Suprema Integration with Gallagher Command Centre

ADMINISTRATOR GUIDE

Version 2.0

English
EN 102.00.SIWG

suprema
SECURITY & BIOMETRICS

CONTENTS

Purpose 4

Introduction 5

Features 5

System Diagram 6

Installation 7

Prerequisites 7

Configuration Flowchart 8

Hardware Wiring Connection 9

Install Prerequisite Software 12

Configuration 26

Gallagher Command Center Configuration 26

Hardware configuration 39

BioStar 2 Setup 71

Suprema Integration with Gallagher v2.0 79

Add Access Group 83

Suprema Integration with Gallagher 87

Enroll the User’s Photo ID in the Command Center for Face Template 98

Enroll the User’s Email ID in the Command Center for the QR Code 102

Default card Selection 110

Smart Card (AOC/TOC) 111

HID ICLASS card 115

QR Code Card 117

Licensed devices 117

Troubleshooting and FAQ **119**

Setup 119

Middleware 140

Purpose

Suprema Integration with Gallagher is a middleware that allows the Gallagher Command Centre 8.8 or later System to communicate with the Suprema Biometric devices, which can register Biometric Face or Finger credentials to users from the Command Centre, and manage connected device settings. With Suprema Integration with Gallagher, you can easily set up and build the Biometric Management System for the Command Centre using Suprema biometric devices.

> **Info**
>
> For more details on the functionality of the Gallagher Command Centre access control system, see the user manuals for the Command Centre.

Introduction

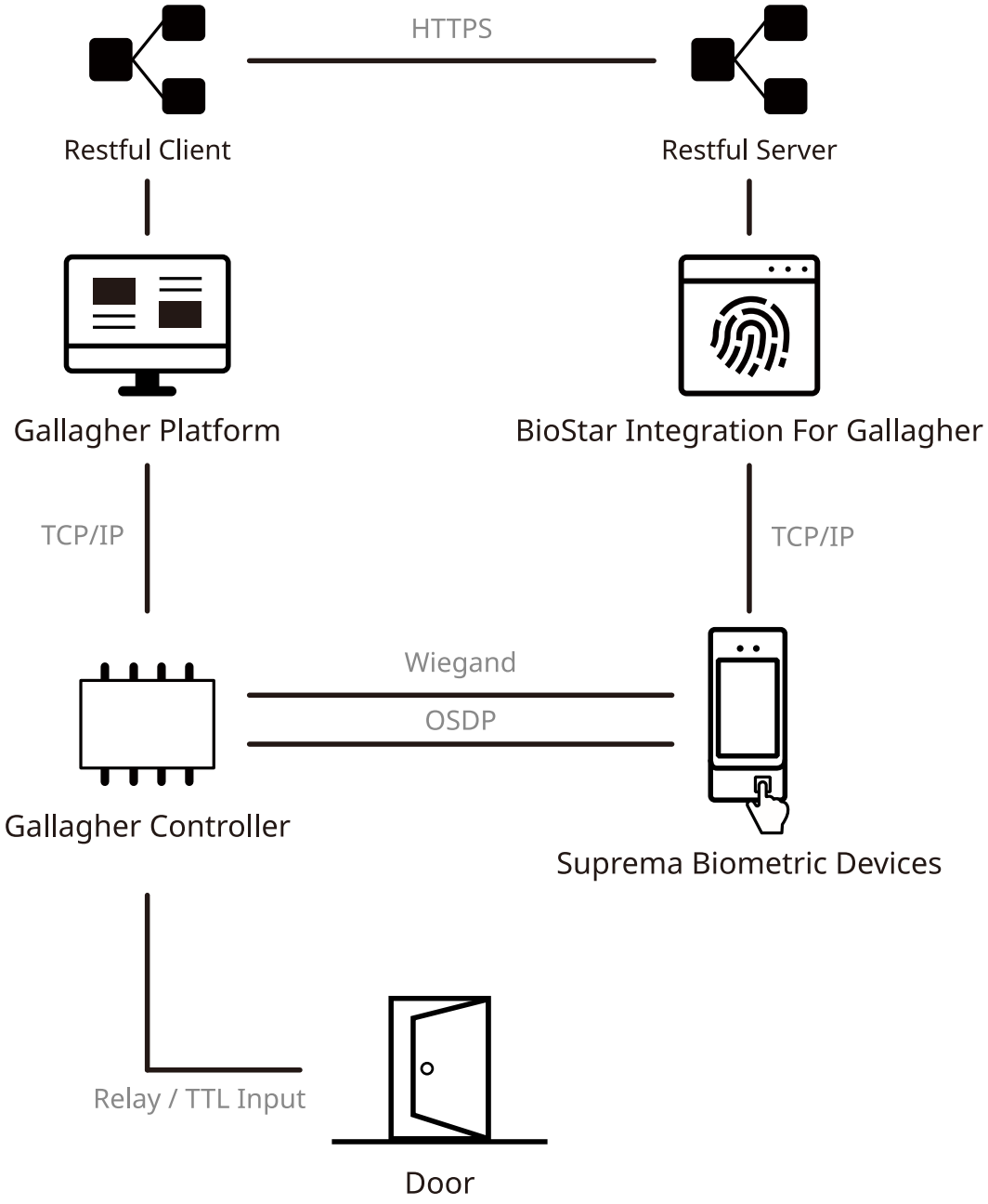
Features

Suprema integration with Gallagher communication between Gallagher Command Centre and Suprema BioStar 2. So, you can generate biometric templates for the Suprema Devices from the Gallagher Command Centre, which then provides a futuristic solution for all end users.

The following are the features provided by Suprema integration with Gallagher:

- Bulk user enrollment and Management from Gallagher Command Centre will be reflected in Suprema BioStar 2.
- From the Suprema Integration, users can register Biometric Visual Face and Fingerprint data through scanning from various Suprema Biometric devices.
- CSN and Wiegand detection and integration with BioStar for automatic data enrichment.
- From the Suprema Integration, users can enroll card data through scanning from biometric devices like X-Station 2, BioLite N2, BioStation 3, FaceStation F2, XPass 2, X-Station 2, BioEntry W3, and BioEntry W2 (These are tested devices).
- Allows up to 1,000 Biometric Devices to Manage.
- All Suprema Device configurations can be done within the same window of the Command Centre.
- Supports a wide range of card types, including TOC cards, QR cards, and even custom card configurations tailored for specific customer needs.
- Integration setup is simplified through a bundled EXE package that includes all necessary prerequisites, ensuring a smooth and efficient installation process.
- Middleware includes built-in support for network-related configurations, along with a comprehensive troubleshooting guide to assist with misconfigurations and fault tolerance scenarios.

System Diagram



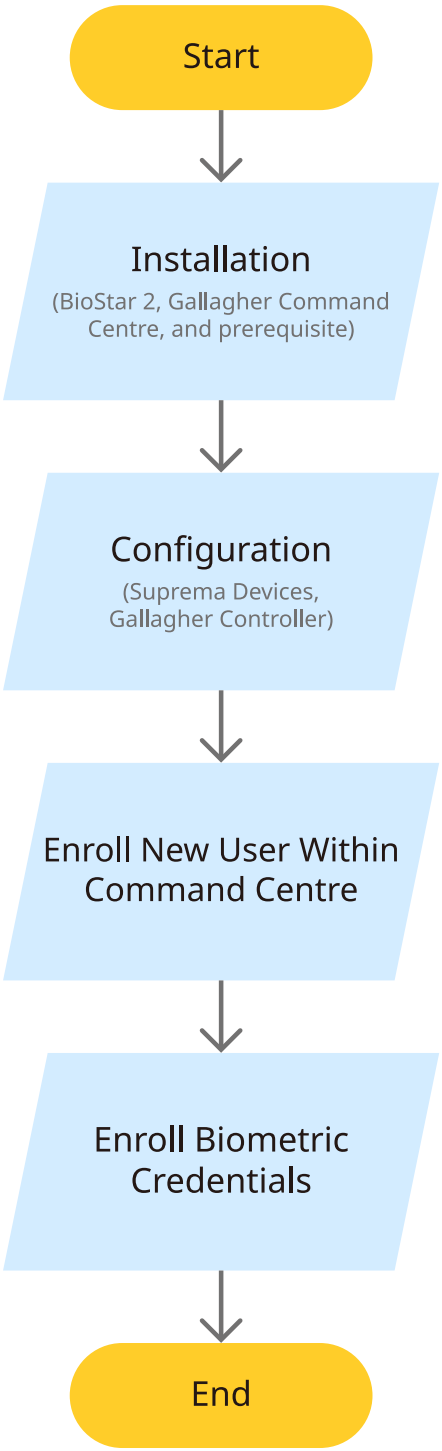
Installation

Prerequisites

The following prerequisites are required to use Suprema Integration with Gallagher. Check the support conditions before installing the Suprema Integration with Gallagher.

Prerequisites	
Microsoft Windows 10(x64) or Later	
Web browsers	New Microsoft Edge
Gallagher Command Centre	Command Center 8.80 or later
Suprema BioStar 2	• x64 bit • Version 2.9.5 or later
Software	• Node v16.17.0 • Postgresql v14.5 • pgAdmin 4 v6.16 • Win64OpenSSL-3.0.5
Middleware system hardware Requirements	• 16 GB RAM • Windows 10 or later • 256 GB SSD/1TB HDD • Intel Iris Xe Graphics (Good to have)
Suprema Biometric Devices	• BioStation 3 • BioLite N2 • FaceStation F2 • BioEntry W2 • XPass 2 • X-Station 2 • BioEntry W3

Configuration Flowchart



Hardware Wiring Connection

For Wiegand Connection

Suprema Device - **Reader 1** to HBUS 4 In 2Out n Door Module Wiegand

(Suprema Device) Wire Name	HBUS 4 In 2 Out Door Module Wiegand Port to connector
Wiegand D0 Out (Green)	R1 Data 0
Wiegand D1 Out (White)	R1 Data 1
Wiegand Ground (Black)	GND
TTL IN0 (Red/Purple)	R1 Out 2
TTL IN1 (Yellow/Brown)	R1 Out 1

Suprema Device - **Reader 2** to HBUS 4 In 2Out n Door Module Wiegand

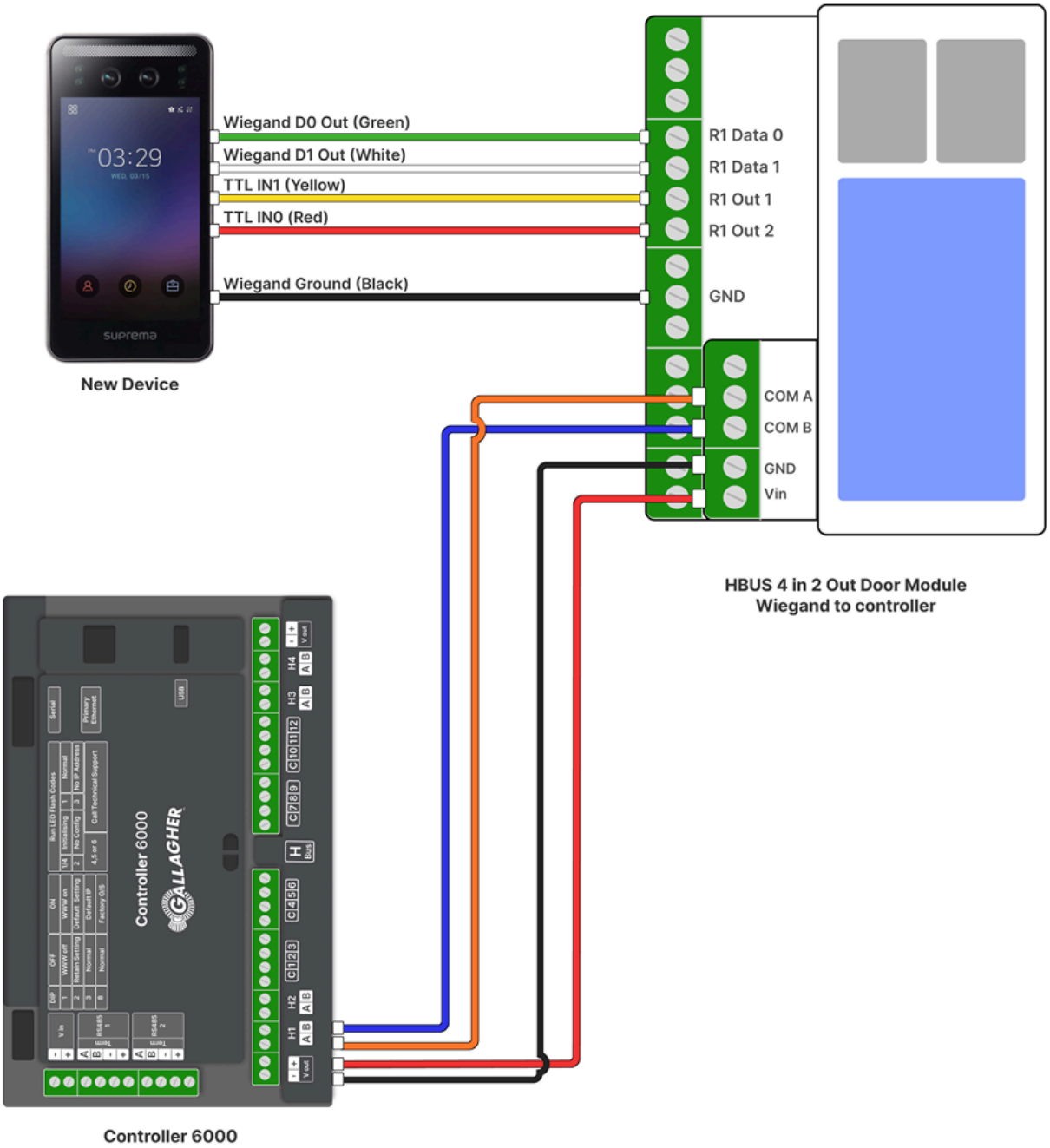
(Suprema Device) Wire Name	HBUS 4 In 2 Out Door Module Wiegand Port to connector
Wiegand D0 Out (Green)	R2 Data 0
Wiegand D1 Out (White)	R2 Data 1
Wiegand Ground (Black)	GND
TTL IN0 (Red/Purple)	R2 Out 2
TTL IN1 (Yellow/Brown)	R2 Out 1

HBUS 4 In 2Out n Door Module Wiegand to Controller 6000 HBus

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 Connection Diagram



For OSDP Connection

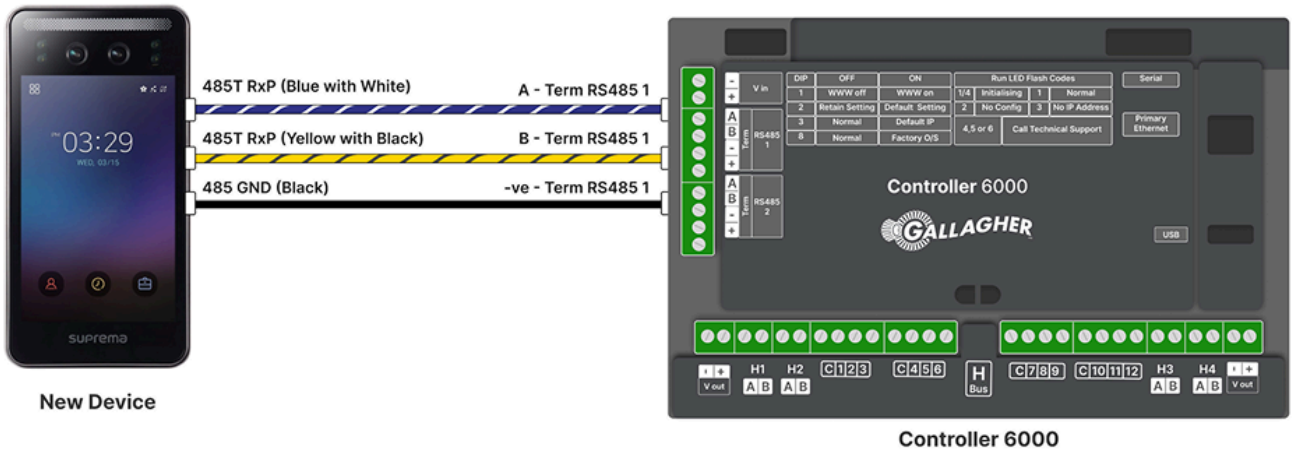
Suprema Device OSDP/RS485 **reader 1** to Controller 6000

(Suprema Devices/OSDP device) Wire Name	Controller 6000 Ports
Blue/Blue With White	RS485 1 A
Yellow/Yellow With Black	RS485 1 B
Black/White With Black	RS485 1 -ve

Suprema Device OSDP/RS485 **reader 2** to Controller 6000

(Suprema Devices/OSDP device) Wire Name	Controller 6000 Ports
Blue/Blue With White	RS485 2 A
Yellow/Yellow With Black	RS485 2 B
Black/White With Black	RS485 2 -ve

OSDP Connection Diagram



Install Prerequisite Software

Installation of Gallagher Command Centre Setup

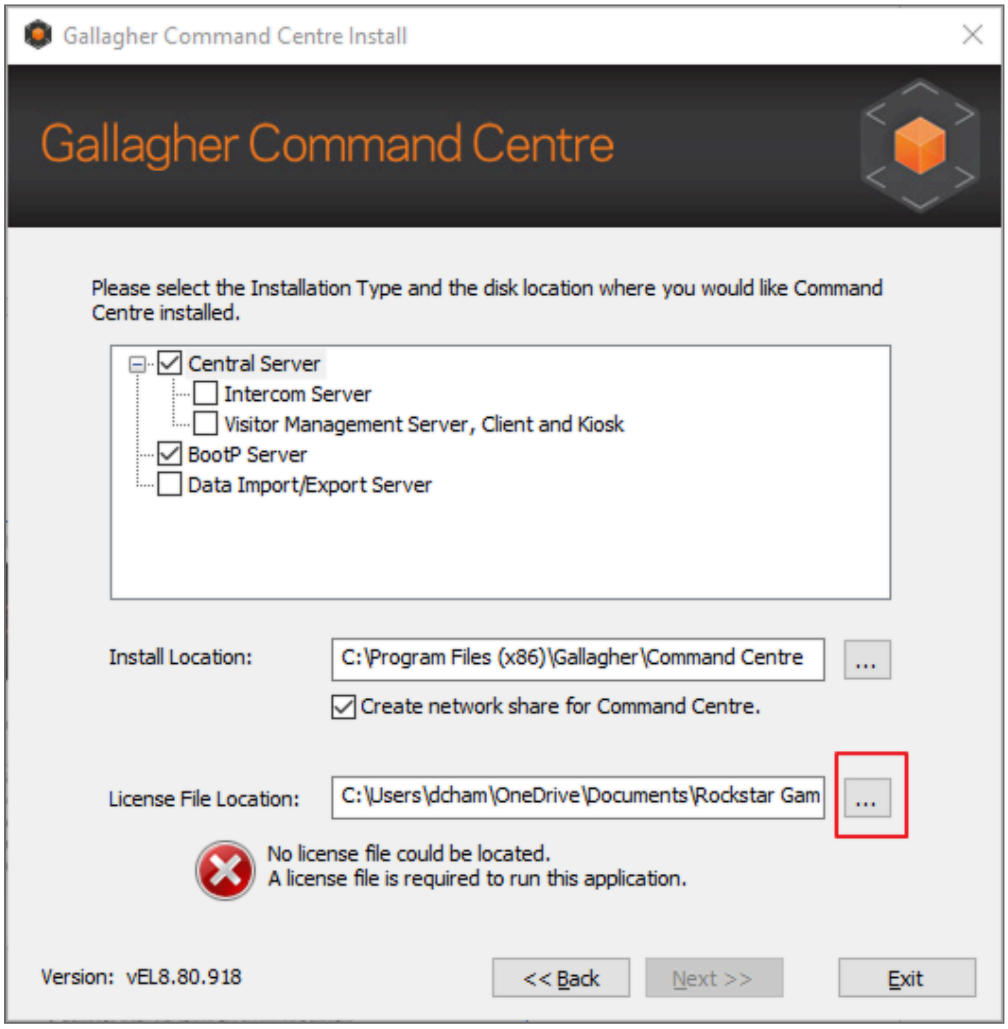
Info

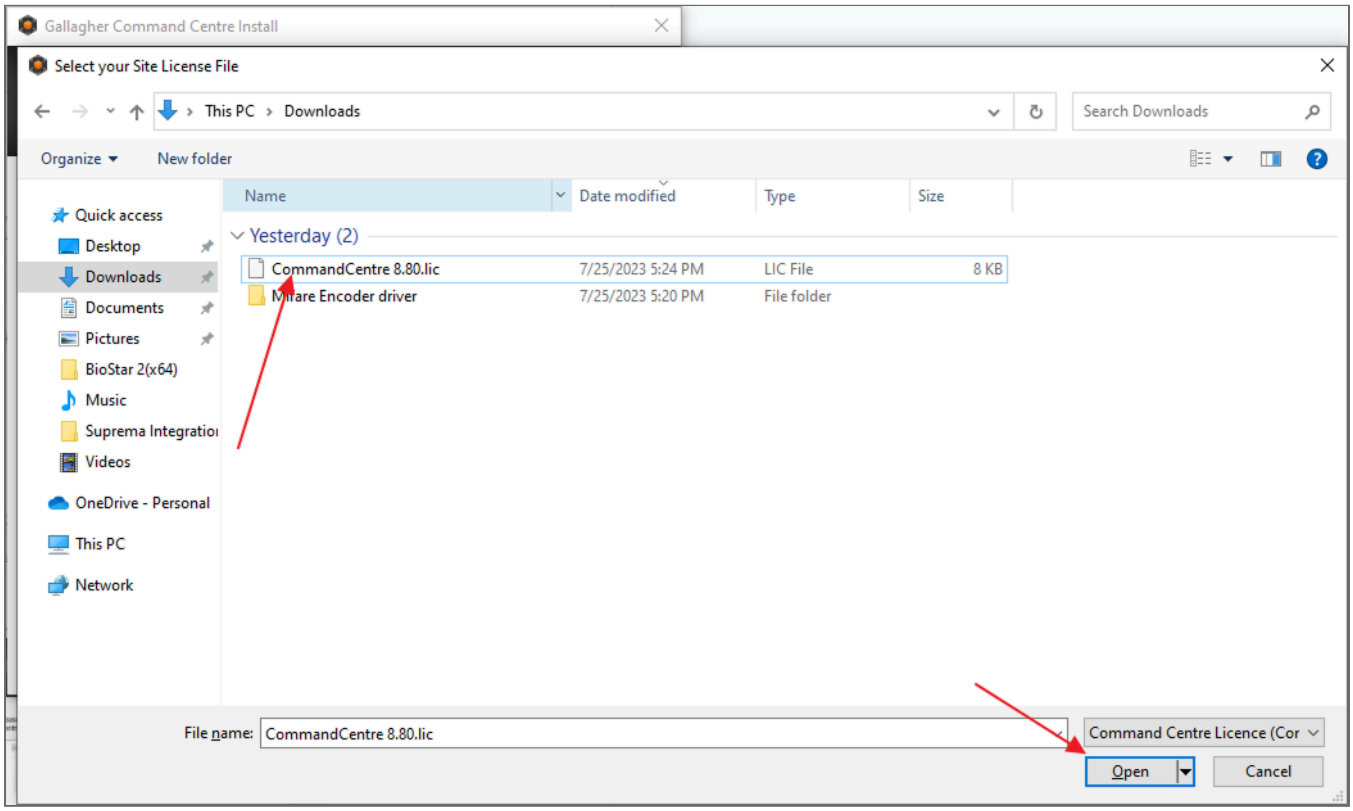
- Please don't change any names and passwords while installing and setting up the configuration.
- To Upgrade the Suprema Integration with the Gallagher version click here.
- Specifically, you can refer to either the **3C4643 Gallagher Command Centre vEL8.80 Release Note** for new installations.
- The **3E0068 Upgrade Procedure** for upgrading purposes for more information in the Release Notes Folder of your Command Centre ISO Directory.
- You must have to extract `Suprema integration With Gallagher.zip` to `C:\Program Files\`.

1. Inside the Gallagher Command Centre folder vEL.8.80 (or Later) → Setup.exe, **tick the checkbox** and press the **Next** button.

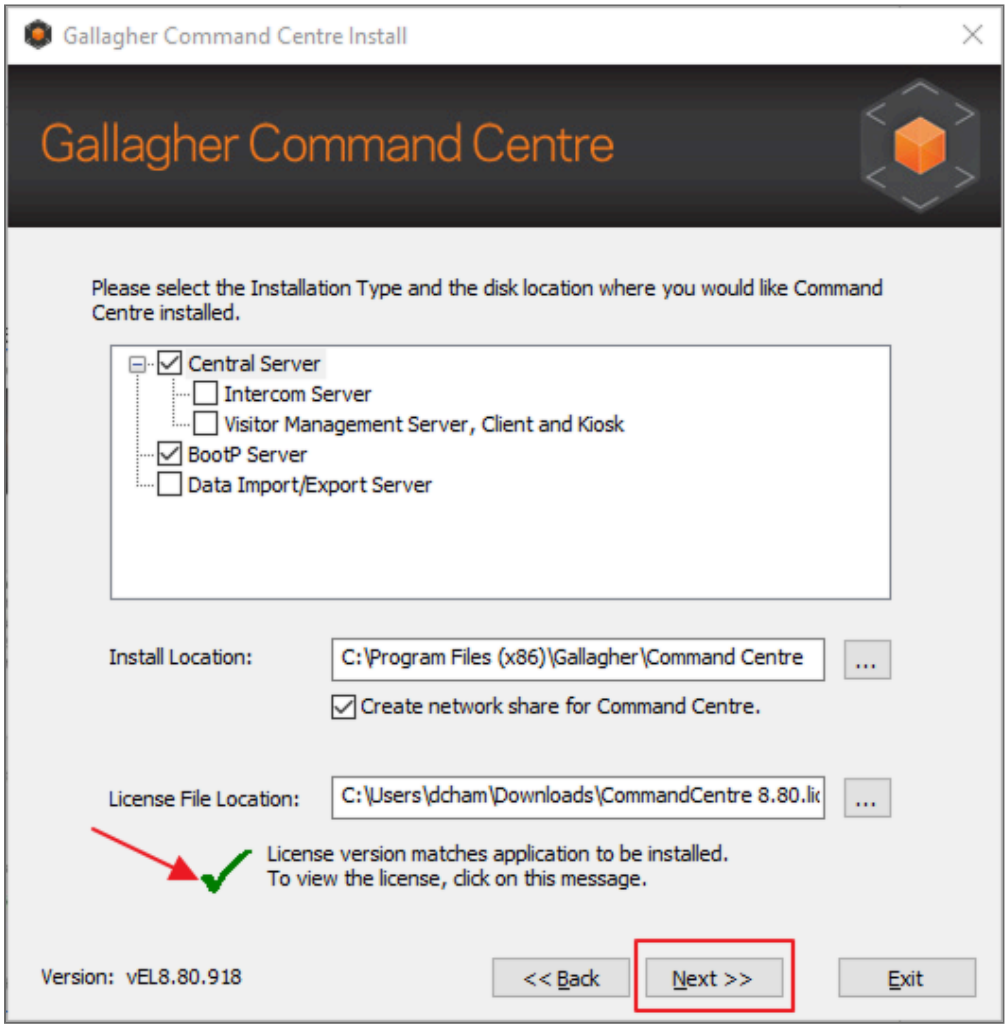


2. **Click** the "..." button and locate the License file provided in the setup.

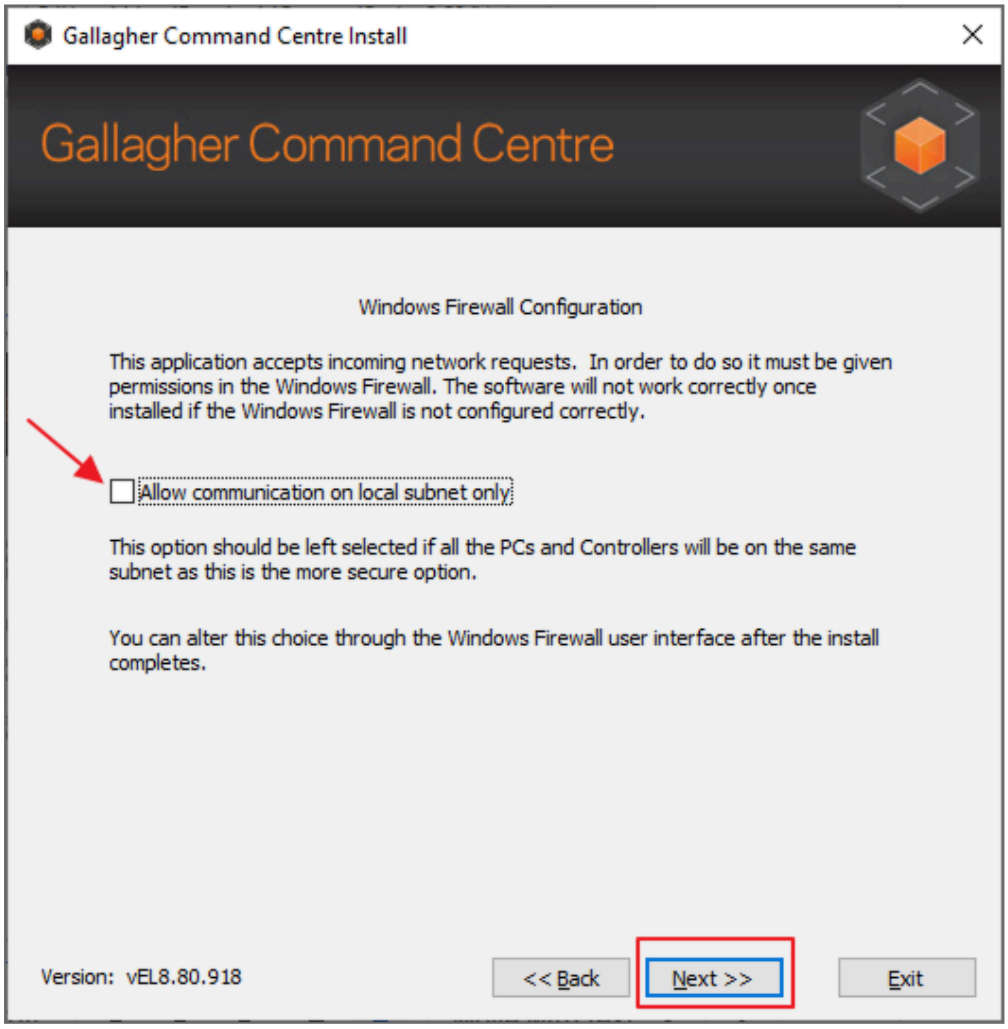




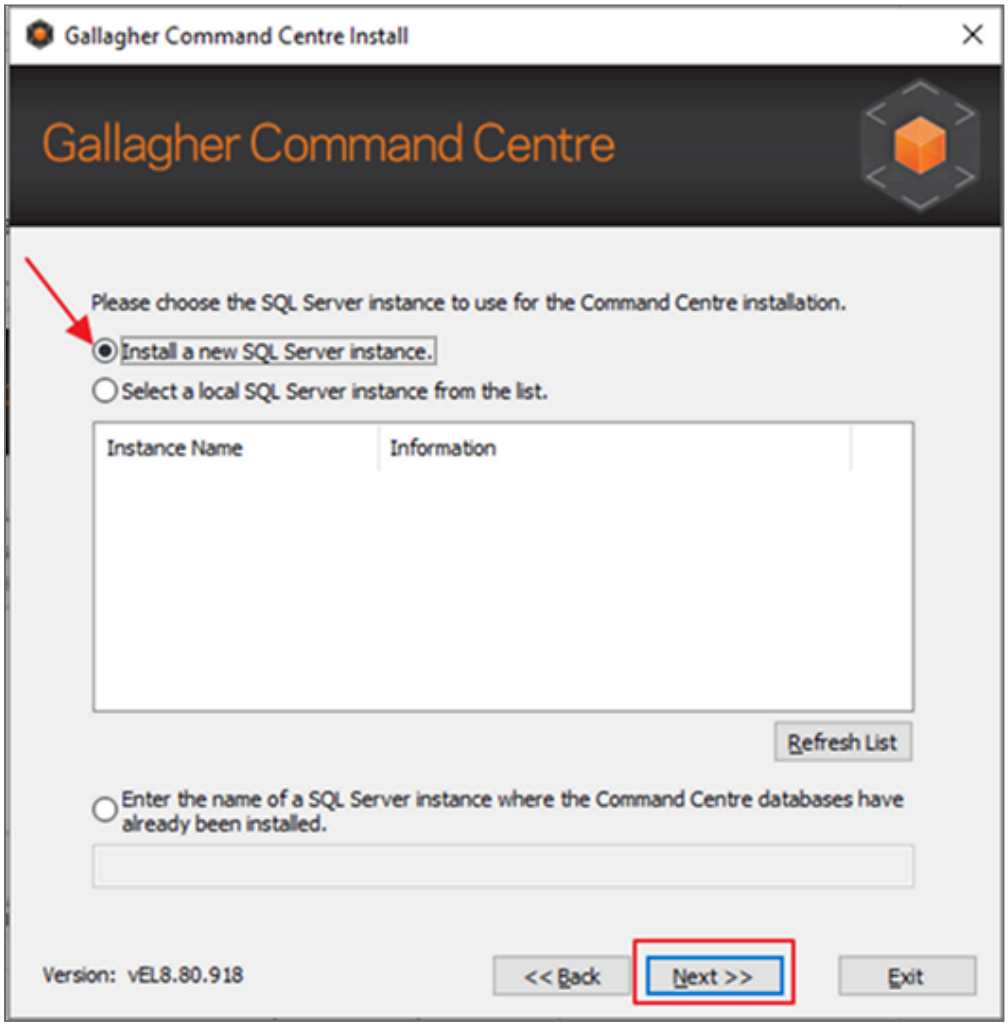
3. When you select the correct license file the icon will change to a tick mark then **press** the **Next** button.



4. **Uncheck** the checkbox of the subnet only and press the **Next** button.

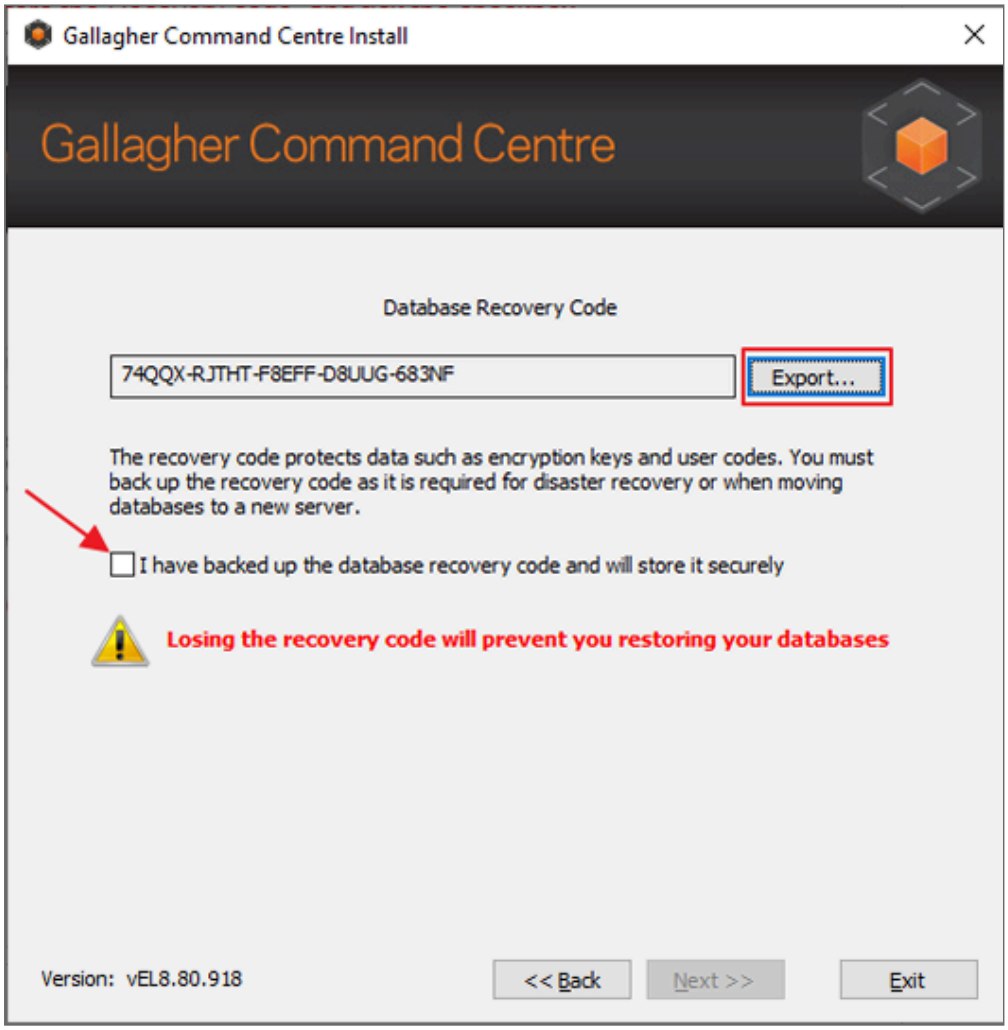


5. **Select** the Install new SQL option and press the **Next** button.

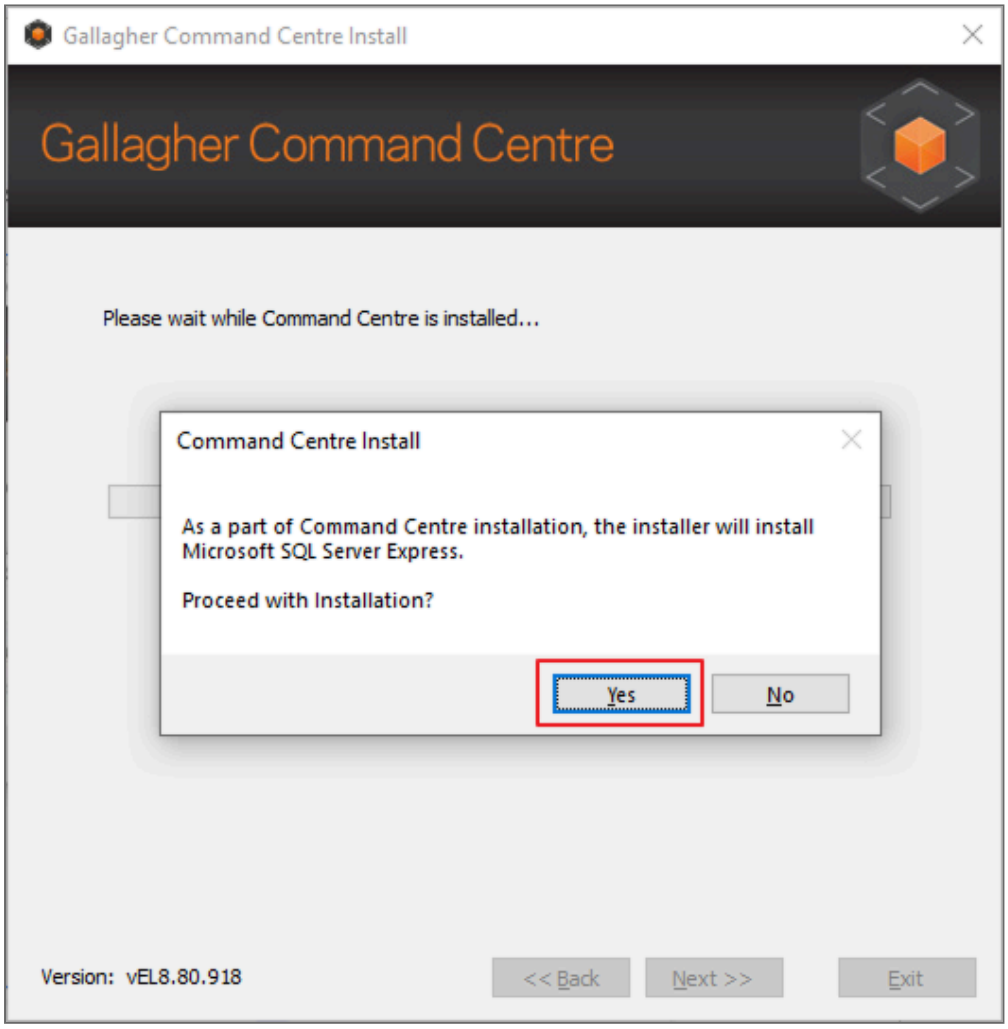


6. **Select** the do not install a database template.
7. Without changing any settings press **Next** until you are recovering the code screen.

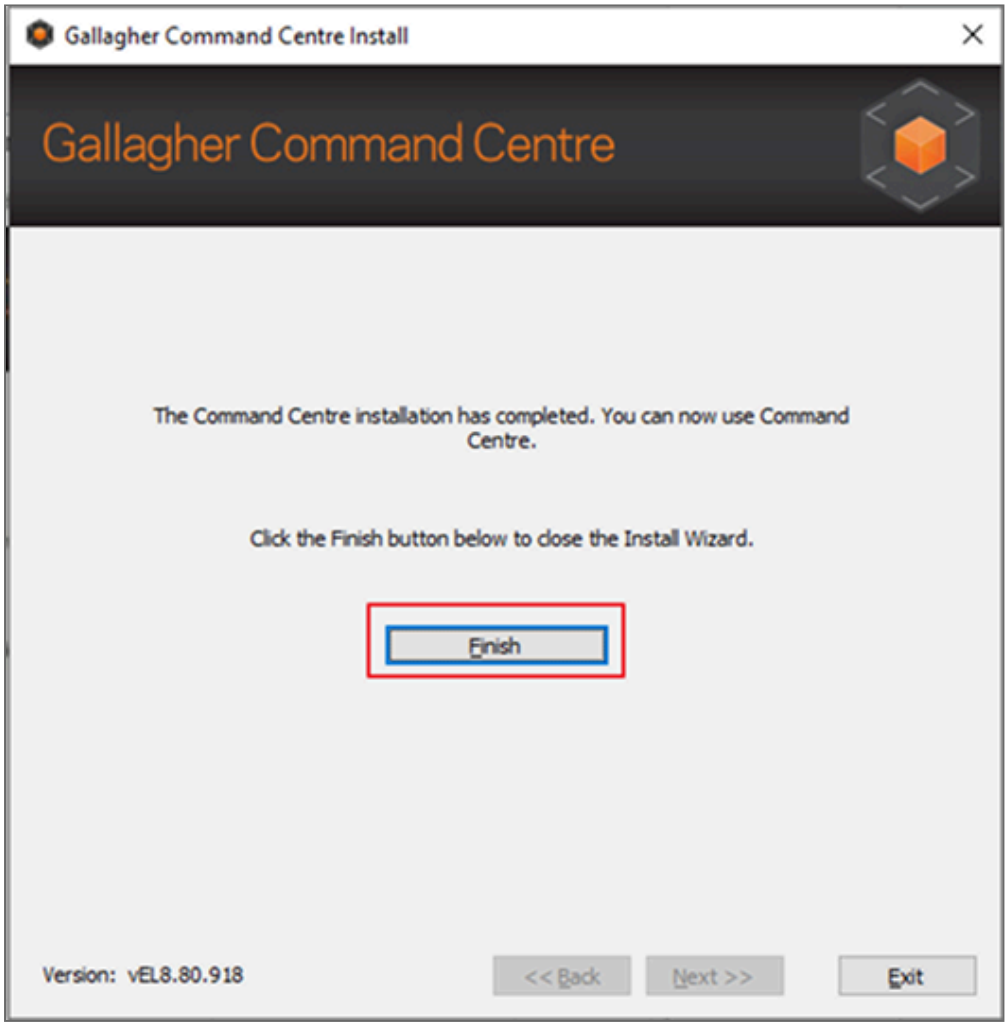
> **Info**
> Click the export button and store the Recovery code, and tick the checkbox.



8. Select **Yes** and the installation will start.



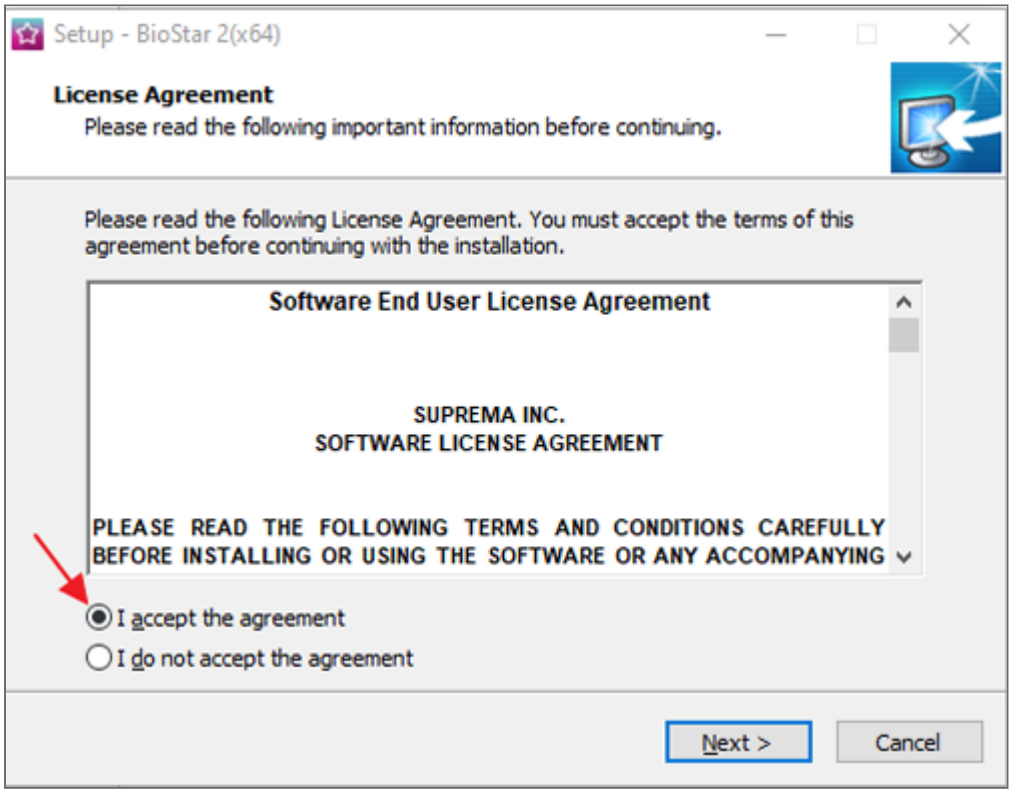
9. After the Installation is complete, press the **Finish** button.



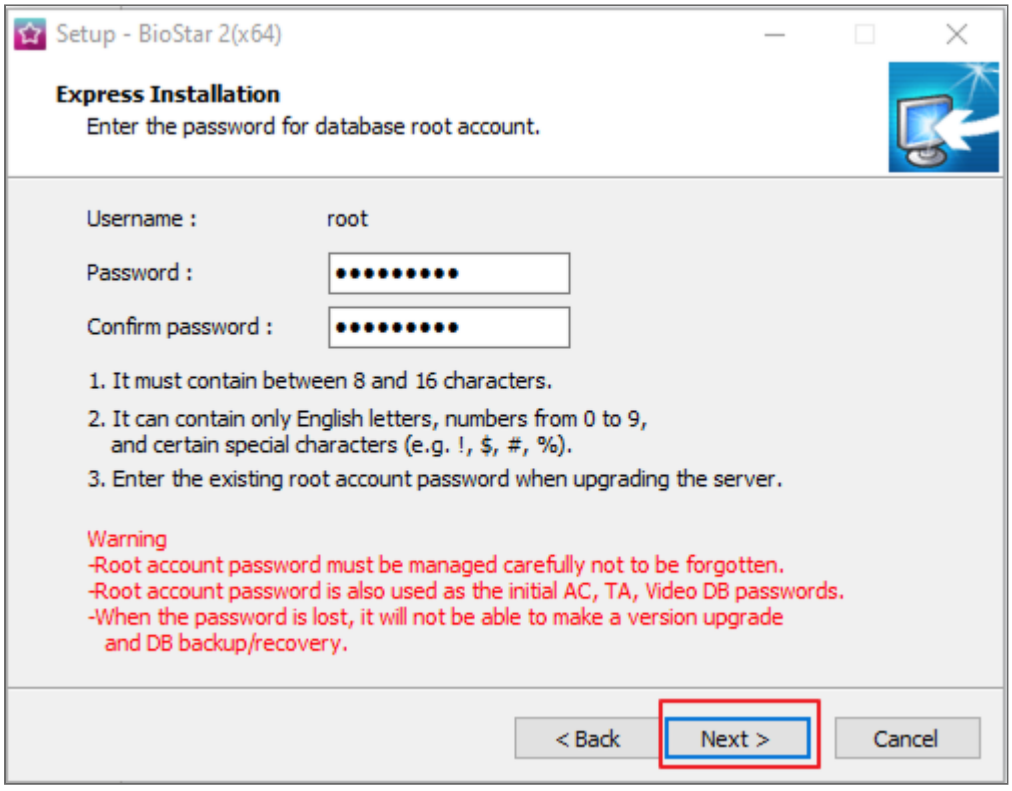
Installation of BioStar 2

1. Open the **BioStar 2.exe** and choose the language & Accept the Agreement press **Next**.

> **Info**
> Download the latest version of BioStar 2 - Click Here.

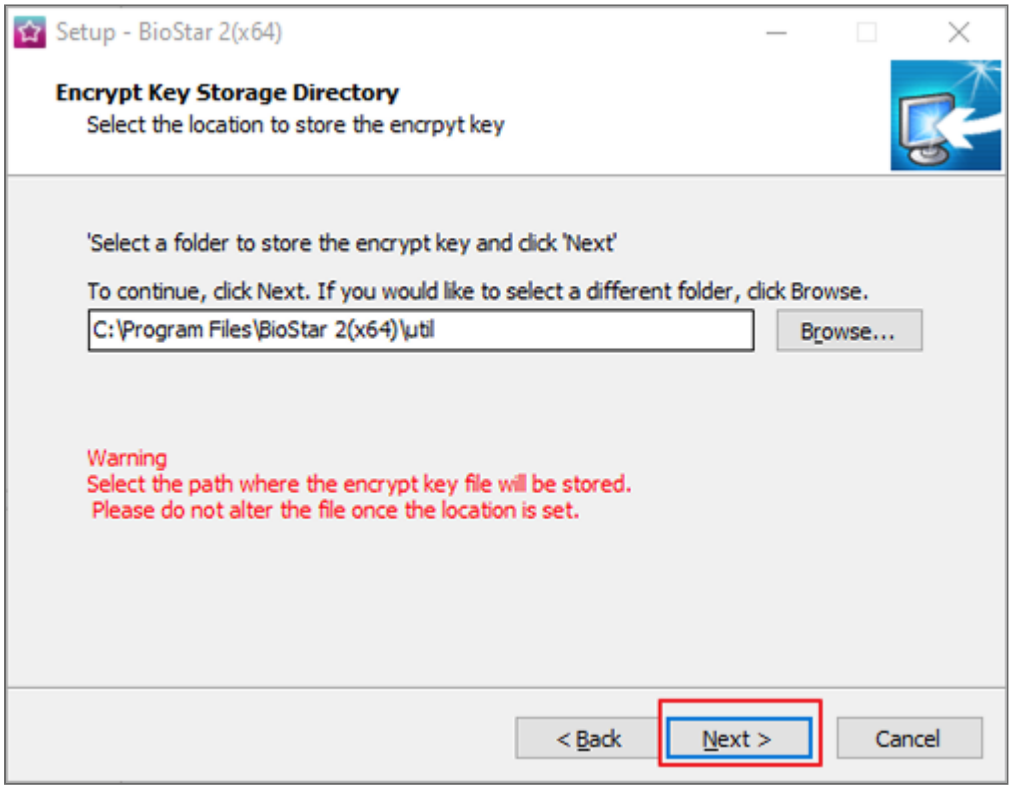


2. Enter your BioStar 2 **Password** here and press the **Next** button.

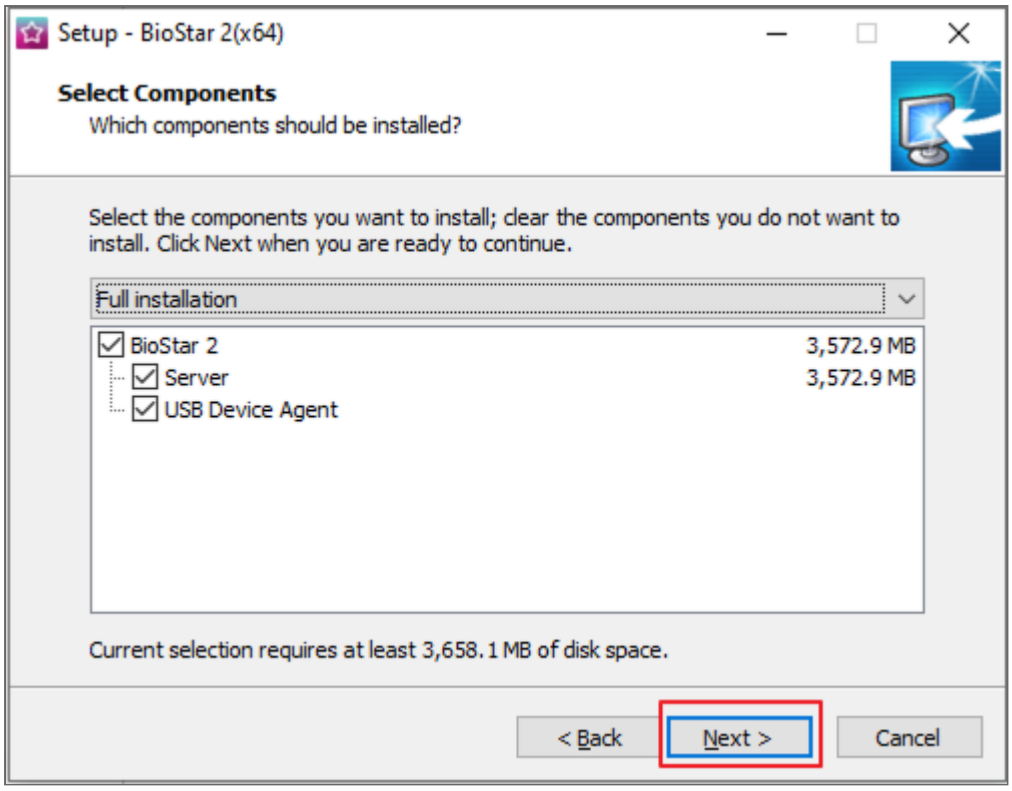


3. Select **Express** Installation and enter the BioStar 2 password again.

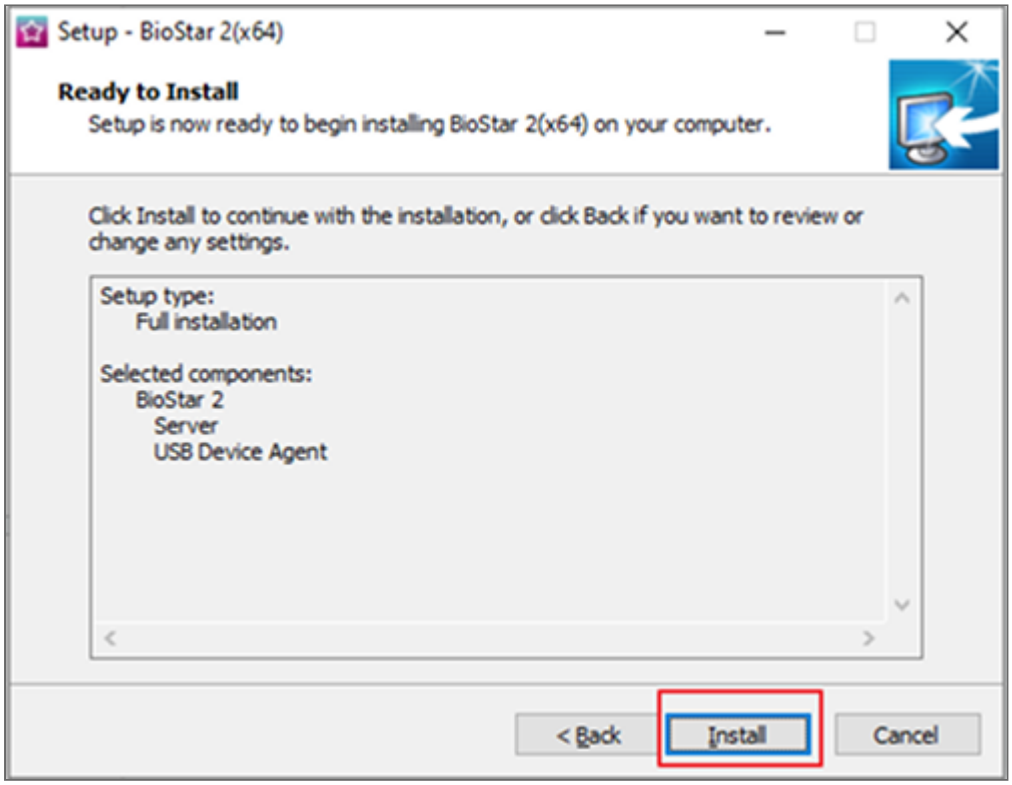
4. Select the location and proceed.



5. Press the **Next** button until you reach the Select the Components screen. Check both options and press the **Next** button.

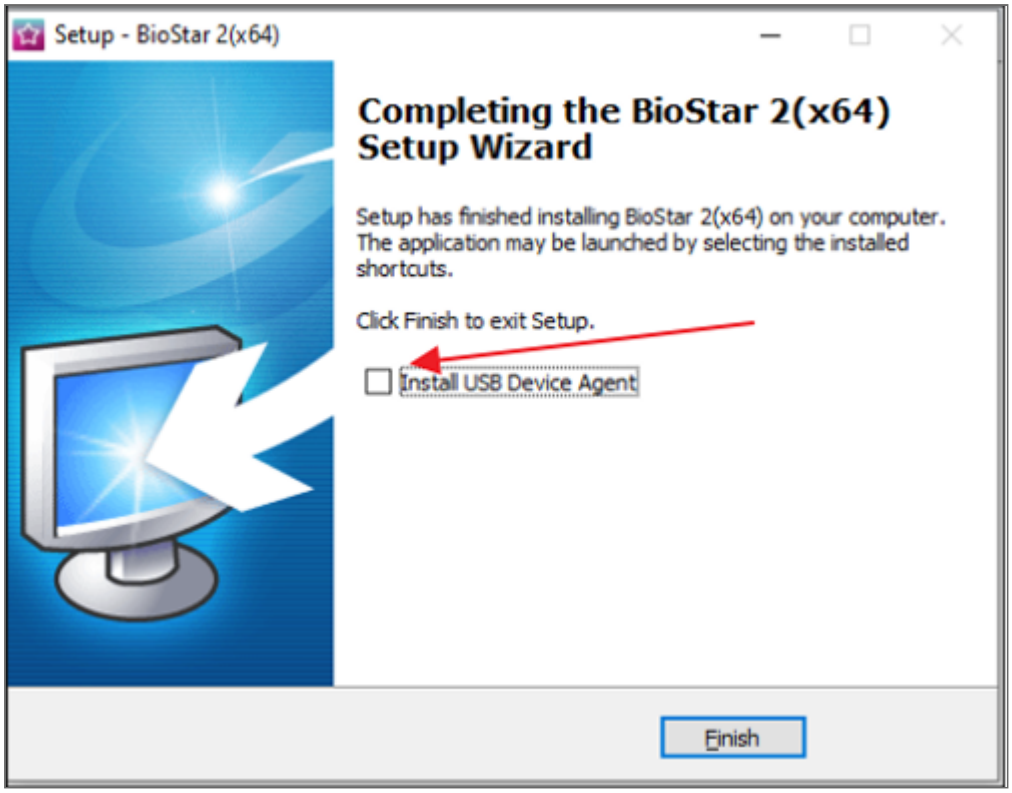


6. Press the **Install** button to start the installation.



7. **Uncheck** the Install USB Device Agent option and press the **Finish** button and BioStar 2 is installed on your PC.

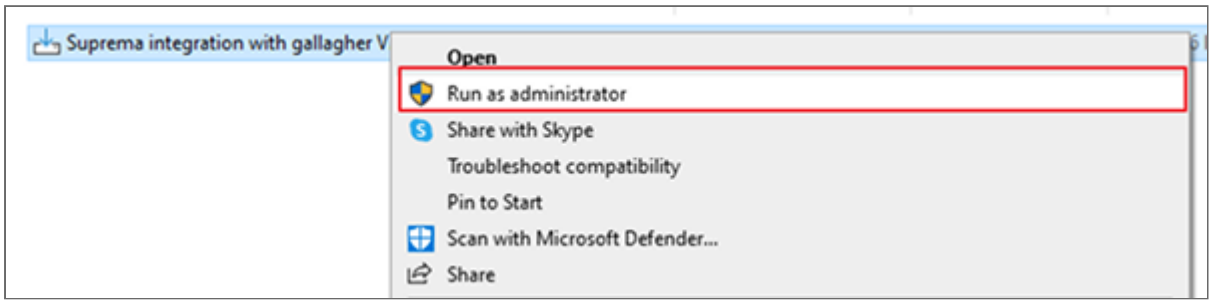
> **Info**
> If you want to use the USB device, you must **check** the Install USB Device Agent.



Installation middleware prerequisites

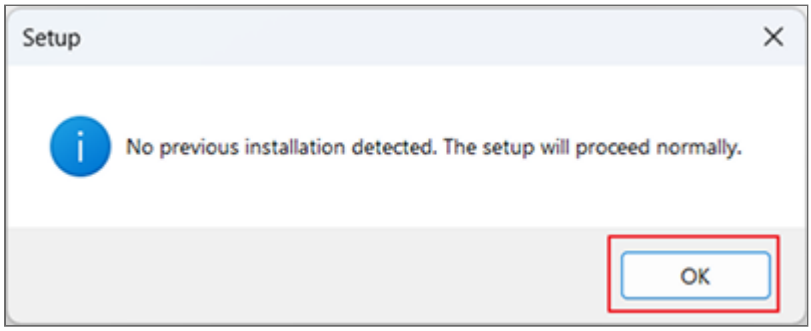
> **Info**
>
> - Before extracting/running Suprema Integration with Gallagher2.0.zip , please turn off the antivirus.
> - If you are upgrading from an older version, please find the solution in the troubleshooting guide.

1. You need to **run** the Suprema Integration with Gallagher 2.0 file as an administrator inside the Suprema Integration with Gallagher 2.0 folder. This will install OpenSSL, PostgreSQL, PgAdmin4, and Node. JS. Also, this will set up the certifications required for our integration.

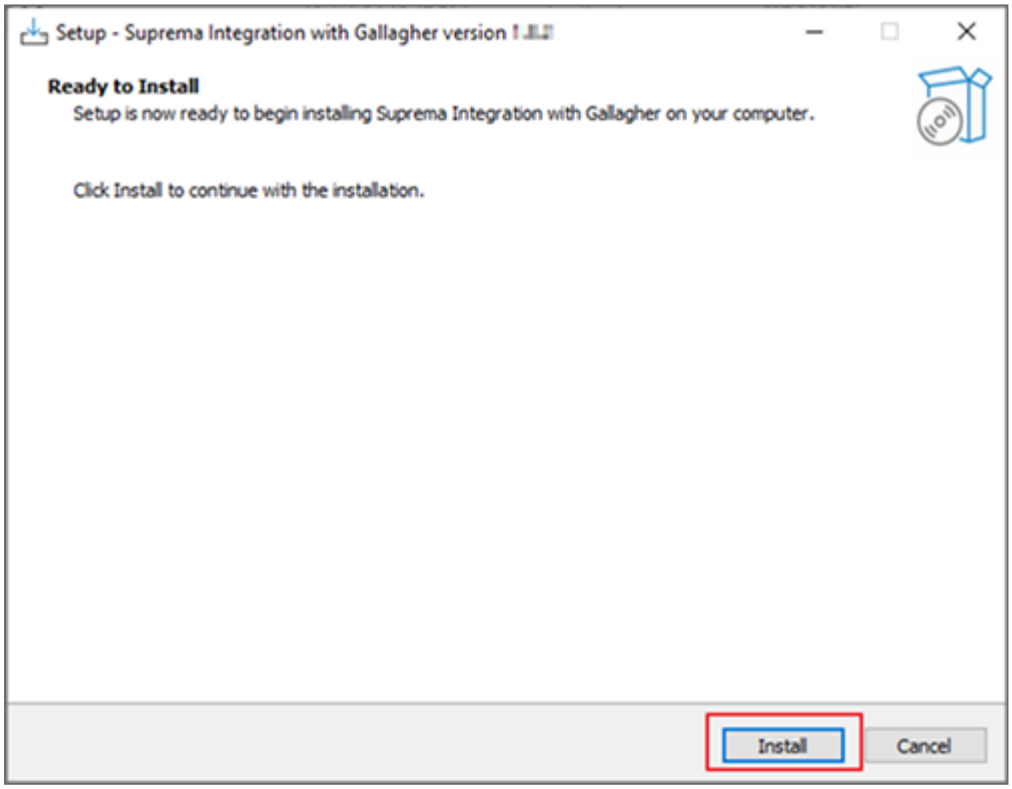


2. Press **Yes** when if it asks for allow from an unknown publisher permissions.

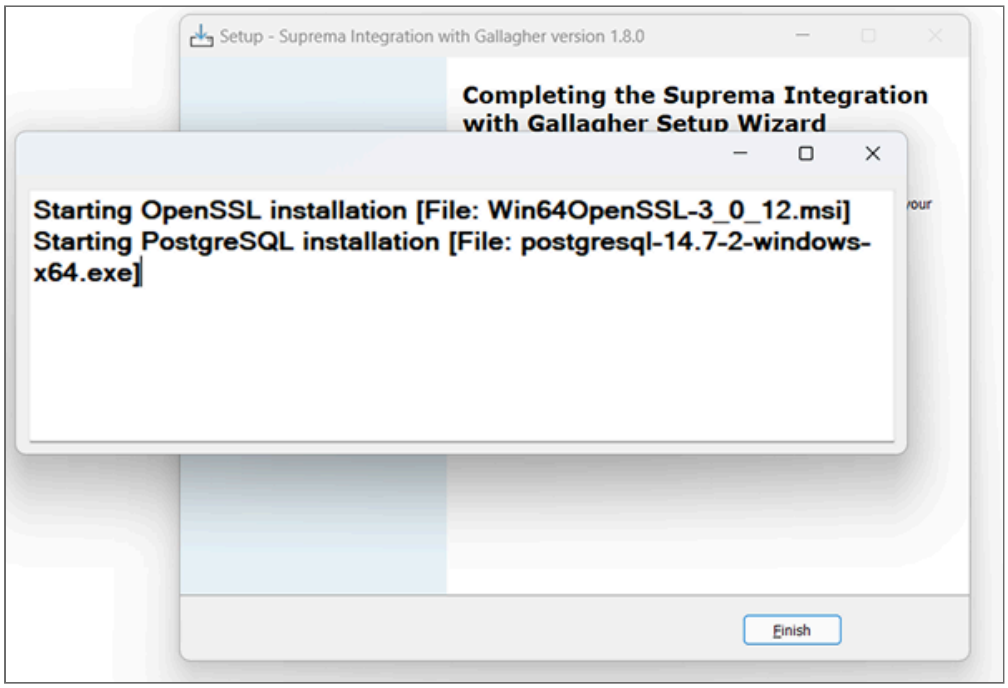
3. Press **OK**.



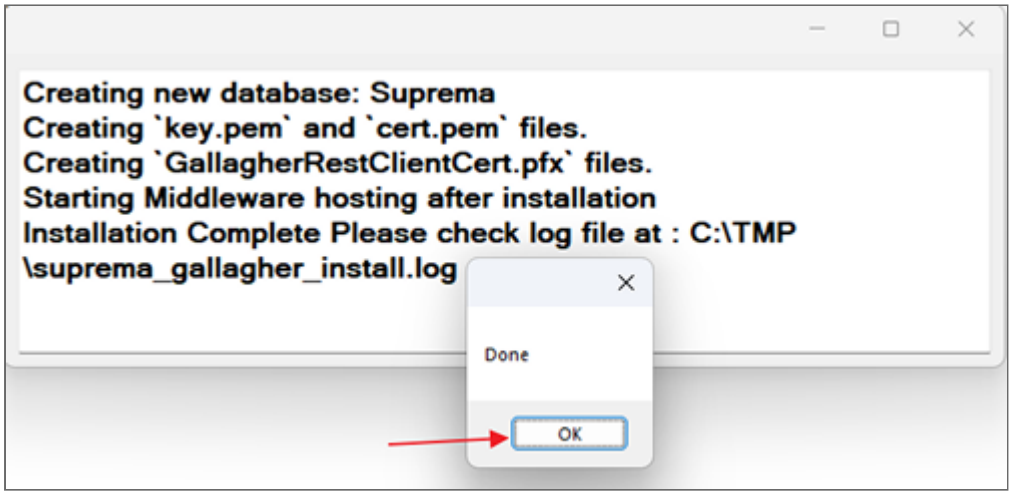
4. Now that you are ready to install the software, press **Install**.



5. It will start the installation for prerequisites, and the software will get installed automatically.

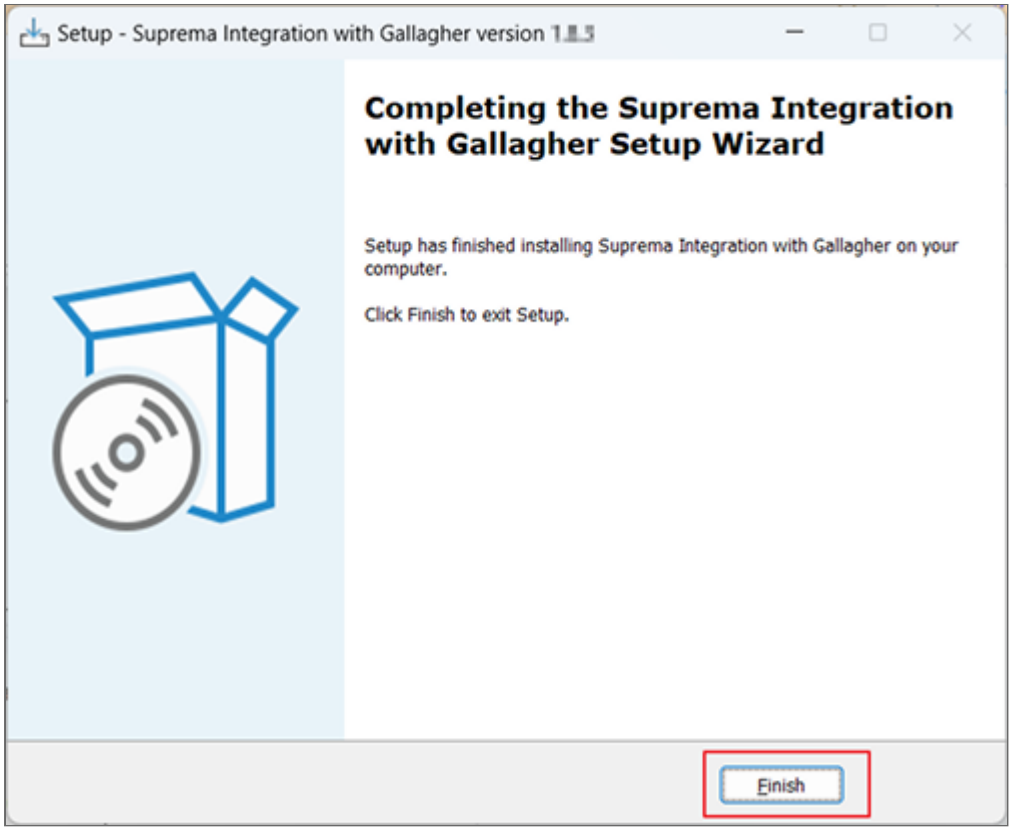


6. Press **OK**, for below pop-up.



7. We are done with the prerequisite installation press **Finish**.

> **Info**
> After installing the middleware, must restart the system once.

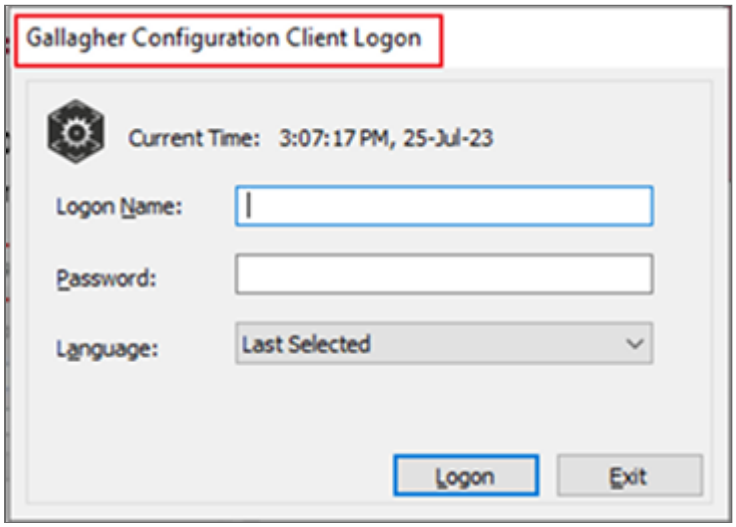


Configuration

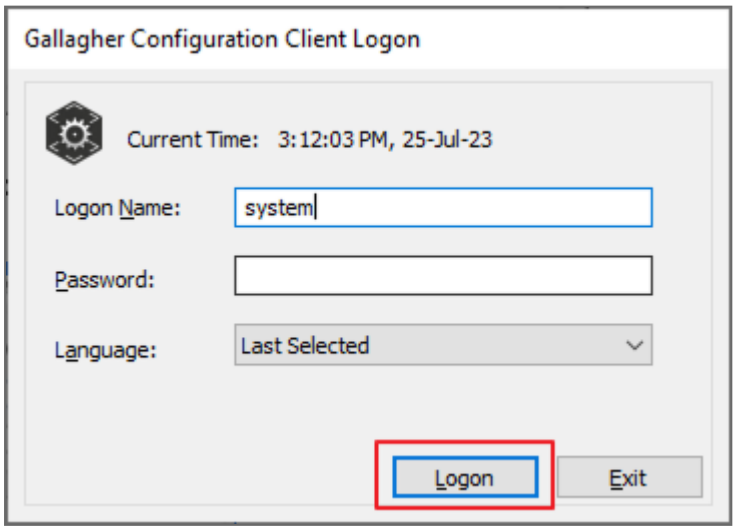
Gallagher Command Center Configuration

Gallagher Configuration Client Logon

1. **Click** The Start Menu & Open Configuration Client.



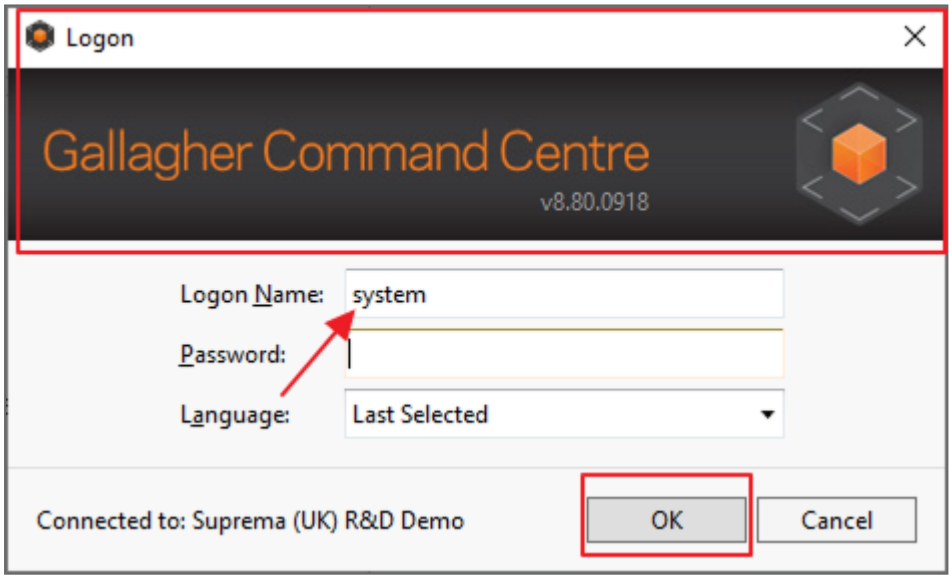
2. Set Logon Name as **system** password will be **none** and **press** the **Logon** button.



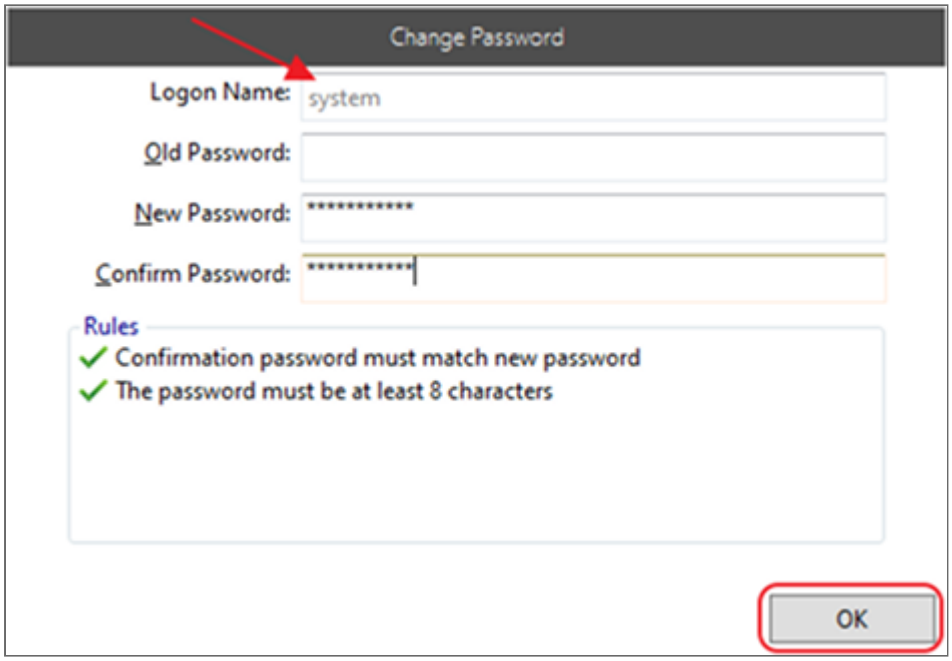
Gallagher Command Centre

> **Info**
> Process to generate Gallagher API Key.

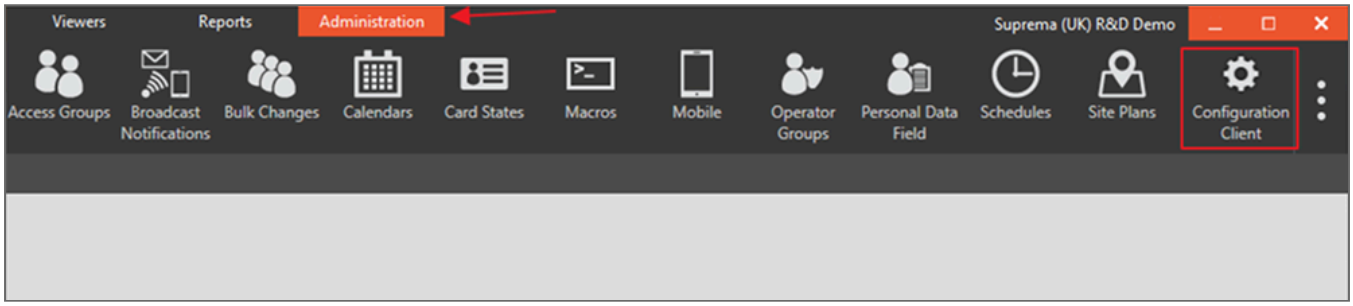
1. Open Gallagher Command Centre, set the Logon name as a system, and press the **OK** button.



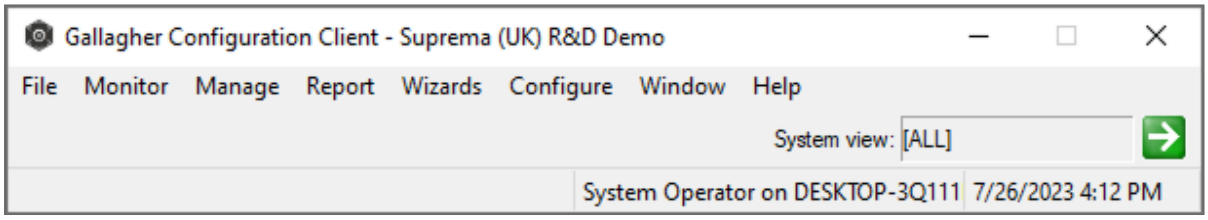
2. **Set** Logon Name as a **system** and set the password for Gallagher Command Centre and press **OK**.



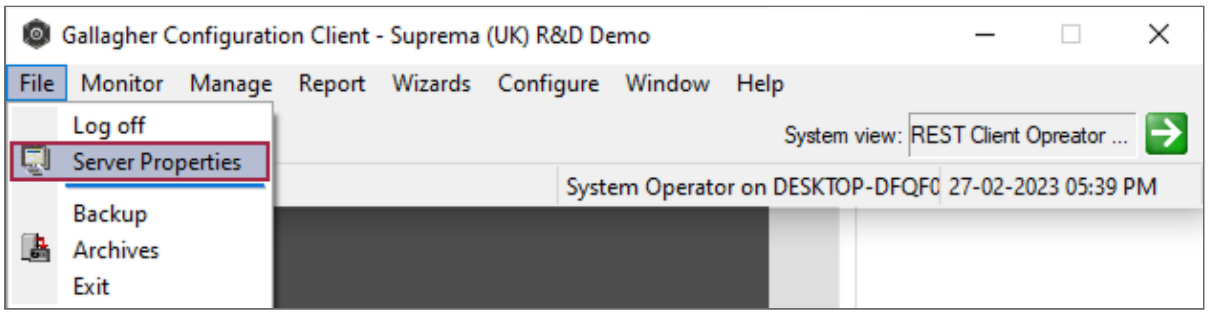
3. Now, go to Administration from the top left corner and **select** Configuration Client, the window will be open.



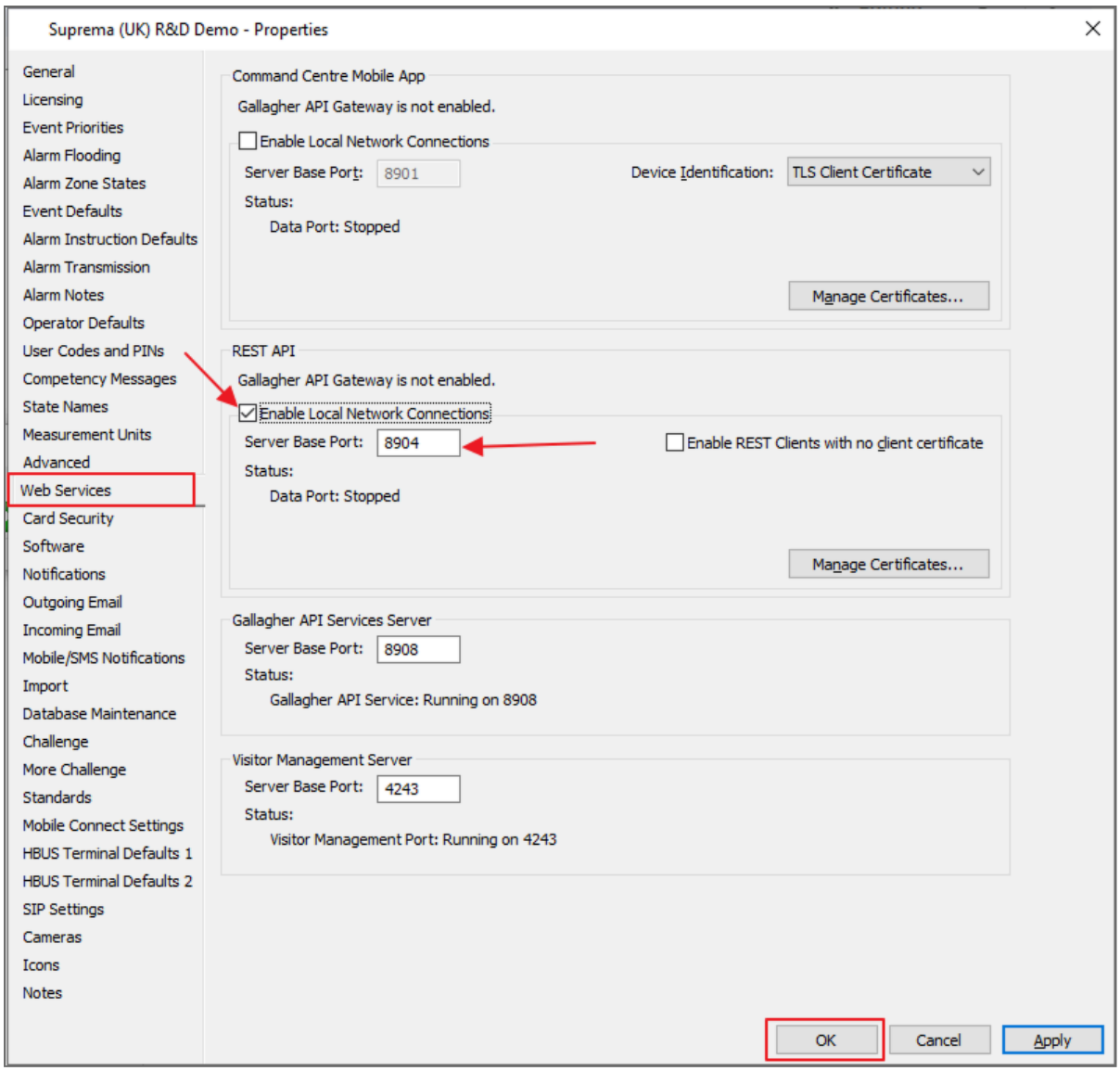
4. The below tab will be open.



5. To configure server properties, **Select File** → **Server Properties**.

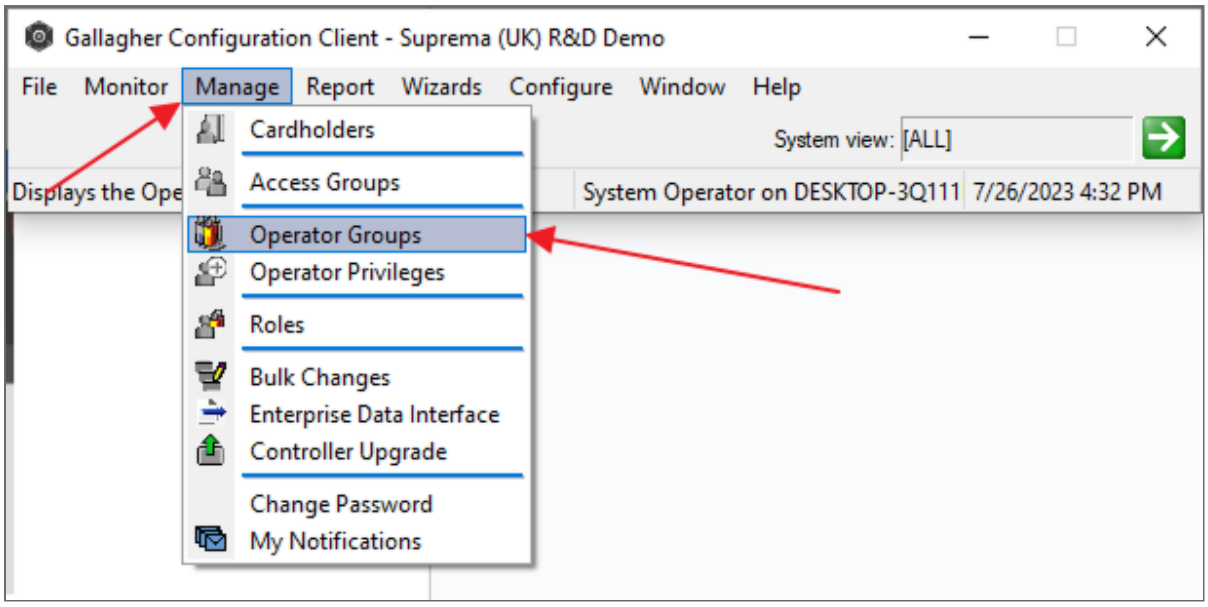


6. The new window will open, now go to **Web Services**, in the **REST API** section, enable local network connection, **set** the server port as **8904**, **uncheck** the Enable REST client with no client certificate, and **press** the **OK** button.

