Suprema Integration with Gallagher Command Centre

GUÍA DEL ADMINISTRADOR DE

Versión 2.0

Español
ES 102.00.SIWG

suprema
SECURITY & BIOMETRICS

CONTENIDO

Propósito 4

Introducción 5

Características 5

Diagrama del sistema 6

Instalación 7

Requisitos previos 7

Diagrama de flujo de la configuración 8

Conexión del cableado de hardware 9

Instalar software de requisitos previos 12

Configuración 26

Configuración de Gallagher Command Centre 26

Configuración de hardware 39

Configuración de BioStar 2 71

Integración de Suprema con Gallagher v2.0 80

Agregar grupo de acceso 84

Integración de Suprema con Gallagher 88

Inscribir la ID de foto del usuario en Command Center para la plantilla facial 99

Inscribir la ID de correo electrónico del usuario en Command Center para el código QR 103

Selección de tarjeta predeterminada 112

Tarjeta inteligente (AOC/TOC) 113

Tarjeta HID ICLASS 117

Tarjeta de código QR 118

Dispositivos con licencia 119

Solución de problemas y preguntas frecuentes **120**

Configuración 120

Middleware 141

Propósito

La integración de Suprema con Gallagher es un middleware que permite al sistema Gallagher Command Centre 8.8 o posterior comunicarse con dispositivos biométricos Suprema, que pueden inscribir credenciales faciales biométricas o de huella dactilar para los usuarios desde Command Centre y administrar la configuración de los dispositivos conectados. Con la integración de Suprema con Gallagher, puede configurar y crear fácilmente el sistema de administración biométrica para Command Centre con dispositivos biométricos Suprema.

> **Información**
> Para obtener más detalles sobre la funcionalidad del sistema de control de acceso Gallagher Command Centre, consulte los manuales de usuario de Command Centre.

Introducción

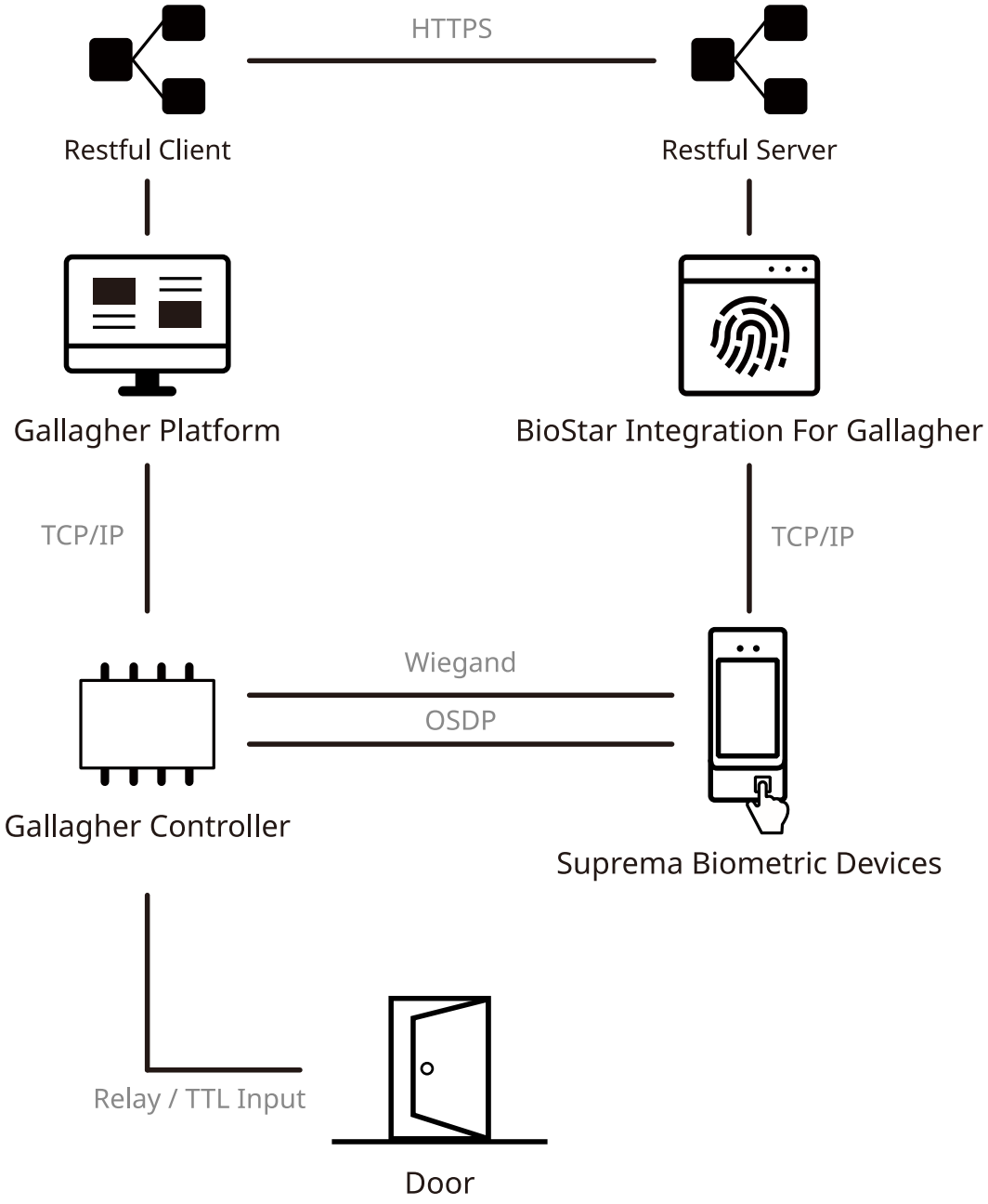
Características

Integración de Suprema con Gallagher: comunicación entre Gallagher Command Centre y Suprema BioStar 2. Así, se pueden generar plantillas biométricas para los dispositivos Suprema desde Gallagher Command Centre, lo que ofrece una solución de vanguardia para todos los usuarios finales.

A continuación se presentan las características que ofrece la integración de Suprema con Gallagher:

- El enrolamiento masivo de usuarios y la gestión desde Gallagher Command Centre se reflejan en Suprema BioStar 2.
- Con la integración de Suprema, los usuarios pueden enrolar datos de rostro visual biométrico y huella dactilar mediante escaneo en diversos dispositivos biométricos Suprema.
- Detección de CSN y Wiegand, e integración con BioStar para el enriquecimiento automático de datos.
- Con la integración de Suprema, los usuarios pueden enrolar datos de tarjeta mediante escaneo desde dispositivos biométricos como X-Station 2, BioLite N2, BioStation 3, FaceStation F2, XPass 2, X-Station 2, BioEntry W3 y BioEntry W2 (estos son los dispositivos probados).
- Permite administrar hasta 1,000 dispositivos biométricos.
- Todas las settings de los dispositivos Suprema se pueden realizar en la misma ventana de Command Centre.
- Compatible con una amplia gama de tipos de tarjeta, incluidas tarjetas TOC, tarjetas QR e incluso configuraciones de tarjeta personalizadas adaptadas a las necesidades específicas del cliente.
- La instalación de la integración se simplifica mediante un paquete EXE incluido que contiene todos los requisitos previos necesarios y garantiza un proceso de instalación fluido y eficiente.
- El middleware incluye soporte integrado para settings relacionadas con la red, junto con una guía completa de solución de problemas para ayudar con errores de configuración y escenarios de tolerancia a fallos.

Diagrama del sistema



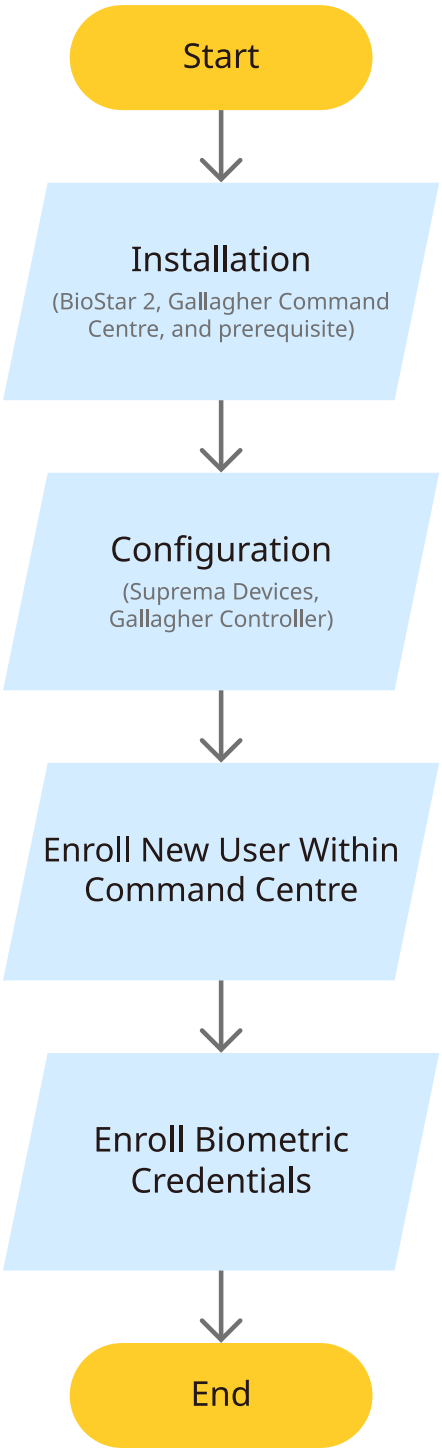
Instalación

Requisitos previos

Se requieren los siguientes requisitos previos para usar la integración de Suprema con Gallagher. Revise las condiciones de soporte antes de instalar la integración de Suprema con Gallagher.

Requisitos previos	
Microsoft Windows 10 (x64) o posterior	
Navegadores web	Nuevo Microsoft Edge
Gallagher Command Centre	Command Centre 8.80 o posterior
Suprema BioStar 2	• 64 bits • Versión 2.9.5 o posterior
Software	• Node v16.17.0 • PostgreSQL v14.5 • pgAdmin 4 v6.16 • Win64OpenSSL-3.0.5
Requisitos de hardware del sistema middleware	• 16 GB de RAM • Windows 10 o posterior • SSD de 256 GB/HDD de 1 TB • Intel Iris Xe Graphics (recomendado)
Dispositivos biométricos Suprema	• BioStation 3 • BioLite N2 • FaceStation F2 • BioEntry W2 • XPass 2 • X-Station 2 • BioEntry W3

Diagrama de flujo de la configuración



Conexión del cableado de hardware

Para conexión Wiegand

Dispositivo Suprema - **Lector 1** a módulo de puerta HBUS 4 In 2 Out 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

Dispositivo Suprema - **Lector 2** a módulo de puerta HBUS 4 In 2 Out Wiegand

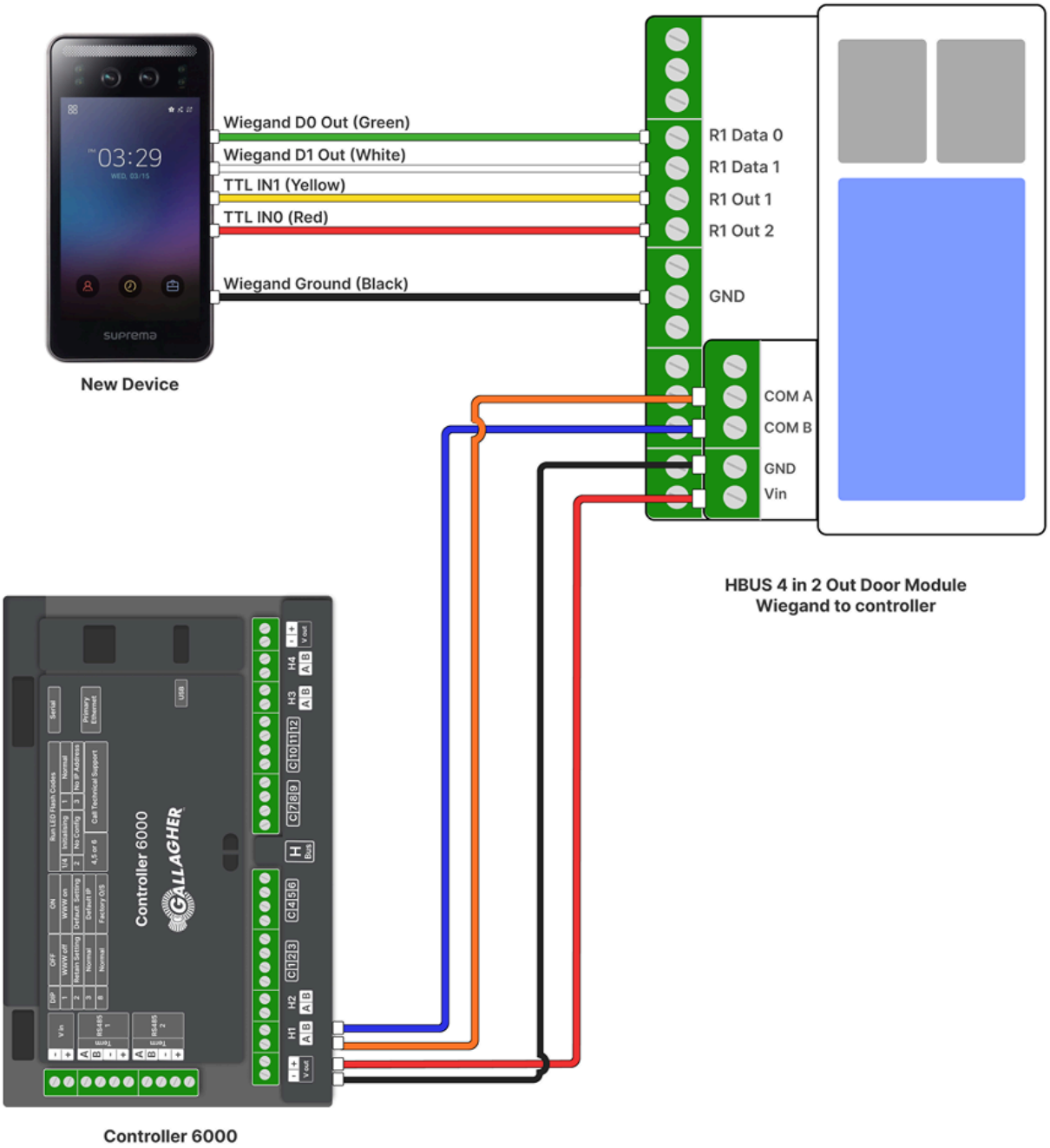
(Suprema Device) Wire Name	HBUS 4 In 2 Out Door Module Wiegand Port to connector
Wiegand D0 Out (Green)	R2 Data 0
Wiegand D1 Out (White)	R2 Data 1
Wiegand Ground (Black)	GND
TTL IN0 (Red/Purple)	R2 Out 2
TTL IN1 (Yellow/Brown)	R2 Out 1

Módulo de puerta HBUS 4 In 2 Out Wiegand a 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

Diagrama de conexión Wiegand



Para conexión OSDP

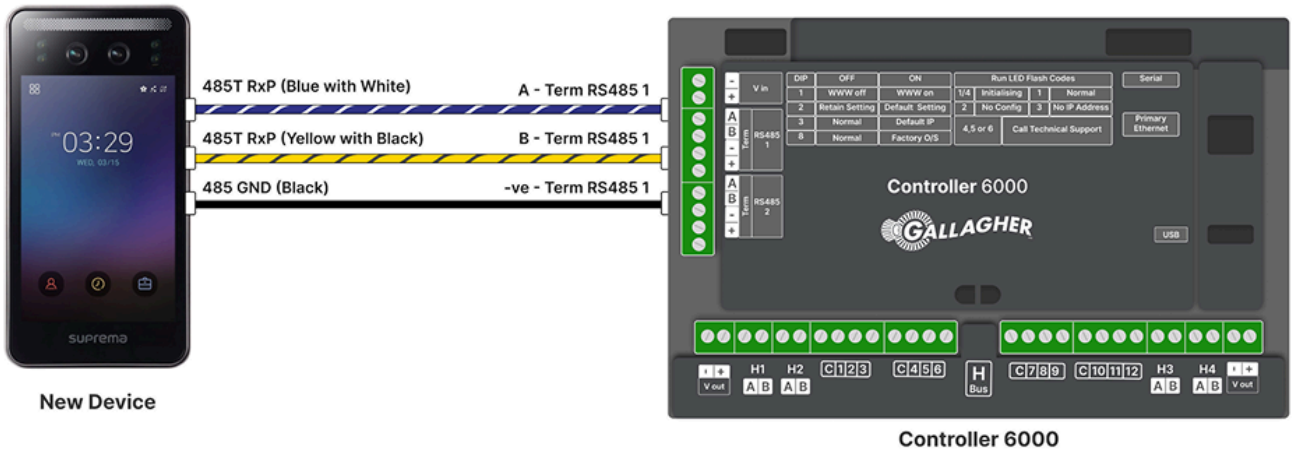
Dispositivo Suprema OSDP/RS485 **lector 1** a Controller 6000

(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

Dispositivo Suprema OSDP/RS485 **lector 2** a 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

