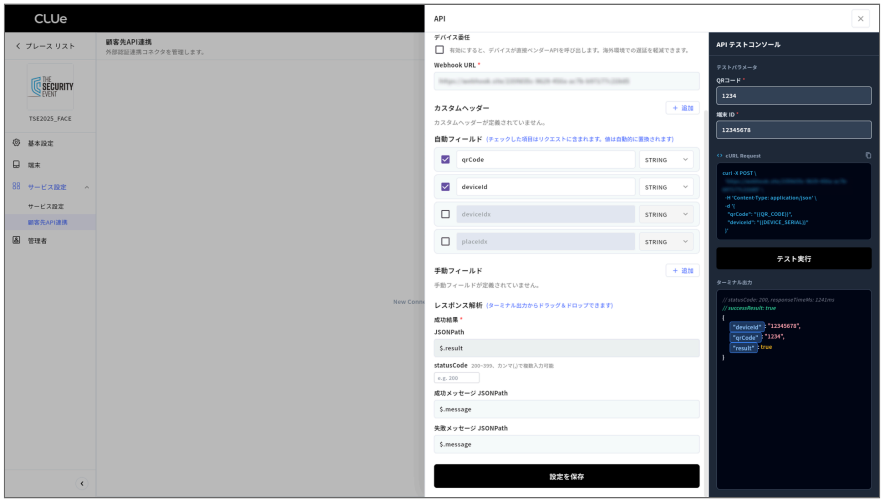
JSONPathを直接入力しづらい場合

応答領域からフィールドを **成功結果 JSONPath**、**成功メッセージ JSONPath**、**失敗メッセージ JSONPath** の入力欄へドラッグ＆ドロップすると、JSONパスが自動で入力されます。 JSONPathを直接書く必要はありません。



13 保存

API パネル下部の **設定を保存** ボタンは、すべての必須項目と判定基準が正しく入力され、APIテストが少なくとも1回成功したときに有効になります。



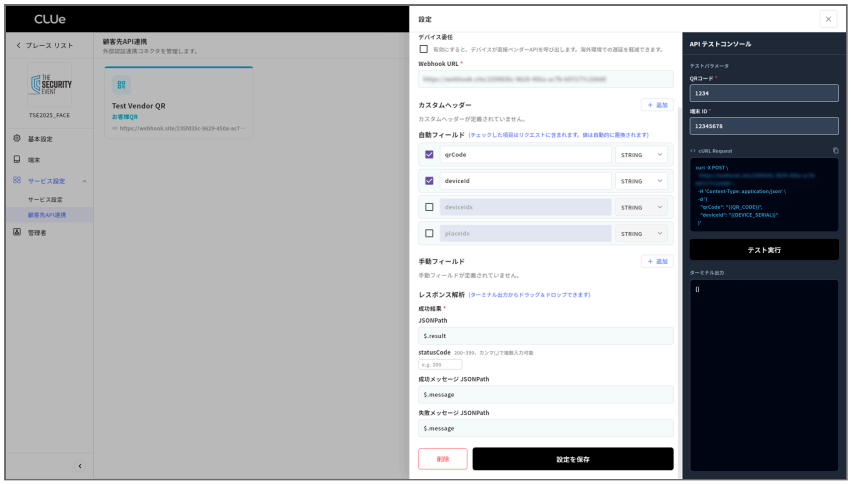
- 必須フィールドの不足、URL形式エラー、指定タイプに変換できない手動フィールド値、判定基準の未入力、テスト未成功（ネットワークエラー含む）のいずれかがある場合、**設定を保存** ボタンは無効のままです。
- 登録を完了するには、**設定を保存** ボタンをクリックしてください。

APIを保存するとパネルが閉じ、新しく登録したAPIが一覧にカードとして表示されます。 カードには、名前、クレデンシャルタイプ、登録済みURLなどの情報が表示されます。



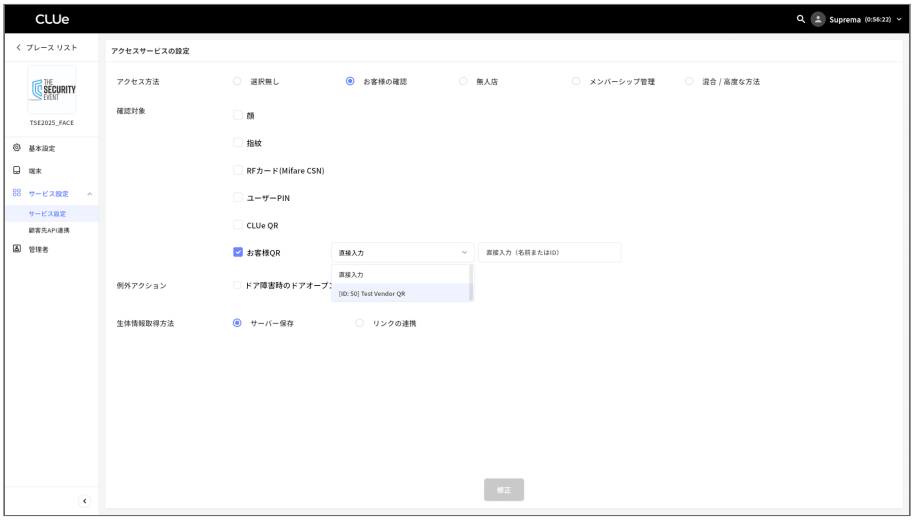
- APIを編集するには、カードをクリックしてください。 編集パネルが開きます。 **コネクタ名**、**Webhook URL**、**自動フィールド**、**手動フィールド**、**レスポンス解析** を編集できます。 **認証方式** は編集できません。

- **削除**: 登録したAPIを削除します。 このAPIがクレデンシャルに連携されていた場合、その連携も自動で解除され、変更はすぐにデバイスへ適用されます。 連携解除されたクレデンシャルは、その後は顧客社検証なしでデバイス本体認証のみで動作します。 運用の空白が心配な場合は、削除前に代替APIを先に登録して連携してください。



3段階 — 各クレデンシャルへのAPI割り当て

画面左側のサイドバーで **サービス設定** → **サービス設定** をクリックしてください。 **確認対象** セクションで、各クレデンシャルに使用するAPIを指定してください。



- 各クレデンシャル横のドロップダウンをクリックすると、登録済みAPIの一覧が表示されます。 選択したクレデンシャルと**認証方式**が一致するAPIのみ表示されます。

- 顔、指紋、RFカード、PIN、CLUe QR、カスタムQRの各クレデンシャルに使用するAPIを選択してください。 クレデンシャルごとに異なるAPIを指定できます。

- APIを指定していないクレデンシャルは、デバイス本体認証のみで動作します。 そのクレデンシャルには顧客社APIへの検証リクエストは送信されません。 顧客社検証が不要と判断したクレデンシャルだけを、未指定のままにしてください。

保存と適用ルール

クレデンシャルに登録したAPIを指定して **修正** ボタンをクリックすると、変更を下位プレースに適用するかどうかの確認ダイアログが表示されます。



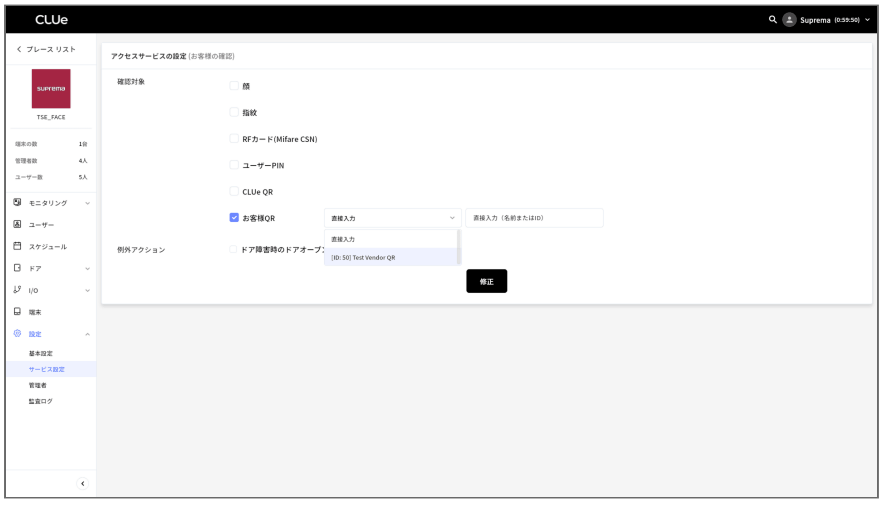
- **確認**: 同じ設定が現在のプレース グループのすべての下位プレースに即時適用されます。 既存のプレース別上書きは、プレース グループ値で上書きされます。
- **キャンセル**: 変更を保存しません。

ほとんどの場合、プレース グループレベルの設定だけで、すべての下位プレースを同じように運用できます。 特定のプレースに別のAPIを上書きする方法は、4段階 — プレース別上書き設定（オプション）を参照してください。

4段階 — プレース別上書き設定（オプション）

プレース グループから継承した設定とは別に、特定のプレースにだけ別のAPIを指定する方法を案内します。 特定のプレースにのみ適用した設定は、他のプレースや上位のプレース グループに影響しません。

1. プレース グループ配下の特定のプレースへ移動してください。
2. 画面左側のサイドバーで **設定** → **サービス設定** をクリックしてください。



3. **確認対象** セクションの各クレデンシャルのドロップダウンで、**このプレースでのみ使用する別のAPI**を選択してください。

4. 変更を保存するには、**修正** ボタンをクリックしてください。

変更は現在のプレースにのみ保存されます。 他のプレースには適用されません。

> **情報**
> そのプレースに管理者として招待されたプレース管理者だけが、**設定** → **サービス設定** にアクセスできます。

> **注意**
> 特定のプレースにAPIを指定した後、上位のプレース グループでクレデンシャル-API指定を変更して保存すると、プレース別上書きはプレース グループ値で上書きされます。 プレース グループ変更後もプレース別設定を維持する必要がある場合は、プレース グループ更新後に特定のプレースの **設定** → **サービス設定** で再指定してください。

入力ルール要約

フィールド	必須かどうか	ルール
コネクタ名	必須	最大64文字
認証方式	必須	保存後は変更不可
Webhook URL	必須	`https://` 必須 / 最大512文字 / CLUeはこのURLに**HTTP POST**/ `application/json` リクエストのみ送信
認証方式 API数	-	クレデンシャルタイプごとに最大**3件**のAPI登録が可能
カスタムヘッダー	任意	Key/Valueペアは最大10件 / 重複名不可（大文字小文字を区別しない）
自動フィールド	任意	チェックした項目のみリクエストに含める / キー（名前）は編集可能 / 値はシステムが自動入力
手動フィールド	任意	自動フィールドと合わせて最大**10件**登録 / 重複名不可 / 値は指定したタイプ（`STRING` / `NUMBER` / `BOOLEAN`）に応じてJSONデータに変換される
ユーザー キー(テスト)	**認証方式**によって異なる	1〜64文字
端末 ID(テスト)	必須	9〜12桁の数字のみ
レスポンス解析	-	**statusCode** または **成功結果 JSONPath** の少なくとも1つが必須（両方入力すると結合検証が有効化）
statusCode	-	100〜399の範囲の整数 / 最大3件 / 重複不可
成功結果 JSONPath	-	1件: `Key` + `Value` + データ形式（`BOOLEAN` / `STRING` / `NUMBER`）

フィールド	必須かどうか	ルール
成功メッセージ JSONPath/**失敗メッセージ JSONPath**	任意	指定すると応答本文から抽出するキー（値は文字列である必要があり、デバイス画面サイズを考慮する必要あり）、指定しないとデバイスにメッセージは表示されない
保存条件	-	テスト成功時のみ保存可能

トラブルシューティング

入室問題（段階別診断）

設定ワークフローの概要を参照して、問題箇所を絞り込んでください。

手順	症状	確認事項
1	特定のクレデンシャルが認識されない	クレデンシャルがデバイスに登録され、有効になっているか確認してください。
2	デバイス-サーバー間の通信失敗	ネットワーク接続状態、デバイス登録状態を確認してください。
3	リクエストが顧客社サーバーに到達しない	登録済みURL（HTTPS）、カスタムヘッダー、ファイアウォールルールを確認してください。
4	顧客社は応答するが、すべての試行が拒否される	判定基準（判定モード、成功キー/値、HTTPステータスコード）を確認してください。
5	許可/拒否は正しく動作するが、メッセージが表示されない	**成功メッセージ JSONPath**/**失敗メッセージ JSONPath**、応答本文のメッセージ文字列を確認してください。

設定を保存 ボタン無効

設定を保存 ボタンをクリックできない場合は、次の項目を順番に確認してください。

- **必須フィールド**: **コネクタ名**、**認証方式**、**Webhook URL** のうち空の項目がないか確認してください。
- **Webhook URL**: `https://` で始まり、最大長（512文字）を超えていないか確認してください。
- **手動フィールド**: 値を指定したタイプ（`STRING` / `NUMBER` / `BOOLEAN`）に変換できるか確認してください

  > *例: `NUMBER` に数字以外の文字を入力した場合*

- **レスポンス解析**: **statusCode** または **成功結果 JSONPath** の少なくとも1つを入力したか確認してください。
  - **成功結果 JSONPath**を使用する場合は、`Key`、`Value`、データ形式をすべて入力したか確認してください。
  - **成功メッセージ JSONPath**/**失敗メッセージ JSONPath**はオプションで、保存に影響しません。
- **APIテスト**: 少なくとも1回テストに成功したか確認してください。 テスト成功なしでは保存できません。