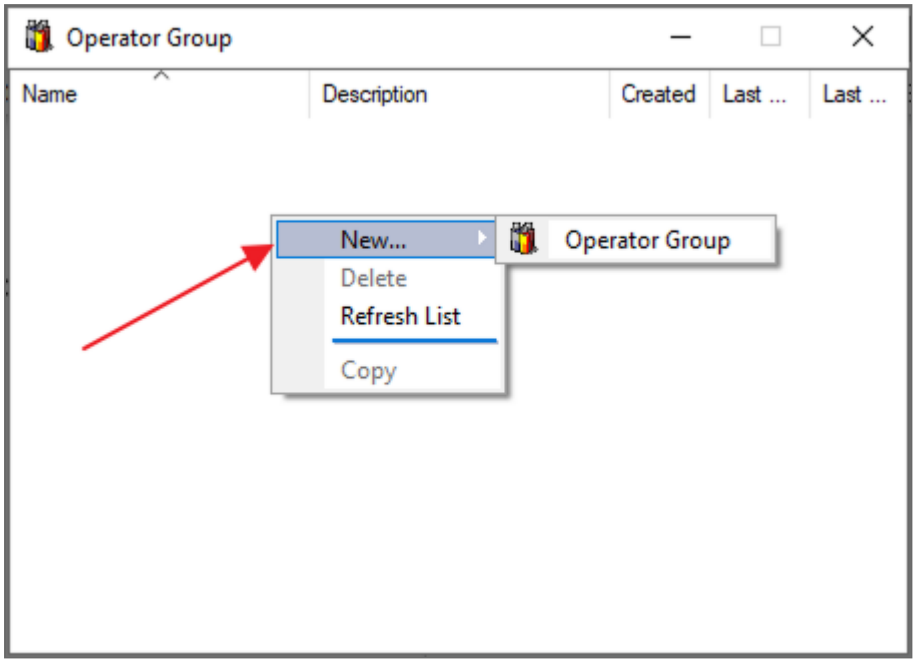


7. **Click** over to **Gallagher Client**.

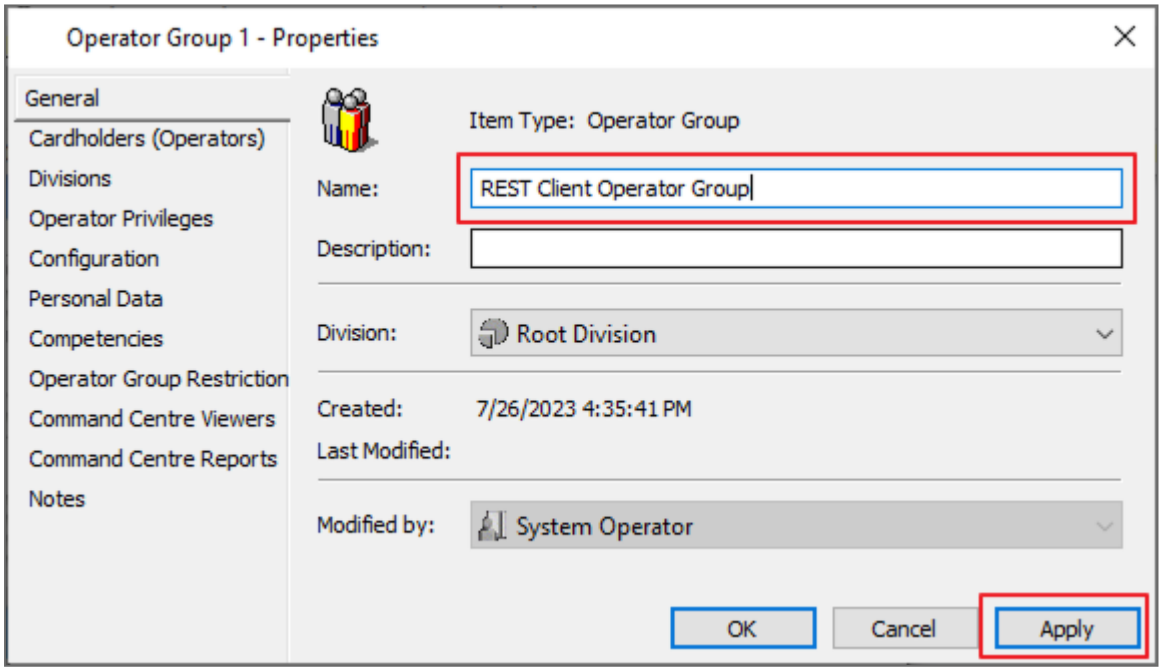
Click on **Manage.** Within the Dropdown, please **select Operator Groups.**



8. The Operator Group window will open, **press right-click** and select **New → Operator Group.**

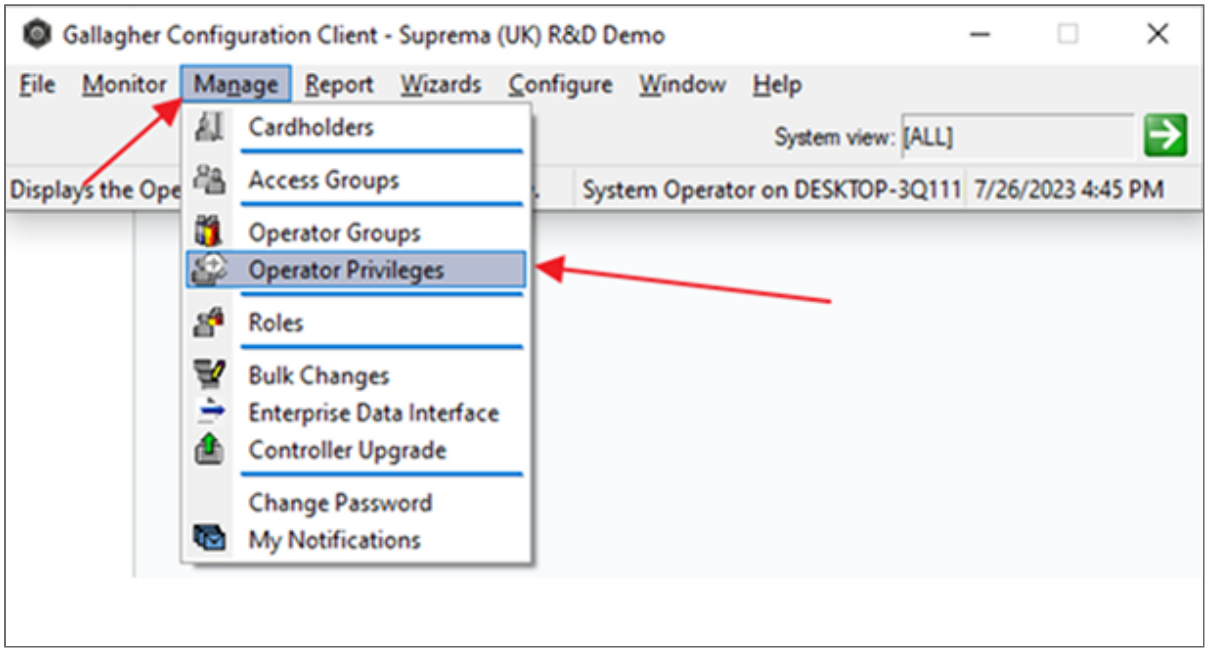


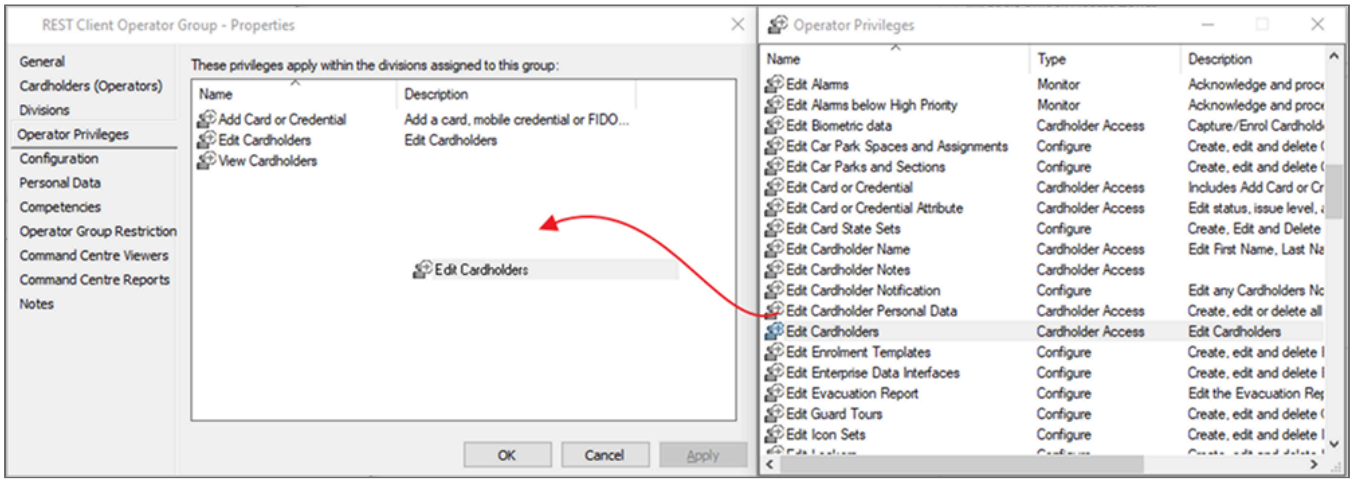
9. In the general setting, the name should be **set** as **REST Client Operator Group**. Then click **Apply.**



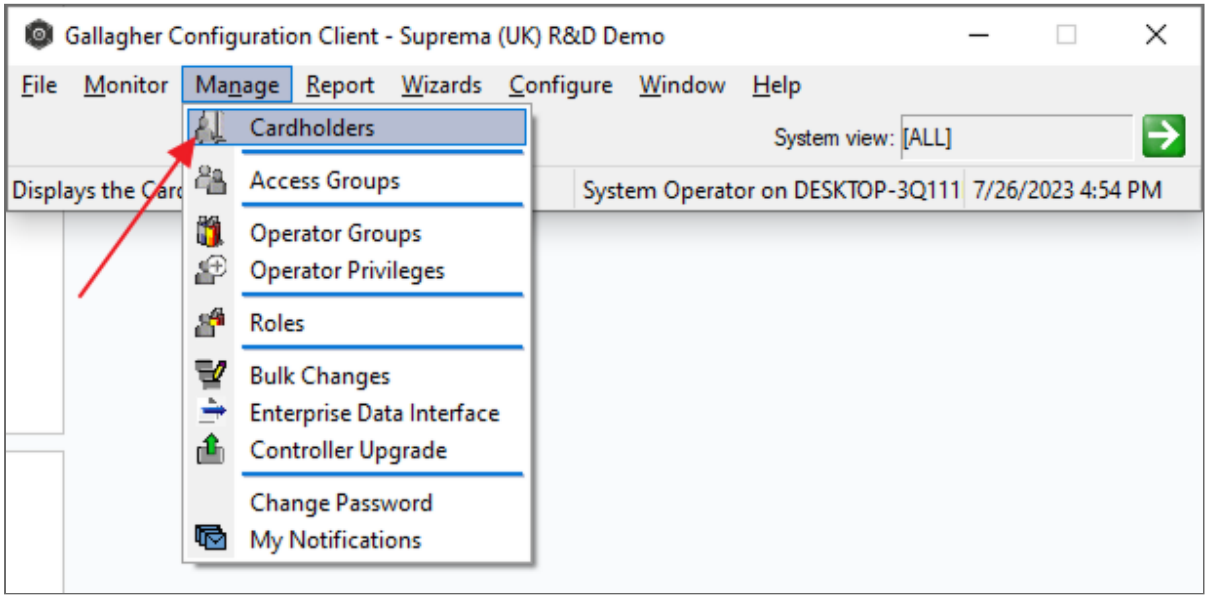
10. Now **select** the **Operator Privileges** setting on Operator group and go to the Gallagher configuration client window Manage → Operator Privileges. Now **drag and drop**.

    You need to add 3 privileges to the Operator Group (Add Card or Credential, Edit Cardholders, View Cardholders) from operator privileges to operator group and **press** the **OK** button, and **close** the operator privileges.

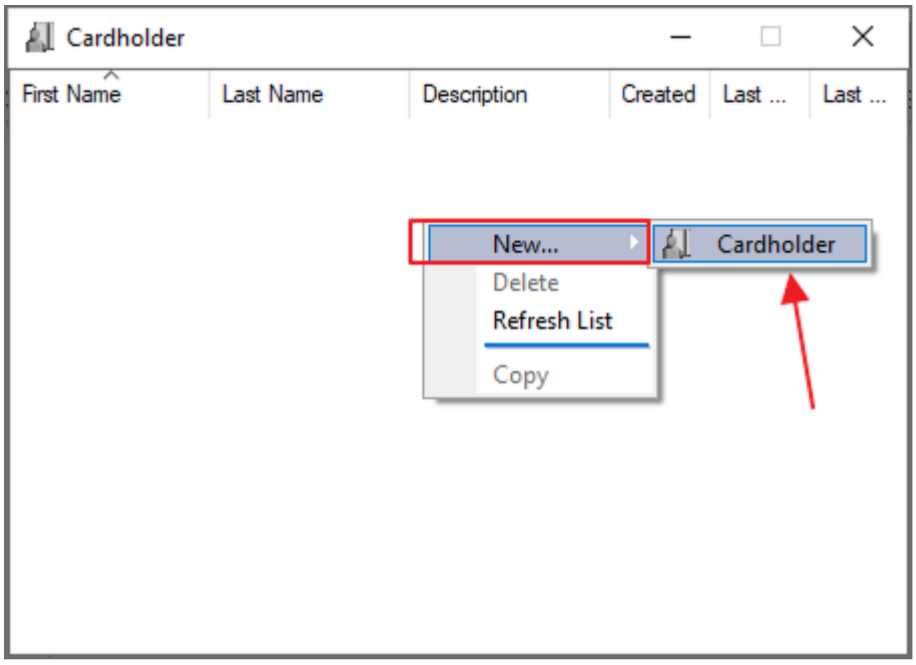




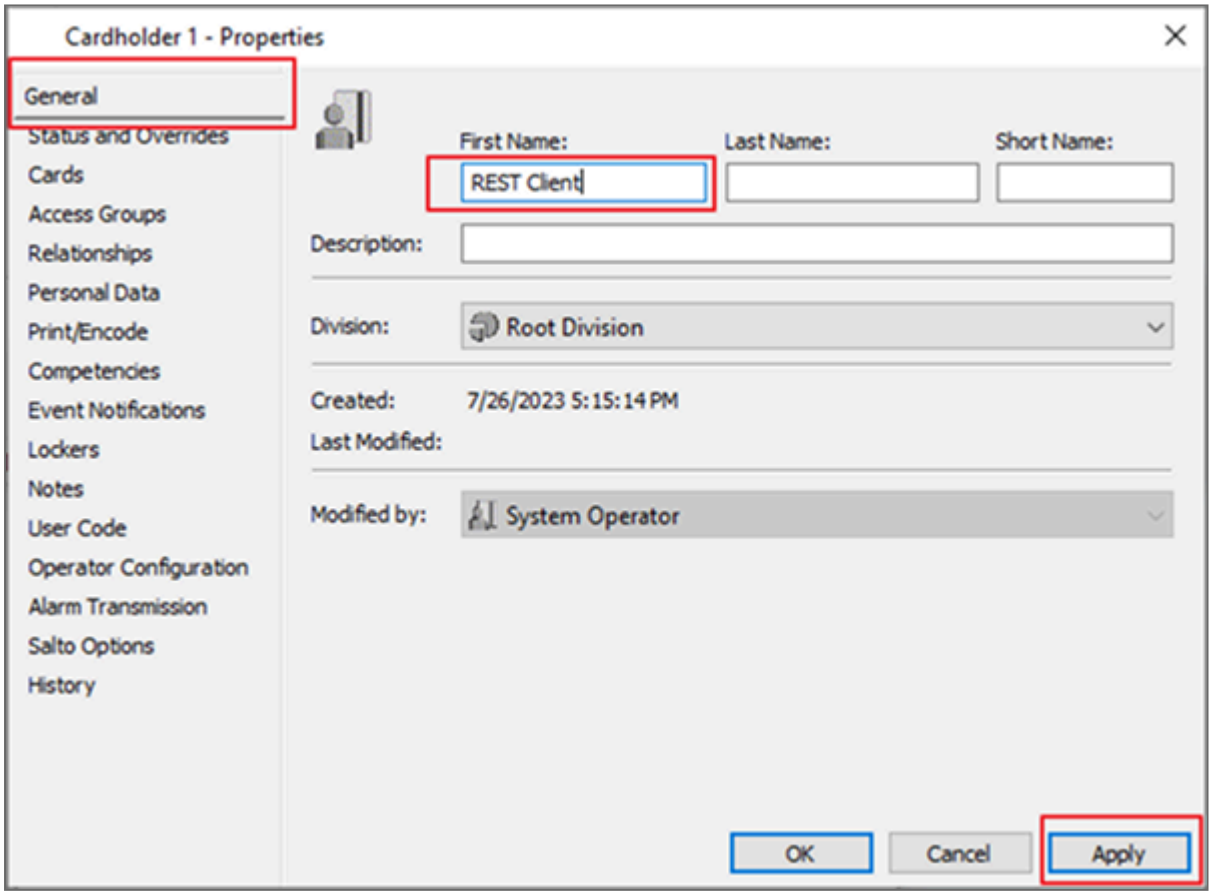
11. Go to Configuration Client and **select Cardholders.**



12. **Press right-click** New → Cardholder.

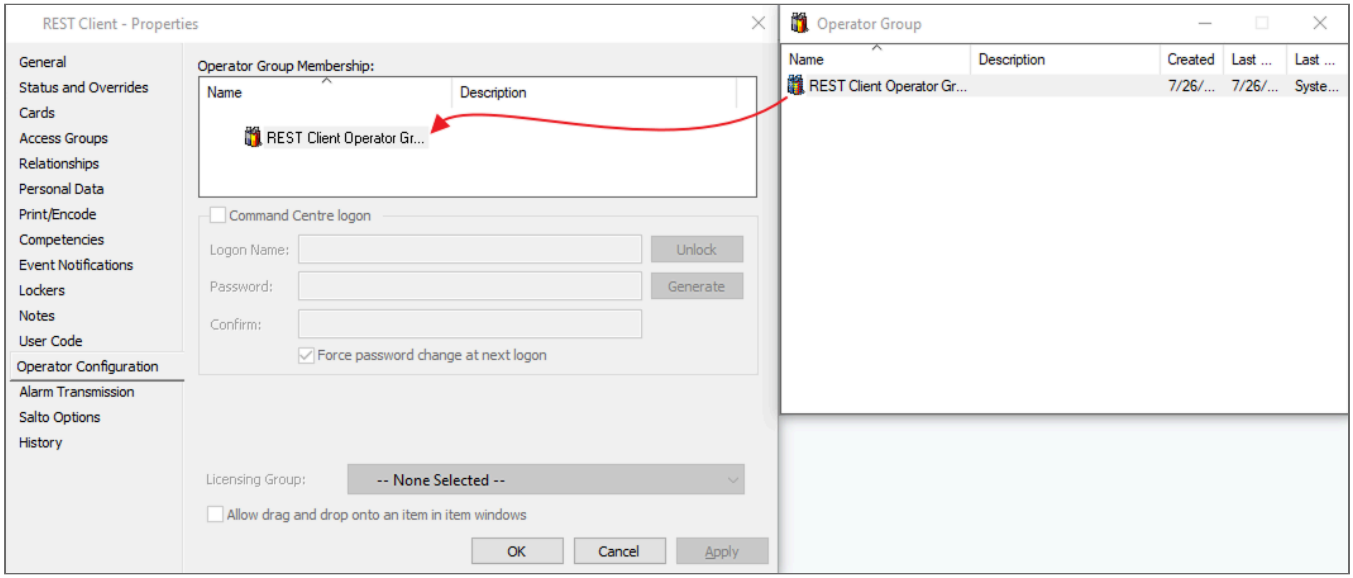


13. In the general setting, the First Name as **REST Client**, and **press Apply.**

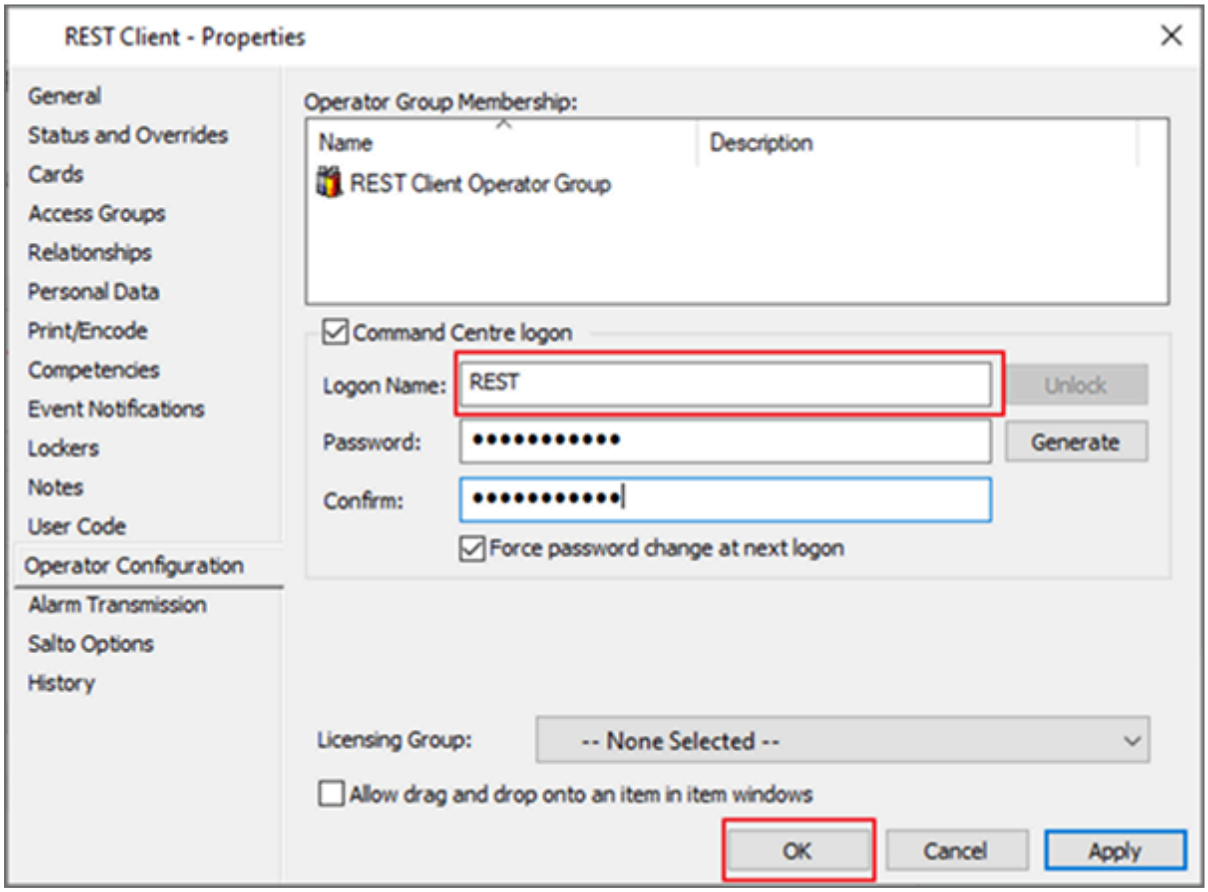


14. **Click** on the **Operator Configuration** tab on the left side within the REST Client Properties. **Drag and Drop** the REST Client operator group that we have created from Operator Group to Operator Group Membership.

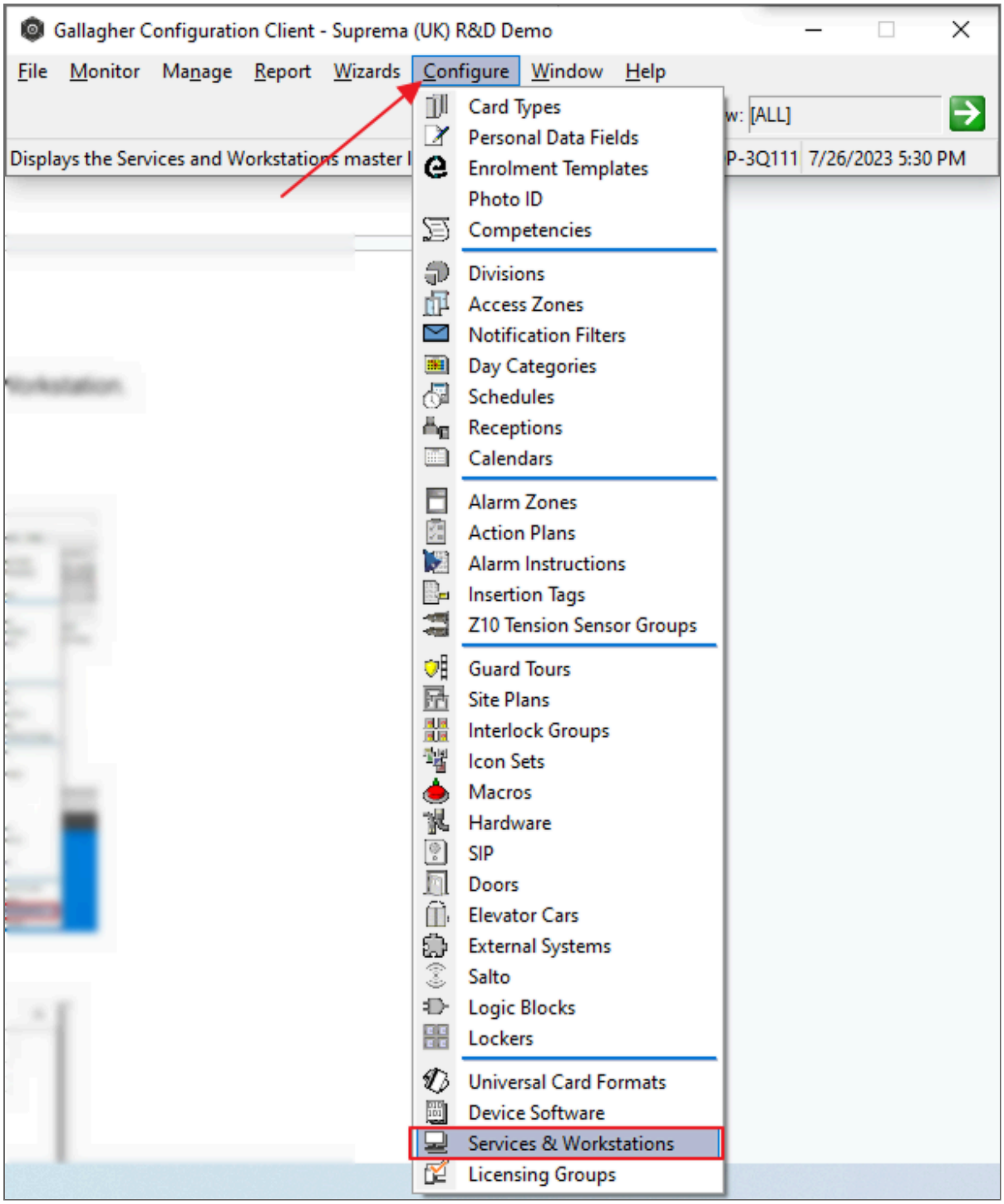
15. **Drag** the REST Client Operator Group over to Operator Group Membership: like the image below:



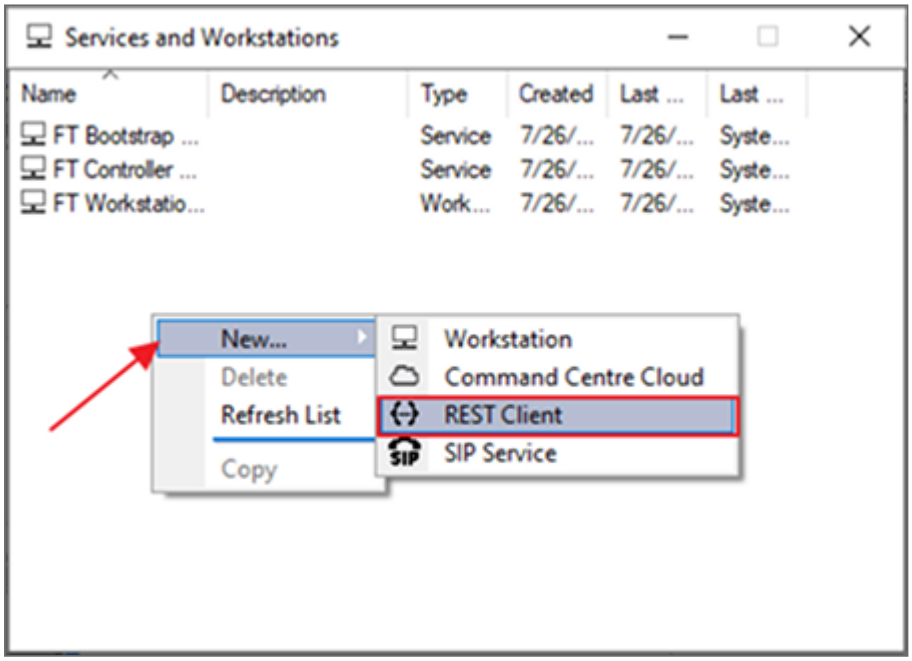
16. **Set** the Logon name to **REST** and **set** the password the same as we set for Gallagher Command Centre. **Click OK**, and also **Close** the Operator Group window.



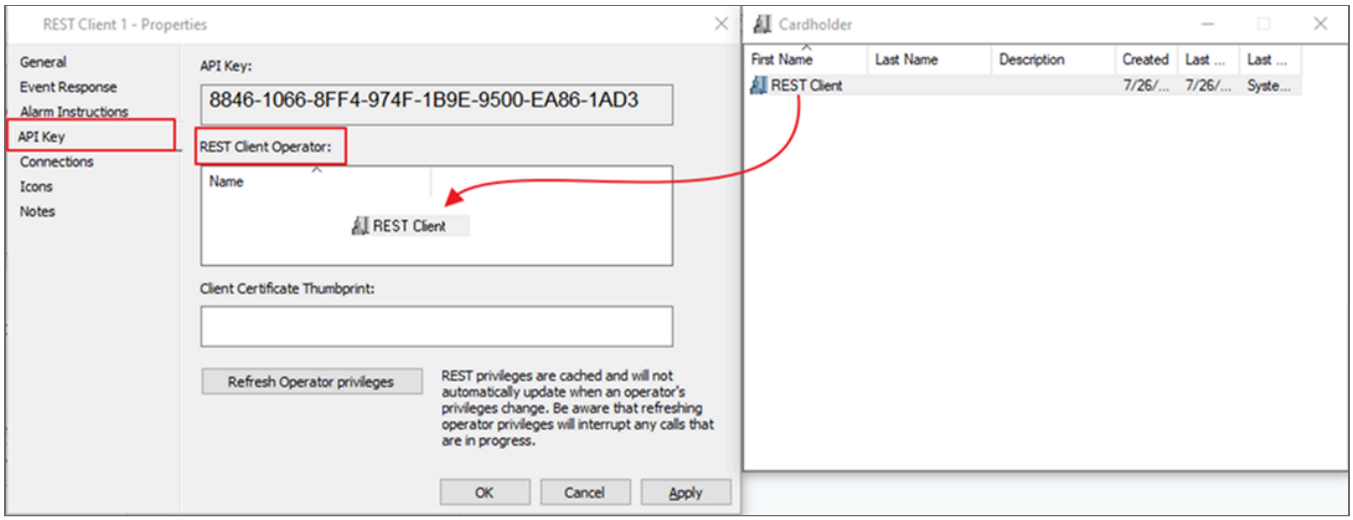
17. On **Configuration** Client go to Configure → Services & Workstations.



18. Now **right-click** New → REST Client.

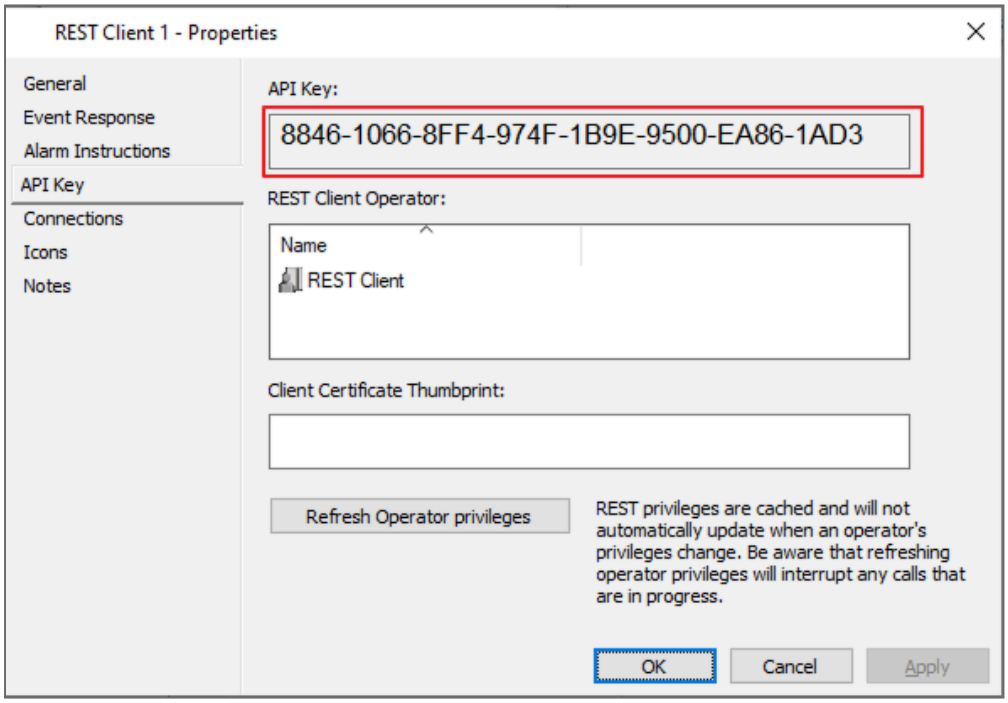


19. In the API key section **Drag and Drop** the REST Client from Cardholder to REST Client Operator. **Click Apply**. **Close** the Cardholder window.



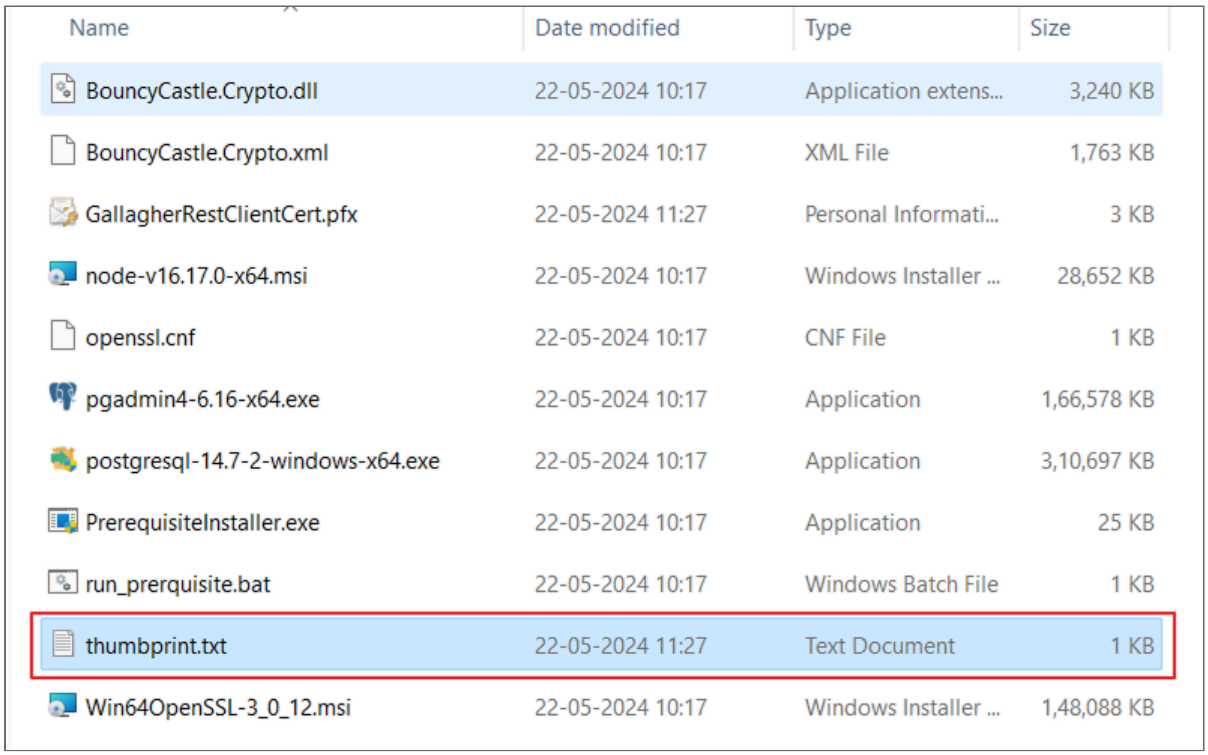
20. The Gallagher API key is there, in the API key section.

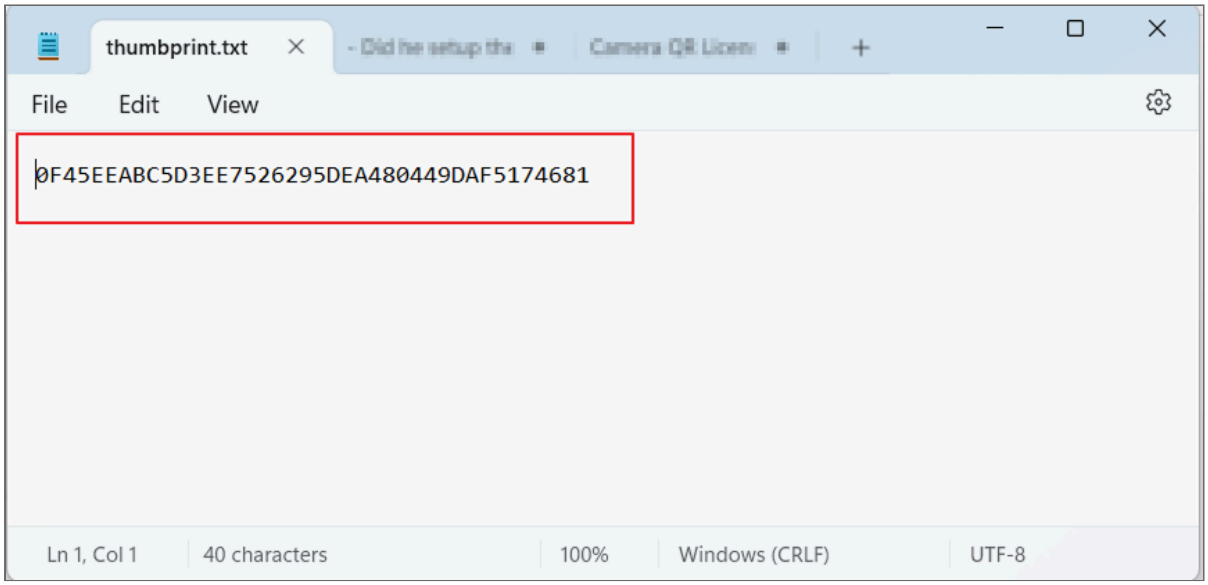
> **Info**
> Save the Gallagher API Key in a safe place.



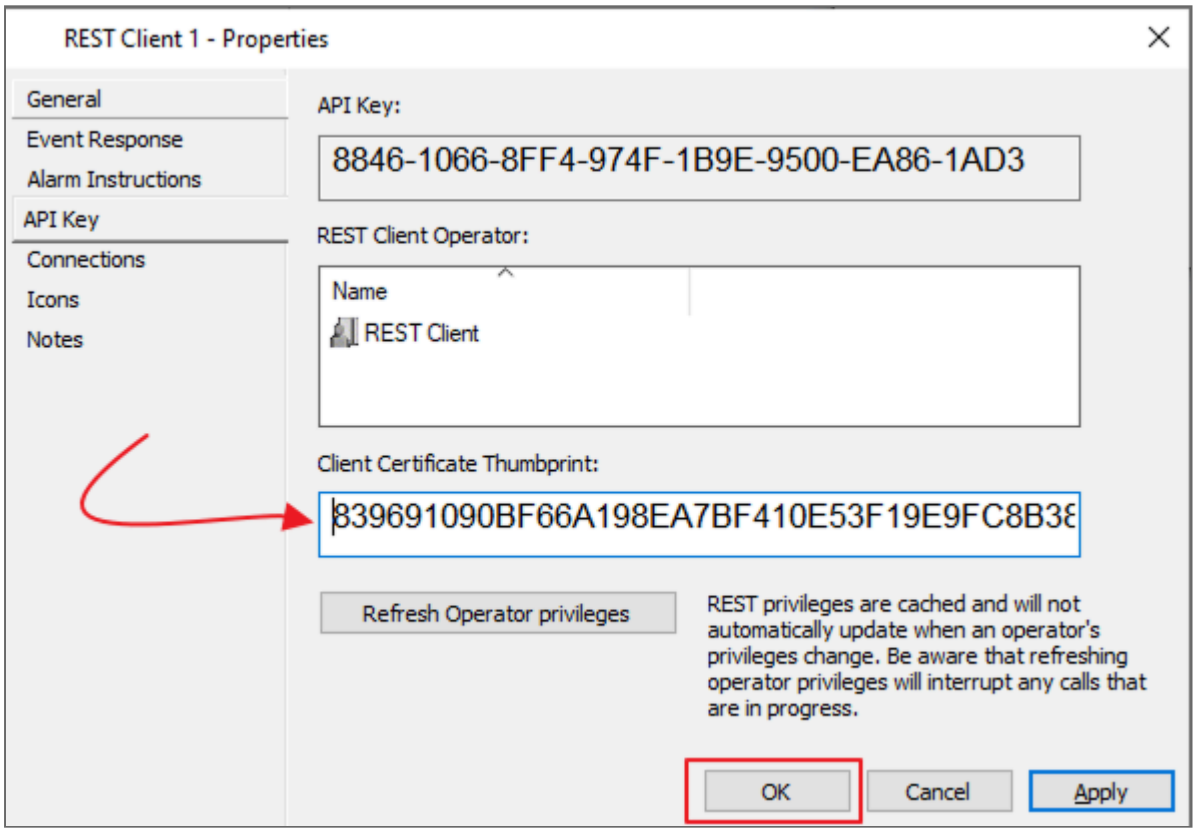
21. To get the thumbprint, go to the `C:\Program Files\Suprema Integration with Gallagher\Prerequisites`, open the thumbprint file, and copy the value of the thumbprint inside it.

> **Info**
> If the thumbprint file is missing. If thumbprint is not generated while running the EXE file.





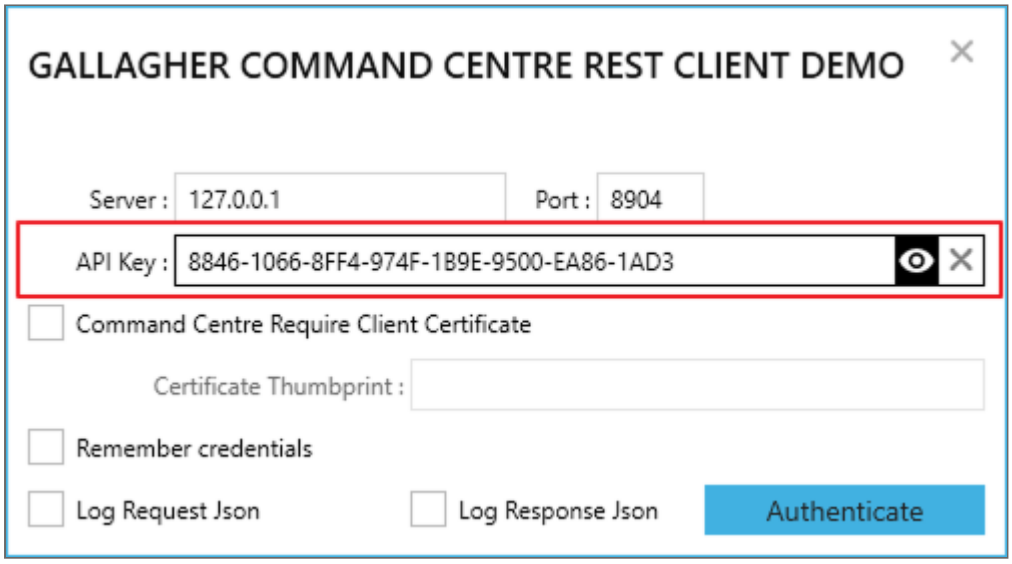
22. **Copy** the thumbprint and **Paste the Client Certificate Thumbprint key** into the Client Certificate thumbprint section **press** the **OK** button and also **Close** the Services and Workstations.



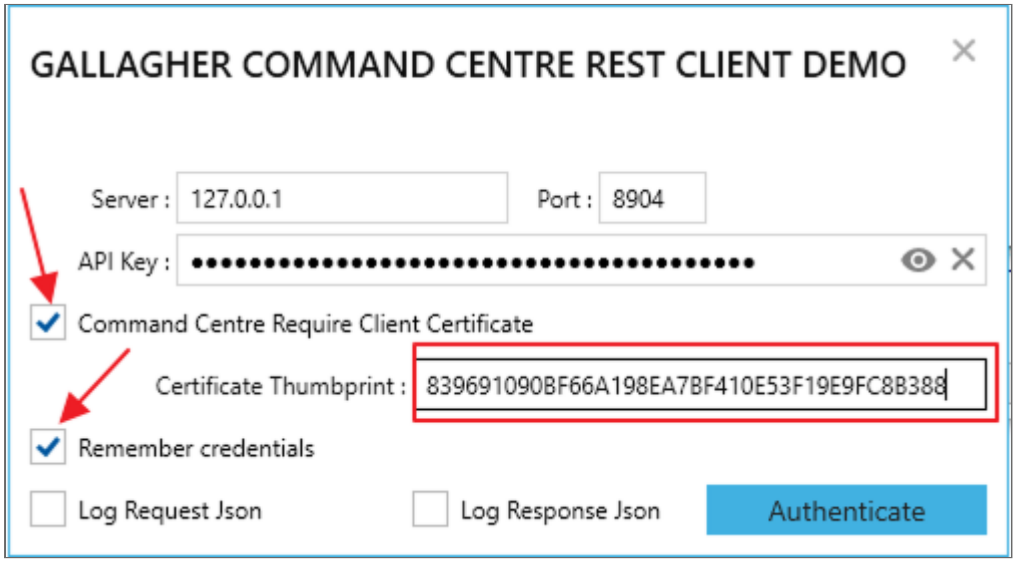
Check the Gallagher API Key

1. Go to Command Centre iso → utilities → REST API → RestClient_v8.60.072 → win-x64 → RestClientDemo, **move** that to the desktop, and **open** the `RESTClientDemo.exe`.

2. **Enter** the Gallagher API key as shown in image.

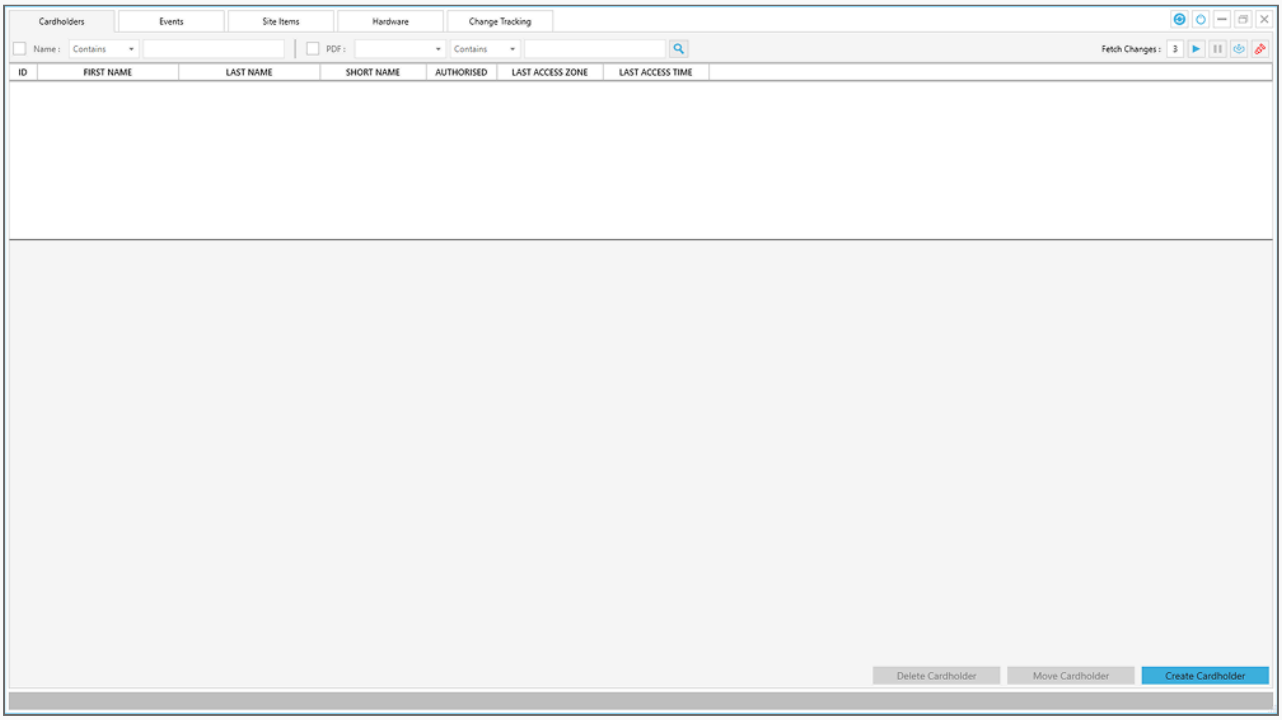


3. **Tick** the Command Centre Requirement Client Certificate and fill in the Certificate Thumbprint, also **tick** the Remember credentials (Optional).



Info

If there is an error it will show in the terminal else a new screen will open as shown in the below image. And after testing you can close this window.



Hardware configuration

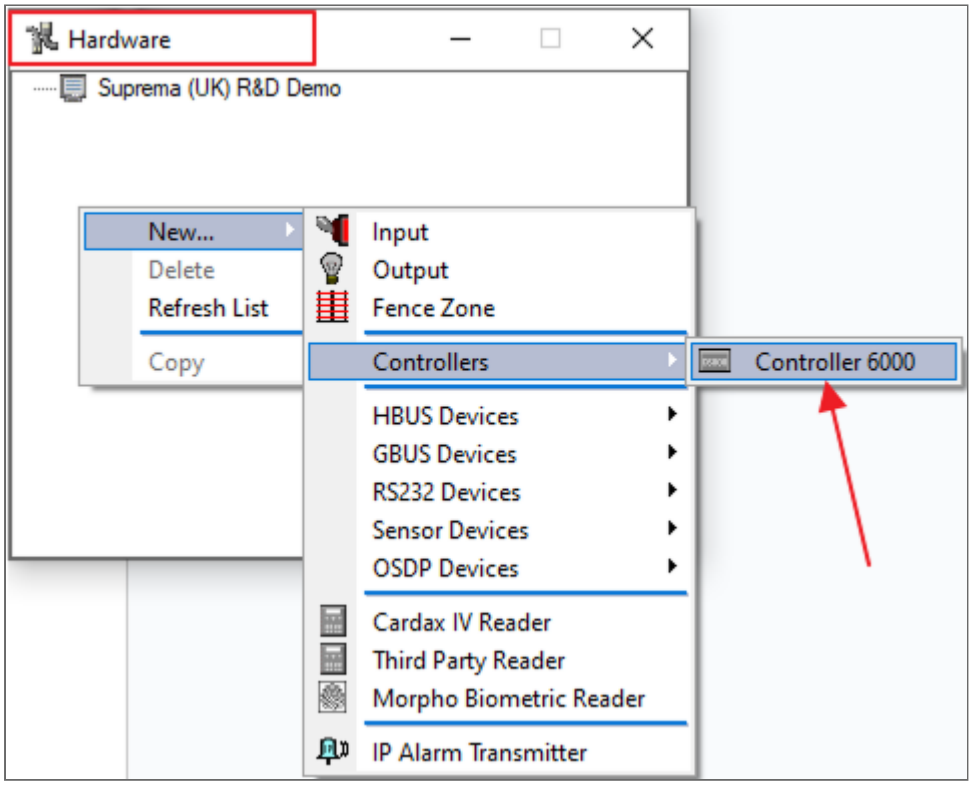
Info

- Skip to BioStar 2 Setup if the hardware has already been configured.
- We are using controller 6000 as a reference, if you have another controller please do the steps accordingly.

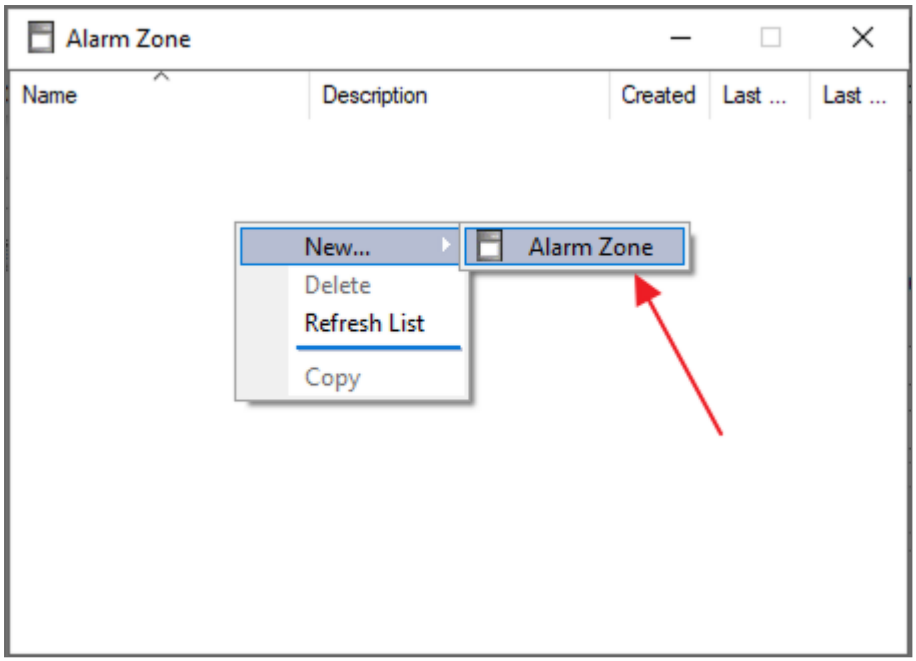
1. First, we have to create controller 6000 (or any other controller you have) to **connect** to the Gallagher controller.

   Open the Gallagher Configuration Client window and go to Configure → Hardware.

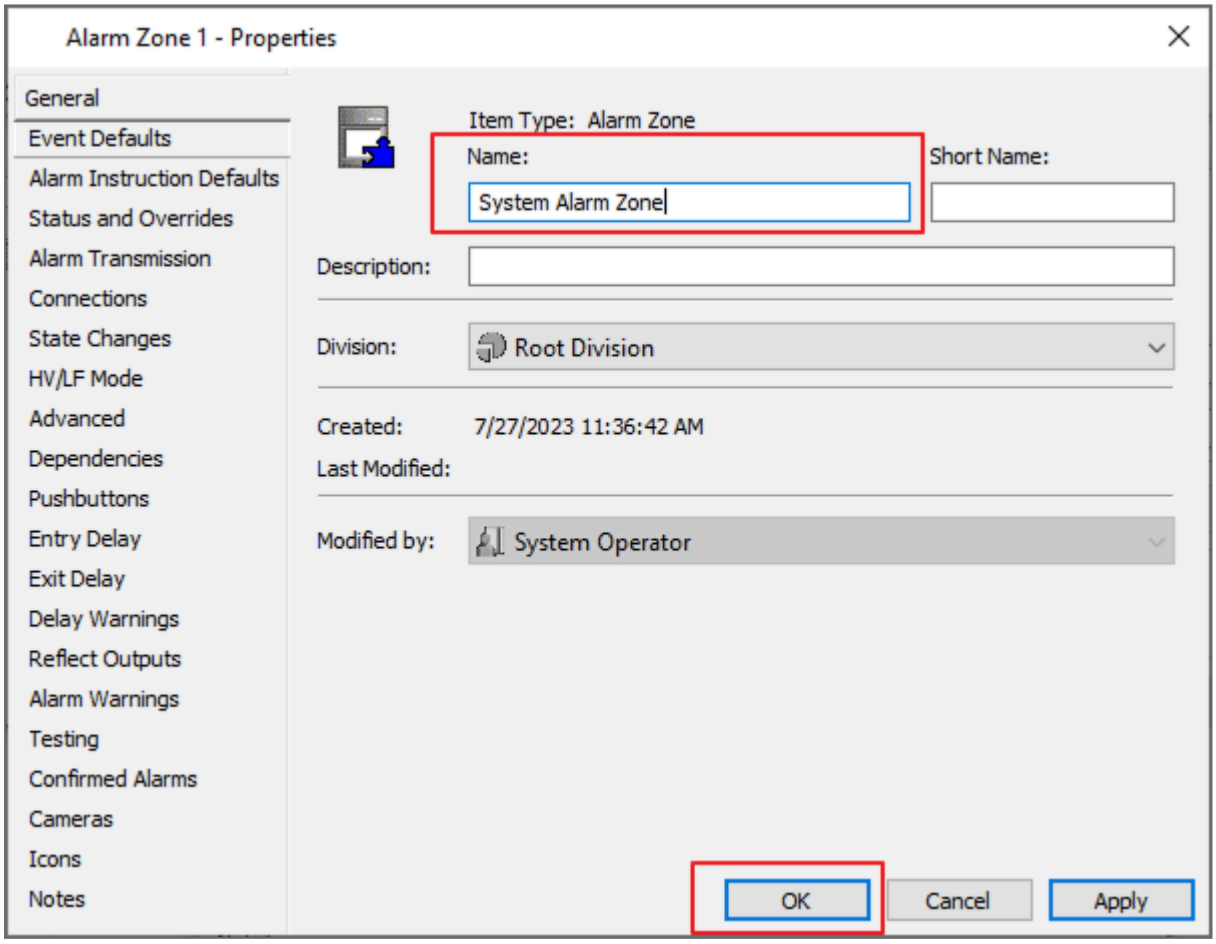
2. In the hardware window press **right-click** then **New** → **Controllers** → **Controller 6000** (if you have a different controller it will display here) and **press apply**. It will create a controller in hardware.



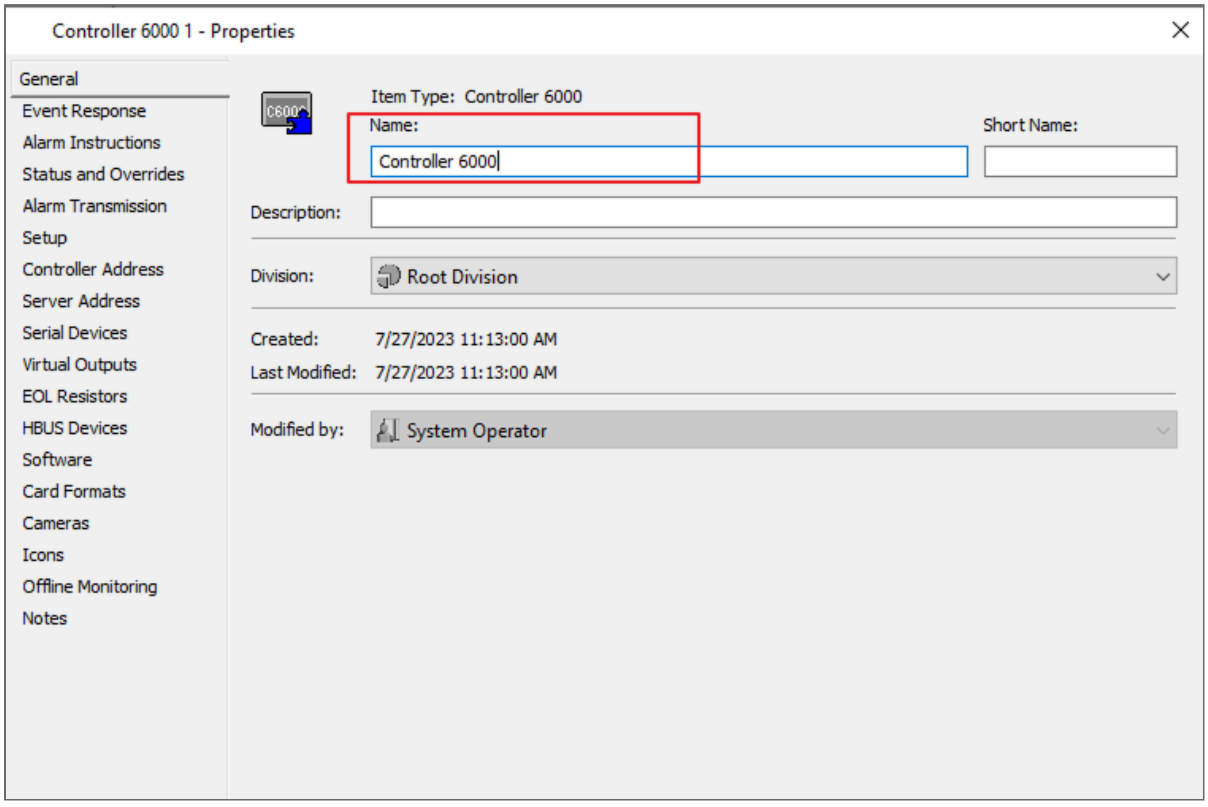
3. Then **go back** to Gallagher Configuration Client and go to configure → Alarm Zones and press **right-click** to create a new alarm zone.



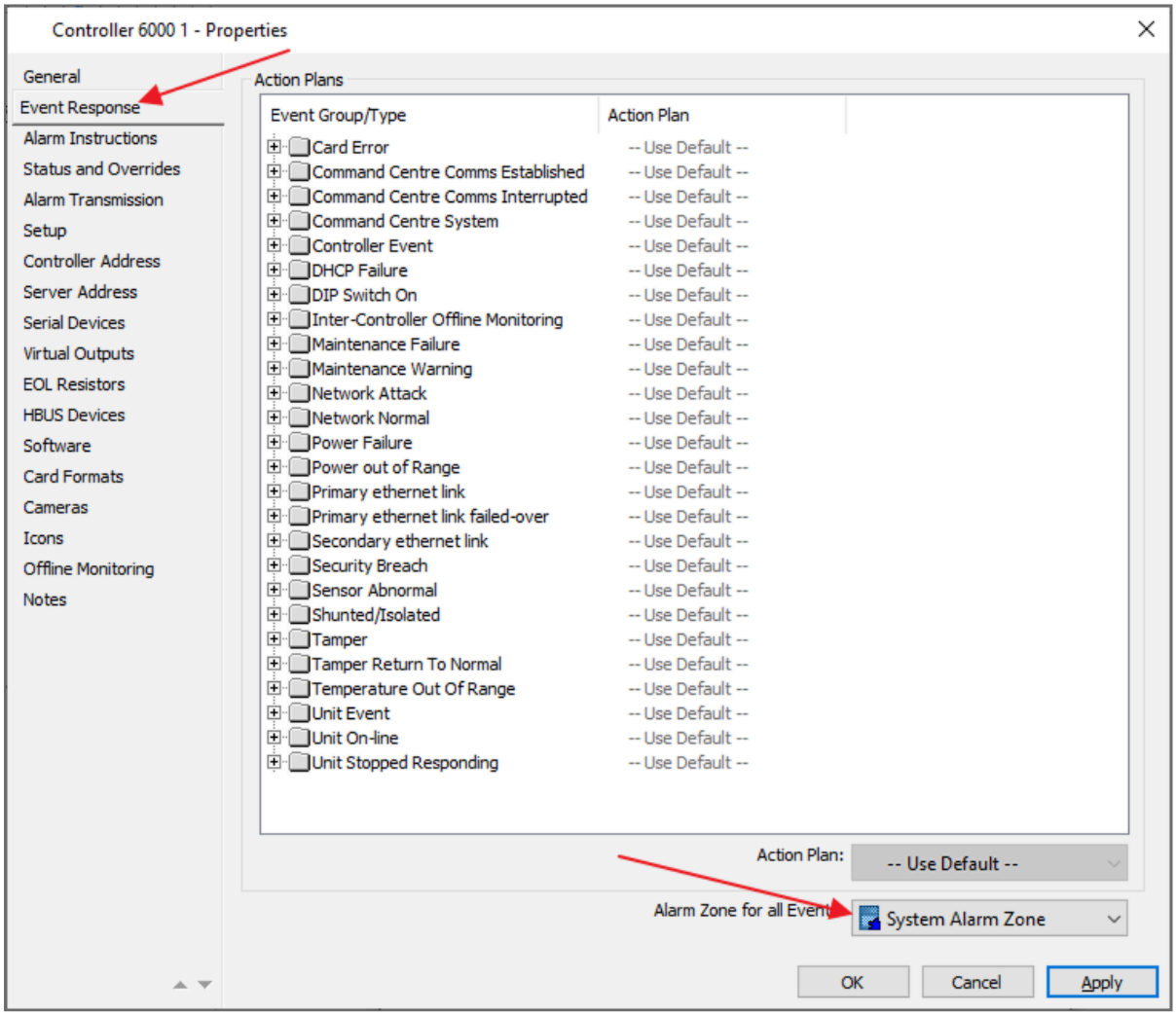
4. To configure the Alarm zone in General settings change the name to **System Alarm Zone** and **press** the **OK** button.



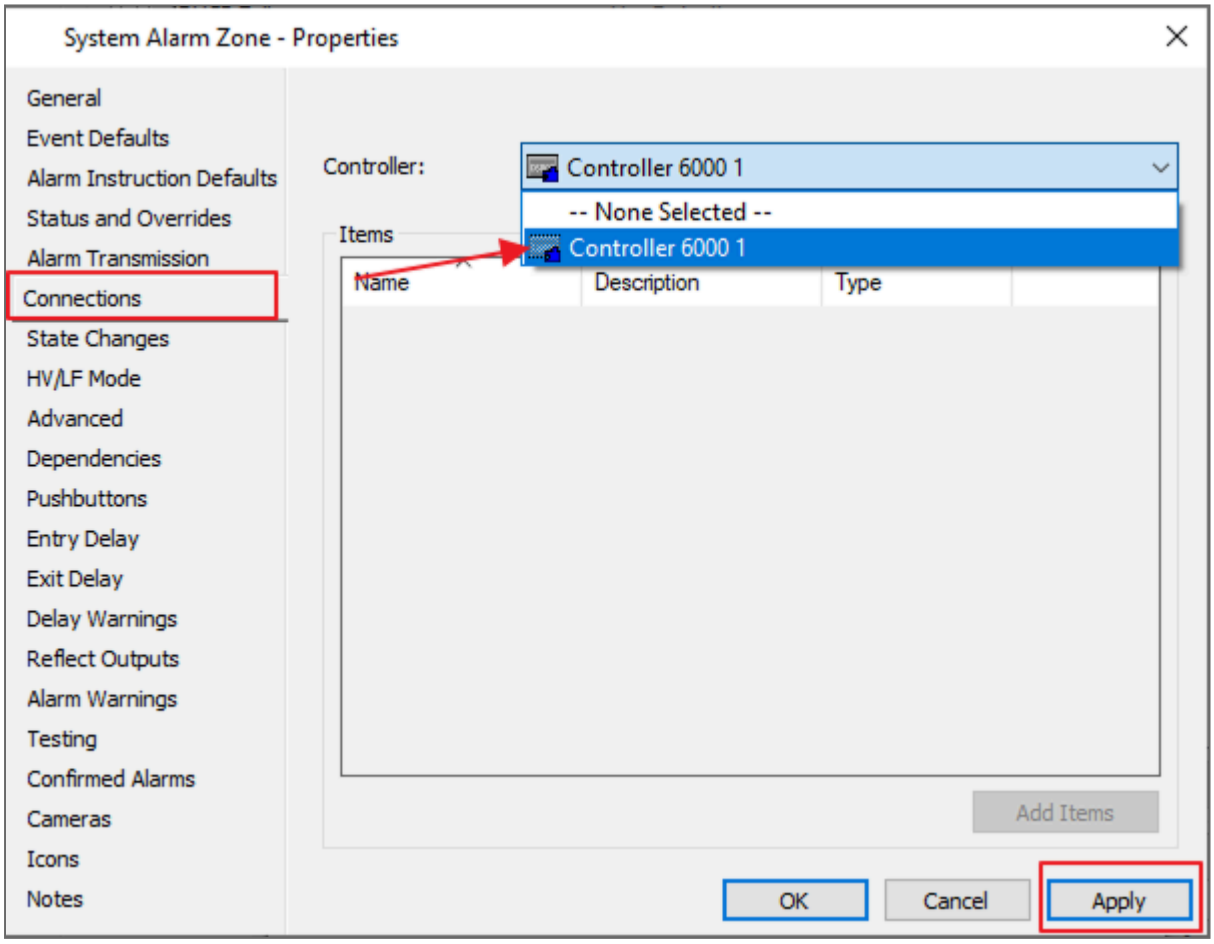
5. Let's configure Controller 6000, In the General setting **set** the name as **Controller 6000** (set name same as your controller).



6. Now **go to** Event Response and select Alarm Zone for all events and select **System Alarm Zone**. And **press** the **Apply** button.

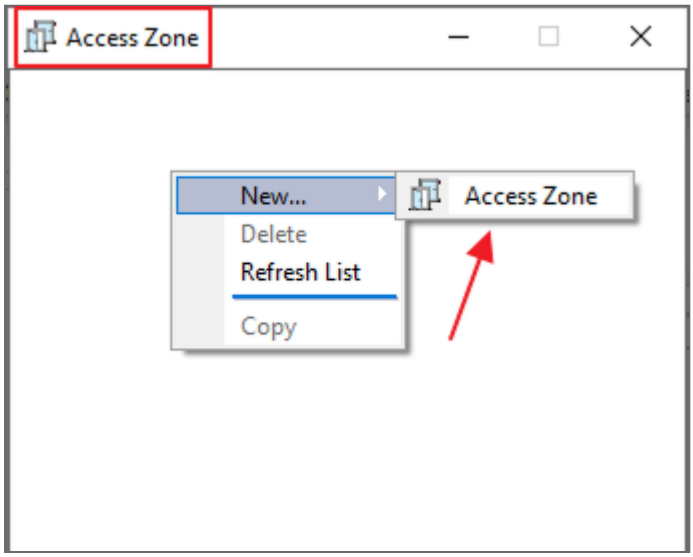


Now go to System Alarm Zone Properties and **select** Connections and in the controller dropdown **choose Controller 6000**. **Press** the **OK** button and **close** the Alarm Zone window.

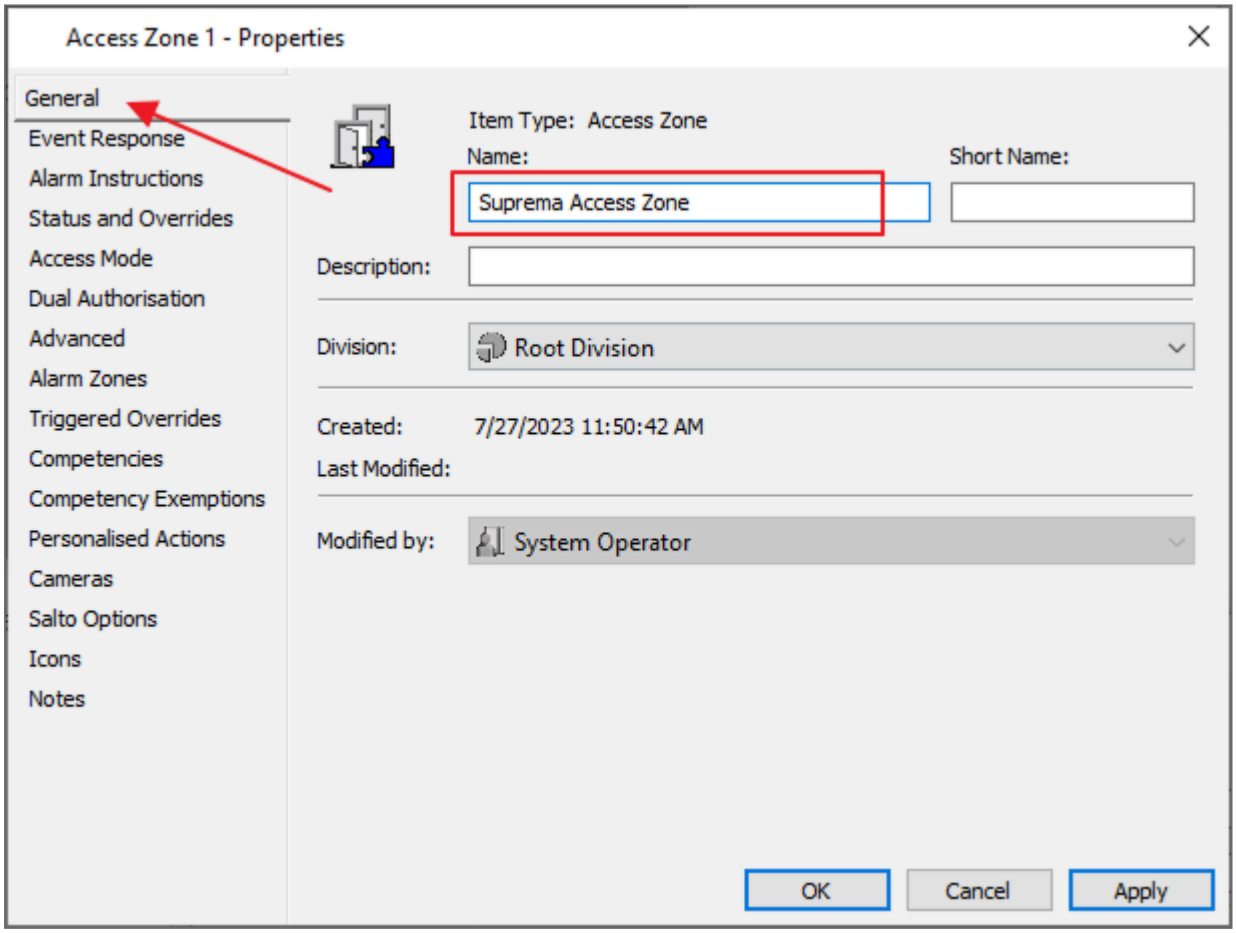


7. Now, we have to **create** an Access Zone in configure.

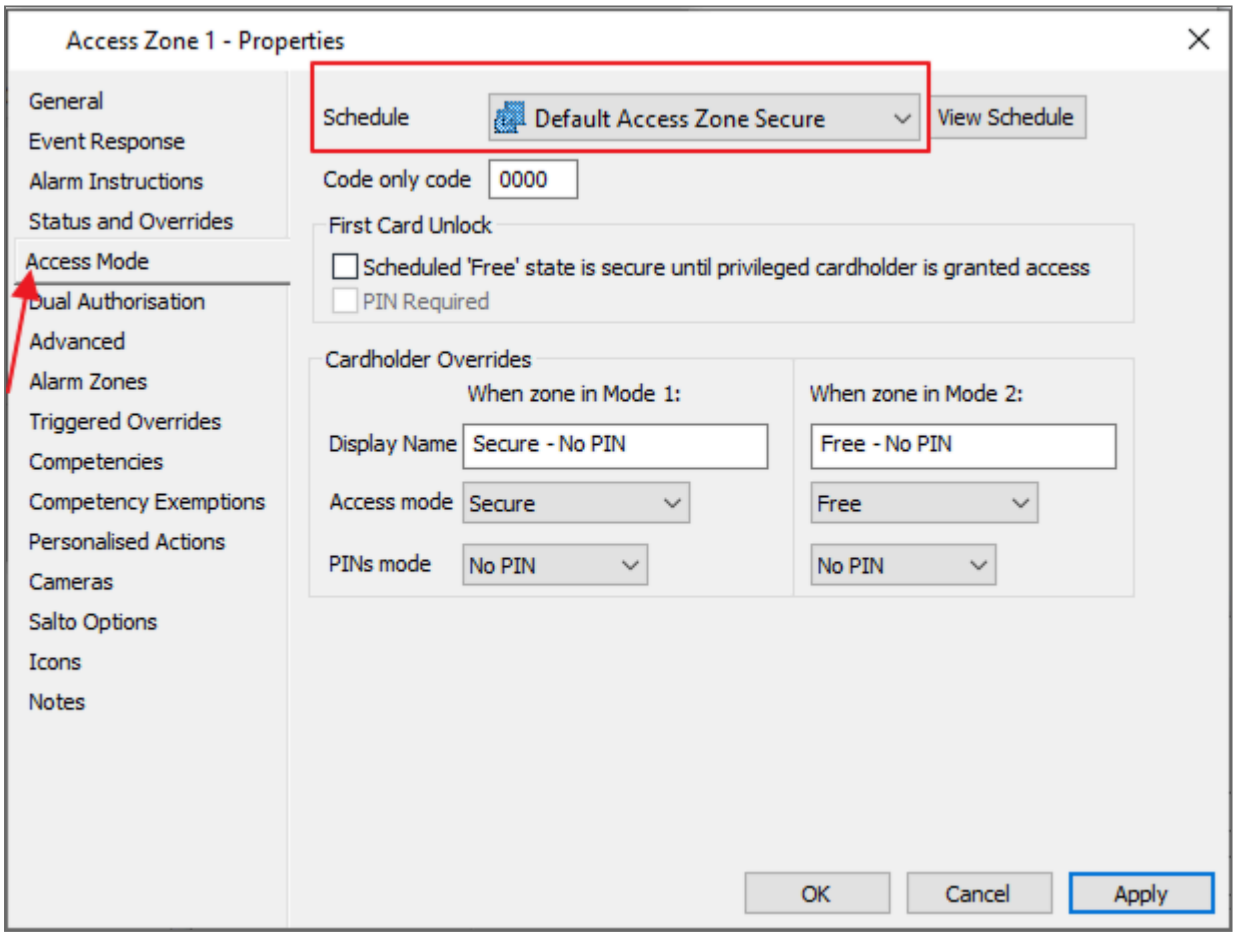
   Go to the Access Zone and the window will open up. Now **press right-click** in the Access Zone Window and **Select** New → Then **click** on Access Zone, and it will create an access zone.



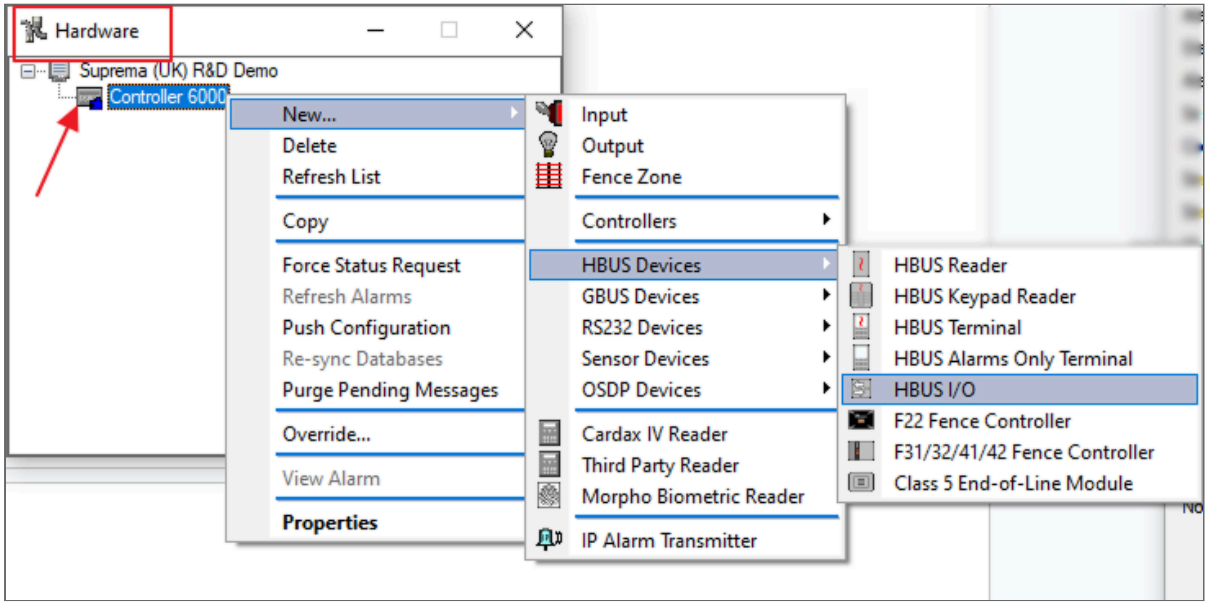
8. **Open** the Access Zone Properties that we have created in the General Setting. Then **set** the name as **Suprema Access Zone**.



9. **Go to** Access Mode Tab Setting. **Select** Schedule as Default Access Zone Secure and **press** the **OK** button.

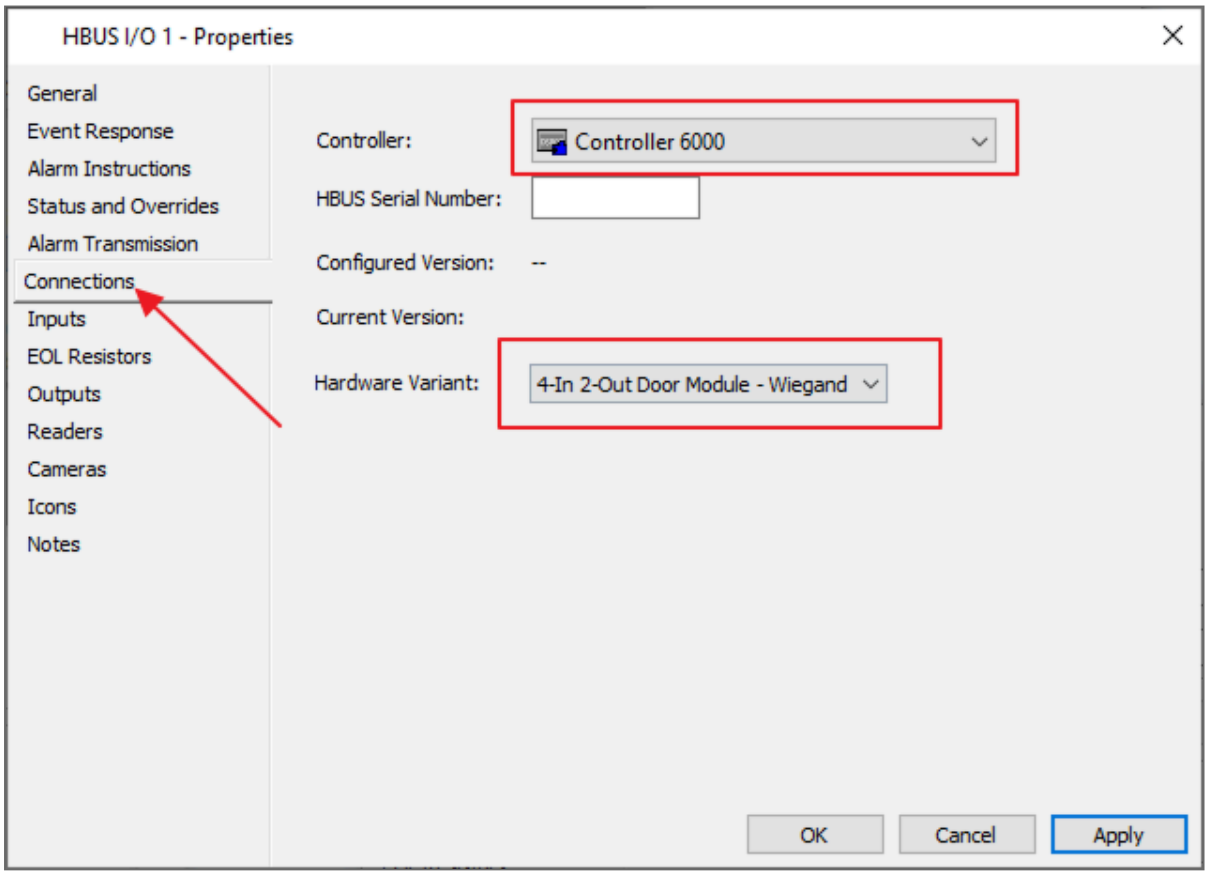


10. Now **go to** the Hardware Window then **right-click** on Controller 6000. Select New → HBUS Devices → HBUS I/O. This step will create HBUS under Controller.