Diagrama de conexión OSDP



Instalar software de requisitos previos

Instalación de la configuración de Gallagher Command Centre

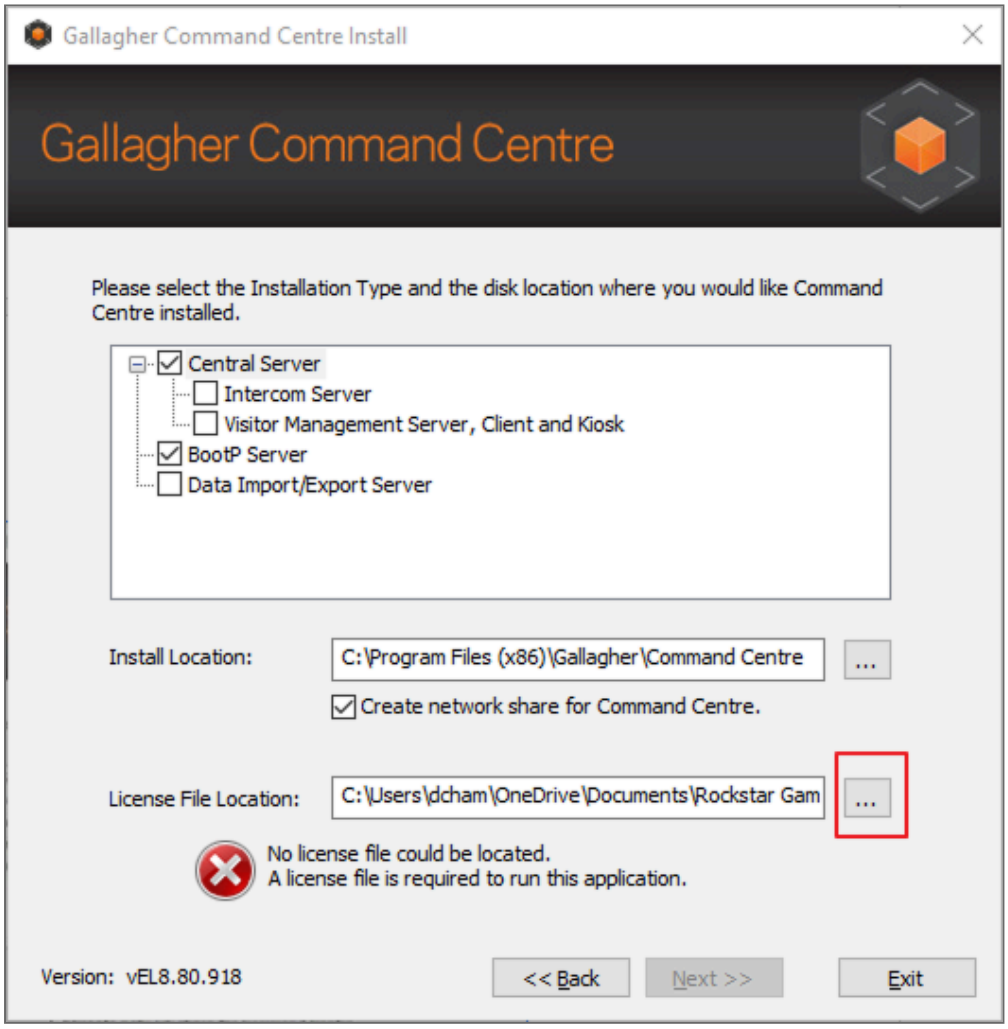
Información

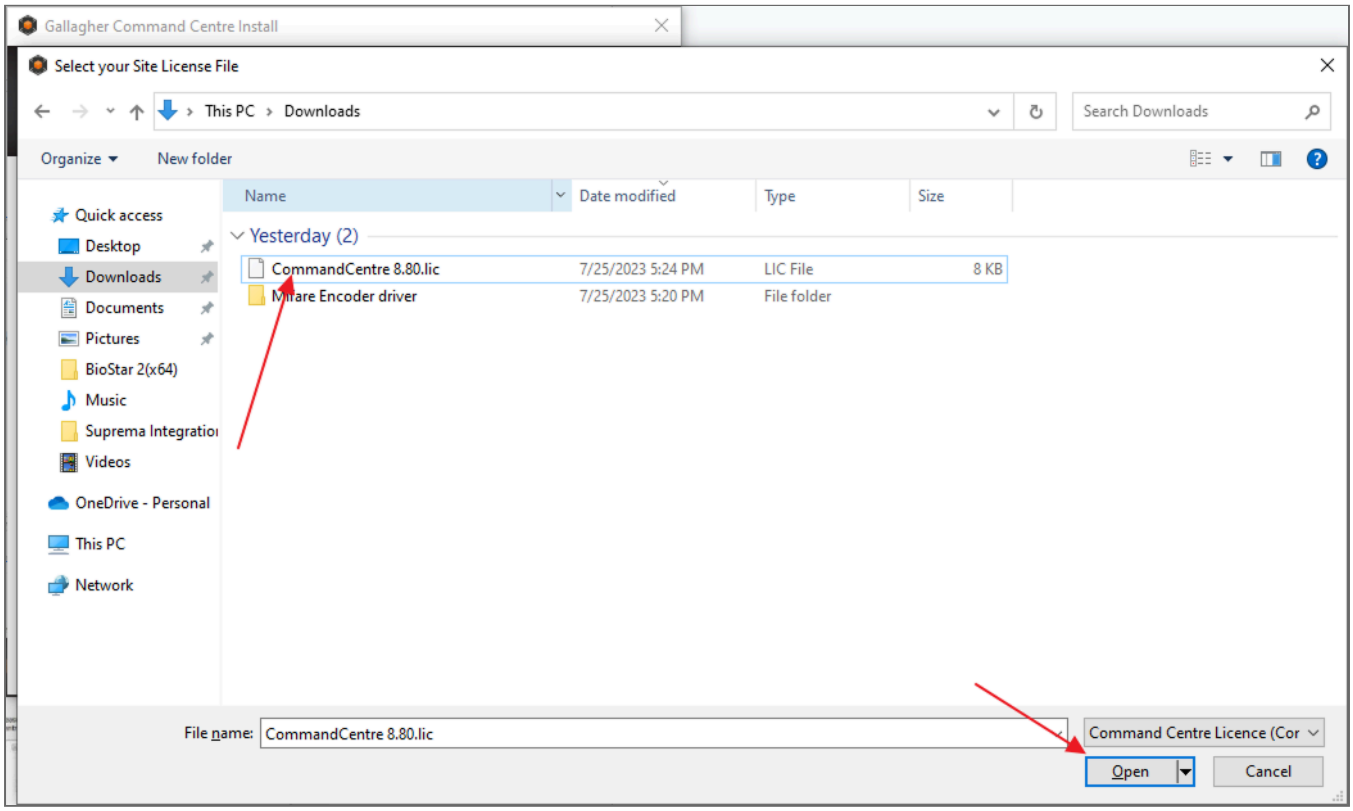
- No cambie ningún nombre ni contraseña durante la instalación y la configuración.
- Para actualizar la integración de Suprema con la versión de Gallagher, haga clic aquí.
- En concreto, puede consultar la **3C4643 Gallagher Command Centre vEL8.80 Release Note** para instalaciones nuevas.
- La **3E0068 Upgrade Procedure** para fines de actualización contiene más información en la carpeta Release Notes de su directorio ISO de Command Centre.
- Debe extraer `Suprema integration With Gallagher.zip` en `C:\Program Files\`.

1. Dentro de la carpeta Gallagher Command Centre vEL.8.80 (o posterior) → Setup.exe, **marque la casilla** y presione el botón **Siguiente**.

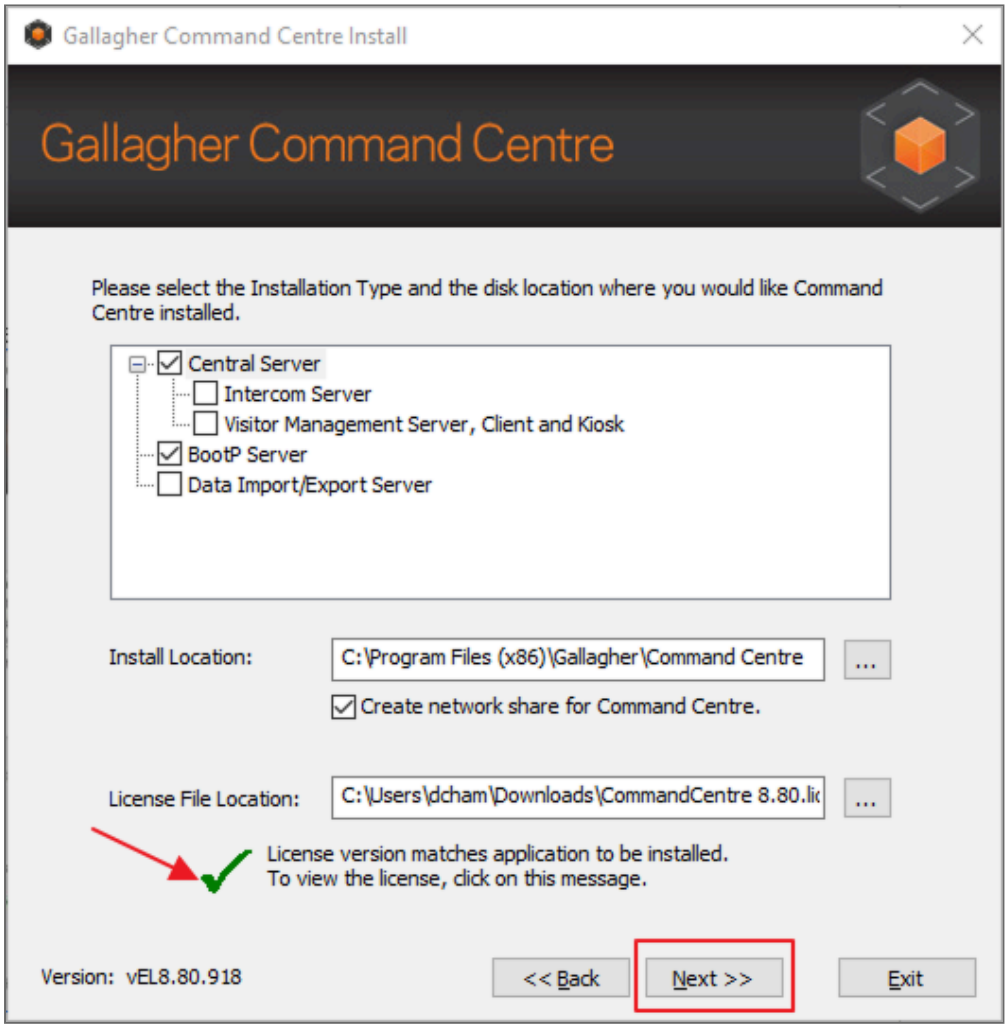


2. **Haga clic** en el botón "..." y ubique el archivo de licencia incluido en la configuración.

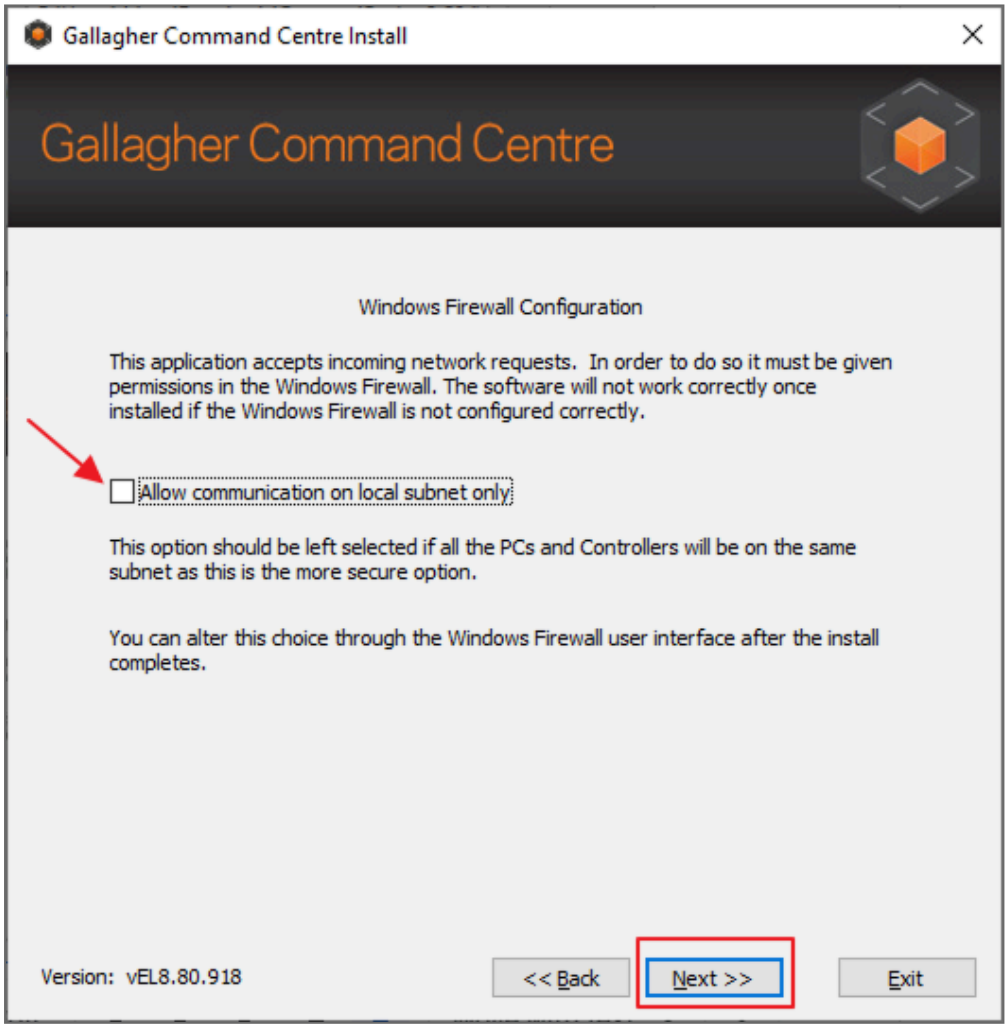




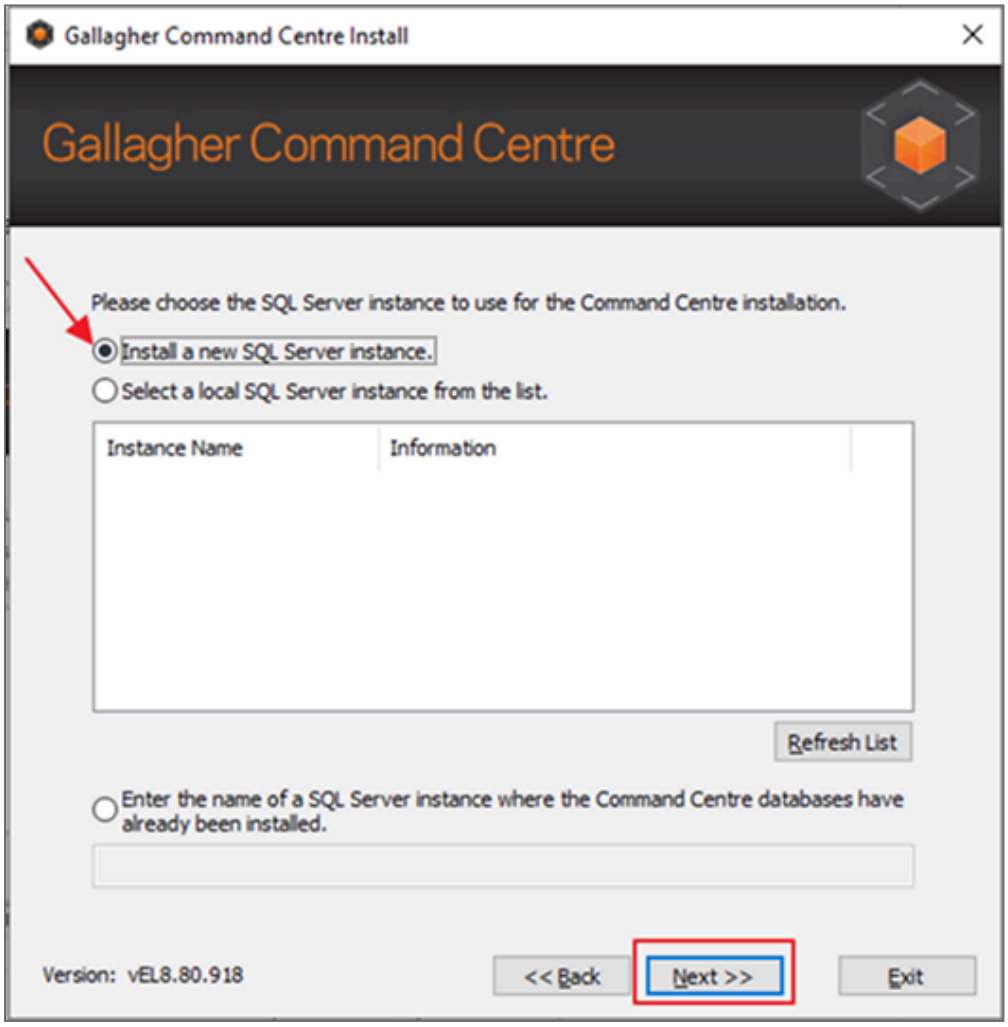
3. Cuando seleccione el archivo de licencia correcto, el icono cambiará a una marca de verificación; después, **presione** el botón **Siguiente**.



4. **Desmarque** solo la casilla de la subred y presione el botón **Siguiente**.