テスト失敗

テスト失敗は3種類に分かれます。

- （A）入力値検証段階でブロックされた
- （B）リクエストは送信されたがテスト失敗
- （C）応答は受信したが期待した結果ではない

（A）入力値検証段階でブロックされた

入力値がルールに合わず、リクエスト自体が送信されません。

症状	確認事項
Webhook URL形式エラー	**Webhook URL** が `https://` で始まり、512文字を超えないか確認してください。
判定基準キー形式エラー	**成功結果 JSONPath**/**成功メッセージ JSONPath**/**失敗メッセージ JSONPath** が `$.` で始まるJSONPath形式（最大128文字）か確認してください。
判定基準未指定	**statusCode** または **成功結果 JSONPath** の少なくとも1つを入力したか確認してください。
成功ステータスコード範囲/件数エラー	各値が100〜399の範囲内か、3件以下か、重複がないか確認してください。
フィールドキー重複	**自動フィールド** と **手動フィールド** のキーが互いに重複なく一意か確認してください。
リクエストヘッダーキー重複	リクエストヘッダーキーが互いに重複なく一意か（大文字小文字を区別しない）確認してください。
制限されたヘッダー名を使用	`Content-Type` または `Accept` をカスタムヘッダーとして追加していないか（大文字小文字を区別しないシステム固定値）確認してください。
フィールド/ヘッダー数超過	**自動フィールド** と **手動フィールド** のフィールドが最大10件、カスタムヘッダーが最大10件か確認してください。
認証方式 登録件数超過	該当クレデンシャルタイプにすでに3件のAPIが登録されているか確認してください。
ユーザー キー 形式エラー	テストコンソールの **ユーザー キー** が、許可文字（英字、数字、`-`、`_`、`@`、`.`）の範囲と1〜64文字の長さを満たすか確認してください。
端末 ID 形式エラー	テストコンソールの **端末 ID** が9〜12桁の数字か確認してください。

（B）リクエストは送信されたがテスト失敗

テスト結果が `success = false` と表示され、この状態では保存できません。

症状	確認事項
接続失敗/ネットワークエラー（顧客社サーバーから応答を受信できない）	顧客社サーバーの外部アクセス可否、HTTPS証明書の有効性、ファイアウォール/ポート設定、カスタムヘッダー（期限切れトークン、 ◇◇◇ポ）
タイムアウト（応答なし）	顧客社サーバーの応答遅延、ネットワーク状態。 テストは数秒以内に応答がないと失敗として処理します
応答は受信したが、本文がJSONではない	顧客社がJSON応答を返すか、応答 `Content-Type` が `application/json` に設定されているか。 HTMLエラーページ、空テキストなどが該当します

（C）応答は受信したが期待した結果ではない

`success = true` とともに、実際のHTTPステータスコードが **statusCode** に、顧客社の元応答が **ターミナル出力** に表示されます。保存可能であり、この段階で応答を基に応答パースを構成する必要があります。

症状	確認事項
ステータスコードは受信したが、すべての入室が拒否される	**モード1、3:** 成功として認めるステータスコード一覧を確認してください。 **モード2:** 本文のキー/値条件を確認してください。 ステータスコードは無視されます。
本文フィールド条件が一致しない	**成功結果 JSONPath** に入力した `Key` 、 `Value` 、データ形式（ `BOOLEAN` / `STRING` / `NUMBER` ）を再確認してください。 応答が `"true"` （STRING）か `true` （BOOLEAN）かを確認してください。タイプが一致している必要があります。
手動フィールド がリクエスト本文で不正な形式として表示される	**手動フィールド** のタイプ（ `STRING` / `NUMBER` / `BOOLEAN` ）が実際の入力値と一致しているか再確認してください。

> **情報**
>
> - テストAPIは応答本文をパースせずそのまま表示するため、**ターミナル出力** に表示された実際の応答JSONを基に、JSONPath、キー、値の設定を合わせてください。
> - デバイス側で失敗原因を特定するには、入室問題（段階別診断）を参照してください。

名前重複の問題

自動フィールド と **手動フィールド** のキー名は互いに重複できません。 リクエストヘッダーキーも互いに重複できません。 **自動フィールド** のキー名を変更した場合は、**手動フィールド** と衝突しないか確認してください。

デバイスにメッセージが表示されない

- 応答本文に **成功メッセージ JSONPath** または **失敗メッセージ JSONPath** で指定したフィールドが実際に存在するか確認してください。
- そのキーの値が**文字列**か確認してください。 数値、オブジェクト、配列は表示されません。
- 設定した **成功メッセージ JSONPath** / **失敗メッセージ JSONPath** 名が、実際の応答のキーと正確に一致するか確認してくだ

さい。

ファームウェアを変更する

CLUeでサポートするデバイスは次のとおりです。 ファームウェアを1回更新するだけで、既存のBioStar対応モードからCLUe対応モードに切り替えられます。

- BioStation 3, BioEntry W3, BioEntry W2, BioLite N2, X-Station 2, XPass 2

> **注意**
> ファームウェアを更新する前に、**デバイスにユーザー情報が残っていないことを確認してください。** ユーザーデータが残っていると、CLUeシステムで同期されるユーザー情報と競合が発生する場合があります。

CLUe対応モードに切り替え

> **情報**
> ファームウェア更新前にデバイスを事前登録する場合は、デバイスのシリアル番号（SN）とモデル名（例: BS3-DB）をSuprema グローバル技術サポートチームに提供してください。 事前登録手続きを進めます。

1 CLUe対応ファームウェアバージョンの準備

Supremaの現地支社またはCLUeチームから入手できます。 デバイスに適用できるバージョンは以下のとおりです。

- *xpass2_v1_x_CL-AU.bin*
- *bs3-all_v1.x._CL-AU.bin*
- *xs2-all_v1.x CL-AU.zip*
- *bln2-oab_v1.x CL-AU.bin*
- *bln2-odb_v1.x CL-AU.bin*
- *bln2-pab_v1.x CL-AU.bin*
- *bew3-all_v1.x CL-AU.bin*
- *bew2_oa/d/hp_v1.x CL-AU.bin*

> **情報**
> 接尾辞 AU は「Auto Update to CLUe FW」を意味します。

2 インターネット接続の確認

ファームウェアを更新する前に、デバイスがインターネットとCLUeサーバーに接続できることを確認してください。

CLUeファームウェアの更新後、デバイスはCLUeサーバーから証明書を自動で取得して適用し、その後 接続を試行するため、インターネット接続が必須です。 また、デバイスは標準でDHCPによりIPアドレスを割り当てられるため、動的IPアドレスを割り当てられるか確認してください。

- 基本ネットワーク設定はDHCPです。
- 8.8.8.8 DNSサーバーを使用します。

3 ファームウェア更新の実施

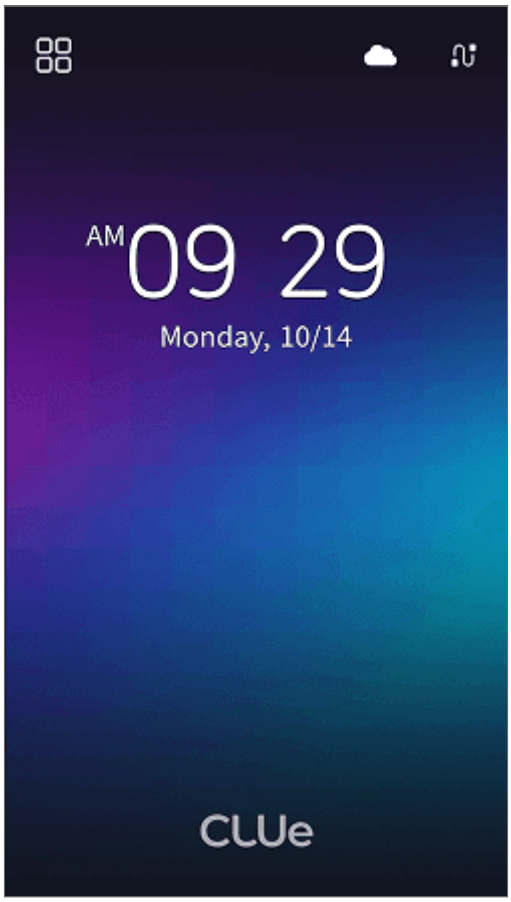
更新の過程で、デバイスは少なくとも2〜3回再起動します。

メインファームウェアの更新には多少時間がかかる場合がありますが、証明書と設定ファームウェアの取得は比較的短時間で完了します。 全体の過程は約3\〜5分かかるため、更新が完了するまでデバイスの電源とインターネット接続を維持してください。

> **情報**
> BioStar 2またはUSBを利用してファームウェアを更新することもできます。

4 更新完了の確認

すべての更新が完了すると、デバイスのメイン画面にCLUeアイコンが表示されます。



ディスプレイのないデバイスは、CLUeポータルでシリアル番号を入力してデバイス登録状態を確認できます。

5 デバイス登録

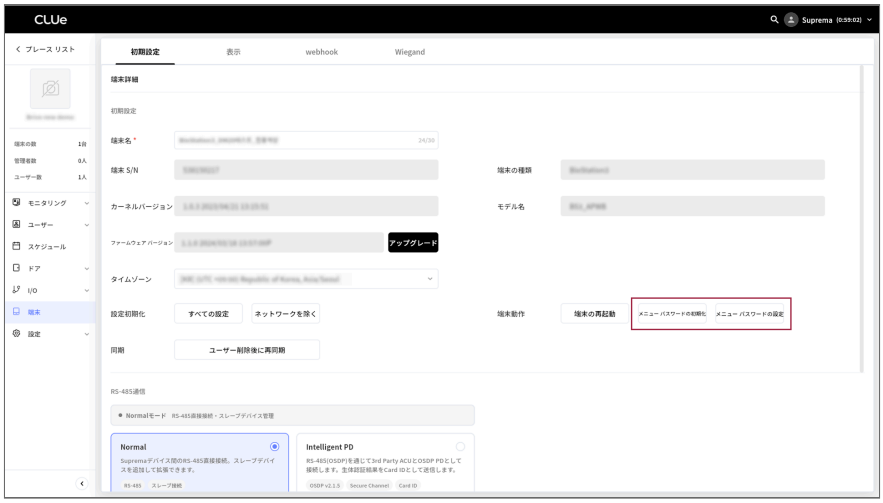
Suprema担当者に、ポータルを通じてデバイスをアカウントに割り当てるよう依頼してください。

その後、指定したプレースにデバイスを割り当て、ドア設定と一緒に使用できます。 安全なデバイス管理のため、CLUeシステムでは各ブランチの管理者がデバイスを該当するプレース グループに割り当てる必要があります。

6 デバイスメニューのパスワード設定

ファームウェア更新後、LCDディスプレイ付きデバイスにはメニューパスワードの設定を求めるメッセージが表示されます。 画面の案内に従ってパスワードを設定してください。 パスワードはCLUeポータルからも設定できます。

BioStarデバイスとは異なり、CLUeデバイスはユーザーデータなしで使用されることが多くあります。 そのため、メニュー設定が不正に変更されないよう、メニューパスワードを設定する必要があります。



トラブルシューティング

デバイス画面にクラウドアイコンが表示されない場合は、次の項目を確認してください。

- まず、インターネット接続状態を確認してください。 デバイスはクラウドサーバーに直接接続するため、必ずインターネットに接続されている必要があります。 また、CLUeファームウェアはアウトバウンド通信に標準HTTPSポート443を使用します。
- クラウドアイコンがまだ表示されない場合は、デバイスで**Pingテスト**を実行してインターネット接続状態を確認してください。

デバイス	パス
BioStation 3	メニュー( ) → **SETTINGS** → **NETWORK** → **Ethernet** → **Ping Test**
BioLite N2	**ESC** → **NETWORK** → **TCP/IP** → **Ping Test**
X-Station 2	メニュー( ) → **NETWORK** → **Ethernet** → **Ping Test**

  - **Pingテスト成功**ポップアップが表示されれば、インターネット接続に問題はありません。

- **不明(Unknown)**または**失敗(Fail)**ポップアップが表示される場合は、ネットワークでそのDNSの使用をブロックしていないか確認してください。

デバイスを追加する

CLUeデバイスを使用するには、Webポータルで**登録**と**割り当て**を完了する必要があります。 デバイス登録はブランチ管理者のみが実行できます。登録が完了したデバイスは、代理店管理者またはプレース グループ管理者が担当プレースに割り当てます。

新規デバイスを購入したお客様は、CLUeファームウェアと証明書が適用されているか確認した後、Supremaの支店にデバイス登録を依頼してください。

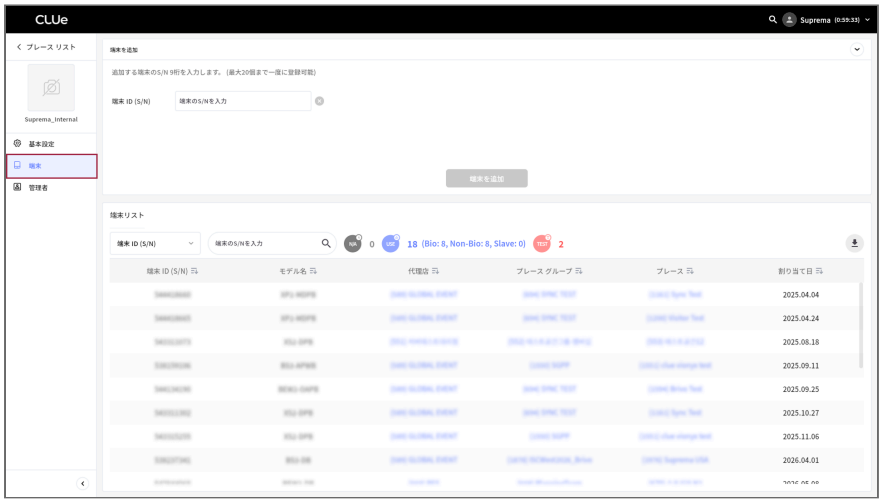
デバイス登録（ブランチ管理者）

ブランチ管理者のみがデバイスを登録できます。 デバイスを登録する前に、デバイスのシリアル番号を確認してください。 シリアル番号は、デバイス背面に貼付されたステッカーで確認できます。

