Suprema Integration with Gallagher Command Centre

管理者ガイド

バージョン 2.0

日本語
JA 102.00.SIWG

suprema
SECURITY & BIOMETRICS

目次

目的 4

概要 5

機能 5

システム構成図 6

インストール 7

前提条件 7

設定フローチャート 8

ハードウェア配線接続 9

前提ソフトウェアをインストールする 12

設定 26

Gallagher Command Centre の設定 26

ハードウェア設定 39

BioStar 2 設定 71

Suprema Integration with Gallagher v2.0 79

アクセスグループを追加 83

Suprema と Gallagher のインテグレーション 87

Command Center で Face Template 用のユーザー写真 ID を登録する 98

Command Center で QR Code 用のユーザーのメール ID を登録する 102

既定のカード選択 110

スマートカード（AOC/TOC） 111

HID ICLASS カード 115

QR Code カード 117

ライセンス済みデバイス 117

トラブルシューティングとFAQ **119**

セットアップ 119

ミドルウェア 140

目的

Suprema Integration with Gallagher は、Gallagher Command Centre 8.8 以降のシステムが Suprema バイオメトリクスデバイスと通信するためのミドルウェアです。Command Centre からユーザーに対してバイオメトリクス顔面認証または指紋認証の Credential を登録し、接続されたデバイスの設定を管理できます。 Suprema Integration with Gallagher を使用すると、Suprema バイオメトリクスデバイスを使って、Command Centre 用のバイオメトリクス管理システムを簡単にセットアップし、構築できます。

> **情報**
> Gallagher Command Centre アクセス制御システムの機能の詳細については、Command Centre のユーザーマニュアルを参照してください。

概要

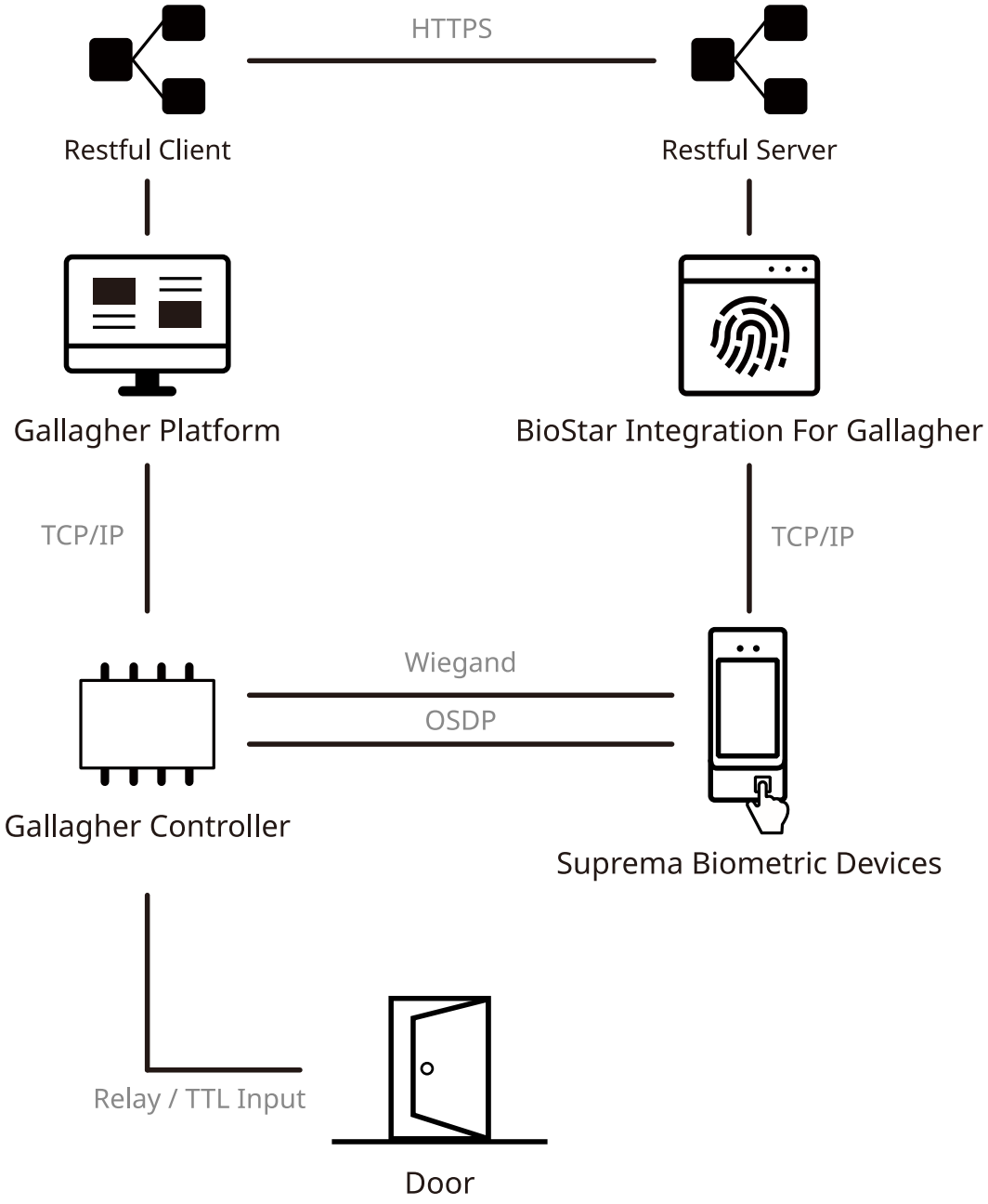
機能

Gallagher Command Centre と Suprema BioStar 2 の間で行う Suprema と Gallagher の通信。 そのため、Gallagher Command Centre から Suprema デバイス用の生体認証テンプレートを生成でき、すべてのエンドユーザーに先進的なソリューションを提供します。

Suprema と Gallagher のインテグレーションで提供される機能は次のとおりです：

- Gallagher Command Centre での一括ユーザー登録と管理が Suprema BioStar 2 に反映されます。
- Suprema インテグレーションにより、ユーザーは各種 Suprema 生体認証デバイスでのスキャンを通じて Visual Face と Fingerprint の生体認証データを登録できます。
- CSN と Wiegand の検出、および BioStar とのインテグレーションによるデータの自動拡充。
- Suprema インテグレーションにより、ユーザーは X-Station 2、BioLite N2、BioStation 3、FaceStation F2、XPass 2、X-Station 2、BioEntry W3、BioEntry W2 などの生体認証デバイスのスキャンを通じてカードデータを登録できます（これらはテスト済みのデバイスです）。
- 最大 1,000 台の生体認証デバイスを管理できます。
- すべての Suprema デバイスの設定は、Command Centre の同じウィンドウ内で行えます。
- TOC カード、QR カード、さらに特定の顧客ニーズに合わせたカスタムカード設定を含む、幅広いカード種別をサポートします。
- 必要な前提条件をすべて含むバンドル EXE パッケージによりインテグレーションのセットアップを簡素化し、スムーズで効率的なインストールを実現します。
- ミドルウェアには、ネットワーク関連の設定に対応する組み込み機能と、設定ミスやフォールトトレランスのシナリオを支援する包括的なトラブルシューティングガイドが含まれます。

システム構成図


HTTPS
Restful Client
Restful Server
Gallagher Platform
BioStar Integration For Gallagher
TCP/IP
TCP/IP
Wiegand
OSDP
Gallagher Controller
Suprema Biometric Devices
Relay / TTL Input
Door

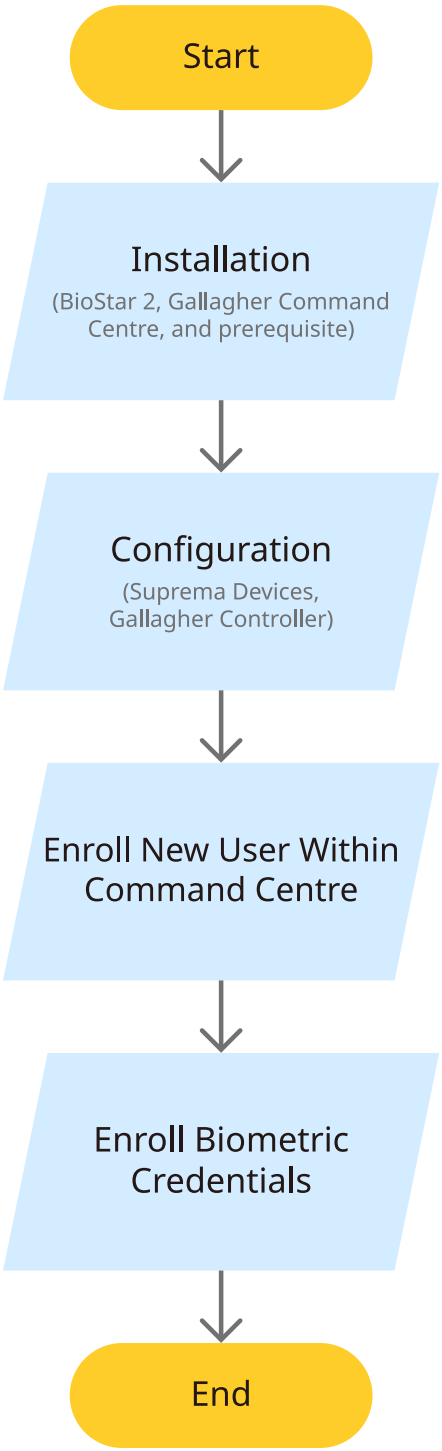
インストール

前提条件

Suprema Integration と Gallagher を使用するには、次の前提条件が必要です。 Suprema Integration と Gallagher をインストールする前に、サポート条件を確認してください。

前提条件	
Microsoft Windows 10（x64）以降	
Web ブラウザー	新しい Microsoft Edge
Gallagher Command Centre	Command Center 8.80 以降
Suprema BioStar 2	• x64 ビット • バージョン 2.9.5 以降
ソフトウェア	• Node v16.17.0 • Postgresql v14.5 • pgAdmin 4 v6.16 • Win64OpenSSL-3.0.5
ミドルウェアシステムのハードウェア要件	• 16 GB RAM • Windows 10 以降 • 256 GB SSD / 1 TB HDD • Intel Iris Xe Graphics（あれば望ましい）
Suprema 生体認証デバイス	• BioStation 3 • BioLite N2 • FaceStation F2 • BioEntry W2 • XPass 2 • X-Station 2 • BioEntry W3

設定フローチャート


Start
Installation
(BioStar 2, Gallagher Command Centre, and prerequisite)
Configuration
(Suprema Devices, Gallagher Controller)
Enroll New User Within Command Centre
Enroll Biometric Credentials
End

ハードウェア配線接続

Wiegand 接続用

Suprema デバイス - **リーダー 1** を HBUS 4 In 2Out n Door Module Wiegand に接続

（Suprema デバイス）配線名	**HBUS 4 In 2 Out Door Module Wiegand ポートのコネクター**
Wiegand D0 Out（緑）	R1 Data 0
Wiegand D1 Out（白）	R1 Data 1
Wiegand Ground（黒）	GND
TTL IN0（赤/紫）	R1 Out 2
TTL IN1（黄/茶）	R1 Out 1

Suprema デバイス - **リーダー 2** を HBUS 4 In 2Out n Door Module Wiegand に接続

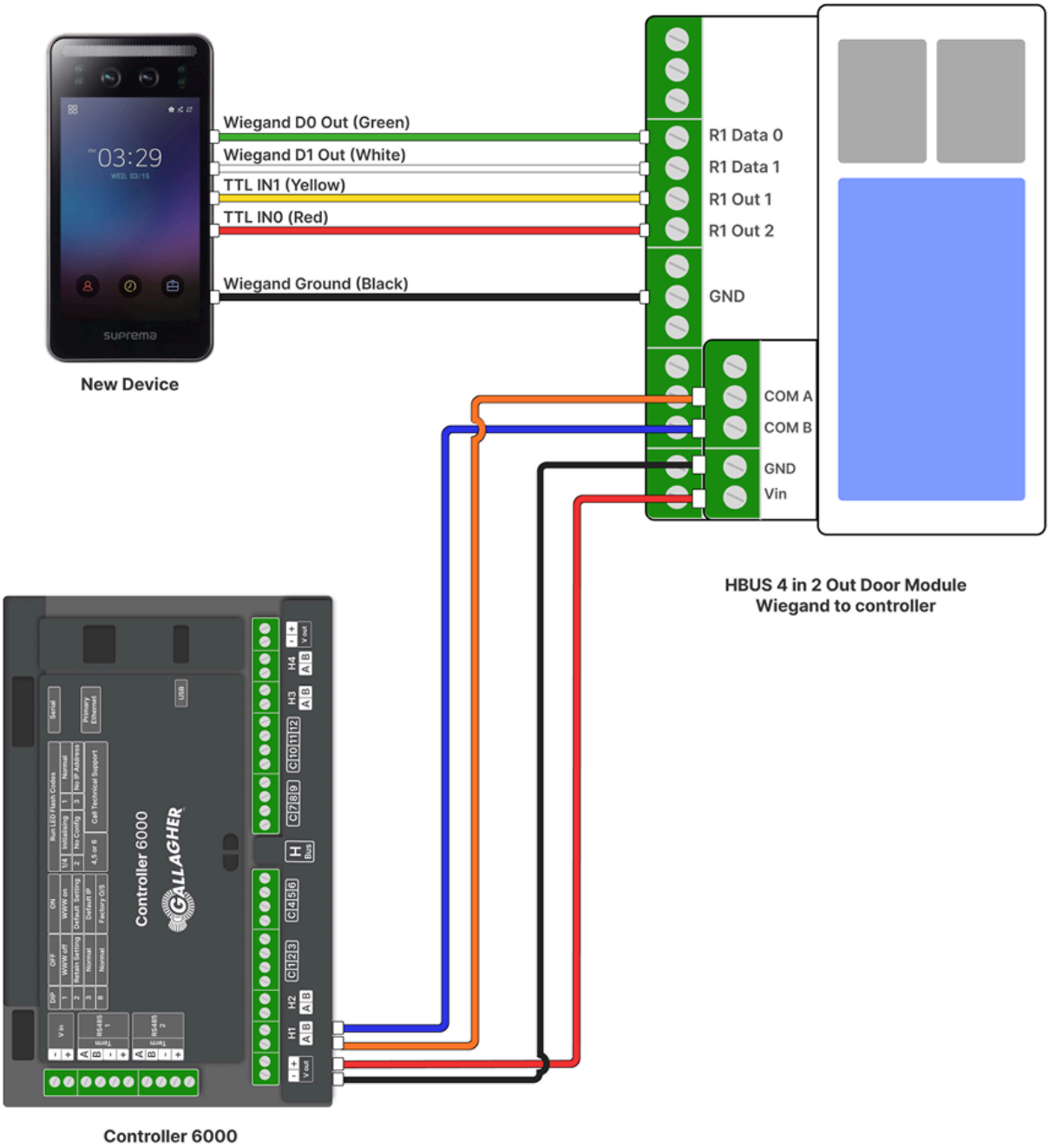
（Suprema デバイス）配線名	**HBUS 4 In 2 Out Door Module Wiegand ポートのコネクター**
Wiegand D0 Out（緑）	R2 Data 0
Wiegand D1 Out（白）	R2 Data 1
Wiegand Ground（黒）	GND
TTL IN0（赤/紫）	R2 Out 2
TTL IN1（黄/茶）	R2 Out 1

HBUS 4 In 2Out n Door Module Wiegand から Controller 6000 HBus へ接続

Controller 6000	**HBUS 4 In 2 Out Door Module Wiegand**
H1 A	COM A
H1 B	COM B
Vout -ve	GND

Controller 6000	HBUS 4 In 2 Out Door Module Wiegand
Vout +ve	Vin

Wiegand 接続図



OSDP 接続用

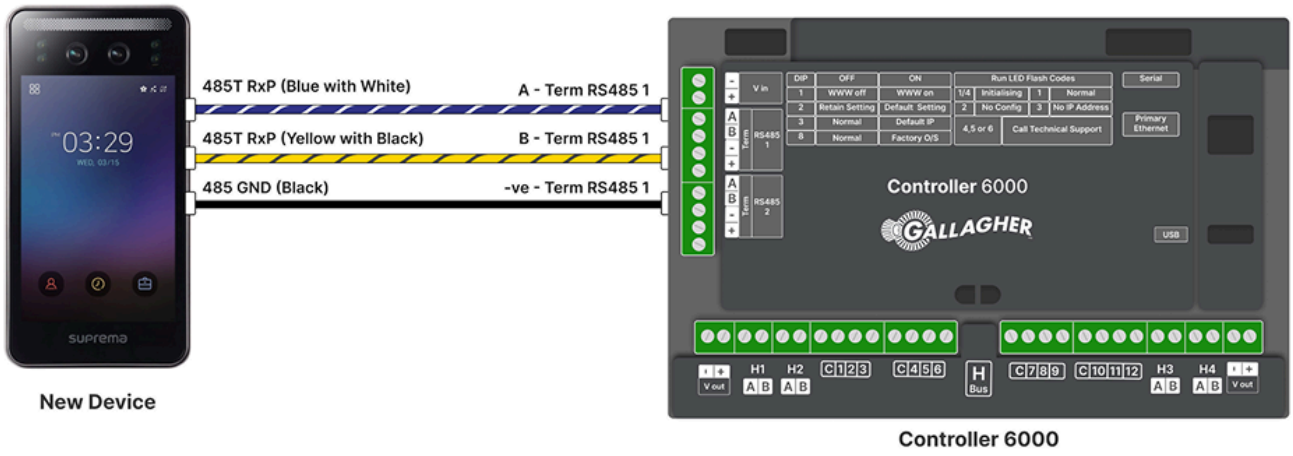
Suprema デバイス OSDP/RS485 **リーダー 1** を Controller 6000 に接続

（Suprema デバイス/OSDP デバイス） 配線名	Controller 6000 ポート
青 / 白線入り青	RS485 1 A
黄 / 黒線入り黄	RS485 1 B
黒 / 白線入り黒	RS485 1 -ve

Suprema デバイス OSDP/RS485 リーダー 2 を Controller 6000 に接続

（Suprema デバイス/OSDP デバイス） 配線名	Controller 6000 ポート
青 / 白線入り青	RS485 2 A
黄 / 黒線入り黄	RS485 2 B
黒 / 白線入り黒	RS485 2 -ve

OSDP 接続図



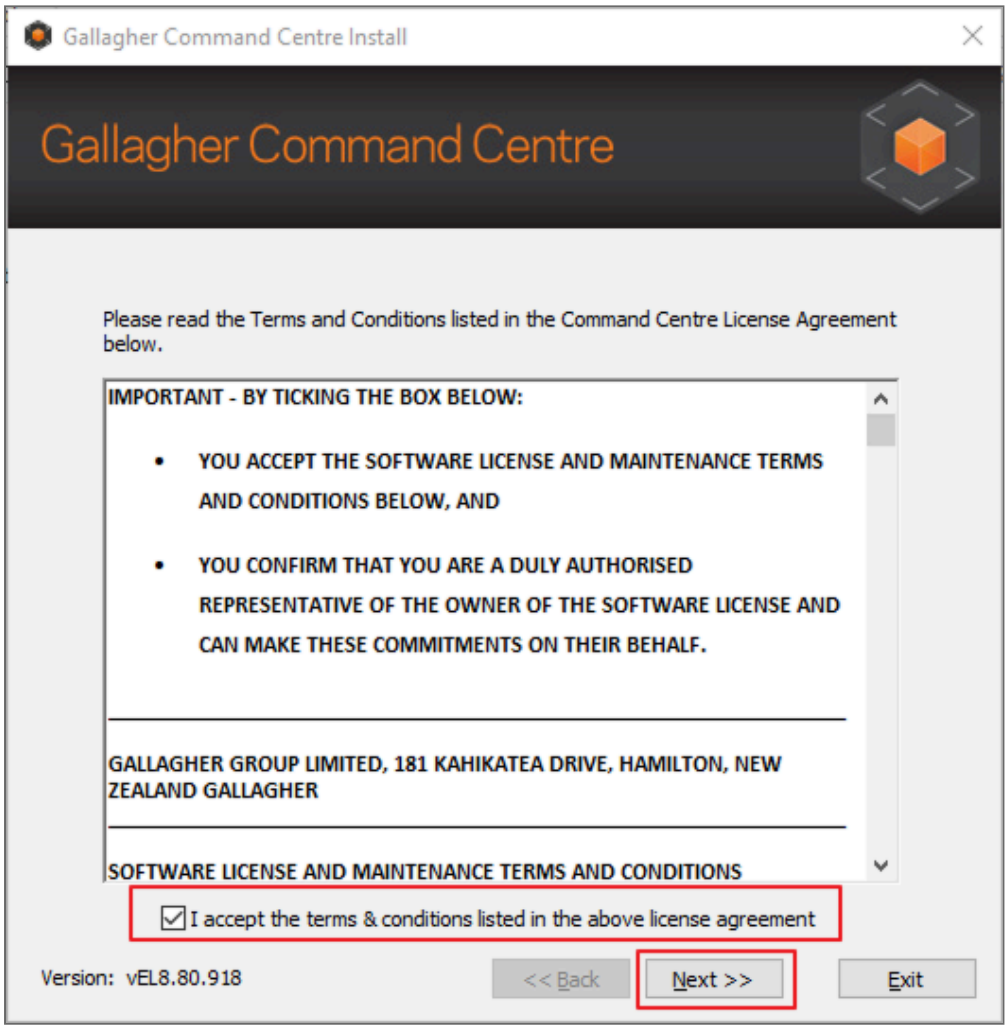
前提ソフトウェアをインストールする

Gallagher Command Centre のセットアップをインストールする

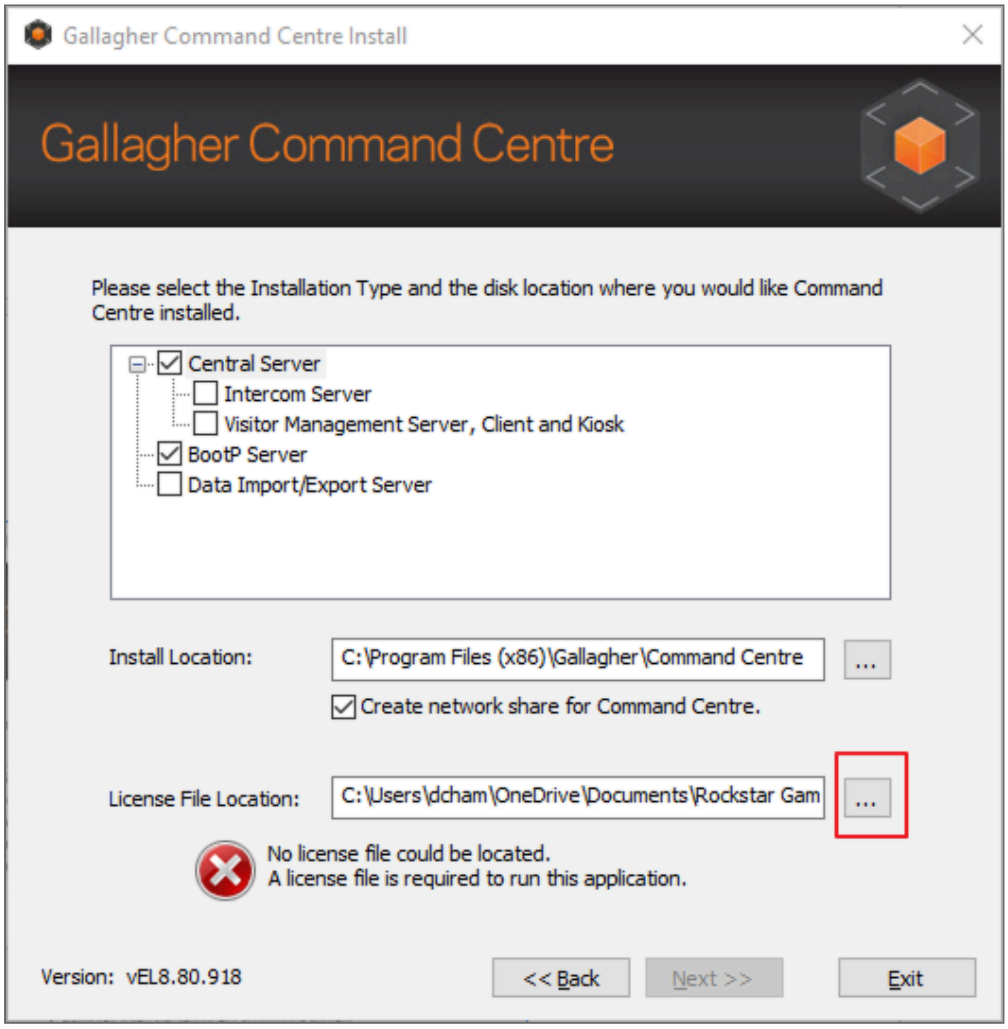
情報

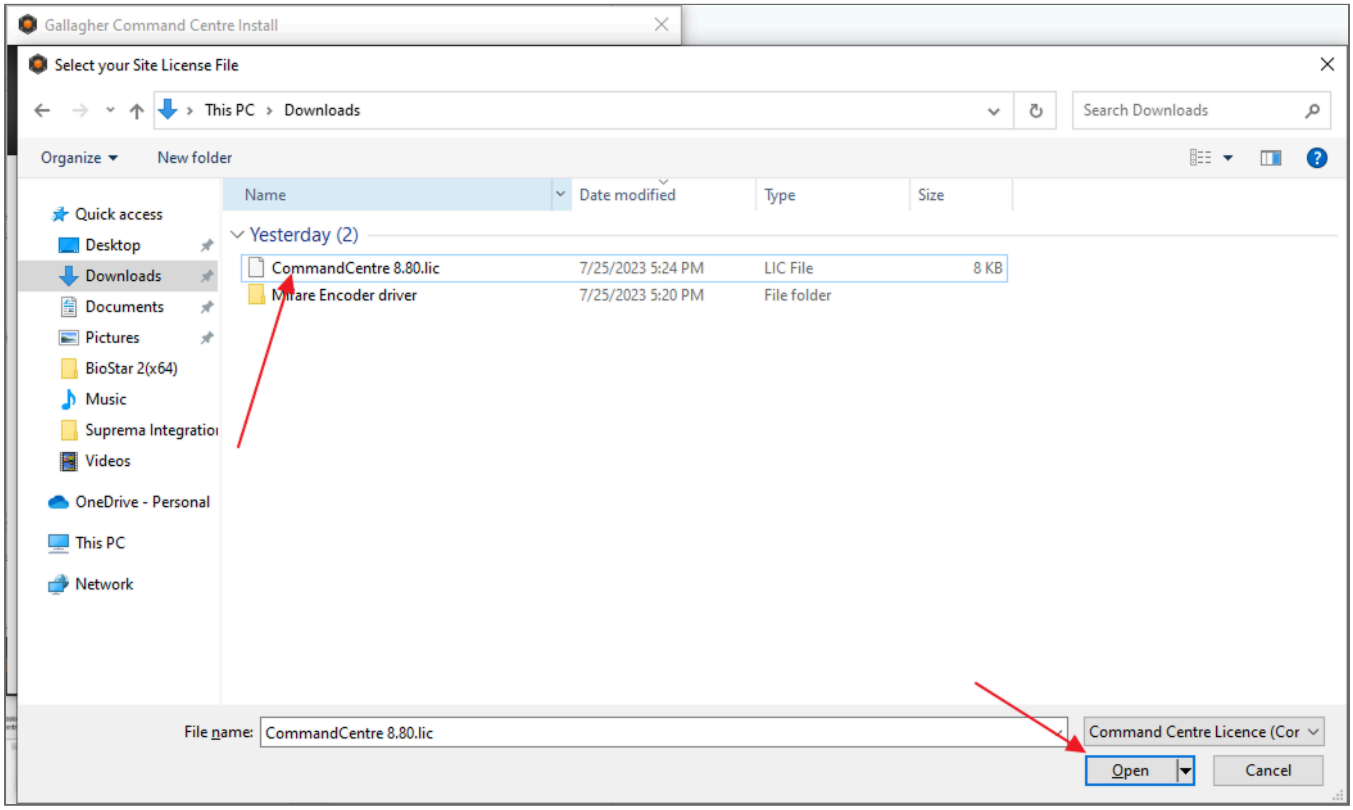
- セットアップと設定中は、名前やパスワードを変更しないでください。
- Suprema Integration with Gallagher のバージョンをアップグレードする場合は、ここをクリックしてください。
- 新規インストールの場合は、**3C4643 Gallagher Command Centre vEL8.80 Release Note** を参照してください。
- アップグレードする場合は、Command Centre の ISO ディレクトリにある Release Notes フォルダーの **3E0068 Upgrade Procedure** を参照してください。
- `Suprema integration With Gallagher.zip` を `C:\Program Files\` に展開してください。

1. Gallagher Command Centre フォルダー vEL.8.80（以降）→ Setup.exe で、**チェックボックスをオンにして Next** ボタンを押します。

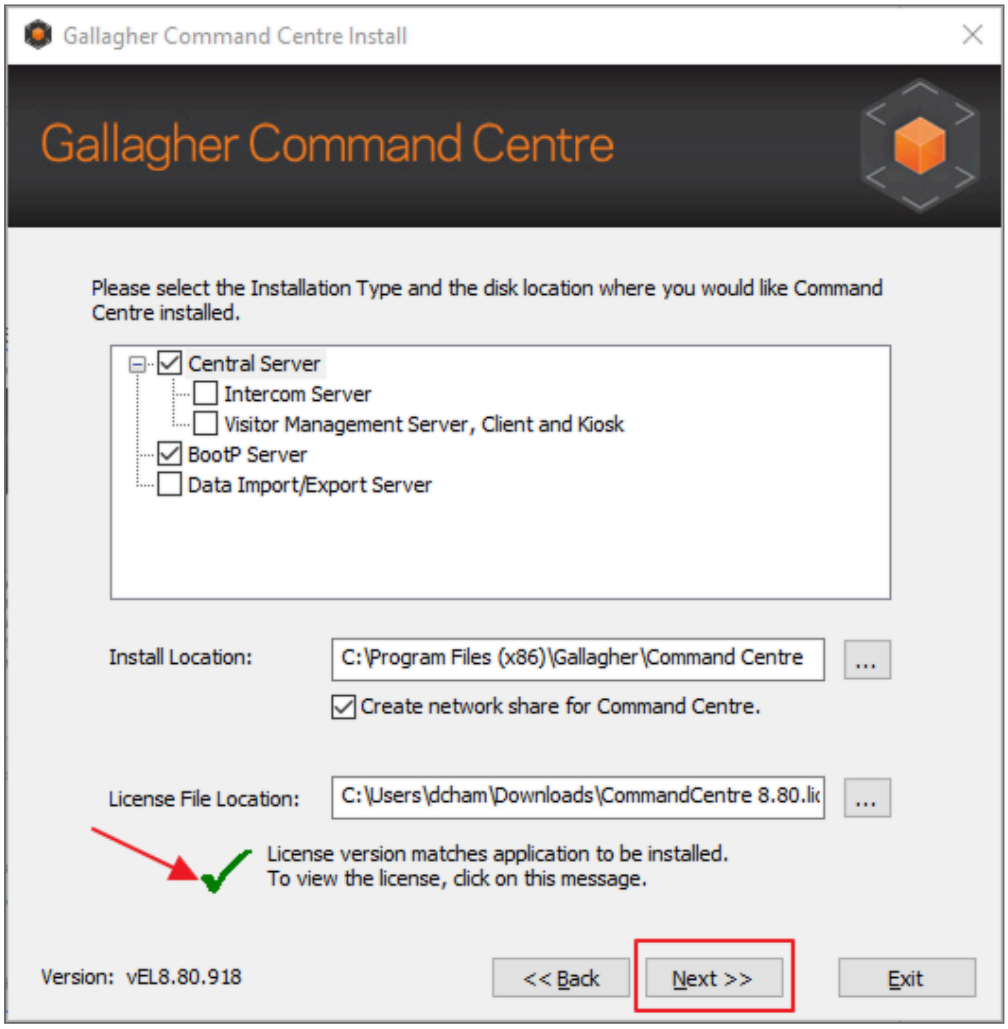


2. 「…」 ボタンをクリックし、セットアップに含まれるライセンスファイルを指定します。

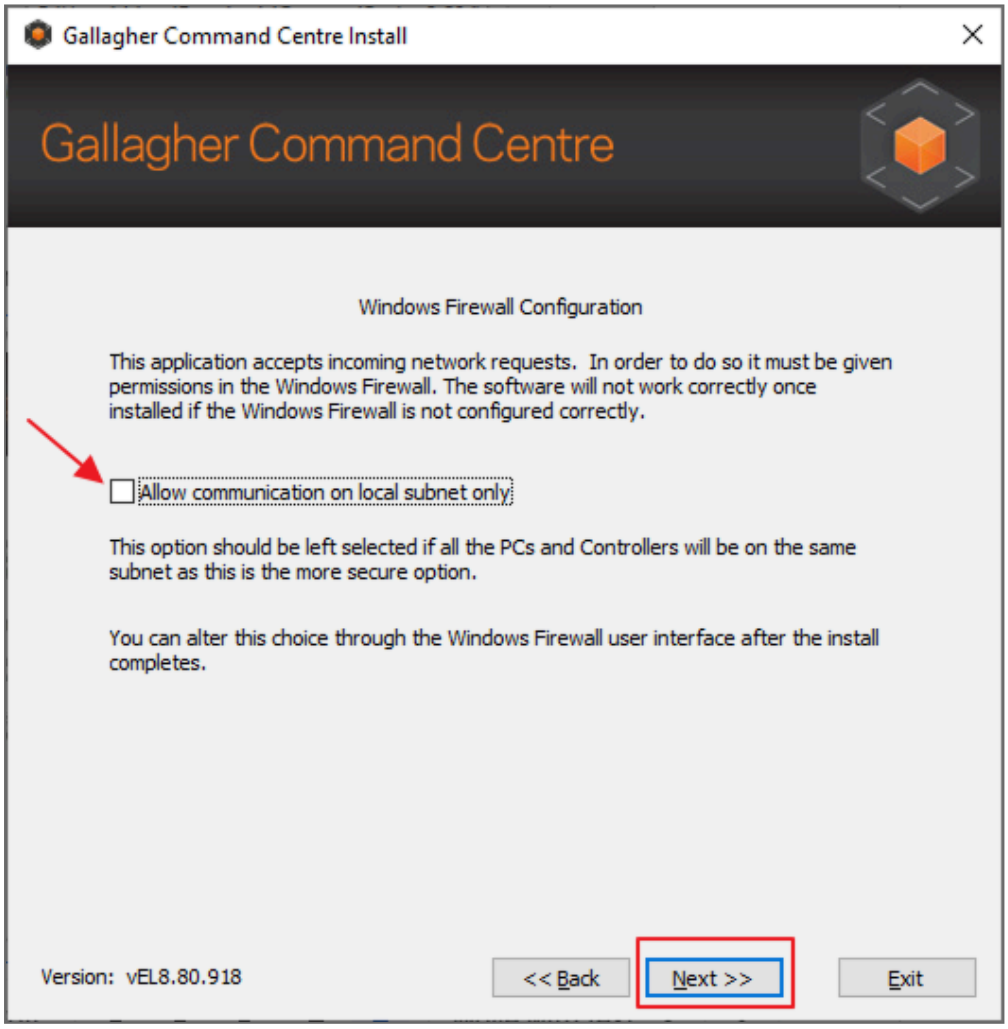




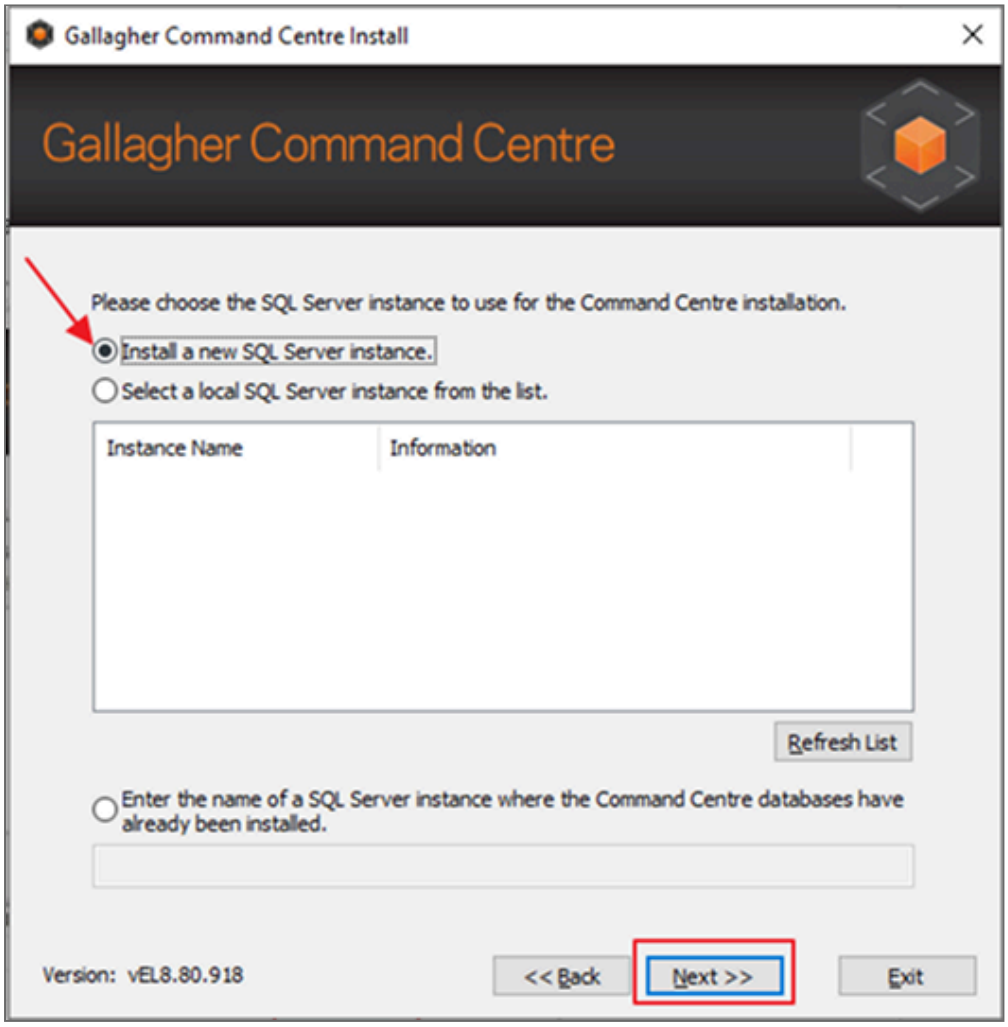
3. 正しいライセンスファイルを選択すると、アイコンがチェックマークに変わります。次に、**Next** ボタンを押します。



4. サブネットのチェックボックスだけを**オフにして**、**Next** ボタンを押します。

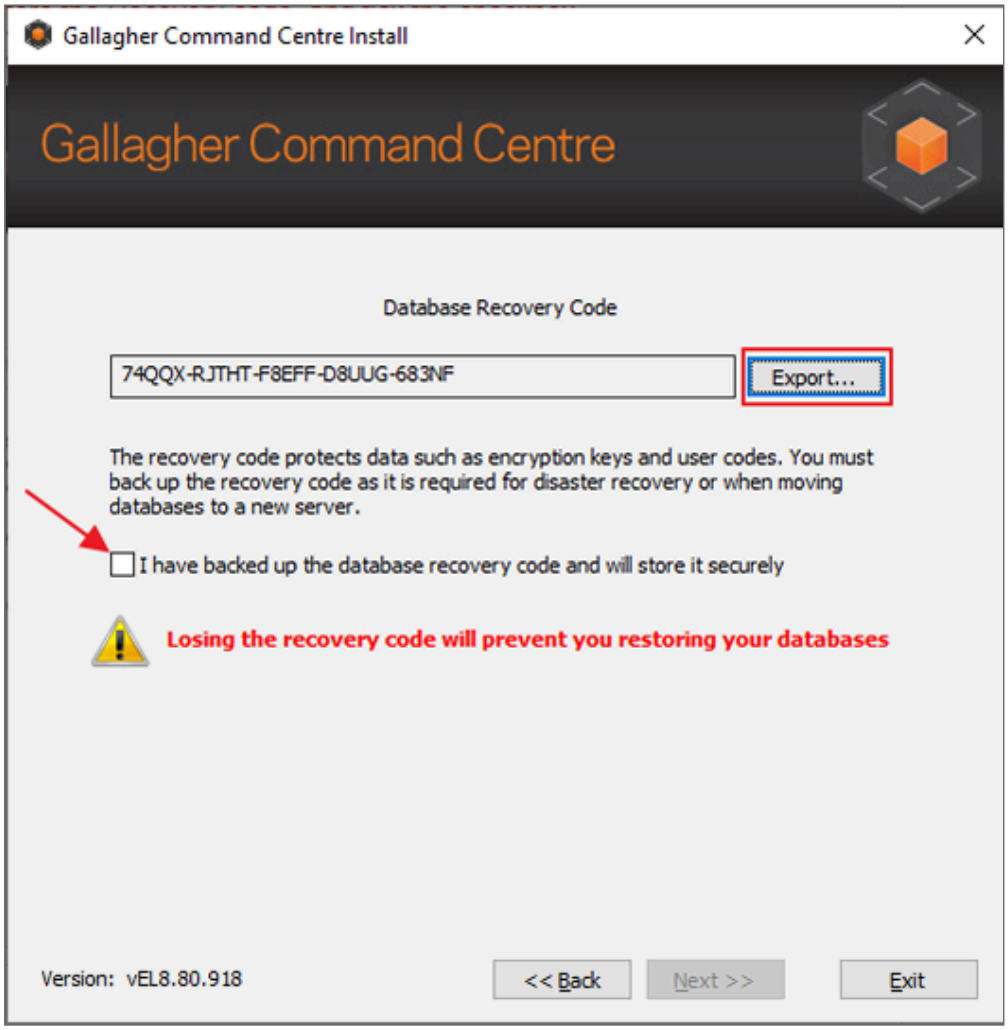


5. **Install new SQL** オプションを選択して、**Next** ボタンを押します。

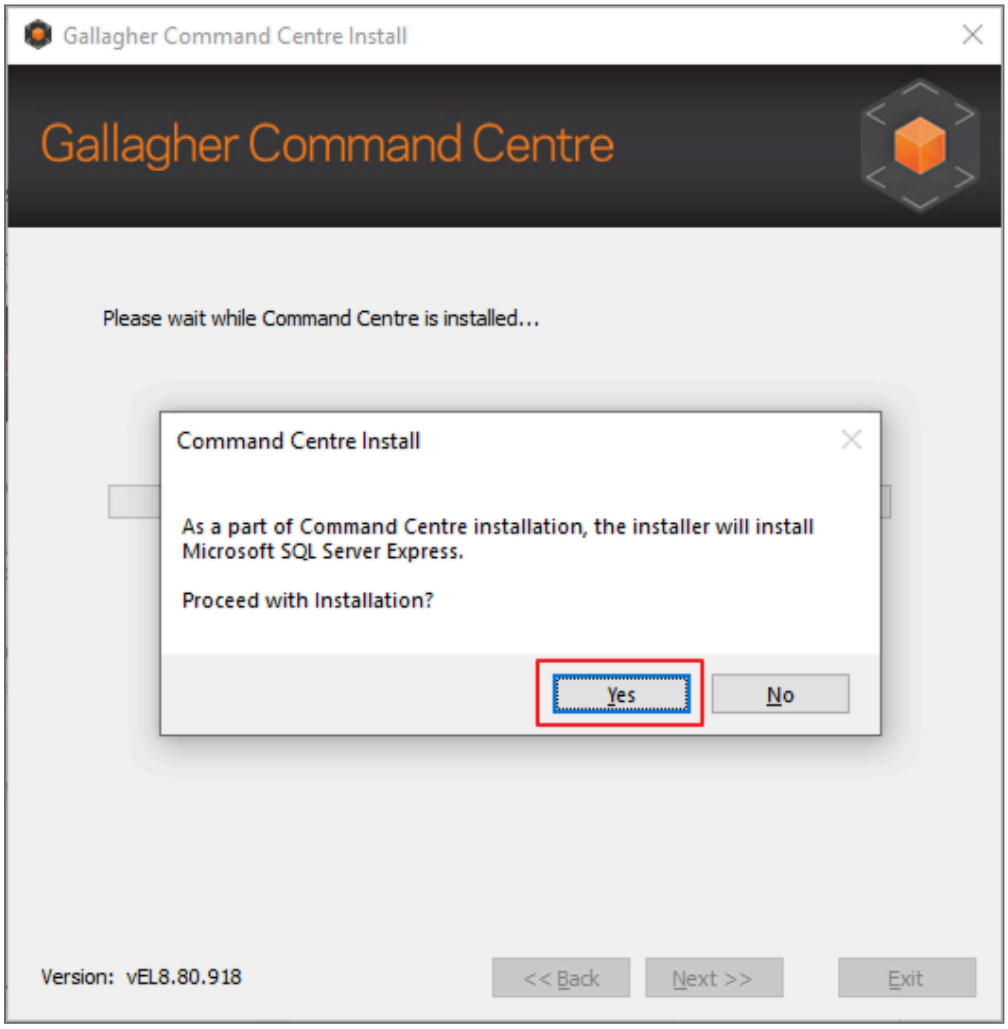


6. データベーステンプレートをインストールしないを**選択します**。
7. 設定を変更せずに、復旧コード画面が表示されるまで **Next** を押します。

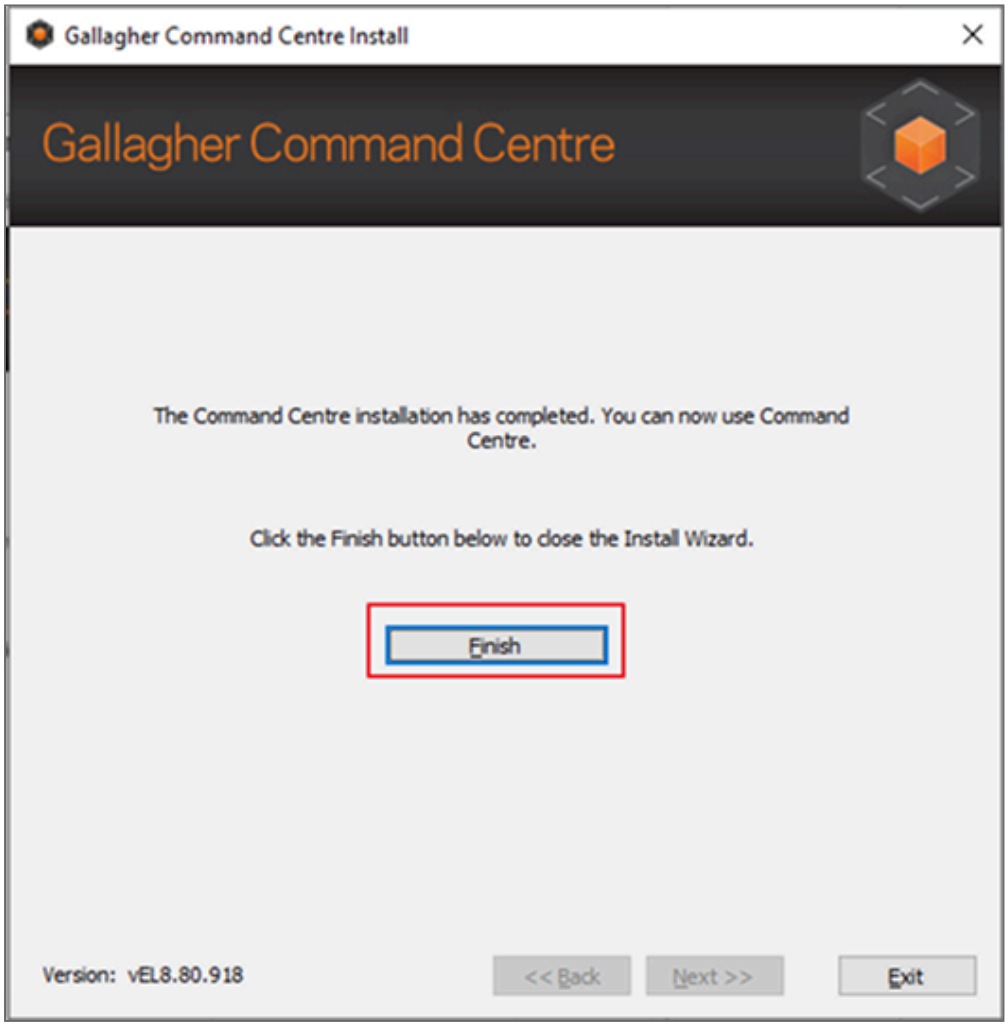
> **情報**
> エクスポートボタンをクリックして復旧コードを保存し、チェックボックスをオンにします。



8. **Yes** を選択すると、インストールが開始されます。



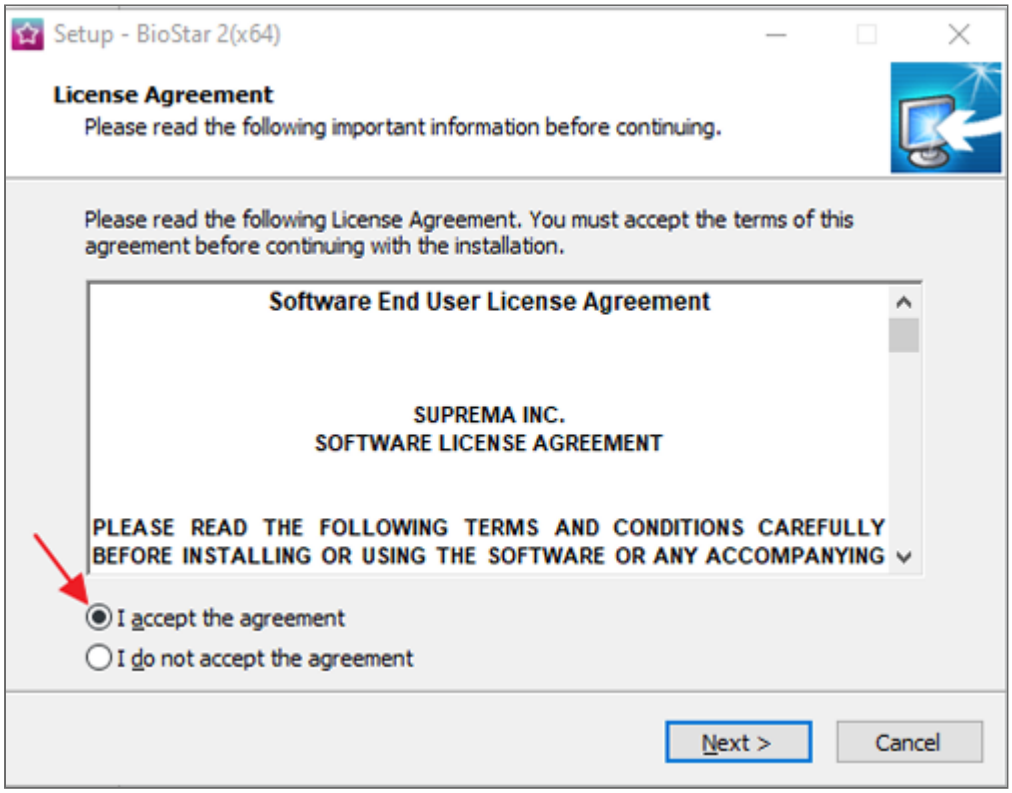
9. インストールが完了したら、**Finish** ボタンを押します。



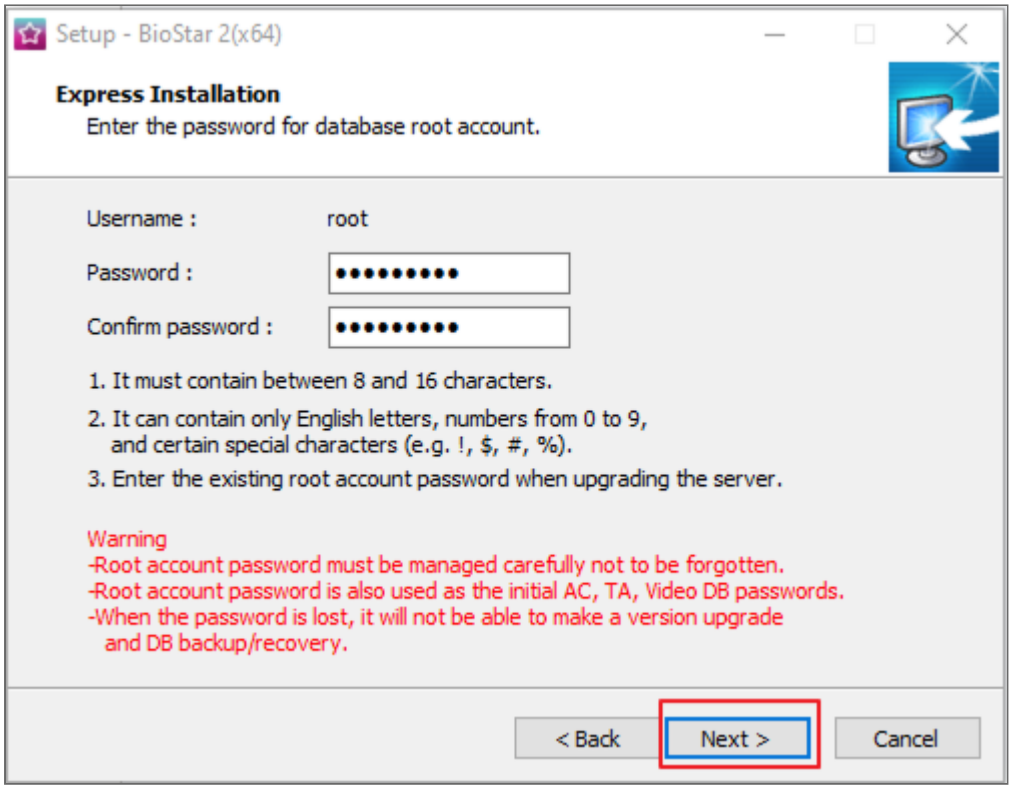
BioStar 2 のインストール

1. **BioStar 2.exe** を開き、言語を選択して使用許諾契約に同意し、**Next** を押します。

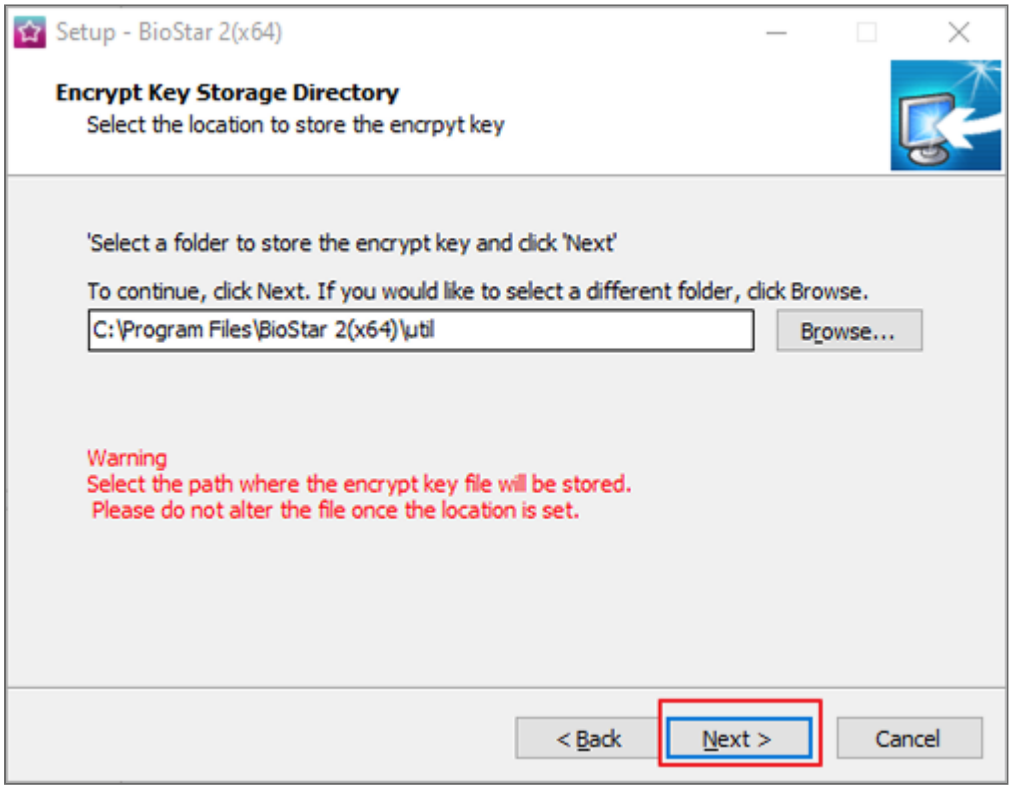
> **情報**
> BioStar 2 の最新バージョンをダウンロードします - ここをクリック。



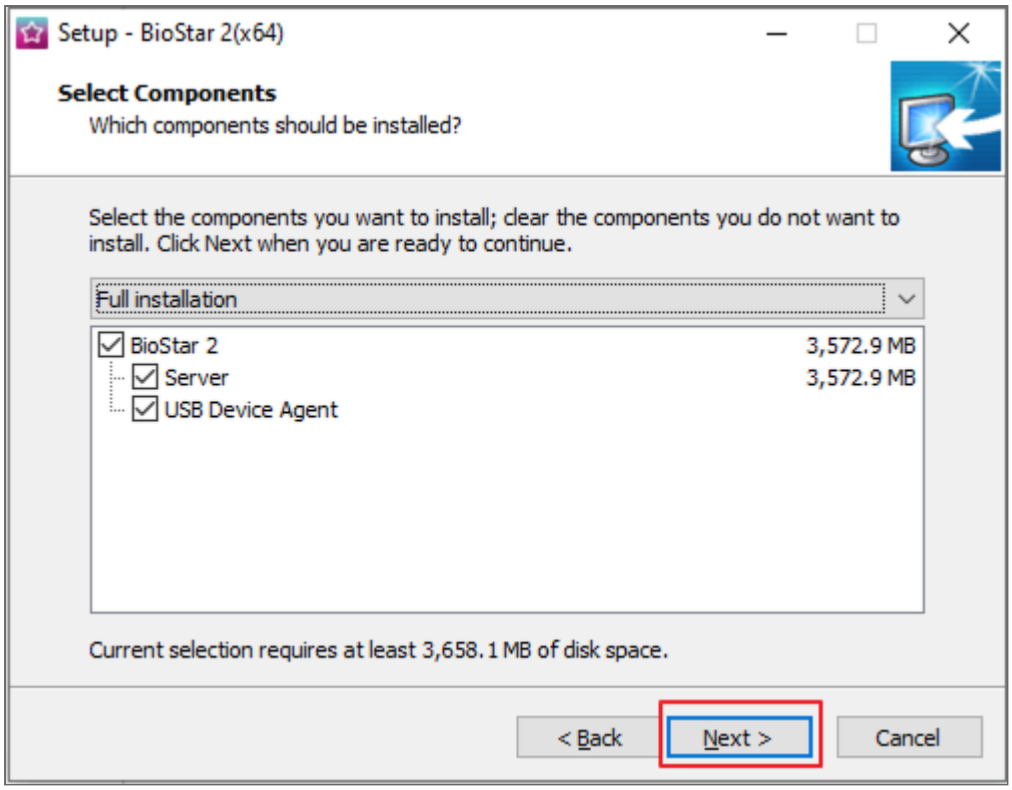
2. BioStar 2 の **Password** を入力し、**Next** ボタンを押します。



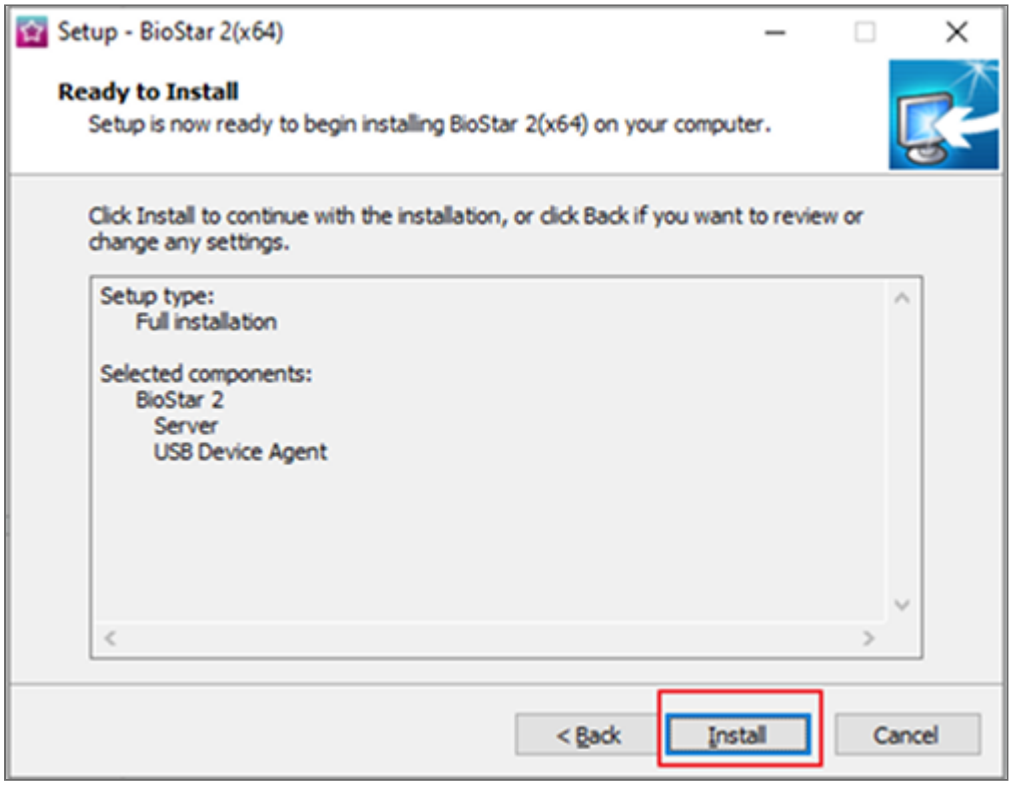
3. **Express** インストールを選択し、BioStar 2 のパスワードを再入力します。
4. 場所を選択して続行します。



5. コンポーネント選択画面が表示されるまで **Next** ボタンを押します。 両方のオプションをチェックして、**Next** ボタンを押します。

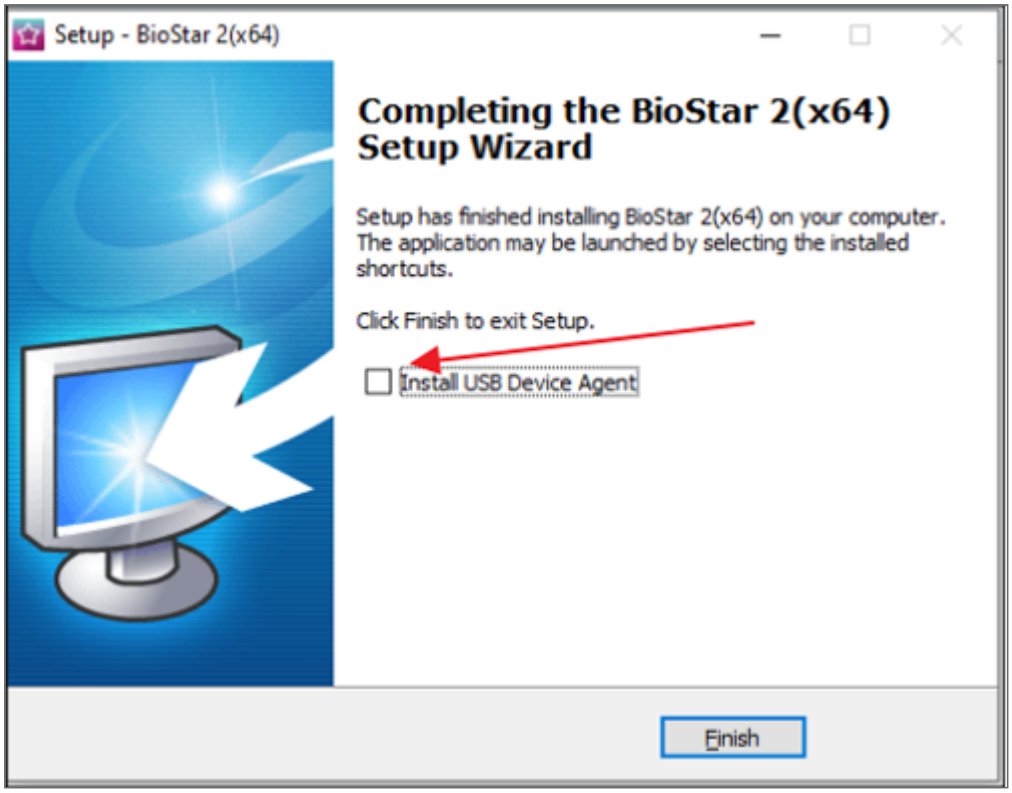


6. **Install** ボタンを押してインストールを開始します。



7. Install USB Device Agent のチェックボックスを**オフにして Finish** ボタンを押すと、BioStar 2 のインストールが完了します。

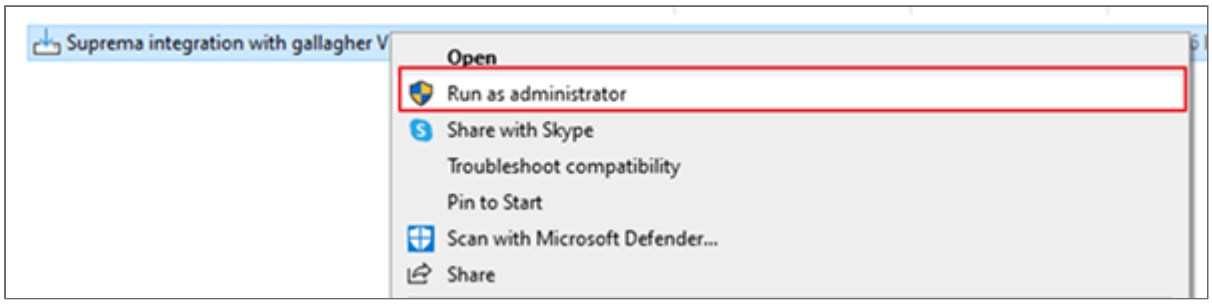
> **情報**
> USB デバイスを使用する場合は、Install USB Device Agent を**チェック**してください。



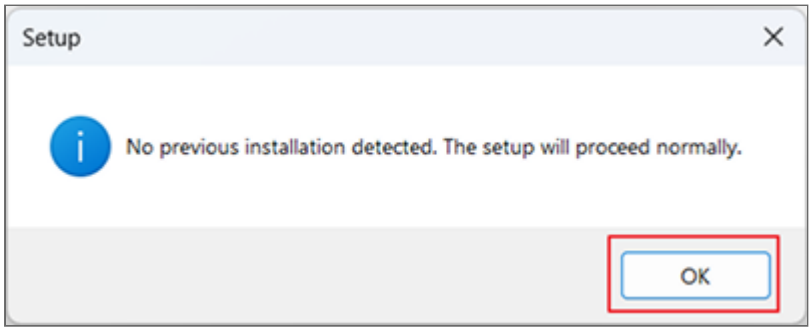
ミドルウェアの前提条件

> **情報**
>
> - Suprema Integration with Gallagher2.0.zip を展開または実行する前に、ウイルス対策ソフトをオフにしてください。
> - 古いバージョンからアップグレードする場合は、トラブルシューティングガイドで解決方法を確認してください。

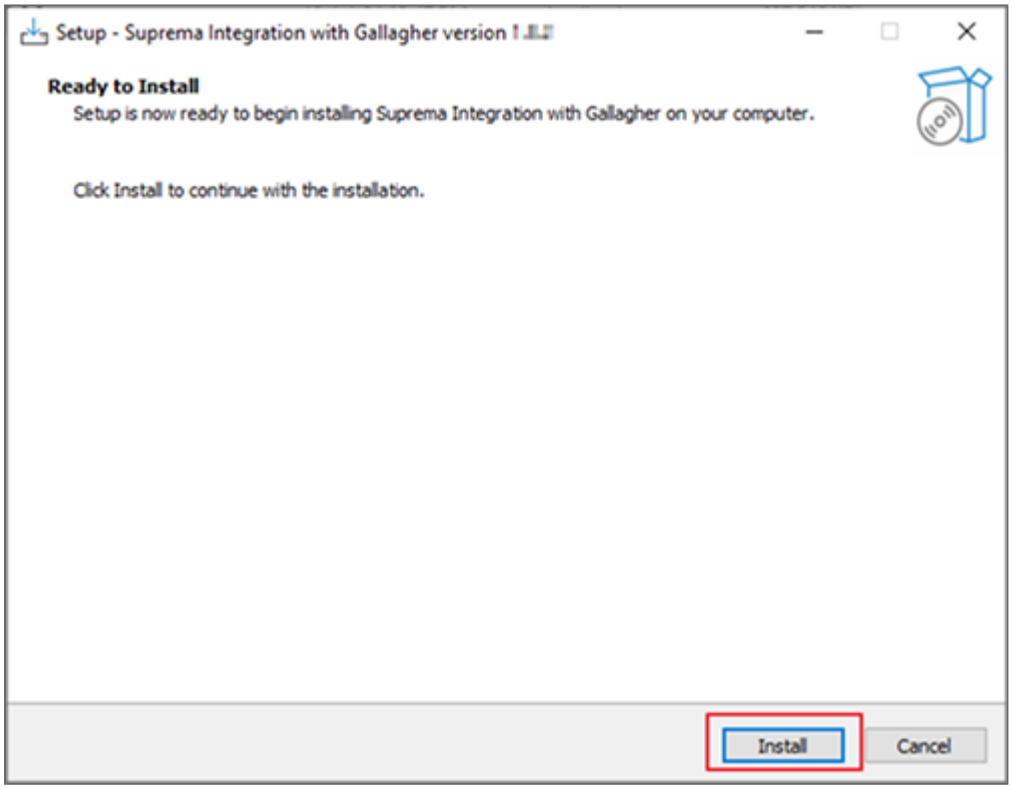
1. Suprema Integration with Gallagher 2.0 フォルダー内で、Suprema Integration with Gallagher 2.0 ファイルを管理者として実行する必要があります。 これにより、OpenSSL、PostgreSQL、PgAdmin4、Node、 JS。 また、インテグレーションに必要な証明書を設定します。



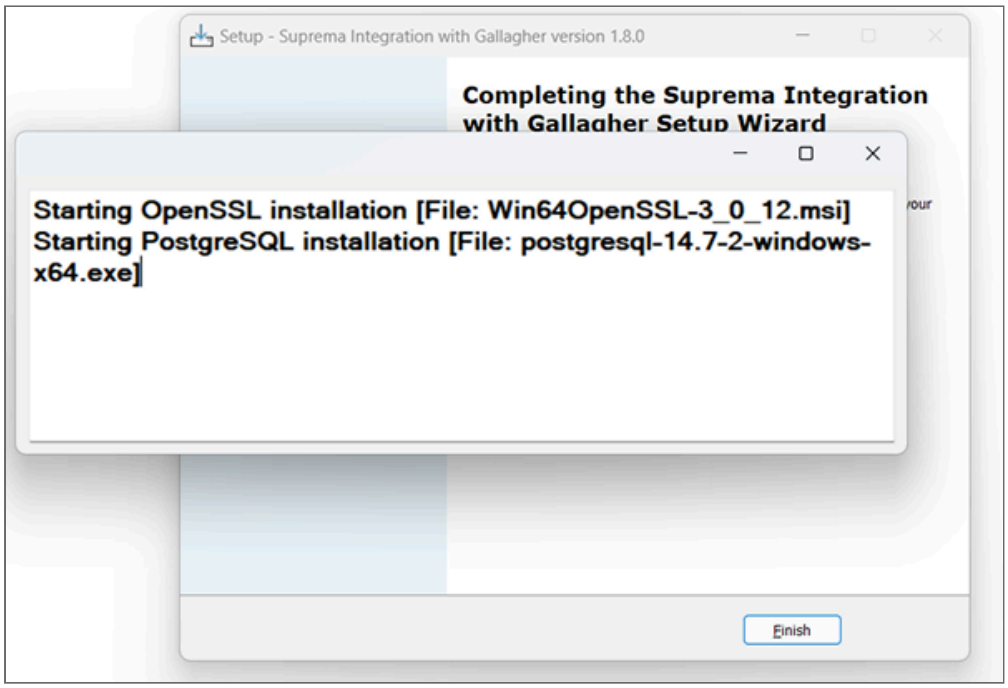
2. 不明な発行元からの許可を求められたら、**Yes** を押します。
3. **OK** を押します。



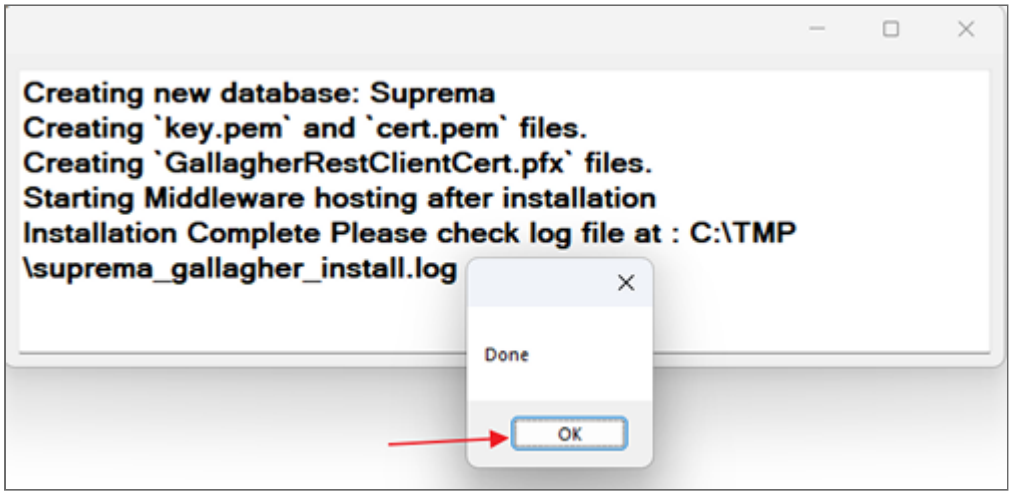
4. ソフトウェアをインストールできる状態になったら、**Install** を押します。



5. 前提条件のインストールが開始され、ソフトウェアは自動的にインストールされます。

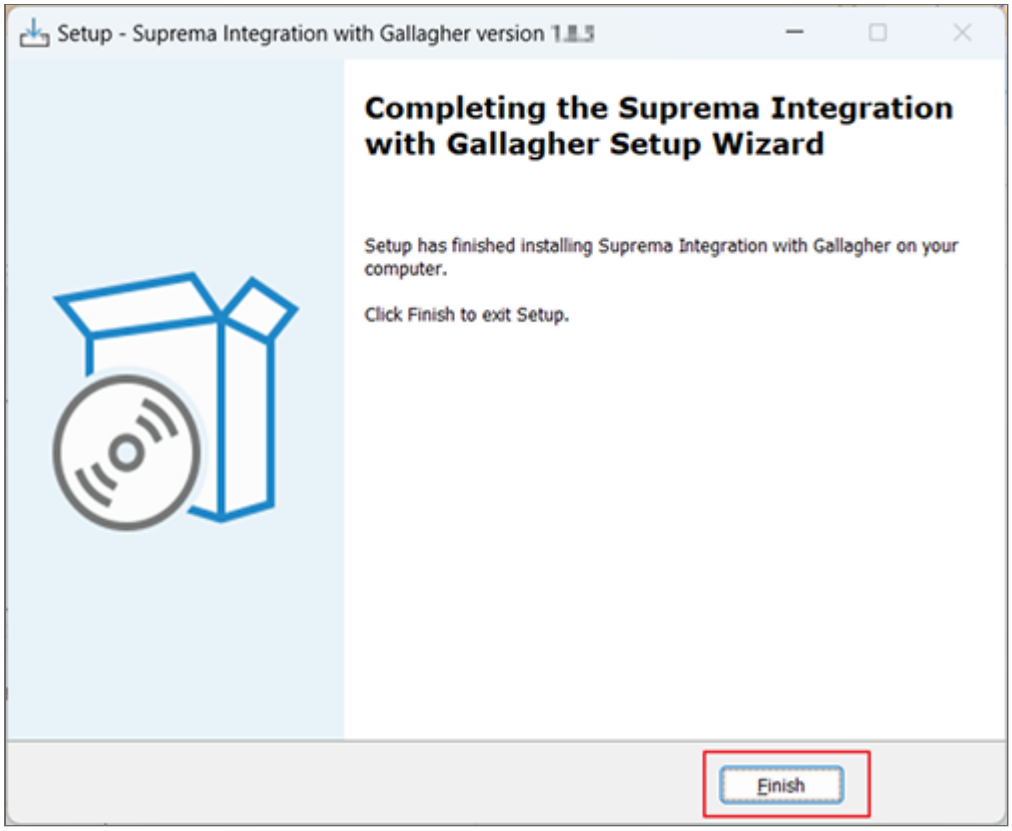


6. 下のポップアップで **OK** を押します。



7. 前提条件のインストールが完了したら、**Finish** を押します。

> **情報**
> ミドルウェアをインストールした後は、システムを 1 回再起動してください。

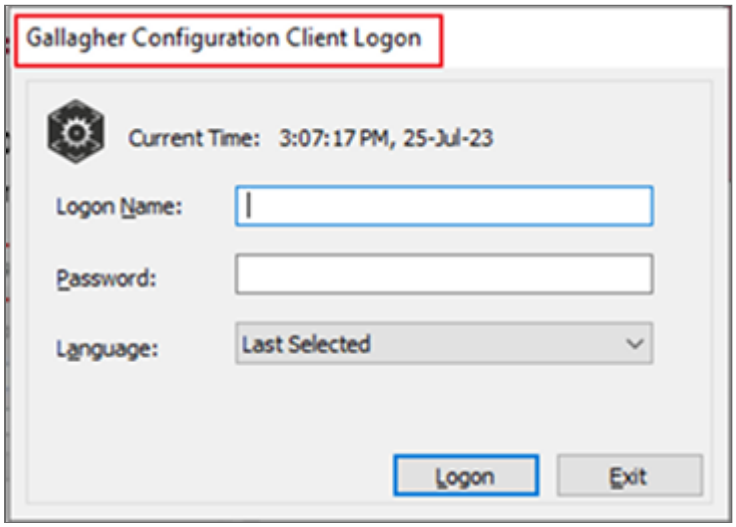


設定

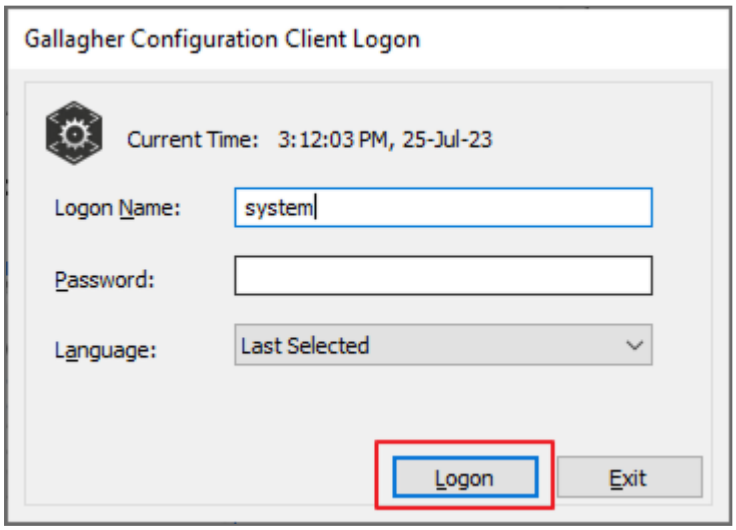
Gallagher Command Centre の設定

Gallagher Configuration Client へのログオン

1. クリックしてスタートメニューを開き、Configuration Client を開きます。



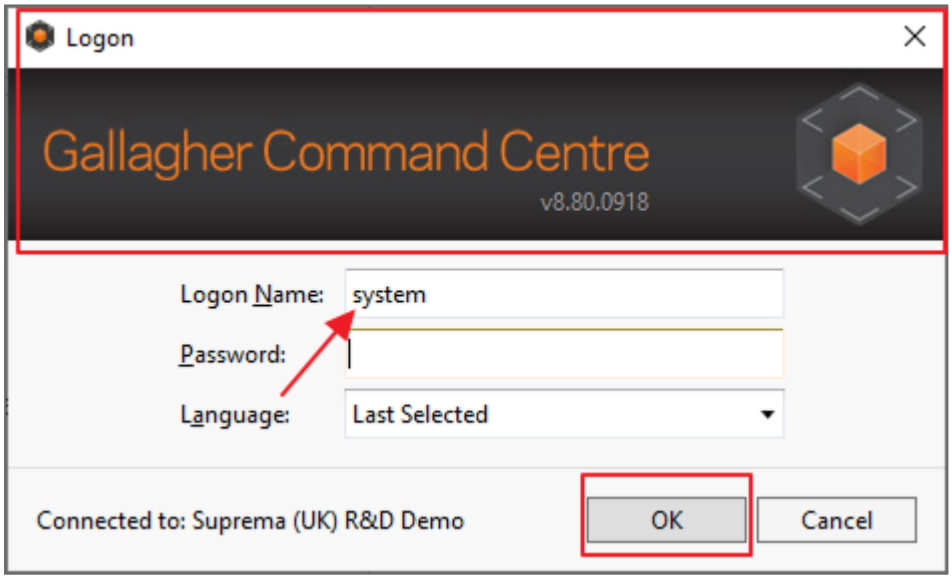
2. ログオン名を **system** に設定し、パスワードは **none** にして、**Logon** ボタンを **押します**。



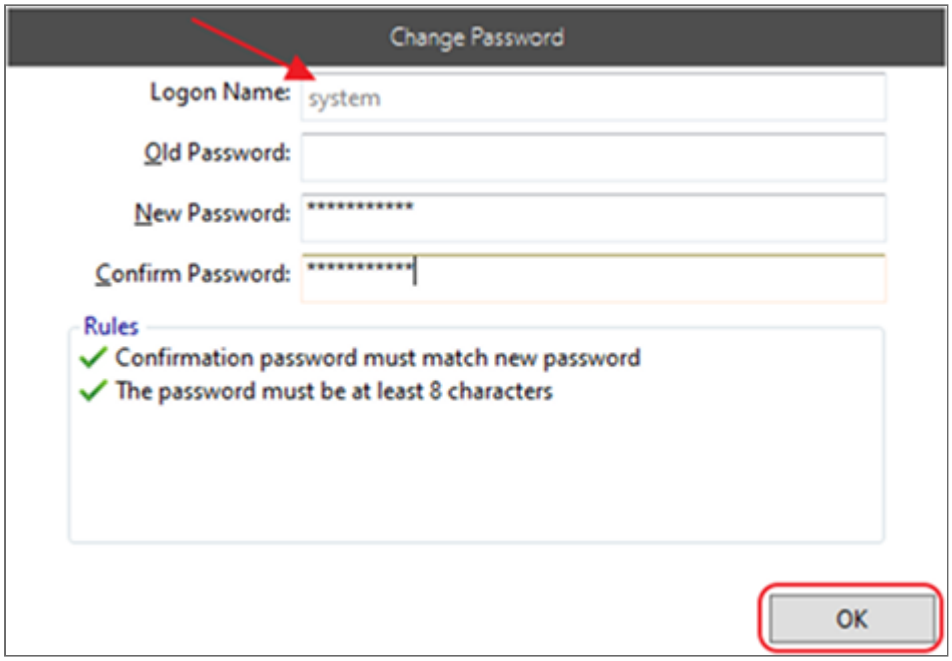
Gallagher Command Centre

> **情報**
> Gallagher APIキーを生成する手順。

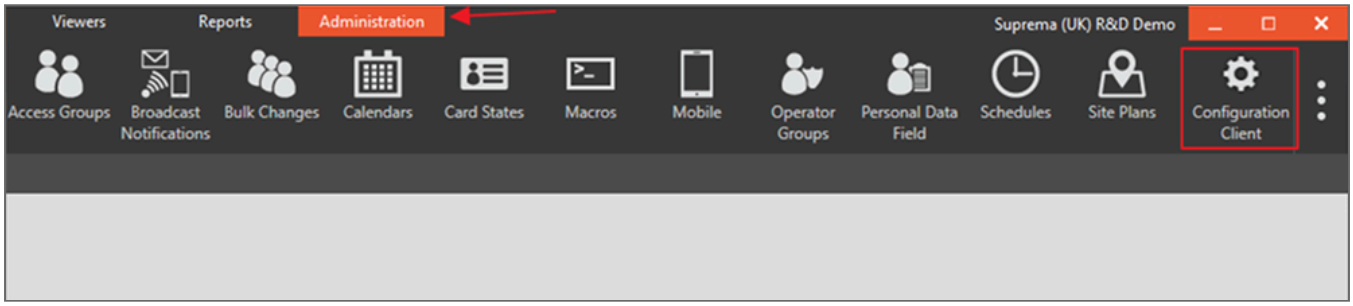
1. Gallagher Command Centre を開き、ログオン名を system に設定して、**OK** ボタンを押します。



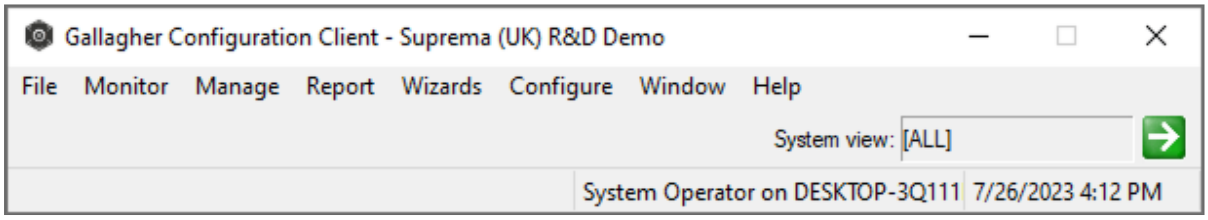
2. ログオン名を **system** に設定し、Gallagher Command Centre のパスワードを設定して、**OK** を押します。



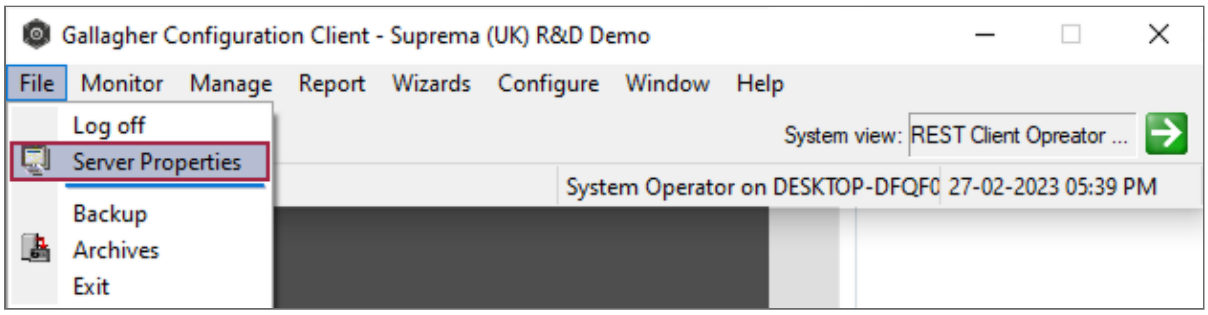
3. 次に、左上隅の Administration に移動し、**Configuration Client** を選択します。ウィンドウが開きます。