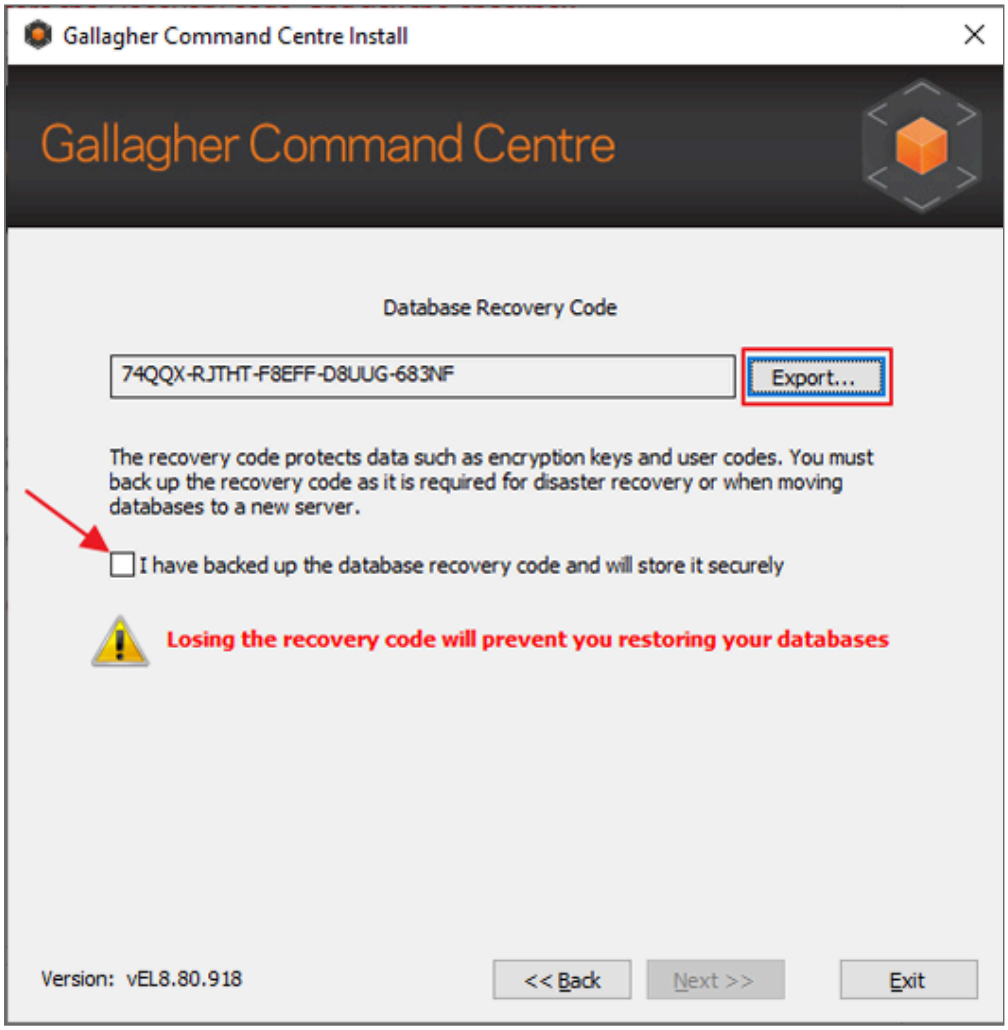


5. **Seleccione** la opción Instalar nueva SQL y presione el botón **Siguiente**.

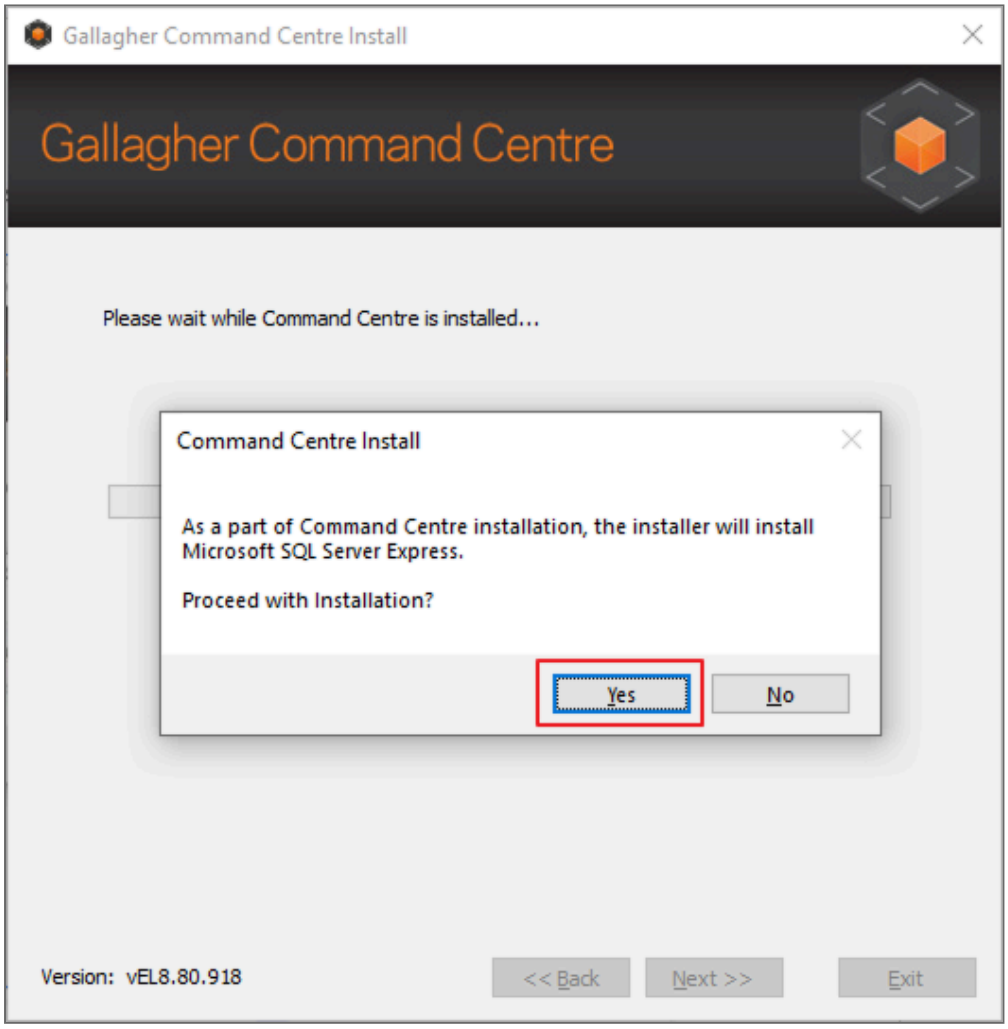


6. **Seleccione** la opción No instalar una plantilla de base de datos.
7. Sin cambiar ninguna opción, presione **Siguiente** hasta llegar a la pantalla del código de recuperación.

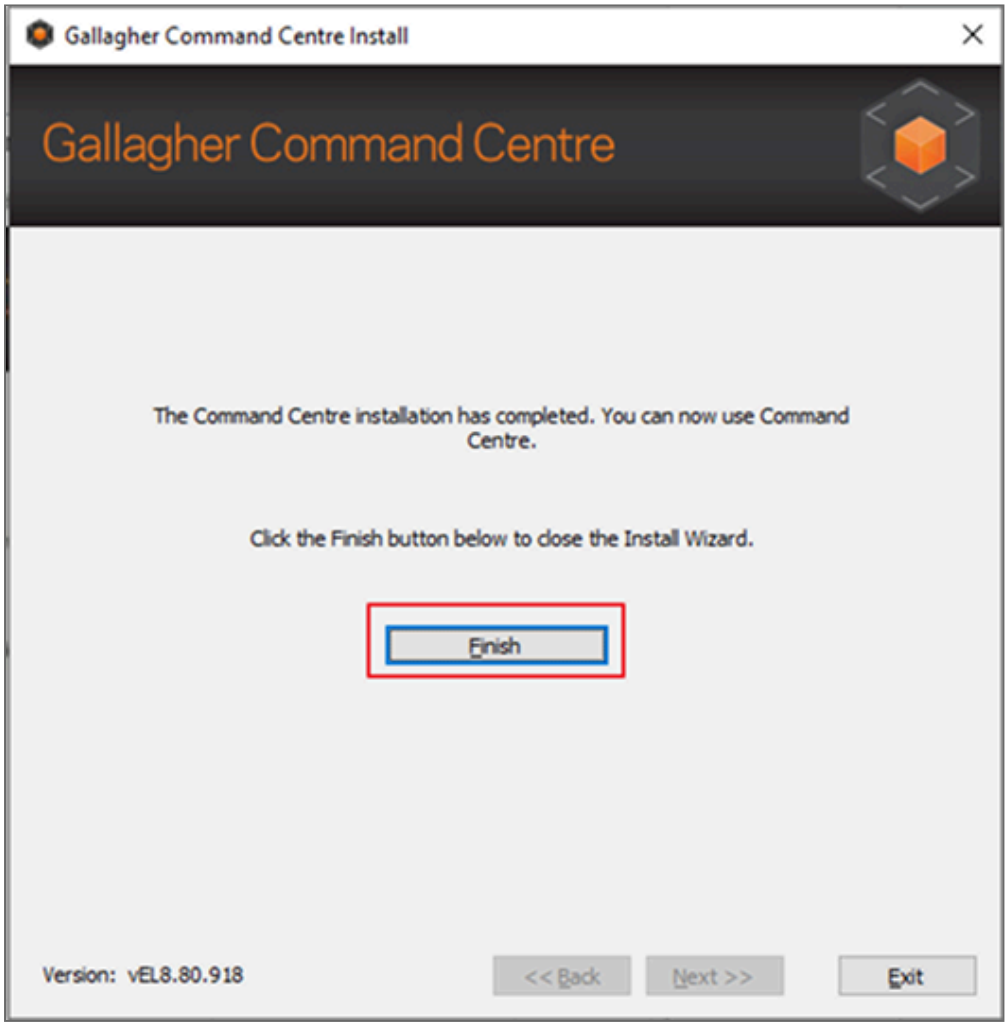
> **Información**
> Haga clic en el botón de exportación, guarde el código de recuperación y marque la casilla.



8. Seleccione **Sí** y comenzará la instalación.



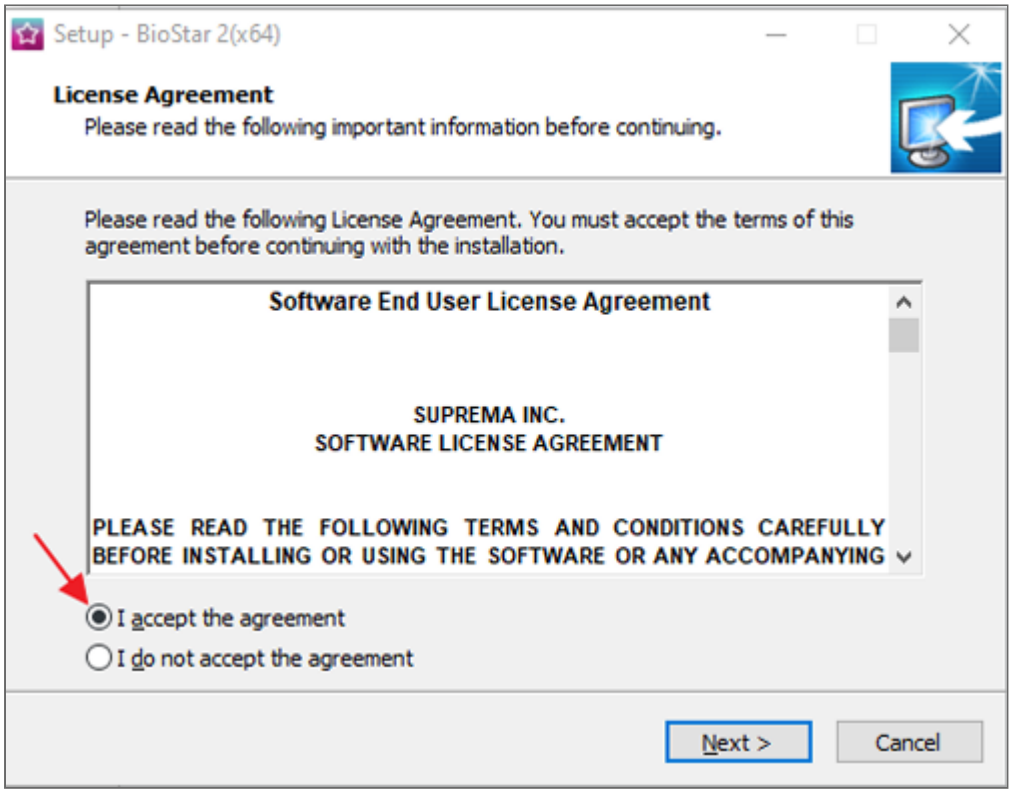
9. Después de completar la instalación, presione el botón **Finalizar**.



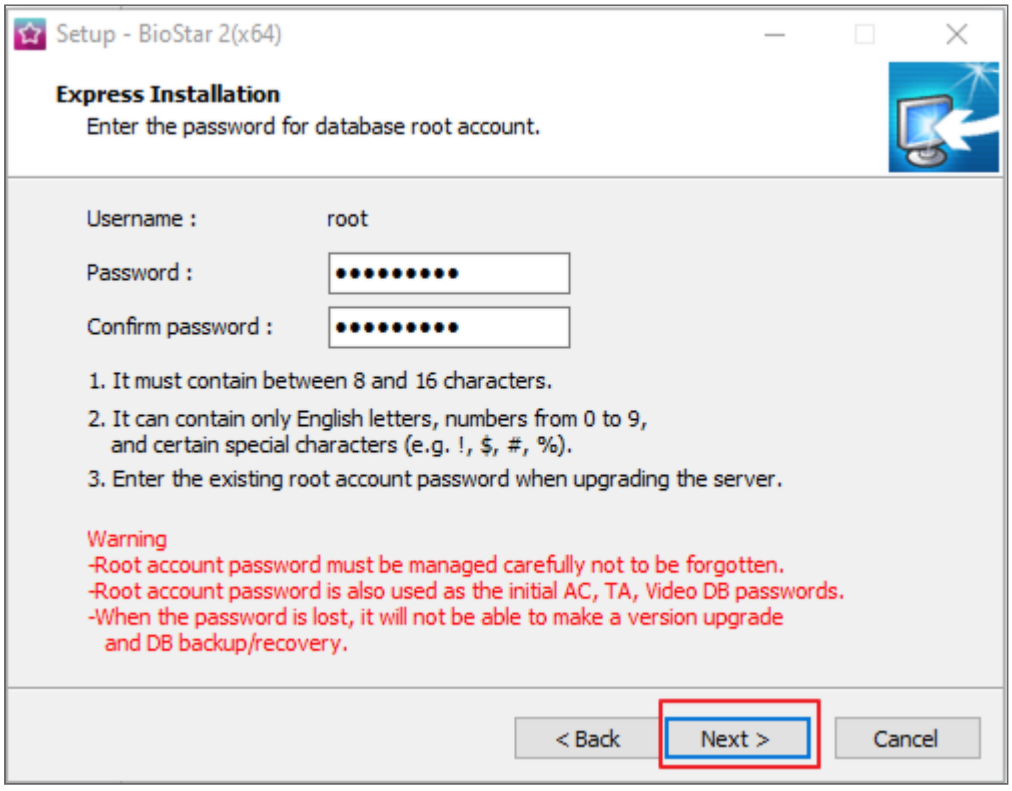
Instalación de BioStar 2

1. Abra **BioStar 2.exe**, elija el idioma, acepte el acuerdo y presione **Siguiente**.

> **Información**
> Descargue la versión más reciente de BioStar 2: Haga clic aquí.