1. CLUe Webポータルにログインしてください。
2. 初期画面で、デバイスを登録するブランチを選択してください。
3. 画面右上の ⋮ → **詳細設定**をクリックしてください。



4. 画面左側のサイドバーで **端末**をクリックしてください。



5. **端末を追加** セクションの **端末 ID (S/N)** 入力フィールドにデバイスのシリアル番号を入力し、**追加** ボタンをクリックしてください。



6. **端末リスト**に追加したデバイスが表示されます。



7. 編集モードを有効にするには、**選択無し** フィールドをクリックし、 ボタンを選択してください。



8. デバイスを割り当てる 代理店、プレース グループ、プレースを選択してください。



9. 選択した項目を適用するには、 ボタンをクリックしてください。

デバイス割り当ての成功メッセージが画面上部に表示されます。 各フィールドをクリックすると、該当する 代理店、プレース グループ、プレースへ移動できる ボタンが有効になります。 ボタンをクリックすると、該当の場所へ移動した後、デバイスとドアを設定できます。



デバイス割り当て

代理店管理者

代理店管理者は、自分に割り当てられたデバイスを下位のプレース グループまたは個別のプレースに割り当てられます。 登録が必要なデバイスが一覧に表示されない場合は、該当のSuprema支店または本社に問い合わせてください。

1. CLUe Webポータルにログインしてください。
2. 初期画面で、デバイスを割り当てる代理店を選択してください。
3. 画面右上の ⋮ → **詳細設定**をクリックしてください。



4. 画面左側のサイドバーで **端末**をクリックしてください。



5. 編集モードを有効にするには、**選択無し** フィールドをクリックし、✎ ボタンを選択してください。



6. デバイスを割り当てる プレース グループ または プレースを選択してください。



7. 選択した項目を適用するには、✓ ボタンをクリックしてください。

デバイス割り当ての成功メッセージが画面上部に表示されます。 各フィールドをクリックすると、該当する プレース グループ、プレースへ移動できる ↖ ボタンが有効になります。 割り当て後は、プレースへ移動してドアを追加することを推奨します。



情報

- 代理店管理者は、プライバシーポリシーにより、既定ではユーザータブとモニタリングタブを表示できません。 アクセスが必要な場合は、プレース グループ、プレース管理者に招待を依頼してください。
- デバイスを削除すると、自動的にブランチレベルのデバイス一覧に戻り、未割り当て状態になります。 誤ってデバイスを削除した場合は、ブランチ管理者に再割り当てを依頼してください。

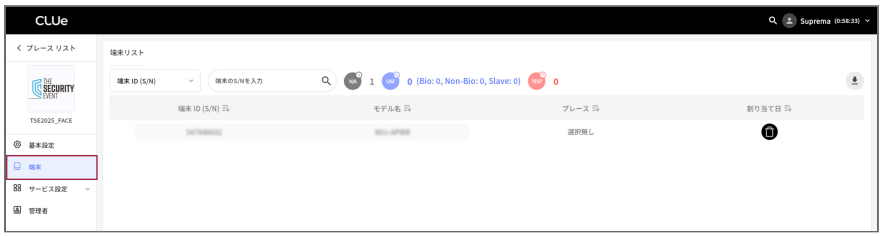
プレース グループ管理者

プレース グループ管理者は、自分に割り当てられたデバイスを下位のプレースに割り当てられます。

1. CLUe Webポータルにログインしてください。
2. 初期画面で、デバイスを割り当てるプレース グループを選択してください。
3. 画面右上の ⋮ → **詳細設定**をクリックしてください。



4. 画面左側のサイドバーで **端末**をクリックしてください。



5. 編集モードを有効にするには、**選択無し** フィールドをクリックし、ボタンを選択してください。



6. デバイスを割り当てる プレースを選択してください。



7. 選択した項目を適用するには、ボタンをクリックしてください。

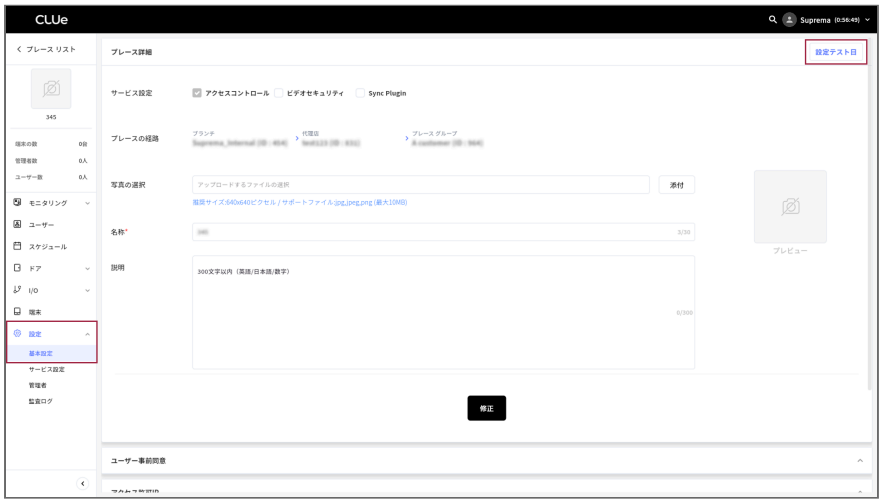
デバイス割り当ての成功メッセージが画面上部に表示されます。 デバイス割り当て後は、該当の プレースへ移動してドアを追加することを推奨します。



テストプレースの設定（ブランチ管理者）

サブスクリプションはデバイス数を基準にするため、テストデバイスを区別して合計から除外する必要があります。 そのため、ブランチ管理者権限のユーザーは、プレース設定で特定のプレースを「テストプレース」に指定できます。

1. CLUe Webポータルにログインしてください。
2. テストプレースとして指定するプレースを選択してください。
3. 画面左側のサイドバーで **設定** → **基本設定**をクリックしてください。



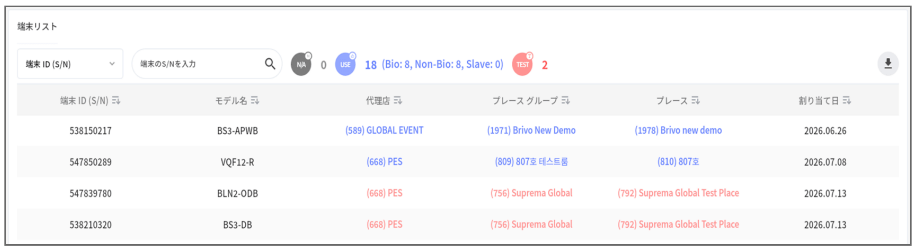
4. 画面右上の **設定テスト日**をクリックしてください。
5. **テスト期間** ポップアップが表示されたら、テスト期間を設定してください。



期間制限なく使用するには、終了日を**9999.12.31 23:59**に設定してください。

6. 設定を完了するには、**確認** ボタンをクリックしてください。

プレースに属するすべてのデバイスが、デバイス一覧で赤色で表示され、テストデバイスとして区別されます。 合計数量情報もあわせて確認できます。



次のステップ

デバイスのファームウェアアップグレード方法を確認してください。

デバイスのセルフ登録

設置担当者が CLUe ポータルにログインできない現場でも、管理者が事前に用意した情報だけでデバイスをプレースに登録できます。 この feature は Device Self-Registration と呼ばれ、管理者が事前に準備する**管理者準備段階**と、設置担当者が現場で実行する**現場登録段階**に分かれます。

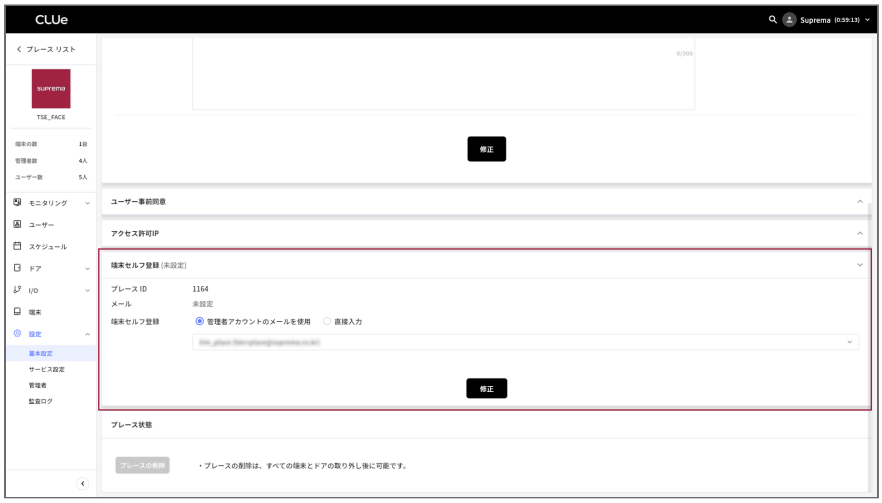
対応デバイスおよびファームウェアバージョン

デバイスモデル	対応ファームウェアバージョン
X-Station 2	2026.06.01 以降
BioStation 3	2026.05.26 以降
BioLite N2	2026.06.01 以降
XPass 2	2026.06.01 以降
BioEntry W3	非対応
BioEntry W2	非対応

管理者準備段階

現場登録を開始する前に、プレース管理者は CLUe ポータルでプレース ID を確認し、デバイス割り当てメールアドレスを設定する必要があります。 設定しないと、現場で割り当てコードを受け取れません。 プレース管理者以上の権限で招待された管理者だけがアクセスできます。

1. CLUe Webポータルにログインしてください。
2. デバイスを割り当てるプレースに移動します。
3. 画面左側のサイドバーで **設定** → **基本設定**をクリックしてください。
4. **端末セルフ登録** セクションをクリックしてください。



プレース ID(読み取り専用)フィールドと**端末セルフ登録**メールアドレス入力欄があります。

プレース ID の確認

プレース IDは読み取り専用です。 この番号を現場の設置担当者に伝えます。 設置担当者は、デバイスにプレース ID をそのまま入力して登録を進められます。 プレース ID の入力ミスは登録失敗の最も一般的な原因です。正確に伝えてください。



デバイス割り当てメールアドレスの設定

デバイス割り当てメールアドレスは、次の 2 つの方法のどちらかで設定します。



- **管理者アカウントのメールを使用**: 現在ログインしている管理者アカウントのメールアドレスが自動入力されます。
- **直接入力**: 任意のメールアドレスを直接入力します。 一般的なメールアドレス形式で入力できます（最大 254 文字）。

どちらの方法でも、入力したメールアドレスはサーバーにそのまま保存されます。 システムは、受信者が管理者、現場の設置担当者、または第三者かを区別しません。 プレースごとに設定できる割り当てメールは 1 つだけです。 新しいプレースを作成すると、割り当てメールは未設定の状態で始まります。セルフ登録 feature を使うには、まずメールを設定してください。

> **メールを設定しないとどうなりますか?**
>
> 割り当てメールが設定されていないプレースで設置担当者が**割り当てコード送信**を実行すると、「管理者が先に割り当てメールアドレスを設定する必要があります。」というエラーが表示されます。

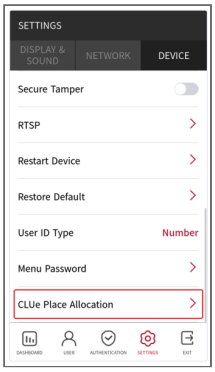
現場登録段階

LCD があるデバイス（LCD デバイスのセルフ登録）と LCD がないデバイス（LCD がないデバイスのセルフ登録（Web サーバー））の登録手順は同じ原理で動作し、画面だけが異なります。 まず、共通して適用される概念を説明します。

手順	動作	結果
割り当てコード送信	プレース ID を入力した後、**割り当てコード送信**を実行してください。	サーバーが 6 桁の割り当てコードを生成し、プレースの割り当てメールに送信します。
割り当てコード入力	指定された時間内に、メールで受け取ったコードを入力してください。	コードが一致すると、デバイスがそのプレースに登録されます。

LCD デバイスのセルフ登録

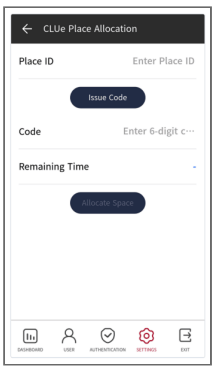
下の画面は例です。実際の画面構成とボタン名は、デバイスモデルとファームウェアバージョンによって異なる場合があります。画面に表示される案内文に従って進めてください。



1 プレース登録へ移動

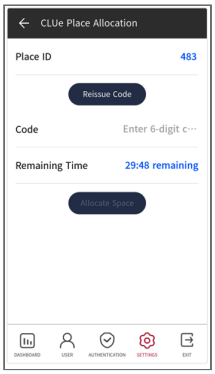
デバイス設定メニューで **DEVICE → CLUe Place Allocation** を選択してください。 プレース登録画面に移動します。

> **情報**
>
> - メニュー名と位置は、デバイスモデルと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。
> - デバイスがすでに特定のプレース（またはプレース グループ、代理店、ブランチ）に属している場合、登録画面には入れず、すでに登録済みというメッセージが表示されます。



2 プレース ID の入力

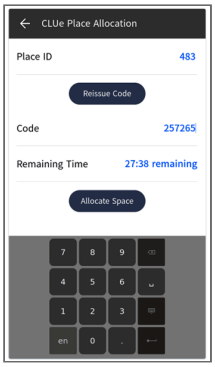
管理者から受け取ったプレース ID を数字キーパッドで入力してください。 存在しない ID、またはプレースではないブランチ、代理店、プレース グループ ID を入力すると、エラーメッセージが表示されます。 プレース ID を再確認してから入力してください。