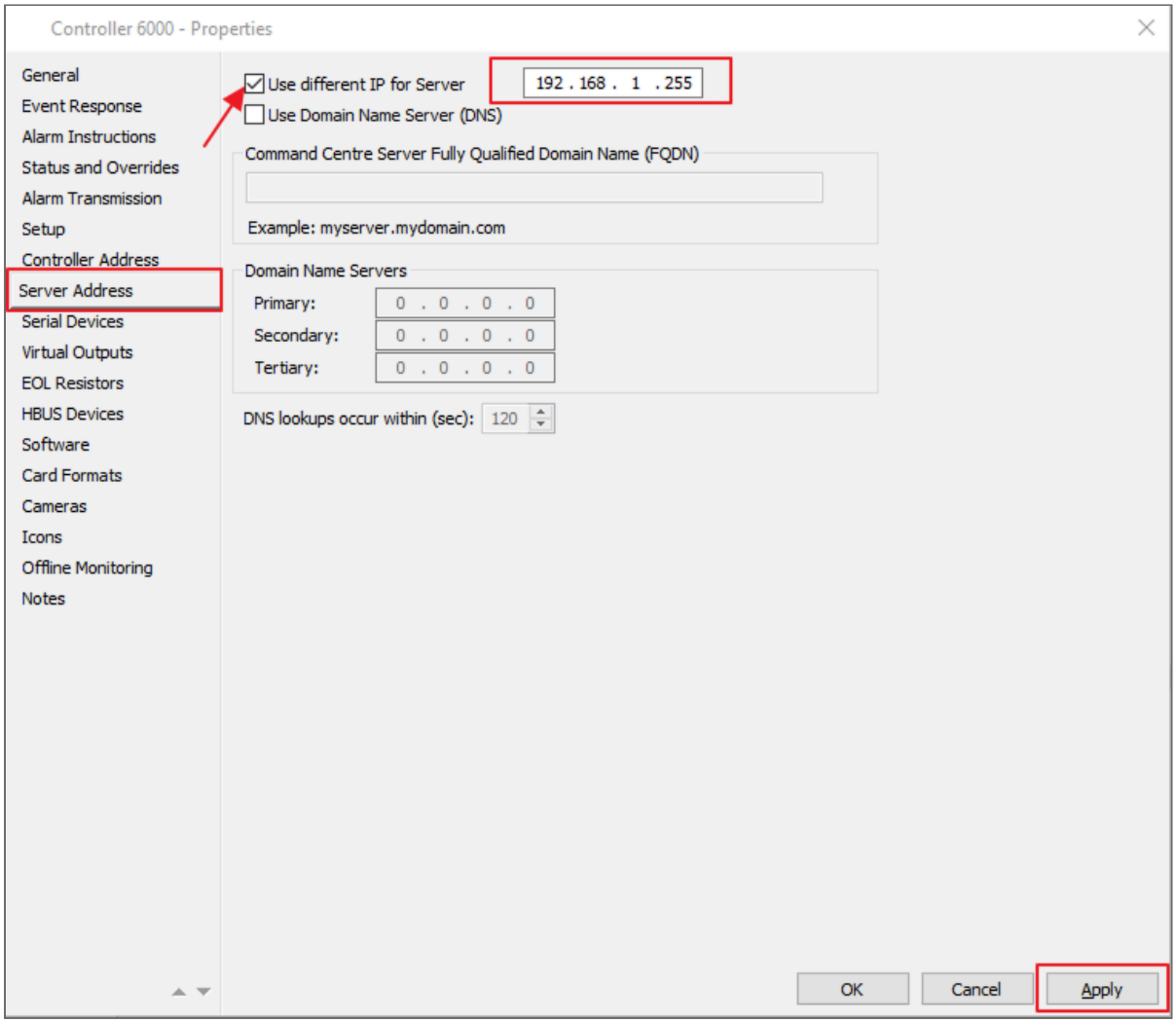


11. Let's Configure the HBUS that we have created by **double-clicking** on it to edit the properties. In the general setting, **set** the name as **HBUS I/O Wiegand Module (Suprema)**.

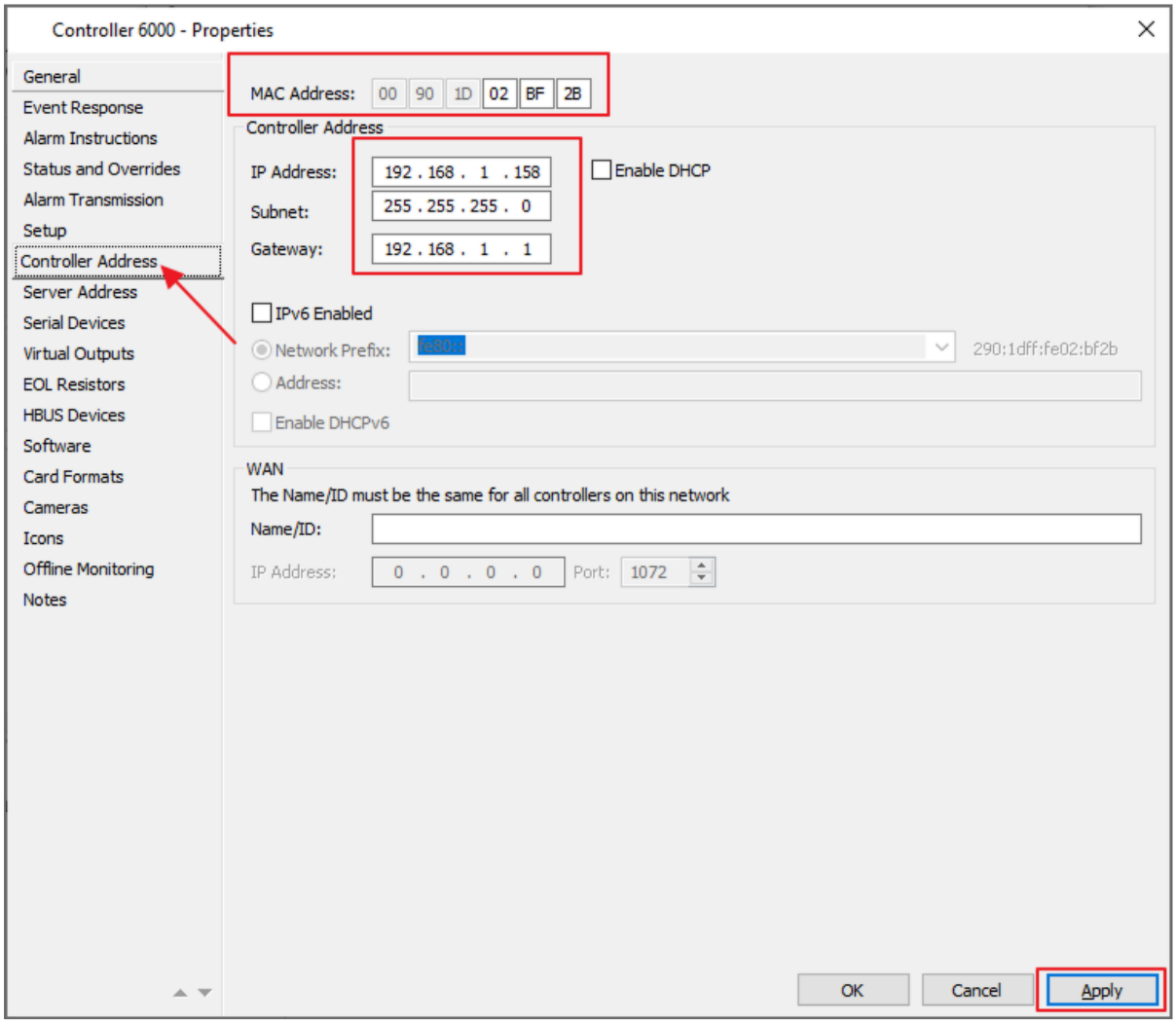
    Go to the Connections Tab and **choose** Controller as Controller 6000, set Hardware Variant as 4 in 2 out, and then press the **OK** button.



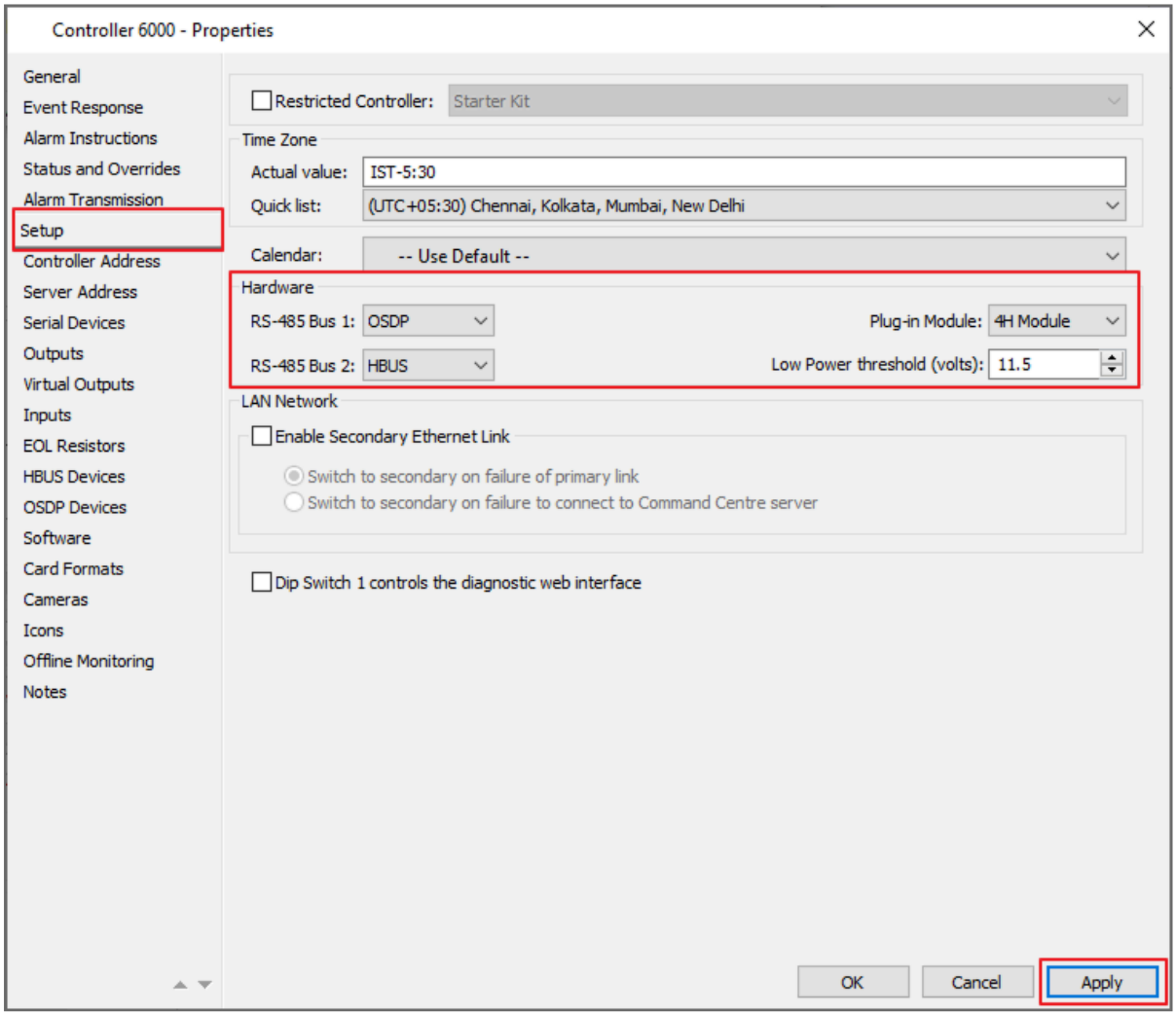
12. To connect your Gallagher Controller to the system, **open** Controller 6000 properties and **click** on the Server Address Tab. Tick use different IP for the server and type your PC/ServerIP address. Then **press** the **Apply** button.



13. In the Controller Address setting set your controller MAC address (Please look at your C6000 controller), Also **set** the IP address assigned for the Controller, Subnet, and Gateway. **Press** the **Apply** button.



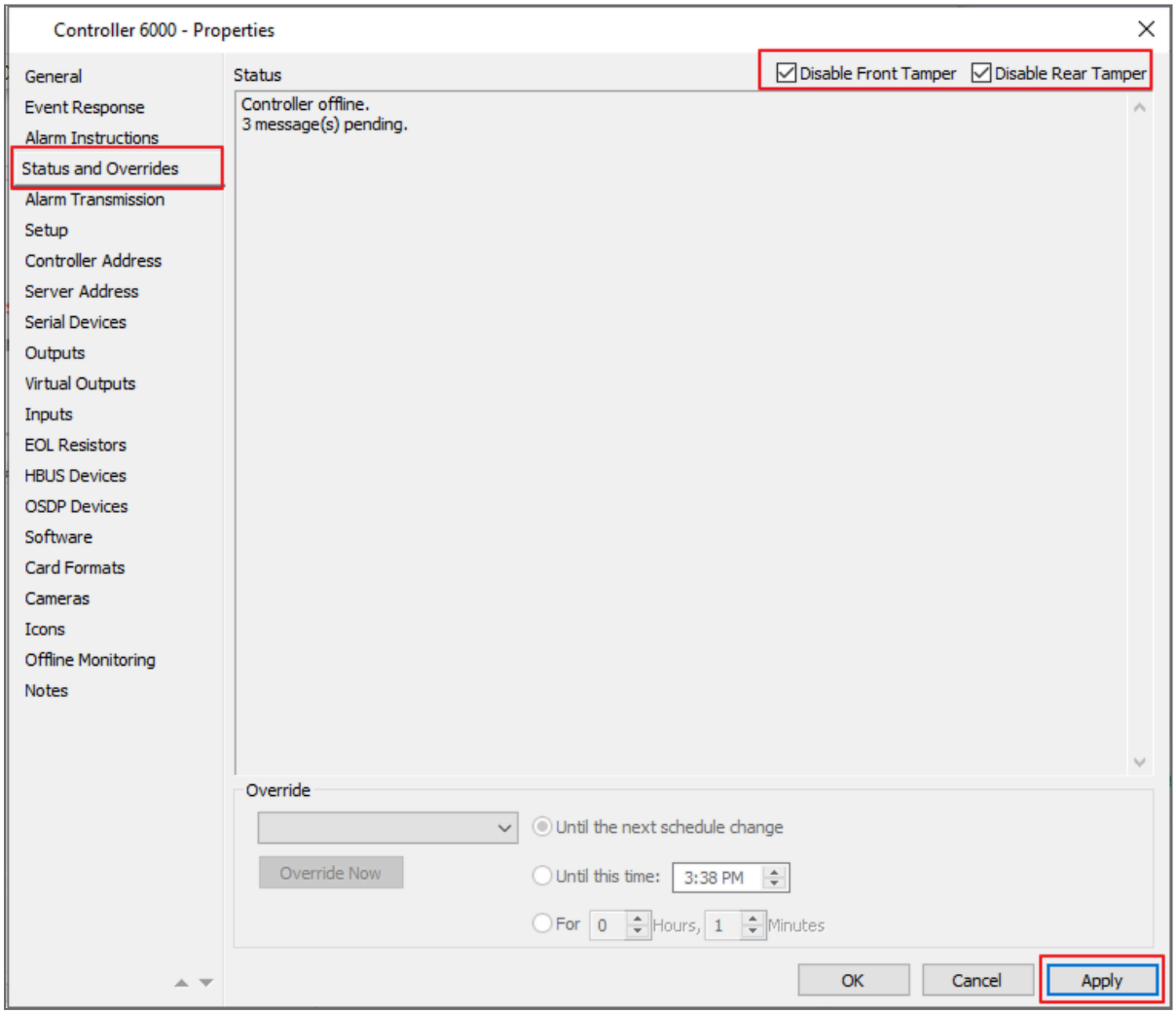
14. In the Setup Tab, set Plug in Module as **4H Module** (choose according to your controller) and in Hardware RS485 Bus 1 as **OSDP** and RS485 Bus 2 as **HBUS** and press Apply.



Info

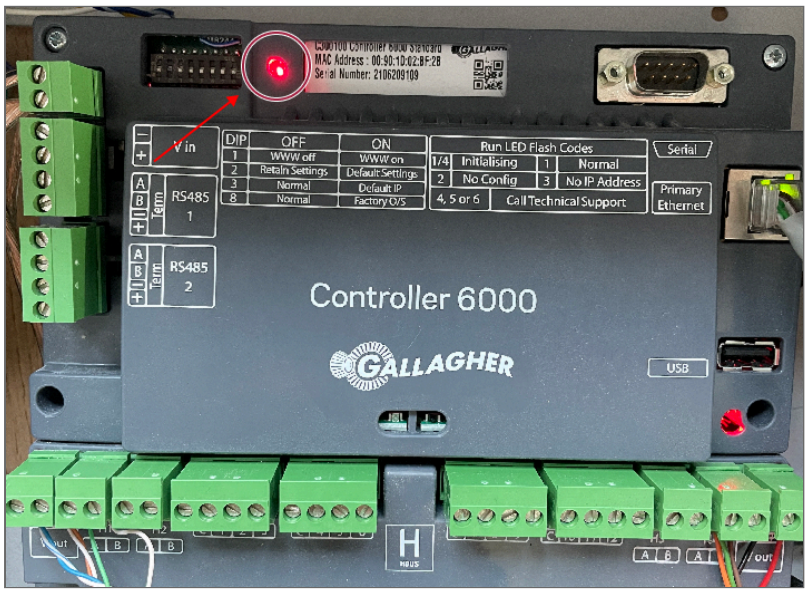
Your Setting could vary depending on your Gallagher devices & components.

15. In the Status and Overrides options **tick** both checkboxes Disable Front Tamper and DisableRear Tamper.



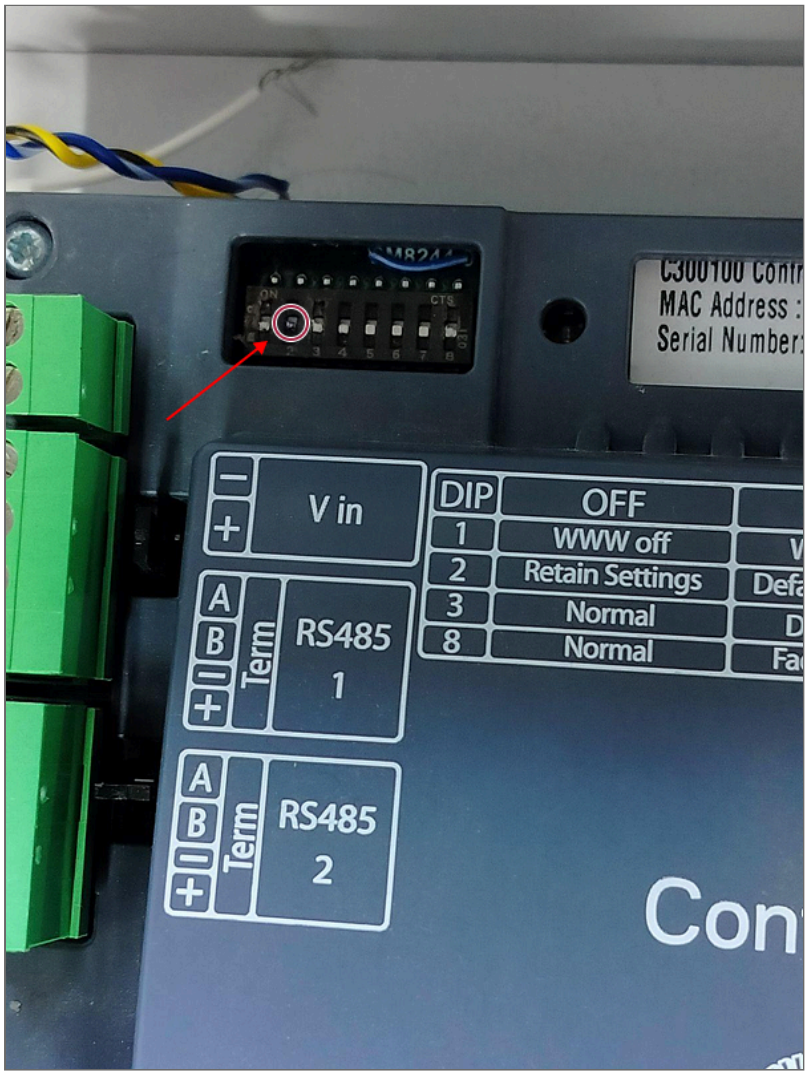
16. To connect your controller to the system, **turn off** the controller, and wait until the red light goes off. Then **turn on** the 2nd button from the left.

> **Info**
> Before performing this step, please ensure that your PC firewall is turned off.



17. When the status on the controller turns normal then **turn off** 2nd button (down/dip the 2nd button).

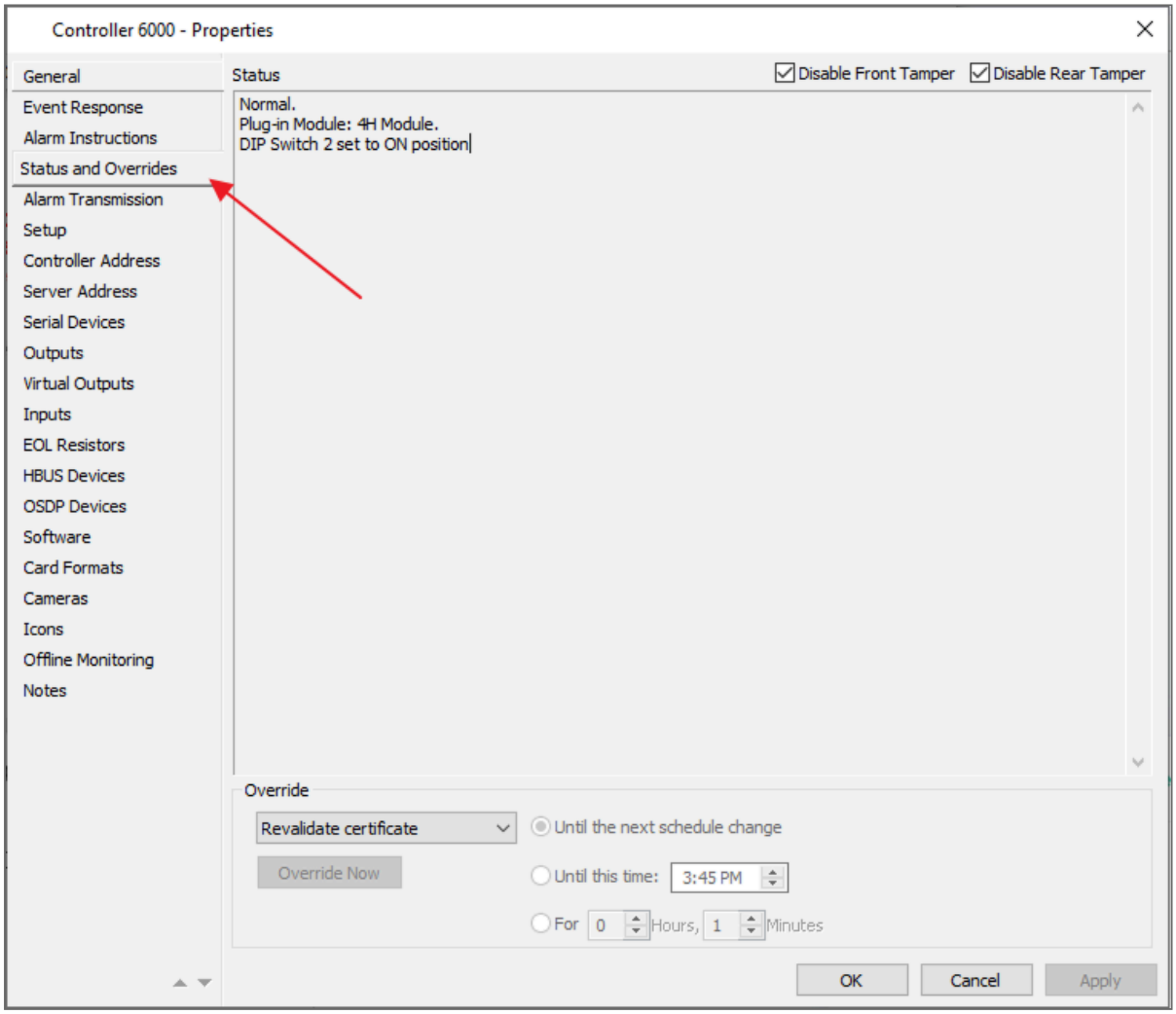
> **Info**
> Once the controller is online and normal, you can turn all dip switches off including 2.



Additional note first time power-up and new controller connection:

You only need #2 on when you first power up a new controller and connect to a server.

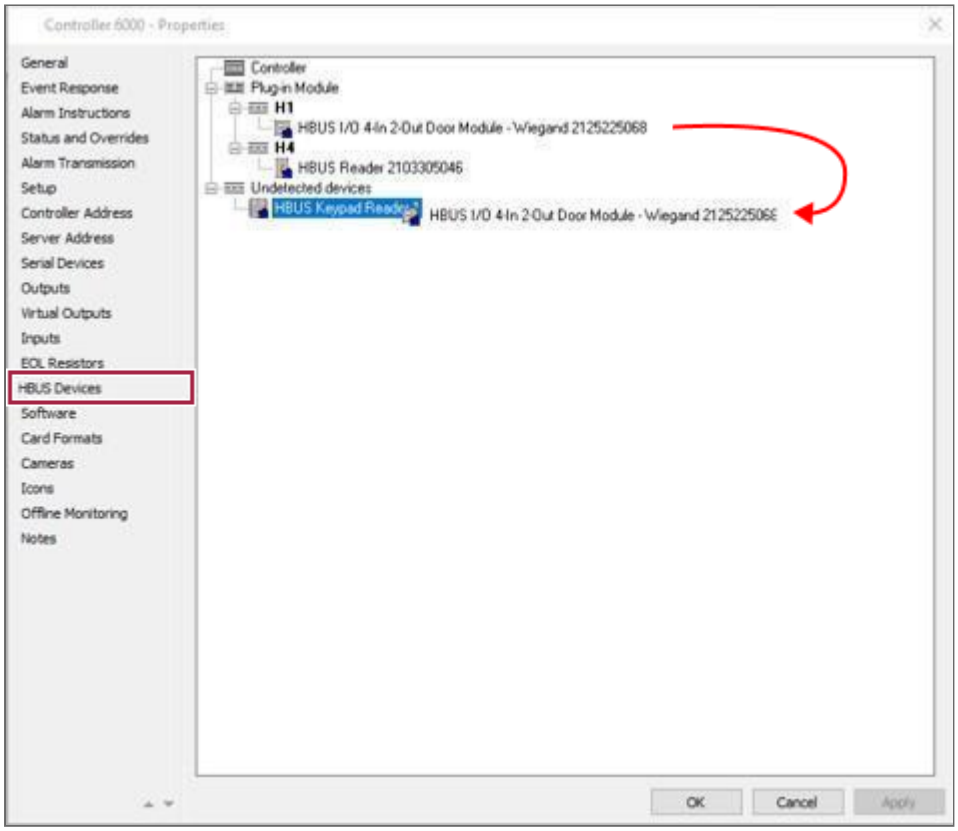
Also, Jumper #2 can be used when doing some resetting of the controller. You want it to be fixed if you are doing upgrades to the controller.



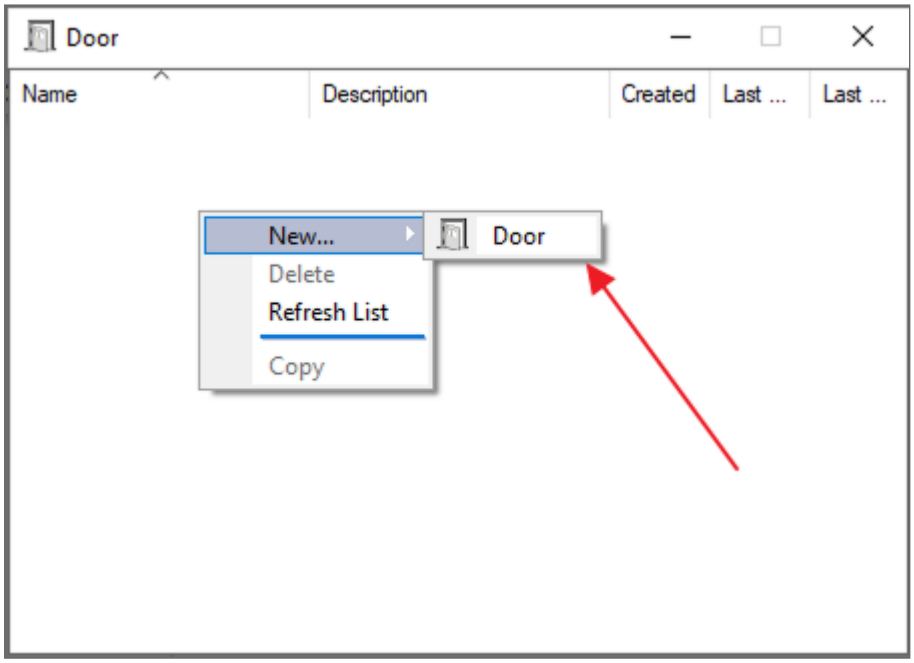
Info

Connect Devices to access HBUS in the controller HBUS setting. (To connect devices please refer to BioStar 2 setup.)

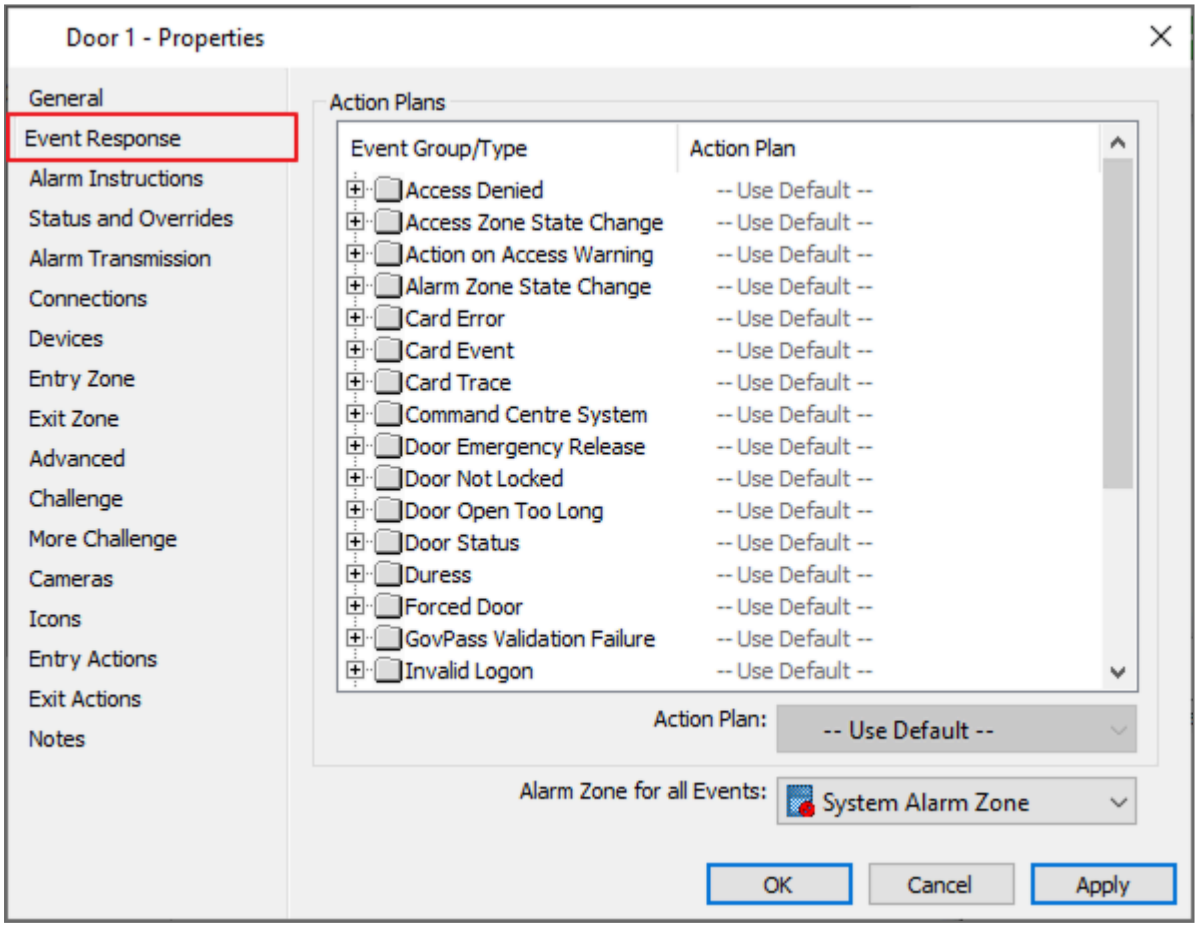
18. In the HBUS Devices option of Controller 6000 **drag and drop** HBUS I/O 4 in 2 Out module - Wiegand from **Plugin Modules** to **Undetected devices** HBUS I/O.



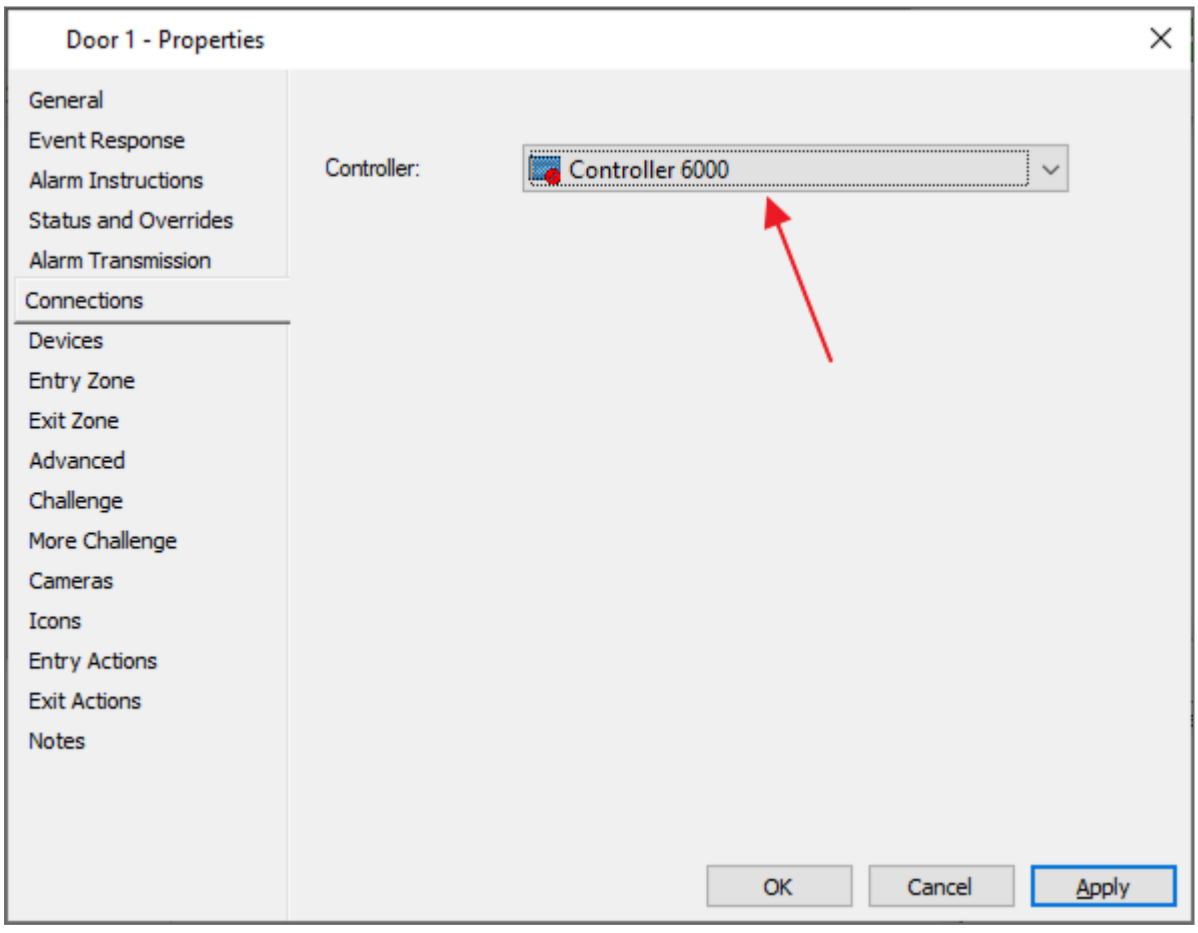
19. To Create Door go to Configure, Door then **press right-click** and create a new door.



20. **Set** the Door name as **Suprema Door** and go to Event Response and **choose** alarm as System Alarm Zone.

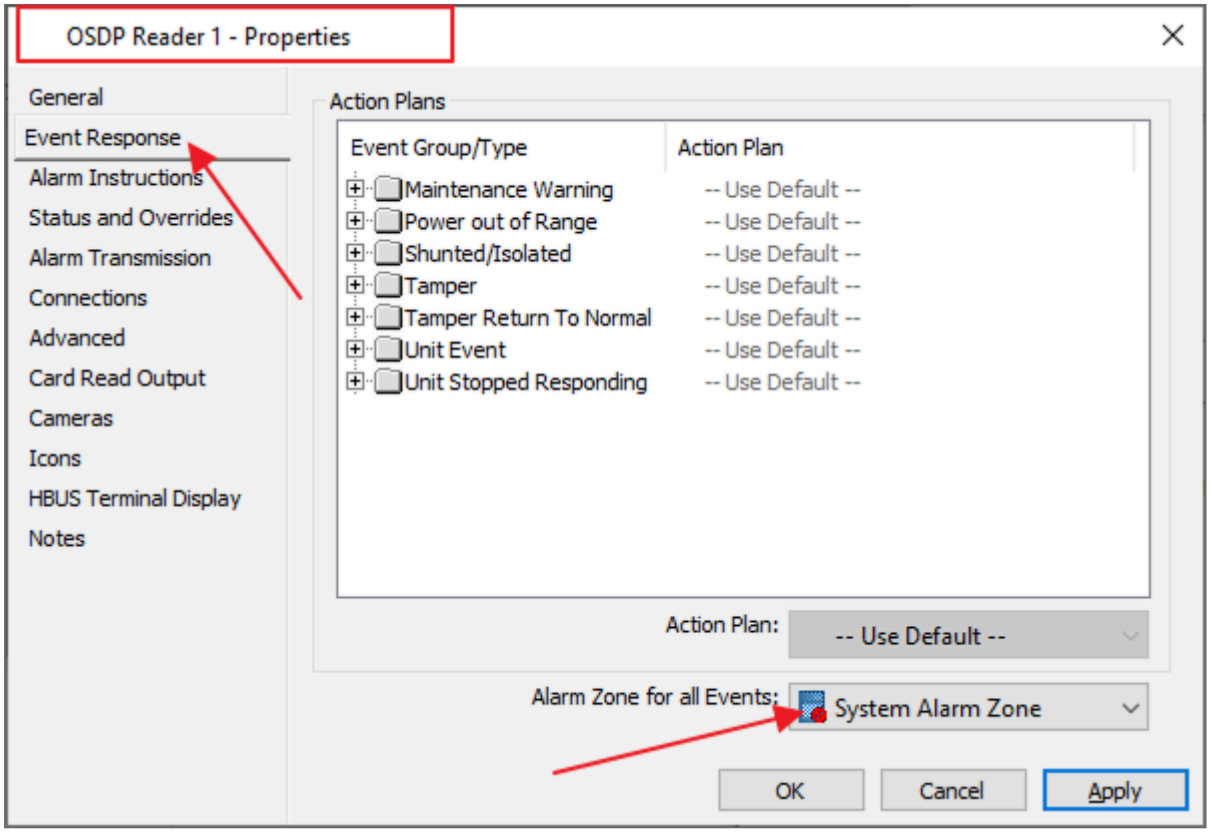


21. In **Connections select** Controller as Controller 6000 and press **Apply** and **OK**.



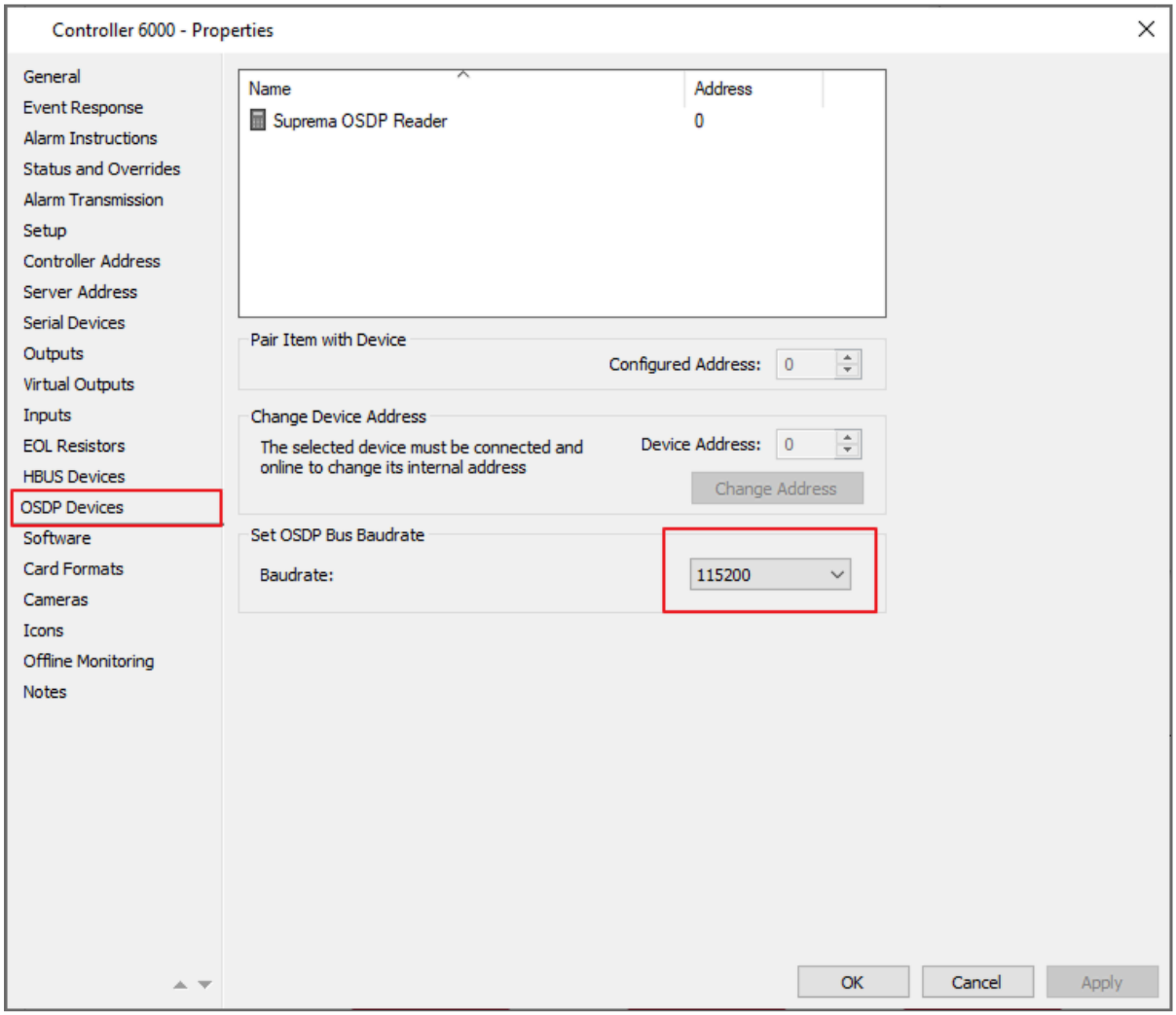
22. To create an **OSDP connection; right-click on the Hardware window. Select New → OSDP Device → Then click on OSDP Reader**, to create OSDP Reader on Hardware.

    A new window opens up. **Set** its name as Suprema OSDP Reader, and in the Event Response settings, tab **set** Alarm Zone for all events: as System Alarm Zone. Then **click** Apply & **press** OK to save the changes.



    Go back to the Hardware Window. **Double click** on Controller 6000 for the Properties. **Click** on OSDP Devices Tab.

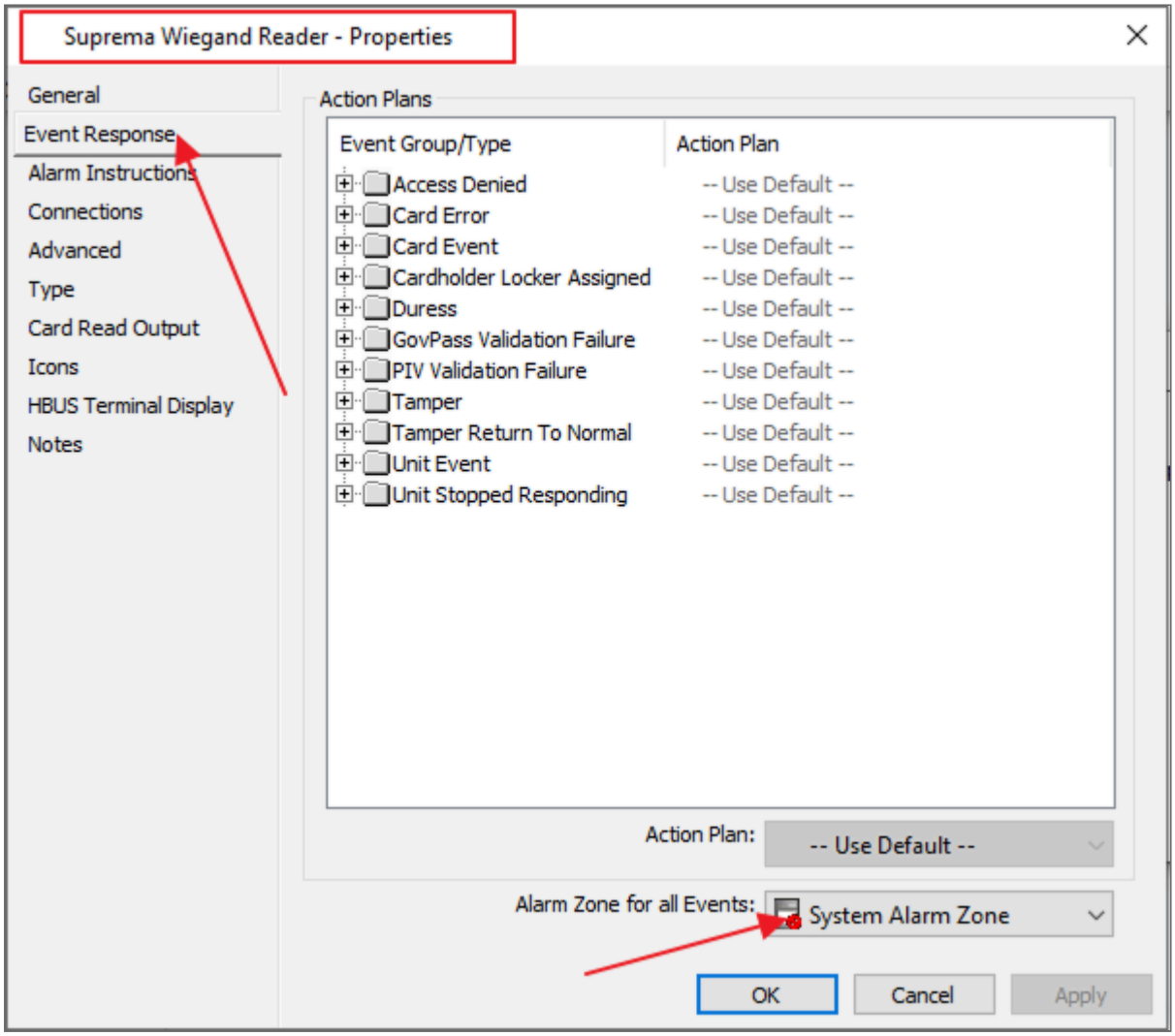
23. **Drag** the OSDP reader from the **Hardware Window to** the **Controller properties** in the OSDP Devices Tab. **Set** Configured Address as 0, Suprema OSDP Device Address as 0, and Baudrate as **115200**.



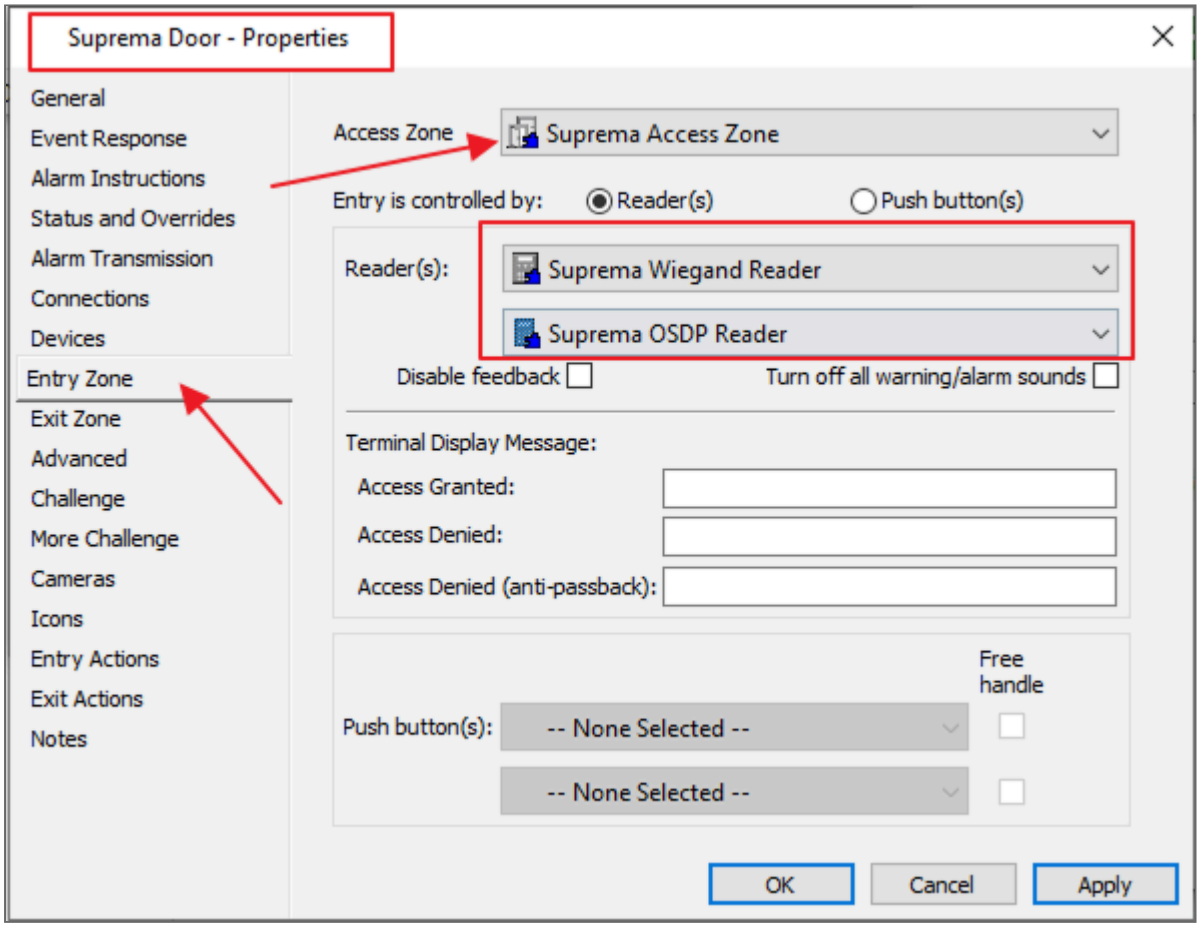
Info

If you have a 2x OSDP Reader please change the OSDP address within BioStar 2.

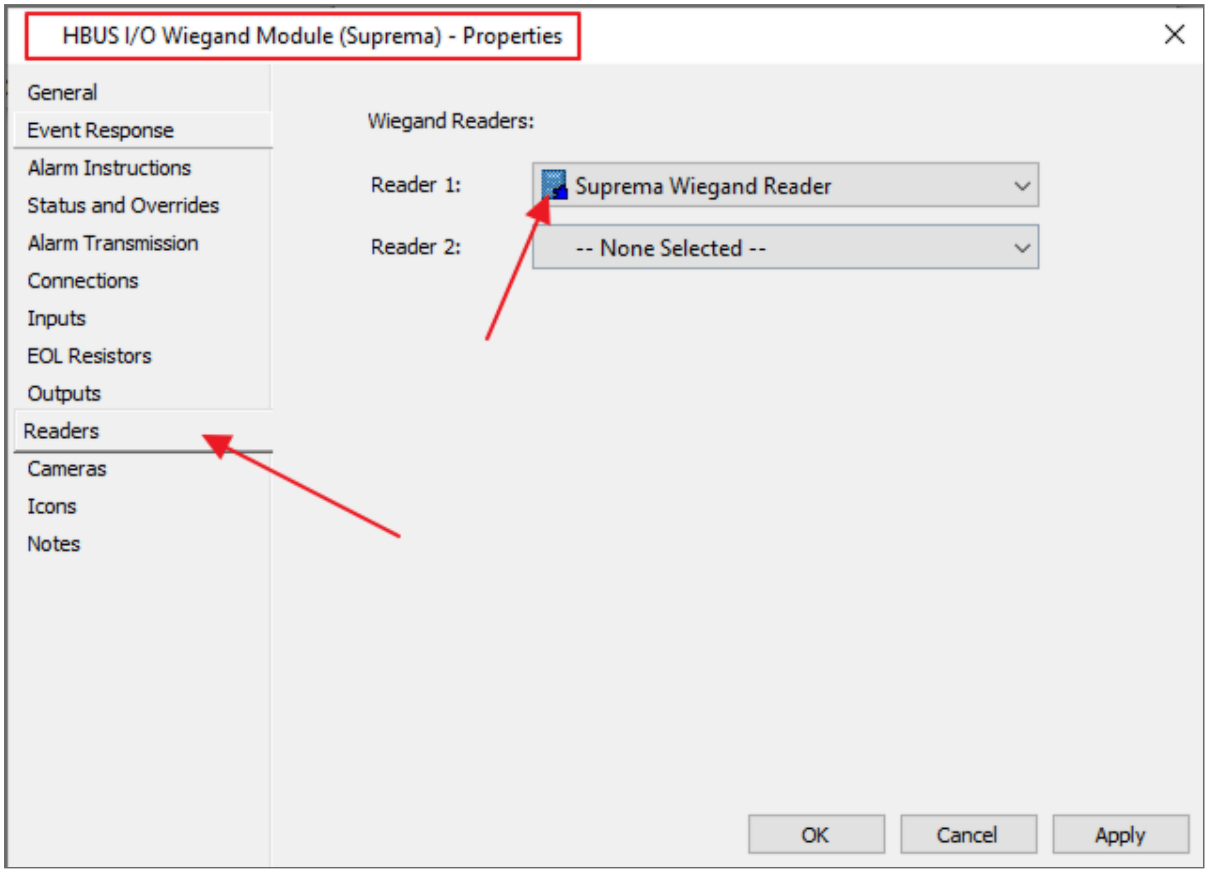
24. To create the Wiegand Reader. **Right-click** on the Hardware Window. Click on New → Third-Party Reader. A New Window appears; **Set** its name as Suprema Wiegand Reader, then in the Event Response Tab. **Choose** the Alarm Zone as System Alarm Zone and **press OK**.



25. **Go to** the Door that we have created in properties **Entry Zone** set Access Zone as **Suprema Access Zone** and reader as **Suprema Wiegand Reader** and **Suprema OSDP Reader**, and **press** the **OK** button.



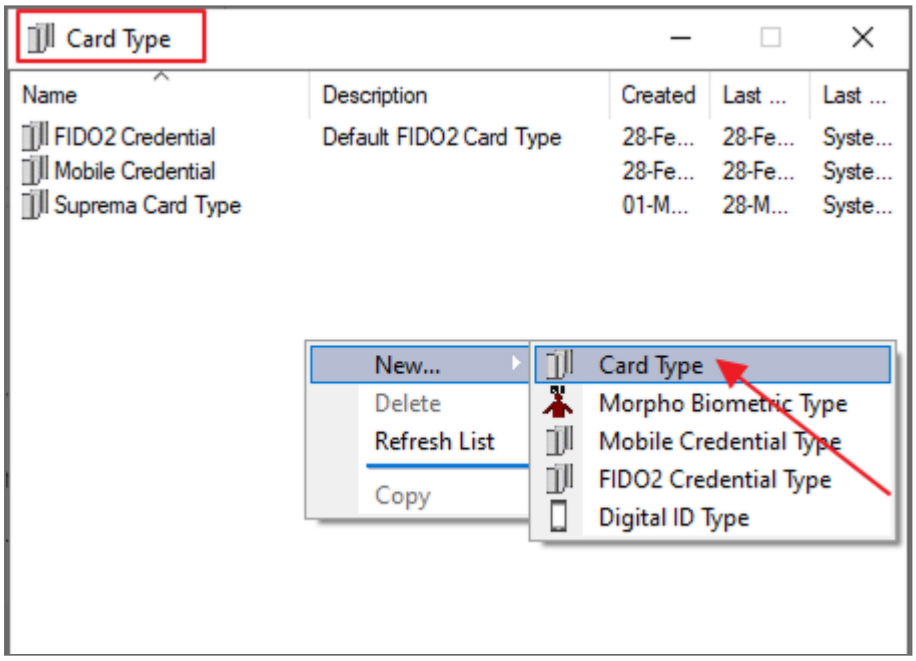
26. In **HBUS I/O** properties go to **Reader** settings and set Reader 1 as Suprema Wiegand Reader, **press** the **OK** button. **Close** the door and Controller window.



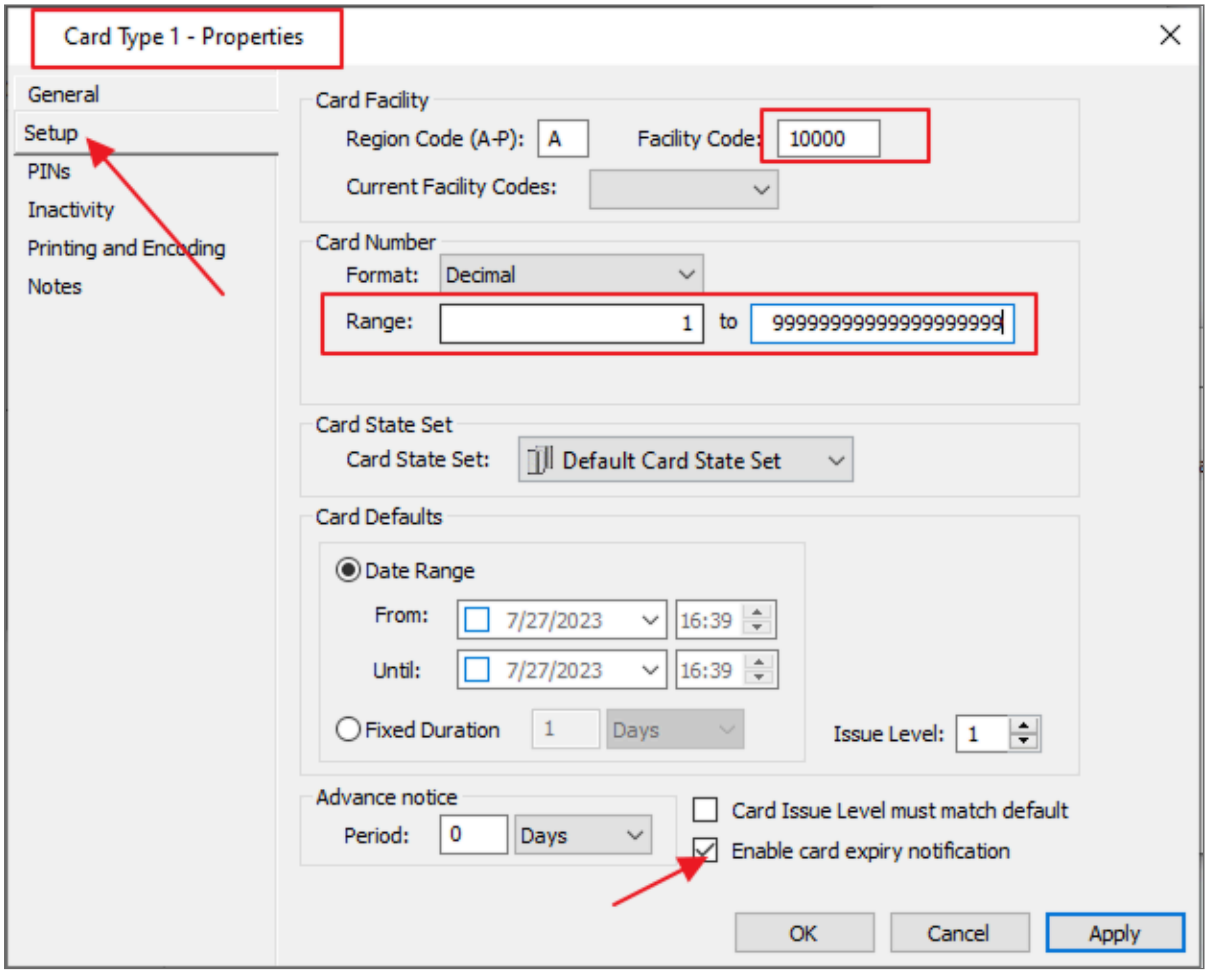
27. To create a card type Configure → Card Type **right-click** and create a new **Card Type. Set** its name as **Suprema Card**

Type.

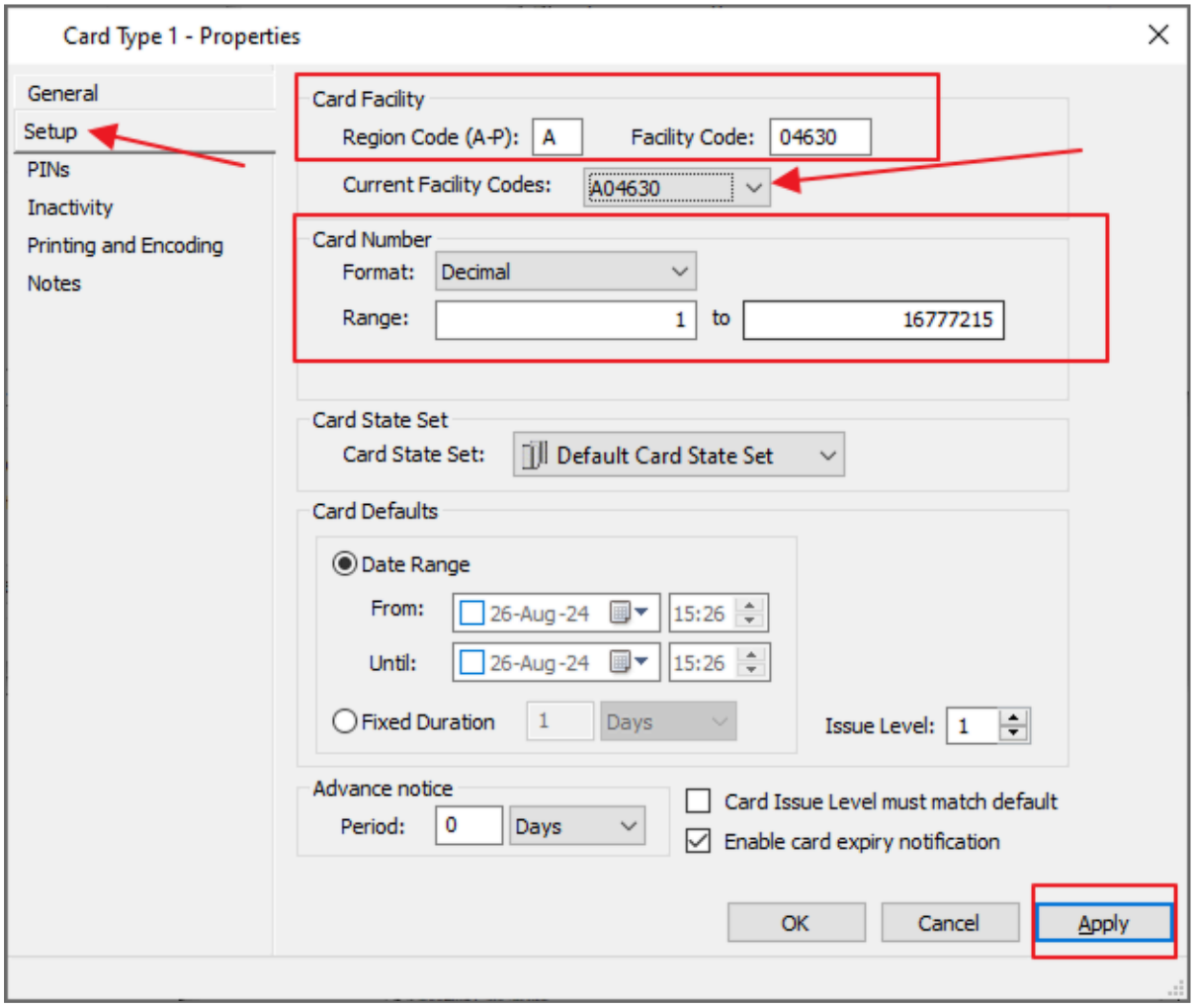
> **Info**
>
> - A QR Device license is needed to read the Gallagher QR Code. Please contact Suprema for it.
> - Please use the same terms as mentioned for the fields.



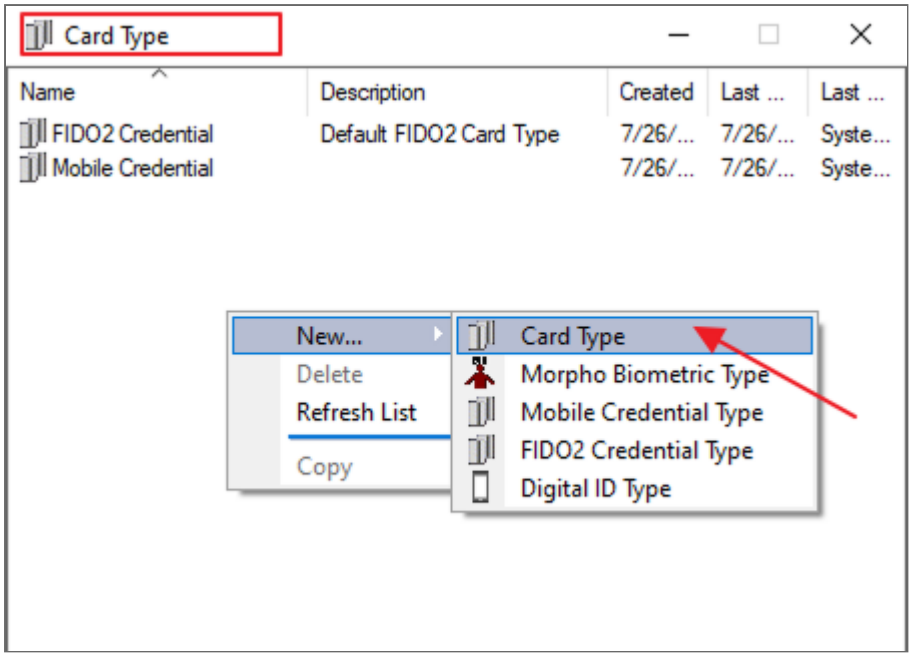
28. In Card type properties **go to** setup option Region code as **A** and Facility code as **10000** card number range as **1 to 99999999999999999999 (20 times)** and enable card expiry notification. **Press OK**.



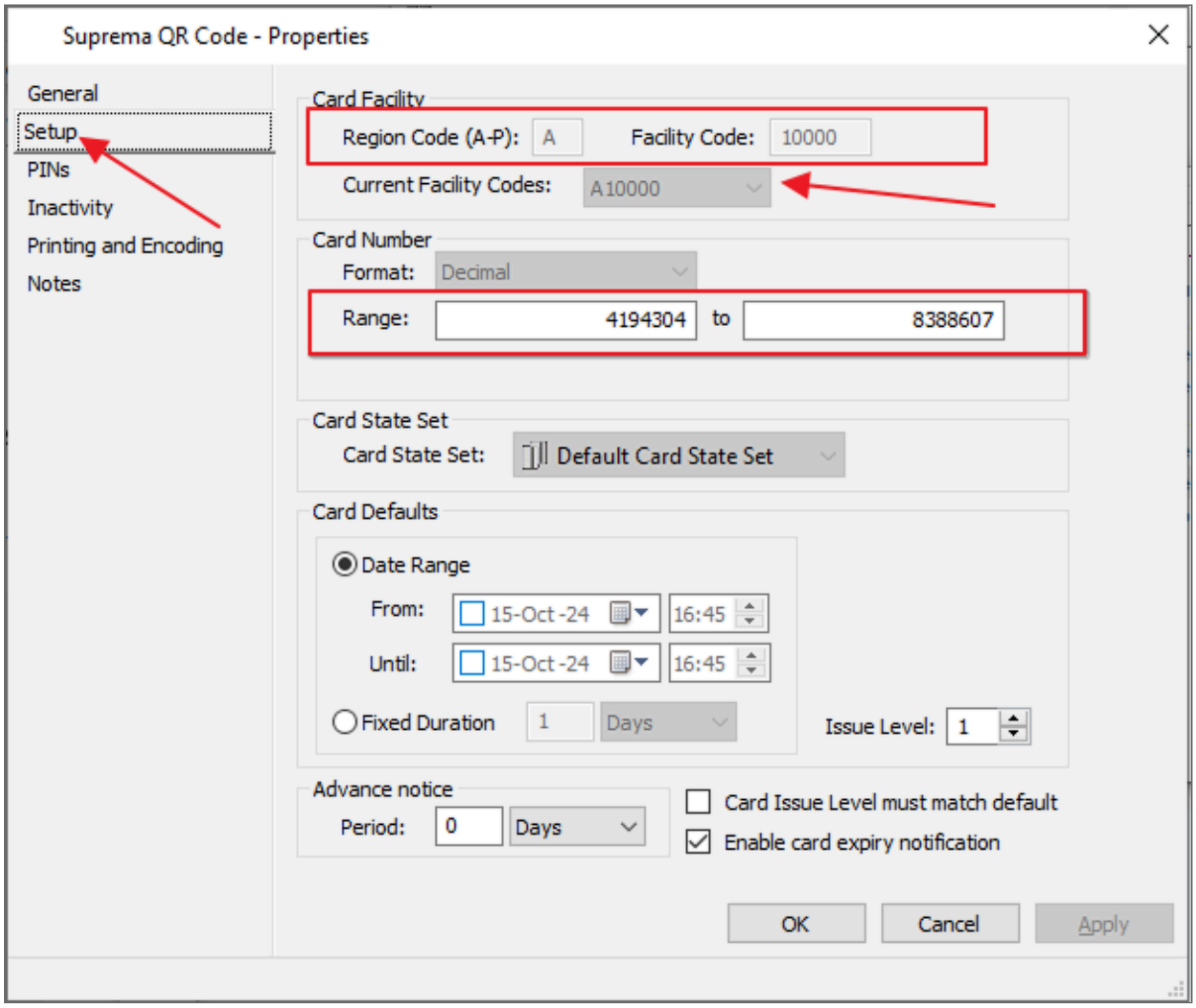
29. Create another card type Configure → Card Type **right-click** and create a new **Card Type**. Set its name as **HID Seos Corporate**. And **go to the** properties (setup) to set up card type. Use the below configurations to configure the card and **press** Apply and **OK**.



30. Create another card type Configure → Card Type **right-click** and create a new **Card Type**. Set its name as **Suprema QR Code**.

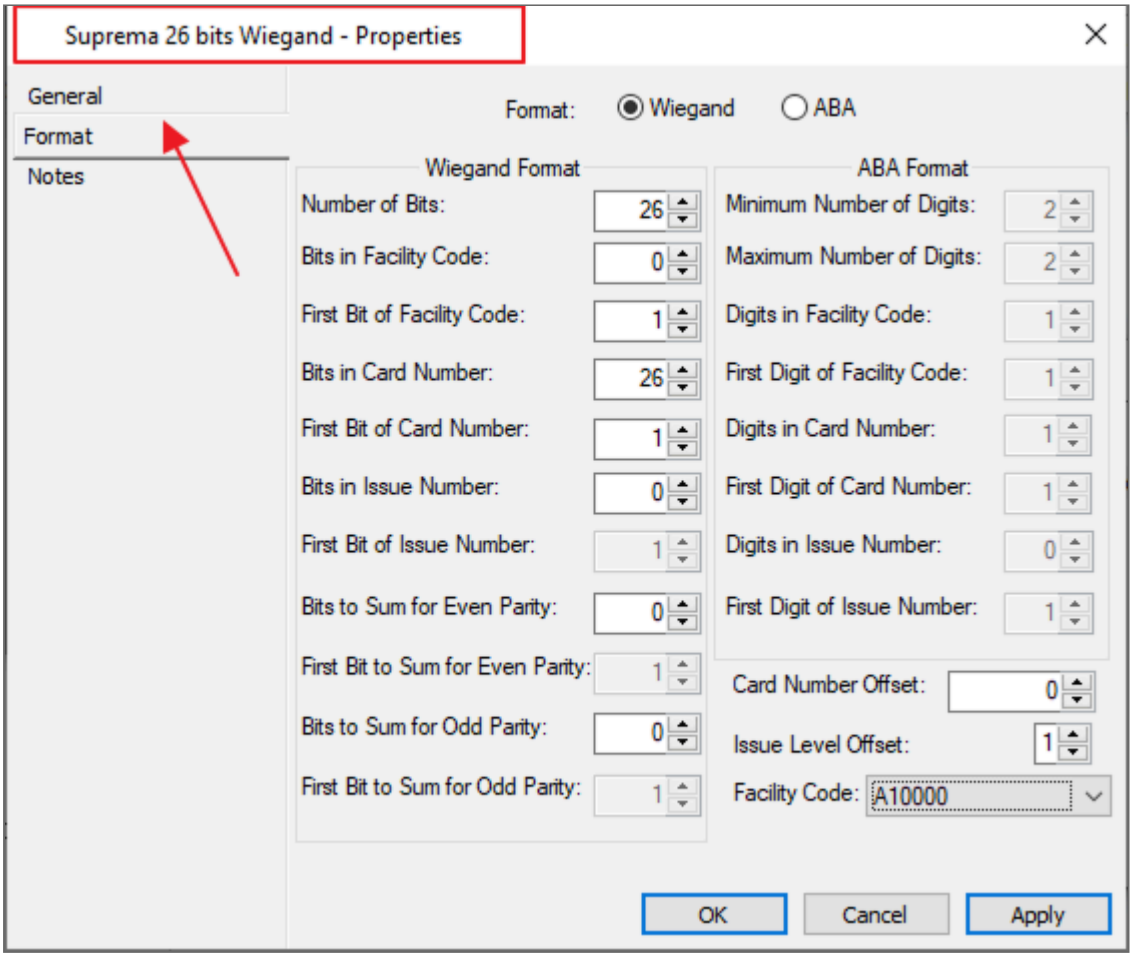


31. In Card type properties **go to** setup option Region code as **A** and Facility code as **10000** card number range as **4194304 to 8388607** and enable card expiry notification. **Press OK.**

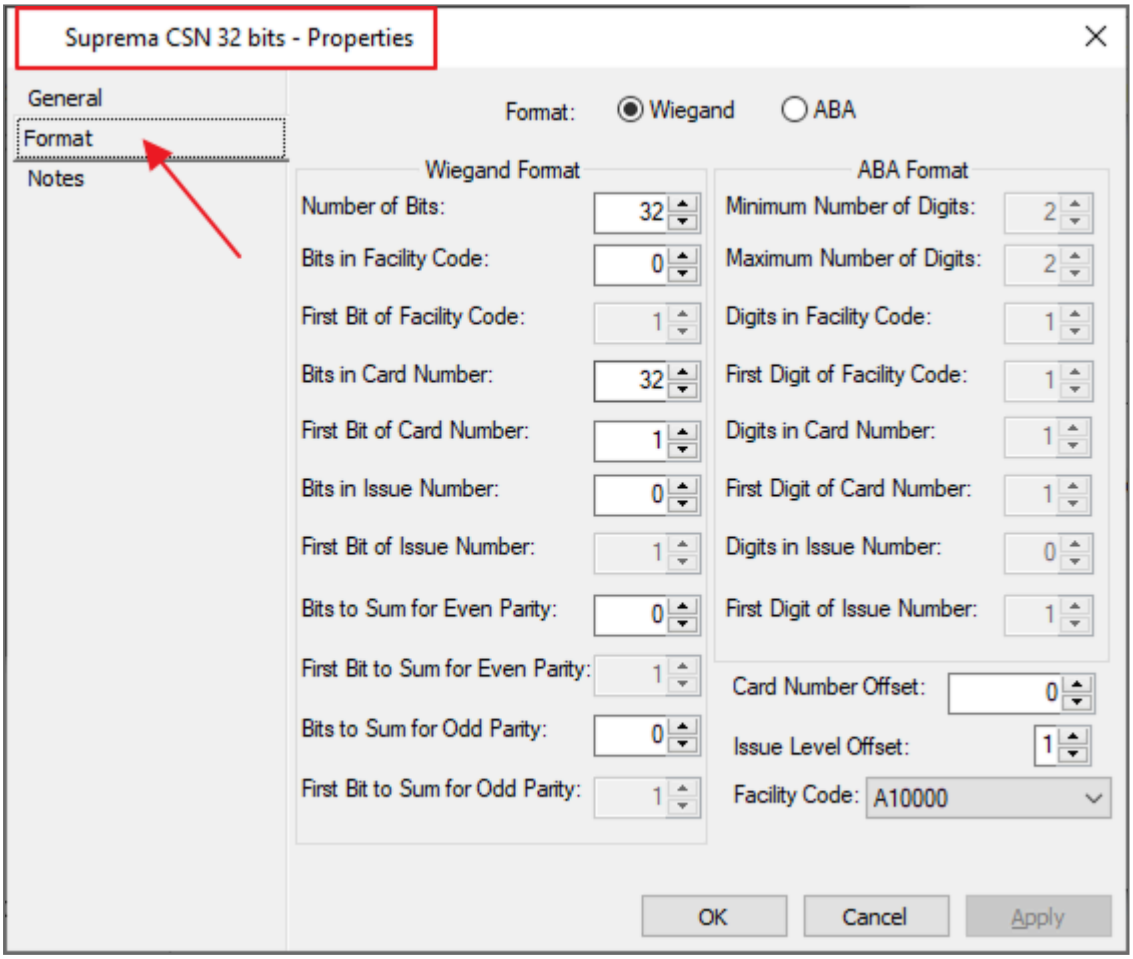


32. To create a universal card type Configure → Universal Card Format **right-click** and create a new universal card format. We have to make 4 card formats.

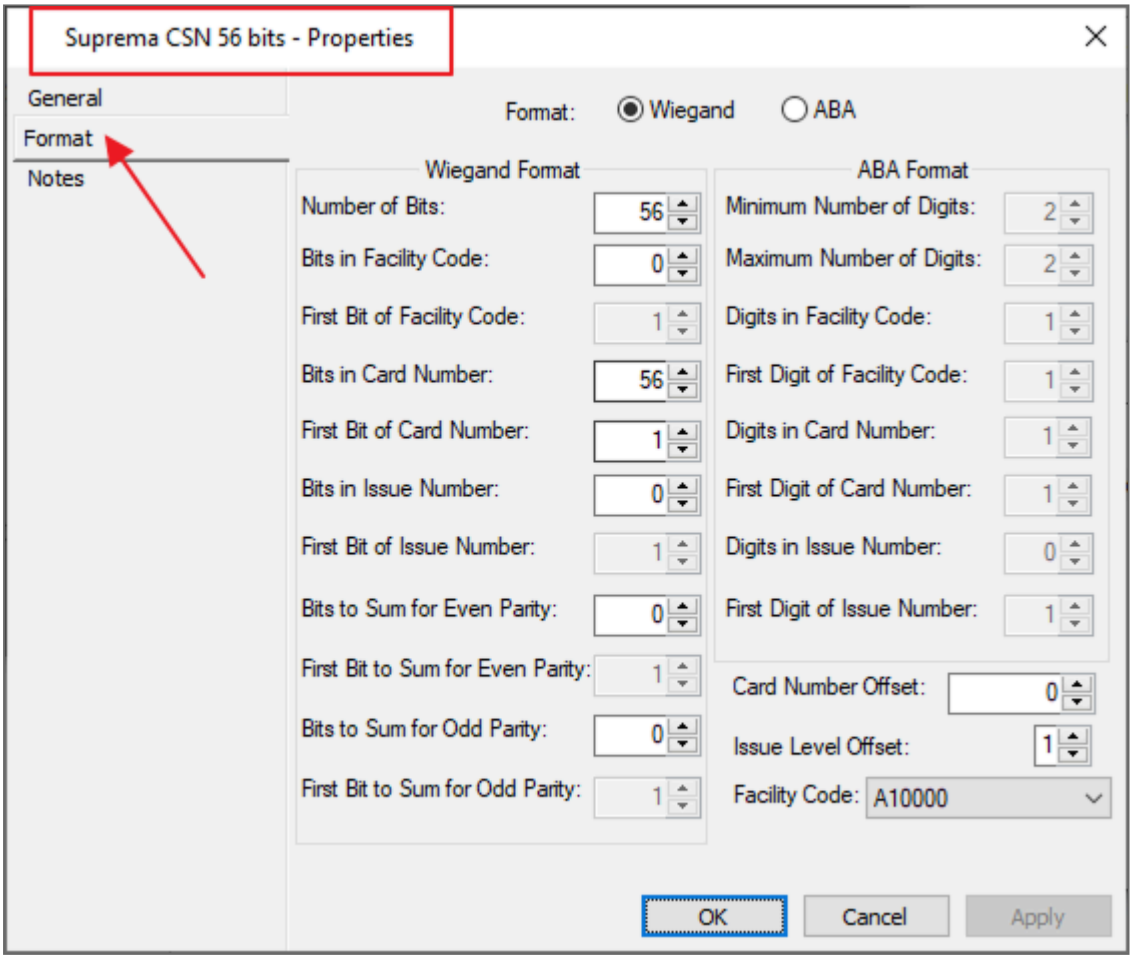
    1. **Create** a new format name as **Suprema 26 bits** Wiegand and set the format as the below image:



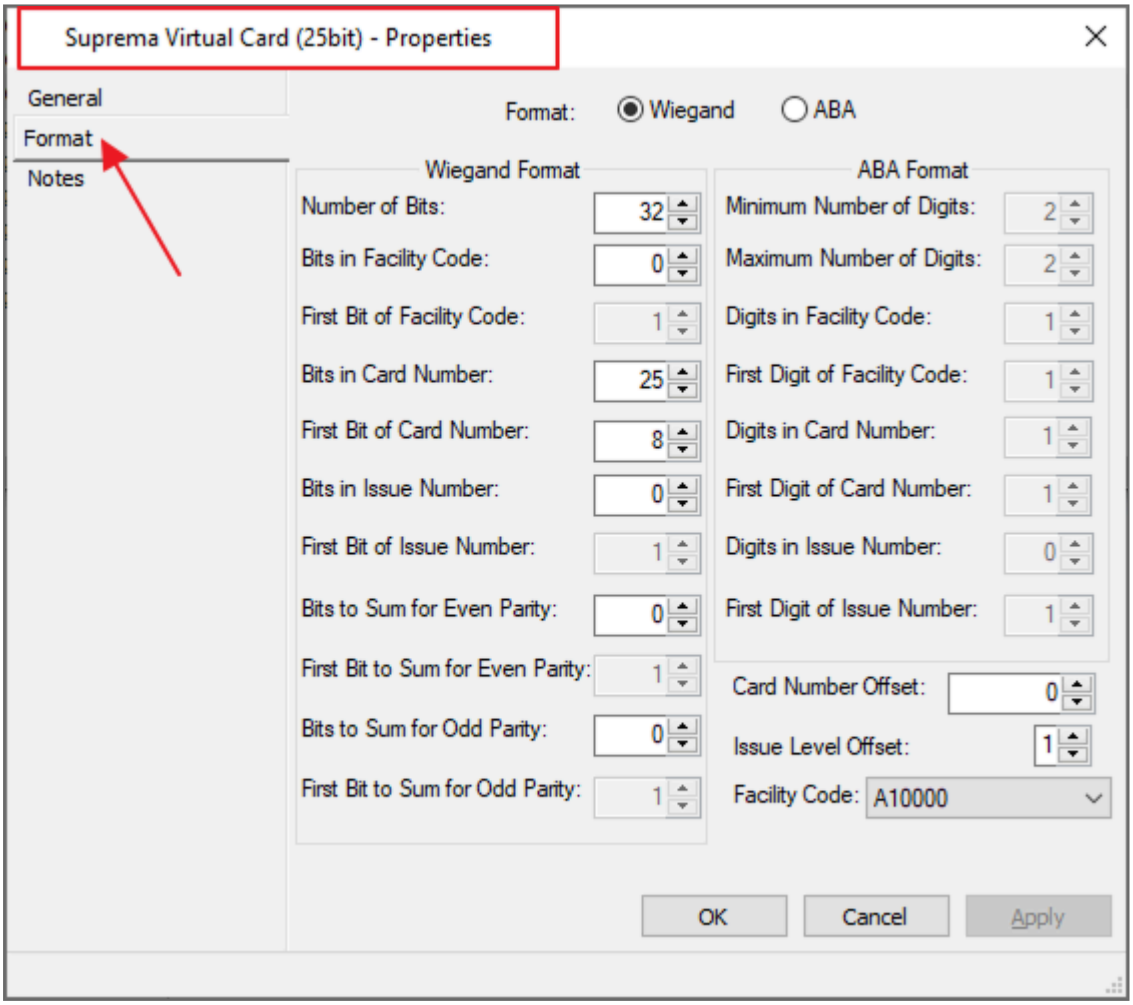
2. **Create** a second card format as **Suprema CSN 32 bits**, and in the format **set** as shown below.



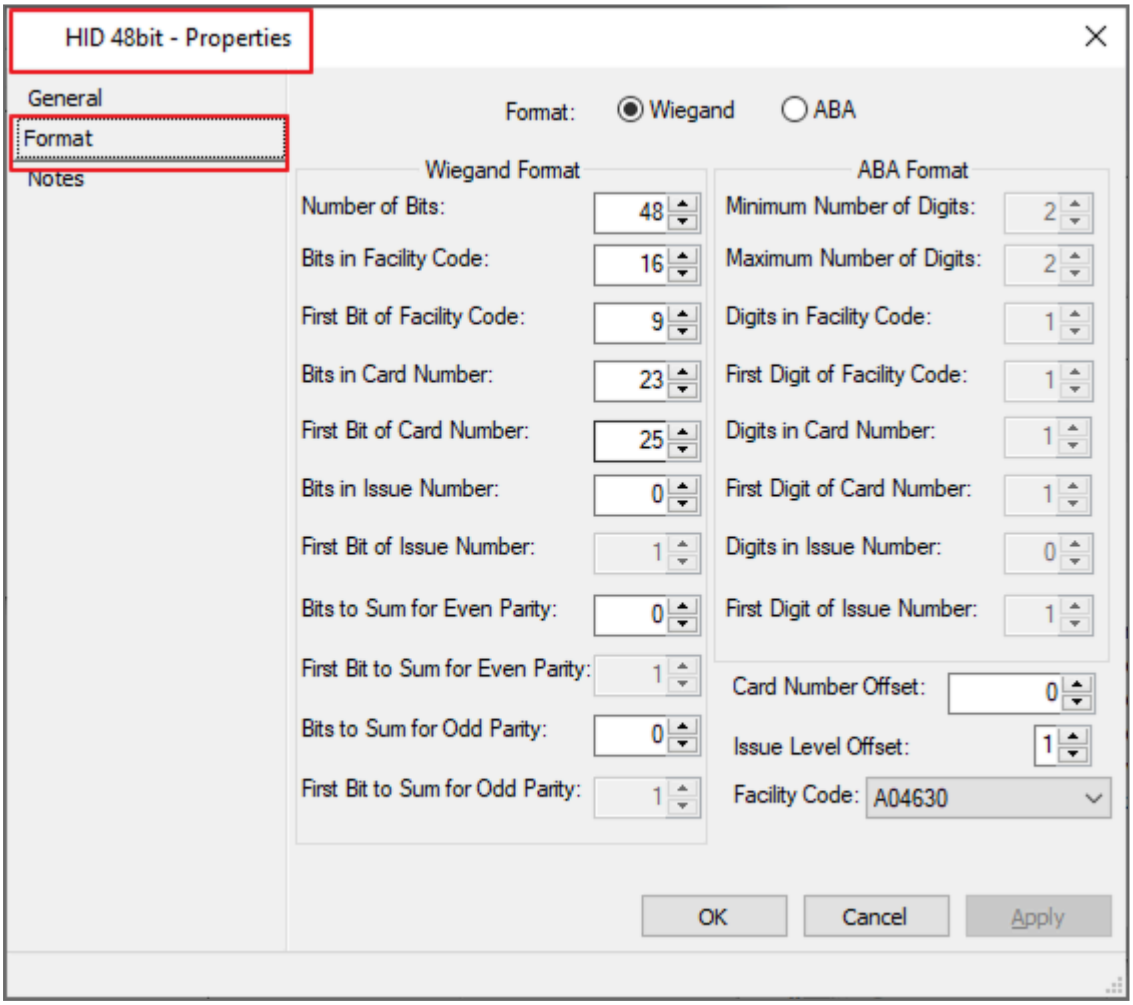
3. **Create** a third card format as **Suprema CSN 56 bits**, and in the format **set** as shown below.