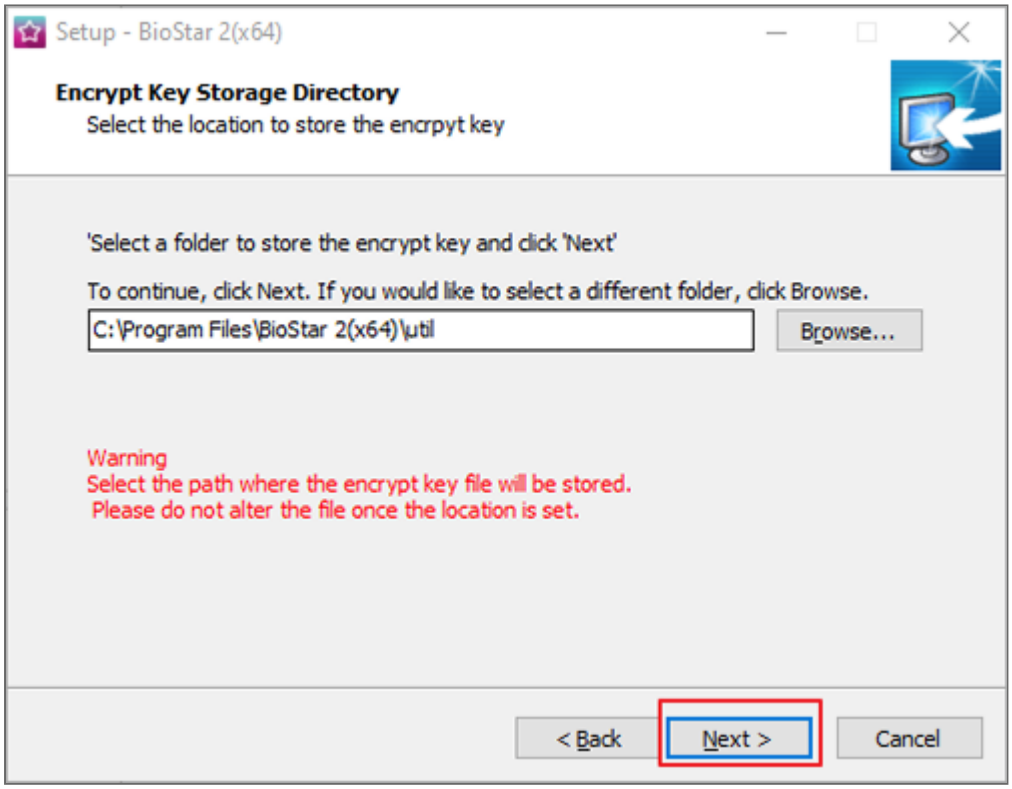


2. Ingrese aquí su **contraseña** de BioStar 2 y presione el botón **Siguiente**.

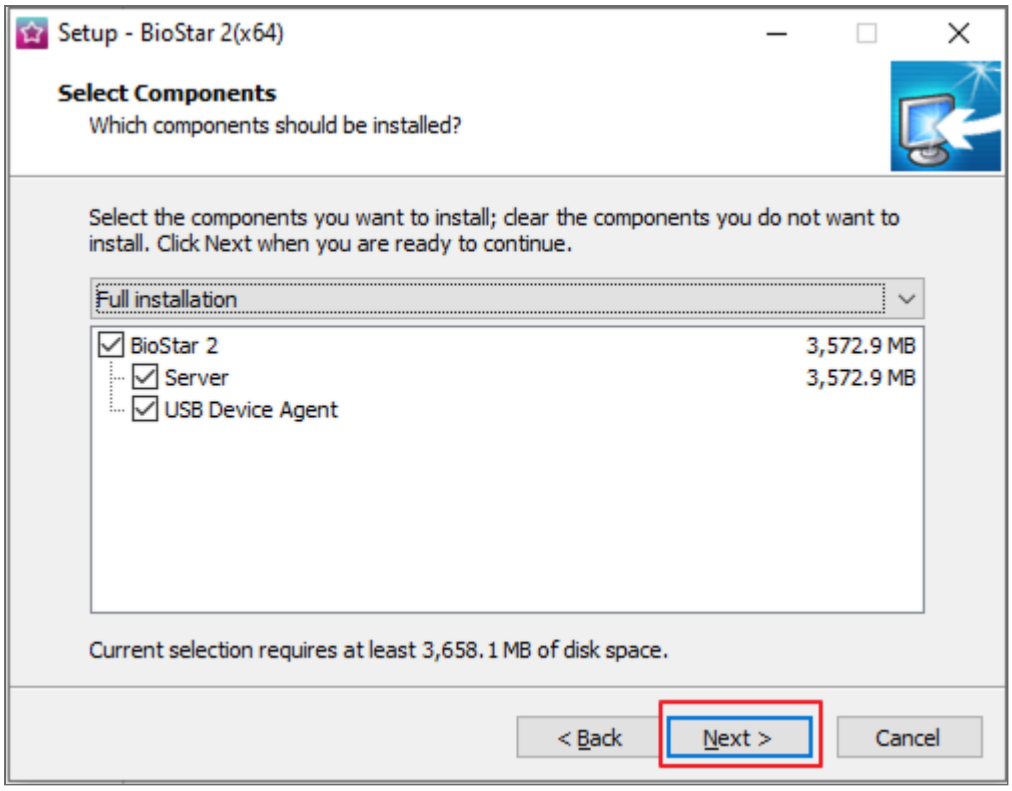


3. Seleccione la instalación **Express** e ingrese de nuevo la contraseña de BioStar 2.

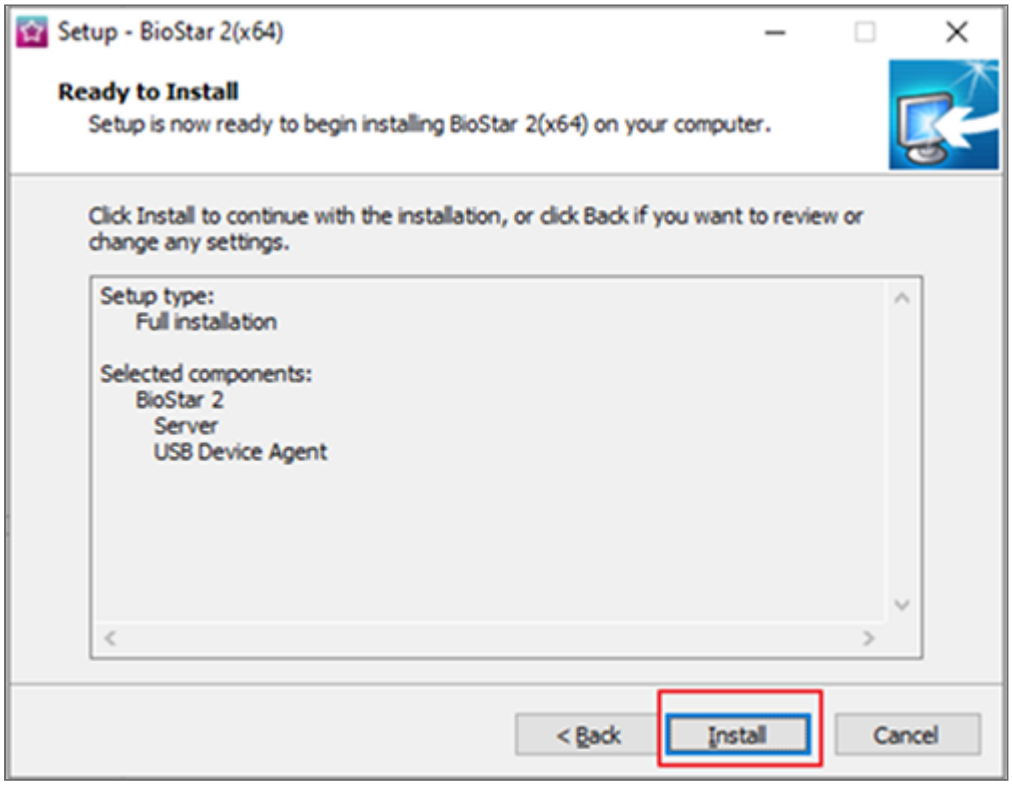
4. Seleccione la ubicación y continúe.



5. Presione el botón **Siguiente** hasta llegar a la pantalla Seleccionar componentes. Marque ambas opciones y presione el botón **Siguiente**.

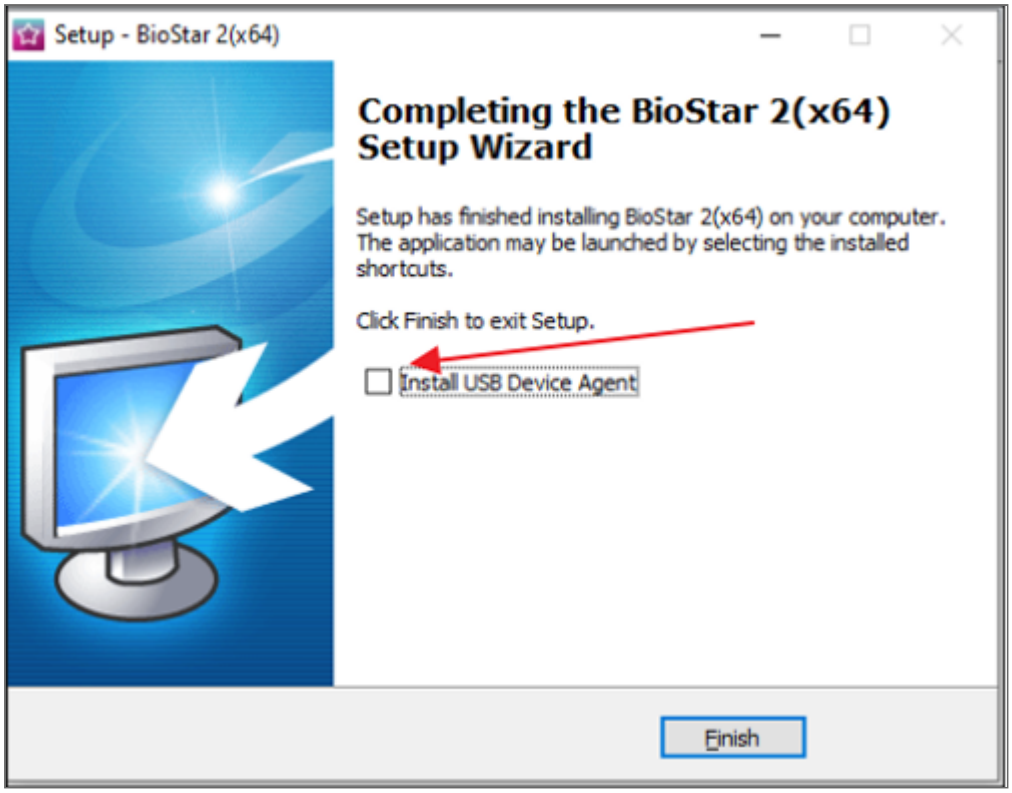


6. Presione el botón **Instalar** para iniciar la instalación.



7. **Desmarque** la opción Instalar USB Device Agent, presione el botón **Finalizar** y BioStar 2 se instalará en su PC.

> **Información**
> Si va a usar el dispositivo USB, debe **marcar** Instalar USB Device Agent.

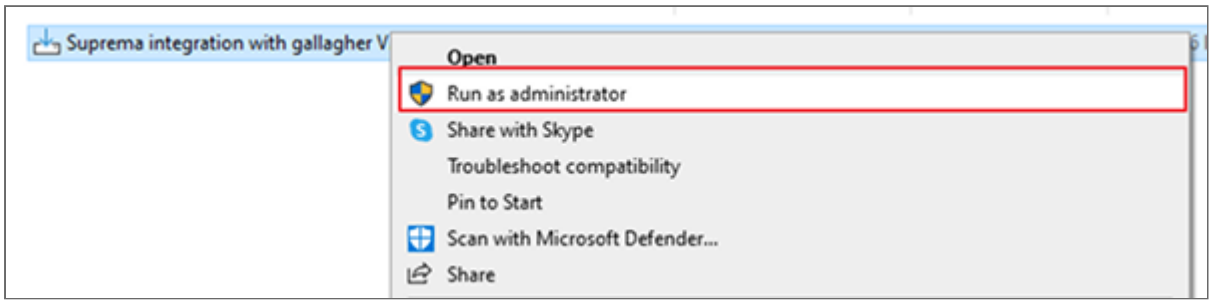


Requisitos previos de instalación del middleware

Información

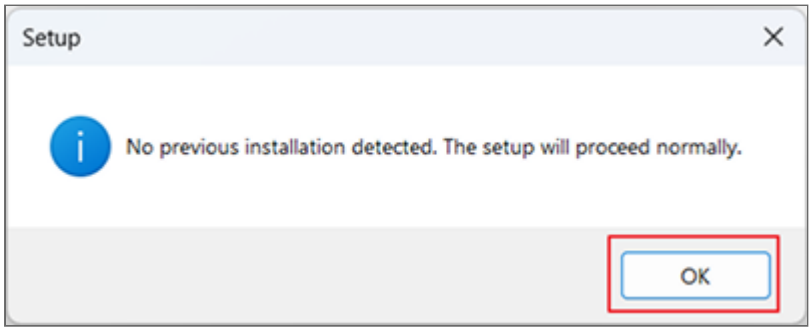
- Antes de extraer o ejecutar Suprema Integration with Gallagher2.0.zip, desactive el antivirus.
- Si está actualizando desde una versión anterior, revise la solución en la guía de solución de problemas.

1. Debe **ejecutar** el archivo Suprema Integration with Gallagher 2.0 como administrador dentro de la carpeta Suprema Integration with Gallagher 2.0. Esto instalará OpenSSL, PostgreSQL, PgAdmin4 y Node. JS. Además, esto configurará los certificados necesarios para nuestra integración.

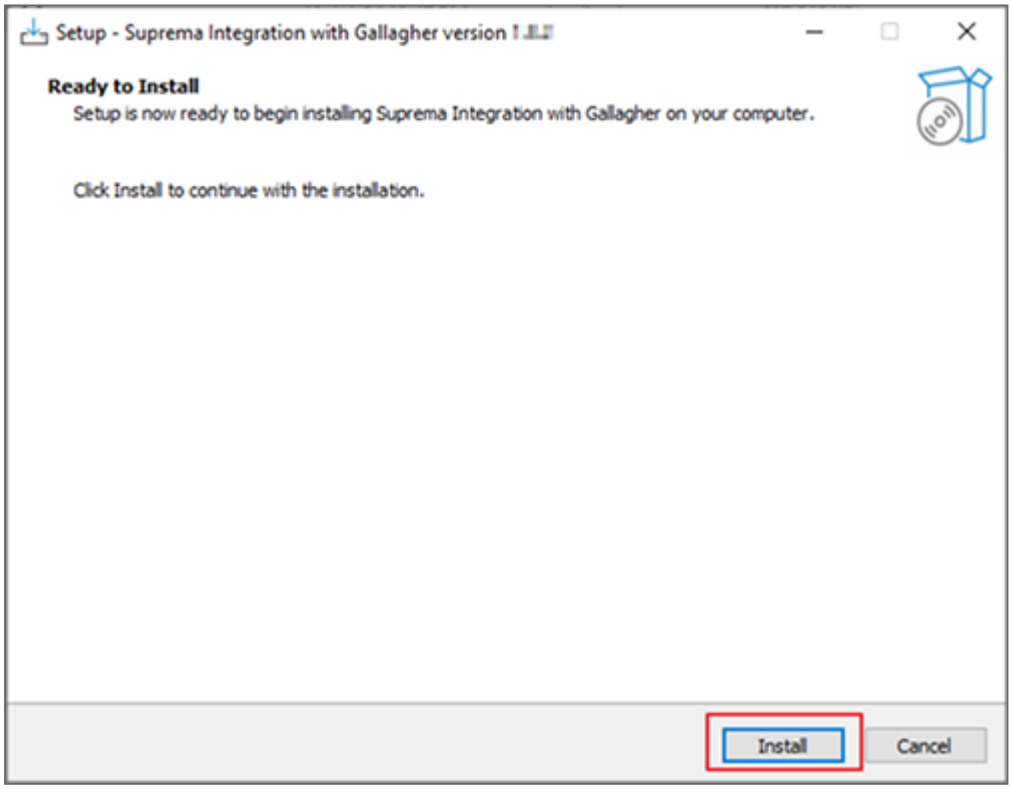


2. Presione **Sí** si solicita permisos para permitir desde un editor desconocido.

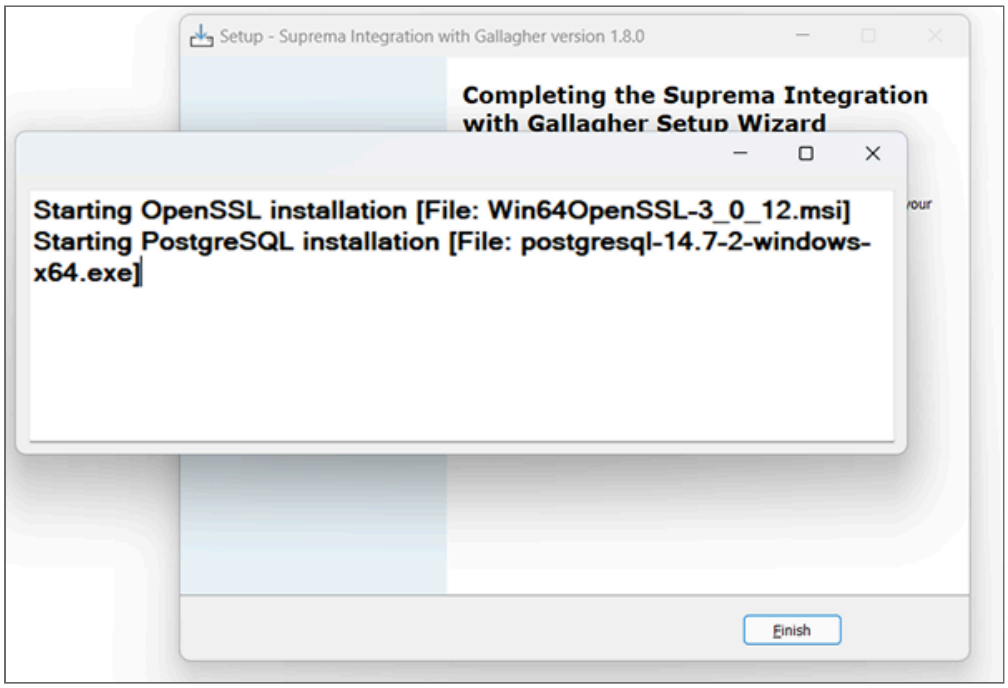
3. Presione **Aceptar**.



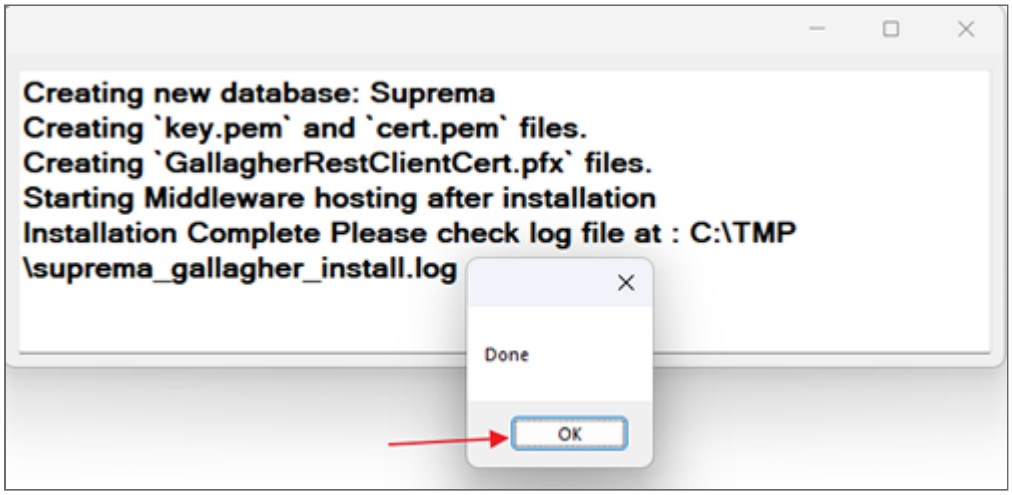
4. Ahora que está listo para instalar el software, presione **Instalar**.