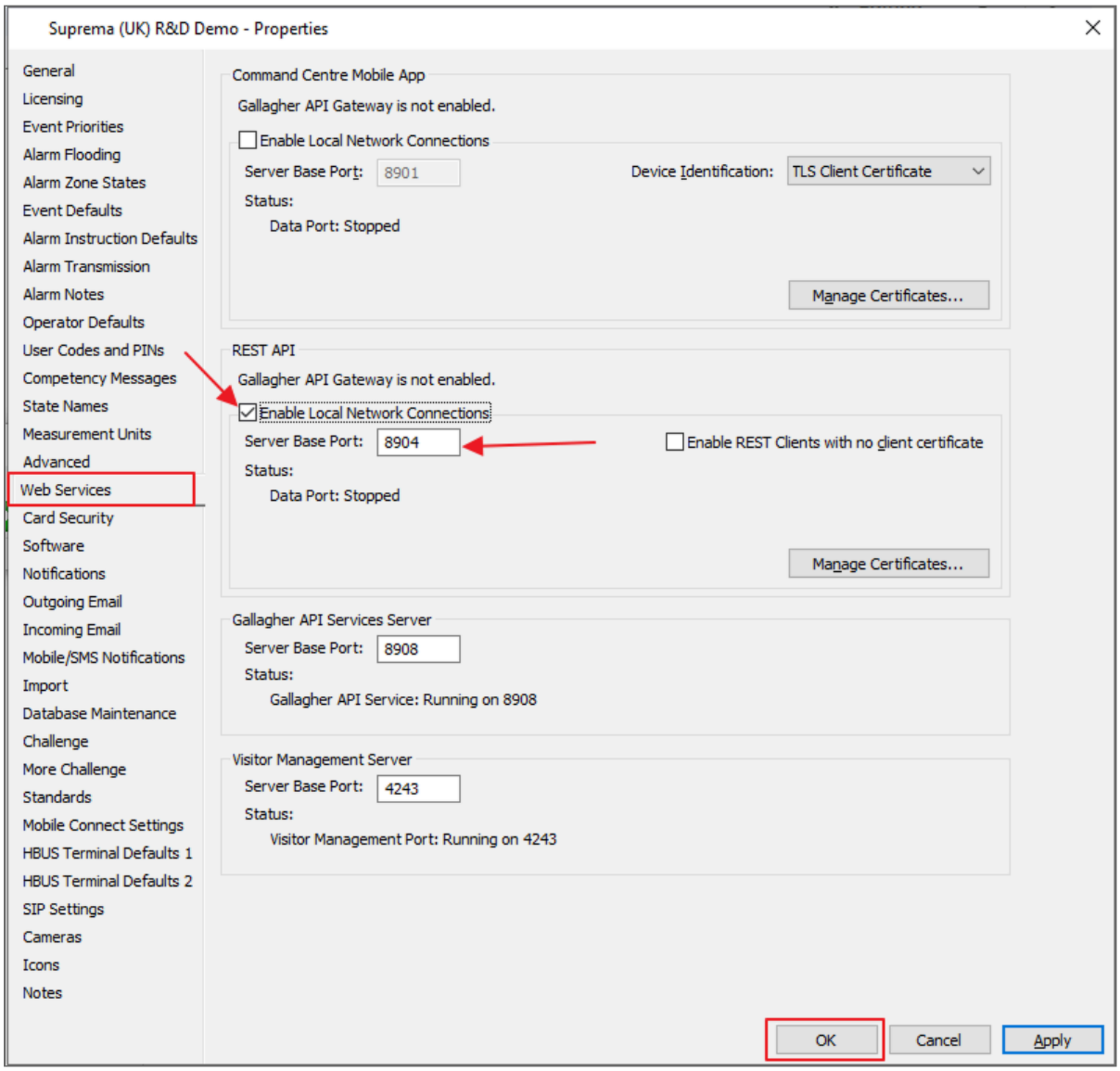
4. 下のタブが開きます。



5. サーバー設定を構成するには、**File** を選択 → **Server Properties**。

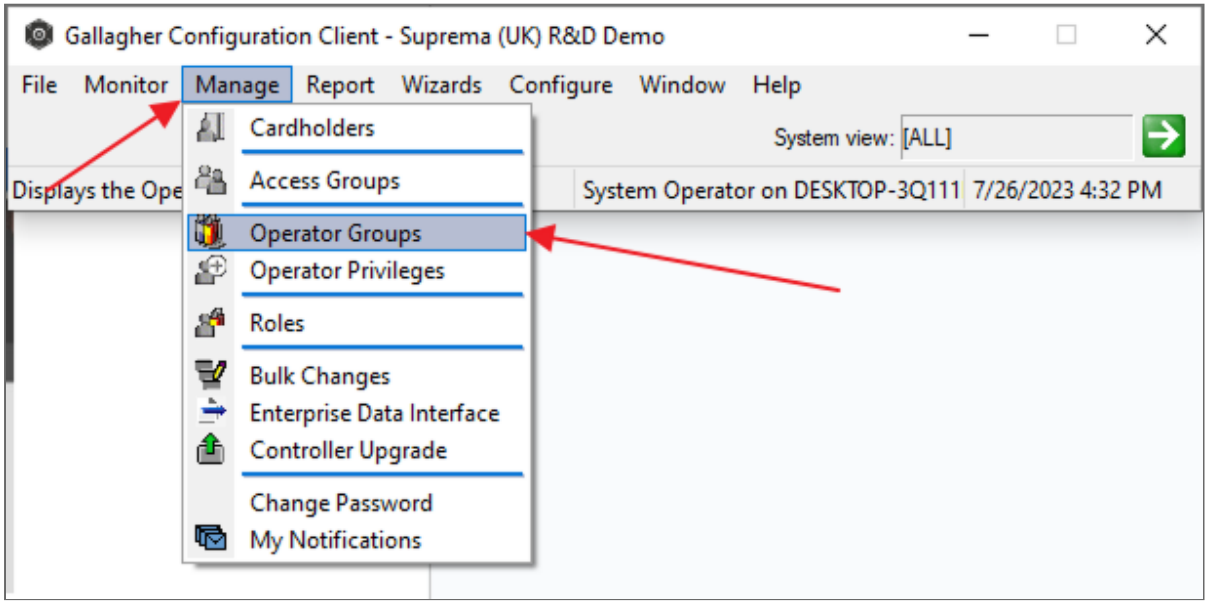


6. 新しいウィンドウが開きます。**Web Services** に移動し、**REST API** セクションでローカルネットワーク接続を有効にします。サーバーポートを **8904** に設定し、Enable REST client with no client certificate のチェックを外して、**OK** ボタンを押します。

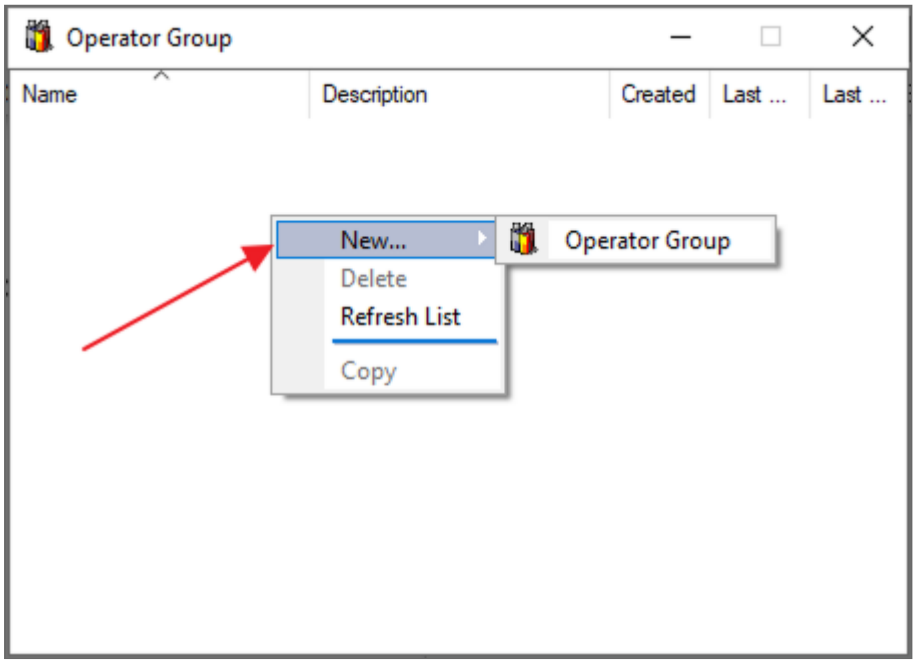


7. **Gallagher Client に切り替えます。**

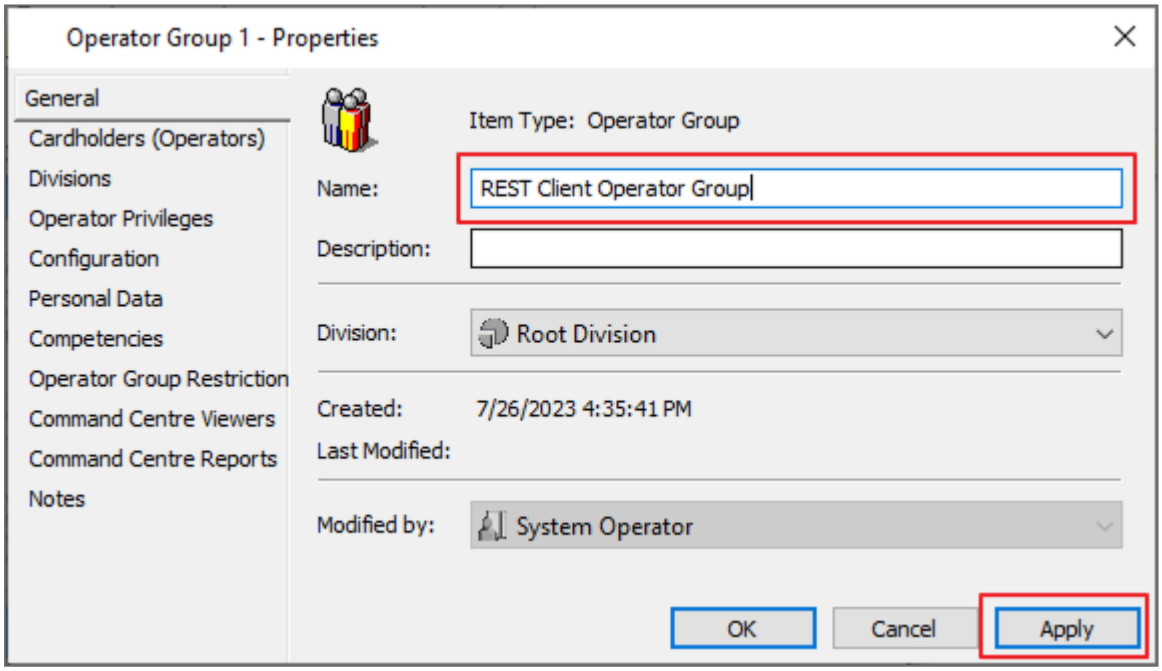
   Manage をクリックします。 ドロップダウンで **Operator Groups を選択します。**



8. Operator Group ウィンドウが開きます。**右クリック**して **New → Operator Group** を選択します。

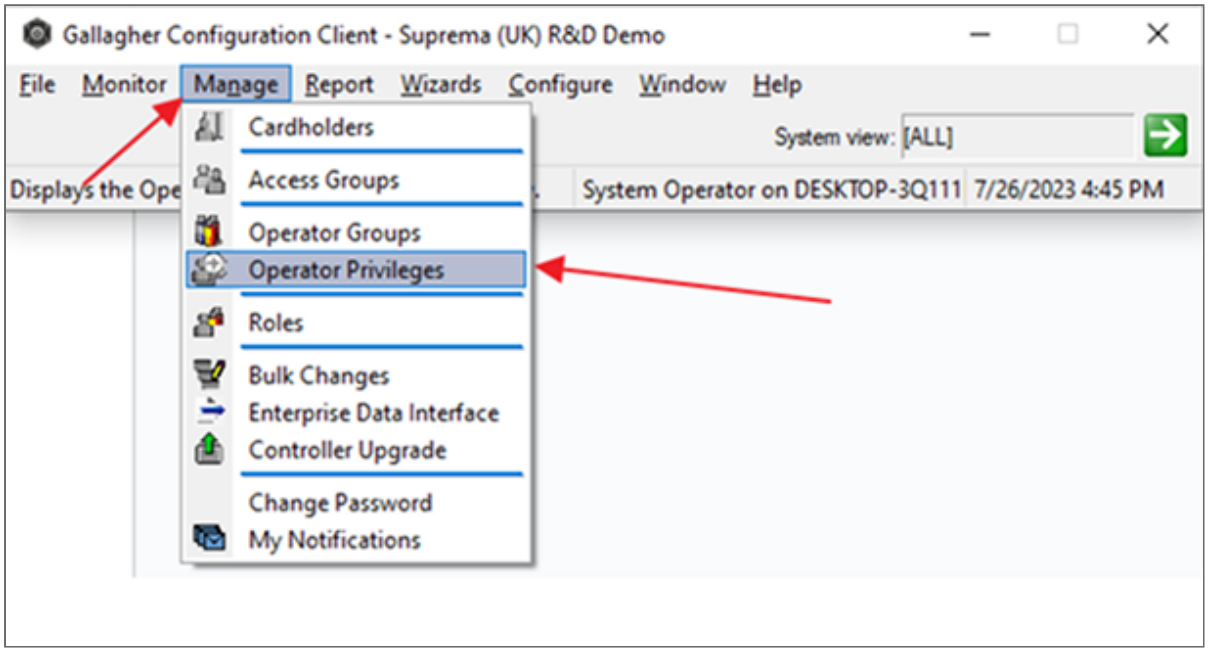


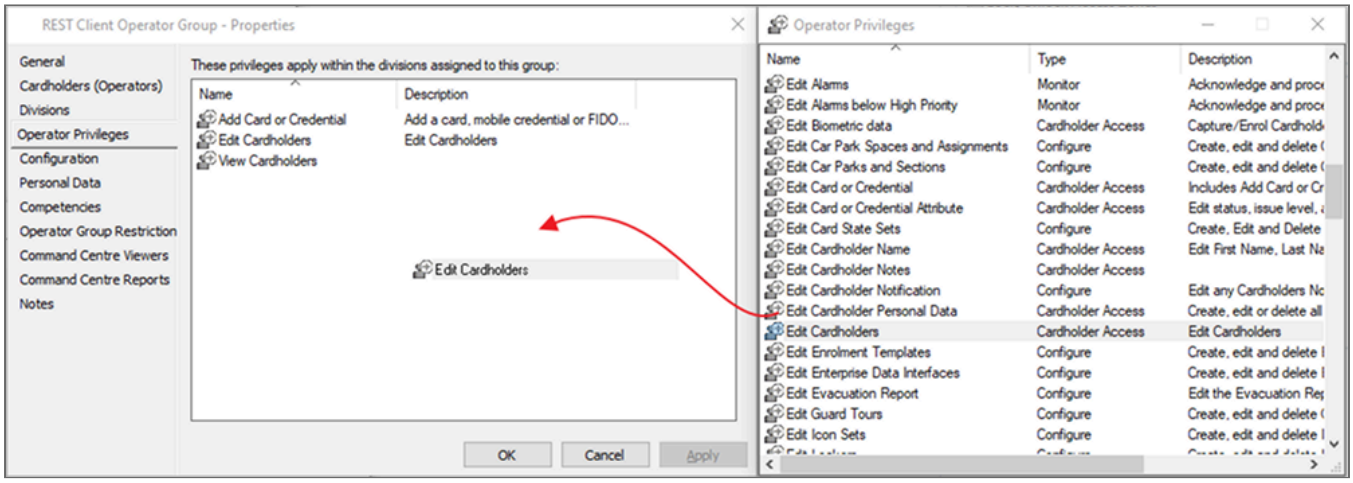
9. 一般設定で、名前を **REST Client Operator Group** に設定します。 次に **Apply** をクリックします。



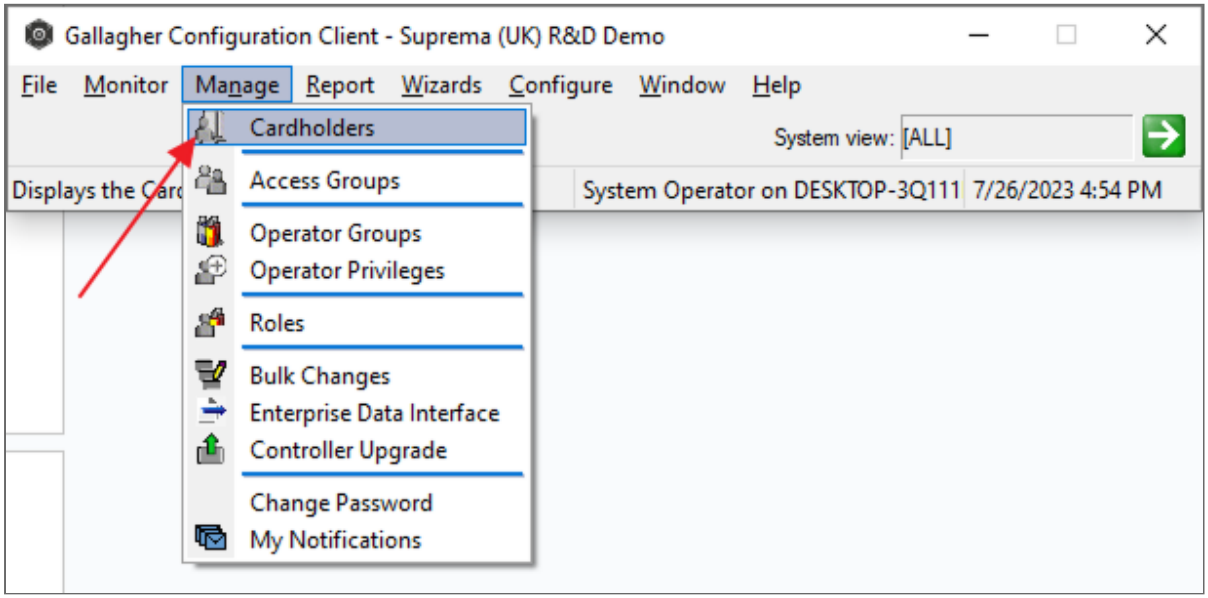
10. 次に、Operator group で **Operator Privileges** 設定を選択し、Gallagher configuration client ウィンドウの Manage → Operator Privileges に移動します。 次に**ドラッグ＆ドロップ**します。

Operator Group に 3 つの権限（Add Card or Credential、Edit Cardholders、View Cardholders）を operator privileges から operator group に追加し、**OK** ボタンを**押して**、operator privileges を**閉じます**。

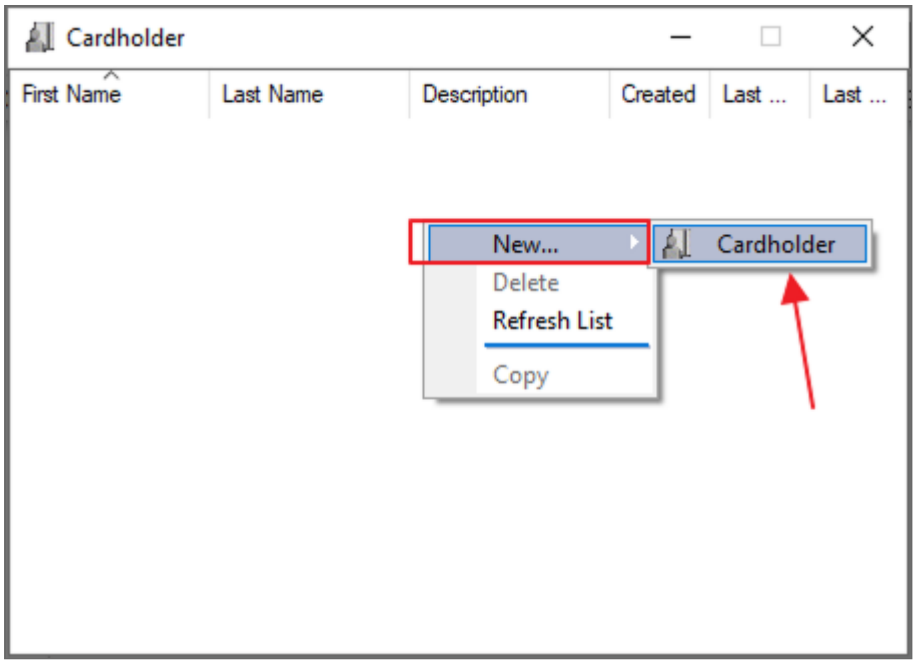




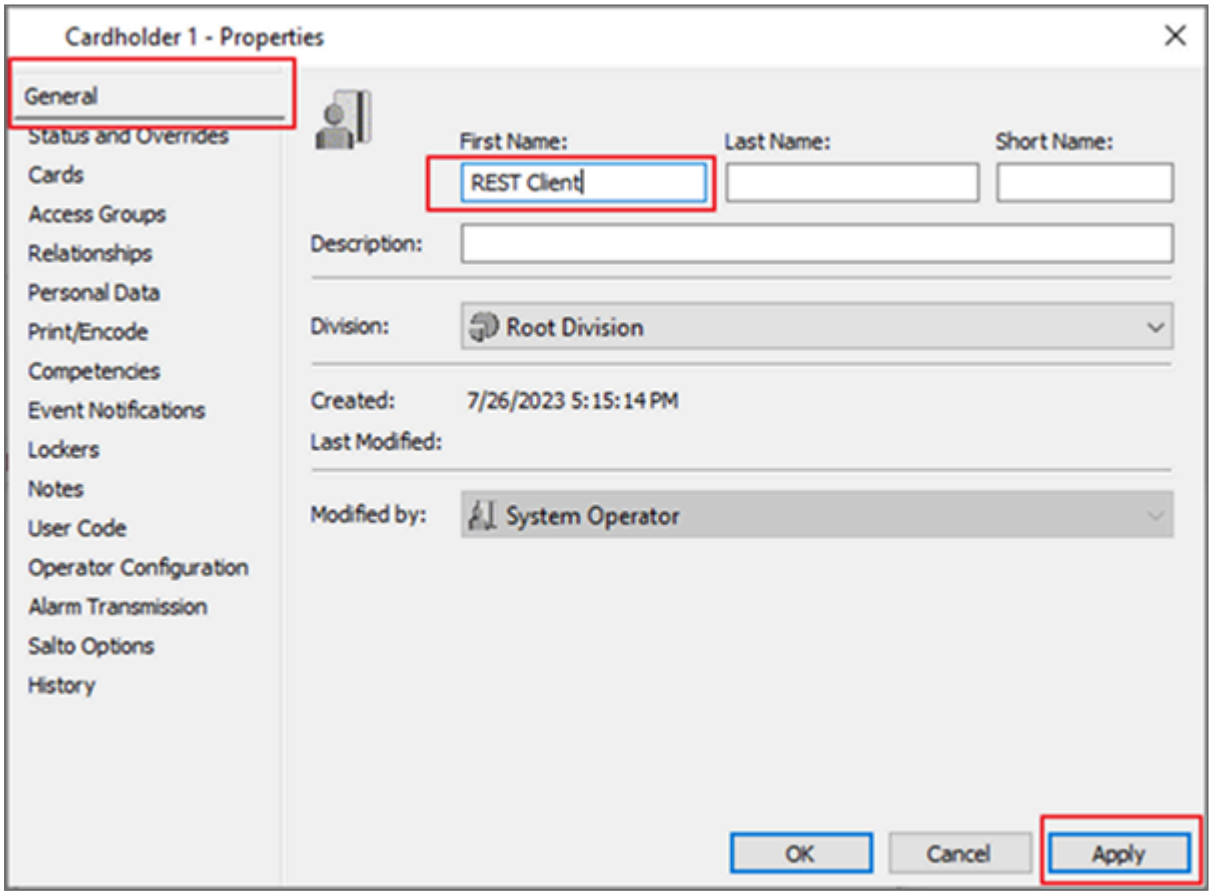
11. Configuration Client に移動し、**Cardholders** を選択します。



12. **右クリック**して New → Cardholder を選択します。

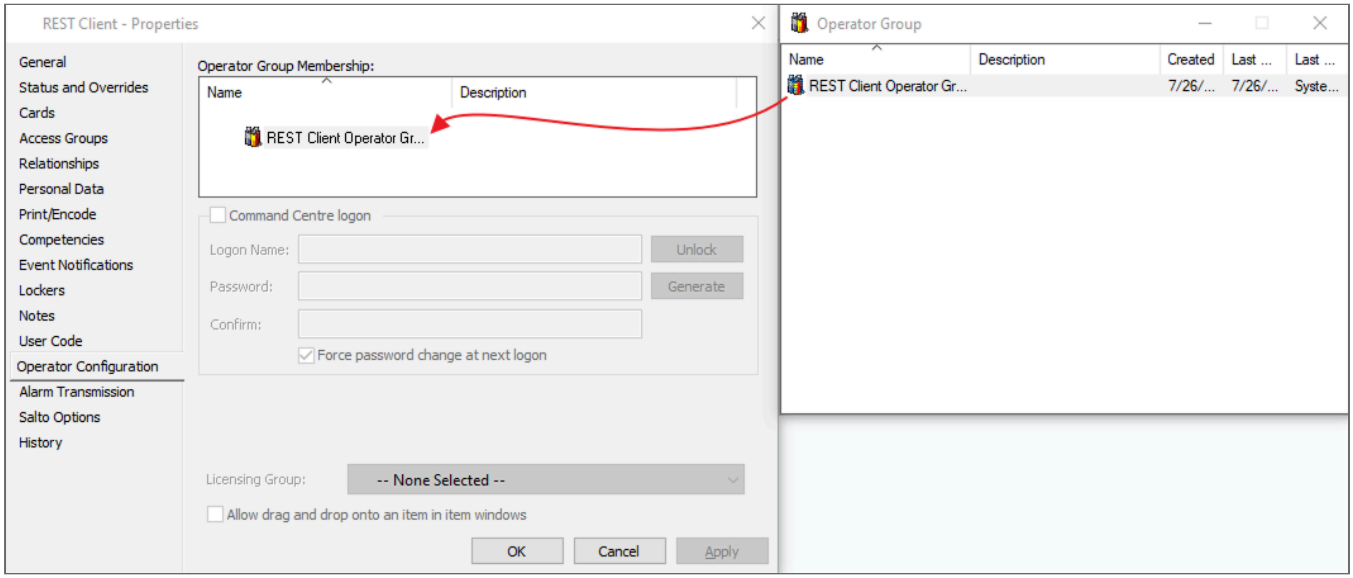


13. 一般設定で First Name を **REST Client** にし、**Apply** を押します。

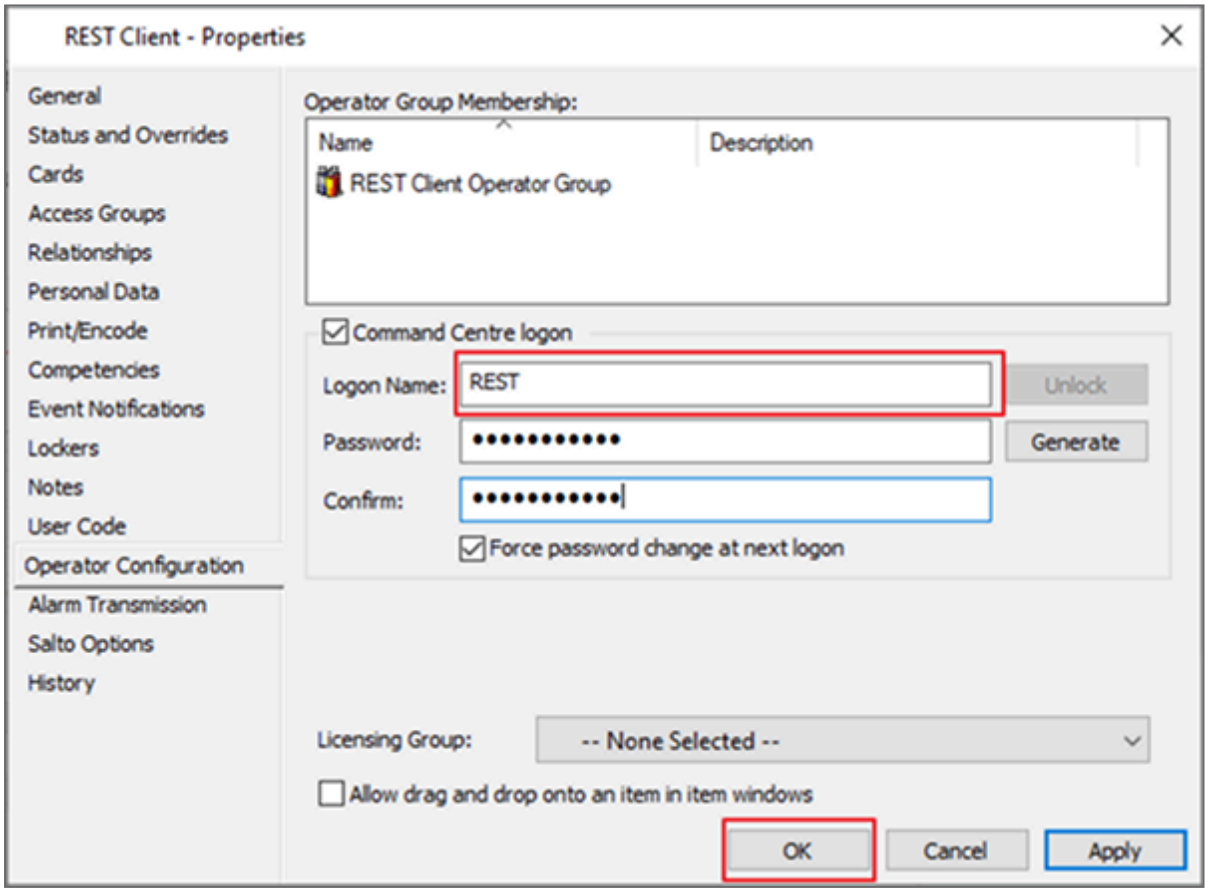


14. REST Client Properties の左側にある **Operator Configuration** タブを**クリック**します。 作成した REST Client operator group を Operator Group から Operator Group Membership に**ドラッグ & ドロップ**します。

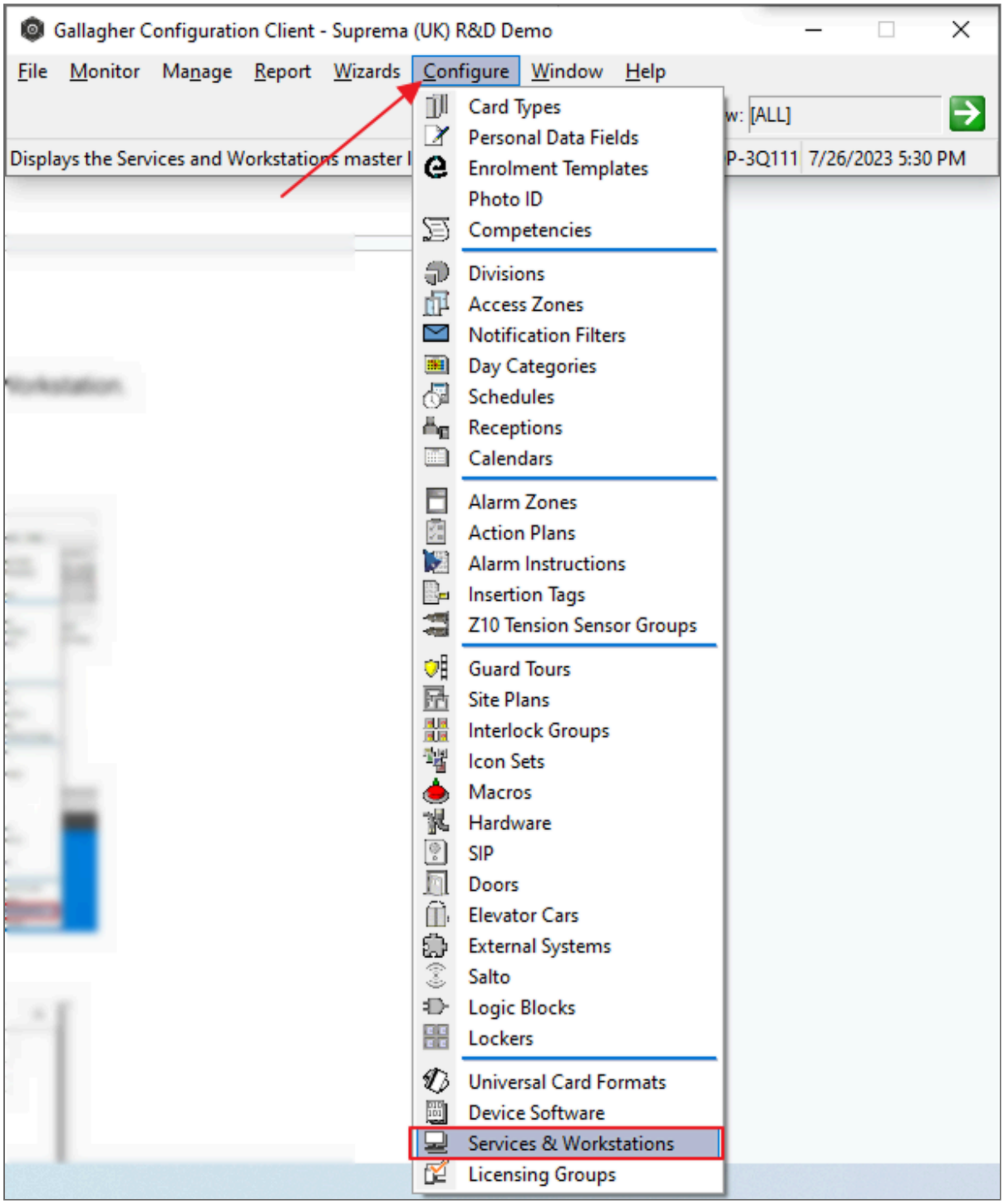
15. REST Client Operator Group を Operator Group Membership に**ドラッグ**します。次の画像のようにします。



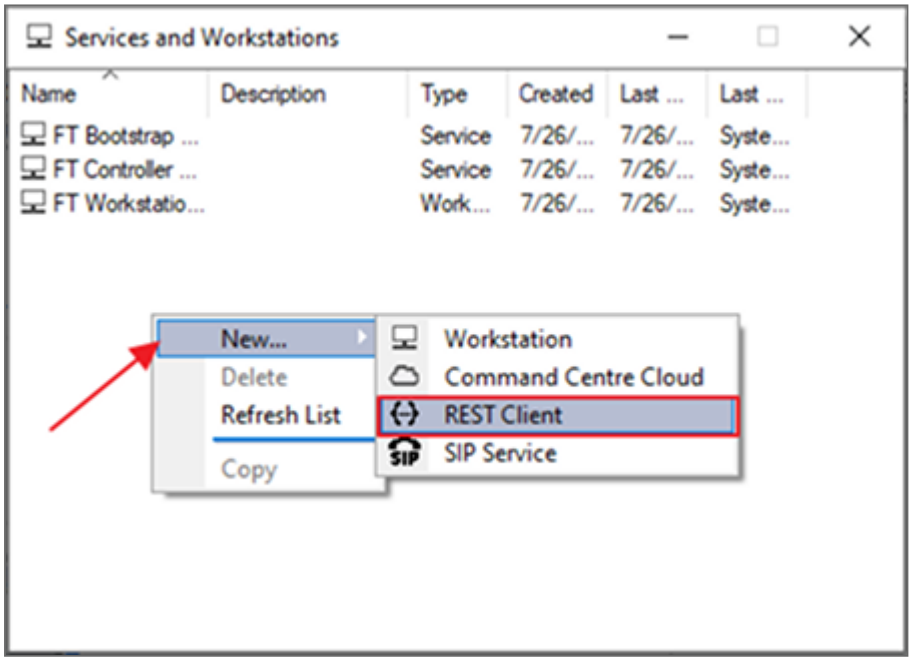
16. ログオン名を **REST** に**設定**し、パスワードは Gallagher Command Centre で設定したものと同じにします。 **OK** をクリックし、Operator Group ウィンドウも**閉じます**。



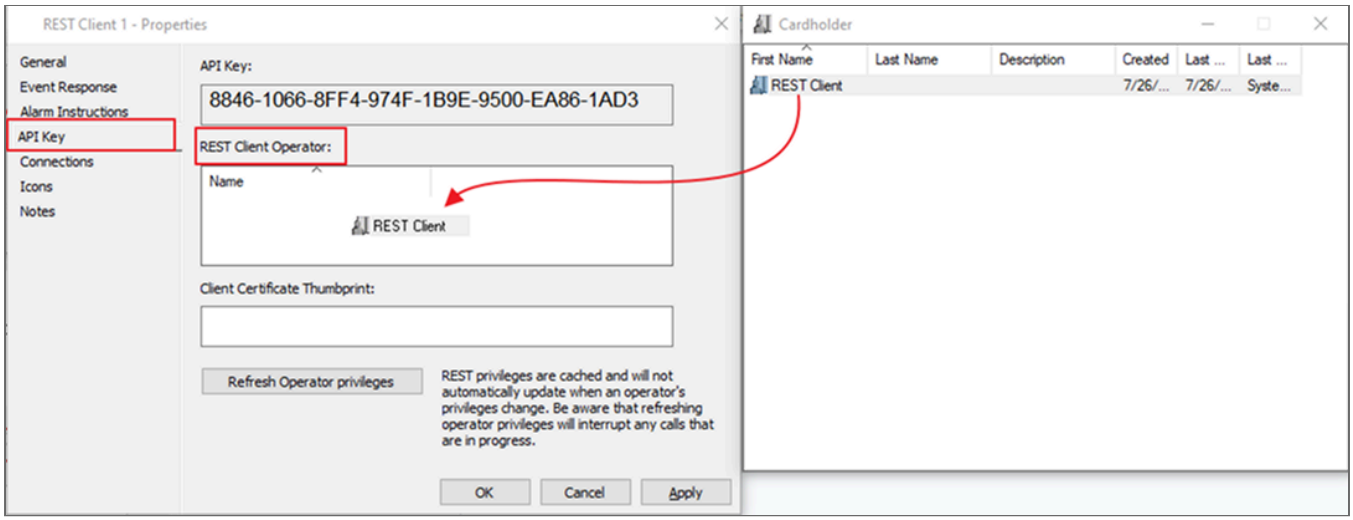
17. Configuration Client で Configure → Services & Workstations に移動します。



18. 次に**右クリック**して New → REST Client を選択します。

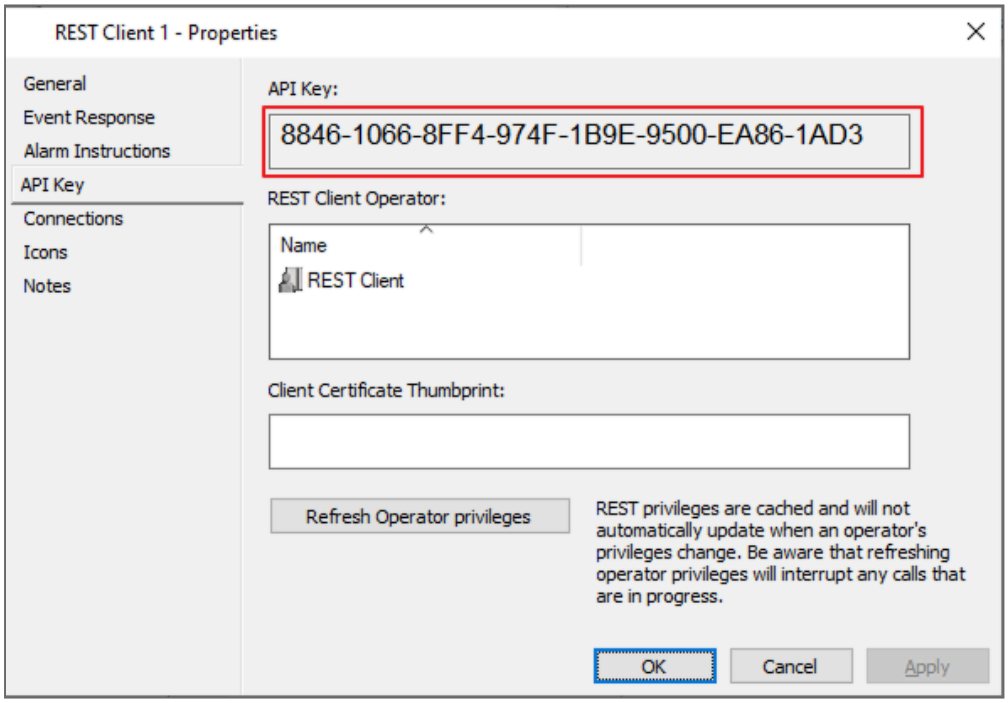


19. APIキー欄で、Cardholder から REST Client を REST Client Operator にドラッグ＆ドロップします。 **Apply** をクリックします。 Cardholder ウィンドウを閉じます。



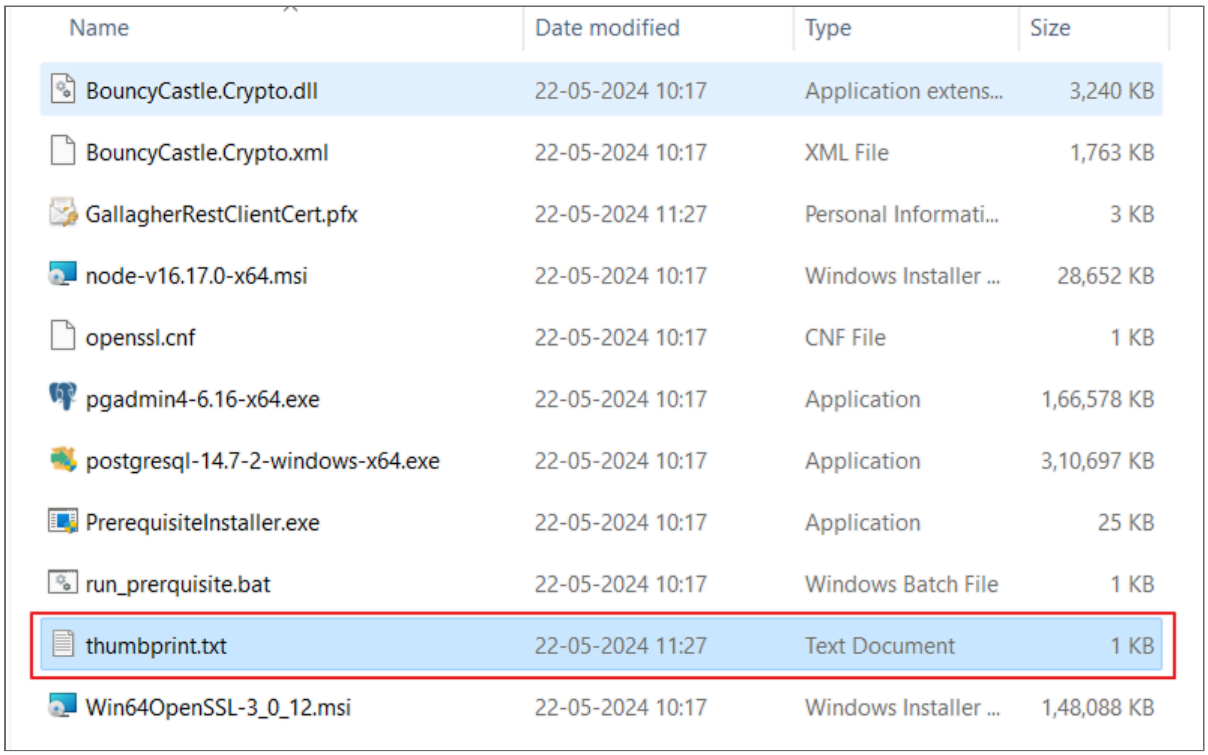
20. Gallagher APIキーは APIキー欄にあります。

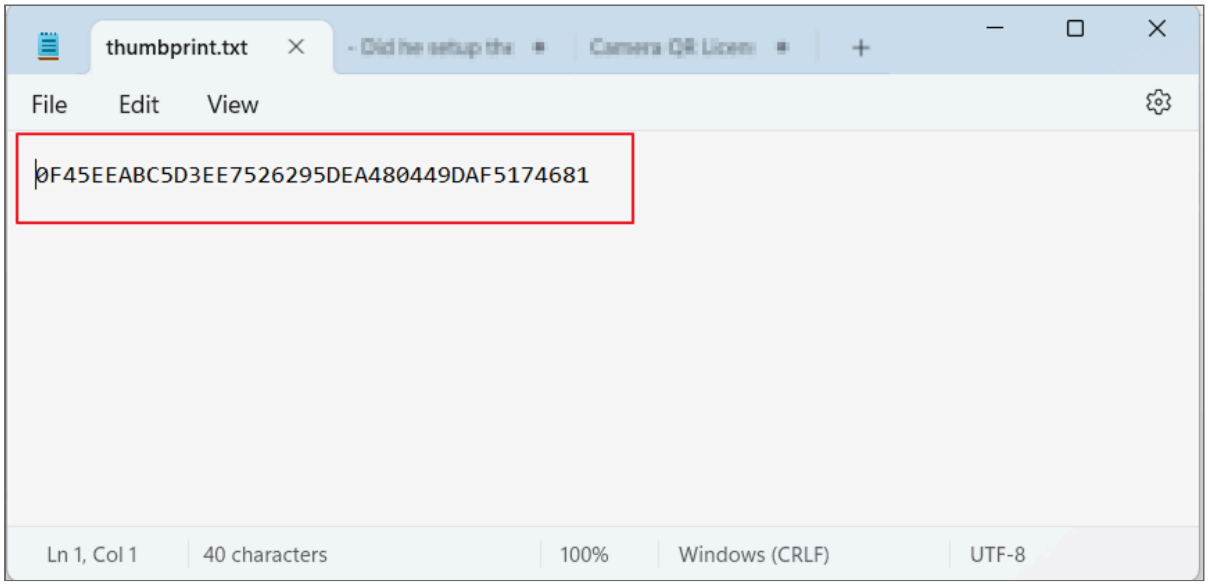
> **情報**
> Gallagher APIキーは安全な場所に保存してください。



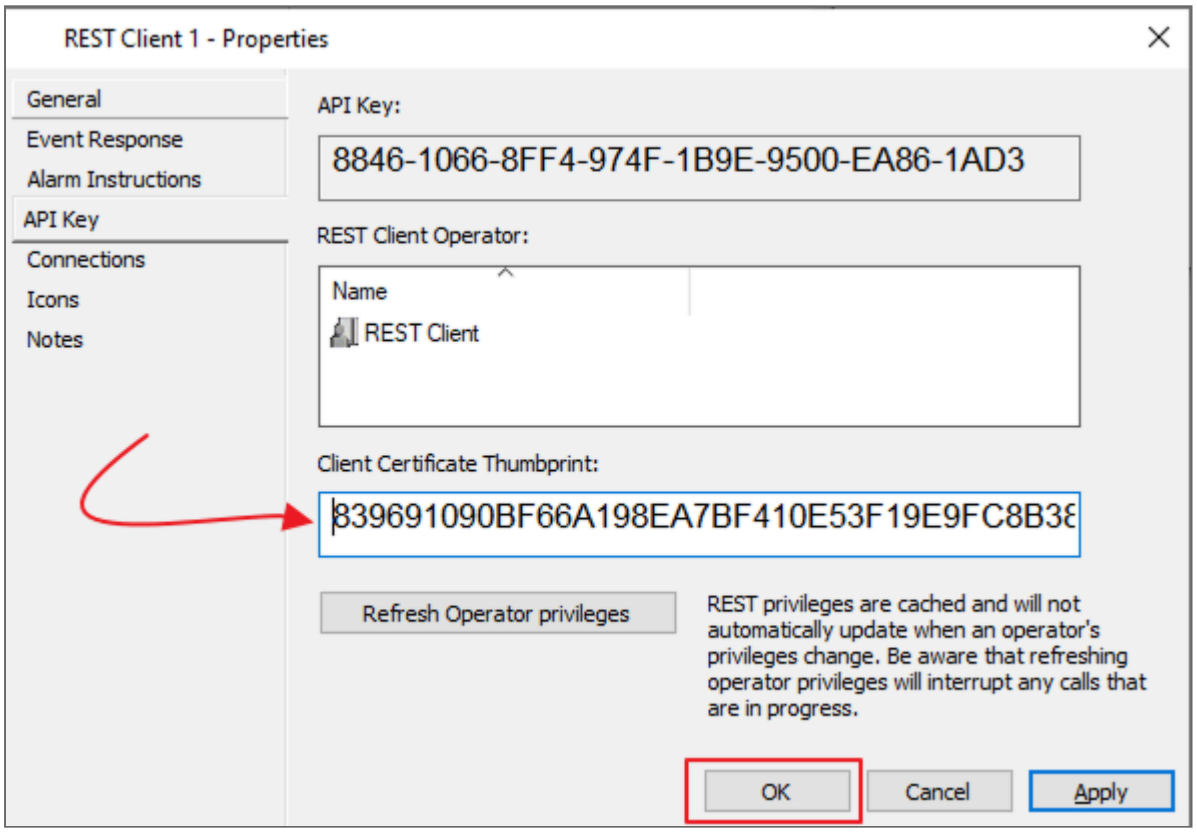
21. thumbprint を取得するには、C:\Program Files\Suprema Integration with Gallagher\Prerequisites に移動し、thumbprint ファイルを開いて、その中の thumbprint の値をコピーします。

> **情報**
> thumbprint ファイルがない場合。 EXE ファイルの実行中に thumbprint が生成されない場合。





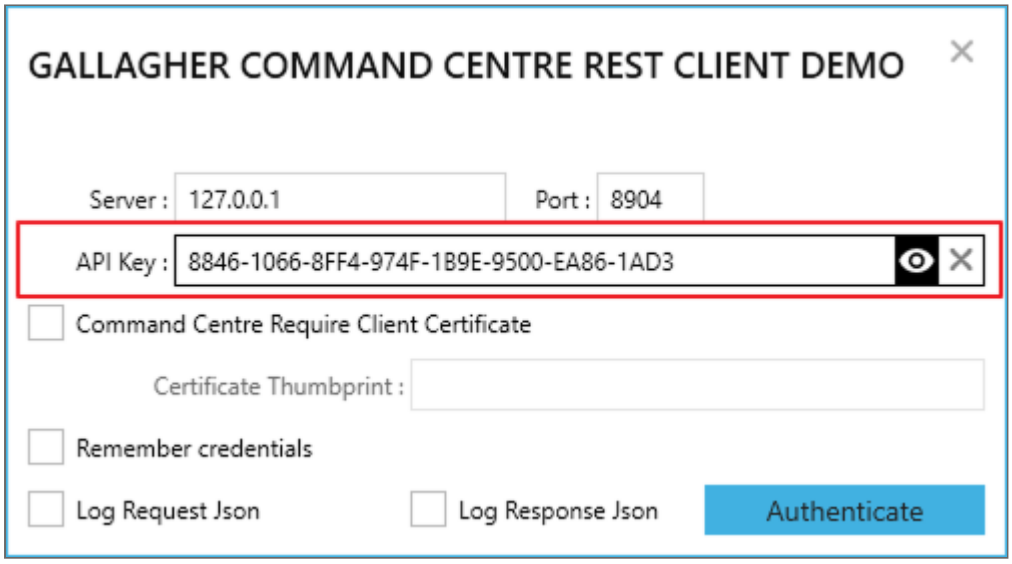
22. Thumbprint をコピーし、Client Certificate Thumbprint セクションに **Client Certificate Thumbprint key** を貼り付け、**OK** ボタンを押して、Services and Workstations も閉じます。



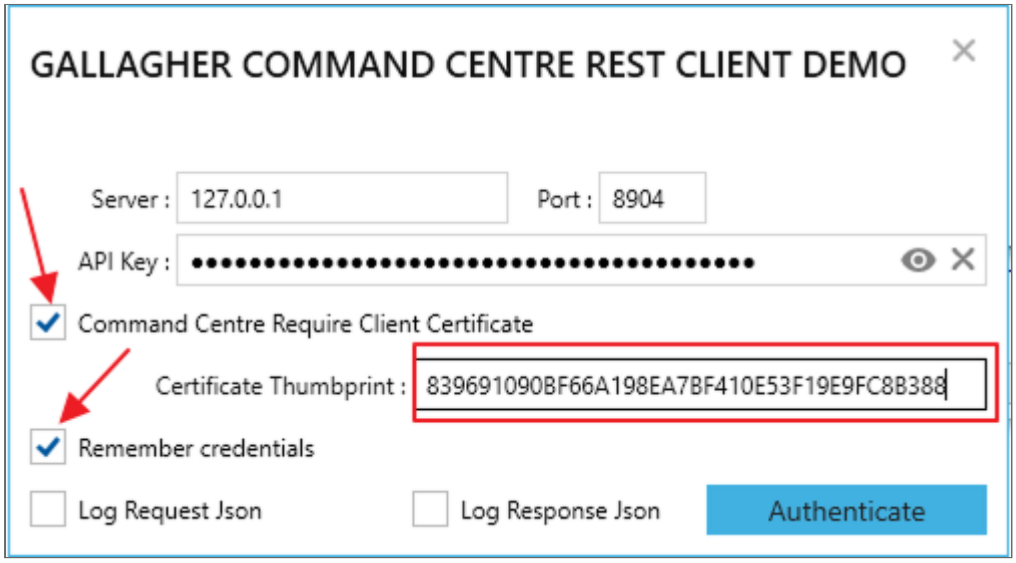
Gallagher APIキーを確認

1. Command Centre iso → utilities → REST API → RestClient_v8.60.072 → win-x64 → RestClientDemo に移動し、それをデスクトップに移動して、`RESTClientDemo.exe` を開きます。

2. 画像のとおり Gallagher APIキーを入力します。

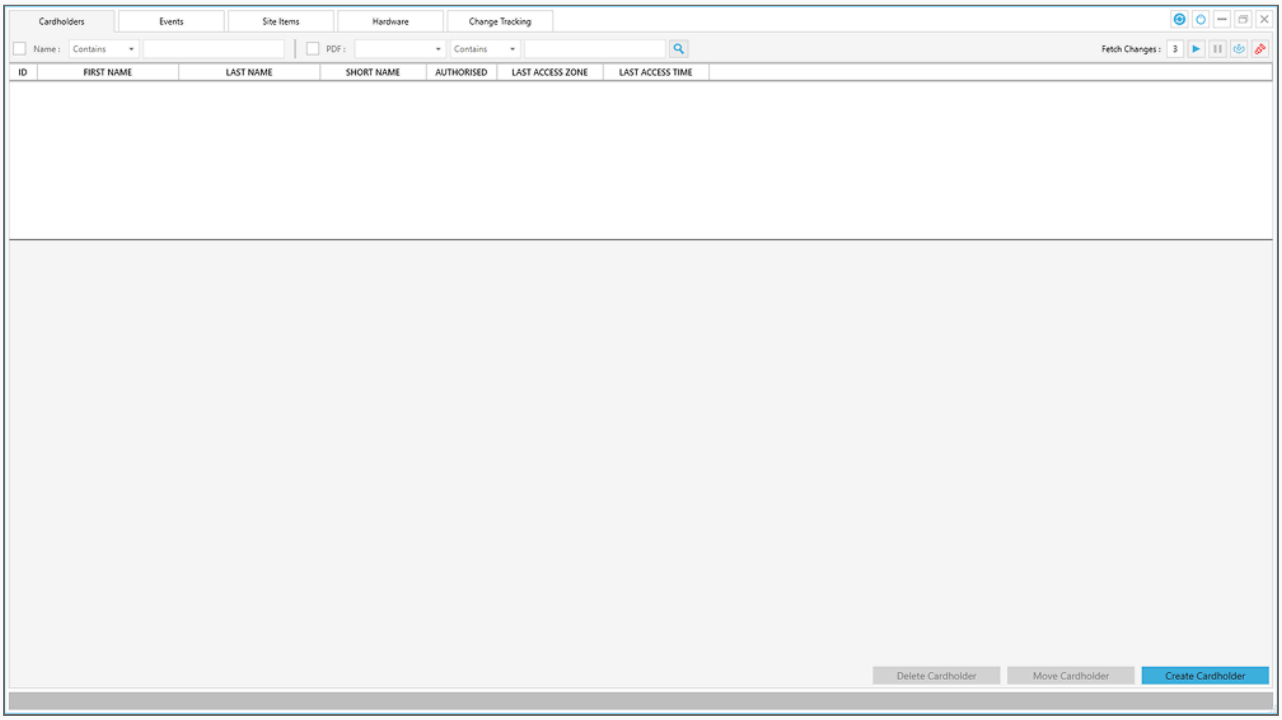


3. Command Centre Requirement Client Certificate にチェックし、Certificate Thumbprint を入力します。Remember credentials (Optional) にもチェックします。



情報

エラーがある場合は端末に表示され、問題がなければ下の画像のように新しい画面が開きます。 テスト後、このウィンドウを閉じます。



ハードウェア設定

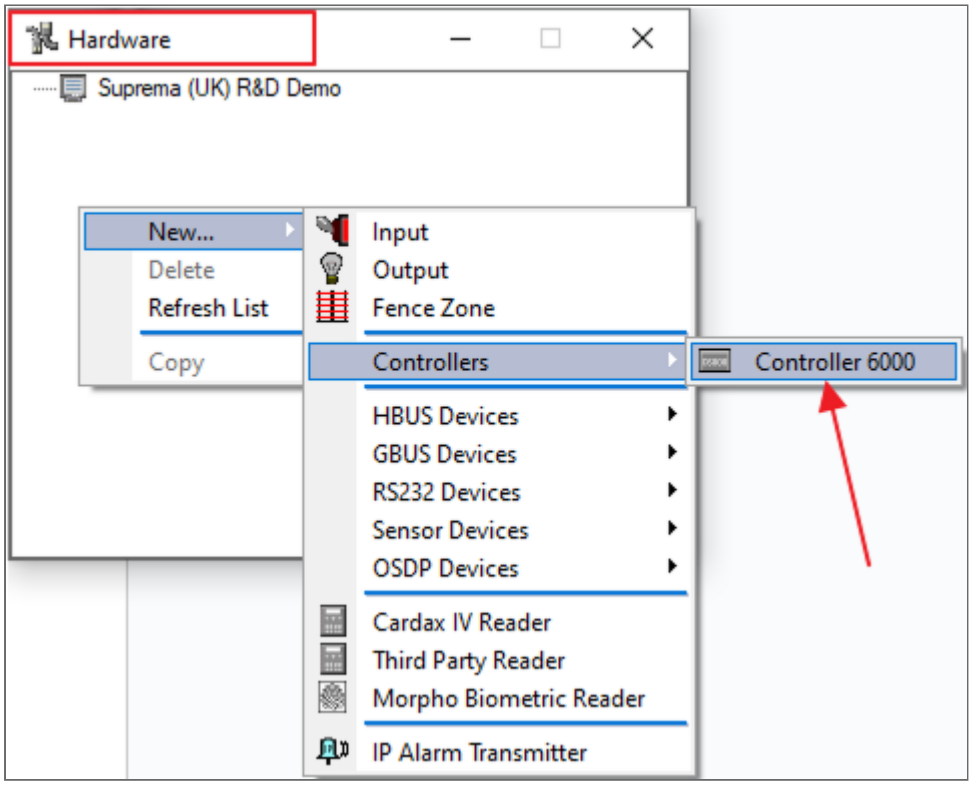
情報

- ハードウェアの設定が完了している場合は、BioStar 2 設定 に進みます。
- ここでは Controller 6000 を例として使用します。別のコントローラーを使用する場合は、それに合わせて手順を実行してください。

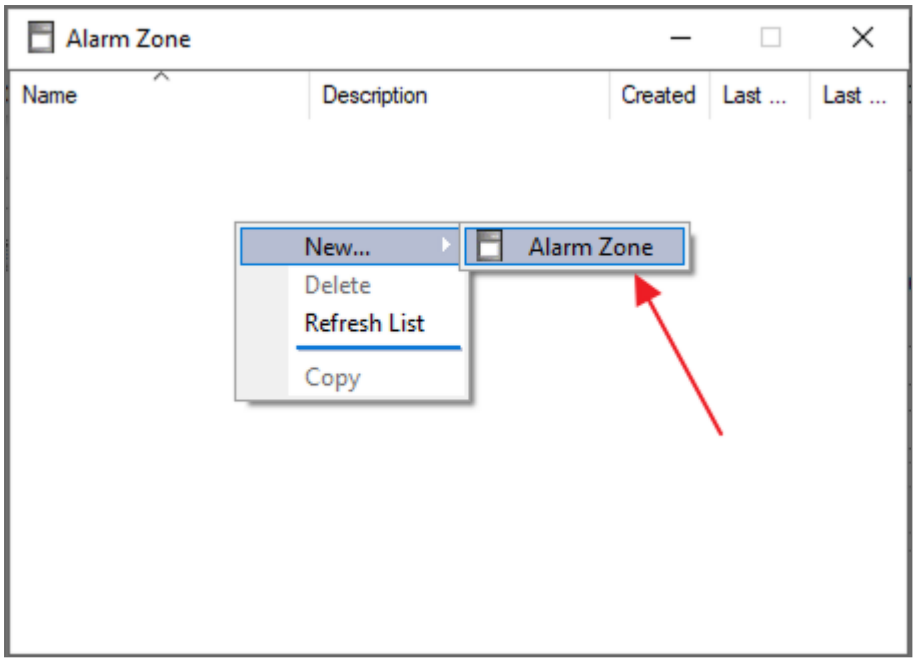
1. まず、Gallagher コントローラーに接続する Controller 6000（または使用中の別のコントローラー）を作成します。

   Gallagher Configuration Client ウィンドウを開き、Configure → Hardware に移動します。

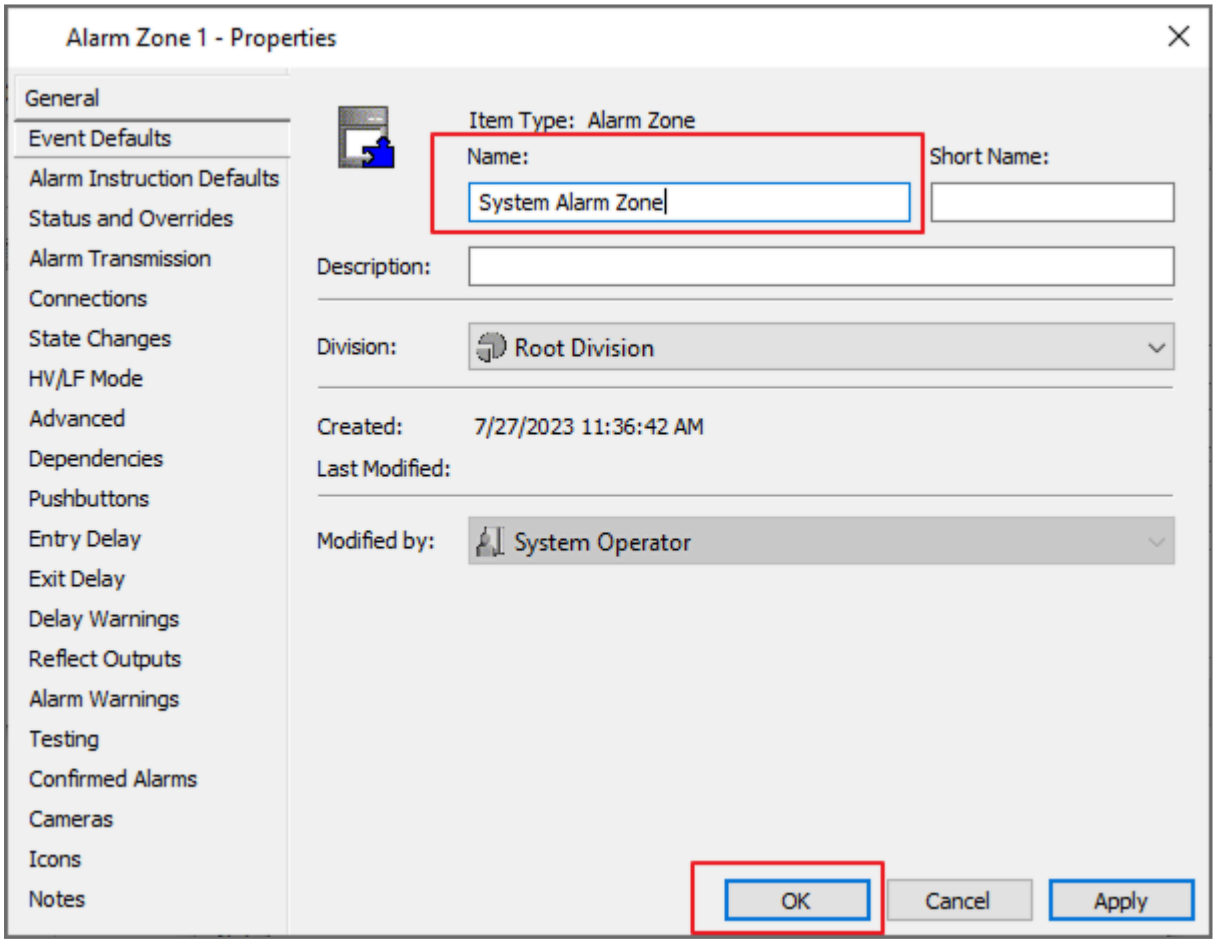
2. ハードウェアウィンドウで**右クリック**し、**New** → **Controllers** → **Controller 6000**（別のコントローラーを使用している場合はここに表示されます）を選び、**Apply** を押します。 これでハードウェアにコントローラーが作成されます。



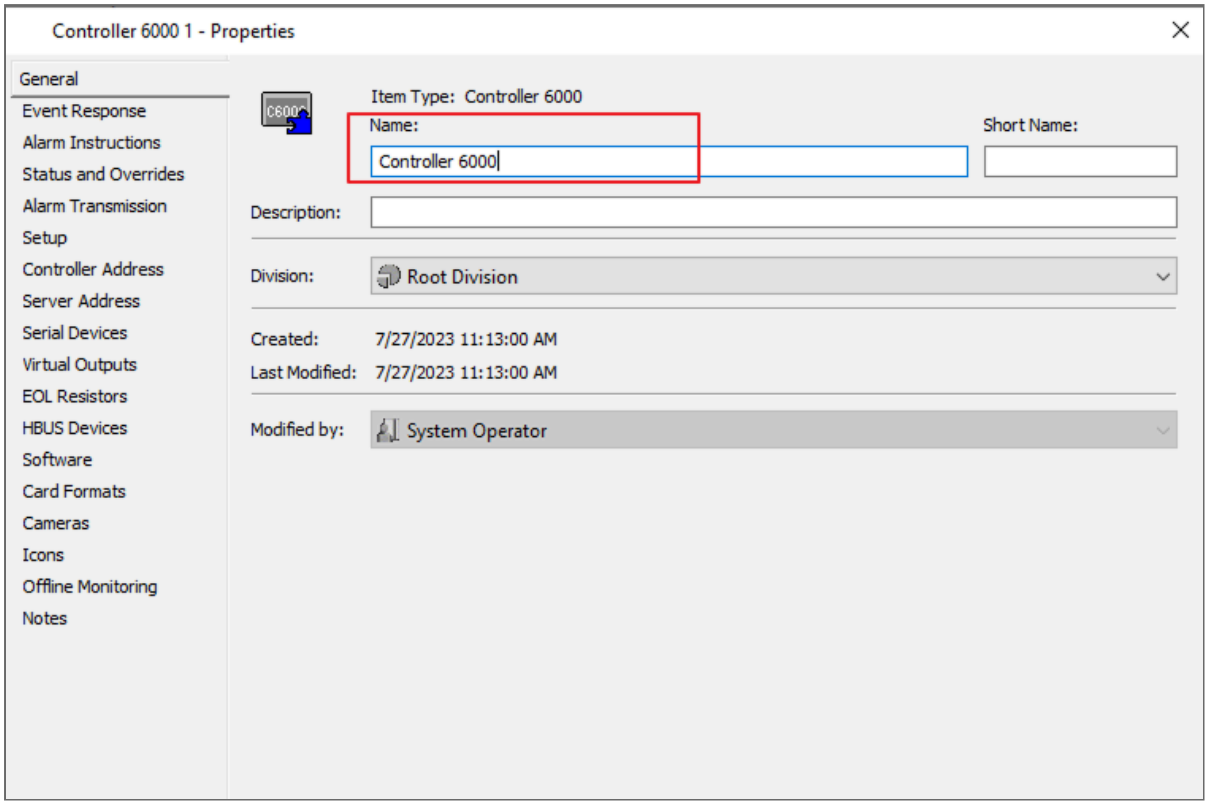
3. 次に Gallagher Configuration Client に戻り、configure → Alarm Zones に移動して**右クリック**し、新しいアラームゾーンを作成します。



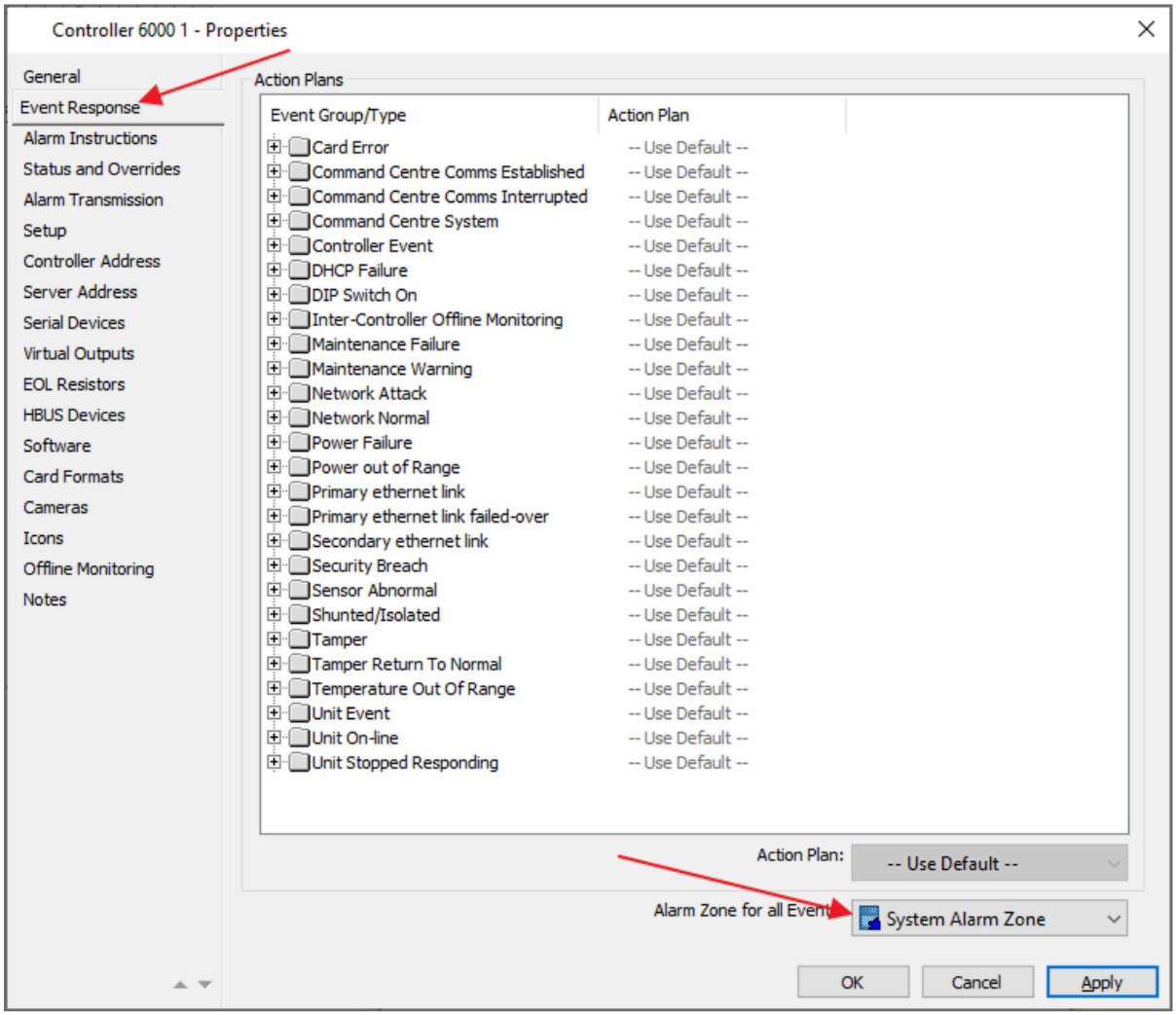
4. アラームゾーンの一般設定で名前を **System Alarm Zone** に変更し、**OK** ボタンを**押します**。



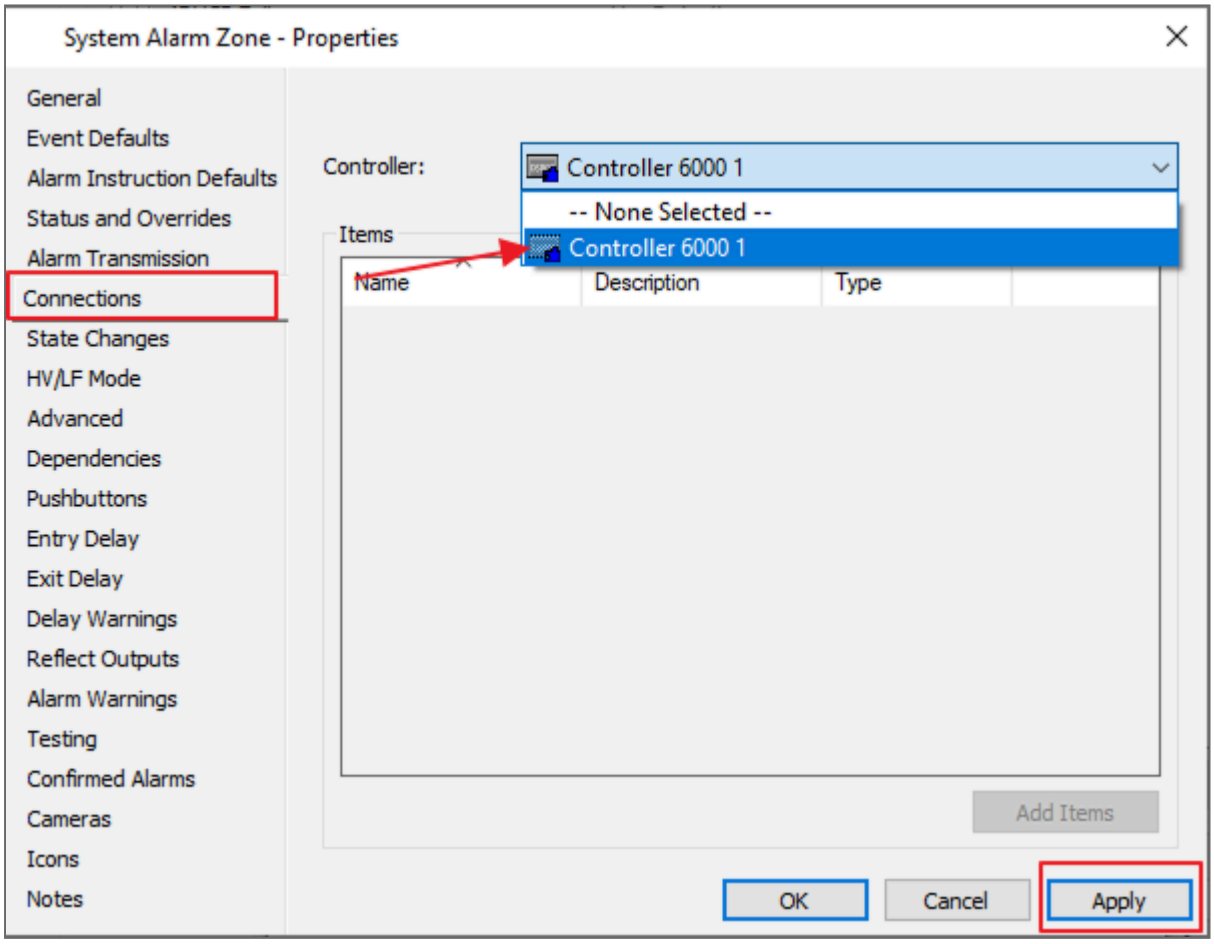
5. Controller 6000 を設定します。一般設定で名前を **Controller 6000** に**設定**します（名前は使用中のコントローラーと同じにします）。



6. 次に **Event Response** に移動し、すべてのイベントで Alarm Zone を選び、**System Alarm Zone** を選択します。 そして **Apply** ボタンを押します。

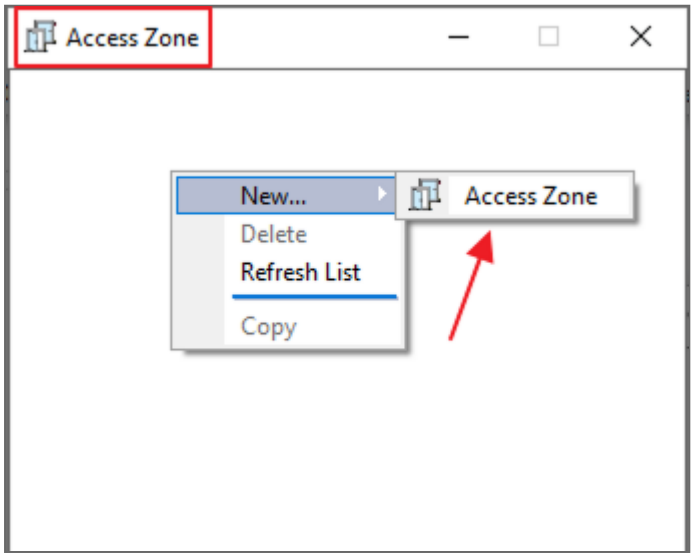


次に System Alarm Zone Properties で **Connections** を選択し、controller のドロップダウンで **Controller 6000** を選択します。 **OK** ボタンを押して、Alarm Zone ウィンドウを閉じます。

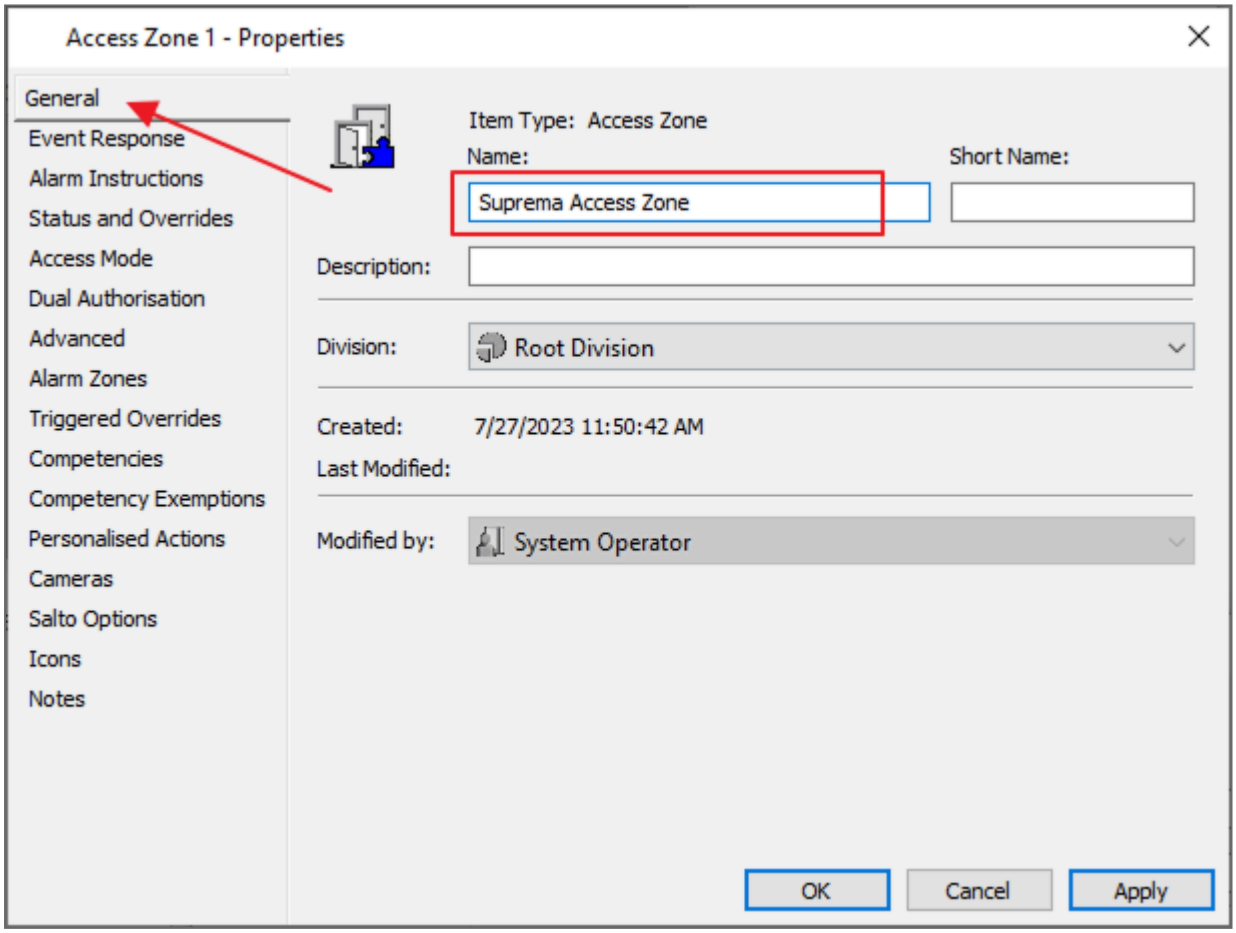


7. 次に、configure で Access Zone を**作成**します。

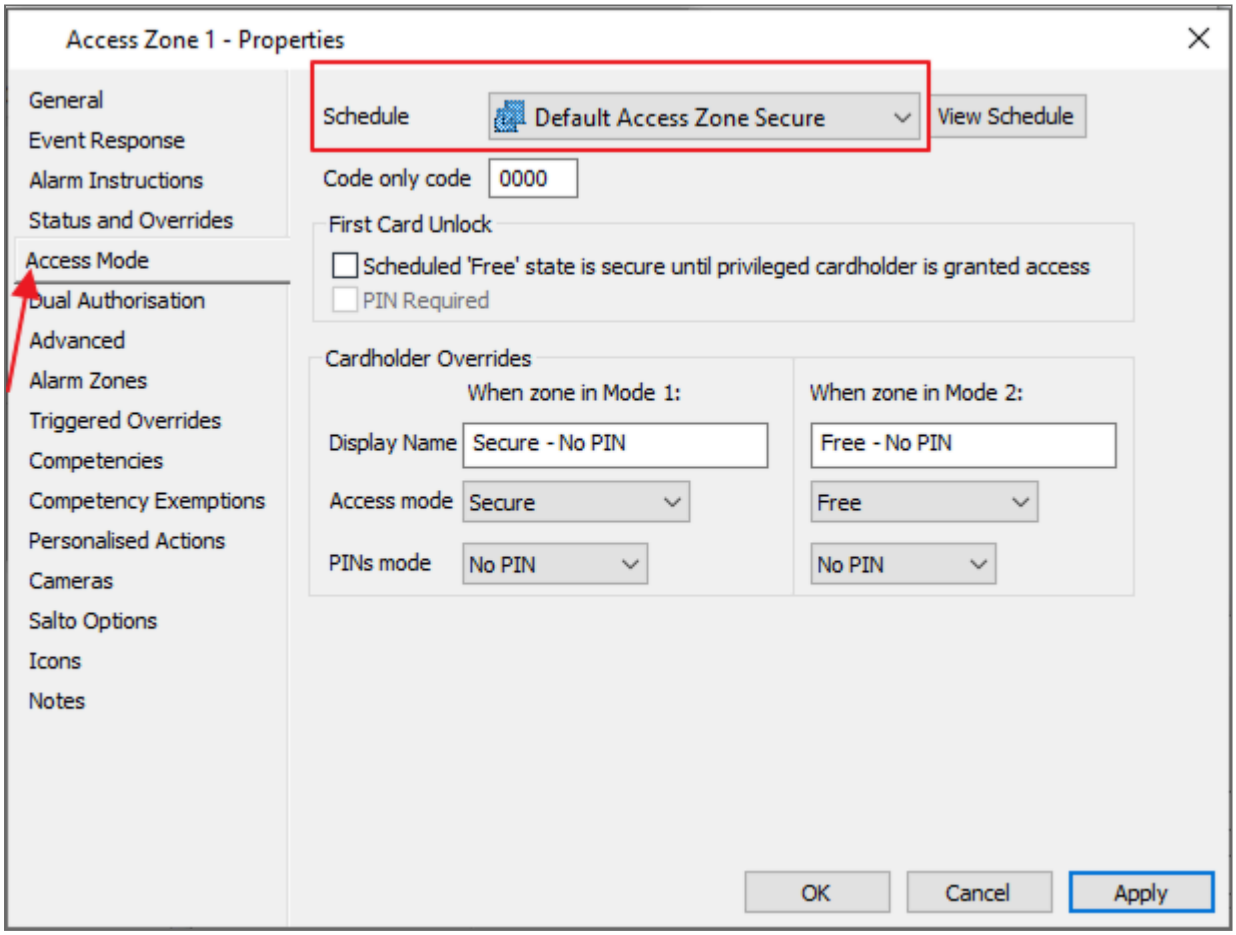
   Access Zone に移動すると、ウィンドウが開きます。 Access Zone ウィンドウで**右クリック**し、New を**選択**してから Access Zone を**クリック**します。これで access zone が作成されます。



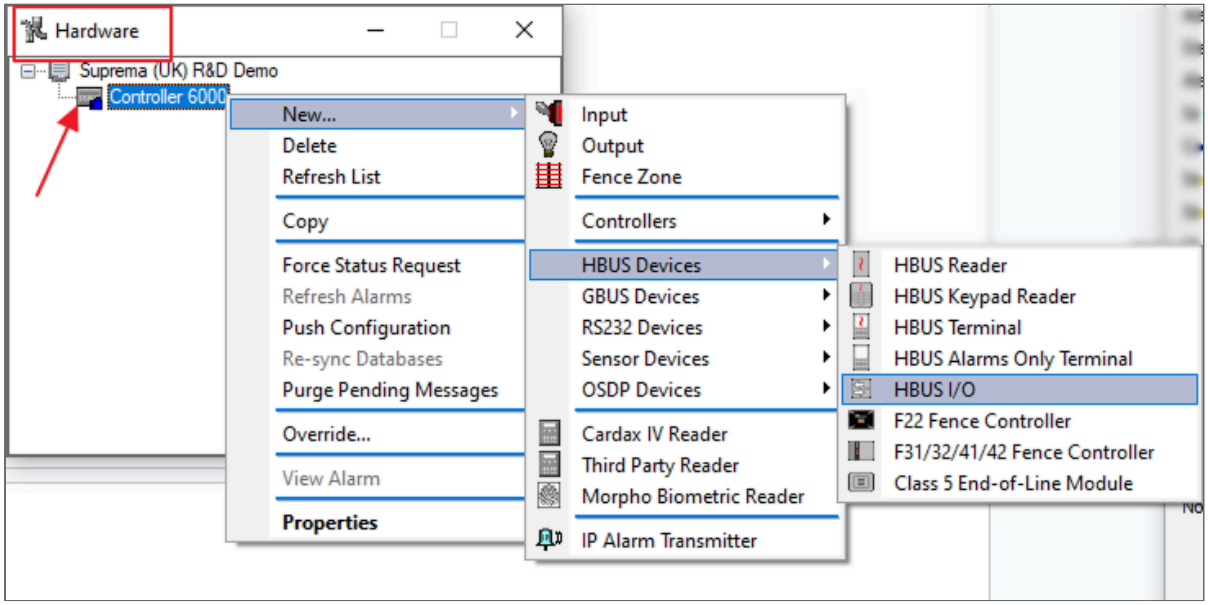
8. 作成した Access Zone Properties を一般設定で**開きます**。 次に名前を **Suprema Access Zone** に**設定**します。



9. Access Mode タブ設定に移動します。 Schedule を Default Access Zone Secure に選択し、**OK** ボタンを押します。

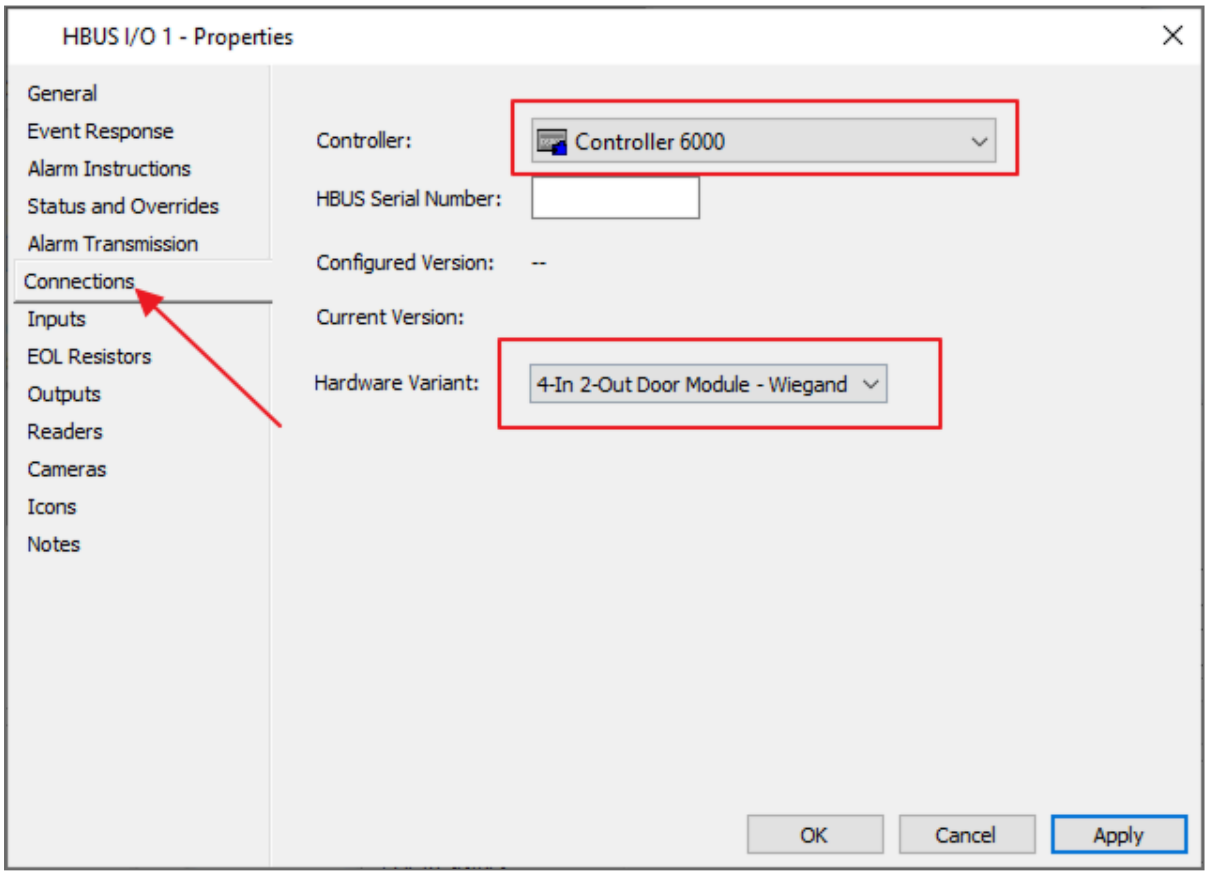


10. 次に Hardware ウィンドウに移動し、Controller 6000 を**右クリック**します。 New → HBUS Devices → HBUS I/O を選択します。 この手順で Controller 配下に HBUS が作成されます。