3 割り当てコード送信

プレース ID を入力して **Issue Code** を実行してください。 サーバーが 6 桁の割り当てコードを生成し、該当プレースの割り当てメールに送信します。 デバイスは割り当てコード入力画面に切り替わります。

> **情報**
> 割り当てメールが設定されていない場合、エラーメッセージが表示されます。 その場合は、管理者に割り当てメールの設定を依頼してください。



4 割り当てコード入力

割り当てメールで受け取った 6 桁のコードを 30 分以内に入力してください。 コードの有効期限が切れているか、一致しない場合は、エラーメッセージが表示されます。

> **情報**
>
> - コードを再入力するか、新しいコードを要求するには、**Reissue Code** ボタンをタップしてください。
> - コードを 5 回連続で誤って入力すると、発行済みのコードは破棄されます。 前の段階に戻って、新しいコードを要求してください。

5 登録完了

Allocate Space ボタンをタップしてください。 コードが一致すると、デバイスがそのプレースに登録され、完了メッセージが表示されます。 その後、デバイスは通常の入退室動作画面に切り替わります。

登録済みのデバイスは、現場でプレースを変更できません。 変更が必要な場合は、CLUe ポータルで実行してください。

LCD がないデバイスのセルフ登録（Web サーバー）

LCD がないデバイスは、本体からプレースを登録できません。 デバイスと同じネットワークに接続した PC またはモバイル機器の Web ブラウザーから、デバイスの Web サーバーにアクセスして登録を進める必要があります。

デバイス Web サーバーへのアクセス

対象デバイスと同じネットワークに接続した機器の Web ブラウザーのアドレスバーに、次のアドレスを入力してアクセスしてください。

> *https://* `{device_IP_address}` *:* `{port}` *— 例: https://192.168.0.27:8443*

- デバイスの IP アドレスとポートの確認方法は、機器ごとのインストールガイドを参照してください。
- 自己署名証明書を使用すると、ブラウザーに「安全ではありません (Not Secure)」というセキュリティ警告が表示される場合があります。 続行すると、登録画面が開きます。

デバイスがまだどのプレースにも登録されていない場合、プレース登録画面（CLUe Device Web Panel）が表示されます。 デバイスが特定のプレースに属している場合、すでに登録済みというメッセージが表示され、登録画面にはアクセスできません。

Web で登録

次の案内に従って、デバイスのセルフ登録を進めてください。



1 プレース ID の入力

管理者から受け取ったプレース ID を **Place ID** 入力フィールドに入力してください。 存在しない ID、または最下位プレースではない ID を入力すると、エラーメッセージが表示されます。 プレース ID を再確認してから入力してください。

2 割り当てコード送信

プレース ID を入力して **Issue Code** ボタンをクリックしてください。 サーバーが 6 桁の割り当てコードを生成し、該当プレースの割り当てメールに送信します。

> **情報**
> 割り当てメールが設定されていない場合、エラーメッセージが表示されます。 その場合は、管理者に割り当てメールの設定を依頼してください。

3 割り当てコード入力

割り当てメールで受け取った 6 桁のコードを 30 分以内に入力してください。 コードの有効期限が切れているか、一致しない場合は、エラーメッセージが表示されます。

> **情報**
> - 現在の登録状態を確認するには、**Check Status** ボタンをクリックしてください。
> - コードを再取得するには、**Reissue Code** ボタンをクリックしてください。 ただし、同じデバイスは前回のコード送信から 60 秒経過しないと再送できません。
> - コードを 5 回連続で誤って入力すると、発行済みのコードは破棄されます。 前の段階に戻って、新しいコードを要求してください。

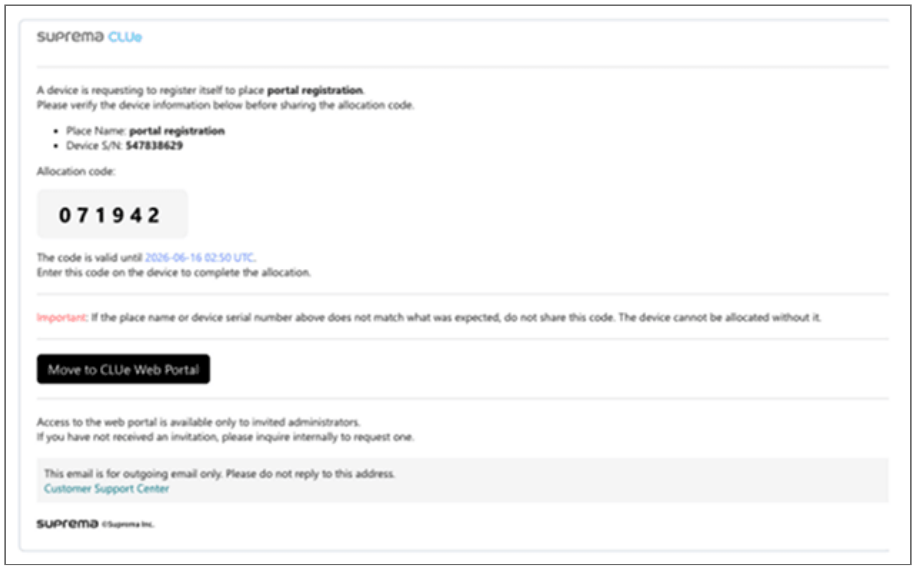
4 登録完了

Allocate Space ボタンをクリックしてください。 コードが一致すると、デバイスがそのプレースに登録され、完了メッセージが表示されます。 登録が完了すると、Web サーバーは約 3 分だけ動作した後、自動で終了します。 その後、同じアドレスにアクセスしても接続できません。 これは、不要なリソース消費を防ぎ、セキュリティを強化するための正常な動作です。 登録後にプレースを変更する場合は、CLUe ポータルで実行してください。

参考

割り当てコードメールの確認

割り当てコード送信（**Issue Code**）を実行すると、プレースに設定された割り当てメールアドレスに割り当てコードメールを送信します。 割り当てコードを入力する前に、受信者はメール本文で登録対象が正しいか確認する必要があります。



メールの件名には、デバイスのシリアル番号（deviceSn）が含まれています。 受信トレイ一覧では、件名だけでどのデバイスのコードか確認できます。 複数のデバイスを同時に設置する場合は、件名のシリアル番号で該当デバイスのメールを区別してください。

すでに登録済みのデバイス（再登録制限）

すでに特定のプレース（またはプレース グループ、代理店、ブランチ）に属しているデバイスは、現場で再登録できません。 LCD デバイスで登録メニュー（**CLUe Place Allocation**）に入るか、LCD がないデバイスの Web サーバーにアクセスすると、次のメッセージが表示され、登録画面へのアクセスがブロックされます。

> *This device is already registered. Changes can be made from the CLUe portal.*

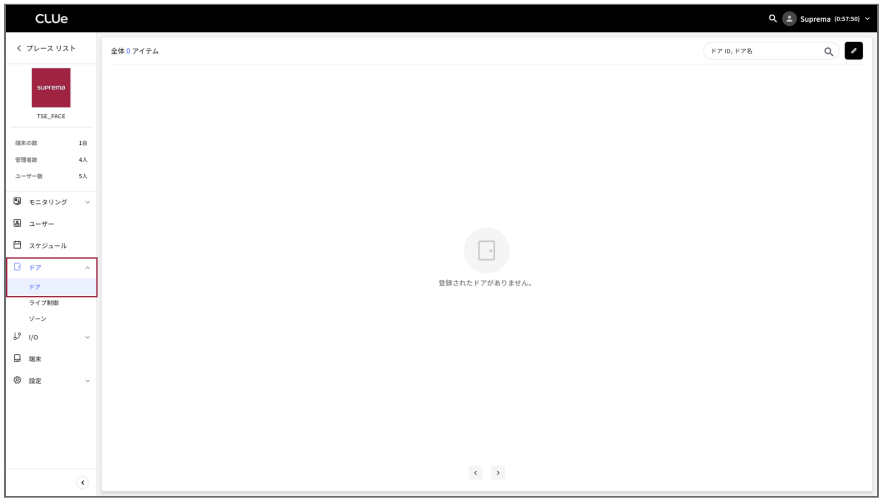
プレース変更や解除は CLUe ポータルでのみ可能で、現場では実行できません。 まれに、デバイス自体は特定のプレースに属していないように見えても、サーバーにはすでに登録されている場合があります（たとえば、ポータルで事前登録された場合）。 この場合も、**割り当てコード送信**を実行すると、同じくすでに登録済みというエラーメッセージが表示されます。 同様に、ポータルで変更を実行してください。

ドアの追加

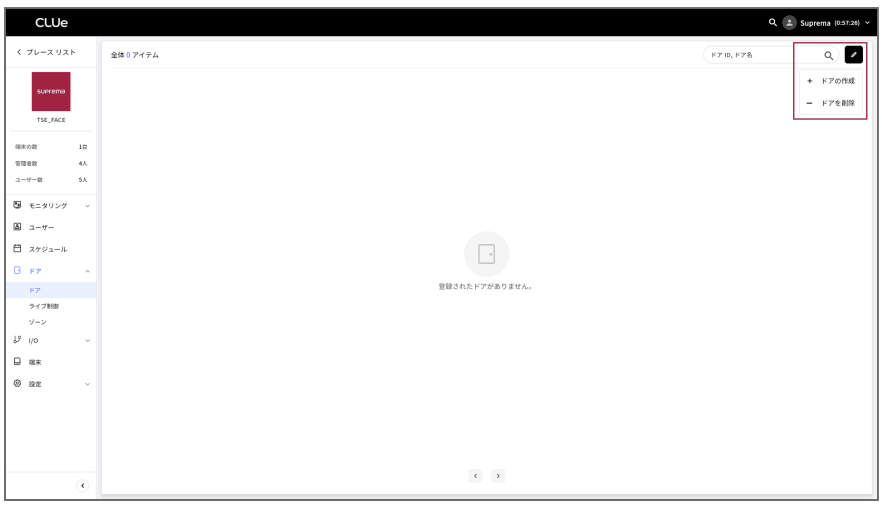
CLUeではドア設定が必須です。 ドアを設定しないと、ユーザー同期を含むサーバーとの通信が正常に動作しません。サービス開始前に必ず完了してください。

ドア設定

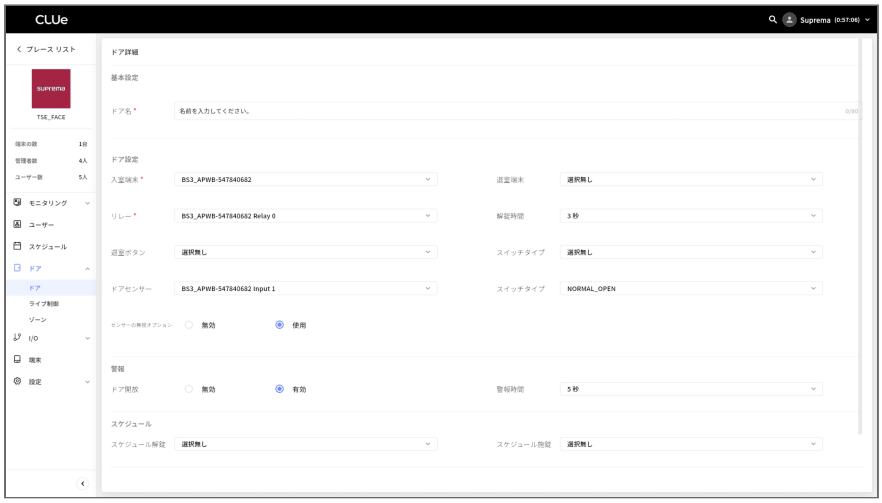
1. CLUe Webポータルにログインしてください。
2. ドアを追加するプレースを選択してください。
3. 画面左側のサイドバーで **ドア** → **ドア** をクリックしてください。



4. 画面右上の  → **ドアの作成** をクリックしてください。



5. ドア名を入力し、入室装置、リレー、退室ボタンなど、その他の必要な設定を選択してください。



6. ドア設定を完了したら、**作成** ボタンをクリックしてください。

> **情報**
>
> **センサーの無視オプション**
>
> - **使用**: ドアセンサーの状態に関係なく、ロック時間が経過するとドアリレーの状態が切り替わります。
> - **無効**: ドアセンサーが開状態を検知しても、ドアリレーは元の状態に切り替わりません。 自動ドアを構成する場合は、このオプションを選択してください。

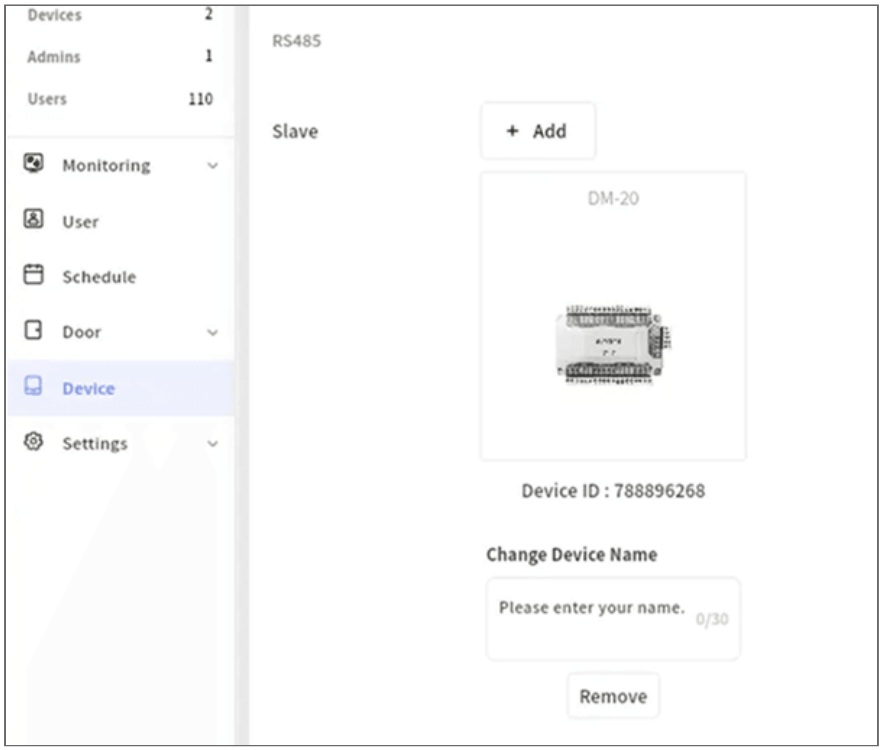
スレーブ装置リレー使用

SIO2、DM-20、DI-24のようなRS485スレーブ装置を使用する場合、マスター装置に接続されていても別のプレースに割り当てる必要があります。 一般装置と同じ方法でプレースに割り当ててください。 装置をプレースに割り当てる方法は デバイスを追加する を参照してください。