5. Comenzará la instalación de los requisitos previos y el software se instalará automáticamente.

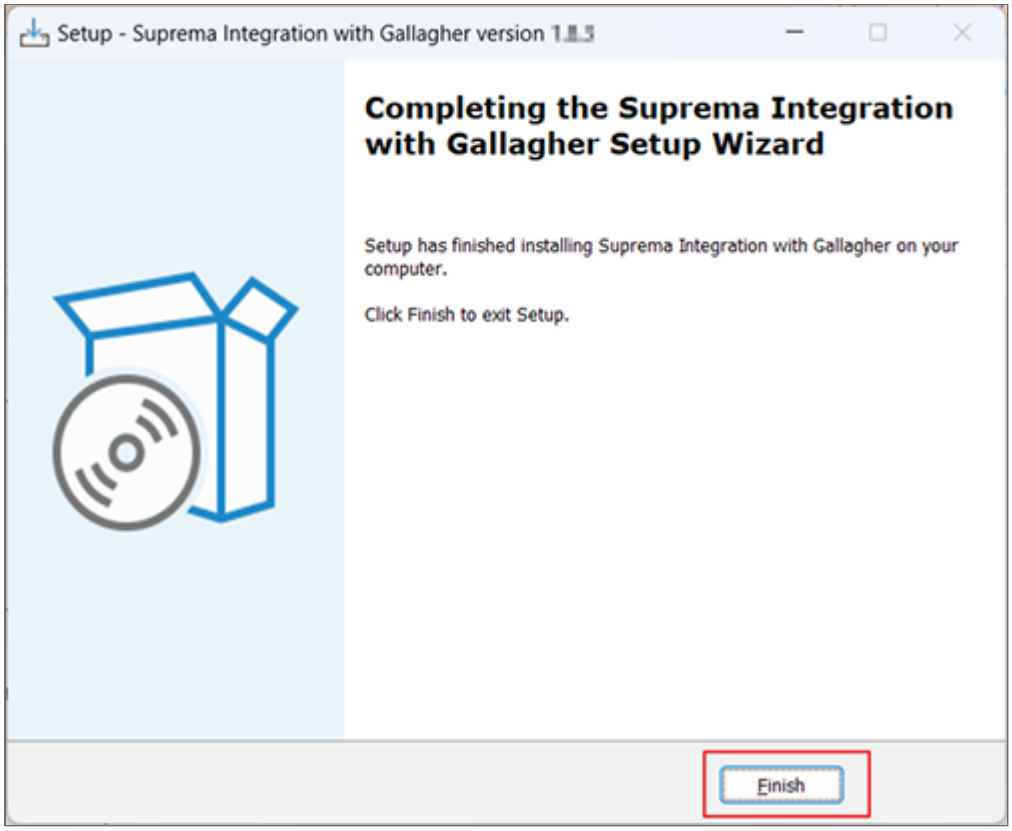


6. Presione **Aceptar** para la ventana emergente siguiente.



7. Ya terminó con la instalación de los requisitos previos; presione **Finalizar**.

> **Información**
> Después de instalar el middleware, reinicie el sistema una vez.

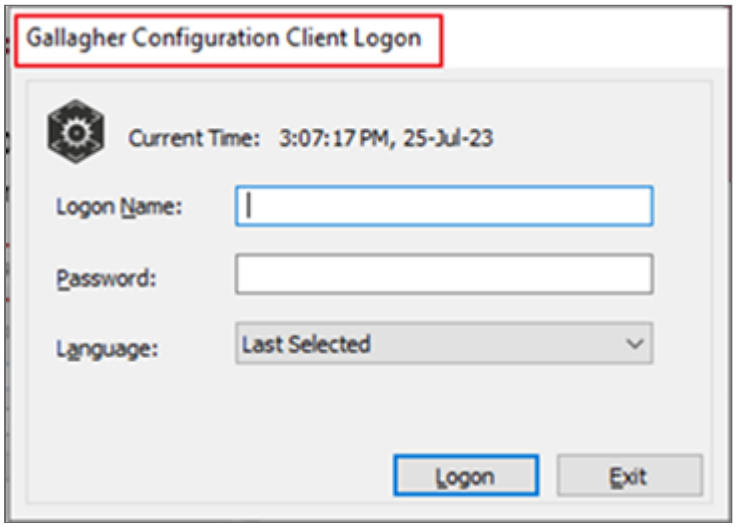


Configuración

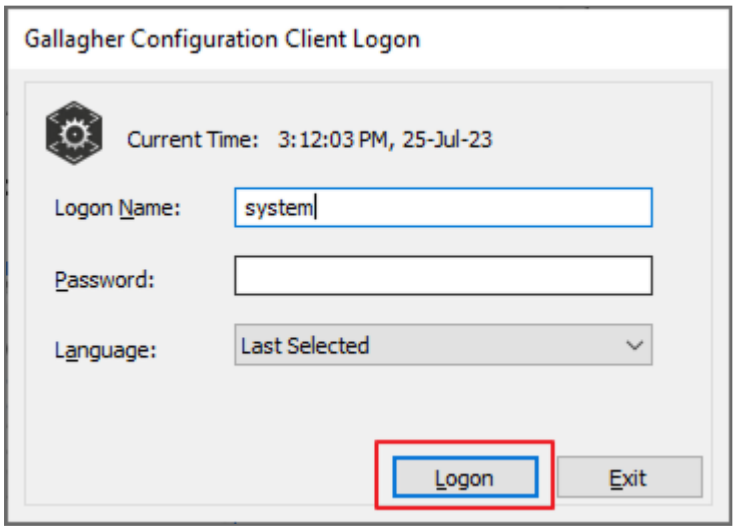
Configuración de Gallagher Command Centre

Inicio de sesión del cliente de configuración de Gallagher

1. **Haz clic** en el menú Inicio y abre Configuration Client.



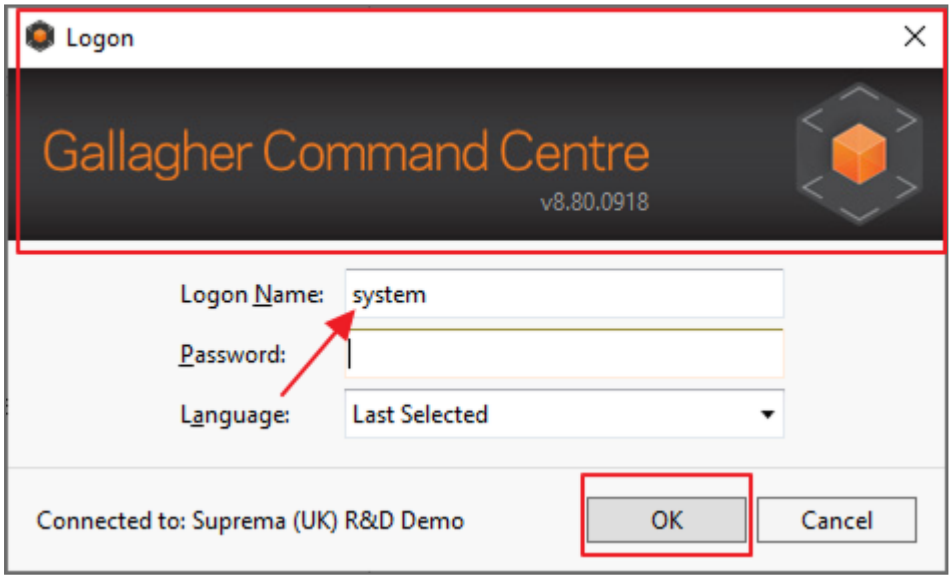
2. Establece el nombre de inicio de sesión como **system**, la contraseña como **none** y **presiona** el botón **Logon**.



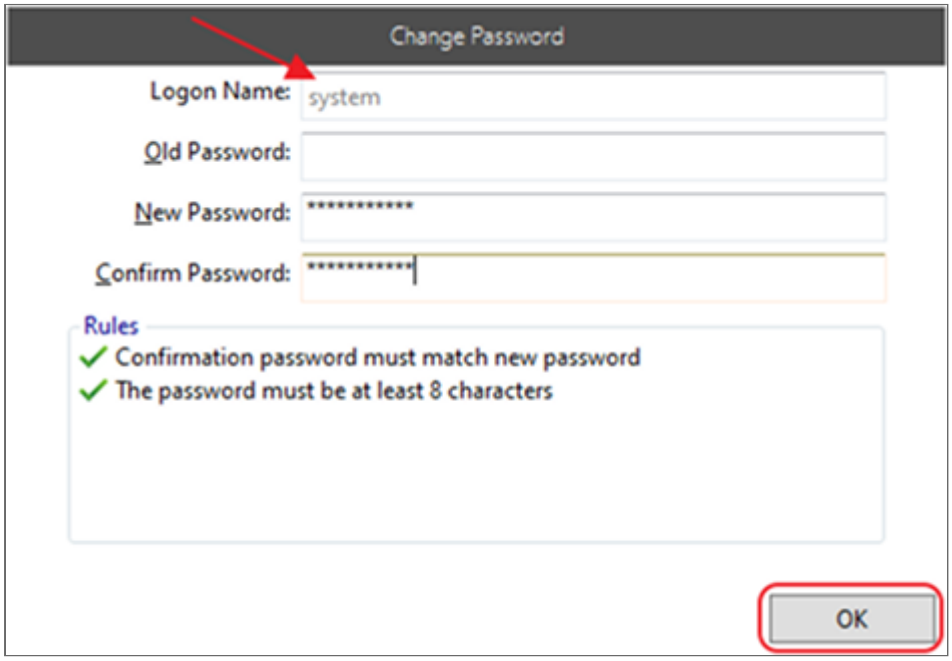
Gallagher Command Centre

> **Información**
> Proceso para generar la clave de API de Gallagher.

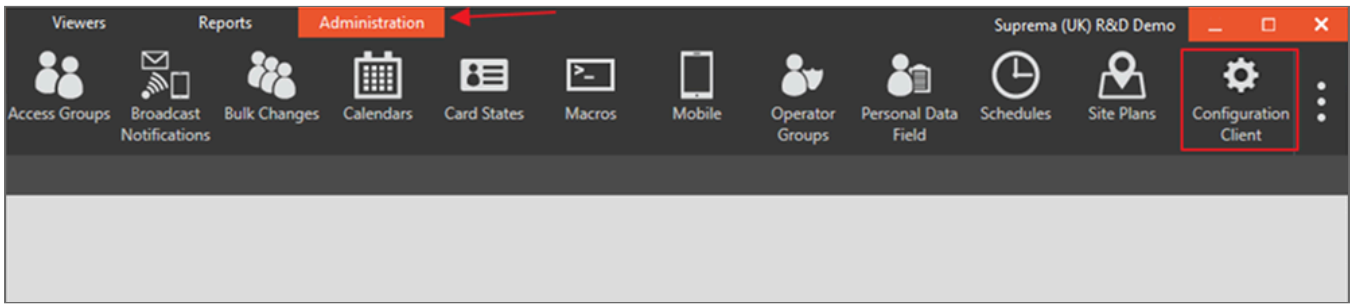
1. Abre Gallagher Command Centre, establece el nombre de inicio de sesión como system y presiona el botón **OK**.



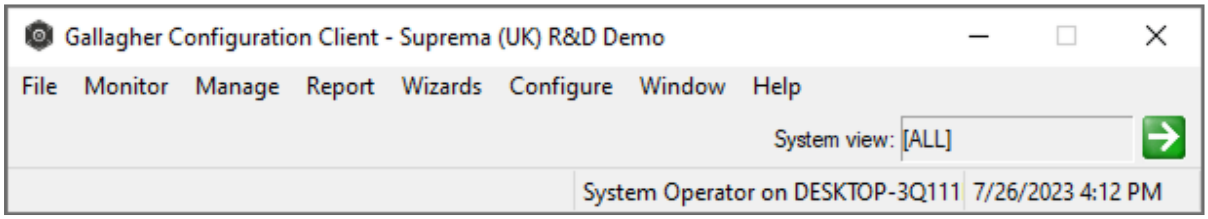
2. **Establece** el nombre de inicio de sesión como **system**, establece la contraseña para Gallagher Command Centre y presiona **OK**.



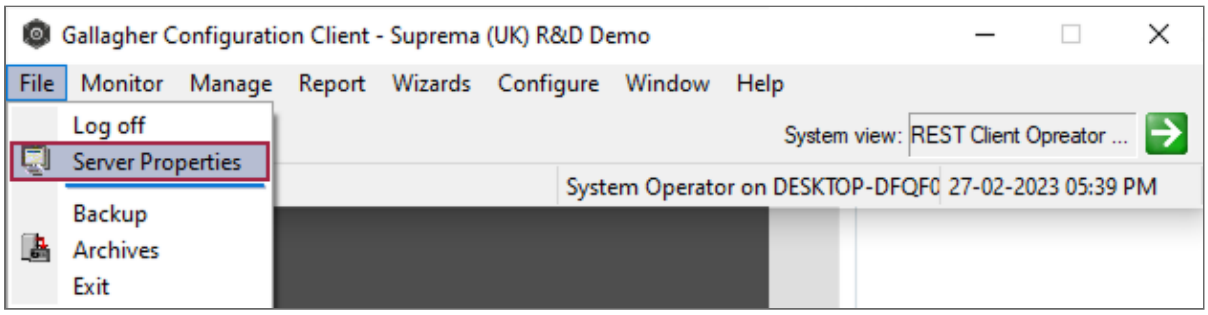
3. Ahora, ve a Administration desde la esquina superior izquierda y **selecciona** Configuration Client; la ventana se abrirá.



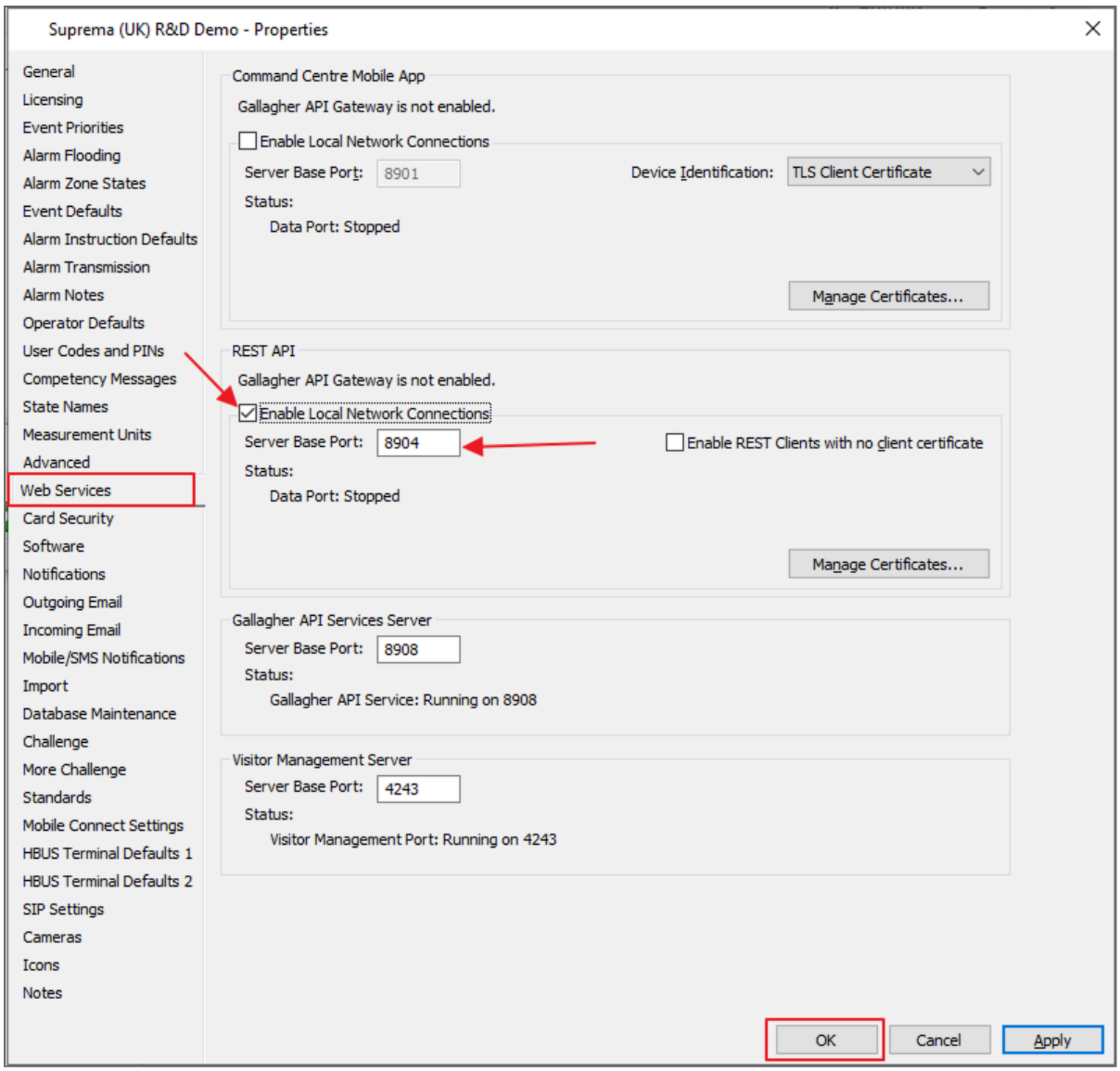
4. Se abrirá la pestaña siguiente.