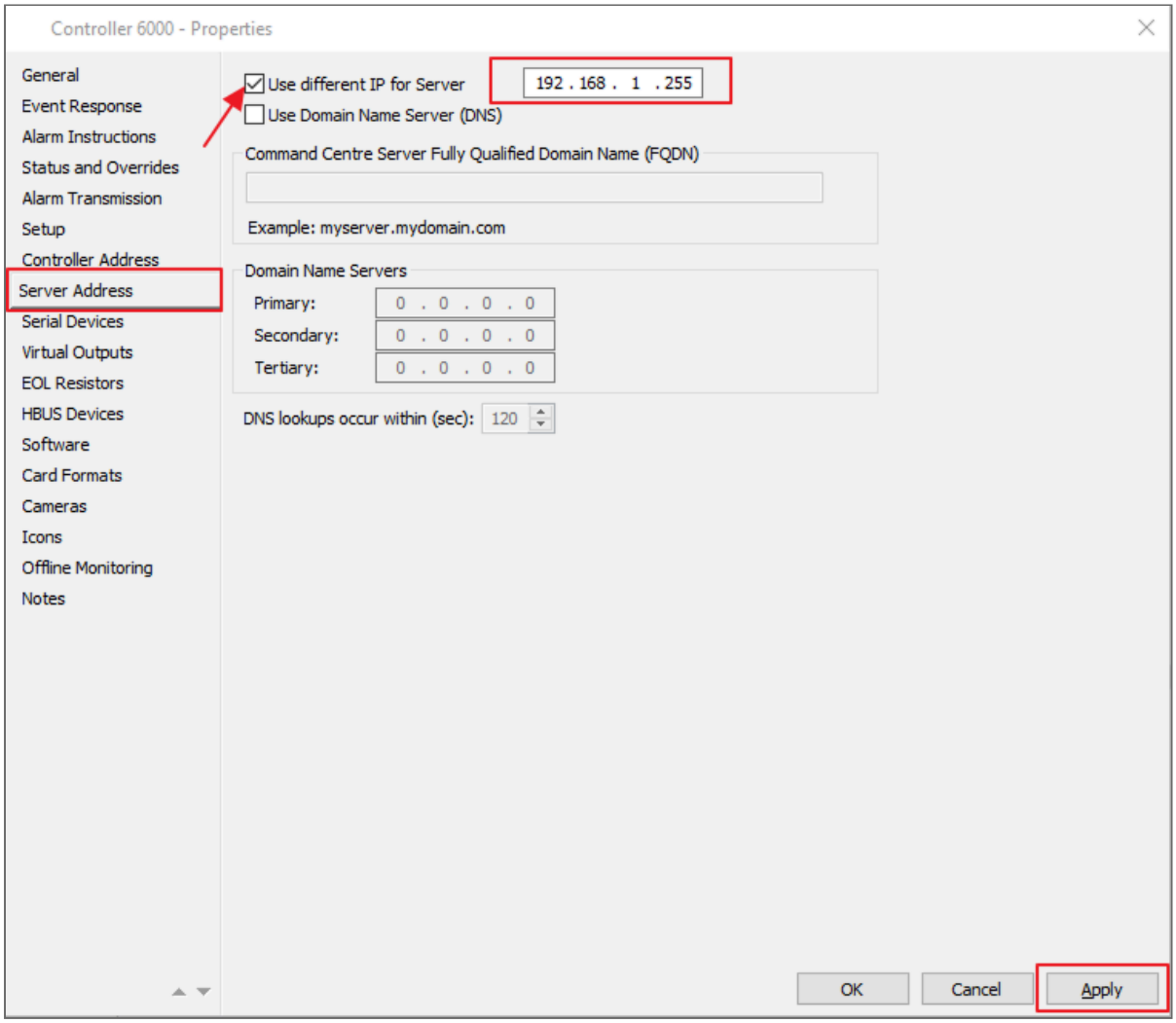


11. 作成した HBUS を**ダブルクリック**して、プロパティを編集し、設定します。 一般設定で名前を **HBUS I/O Wiegand Module (Suprema)** に**設定**します。

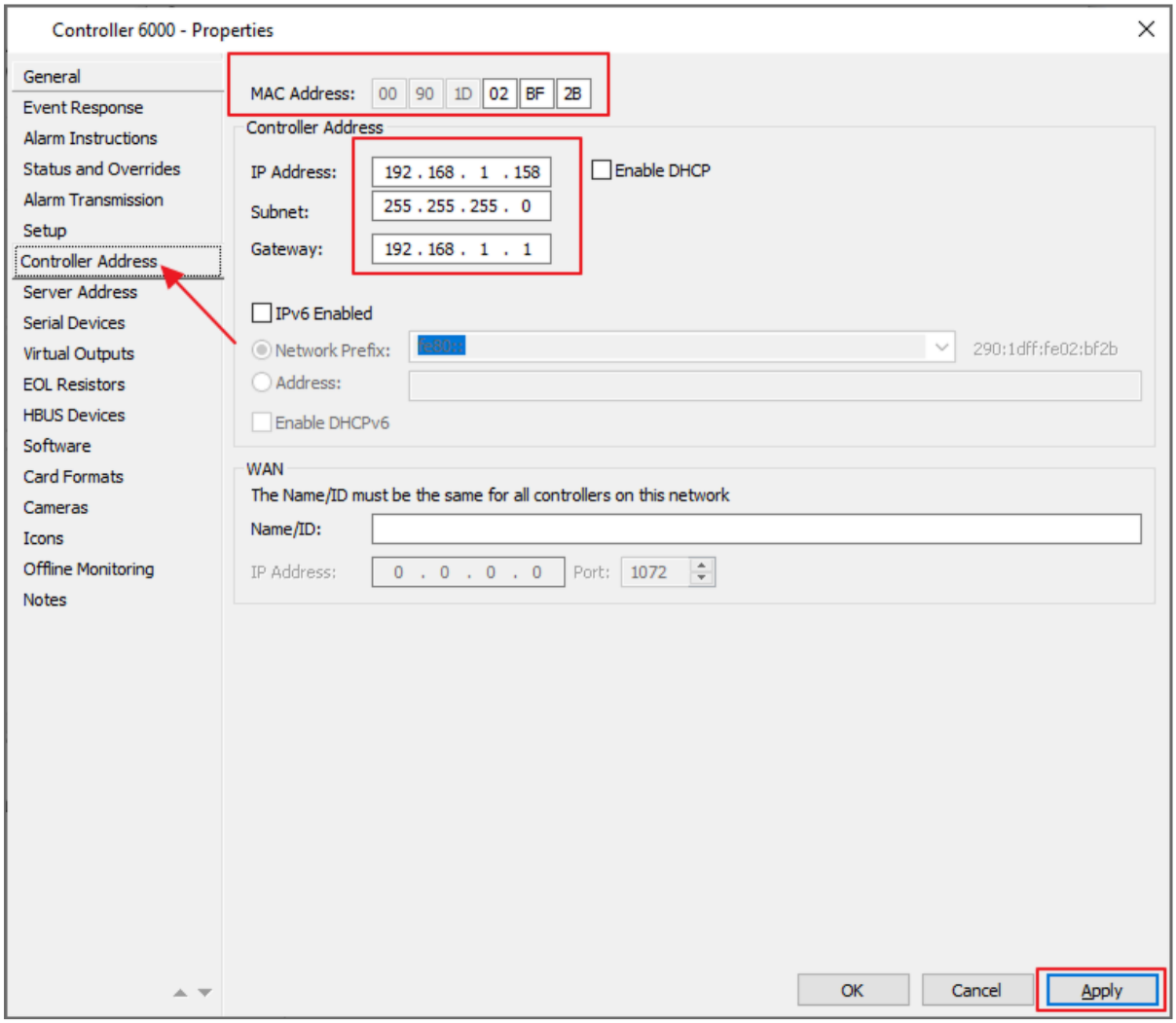
    Connections タブに**移動**し、Controller を Controller 6000 に**選択**します。Hardware Variant を 4 in 2 out に設定し、**OK** ボタンを押します。



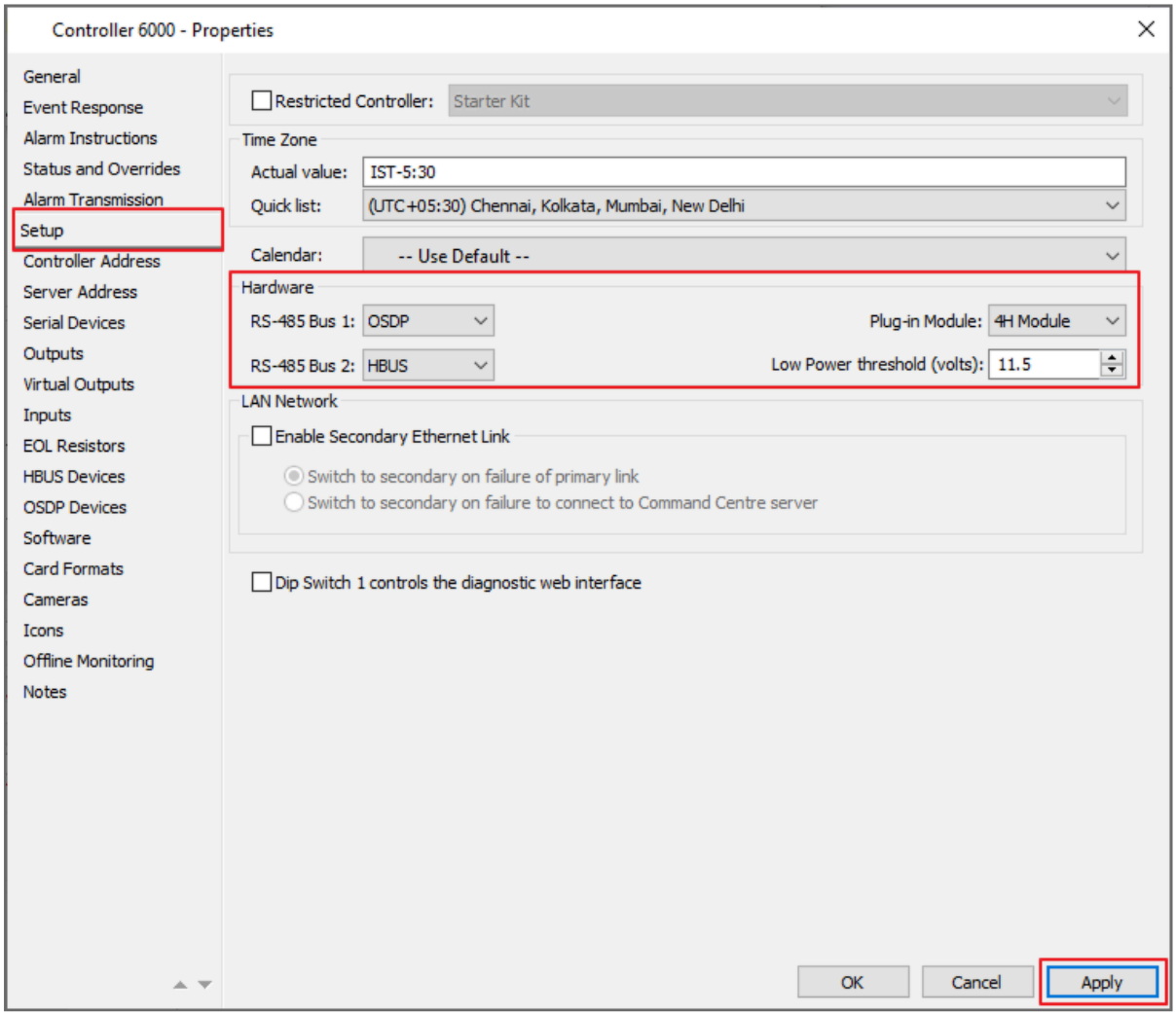
12. Gallagher Controller をシステムに接続するには、Controller 6000 のプロパティを**開き**、Server Address タブを**クリック**します。 サーバーに別の IP を使用するに**チェック**し、PC/サーバーの IP アドレスを入力します。 次に **Apply** ボタンを**押します**。



13. Controller Address 設定でコントローラーの MAC アドレスを設定します（C6000 コントローラーを確認してください）。また、コントローラーに割り当てた IP アドレス、サブネット、ゲートウェイも設定します。 **Apply** ボタンを押します。



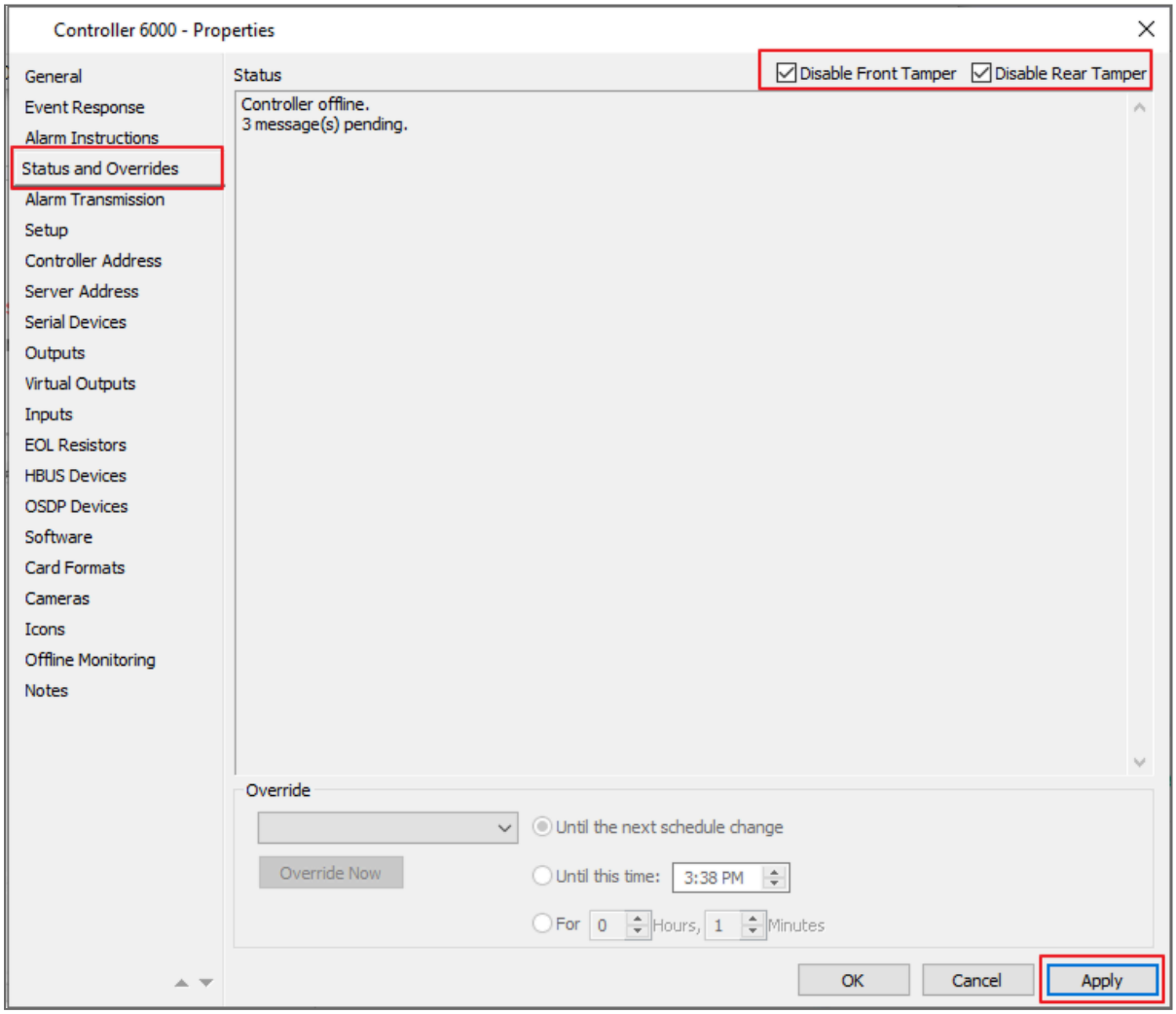
14. Setup タブで Plug in Module を **4H Module** に設定します（コントローラーに合わせて選択します）。Hardware RS485 Bus 1 は **OSDP**、RS485 Bus 2 は **HBUS** にし、Apply を押します。



情報

設定は Gallagher デバイスとコンポーネントによって異なる場合があります。

15. Status and Overrides のオプションで、Disable Front Tamper と DisableRear Tamper の両方のチェックボックスを**オンにします**。



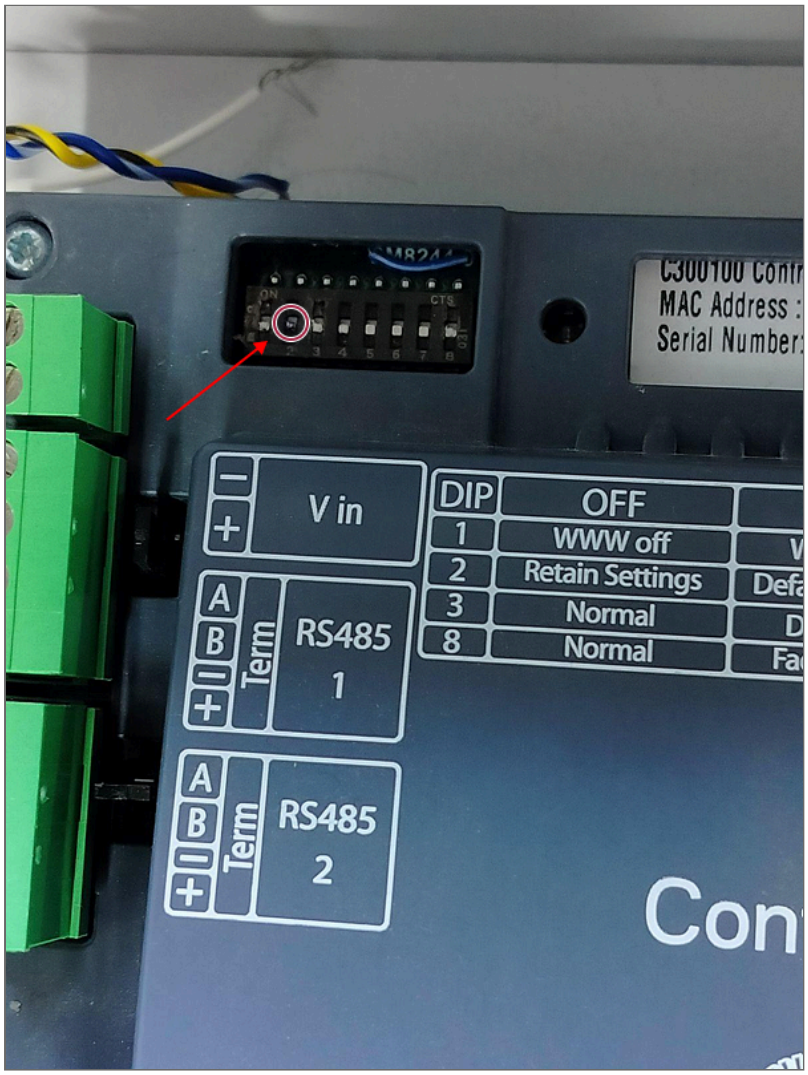
16. コントローラーをシステムに接続するには、コントローラーの電源を**切り**、赤いランプが消えるまで待ちます。 次に左から 2 番目のボタンを**オンにします**。

> **情報**
> この手順を行う前に、PC のファイアウォールがオフになっていることを確認してください。



17. コントローラーの状態が正常になったら、2 番目のボタンを**オフにします**（2 番目のボタンを下げます）。

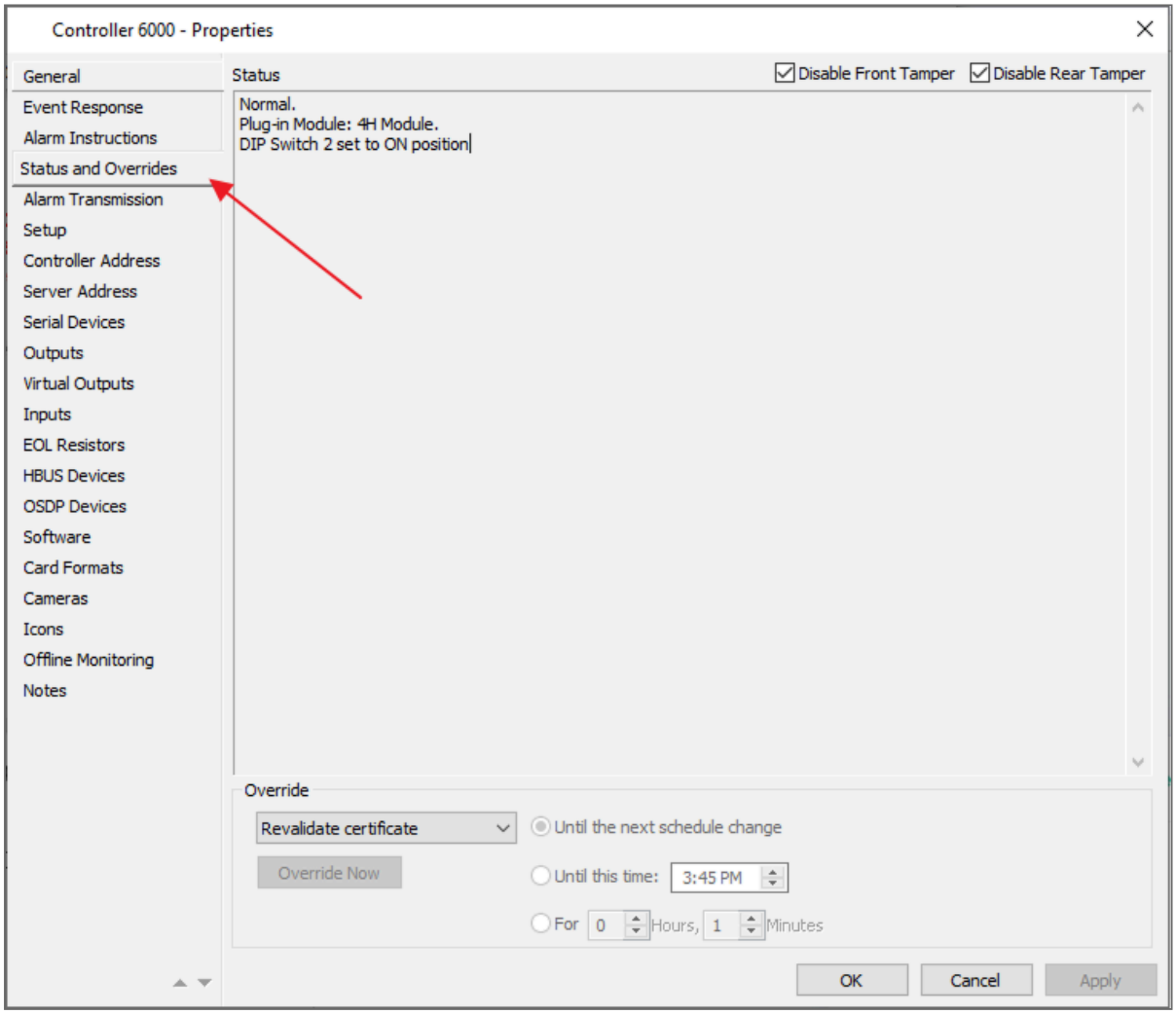
> **情報**
> コントローラーがオンラインで正常になったら、2 番目を含むすべての DIP スイッチをオフにできます。



補足：初回電源投入と新しいコントローラー接続：

新しいコントローラーの初回電源投入時にサーバーへ接続する場合のみ #2 をオンにします。

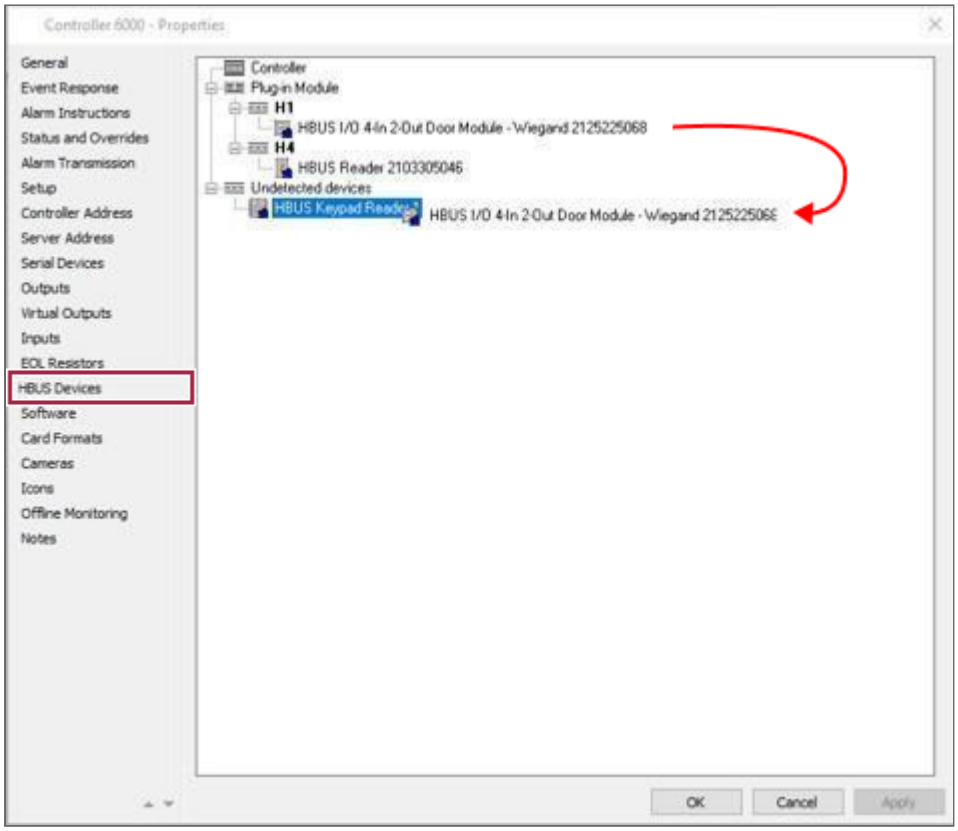
また、Jumper #2 はコントローラーのリセット時にも使用できます。 コントローラーをアップグレードする場合は、固定してください。



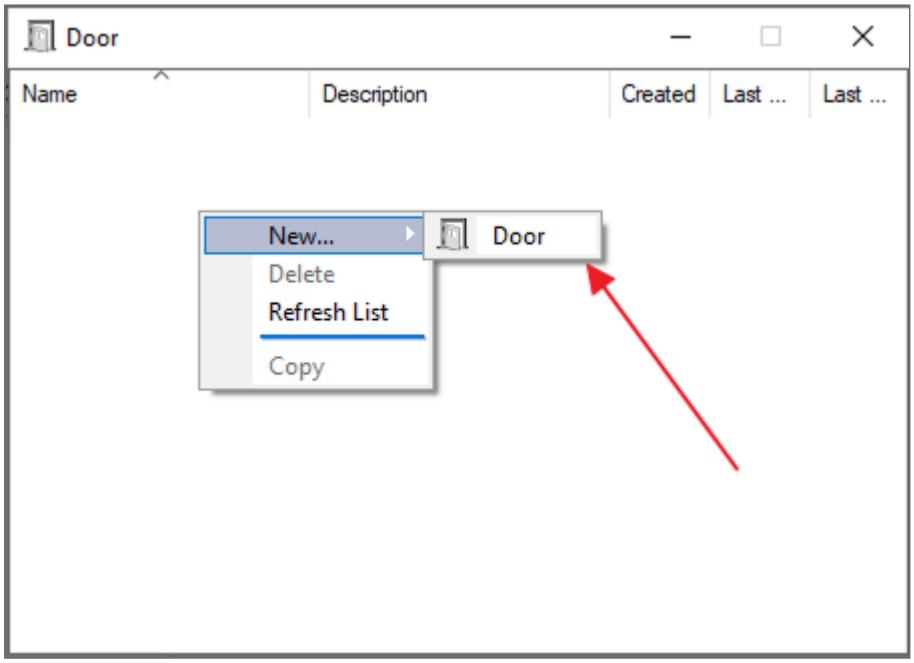
情報

コントローラーの HBUS 設定で HBUS にアクセスするには、デバイスを接続します。（デバイスの接続方法は BioStar 2 設定を参照してください。）

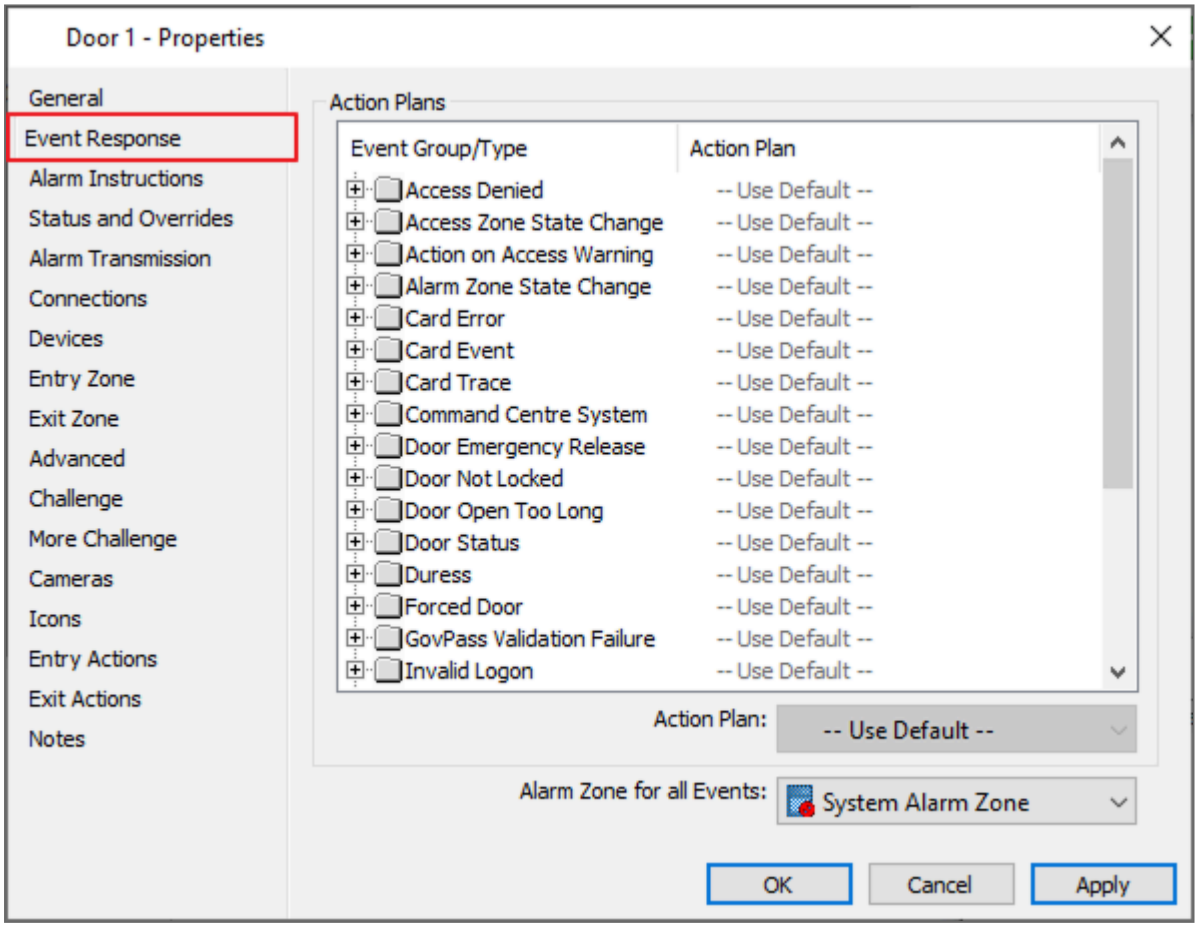
18. Controller 6000 の HBUS Devices オプションで、HBUS I/O 4 in 2 Out module - Wiegand を Plugin Modules から Undetected devices の HBUS I/O に**ドラッグ＆ドロップ**します。



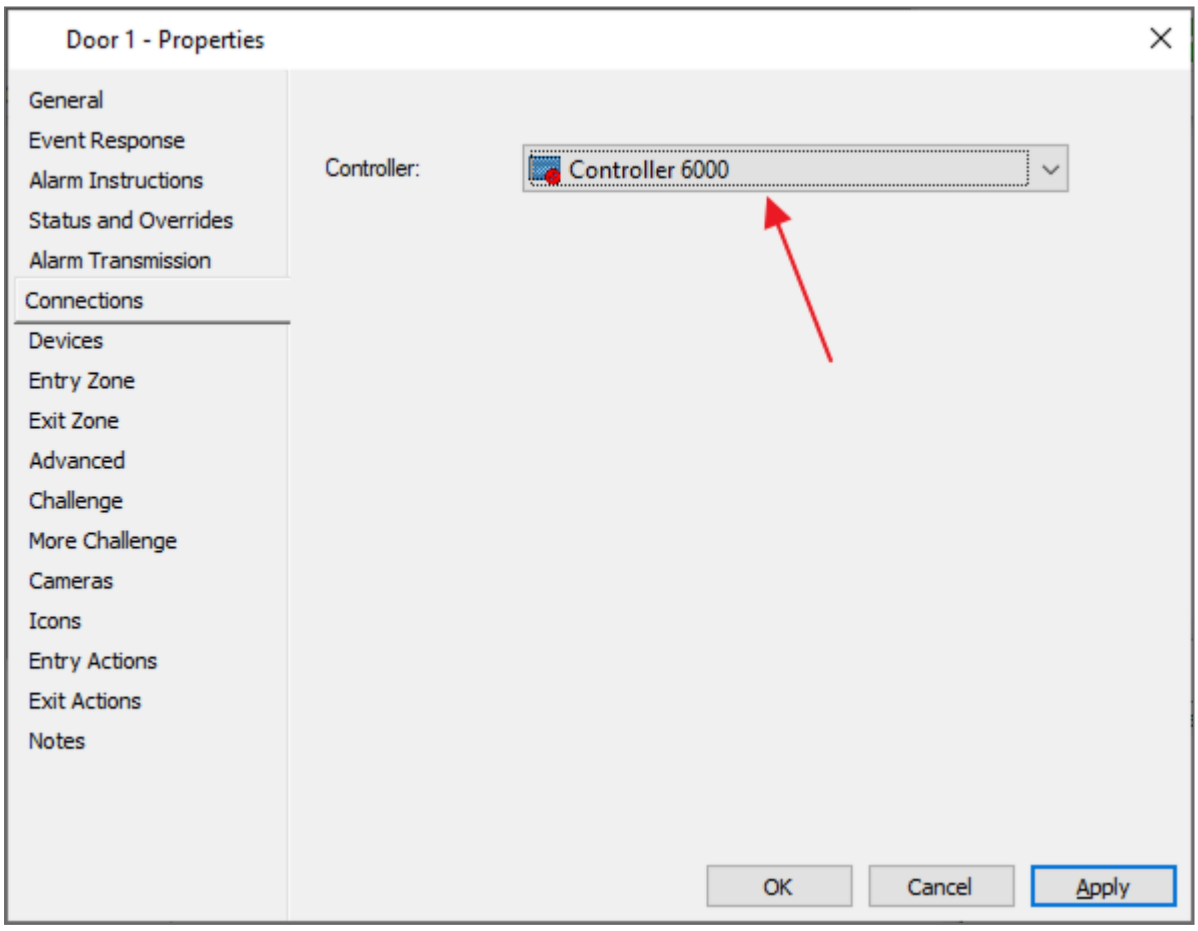
19. ドアを作成するには Configure → Door に移動し、**右クリック**して新しいドアを作成します。



20. ドア名を **Suprema Door** に設定し、Event Response に移動してアラームを System Alarm Zone に選択します。

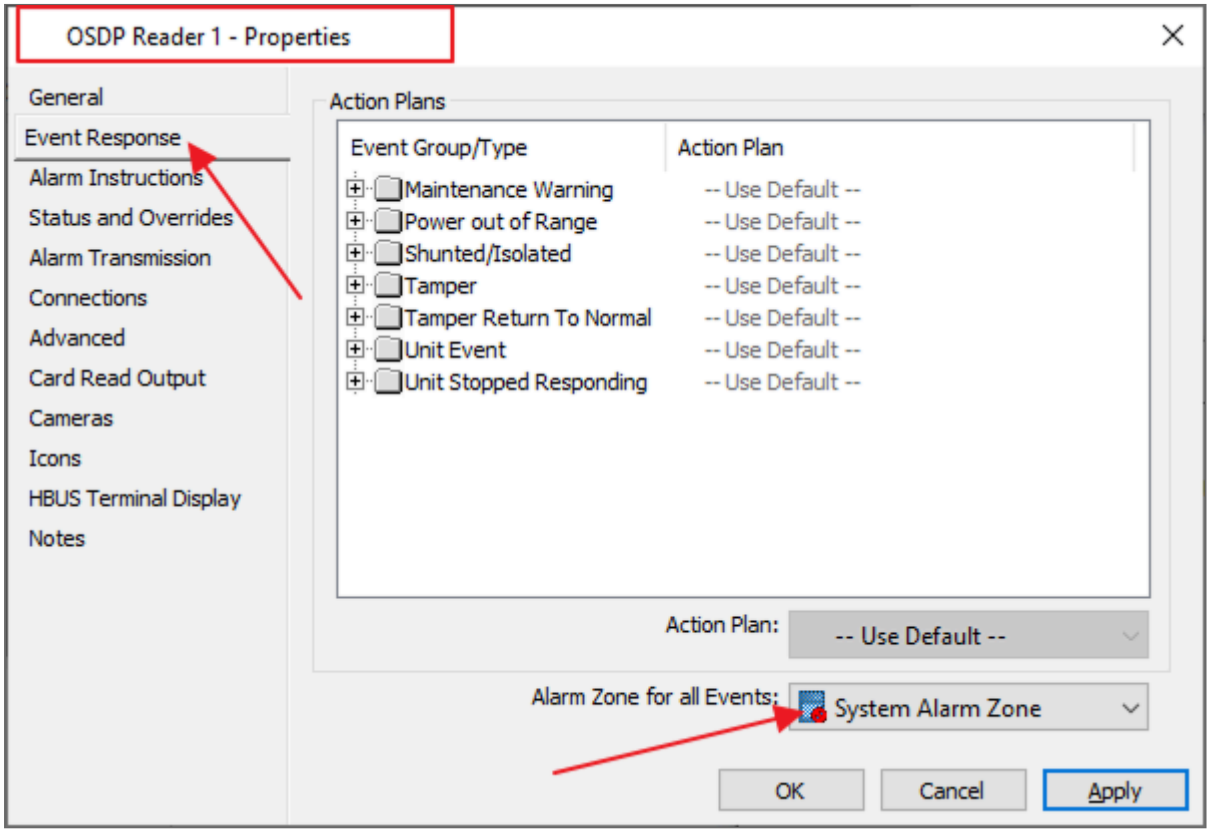


21. Connections で Controller を Controller 6000 に選択し、**Apply** と **OK** を押します。



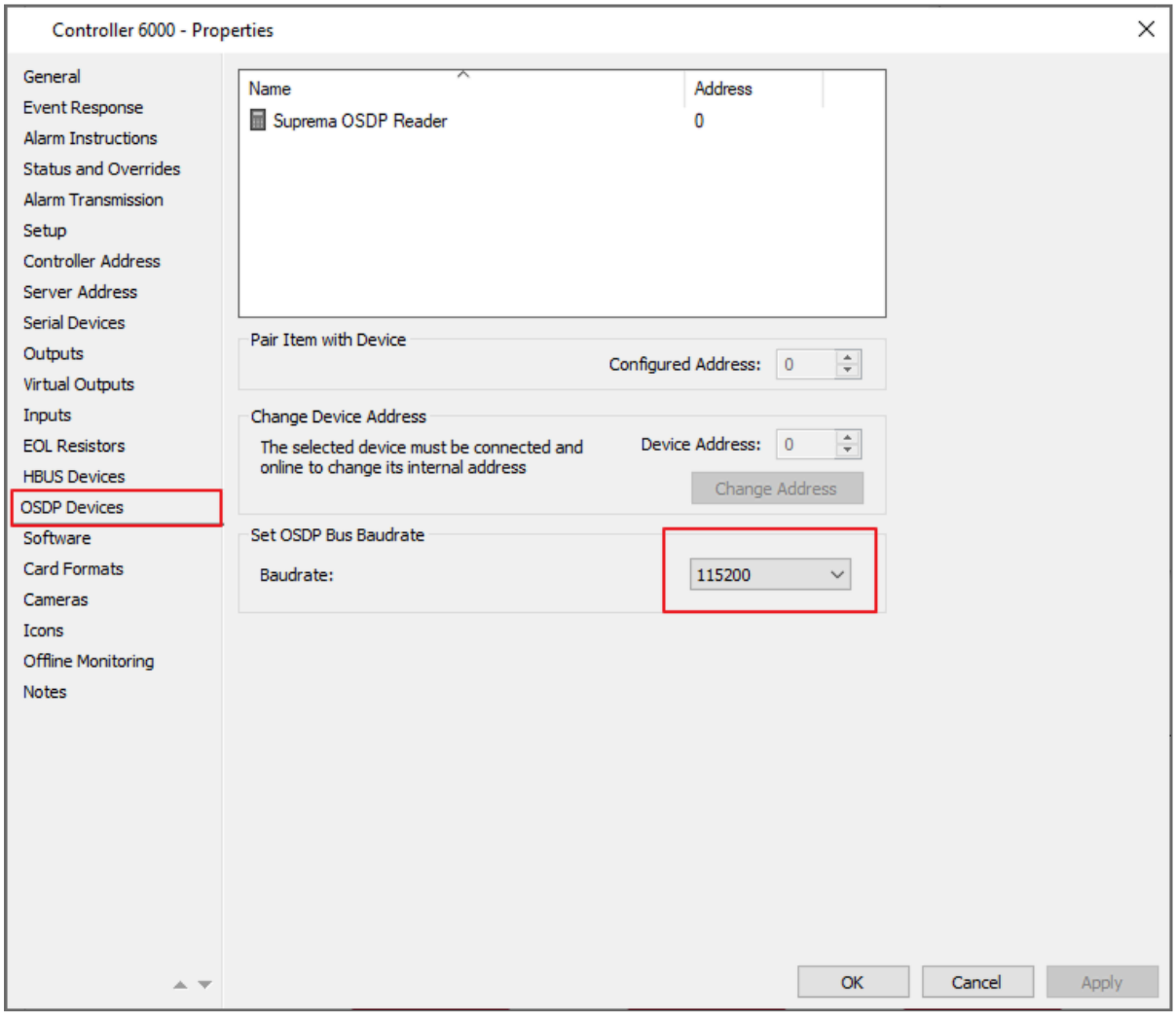
22. **OSDP 接続を作成するには、Hardware ウィンドウを右クリックします。 New → OSDP Device** → そして OSDP Reader をクリックし、Hardware に OSDP Reader を作成します。

    新しいウィンドウが開きます。 名前を Suprema OSDP Reader に**設定**し、Event Response 設定タブで Alarm Zone for all events を System Alarm Zone に**設定**します。 次に Apply をクリックし、**OK** を押して変更を保存します。



    Hardware ウィンドウに**戻ります**。 Controller 6000 を**ダブルクリック**してプロパティを開きます。 OSDP Devices タブを**クリック**します。

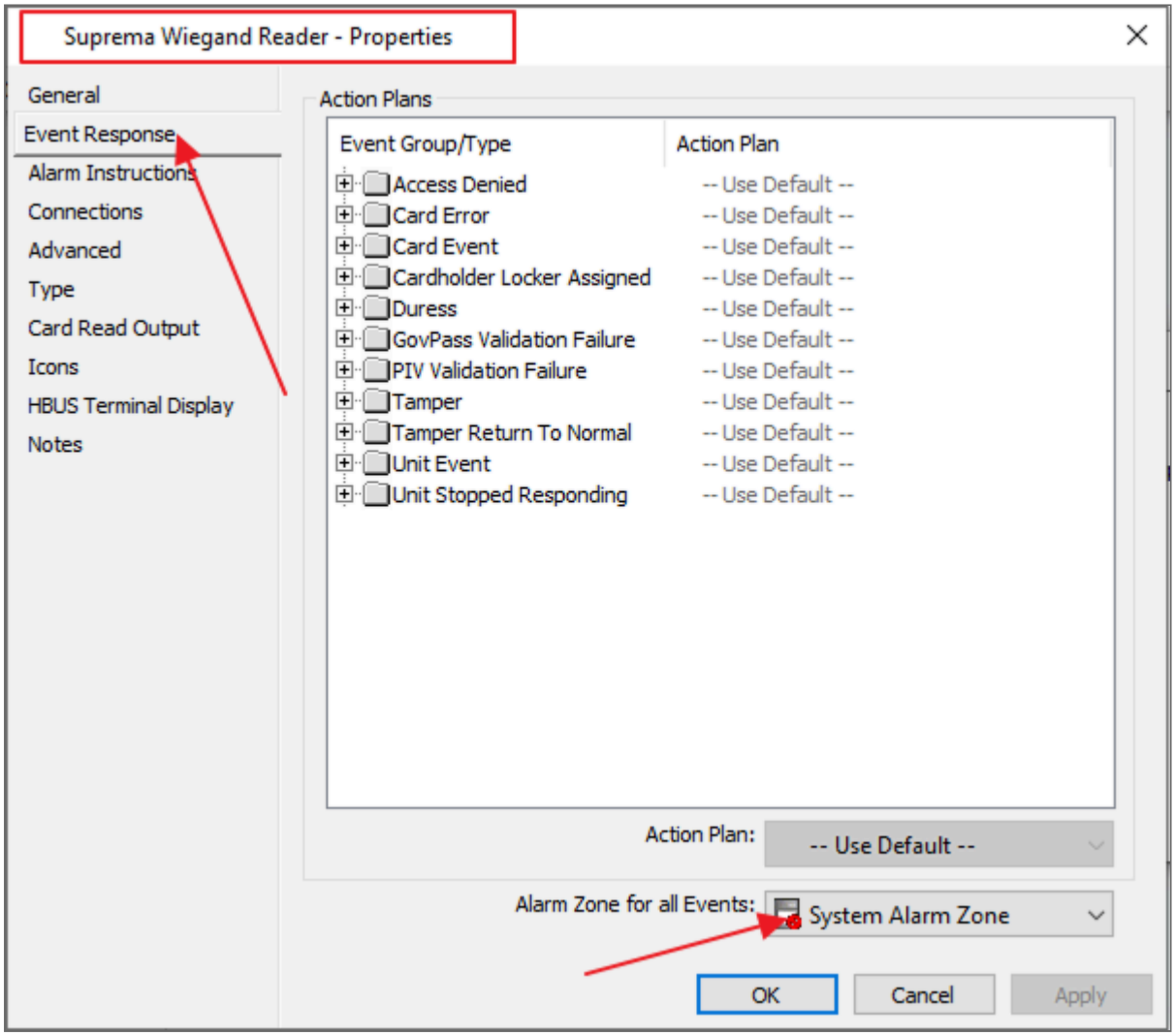
23. OSDP reader を **Hardware Window から** OSDP Devices タブの **Controller properties にドラッグ**します。 Configured Address を 0、Suprema OSDP Device Address を 0、Baudrate を **115200** に**設定**します。



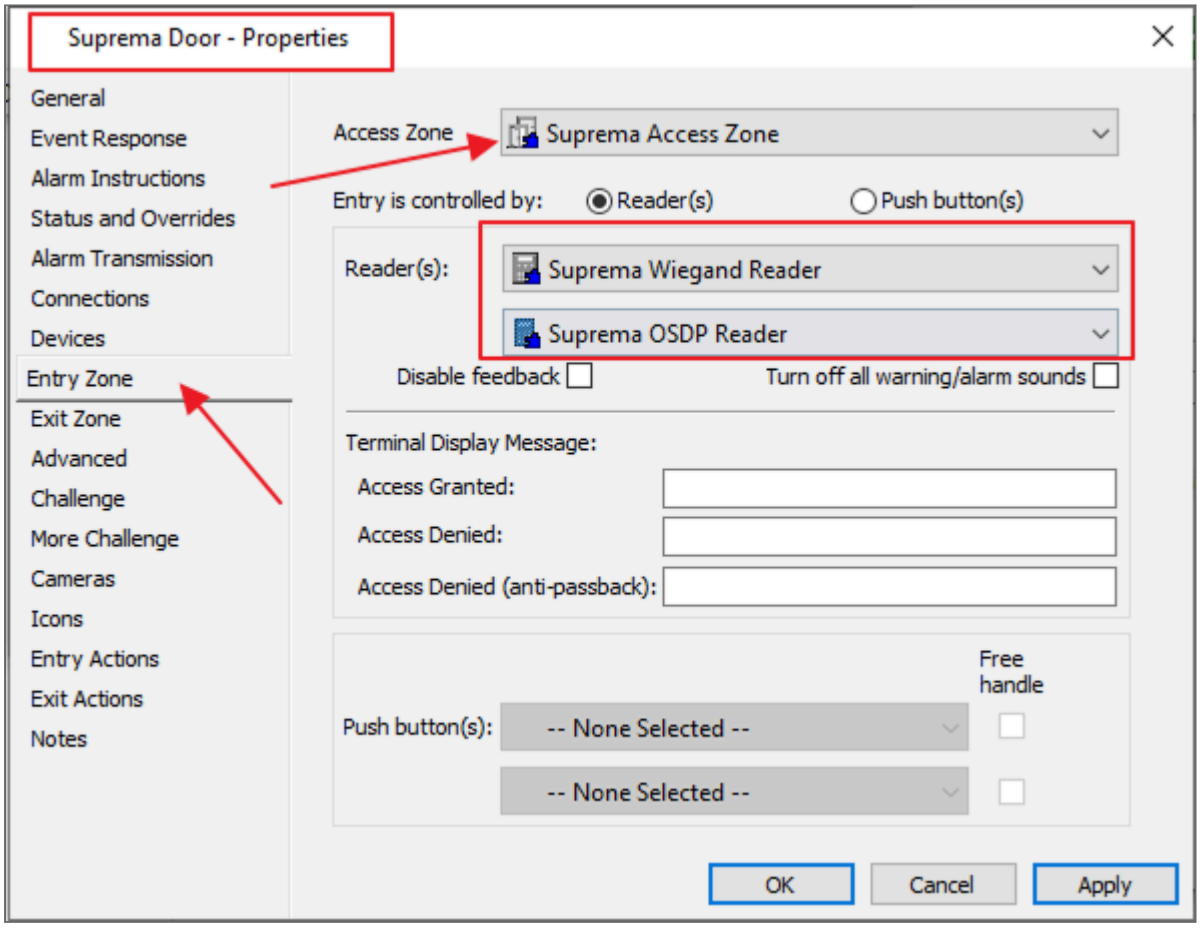
情報

2x OSDP Reader を使用している場合は、BioStar 2 で OSDP アドレスを変更してください。

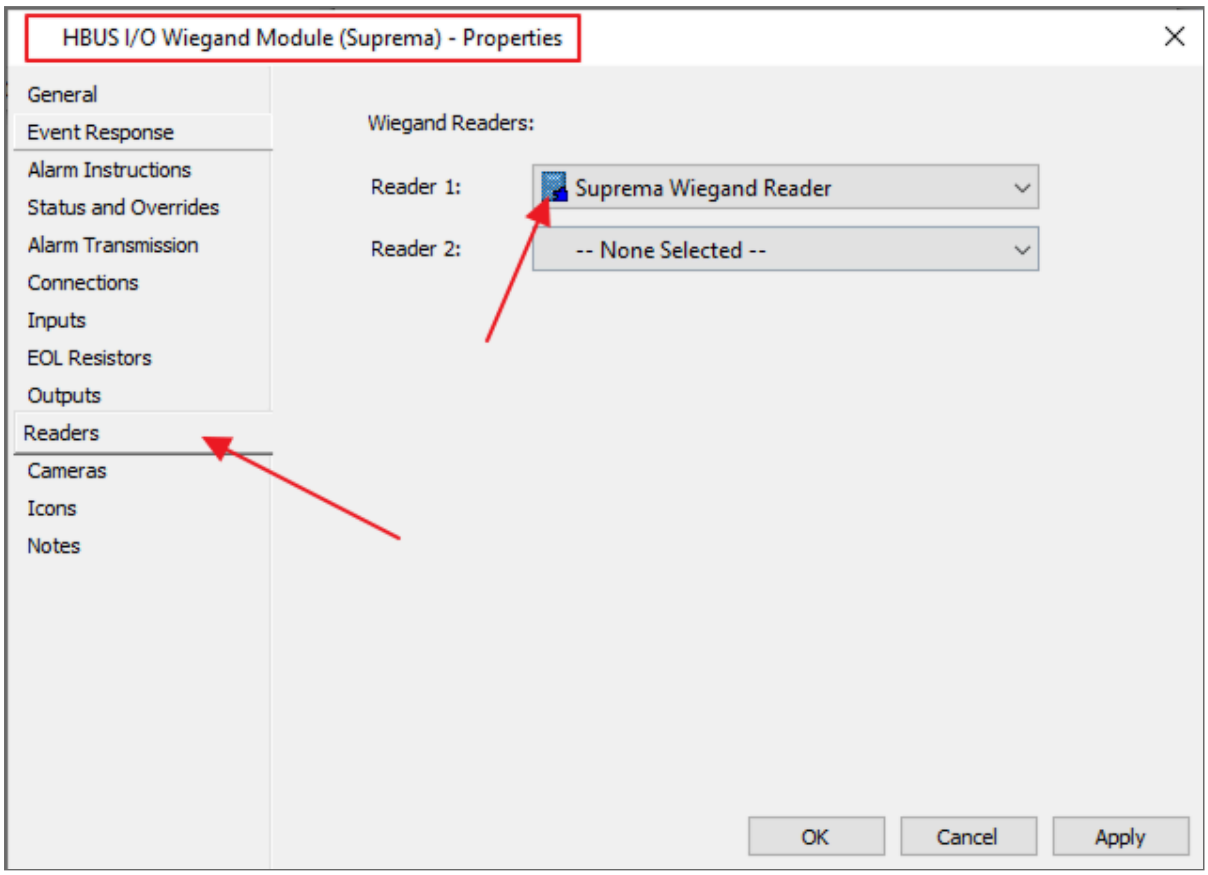
24. Wiegand Reader を作成します。 Hardware ウィンドウを**右クリック**します。 New → Third-Party Reader をクリックします。 新しいウィンドウが表示されます。名前を Suprema Wiegand Reader に**設定**し、Event Response タブに移動します。 Alarm Zone を System Alarm Zone に**選択**し、**OK** を押します。



25. 作成した Door のプロパティで **Entry Zone** に移動し、Access Zone を **Suprema Access Zone**、reader を **Suprema Wiegand Reader** と **Suprema OSDP Reader** に設定して、**OK** ボタンを押します。



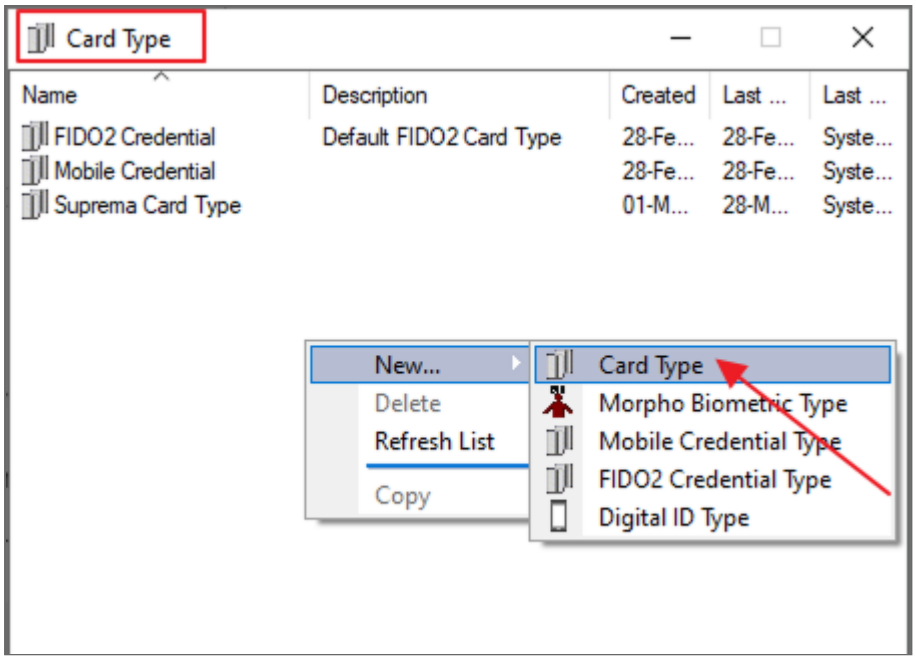
26. HBUS I/O のプロパティで Reader 設定に移動し、Reader 1 を Suprema Wiegand Reader に設定して、**OK** ボタンを押します。 Door ウィンドウと Controller ウィンドウを閉じます。



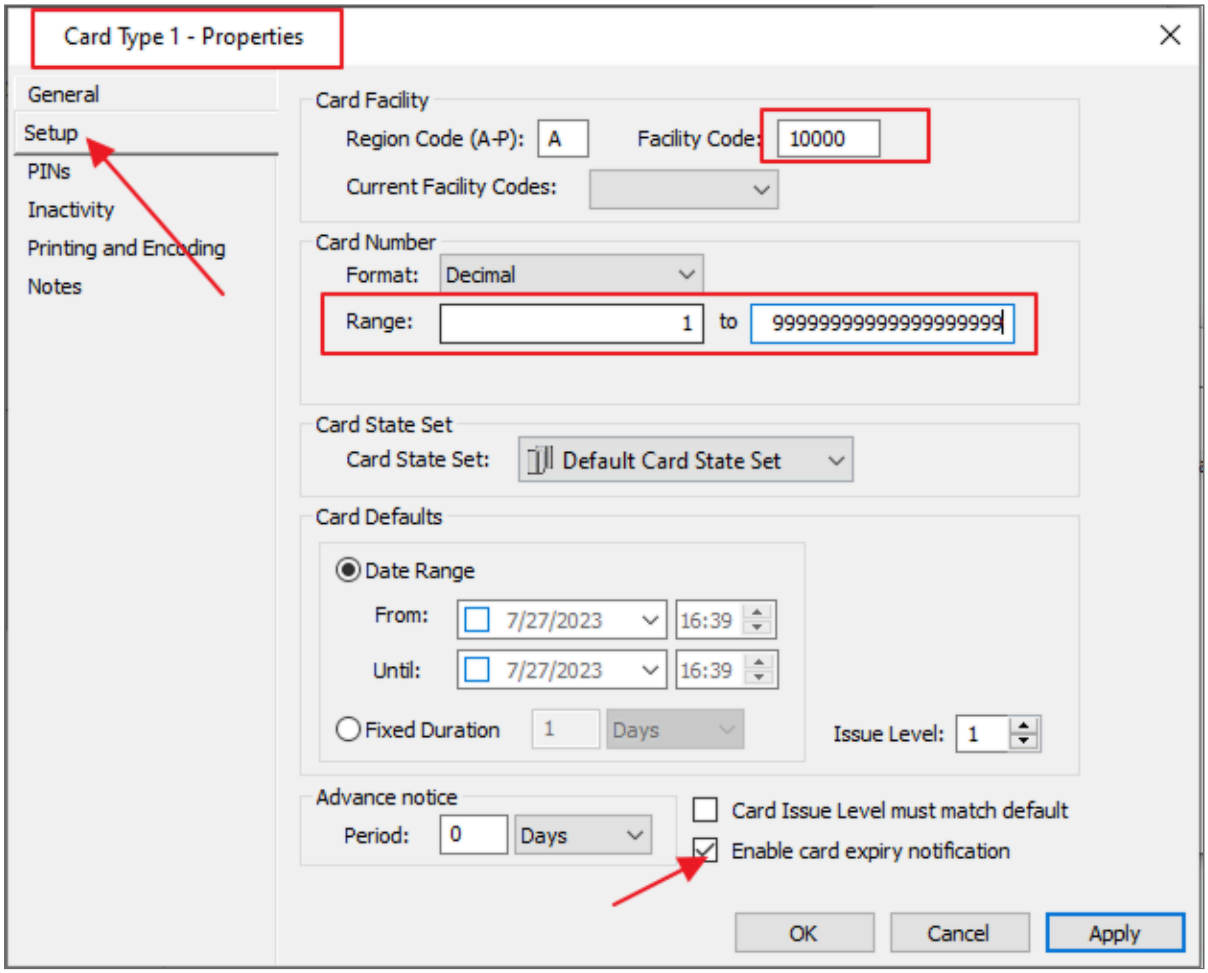
27. カード種別を作成するには Configure → Card Type を**右クリック**し、新しい **Card Type** を作成します。 名前を **Suprema**

Card Type に設定します。

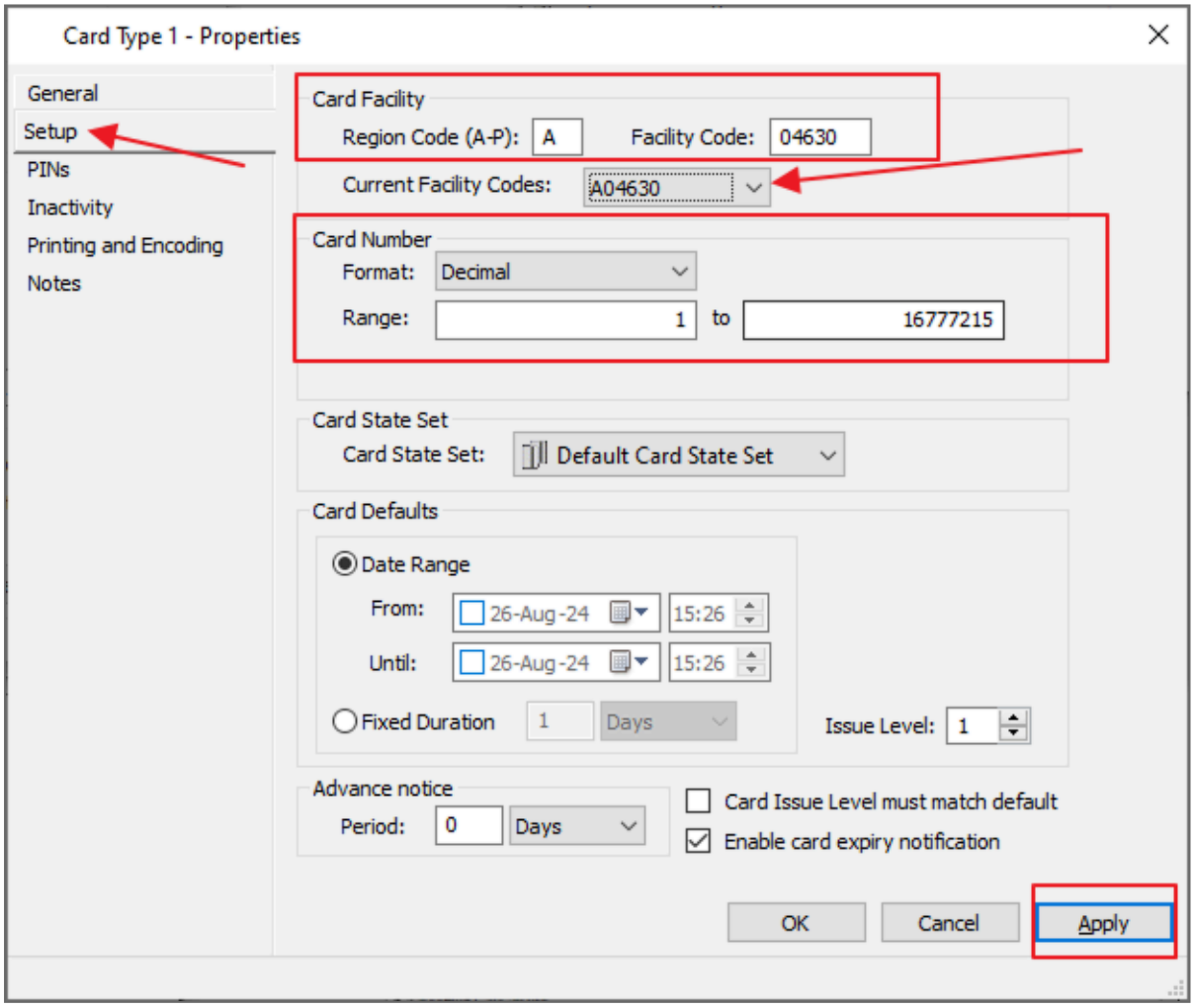
> **情報**
>
> - Gallagher QR Code を読み取るには QR Device ライセンスが必要です。 必要な場合は Suprema にお問い合わせください。
> - フィールド名は記載されている用語をそのまま使用してください。



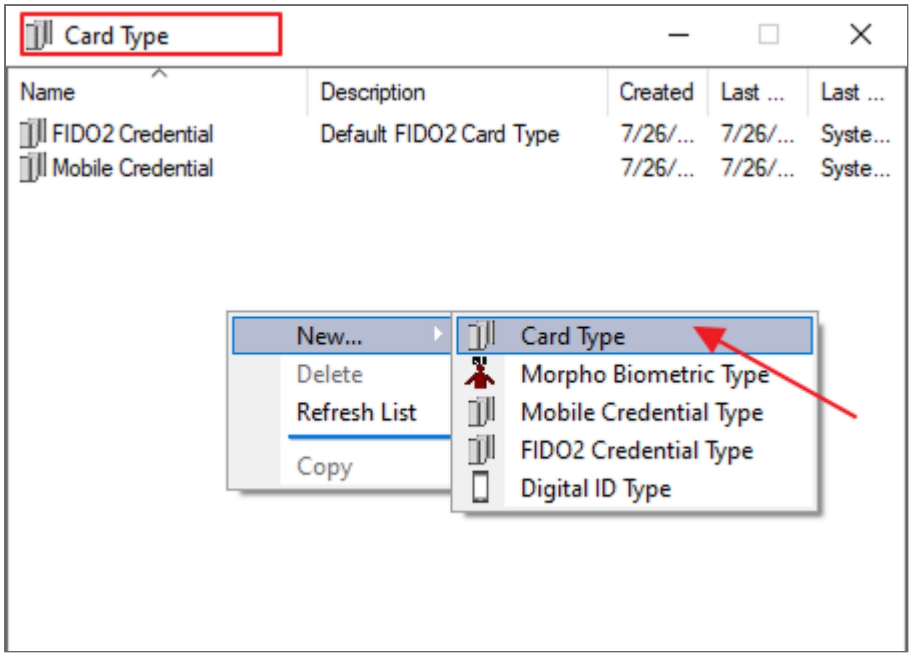
28. Card type properties で setup オプションに**移動**し、Region code を **A**、Facility code を **10000**、card number range を **1 to 99999999999999999999 (20 times)** に設定し、card expiry notification を有効にします。 **OK** を押します。



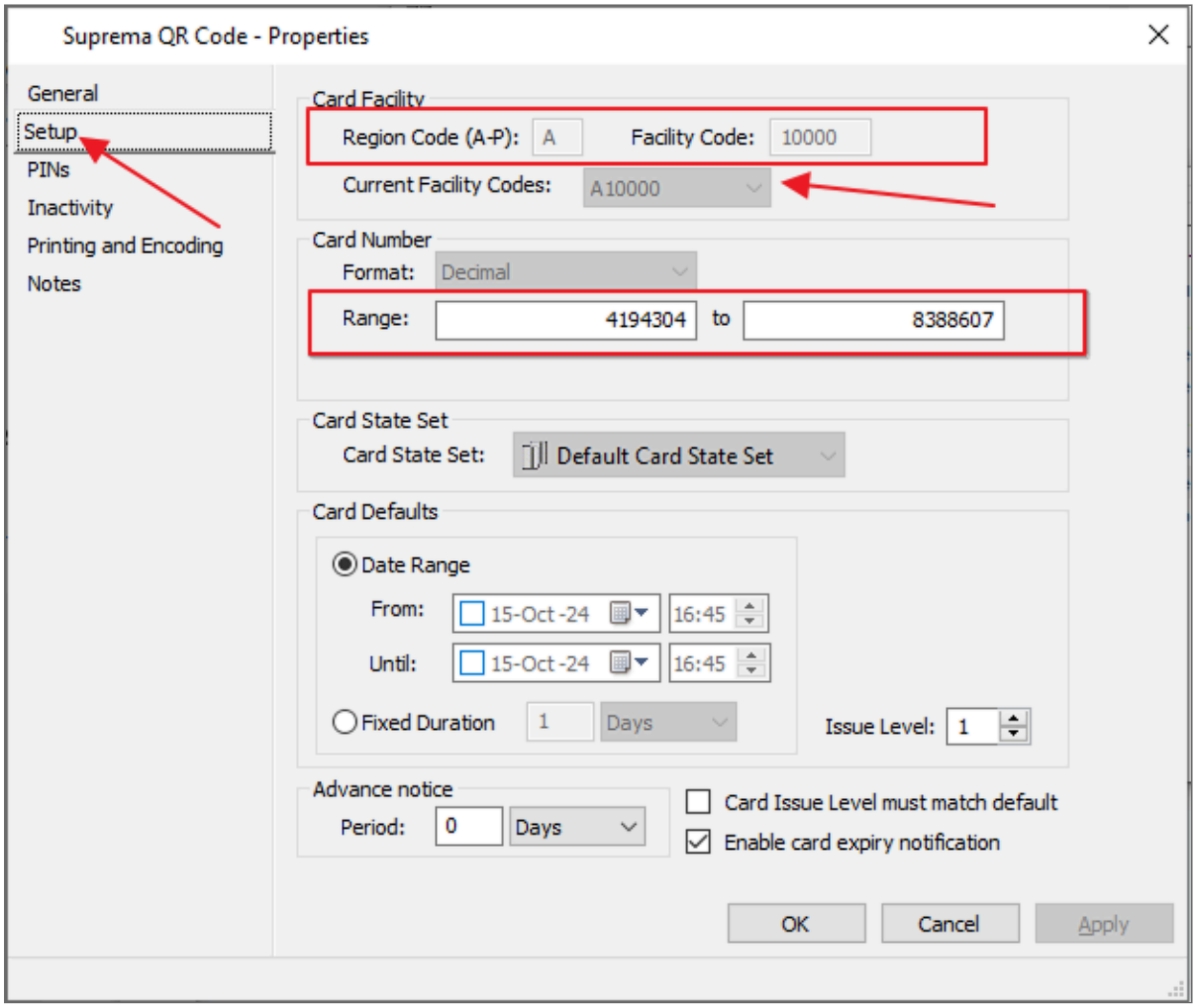
29. 別のカード種別を作成するには Configure → Card Type を**右クリック**し、新しい **Card Type** を作成します。 名前を **HID Seos Corporate** に設定します。 そしてカード種別を設定するため、プロパティ（setup）に**移動します**。 下の設定を使ってカードを構成し、**Apply** と **OK** を押します。



30. 別のカード種別を作成するには Configure → Card Type を**右クリック**し、新しい **Card Type** を作成します。 名前を **Suprema QR Code** に設定します。

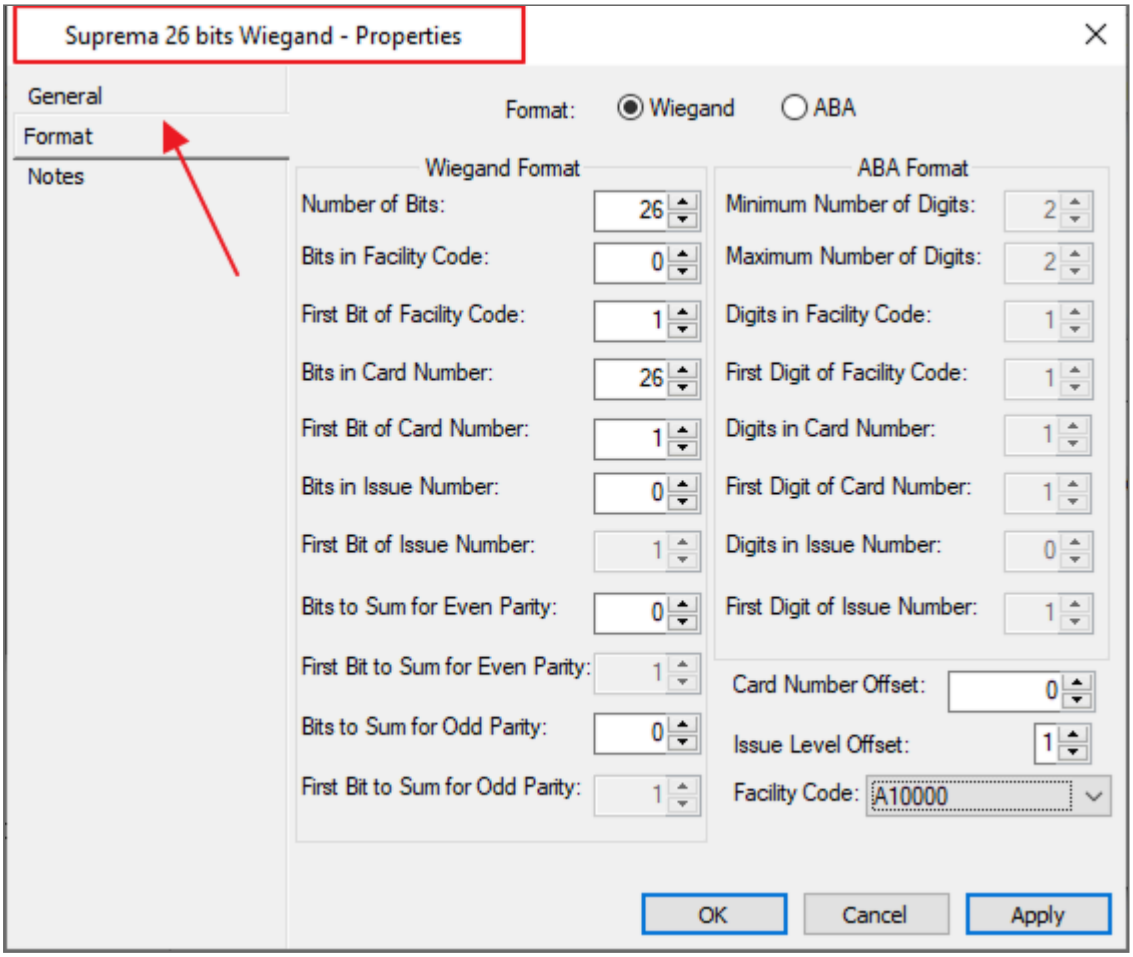


31. Card type properties で setup オプションに**移動**し、Region code を **A**、Facility code を **10000**、card number range を **4194304 to 8388607** に設定し、card expiry notification を有効にします。 **OK** を押します。

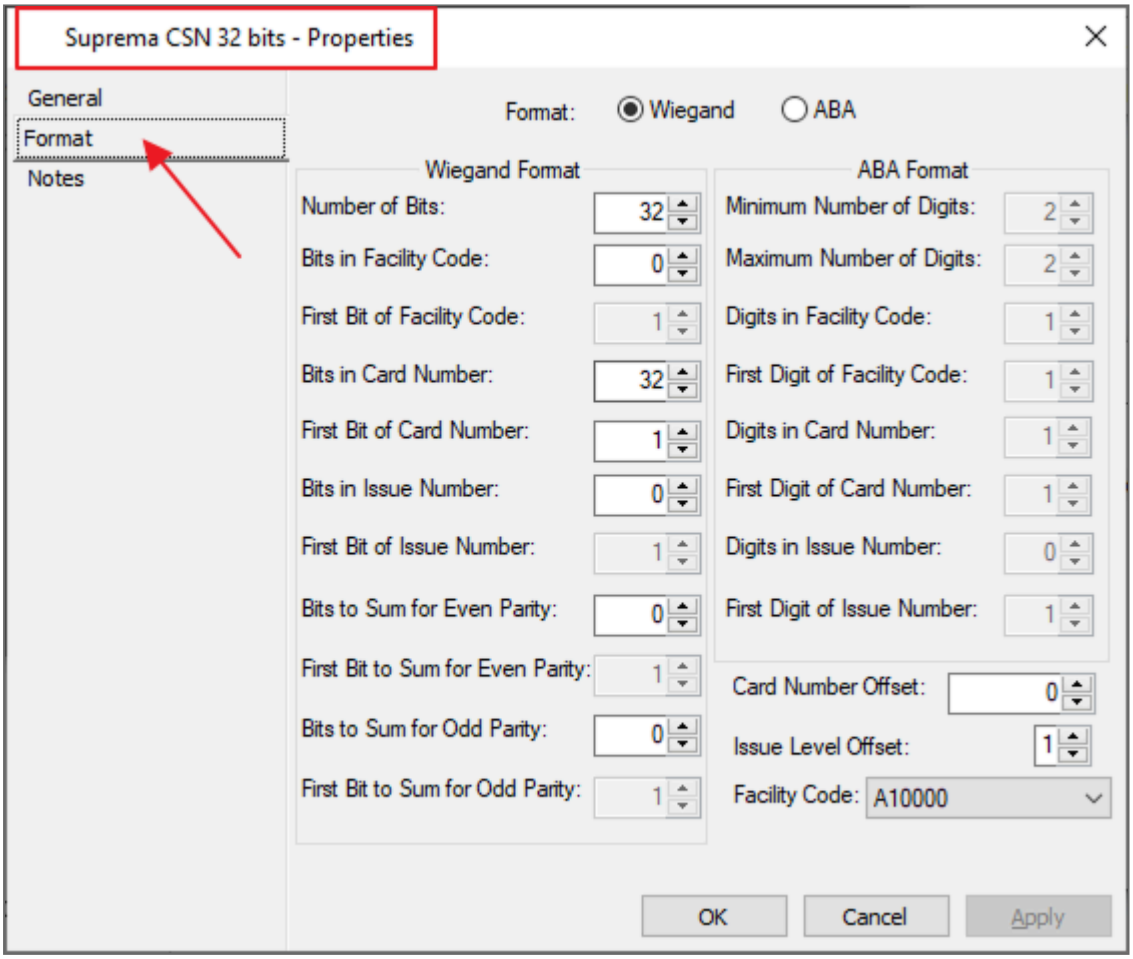


32. ユニバーサルカード形式を作成するには Configure → Universal Card Format を**右クリック**し、新しい universal card format を作成します。 4 つのカード形式を作成する必要があります。

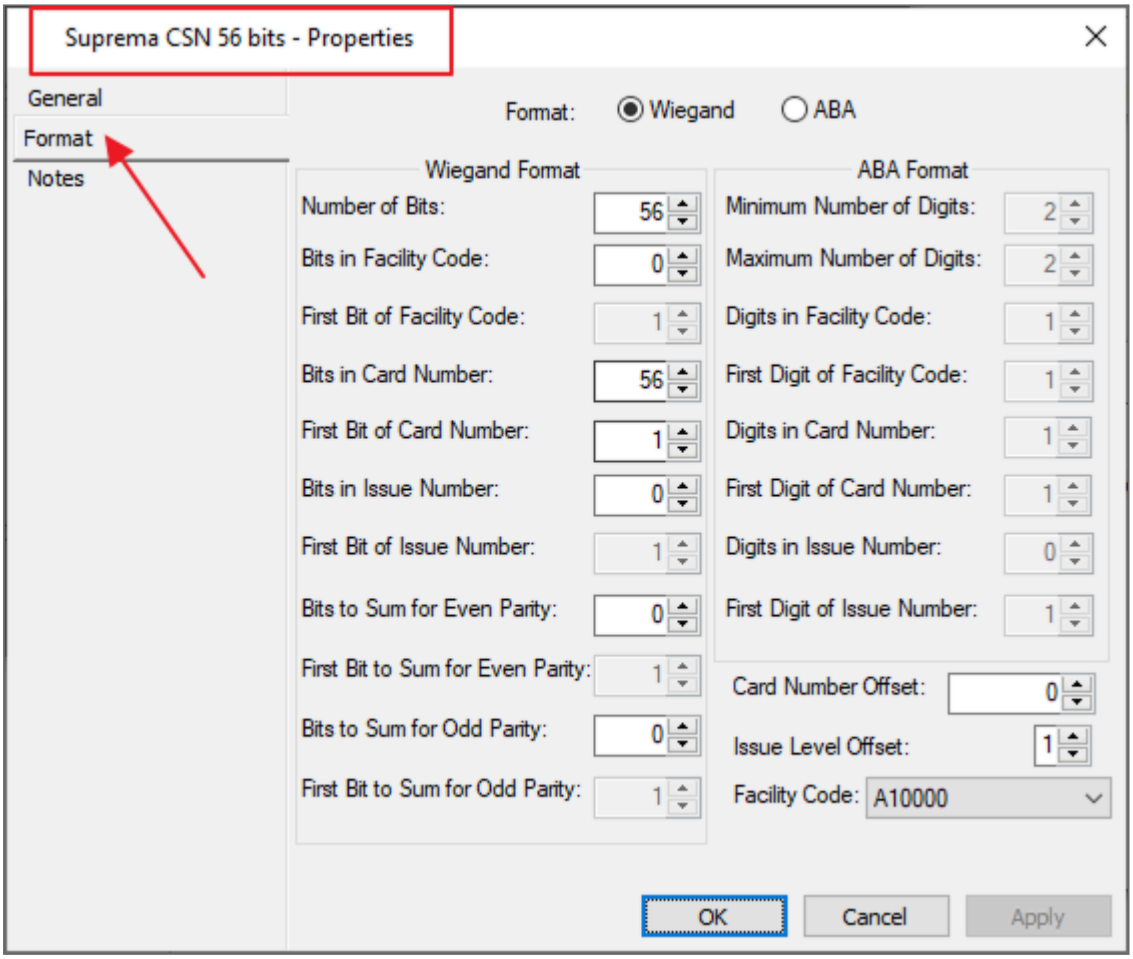
    1. 新しい形式名を **Suprema 26 bits** Wiegand として**作成**し、形式を下の画像のとおりに設定します。



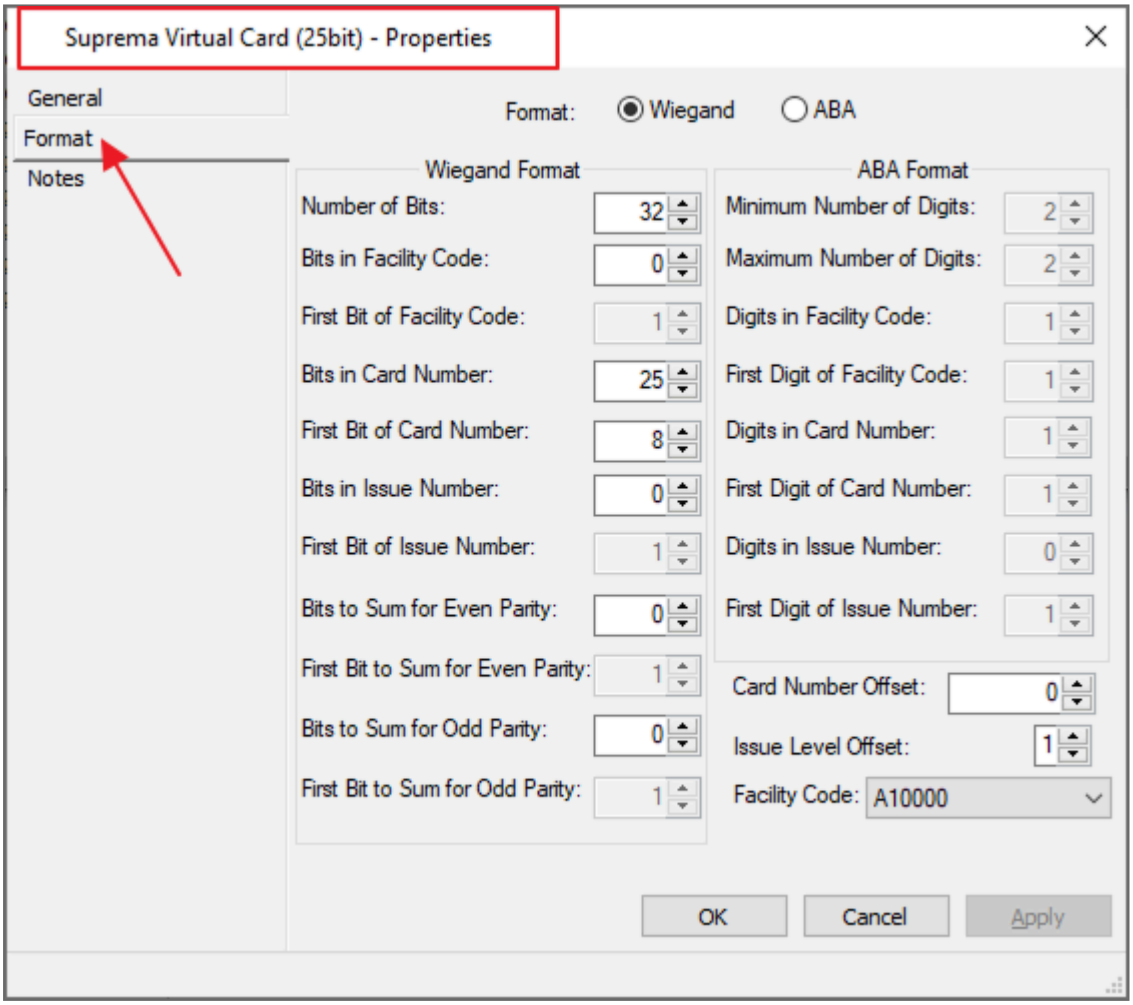
2. 2 つ目のカード形式を **Suprema CSN 32 bits** として作成し、形式を下のとおりに設定します。



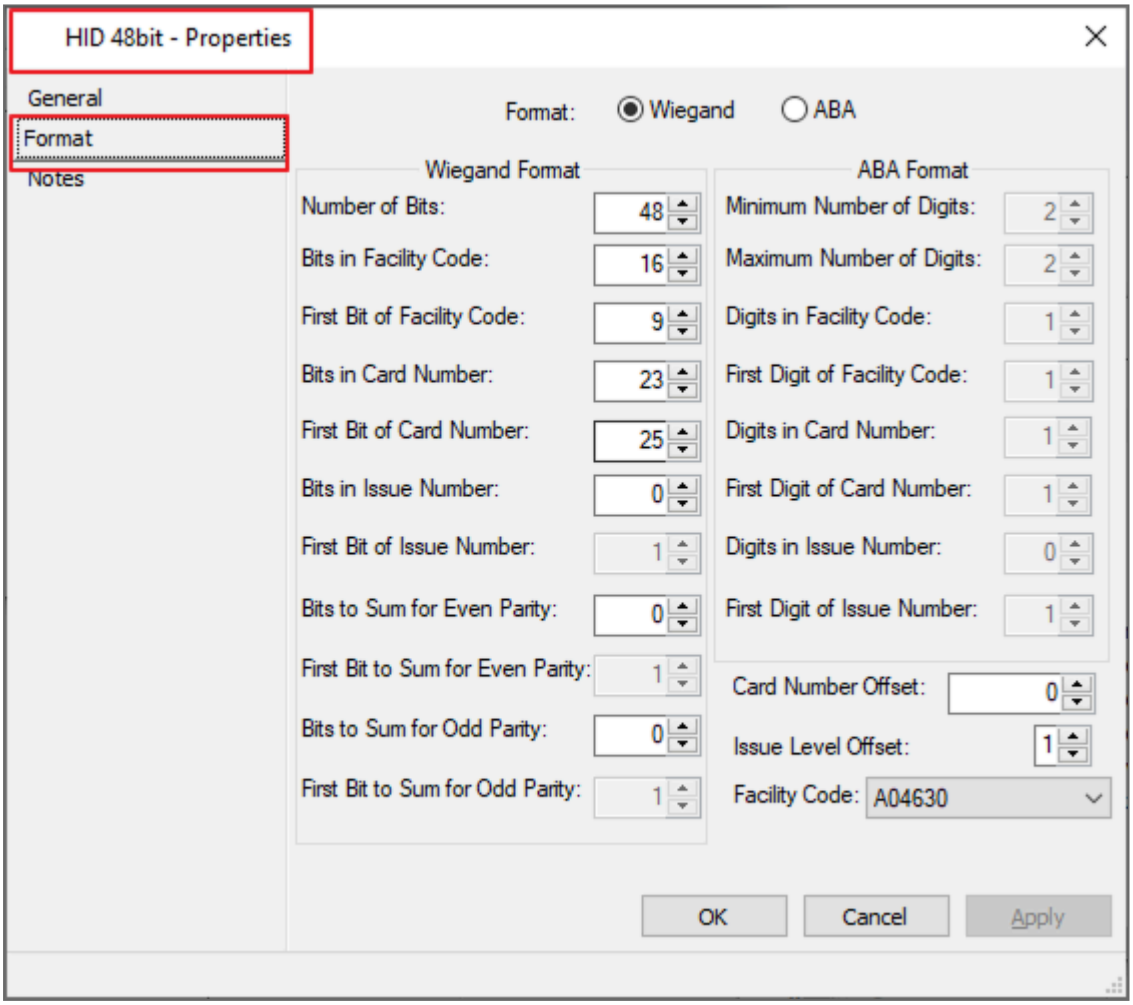
3. 3 つ目のカード形式を **Suprema CSN 56 bits** として作成し、形式を下のとおりに設定します。