- 装置一覧でスレーブ装置を確認してください。



- マスター装置を選択し、接続されたスレーブ装置を追加してください。 その後、スレーブ装置のリレーと入力ポートを使用できます。


Devices 2
Admins 1
Users 110
Monitoring
User
Schedule
Door
Device
Settings
RS485
Slave
+ Add
DM-20
Device ID : 788896268
Change Device Name
Please enter your name.
0/30
Remove

ファームウェアをアップグレードする

CLUeデバイスのファームウェアを最新バージョンにアップグレードすると、新しい機能、性能の改善、セキュリティパッチを適用できます。 アップグレードはCLUe Webポータルで数回クリックするだけで進み、完了まで約5〜10分かかります。

アップグレードを開始する前に、次の事項を確認してください。

- アップグレード中はデバイスを使用できず、再起動時にロック装置の接続方式によっては出入口が一時的に開閉することがあります。
- アップグレード中にデバイス設定を変更した場合、完了後に反映されます。

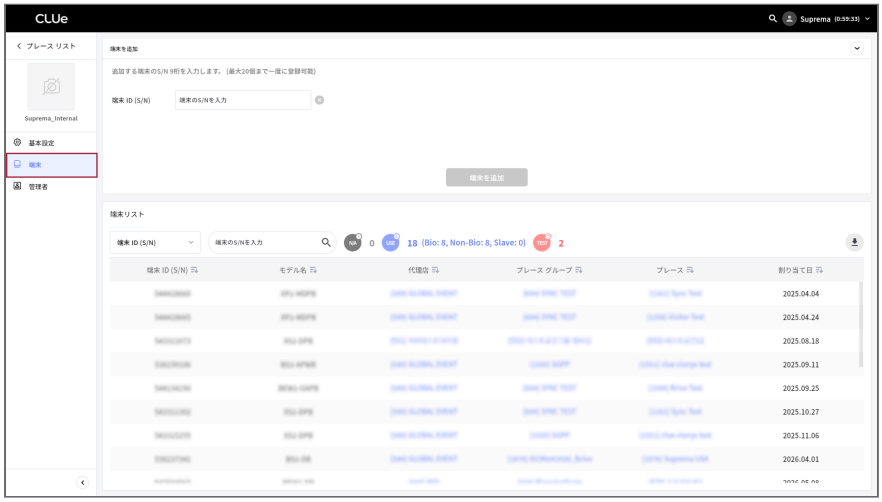
プレースへ移動

プレースに割り当てられた出入口デバイスをアップグレードするには、該当のプレースへ直接移動するか、上位のブランチ、代理店、プレース グループから移動できます。

1. CLUe Webポータルにログインしてください。
2. 初期画面でブランチ、代理店、またはプレース グループを選択してください。
3. 画面右上の ⋮ → **詳細設定** をクリックしてください。



4. 画面左側のサイドバーで **端末**をクリックしてください。



5. **端末リスト**で、ファームウェアをアップグレードするデバイスの **プレース** 列をクリックしてください。

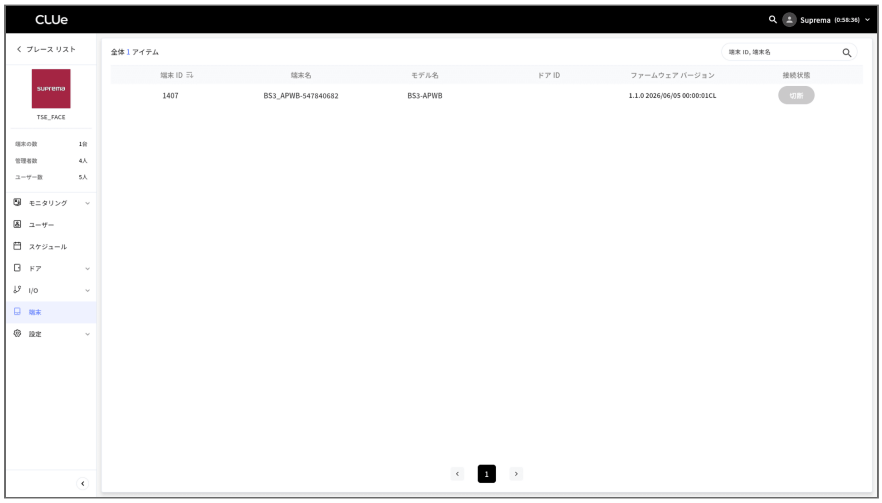


6. ボタンが有効になったらクリックしてください。

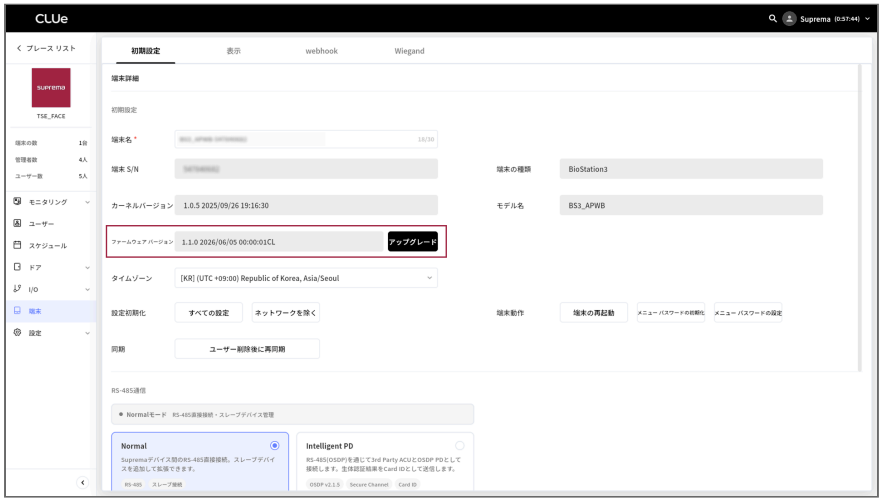
選択したデバイスが割り当てられたプレースの **端末** 画面に移動します。

ファームウェアをアップグレードする

1. デバイスが割り当てられたプレースの **端末** 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てください。

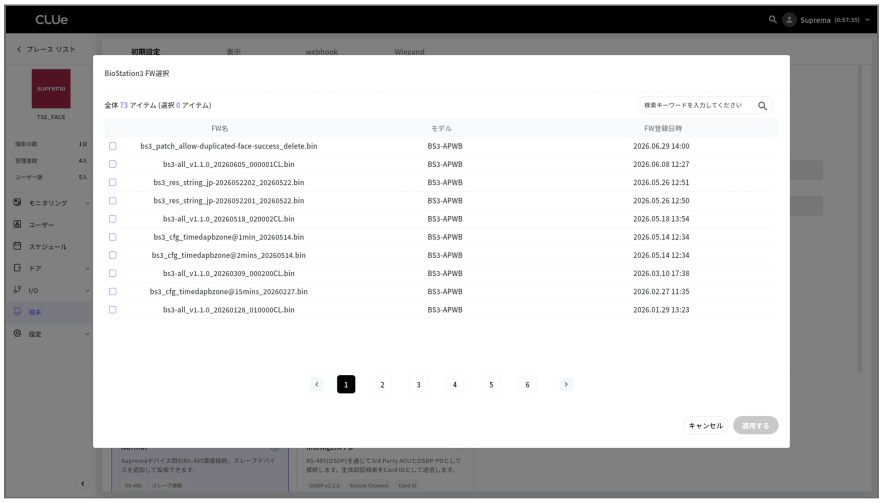


2. 選択したデバイスの **初期設定** 画面が表示されたら、**ファームウェア バージョン** 項目で現在のファームウェアバージョンを確認してください。



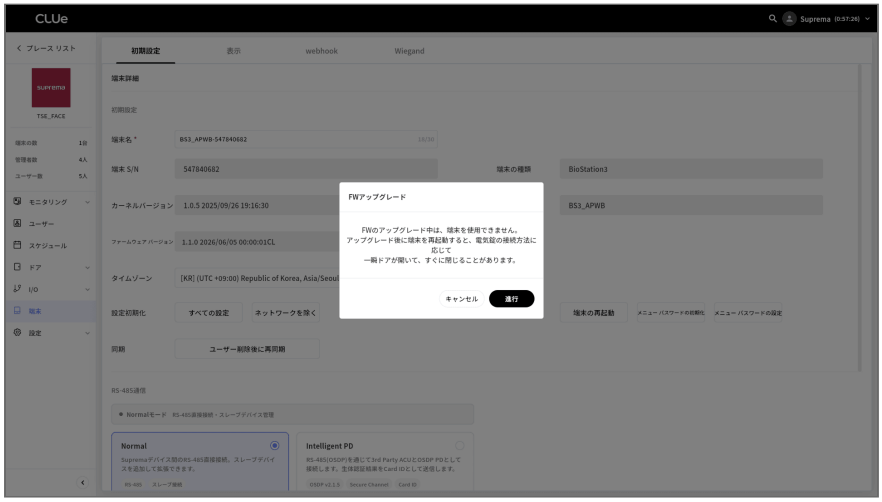
3. **アップグレード** ボタンをクリックしてください。

4. ファームウェア選択ウィンドウが表示されたら、アップグレードするファームウェアのチェックボックスをクリックしてください。

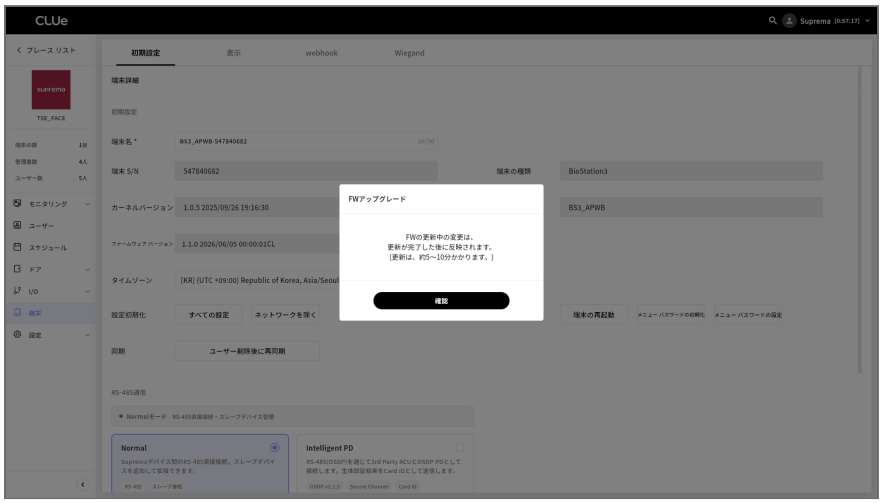


> 選択できるファームウェアバージョンは1つだけです。

5. 右下の **適用する** ボタンをクリックしてください。
6. アップグレード確認ウィンドウが表示されたら、**進行** ボタンをクリックしてください。



7. メッセージウィンドウが表示されたら内容を確認し、**確認** ボタンをクリックしてください。



デバイス Webhook 設定

CLUe ポータルで Webhook を設定すると、指定したイベントが発生したときに、デバイスが指定したエンドポイント（外部サーバー）へリアルタイムイベントを送信します。 この機能で、次のユースケースを実現できます。

- **勤怠管理システム**との連携
- **重複顔検出**イベントの受信

ほかにも、システムとのさまざまなリアルタイムイベント連携に活用できます。

対応デバイス

デバイス	モデル	対応ファームウェアバージョン
BioStation 3	BS3-DB, BS3-APWB	`bs3-all_v1.1.0_20250626` 以降

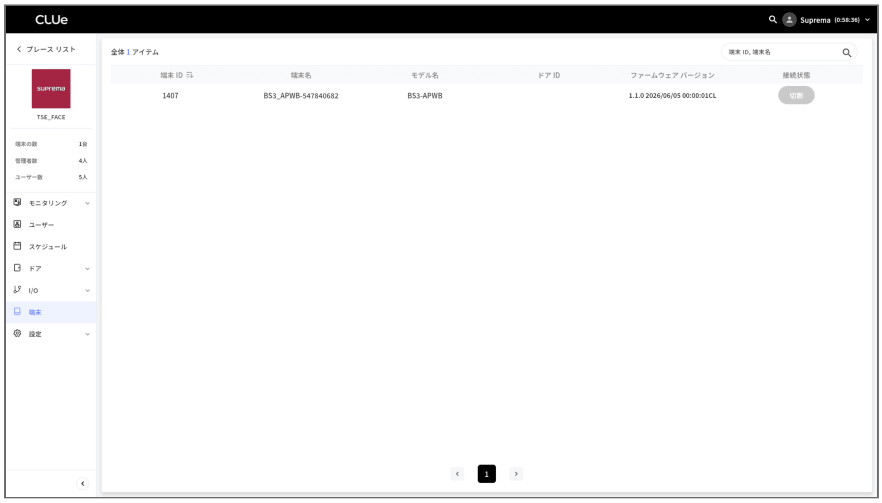
> **情報**
> 次の CLUe 対応デバイスでも Webhook をサポートする予定です。
> - BioEntry W3, BioLite N2, X-Station 2, XPass 2