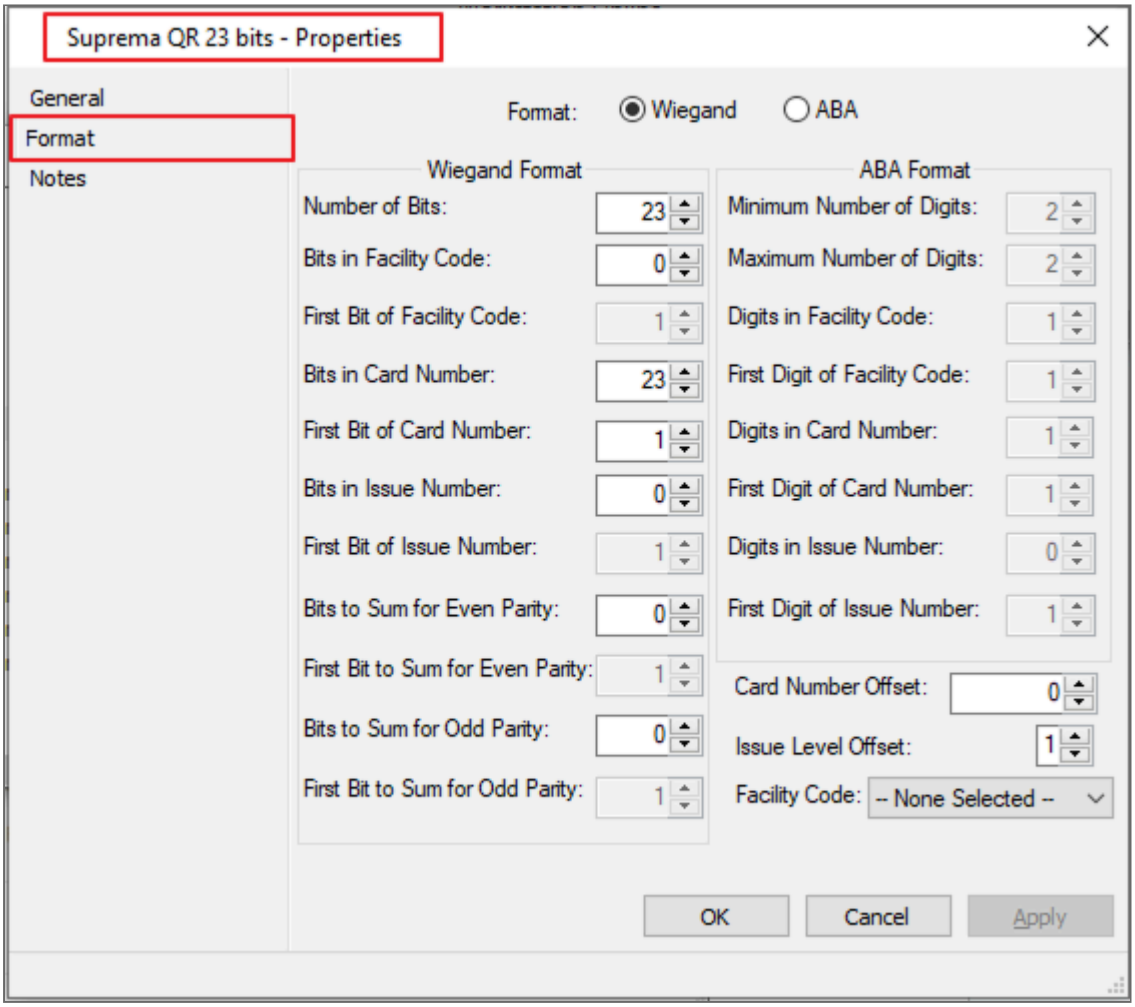
4. **Create** a fourth card format as **Suprema Virtual Card (25bit)**, and in the format **set** as shown below.



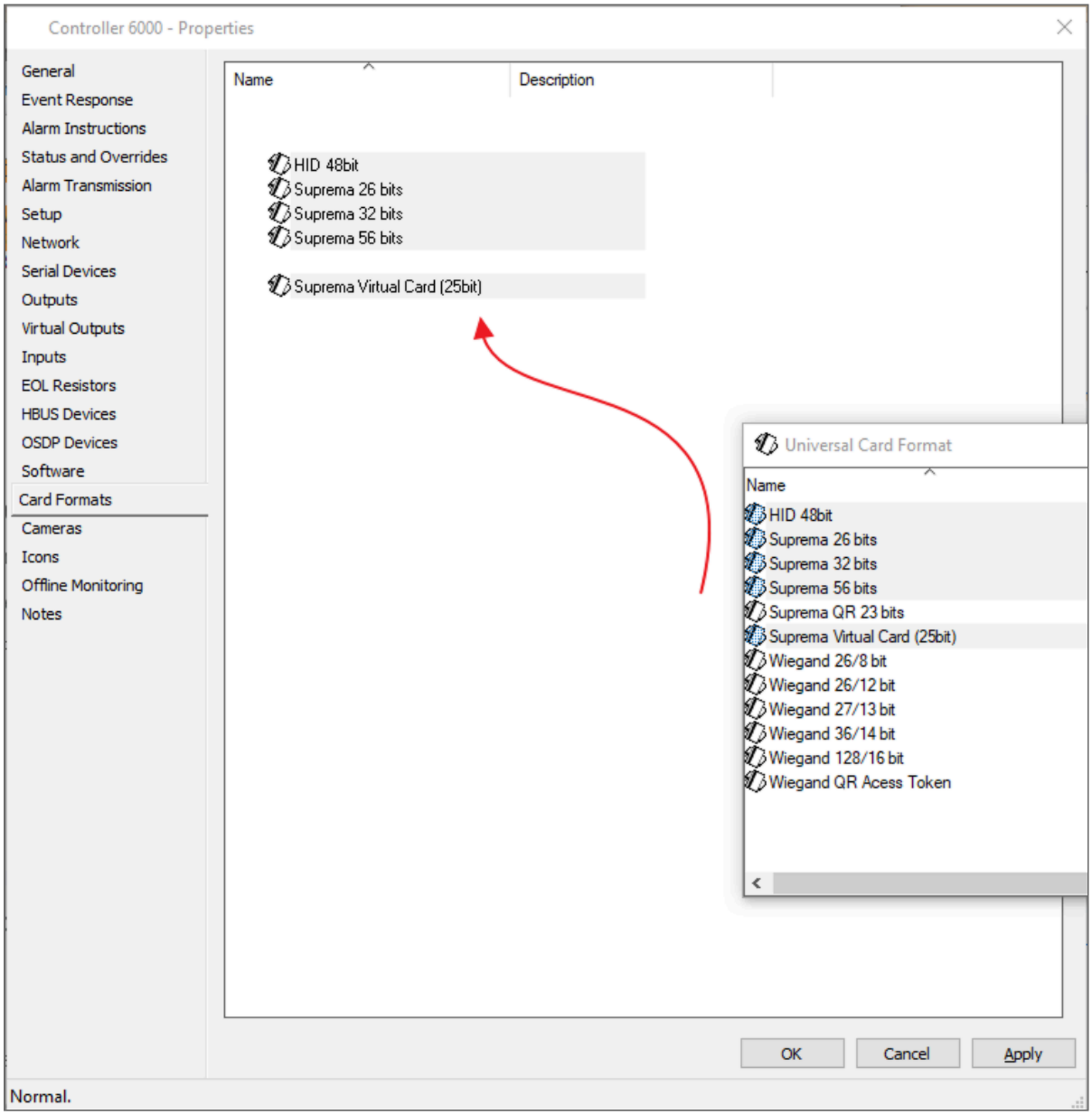
5. **Create** a fifth card format as **HID 48bit**, and in the format **set** as shown below.



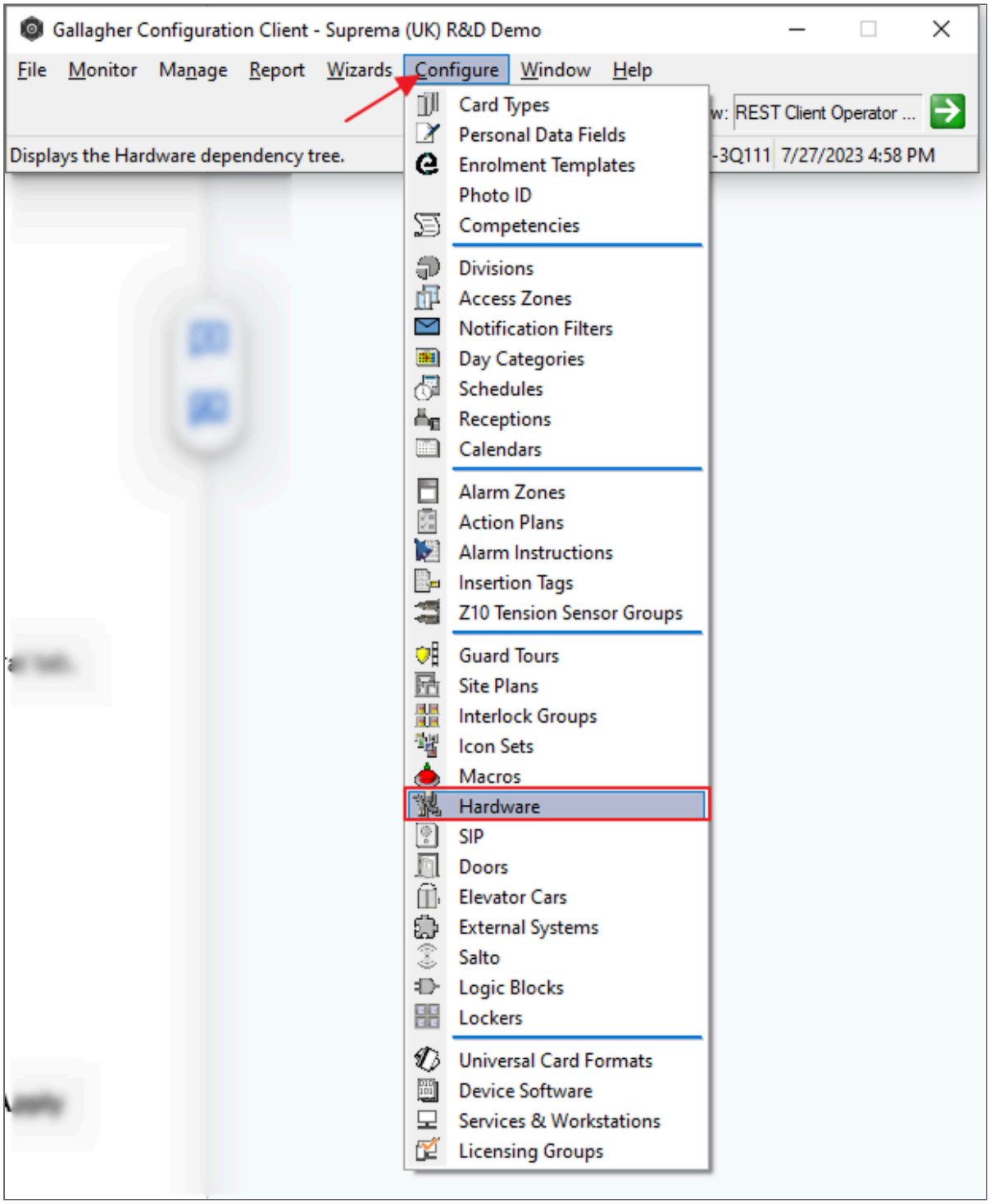
6. **Create** a sixth card format as **Suprema QR 23 bits**, and in the format **set** as shown below.



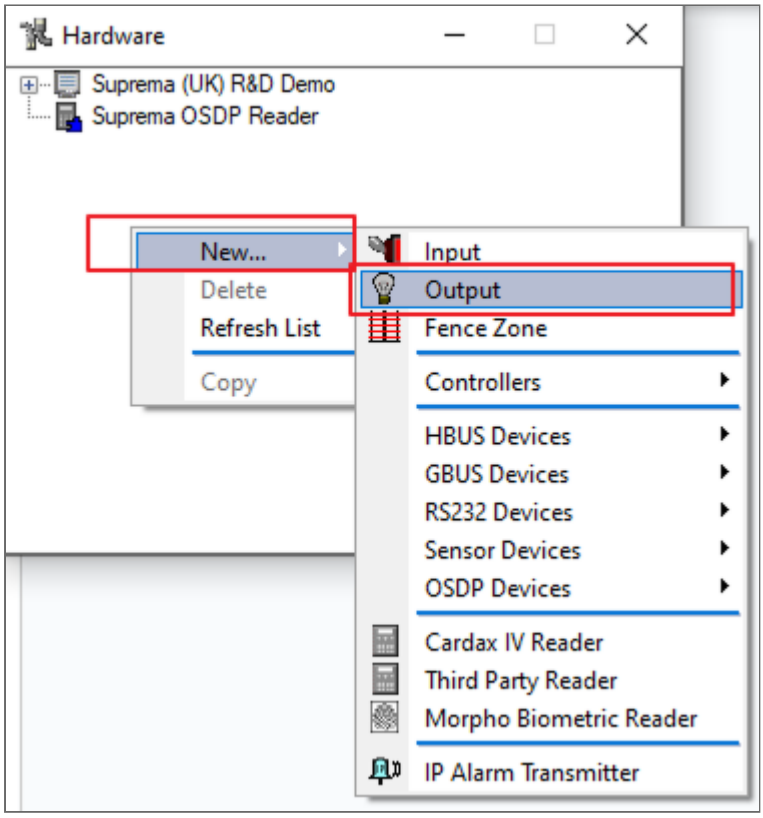
33. **Drag** all six card types and drop them on Controller properties, Card Format Setting, and **Apply** the settings. **Press** the **OK** and **Close** all the windows of Gallagher Configuration Client.



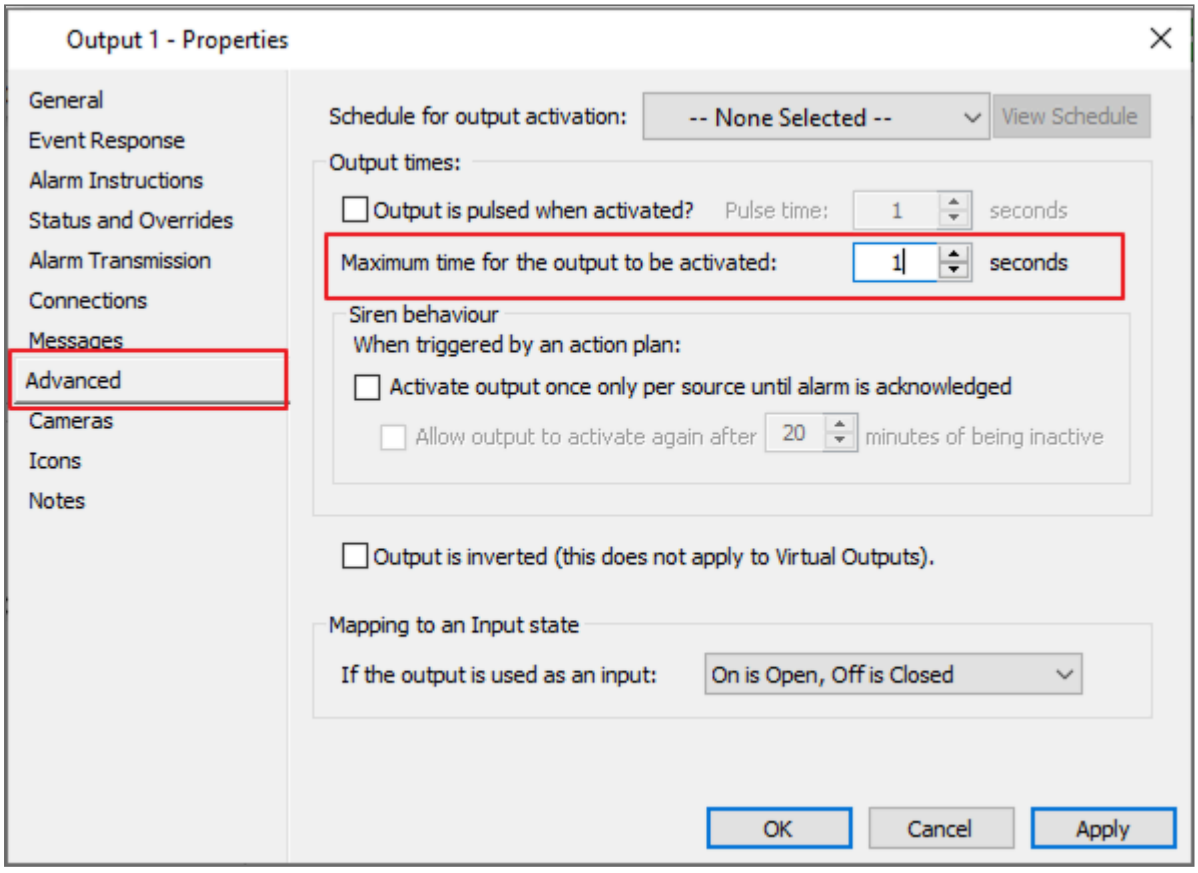
34. **Go to** Config Client Configure → Hardware.



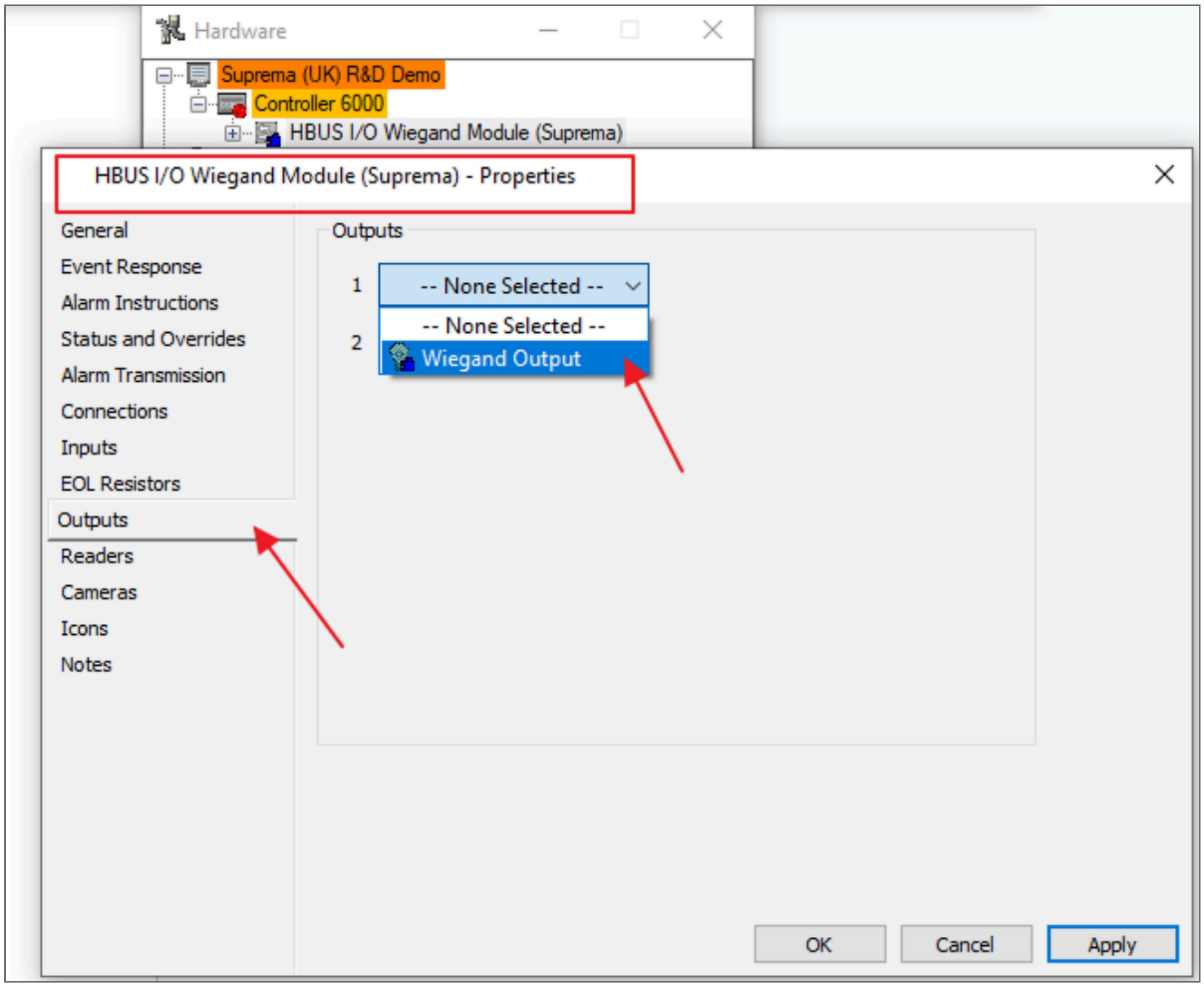
Then **Right click** on the Window and **create** output and **set** the name as **Wiegand Output** in the general tab.



35. Now **click** on Advance on the left side **set** 1 second in the Output times option and **press Apply** and **OK**.

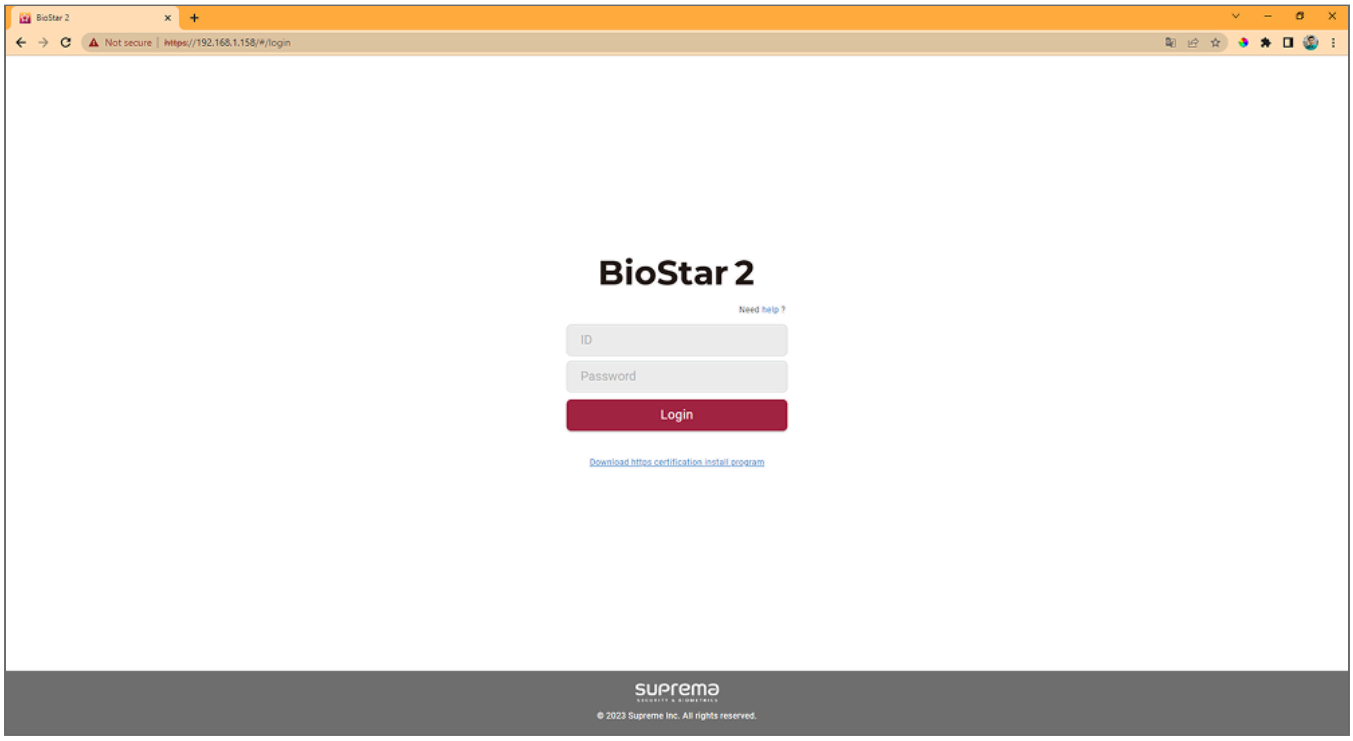


36. Now **go to** hardware window → **double click** on HBUS I/O Wiegand Module (Suprema) on the left side **go to** Outputs and **select** Wiegand Output **press Apply** and **OK**.

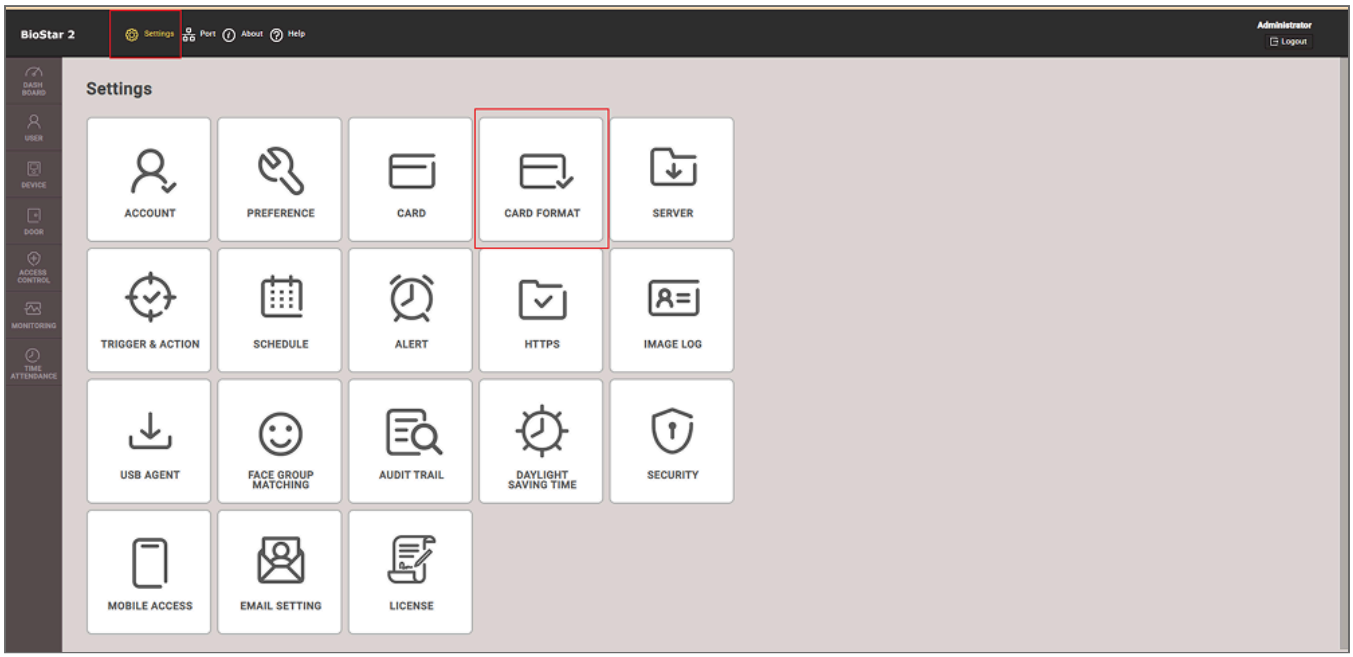


BioStar 2 Setup

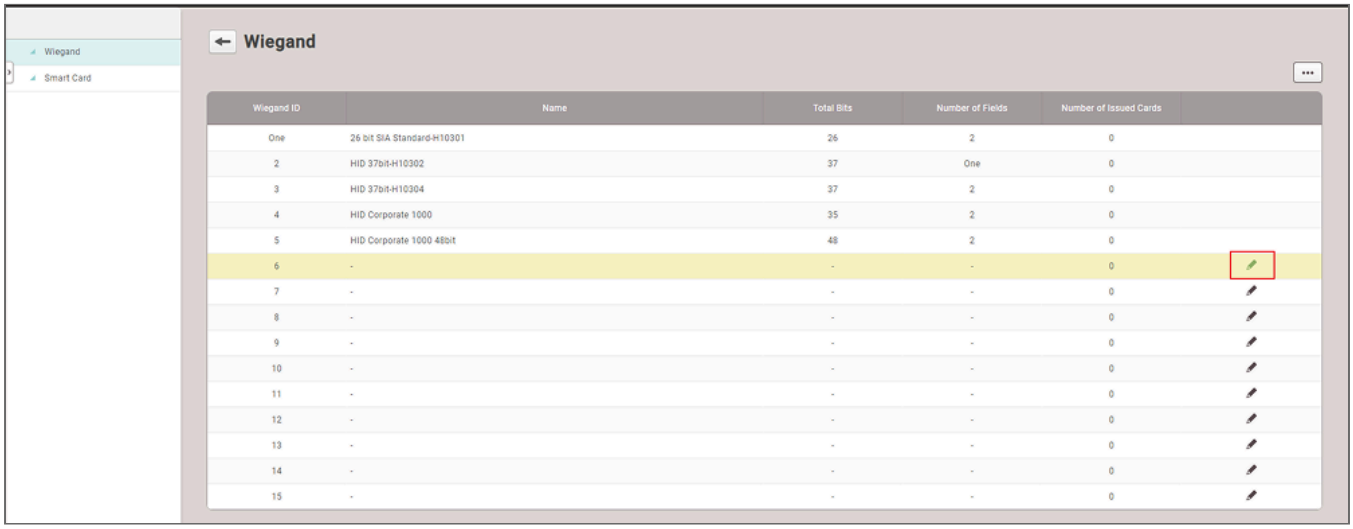
1. To open BioStar 2 **type** https://[Your system IP Address]/#/login in your browser it will open the login form.



2. **Fill** in your BioStar 2 credentials to log in, **go to** the setting page, and **select** Card Format.

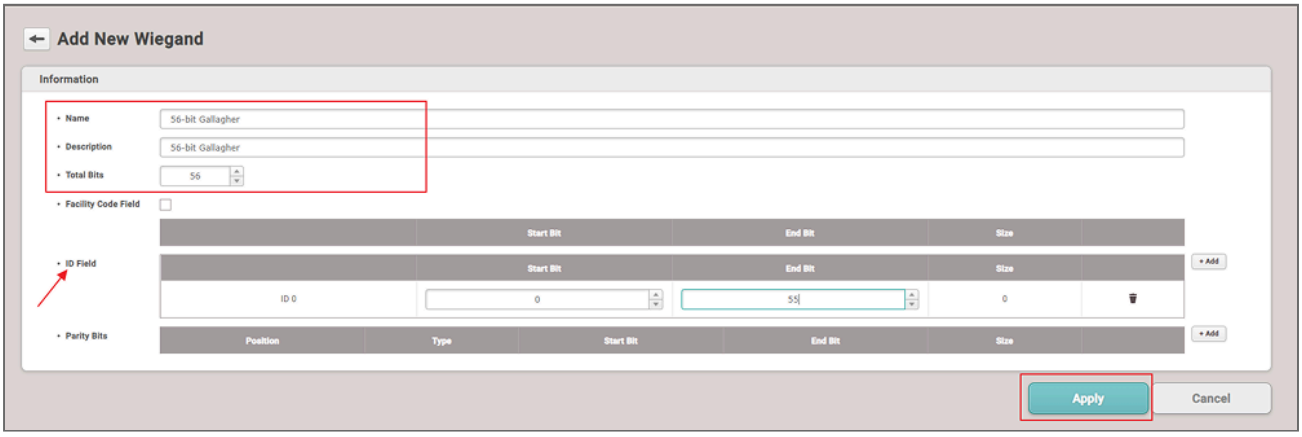


3. In the card, setting **click** on the **edit** button to create a new card format.



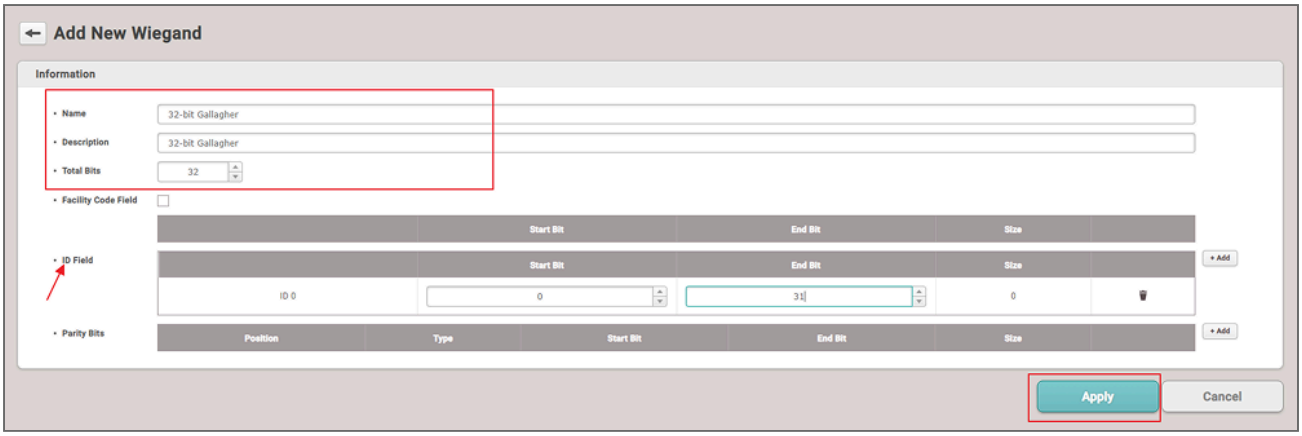
4. Here also we have to create three card types **56-bit**, **32-bit**, **and 26-bit**.

   1. **Set** name as **56-bit Gallagher** total bits as 56 and in ID field **press** add **set** start bit as 0 and end bit as 55.

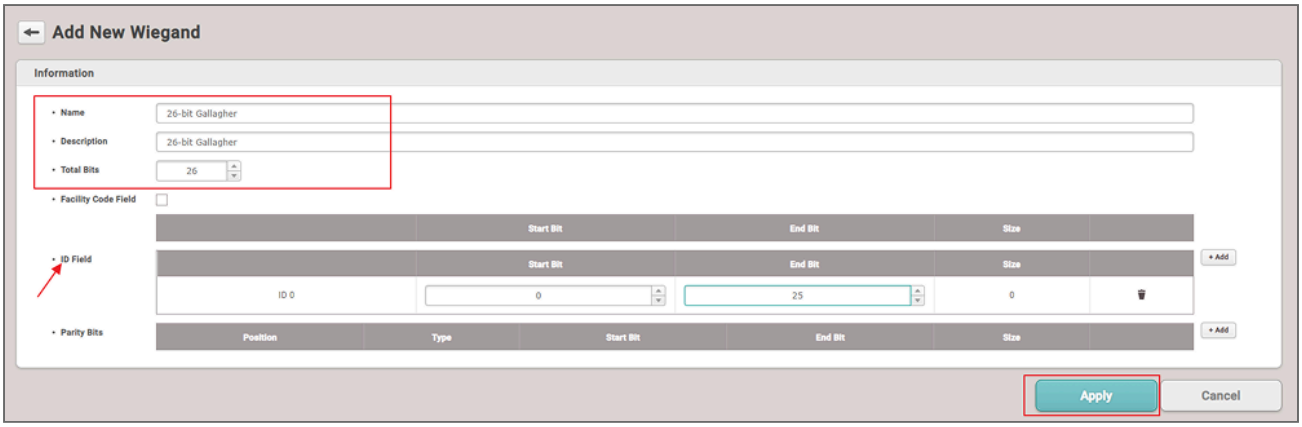


   2. **Set** name as **32-bit Gallagher** total bits as 32 and **ID field** and in the ID field **press** add & **set** start bit as 0 and end

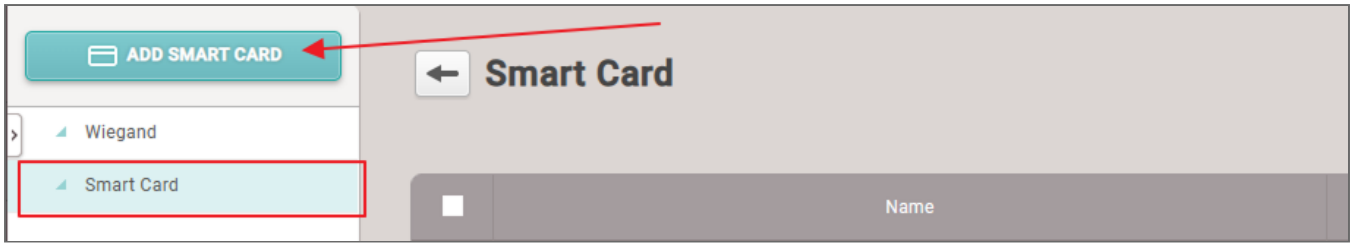
bit as 31.



3. **Set** the name as **26-bit Gallagher** total bits as 26 and **ID field** and in the ID field **press** add & **set** the start bit as 0 and end bit as 25.

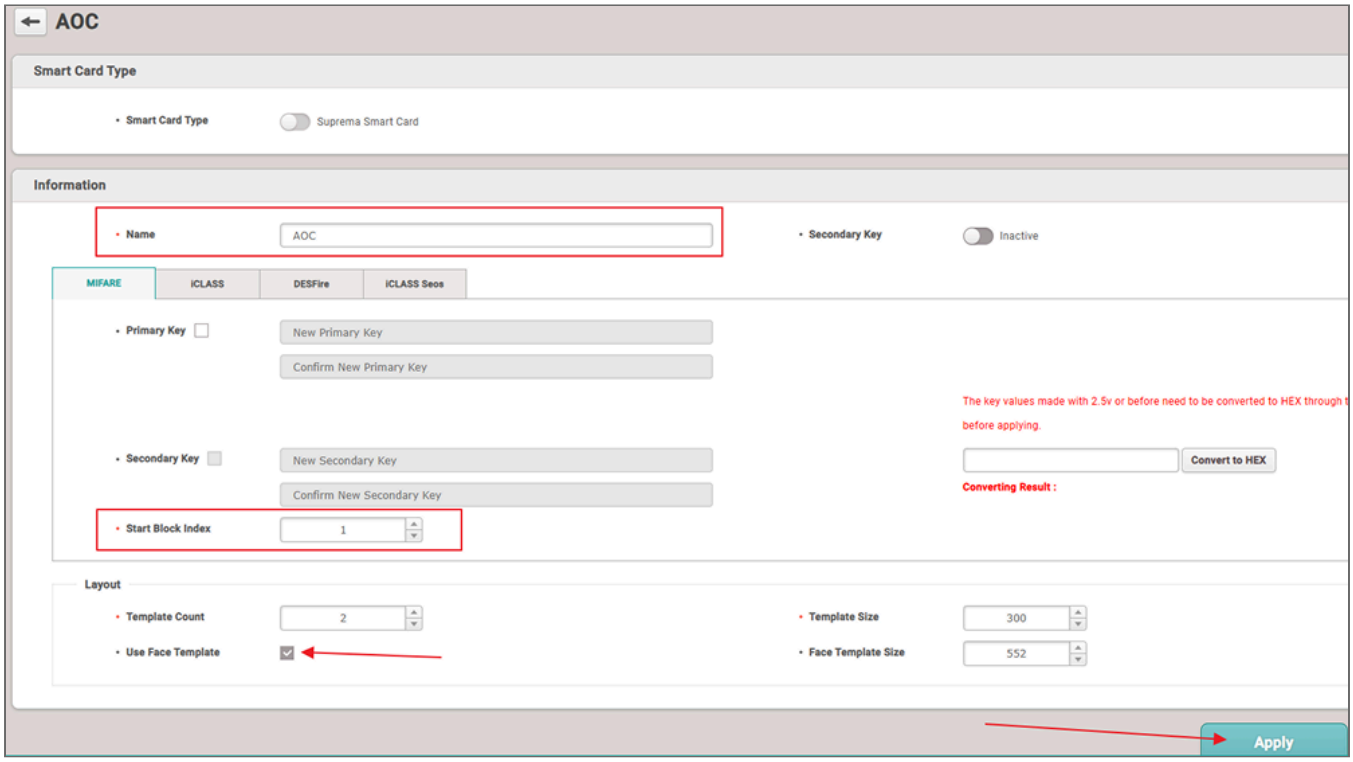


5. Now inside the card format **go to** the smart card section by **pressing** the smart card button and **click** on the ADD SMART CARD button.

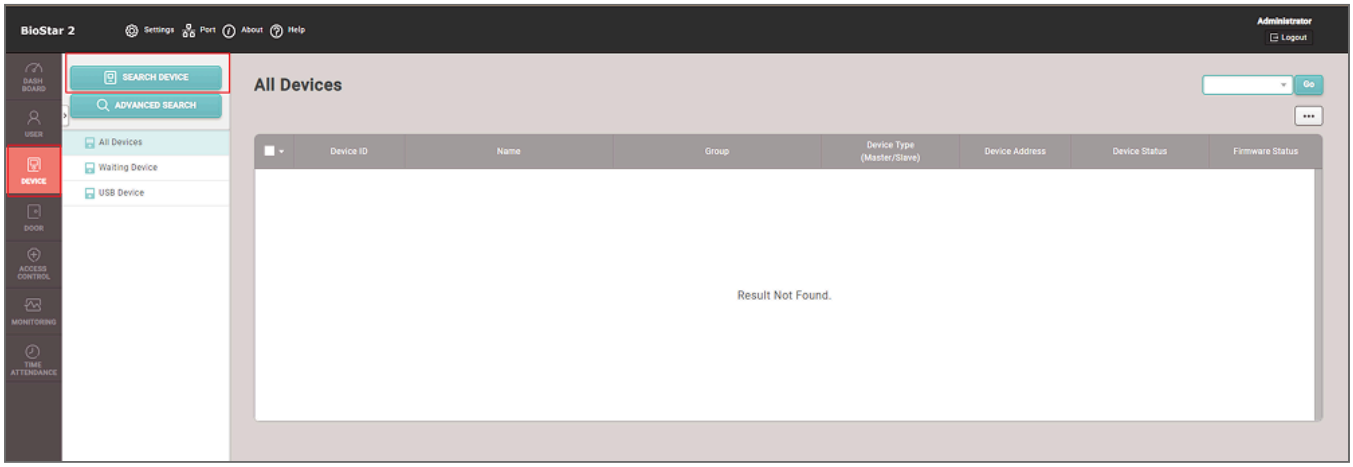


6. Now enter the **name** as AOC Inside MIFARE type **enter 1** for Start Block Index, **tick** the checkbox for Use Face template, and **press the** Apply button.

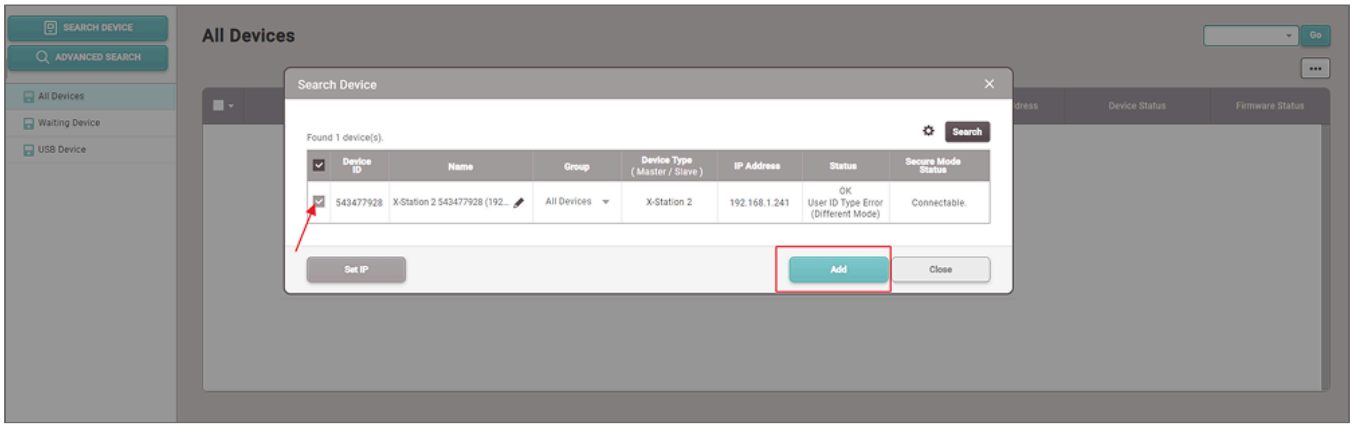
> **Info**
> If you don't want to use a visual face and only want to use a fingerprint on the smart card you can untick the checkbox.



7. To connect devices to the system **go to** the device panel and **press** the SEARCH DEVICE button.



8. Now **press** the search button and **select** the device and **press** Add button.



9. The connected devices will be listed on the device panel on the left side.



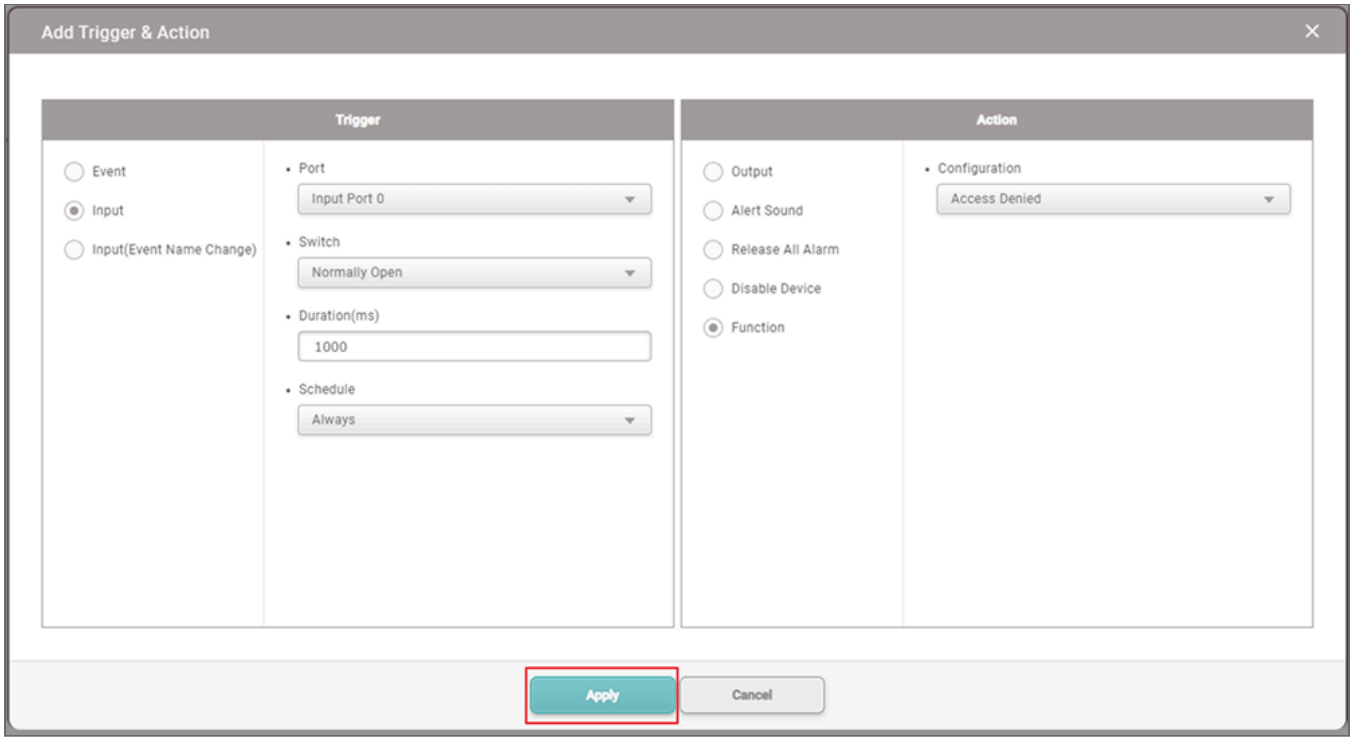
Wiegand's READER CONNECTION

1. **Click** on the device that is connected via the Wiegand connection. **Scroll down** until you see Card Type.

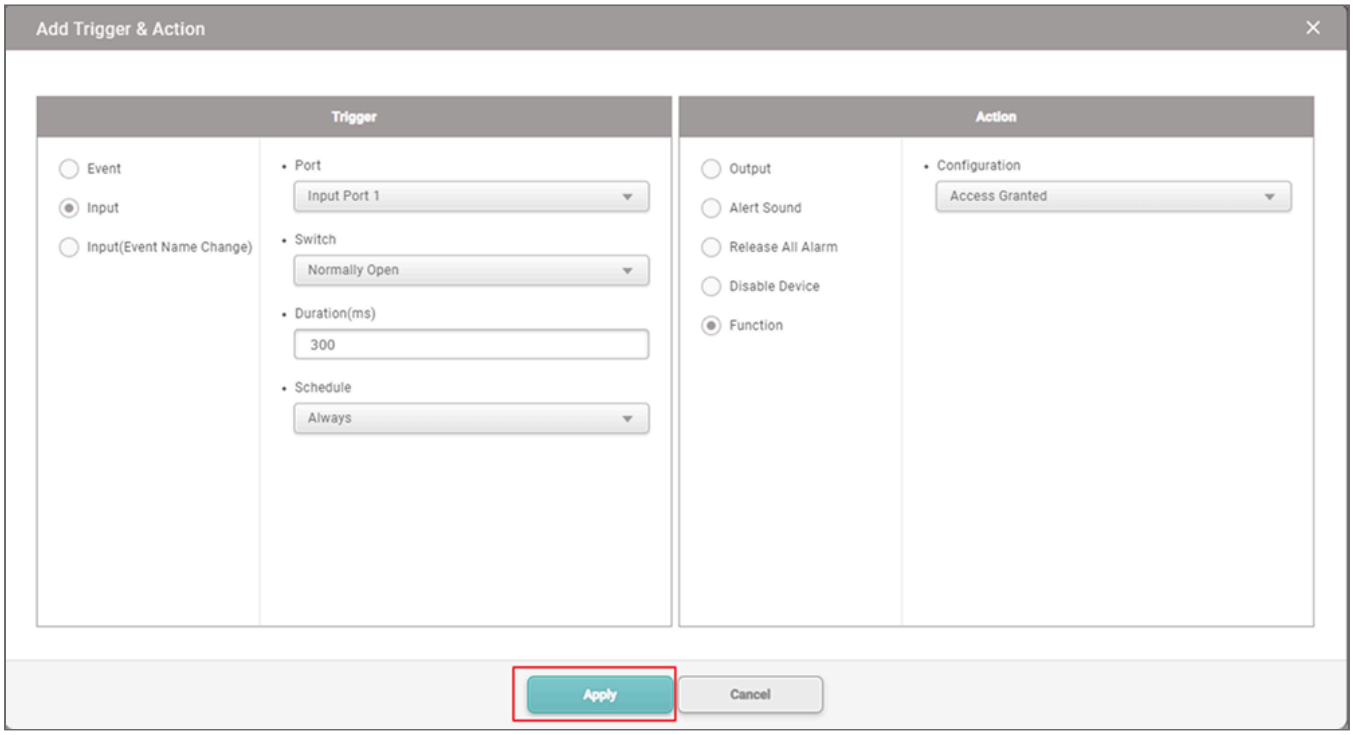
   Please **turn on** the **CSN card**, **tick** the **Mifare/Felica**, **set** the format type as **Wiegand**, Byte order as **LSB**, and Wiegand format as **56-bit Gallagher**.



2. Now **go to** the advanced setting and scroll down until you see the trigger and action **press** add button, and **set** the field as shown in the image.



3. Again **press** the add button to add another trigger and action.



4. In the Advanced Section below Trigger & Action: Wiegand setting Input/Output should be set as **Output**, Wiegand Input Format as Default, Pulse width as **40**, pulse interval as **10000**, output mode as **normal**, check fail code, and output info to the **Card ID**.



OSDP READER CONNECTION

1. For OSDP connection **click** on the device that is connected to the OSDP panel and scroll down until you see Serial.

   Set RS485 as Default and Baud rate as **115200**.



2. In intelligent slave expectation code as **Enabled**, output info as Card ID OSDP ID as **0**.

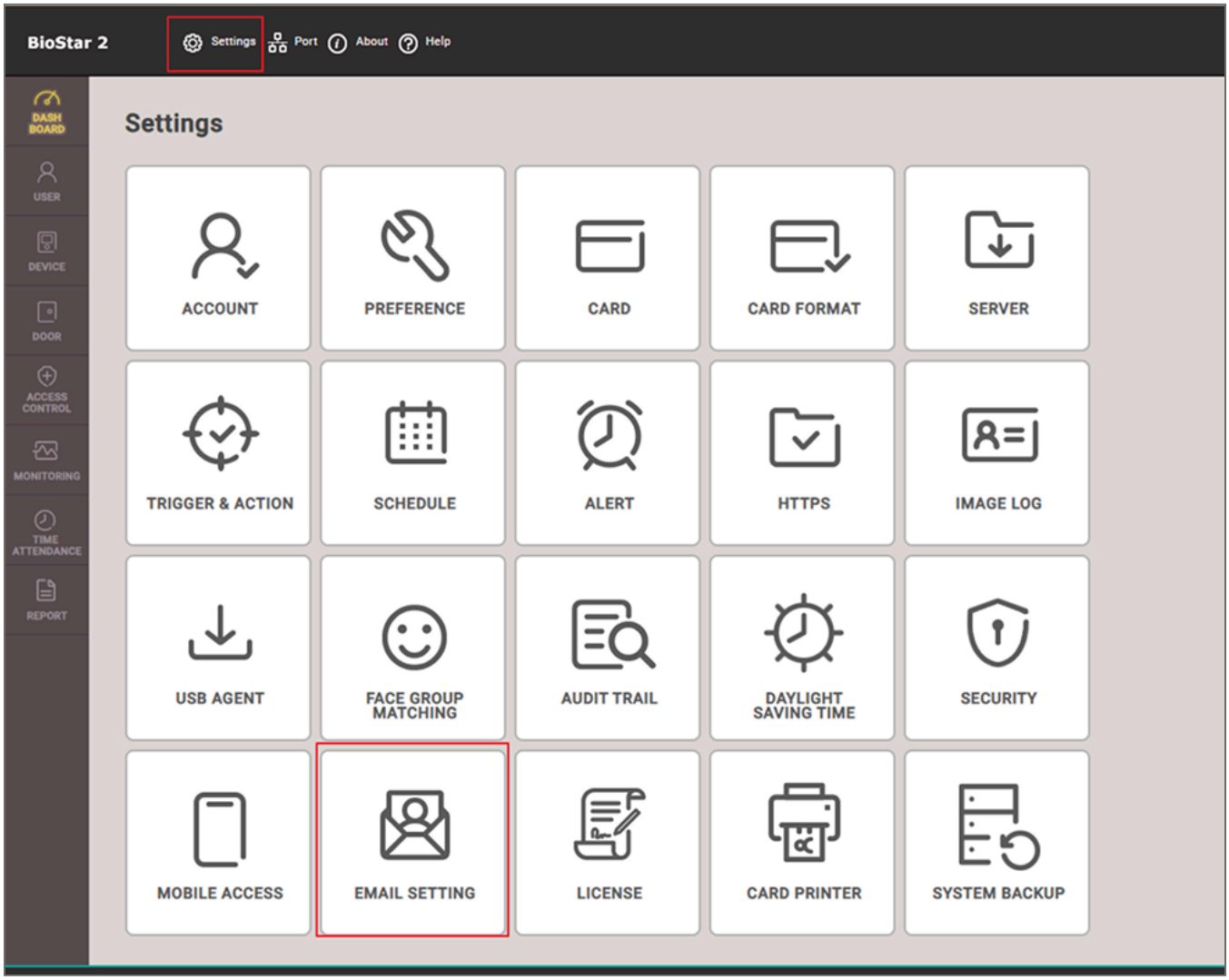
> **Info**
> If you have more OSDP devices then please **change** the OSDP ID to another number and for output, Info must be Card ID.



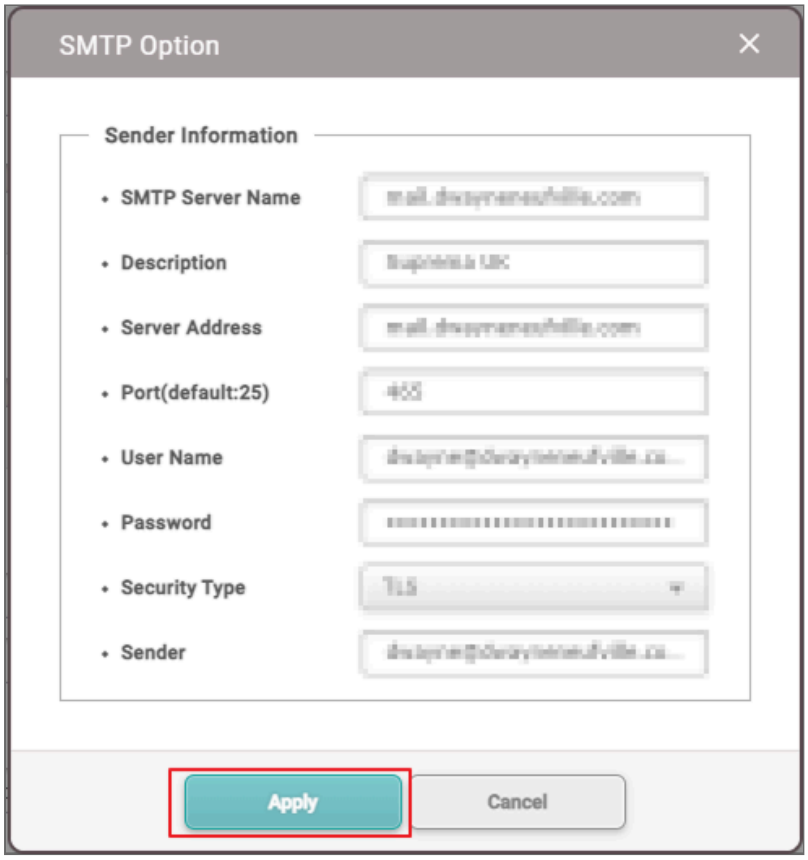
Email Configurations for QR Code

> **Info**
>
> - Email confirmations and Emails for user profiles are a must be required for QR Code.
> - Licenses are required for emails. Please contact the administrator to obtain the necessary licensing.

1. **Go to** the settings page and **select** Email Settings.

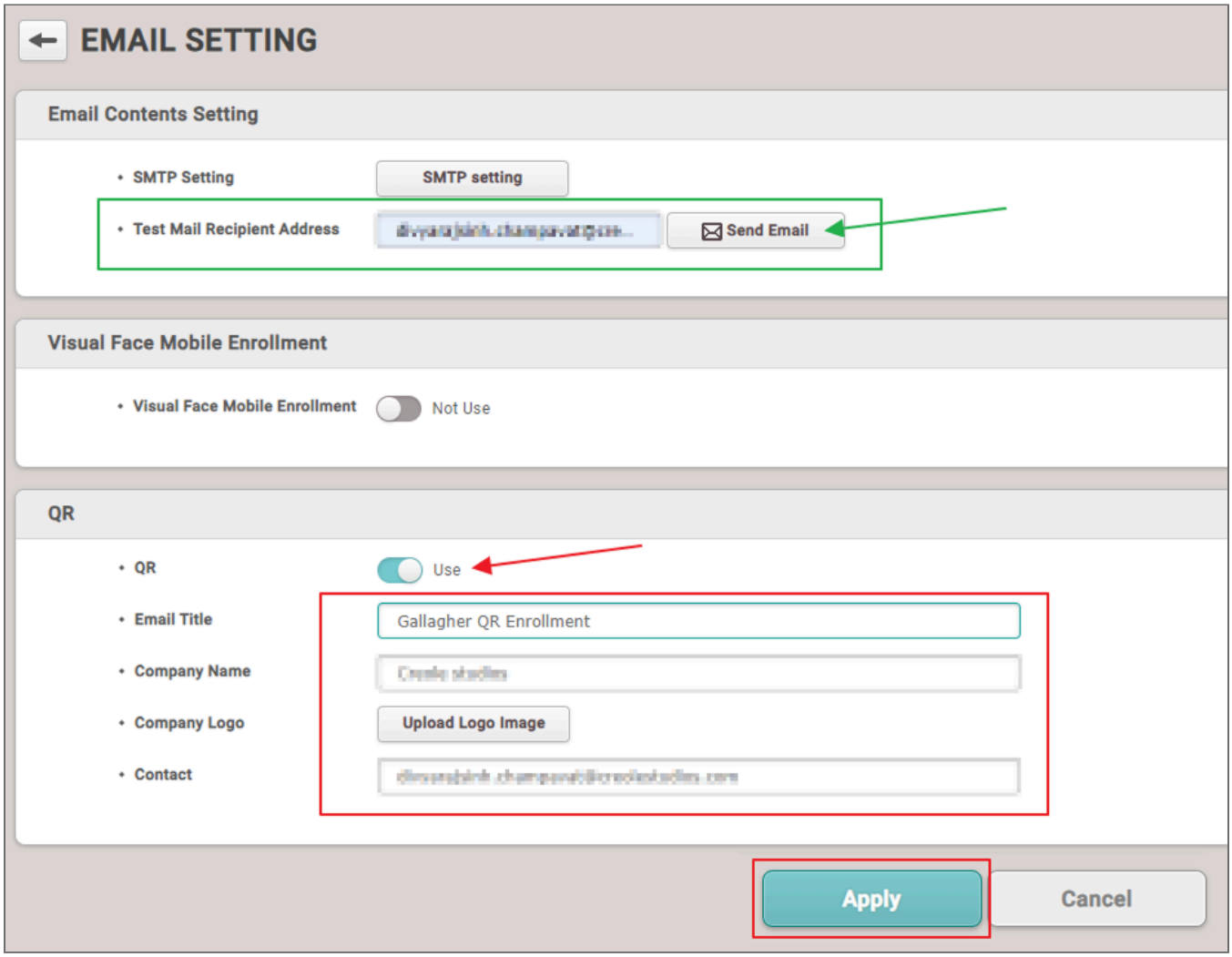


2. **Press** the SMTP setting button inside the email setting, fill in the details for the SMTP Option, and **press the** Apply button.



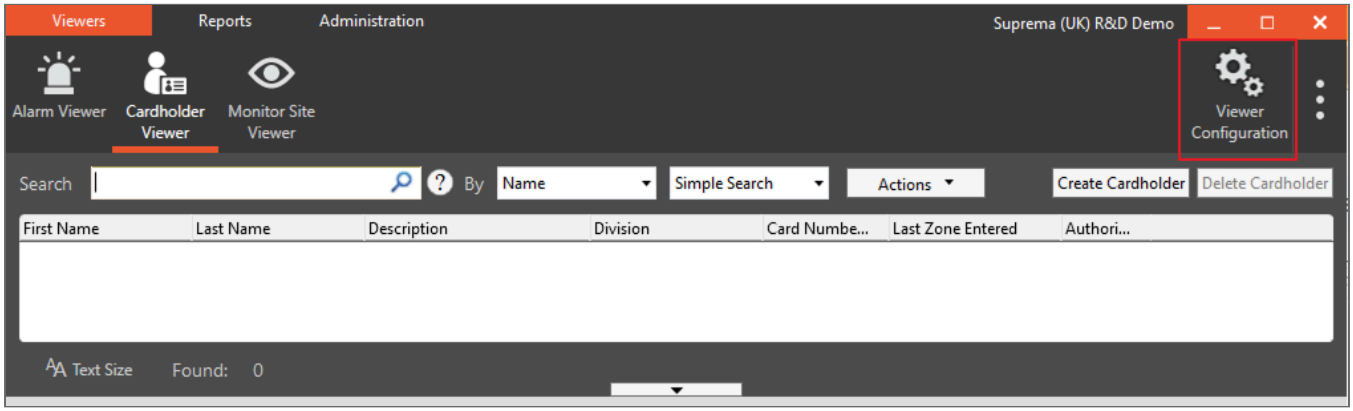
3. To cross-check, you can use the test mail functionality, where you need to put the email address you want to test with and **press the** send email button.

   To use the QR Code card, **enable** the QR option inside the settings, Put the details as per requirements, and **press** the Apply button.



Suprema Integration with Gallagher v2.0

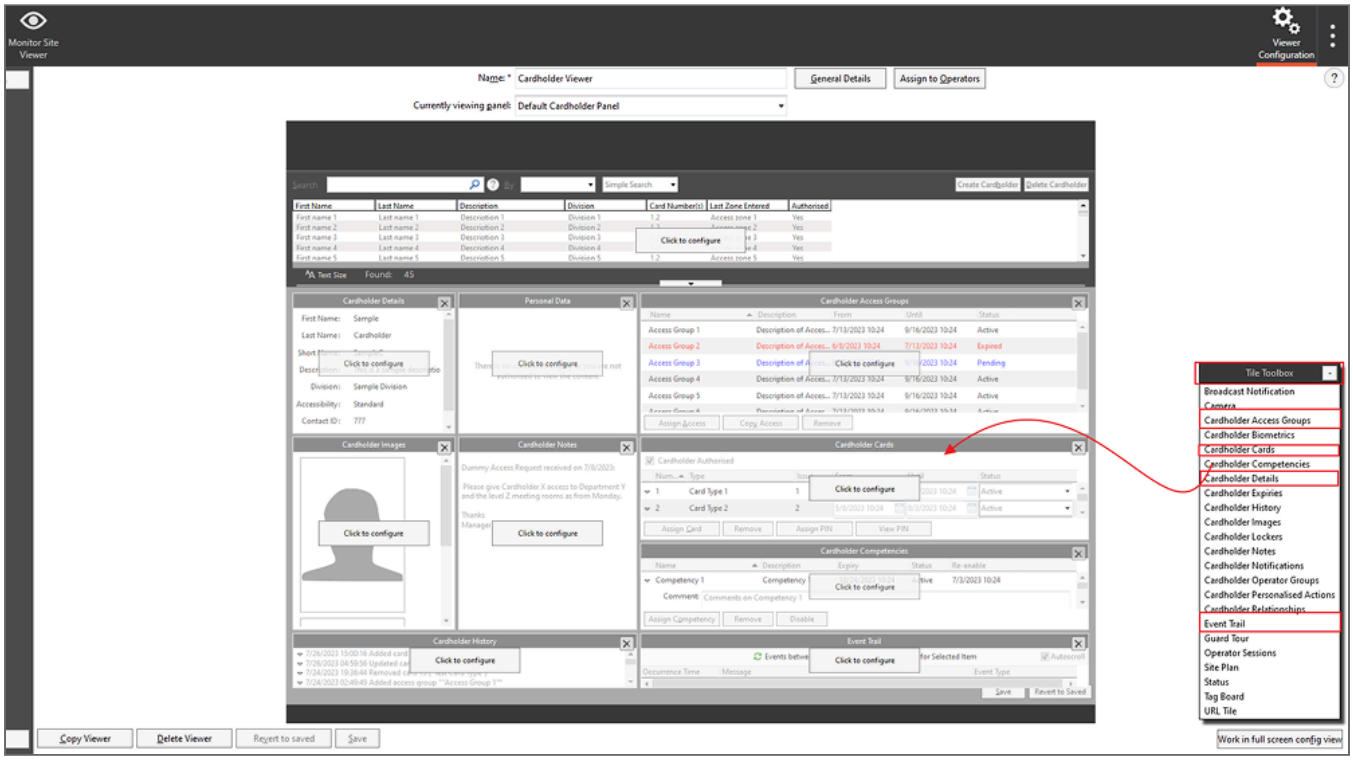
1. **Open** Gallagher Command Centre in the Cardholder viewer option and **go to** viewer configuration.



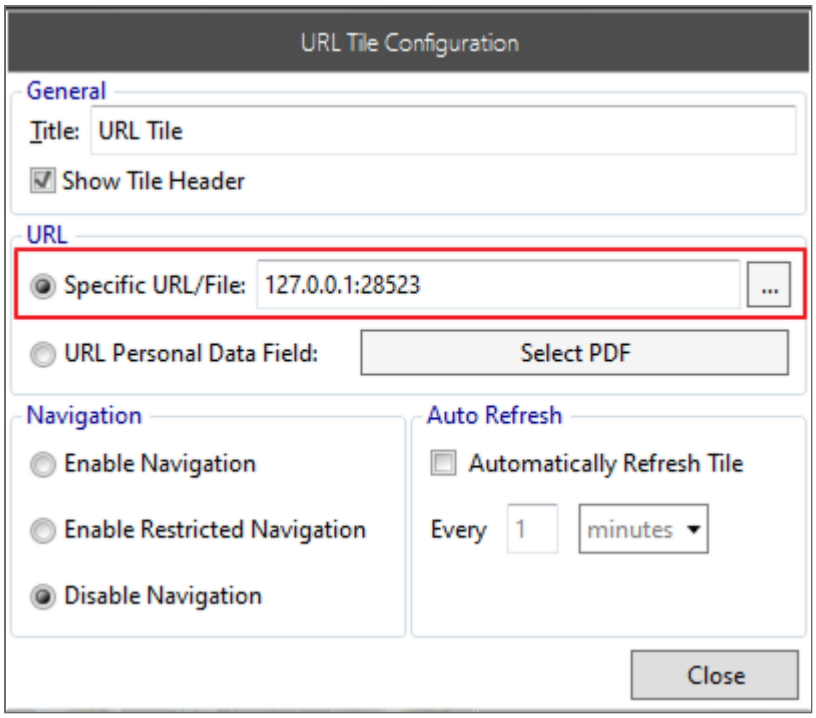
2. In Viewer Configuration, set windows as shown in the image below, and use the window toolbox to **drag and drop** windows.

   - Cardholder Details
   - Cardholder Access Groups
   - Cardholder Cards

- Event trail
- URL Tile
- Cardholder Images



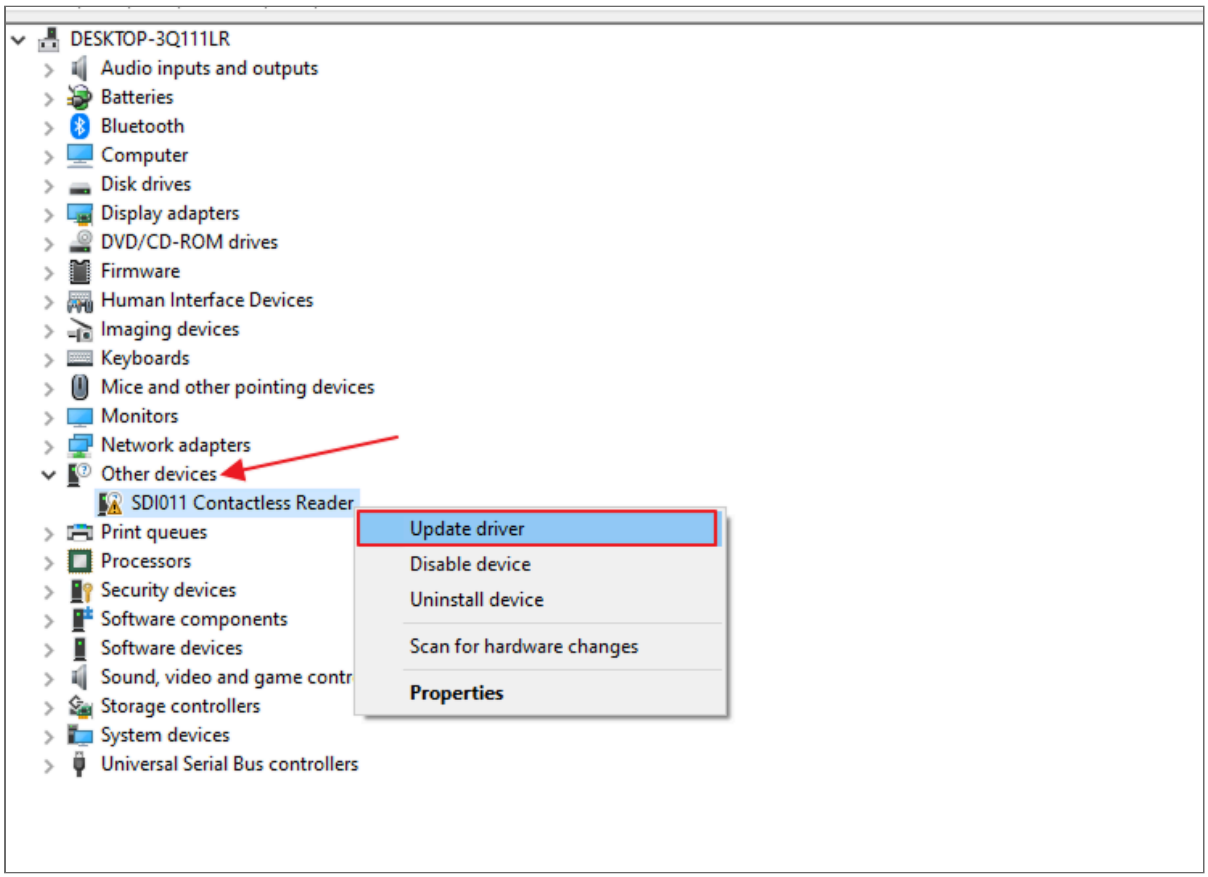
3. In the URL window **press** click to configure the set Specific URL to `<127.0.0.1>:28523` and choose navigation as Disable Navigation. And **press** the **save button** to save the settings.



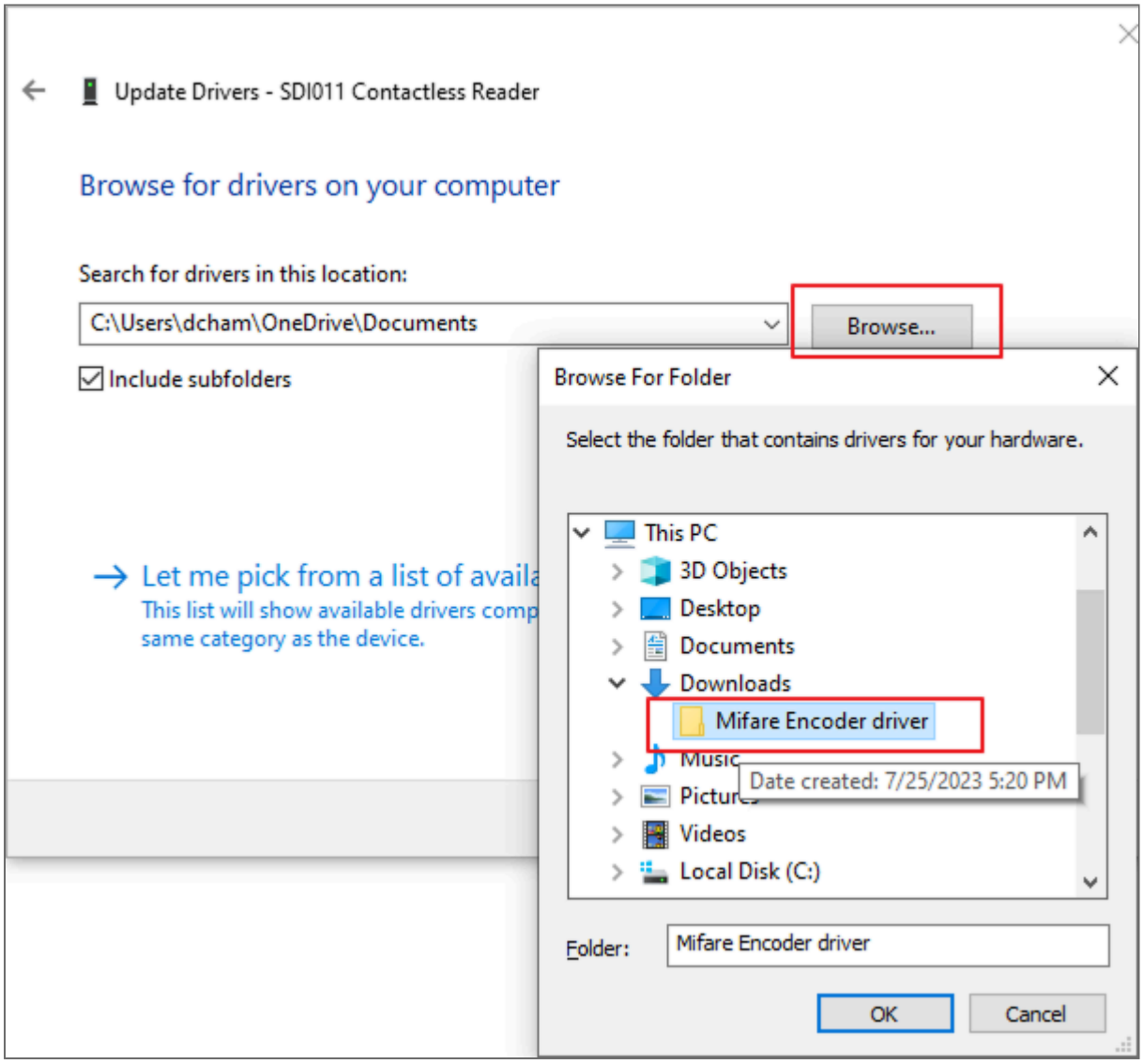
4. After completing the configuration **press** the **save button** then **right-click** on viewer configuration and reload the viewer to see the change.

5. **Connect** the **Mifare Encoder** to the PC.

6. **Go to** the device manager in your system in other devices SDI011 Contactless Reader (In your case it can be a different device) **right-clicking** on that and choose the update driver.



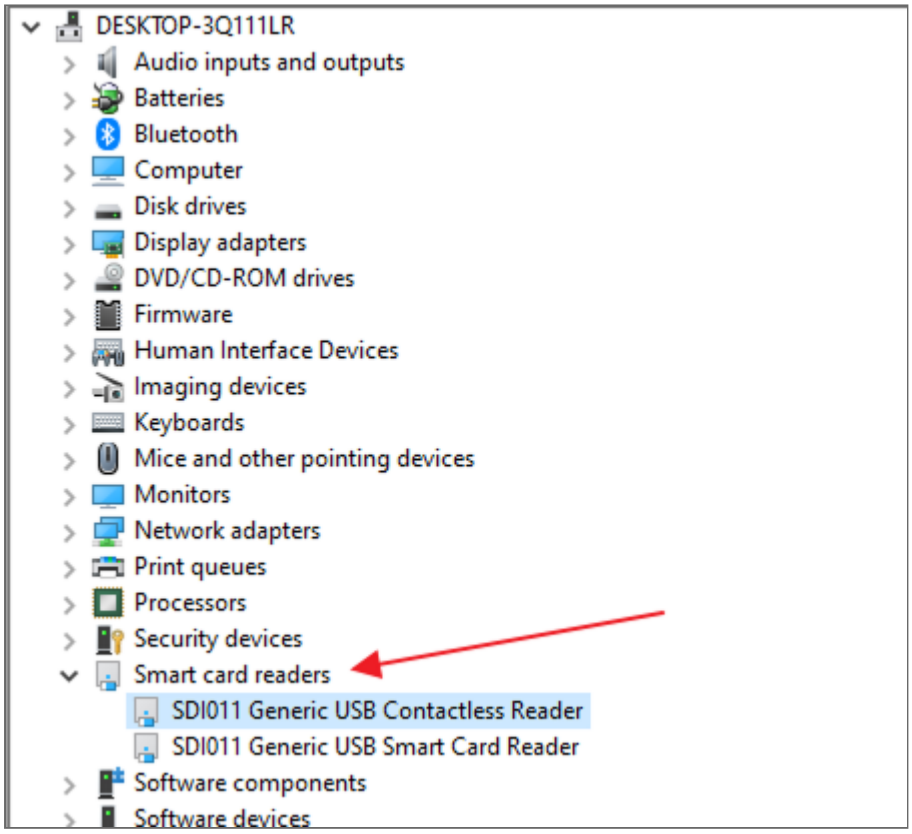
7. **Browse my computer** for the driver and select the folder that we have provided.



8. When you update the driver for the first time then a smart card reader will be available.

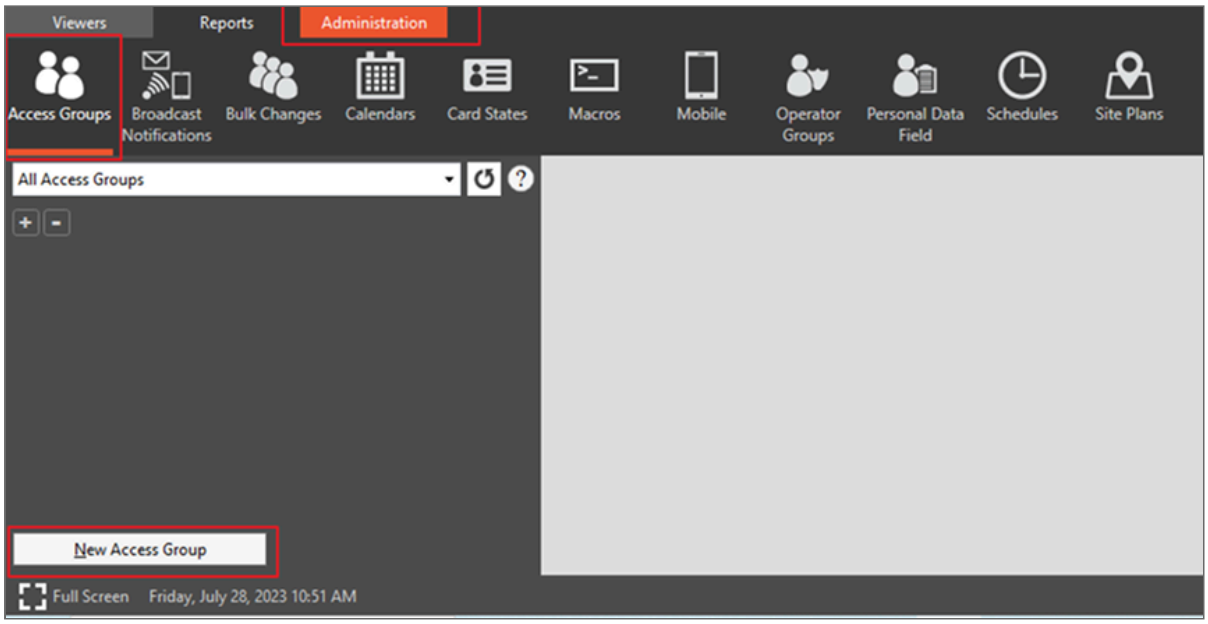
> **Info**
> The name USB device name could differ from device to device.

9. Now we have to update the Contactless Reader driver **again** with the same file. After you will see the new smart card driver will be available.

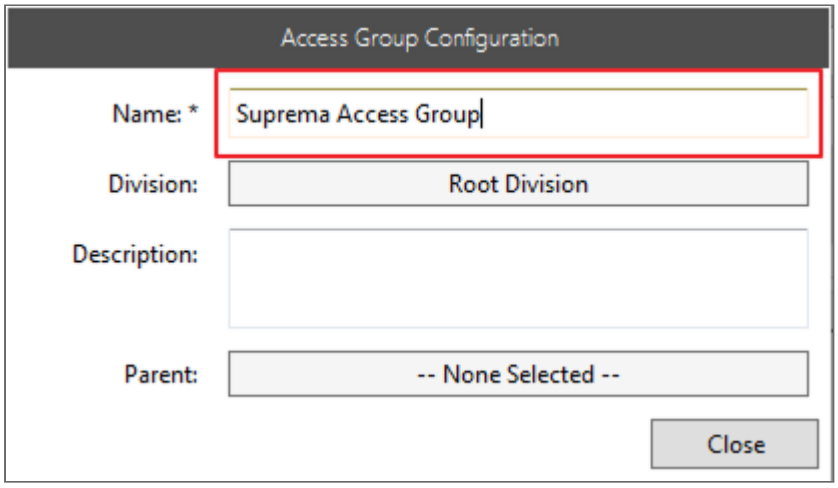


Add Access Group

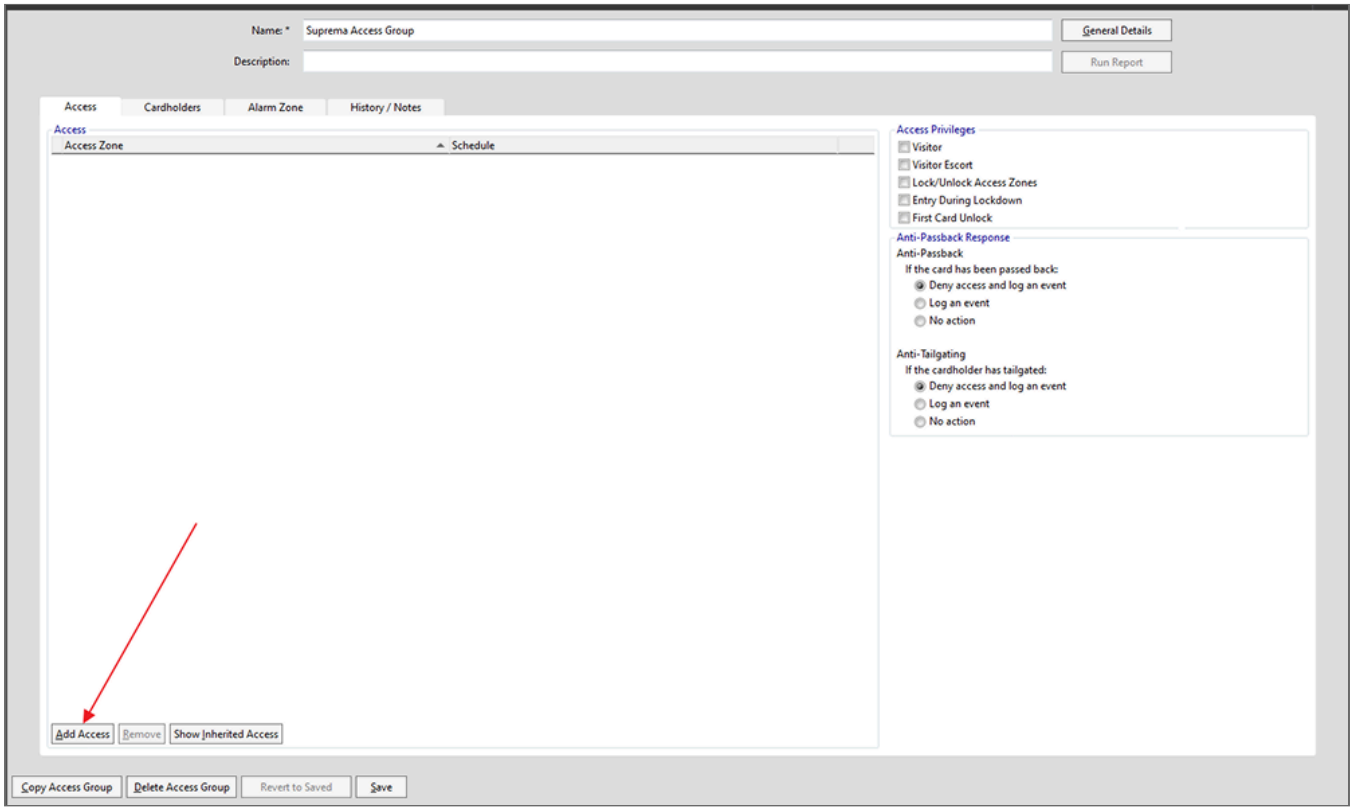
1. **Go to** Administration, where you can see **Access Groups** at the top left side **click** on that then you can see the **New Access Group** button at the bottom left side. **Click** on that button.