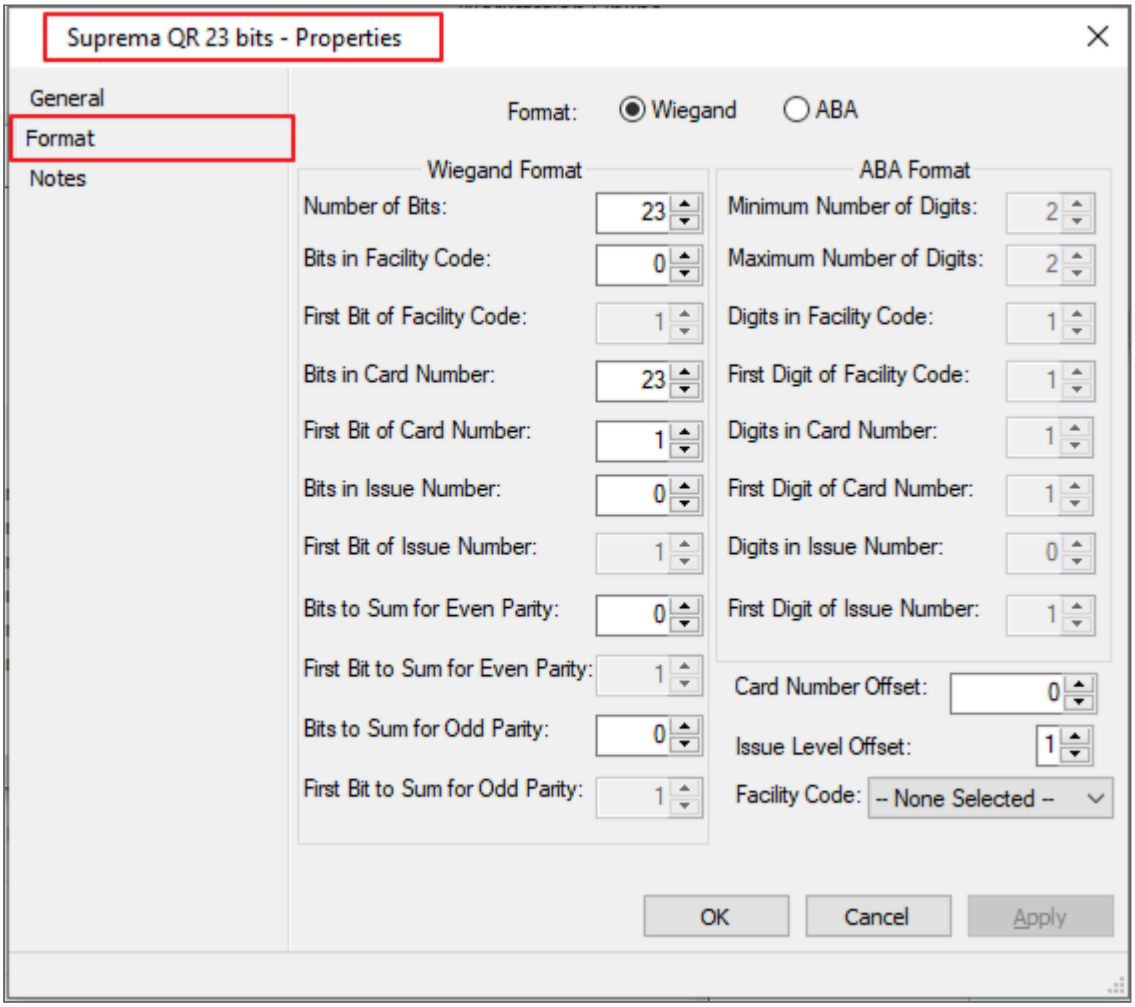
4. 4 つ目のカード形式を **Suprema Virtual Card (25bit)** として**作成**し、形式を下のとおりに**設定**します。



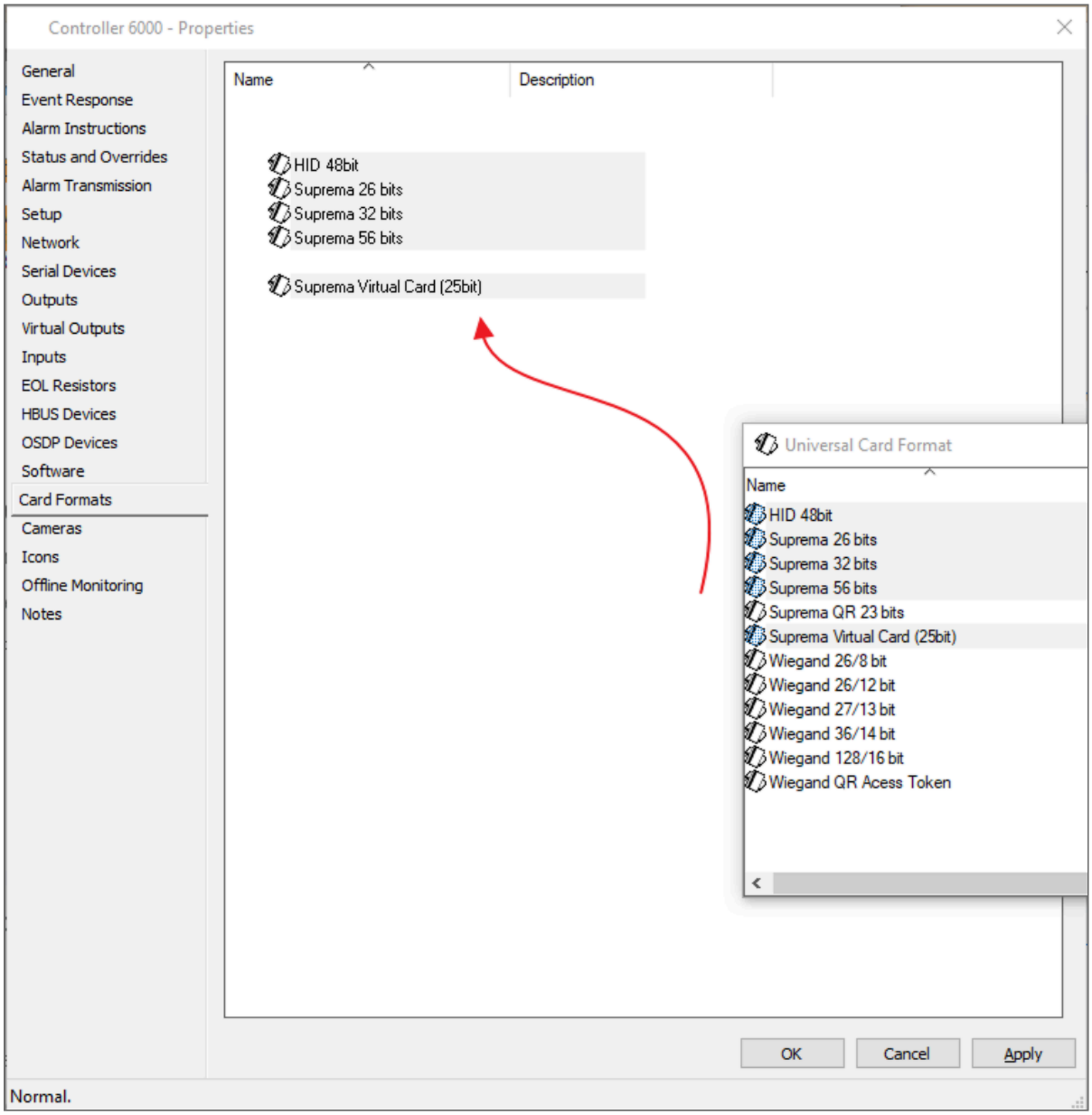
5. 5 つ目のカード形式を **HID 48bit** として**作成**し、形式を下のとおりに**設定**します。



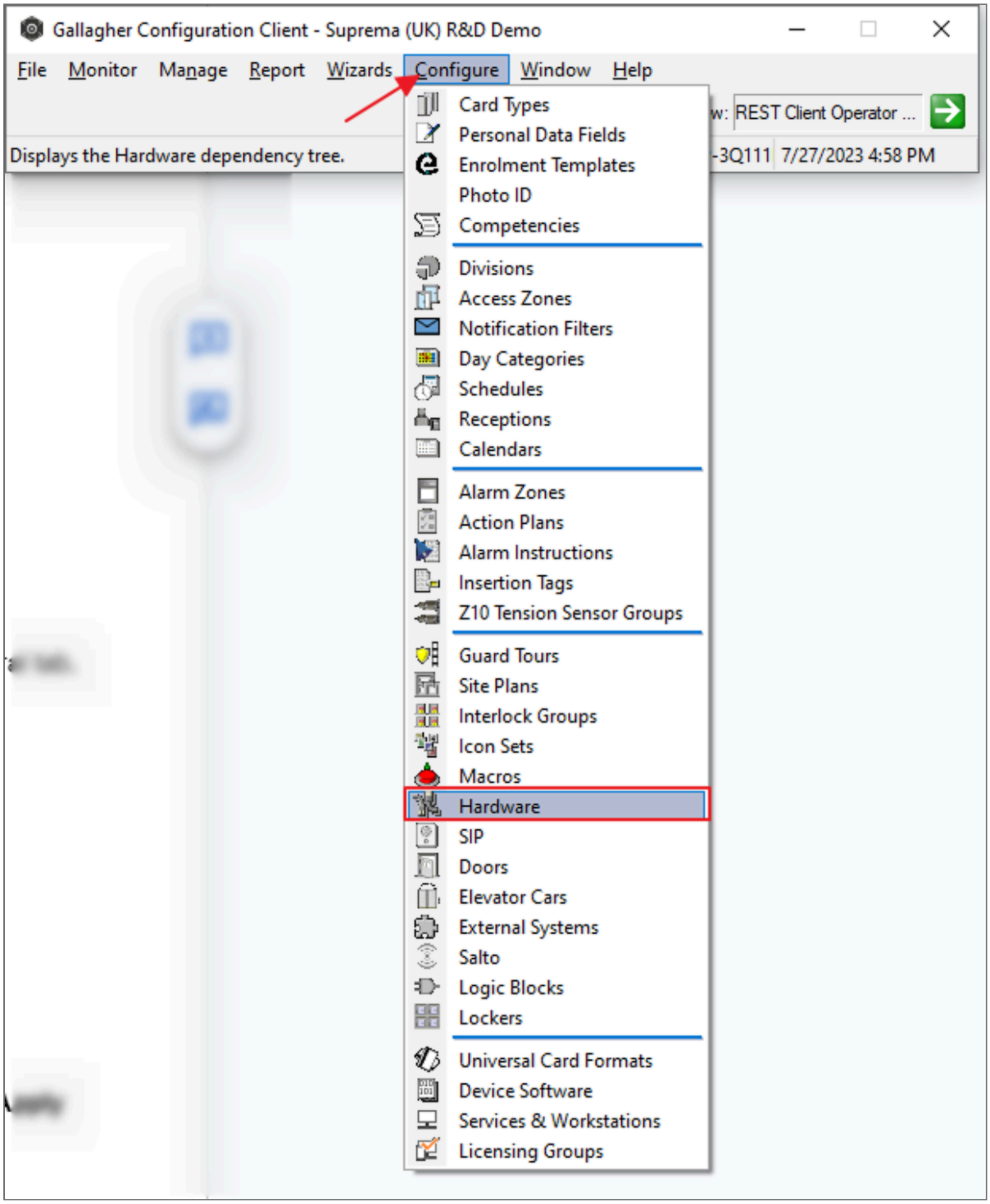
6. 6 つ目のカード形式を **Suprema QR 23 bits** として作成し、形式を下のとおりに設定します。



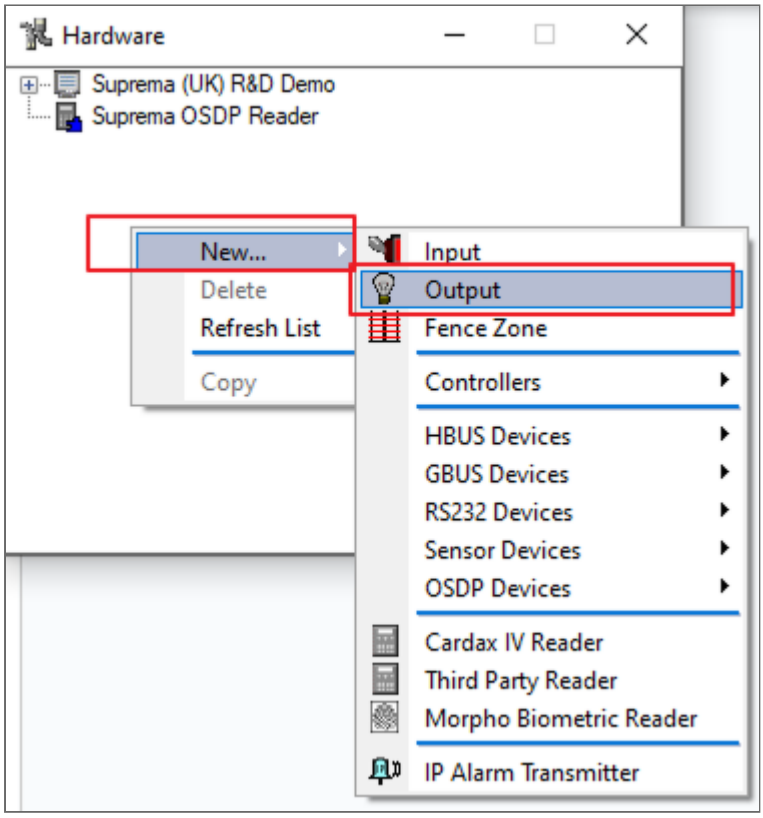
33. 6 つのカード種別をすべてドラッグして Controller properties の Card Format Setting にドロップし、設定を適用します。**OK** を押して、Gallagher Configuration Client のすべてのウィンドウを閉じます。



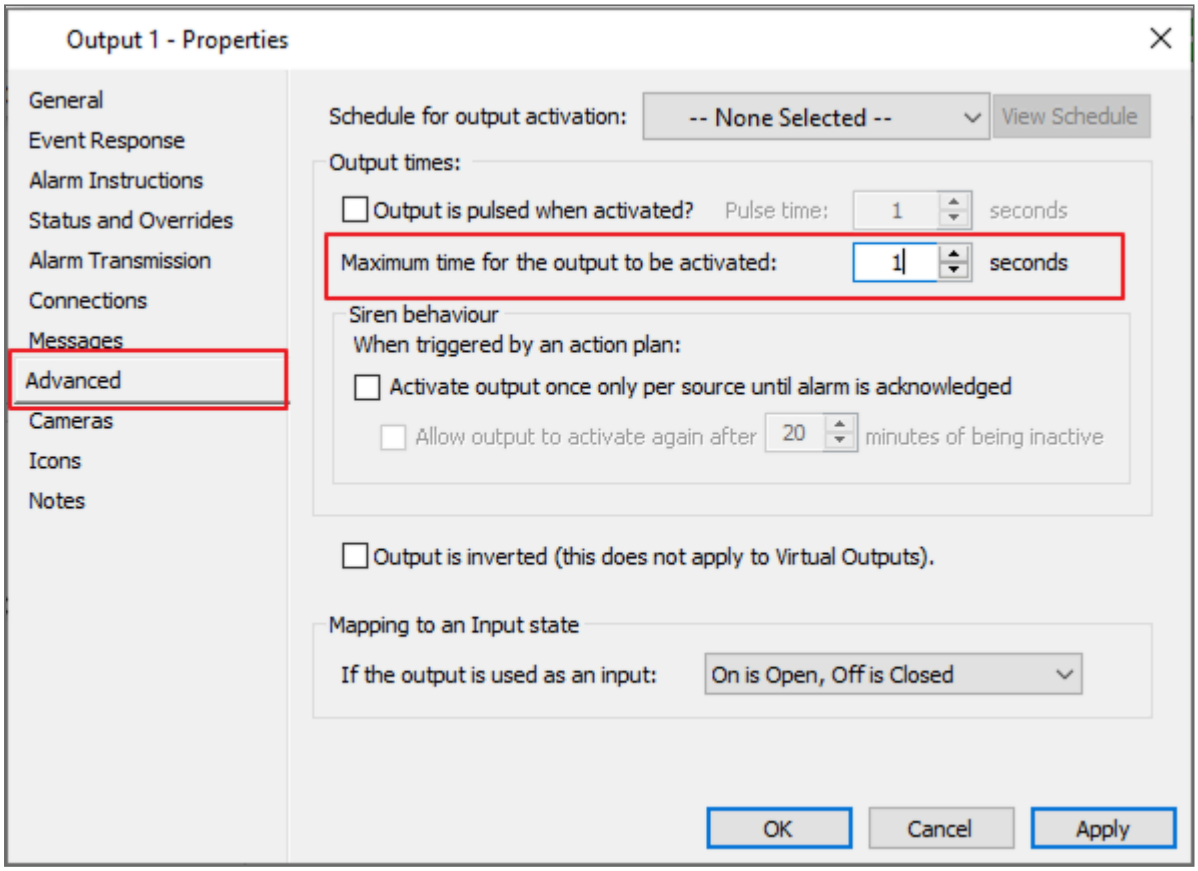
34. Config Client の Configure → Hardware に移動します。



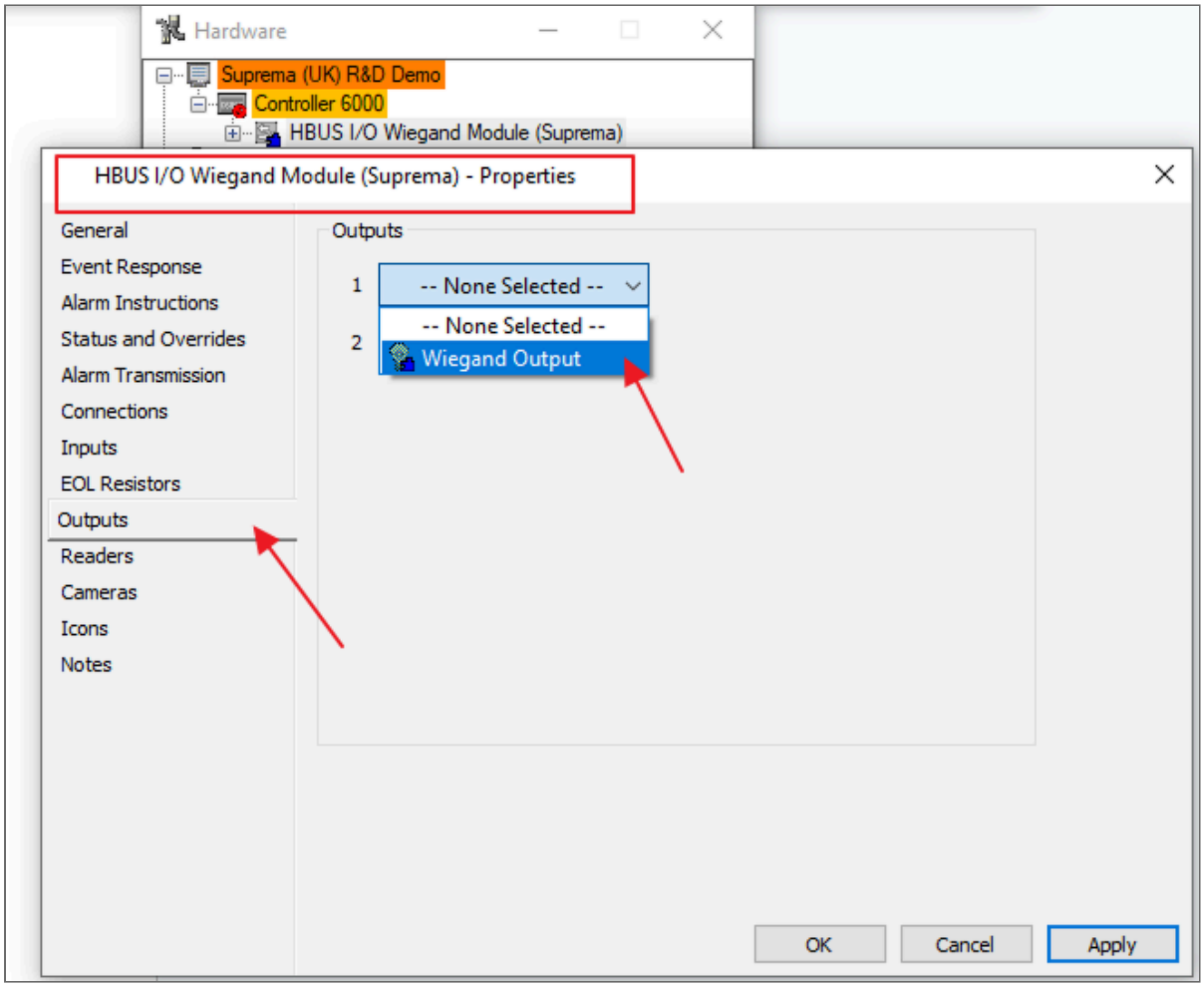
次にウィンドウを**右クリック**し、出力を**作成**して、一般タブで名前を **Wiegand Output** に**設定**します。



35. 次に左側の Advance をクリックし、Output times オプションで 1 秒に設定して、**Apply** と **OK** を押します。

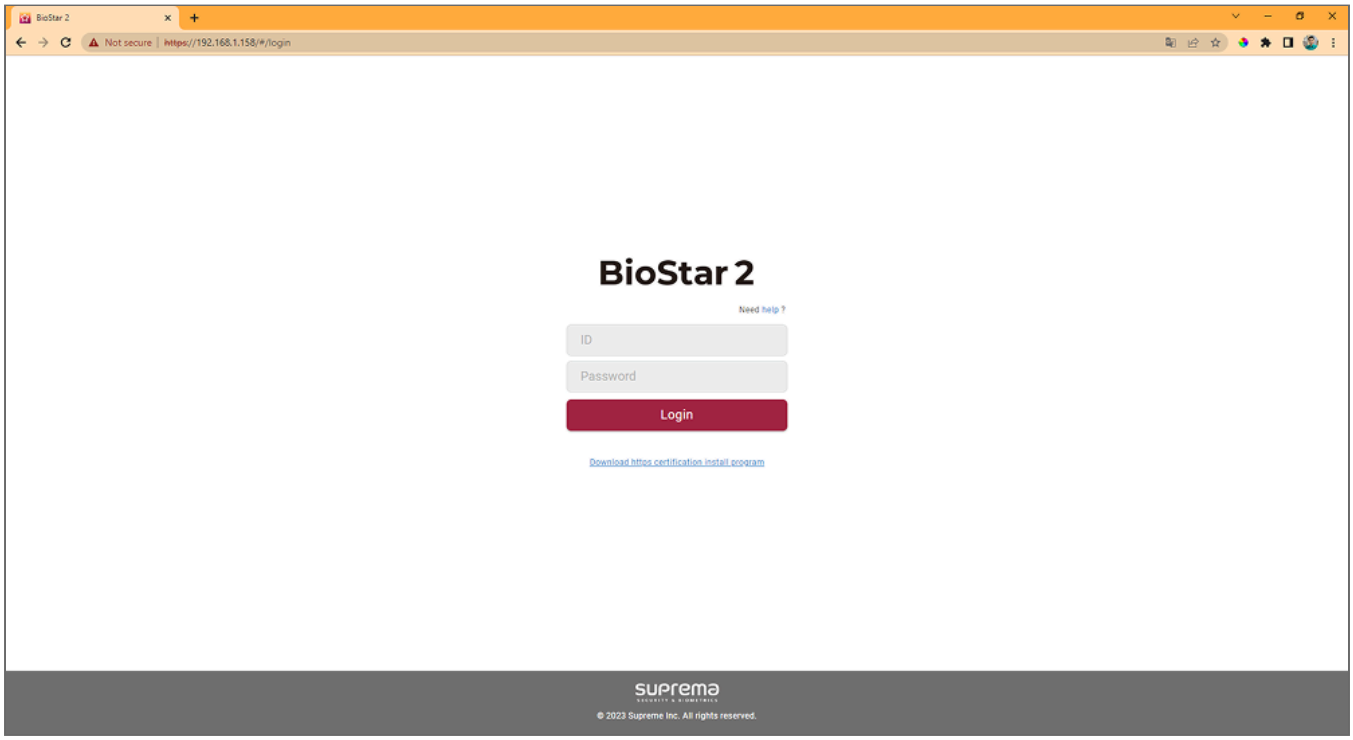


36. 次に hardware window → HBUS I/O Wiegand Module (Suprema) を左側でダブルクリックし、Outputs に移動して Wiegand Output を選択し、**Apply** と **OK** を押します。

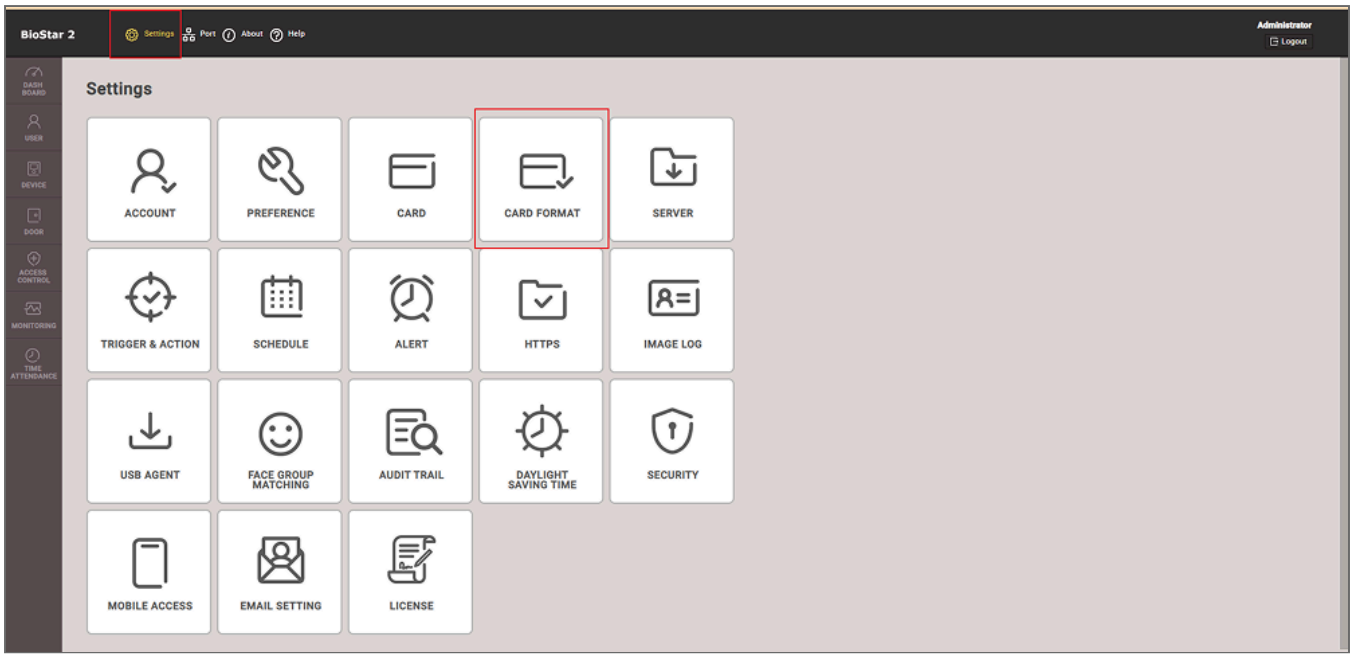


BioStar 2 設定

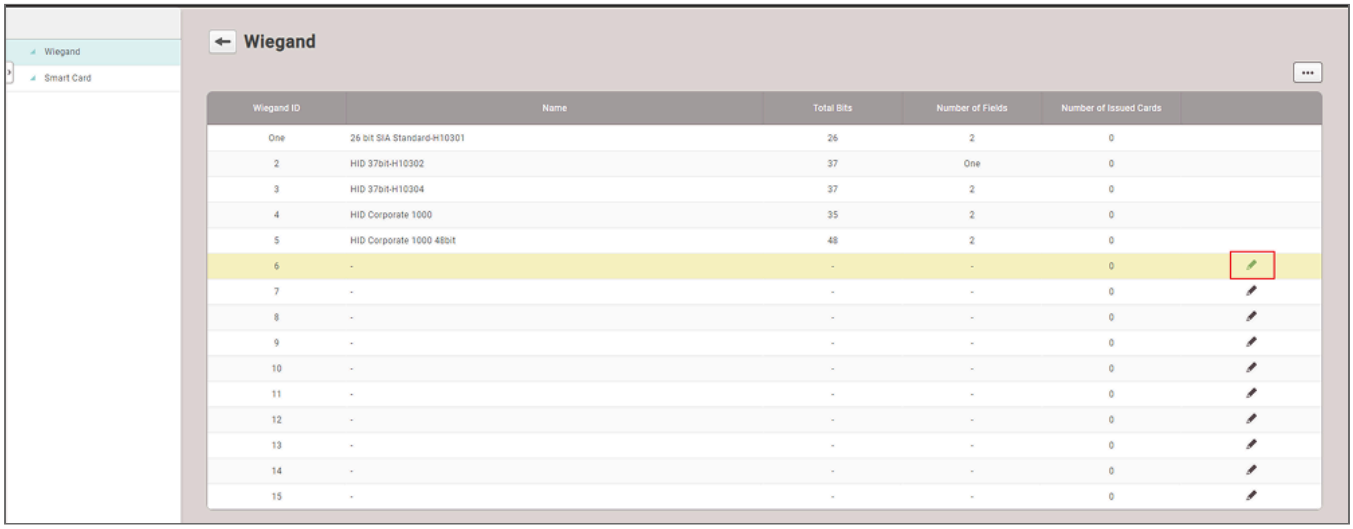
1. BioStar 2 を開くには、ブラウザーで https://[Your system IP Address]/#/login と入力すると、ログインフォームが開きます。



2. BioStar 2 の資格情報を**入力**してログインし、設定ページに**移動**して、Card Format を**選択**します。

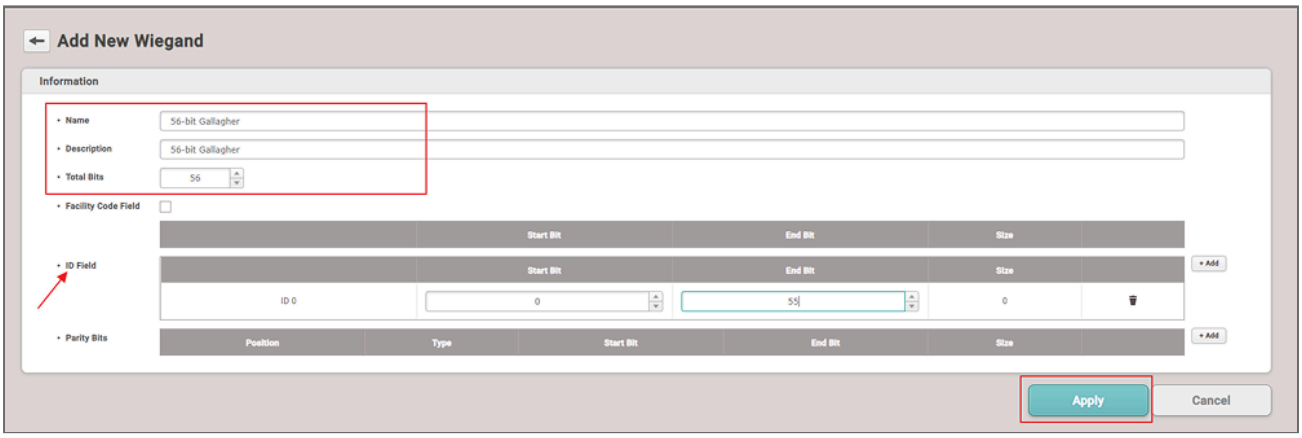


3. カード設定で **edit** ボタンを**クリック**し、新しいカード形式を作成します。

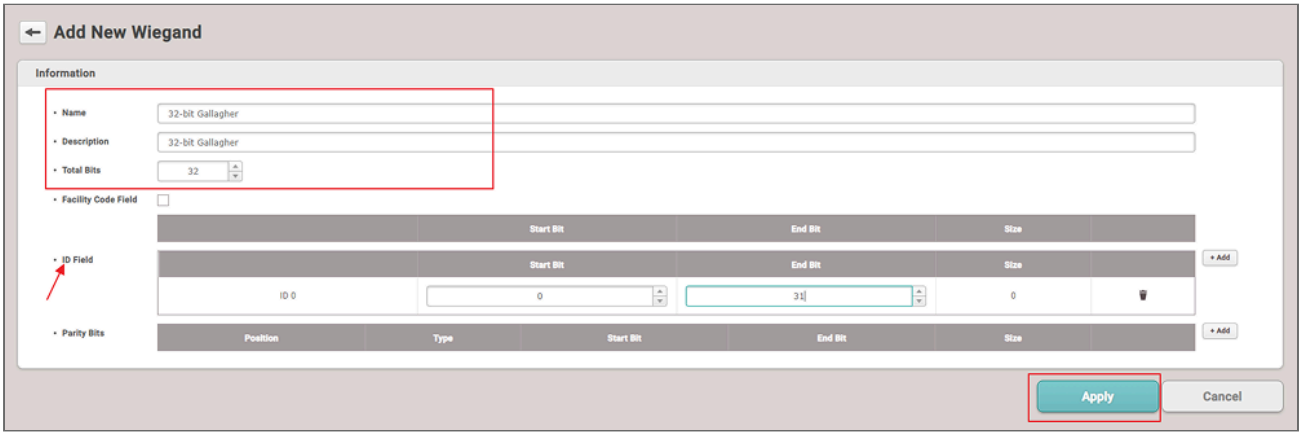


4. ここでも **56-bit、32-bit、26-bit** の 3 つのカード種別を作成する必要があります。

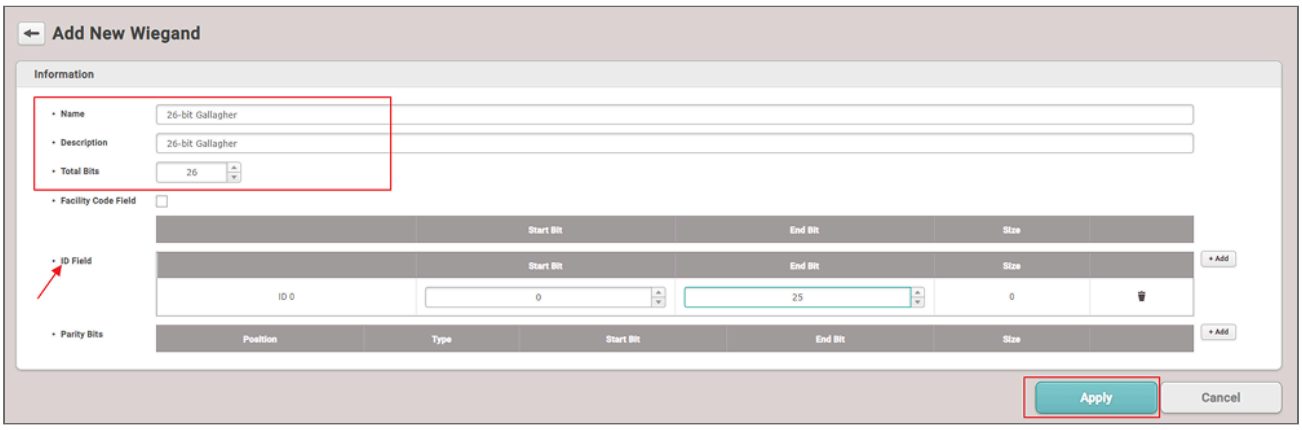
    1. 名前を **56-bit Gallagher**、total bits を 56 に**設定**し、ID field で **add** を**押して** start bit を 0、end bit を 55 に**設定**します。



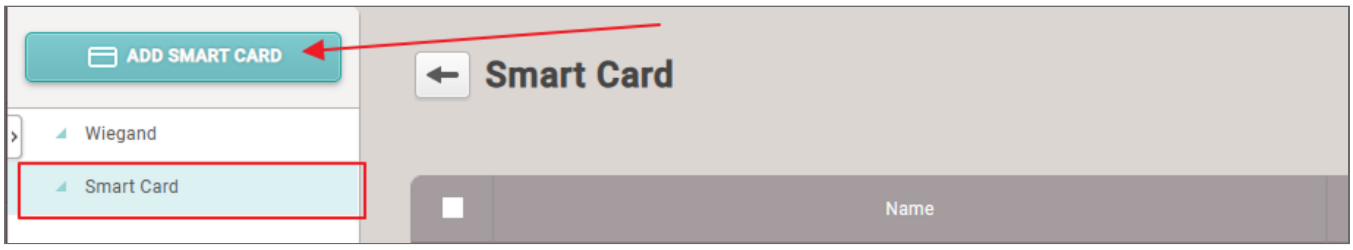
2. 名前を **32-bit Gallagher**、total bits を 32 に**設定**し、ID field で **add** を押して start bit を 0、end bit を 31 に**設定**します。



3. 名前を **26-bit Gallagher**、total bits を 26 に**設定**し、ID field で **add** を押して start bit を 0、end bit を 25 に**設定**します。

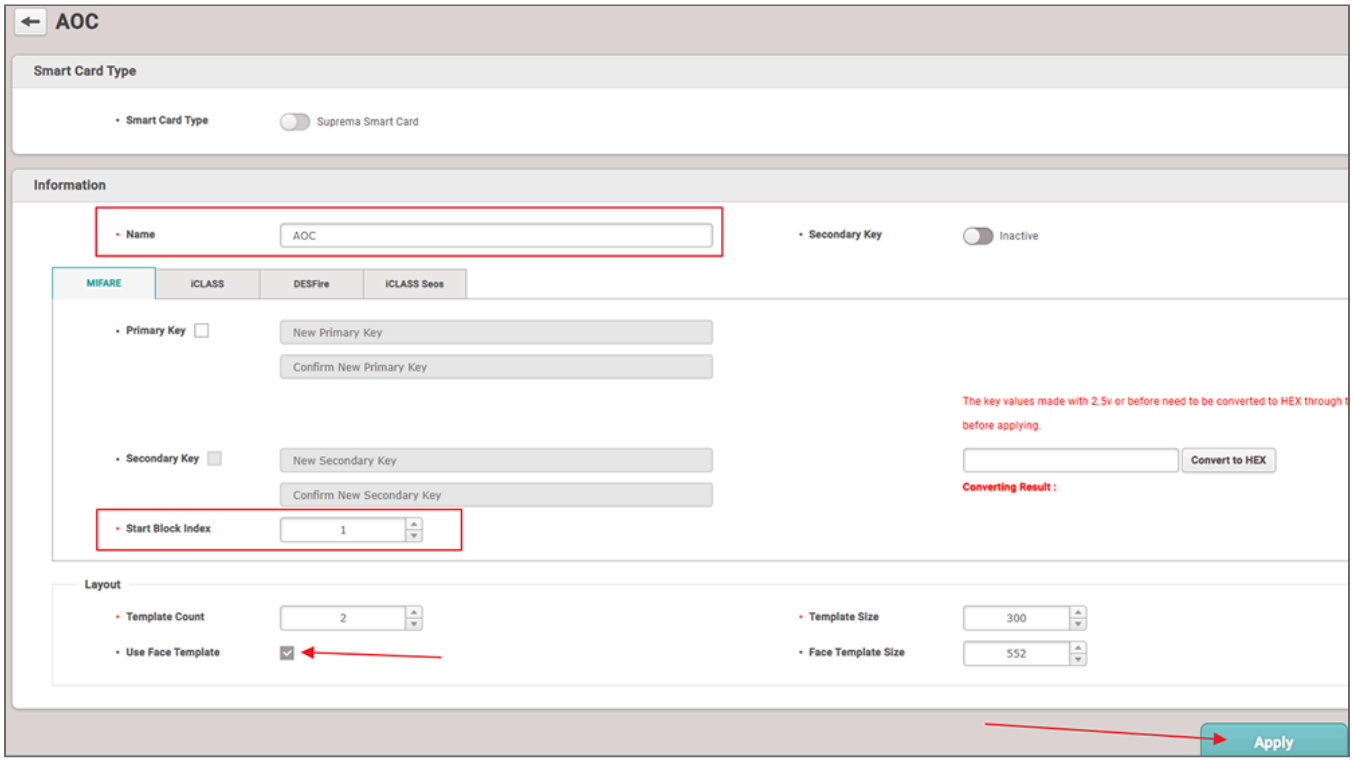


5. 次にカード形式内で、smart card ボタンを**押して** smart card セクションに**移動**し、ADD SMART CARD ボタンを**クリック**します。

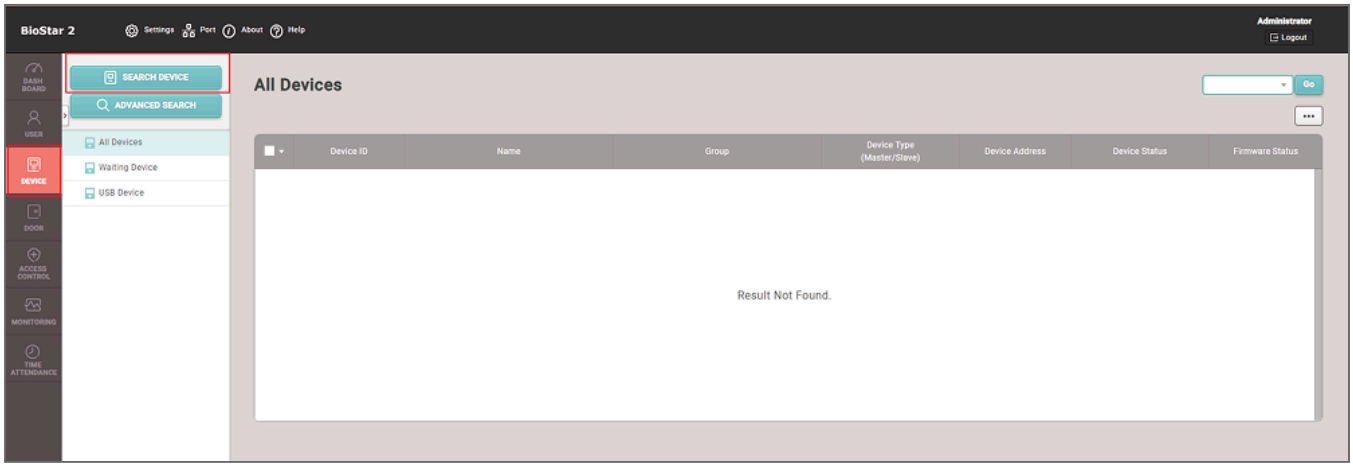


6. 次に名前を AOC Inside MIFARE に**入力**し、Start Block Index に 1 を**入力**し、Use Face template のチェックボックスを**オンにして**、Apply ボタンを**押します**。

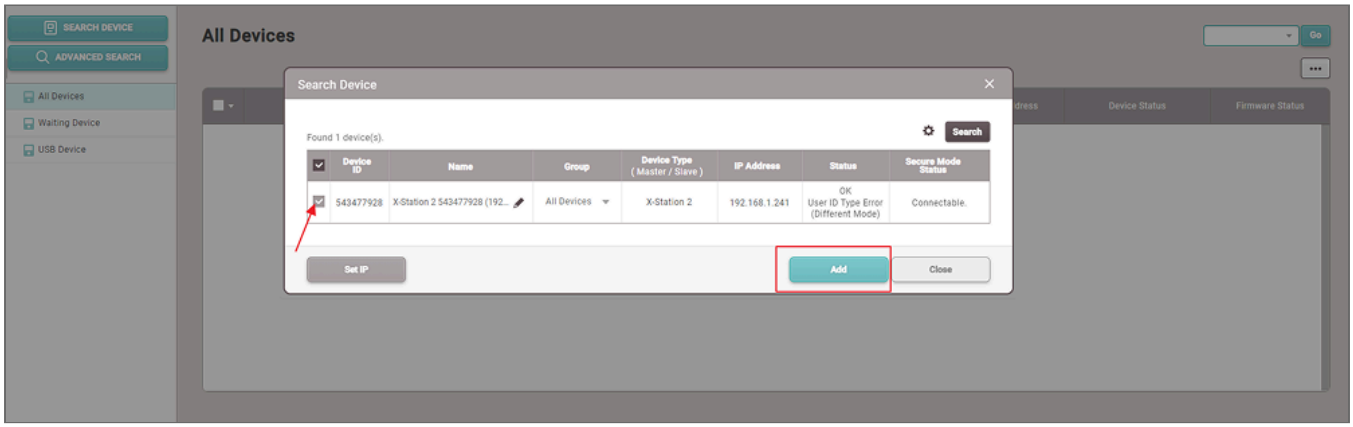
> **情報**
> 顔の表示を使わず、smart card では fingerprint のみを使う場合は、チェックボックスをオフにできます。



7. デバイスをシステムに接続するには、device panel に移動し、SEARCH DEVICE ボタンを押します。



8. 次に search ボタンを押し、デバイスを選択して、Add ボタンを押します。



9. 接続したデバイスは、左側の device panel に一覧表示されます。



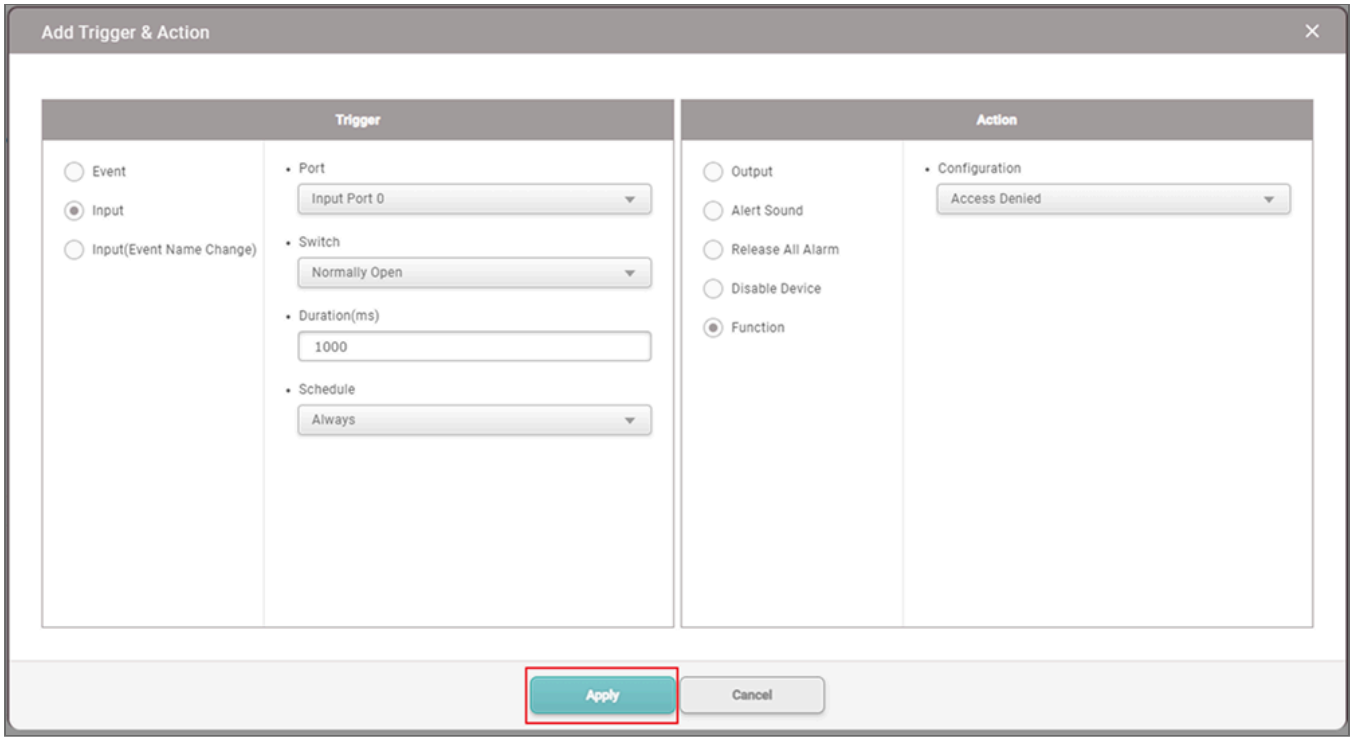
Wiegand の READER CONNECTION

1. Wiegand 接続で接続されたデバイスを**クリック**します。 Card Type が表示されるまで**下にスクロール**します。

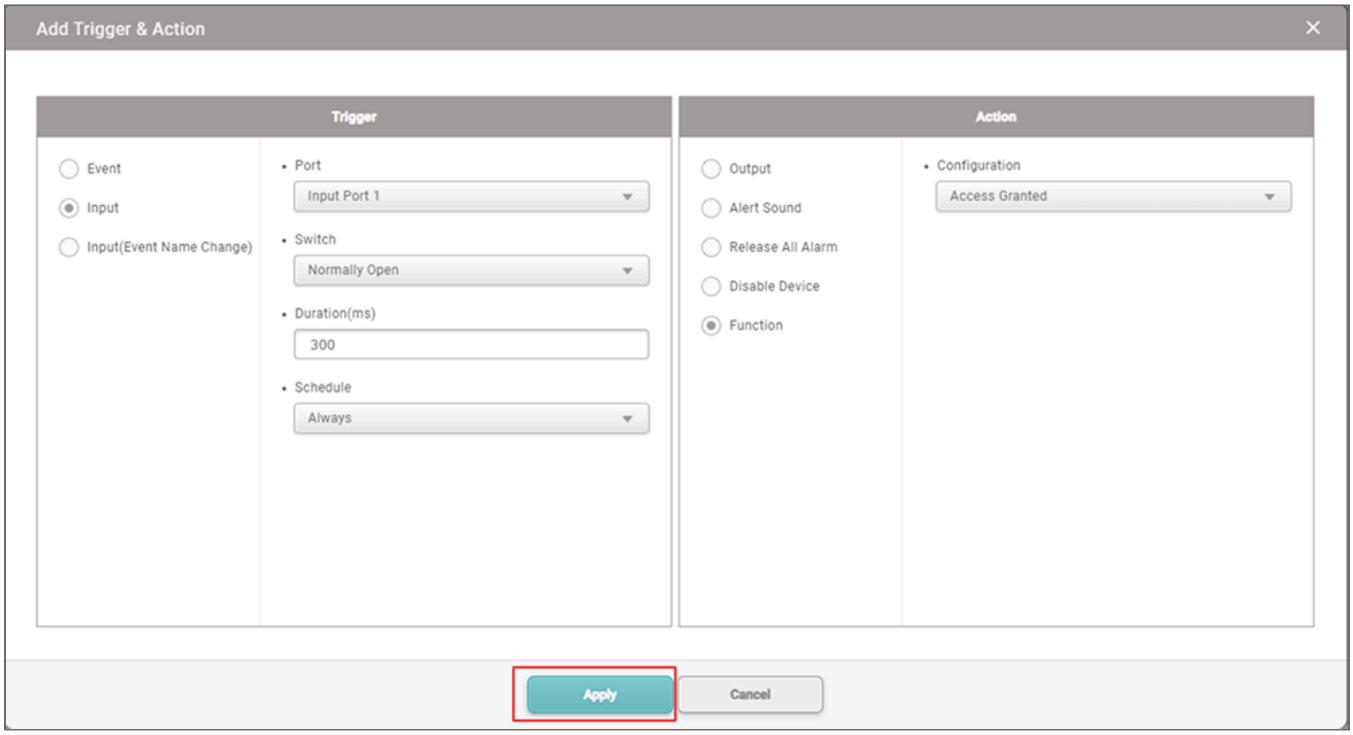
   CSN card を**オンにし**、**Mifare/Felica** にチェックし、形式 type を **Wiegand**、Byte order を **LSB**、Wiegand format を **56-bit Gallagher** に**設定**します。



2. 次に advanced setting に**移動**し、trigger and action が表示されるまで下にスクロールして add ボタンを**押し**、画像のとおりに field を**設定**します。



3. もう一度 add ボタンを**押して**、別の trigger and action を追加します。



4. Advanced Section の Trigger & Action：Wiegand setting では、Input/Output を **Output**、Wiegand Input Format を Default、Pulse width を **40**、pulse interval を **10000**、output mode を **normal** に設定し、fail code を確認して、output info を **Card ID** にします。



OSDP READER CONNECTION

1. OSDP 接続では、OSDP パネルに接続されたデバイスを**クリック**し、Serial が表示されるまで下にスクロールします。

   RS485 を Default に、Baud rate を **115200** に**設定**します。



2. intelligent slave expectation code を **Enabled**、output info を Card ID、OSDP ID を **0** にします。

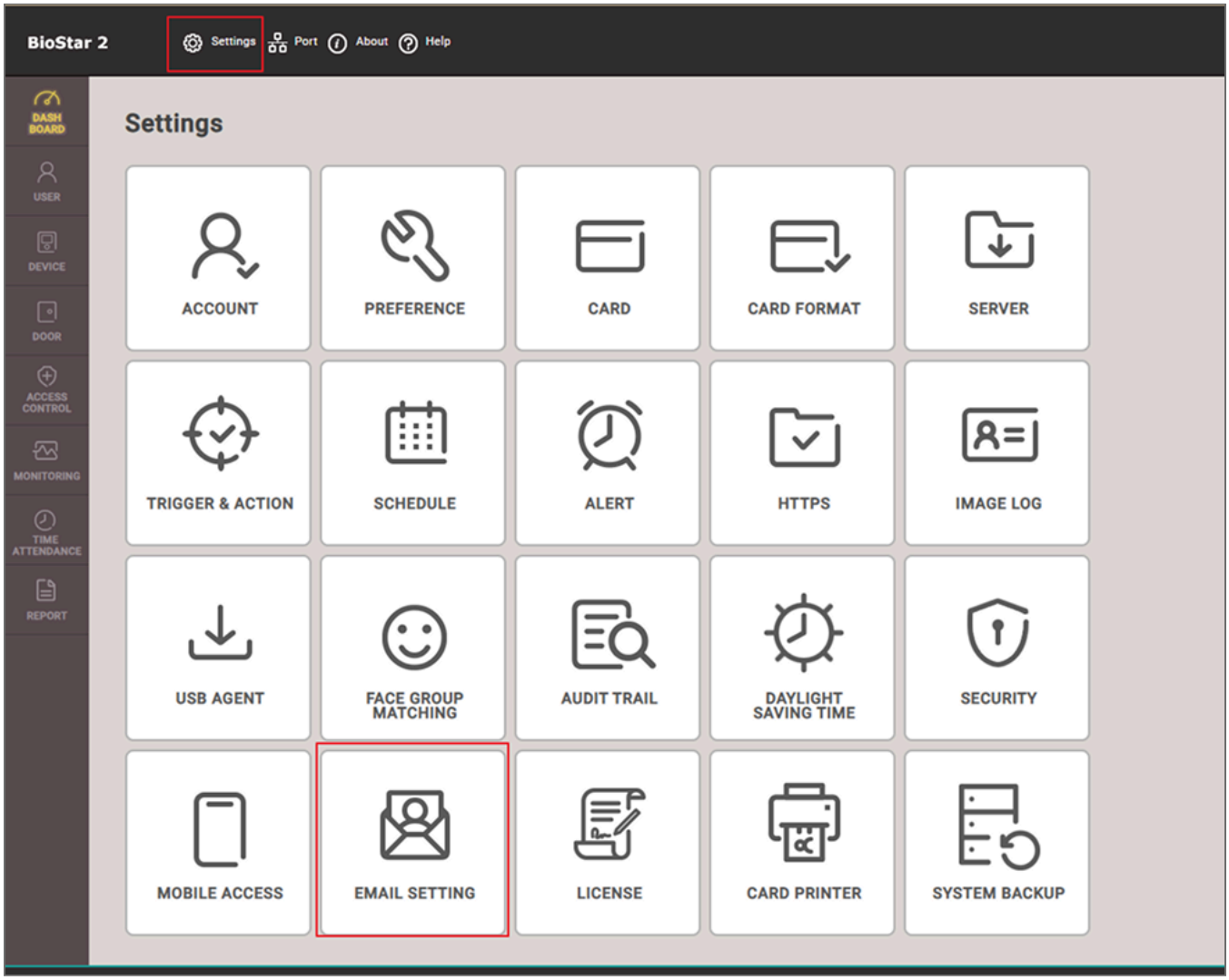
> **情報**
> OSDP デバイスが複数ある場合は、OSDP ID を別の番号に変更し、output の Info は Card ID にしてください。



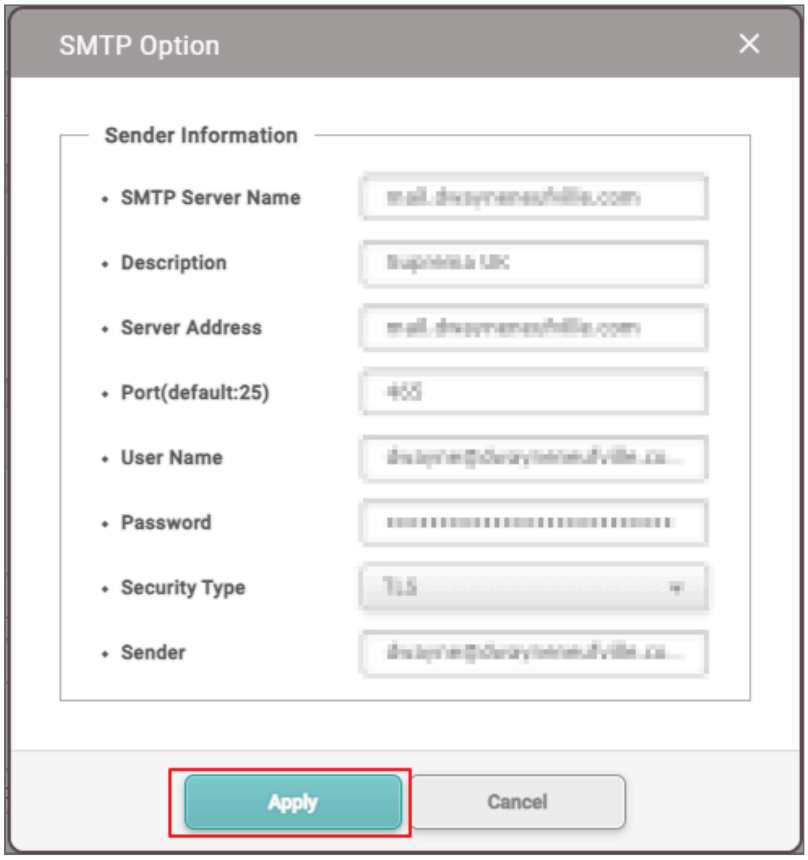
QR コード用のメール設定

> **情報**
>
> - QR コードには、メール確認とユーザープロファイルのメールが必須です。
> - メールにはライセンスが必要です。 必要なライセンスを取得するには管理者にお問い合わせください。

1. 設定ページに移動し、Email Settings を選択します。

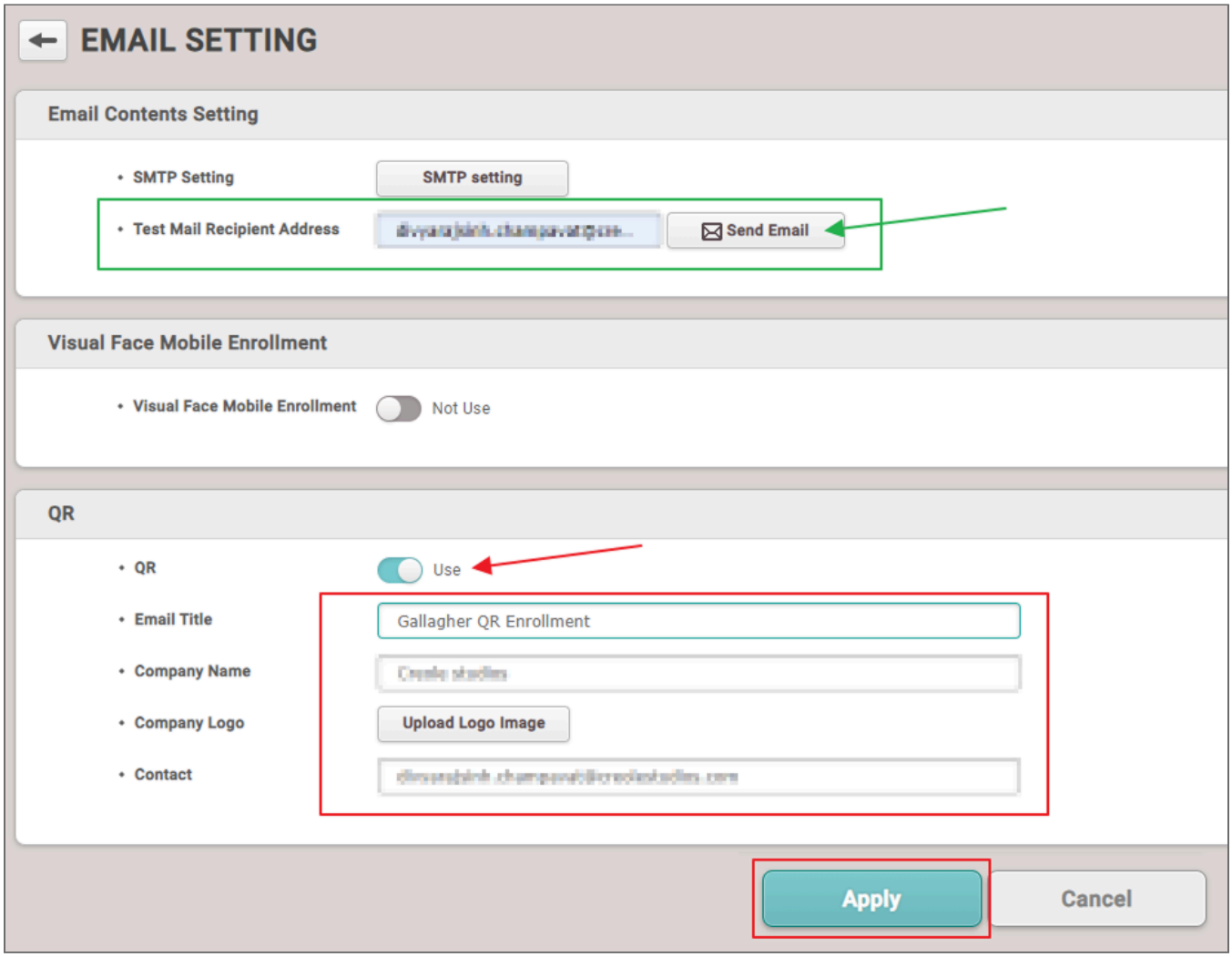


2. メール設定内の SMTP setting ボタンを押し、SMTP オプションの詳細を入力して、**Apply** ボタンを押します。



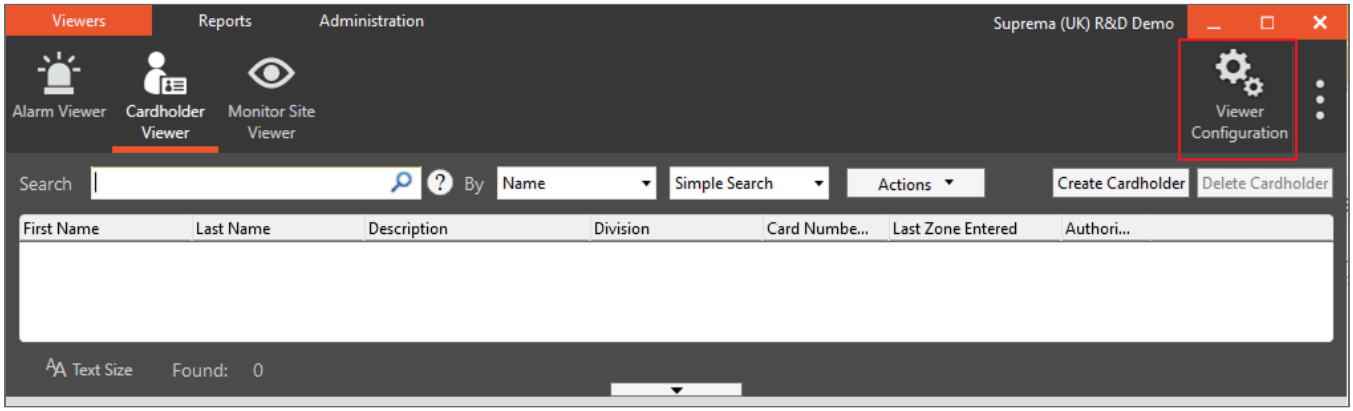
3. 確認用にはテストメール機能を使用できます。送信先のメールアドレスを入力し、send email ボタンを**押します**。

   QR Code カードを使うには、設定内で QR オプションを**有効にし**、要件に従って詳細を入力して、Apply ボタンを**押します**。



Suprema Integration with Gallagher v2.0

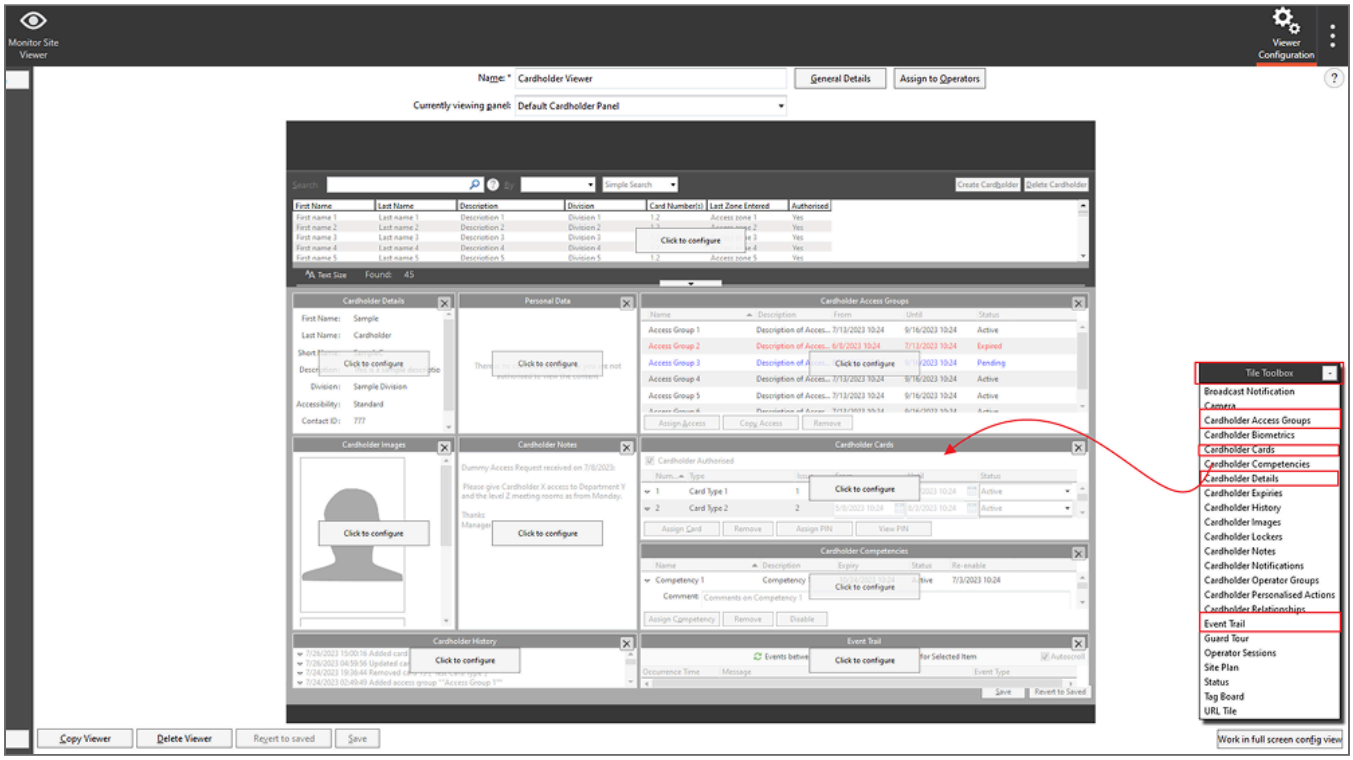
1. Cardholder viewer オプションで Gallagher Command Centre を開き、viewer configuration に移動します。



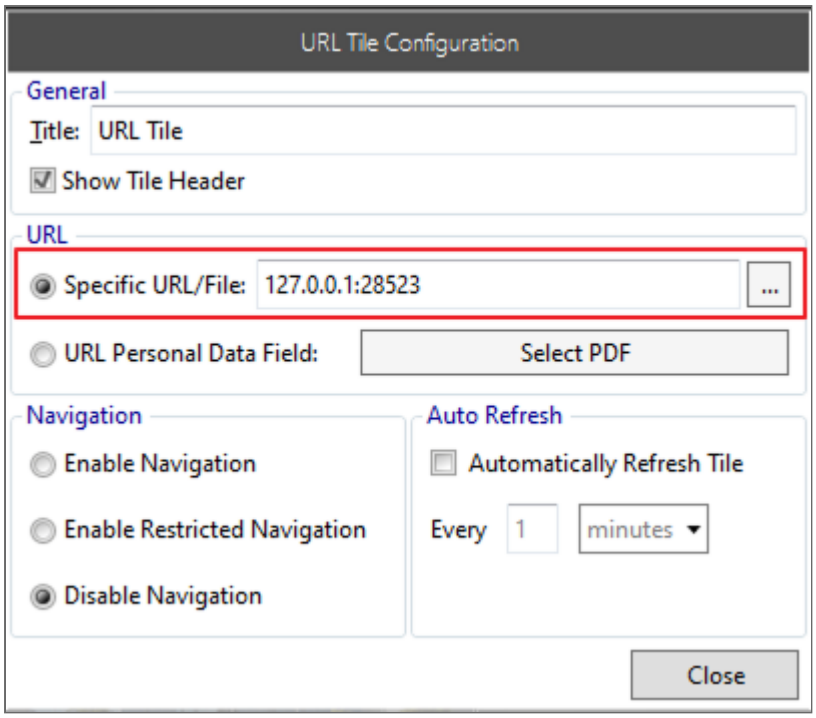
2. Viewer Configuration で、下の画像のようにウィンドウを設定し、window toolbox を使ってウィンドウを**ドラッグ＆ドロップ**します。

   - Cardholder Details
   - Cardholder Access Groups
   - Cardholder Cards

- Event trail
- URL Tile
- Cardholder Images

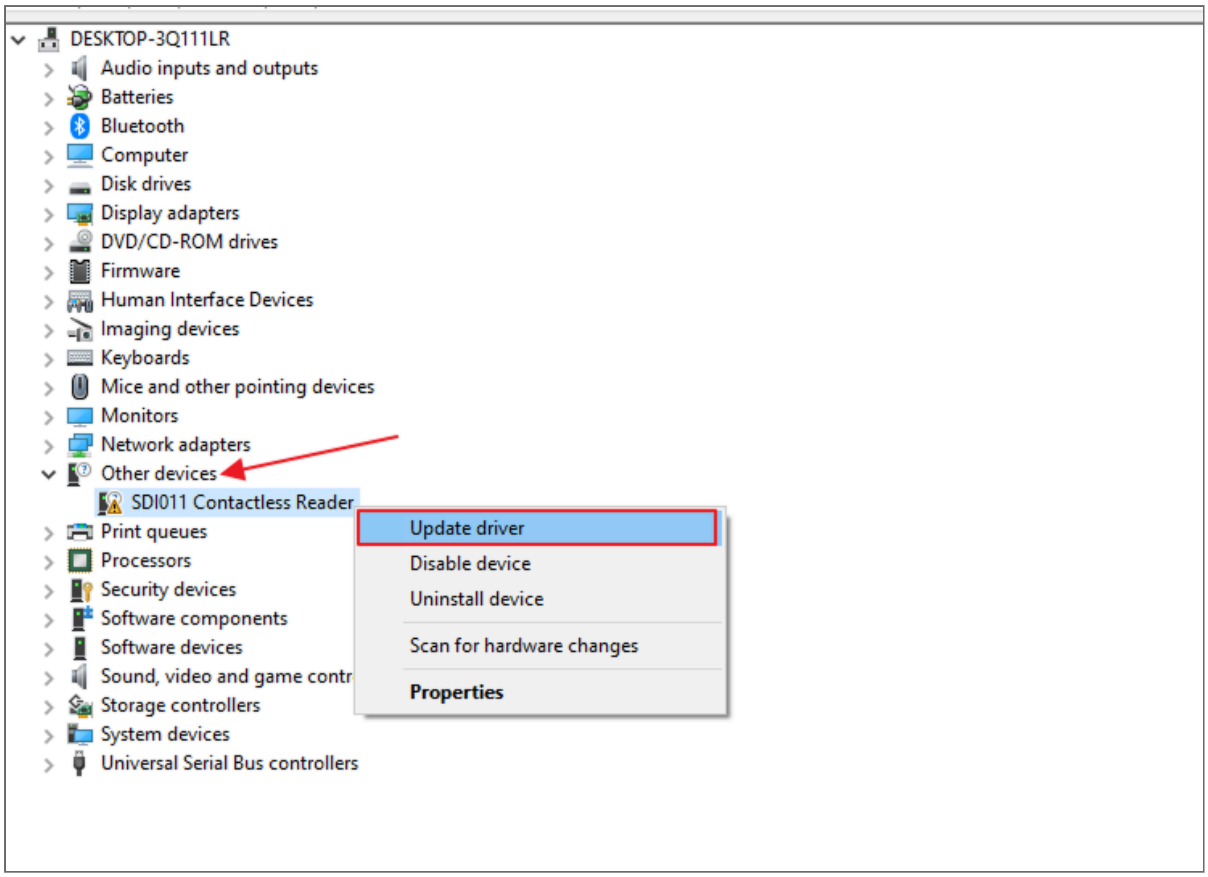


3. URL ウィンドウで**クリック**し、Specific URL を `<127.0.0.1>:28523` に設定して、navigation を Disable Navigation に**選択**します。 そして **save button を押して**設定を保存します。

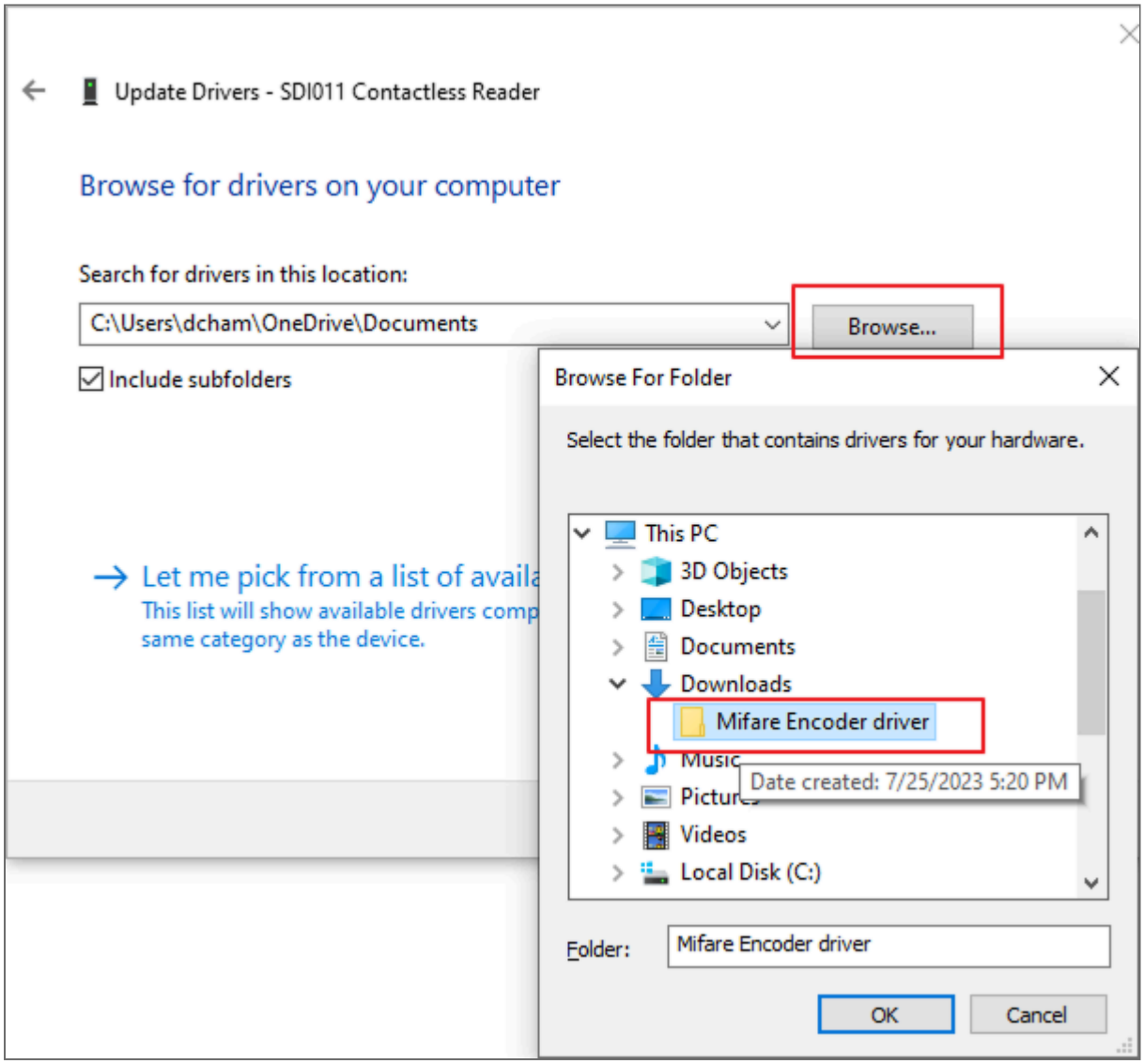


4. 設定完了後、**save button を押し**、viewer configuration を**右クリック**して viewer を再読み込みし、変更を確認します。
5. **Mifare Encoder を PC に接続します。**
6. システムのデバイスマネージャーのその他のデバイスにある SDI011 Contactless Reader（環境によっては別のデバイス）を

右クリックし、ドライバーの更新を**選択**します。



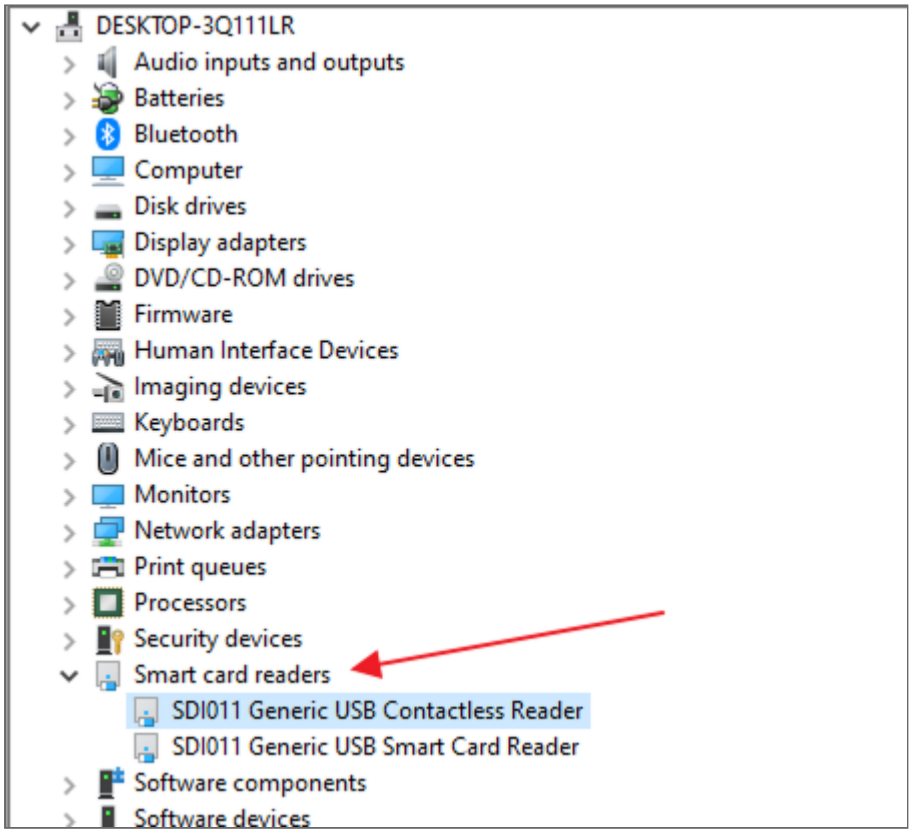
7. ドライバーをコンピューター上で検索し、提供されたフォルダーを**選択**します。



8. ドライバーを初めて更新すると、スマートカードリーダーが使用可能になります。

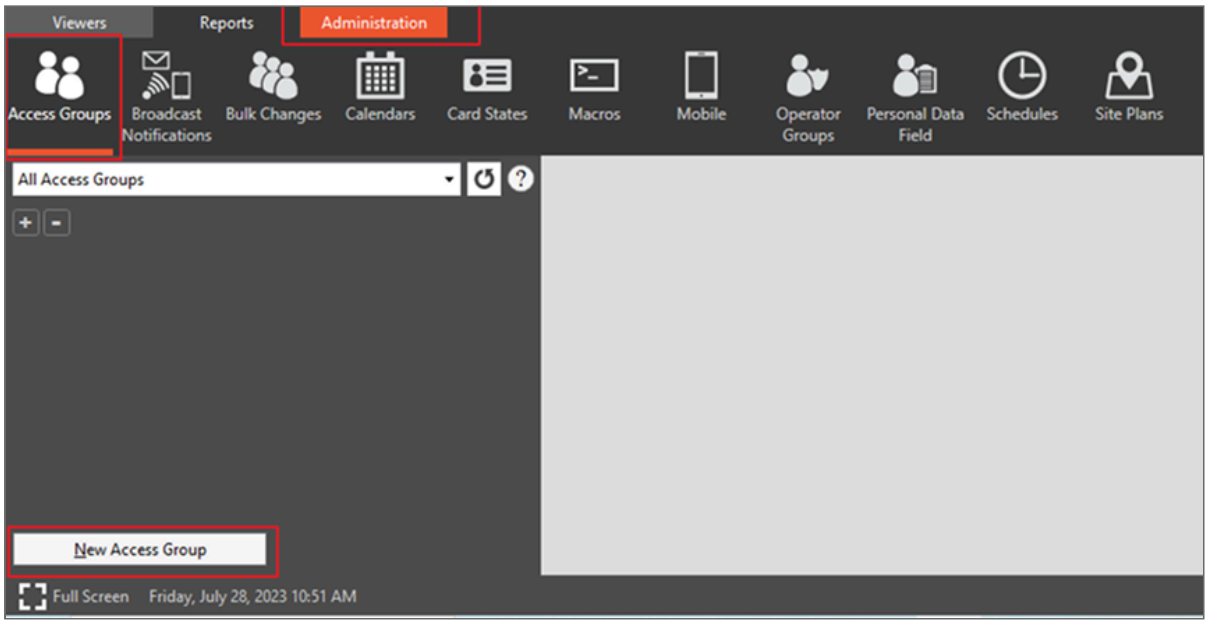
> **情報**
> USB デバイス名はデバイスごとに異なる場合があります。

9. 次に同じファイルで Contactless Reader ドライバーを**再度更新**します。 その後、新しいスマートカードドライバーが使用可能になります。

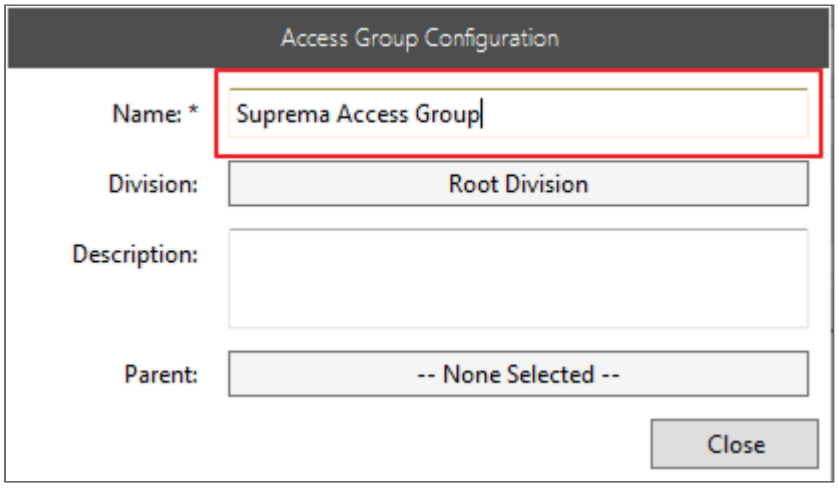


アクセスグループを追加

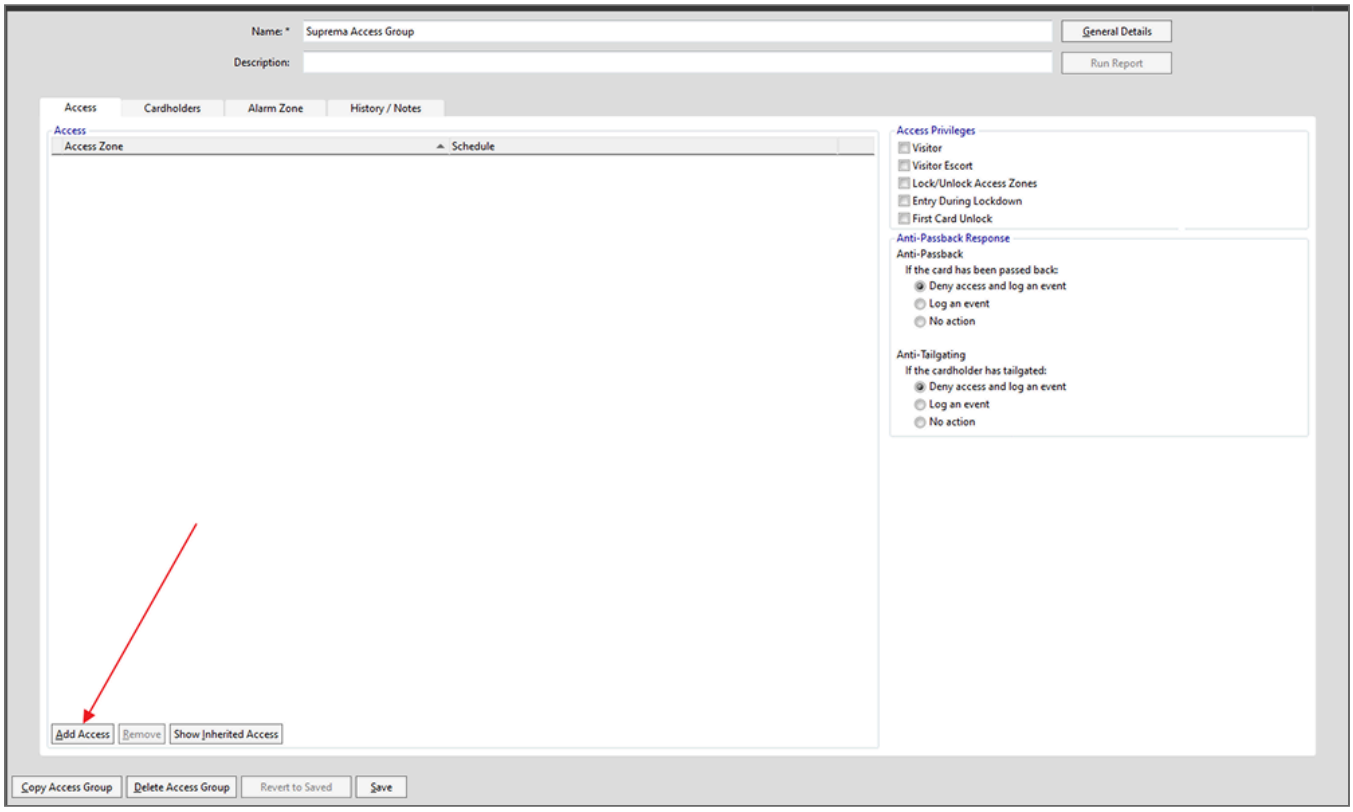
1. **Administration** に移動し、左上にある **Access Groups** をクリックします。すると左下に **New Access Group** ボタンが表示されます。 そのボタンをクリックします。