主な利点

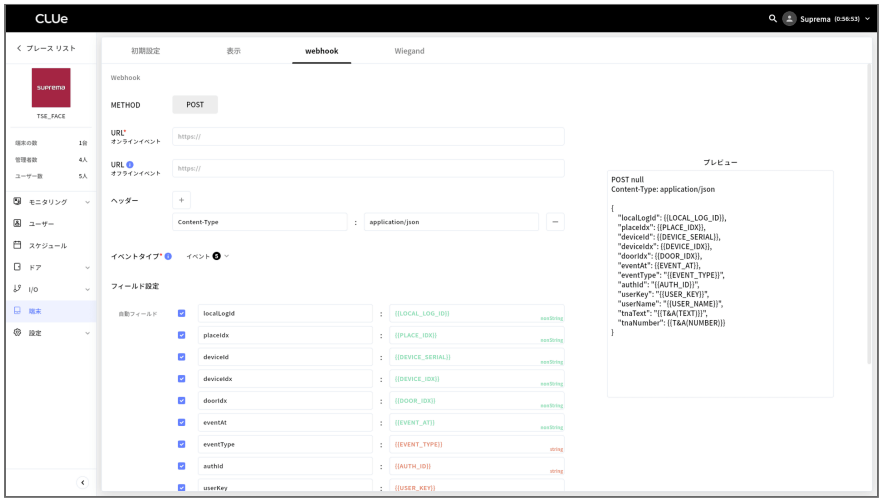
- デバイスのリアルタイムイベント通知を外部システムへ送信できます。
- Webhook を通じて外部システムと簡単に連携できます。
- 勤怠連携、セキュリティイベント監視などのユースケースをサポートします。

Webhook 設定

1. CLUe Webポータルにログインしてください。
2. Webhook を設定するデバイスが割り当てられたスペースに移動してください。
3. 画面左側のサイドバーで **端末** をクリックしてください。
4. デバイス一覧から Webhook を設定するデバイスを選択してください。



5. 画面上部の **webhook** タブをクリックしてください。



> **情報**
>
> **webhook** タブが表示されない場合は、デバイスの **CLUe ファームウェアバージョン**を確認し、対応するファームウェアバージョン以降 に更新してください。

1 メソッド

Webhook は既定で **POST** メソッドを使用します。

2 エンドポイント（URL）設定

- **オンラインイベント**: デバイスがオンライン状態のときに指定したイベントが発生すると、リアルタイムの Webhook 呼び出しを送信するエンドポイントです。
- **オフラインイベント**: デバイスがオフライン状態から再びオンライン状態に切り替わると、その間に発生したイベントを一覧形式で送信するエンドポイントです。

3 ヘッダー設定

Webhook サーバーに必要なキーまたは認証値をリクエストヘッダーに設定してください。 ヘッダーを追加するには ＋ ボタンをクリックしてください。



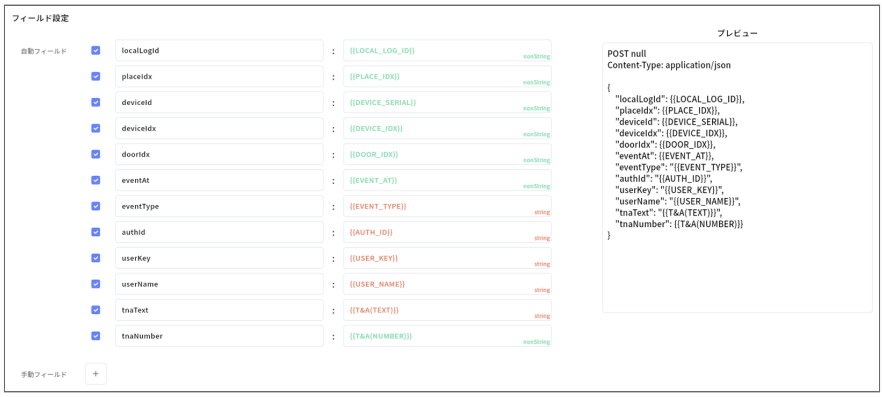
4 トリガーイベントの指定

Webhook 呼び出しをトリガーするイベントを選択してください。 既定で選択されたイベント以外にも、**重複顔検出** のようなイベントを追加で選択できます。



5 Webhook フィールドの構成

デバイスが送信するデータを定義するには、**Webhook フィールド**を構成してください。



- **自動フィールド**: デバイスが送信できるデータセットの種類を示します。
- **nonString**: Boolean、int のように引用符（""）で囲まないデータ型を指します。

必要なデータフィールドを選択した後、**プレビュー** パネルで Webhook ペイロードを事前確認できます。

追加で固定値を含める必要がある場合は、**手動フィールド** で追加できます。 この値は Webhook ペイロードと一緒に固定値として送信されます。

6 テスト呼び出しの実行

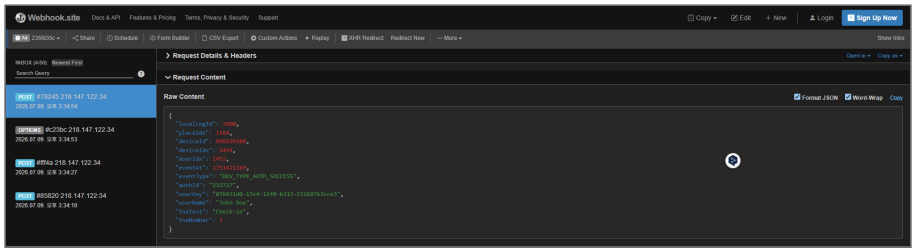
設定が完了したら、**テストコール** を実行できます。



> **情報**
> テスト呼び出しでは、実際のデバイスではなく、ブラウザーから直接設定したエンドポイントに送信されるデータの構造と形式を確認できます。

参考

サーバーがまだ準備されていなくても、インターネット上で公開されている Webhook テストサービスを使って Webhook テストを実行できます。 たとえば、Webhook.site を使って Webhook 呼び出しを簡単に確認できます。

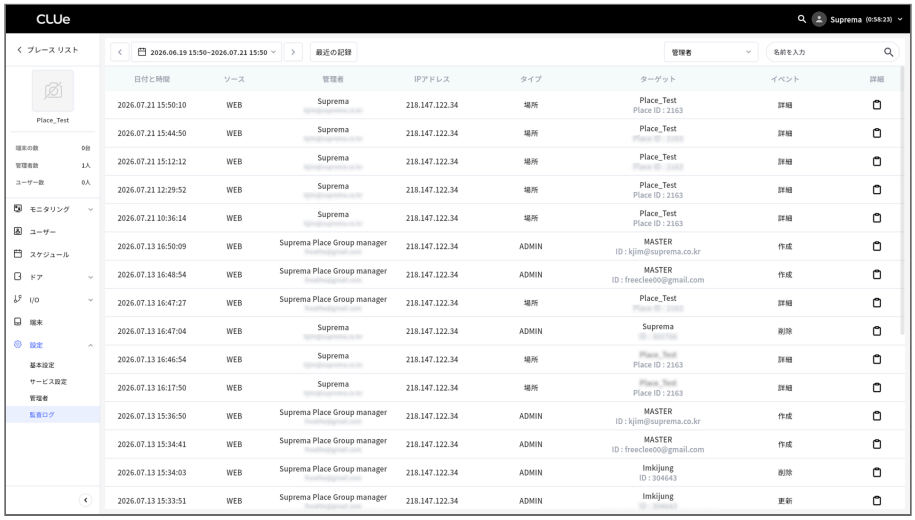

Webhook.site
Docs & API
Features & Pricing
Terms, Privacy & Security
Support
Copy
Edit
New
Login
Sign Up Now
Share
Schedule
Form Builder
CSV Export
Custom Actions
Replay
XHR Redirect
Redirect Now
More
Show Intro
INBOX (4/50)
Newest First
Search Query
POST #78245 218.147.122.34
2026.07.09. 오후 3:34:54
OPTIONS #c23bc 218.147.122.34
2026.07.09. 오후 3:34:53
POST #ff4fa 218.147.122.34
2026.07.09. 오후 3:34:27
POST #85820 218.147.122.34
2026.07.09. 오후 3:34:16
Request Details & Headers
Open in
Copy as
Request Content
Raw Content
Format JSON
Word-Wrap
Copy
{
"locallogId": 7600,
"placeId": 1150,
"deviceId": 69015190,
"deviceIdx": 3854,
"doorIdx": 105,
"eventAt": 1751421169,
"eventType": "DEV_TYPE_AUTH_SUCCESS",
"authId": "232727",
"userKey": "07641140-11c4-11f0-8313-2326876ccea3",
"userName": "John Doe",
"tnalext": "Check-in",
"cnaNumber": 1
}

監査ログを確認する

監査ログは、CLUeポータルのプレースで発生するすべてのアクティビティを記録し、追跡する機能です。 管理者は監査ログを使用して、誰が、いつ、どのアクティビティを実行したかを確認し、セキュリティ要件とコンプライアンス要件を満たせます。

監査ログを照会する

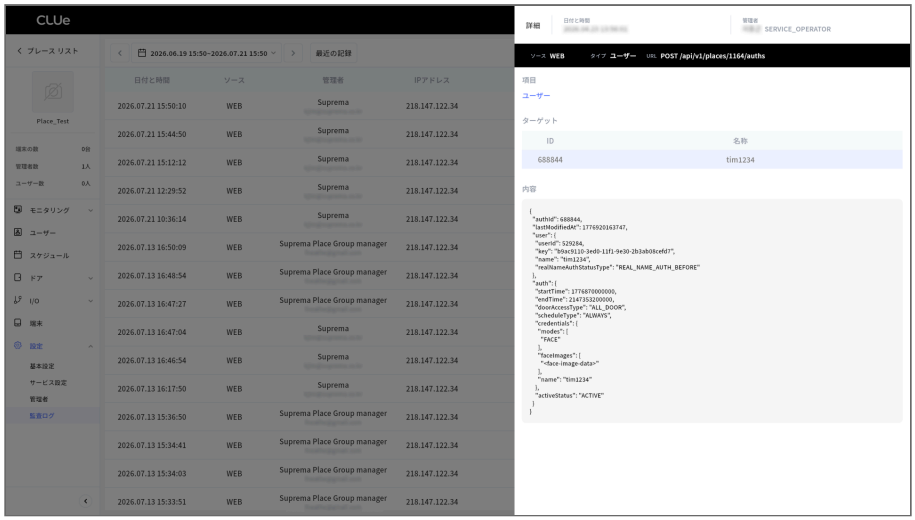
1. CLUe Webポータルにログインしてください。
2. 監査ログを確認するプレースを選択してください。
3. 画面左のサイドバーで**設定** → **監査ログ**をクリックしてください。



最新の監査ログが新しい順に一覧に表示されます。 各ログ項目では、アクティビティを実行した**日付と時間**、**ソース**、**管理者**、**IPアドレス**、**タイプ**、**ターゲット**、**イベント**を確認できます。

詳細情報の確認

監査ログ項目の詳細情報を確認するには、一覧の一番右にある**詳細**列で📋ボタンをクリックしてください。 画面右側に**詳細**パネルが表示されます。



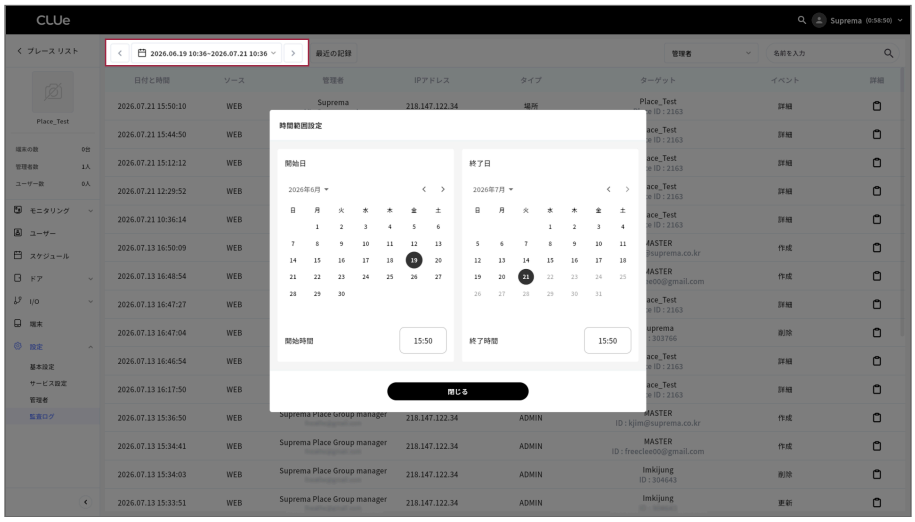
詳細パネルでは、日付と時刻、管理者アカウントに加え、**ソース**、**タイプ**、関連APIを確認でき、次の情報も表示します。

- **項目**: アクティビティが発生したカテゴリを表示します。
- **ターゲット**: アクティビティが適用された対象のIDと名前を表示します。
- **内容**: APIリクエスト本文データを表示します。 リクエスト本文がない場合は、空の値({})で表示されます。

照会期間の設定

現在設定されている照会期間の単位で照会期間を変更するには、監査ログ一覧の左上にある < または > をクリックしてください。

特定の期間の監査ログを照会するには、日付と時刻の領域( )をクリックしてください。 **時間範囲設定**ウィンドウが表示されたら、開始日時と終了日時を設定してください。 設定した期間の監査ログを照会できます。