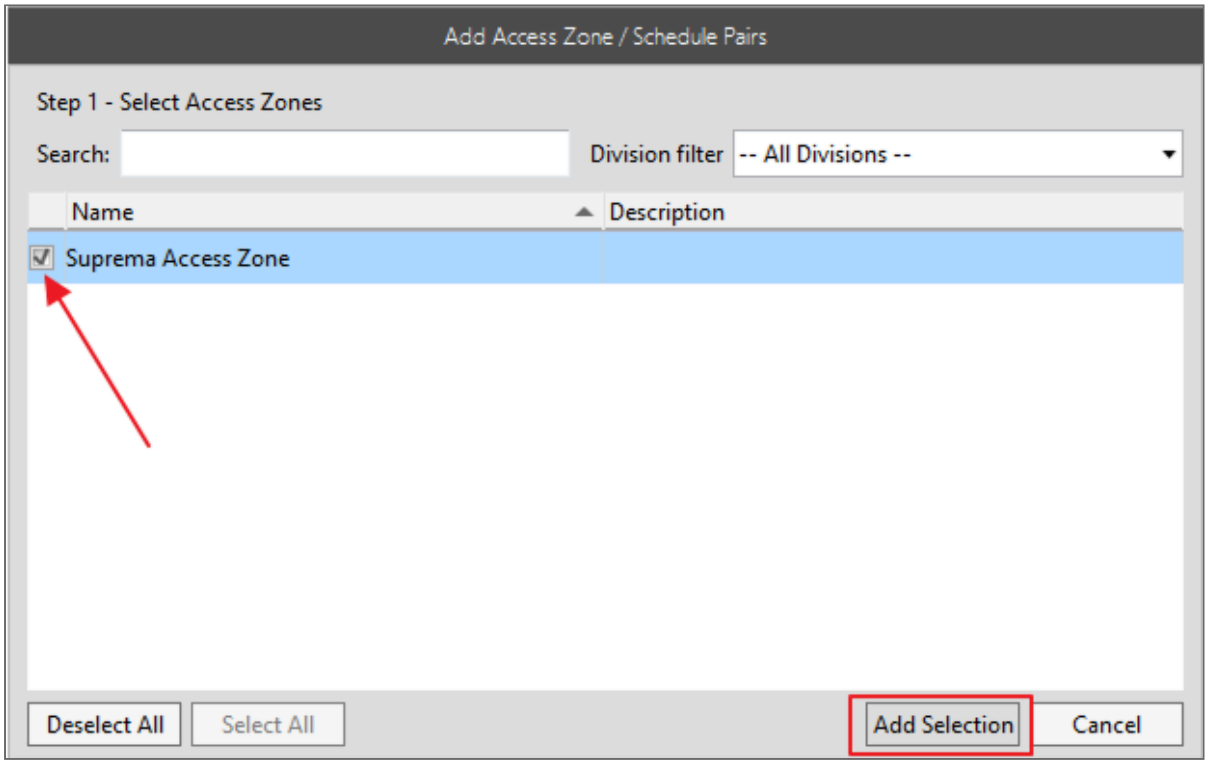
2. After **clicking New Access Group button**, a pop-up will be opened as shown below image **set** the Name as **Suprema Access Group** and **click** on the Close button then a pop-up will be closed.



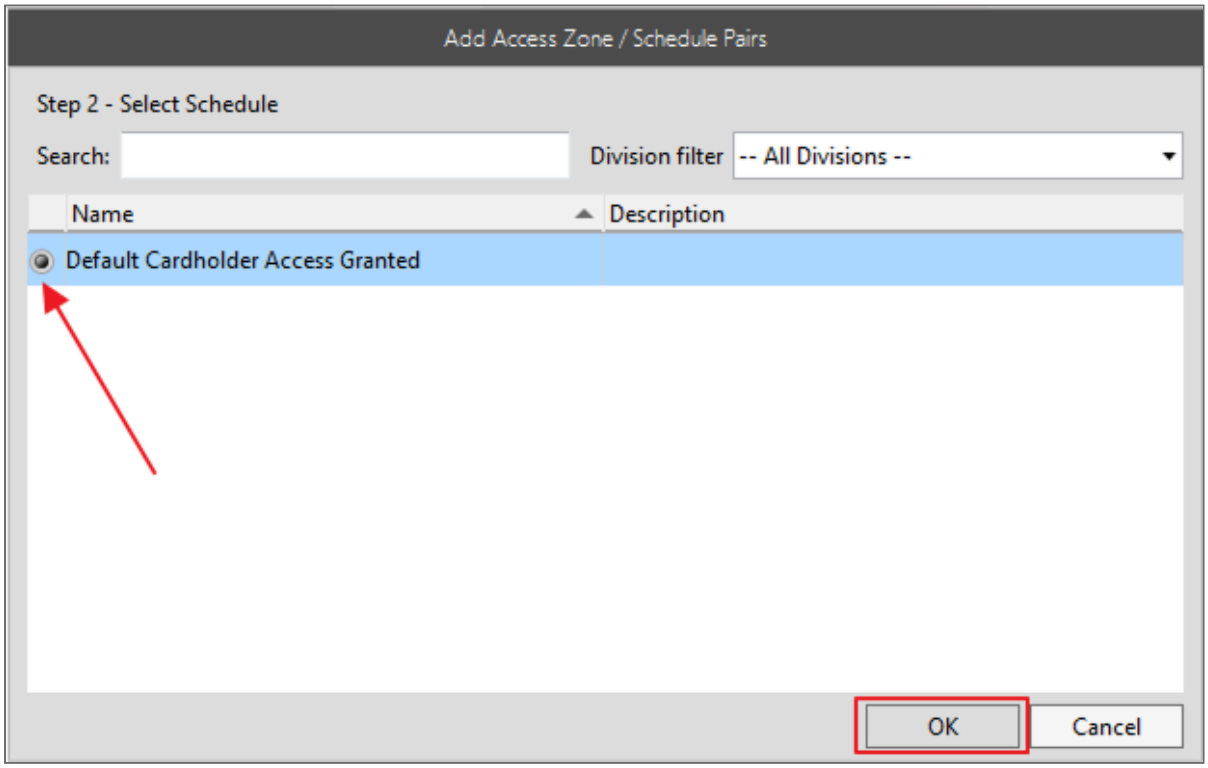
3. After **clicking** the close button, you will screen as shown in the below image, **click** on **Add Access button** at the left bottom corner.



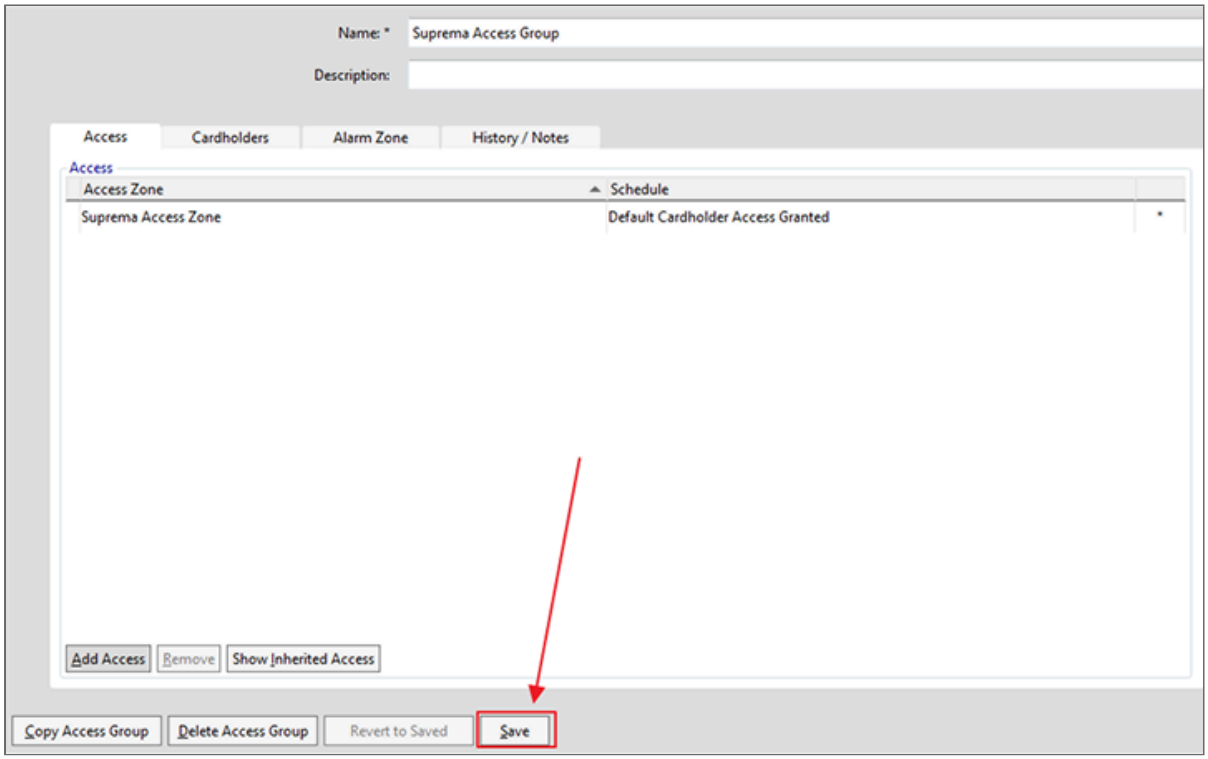
4. After **clicking Add Access** button, a pop-up will be opened as shown below image, in that **checked** the **checkbox** and then click on the Add **Selection** button.



Then **check** the **radio** button and click on the **OK** button the pop-up will be closed.

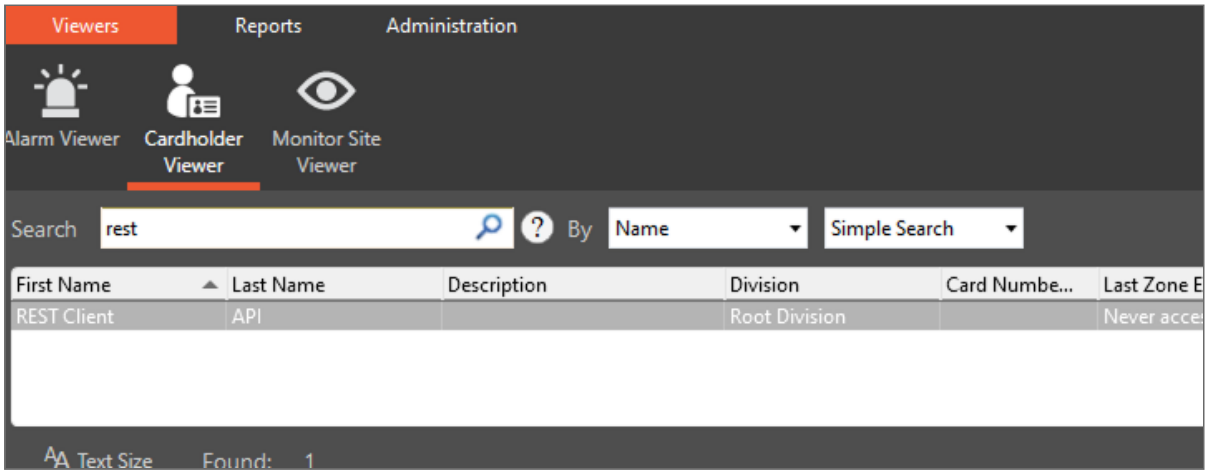


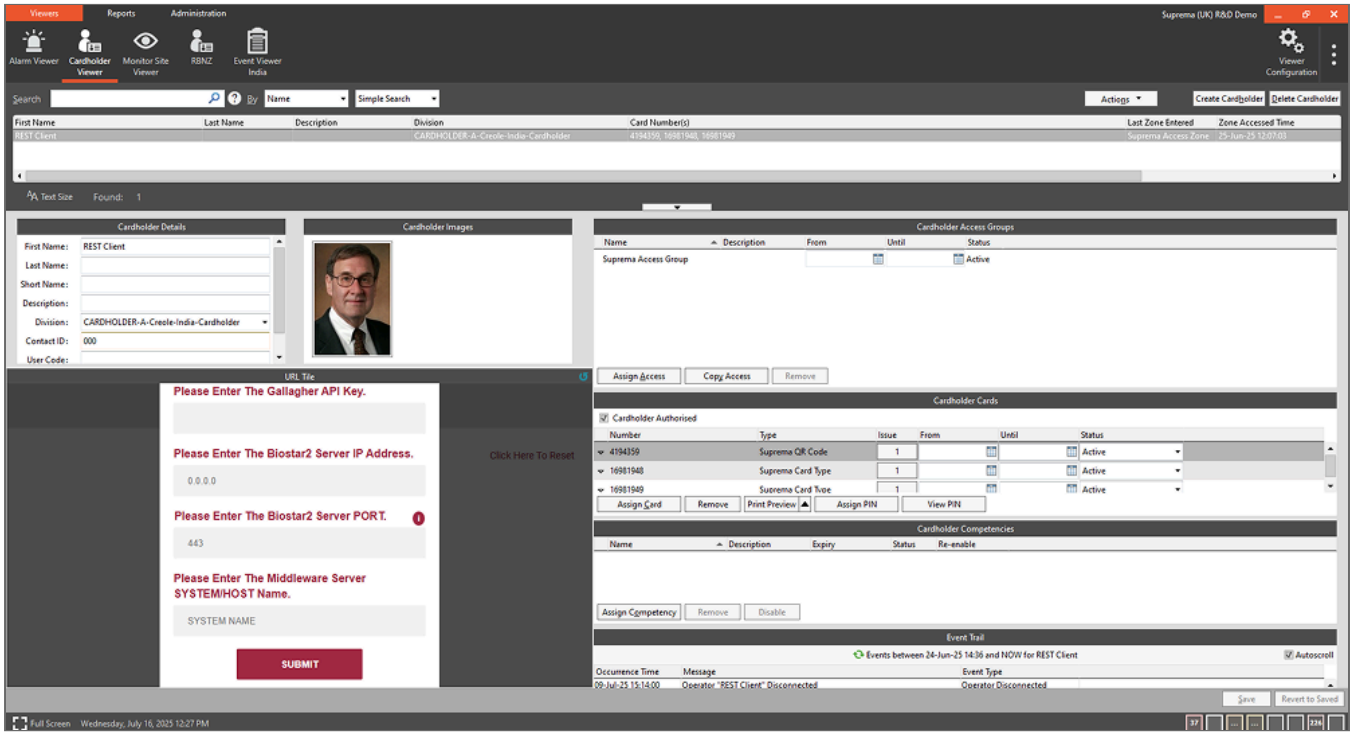
5. **Click** on the **Save** button your Access Group will be added successfully.


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 Integration with Gallagher

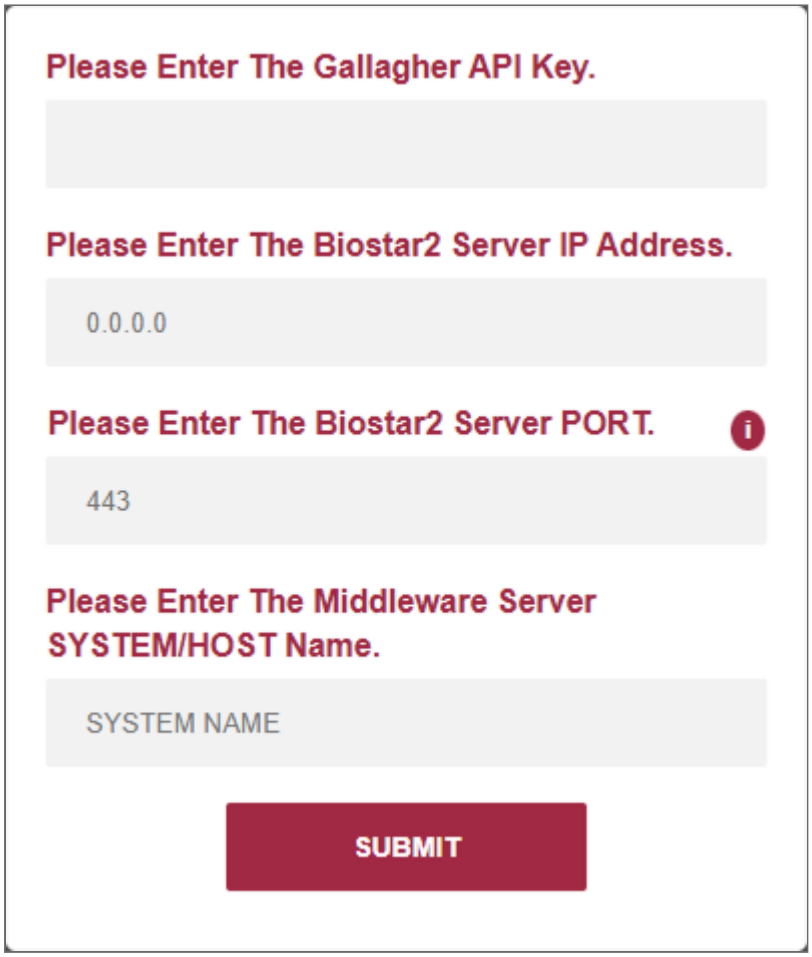
1. In Cardholder Viewer search rest and it will load all the windows.



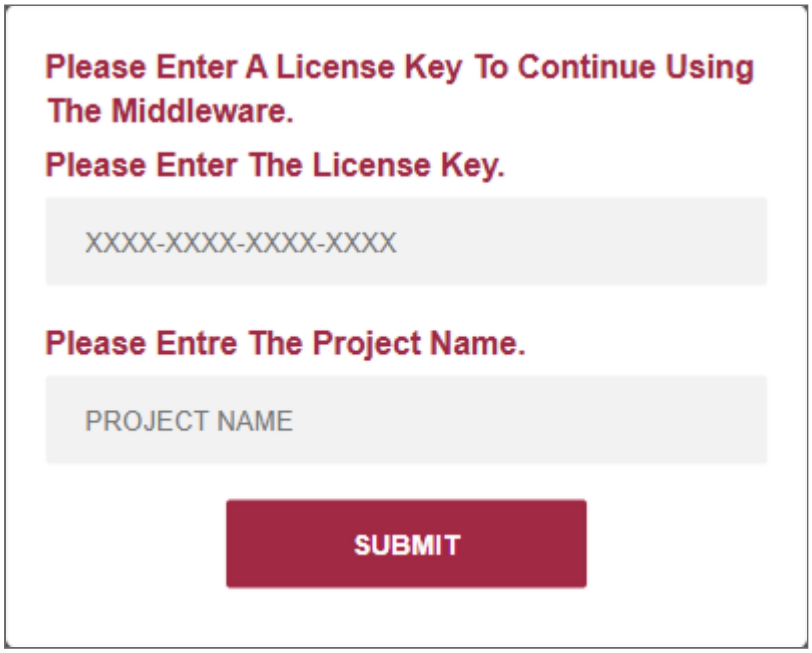


2. First, the screen below appears, and you need to **enter** the Gallagher API Key, BioStar 2 server IP, BioStar 2 server PORT, and SYSTEM/HOST name of the middleware address to move forward.

> **Info**
>
> If you are running the middleware on a specific port on two different servers with particular IP addresses, kindly refer to: Configure the inbound rules for the middleware.

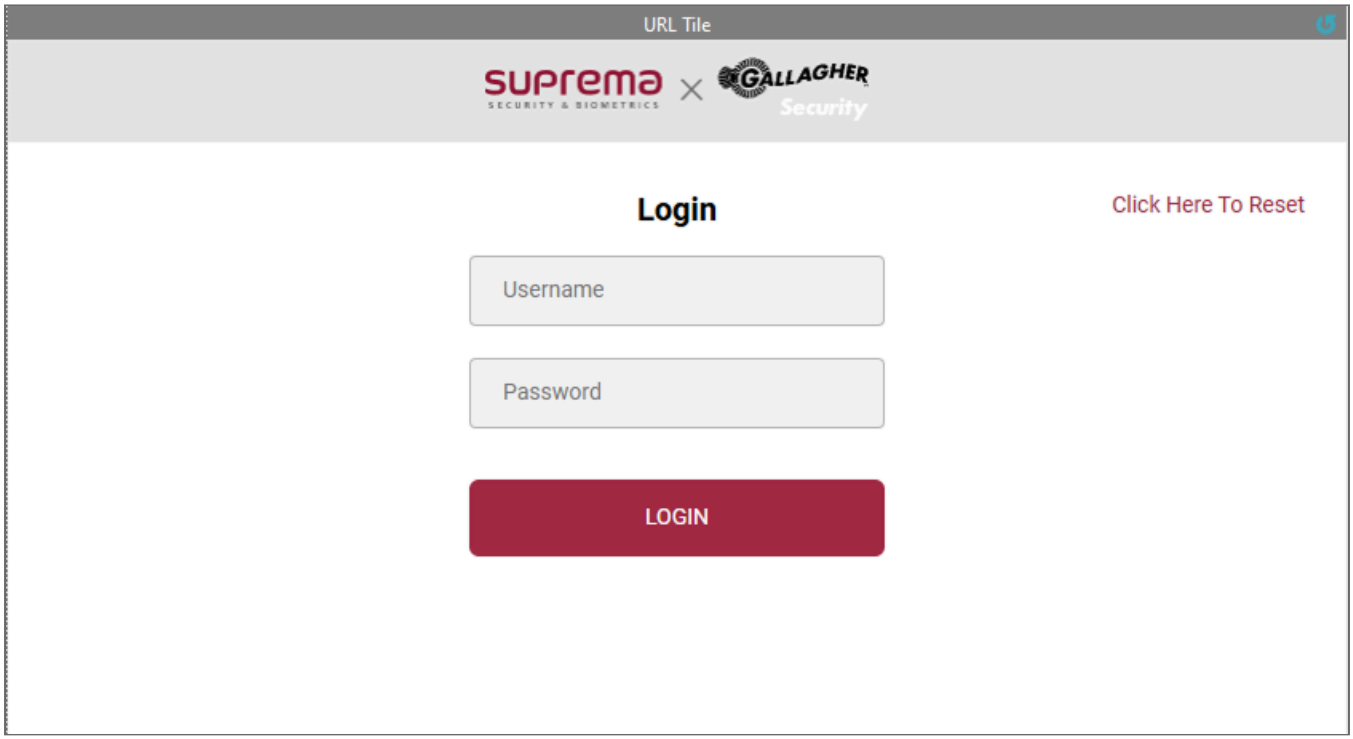


3. On the License screen, **enter** the License key and the **exact** project name that you get from the admin.

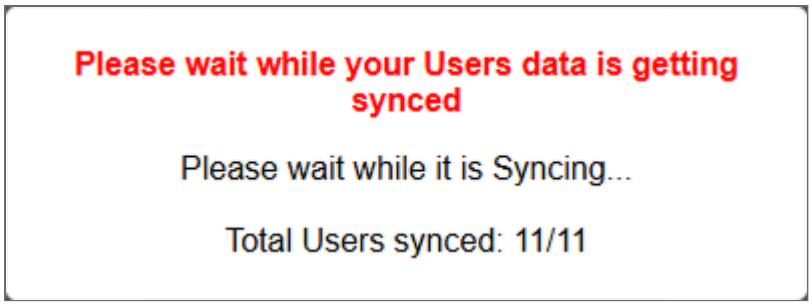


4. On the login screen, **enter** the credentials of Suprema BioStar 2.

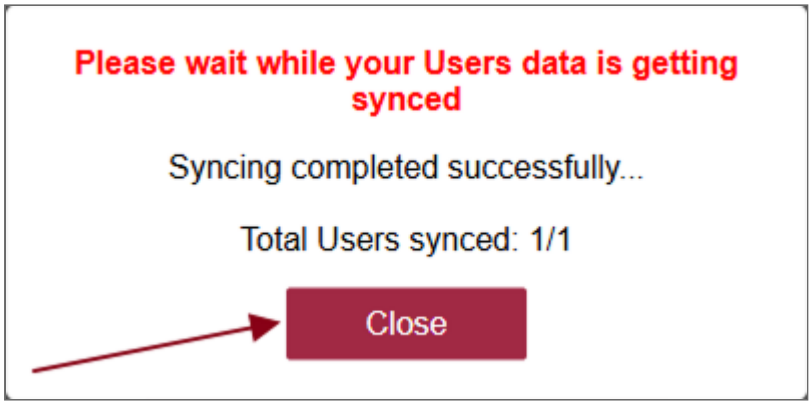
> **Info**
> On the Login screen if you get an **error** for **LAN is disconnected or IP is changed for (IP Address)**. Kindly refer to: Troubleshoot login page error.



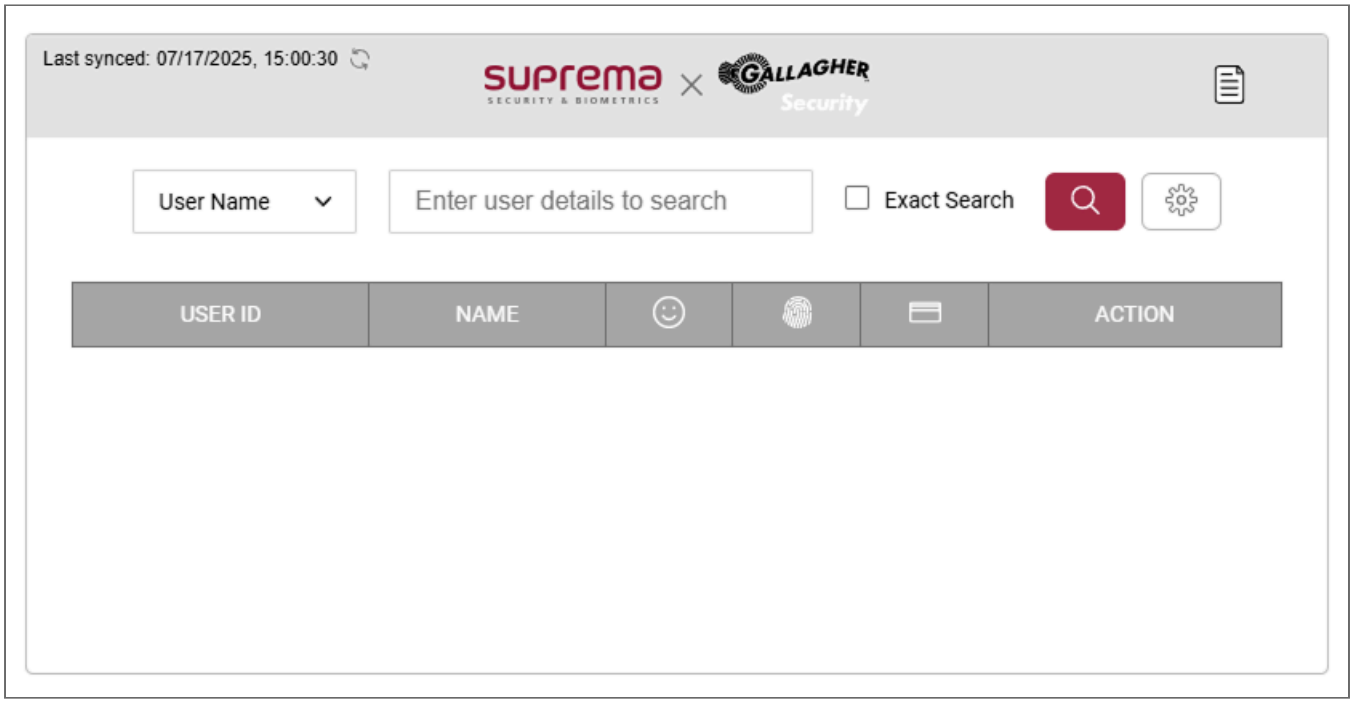
After entering the correct credentials, the below user sync screen will open for initial sync.



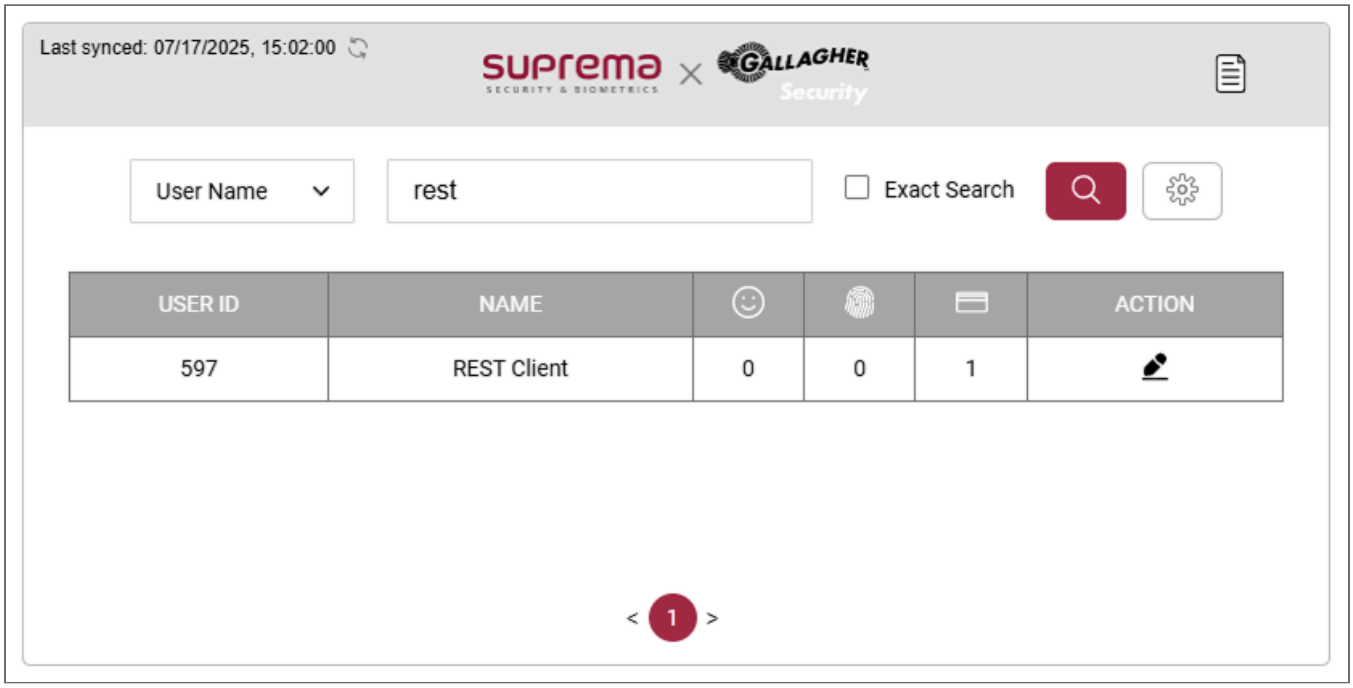
After successfully syncing the users, the close button will appear on the screen, and **pressing the** Close button to move further.



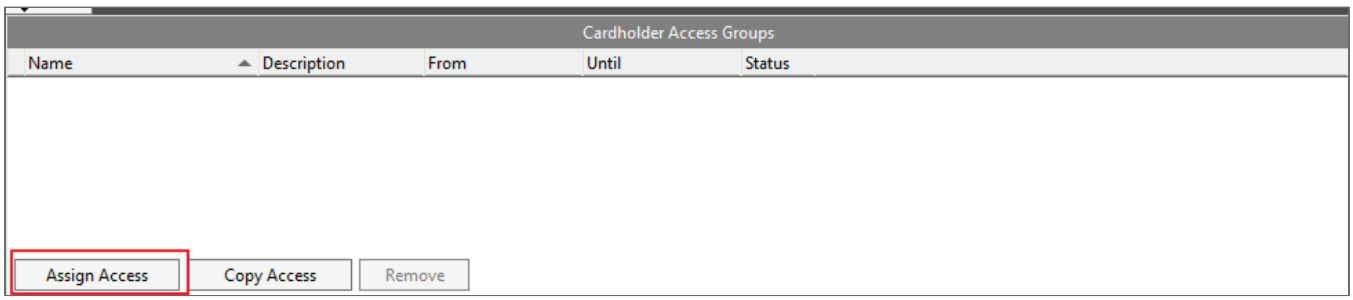
After successfully syncing the users, the user search screen will appear.

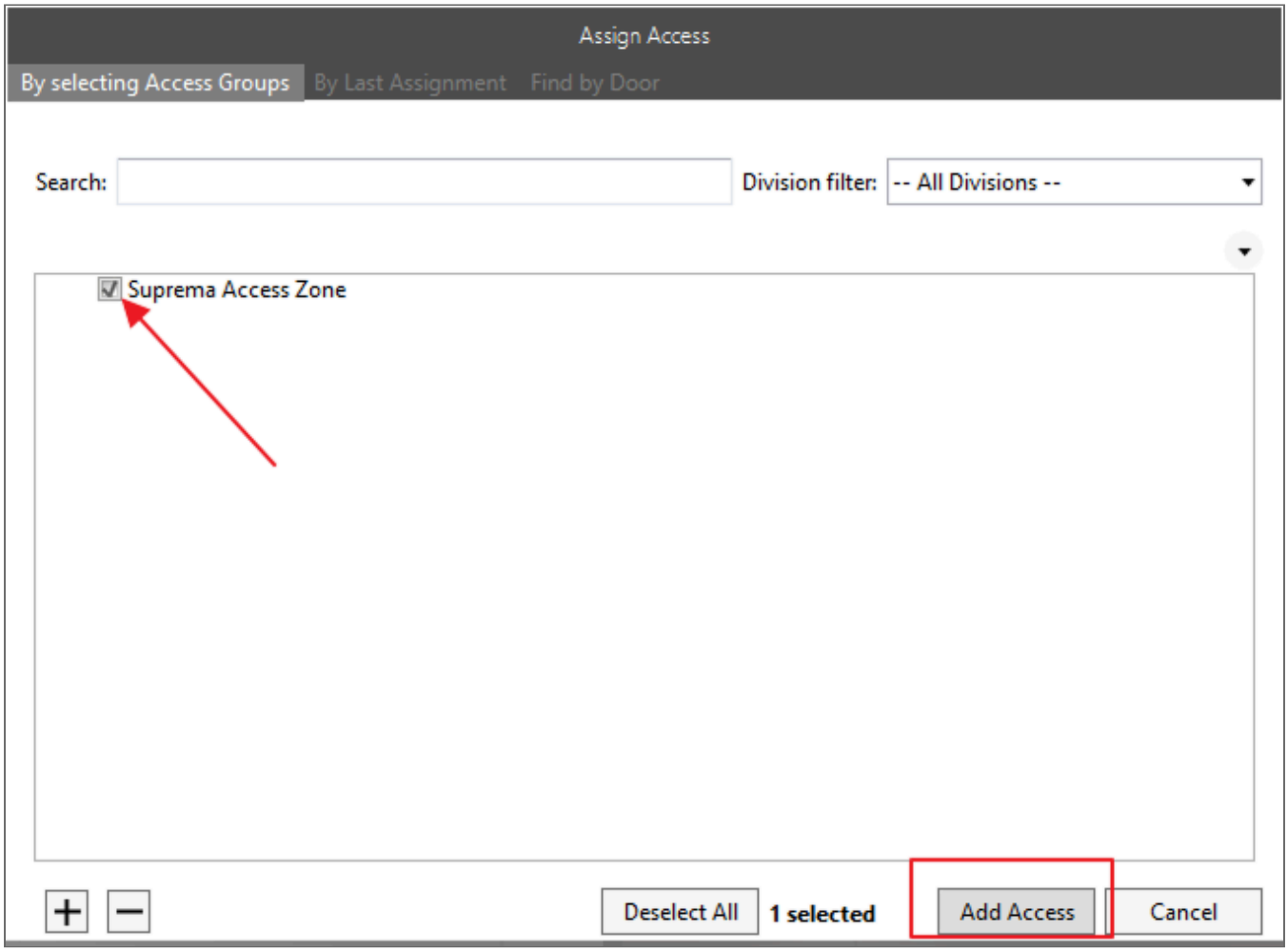


5. **Search** rest and press the search button and the search user will appear in the table.



6. Now, connect the Mifare Encoder to the system. **Press** the Assign Access button, choose the Suprema Access group we created, and **press** the Save button.

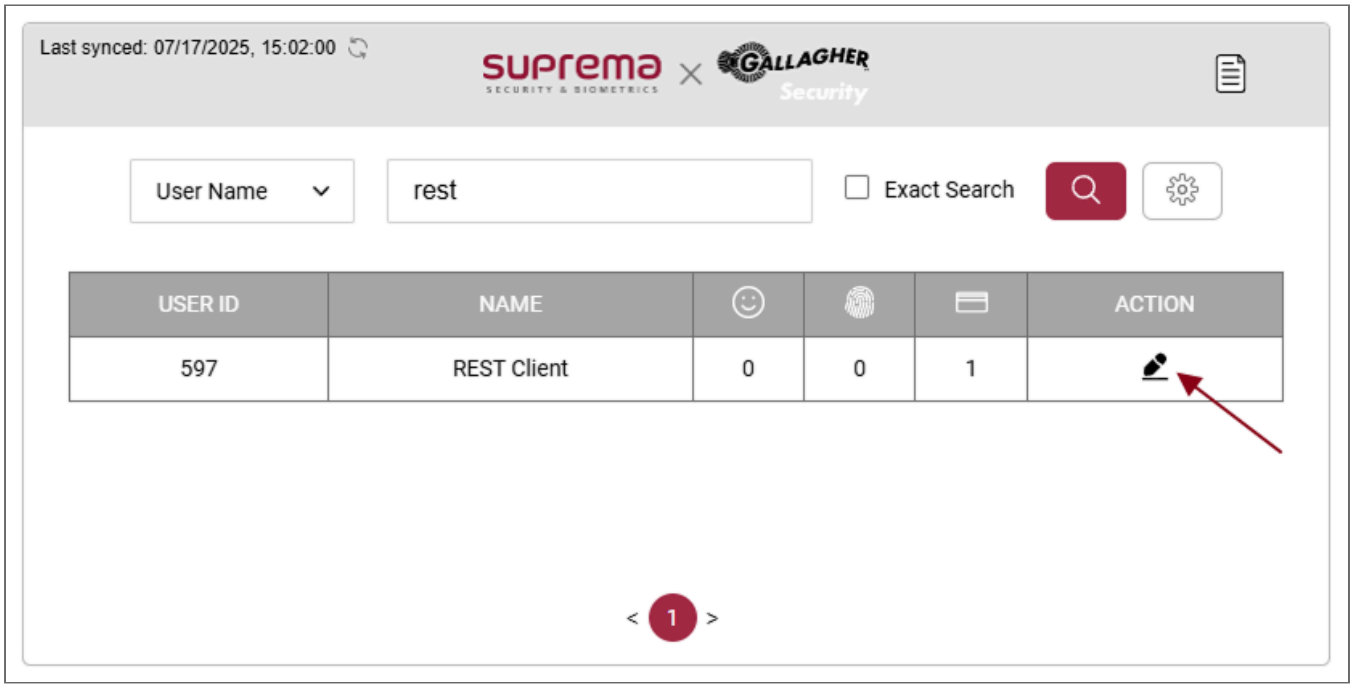




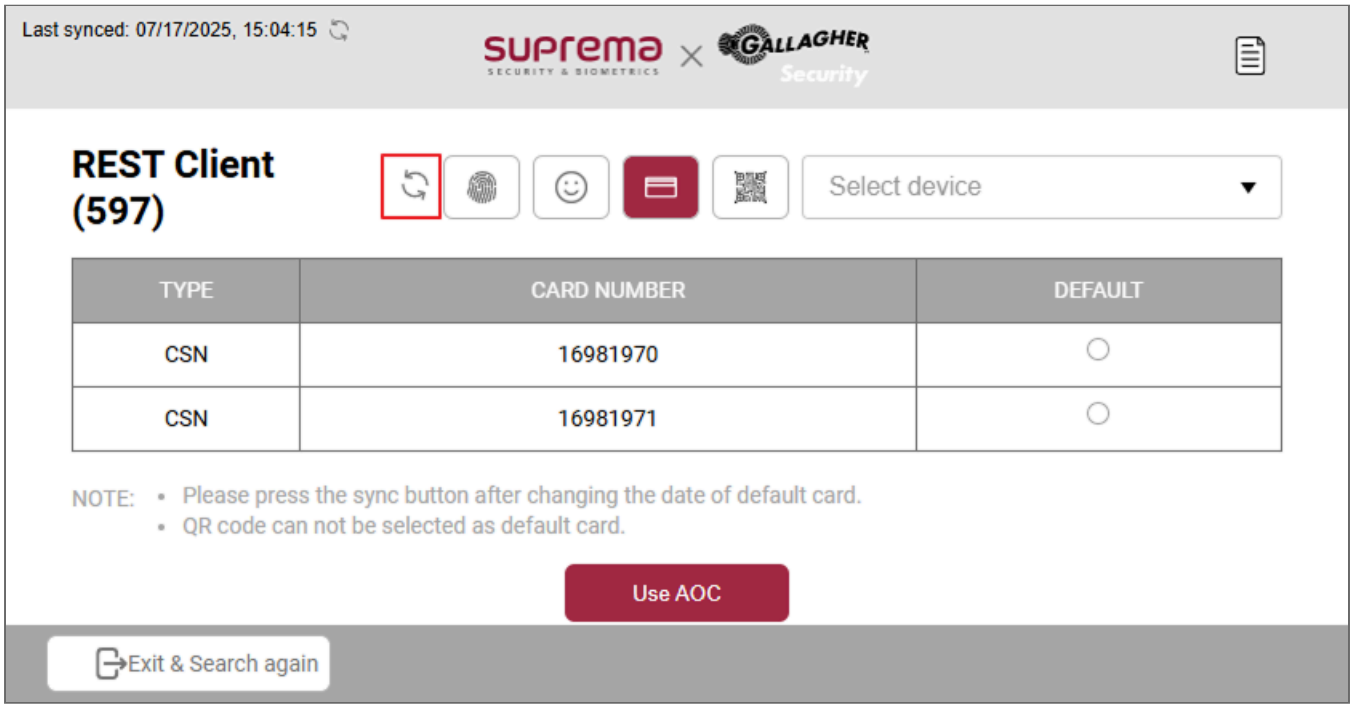
7. After adding the access group and connecting the Mifare Encoder **right-click** on Viewer Configuration and reload the viewer.

8. **Putting** the card on the Encoder Assign Card from the Encoder button will actively **press** that button will assign the card to the user, after that **press** the **Save** button. Then **press** the **Edit** button in the middleware.

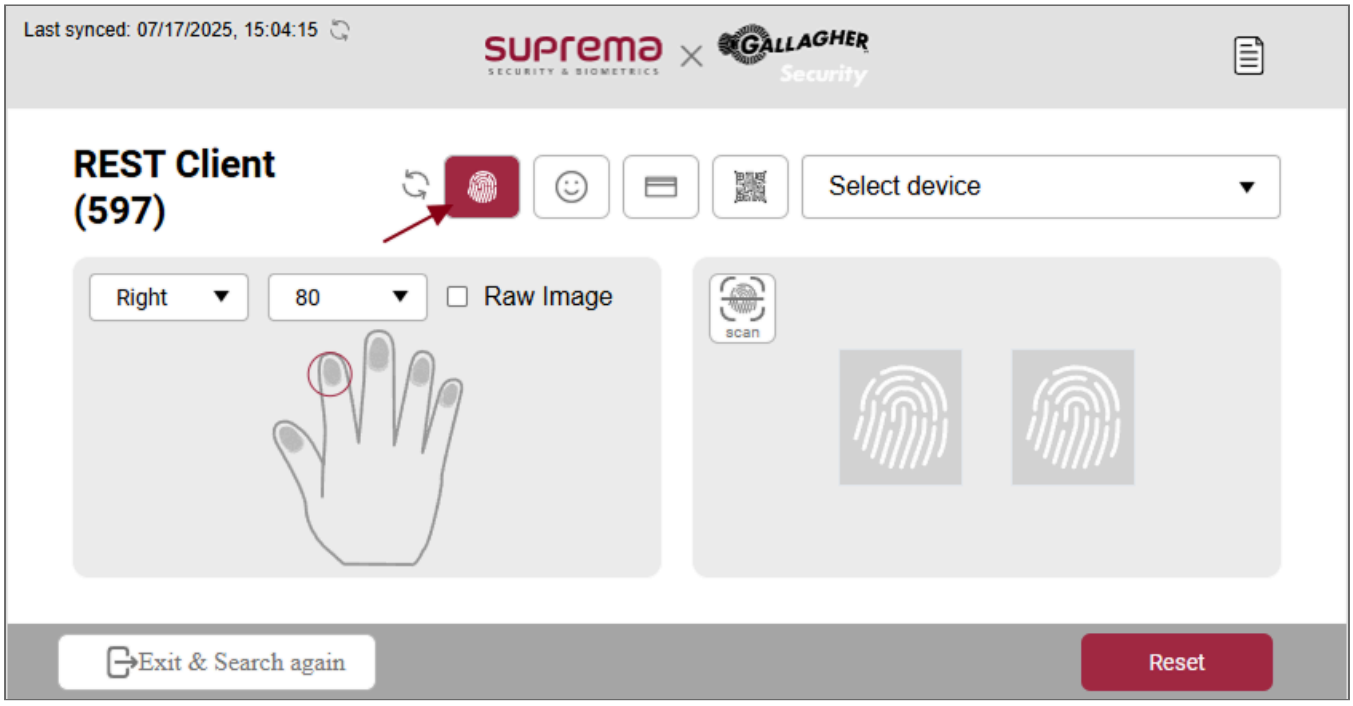
> **Info**
> If you want to enroll only Biometric then don't assign any card in advance, just **press** the Edit button after assigning the access zone.



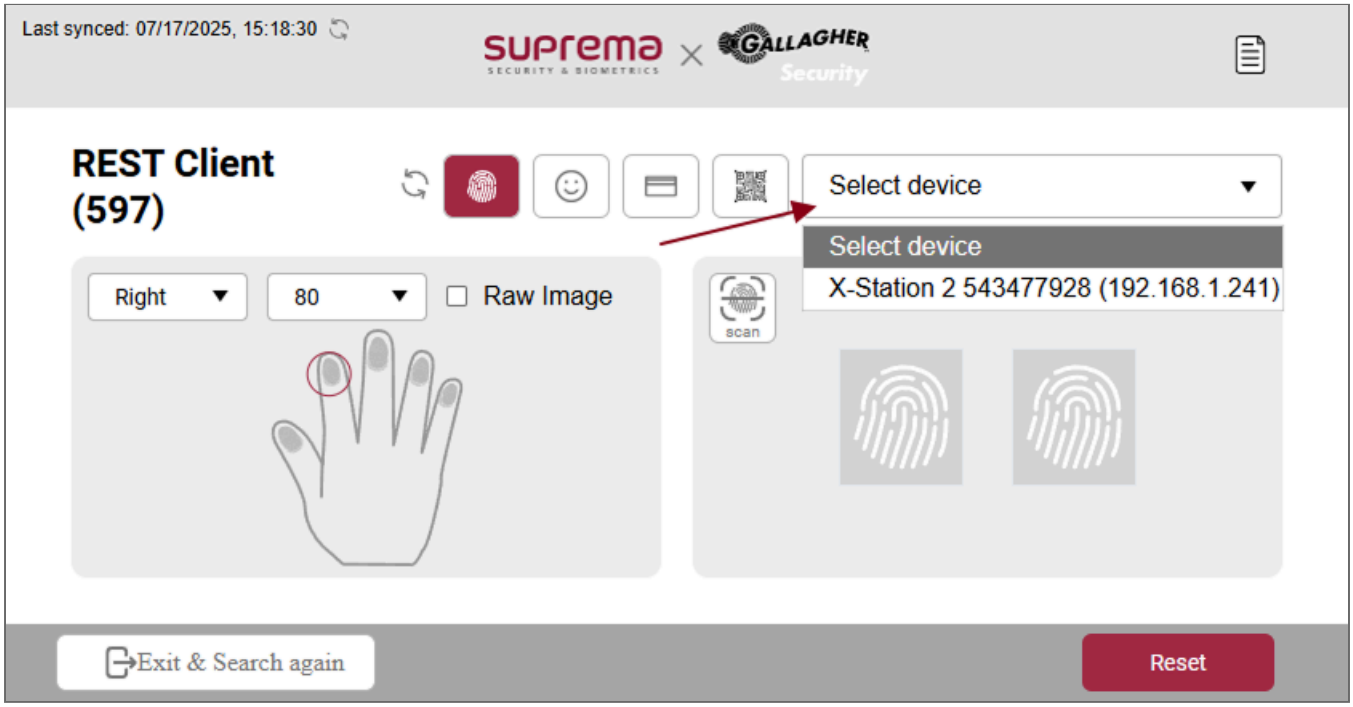
You can assign multiple cards to the user when you assign the card and **press** the Save button **press** the green **sync button** it will sync the whole data of the particular user.



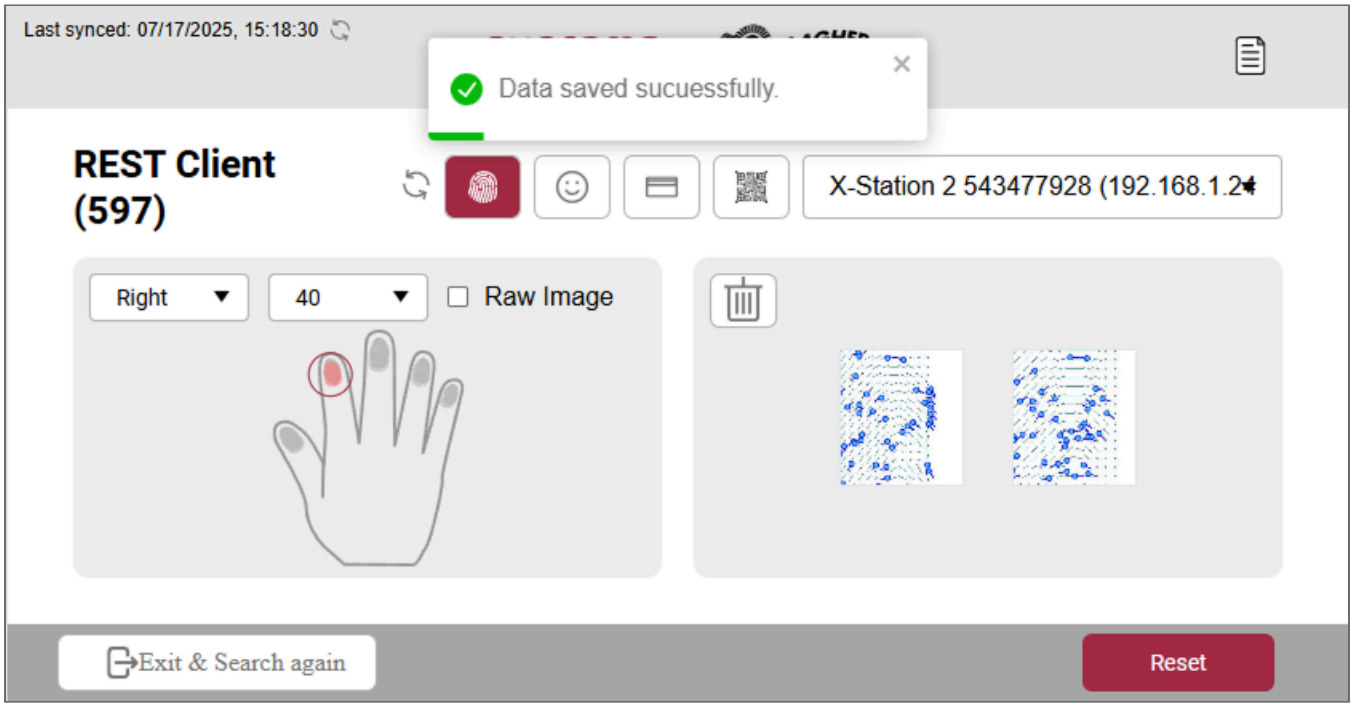
9. **Press** the Fingerprint button, and it will load the fingerprint module.



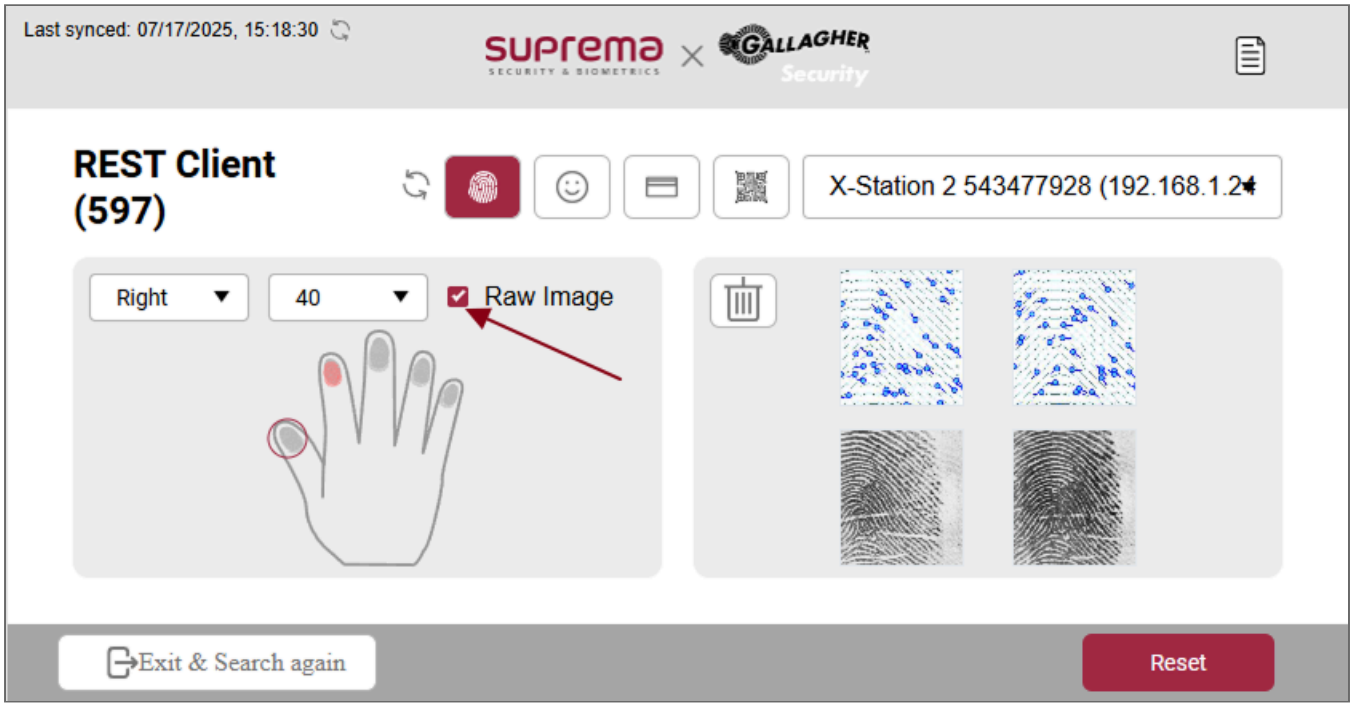
10. **Select** the device from the list.



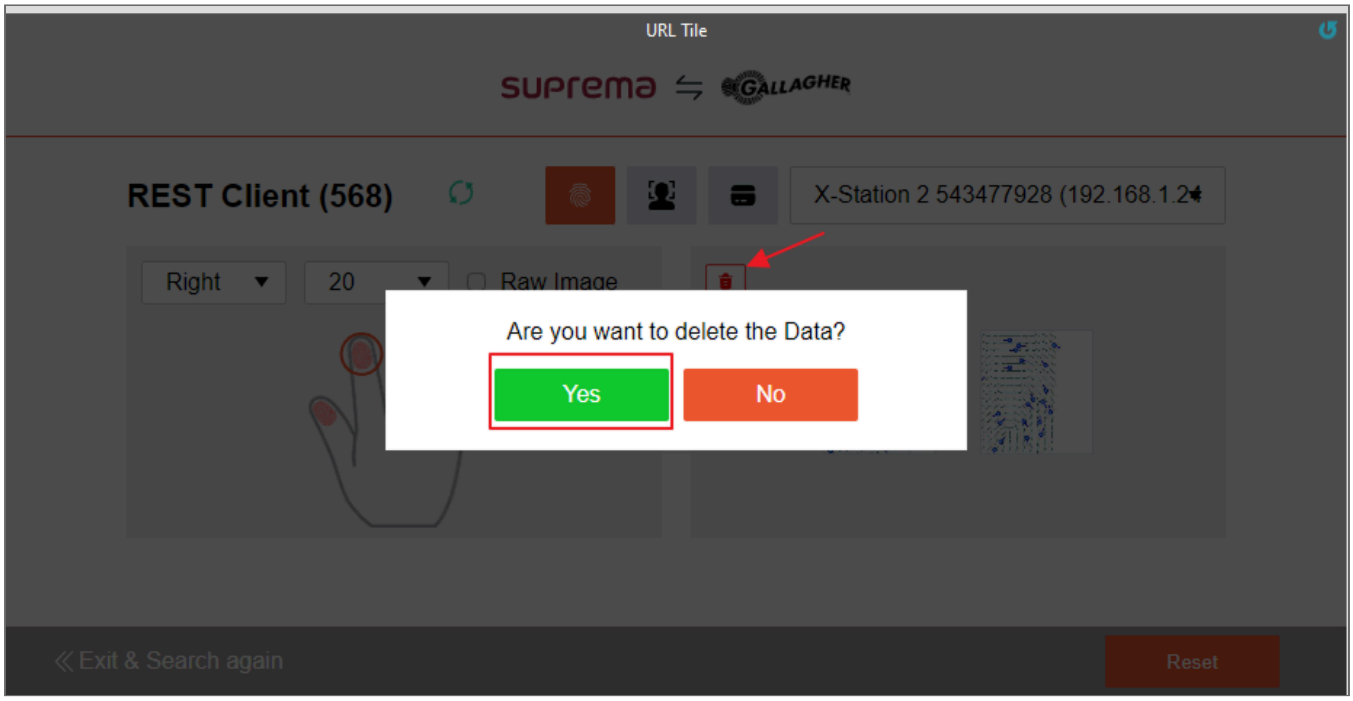
11. You can **select** the left or right hand, after that quality of the fingerprint and **press** the scan button, it will start scanning. When the scanning is complete, the scan button will change to the delete button and the fingerprint will appear on the display, Data will be stored automatically when the data is saved successfully the saved fingerprint will be colored.



12. If you want a raw image then **tick** the Raw Image checkbox and then **scan** the finger.

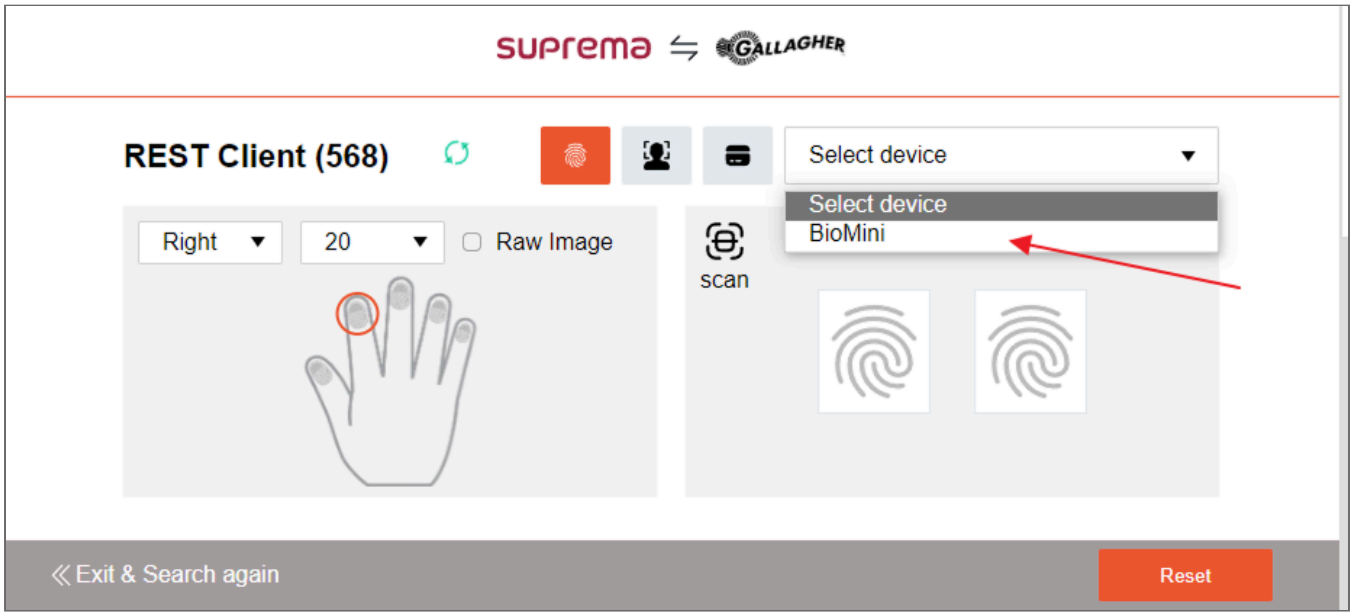


13. To delete the single fingerprint **press** the **delete** button and the pop-up will appear then **press** the **Yes** button, it will delete that particular fingerprint.

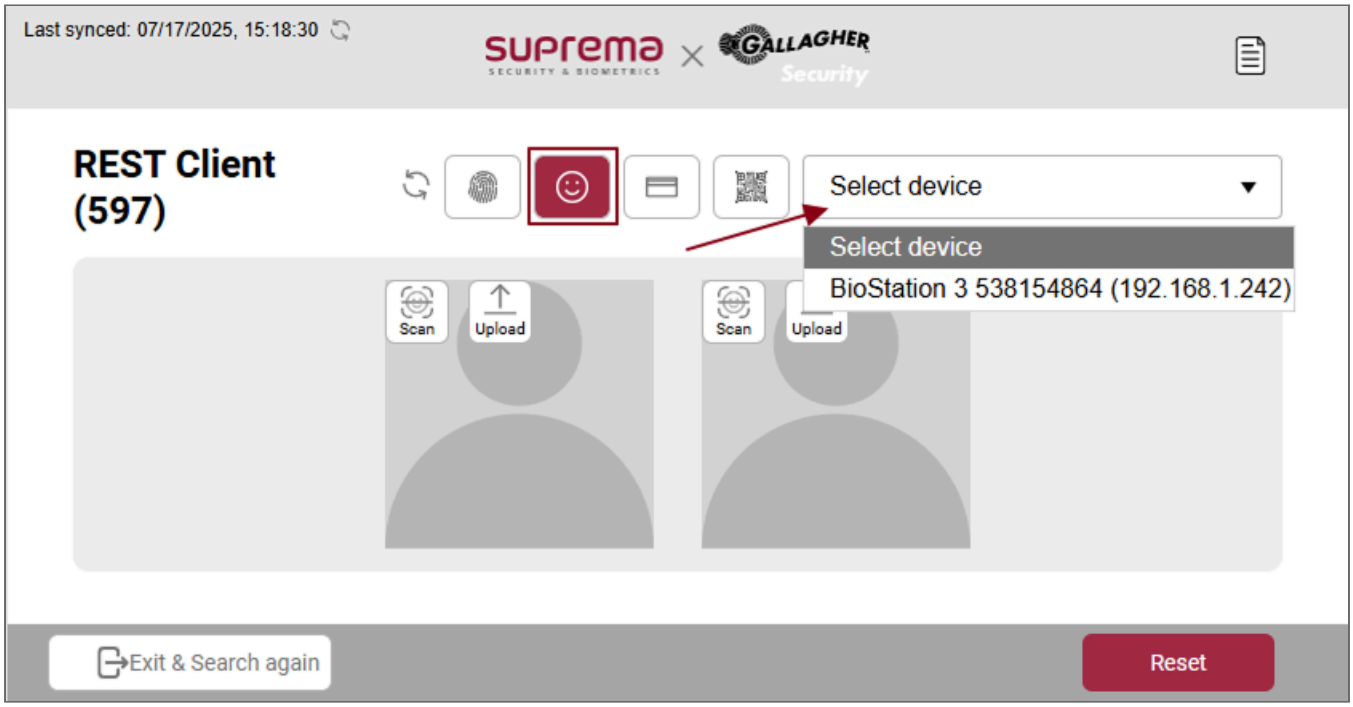


To Reset all the fingerprint data, **press** the **reset** button and the pop-up will appear then **press** Yes it will reset all the fingerprint data.

14. We can use BioMini Plus 2 to enroll user fingerprint data. For that just connect the device and you will see it inside the fingerprint select device **section**. **Select the** device and start enrolling data for the user.



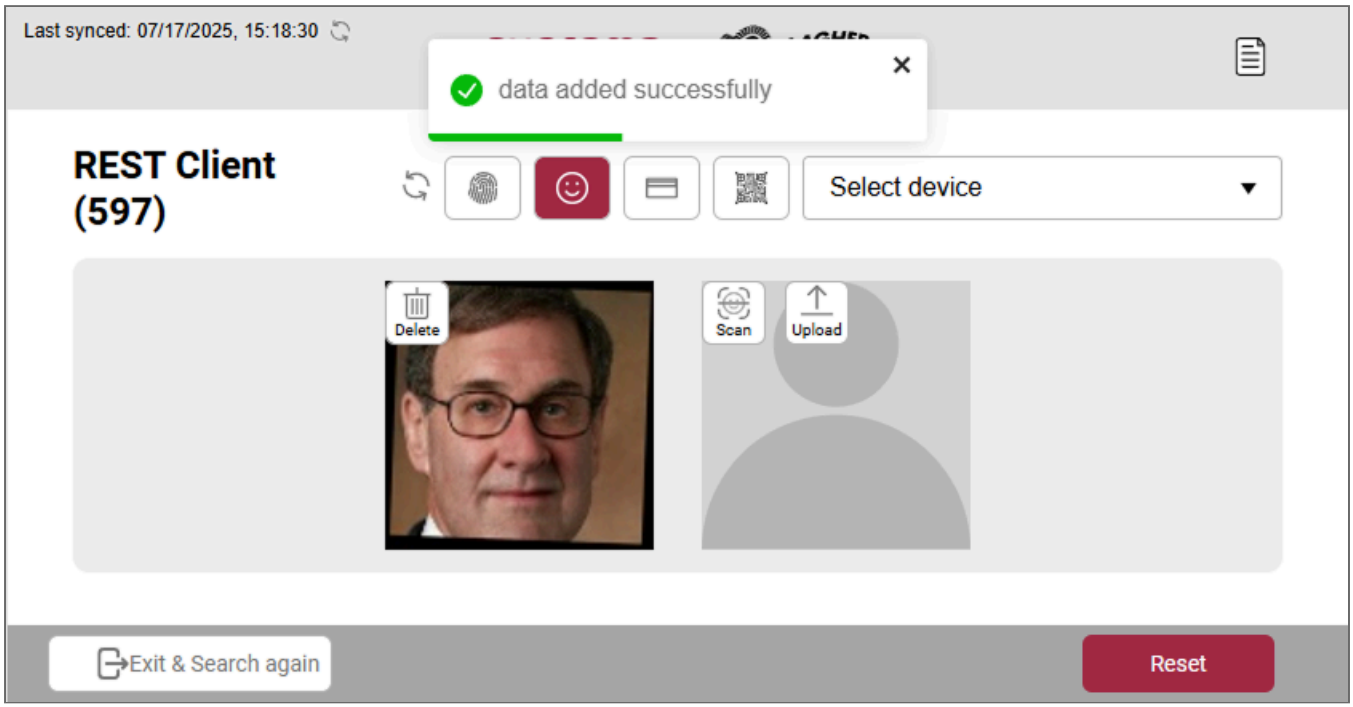
15. To enroll the visual face, **press** the button beside the fingerprint it will load the visual face module.



There are two methods to scan the visual face. We can upload it or we can scan the face to enroll.

16. **Press** the **upload** icon, then a new window will open then you can choose the image you want to upload.

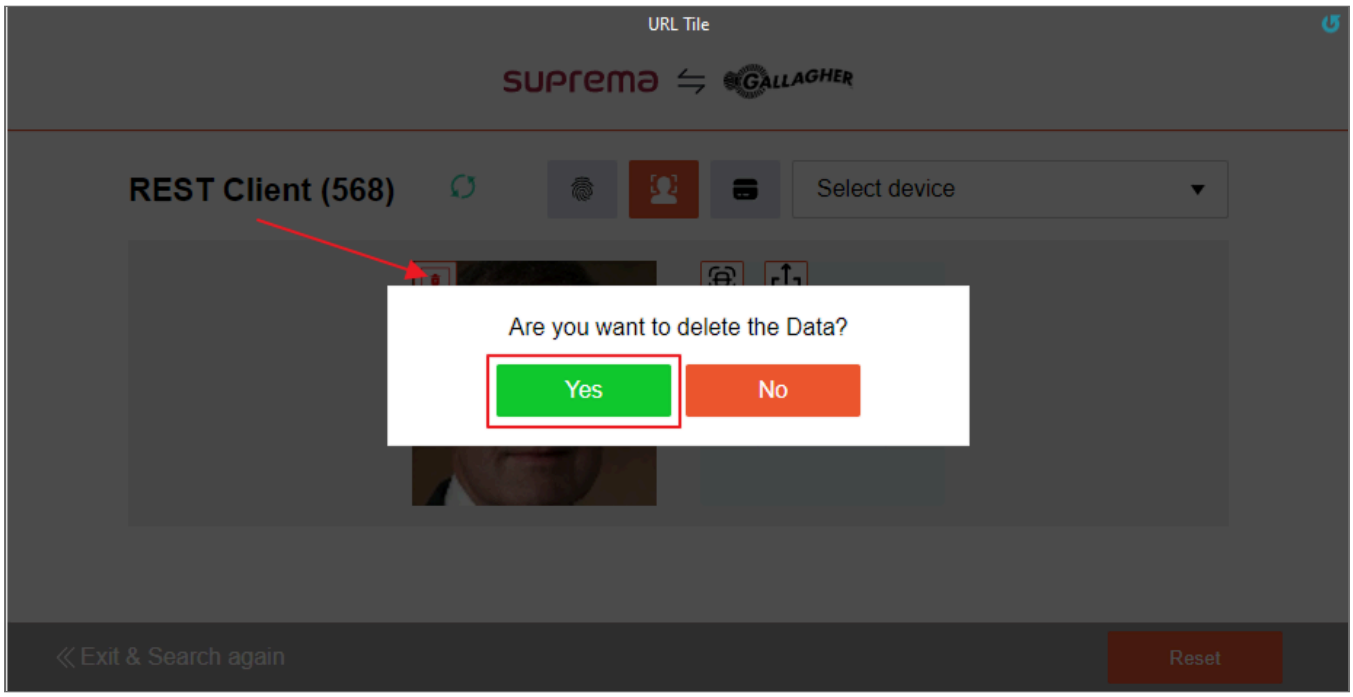
If you **press** the **scan** button it will activate the device that you have selected, use that selected device to scan your face. Data will be stored automatically after uploading or scanning the visual face and then a success message will pop up.



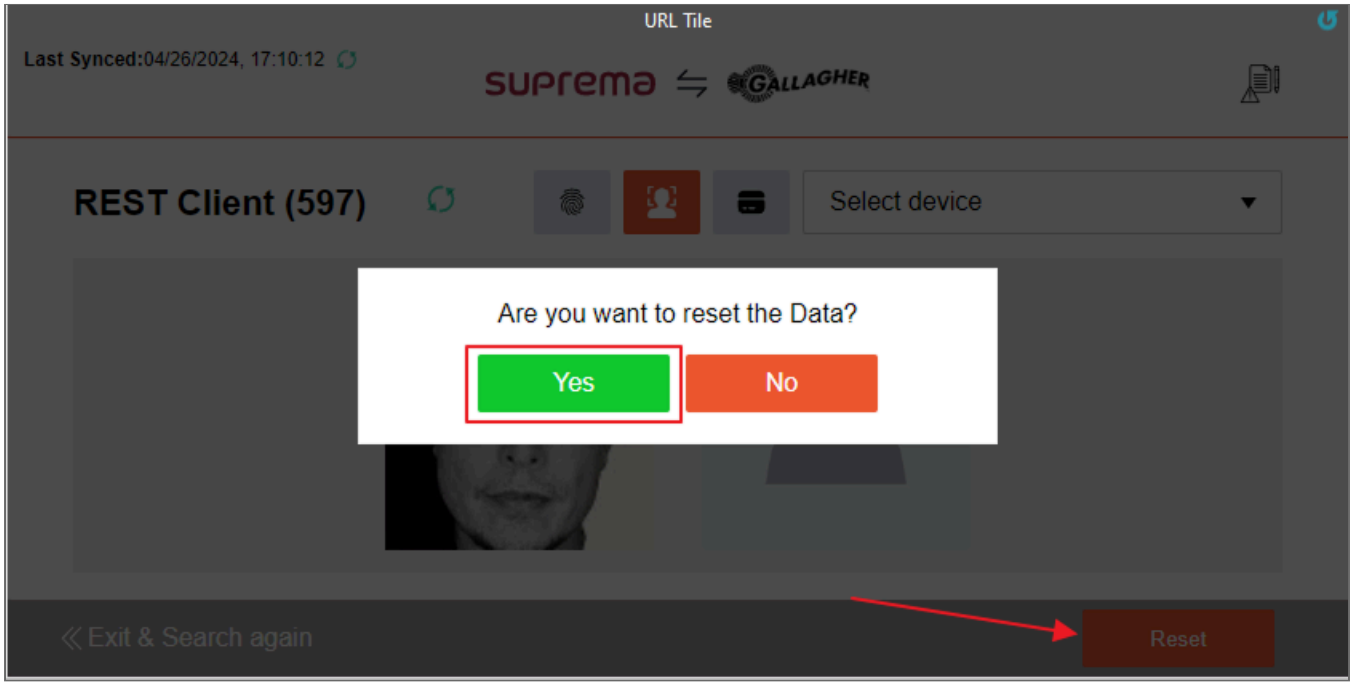
Info

- The supported image file size is up to 2MB.
- Supported image file formats are JPG, JPEG, and PNG.
- If an error occurs while entering a visual face with a profile image, please use a sharper image.

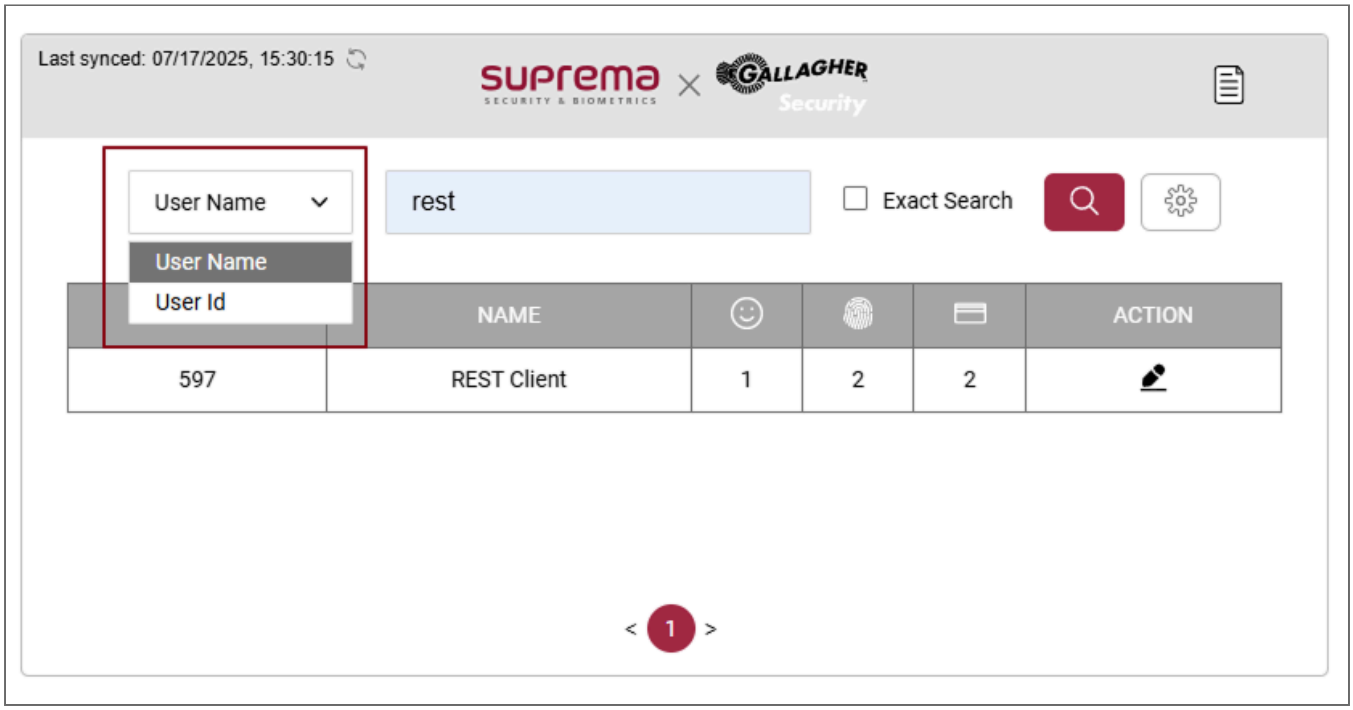
17. If you want to rescan or re-upload the data you need to delete the old data **press** the **red delete button** pop-up and **press Yes** and it will delete that image.



18. And if you want to reset all visual face data **press** the **reset** button and **press** Yes it will reset all the data.



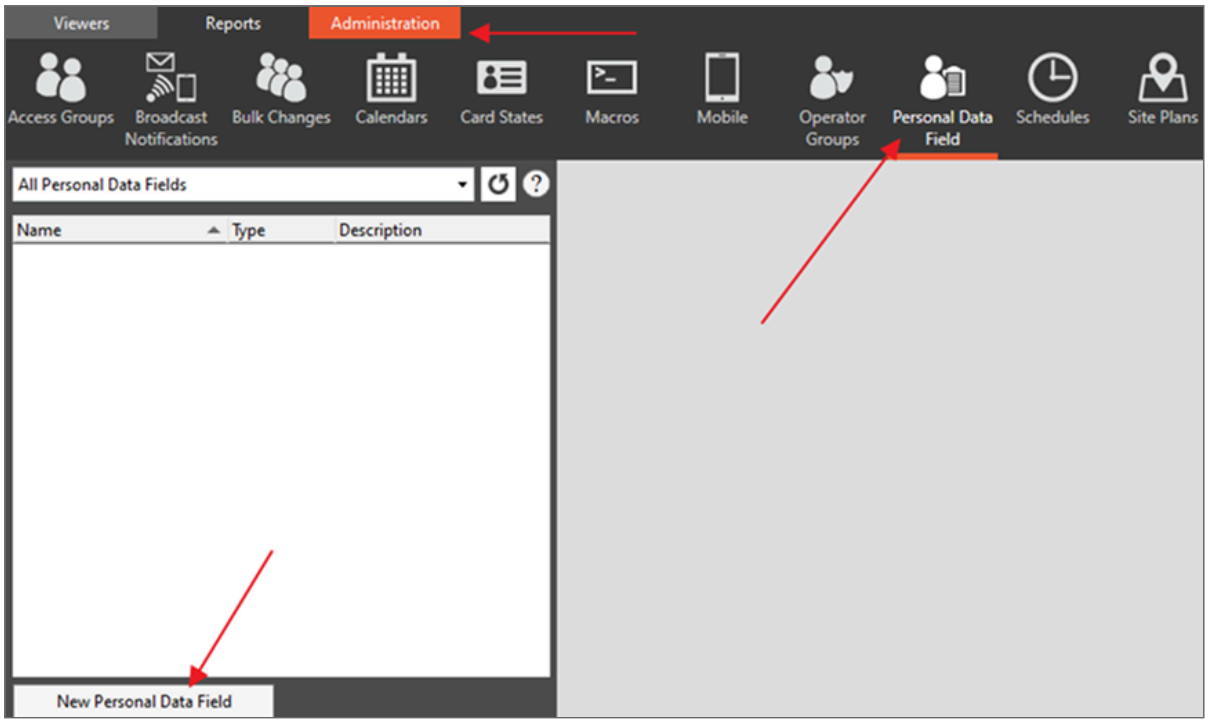
19. If you exit and search for the user again, all the saved data will appear in the table.



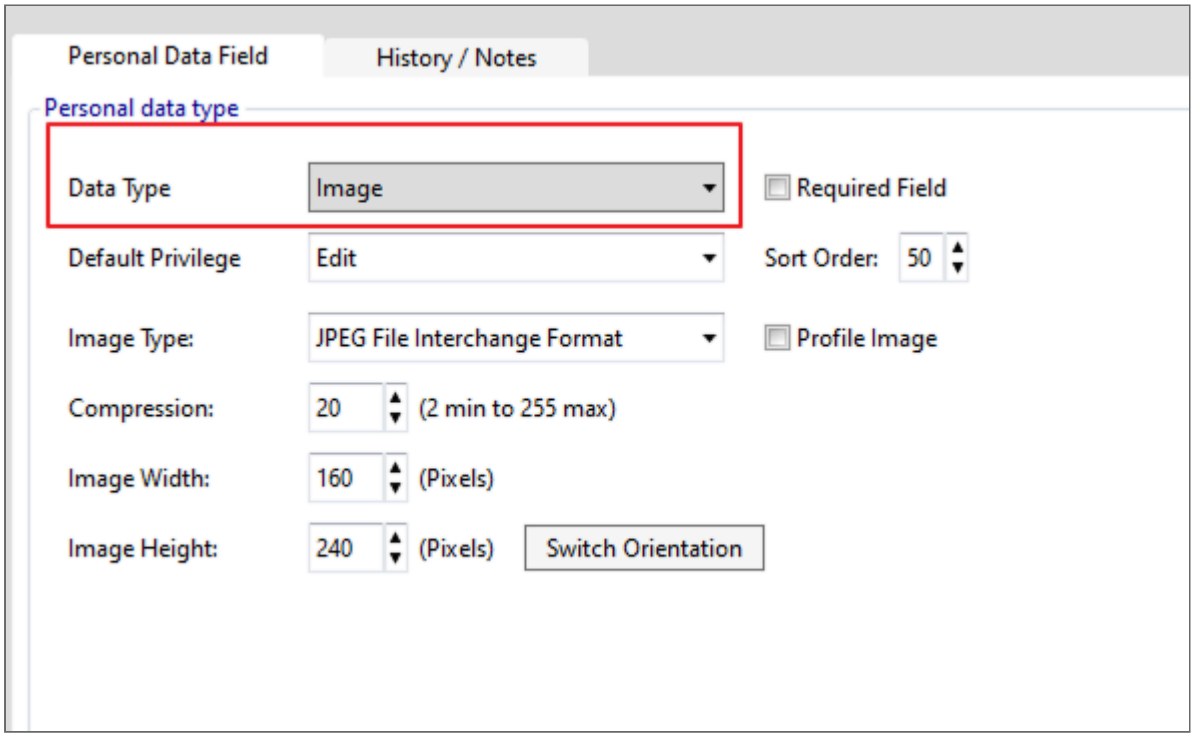
You can also search for the user with its id **change** the drop-down user name to user id and **search** for a user with id.

Enroll the User's Photo ID in the Command Center for Face Template

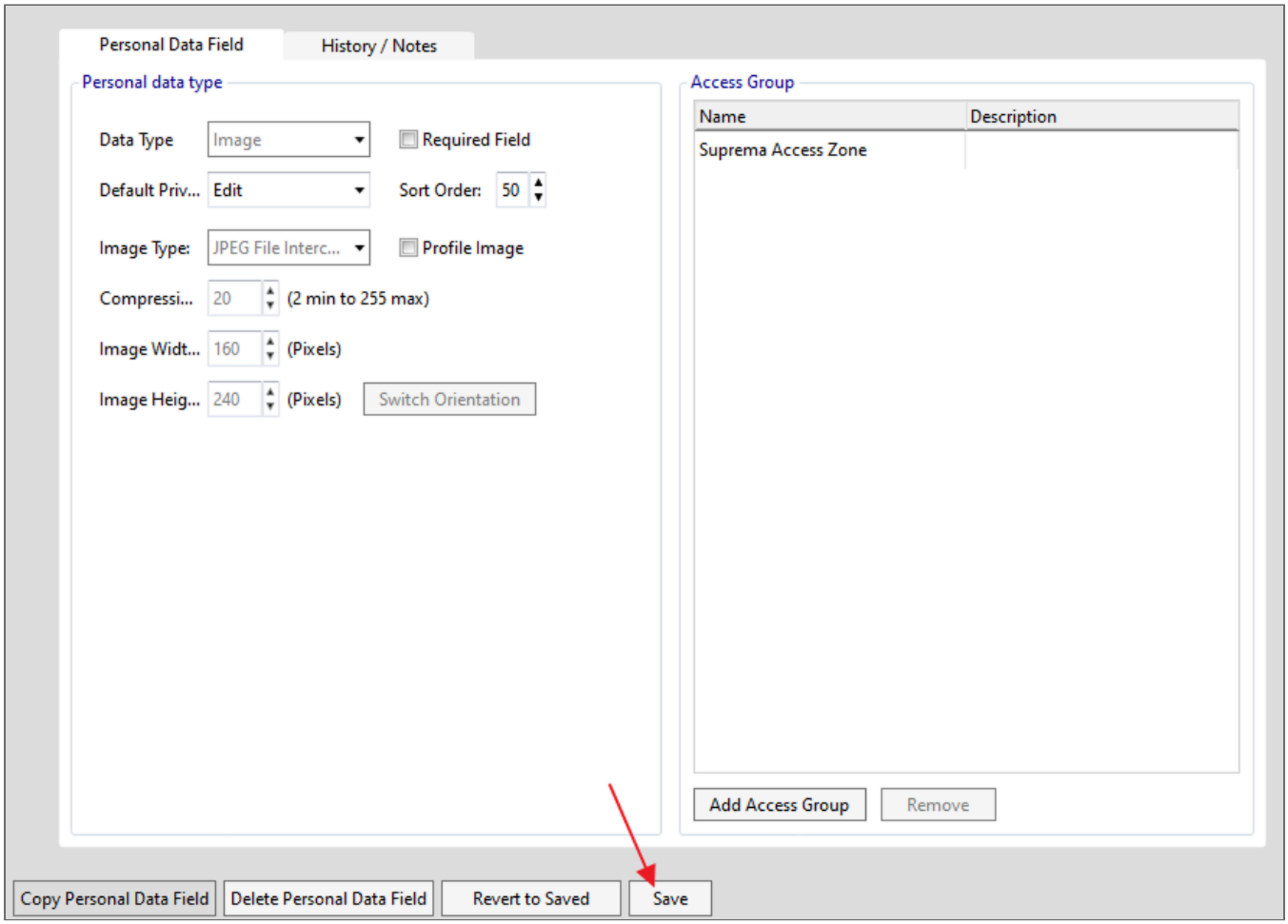
1. **Go to** the Administration and **Click** on Personal Data Field and **press** on New Personal Data Field.