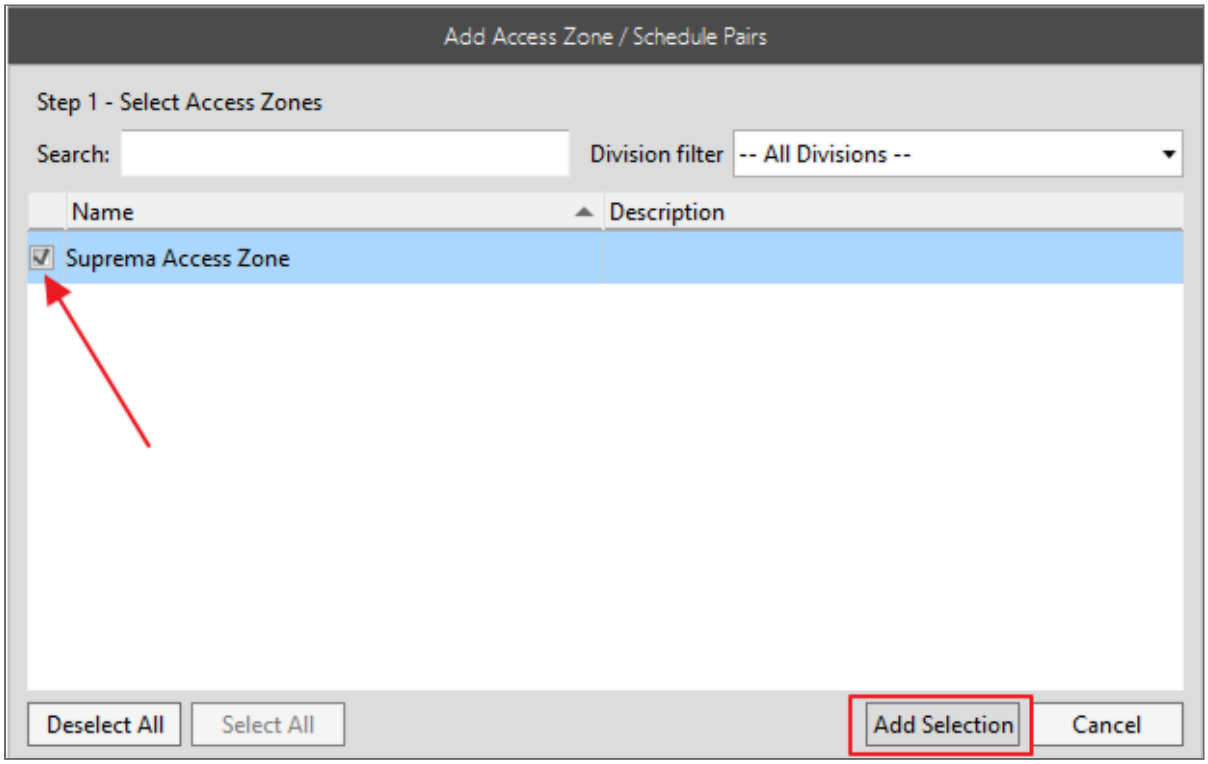
2. **New Access Group** ボタンをクリックすると、下の画像のようなポップアップが開きます。名前を **Suprema Access Group** に設定し、Close ボタンをクリックするとポップアップが閉じます。



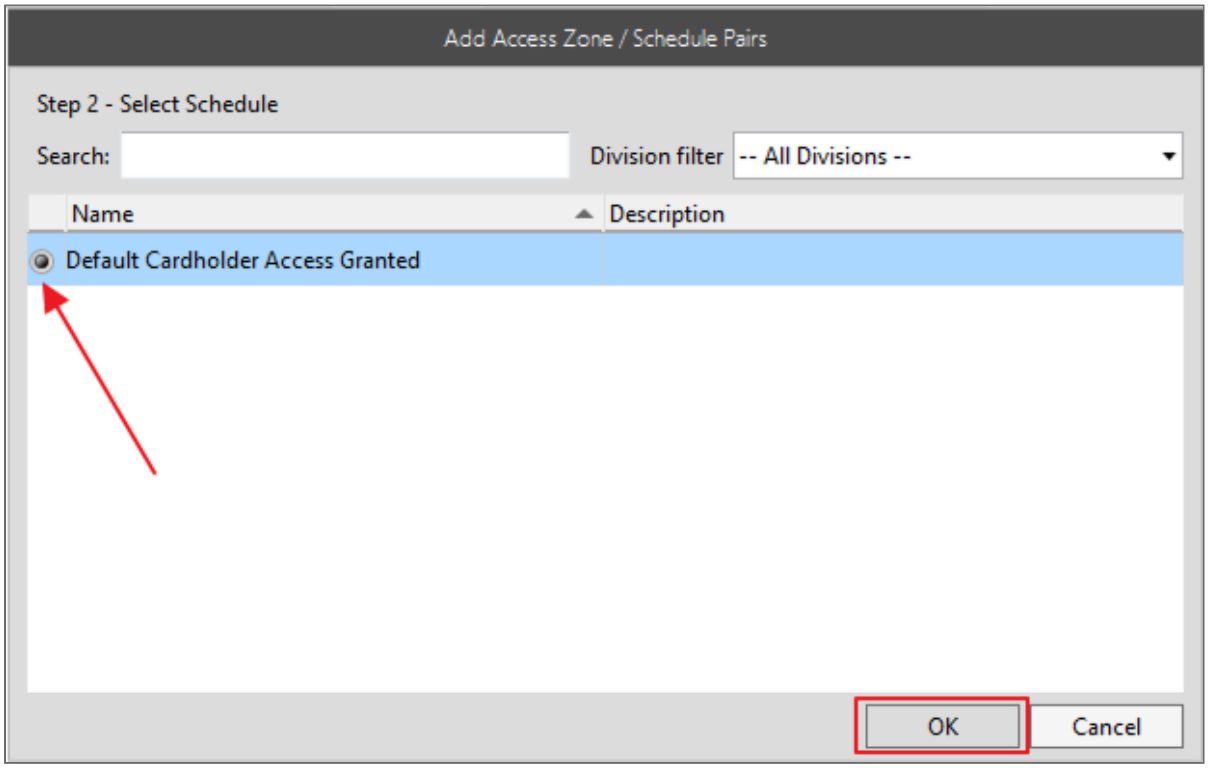
3. Close ボタンをクリックすると、下の画像のような画面が表示されるので、左下隅の **Add Access** ボタンをクリックします。



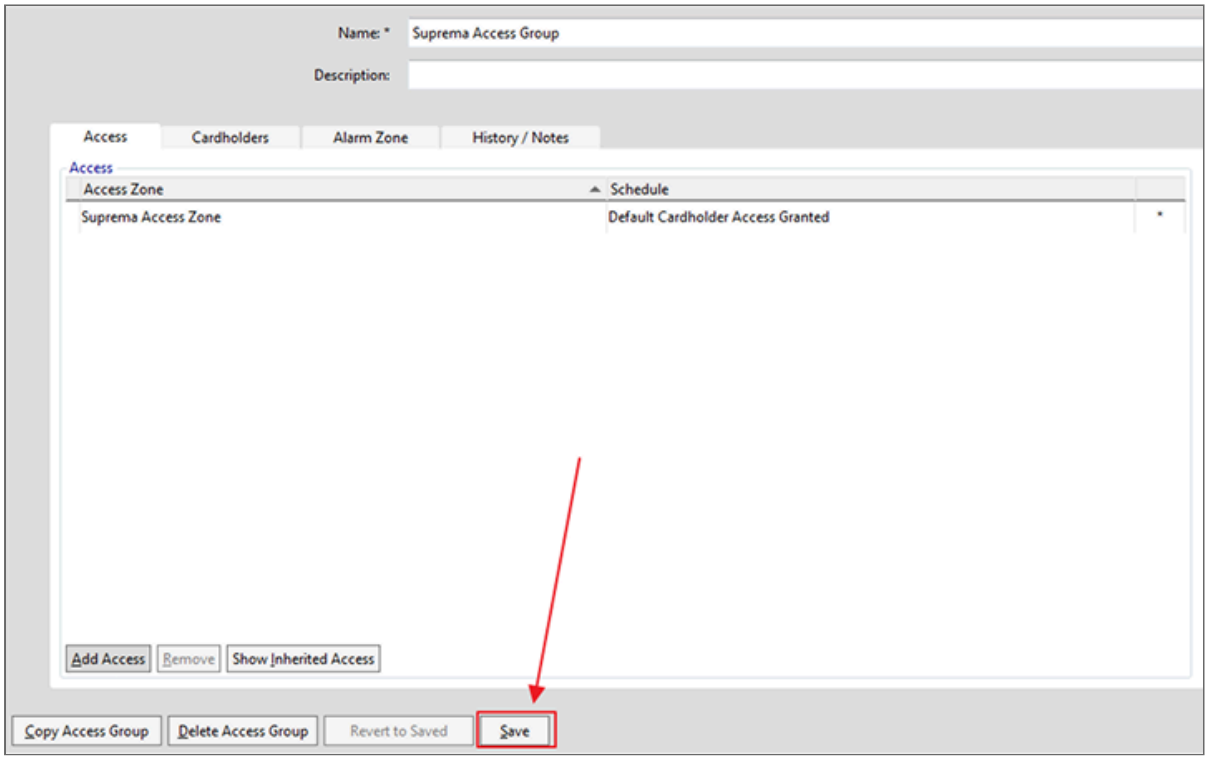
4. **Add Access** ボタンをクリックすると、下の画像のようなポップアップが開きます。そこで **checkbox** にチェックし、Add **Selection** ボタンをクリックします。



次に **radio** ボタンを**選択**し、**OK** ボタンをクリックするとポップアップが閉じます。

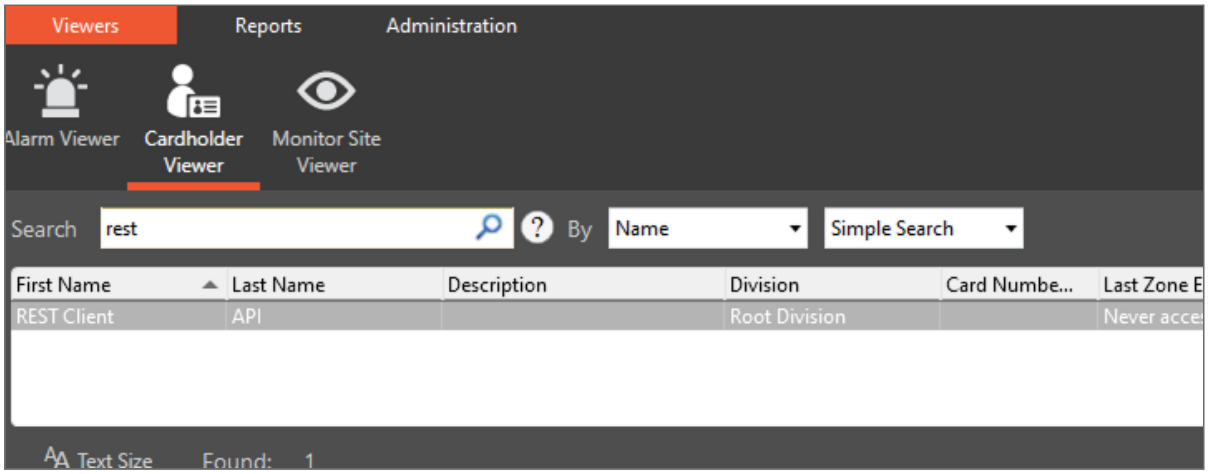


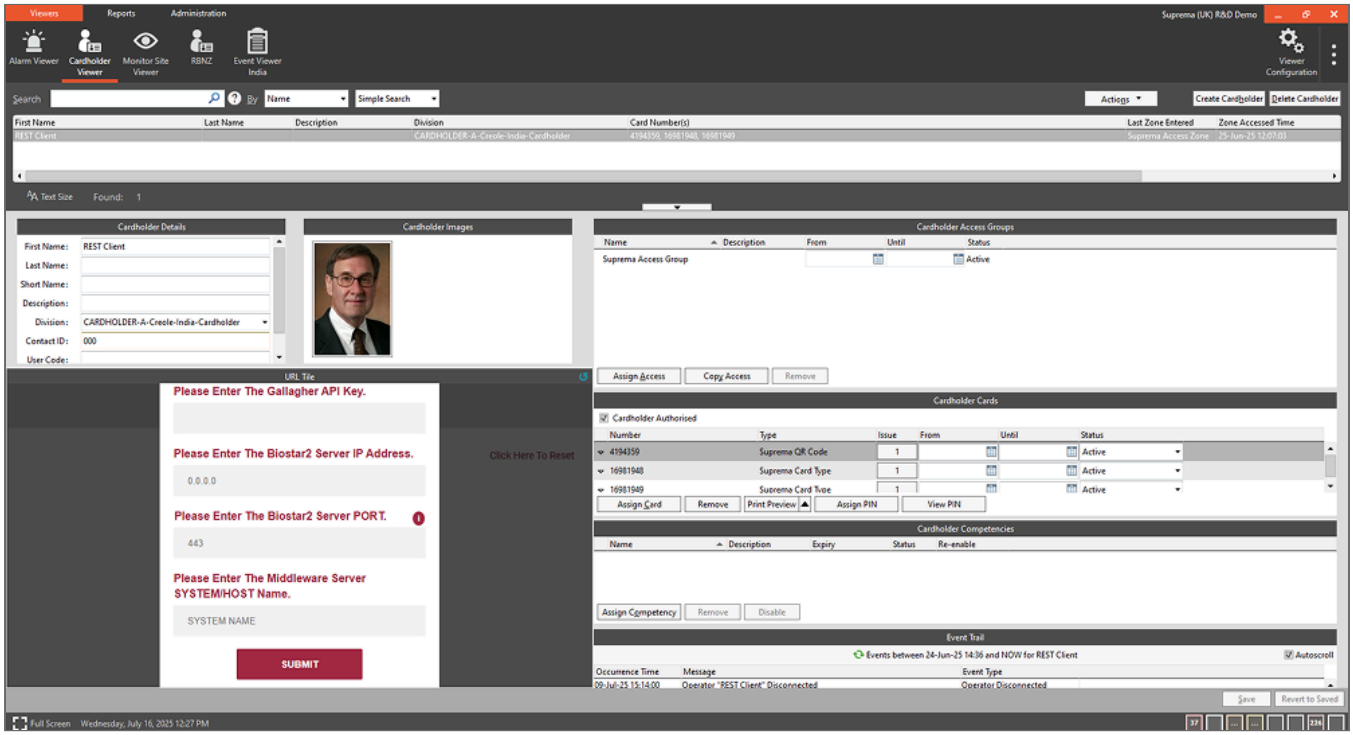
5. **Save** ボタンを**クリック**すると、Access Group が正常に追加されます。


Name: *
Suprema Access Group
Description:
Access
Cardholders
Alarm Zone
History / Notes
Access
Access Zone
Schedule
Suprema Access Zone
Default Cardholder Access Granted
Add Access
Remove
Show Inherited Access
Copy Access Group
Delete Access Group
Revert to Saved
Save

Suprema と Gallagher のインテグレーション

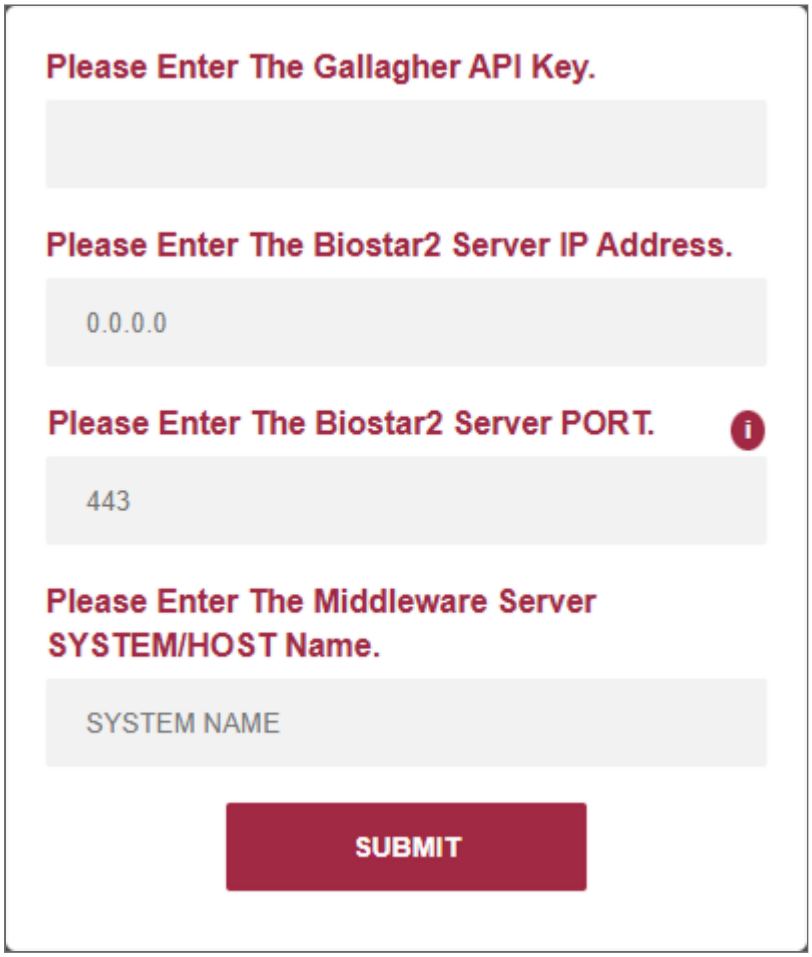
1. Cardholder Viewer の検索で rest を実行すると、すべてのウィンドウが読み込まれます。



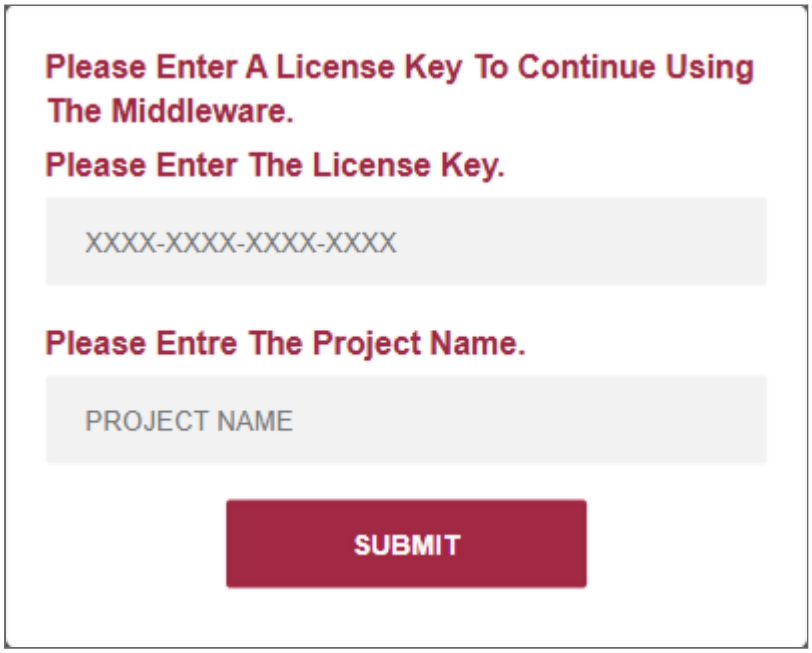


2. 最初に以下の画面が表示されるので、先に進むには Gallagher API キー、BioStar 2 サーバー IP、BioStar 2 サーバー ポート、およびミドルウェア アドレスの SYSTEM/HOST 名を**入力**します。

> **情報**
>
> 特定の IP アドレスを持つ 2 台の異なるサーバーで、特定のポートを使用してミドルウェアを実行する場合は、ミドルウェアの受信ルールを設定するを参照してください。

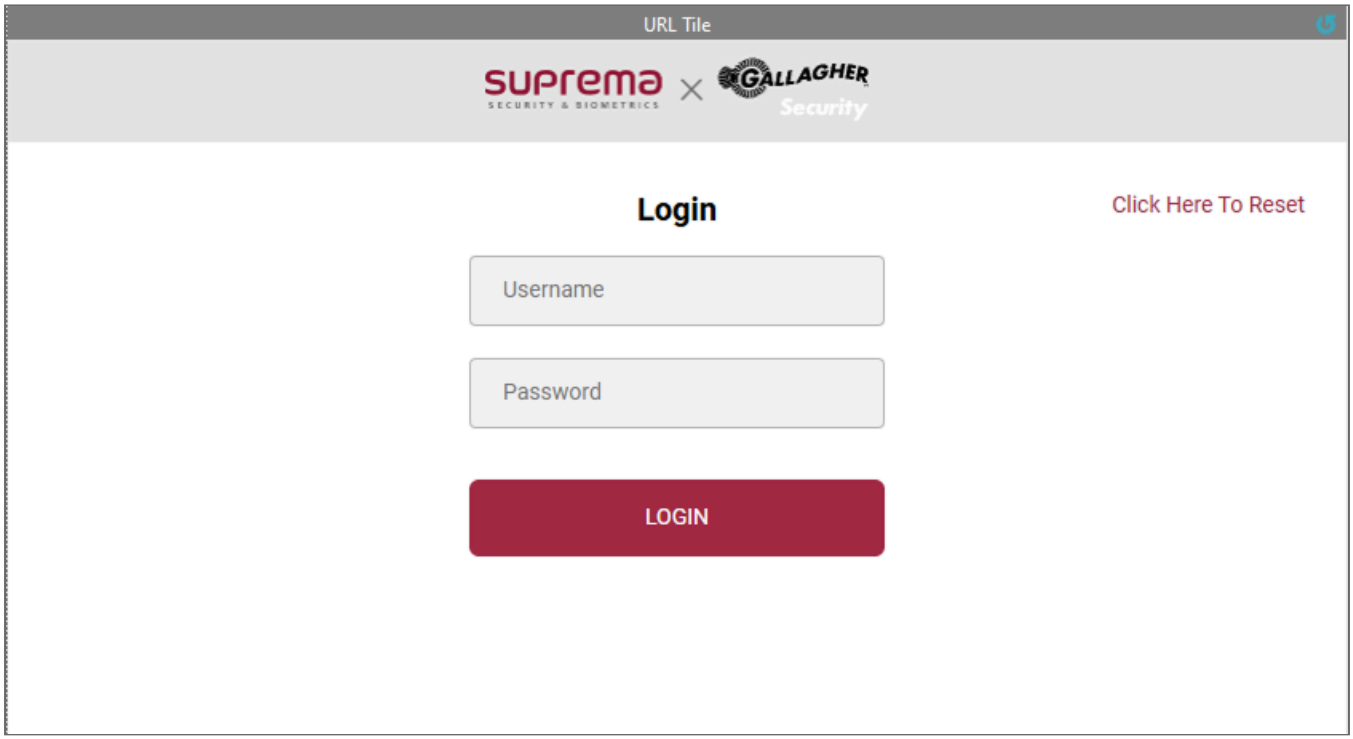


3. ライセンス画面で、管理者から取得したライセンス キーと**正確な**プロジェクト名を**入力**します。

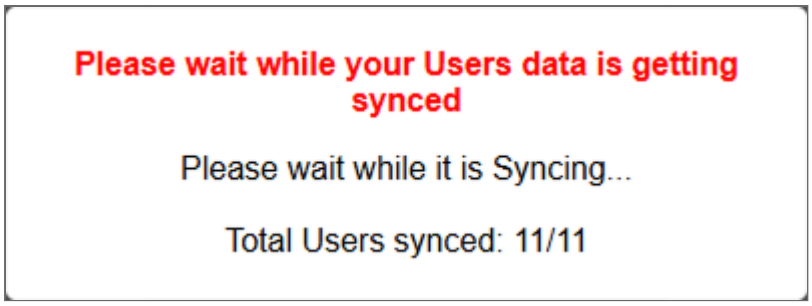


4. ログイン画面で、Suprema BioStar 2 の認証情報を**入力**します。

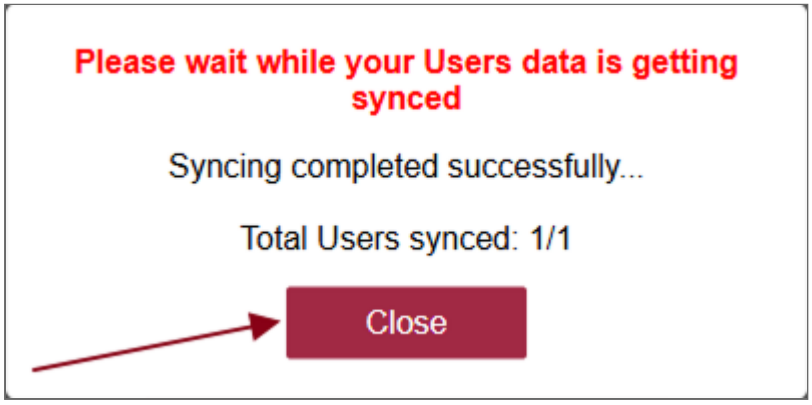
> **情報**
> ログイン画面で、**LAN が切断されているか、IP Address の IP が変更されている**という**エラー**が表示される場合があります。 ログインページのエラーをトラブルシューティングするを参照してください。



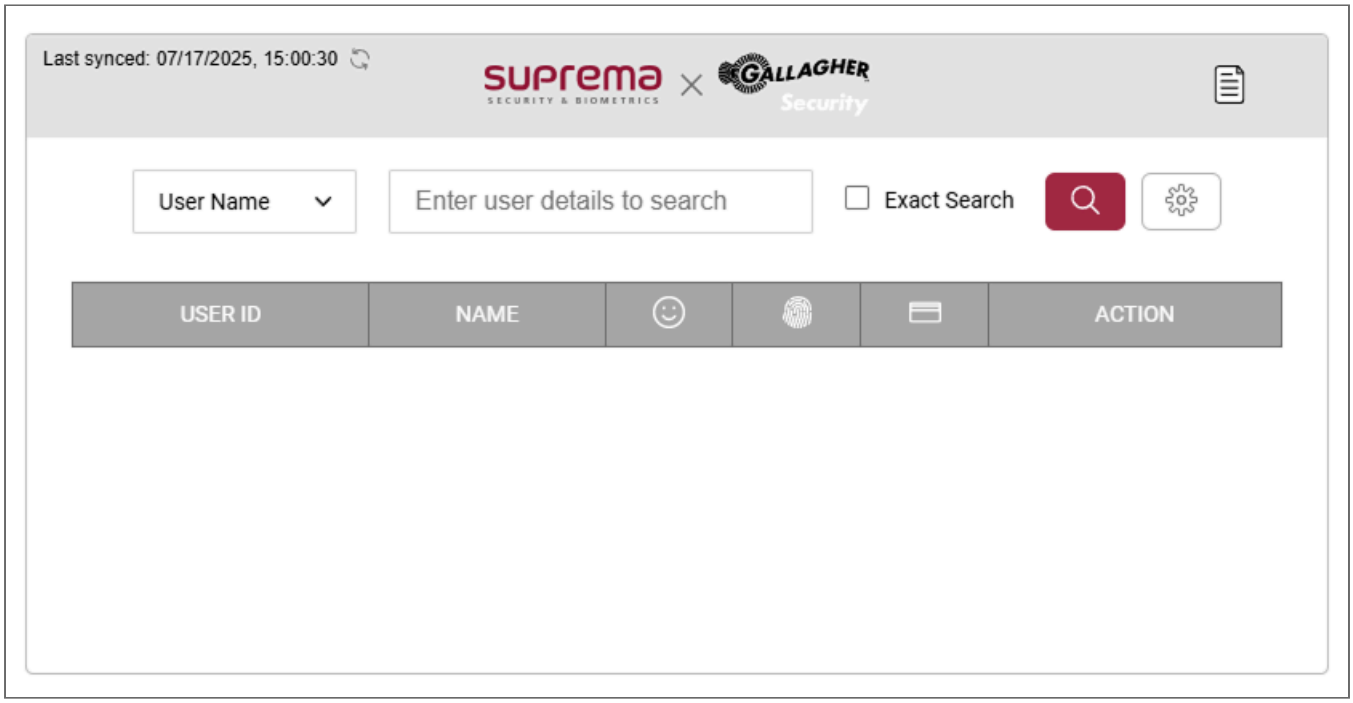
正しい認証情報を入力すると、初期同期用のユーザー同期画面が開きます。



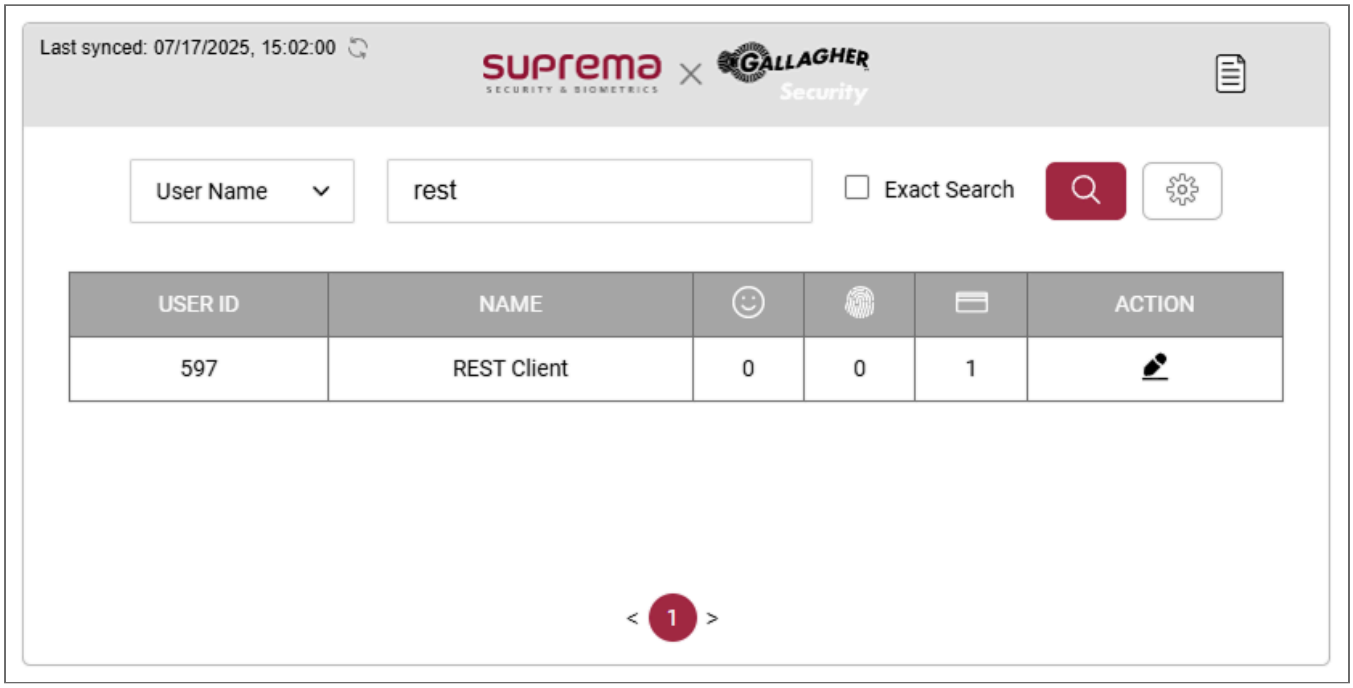
ユーザーの同期が正常に完了すると、画面に Close ボタンが表示されるので、続けるには Close ボタンを**押します**。



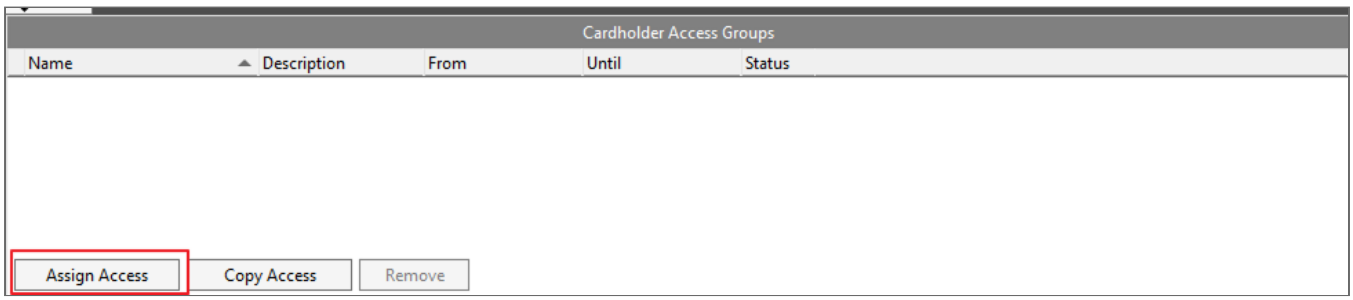
ユーザーの同期が正常に完了すると、ユーザー検索画面が表示されます。

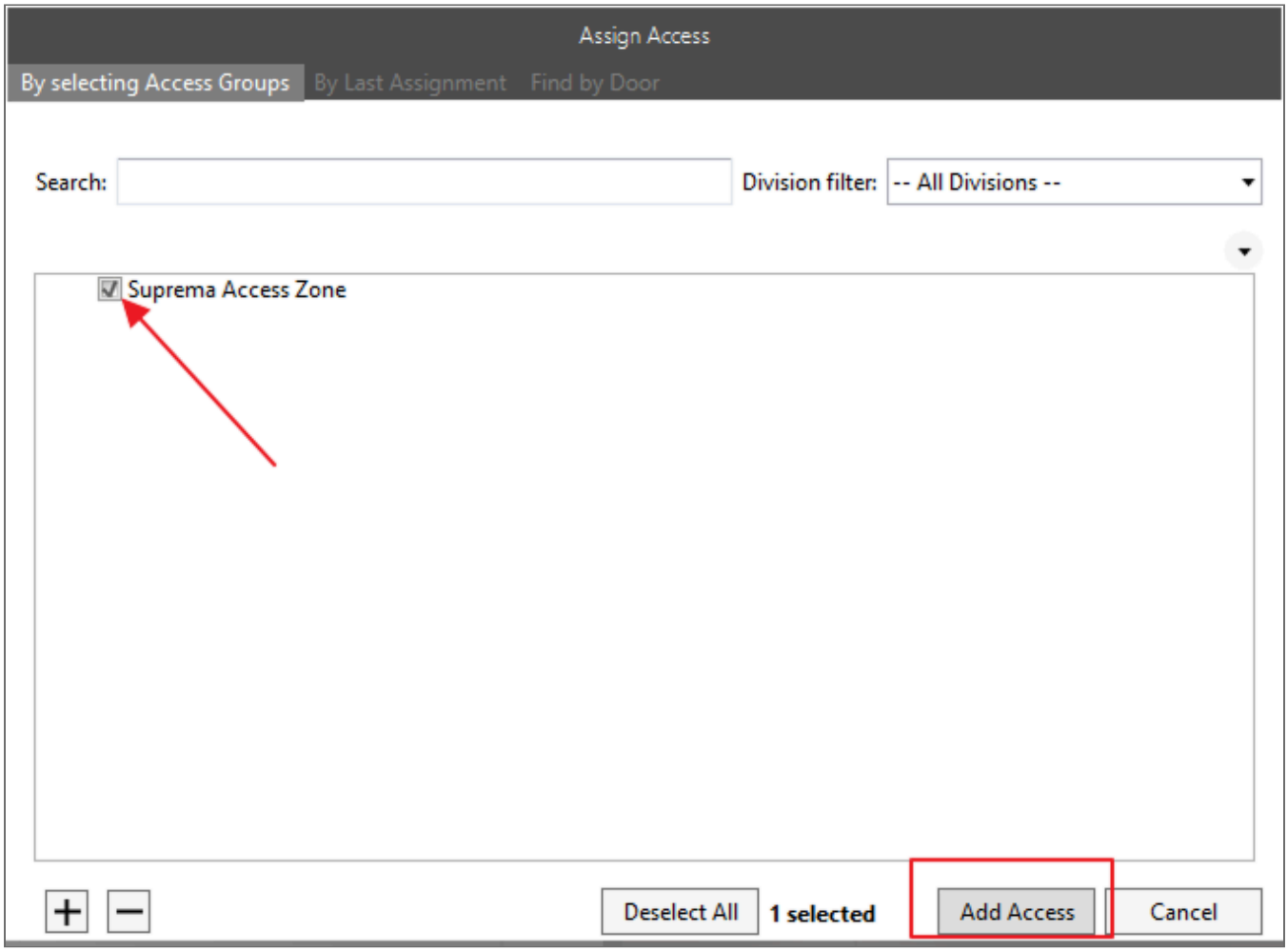


5. 検索で rest を実行し、検索ボタンを押すと、検索したユーザーが表に表示されます。



6. Mifare Encoder をシステムに接続します。 Assign Access ボタンを押し、作成した Suprema Access グループを選択し、Save ボタンを押します。

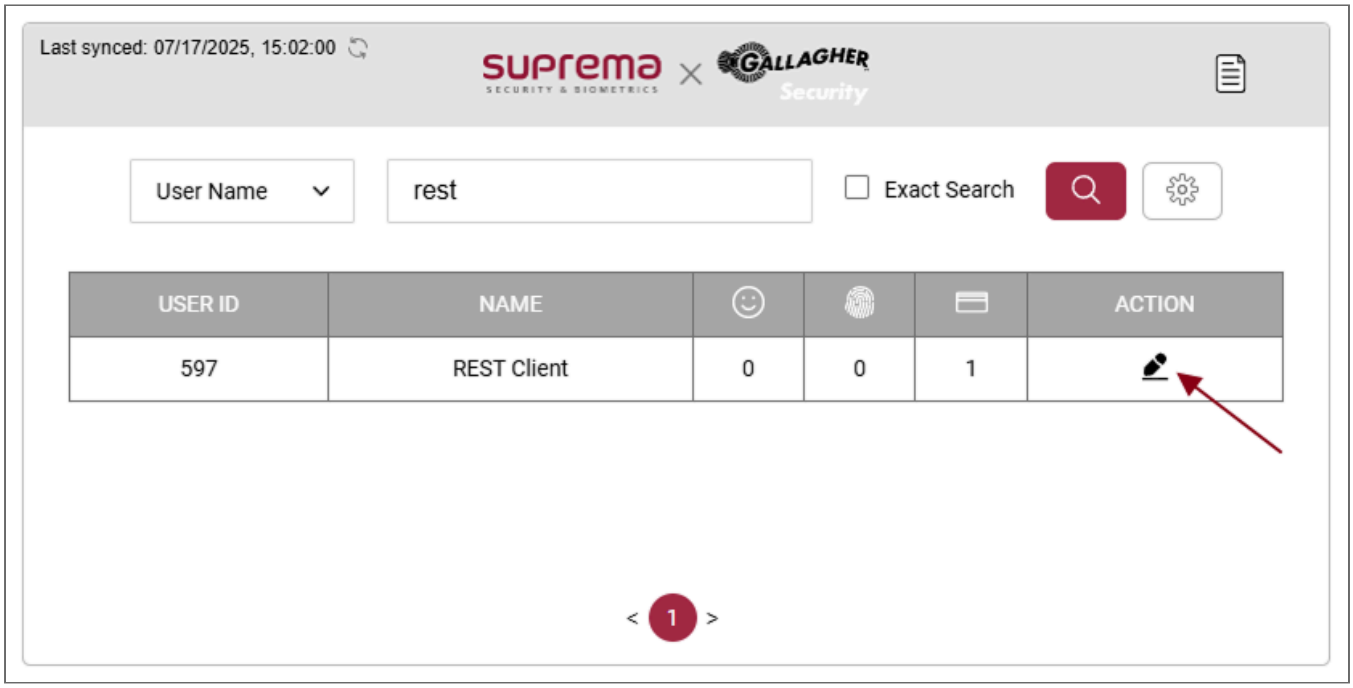




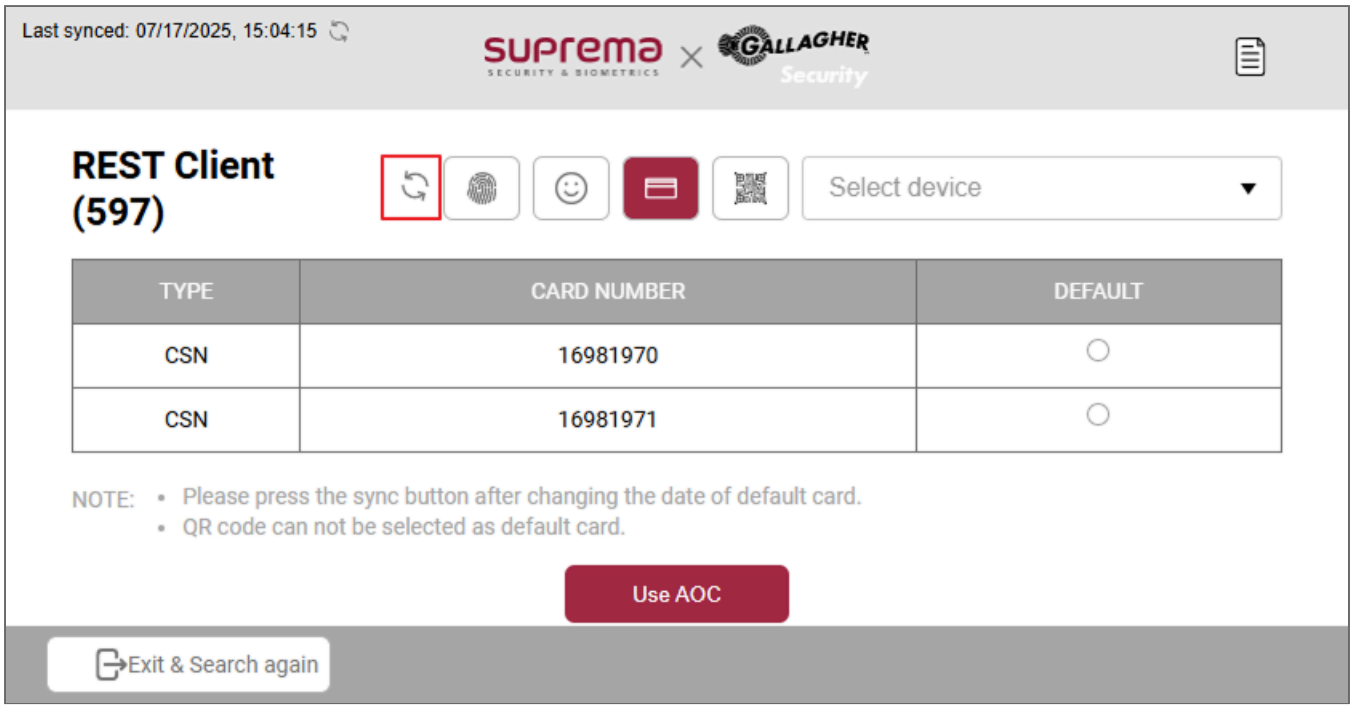
7. アクセス グループを追加し、Mifare Encoder を接続したら、Viewer Configuration を**右クリック**してビューアーを再読み込みします。

8. Encoder のボタンから Encoder Assign Card にカードを**置き**、そのボタンを**押す**とカードがユーザーに割り当てられ、その後 Save ボタンを**押します**。 その後、ミドルウェアで Edit ボタンを**押します**。

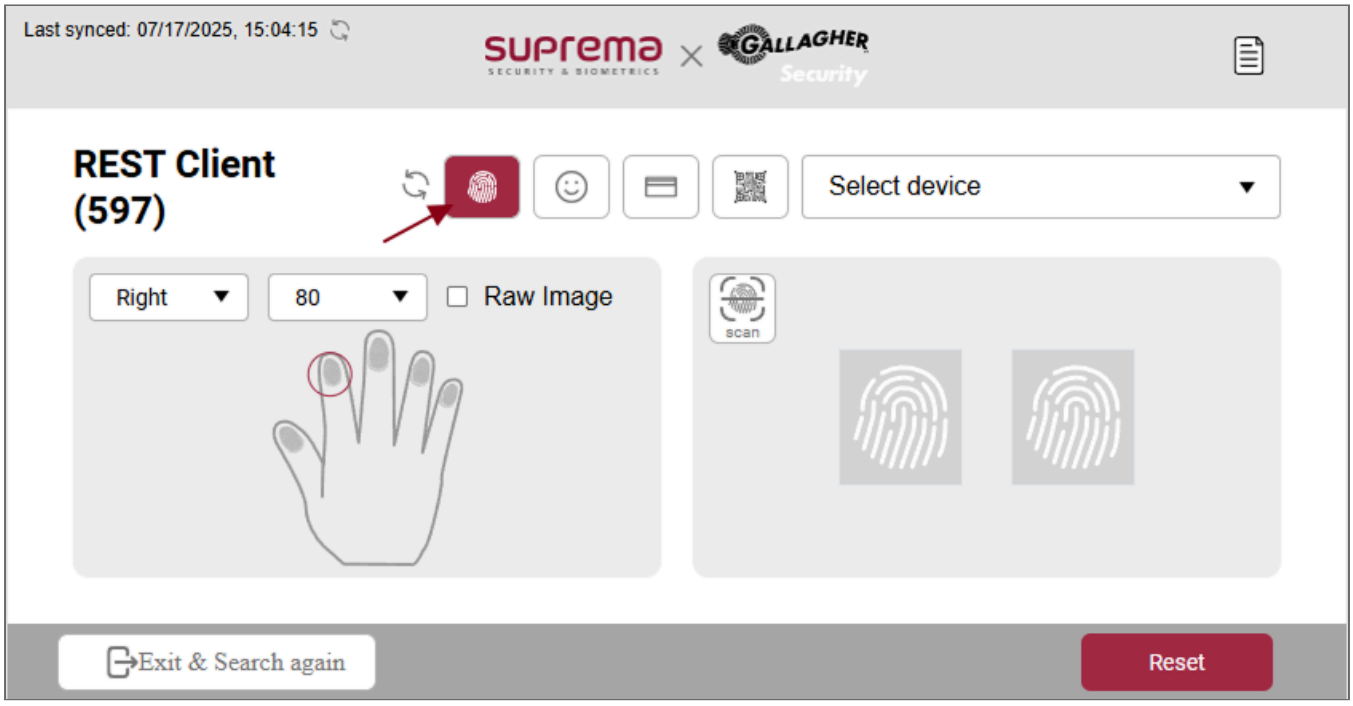
> **情報**
> 生体認証のみを登録する場合は、事前にカードを割り当てず、アクセス ゾーンを割り当てた後に Edit ボタンを**押します**。



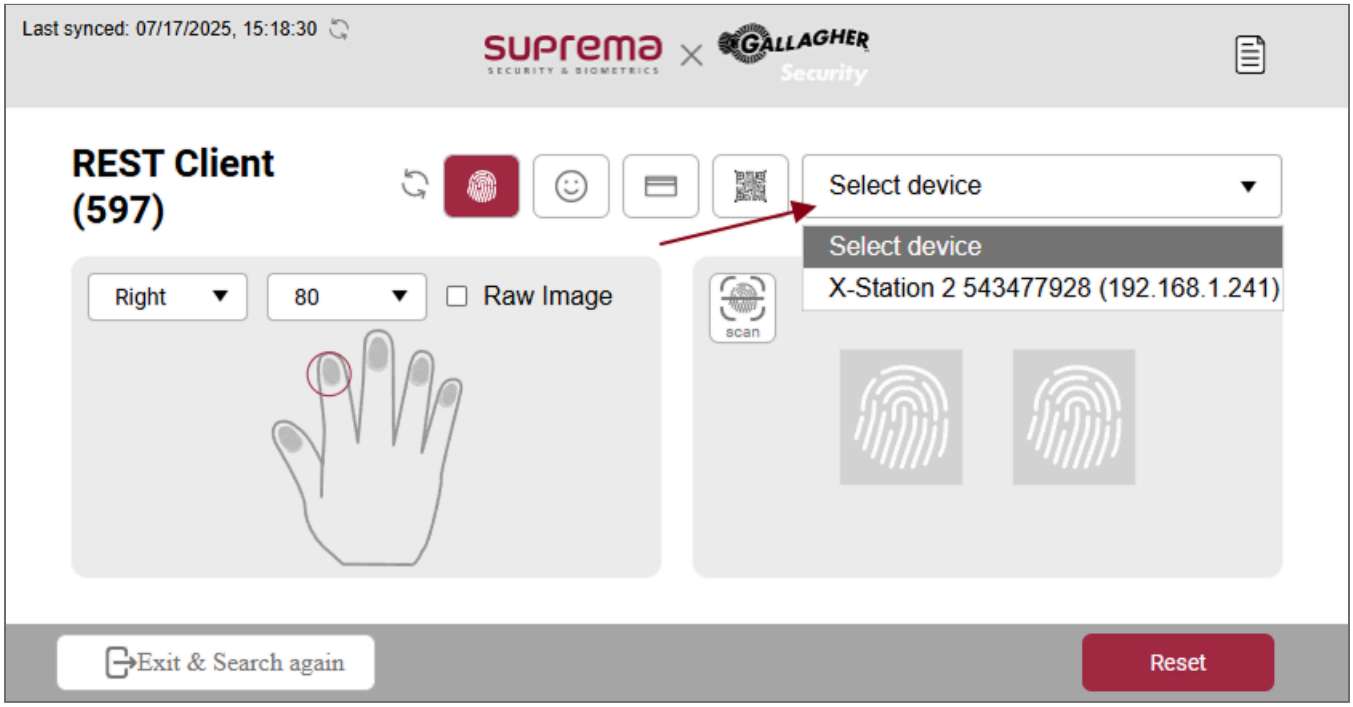
カードを割り当てて Save ボタンを押した後、緑の sync button を押すと、そのユーザーの全データが同期されます。



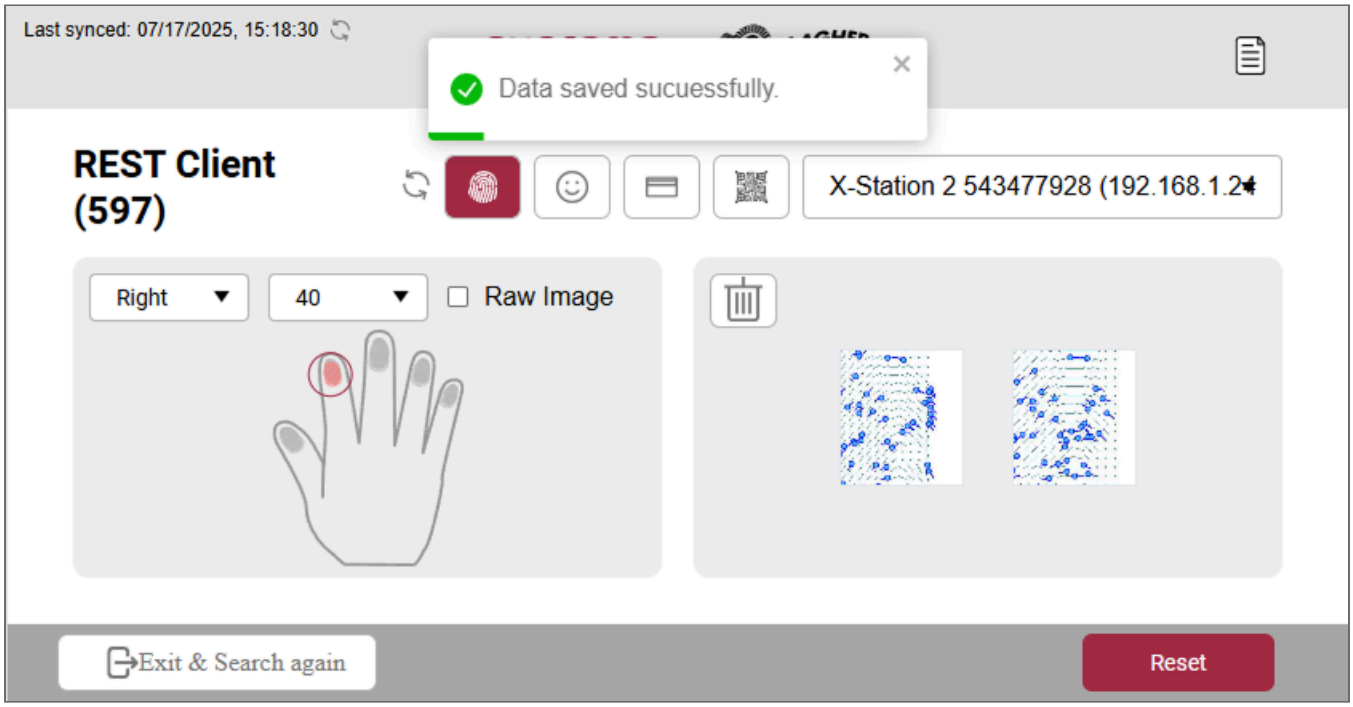
9. Fingerprint ボタンを押すと、指紋モジュールが読み込まれます。



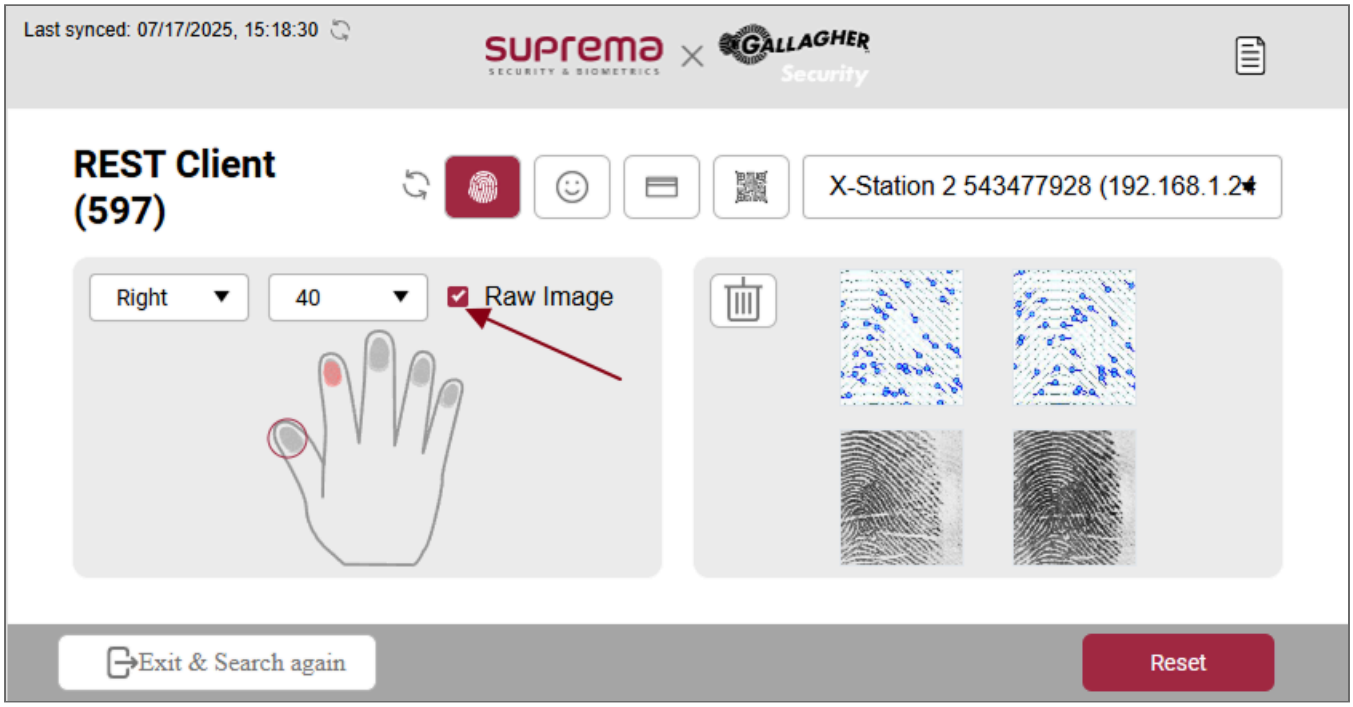
10. 一覧からデバイスを選択します。



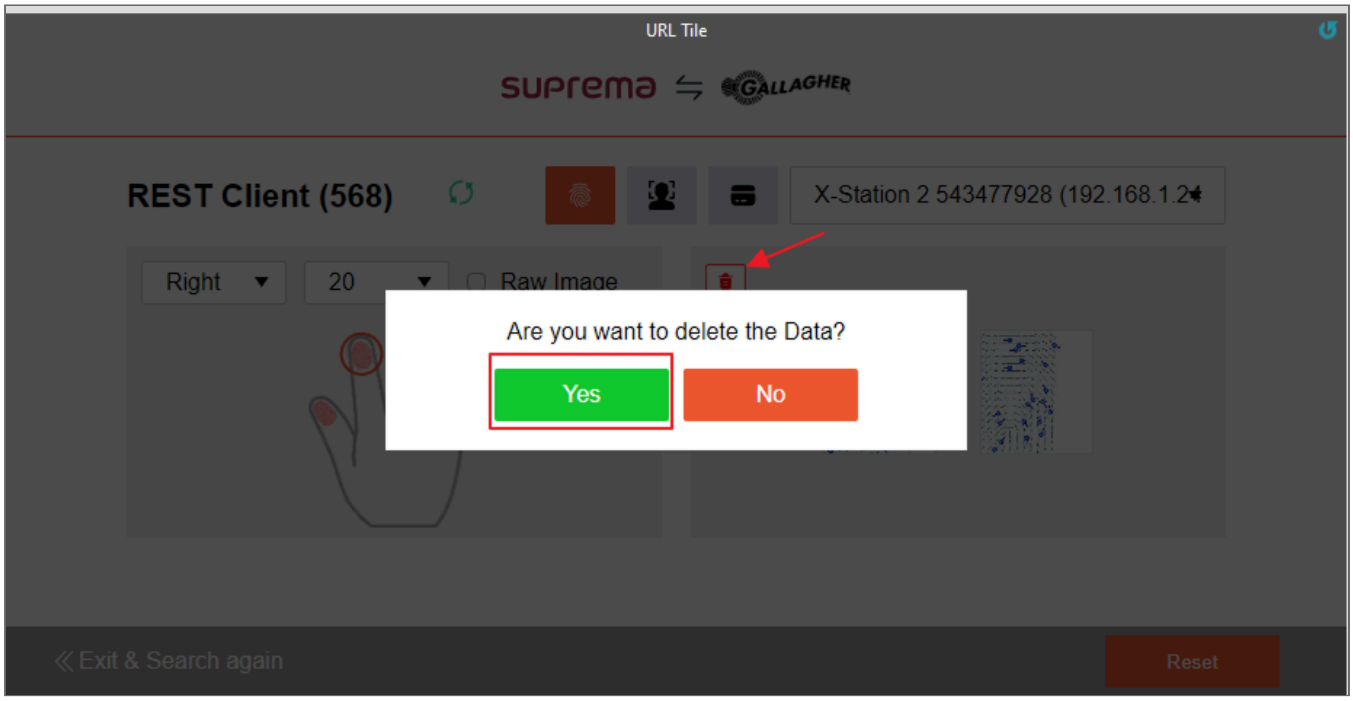
11. 左手または右手を選択し、指紋の品質を設定した後に scan ボタンを押すと、スキャンが開始されます。 スキャンが完了すると、scan ボタンは delete ボタンに変わり、指紋が画面に表示されます。データは自動的に保存され、保存が成功すると、保存された指紋に色が付きます。



12. 生画像が必要な場合は、Raw Image チェックボックスをオンにしてから指を**スキャン**します。

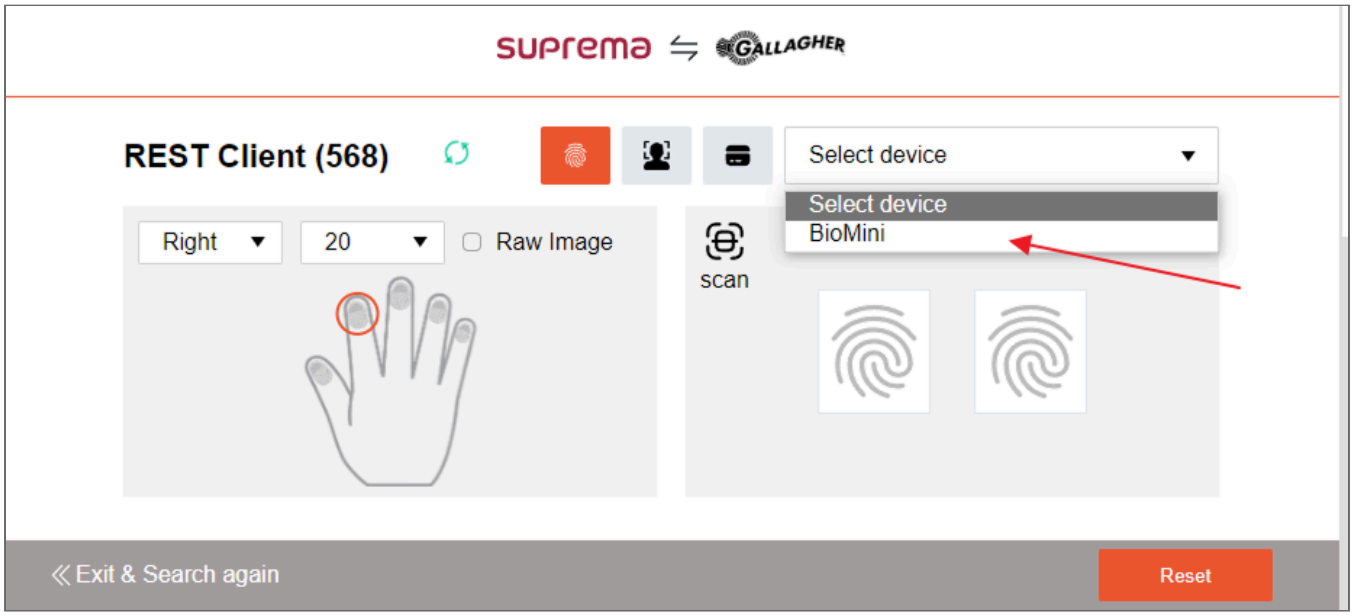


13. 単一の指紋を削除するには、**delete** ボタンを**押し**、ポップアップが表示されたら **Yes** ボタンを**押す**と、その指紋が削除されます。

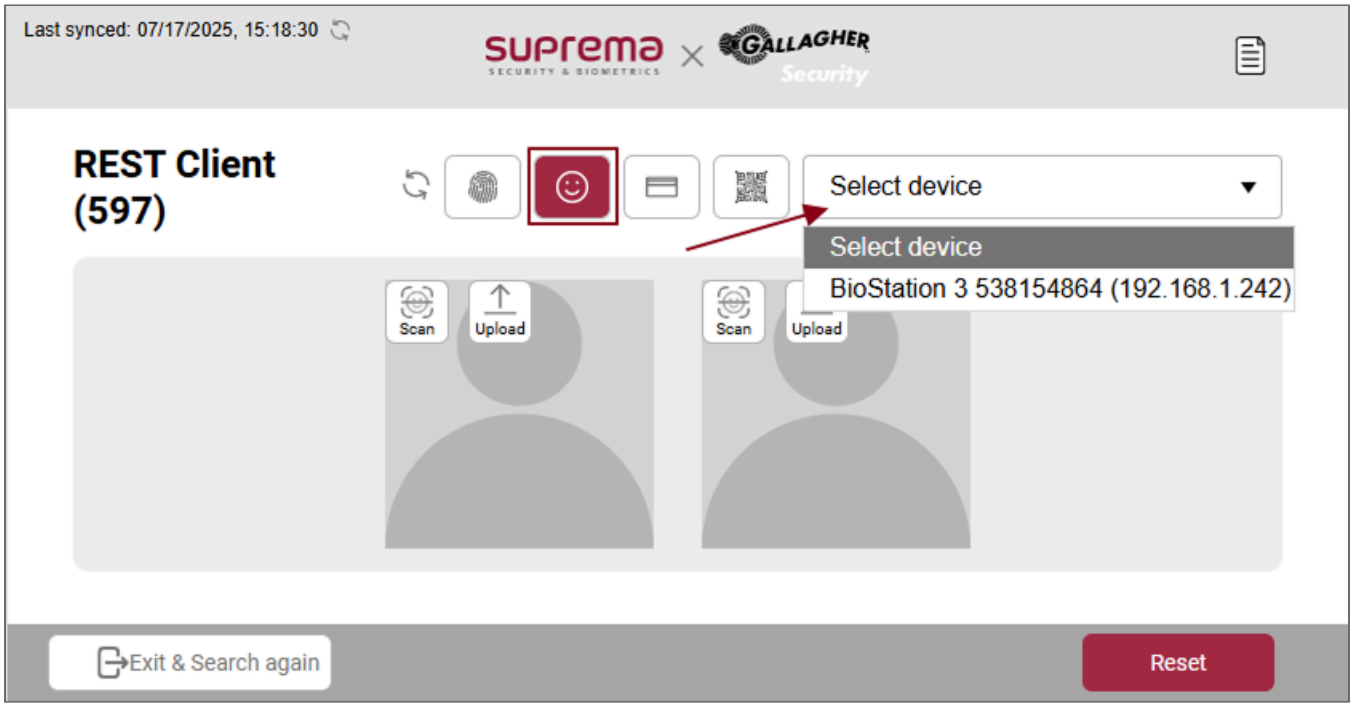


すべての指紋データをリセットするには、**reset** ボタンを**押し**、ポップアップが表示されたら Yes を**押す**と、すべての指紋データがリセットされます。

14. BioMini Plus 2 を使用して、ユーザーの指紋データを登録できます。 そのためにはデバイスを接続すると、指紋のデバイス選択セクションに表示されます。 デバイスを**選択**して、ユーザーのデータ登録を開始します。



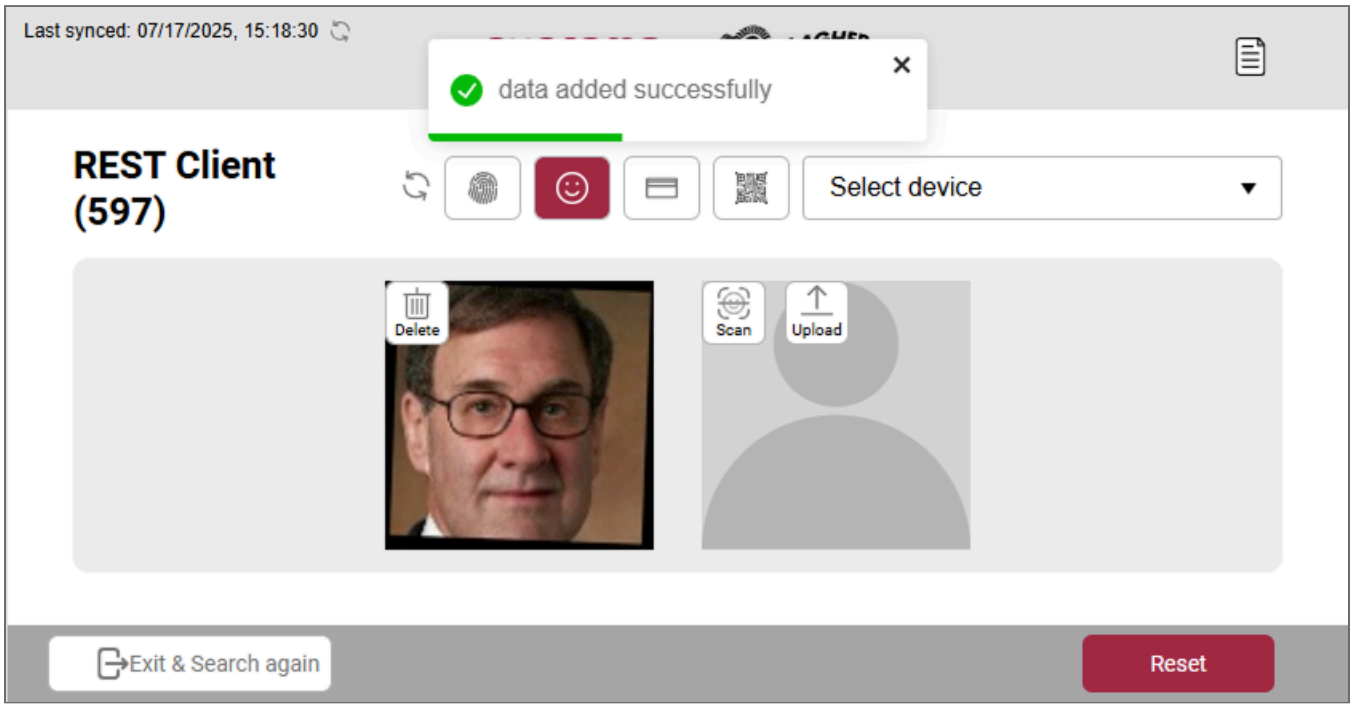
15. Visual Face を登録するには、指紋の横にあるボタンを**押す**と、Visual Face モジュールが読み込まれます。



Visual Face のスキャン方法は 2 つあります。 アップロードするか、顔をスキャンして登録できます。

16. **upload** アイコンを押すと、新しいウィンドウが開き、アップロードする画像を選択できます。

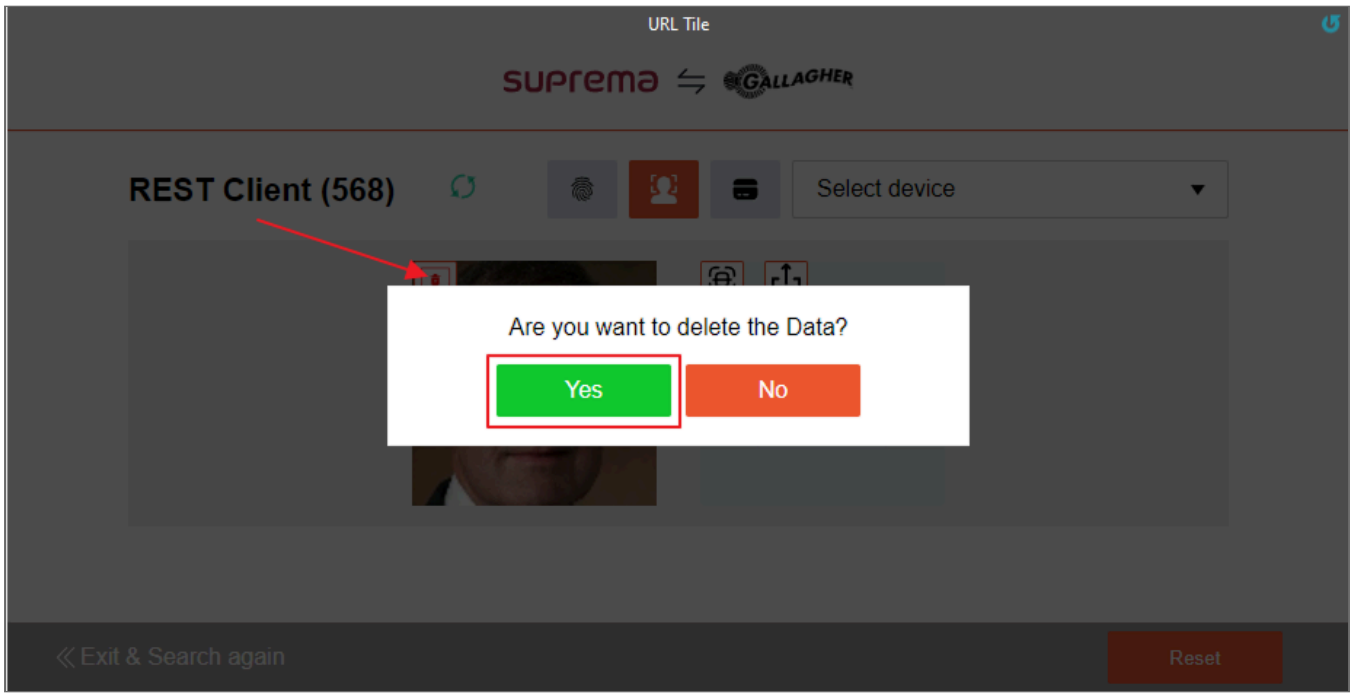
scan ボタンを押すと、選択したデバイスが有効になります。選択したデバイスを使用して顔をスキャンします。 Visual Face のアップロードまたはスキャン後、データは自動的に保存され、成功メッセージが表示されます。



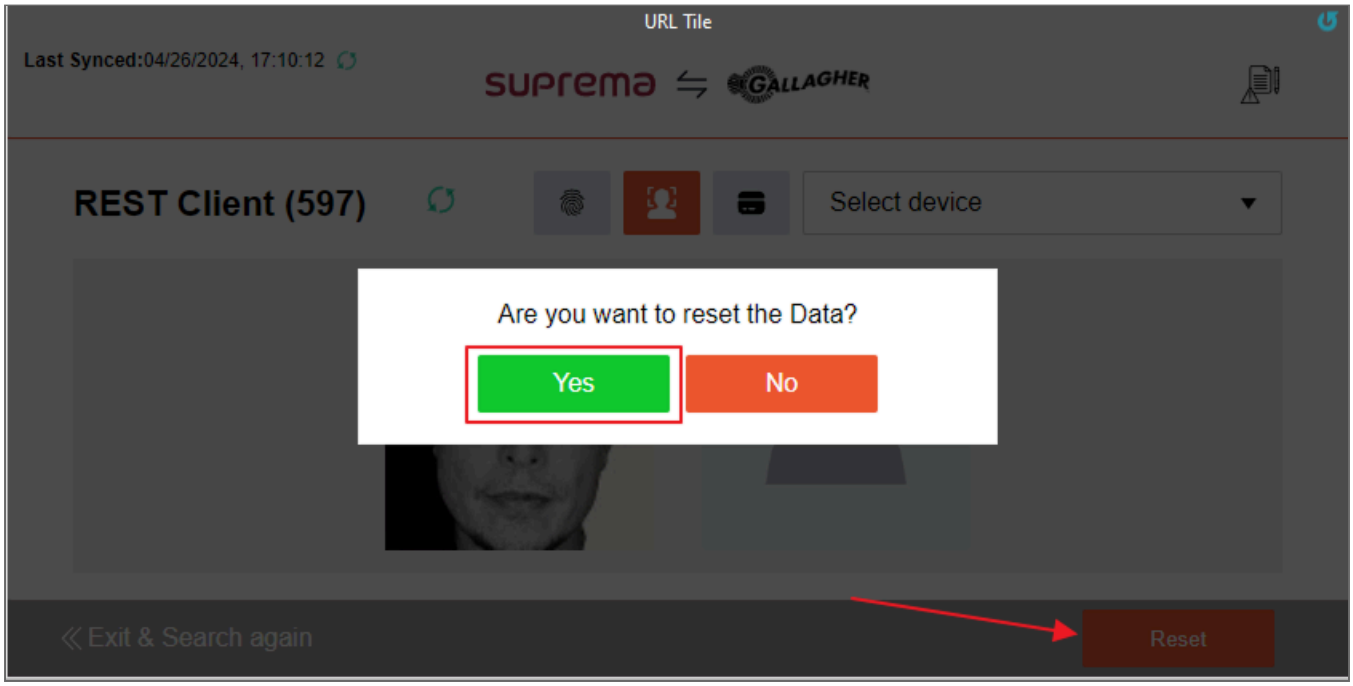
情報

- 対応している画像ファイルサイズは最大 2MB です。
- 対応している画像ファイル形式は JPG、JPEG、PNG です。
- プロフィール画像で Visual Face の登録中にエラーが発生した場合は、より鮮明な画像を使用してください。

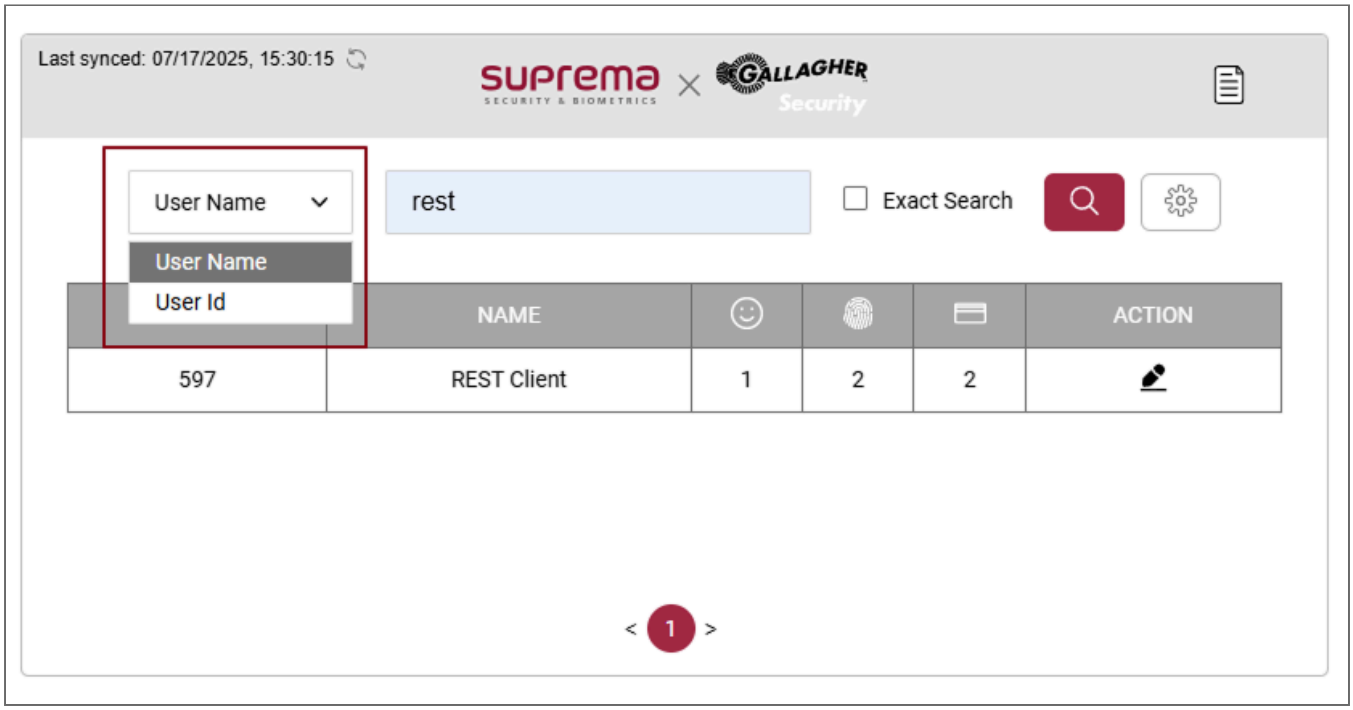
17. 再スキャンまたは再アップロードする場合は、古いデータを削除する必要があります。**赤い delete ボタンを押し**、ポップアップで **Yes** を**押す**と、その画像が削除されます。



18. すべての Visual Face データをリセットする場合は、**reset** ボタンを**押し**、**Yes** を**押す**と、すべてのデータがリセットされます。



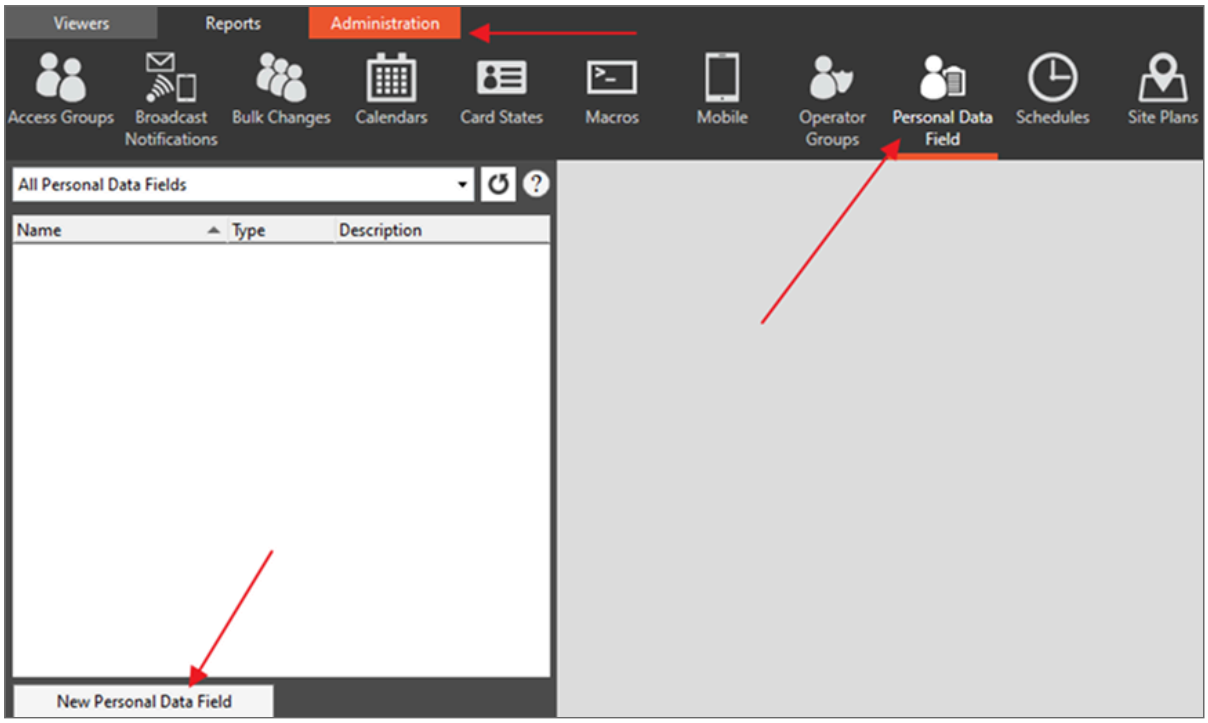
19. 終了してからもう一度ユーザーを検索すると、保存されたすべてのデータが表に表示されます。



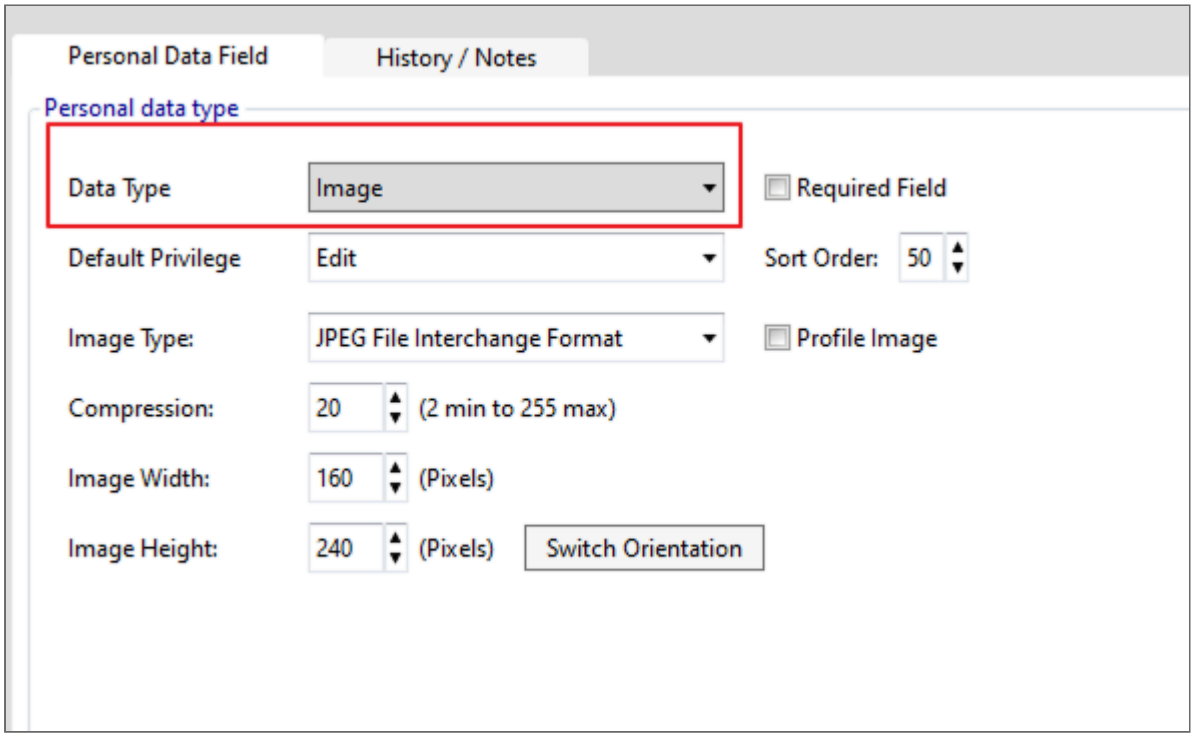
ユーザー ID でも検索できます。ドロップダウンの user name を user id に変更し、ID でユーザーを検索します。

Command Center で Face Template 用のユーザー写真 ID を登録する

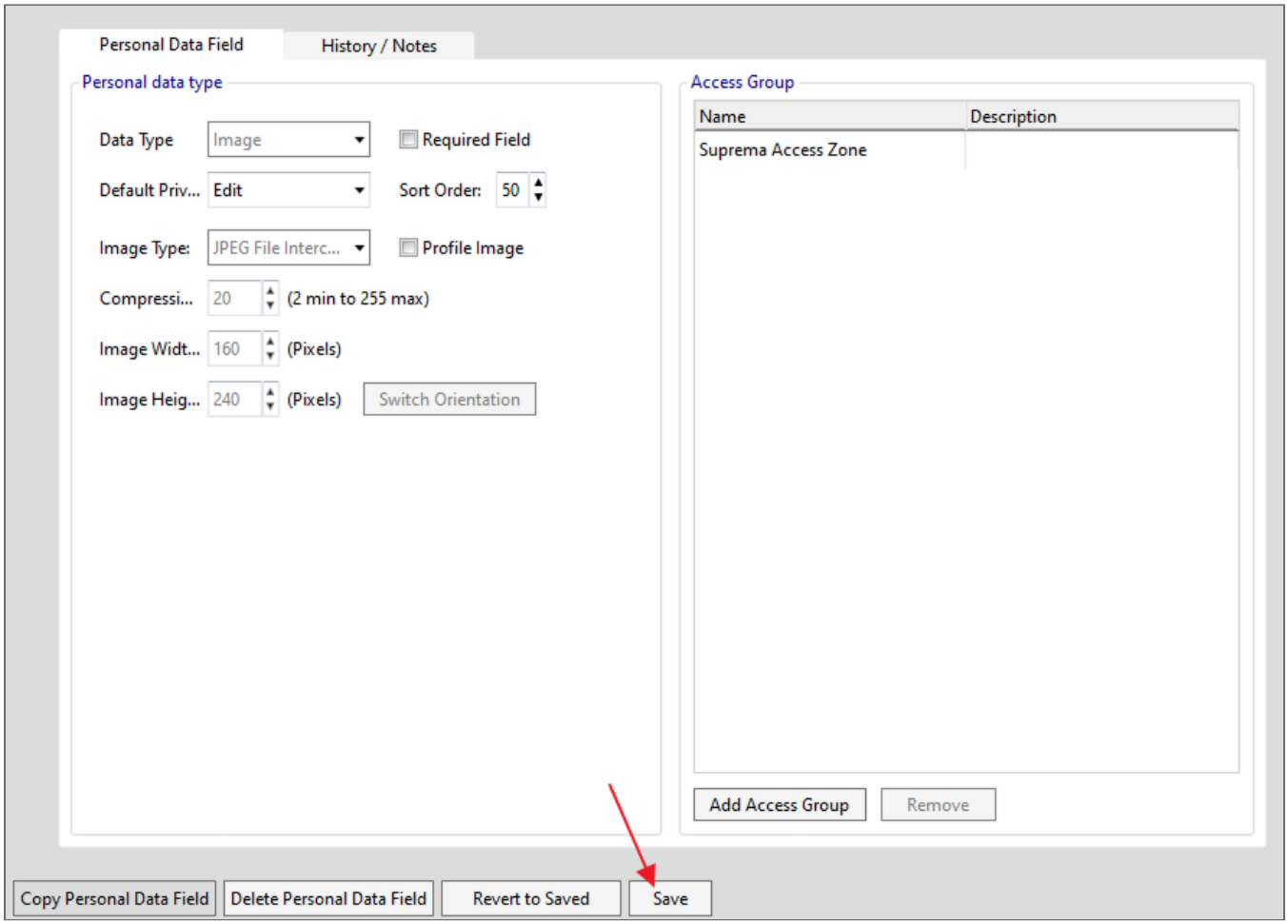
1. Administration に移動し、Personal Data Field をクリックして、New Personal Data Field を押します。



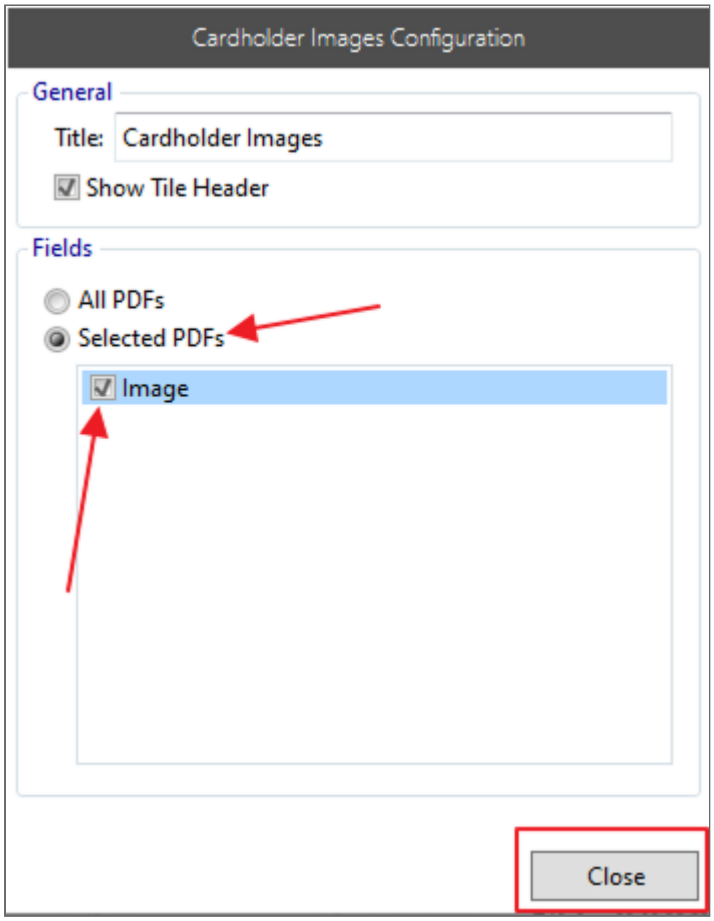
2. ポップアップで名前を Image に設定し、Close ボタンを押します。 Data Type フィールドで Data Type を Image に選択します。ここは変更しません。Access Group セクション内の Add Access Group ボタンを押し、Suprema Access Zone を選択して Access Group を割り当てます。Access Zone を選択した後、フィールドの Add Selection ボタンを押します。