> **情報**
> 設定した照会期間を初期化するには、**最近の記録**ボタンをクリックしてください。

検索

監査ログ一覧の各列の値を基準に、目的のデータを検索したりフィルタリングできます。 監査ログ一覧の右上にある検索ツールを使用してください。



- **管理者**: 管理者名を入力して検索できます。 大文字と小文字を区別して検索します。
- **IPアドレス**: IPアドレスを基準に検索できます。 正確なIPアドレスを入力する必要があります。

  > *例: 192.168.1.1*

- **ソース**: ユーザーがどのプラットフォームでアクティビティを行ったかの条件を選択できます。

> *Web(**WEB**)、モバイル(**MOBILE**)、API(**API_TOKEN**)*

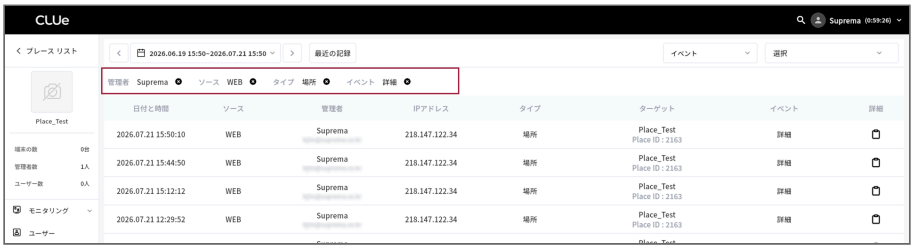
- **タイプ**: ユーザーのアクティビティカテゴリを選択できます。

  > ***端末**、**ドア**、**場所**、**ユーザー**、**資格情報戦略**、**ADMIN**、**個人情報の閲覧***

- **イベント**: 次のイベント条件を選択できます。

  > ***詳細**、**リスト**、**作成**、**更新**、**削除**、**命令***

複数のフィルター項目を同時に選択してフィルタリングできます。 異なる項目を選択すると AND 条件で、同じ項目に複数の値を選択すると OR 条件でフィルタリングします。 フィルタリングを解除するには、 ✕ ボタンをクリックしてください。





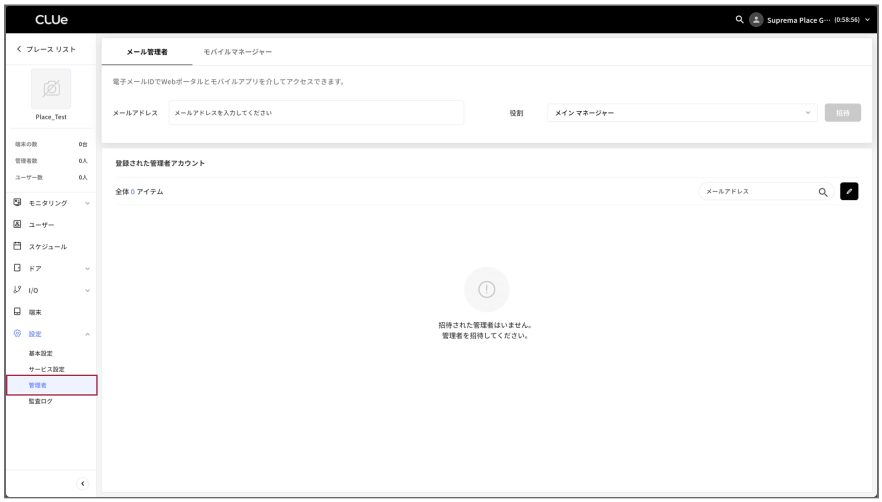
モバイルアプリの使用方法

CLUeモバイルアプリを使うと、スマートフォンでドアをリモート制御し、ユーザーを管理し、プレースのイベントをリアルタイムで確認できます。 この文書では、プレース管理者の招待方法からアプリのダウンロード、ログイン、主要機能まで案内します。

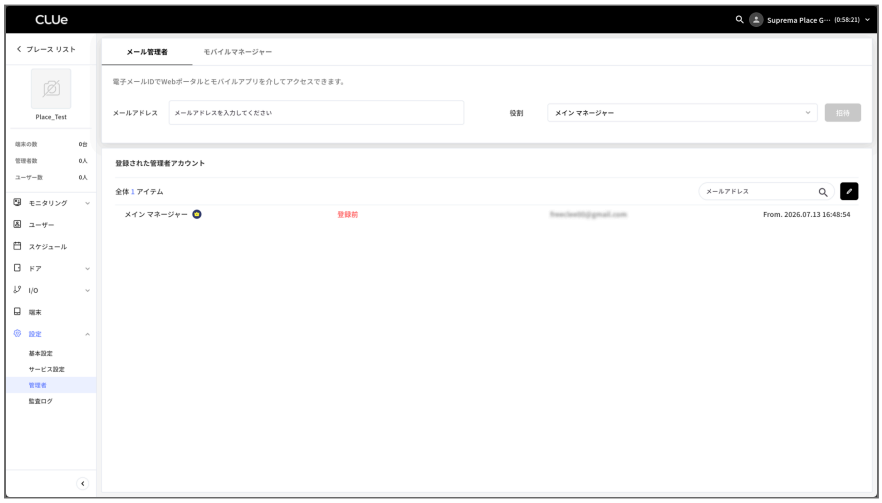
CLUeモバイルアプリの管理者招待

プレースグループ管理者は、プレース設定でメールによりプレース管理者を招待できます。

1. CLUe Webポータルにログインしてください。
2. モバイルアプリの管理者を招待するプレースを選択します。
3. 画面左のサイドバーで **設定** → **管理者** をクリックします。



4. メールアドレスを入力し、役割を選択します。
5. **招待** ボタンをクリックします。

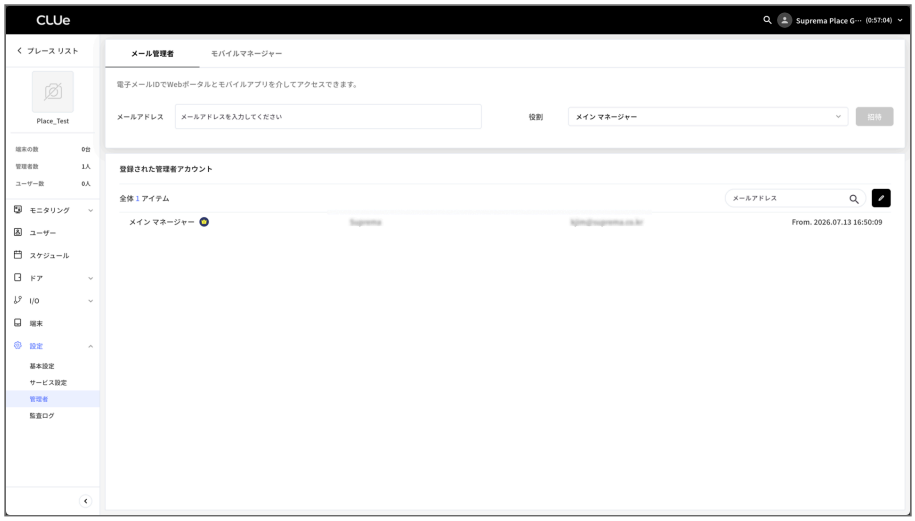


登録された管理者アカウント リストで招待ステータスを確認できます。

招待が完了すると、管理者に招待メールが送信されます。 招待された管理者は、メールに含まれるリンクから参加できます。



参加を完了すると、管理者リストでステータスの変更を確認できます。



> **CLUeモバイルアプリで直接参加できますか?**
>
> CLUe Webポータルにアクセスできない管理者は、CLUeアプリをダウンロードしてモバイルアプリから参加できます。ただし、実際に使用するには、必ずプレースに招待されている必要があります。

CLUeアプリのダウンロード

下のリンクまたはQRコードからCLUeアプリをダウンロードできます。

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

> **情報**
> アプリが見つからない場合は、アプリストアで「suprema clue」を検索します。

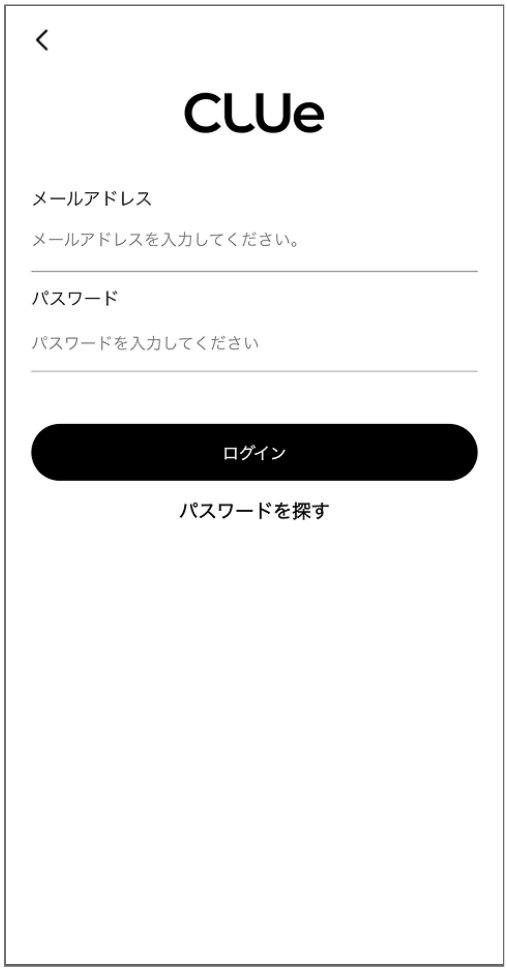
ログイン

アプリをインストールした後、招待されたメールアドレスでログインできます。

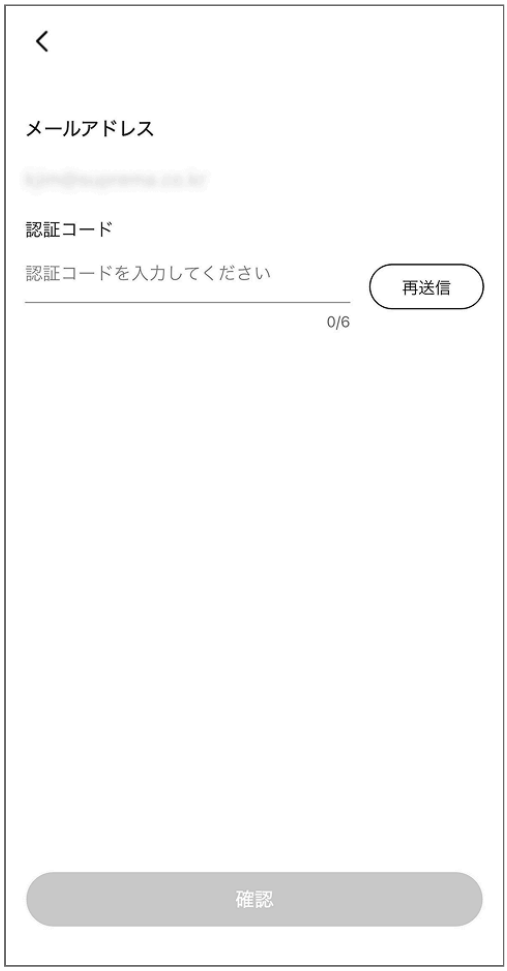
1. モバイル端末でCLUeアプリを起動します。
2. **メールでログイン**を選択します。



3. メールアドレスとパスワードを入力し、**ログイン**ボタンをタップしてください。

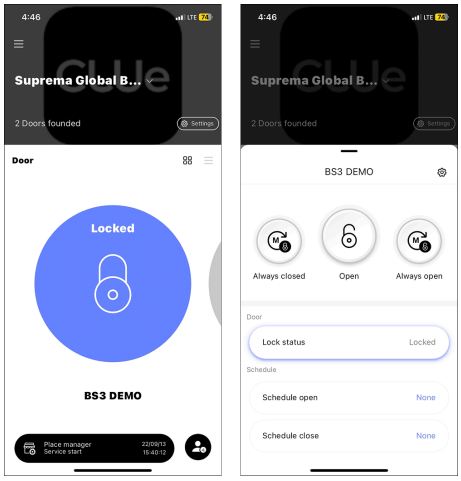


4. メールアドレスに送信された認証コードを入力し、**確認**ボタンをタップします。



ログアウトするまでログイン状態が維持されます。

CLUeアプリの主要機能



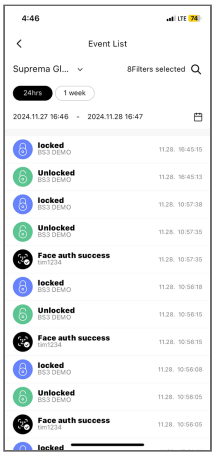
リモートドア制御

ドアの現在のロック状態を確認し、リモートで制御できます。 スケジュールを設定して、指定した時刻に自動で開閉するように設定できます。



ユーザー管理

ユーザーを招待または管理できます。 CLUeモバイルアプリとSuprema機器を使用して、顔、指紋、RFカードなどのクレデンシャルをエンロールできます。



イベントモニタリング

ドアの施錠と解錠、認証の成功と失敗など、プレースで発生したイベントをリアルタイムで確認できます。 24時間単位または1週間単位で検索したり、フィルターを適用して目的のイベントをすばやく見つけたりできます。

CLUe APIガイド

このドキュメントで、Suprema CLUe APIをすばやく簡単に連携できます。 APIキーの発行方法からリクエスト／レスポンス形式、エラーコード、呼び出し制限まで、CLUe APIの利用に必要な基本情報を案内します。 CLUe APIはSuprema CLUe Webポータルの設定と連携して動作するため、CLUe Webポータルのアカウントがない場合は、先にアカウントを依頼してください。