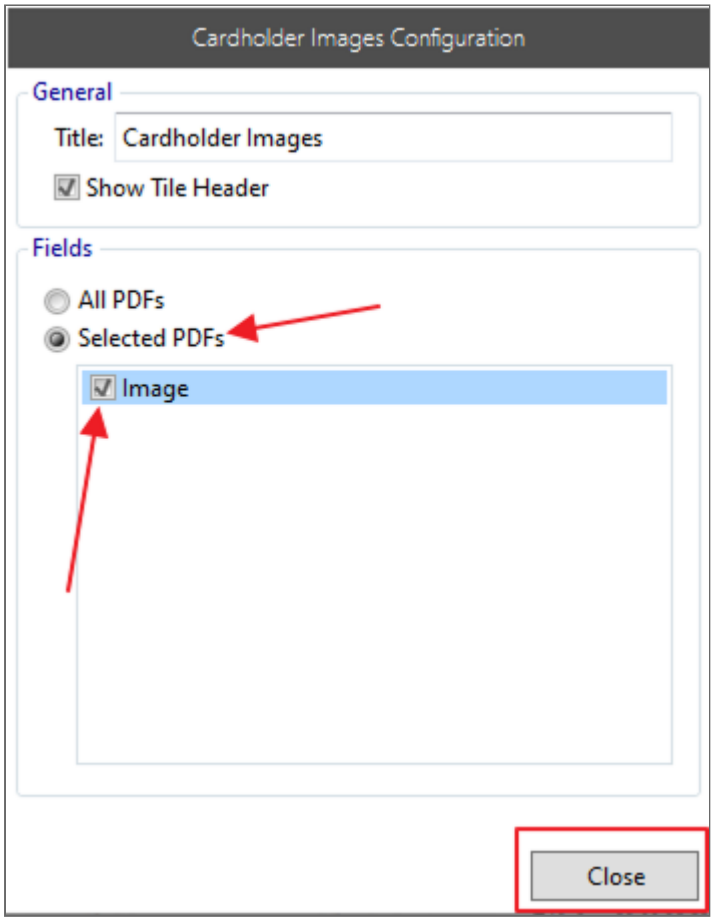
2. Now inside the pop-up **set** the name as Image and **press** the Close button. In the Data Type field **select** Image as a Data Type Don't change anything here and assign Access Group by **pressing** on the Add Access Group button inside the Access Group section and **selecting** Suprema Access Zone After **selecting** Access Zone **press** the Add Selection button for the field.



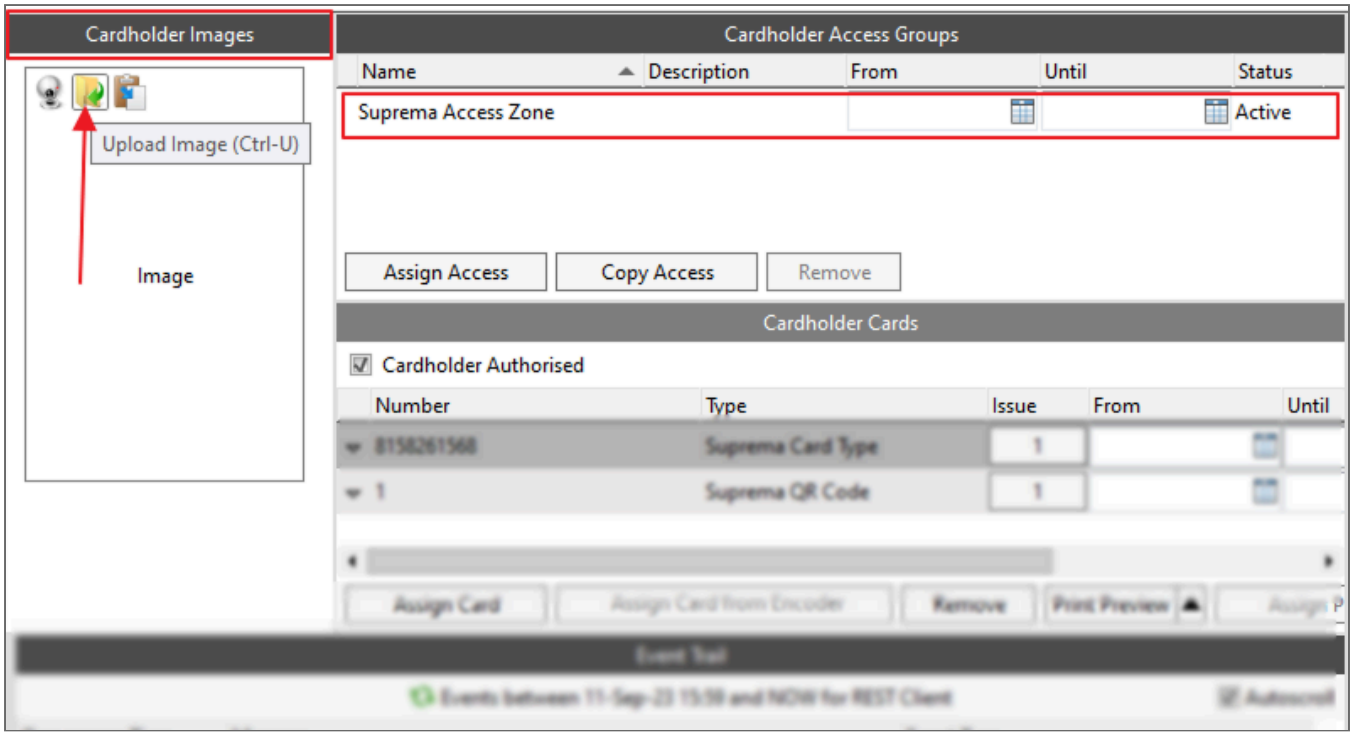
3. After Assigning Access Zone **press** the Save button on the bottom.



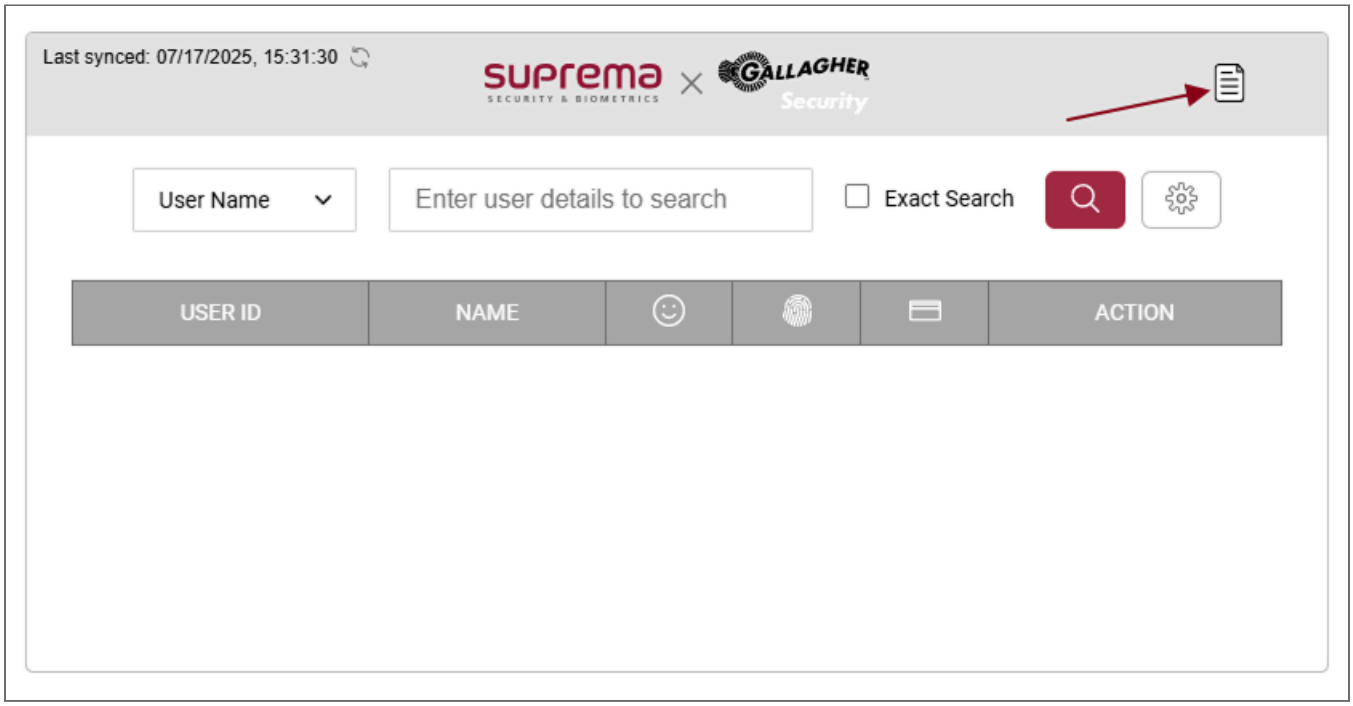
4. Now **go to** the Viewer Configuration and **press** Click to configure for Cardholder Images. Inside Cardholder Images Configuration **Choose** Selected PDFs, **select** the Image field and **press** the Close button. Now **press** the Save button on the bottom left side to save the changes. Now **right-click** on Viewer Configuration and reload the viewer to reflect the changes.



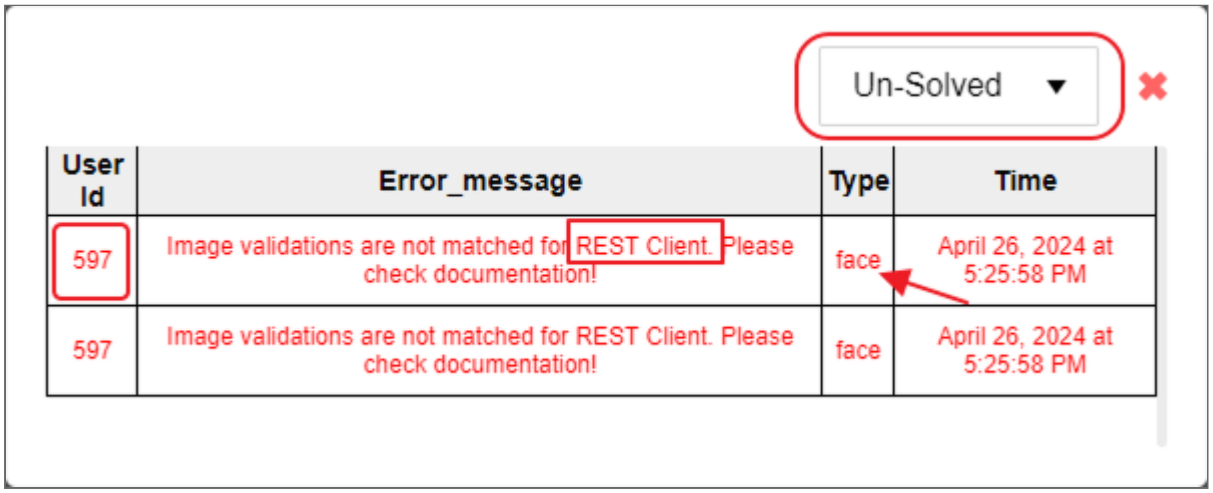
5. Now inside the Cardholder Viewer, you can see the Cardholder Images tab You can upload images by **clicking** on the yellow icon. For this, we must assign an Access Zone to the user. After Uploading the image **press** the Save button.



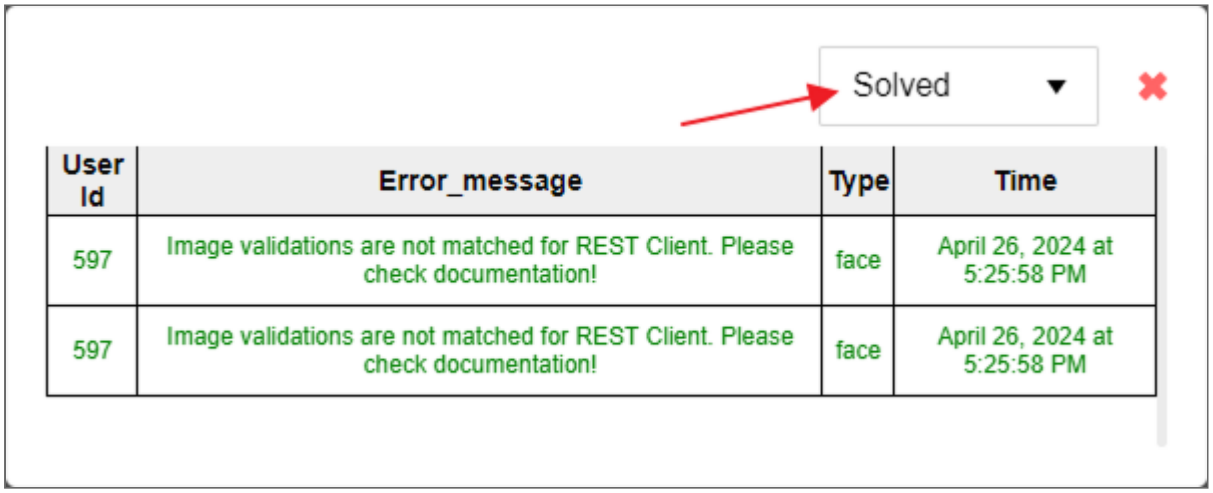
6. If you want to see the error message that occurs for users while updating the user information, you can find that inside the ErrorLog section by **clicking** on this icon A pop-up will open, which shows different errors for the user.



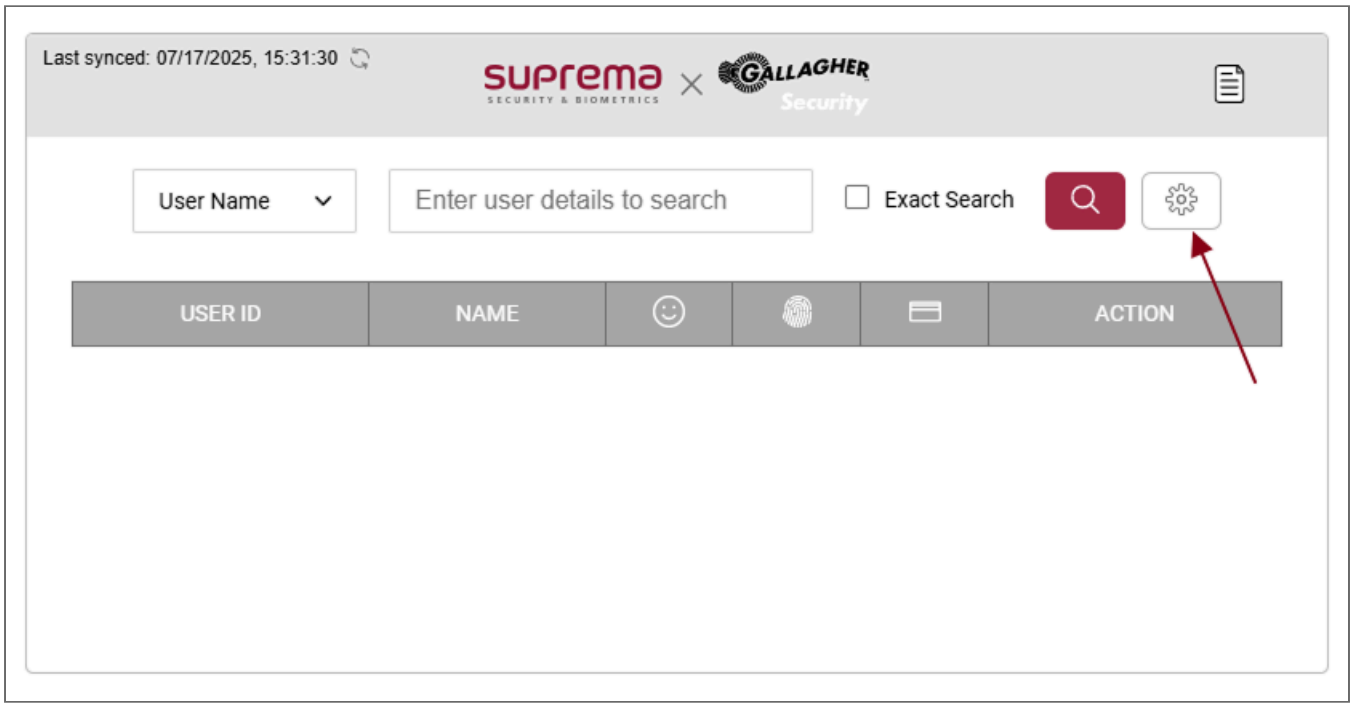
7. As in the below Image, we have an error for one user, Here the **Type** defines what type of error it is, **Status** Un-solved means the Error is not solved for the user yet and Solved indicates the error is solved for the user. Now the one red box indicates the name of the user and the another red box indicates the user ID.



8. Now the below image is after changing the user image from the Gallagher Command center as we get the error while enrolling the face for the user and after successful enrollment the color of the Error message is also changed and **Status** is also changed.

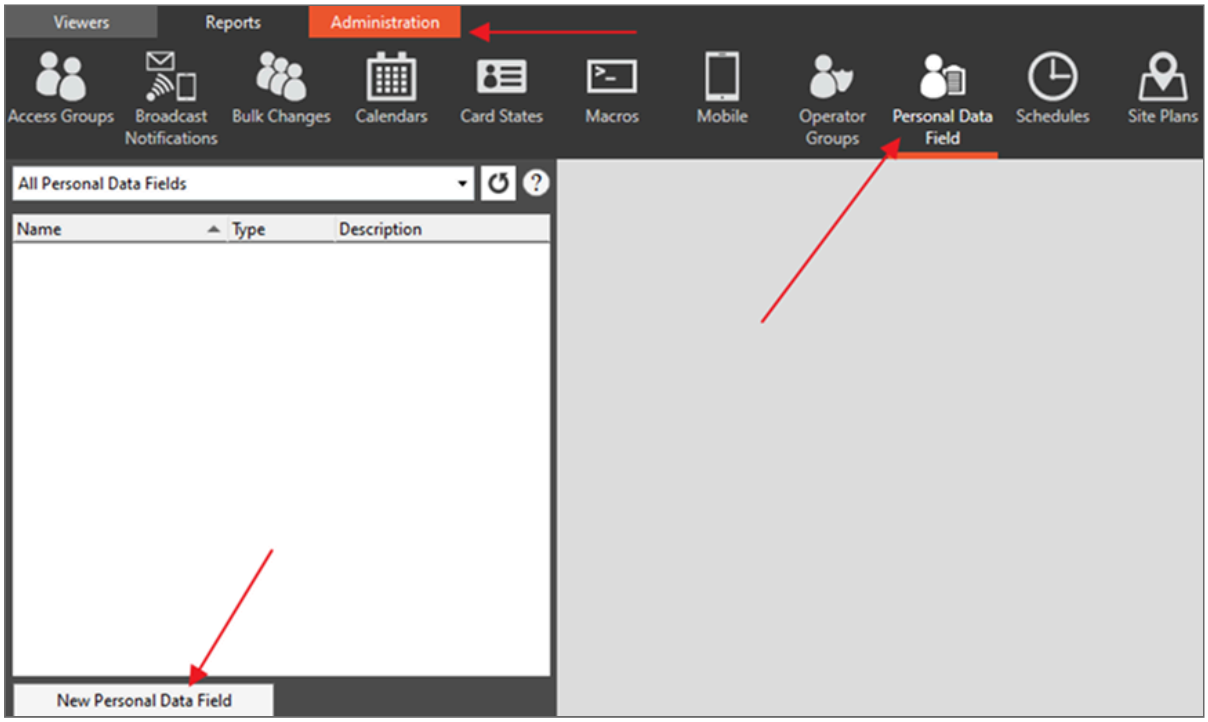


9. If you want to change the settings on the device, **press** the **settings** button, and you can see the below screens:



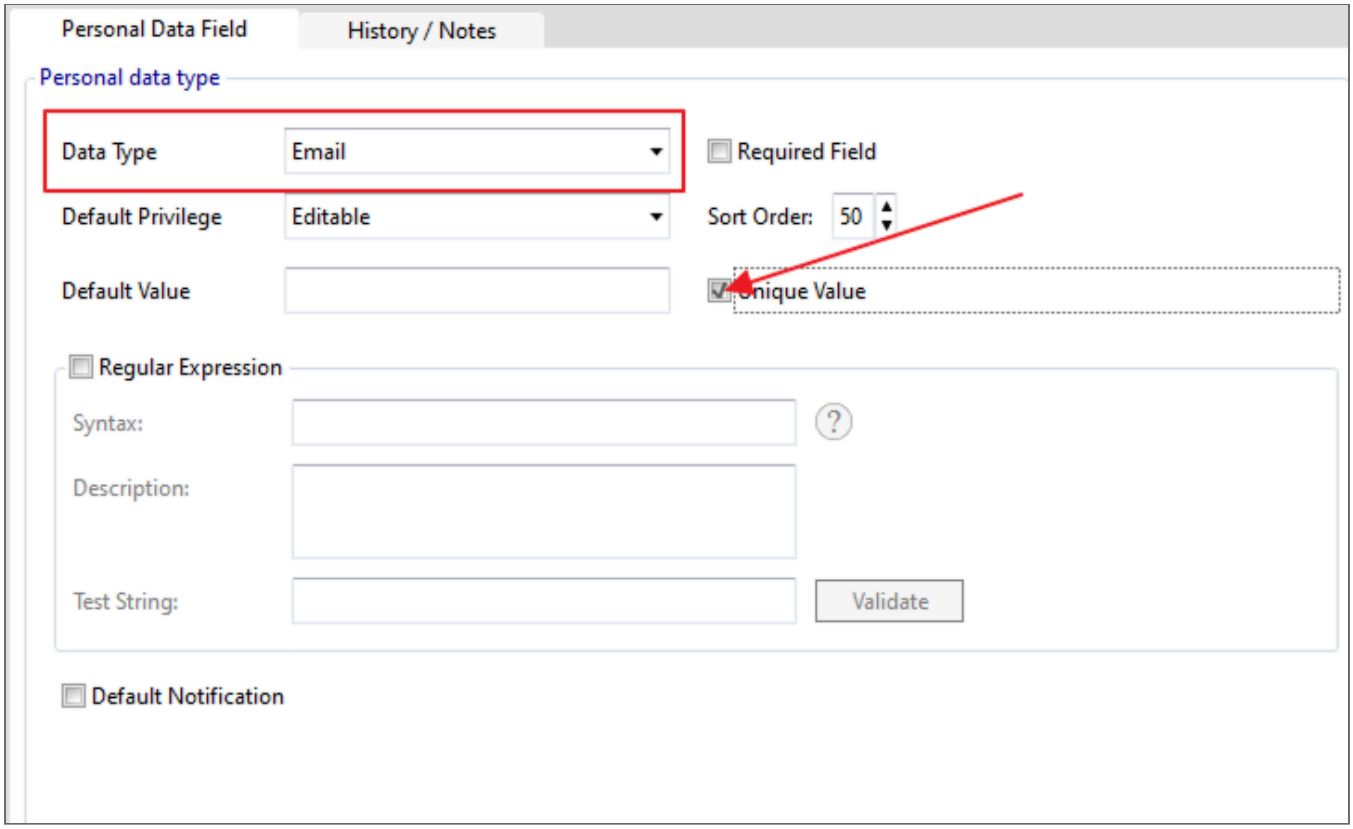
Enroll the User's Email ID in the Command Center for the QR Code

1. **Go to** the Administration and **Click** on Personal Data Field and **press** on New Personal Data Field.

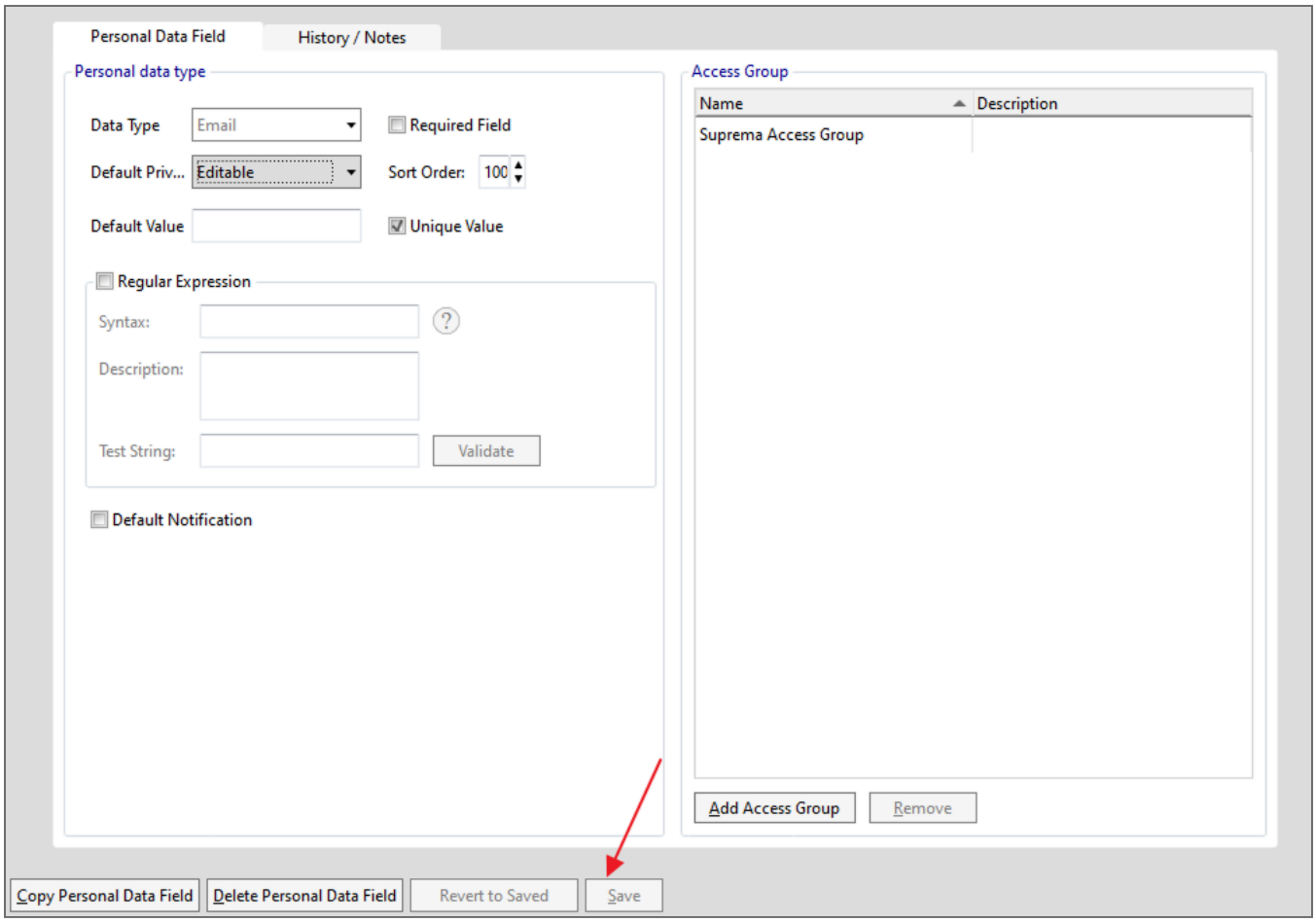


2. Now inside the pop-up **set** the name as Email and **press** the Close button. In the Data Type field **select** Email as a Data Type and **Tick** the Unique Value checkbox. Don't change anything here and assign Access Group by **pressing** on the Add Access Group button inside the Access Group section and **selecting** Suprema Access Zone After **selecting** Access Zone **press** the Add Selection button for the field.

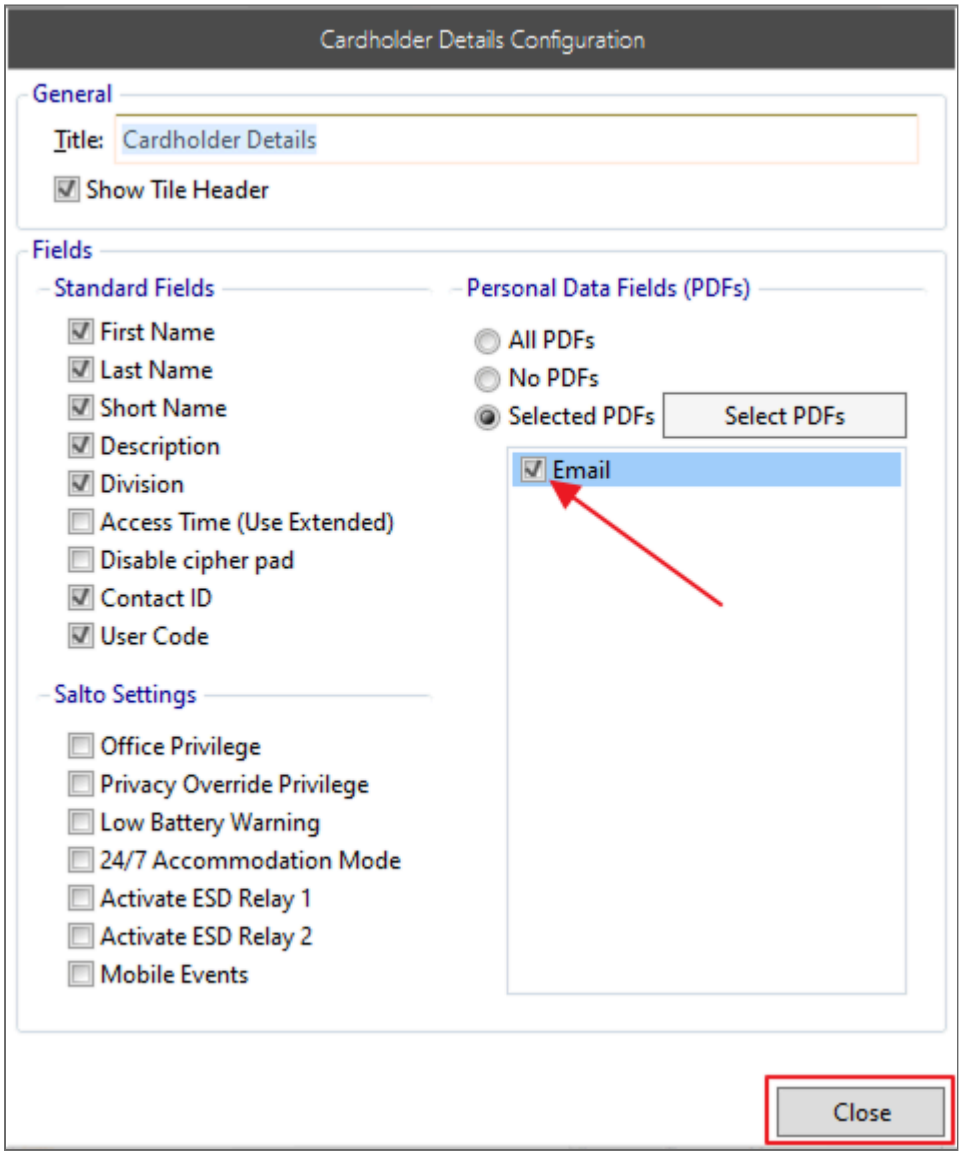
> **Info**
> Please use the same terms as mentioned for the fields.



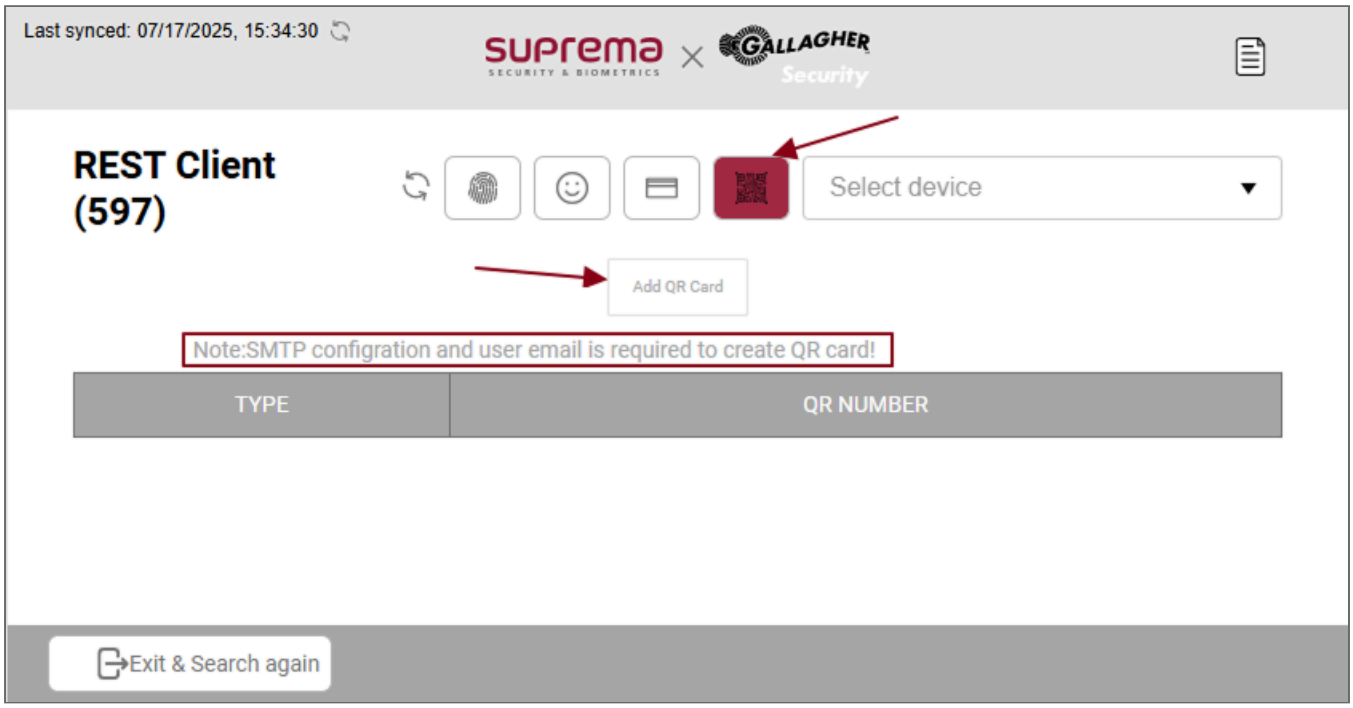
3. After Assigning Access Zone **press** the Save button on the bottom.



4. Now **go to** the Viewer Configuration and **press** Click to configure for Cardholder Details. Inside Cardholder Details Configuration **Choose** Selected PDFs and **select** Email field and **press** the Close button. Now **press** the Save button on the bottom left side to save the changes. Right-click on Viewer Configuration and **press** reload viewer.

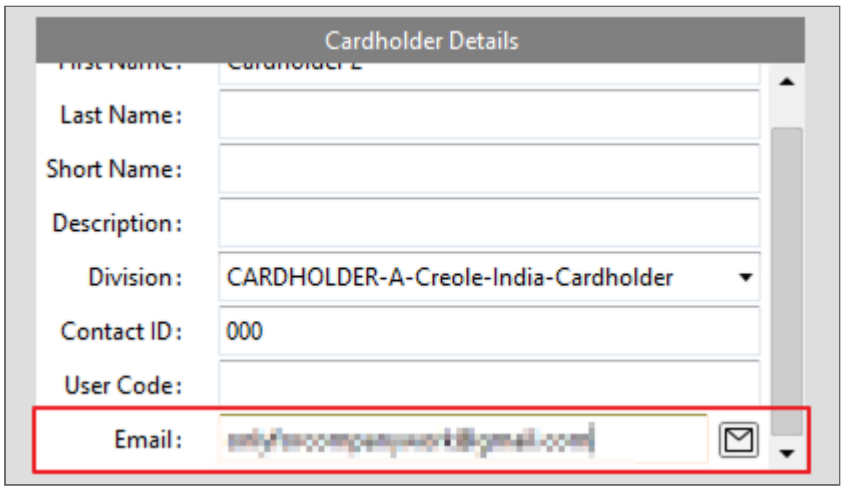


5. To assign the QR Code, go to the user profile within the middleware and **click** on the QR icon. As shown below, the Add QR button is **disabled**, and there's a note indicating that the user's email hasn't been assigned in Gallagher.

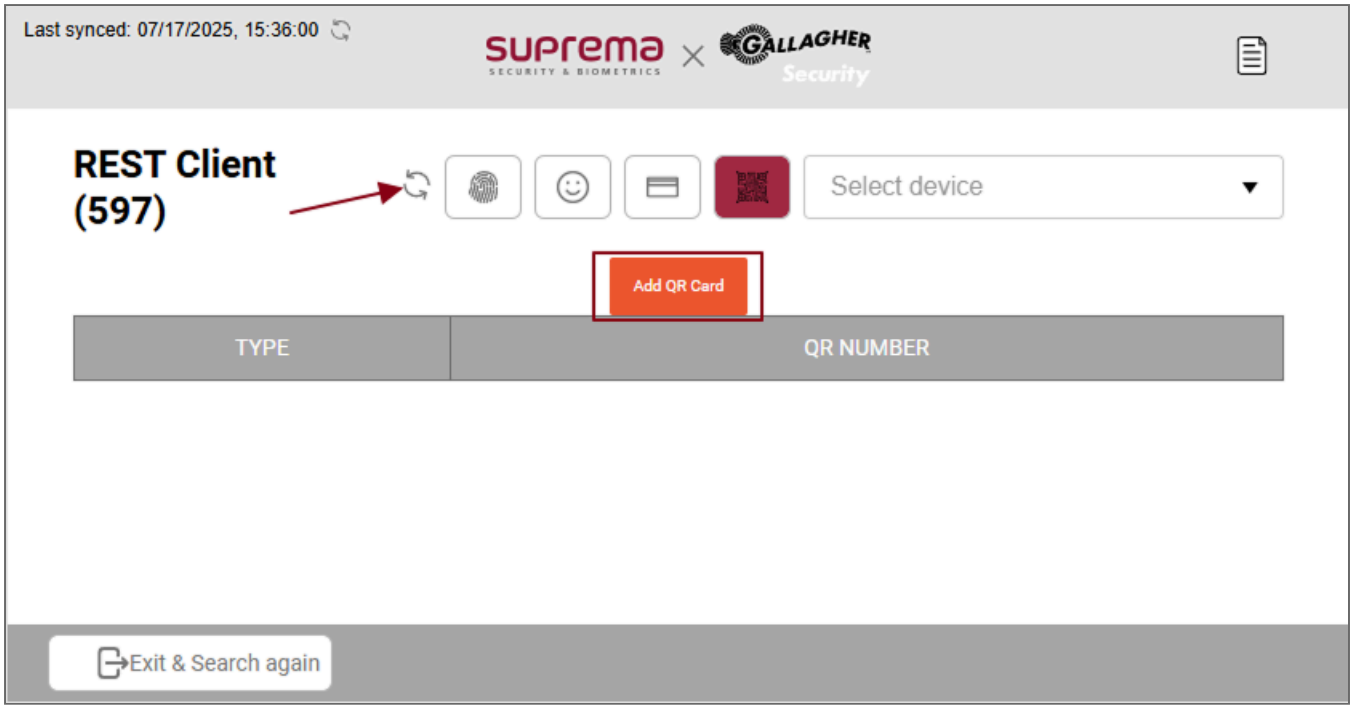


> **Info**
>
> - To configure the SMPT configurations - Configure SMTP for QR Code.
> - To configure the email address in Gallagher, email configuration in Gallagher.
> - Configure the QR Card type in Gallagher - Create QR Code card Type.

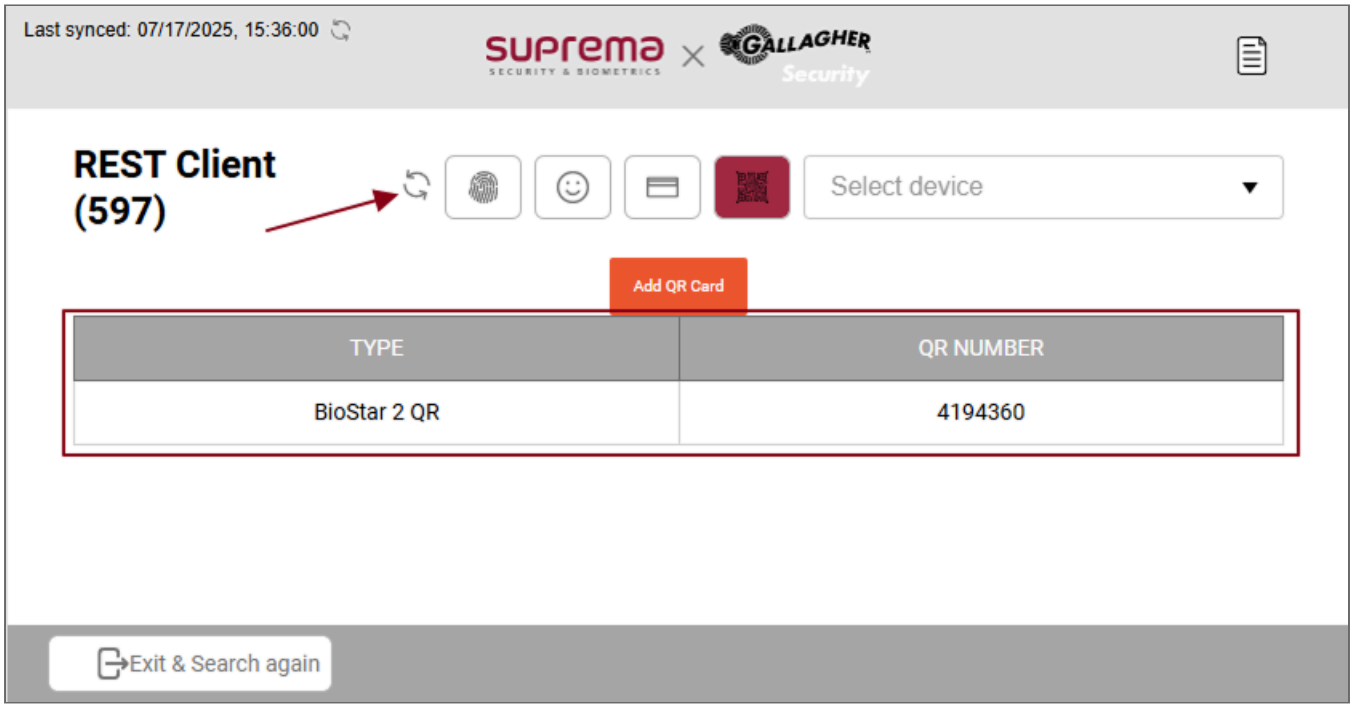
6. To assign an email address to a user, Inside the command center go to the user details and put user email inside the Cardholder details email field and **press** the save button.



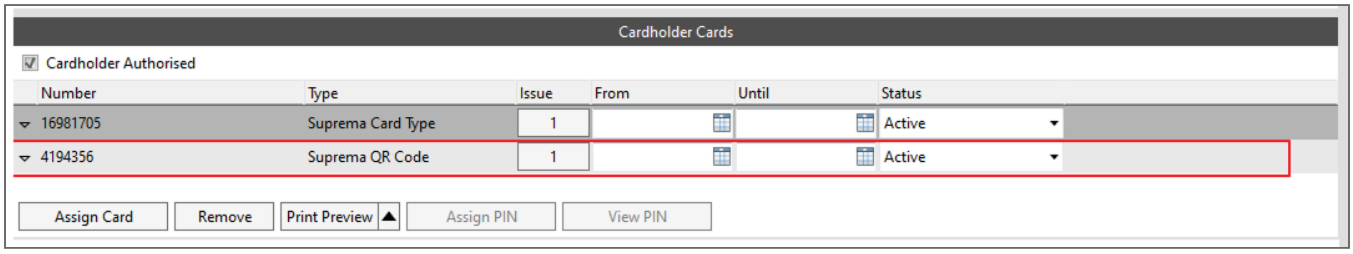
7. In the middleware user profile, **press** the sync button, and the email will be automatically assigned to the user profile in BioStar 2. The email button will now be enabled, and the note will be removed.



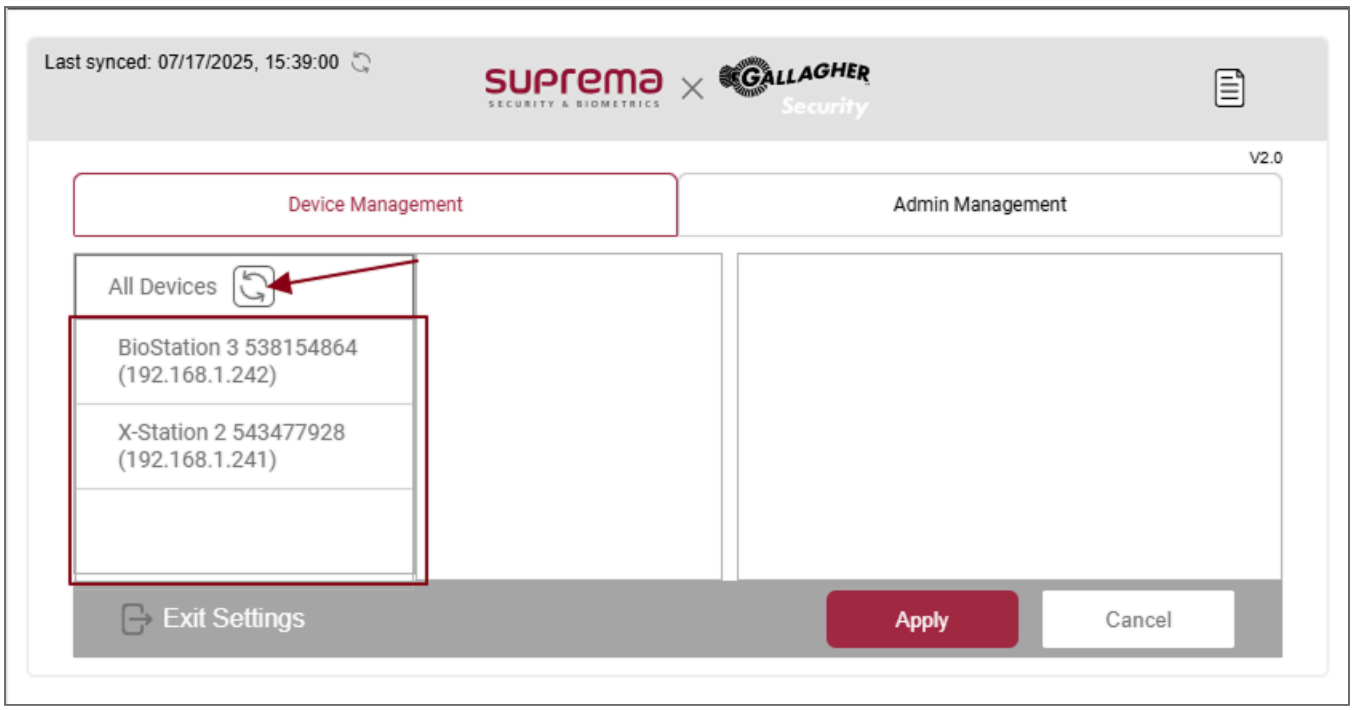
8. Now **press** the Add QR Code button inside the QR section of the user profile it will add the QR Code to Gallagher and BioStar 2 and **send** the QR Code to the email address that we assigned above!



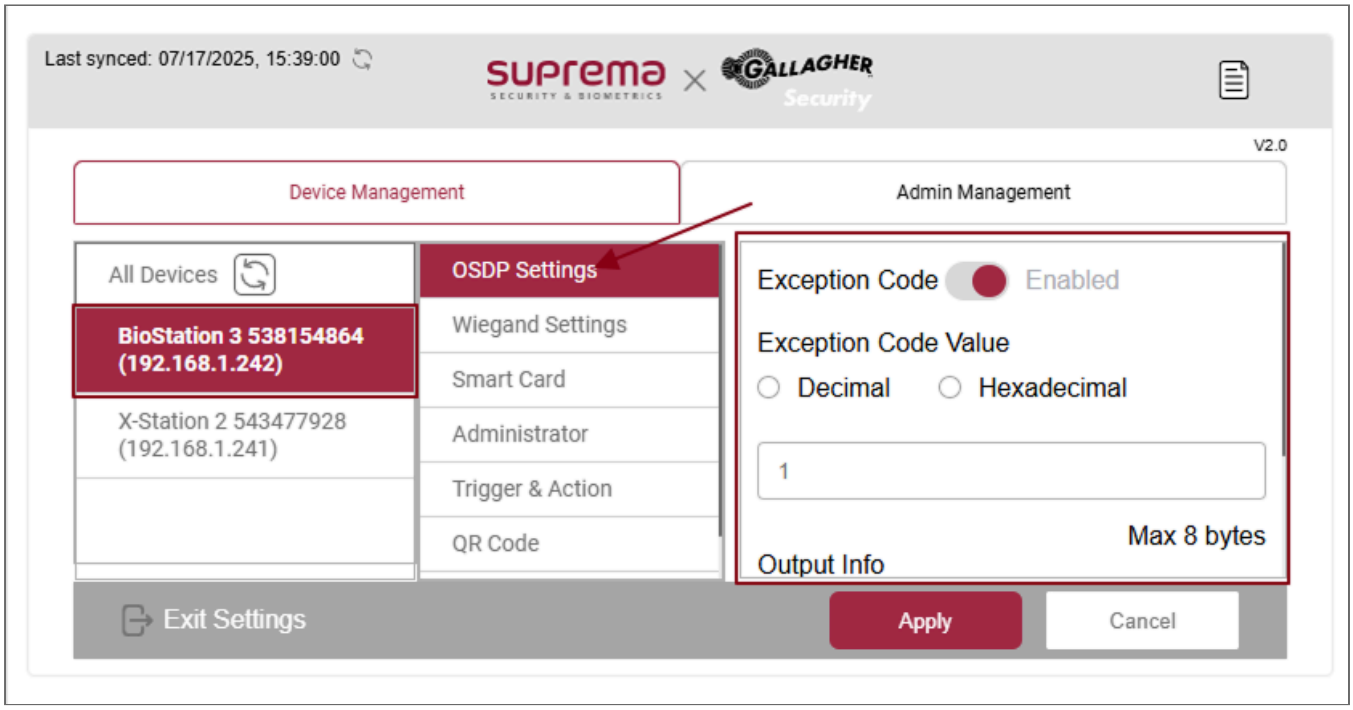
Once the Qr is added you can refresh the data by **pressing** the sync button.



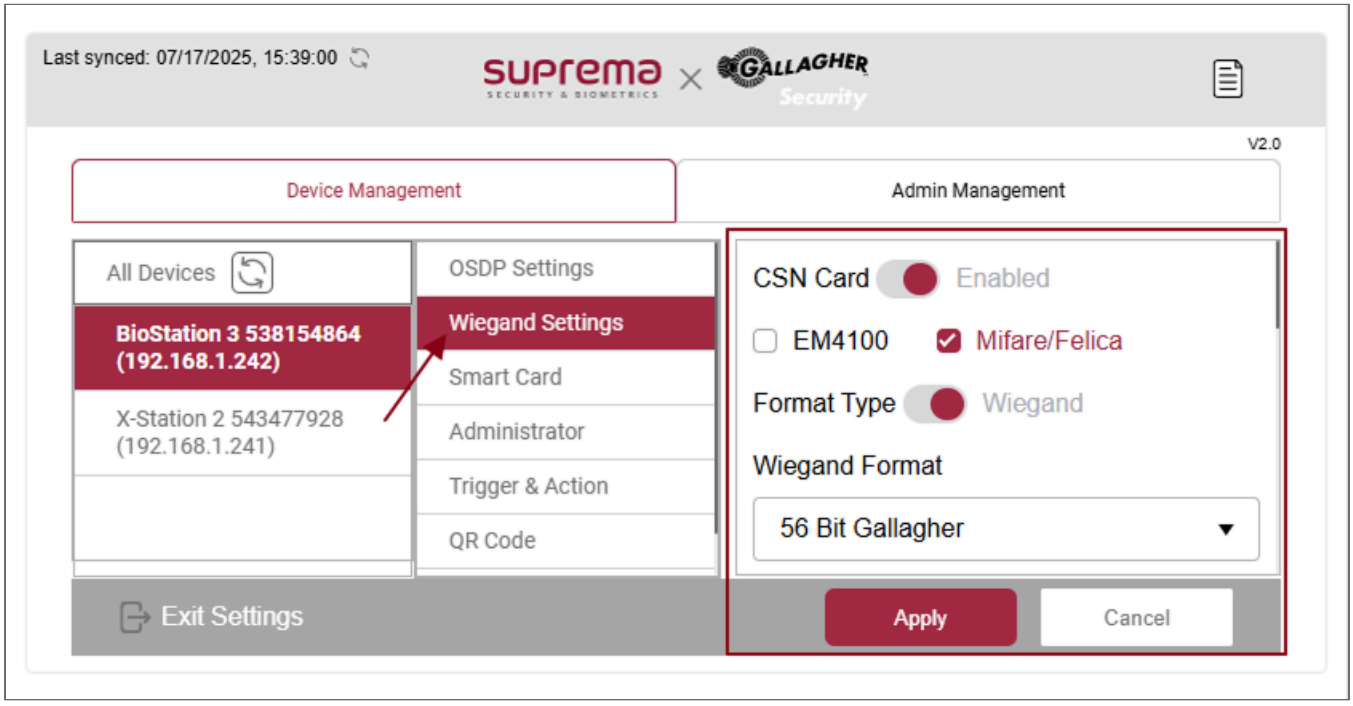
9. You have to **press** the sync button to sync the devices and you can see all the connected devices from here and select any of the connected devices to see the device setting.

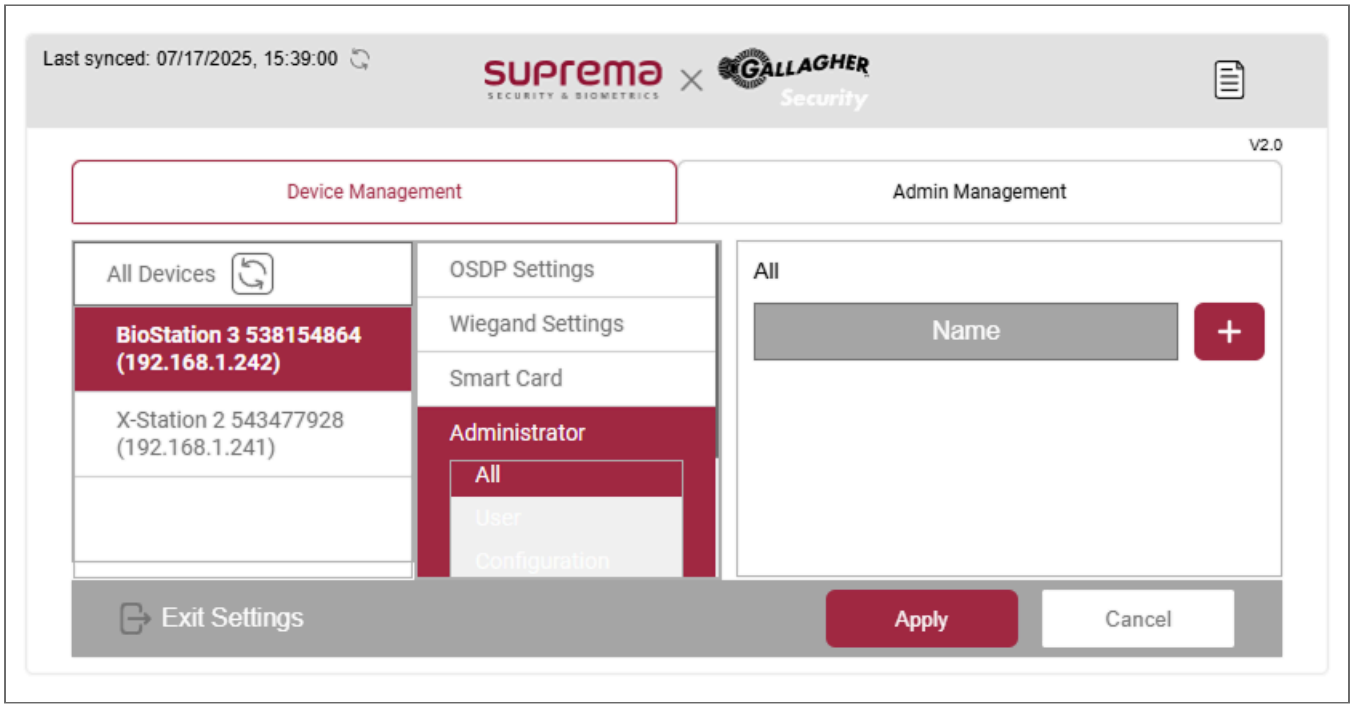


10. The below image indicates the device's OSDP settings.

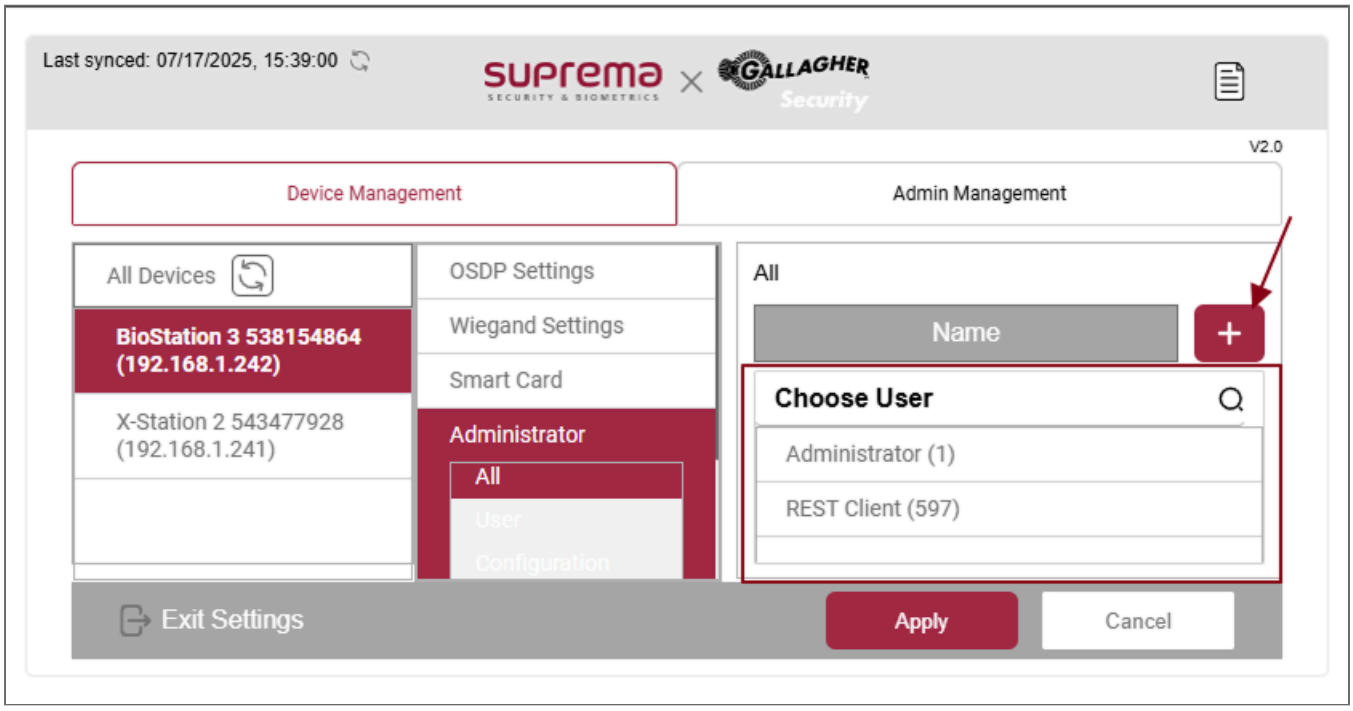


11. The images below are for the device's Wiegand setting.

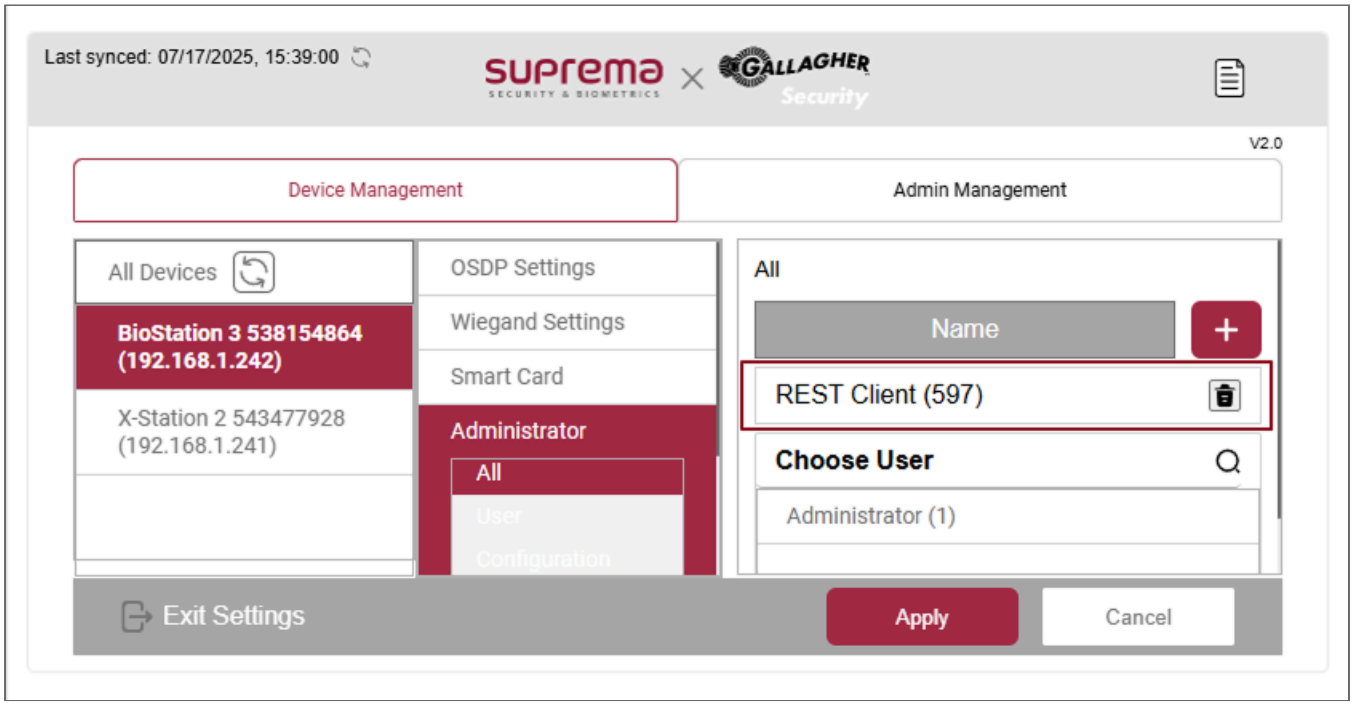




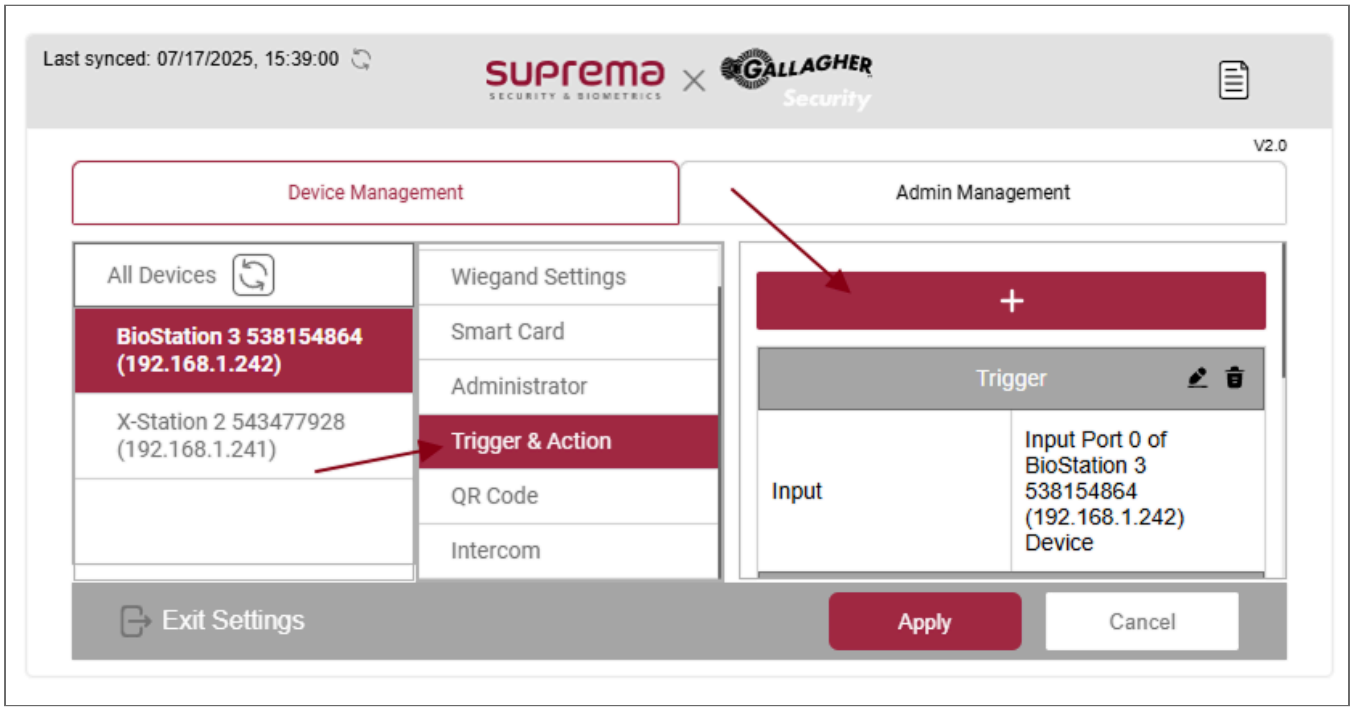
12. So the above image is for administrator mode where you can choose modes according to your needs, as you can see in the below image by **pressing** the + button you can select different users from the dropdown.



13. After **selecting** the user it can be displayed like the below image, you can delete the user from the list by **clicking** on the delete button.

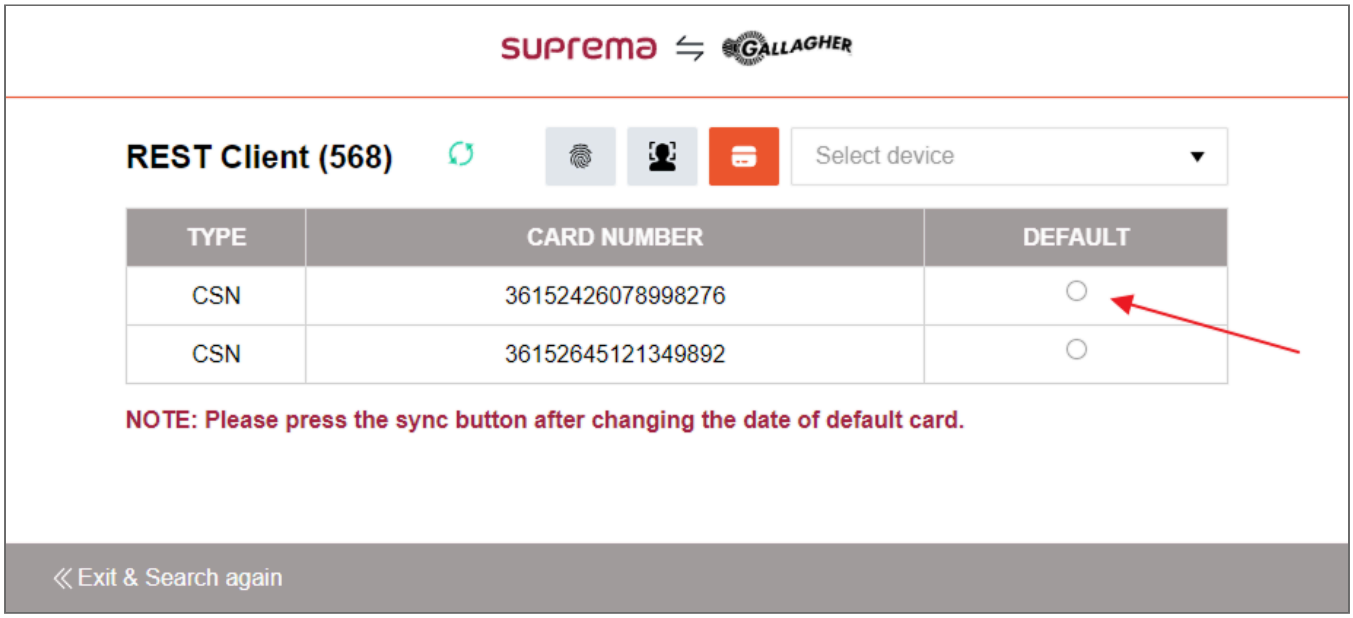


14. This is the trigger and action mode for the device's output mode. You can configure it by **pressing** the + button.

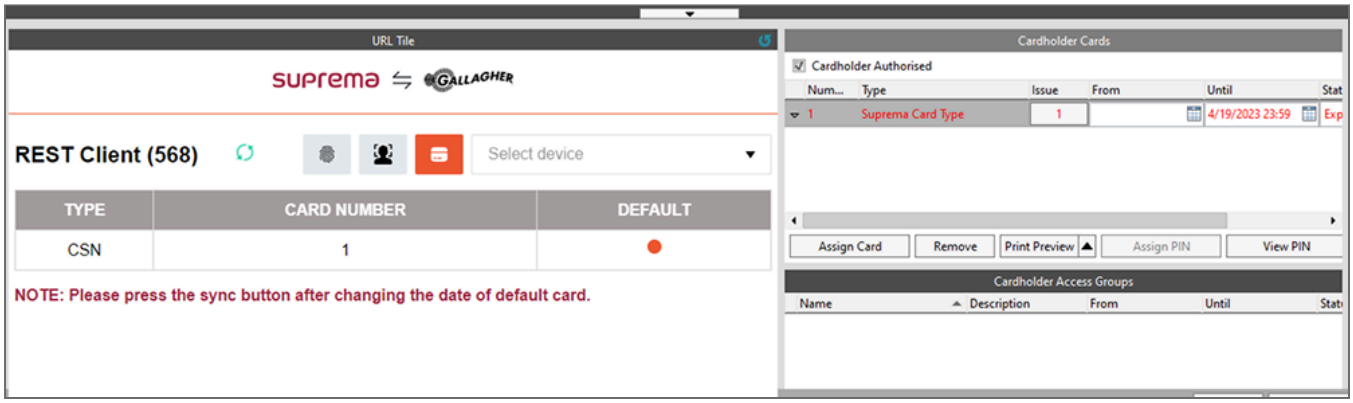


Default card Selection

1. You can select the default card by **pressing** the radio button for the user.



2. You can **set** cardholder expiry by setting the expiry date to default card.

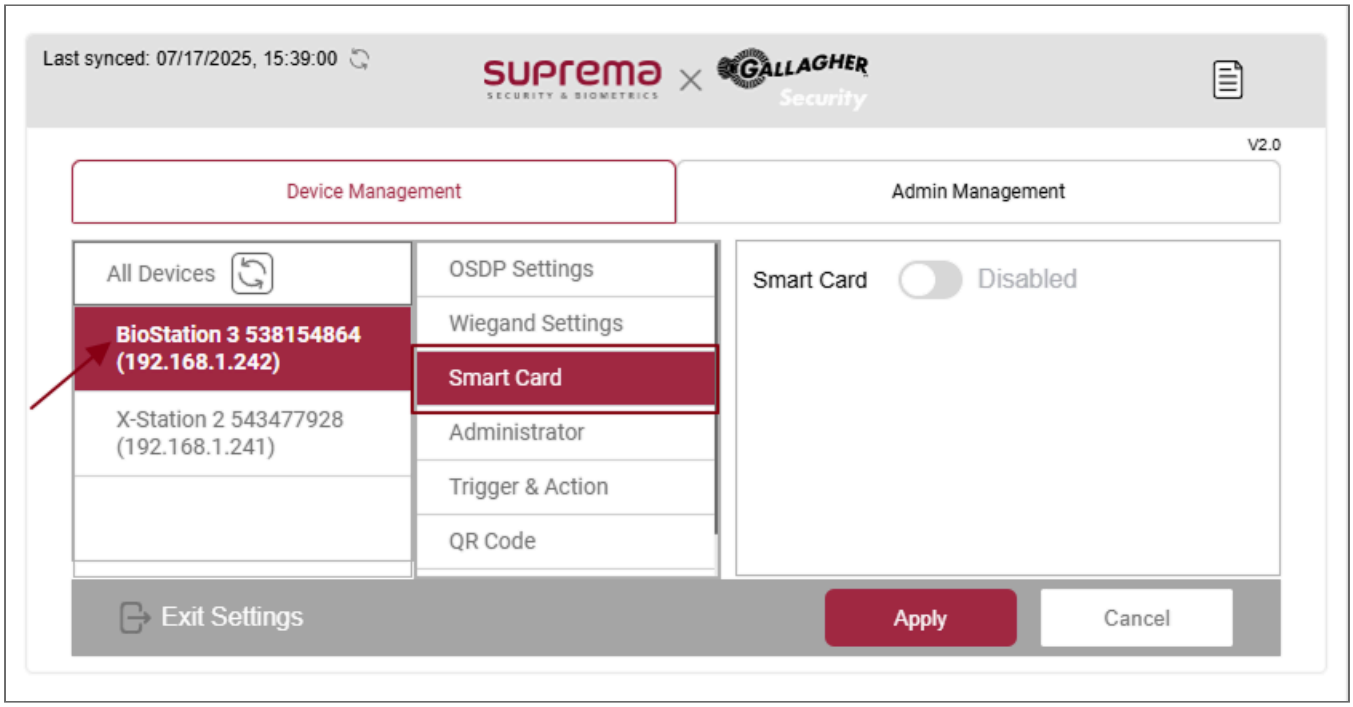


> **Info**
> If you made any changes in cardholder details, from the Command Centre. You need to open the same user in Suprema integration with middleware and press the sync button.

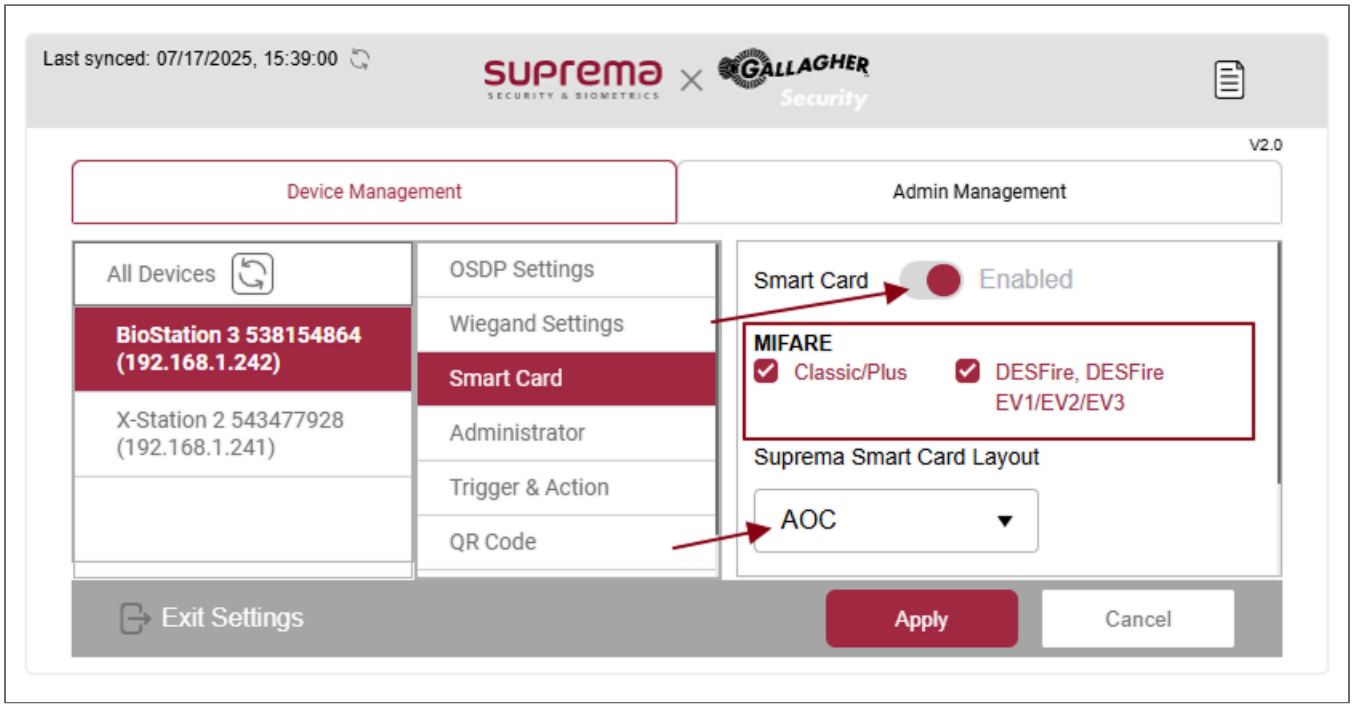
Smart Card (AOC/TOC)

> **Info**
> You must have a 2.9.4 or above version of BioStar 2 to use the smartcard feature.

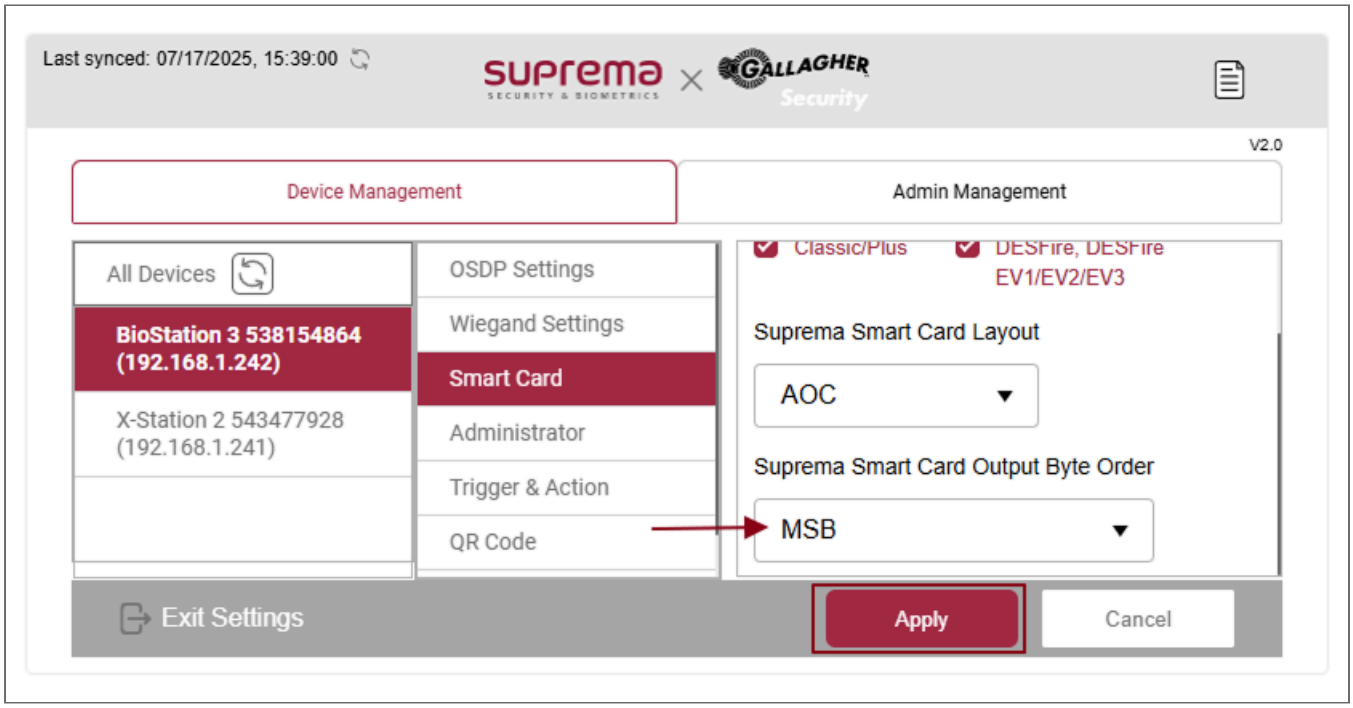
1. If you want to use the Smart Card (AOC/TOC) option go to settings in the device, **press** the **settings** button, and inside Device Management **select** the device you want to configure and **select** the Smart Card option.



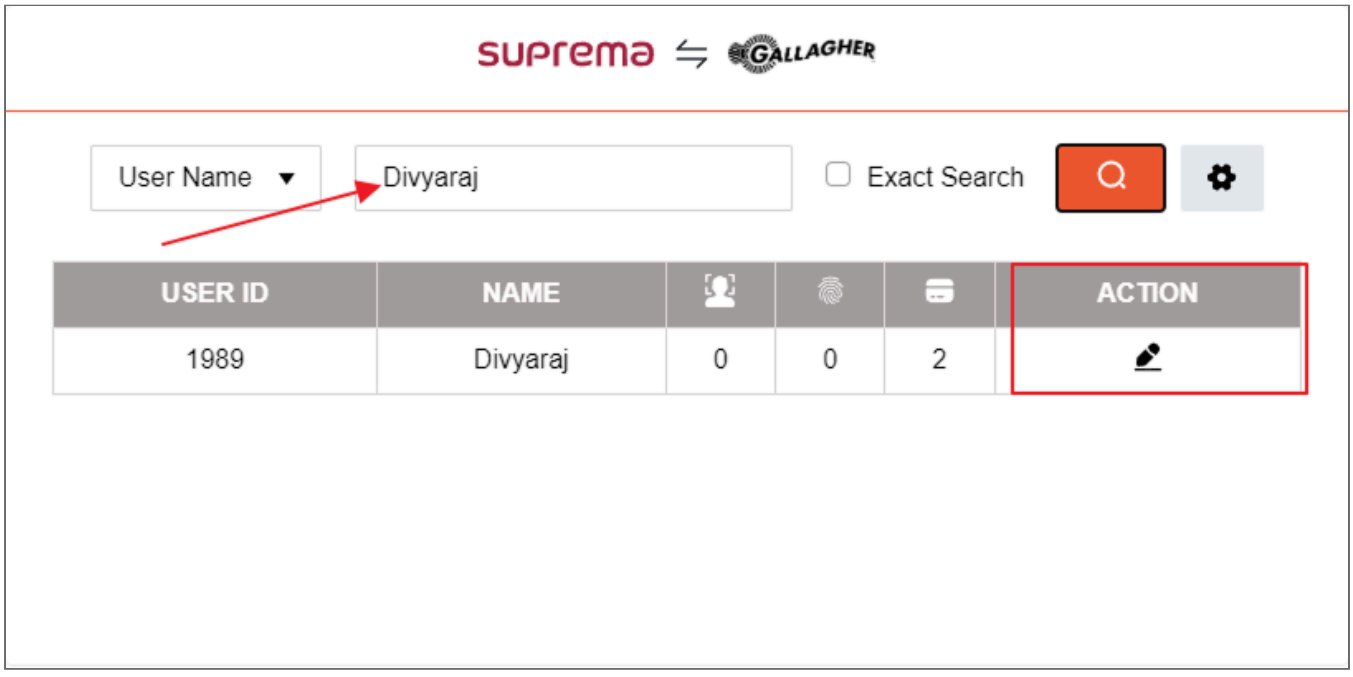
2. Now **enable** the Smart Card toggle and do the following settings as below screen.



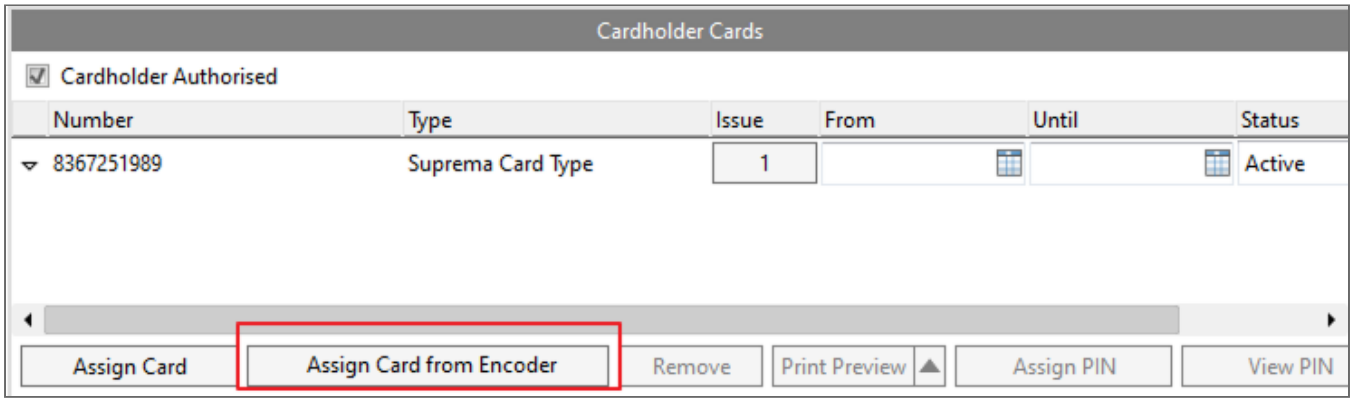
3. After changing all the settings, **press** the Apply button. After that, **press** the Exit Settings button from the bottom left corner to exit from the settings tab.



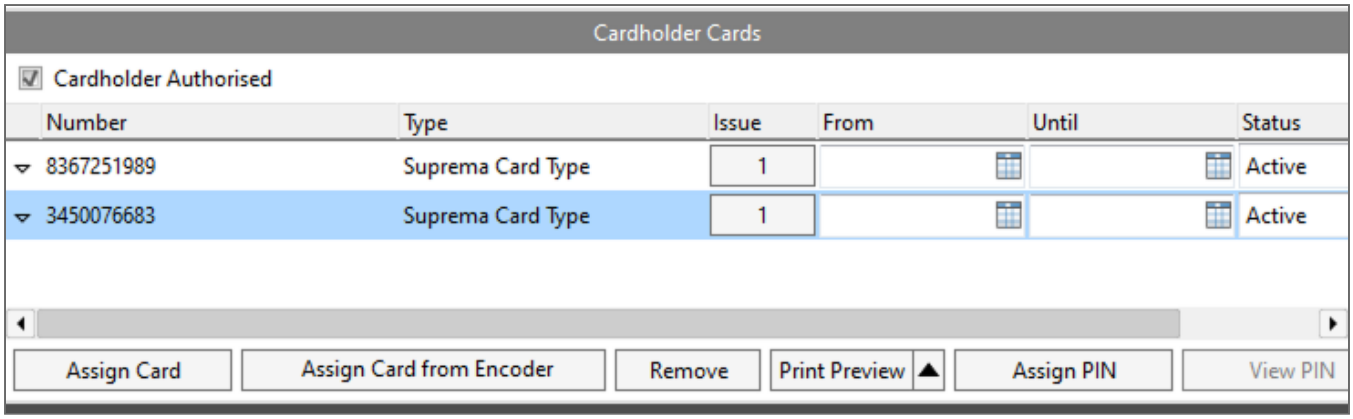
4. Now search for the user on the user search screen, you want to apply the smart card and **press** the edit button to view user details.



5. Now to assign the smart card you need to assign a card from the encoder from the Gallagher inside cardholder cards tab.