5. Para configurar las propiedades del servidor, **selecciona File → Server Properties.**

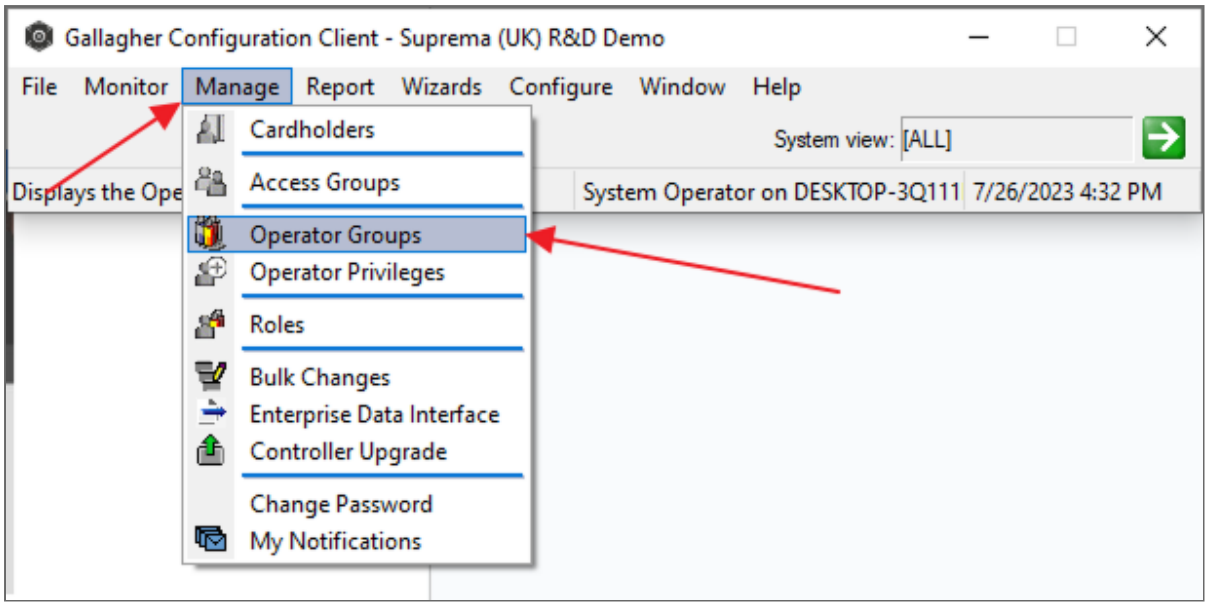


6. Se abrirá la nueva ventana. Ahora ve a **Web Services**. En la sección **REST API**, habilita la conexión a la red local, **establece** el puerto del servidor en **8904**, **desmarca** Enable REST client with no client certificate y **presiona** el botón **OK**.

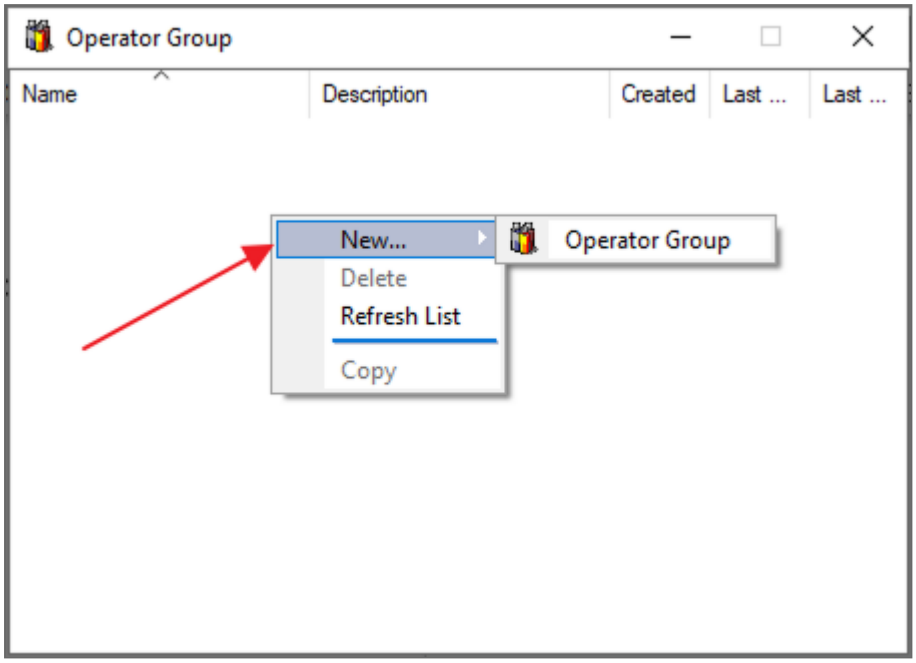


7. **Haz clic en Gallagher Client.**

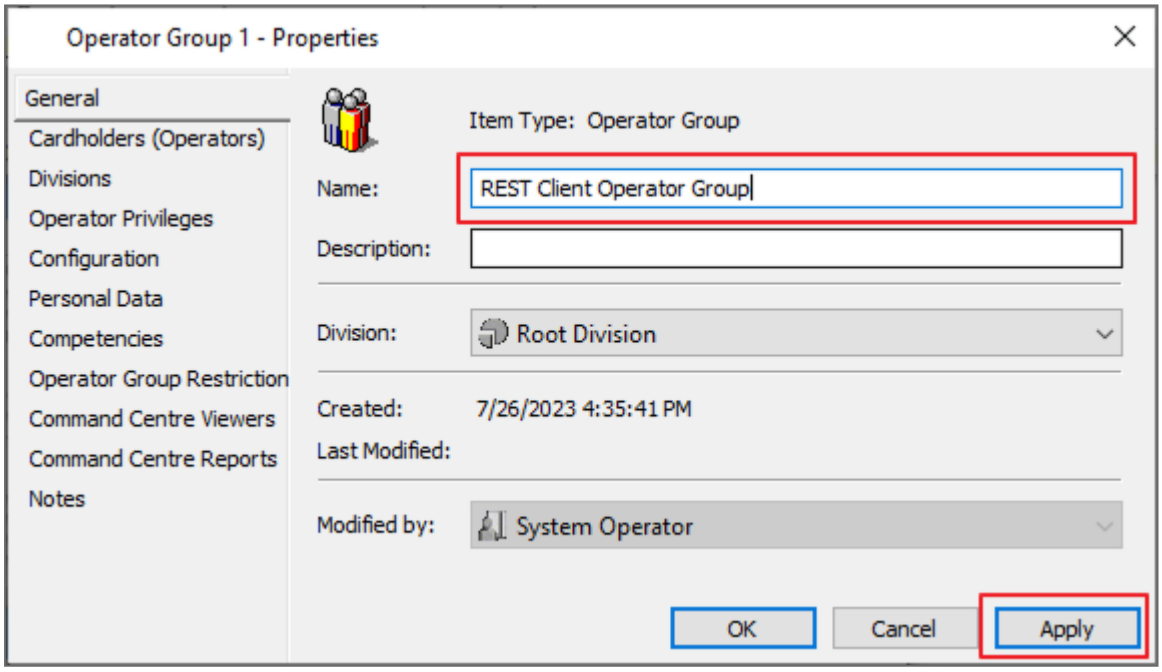
Haz clic en **Manage**. En el menú desplegable, **selecciona Operator Groups**.



8. Se abrirá la ventana de Operator Group. **Haz clic derecho** y selecciona **New → Operator Group**.

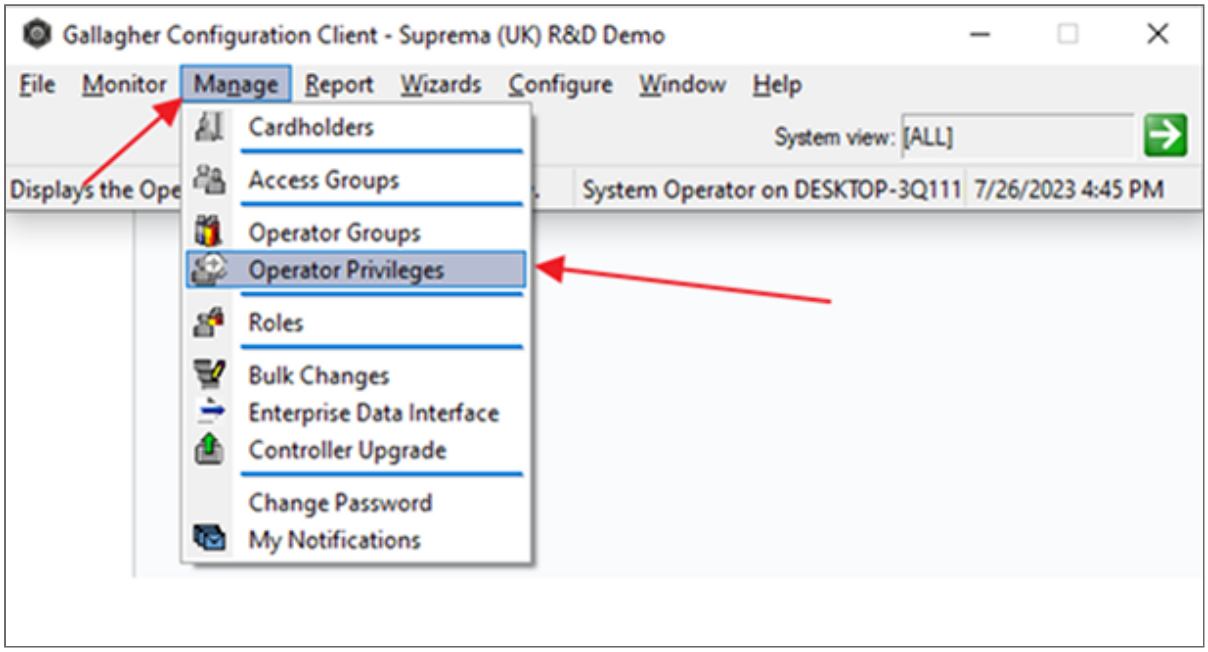


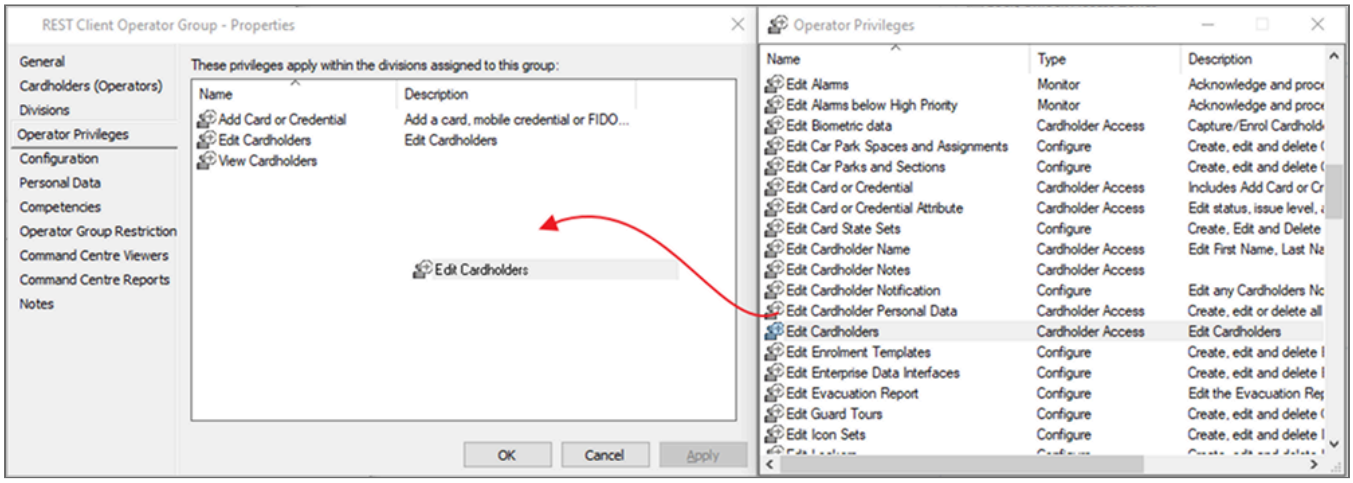
9. En la configuración general, el nombre debe establecerse como **REST Client Operator Group**. Luego haz clic en **Apply**.



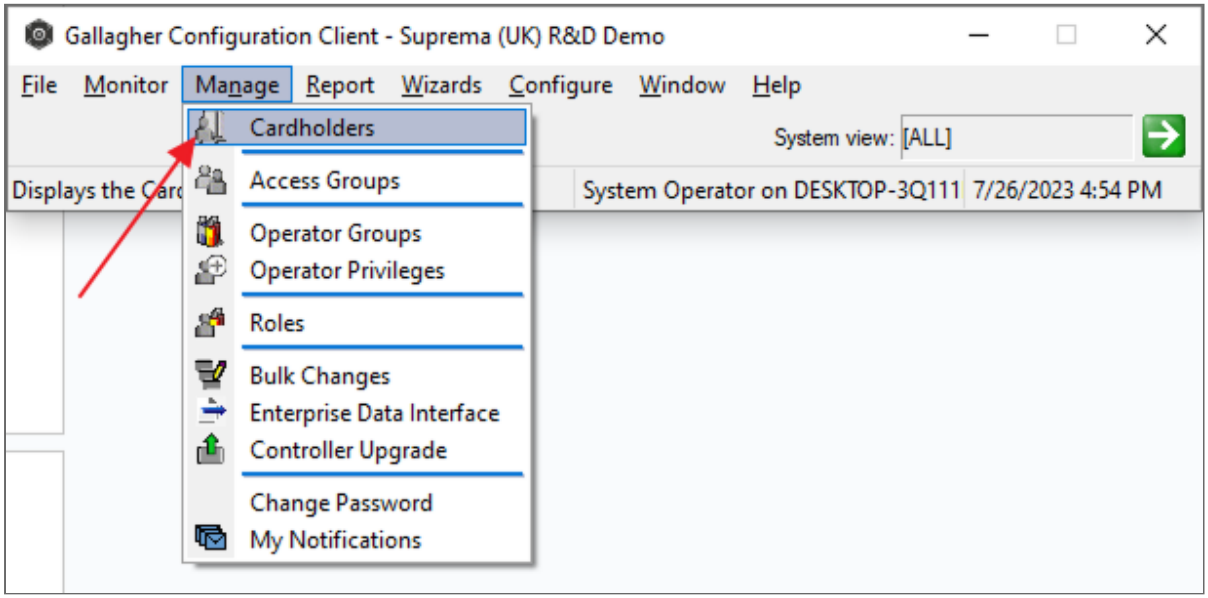
10. Ahora **selecciona** la configuración **Operator Privileges** en Operator group y ve a la ventana de cliente de configuración de Gallagher: Manage → Operator Privileges. Ahora **arrastra y suelta**.

Debes agregar 3 privilegios al Operator Group (Add Card or Credential, Edit Cardholders, View Cardholders) desde operator privileges al operator group y **presionar** el botón **OK**; luego **cierra** operator privileges.

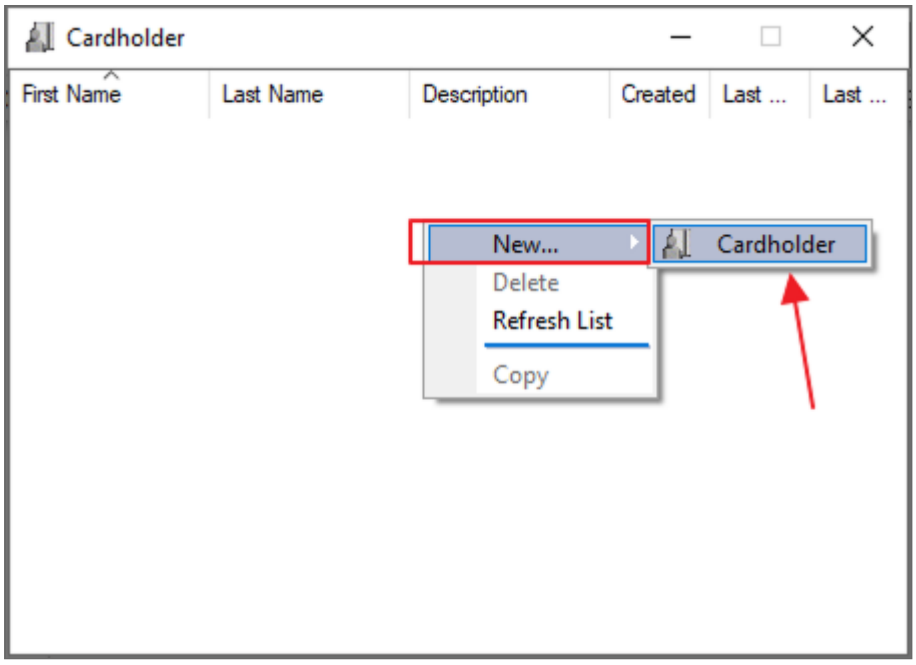




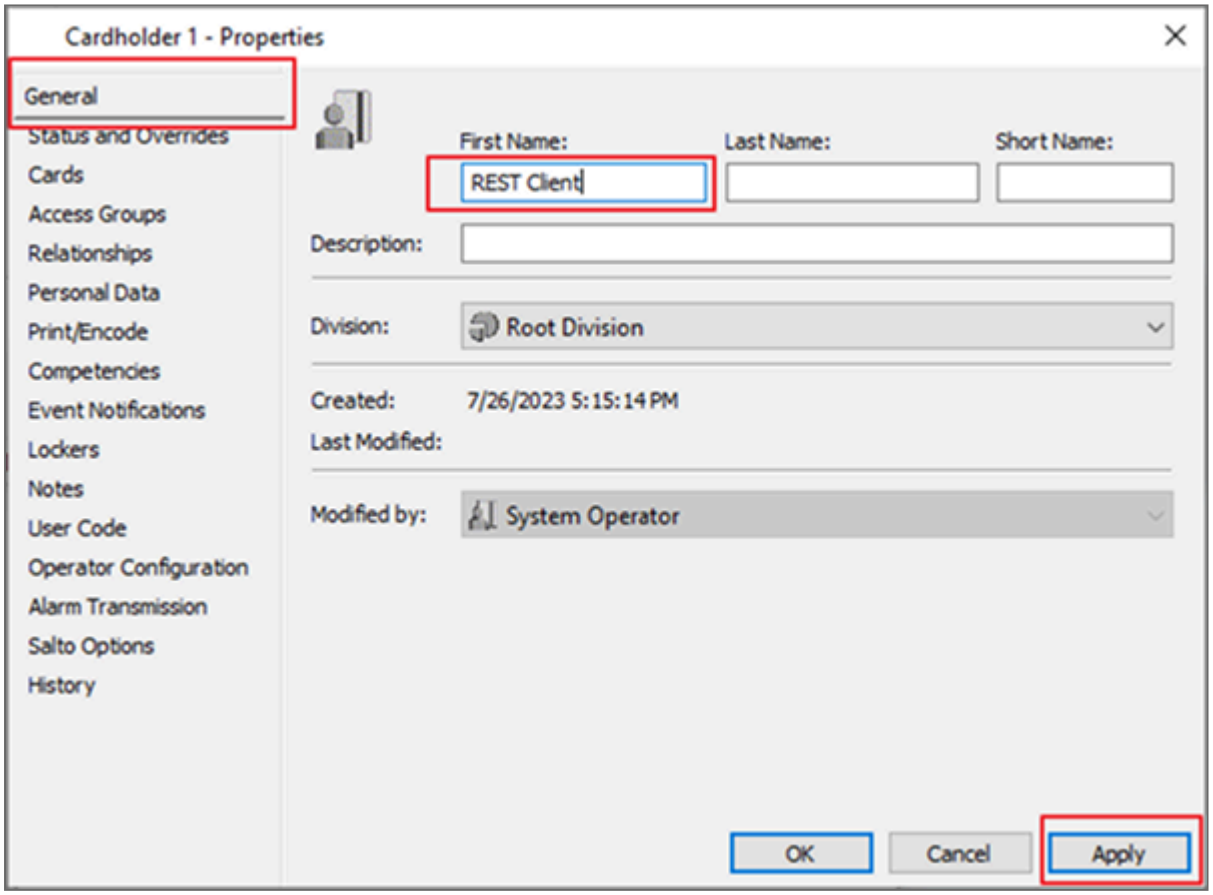
11. Ve a Configuration Client y **selecciona Cardholders**.