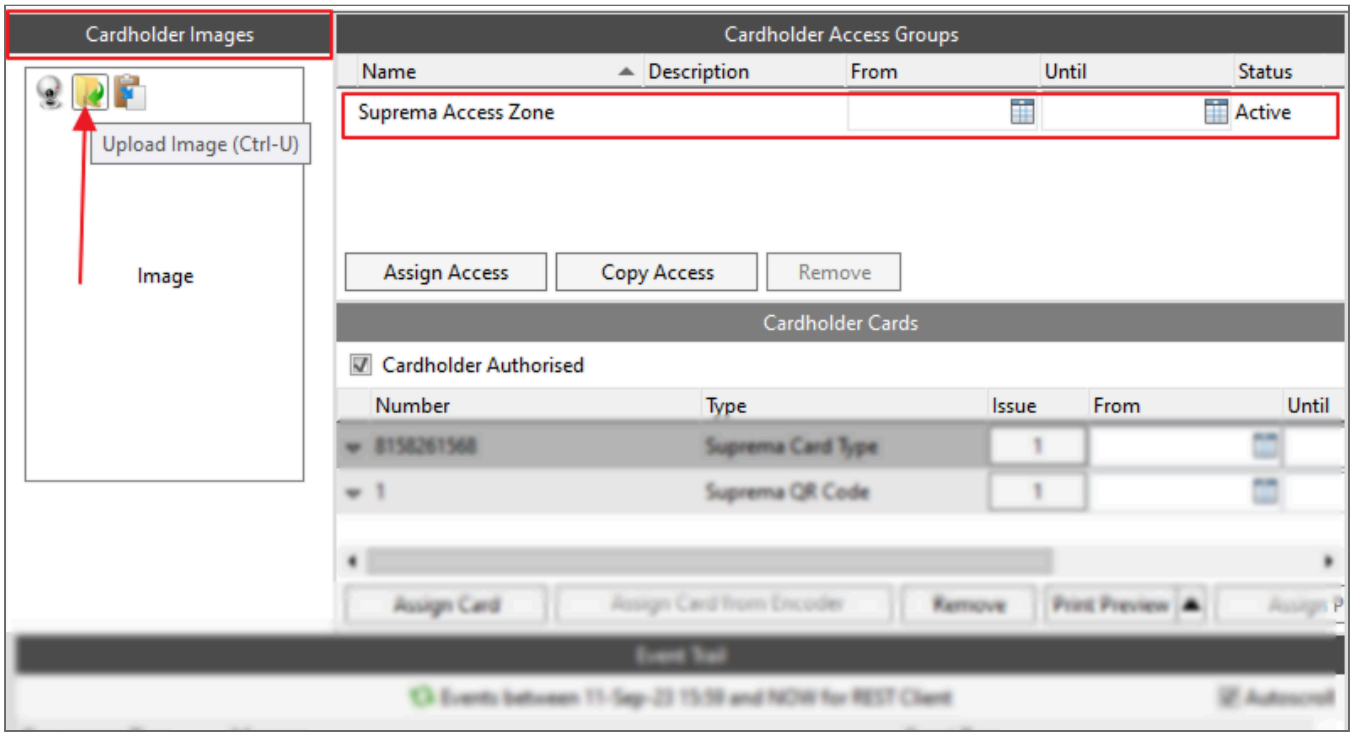
3. Access Zone を割り当てた後、下部の Save ボタンを**押します**。



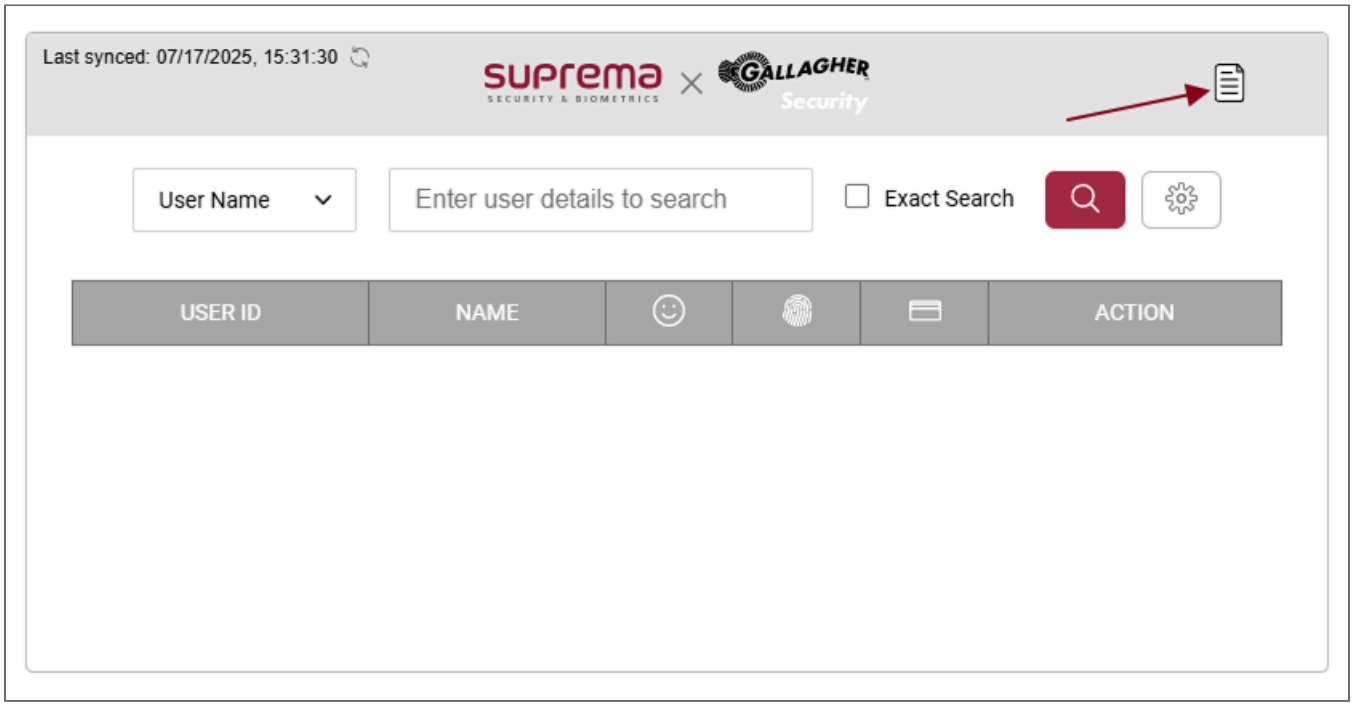
4. Viewer Configuration に**移動**し、Cardholder Images を設定するために Click を**押します**。 Cardholder Images Configuration で Selected PDFs を**選択**し、Image フィールドを**選択**して、Close ボタンを**押します**。 変更を保存するには、左下の Save ボタンを**押します**。 Viewer Configuration を**右クリック**して、ビューアーを再読み込みし、変更を反映します。



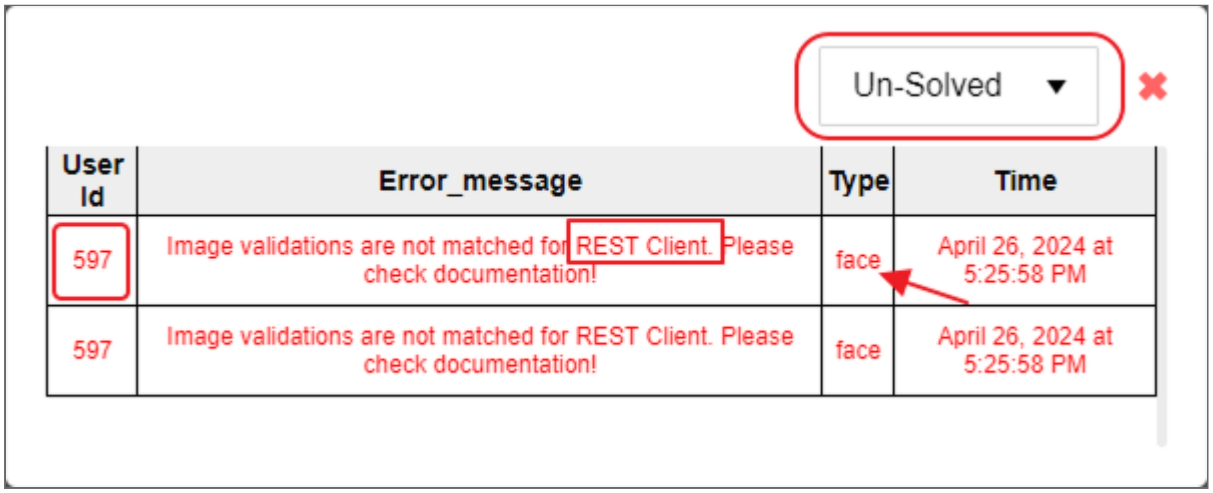
5. Cardholder Viewer では Cardholder Images タブが表示され、黄色のアイコンを**クリック**して画像をアップロードできます。そのためには、ユーザーに Access Zone を割り当てる必要があります。 画像をアップロードした後、Save ボタンを**押します**。



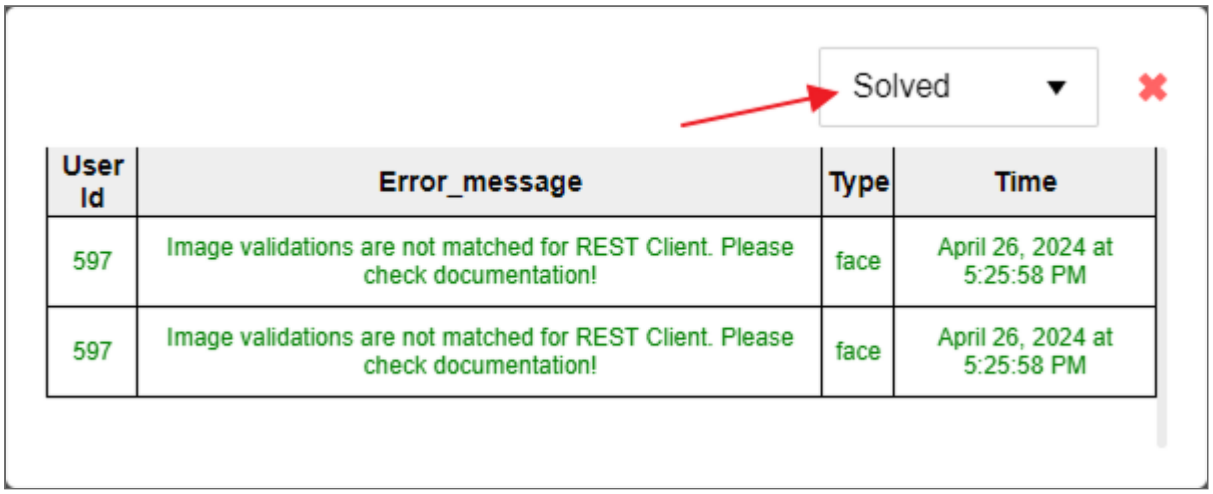
6. ユーザー情報の更新中に発生するエラーメッセージを確認するには、このアイコンを**クリック**して ErrorLog セクションで確認します。ポップアップが開き、ユーザーごとのさまざまなエラーが表示されます。



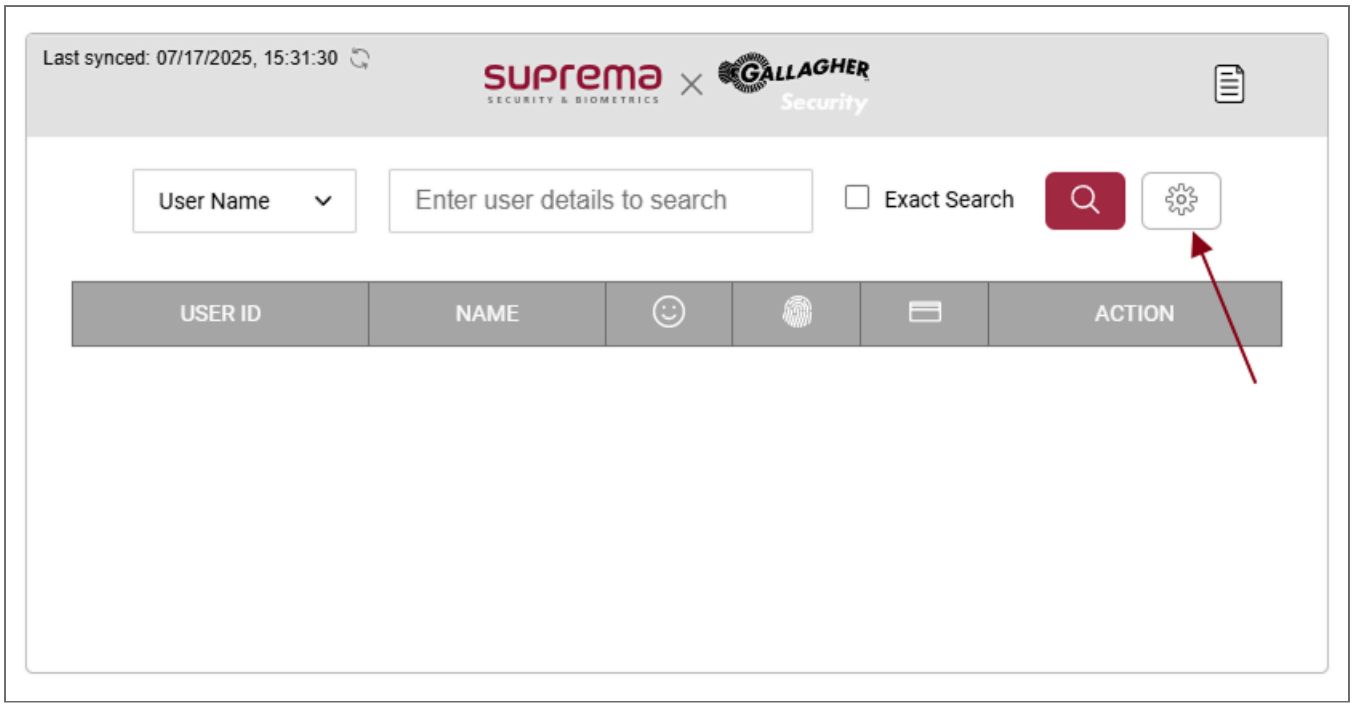
7. 下の画像のように、1 人のユーザーにエラーがあります。ここで **Type** はエラーの種類を示し、**Status** の Un-solved はエラーがまだ解決されていないことを示し、Solved はユーザーのエラーが解決済みであることを示します。 赤い枠の 1 つはユーザー名を示し、もう 1 つの赤い枠はユーザー ID を示します。



8. 下の画像は、Gallagher Command Center でユーザー画像を変更した後の状態です。ユーザーの顔登録時にエラーが発生し、登録が成功するとエラーメッセージの色と Status も変わります。

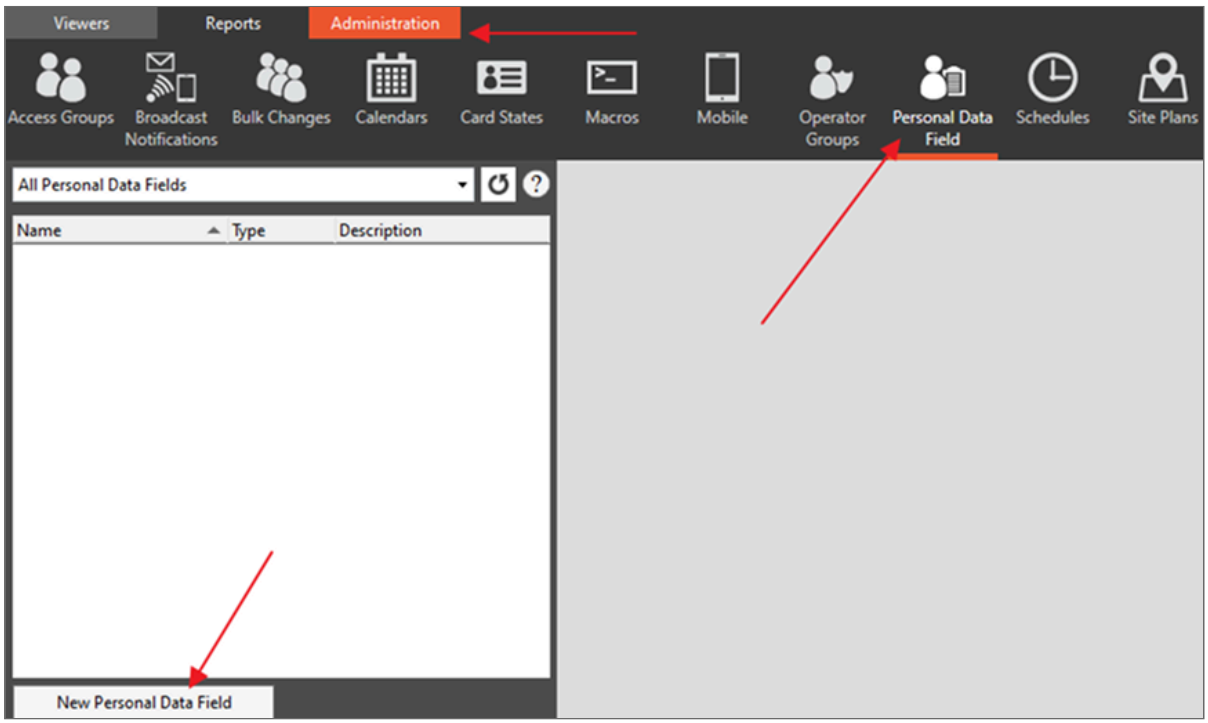


9. デバイスの設定を変更する場合は、**settings** ボタンを**押す**と、以下の画面が表示されます。



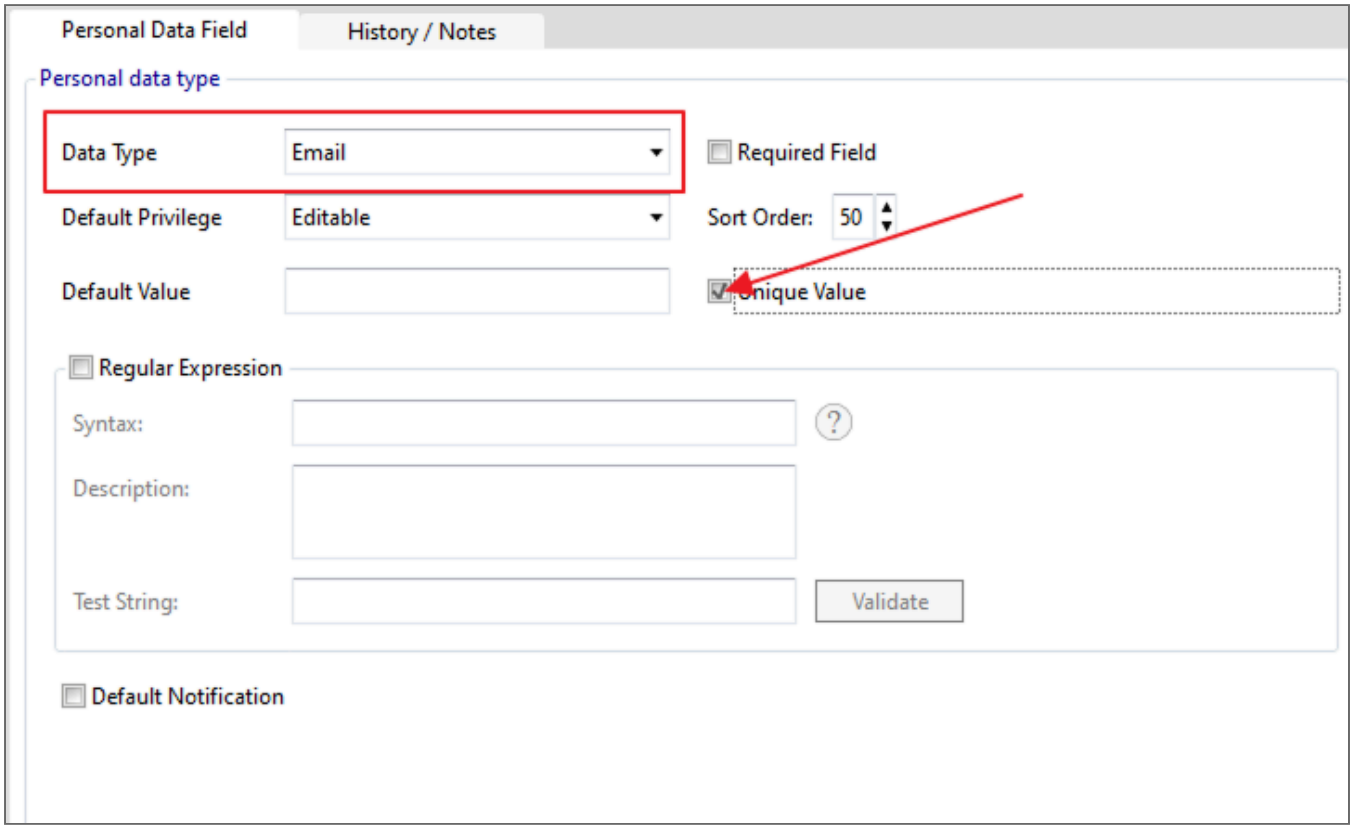
Command Center で QR Code 用のユーザーのメール ID を登録する

1. Administration に**移動**し、Personal Data Field を**クリック**して、New Personal Data Field を**押します**。

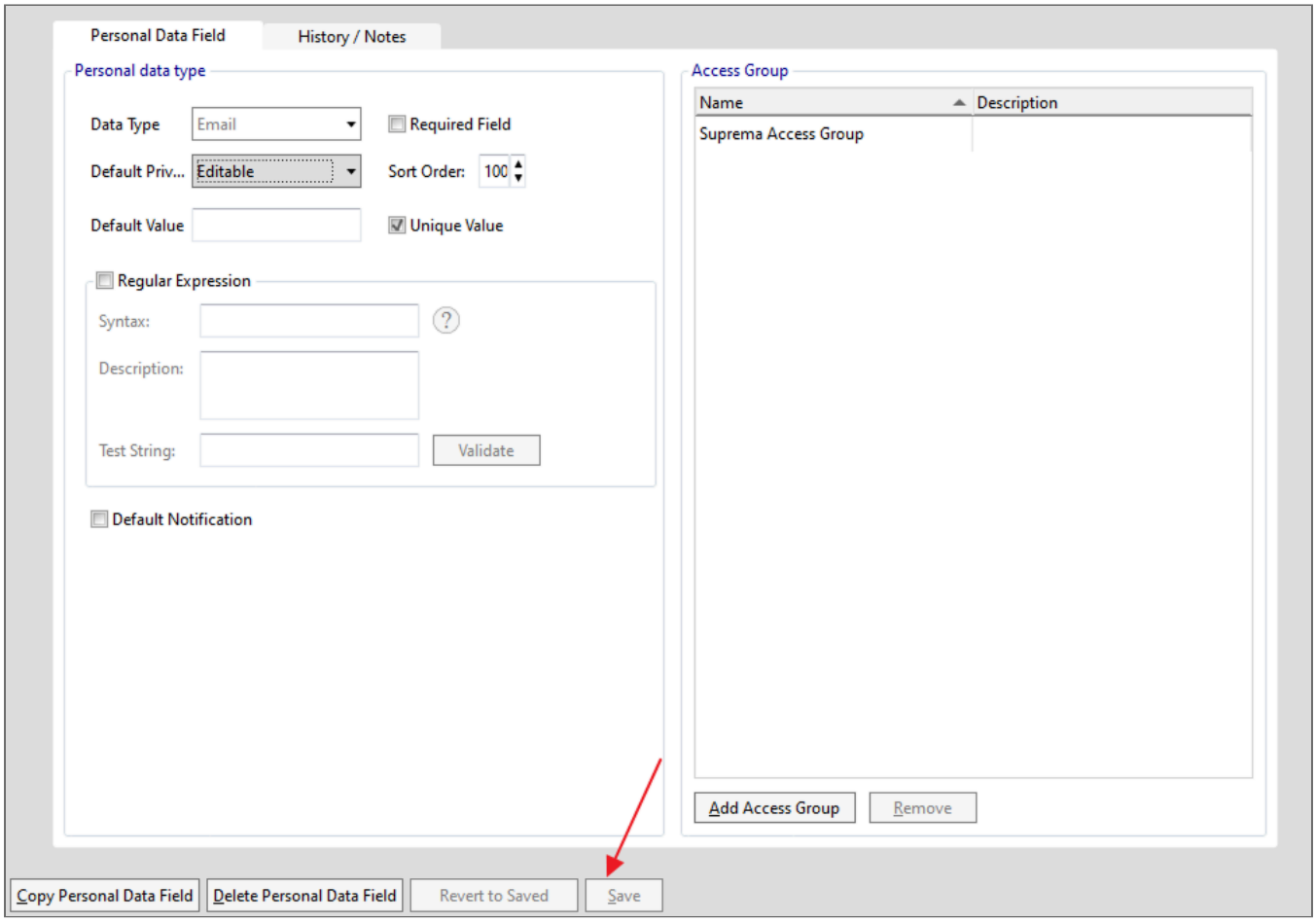


2. ポップアップで名前を Email に**設定**し、Close ボタンを**押します**。 Data Type フィールドで Data Type を Email に**選択**し、Unique Value チェックボックスを**オン**にします。 ここは変更しません。Access Group セクション内の Add Access Group ボタンを**押し**、Suprema Access Zone を**選択**して Access Group を割り当てます。Access Zone を**選択**した後、フィールドの Add Selection ボタンを**押します**。

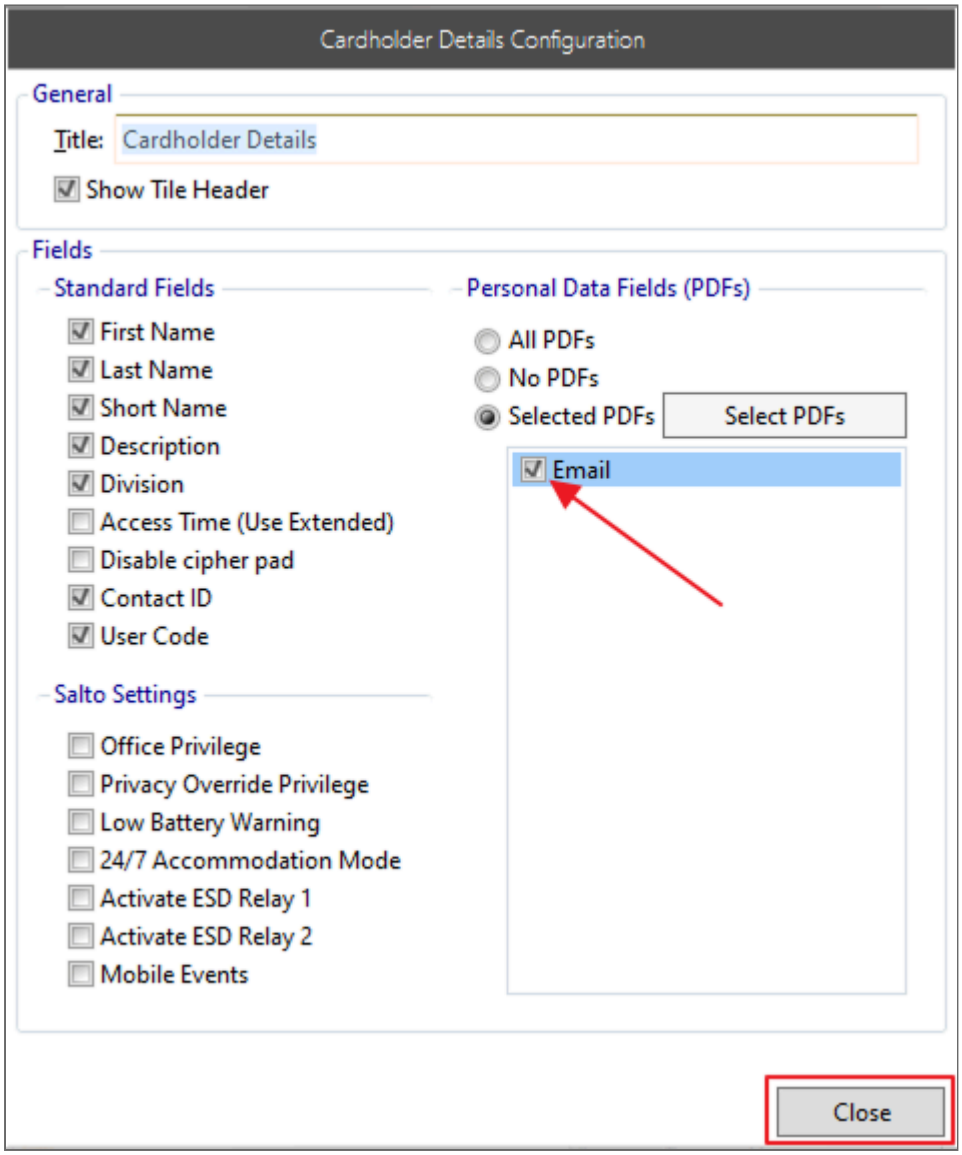
> **情報**
> フィールド名は記載されている用語をそのまま使用してください。



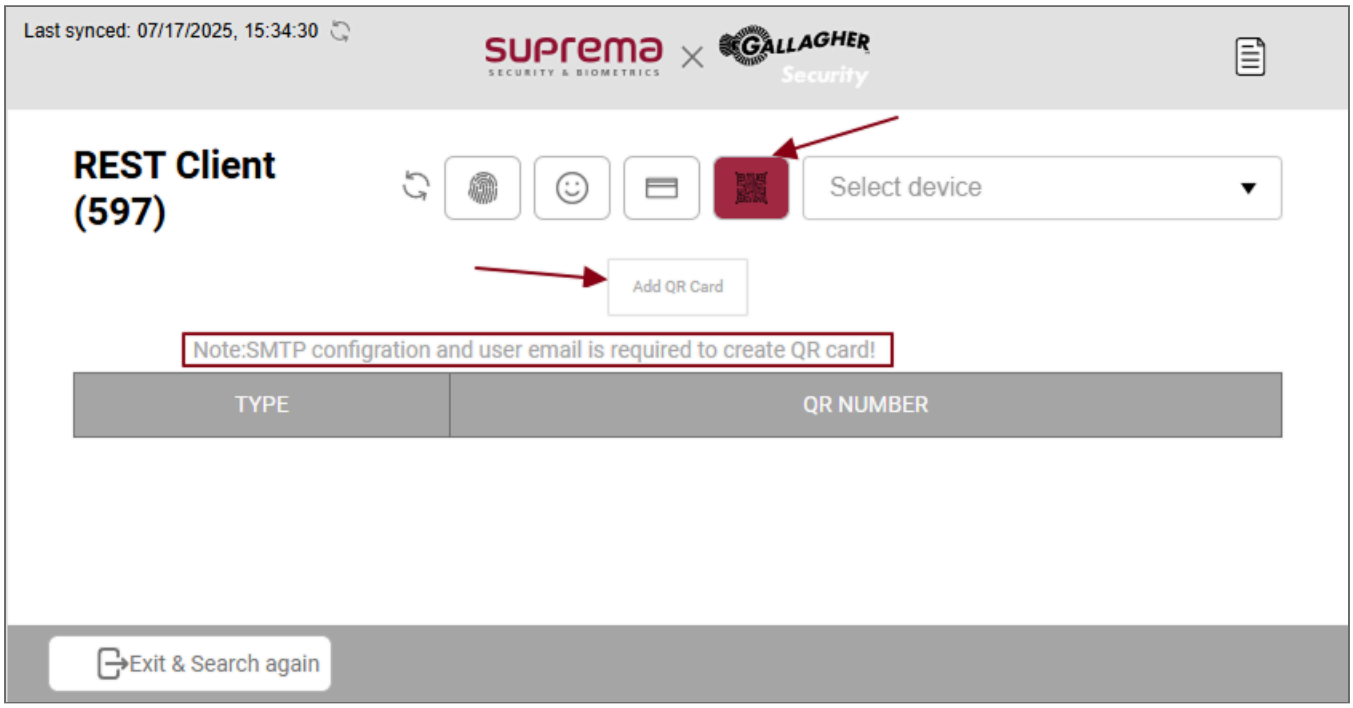
3. Access Zone を割り当てた後、下部の Save ボタンを**押します**。



4. Viewer Configuration に**移動**し、Cardholder Details を設定するために Click を**押します**。 Cardholder Details Configuration で Selected PDFs を**選択**し、Email フィールドを**選択**して、Close ボタンを**押します**。 変更を保存するには、左下の Save ボタンを**押します**。 Viewer Configuration を右クリックし、ビューアーを再読み込みします。

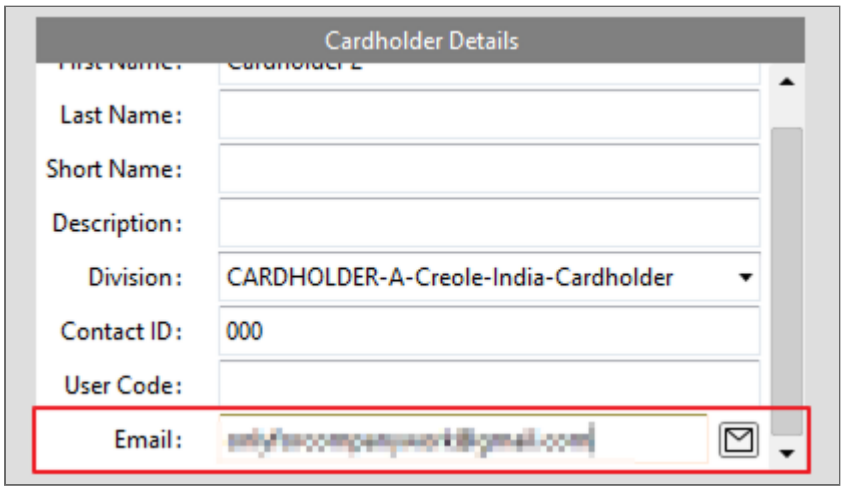


5. QR Code を割り当てるには、ミドルウェア内のユーザー プロファイルに移動し、QR アイコンを**クリック**します。 下のように、Add QR ボタンは**無効**で、ユーザーのメールアドレスが Gallagher に割り当てられていないことを示す注記があります。

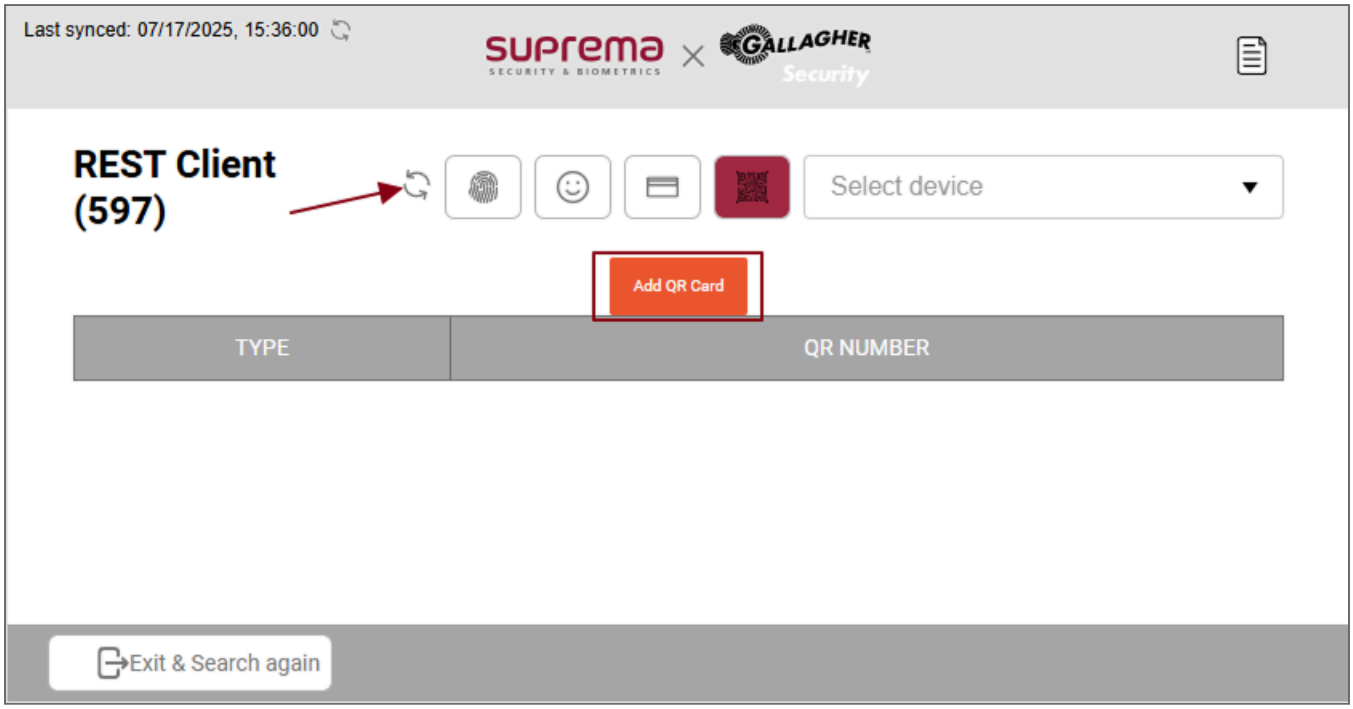


> **情報**
>
> - SMPT 設定を行うには、QR Code 用 SMTP を設定するを参照してください。
> - Gallagher でメールアドレスを設定するには、Gallagher でのメール設定を参照してください。
> - Gallagher で QR Card タイプを設定するには、QR Code カードタイプを作成するを参照してください。

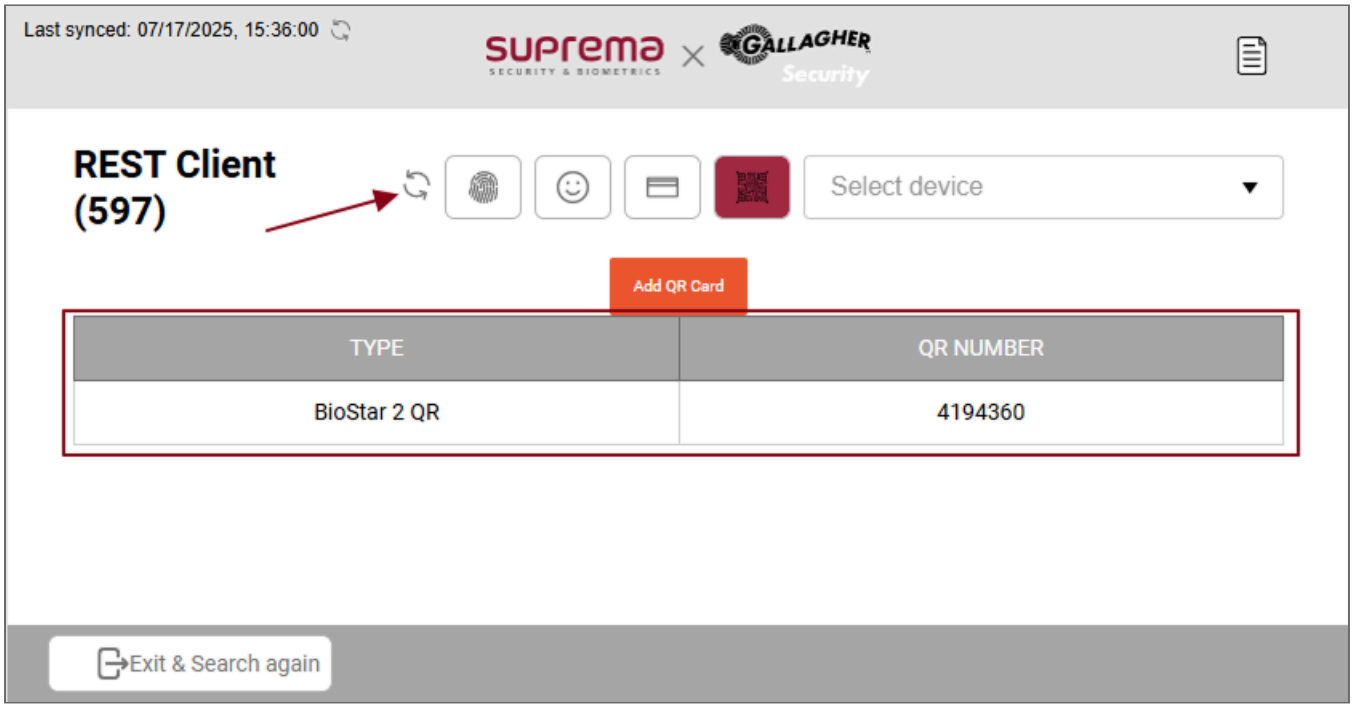
6. ユーザーにメールアドレスを割り当てるには、Command Center でユーザー詳細を開き、Cardholder details の email フィールドにユーザーのメールを入力して、save ボタンを押します。



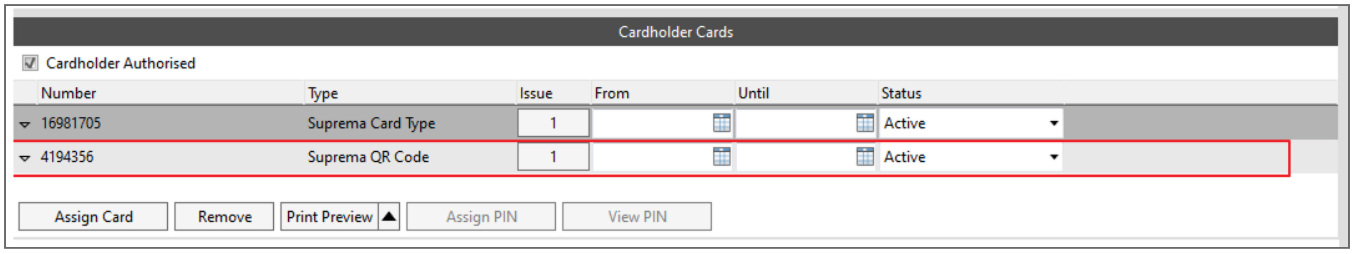
7. ミドルウェアのユーザー プロファイルで sync ボタンを押すと、メールは BioStar 2 のユーザー プロファイルに自動的に割り当てられます。 メール ボタンが有効になり、注記は削除されます。



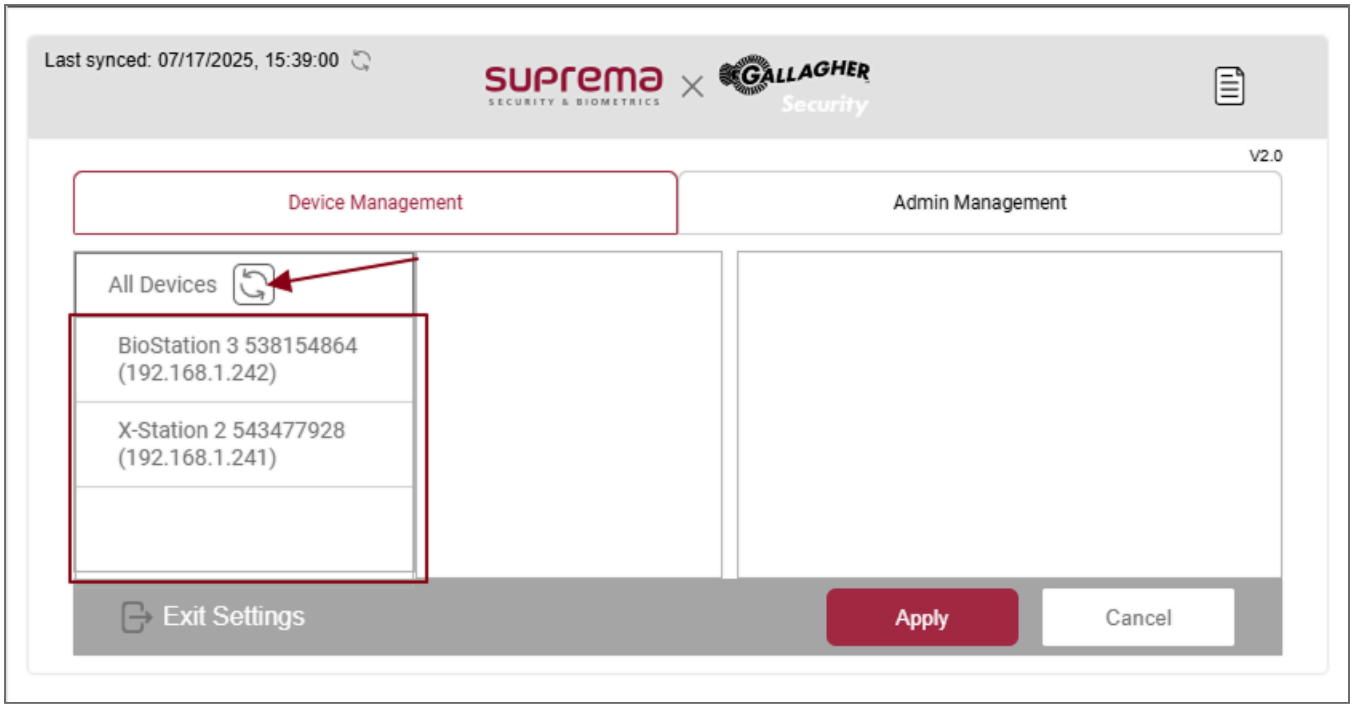
8. 次に、ユーザー プロファイルの QR セクション内で Add QR Code ボタンを押すと、QR Code が Gallagher と BioStar 2 に追加され、上で割り当てたメールアドレスに QR Code が送信されます。



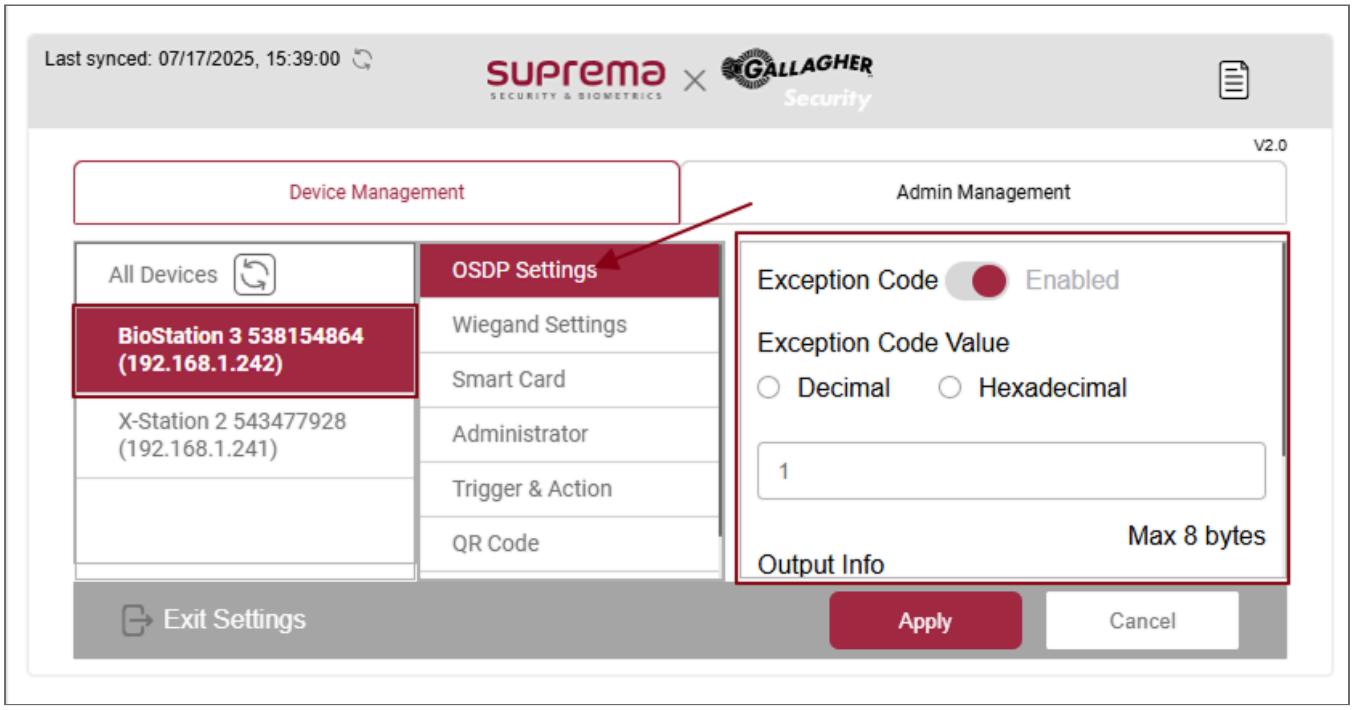
QR を追加したら、sync ボタンを**押して**データを更新できます。



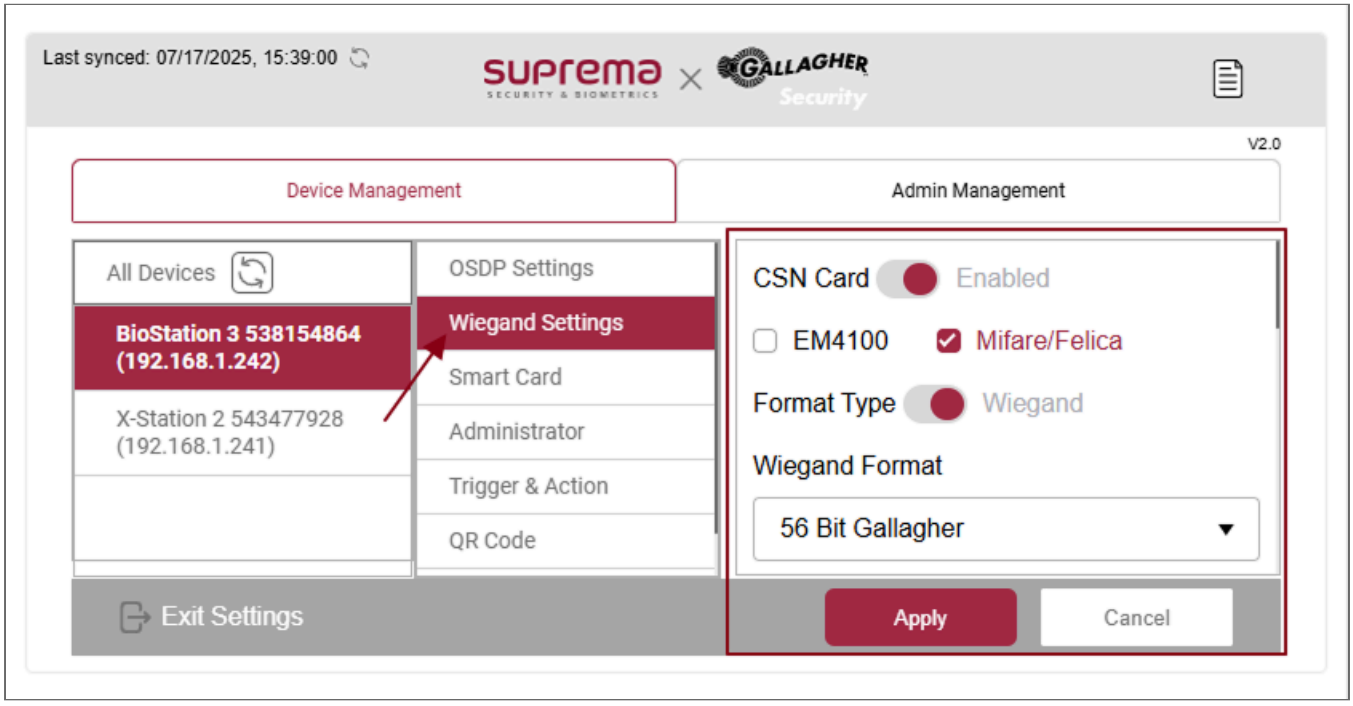
9. デバイスを同期するには sync ボタンを**押します**。ここで接続済みデバイスをすべて確認でき、任意の接続済みデバイスを選択してデバイス設定を表示できます。

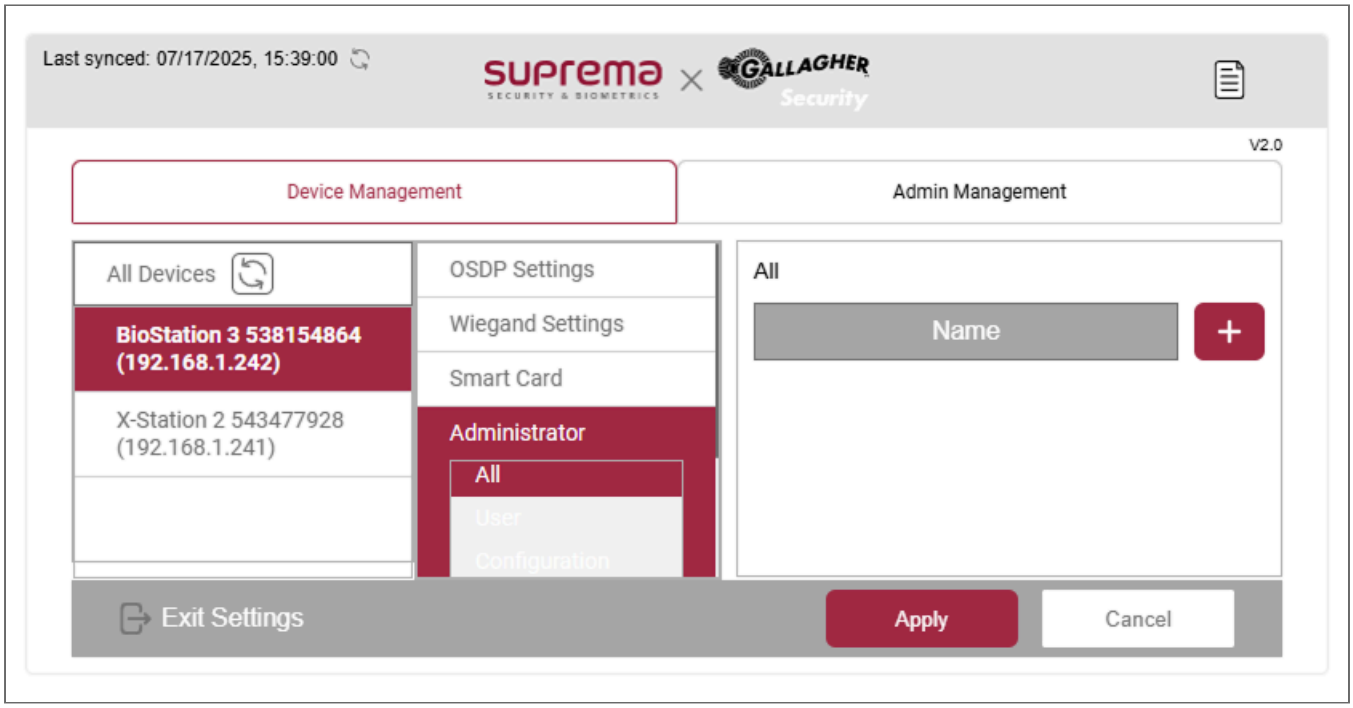


10. 下の画像はデバイスの OSDP 設定を示しています。

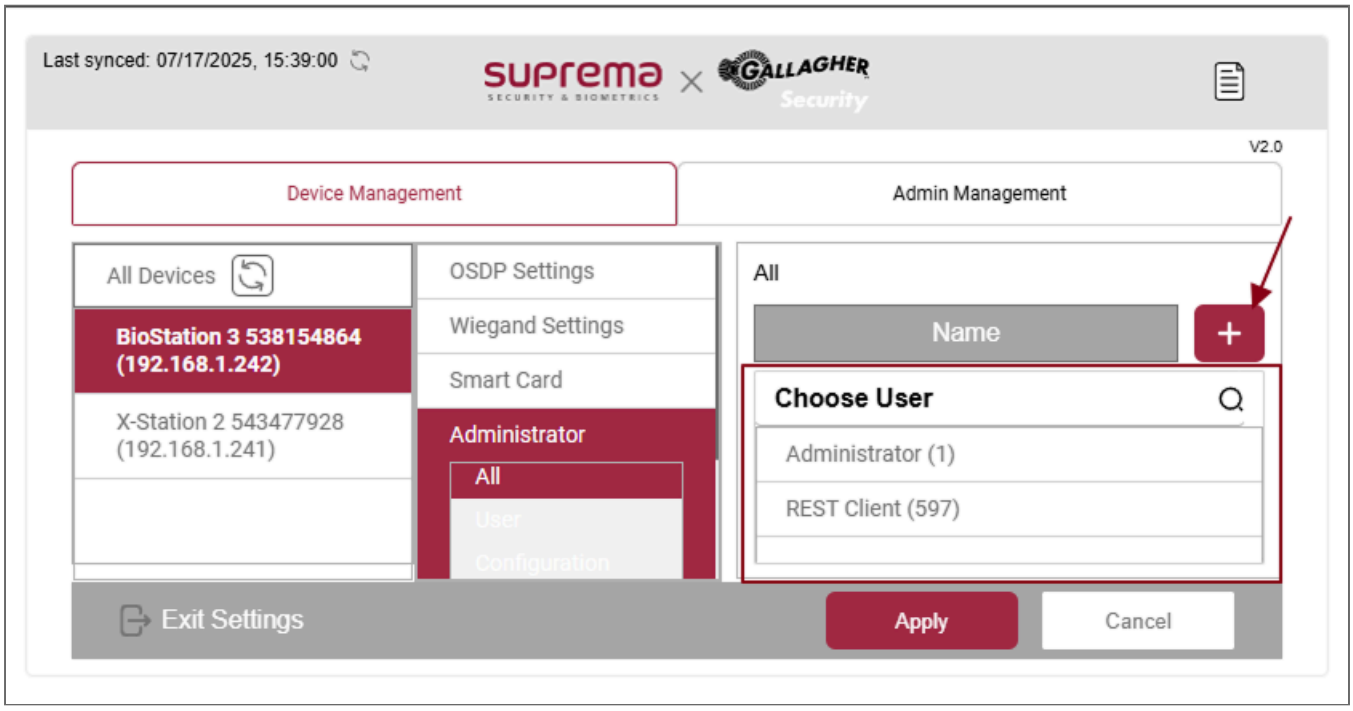


11. 下の画像はデバイスの Wiegand 設定です。

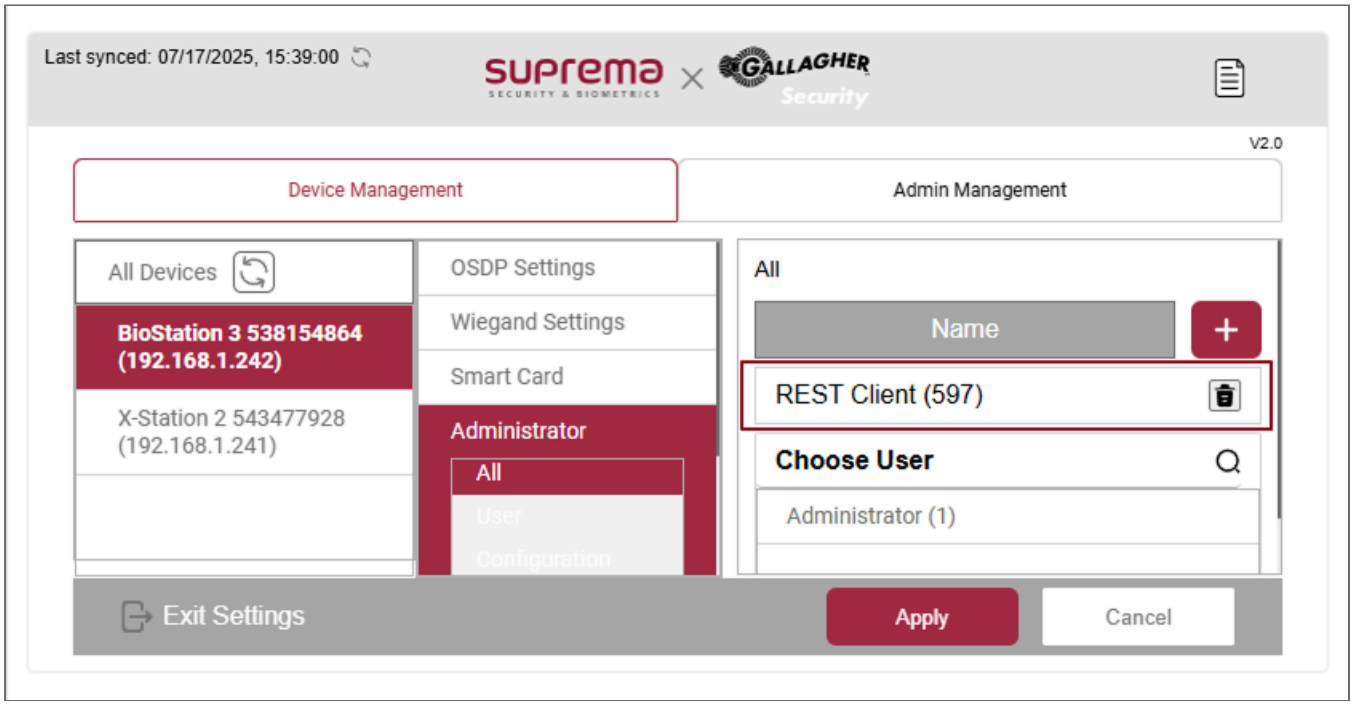




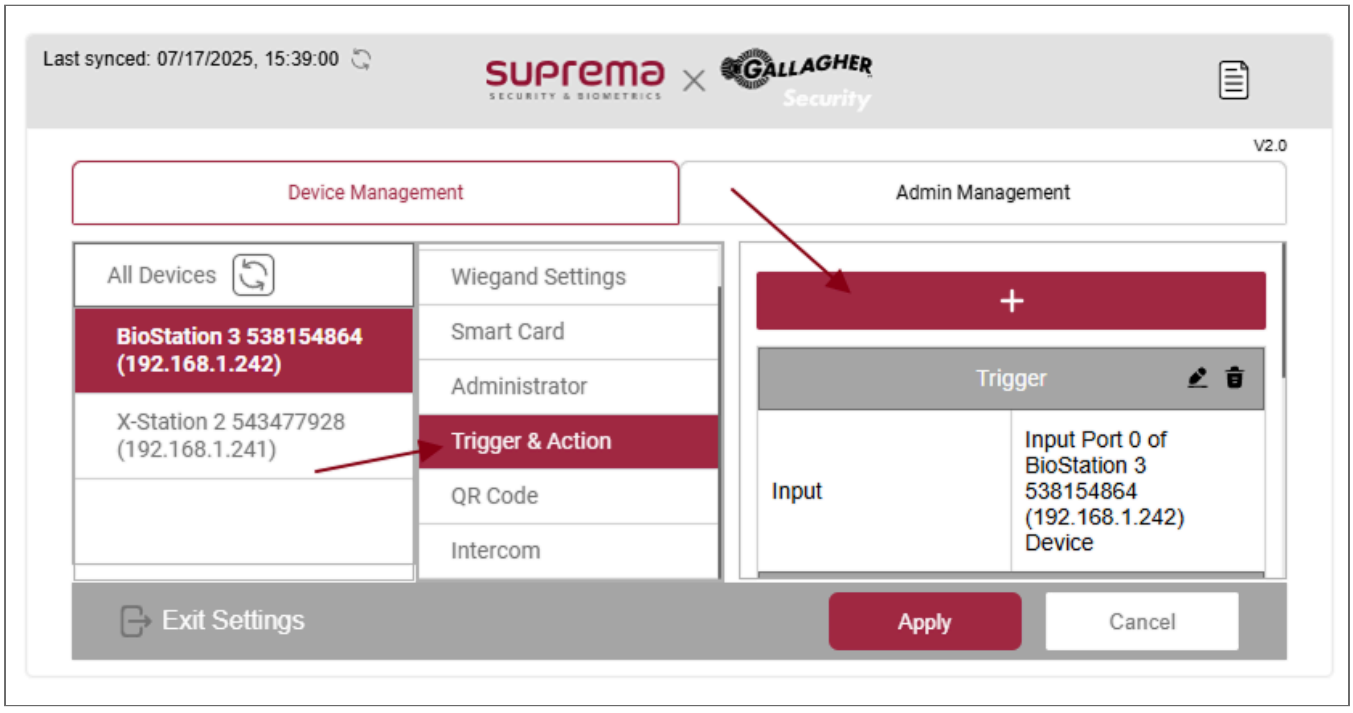
12. 上の画像は管理者モードです。必要に応じてモードを選択できます。下の画像のように + ボタンを**押す**と、ドロップダウンからさまざまなユーザーを選択できます。



13. ユーザーを**選択**すると、下の画像のように表示されます。delete ボタンを**クリック**すると、一覧からユーザーを削除できます。

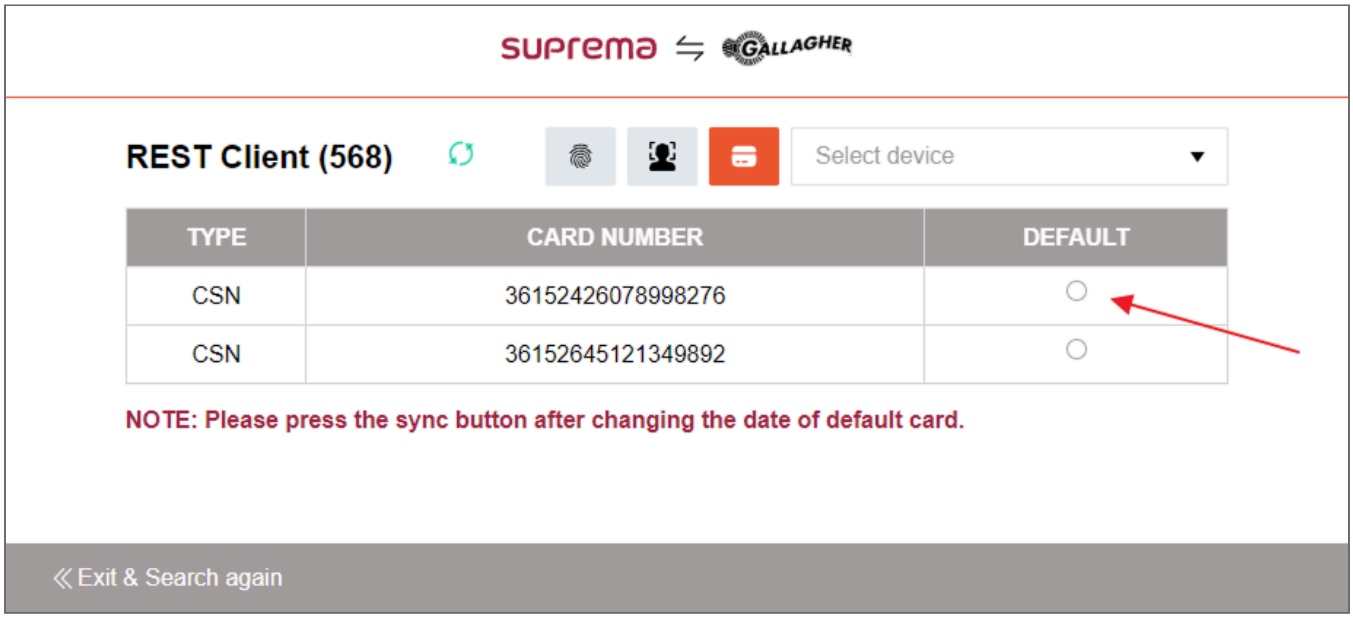


14. これはデバイスの出力モードのトリガーとアクション モードです。 + ボタンを押して設定できます。

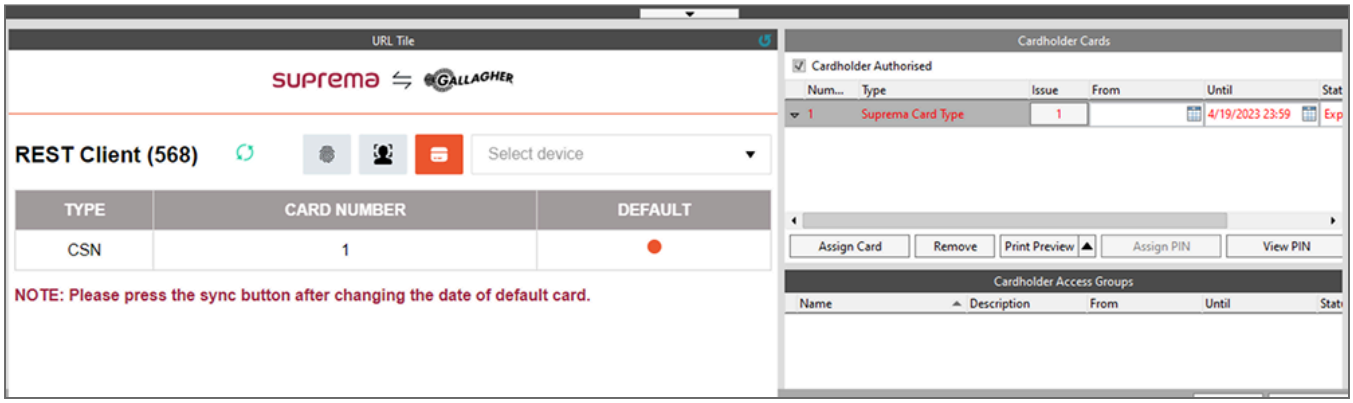


既定のカード選択

1. ユーザーのラジオ ボタンを押して既定のカードを選択できます。



2. 既定のカードに有効期限を設定して、カードホルダーの有効期限を**設定**できます。

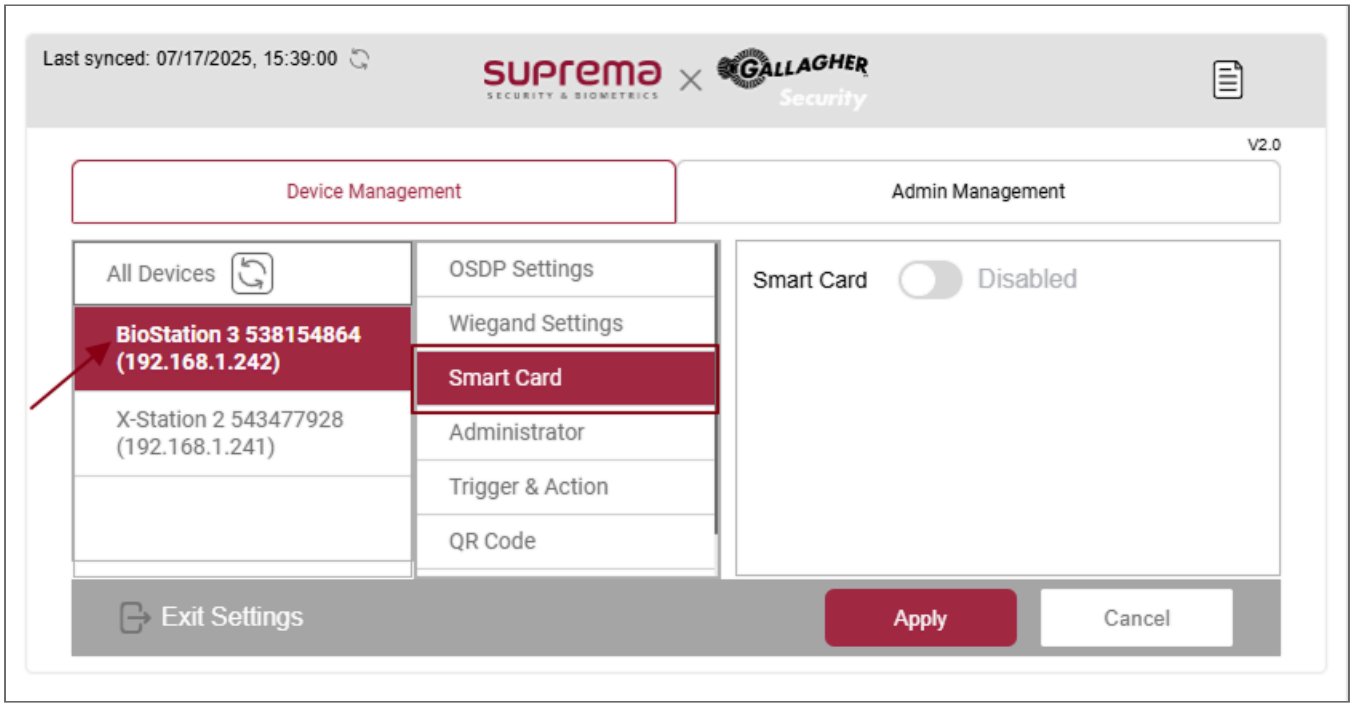


> **情報**
> Command Center で cardholder details を変更した場合は、 同じユーザーを Suprema integration with middleware で開き、sync ボタンを押す必要があります。

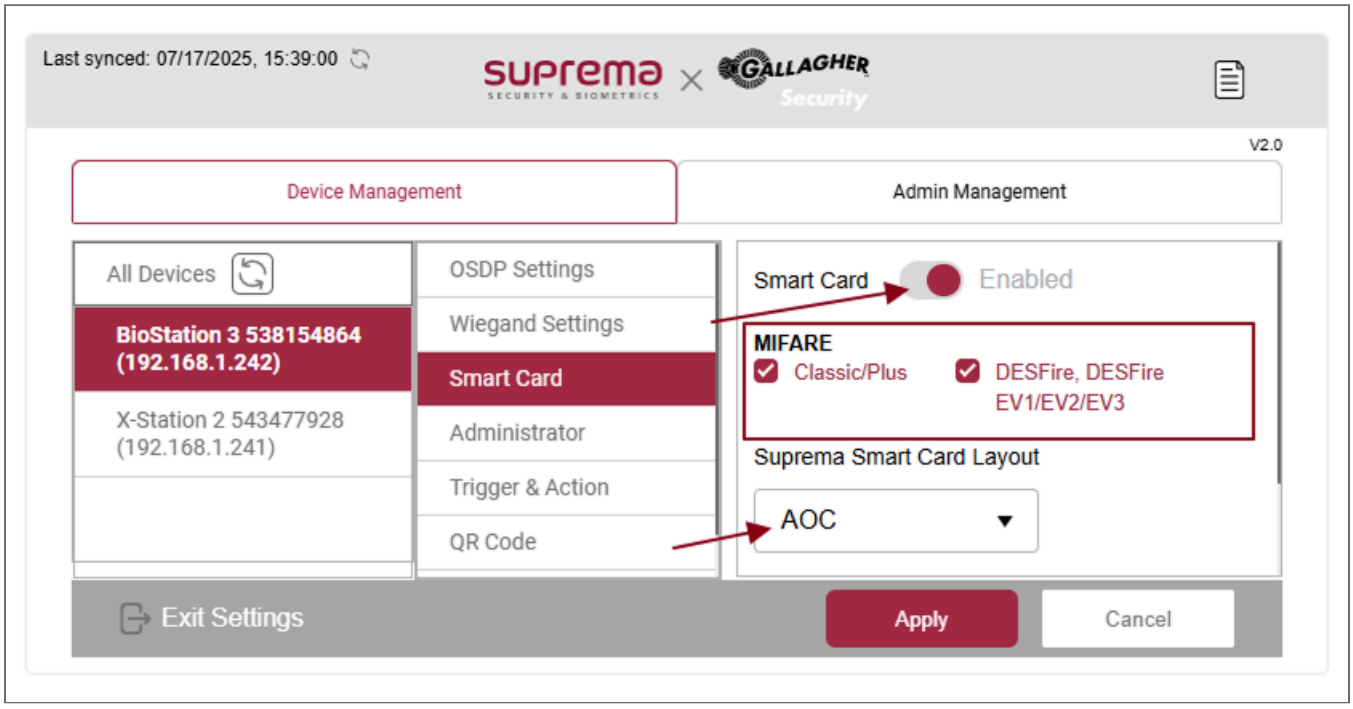
スマートカード（AOC/TOC）

> **情報**
> スマートカード機能を使用するには、BioStar 2 のバージョン 2.9.4 以上が必要です。

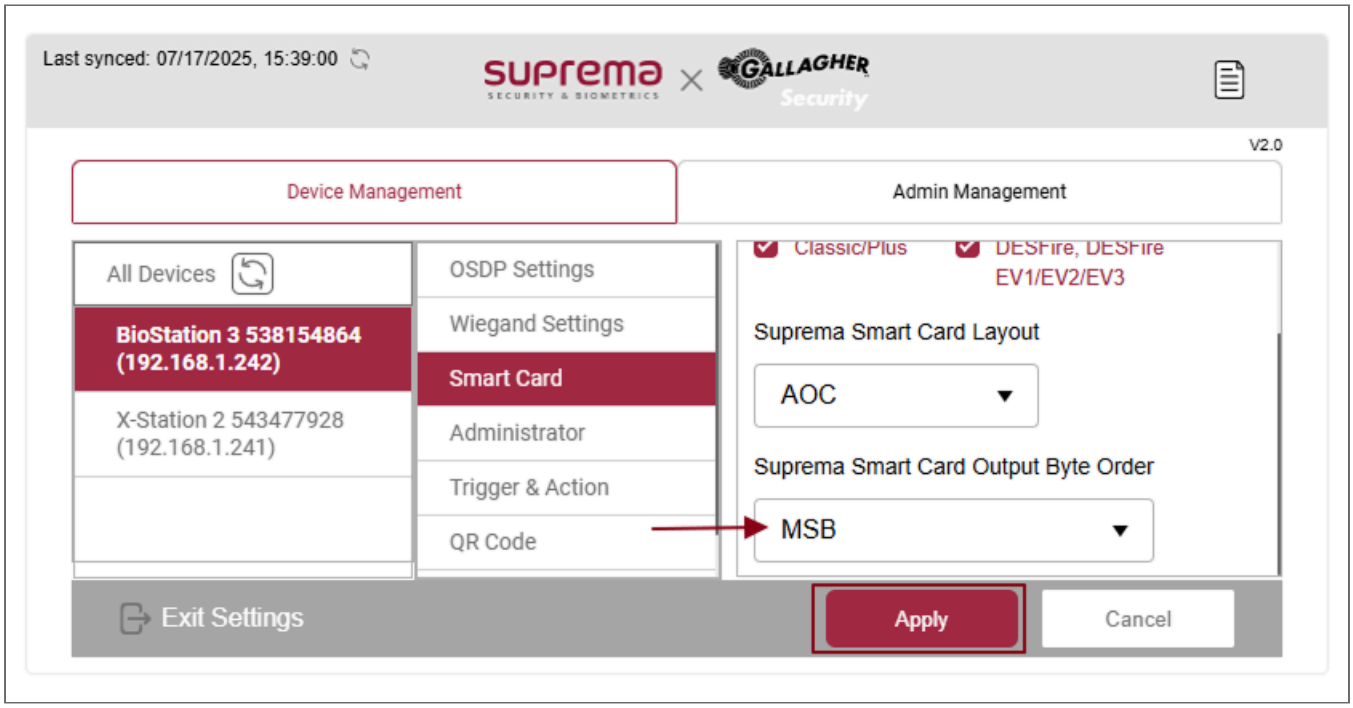
1. Smart Card（AOC/TOC）オプションを使用する場合は、デバイスの設定に移動し、**settings** ボタンを**押し**、Device Management で設定するデバイスを**選択**してから Smart Card オプションを**選択**します。



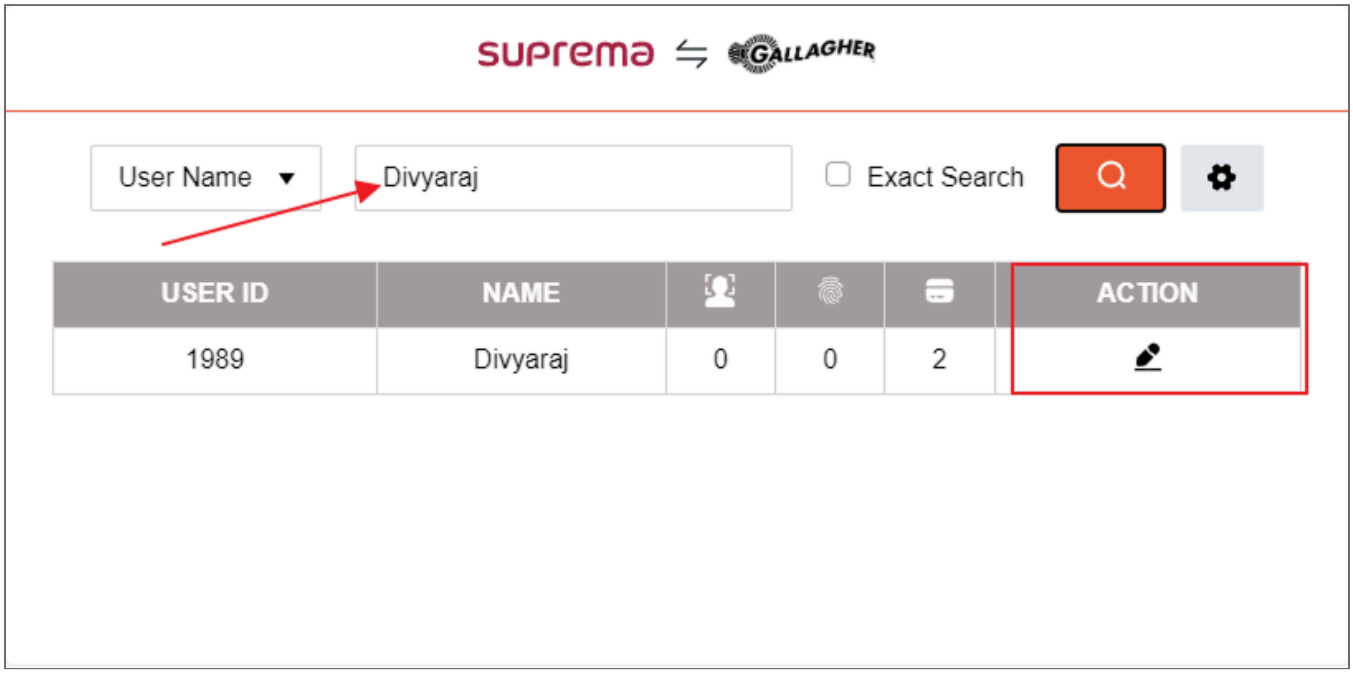
2. Smart Card トグルを**有効にし**、以下の画面のとおりに設定します。



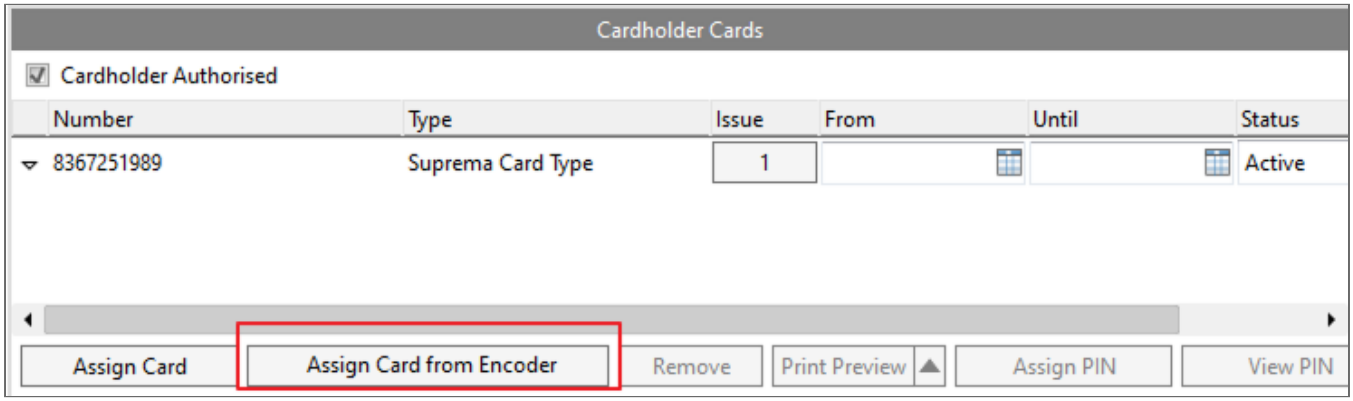
3. すべての設定を変更したら、Apply ボタンを**押します**。 その後、左下隅の Exit Settings ボタンを**押して**、設定タブを終了します。



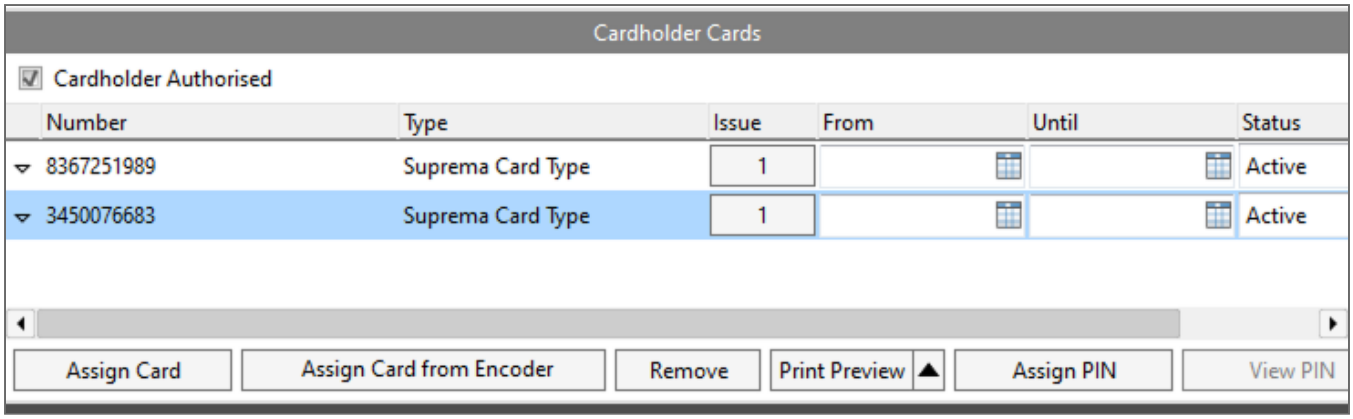
4. ユーザー検索画面で Smart Card を適用するユーザーを検索し、Edit ボタンを押してユーザー詳細を表示します。