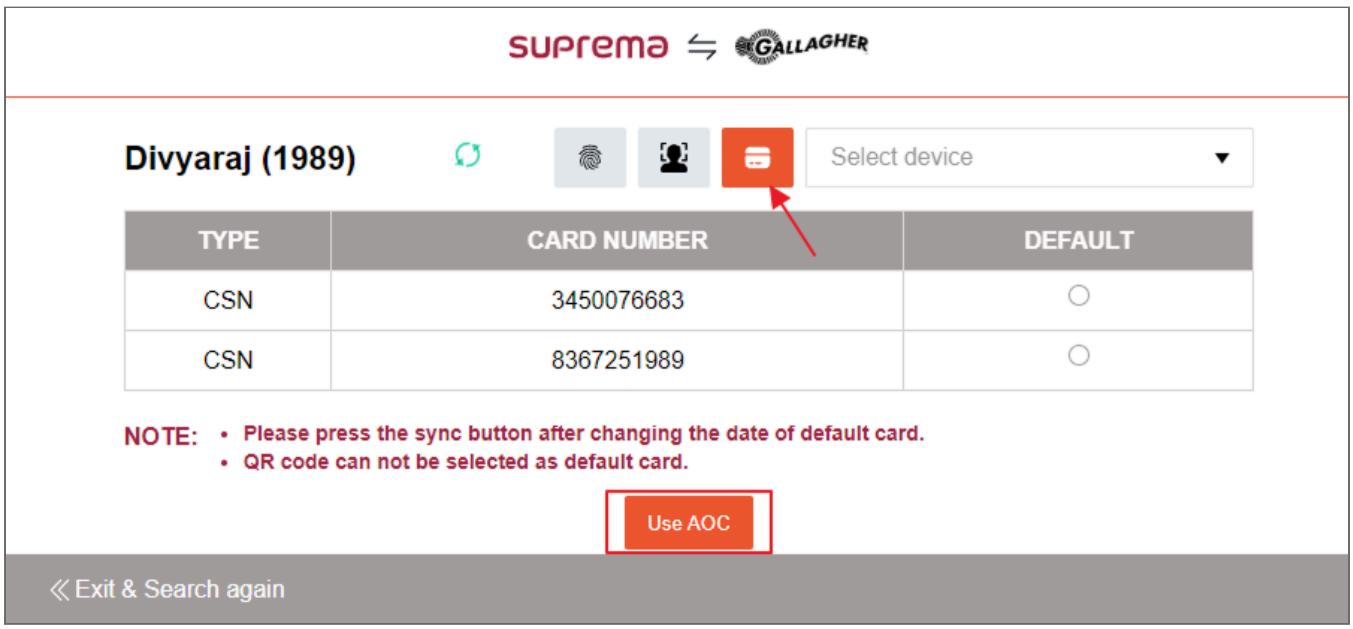


6. After pressing the button you can see the card number now you have to **press** save to inside Gallagher and you can see the newly assigned card.

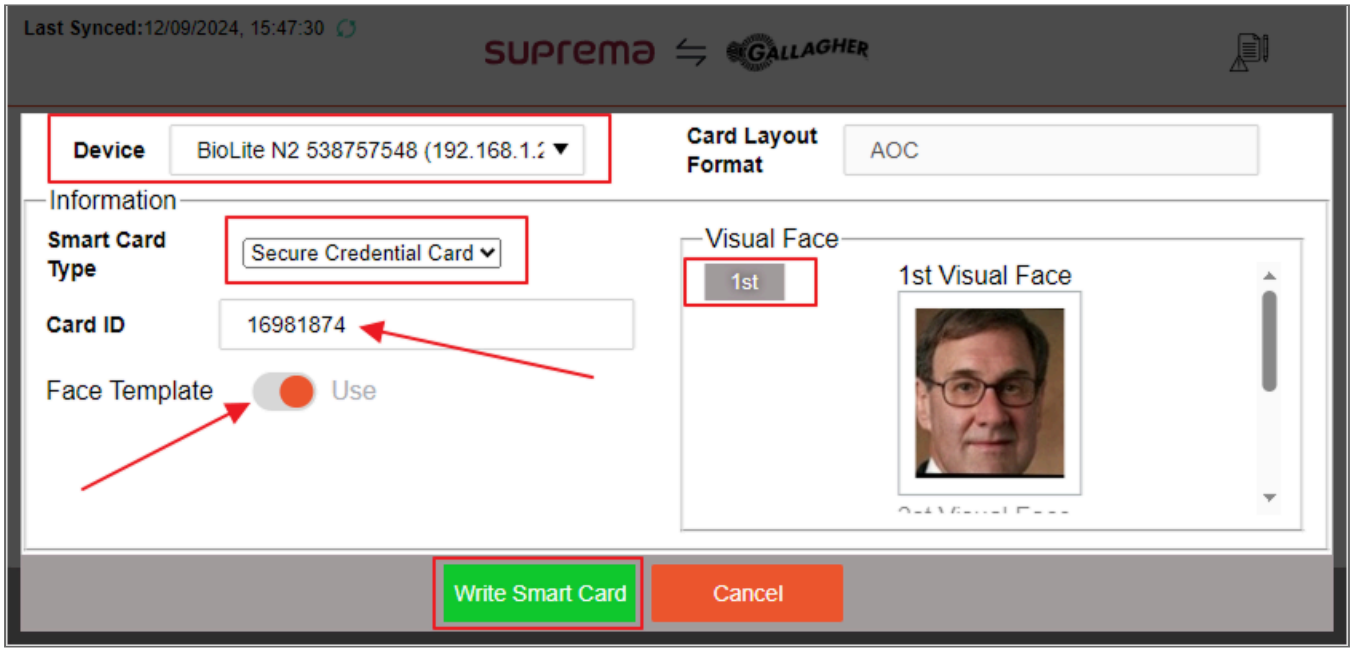


7. Now inside the user details table **go** inside the card section and **press** the Use AOC button to assign a smart card to the user.

> **Info**
> To assign a Smart Card (AOC) for the user, the user must need the biometrics.



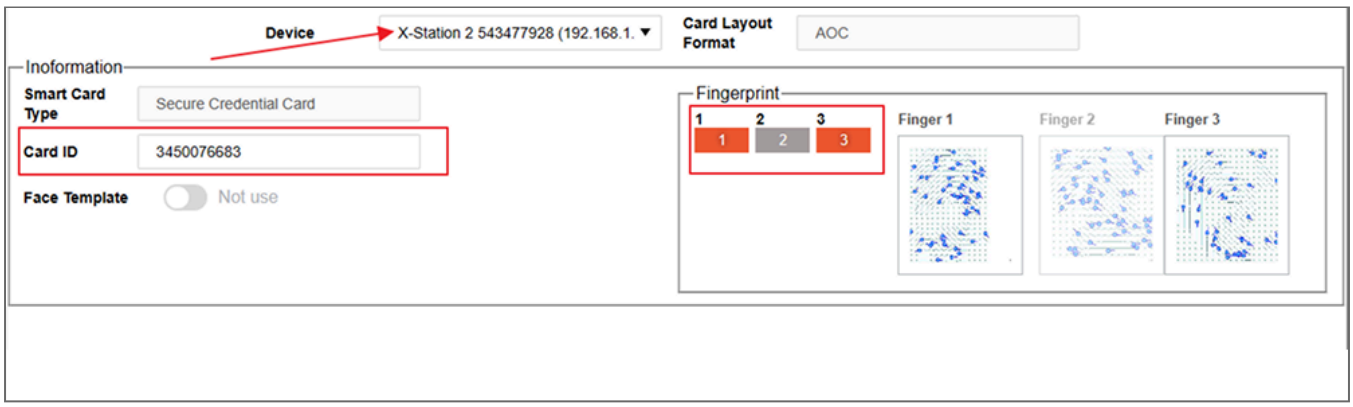
8. Now **select** the device you want to use for AOC, and **use** the same number for the card ID we get while assigning from the encoder. **Select** the face template and **choose an** image of the visual face tab. **Press** the write smart card button.



9. Now you have to **scan** the same card against the selected device to assign the card to the user. If you are not scanning the same card you will get an error message, else it will write the card for the user and clear all the biometric information for the user.

> **Info**
> You can only assign one biometric to the Smart Card (AOC) for the user.

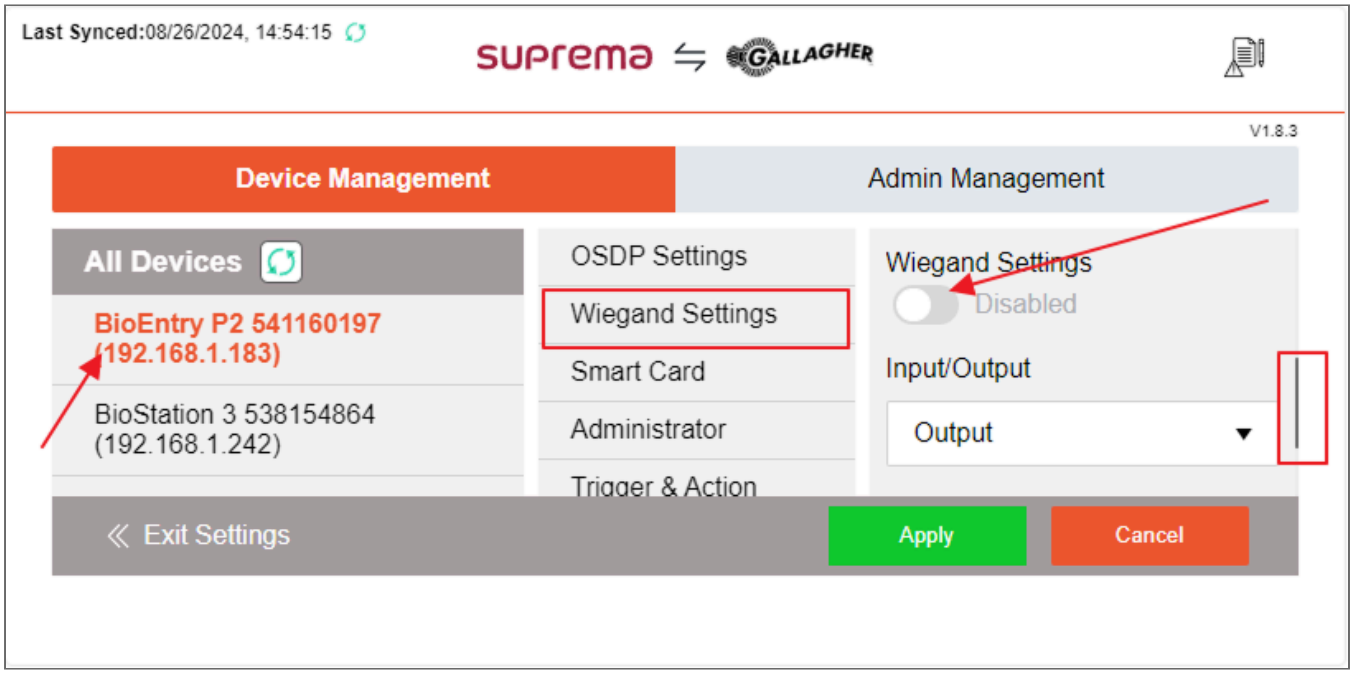
10. To assign the smart card with a fingerprint user must need a fingerprint, the user can assign up to 2 fingerprints per card. Inside the user card section **press** the Use AOC button and select the device, **use** the same number for the card ID we get, while assigning a card from the encoder. **Select** the fingerprints that you want to use for the smart card. **Press** the write smart card button.



11. Now you have to **scan** the same card against the selected device to assign the card to the user. If you are not scanning the same card you will get an error message, else it will write the card for the user and clear all the biometric information for the user.

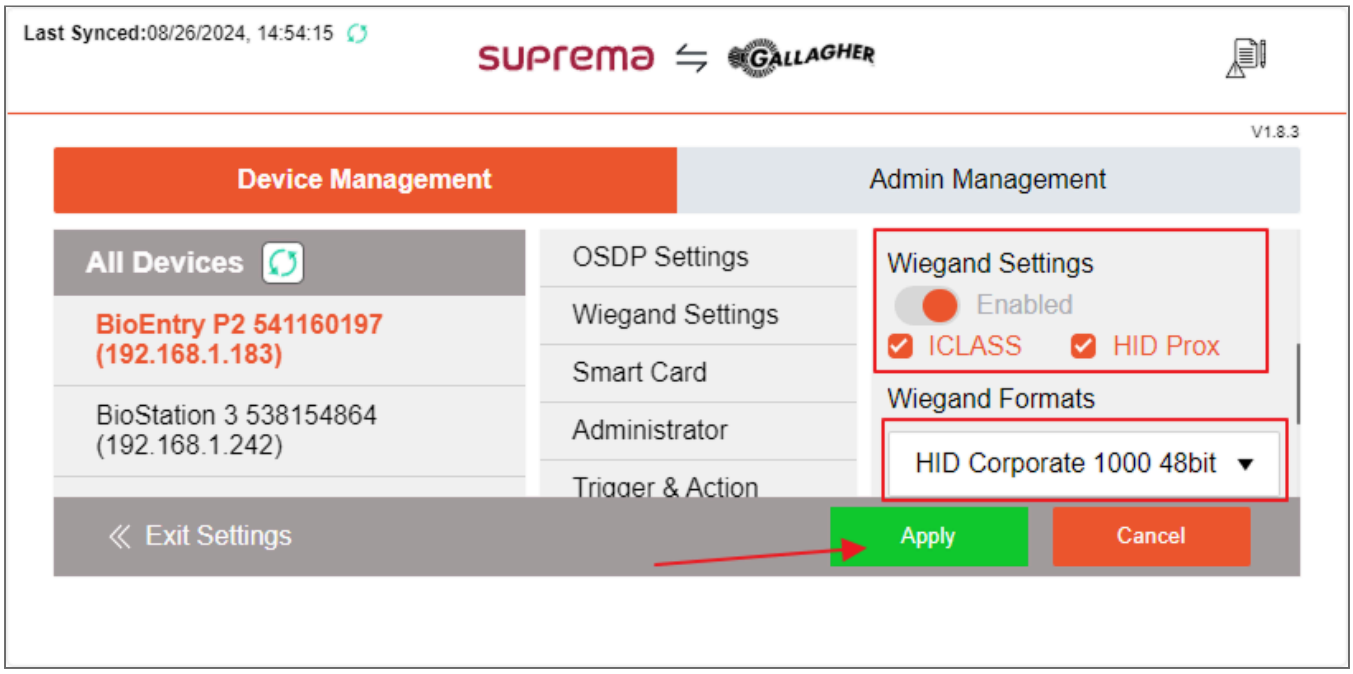
HID ICLASS card

1. If you want to use the HID ICLASS card option go to settings in the device, **press** the **settings** button, and inside Device Management **select** the device you want to configure and **select** the Wiegand Settings option then scroll down and find the Wiegand settings.

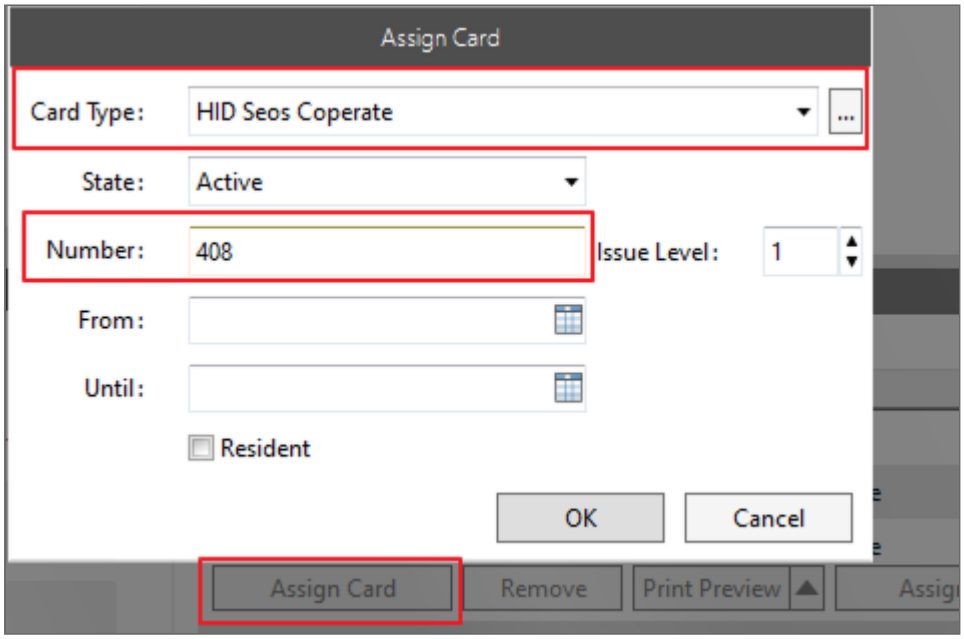


2. Now enable the Wiegand Settings option, and **select** ICLASS AND HID PROX Options. The Wiegand format must be the same as the selected default in the dropdown. **Press** Apply the button to save the changes.

> **Info**
> To use the Wiegand card you must need at least one biometric for users.

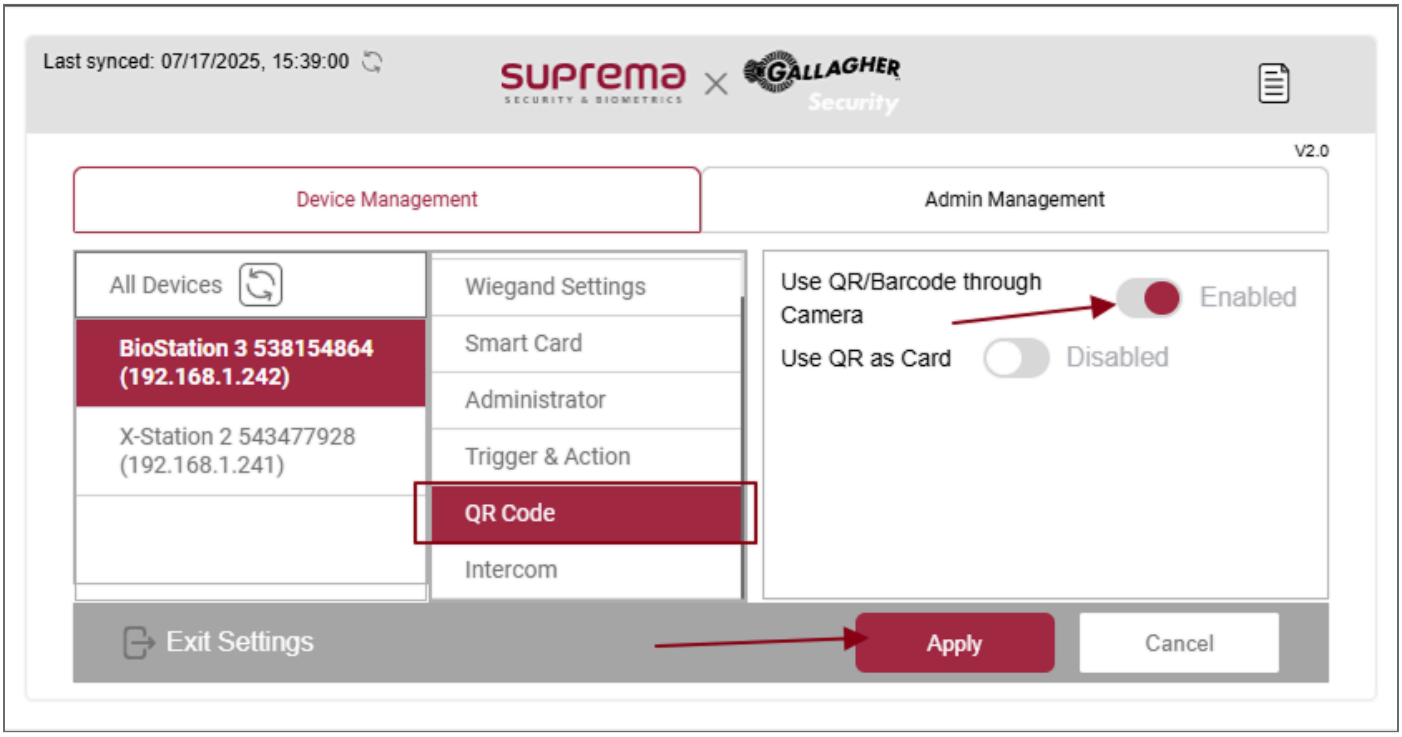


3. To use the feature, you have to assign the card to the user. Go to the Gallagher command center, press the assign card button, **select** the HID Seos Corporate, **enter** the number, **press the** OK button, and **press** Save.



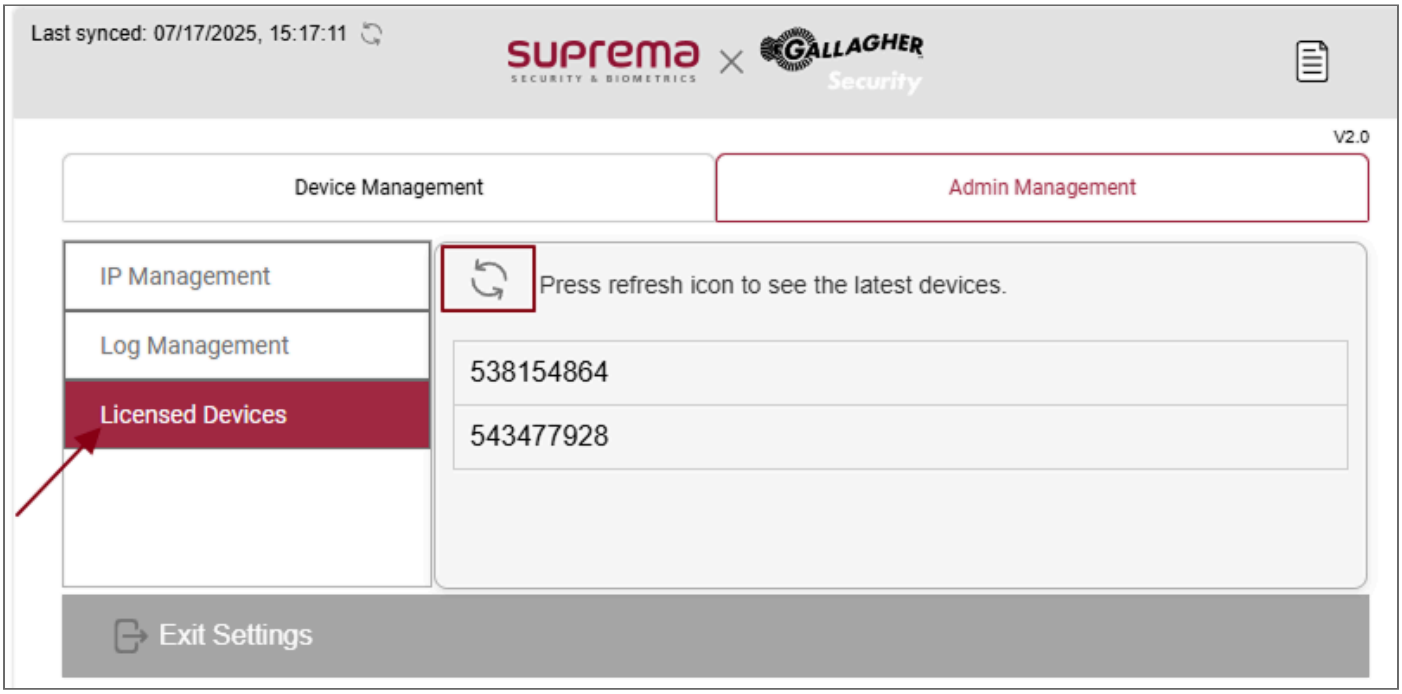
QR Code Card

If you want to use the QR Code card option, go to settings by **pressing** the **settings** button, and inside Device Management, **select** the device you want to configure. Then, **select** the QR Code Settings option, and **enable** the use of QR/Barcode through the camera option settings. **Press** the Apply button to save the changes.



Licensed devices

If you want to check the devices associated with the **license**, you need to go to **Admin Management** under **settings** and **click** on the Licensed devices, and then need to **press the** sync button. It will show the latest devices list associated under your license.


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

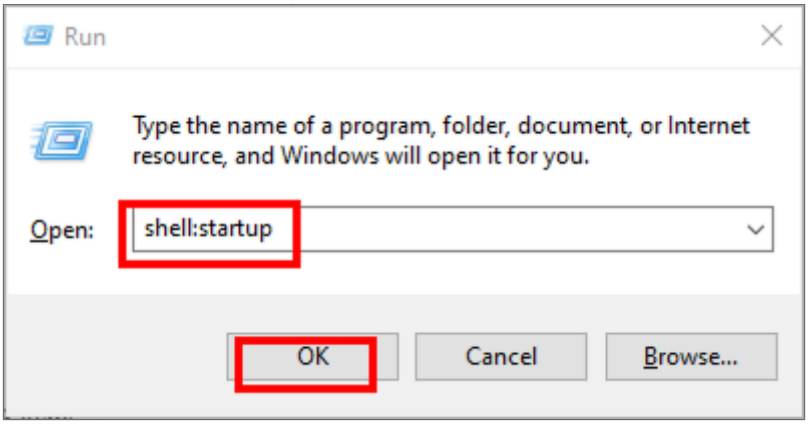
Troubleshooting and FAQ

Setup

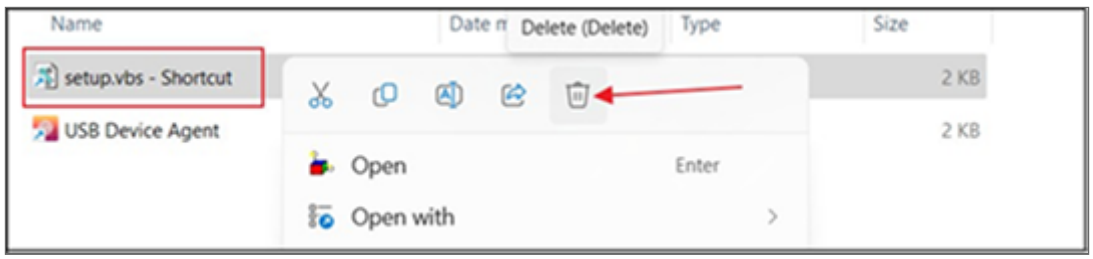
Q. Upgrade only middleware to the new version (Manual process).

A. If you want to upgrade only middleware you just need to follow the steps shown below.

> **Info**
> If you are upgrading middleware to V1.8.3, please refer: Create Migration Manually.

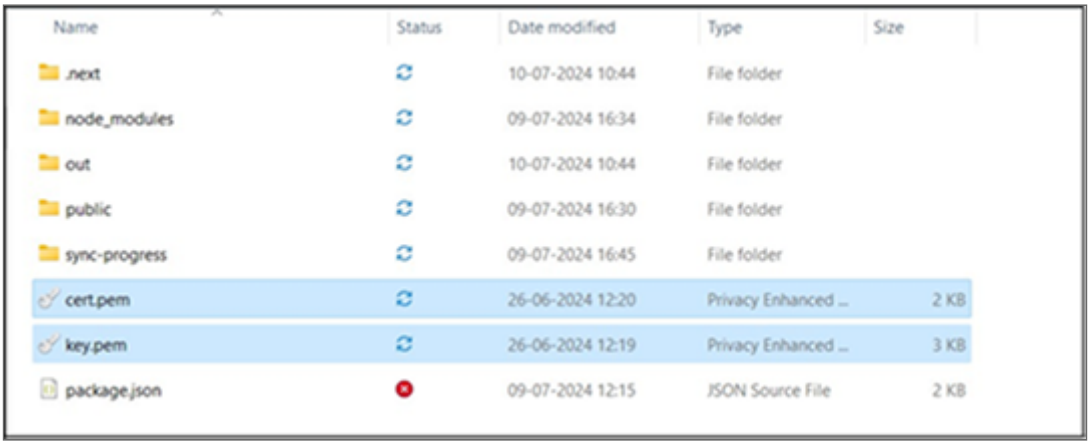


Delete the previous version `setup.vbs - Shortcut`.



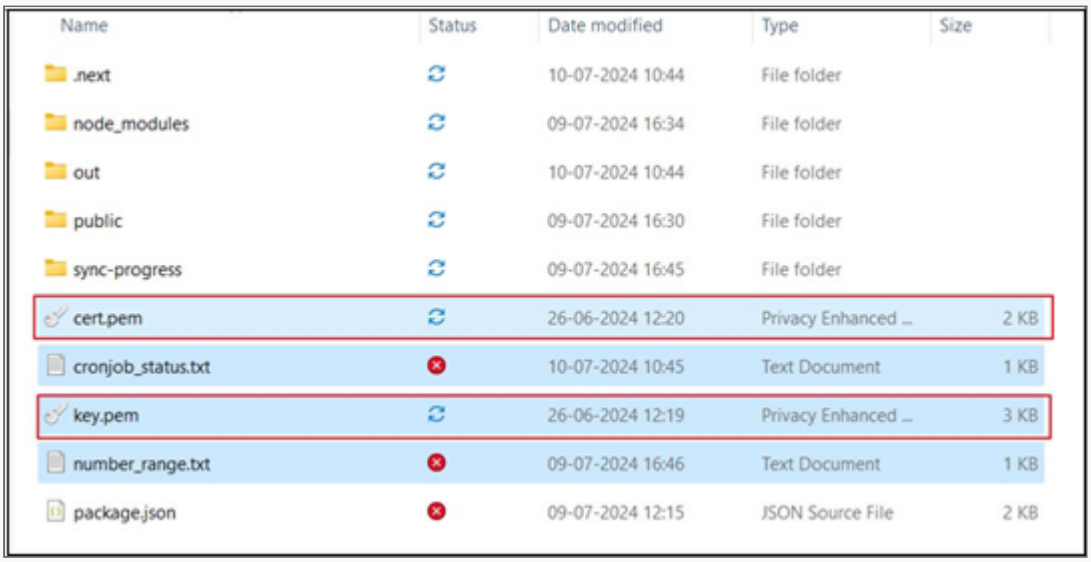
Cut cert and key files from the version you are currently using as shown in the below image.

The default path would be: `C:\Program Files\Suprema Integration with Gallagher\Suprema Integration with Gallagher v(Current working version)\files`

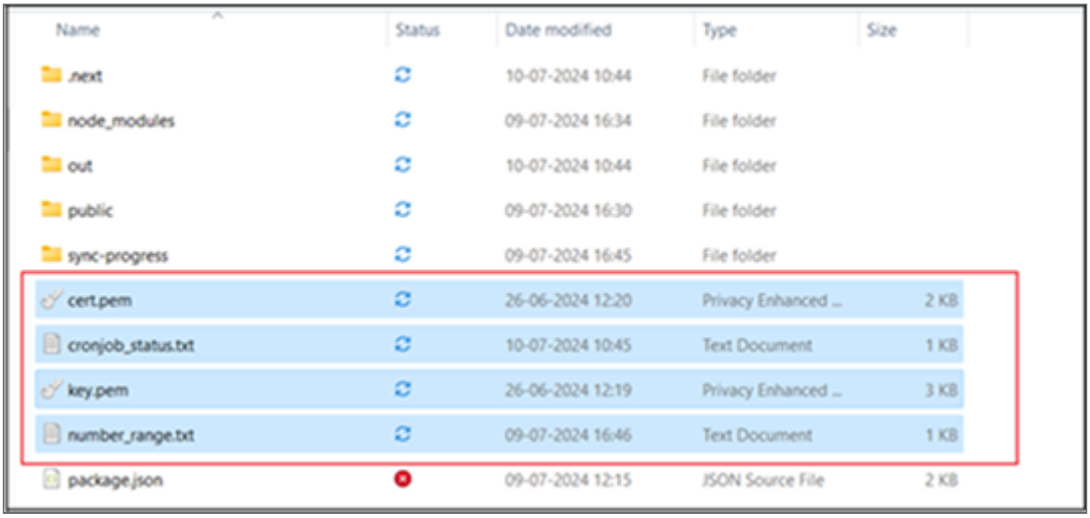


Info

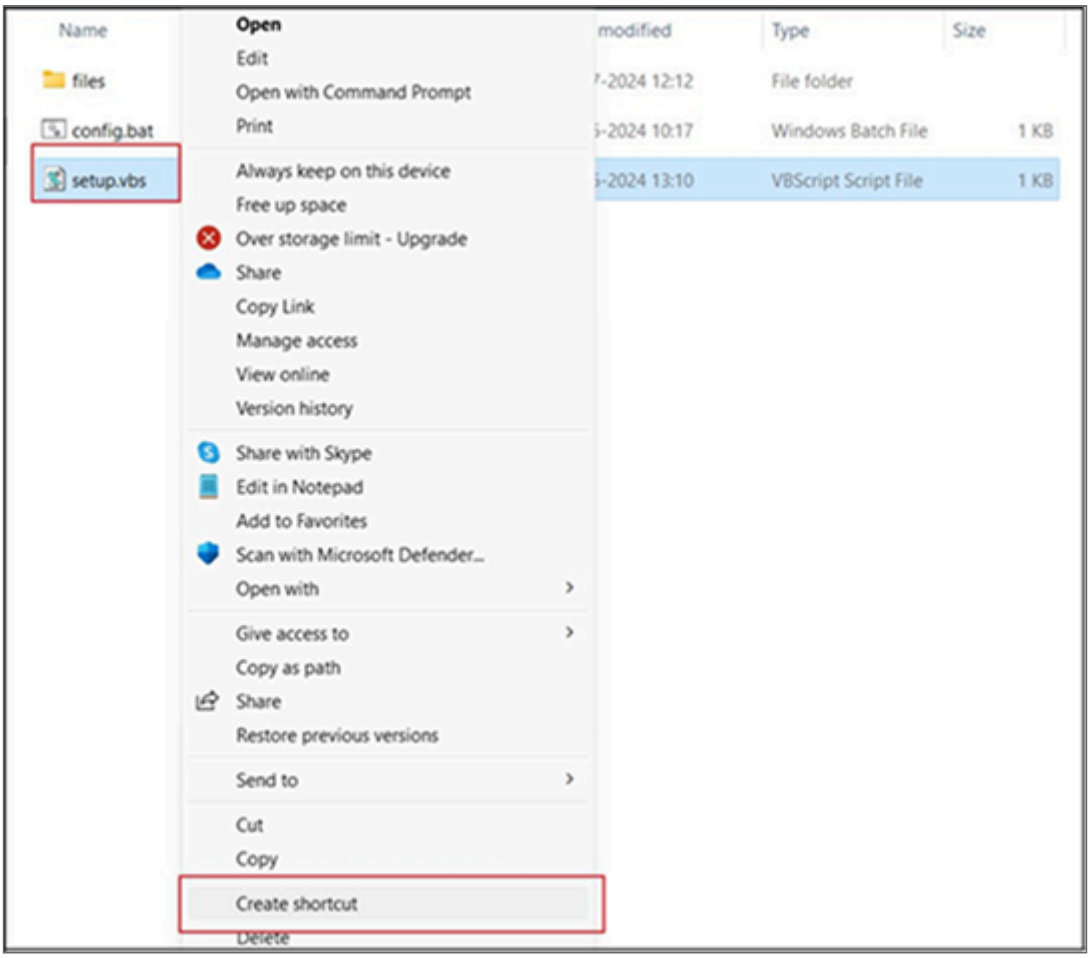
- If you are upgrading from the 1.8.0 or above version you will need to cut a total of four files, Which are `key.pem` , `cert.pem` , `cronjob_status.txt` and `number_range.txt` .
- In the 1.7.0 version only number_range is not available so cut the other three files.



Now **paste** the files into the new version of Suprema integration with `Gallagher V(new version)\files` , as mentioned above if you are upgrading from 1.8.0 or more you will need to cut 4 file and below image show the image that are pasted to new version with 4 files, so in case if you dont have 4 files just paste 2 files from old version to new version.



Create short cut of setup.vbs of the latest version of Suprema integration with Gallagher and cut the shortcut file.



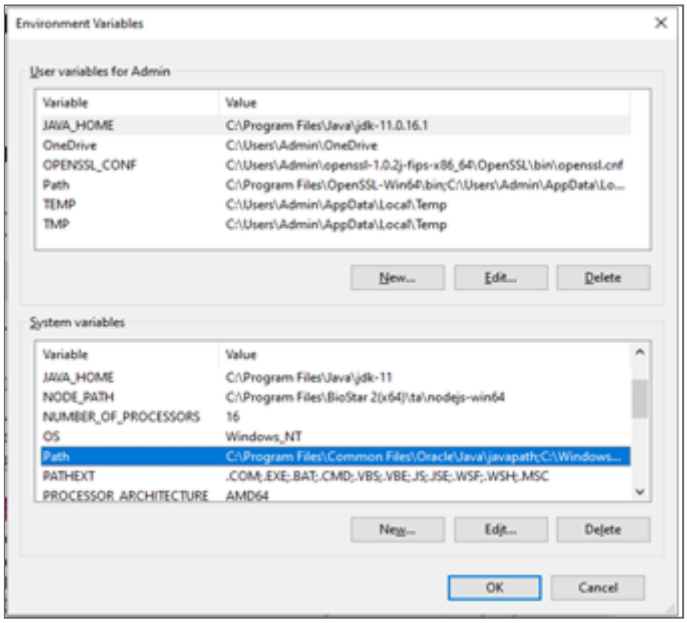
Go Run `Win + R` and paste it on `shell:startup` and after that restart your desktop.

Q. If the middleware is not getting started automatically.

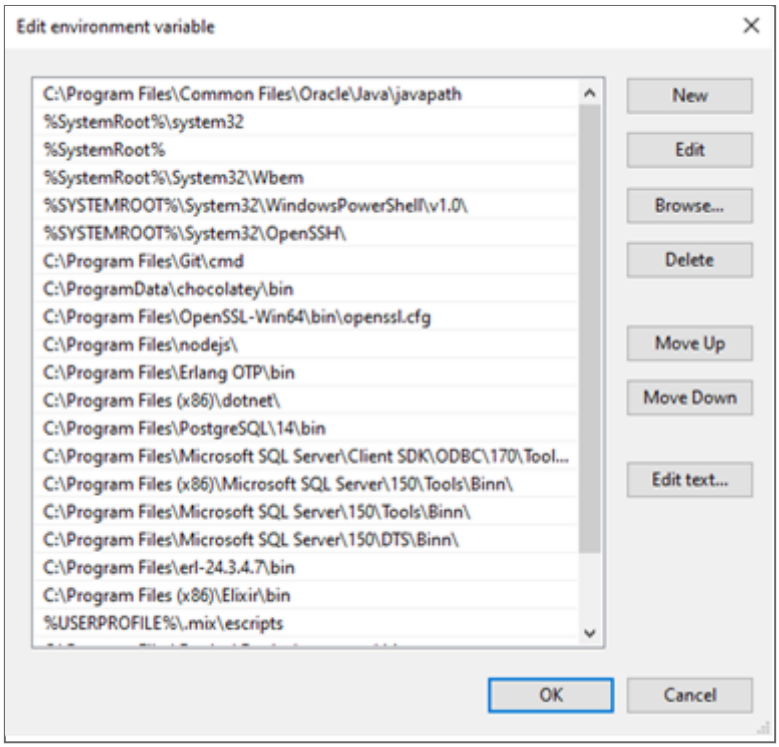
A. First, make sure that the shortcut of the setup.vbs file is present on the `shell:startup`. If setup.vbs is not present please paste it to `shell:startup` and restart your system.

Still, the middleware is not getting started automatically then check for the environment variable, you can access it by pressing Start ⊞ → Edit the system environment variables → click the **Advanced** tab → **Environment variables** button near the bottom of that tab.

In the *Environment Variables* window (pictured below), select the **Path** variable in the *System Variables* section and click the **Edit** button.



The edit environment variable window will be open (pictured below), click on the **New** button and add the `C:\Program Files\nodejs\` path and press the **OK** button.



Press the **OK** button for the *Environment Variables* window then press the **OK** button for the system properties.

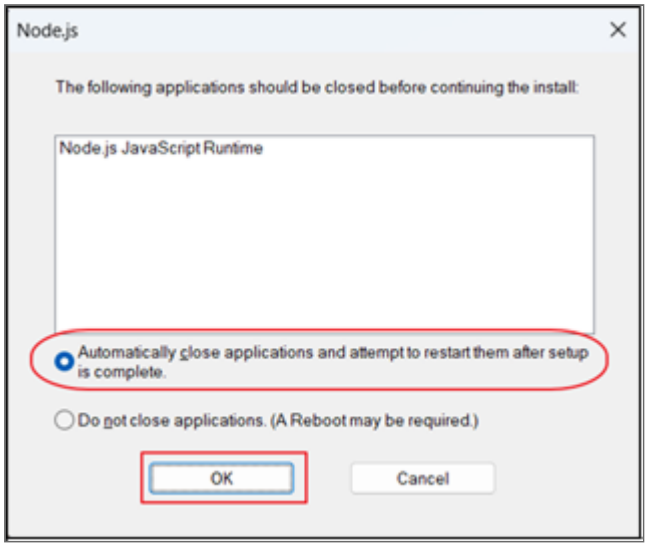
> **Info**
> After creating or modifying the environment variables, restart the computer for those changes to take effect in Windows.

Q. To uninstall the middleware prerequisites list.

A.

So below are the steps to uninstall the middleware prerequisites,

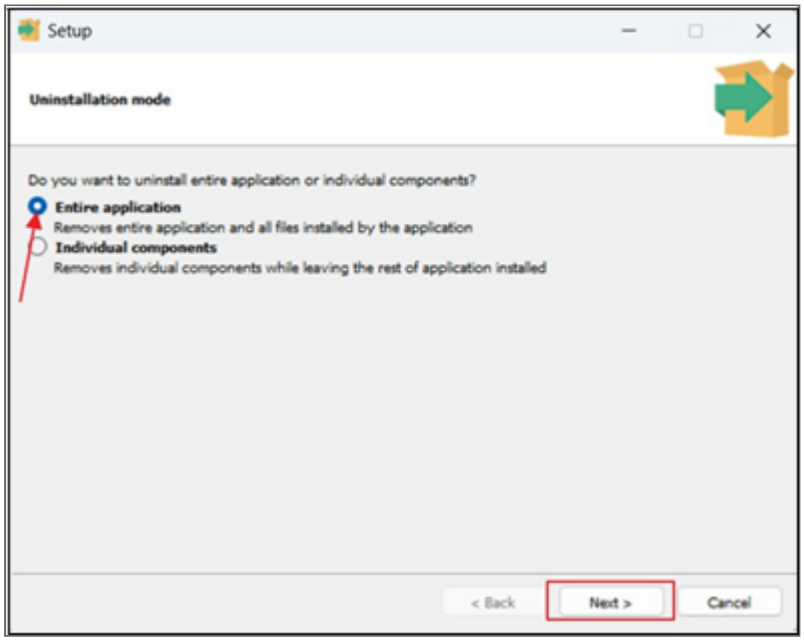
1. **Open** the control panel and go to the Programs and Features section.
2. Scroll down and **search** Node.js, Right click on that and **select** Uninstall.
3. It asked to uninstall Node.js, **press** Yes and it started uninstalling.
4. After some time when it asks for Runtime application, Follow the below and **press** OK. Skip this step if it does not apply to you.



5. Now search for **OpenSSL**, Right click on that and **press** uninstall.
6. It asked to uninstall OpenSSL, press **Yes** and it started uninstalling.
7. Now search for **PgAdmin 4**, Right-click on that, and **press** uninstall.

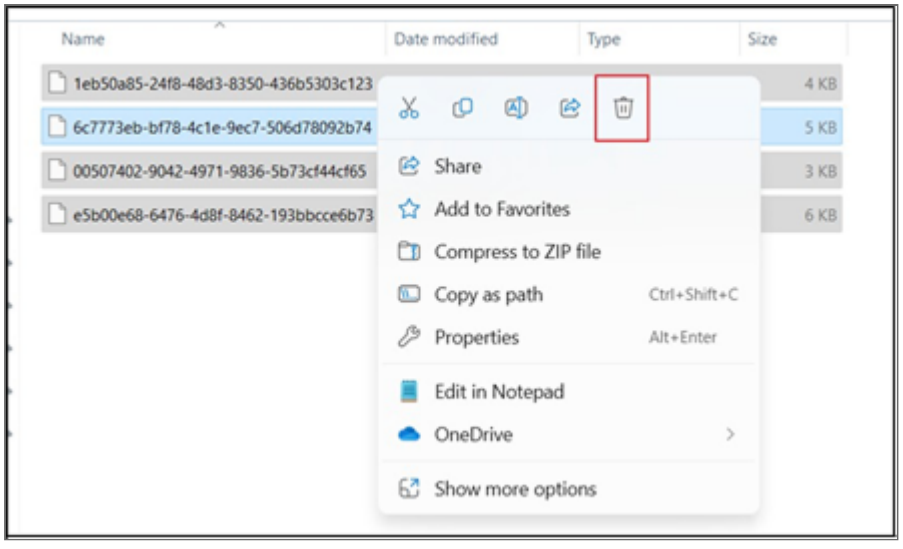
> **Info**
> If you are not able to see/uninstall the PgAdmin 4 just skip the step And follow the next steps.

8. It asked to uninstall PgAdmin 4, press **Yes** and it started uninstalling.
9. Now **search** for PostgreSQL 14, Right click on that and **press** uninstall.
10. It asked to uninstall PostgreSQL 14, press **Yes** and it started uninstalling.
11. When Uninstallation mode is open, **Select** the Entire application Radio Box and press **Next**.



12. Now **go to** the `C:\Users\<YourUser>\AppData\Roaming\pgadmin\sessions` delete all the files inside this folder.

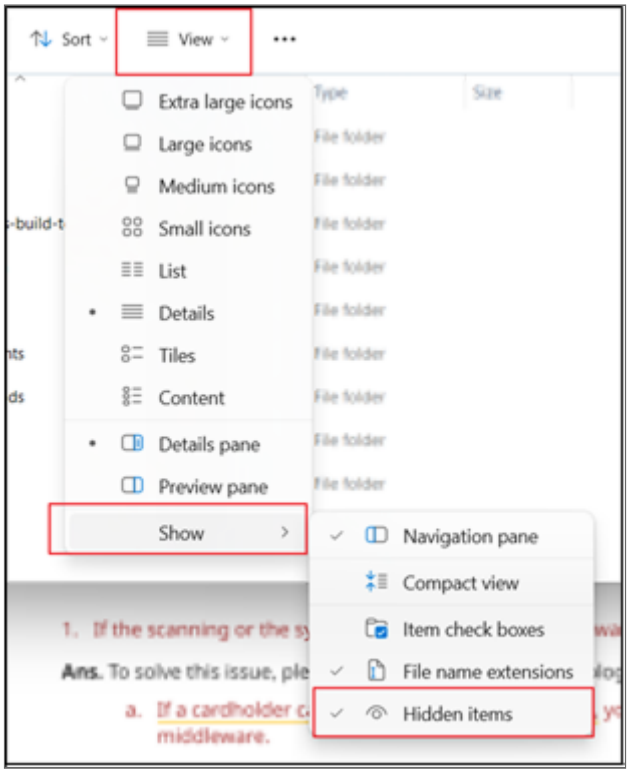
> **Info**
> If not able to see the AppData folder: Open the AppData folder in Windows.



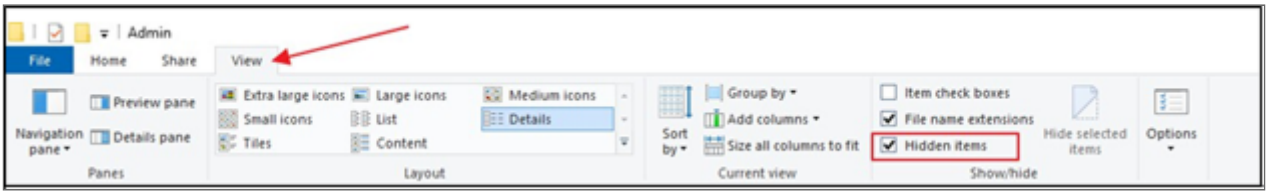
13. Now **go to** the `C:\Users\<Your User>\AppData\Local` and select PgAdmin and PgAdmin4 folder and **delete** the folders.
14. Now **go to** the `C:\Program Files` and delete the PostgreSQL folder.

Q. How to Open the AppData folder in Windows.

A. So if you are using Windows 11, Inside the file manager click on the View tab and **select** Show and **click** on Hidden items.



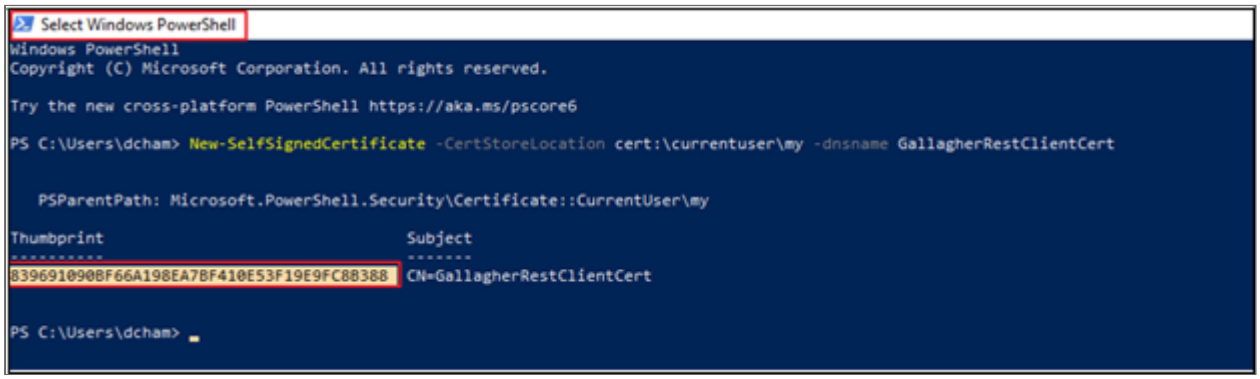
If you are using Windows 10, open File Manager and **click on** View and **select Hidden items**.



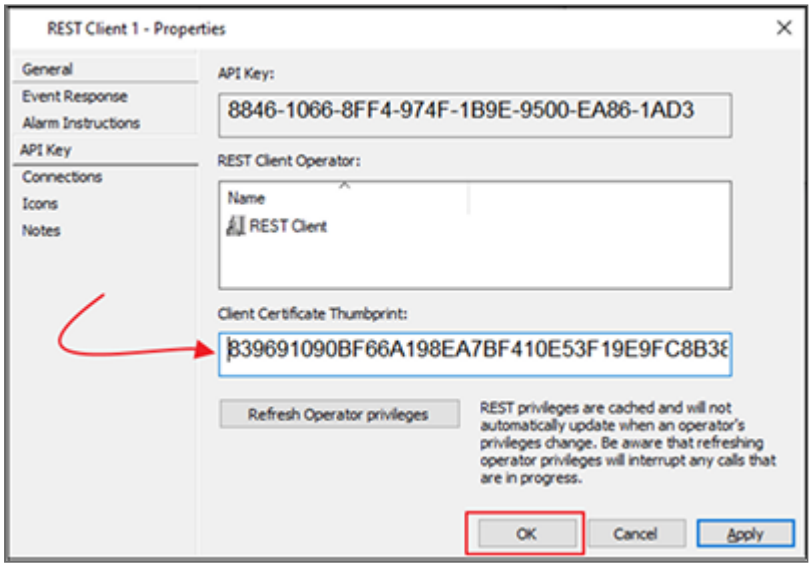
Q. How to generate the thumbprint and certificate manually.

A. 1. To generate Client Certificate Thumbprint, go to Windows PowerShell and run this command to get the certificate thumbprint.

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

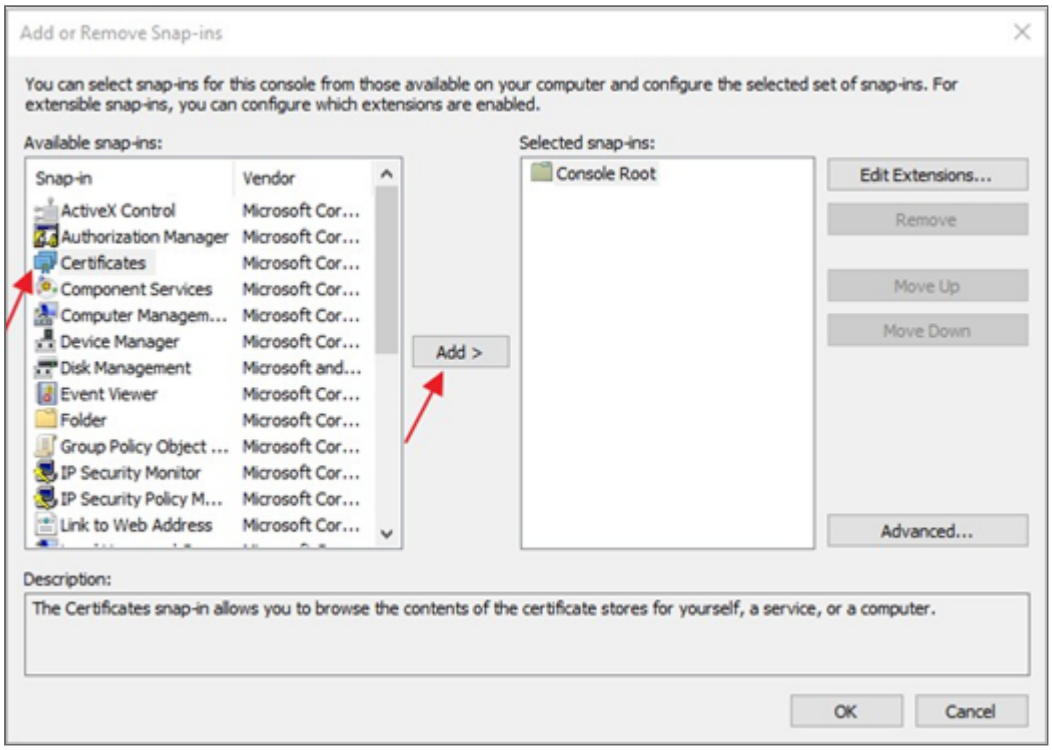


2. **Copy** the thumbprint and **Paste the Client Certificate Thumbprint key** into the Client Certificate thumbprint section **press** the **OK** button and also **Close** the Services and Workstations.

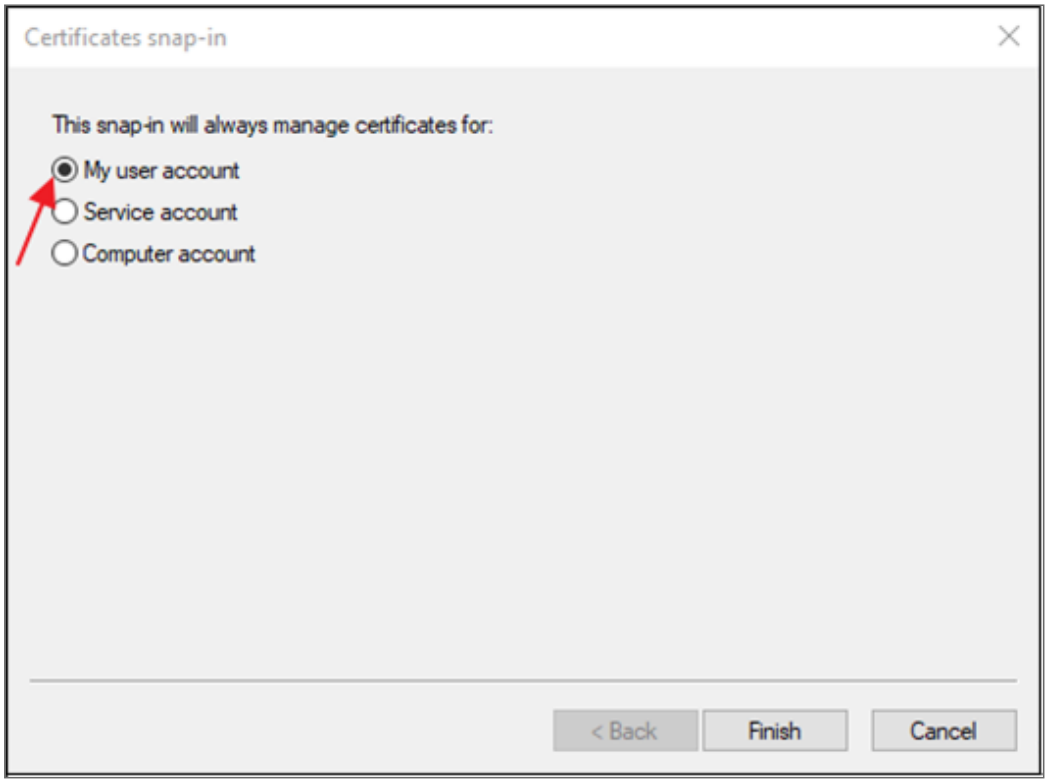


SSL Certificate Generation

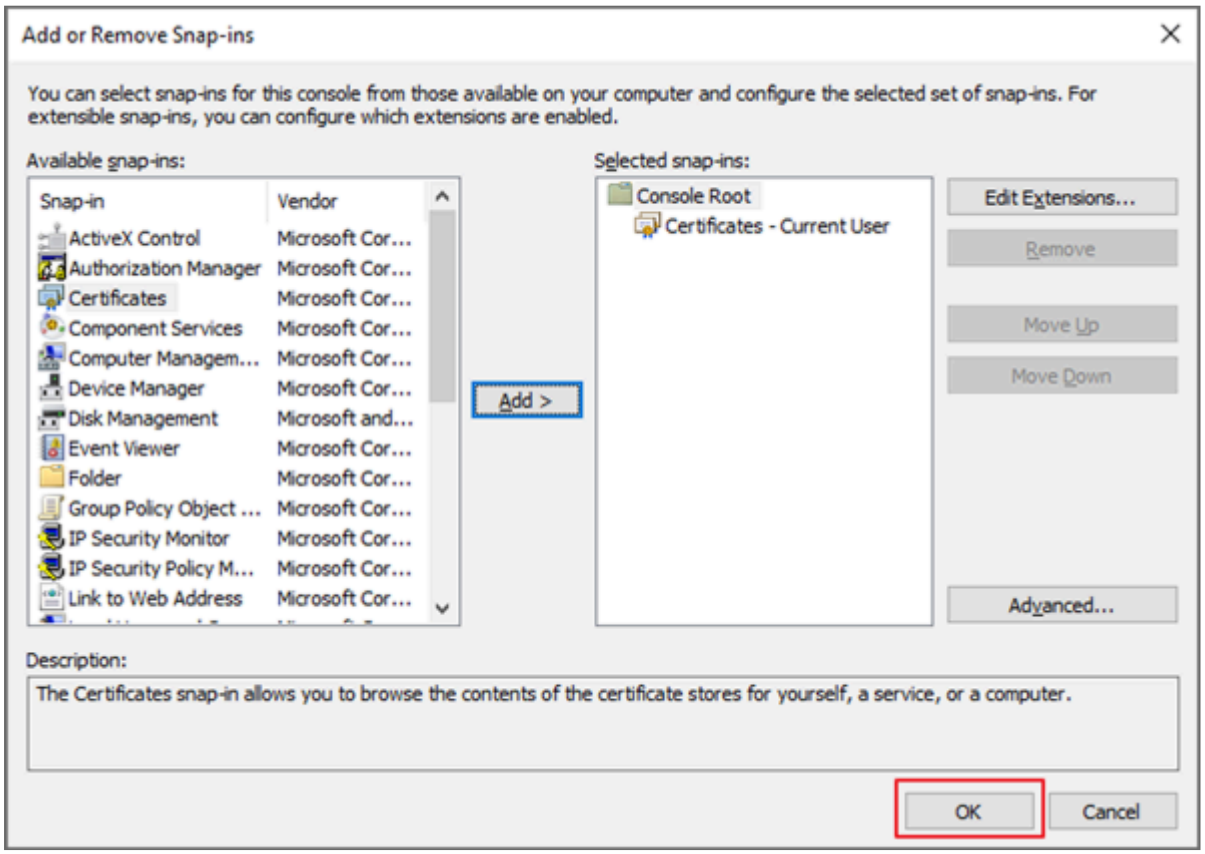
1. Go to the start menu and **Open** the **MMC** Application.
2. Go to **File** → **Add/Remove Snap-in...** you can see below screen.



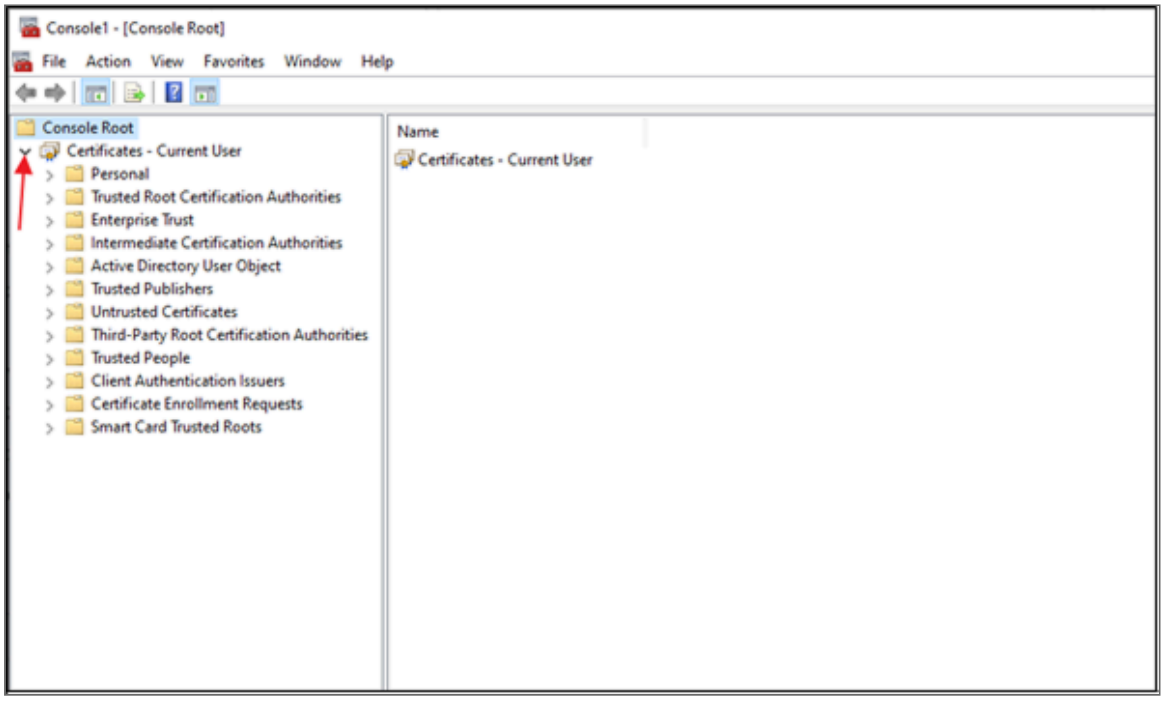
3. **Select Certificates** and **click** on **Add** button then you will see the below screen where **select** the **My user account** radio button and **click** on **Finish** button.

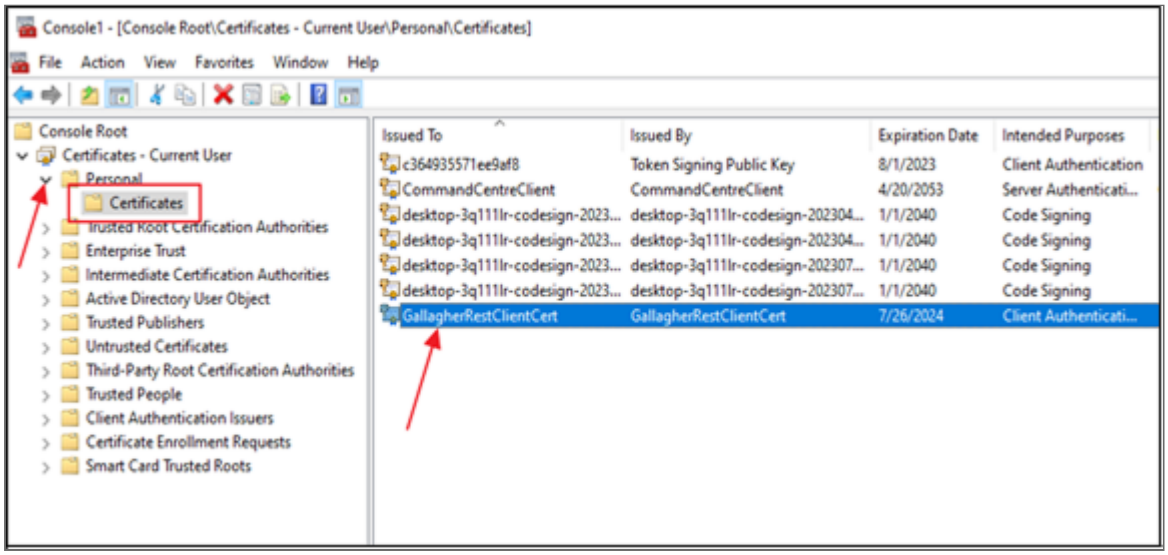


4. After clicking on the finish you will see the below screen now **click** on the **OK** button. The certificate will be added successfully.

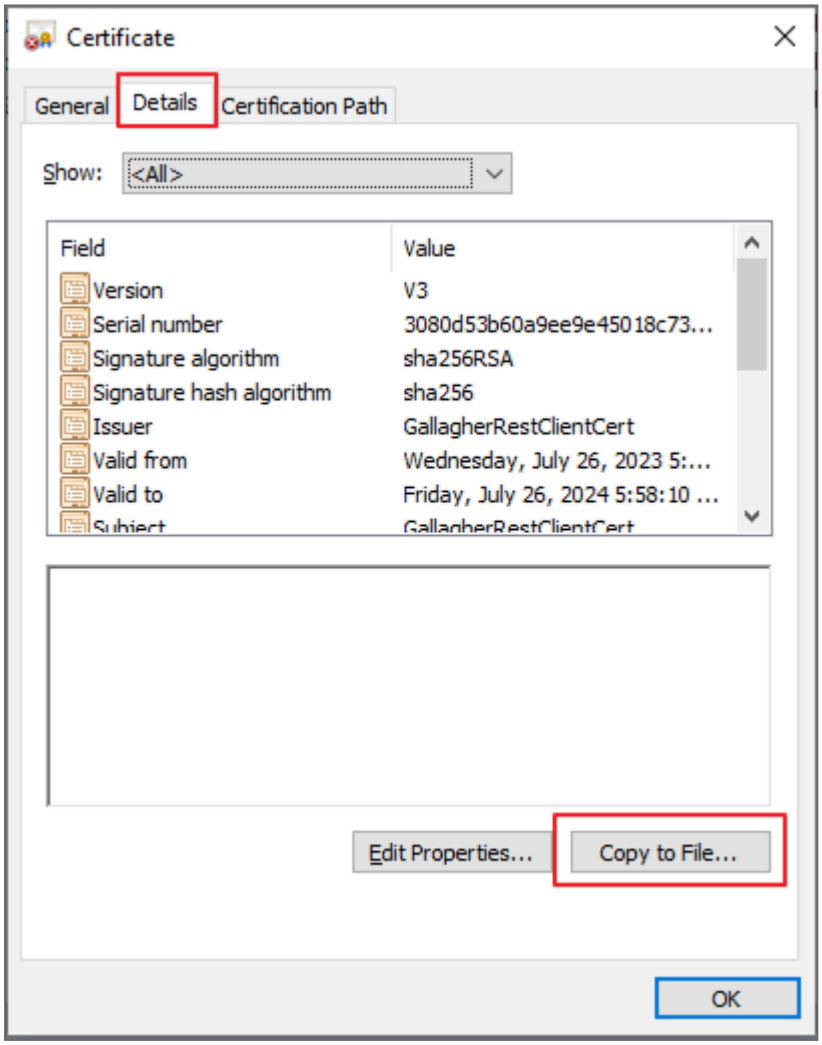


5. Now go to **Certificates - Current User** → **Personal** → **Certificates** and select **GallagherRestClientCert** certificate.





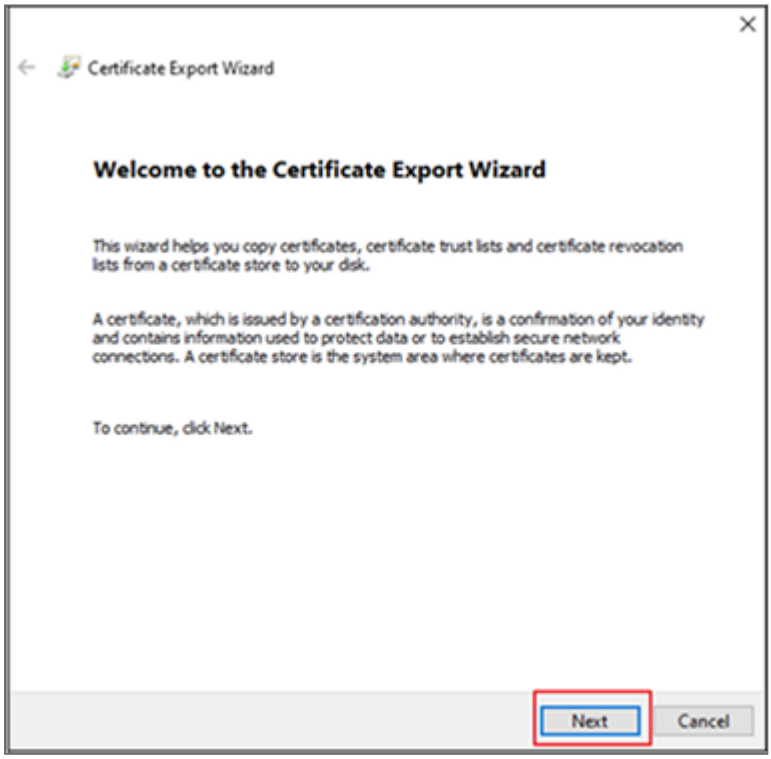
6. Go to **Details** and **click** on **Copy to File**.

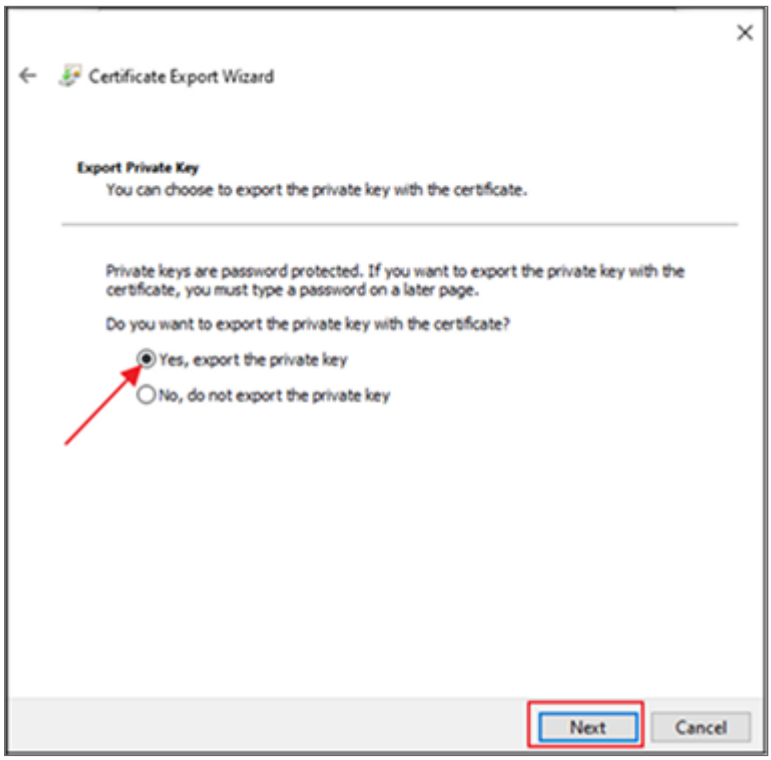


Now follow the below screenshots and **click** on **next** simultaneously.

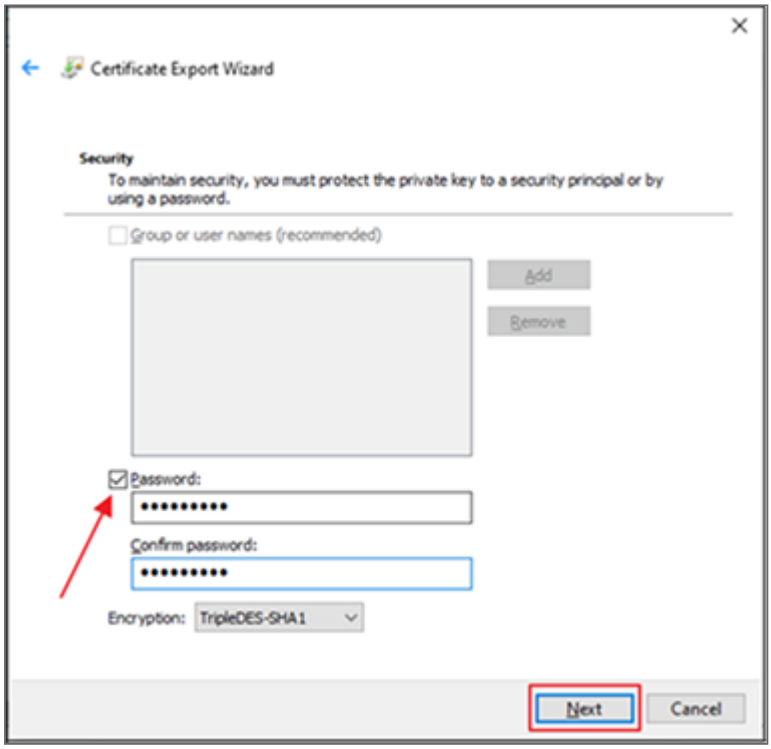
Info

Please validate that the Thumbprint is correct if you have more than one Certificate.

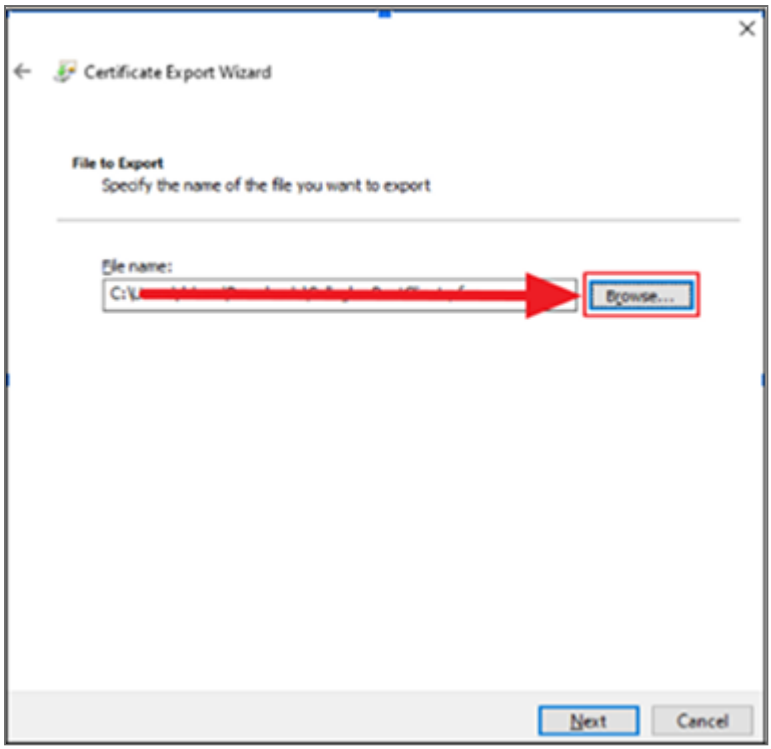


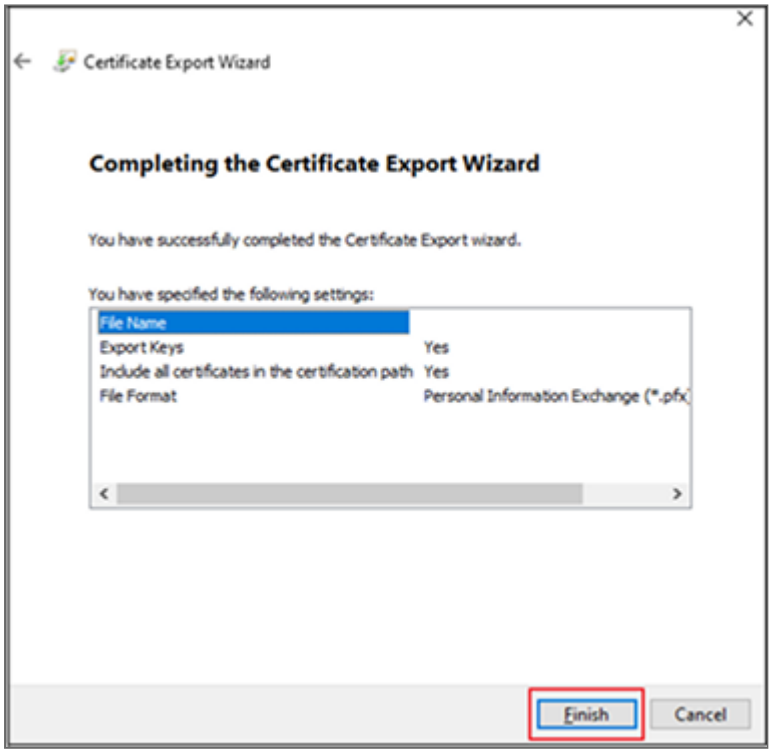


7. Now you will see the below screen check the password checkbox and **set** the password as the below password: **G@ll@gher**



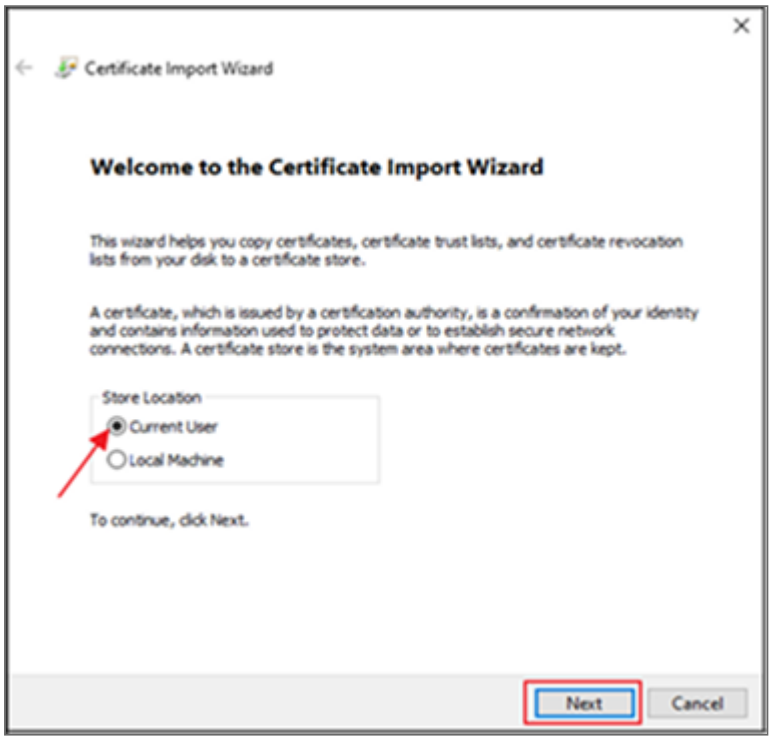
8. Now **browse** the path C:\Program Files\Suprema Integration with Gallagher\Prerequisites to export the file and **save** this file as **GallagherRestClient.pfx** then **click** on **Next**.



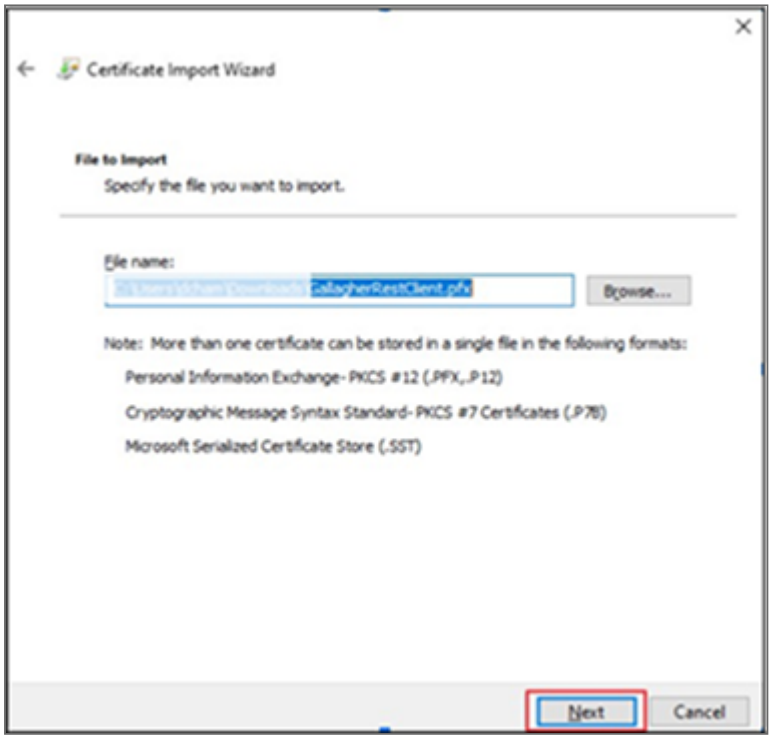


Click on **Finish** and your certificate will be exported successfully and **close the certificate** and MMC window.

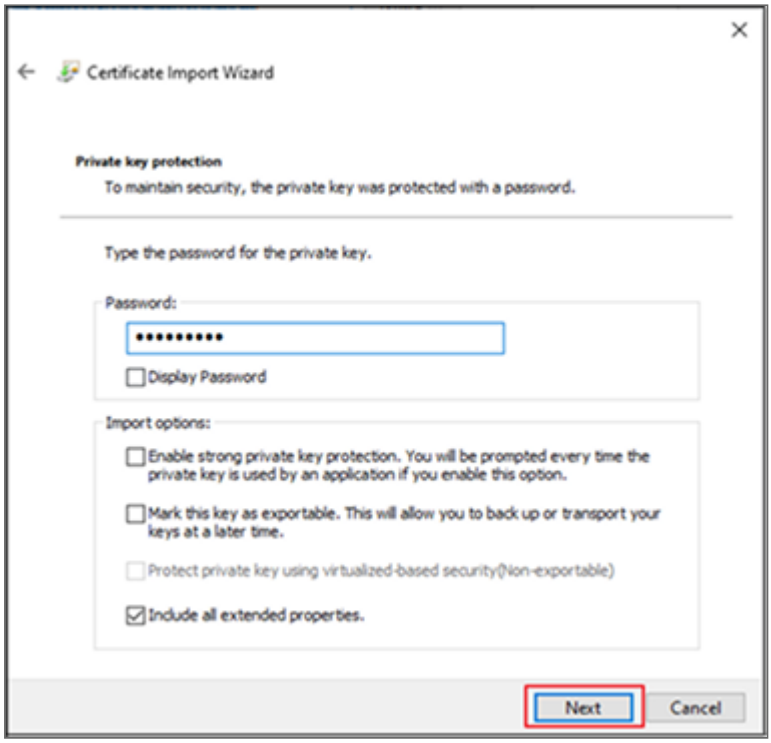
9. Now, go to the path `C:\Program Files\Suprema Integration with Gallagher\Prerequisites` where we exported the **GallagherRestClient.pfx** certificate file, and **double-click** on the **GallagherRestClient.pfx** file, **select** the **Current User** radio button as shown below image then **click** on the **Next**.



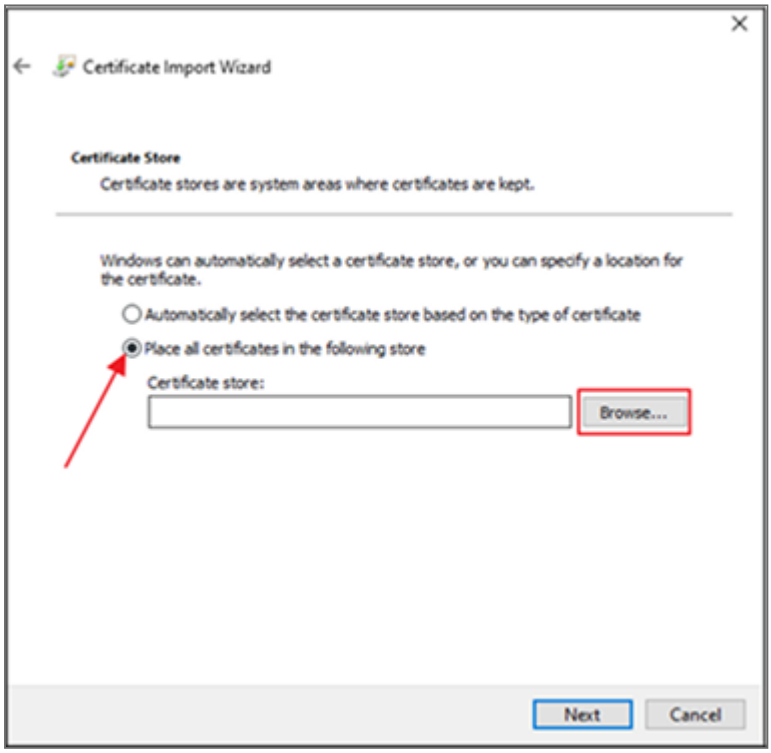
10. Now, **browse** the `C:\Program Files\Suprema Integration with Gallagher\Prerequisites` where we saved **GallagherRestClient.pfx** then **click** on the **Next**.

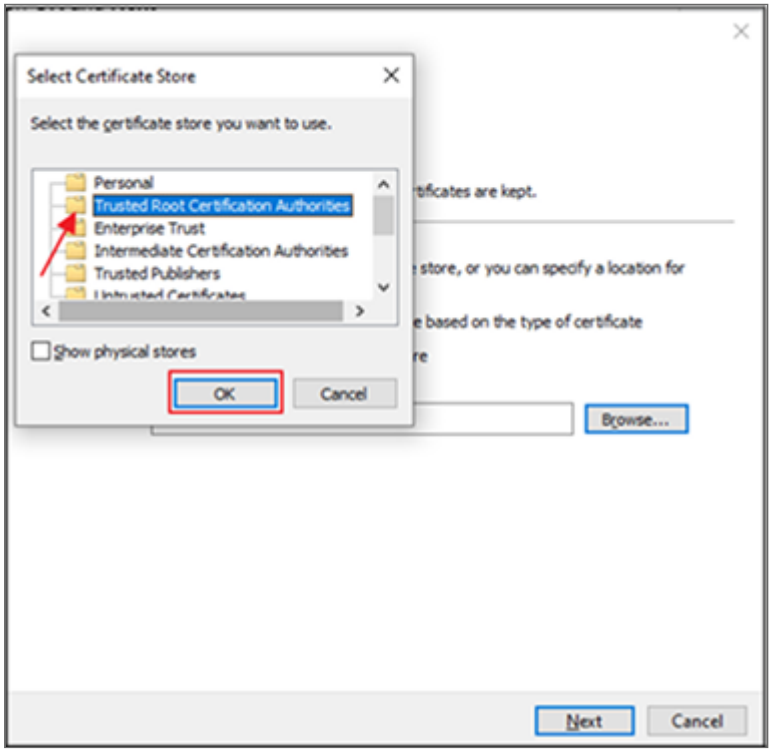


11. Now, **Enter** Password **G@ll@gher** and **check** the checkbox as shown below the image then **click** on the **Next**.