CLUe APIの利用に関する詳細をご確認ください。

APIキーとは

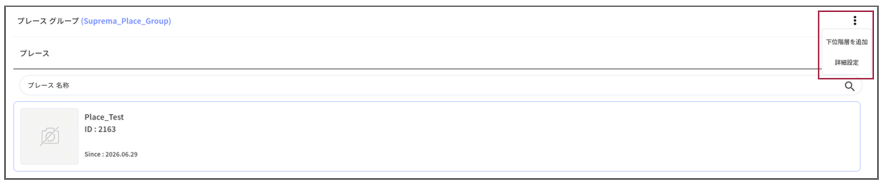
CLUe APIを呼び出すにはAPIキーが必要です。 プレース グループの管理者メニューで発行できます。 CLUe APIは、リクエストヘッダーにBearerトークンとしてAPIキーを必須で含める必要があります。 APIキーはCLUe Webポータルで発行、管理できます。

会員登録するには、上位管理者または同じプレース グループの管理者から招待を受ける必要があります。

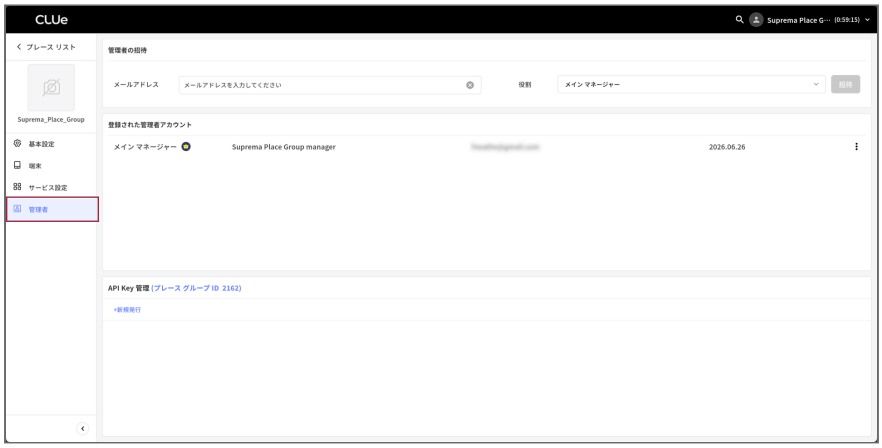
> **プレース(Place)とプレース グループ(Place Group)とは?**
>
> CLUeはマルチテナントシステムをサポートするため、**プレース**は会社やブランチのような独立した単位を意味し、**プレース グループ**は複数のプレースをまとめて管理する上位概念です。

APIキーの発行

1. CLUe Webポータルにログインしてください。
2. API連携のためのプレース グループを選択してください。
3. 画面右上の ⋮ → **詳細設定** をクリックしてください。



4. 画面左のサイドバーで **管理者** をクリックします。



5. **API Key 管理** セクションで **+新規発行** をクリックしてください。
6. 希望の有効期間を選択してください。



> **直接入力** を選択すると、有効期間を最大 365,000 日まで設定できます。

7. 新しい API キーを発行するには、**作成** ボタンをクリックしてください。
8. 新しい API キーが作成されたら、**コピー** ボタンをクリックして、CLUe API 呼び出し時の Bearer トークンとして使用してください。



> **注意**
> API キーは CLUe API へのアクセス権限をそのまま付与するため、外部に公開しないよう安全に保管してください。 不正使用によって発生する問題について、Suprema は責任を負いません。

CLUe APIの基本

Base URL

すべてのAPIリクエストを送信する基本URLは `https://api.moon.supremainc.com/v1` です。 すべてのAPIリクエストはHTTPS経由で送信してください。

CLUe APIは可能な限りRESTful原則に従い、ページおよびデータベースリソースに対するほとんどの操作を `GET` 、 `POST` 、 `PATCH` 、 `DELETE` リクエストで実行します。 リクエスト本文とレスポンス本文はどちらもJSON形式でエンコードされます。

API成功応答

応答が成功すると、次の状態が返されます。

HTTPステータスコード: `200`

フィールド	説明	選択の有無
code	API応答コード	
status	API応答状態	
message	API応答メッセージ	true
data	API応答データ	true

API失敗応答

応答が失敗すると、次の状態のいずれかが返されます。

HTTPステータスコード: 400 / 500

フィールド	説明	選択の有無
errors	API失敗応答	
errors.code	失敗エラーコード	
errors.message	失敗参照メッセージ	
errors.details	失敗詳細情報	true

一般エラーコード

コード	説明
e1000	内部サーバーエラー
e1001	権限拒否
e1002	非対応
e1003	不正な形式
e1004	JSON解析エラー
e1005	不正なメソッド引数
e1006	不正なリクエスト
e1007	存在しないリソース

コード	説明
e1008	メソッド引数の型不一致
e1009	リクエストヘッダーの不足

API呼び出し制限

注意

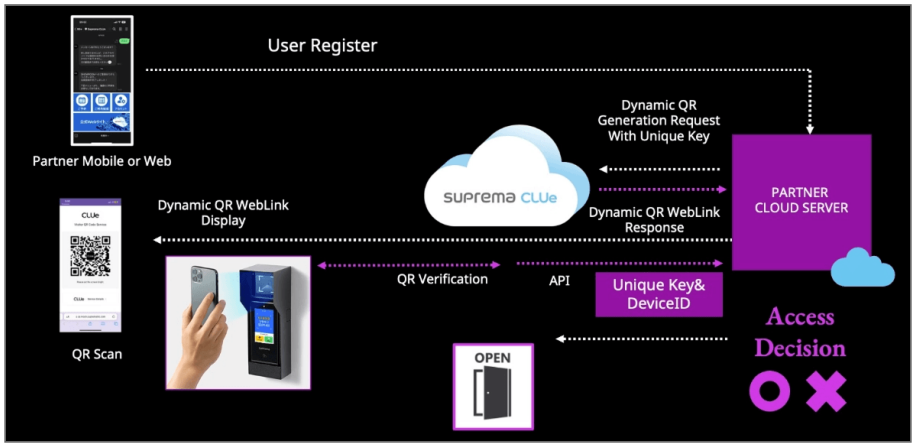
CLUeはAPIごとに5分あたり300回の呼び出し制限を設けており、この制限は呼び出し元単位で適用されます。 ただし、顔画像を追加するAPIには、テンプレート抽出および生成のように処理時間を要する作業が含まれるため、呼び出しの間に少し待機時間を置くことを推奨します。

Dynamic QRコード連携

CLUe Dynamic QRコードは、生成から検証までの全工程をサポートする統合QRソリューションです。 このドキュメントは、CLUe Dynamic QRコードを自社システムに連携する開発者向けに、APIキーの発行からサービス設定までの手順を案内します。

CLUe Dynamic QRコードとは

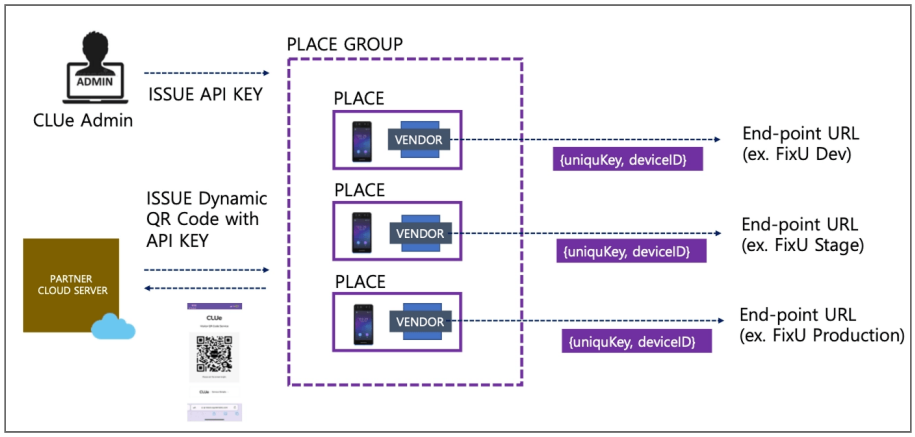
CLUe Dynamic QRコードは、生成から検証までの全工程をサポートする統合ソリューションです。顧客は、QRコード機能を最初から独自に開発せずに、自社システムへ簡単に連携できます。



> **情報**
> CLUe Dynamic QRコードは、**顧客確認(Vendor)**サービス方式と併用できます。 **顧客確認**設定の詳細は、サービスを設定するを参照してください。

開始する前に

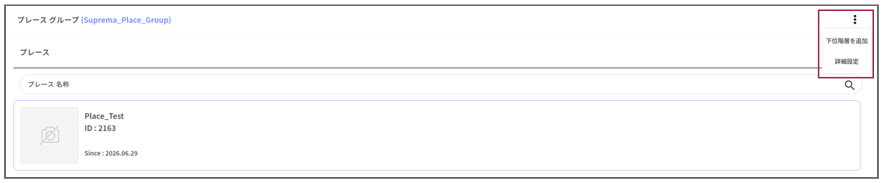
CLUe Dynamic QRコードは連携を目的とするため、プレース グループ(Place Group) APIキーが必要です。また、テスト用のベンダーコードも適用する必要があります。



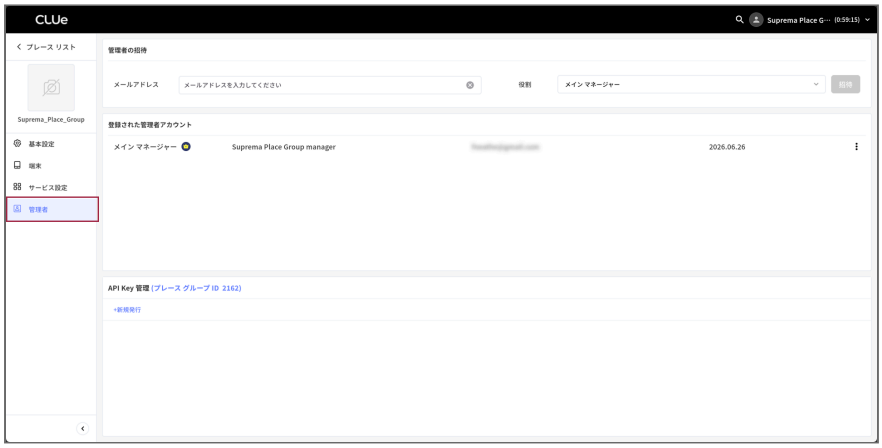
APIキーの発行

1. CLUe Webポータルにログインしてください。

2. API連携のためのプレース グループを選択してください。
3. 画面右上の ⋮ → **詳細設定** をクリックしてください。



4. 画面左のサイドバーで **管理者** をクリックします。



5. **API Key 管理** セクションで **+新規発行** をクリックしてください。
6. 希望の有効期間を選択してください。



> **直接入力** を選択すると、有効期間を最大 365,000 日まで設定できます。

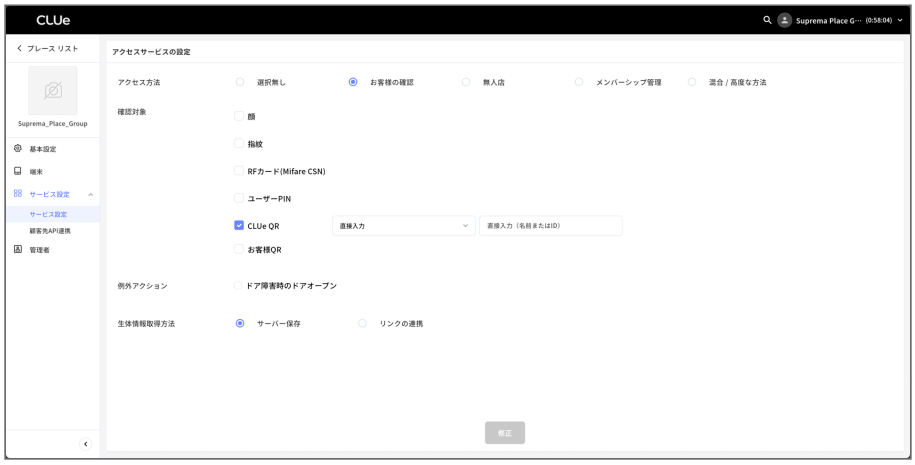
7. 新しい API キーを発行するには、**作成** ボタンをクリックしてください。
8. 新しい API キーが作成されたら、**コピー** ボタンをクリックして、CLUe API 呼び出し時の Bearer トークンとして使用してください。



> **注意**
> API キーは CLUe API へのアクセス権限をそのまま付与するため、外部に公開しないよう安全に保管してください。 不正使用によって発生する問題について、Suprema は責任を負いません。

サービス設定

プレース グループの**サービス設定**で**アクセス方法**を**お客様の確認**に設定し、**CLUe QR**を選択してください。



顧客確認コードは、QR連携手順に従ってSuprema CLUeチームから発行を受け、設定します。

> **顧客確認コードなしでテストできますか?**
>
> 可能です。 ただし、この場合はシステムに**テスト用顧客確認コード**を設定する必要があります。 Supremaの担当者に連絡し、サポートを依頼してください。 テスト用顧客確認コードは、アクセス権限や有効期限を検証せずにアクセスを許可します。

次のステップ

Dynamic CLUe QR APIの使用に関する詳細を確認してください。

Suprema Inc.

17F Parkview Tower, 248, Jeongjail-ro, Bundang-gu, Seongnam-si, Gyeonggi-do, 13554, Rep. of KOREA

電話: +82 31 783 4502 | Fax: +82 31 783 4503 | お問い合わせ: sales_sys@supremainc.com

Supremaのグローバル支社の詳細については、
QRコードをスキャンして以下のWebページにアクセスしてください。
https://www.supremainc.com/en/about/contact-us.asp

© 2026 Suprema, Inc. 本書に記載されている Suprema および Suprema 社の製品名および番号は、Suprema, Inc. の登録商標です。Suprema 社以外のすべてのブランドおよび製品名は、それぞれの企業の商標または登録商標です。製品の外観、ビルドステータスおよび/または仕様は、予告なく変更されることがあります。