5. 次にスマートカードを割り当てるには、Gallagher の cardholder cards タブで encoder からカードを割り当てます。

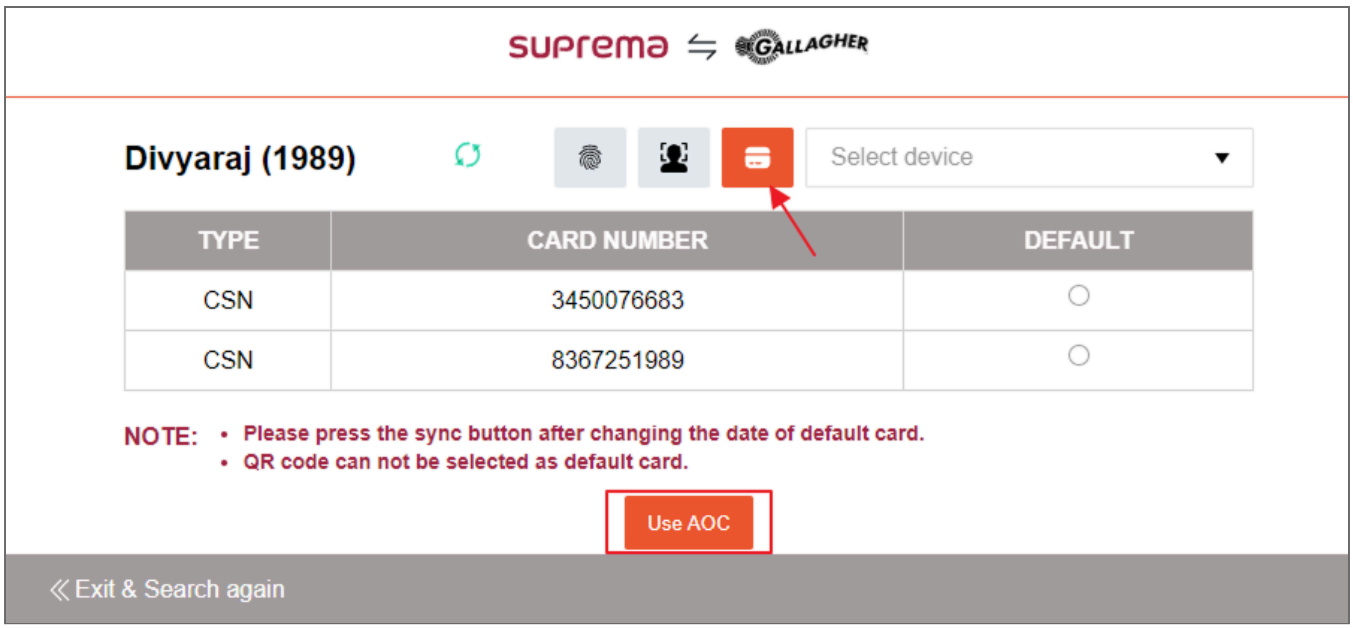


6. ボタンを押すとカード番号が表示されます。Gallagher で save を押すと、割り当てたカードが表示されます。

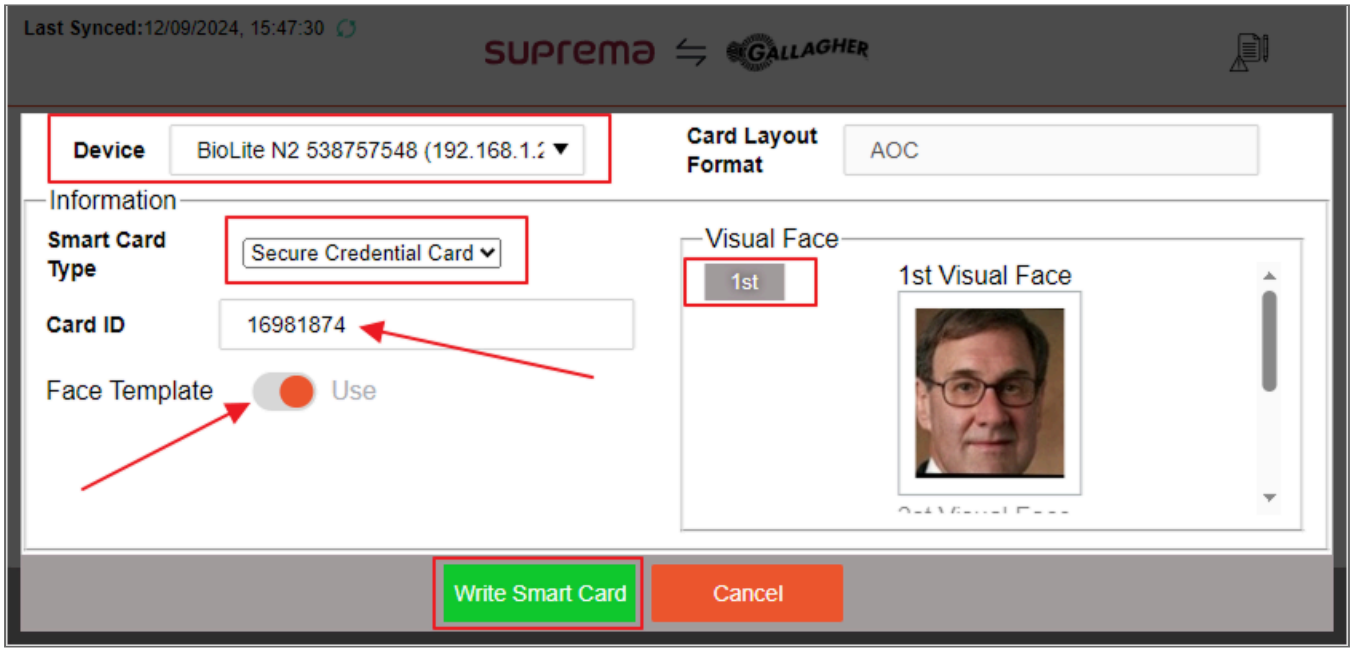


7. 次にユーザー詳細表の card セクションに移動し、Use AOC ボタンを押してユーザーにスマートカードを割り当てます。

> **情報**
> ユーザーに Smart Card（AOC）を割り当てるには、ユーザーに生体情報が必要です。



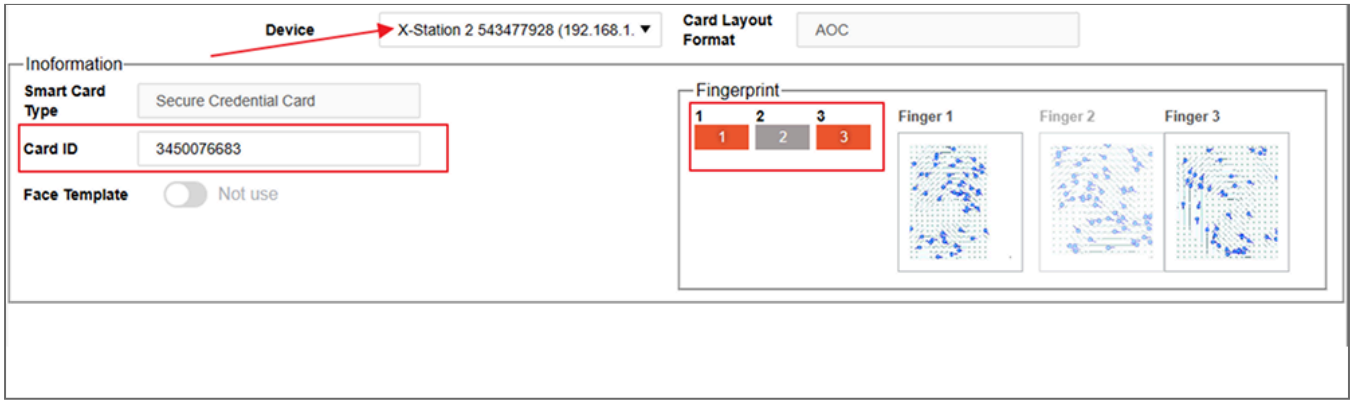
8. AOC に使用するデバイスを選択し、encoder で割り当てる際に取得したカード ID と同じ番号を使用します。 顔テンプレートを選択し、Visual Face タブの画像を選択します。 write smart card ボタンを押します。



9. 次に、選択したデバイスに同じカードを**スキャン**して、ユーザーにカードを割り当てます。 同じカードをスキャンしない場合はエラーメッセージが表示され、それ以外の場合はユーザーにカードを書き込み、ユーザーの生体情報をすべて削除します。

> **情報**
> ユーザーに割り当てられる Smart Card（AOC）の生体情報は 1 つだけです。

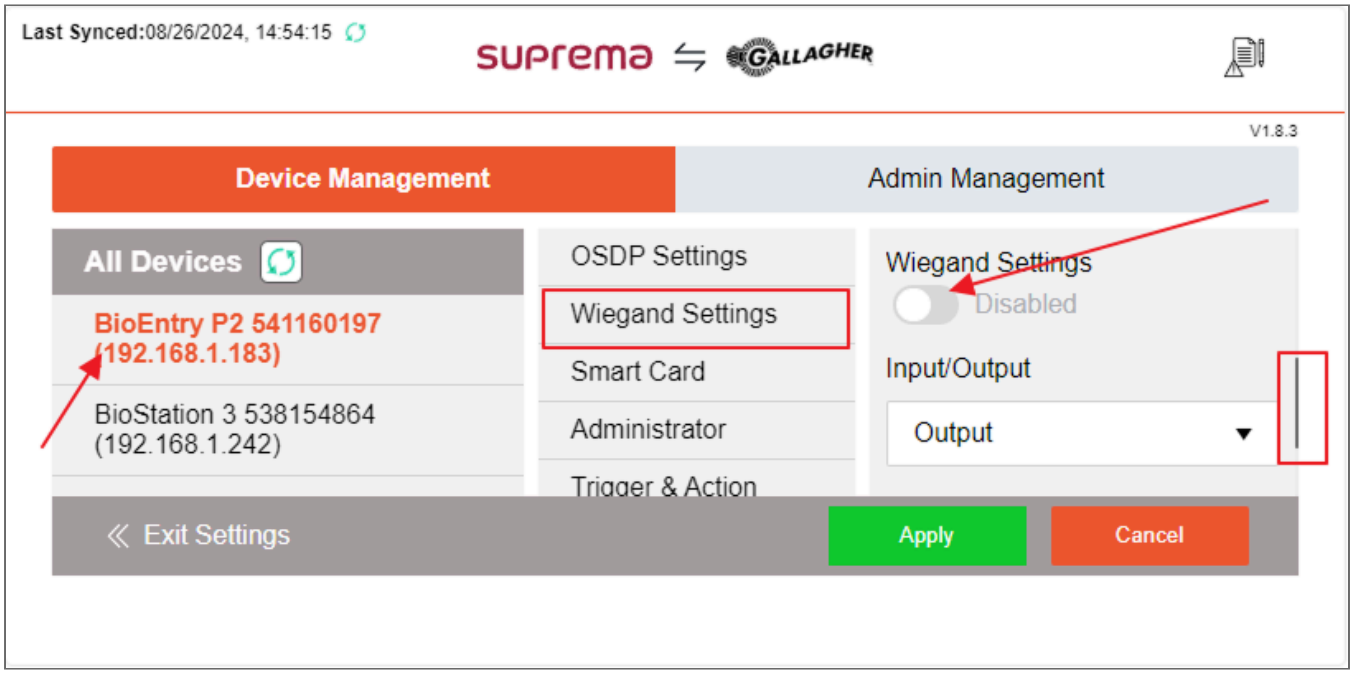
10. 指紋ユーザーにスマートカードを割り当てるには指紋が必要で、1 枚のカードに対して最大 2 つの指紋を割り当てられます。 ユーザーのカード セクションで Use AOC ボタンを**押し**、デバイスを選択します。encoder からカードを割り当てる際に取得したカード ID と同じ番号を**使用します**。 スマートカードに使用する指紋を**選択**します。 write smart card ボタンを**押します**。



11. 次に、選択したデバイスに同じカードを**スキャン**して、ユーザーにカードを割り当てます。 同じカードをスキャンしない場合はエラーメッセージが表示され、それ以外の場合はユーザーにカードを書き込み、ユーザーの生体情報をすべて削除します。

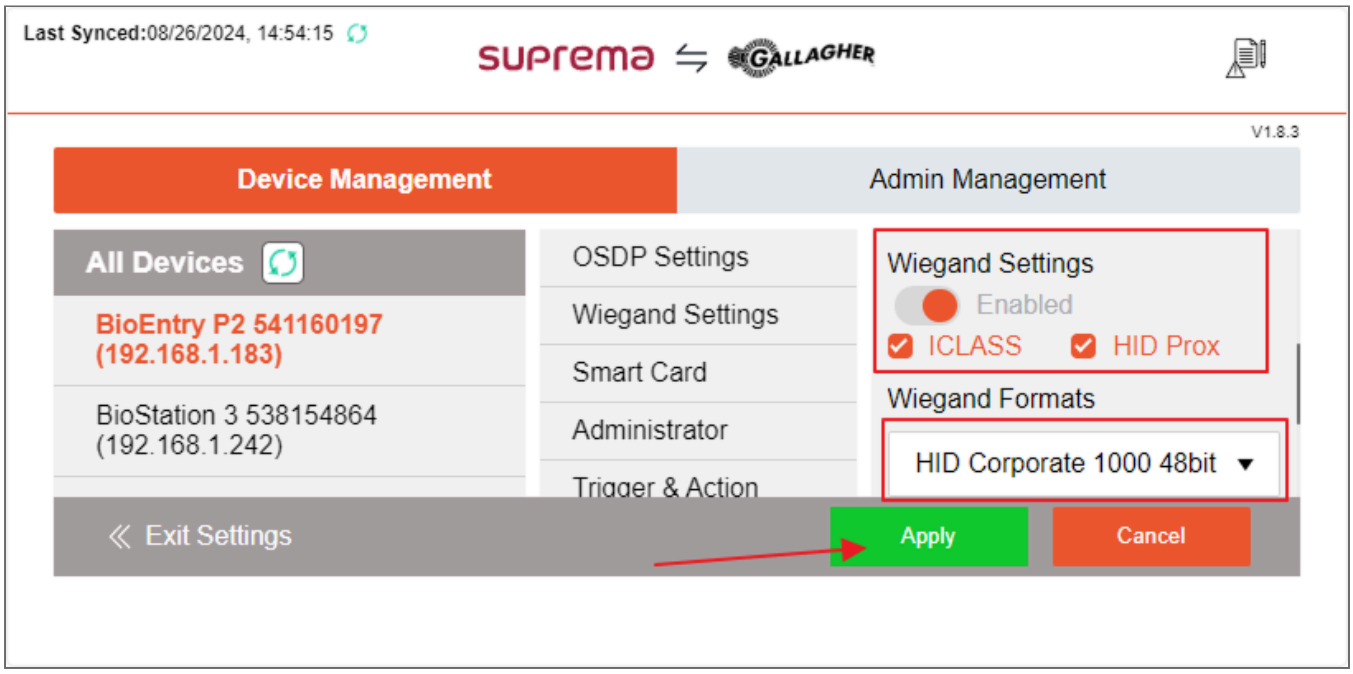
HID ICLASS カード

1. HID ICLASS カード オプションを使用する場合は、デバイスの設定に移動し、**settings** ボタンを**押し**、Device Management で設定するデバイスを**選択**してから Wiegand Settings オプションを**選択**し、下にスクロールして Wiegand 設定を見つけます。

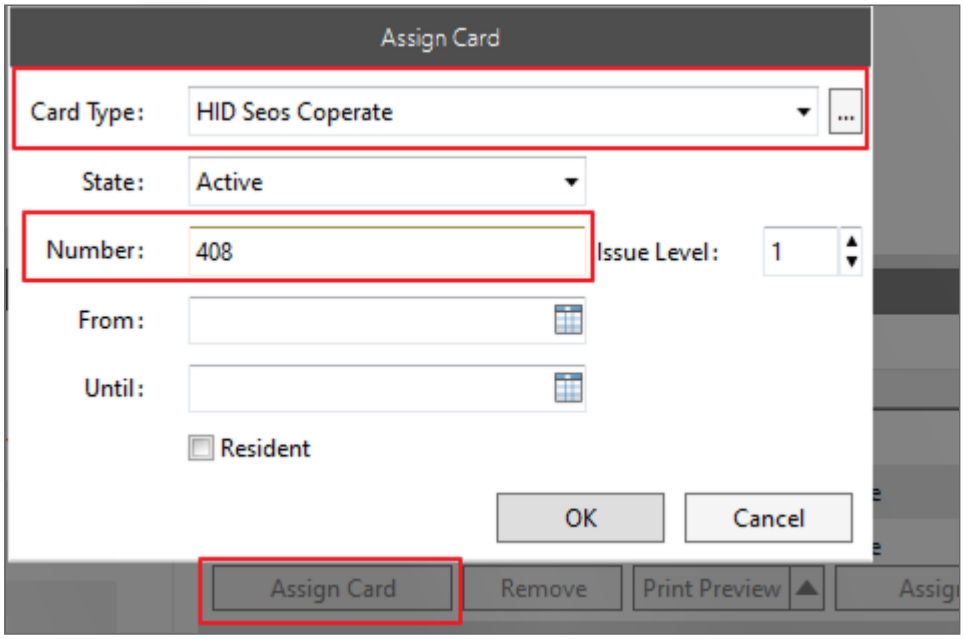


2. Wiegand Settings オプションを有効にし、ICLASS AND HID PROX オプションを選択します。 Wiegand 形式は、ドロップダウンで選択した既定値と同じである必要があります。 変更を保存するには Apply ボタンを押します。

> **情報**
> Wiegand カードを使用するには、ユーザーに少なくとも 1 つの生体情報が必要です。

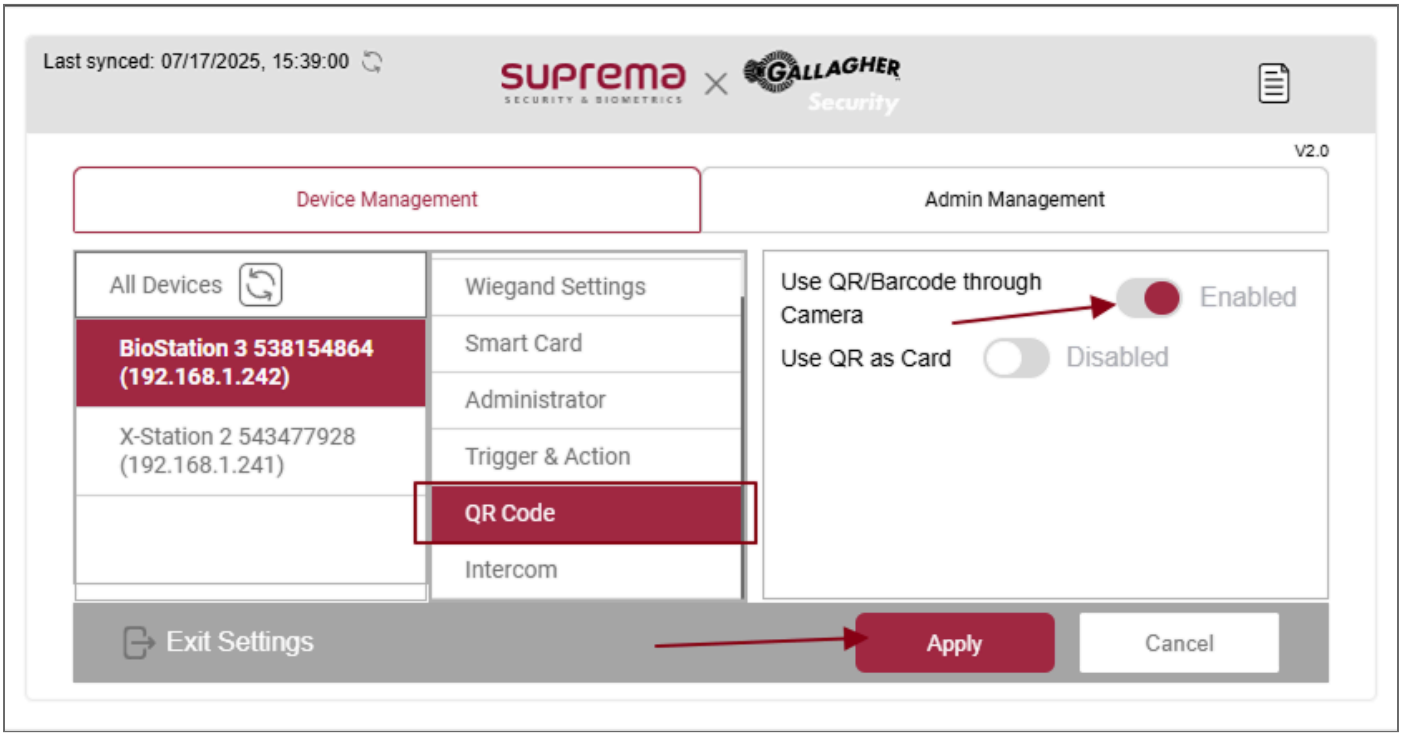


3. この機能を使用するには、ユーザーにカードを割り当てる必要があります。 Gallagher command center に移動し、assign card ボタンを押して HID Seos Corporate を選択し、番号を入力して OK ボタンを押し、Save を押します。



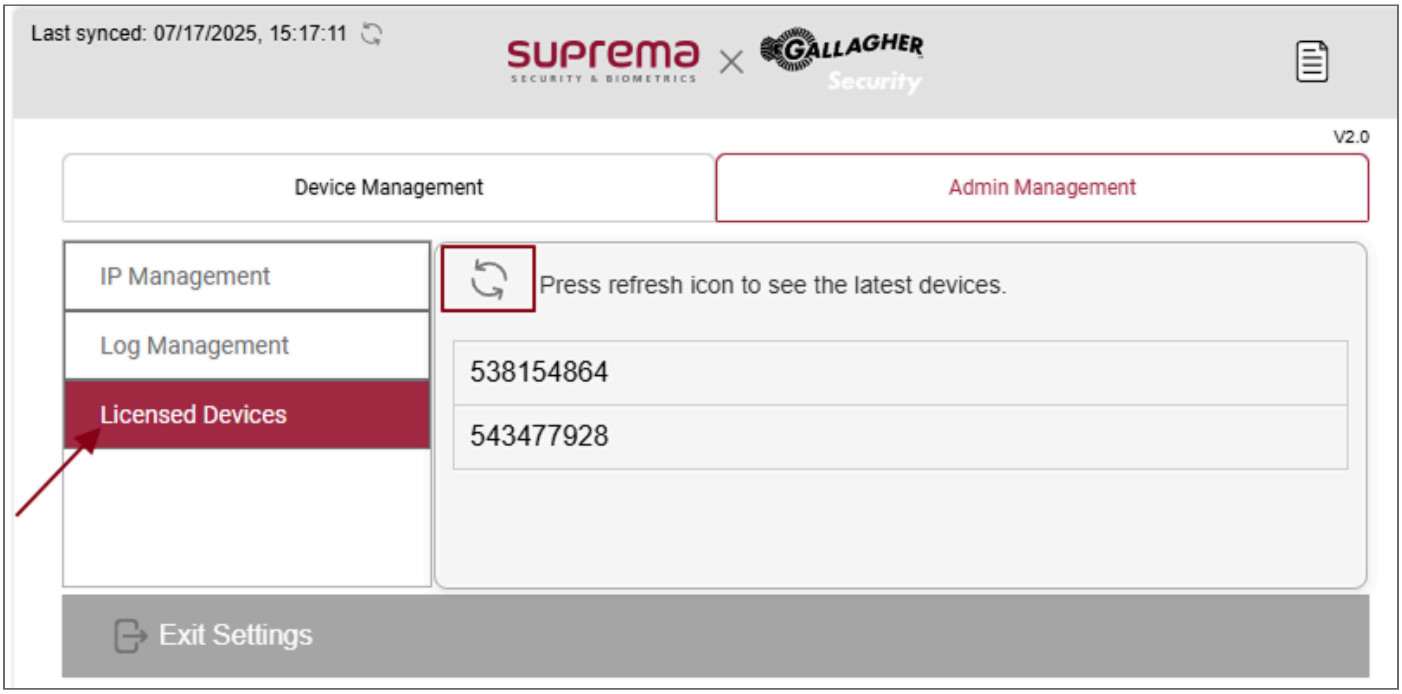
QR Code カード

QR Code カード オプションを使用する場合は、**settings** ボタンを**押して**設定に移動し、Device Management で設定するデバイスを**選択**します。 次に、QR Code Settings オプションを**選択**し、カメラ オプション設定による QR/Barcode の使用を**有効にします**。 変更を保存するには Apply ボタンを**押します**。



ライセンス済みデバイス

ライセンスに関連付けられているデバイスを確認するには、**settings** の下にある **Admin Management** に移動し、Licensed devices を**クリック**してから、sync ボタンを**押す**必要があります。 ライセンスに関連付けられた最新のデバイス一覧が表示されます。


Last synced: 07/17/2025, 15:17:11
suprema
SECURITY & BIOMETRICS
GALLAGHER
Security
V2.0
Device Management
Admin Management
IP Management
Log Management
Licensed Devices
Press refresh icon to see the latest devices.
538154864
543477928
Exit Settings

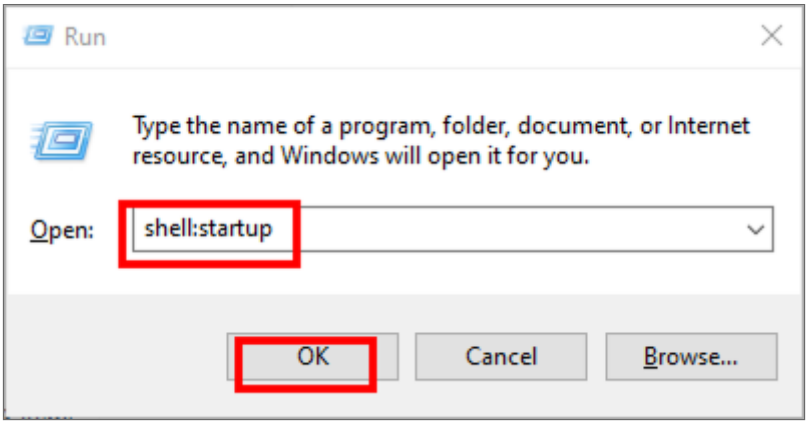
トラブルシューティングとFAQ

セットアップ

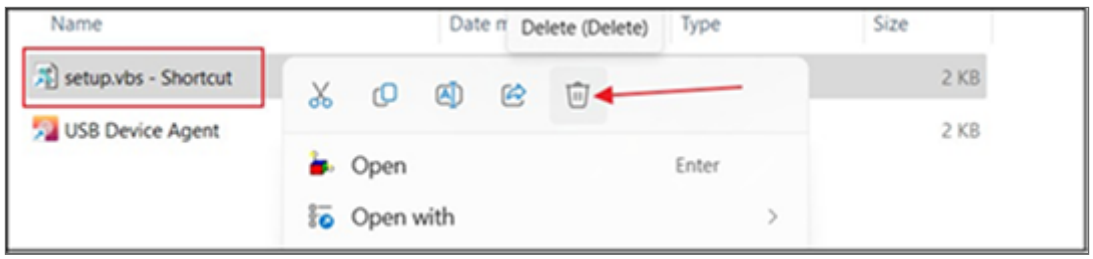
Q. ミドルウェアのみを新しいバージョンにアップグレードする（手動手順）。

A. ミドルウェアのみをアップグレードする場合は、以下の手順に従ってください。

> **情報**
> ミドルウェアを V1.8.3 にアップグレードする場合は、Migration を手動で作成する を参照してください。

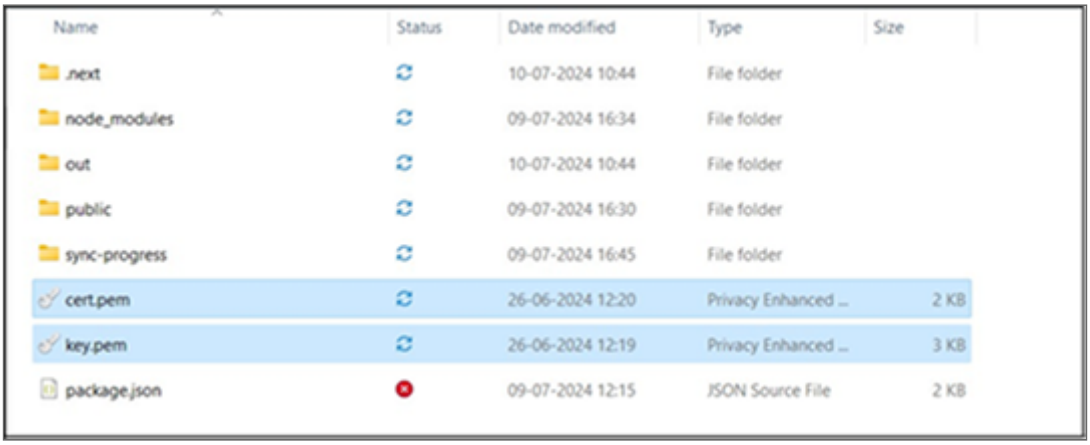


以前のバージョンの `setup.vbs - Shortcut` を削除します。



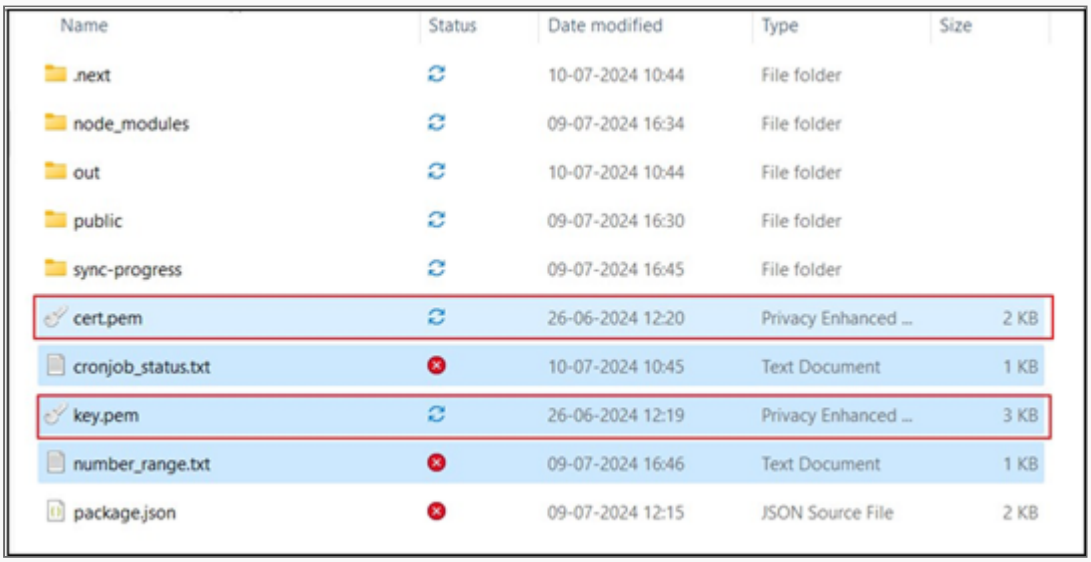
下の画像のように、現在使用しているバージョンから cert ファイルと key ファイルを切り取ります。

既定のパスは次のとおりです：`C:\Program Files\Suprema Integration with Gallagher\Suprema Integration with Gallagher v(Current working version)\files`

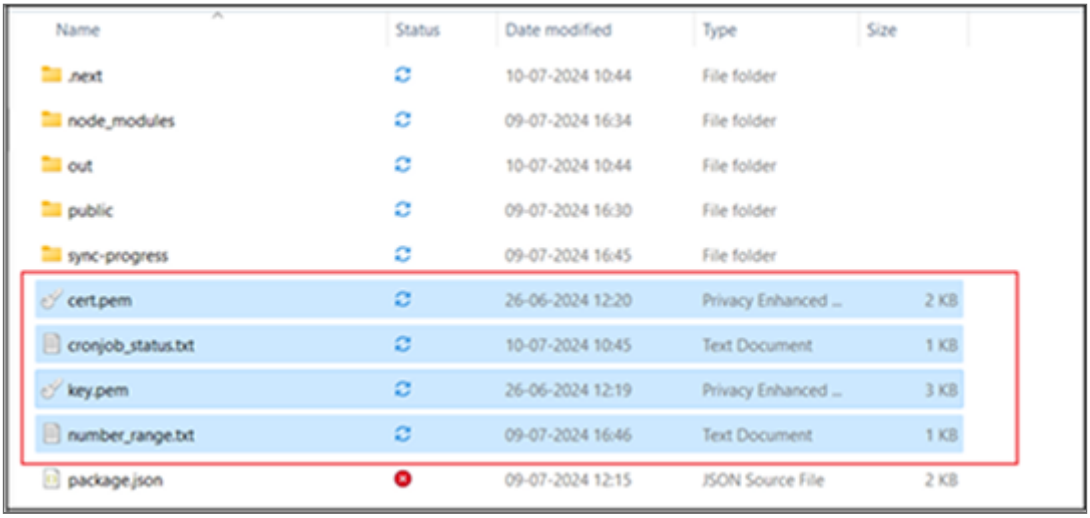


情報

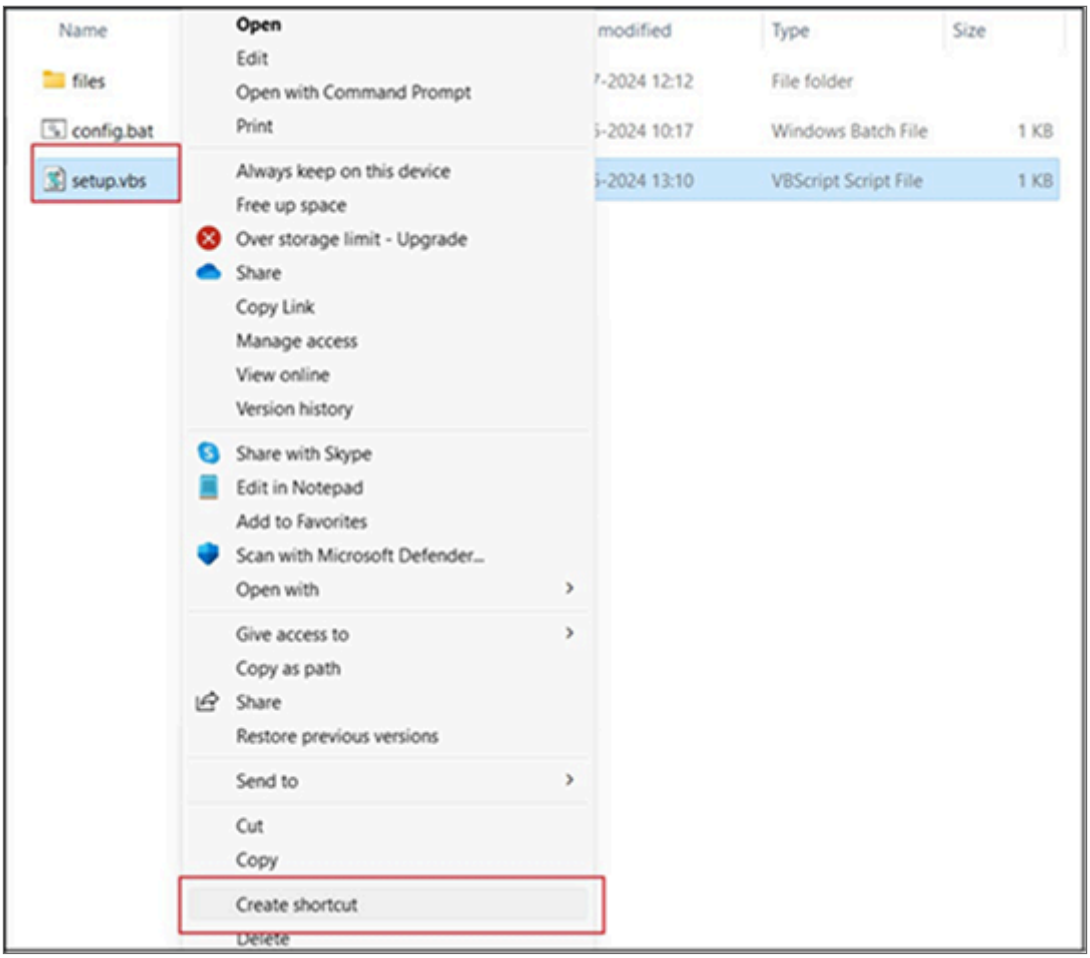
- 1.8.0 以降のバージョンからアップグレードする場合は、`key.pem`、`cert.pem`、`cronjob_status.txt`、`number_range.txt` の4ファイルを切り取る必要があります。
- 1.7.0 では `number_range` のみ使用できないため、他の3ファイルを切り取ります。



次に、上記のとおり `Gallagher V(new version)\files` にファイルを**貼り付け**ます。1.8.0 以降からアップグレードする場合は4ファイルを切り取る必要があります。下の画像は4ファイルを新しいバージョンに貼り付けた例です。4ファイルがない場合は、旧バージョンから新バージョンへ2ファイルを貼り付けてください。



Suprema Integration with Gallagher の最新バージョンの setup.vbs のショートカットを作成し、そのショートカットファイルを切り取ります。



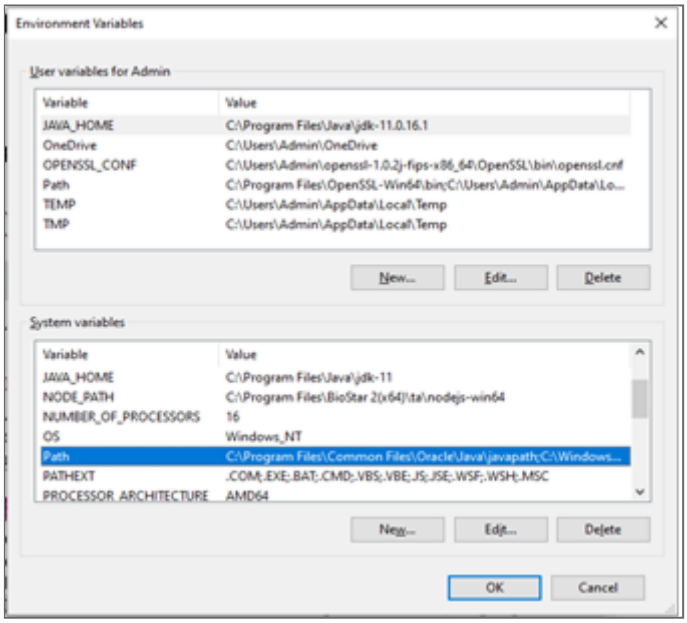
Win + R を実行し、 shell:startup に貼り付けたあと、デスクトップを再起動します。

Q. ミドルウェアが自動的に起動しない場合。

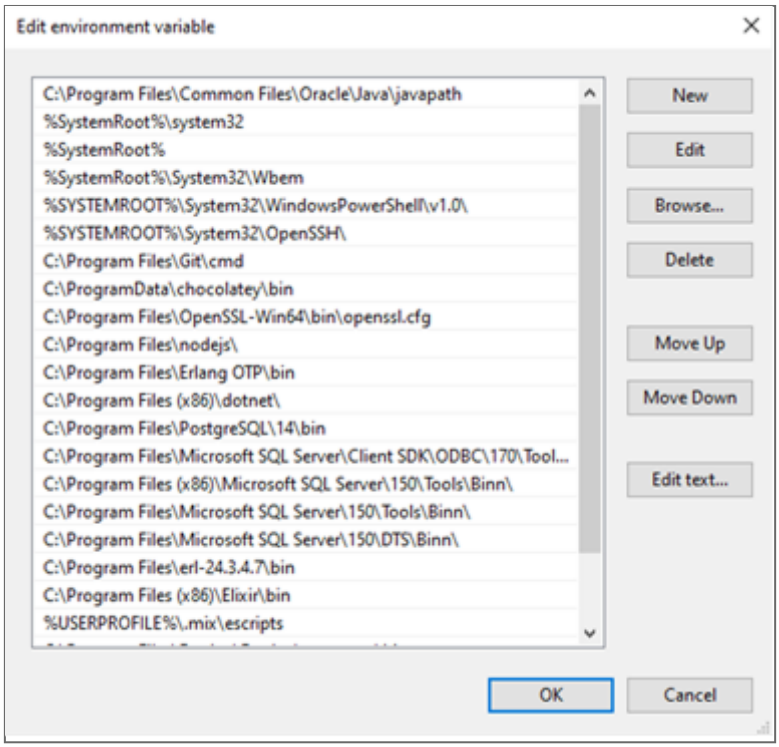
A. まず、setup.vbs ファイルのショートカットが shell:startup にあることを確認します。 setup.vbs がない場合は、 shell:startup に貼り付けてシステムを再起動します。

それでもミドルウェアが自動的に起動しない場合は、環境変数を確認します。開始 → システムの環境変数を編集 → **詳細設定** タブ → タブ下部の **環境変数** ボタンから開けます。

環境変数 ウィンドウ（下図）で、システム*環境変数* セクションの **Path** 変数を選択し、**編集** ボタンをクリックします。



環境変数の編集ウィンドウ（下図）が開いたら、**新規** ボタンをクリックし、`C:\Program Files\nodejs\` のパスを追加して **OK** ボタンを押します。



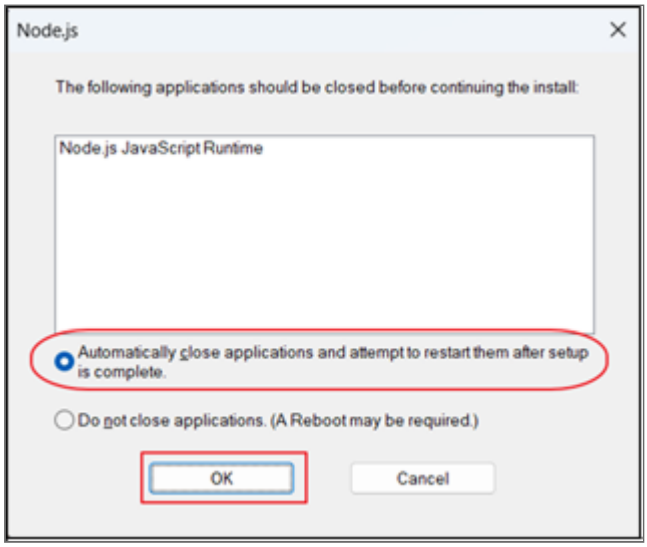
環境変数 ウィンドウで **OK** ボタンを押し、続いてシステムのプロパティでも **OK** ボタンを押します。

> **情報**
> 環境変数を作成または変更したあと、変更を Windows に反映するためにコンピューターを再起動します。

Q. ミドルウェアの前提条件リストをアンインストールする。

A. 以下は、ミドルウェアの前提条件をアンインストールする手順です。

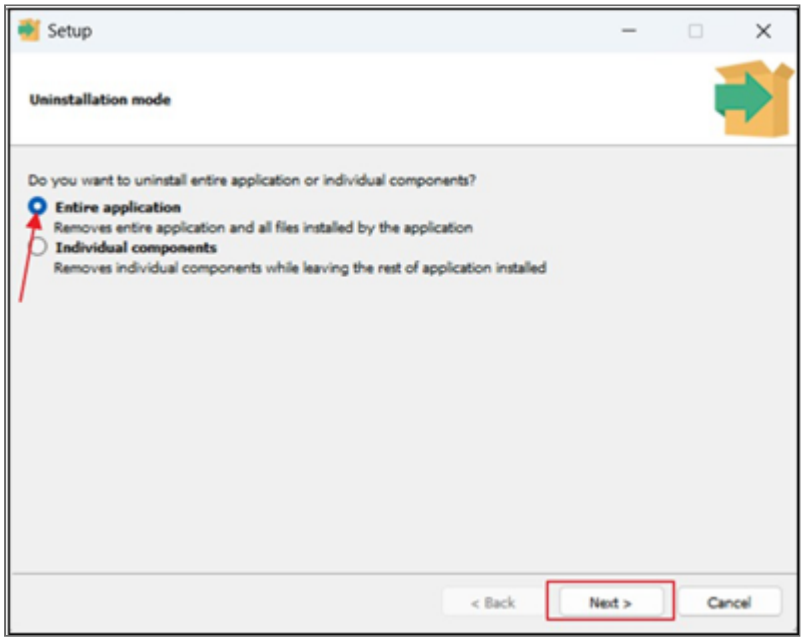
1. **コントロール パネル** を開き、**プログラムと機能** に移動します。
2. 下へスクロールして **Node.js** を検索し、右クリックして **アンインストール** を選択します。
3. Node.js のアンインストールを求められたら、**はい** を押してアンインストールを開始します。
4. しばらくすると Runtime application の削除を求められるので、以下に従って **OK** を押します。 該当しない場合は、この手順をスキップしてください。



5. 次に **OpenSSL** を検索し、右クリックして **アンインストール** を押します。
6. OpenSSL のアンインストールを求められたら、**はい** を押し、アンインストールを開始します。
7. 次に **PgAdmin 4** を検索し、右クリックして **アンインストール** を押します。

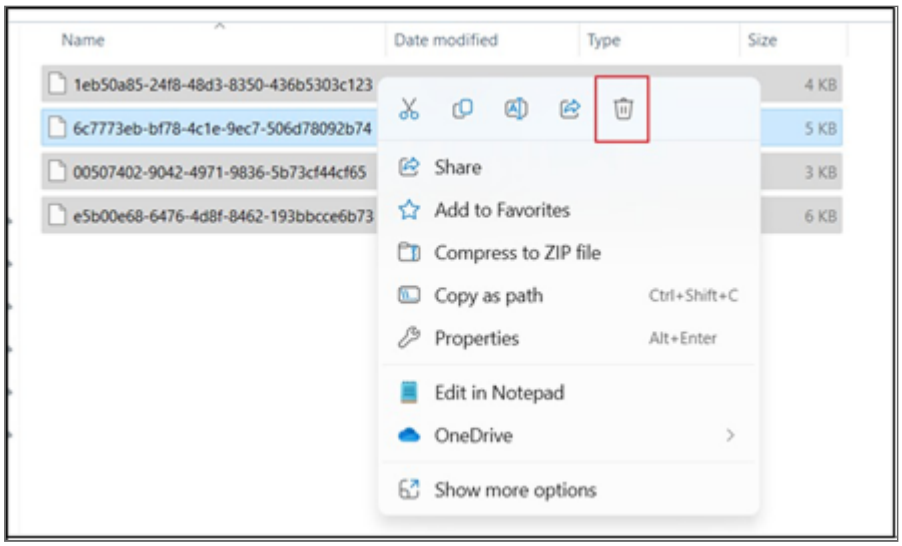
> **情報**
> PgAdmin 4 が表示されない、またはアンインストールできない場合は、この手順をスキップして次へ進んでください。

8. PgAdmin 4 のアンインストールを求められたら、**はい** を押し、アンインストールを開始します。
9. 次に PostgreSQL 14 を検索し、右クリックして **アンインストール** を押します。
10. PostgreSQL 14 のアンインストールを求められたら、**はい** を押し、アンインストールを開始します。
11. アンインストール モードが開いたら、**アプリケーション全体** のラジオ ボタンを選択し、**次へ** を押します。



12. 次に C:\Users\<YourUser>\AppData\Roaming\pgadmin\sessions に移動し、このフォルダー内のすべてのファイルを削除します。

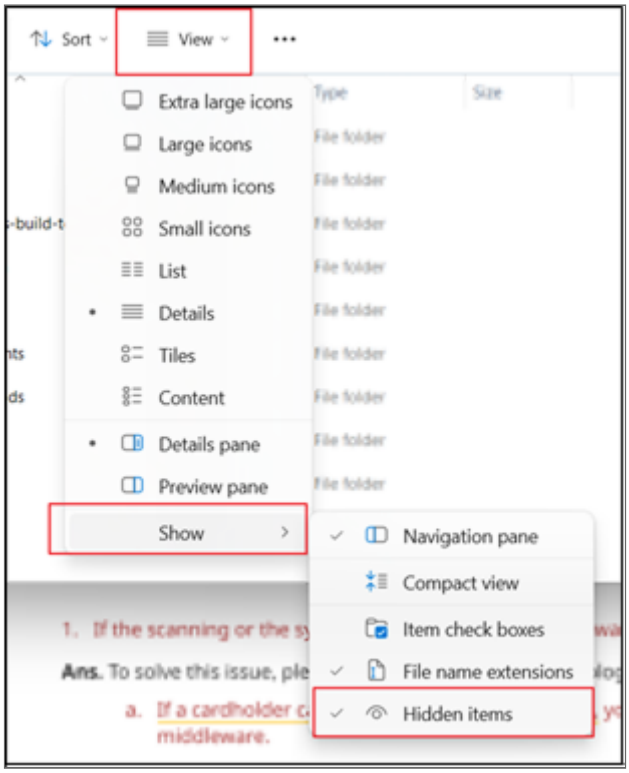
> **情報**
> AppData フォルダーが表示されない場合：Windows で AppData フォルダーを開く。



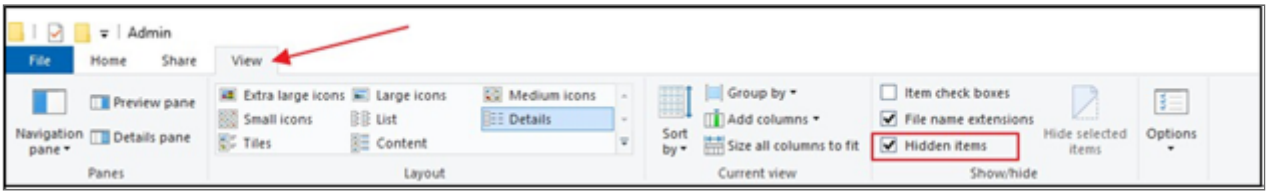
13. 次に C:\Users\<Your User>\AppData\Local に移動し、PgAdmin フォルダーと PgAdmin4 フォルダーを選択してフォルダーを削除します。
14. 次に C:\Program Files に移動し、PostgreSQL フォルダーを削除します。

Q. Windows で AppData フォルダーを開く方法。

A. Windows 11 を使用している場合は、ファイル マネージャーで **表示** タブをクリックし、**表示** を選択して **隠しファイル** をクリックします。



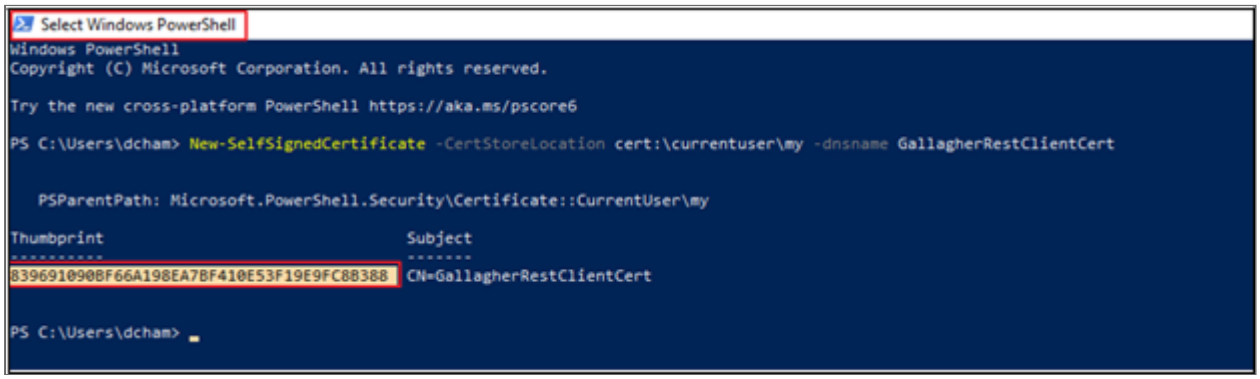
Windows 10 を使用している場合は、ファイル マネージャーを開き、**表示** を**クリック**して **隠しファイル** を**選択**します。



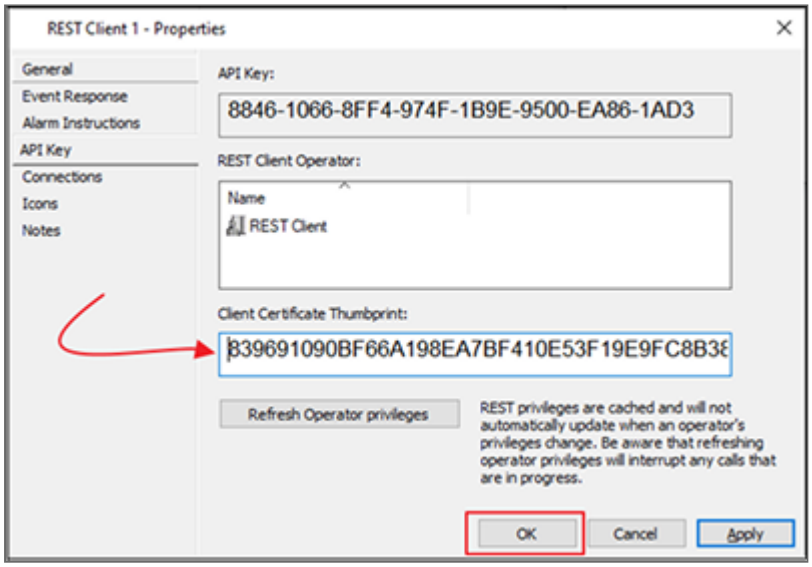
Q. thumbprint と証明書を手動で生成する方法。

A. 1. Client Certificate の Thumbprint を生成するには、Windows PowerShell を開き、このコマンドを実行して証明書の Thumbprint を取得します。

> *New-SelfSignedCertificate -CertStoreLocation cert:\currentuser\my -dnsname GallagherRestClientCert*

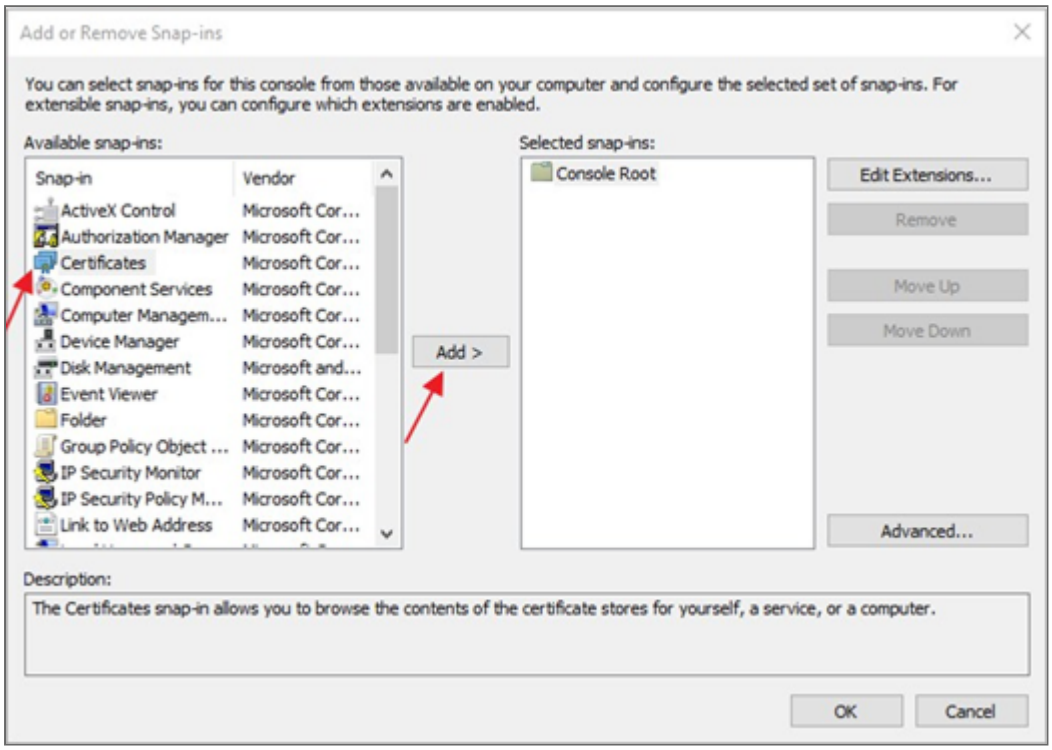


2. Thumbprint をコピーし、Client Certificate Thumbprint セクションに **Client Certificate Thumbprint key** を貼り付け、**OK** ボタンを押して、Services and Workstations も閉じます。

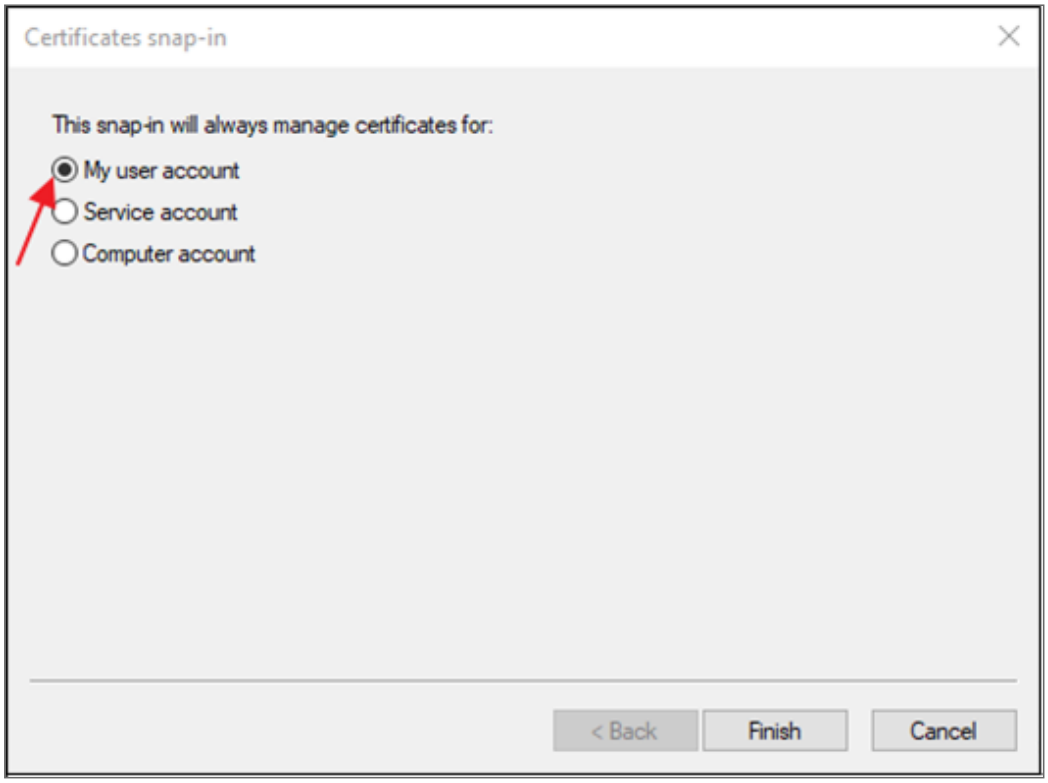


SSL証明書の生成

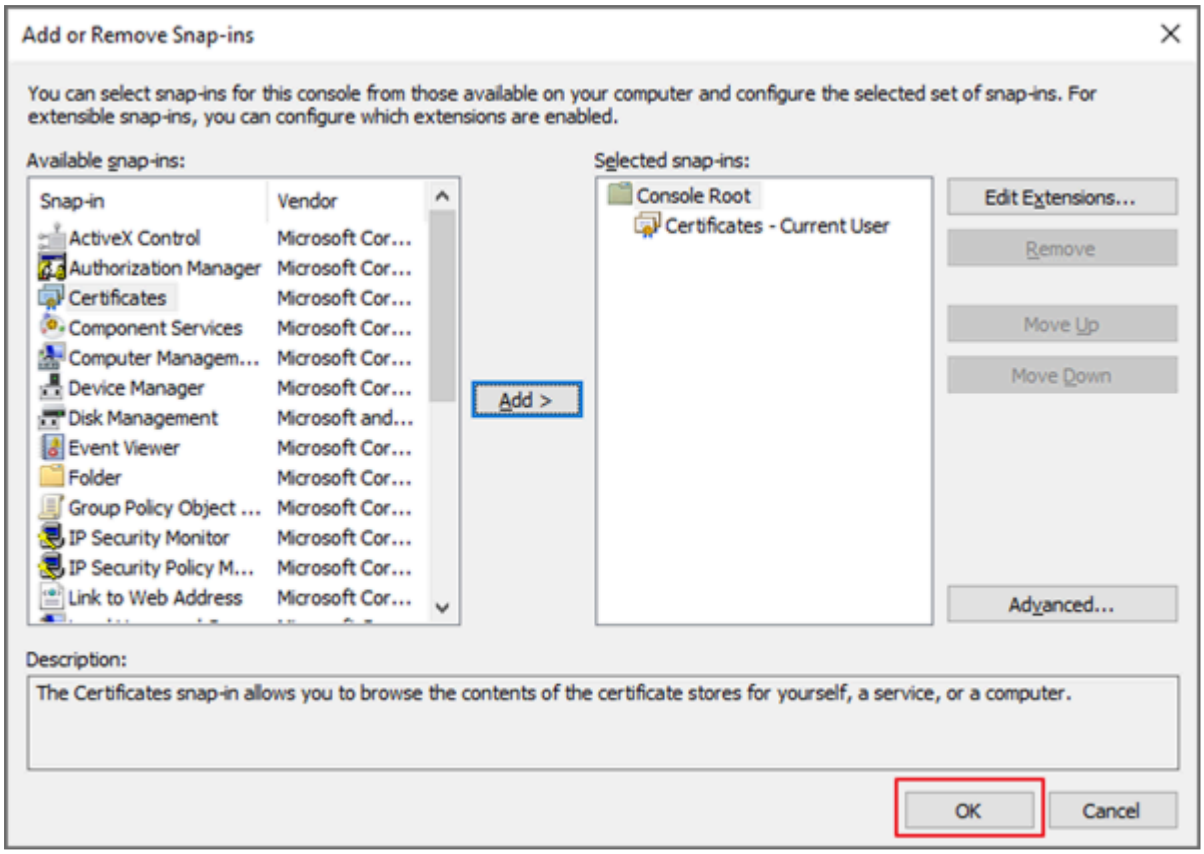
1. スタート メニューを開き、MMC アプリケーションを開きます。
2. **ファイル → スナップインの追加と削除…** に進み、下の画面を表示します。



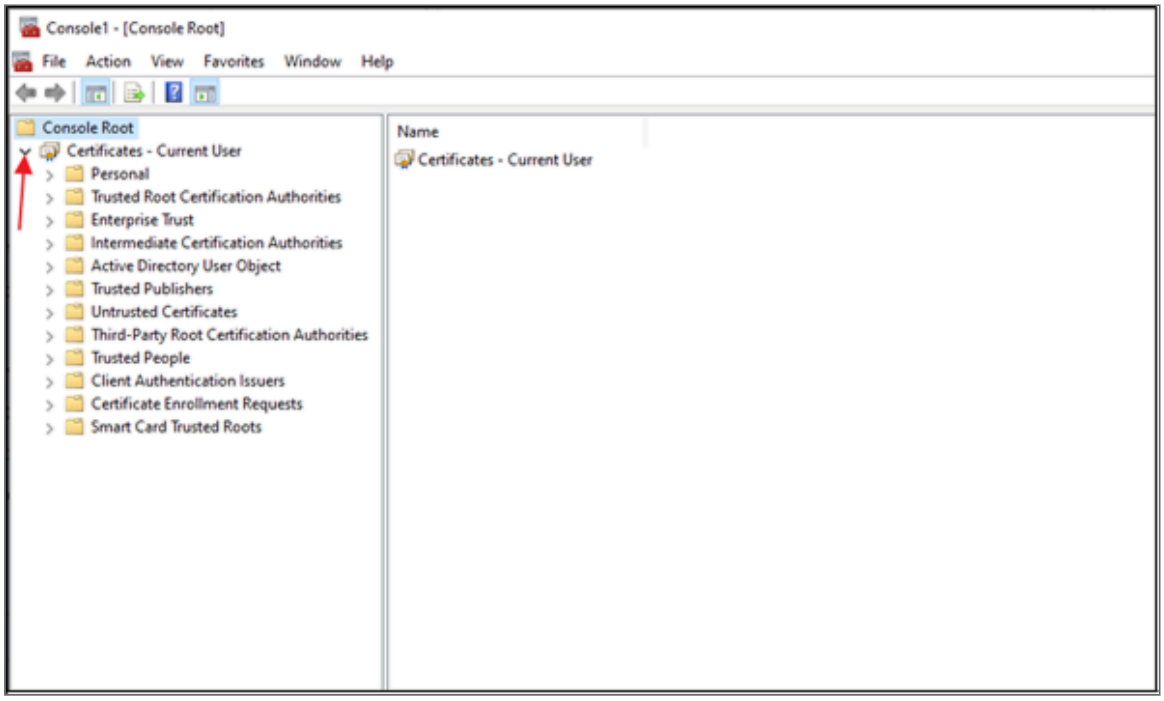
3. **Certificates** を選択して **追加** ボタンを**クリック**すると、下の画面が表示されます。そこで **My user account** のラジオ ボタンを選択し、**Finish** ボタンを**クリック**します。

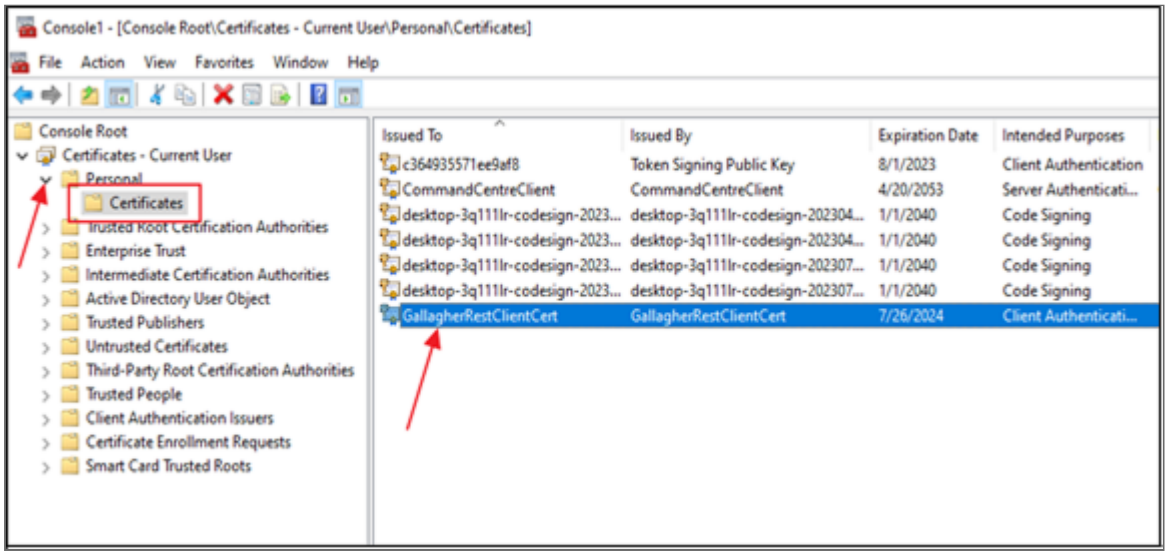


4. Finish をクリックすると下の画面が表示されるので、**OK** ボタンを**クリック**します。 証明書が正常に追加されます。

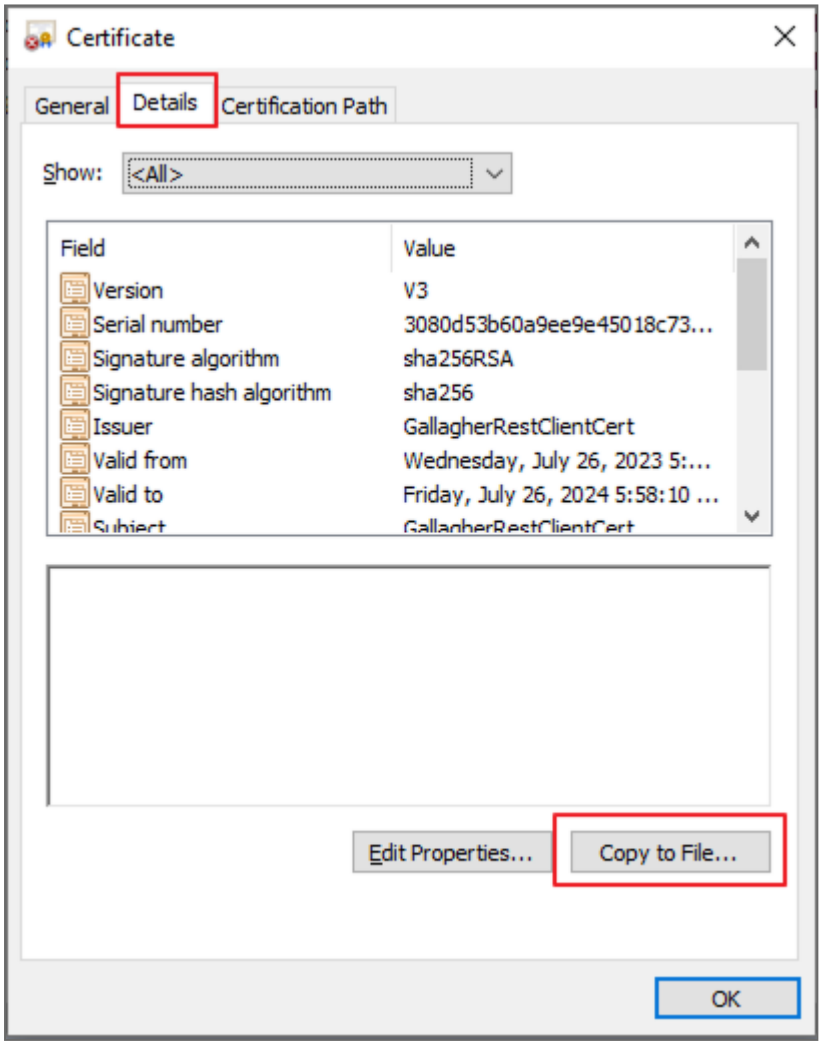


5. 次に **Certificates - Current User** → **Personal** → **Certificates** に移動し、**GallagherRestClientCert** 証明書を選択します。



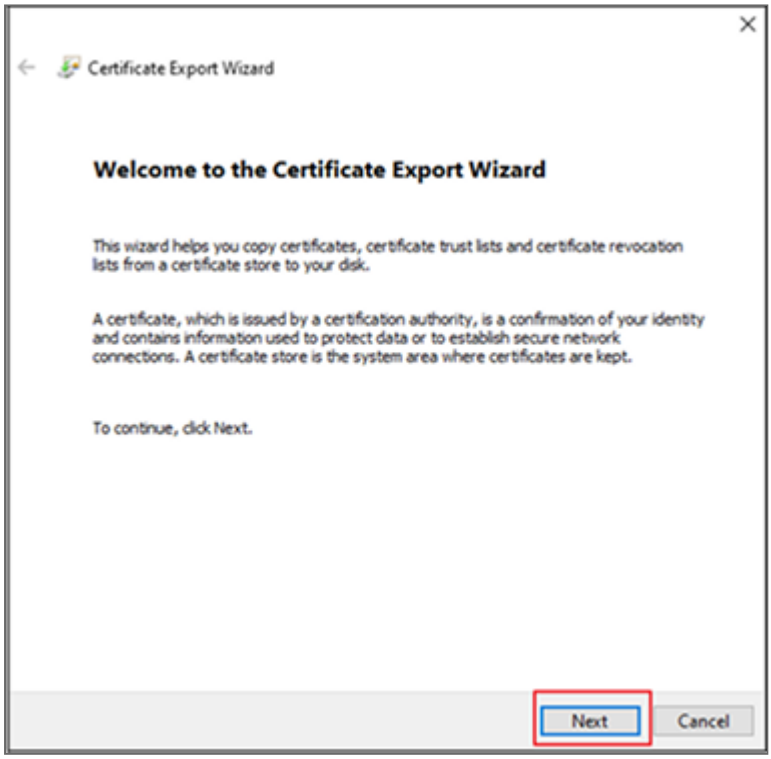


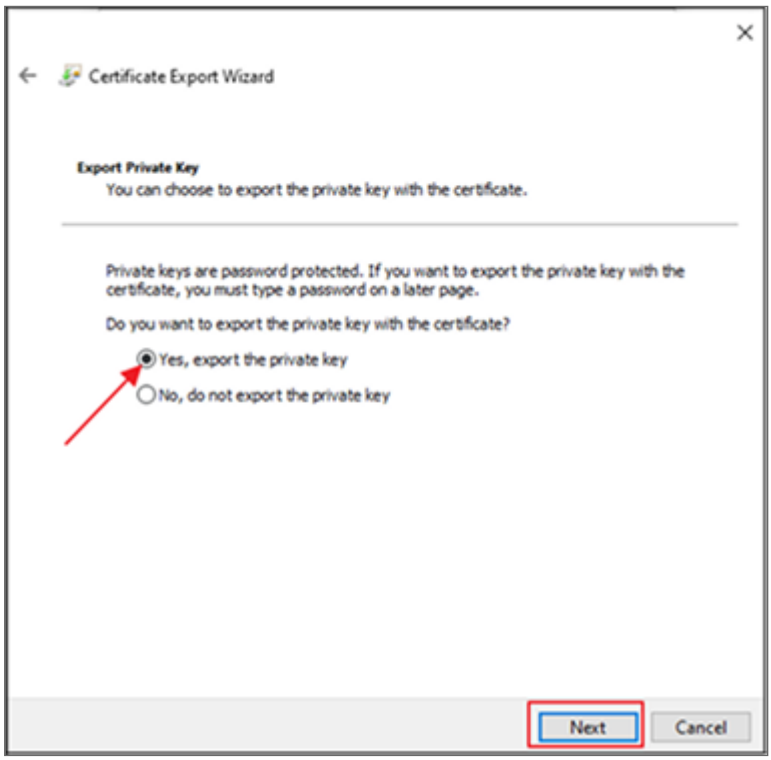
6. **Details** に移動し、**Copy to File** をクリックします。



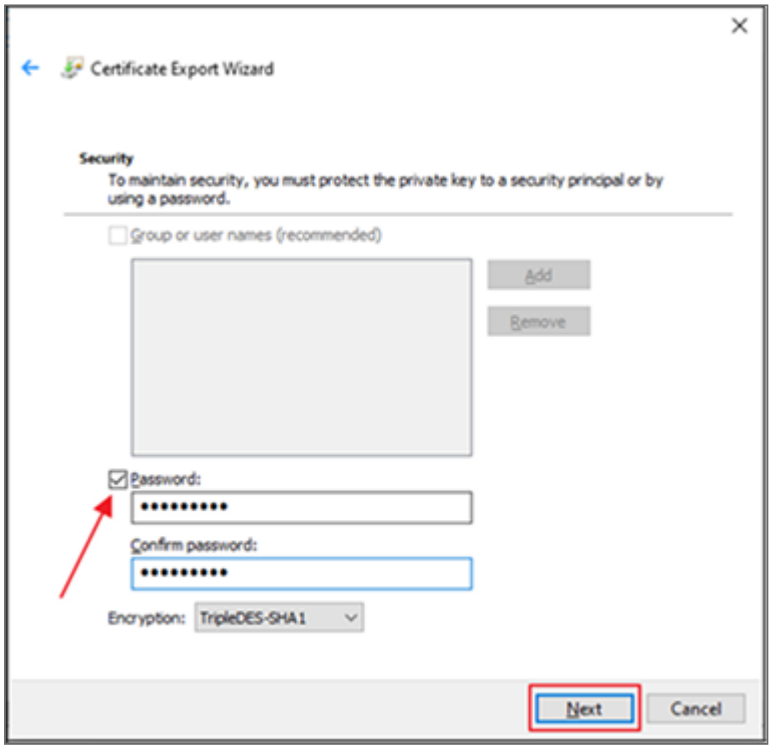
次に、以下のスクリーンショットに従って **Next** を順に**クリック**します。

> **情報**
> 証明書が複数ある場合は、Thumbprint が正しいことを確認してください。

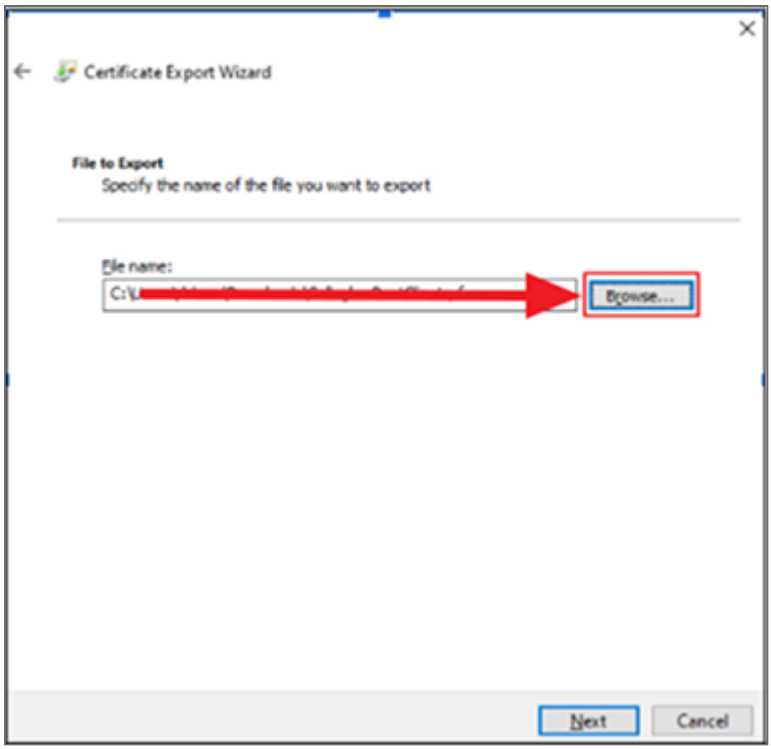


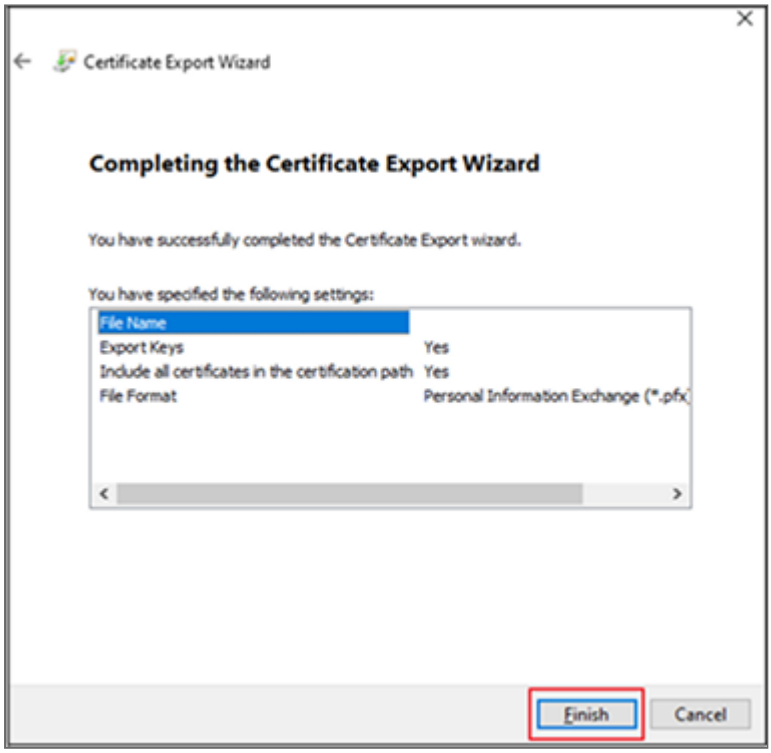


7. 次の画面が表示されたら、パスワードのチェックボックスをオンにし、パスワードを次のように設定します：**G@ll@gher**



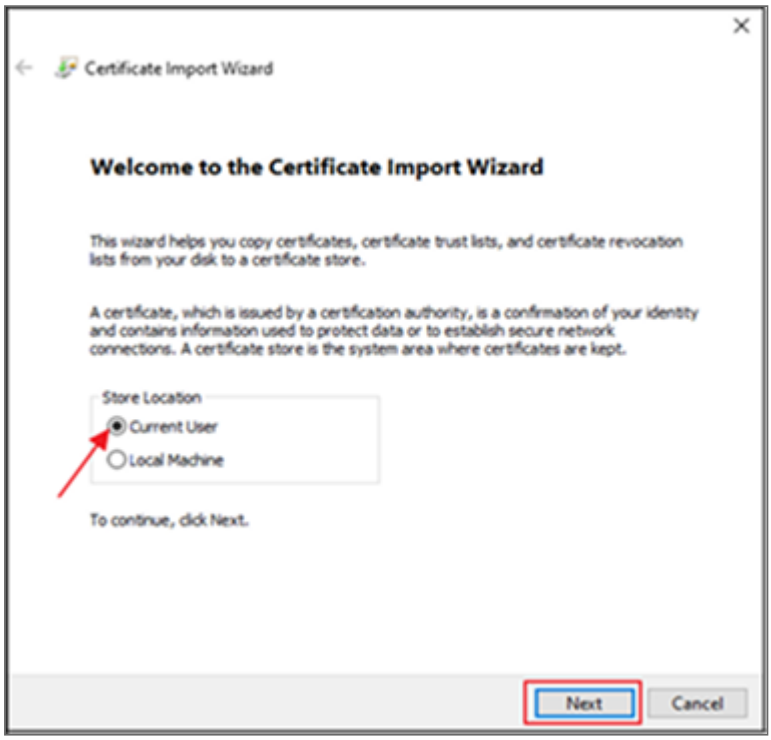
8. 次に、 C:\Program Files\Suprema Integration with Gallagher\Prerequisites のパスを参照してファイルをエクスポートし、このファイルを **GallagherRestClient.pfx** として保存してから、**Next** をクリックします。



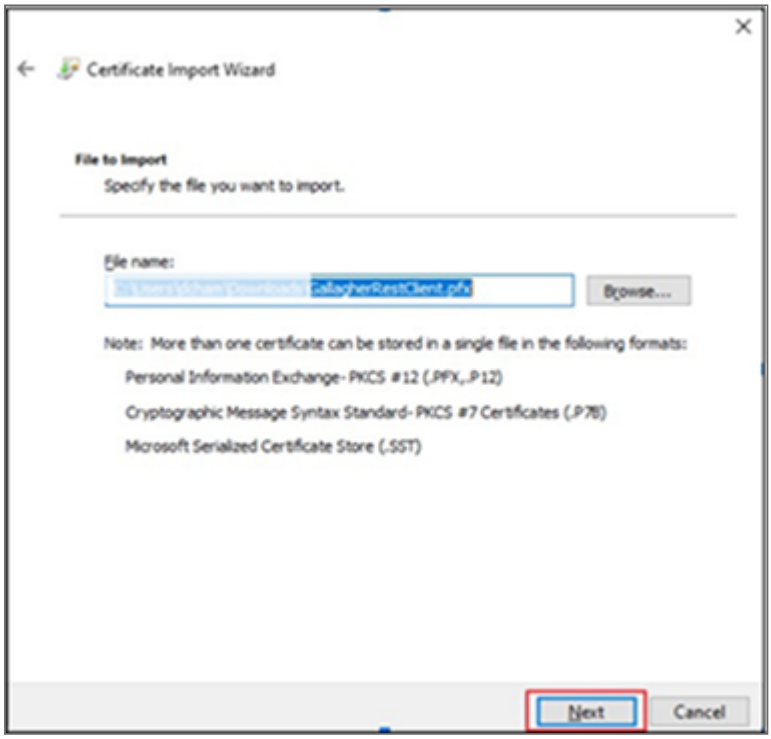


Finish をクリックすると証明書のエクスポートが正常に完了します。証明書と MMC ウィンドウを閉じます。

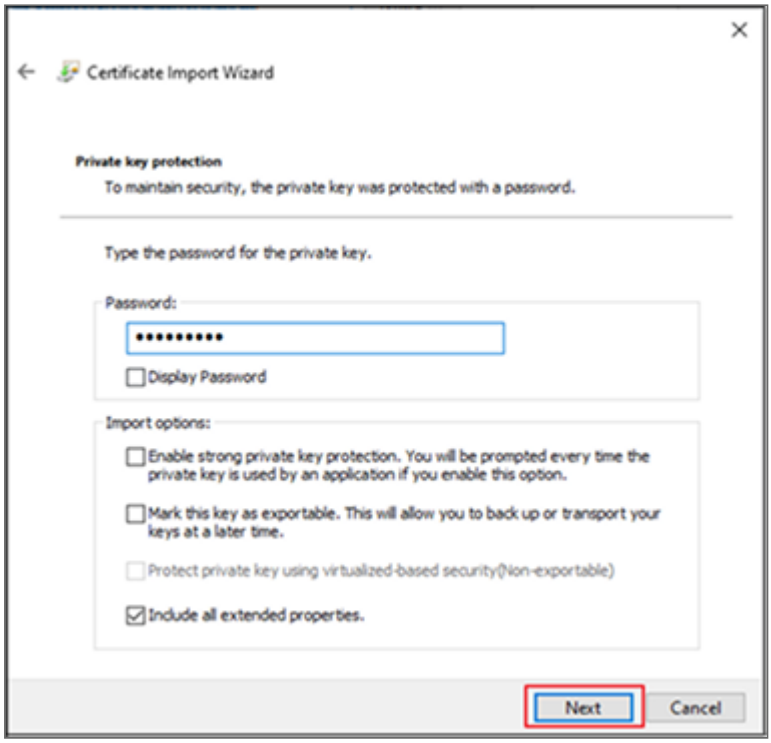
9. 次に、**GallagherRestClient.pfx** 証明書ファイルをエクスポートした C:\Program Files\Suprema Integration with Gallagher\Prerequisites に移動し、**GallagherRestClient.pfx** ファイルを**ダブルクリック**します。下の画像のように **Current User** のラジオ ボタンを選択し、**Next** をクリックします。



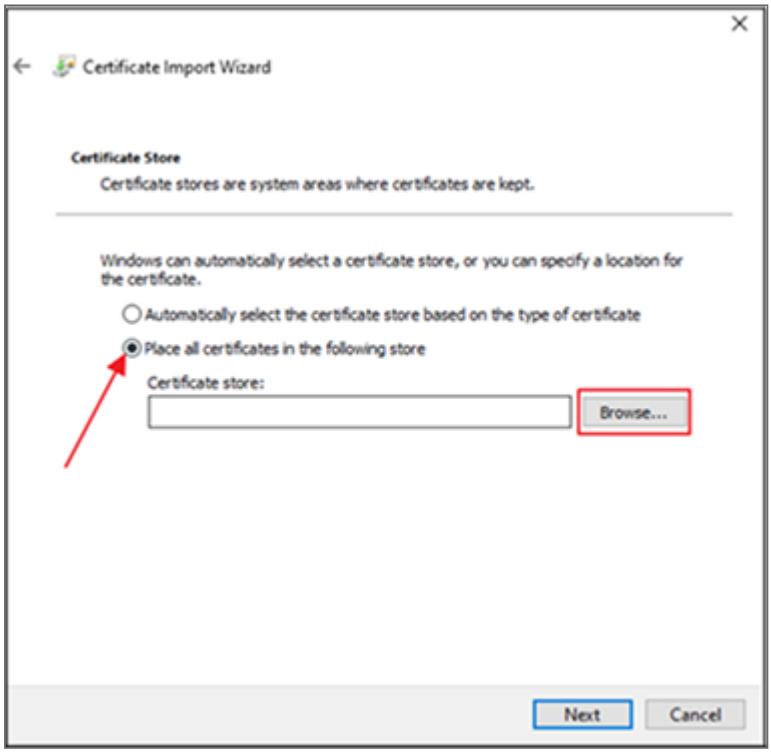
10. 次に、**GallagherRestClient.pfx** を保存した C:\Program Files\Suprema Integration with Gallagher\Prerequisites を参照し、**Next** をクリックします。

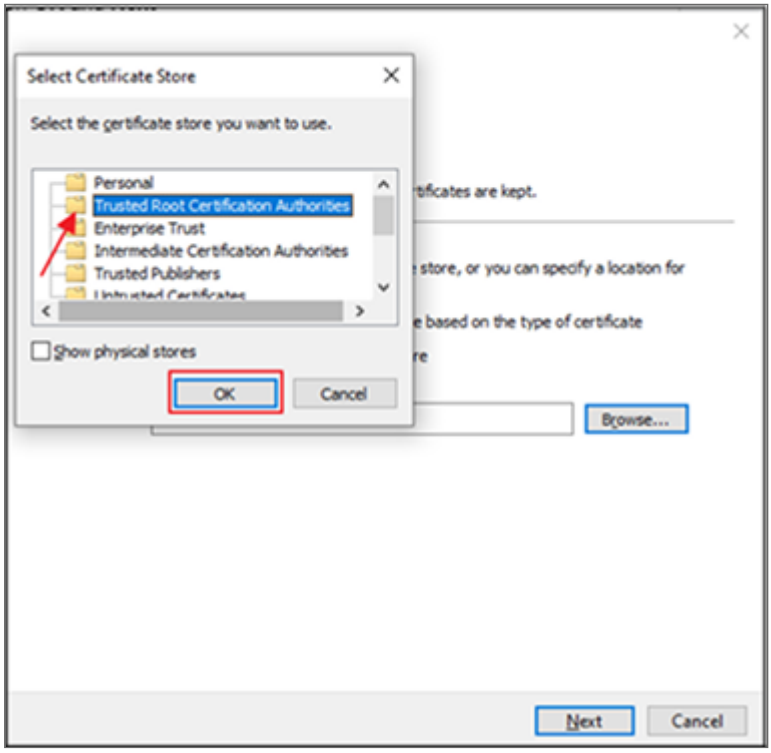


11. 次に、パスワード **G@ll@gher** を入力し、下の画像のようにチェックボックスをオンにしてから **Next** をクリックします。

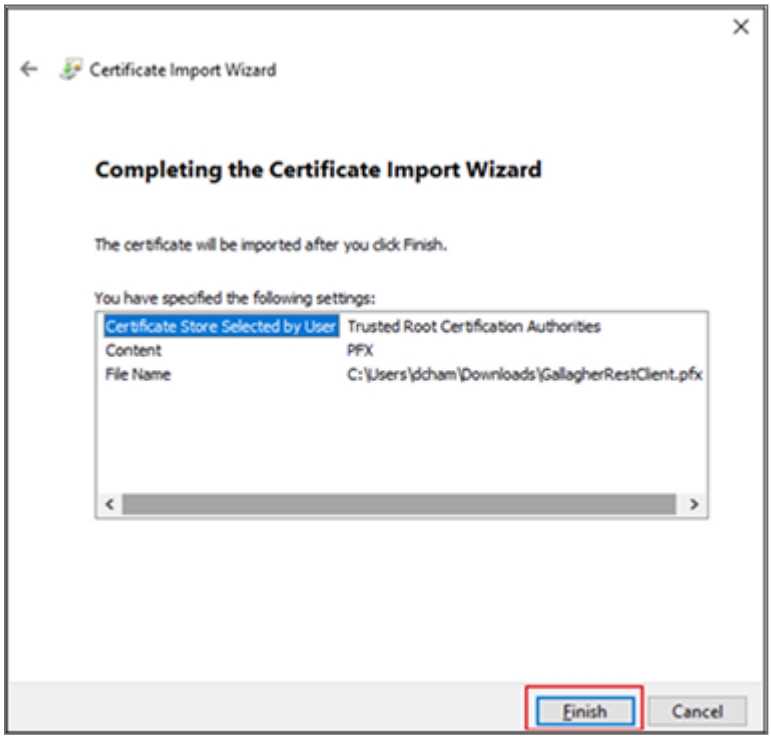


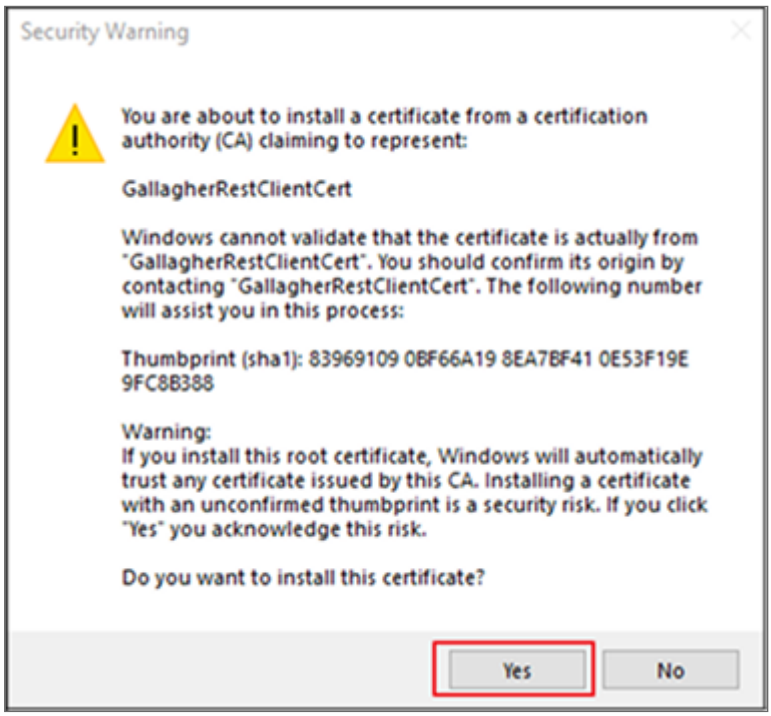
12. **Place all certificates in the following store** のラジオ ボタンを選択し、**Trusted Root Certification Authorities** フォルダーを参照してから **OK** と **Next** をクリックします。





13. **Finish をクリック**するとセキュリティ警告が表示されるので、**Yes をクリック**します。



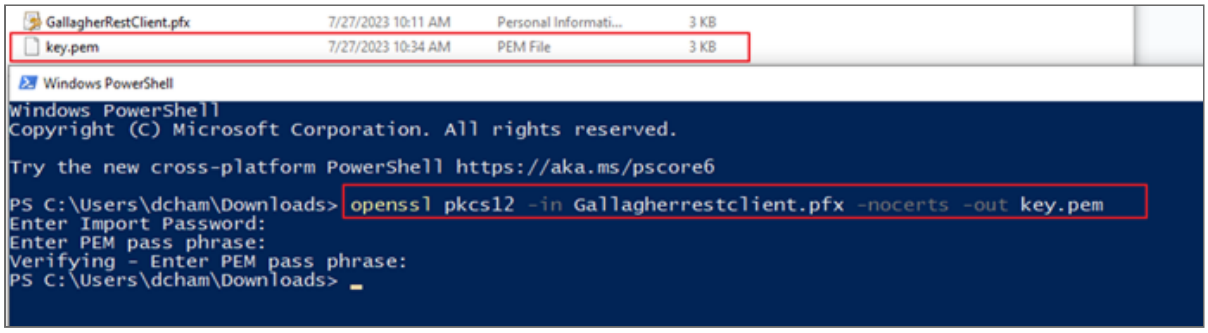


次に、GallagherRestClient.pfx ファイルを保存した C:\Program Files\Suprema Integration with Gallagher\Prerequisites に移動し、ここで Powershell を開きます。フォルダー URL に **PowerShell** と入力して PowerShell を開きます。

14. 以下のコマンドを入力して **key.pem** ファイルを生成します。

    openssl pkcs12 -in Gallagherrestclient.pfx -nocerts -out key.pem

15. 次に、パスワードを求められます。 そのため、以前設定したパスワード、つまり **G@ll@gher** を入力します。

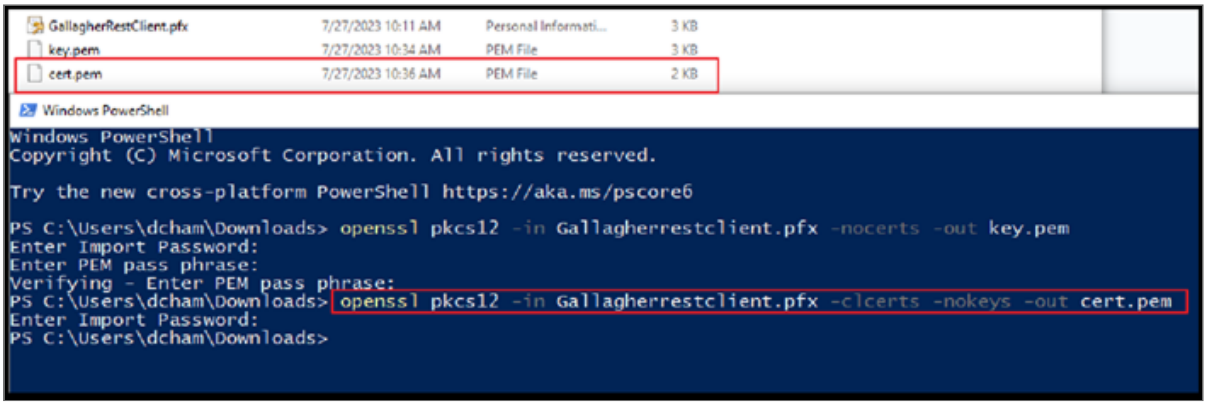


key.pem ファイルが正常に生成されます。

> **情報**
> ここではパスワードを3回入力する必要があります。

1. 次に、以下のコマンドを**入力**して **cert.pem** ファイルを生成します：

   > *command: openssl pkcs12 -in Gallagherrestclient.pfx -clcerts -nokeys -out cert.pem*

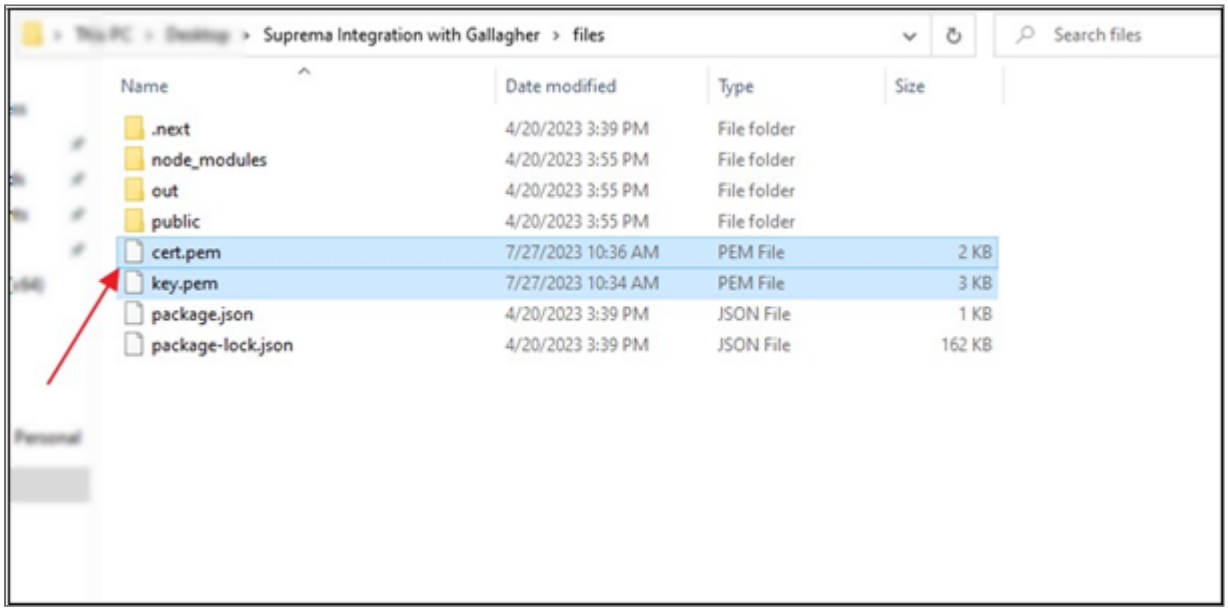
   

   次に、パスワードを求められます。 そのため、以前設定したパスワード **G@ll@gher** を**入力**します。

   cert.pem ファイルが正常に生成されます。

   > **情報**
   > ここではパスワードを1回入力する必要があります。

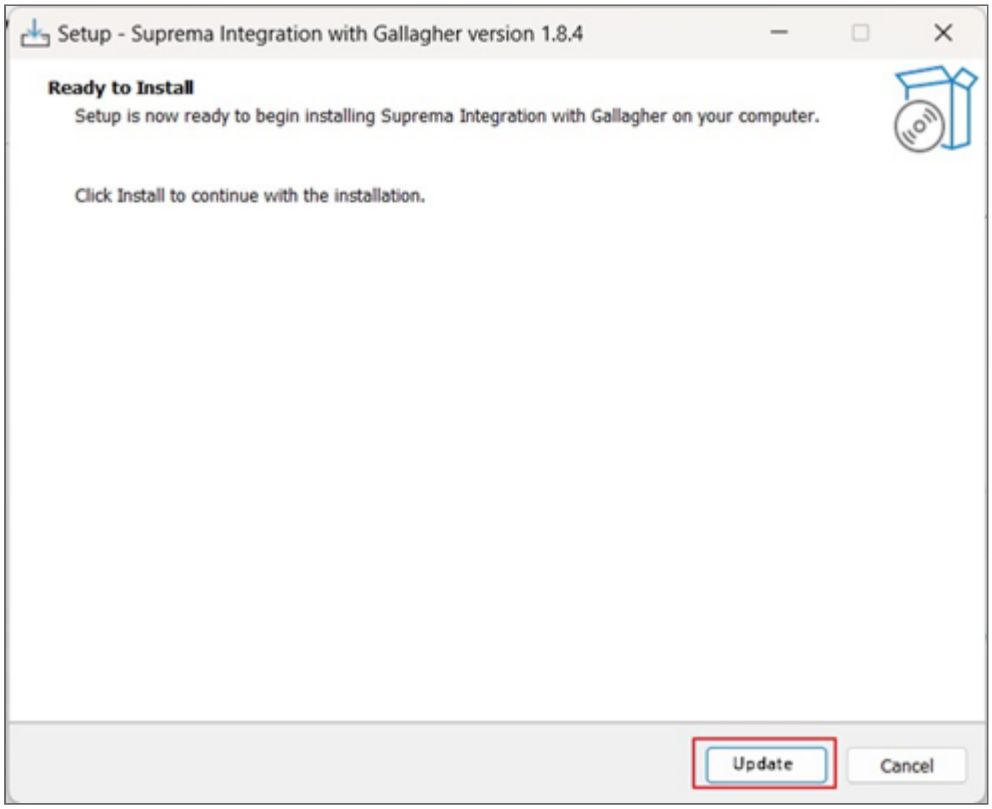
16. 次に、**key.pem** と **cert.pem** の両方を**コピー**し、次のパス `C:\Program Files\Suprema Integration with Gallagher\Suprema Integration with Gallagher v(lateast version)\files` に貼り付けます。



Q. EXE アプリケーションからミドルウェアを直接アップグレードする。

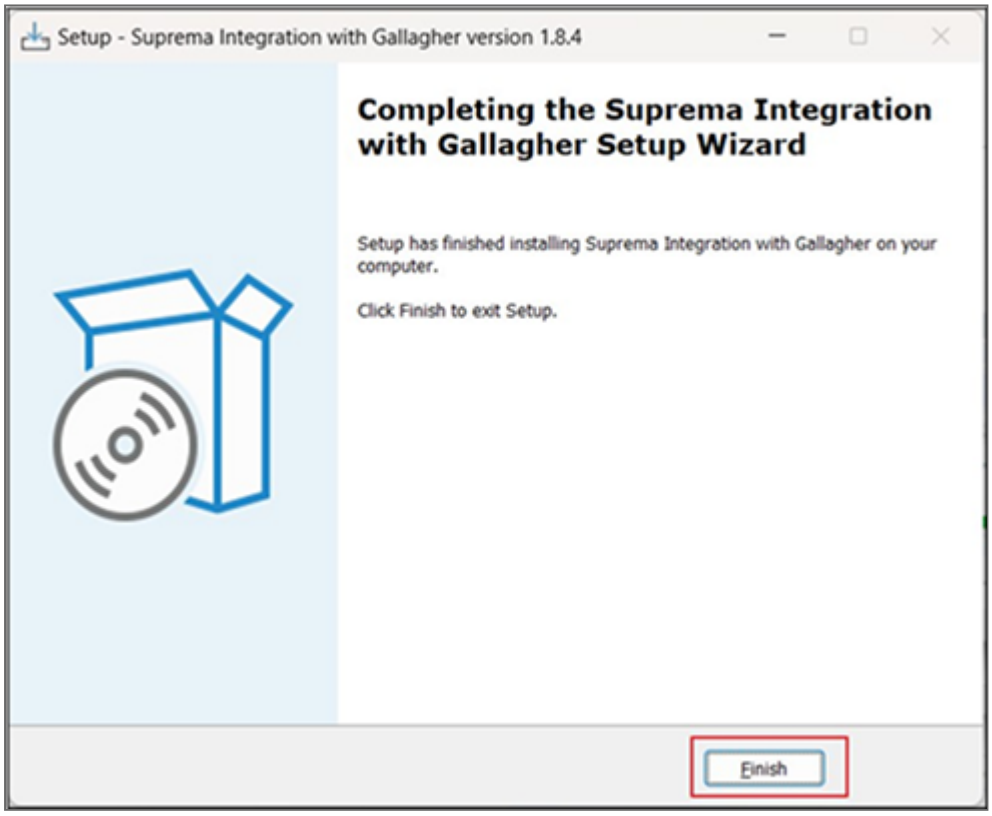
A.