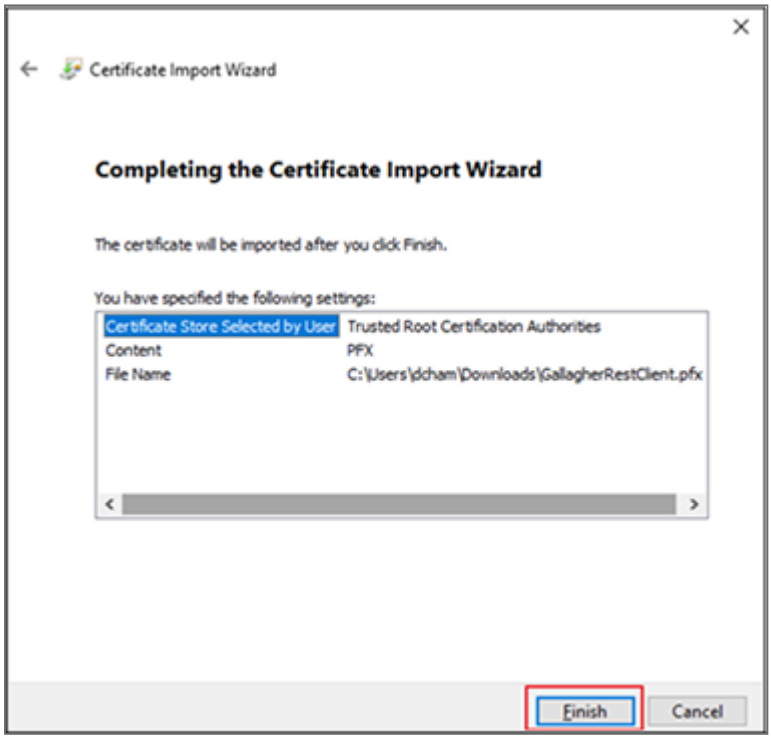


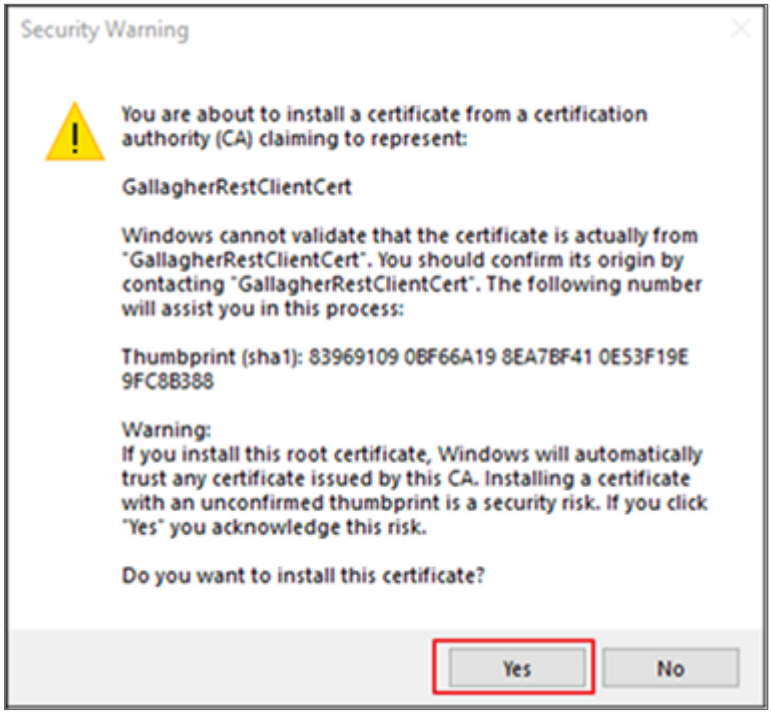
12. **Select** Place all certificates in the following store Radio button and **browse** the **Trusted Root Certification Authorities** folder then **click** on **OK** and **Next**.





13. **Click** on **Finish** you will see a security Warning, **click** on **Yes**.



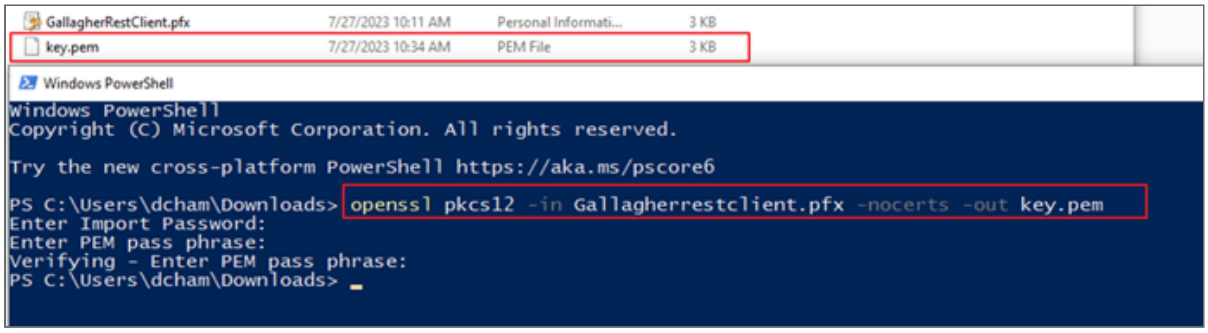


Now, **go to** the path `C:\Program Files\Suprema Integration with Gallagher\Prerequisites` we saved GallagherRestClient.pfx file, **open** Powershell here, and **Type PowerShell** in the Folder URL to open PowerShell.

14. **Type** the below command to Generate the **key.pem** file.

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

15. Next, it will ask for the password. So **enter** the password which you set earlier i.e, **G@ll@gher**.

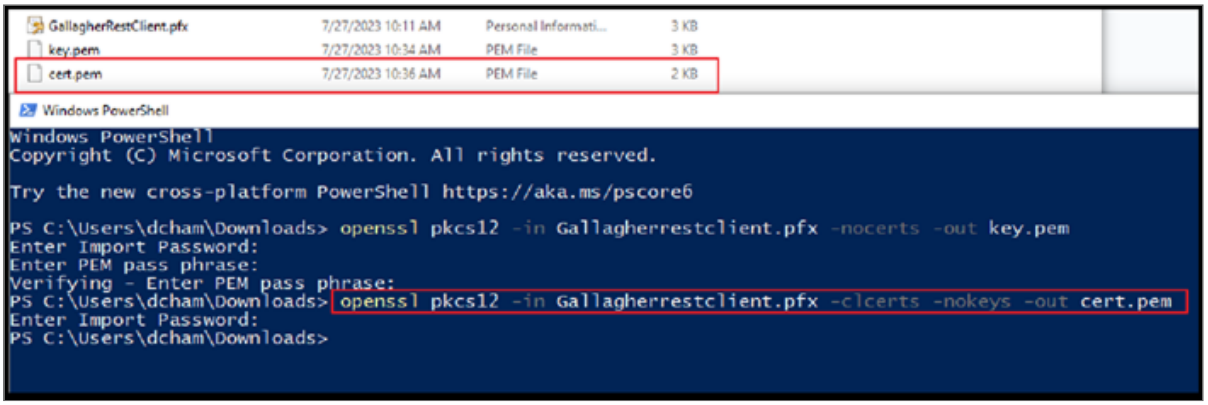


Your **key.pem** file will be generated successfully.

> **Info**
> You need to enter the password three times here.

1. Next, **type** the below command to Generate a **cert.pem** file:

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

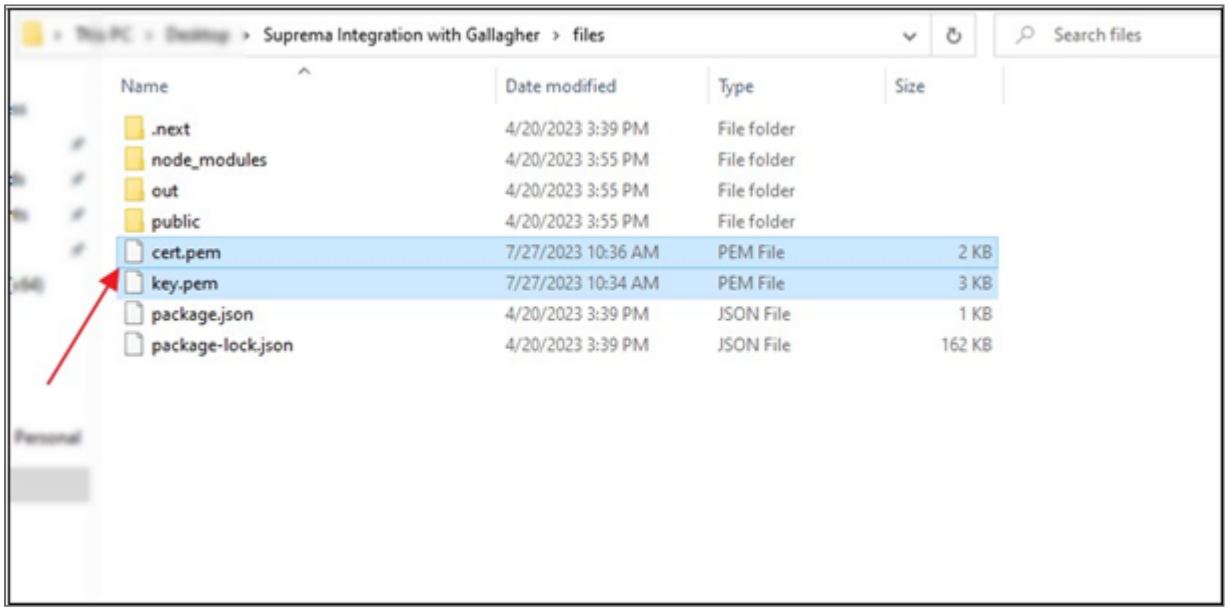
   

   Next, it will ask for a password. So **enter** the password that we set earlier **G@ll@gher**.

   Your **cert.pem** file will be generated successfully.

   > **Info**
   > You need to enter the password One time here.

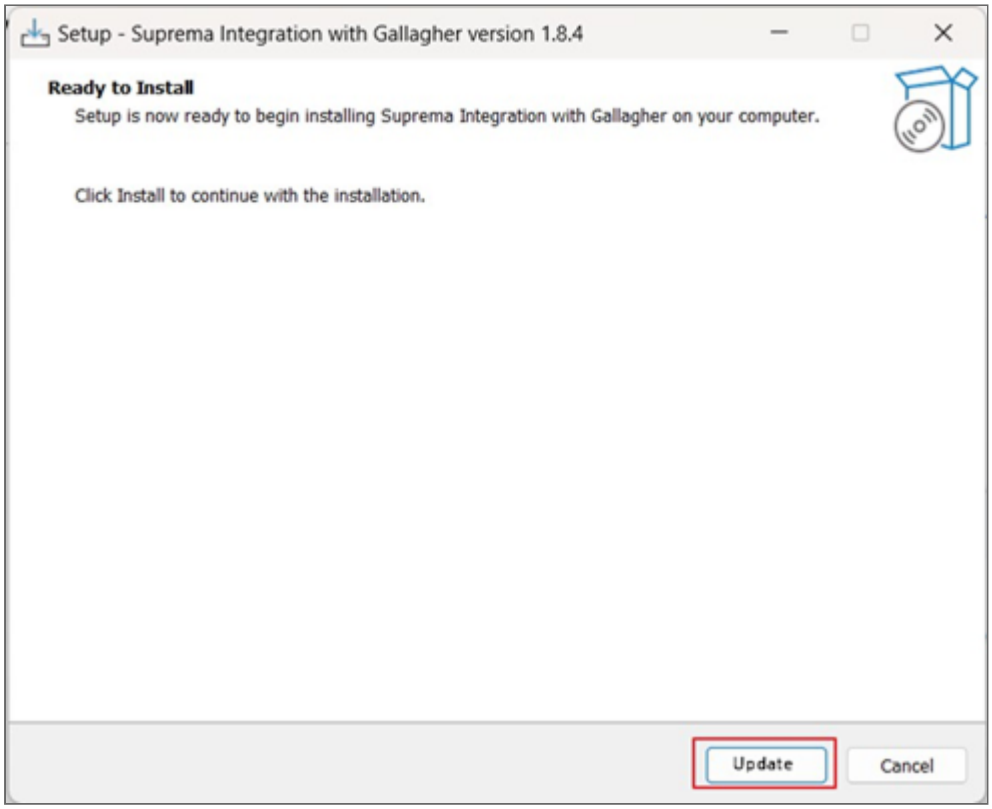
16. Next **copy** both file **key.pem and cert.pem** and paste that at below path `C:\Program Files\Suprema Integration with Gallagher\Suprema Integration with Gallagher v(lateast version)\files` .



Q. Upgrading the middleware from EXE application directly.

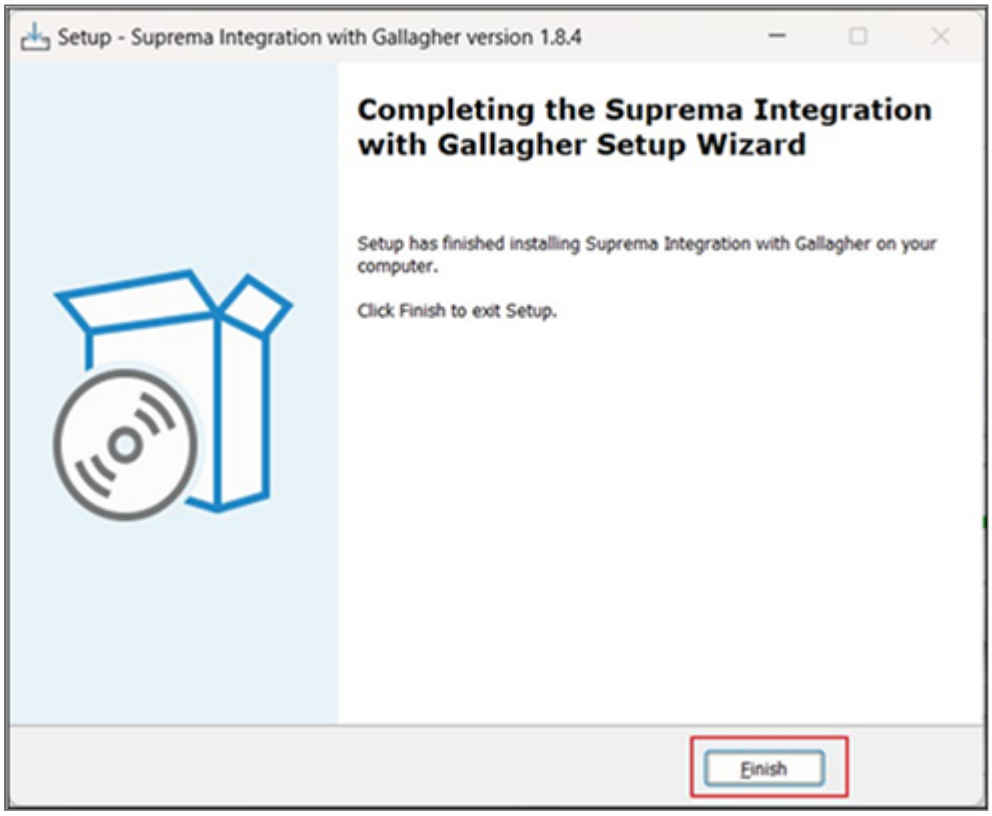
A.

1. If you are upgrading the version, **press** OK on pop-up.
2. Then **press** Update button.



3. It will start upgrading the middleware.
4. After Successfully installing the middleware you need **press** Finish button.

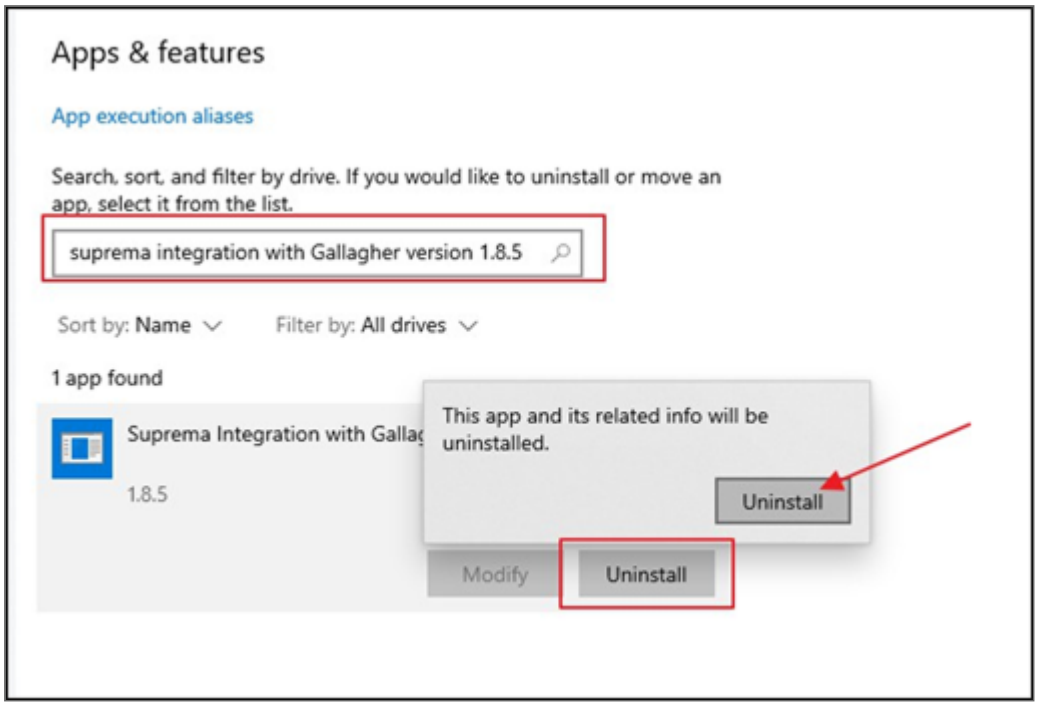
> **Info**
> For latest changes It is necessary to restart the system!



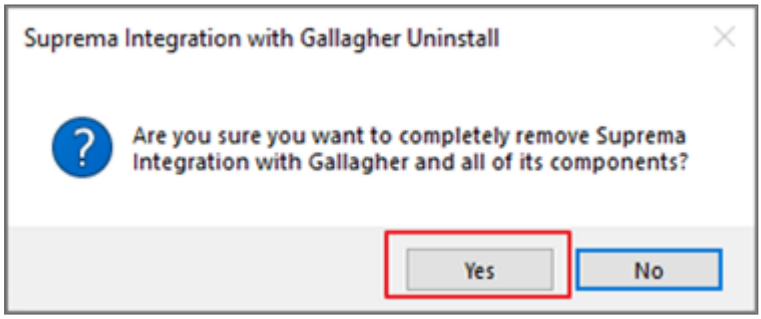
Q. Uninstall the middleware from EXE application directly.

A. 1. **Press** windows Start button, **Search, and open** Add or Remove programs.

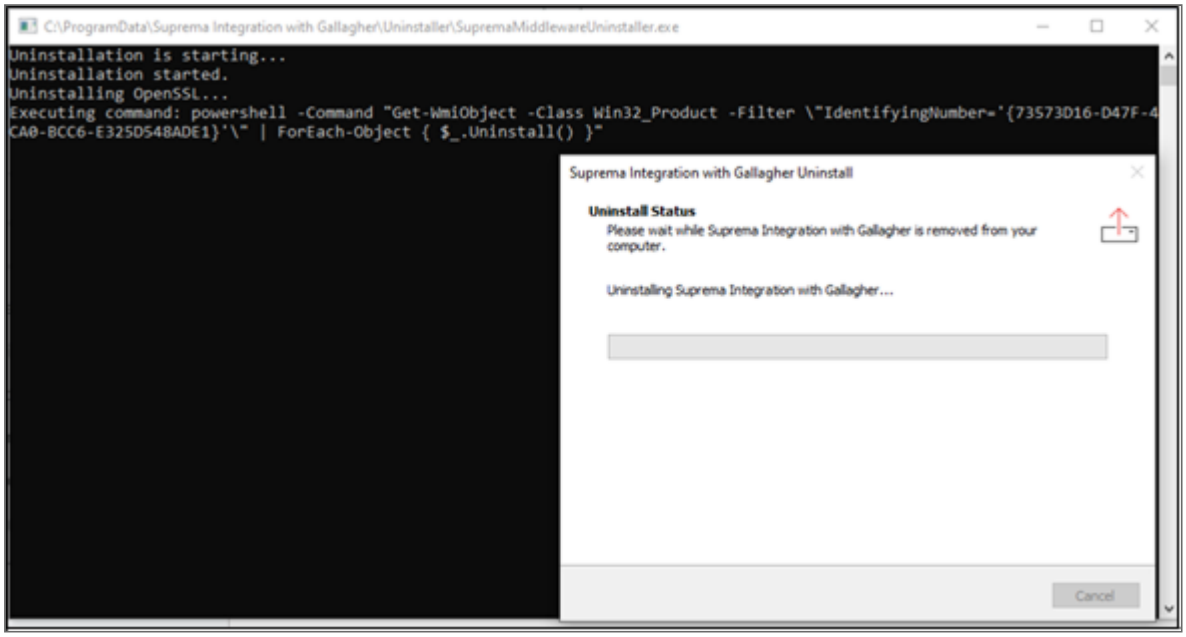
2. Inside the Apps & features search list, **search** for Suprema integration with the Gallagher version, select the version, and **click on** Uninstall it shows a small pop-up **press** Uninstall another time.



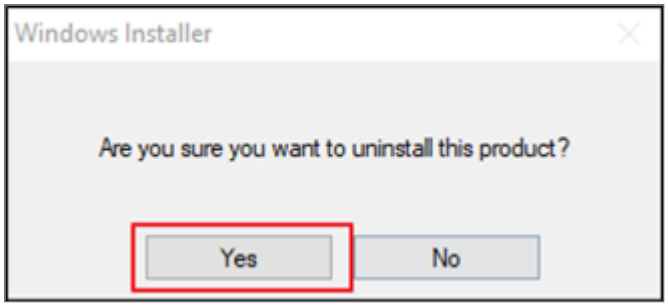
3. **Press** Yes on the remove all component of integration pop-up.



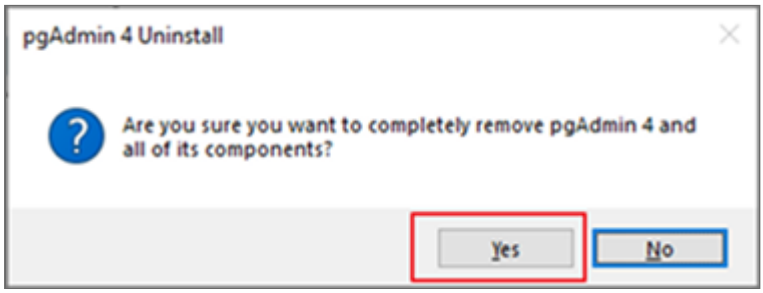
4. The uninstallation will start and you can see something like the screens below.



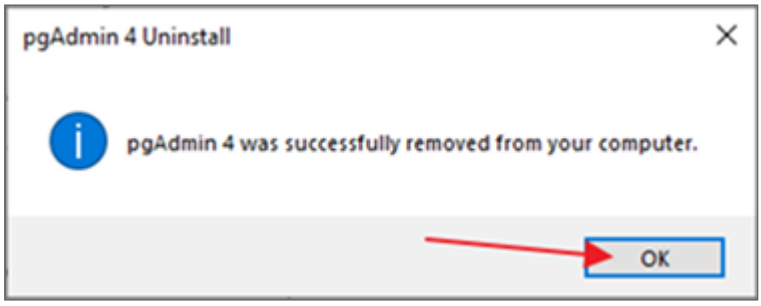
5. **Press** Yes on the below pop-up.



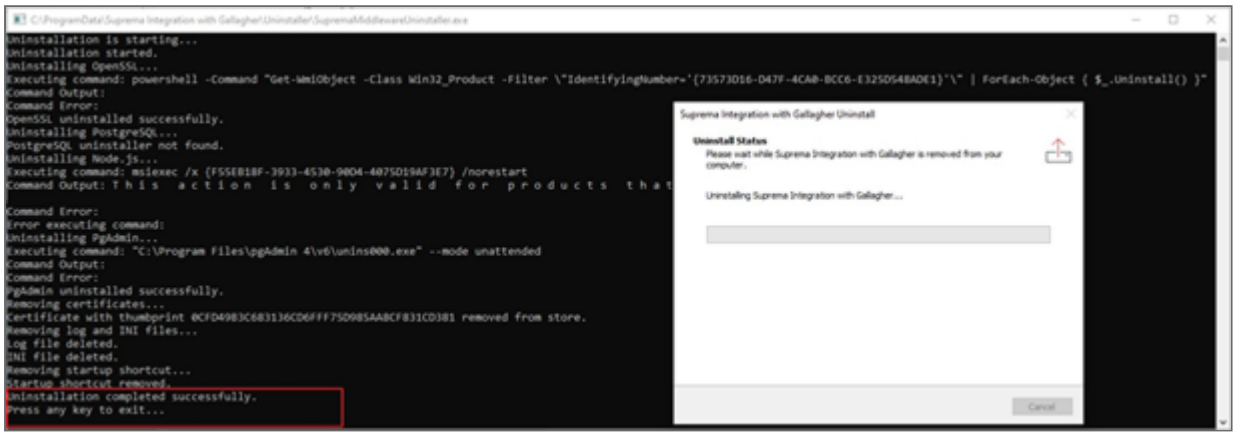
6. **Press** Yes for the below pop-up.



7. **Press** OK.

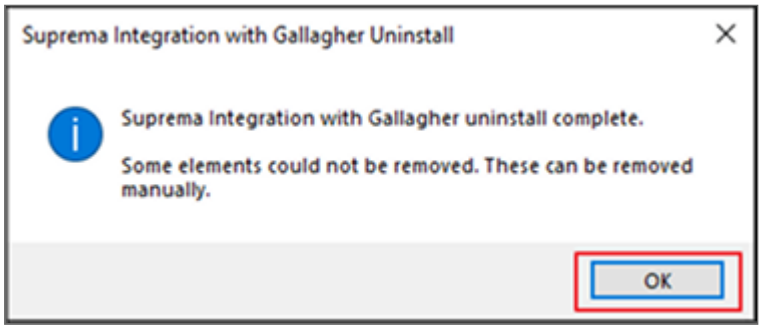


8. Now click inside the terminal and **press** enter to complete the uninstallation process.



9. **Press** OK on the pop-up below and you have successfully removed the middleware.

> **Info**
> You must need to restart the system to reflect the changes.

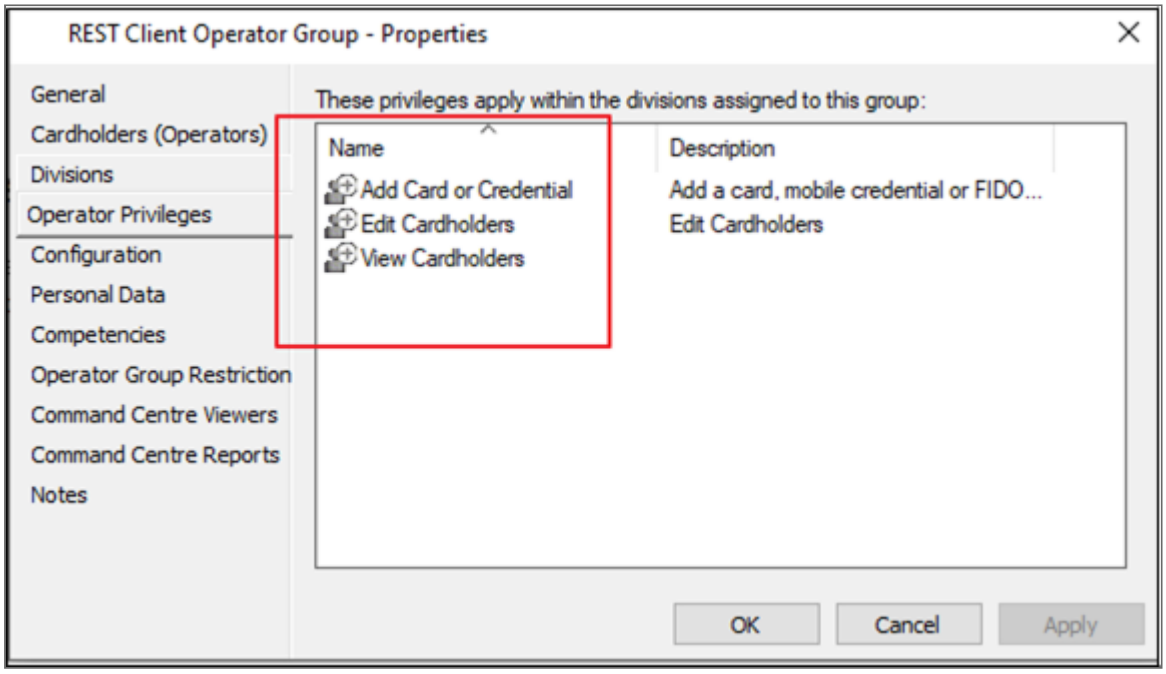


Middleware

Q. If the scanning or the syncing of the data in the middleware is extremely slow.

A.

- To solve this issue, please click here and refer to the blog.
  - You cannot see any card in the middleware if a cardholder card is automatically not created.
- You need to add 3 privileges to the Operator Group.



After adding these three privileges please restart your system.

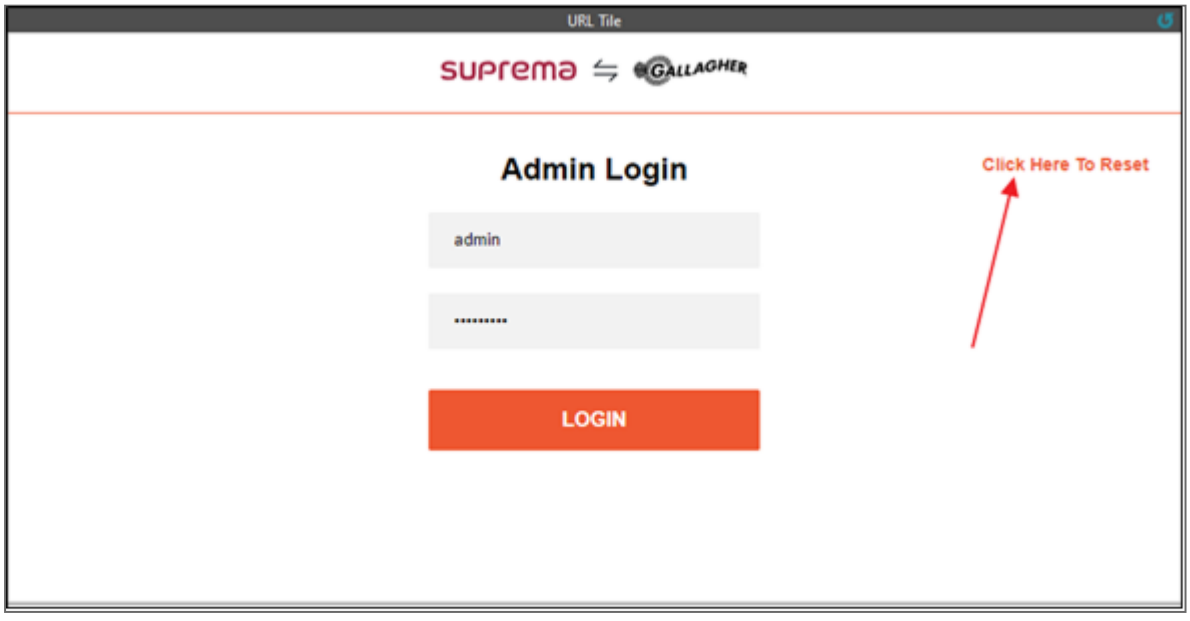
Q. There is an error on the log-in page stating that "LAN is disconnected or IP is changed for (IP Address)".

A.

- To solve this issue, please check the below troubleshooting scenarios:

  1. Make sure the LAN cable is connected.
  2. Check If the IP has not changed and if the IP address is the same for the BioStar 2 Server you have entered the wrong IP Address.

- If you receive the error **LAN is disconnected or IP is changed for (IP Address)** on the login screen, you must **press** the **click here to Reset button** in the middleware.



It asks for permission to reset the middleware, **press** the Yes **button**.

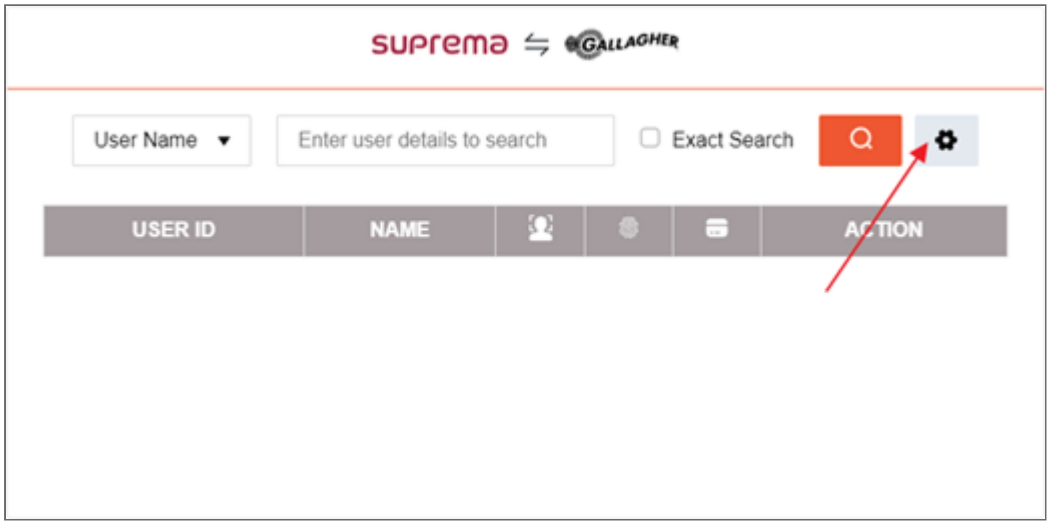


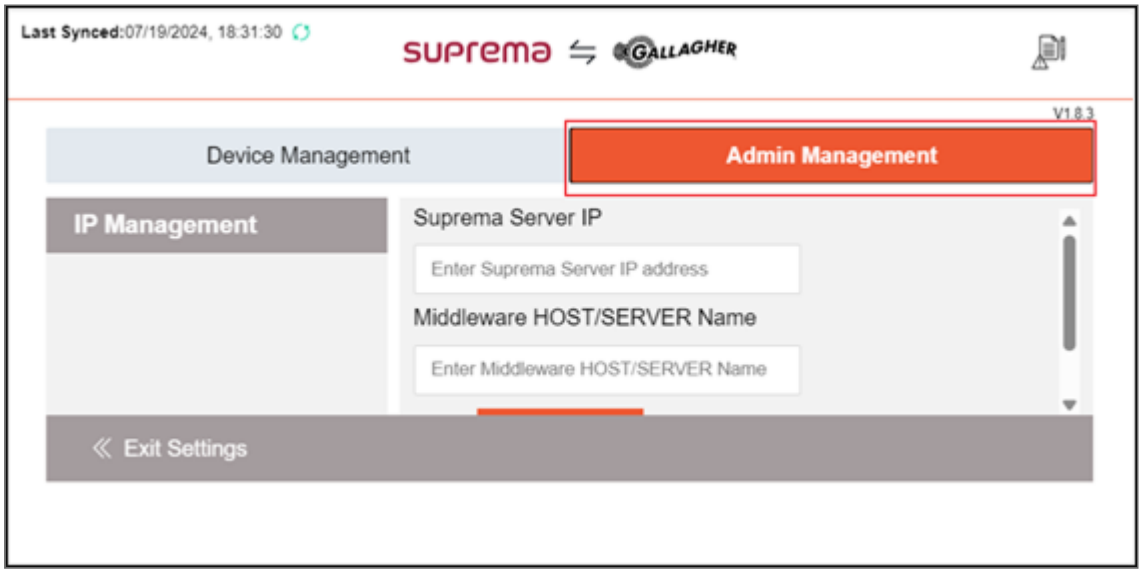
Once it is reset you can see the initial screen for the middleware and follow the further steps.

Q. If you get an error for "LAN is disconnected or IP is changed for (IP Address)" between running the middleware on any page.

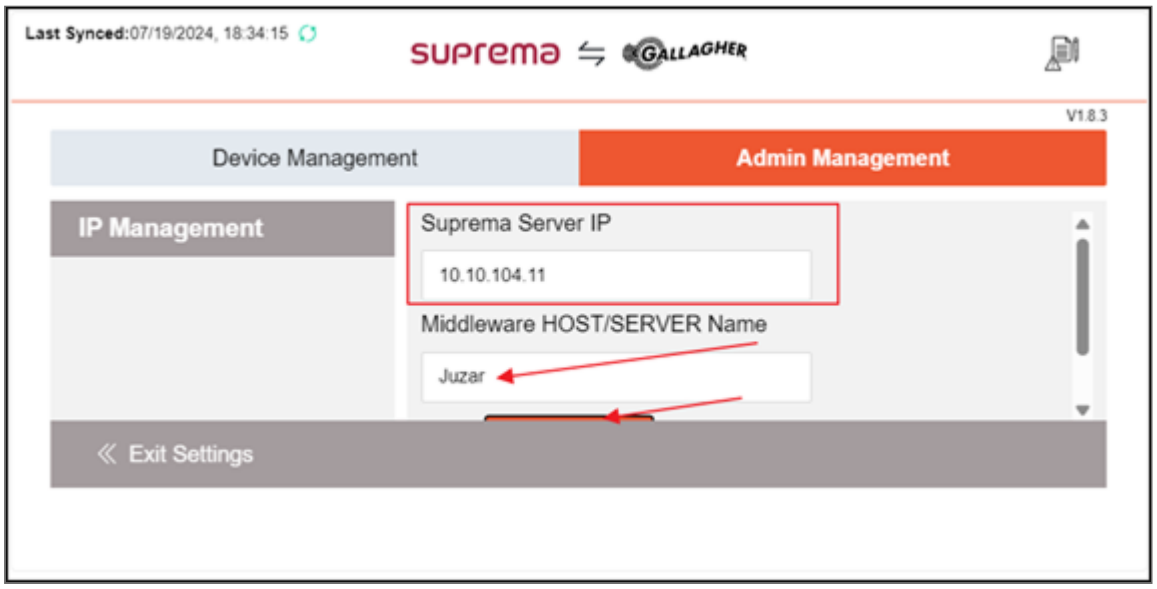
A.

- To solve this issue, please check the below troubleshooting scenarios:
  1. Make sure the LAN cable is connected.
  2. Check If the IP has not changed and if the IP address is changed for the BioStar 2 Server.
- In this case, just go to the Settings → Admin Management → IP management section inside the middleware.





Now inside the text box enter the IP address of the BioStar 2 server and the HOST/SERVER name of the middleware press the Submit button to start the BioStar 2 services for the middleware.



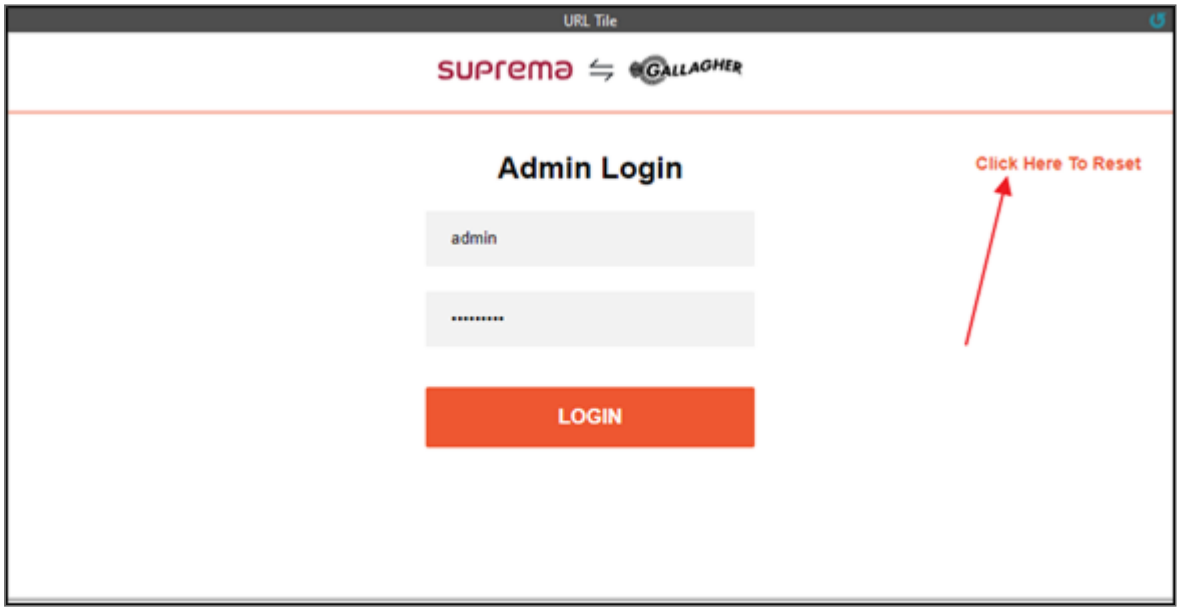
After **pressing** the submit **button** you get the success message for IP change and **press** the Exit setting **button** to leave the setting screen.

Q. How to Use middleware on multiple servers on older versions.

A. From version 1.7.0 we have added one separate screen to get the BioStar 2 server IP address. So this is the solution for use with the middleware version below 1.7.0.

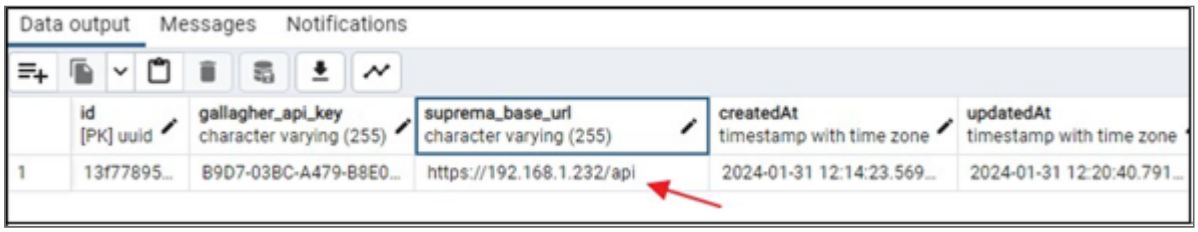
Below are the steps to change the IP address,

1. Go to Pgadmin → tables and right-click on the table and Tuncate → Truncate Restart Identity (for all three tables).
2. Go inside the Gallagher command center if you can't see the API key window and are just able to see the login screen, **click on** the reset middleware link and reset the middleware.



3. After entering the API key for the middleware do the login and open Pgadmin, right-click on the credential table, and view/edit data → All Rows.

4. It will load the data for the table. Now, change the IP address according to your BioStar server IP and press the F6 button to save the changes.



5. After this, you have to truncate the globaluserrecord table inside Pgadmin.
6. Restart the system to reflect the changes.

Q. Run the middleware on a specific port on two different servers with specific IP addresses/ Configure the inbound rules for the middleware.

A. Below are the instructions to run the middleware on a specific port on two different servers with specific IP addresses.

We found our middleware is using the 28523 port to call the backend of our application (middleware-backend) inside the backend we called the BioStar 2 server APIs so for that the only port used is 443 as it is the web server HTTPS default port.

So for this inside the server2 which is the BioStar 2 server we have set the Protocol type as TCP and provide 443,8081 ports for the local port. Leave the remote port option as All ports.

Server 1 has Gallagher and Middleware within,

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

Server 2 has BioStar 2 within,

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

Here are the steps to create Inbound rules:

> **Info**
> The below steps need to run on the BioStar 2 server.

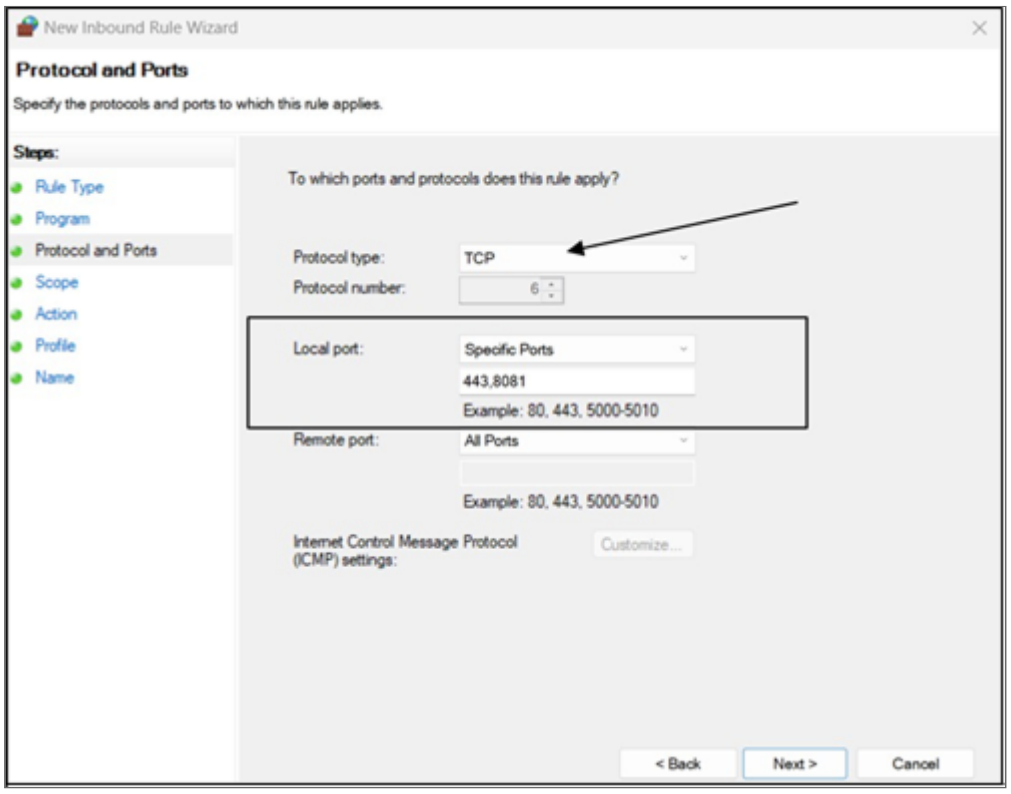
1. Open Windows Defender Firewall Settings:
   - Press the `Win + R` to open the Run dialog.
   - Type `control firewall.cpl` and press Enter. This will open the Windows Defender Firewall settings.
2. Access Advanced Settings:
   - In the Windows Defender Firewall window, you'll see options on the left-hand side. Click on **Advanced settings**. This opens the Windows Defender Firewall with the Advanced Security console.
3. Create New Inbound Rule:
   - In the Windows Defender Firewall with Advanced Security console, you'll see options on the left-hand side including **Inbound Rules** and **Outbound Rules**.

- Click on **Inbound Rules**.
- In the right-hand pane, click on **New Rule...**. This opens the New Inbound Rule Wizard.

4. Select Rule Type:
   - In the New Inbound Rule Wizard, select **Custom** and click **Next**.
5. Configure Program:
   - If you want to apply this rule to a specific program, you can specify it here. Since we're dealing with ICMP traffic, leave this as **All programs** and click **Next**.
6. Configure Protocol and Ports:

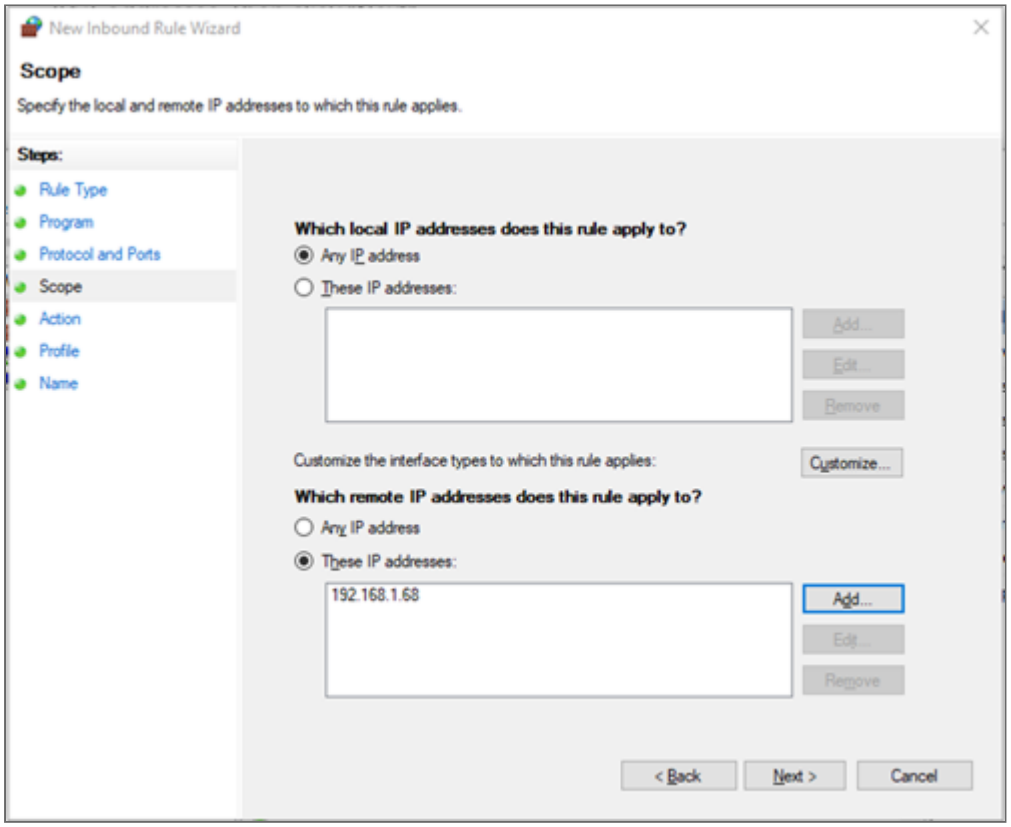
   - In the Protocol and Ports window, select **TCP** as we are going to work with specific ports. Now inside the local port, we have to select specific Ports and enter 443, and 8081 ports. Leave the Remote Port as All Ports. Then click **Next**.

> **Info**
>
> Here we have assigned the 8081 port as BioStar 2 using it for USB devices.



7. Configure Scope:

   - In the Scope window, you can specify which IP addresses are allowed to send ICMP traffic to the server. So local IP addresses leave it as it is and for remote IP addresses fill in the IP address of the Gallagher&Middleware server, now choose These IP addresses: Click on the Add button then in the IP address wizard enter the IP Address of Gallagher&Middleware server, and press OK. Please refer below image for reference.



8. Configure Action:
   - In the Action window, select **Allow the connection** and click **Next**.
9. Configure Profile:
   - In the Profile window, select the profiles for which this rule will apply. Typically, you would want to enable this for all profiles (Domain, Private, Public). Then click **Next**.
10. Name and Description:
    - Give your rule a name and description. For example, you can name it **Allow ICMP Echo Request for middleware**. Then click **Finish**.
11. Enable the Rule:
    - After creating the rule, you should see it listed in the Inbound Rules section of the Windows Defender Firewall with Advanced Security console.
    - Right-click on the rule you just created and select **Enable Rule** if it is not enabled automatically. This ensures that the rule is active and will allow ICMP traffic.

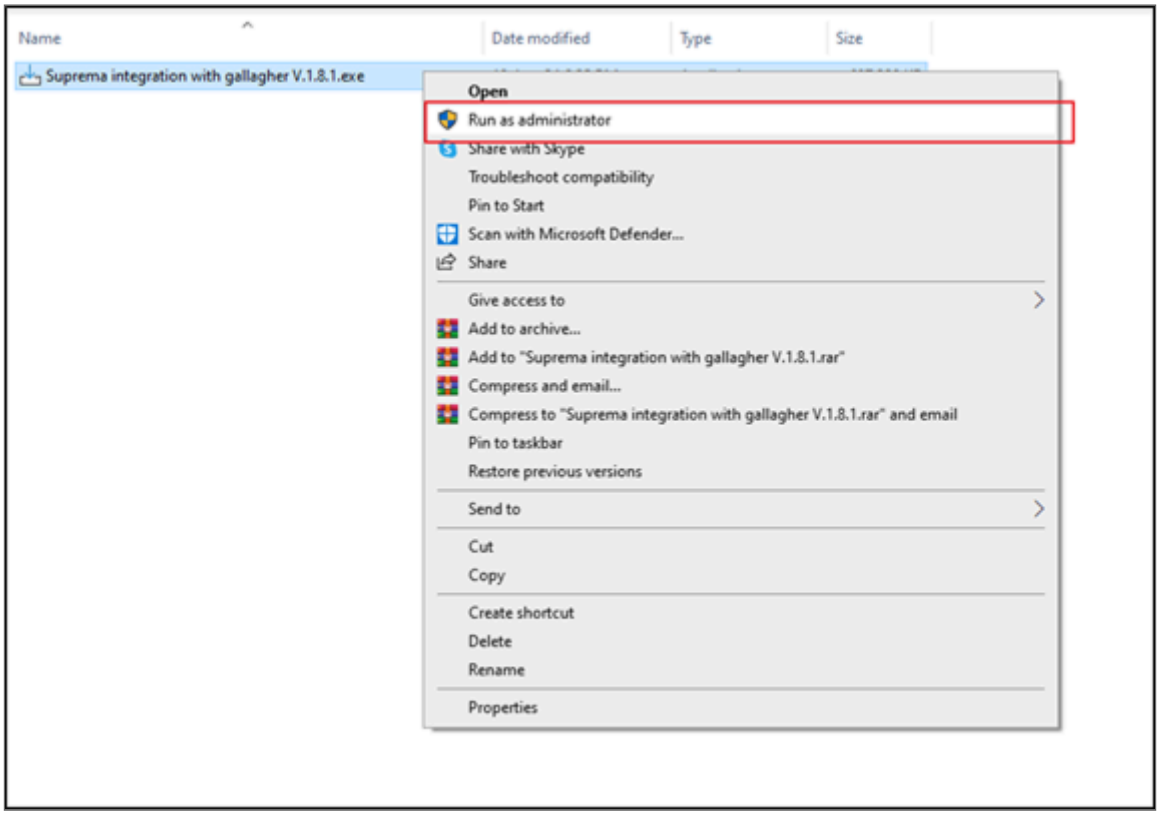
Q. If the BioStar server IP changes and Middleware gets slow.

A. If you facing the error where your IP is changed, check the following link: https://support.supremainc.com/en/support/solutions/articles/24000041659--biostar-2-troubleshooting-when-the-server-ip-changed.

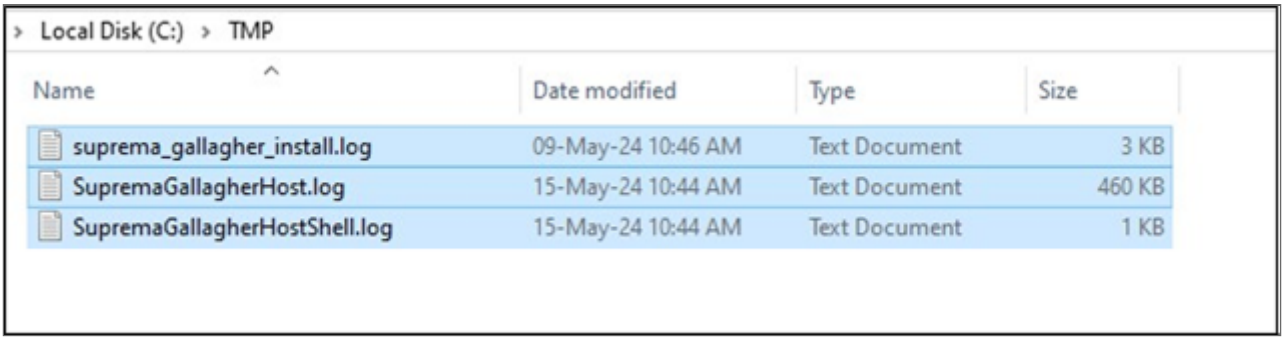
Q. If a thumbprint is not generated while running the EXE file.

A. If you have installed middleware and a thumbprint is not generated then try again running our EXE file with administrator rights, to do this follow the below instructions.

Right-click on our Suprema integration with the gallagher.exe file and **select** Run as administrator option as shown in the below screenshot. Now it asks for permission **click** Yes to run our exe file.



Still, the thumbprint file is not generated, please go to the `C:\TMP` and share all the log Files with the development team.



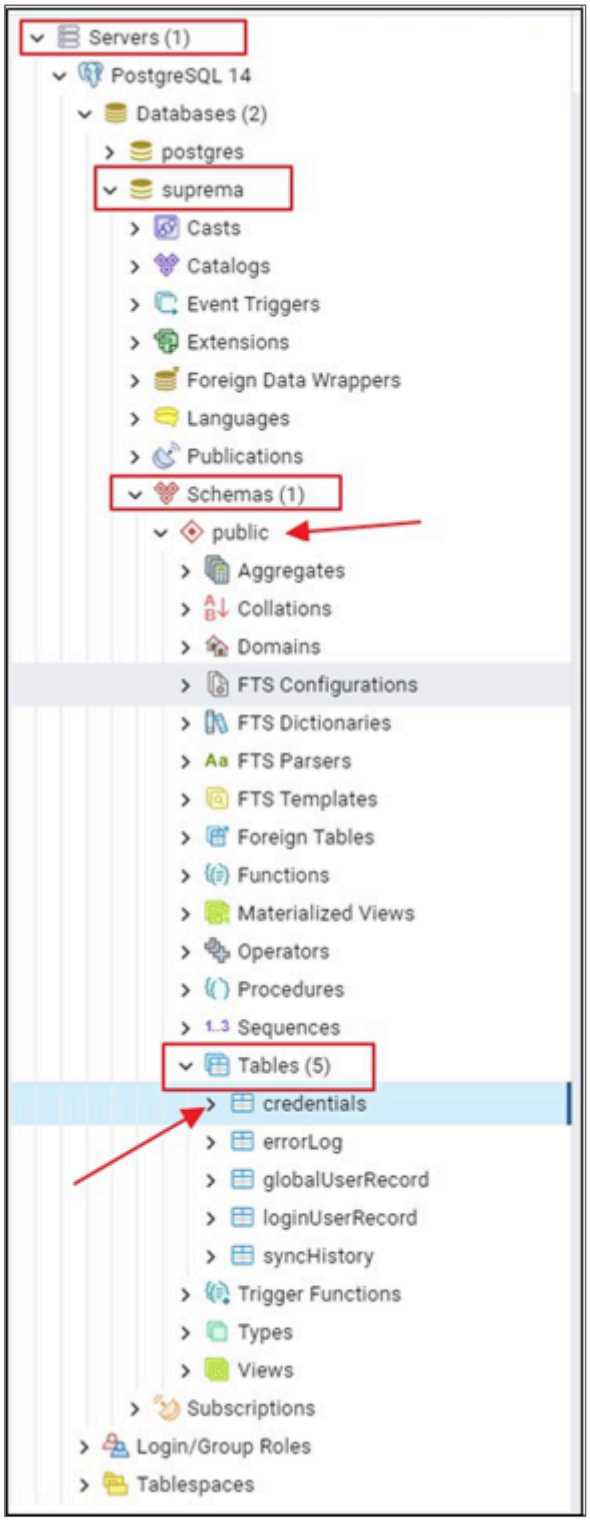
Till then please refer to the article which helps to manually generate the thumbprint. Refer: How to generate the thumbprint manually.

Q. Create Migration Manually.

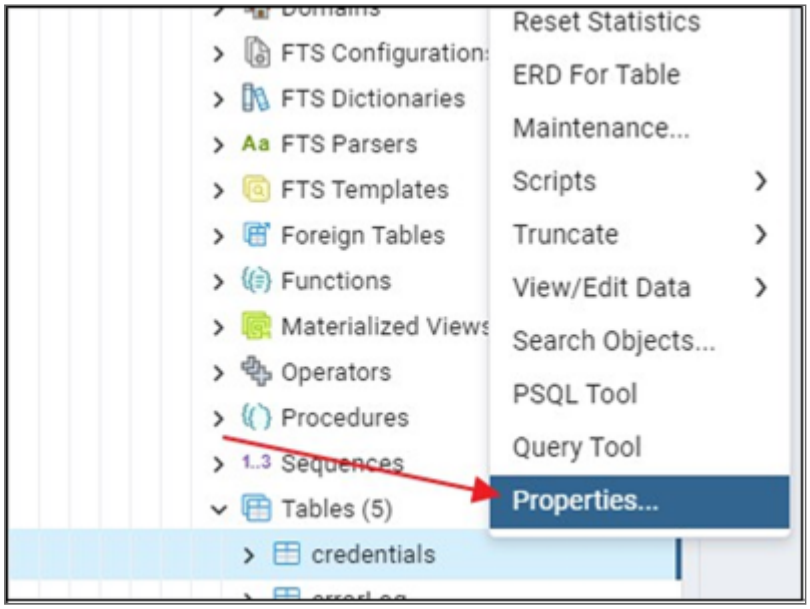
A. We are doing the migrations because from the middleware V1.8.3 is supporting the Hostname so we can use our middleware using the Gallagher workstation client.

To create the migration manually Please follow the steps below:

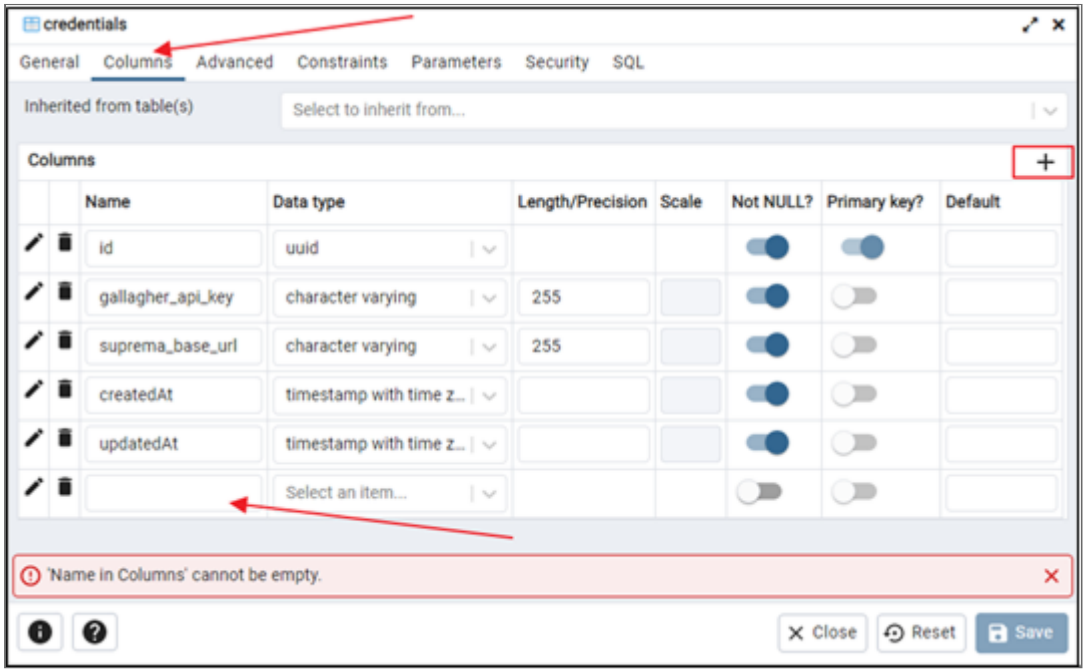
1. Go to the Pgadmin. It asks for the password, Write The password **G@ll@gher** as it default password we set during the installation.
2. Now **click on** the Servers, If it asks for the password use the same **G@ll@gher** as Password, now **click on** the Databases and **Expand** the Suprema → Schemas → public → Tables. Now **select** the credentials table.



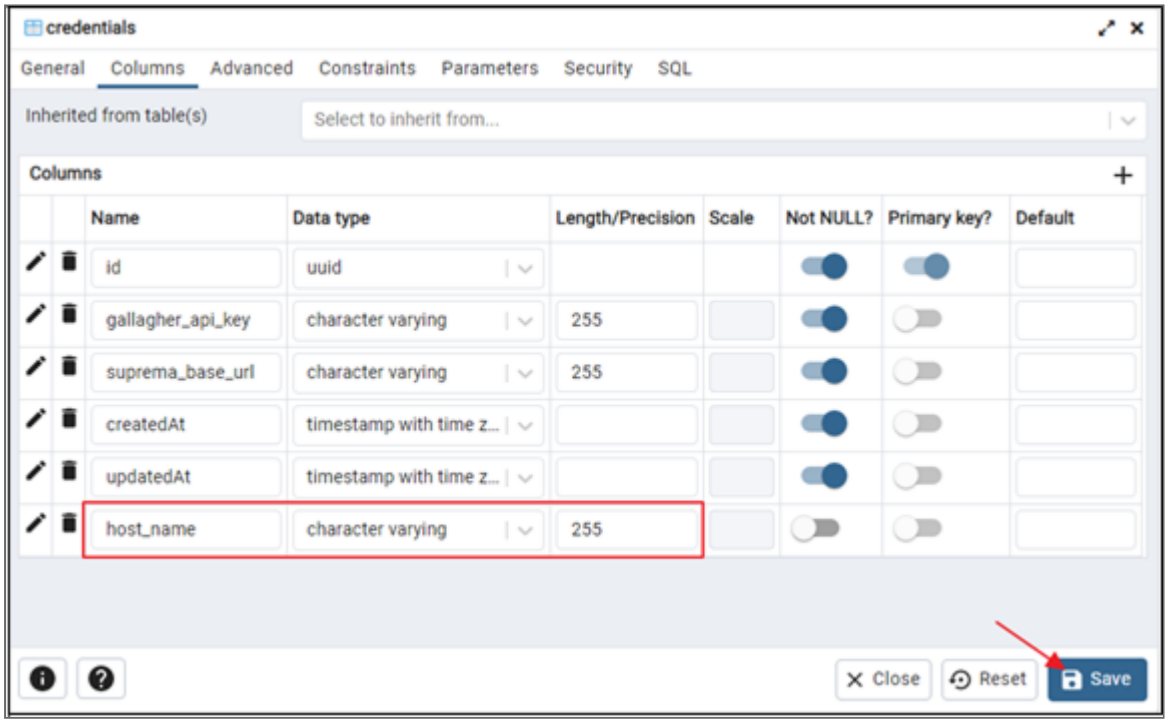
3. Now **Right click on** the credentials table, and **select** the Properties option from the list.



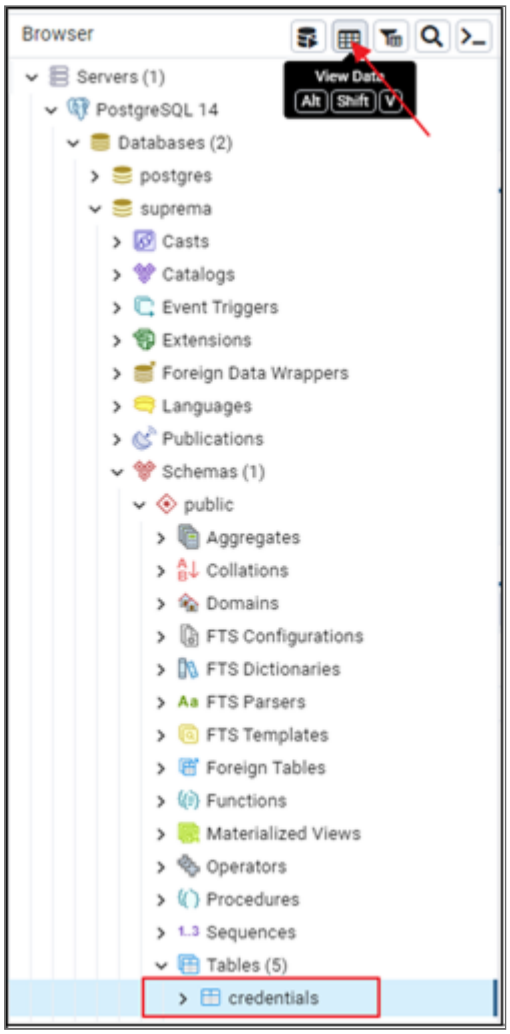
4. Now inside the window **select** the Columns option, then **click on** the + icon, it will generate the new column option for you as shown in the below image!



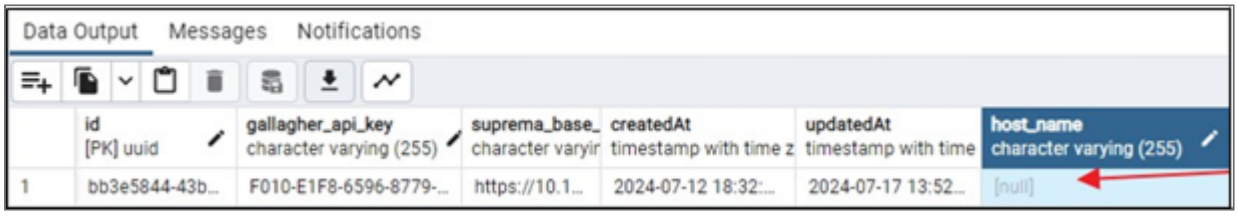
5. Now inside the Columns option, **set** the name as host_name, and **set** the datatype as the character varying, **set** the Length/Precision as 255 and **hit** the Save button.



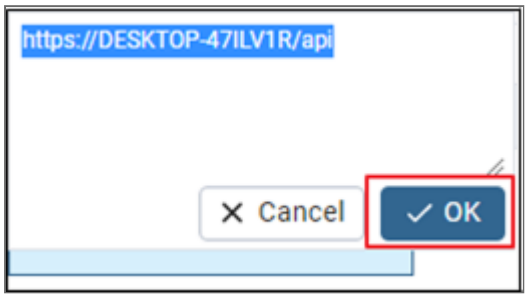
6. Now **select** the credentials table, and **click on** the View Data button.



7. Now inside the column host_name, **double-click** on the box, and the pop-up will open.



8. Inside the pop-up write `https://[YOUR-HOST/SYSTEM-NAME]/api` and **press** OK.



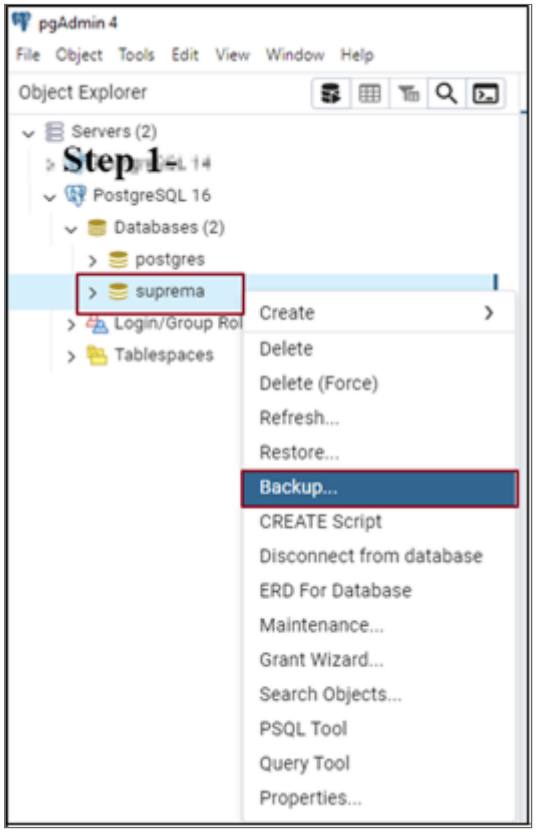
9. Now **press** `F6` to save the changes.

Q. Steps to Backup PostgreSQL 14 Database, Upgrade to Version 16, and Restore Database.

A. Backup Database in PostgreSQL 14

1. Open pgAdmin 4:

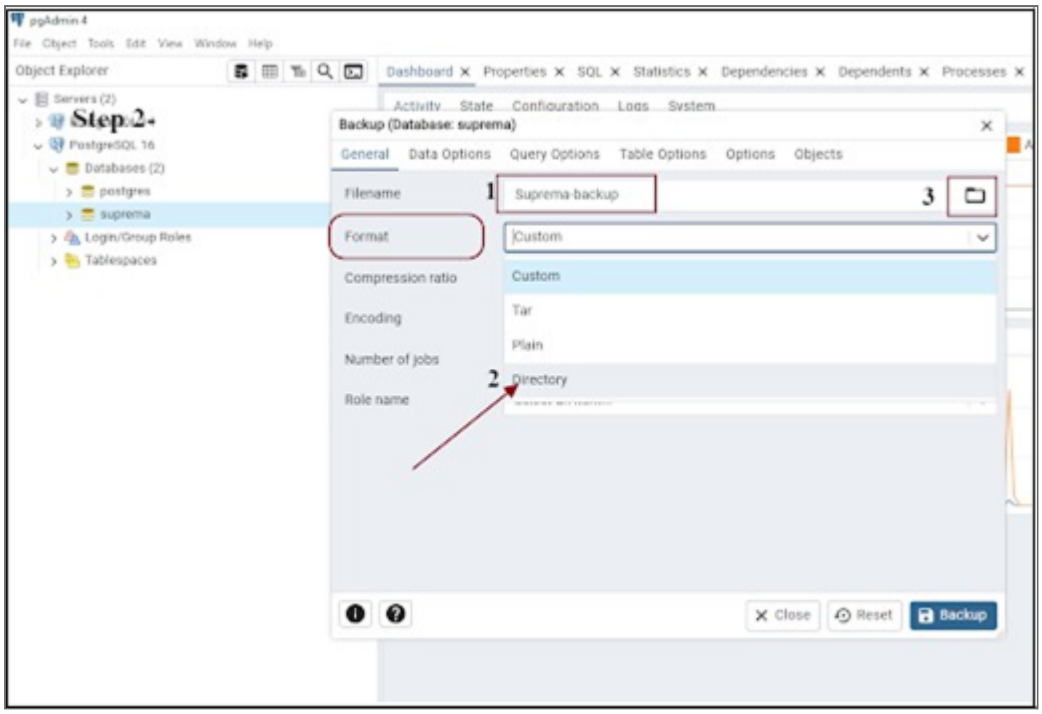
   - Right-click on the **Suprema** database under the **Databases** section and select **Backup**.



2. Set Backup File Name and Format:

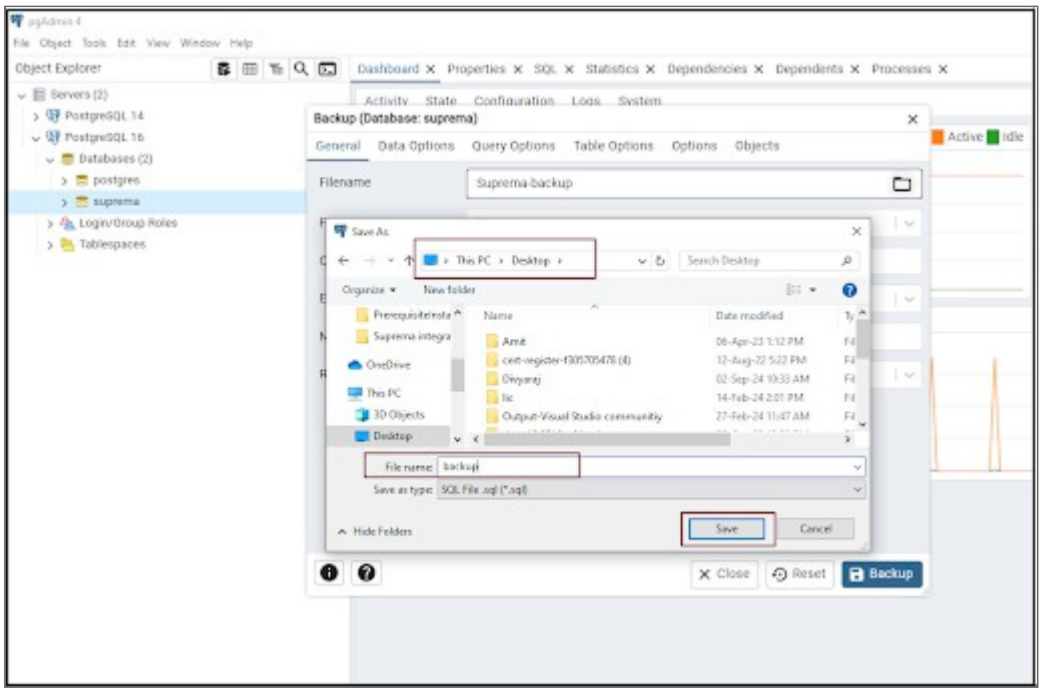
   - In the **File name** field, enter **Suprema-backup** as the name, and choose **Directory** as the format.

- **Click** the file icon to select a save location.



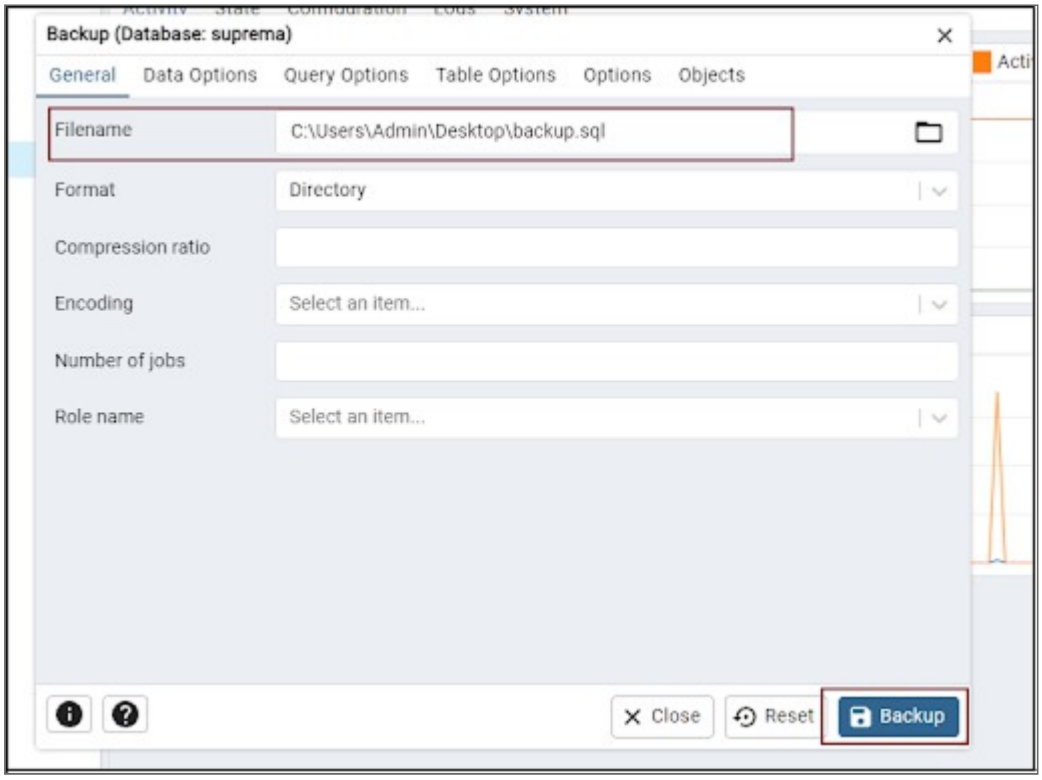
3. Choose Save Location:

- Select the directory where you'd like to save the backup (e.g., Desktop). Enter the file name and press **Save**.



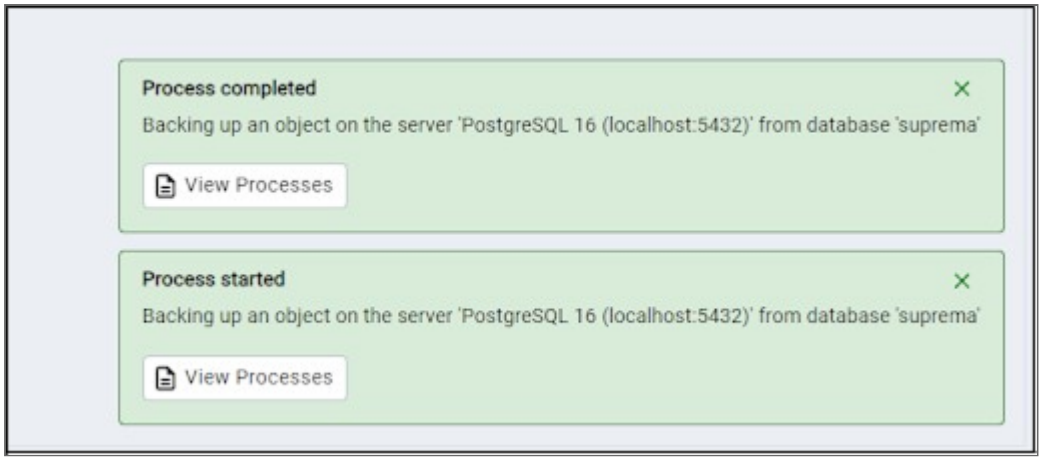
4. Start Backup:

- You'll see the file name updated with the location you selected. Press the **Backup** button.



5. Confirm Backup Completion:

   - A notification will appear once the backup is completed. Now, your database is safely backed up.



Upgrade PostgreSQL to Version 16

1. Stop Middleware and PostgreSQL Services:
   - Stop running middleware and terminate PostgreSQL services by stopping processes on ports 28523 and 5432.
2. Update Password (if required):
   - Set the password to **G@ll@gher** to ensure compatibility during the upgrade.
3. Install PostgreSQL 16:
   - Download and install PostgreSQL 16 from the official PostgreSQL website, following the installation steps for your operating system, or refer to the link to directly get V16.4.1: https://drive.google.com/file/d/17ehlTpedaGeWezOHZiMd6-ircQhTqBAJ/view?usp=drive_link.
4. Migrate Data (Optional):
   - Please refer to the Restore Database in Postgresql 16.
5. Uninstall PostgreSQL 14 (Optional):
   - After confirming the upgrade, you may uninstall PostgreSQL 14 if it's no longer needed. Refer: Uninstall the postgresql14 after upgrading to version 16.

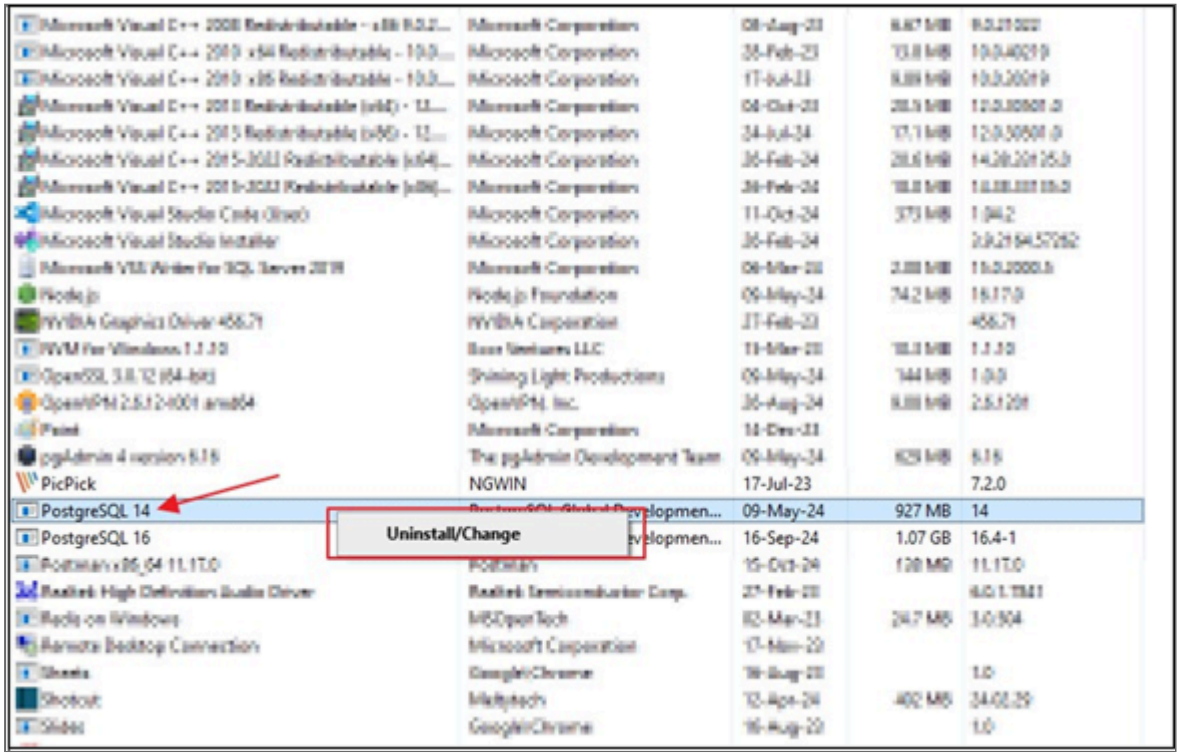
Restore Database in PostgreSQL 16

1. Open pgAdmin 4 (connected to PostgreSQL 16).
2. Create a New Database:
   - In pgAdmin, right-click on **Databases** and select **Create → Database**.
   - Name the database **Suprema** and save.
3. Restore the Backup:
   - Right-click on the newly created **Suprema** database, and select **Restore**.
4. Select Backup File:
   - In the **Filename** field, select the directory backup file (Suprema-backup) you created earlier.
5. Initiate Restore:
   - Click **Restore**. Wait for the process to complete.
6. Verify Restore Completion:
   - Once the restore is finished, you should see a success message. You can now access and verify your data in PostgreSQL 16.

Q. Uninstall Postgresql 14 after upgrading the Postgresql to version 16.

A. To uninstall Postgresql 14 follow the below steps,

1. Go to **Control Panel → Programs → Programs and Features**.
2. Find **PostgreSQL 14** in the list of installed programs.
3. Right-click on **PostgreSQL 14** and select **Uninstall**. Follow the prompts to complete the uninstallation.

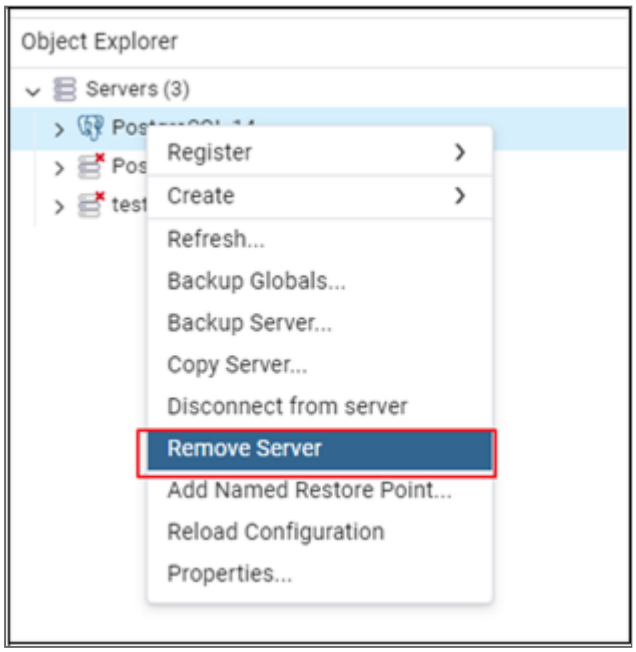


4. You might want to check the installation directory (usually in `C:\Program Files\PostgreSQL\14`) and delete any remaining files or folders.

> **Info**
> If PostgreSQL 14 still shows up in pgAdmin even after uninstalling it, it's likely because pgAdmin is still retaining the server configuration for it.

You can manually remove it from pgAdmin by following these steps:

1. **Right-click** on **PostgreSQL 14** in the Object Explorer panel in pgAdmin.
2. **Select** Delete/Remove Server from the context menu.



3. **Confirm** the deletion prompted.



This will remove the PostgreSQL 14 server configuration from pgAdmin without affecting your PostgreSQL 16 installation.

Suprema Inc.

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

Tel: +82 31 783 4502 | Fax: +82 31 783 4503 | Inquiry: sales_sys@supremainc.com

For more information about Suprema's global branch offices,
visit the webpage below by scanning the QR code.
https://supremainc.com/en/about/global-office.asp

© 2026 Suprema Inc. Suprema and identifying product names and numbers herein are registered trade marks of Suprema, Inc.
All non-Suprema brands and product names are trademarks or registered trademarks of their respective companies.
Product appearance, build status and/or specifications are subject to change without notice.