12. **Haz clic derecho** en New → Cardholder.

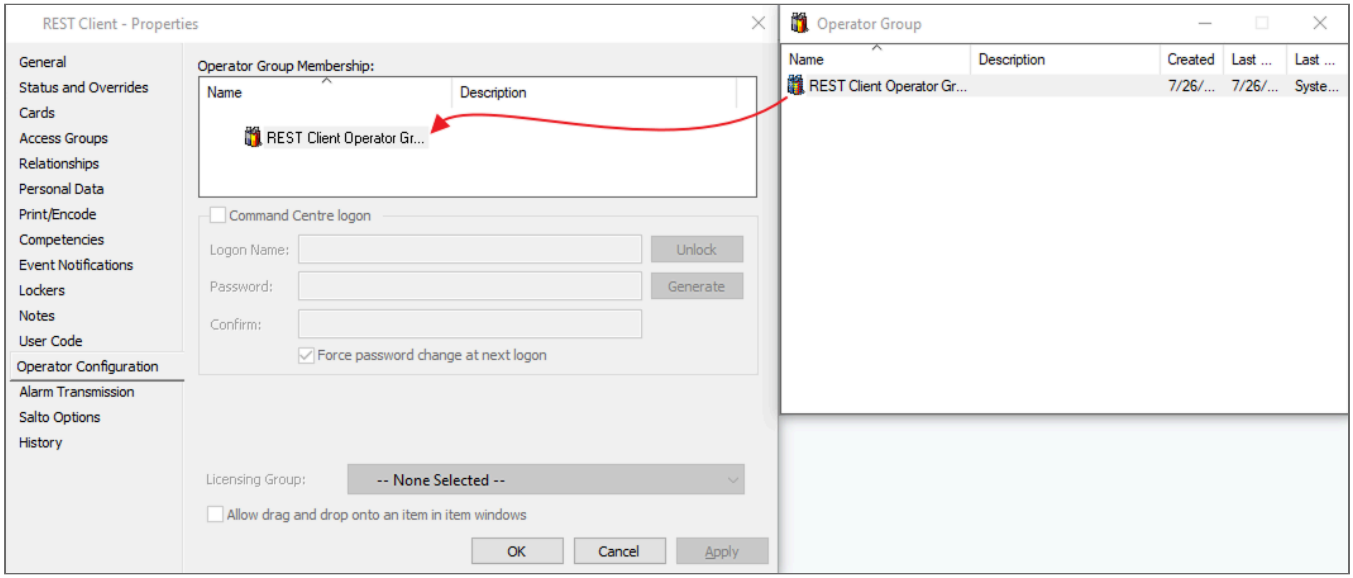


13. En la configuración general, establece First Name como **REST Client** y **presiona Apply**.

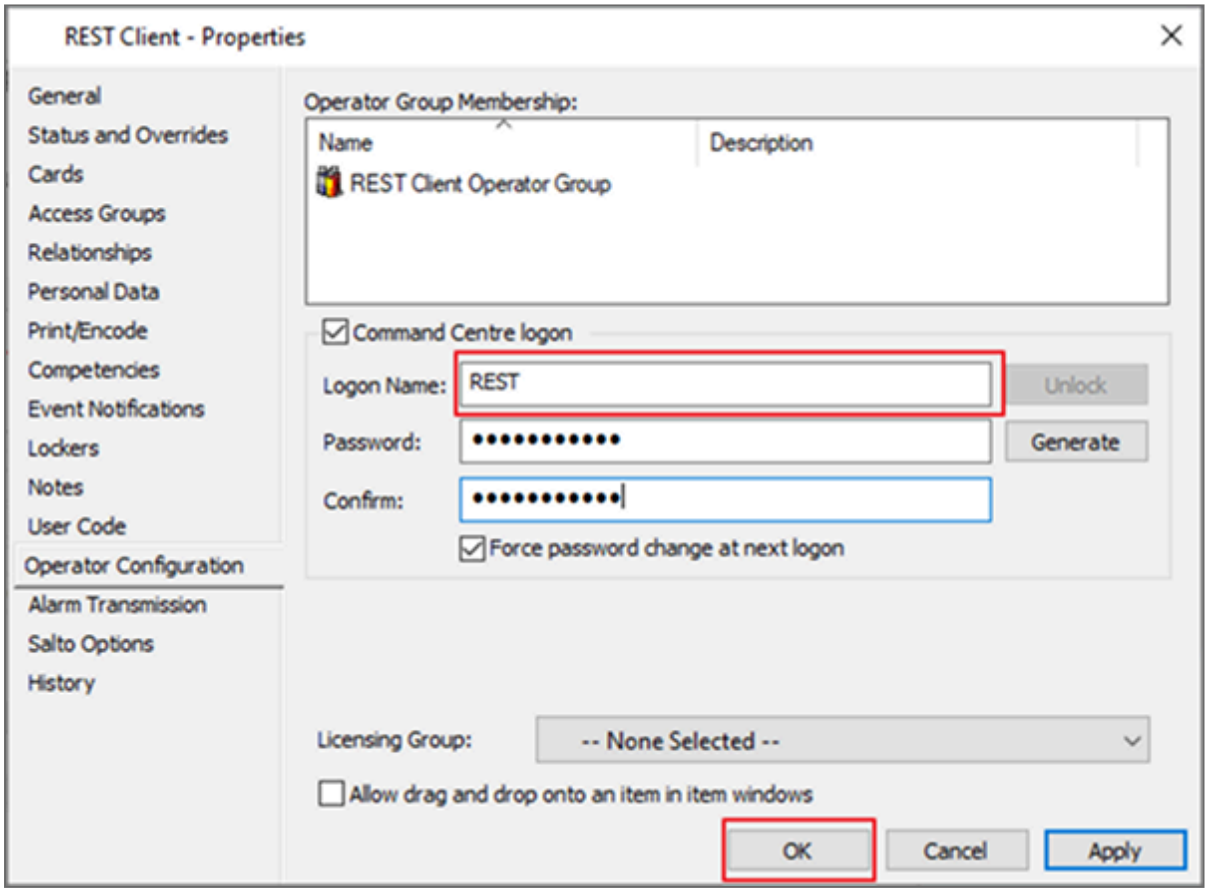


14. **Haz clic** en la pestaña **Operator Configuration** del lado izquierdo dentro de REST Client Properties. **Arrastra y suelta** el grupo de operadores REST Client que creamos desde Operator Group hasta Operator Group Membership.

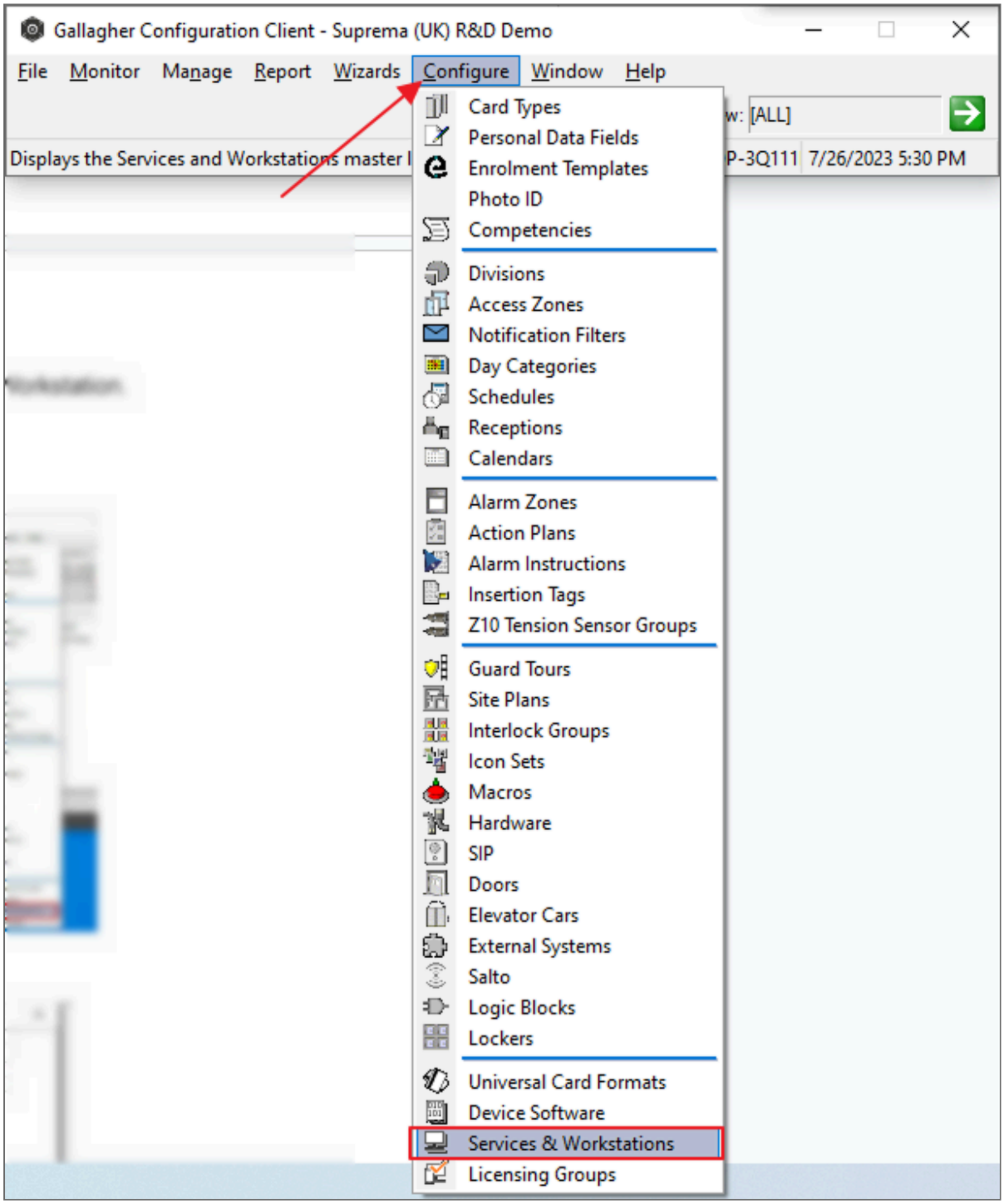
15. **Arrastra** REST Client Operator Group hasta Operator Group Membership, como en la imagen siguiente:



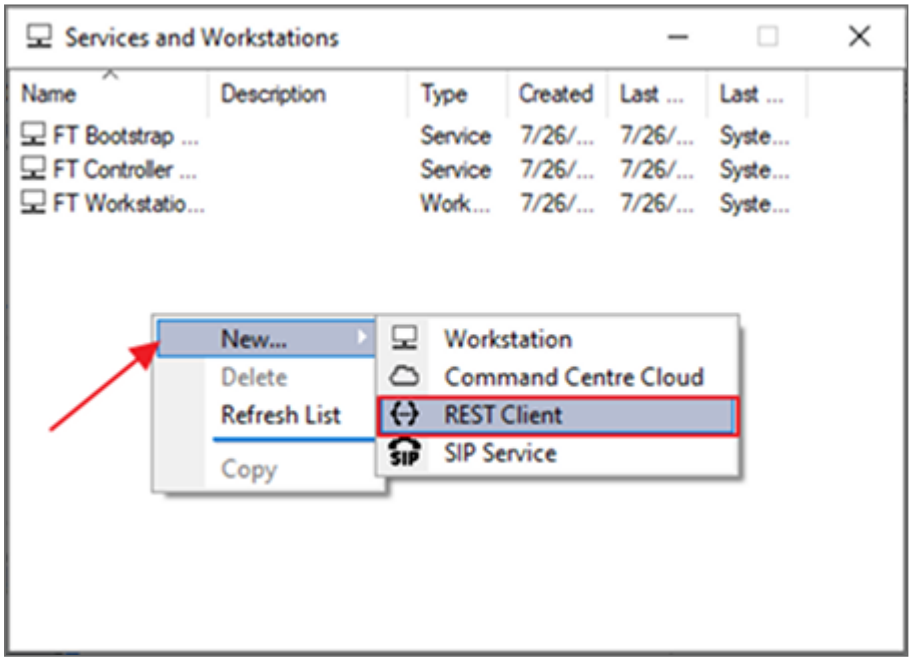
16. **Establece** el nombre de inicio de sesión en **REST** y **establece** la contraseña igual a la que configuramos para Gallagher Command Centre. **Haz clic en OK** y también **cierra** la ventana de Operator Group.



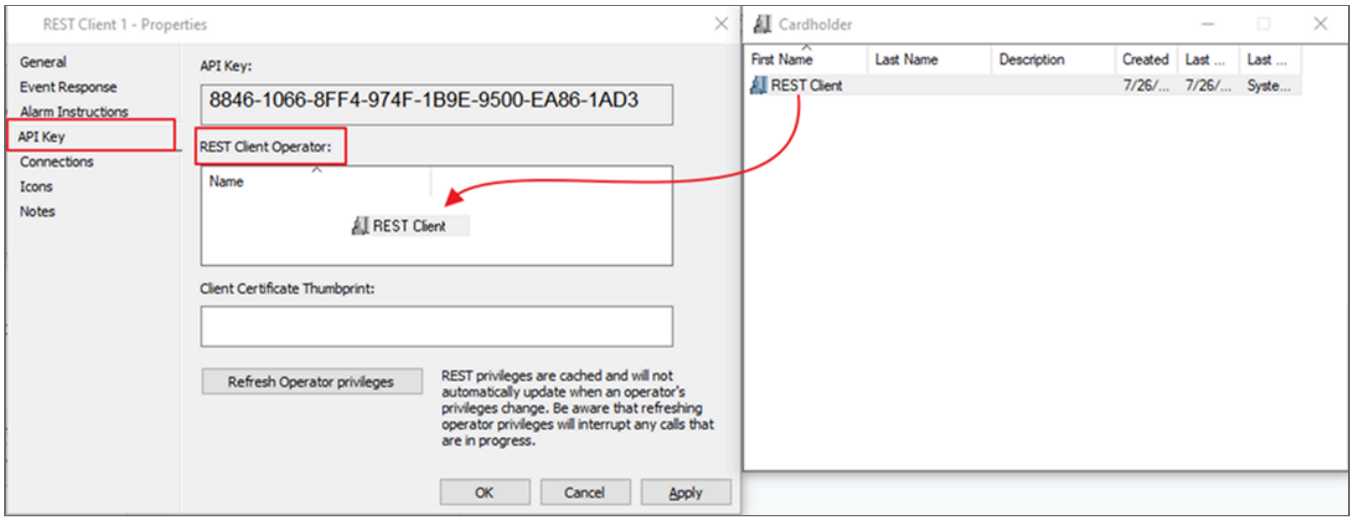
17. En **Configuration** Client, ve a Configure → Services & Workstations.