1. バージョンをアップグレードする場合は、ポップアップで **OK** を押します。
2. その後、**Update** ボタンを押します。



3. ミドルウェアのアップグレードが始まります。
4. ミドルウェアのインストールが正常に完了したら、**Finish** ボタンを押します。

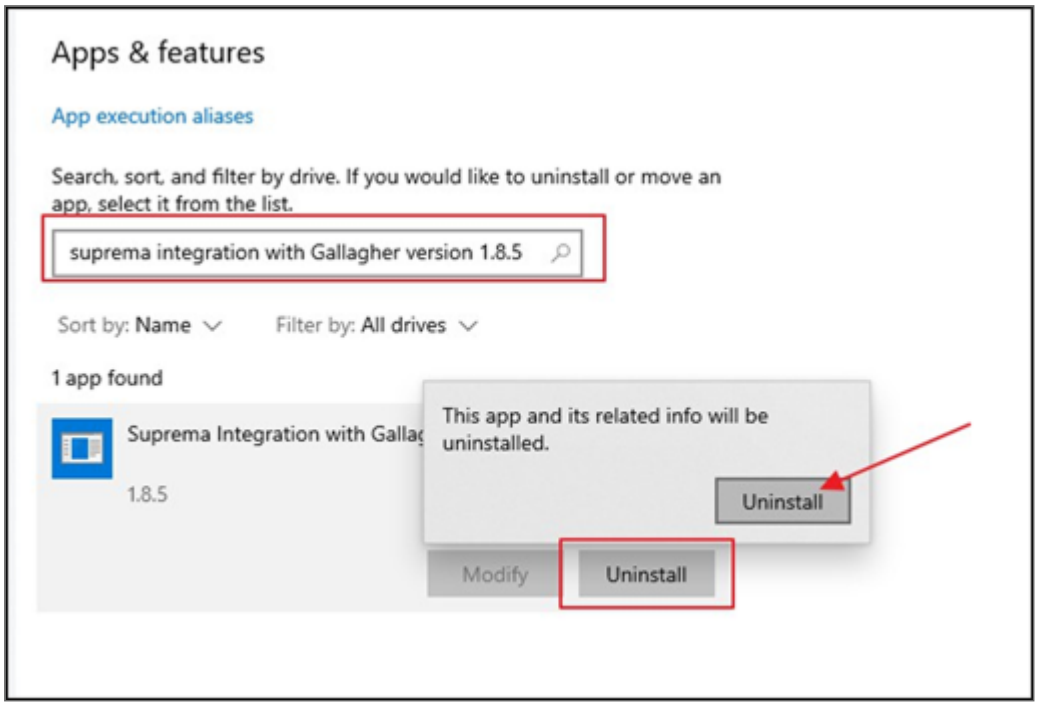
> **情報**
> 最新の変更を反映するには、システムの再起動が必要です。



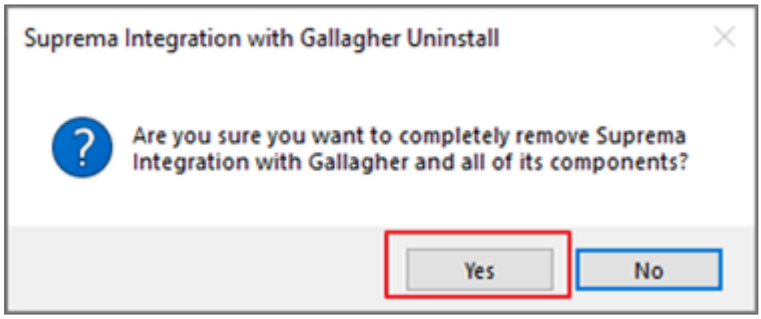
Q. EXE アプリケーションからミドルウェアを直接アンインストールする。

A.

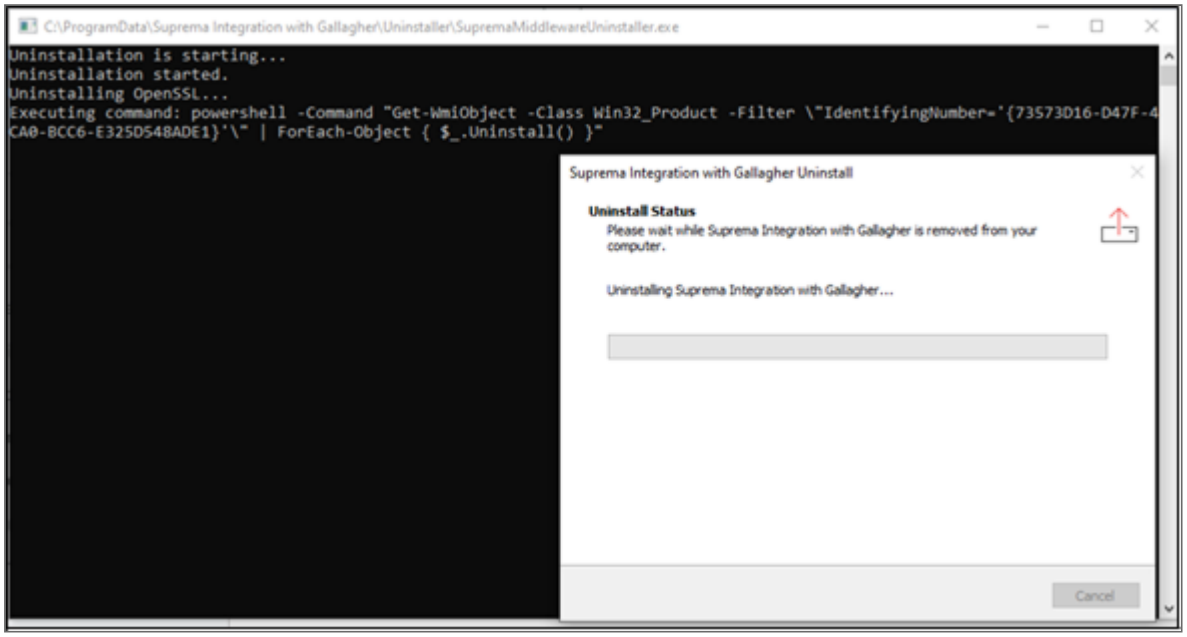
1. Windows の 開始 ボタンを**押し**、**検索**して、**アプリの追加と削除** を開きます。
2. アプリと機能の検索一覧で、Suprema integration with the Gallagher のバージョンを**検索**して選択し、**アンインストール** を**クリック**します。小さなポップアップが表示されたら、もう一度 **アンインストール** を**押し**ます。



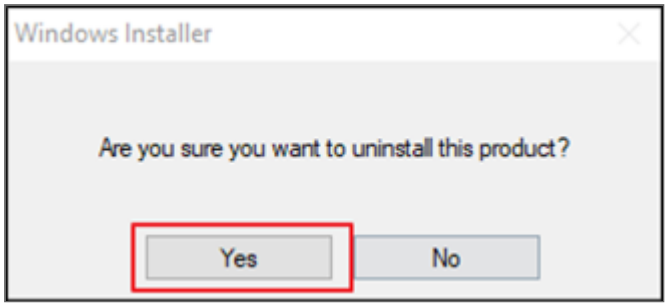
3. インテグレーションのすべてのコンポーネントを削除するポップアップで**はい**を**押し**ます。



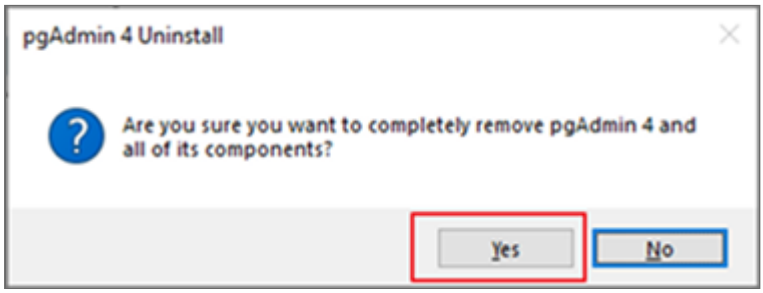
4. アンインストールが始まり、下の画面のような表示が見えます。



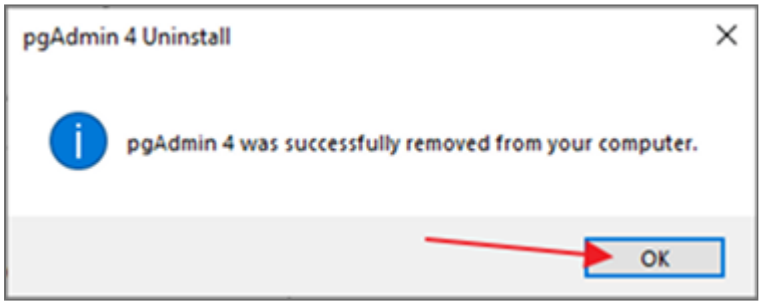
5. 下のポップアップで **はい** を押します。



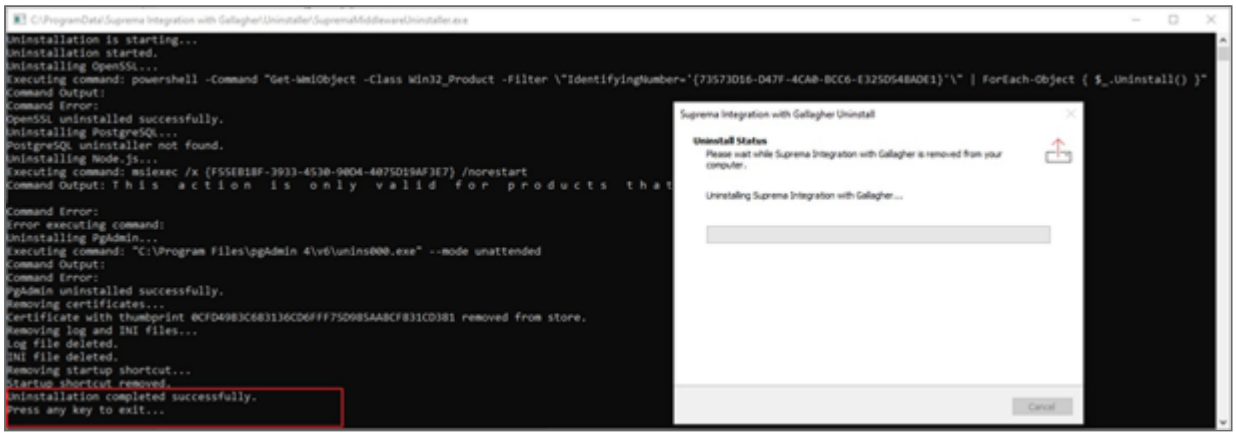
6. 下のポップアップでも **はい** を押します。



7. **OK** を押します。

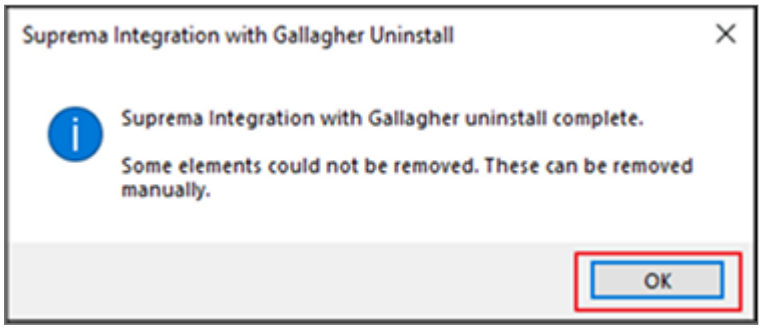


8. 次に端末内をクリックし、**Enter** を押してアンインストールを完了します。



9. 下のポップアップで **OK** を押します。これでミドルウェアの削除は完了です。

> **情報**
> 変更を反映するには、システムを再起動する必要があります。

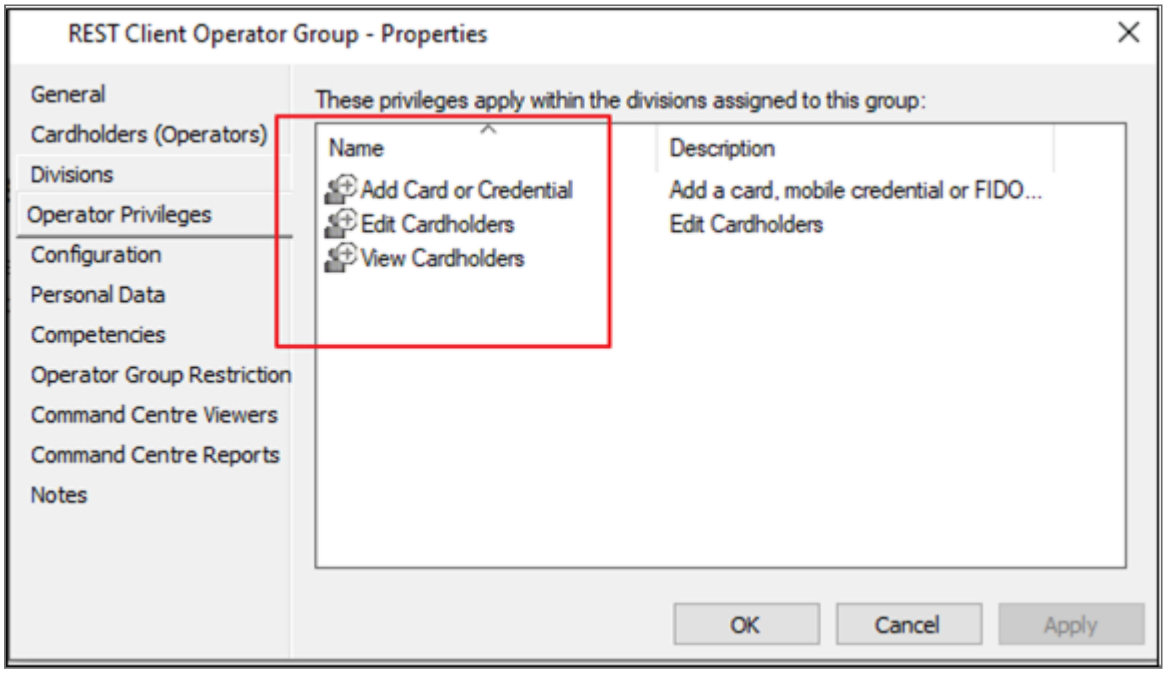


ミドルウェア

Q. ミドルウェアでのスキャンまたはデータ同期が非常に遅い場合。

A.

- この問題を解決するには、ここをクリックしてブログを参照してください。
  - カード所有者カードが自動作成されない場合、ミドルウェアでカードは表示されません。
- オペレーター グループに3つの権限を追加する必要があります。



これら3つの権限を追加したあと、システムを再起動してください。

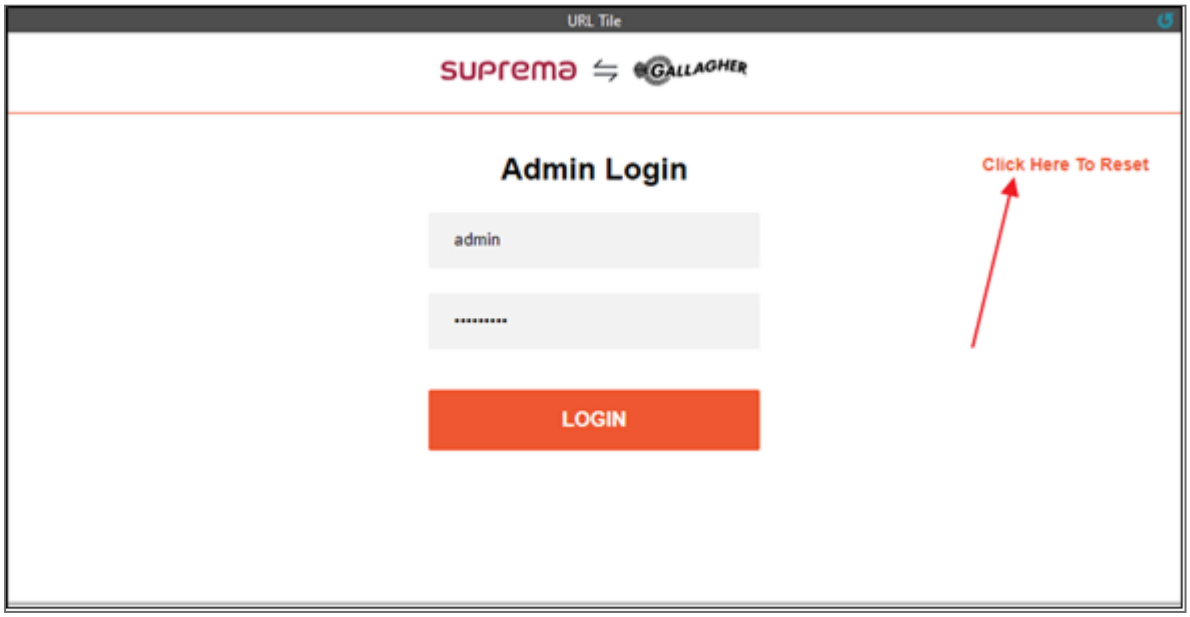
Q. ログイン ページに「LAN is disconnected or IP is changed for (IP Address)」というエラーが表示される場合。

A.

- この問題を解決するには、次のトラブルシューティング項目を確認してください：

  1. LAN ケーブルが接続されていることを確認します。
  2. IP が変更されていないこと、また BioStar 2 Server の IP アドレスが同じであることを確認してください。誤った IP アドレスを入力している可能性があります。

- ログイン画面で **LAN is disconnected or IP is changed for (IP Address)** のエラーを受信した場合は、ミドルウェアの **click here to Reset ボタン**を**押す**必要があります。



ミドルウェアのリセット許可を求められたら、**Yes ボタン**を**押します**。

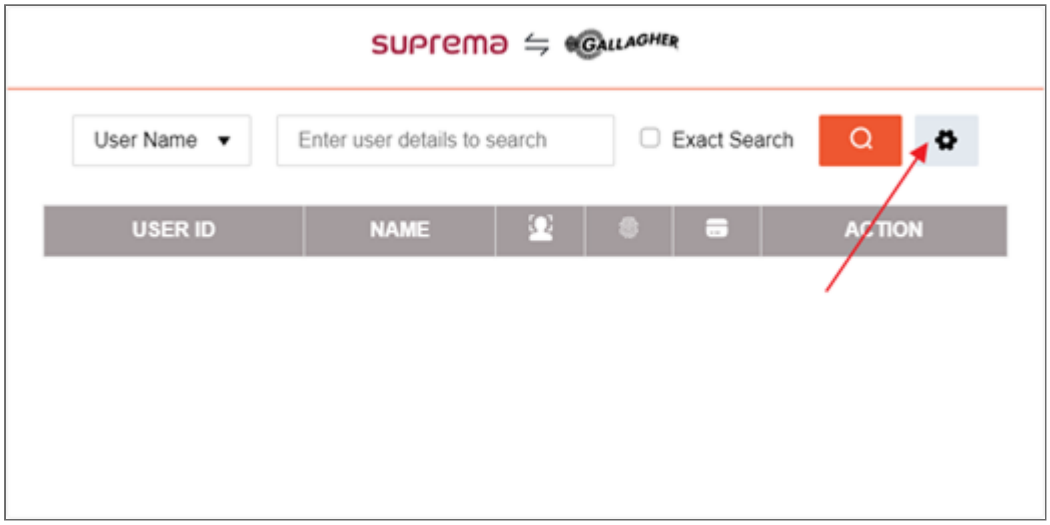


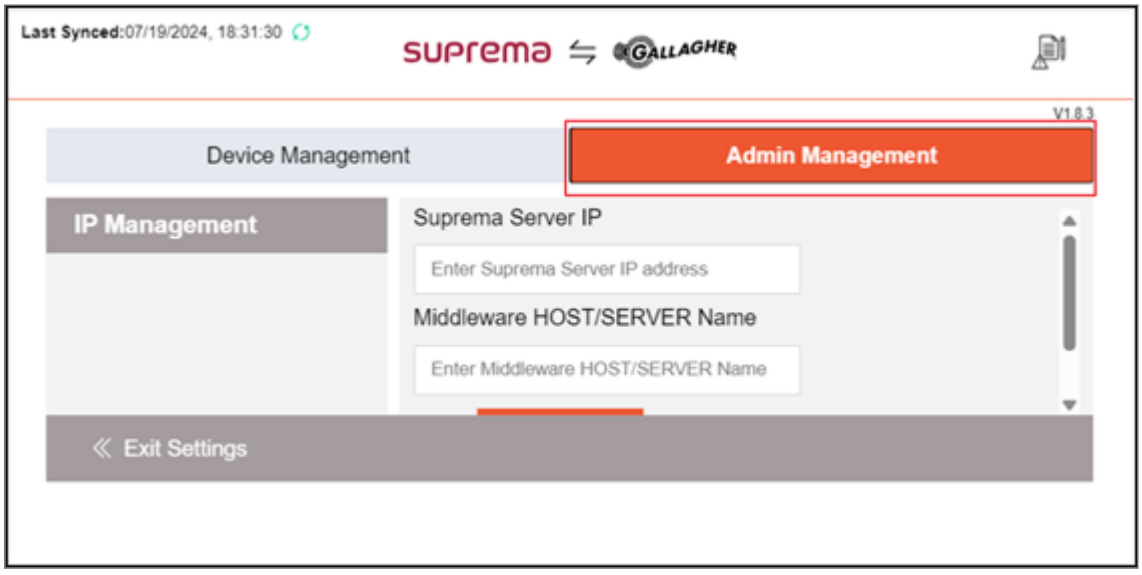
リセットすると、ミドルウェアの初期画面が表示されるので、続きの手順に従います。

Q. 任意のページでミドルウェア実行中に「LAN is disconnected or IP is changed for (IP Address)」というエラーが発生する場合。

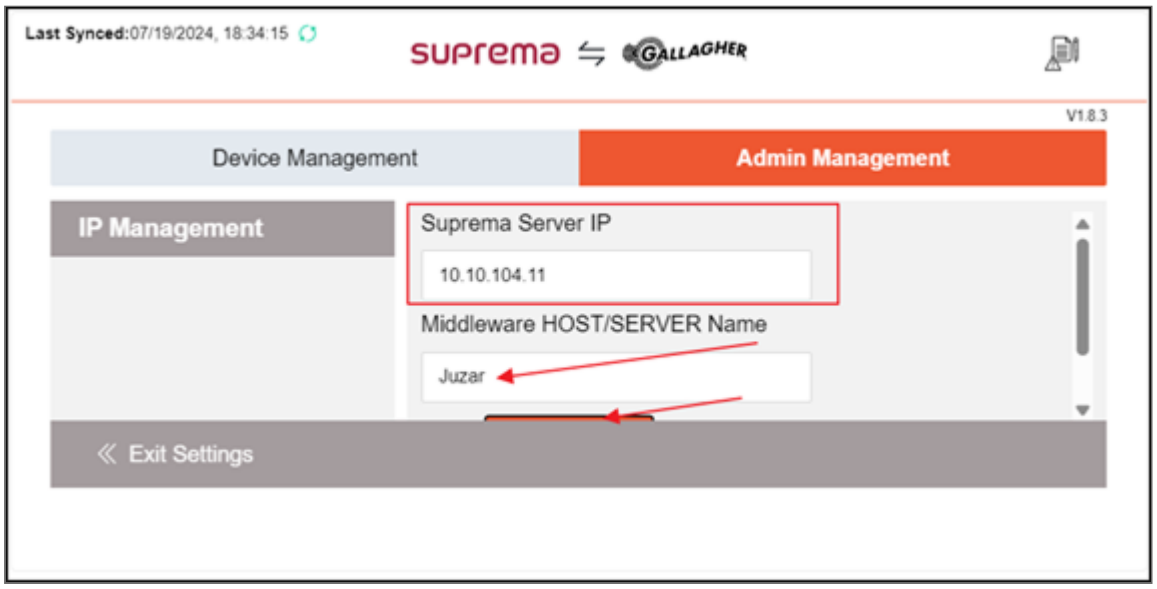
A.

- この問題を解決するには、次のトラブルシューティング項目を確認してください：
  1. LAN ケーブルが接続されていることを確認します。
  2. IP が変更されていないこと、また BioStar 2 Server の IP アドレスが変更されていることを確認してください。
- その場合は、ミドルウェア内の **Settings** → **Admin Management** → **IP management** セクションに移動します。





次に、テキスト ボックスに BioStar 2 server の IP アドレスとミドルウェアの HOST/SERVER 名を入力し、**Submit** ボタンを押してミドルウェア用の BioStar 2 サービスを開始します。



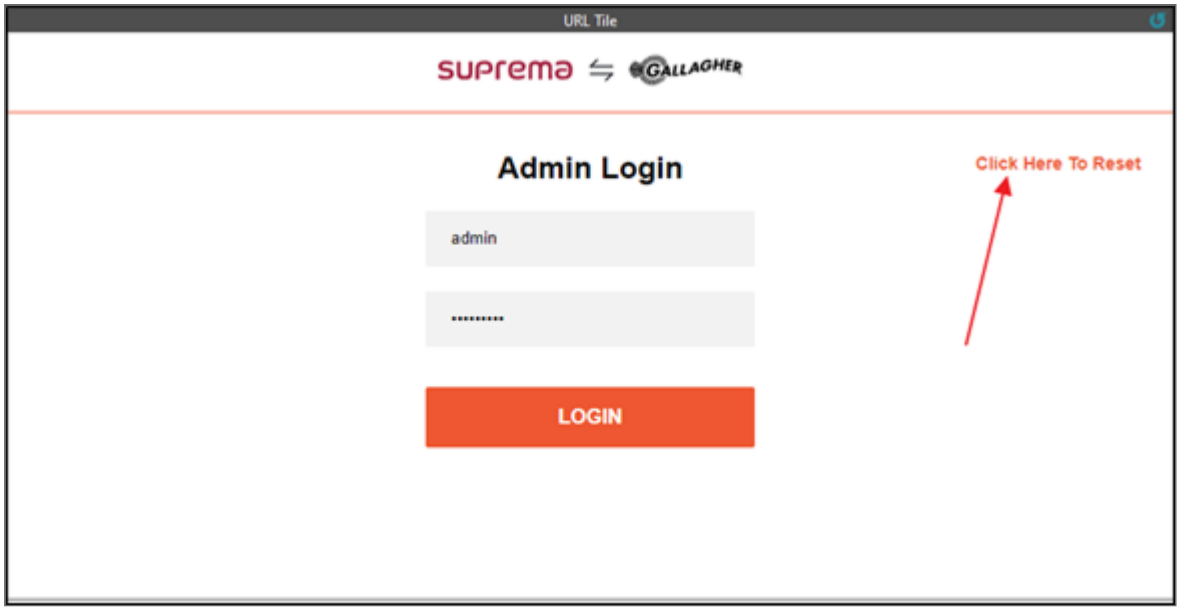
Submit button を押すと IP 変更の成功メッセージが表示されるので、**Exit setting button** を押して設定画面を終了します。

Q. 古いバージョンで複数サーバー上のミドルウェアを使用する方法。

A. バージョン 1.7.0 から、BioStar 2 server の IP アドレスを取得するための独立した画面を追加しました。 そのため、これは 1.7.0 未満のミドルウェア バージョンで使用するための解決策です。

IP アドレスを変更する手順は次のとおりです。

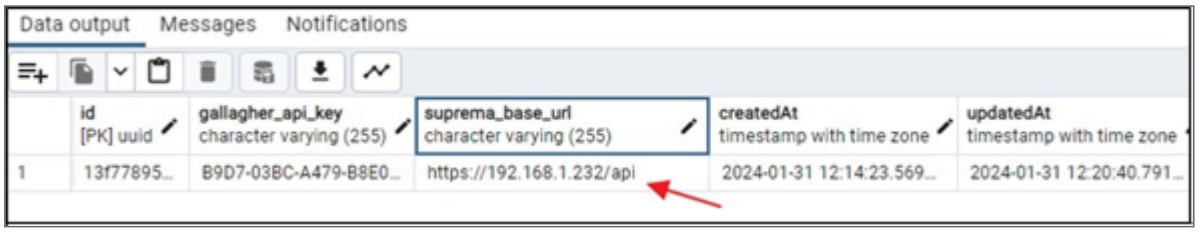
1. PgAdmin → テーブル に移動し、テーブルを右クリックして **Truncate** → **Truncate Restart Identity**（3つのテーブルすべて）を実行します。
2. API key ウィンドウが表示されず、ログイン画面しか表示されない場合は、Gallagher command center に入って **reset middleware** リンクをクリックし、ミドルウェアをリセットします。



3. ミドルウェアの API key を入力したあとにログインし、Pgadmin を開き、資格情報テーブルを右クリックして、**View/**

Edit Data → All Rows を開きます。

4. テーブルのデータが読み込まれます。 次に、BioStar server の IP に合わせて IP アドレスを変更し、**F6** ボタンを押して変更を保存します。



5. そのあと、Pgadmin 内の globaluserrecord テーブルを truncate します。
6. 変更を反映するためにシステムを再起動します。

Q. 特定の IP アドレスを持つ 2 台の異なるサーバーで特定のポート上でミドルウェアを実行する / ミドルウェアの受信ルールを構成する。

A. 以下は、特定の IP アドレスを持つ 2 台の異なるサーバーで特定のポート上でミドルウェアを実行する手順です。

ミドルウェアが 28523 ポートを使ってアプリケーションのバックエンド（middleware-backend）を呼び出していることが分かりました。バックエンドでは BioStar 2 server API を呼び出しているため、使用するポートは Web サーバーの HTTPS 既定ポートである 443 のみです。

そのため、BioStar 2 server である server2 では、プロトコル タイプを TCP に設定し、ローカル ポートに 443、8081 を指定します。 リモート ポート オプションは **All ports** のままにします。

Server 1 には Gallagher と Middleware が含まれます。

- IP Address: 192.168.1.68
- Subnet mask: 255.255.255.0
- Default Gateway: 162.168.1.1

Server 2 には BioStar 2 が含まれます。

- IP Address: 10.10.104.13
- Subnet mask: 255.255.254.0
- Default Gateway: 10.10.104.1

受信ルールを作成する手順は次のとおりです：

> **情報**
> 以下の手順は BioStar 2 server で実行する必要があります。

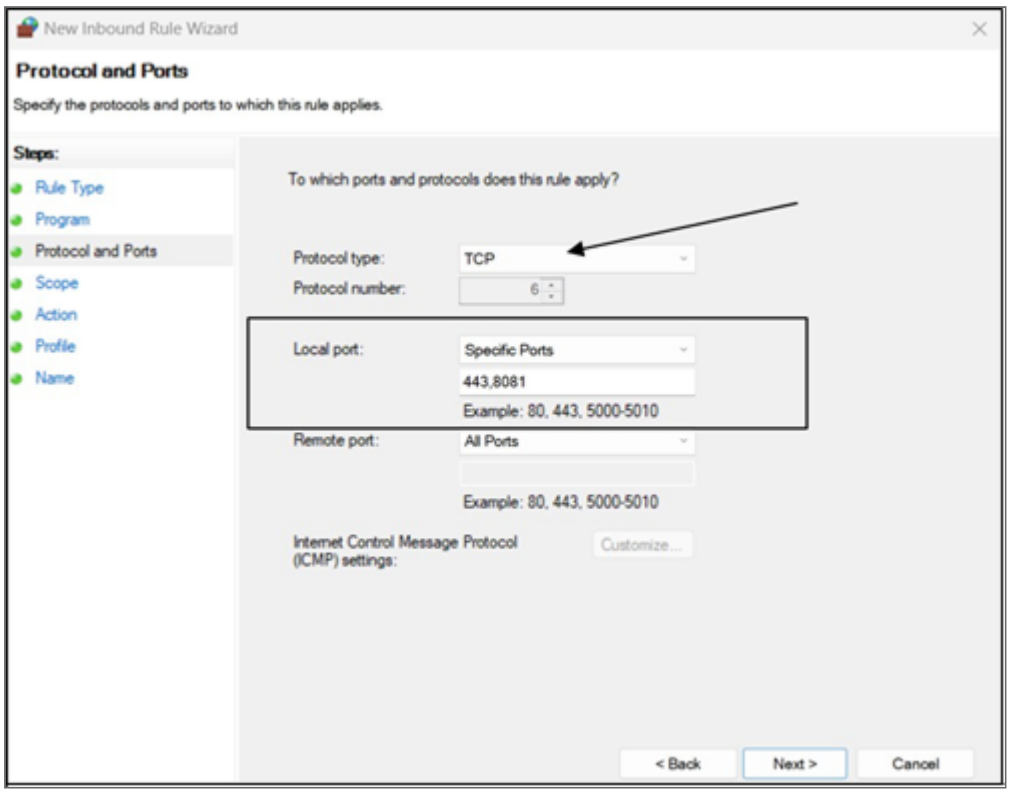
1. Windows Defender Firewall の設定を開く：
   - `Win + R` を押して、[ファイル名を指定して実行] ダイアログを開きます。
   - `control firewall.cpl` と入力し、Enter を押します。 Windows Defender Firewall の設定が開きます。
2. 詳細設定にアクセスする：
   - Windows Defender Firewall ウィンドウでは、左側にオプションが表示されます。 **詳細設定** をクリックします。 Windows Defender Firewall with Advanced Security コンソールが開きます。
3. 新しい受信ルールを作成する：

- Windows Defender Firewall with Advanced Security コンソールでは、左側に **Inbound Rules** と **Outbound Rules** を含むオプションが表示されます。
- **Inbound Rules** をクリックします。
- 右側のペインで **New Rule...** をクリックします。 New Inbound Rule Wizard が開きます。

4. ルールの種類を選択する：
   - New Inbound Rule Wizard で **Custom** を選択し、**Next** をクリックします。
5. プログラムを構成する：
   - このルールを特定のプログラムに適用する場合は、ここで指定します。 ICMP トラフィックを扱うため、ここは **All programs** のままにして **Next** をクリックします。
6. プロトコルとポートを構成する：

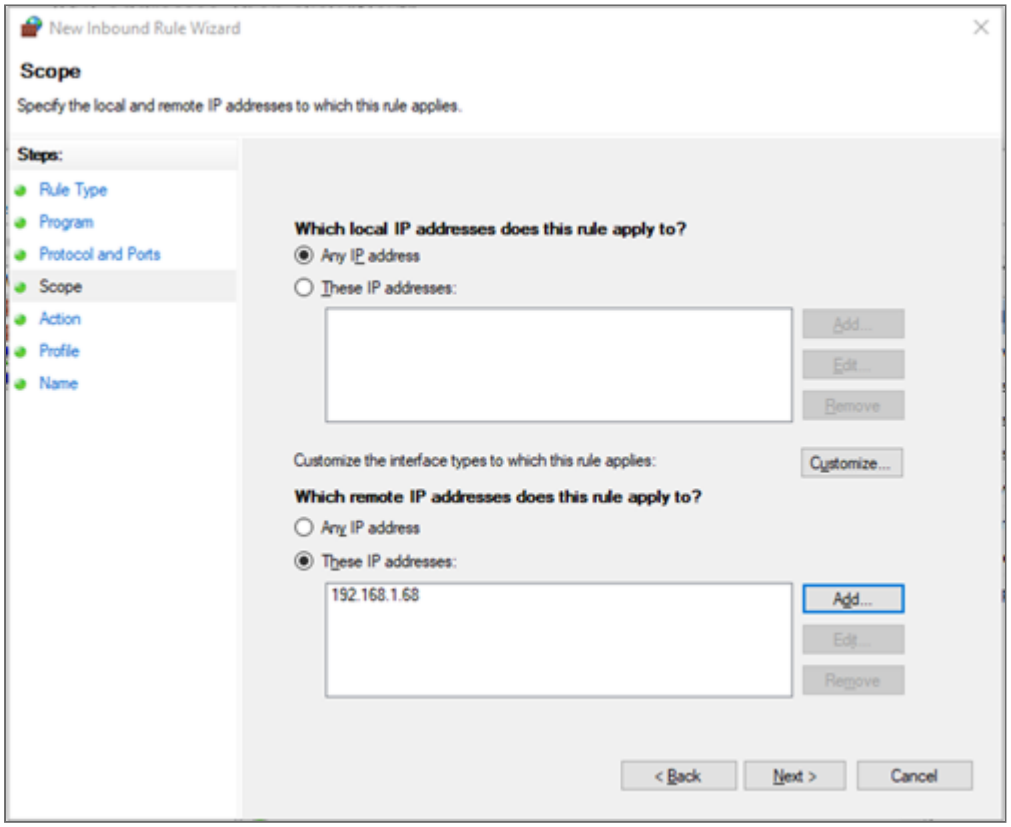
   - プロトコルとポートのウィンドウで、特定のポートを使用するため **TCP** を選択します。 次にローカル ポートで **Specific Ports** を選択し、443 と 8081 を入力します。 リモート ポートは **All Ports** のままにします。 その後、**Next** をクリックします。

> **情報**
> ここでは、8081 ポートを BioStar 2 の USB デバイス用として割り当てています。



7. スコープを構成する：

   - Scope ウィンドウでは、どの IP アドレスがサーバーに ICMP トラフィックを送信できるかを指定できます。 そのため、ローカル IP アドレスはそのままにし、リモート IP アドレスには Gallagher と Middleware のサーバーの IP アドレスを入力します。次に **These IP addresses：** を選び、**Add** ボタンをクリックします。IP address wizard で Gallagher と Middleware のサーバーの IP Address を入力し、**OK** を押します。 参照用に下の画像を確認してください。



8. アクションを構成する：
   - Action ウィンドウで **Allow the connection** を選択し、**Next** をクリックします。
9. プロファイルを構成する：
   - Profile ウィンドウで、このルールを適用するプロファイルを選択します。 通常は、すべてのプロファイル（Domain、Private、Public）で有効にします。 その後、**Next** をクリックします。
10. 名前と説明：
    - ルールに名前と説明を付けます。 たとえば、**Allow ICMP Echo Request for middleware** という名前にします。 その後、**Finish** をクリックします。
11. ルールを有効にする：
    - ルールを作成すると、Windows Defender Firewall with Advanced Security コンソールの Inbound Rules セクションに表示されます。
    - 作成したルールを右クリックし、自動で有効にならない場合は **Enable Rule** を選択します。 これでルールが有効になり、ICMP トラフィックを許可します。

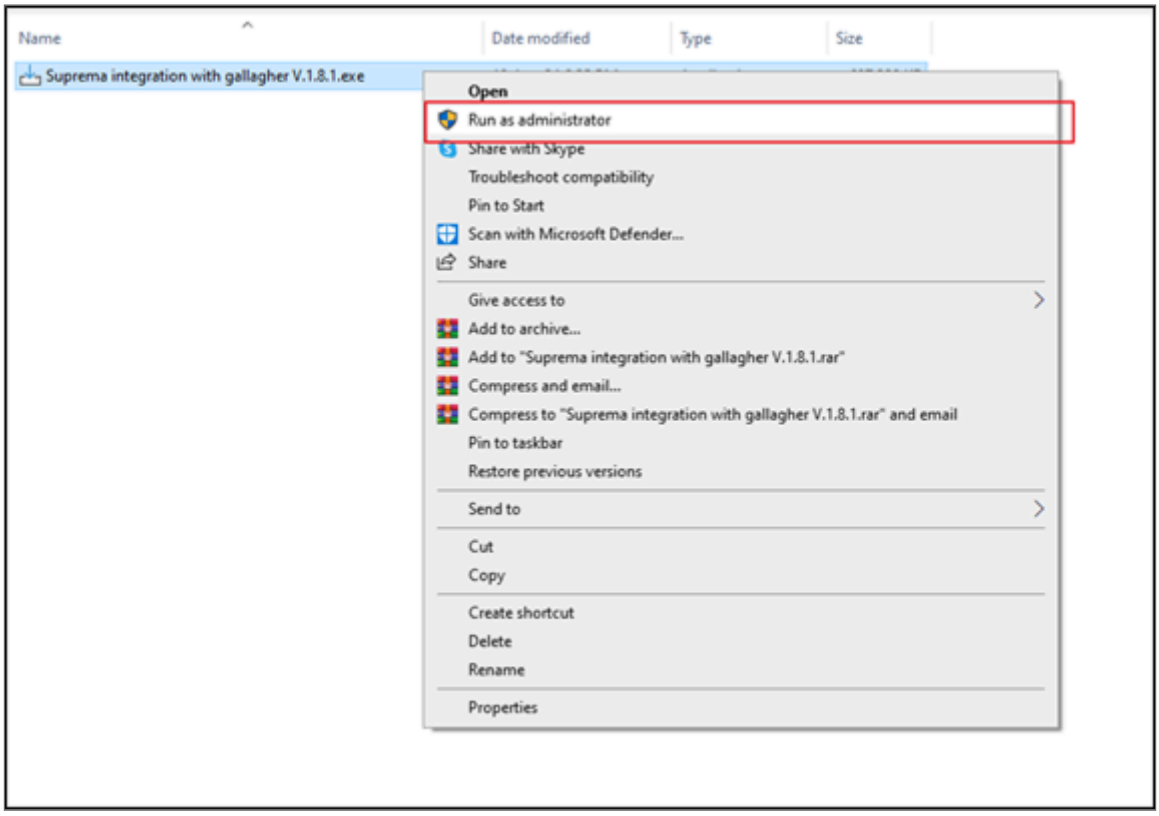
Q. BioStar サーバーの IP が変更され、ミドルウェアの動作が遅くなった場合。

A. IP が変更されたというエラーが発生した場合は、次のリンクを確認してください：https://support.supremainc.com/en/support/solutions/articles/24000041659--biostar-2-troubleshooting-when-the-server-ip-changed.

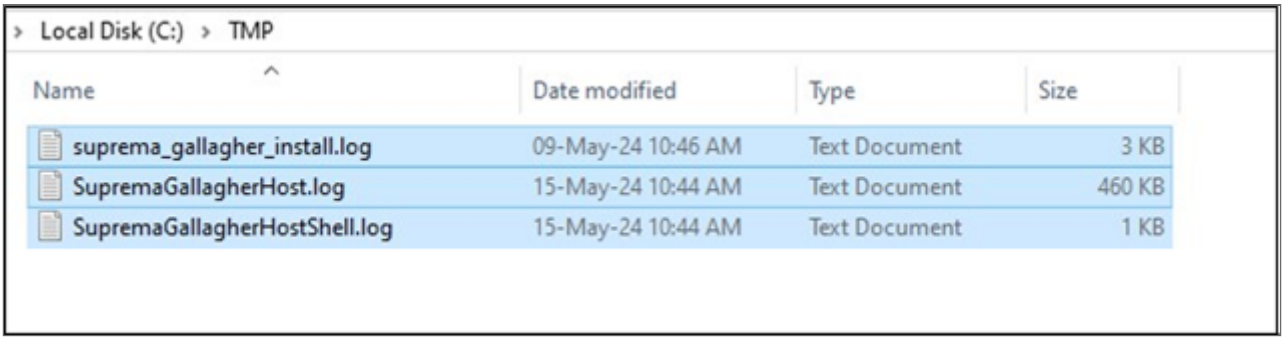
Q. EXE ファイル実行時に thumbprint が生成されない場合。

A. ミドルウェアをインストールしても thumbprint が生成されない場合は、管理者権限で EXE ファイルを再度実行してください。手順は次のとおりです。

下のスクリーンショットのように、Suprema integration with the gallagher.exe ファイルを右クリックし、**管理者として実行**を選択します。 続いて許可を求められるので、**はい** をクリックして exe ファイルを実行します。



それでも thumbprint ファイルが生成されない場合は、C:\TMP に移動し、すべてのログ ファイルを開発チームと共有してください。



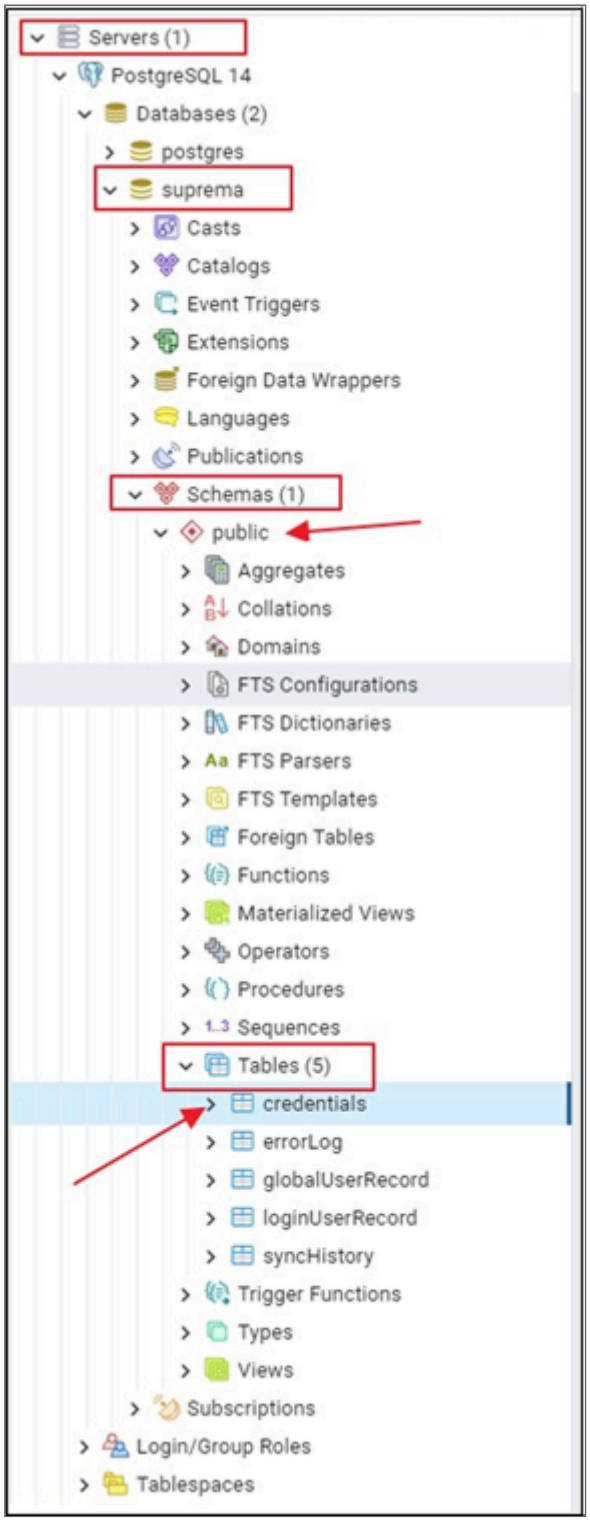
それまでの間、thumbprint を手動で生成する方法の記事を参照してください。 参照：thumbprint を手動で生成する方法。

Q. Migration を手動で作成する。

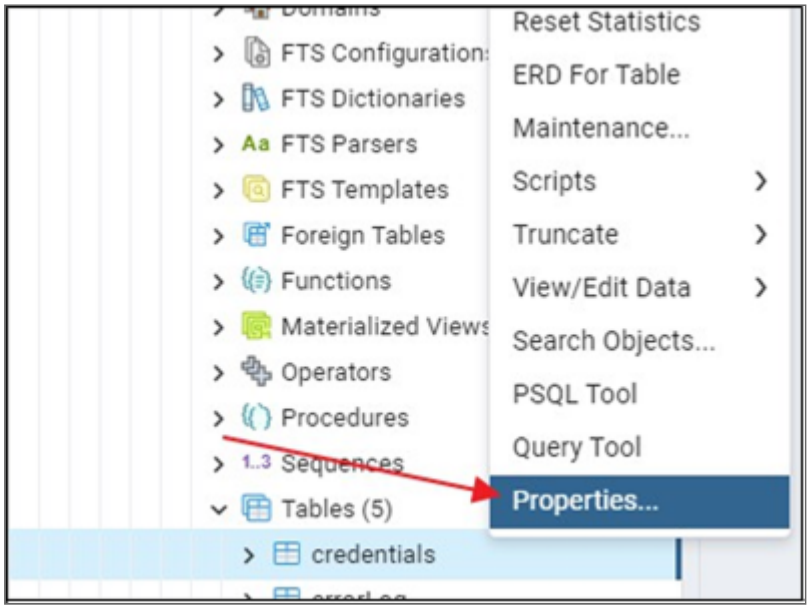
A. ミドルウェア V1.8.3 では Hostname に対応したため、Gallagher workstation client を使ってミドルウェアを使用できるように、Migration を実施しています。

Migration を手動で作成するには、以下の手順に従ってください：

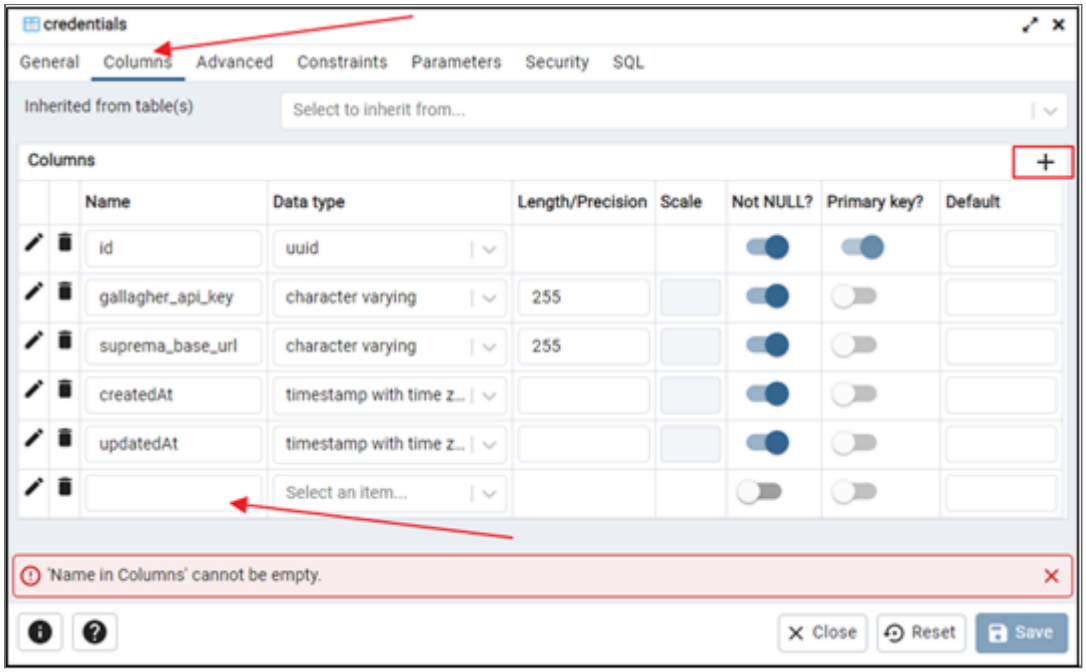
1. Pgadmin に移動します。 パスワードを求められたら、インストール時に設定した既定のパスワード **G@ll@gher** を入力します。
2. 次に **Servers** を**クリック**します。パスワードを求められたら同じ **G@ll@gher** をパスワードとして使用します。続いて **Databases** を**クリック**し、Suprema → Schemas → public → Tables を**展開**します。 次に credentials テーブルを**選択**します。



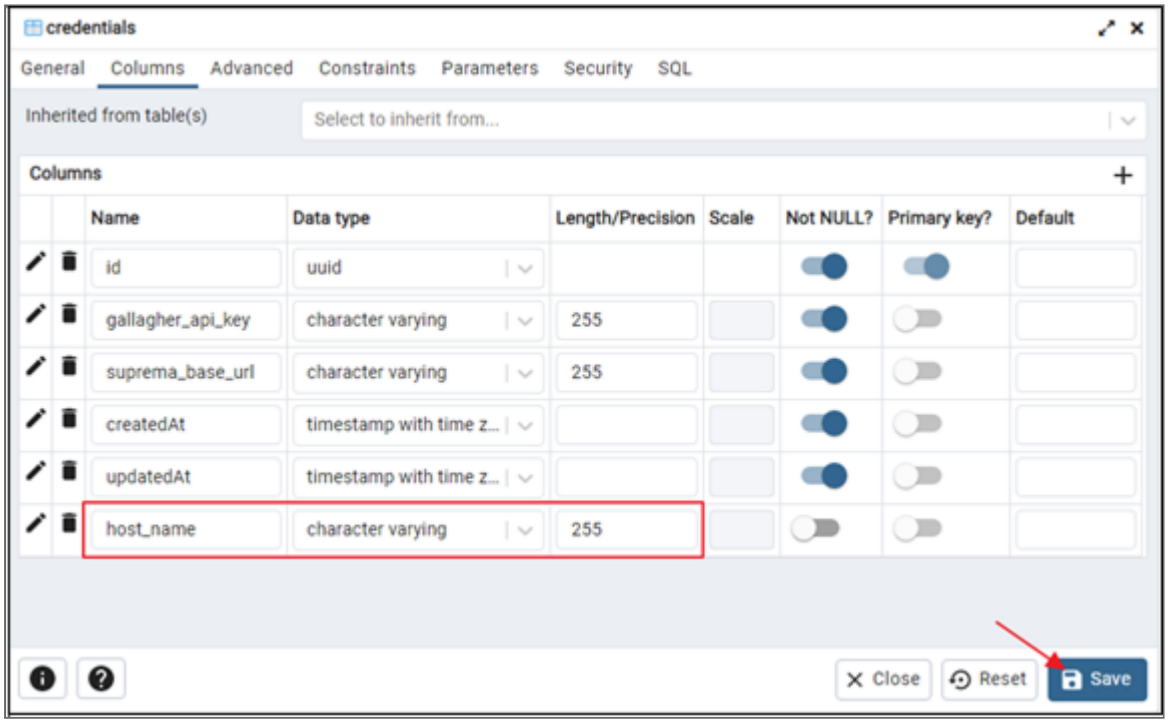
3. 次に credentials テーブルを**右クリック**し、一覧から **Properties** オプションを**選択**します。



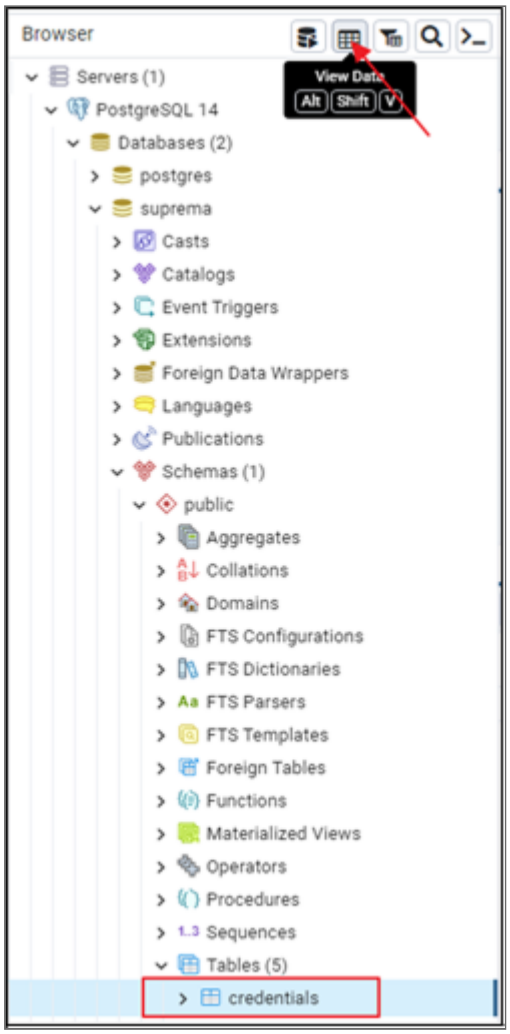
4. 次のウィンドウで **Columns** オプションを**選択**し、+ アイコンを**クリック**すると、下の画像のように新しい列オプションが表示されます。



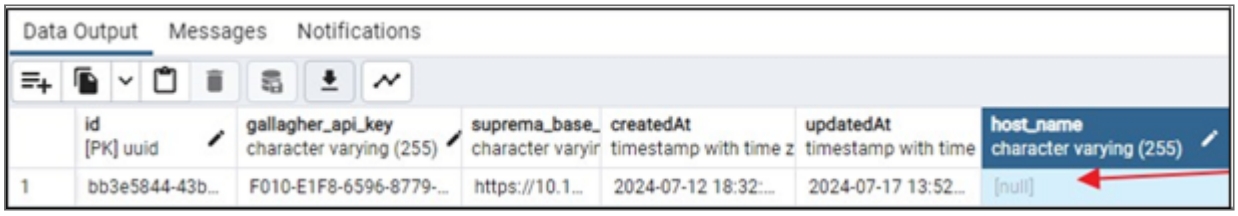
5. 次に Columns オプション内で、名前を host_name、データ型を character varying、Length/Precision を 255 に設定し、**Save** ボタンを**クリック**します。



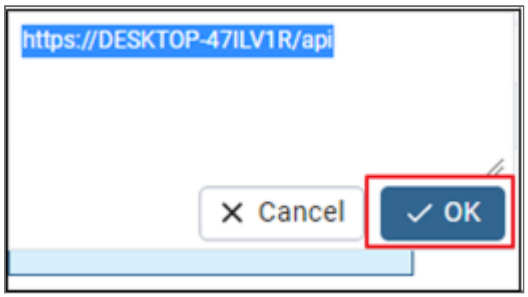
6. 次に credentials テーブルを選択し、**View Data** ボタンを**クリック**します。



7. 次に host_name 列内のボックスを**ダブルクリック**すると、ポップアップが開きます。



8. ポップアップに `https://[YOUR-HOST/SYSTEM-NAME]/api` と入力し、**OK** を押します。

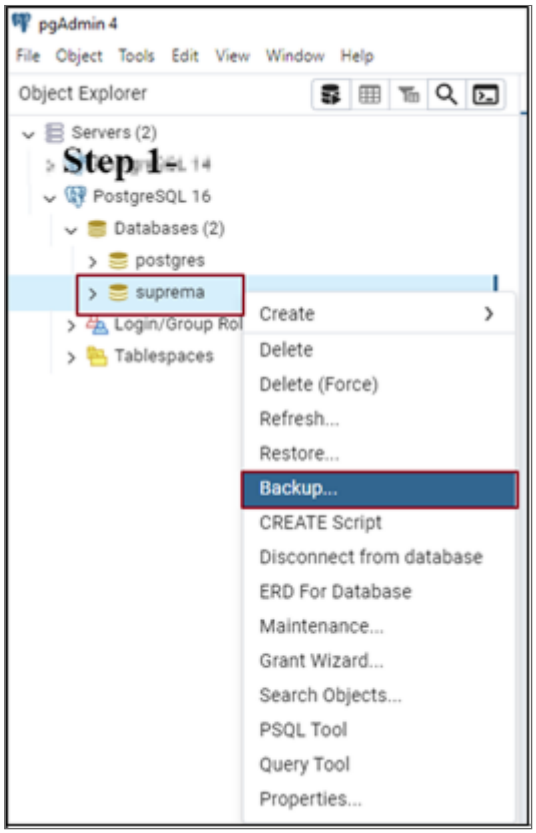


9. 次に `F6` を押して変更を保存します。

Q. PostgreSQL 14 のデータベースをバックアップし、バージョン 16 にアップグレードして、データベースを復元する手順。

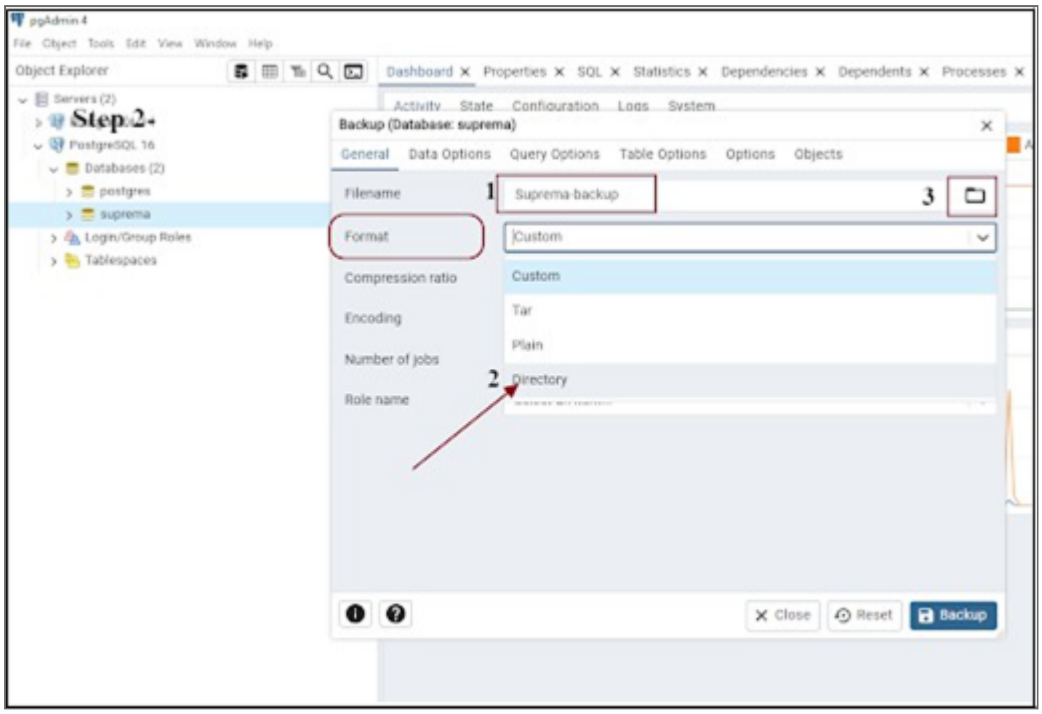
A. PostgreSQL 14 でデータベースをバックアップする

1. pgAdmin 4 を開く：
   - **Databases** セクションの下にある **Suprema** データベースを右クリックし、**Backup** を選択します。



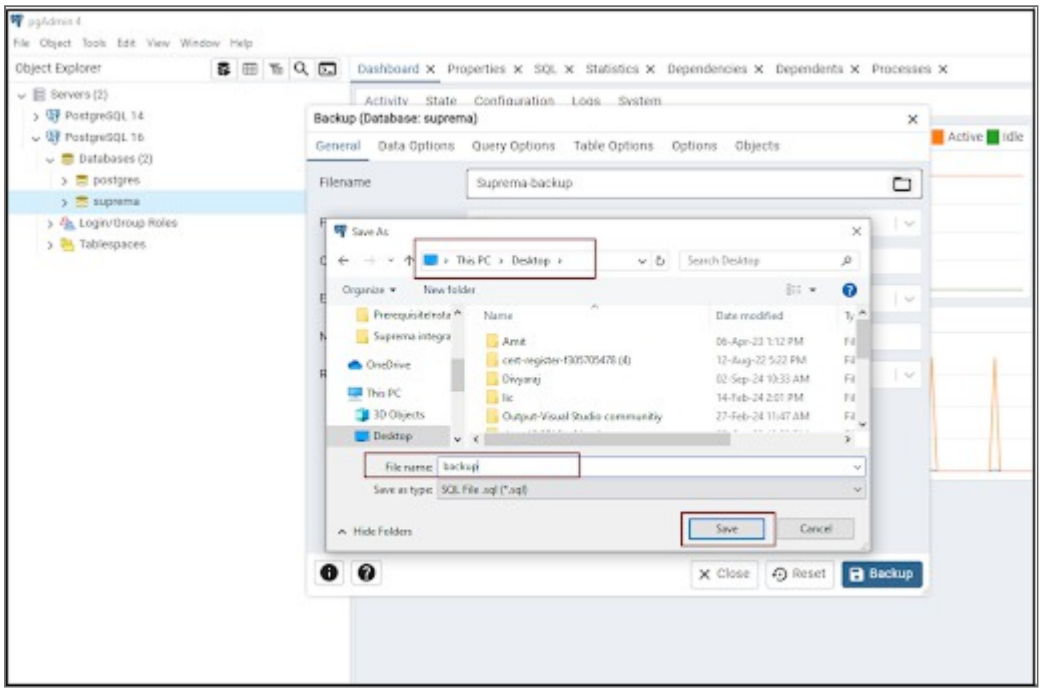
2. バックアップ ファイル名と形式を設定する：
   - **File name** フィールドに **Suprema-backup** と入力し、形式として **Directory** を選択します。

- **ファイル** アイコンをクリックして保存先を選択します。



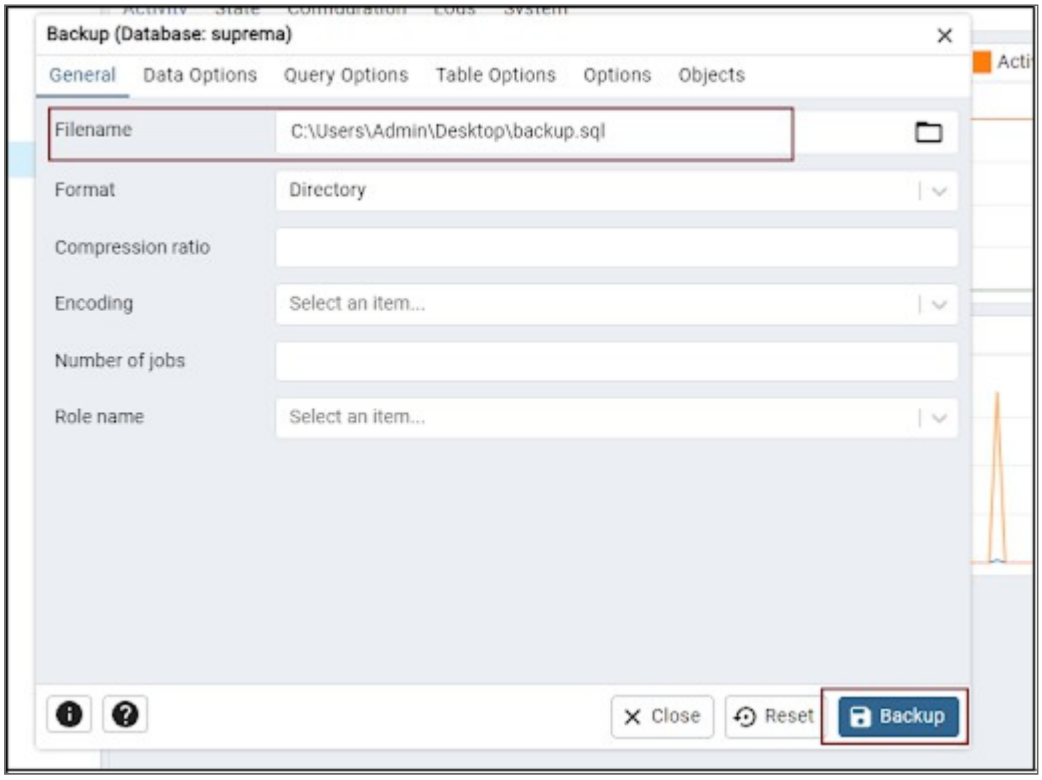
3. 保存先を選択する：

- バックアップを保存するディレクトリを選択します（例：デスクトップ）。 ファイル名を入力し、**Save** を押します。



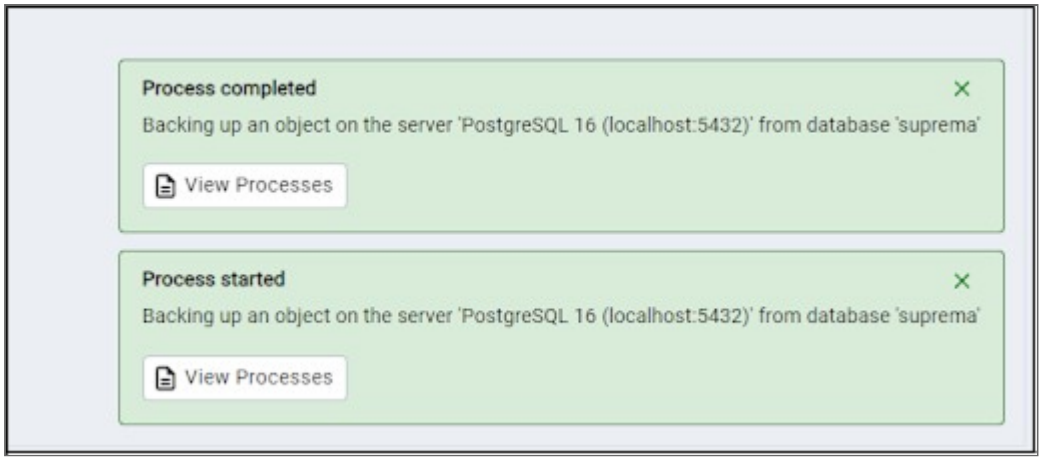
4. バックアップを開始する：

- 選択した場所が反映されたファイル名が表示されます。 **Backup** ボタンを押します。



5. バックアップ完了を確認する：

   - バックアップが完了すると通知が表示されます。 これでデータベースのバックアップは安全に保存されました。



PostgreSQL をバージョン 16 にアップグレードする

1. ミドルウェアと PostgreSQL のサービスを停止する：
   - 28523 ポートと 5432 ポートのプロセスを停止して、実行中のミドルウェアと PostgreSQL のサービスを終了します。
2. パスワードを更新する（必要な場合）：
   - アップグレード中の互換性を確保するため、パスワードを **G@ll@gher** に設定します。
3. PostgreSQL 16 をインストールする：
   - 公式 PostgreSQL Web サイトから PostgreSQL 16 をダウンロードしてインストールし、OS に応じた手順に従ってください。直接 V16.4.1 を取得する場合は、次のリンクを参照してください：https://drive.google.com/file/d/17ehlTpedaGeWezOHZiMd6-ircQhTqBAJ/view?usp=drive_link.
4. データを移行する（任意）：
   - Postgresql 16 でデータベースを復元する を参照してください。
5. PostgreSQL 14 をアンインストールする（任意）：
   - アップグレードを確認したあと、不要であれば PostgreSQL 14 をアンインストールできます。 参照：バージョン 16

へアップグレードしたあとに postgresql14 をアンインストールする。

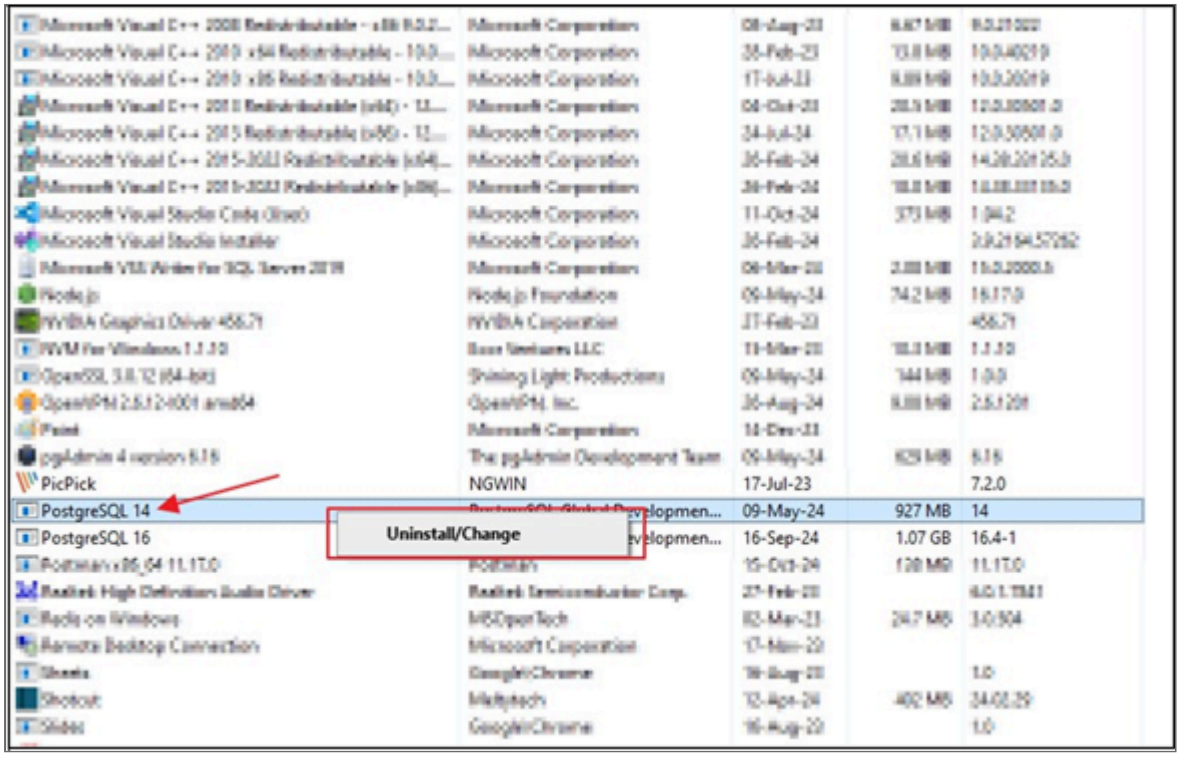
PostgreSQL 16 でデータベースを復元する

1. pgAdmin 4 を開きます（PostgreSQL 16 に接続済み）。
2. 新しいデータベースを作成する：
   - pgAdmin で **Databases** を右クリックし、**Create** → **Database** を選択します。
   - データベース名を **Suprema** にして保存します。
3. バックアップを復元する：
   - 新しく作成した **Suprema** データベースを右クリックし、**Restore** を選択します。
4. バックアップ ファイルを選択する：
   - **Filename** フィールドで、以前作成したディレクトリ バックアップ ファイル（Suprema-backup）を選択します。
5. 復元を開始する：
   - **Restore** をクリックします。 処理が完了するまで待ちます。
6. 復元完了を確認する：
   - 復元が完了すると、成功メッセージが表示されます。 これで PostgreSQL 16 でデータにアクセスし、確認できます。

Q. PostgreSQL をバージョン 16 にアップグレードしたあと、PostgreSQL 14 をアンインストールする。

A. PostgreSQL 14 をアンインストールするには、以下の手順に従ってください。

1. **コントロール パネル** → **プログラム** → **プログラムと機能** に移動します。
2. インストール済みプログラムの一覧で **PostgreSQL 14** を見つけます。
3. **PostgreSQL 14** を右クリックし、**アンインストール** を選択します。 表示される案内に従ってアンインストールを完了します。

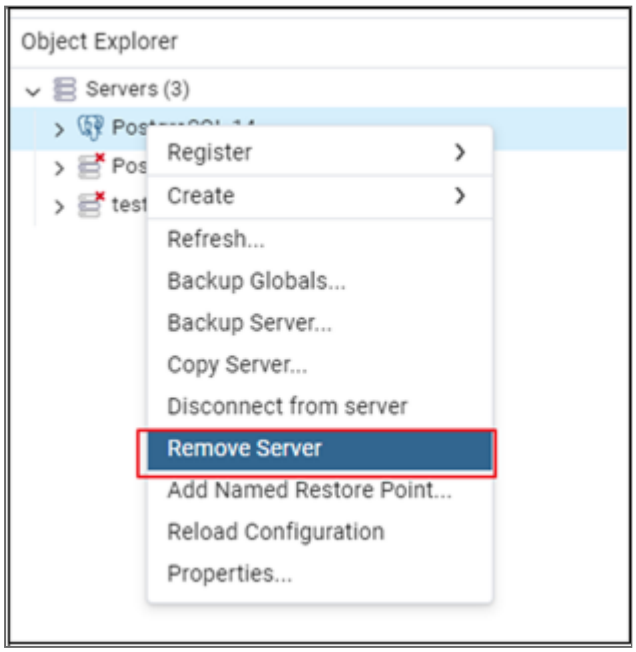


4. インストール ディレクトリ（通常は `C:\Program Files\PostgreSQL\14`）を確認し、残っているファイルやフォルダーを削除します。

> **情報**
> アンインストール後も pgAdmin に PostgreSQL 14 が表示される場合、pgAdmin がサーバー設定を保持している可能性があります。

次の手順で pgAdmin から手動で削除できます：

1. pgAdmin の Object Explorer パネルで **PostgreSQL 14** を**右クリック**します。
2. コンテキスト メニューから **Delete/Remove Server** を**選択**します。



3. 表示される削除確認を**確定**します。



これで PostgreSQL 16 のインストールに影響を与えずに、pgAdmin から PostgreSQL 14 のサーバー設定が削除されます。

Suprema Inc.

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

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

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

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