18. Ahora **haz clic derecho** en New → REST Client.

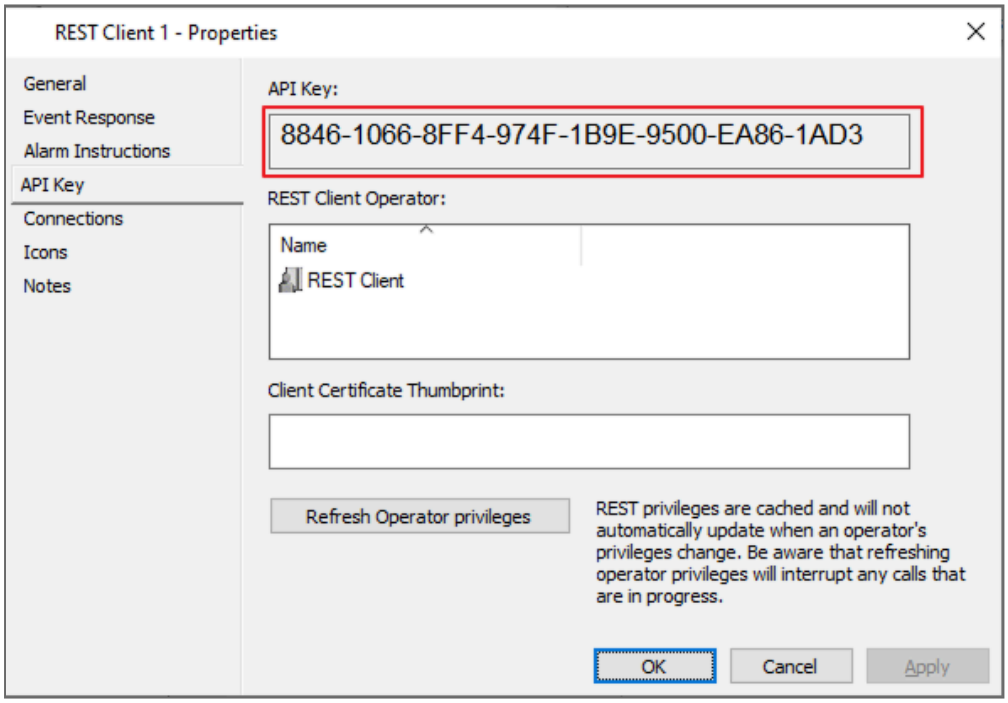


19. En la sección de clave de API, **arrastra y suelta** el REST Client de Cardholder a REST Client Operator. **Haz clic en Apply**. **Cierra** la ventana de Cardholder.



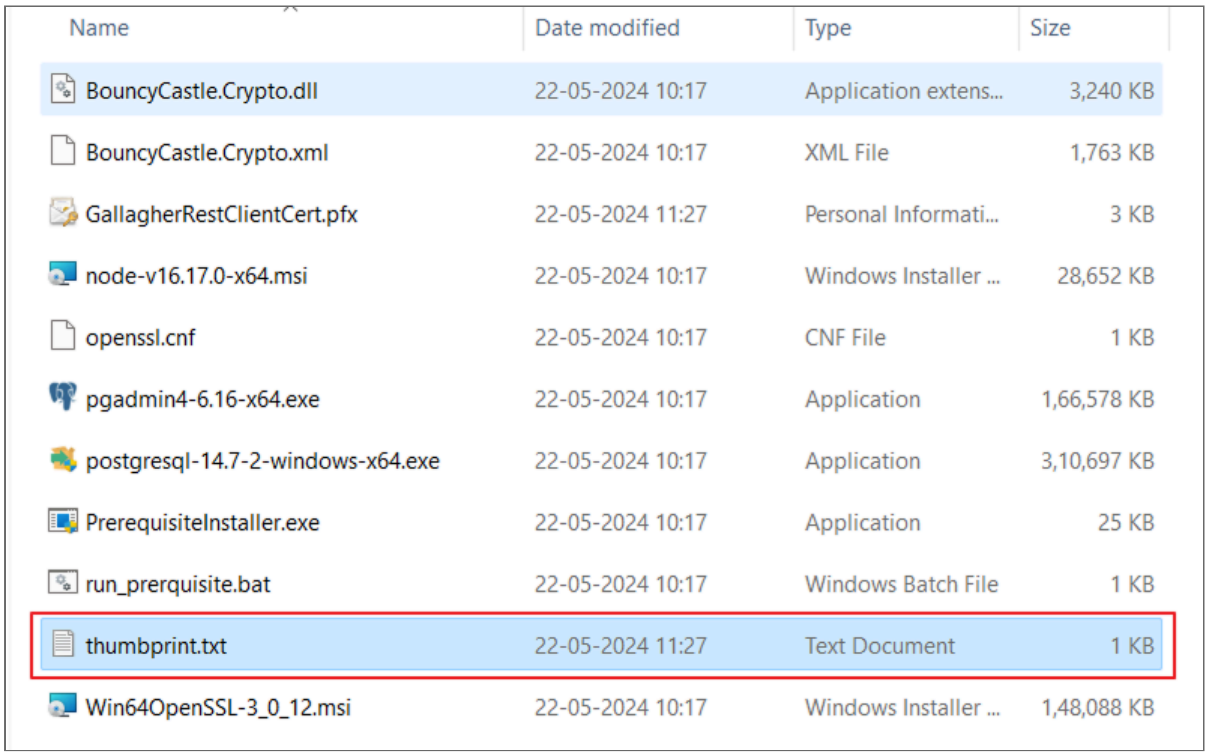
20. La clave de API de Gallagher está allí, en la sección de clave de API.

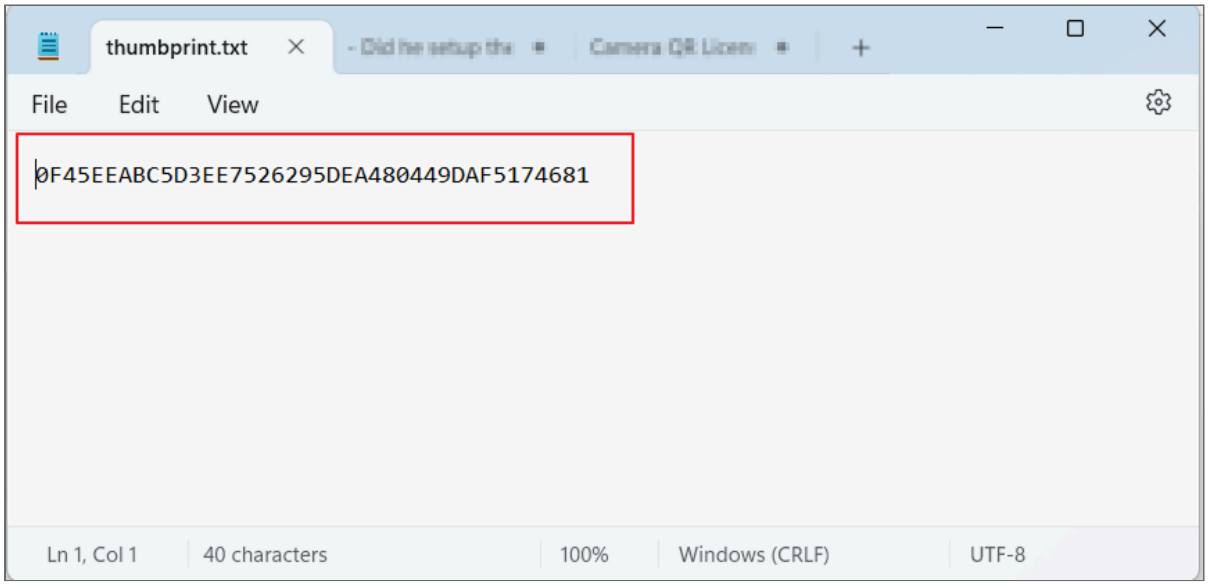
> **Información**
> Guarda la clave de API de Gallagher en un lugar seguro.



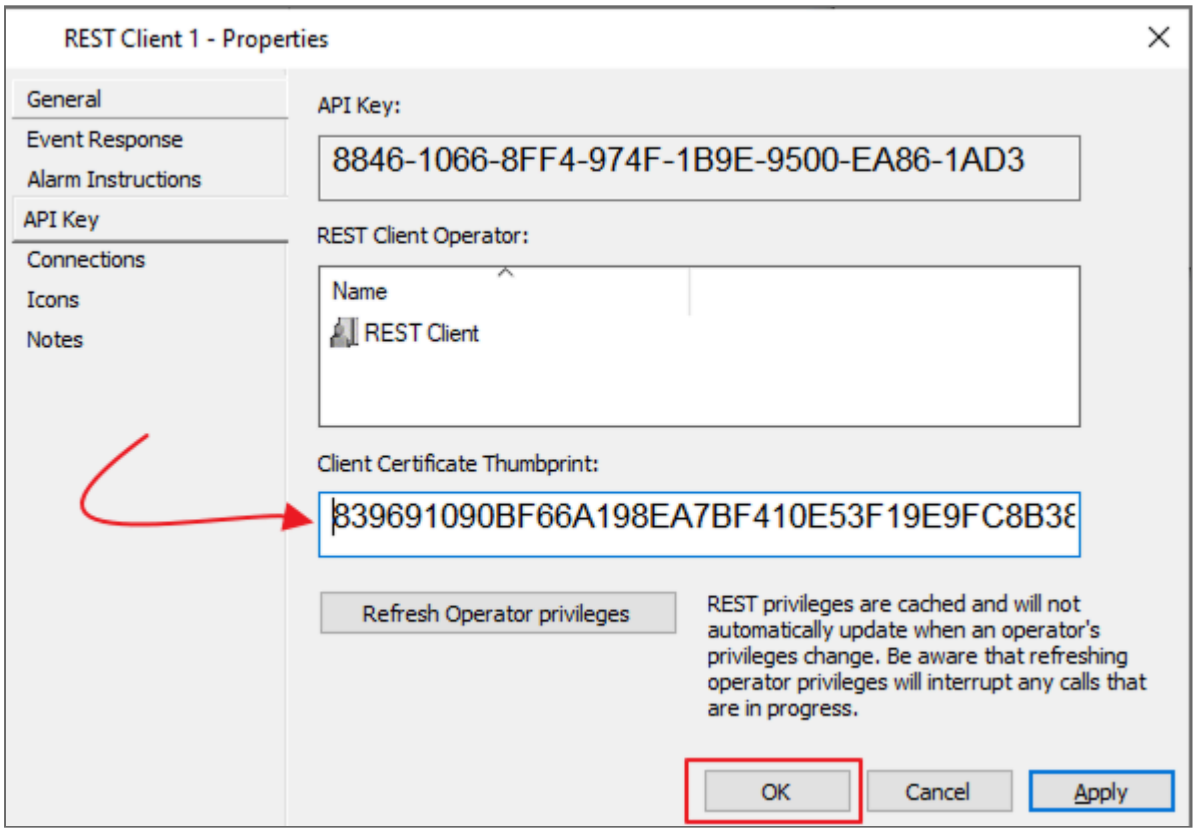
21. Para obtener el thumbprint, ve a `C:\Program Files\Suprema Integration with Gallagher\Prerequisites`, abre el archivo del thumbprint y copia el valor del thumbprint que contiene.

> **Información**
> Si falta el archivo del thumbprint. Si el thumbprint no se genera al ejecutar el archivo EXE.





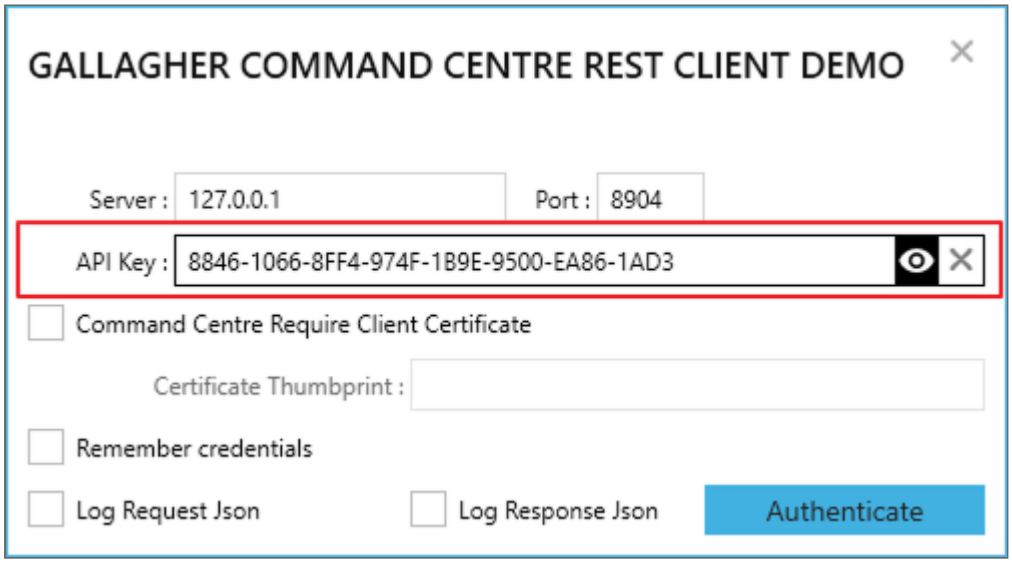
22. **Copie** el thumbprint y **pegue la clave del thumbprint del certificado del cliente** en la sección correspondiente. **Presione** el botón **OK** y también **cierre** Services and Workstations.



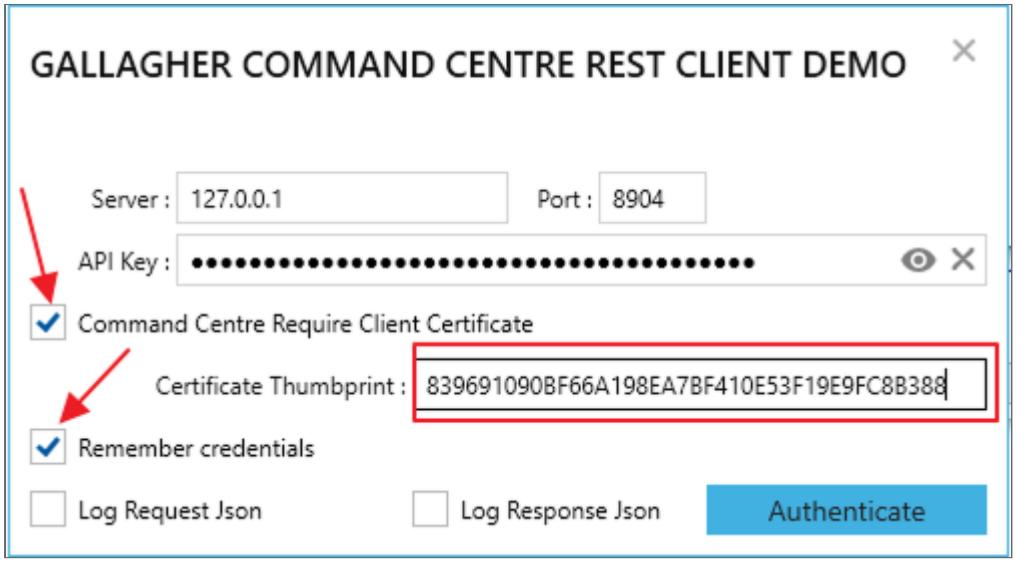
Verificar la clave de API de Gallagher

1. Ve a Command Centre iso → utilities → REST API → RestClient_v8.60.072 → win-x64 → RestClientDemo, **muévelo** al escritorio y **abre** RESTClientDemo.exe.

2. **Ingresa** la clave de API de Gallagher como se muestra en la imagen.

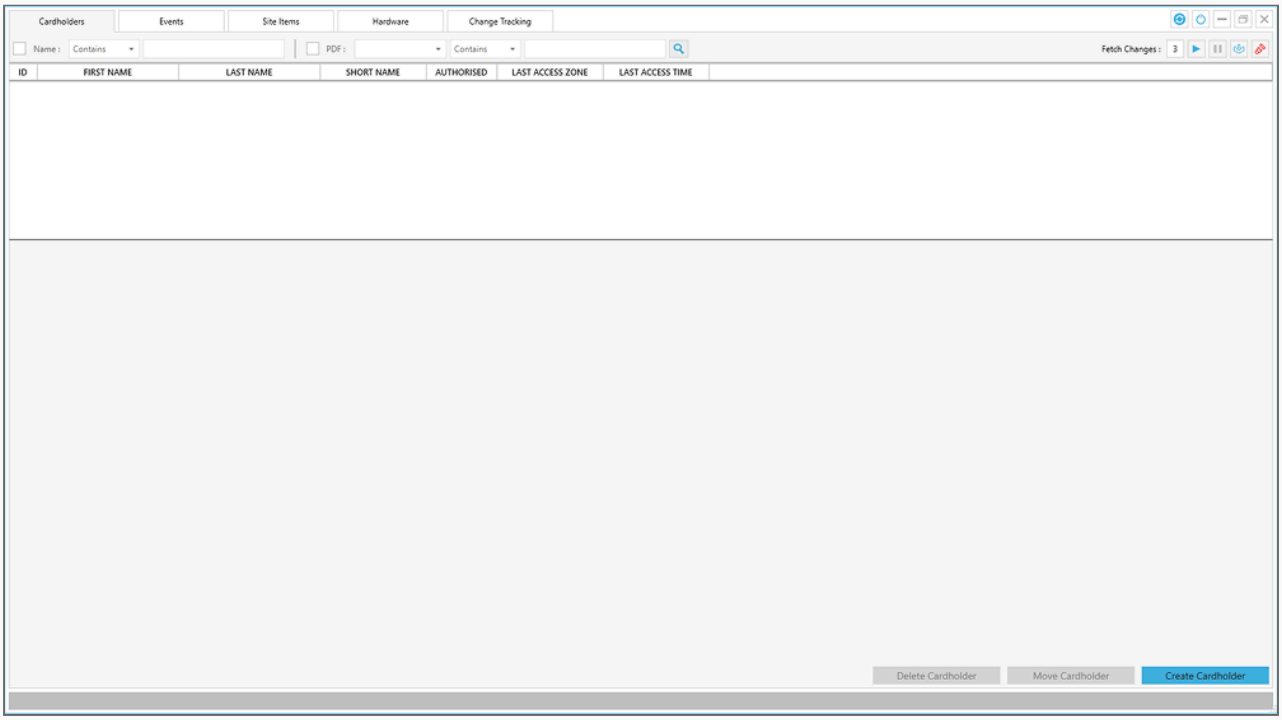


3. **Marca** Command Centre Requirement Client Certificate y completa Certificate Thumbprint; además, **marca** Remember credentials (Optional).



Información

Si hay un error, se mostrará en la terminal; de lo contrario, se abrirá una nueva pantalla como se muestra en la imagen siguiente. Después de la prueba, cierra esta ventana.



Configuración de hardware

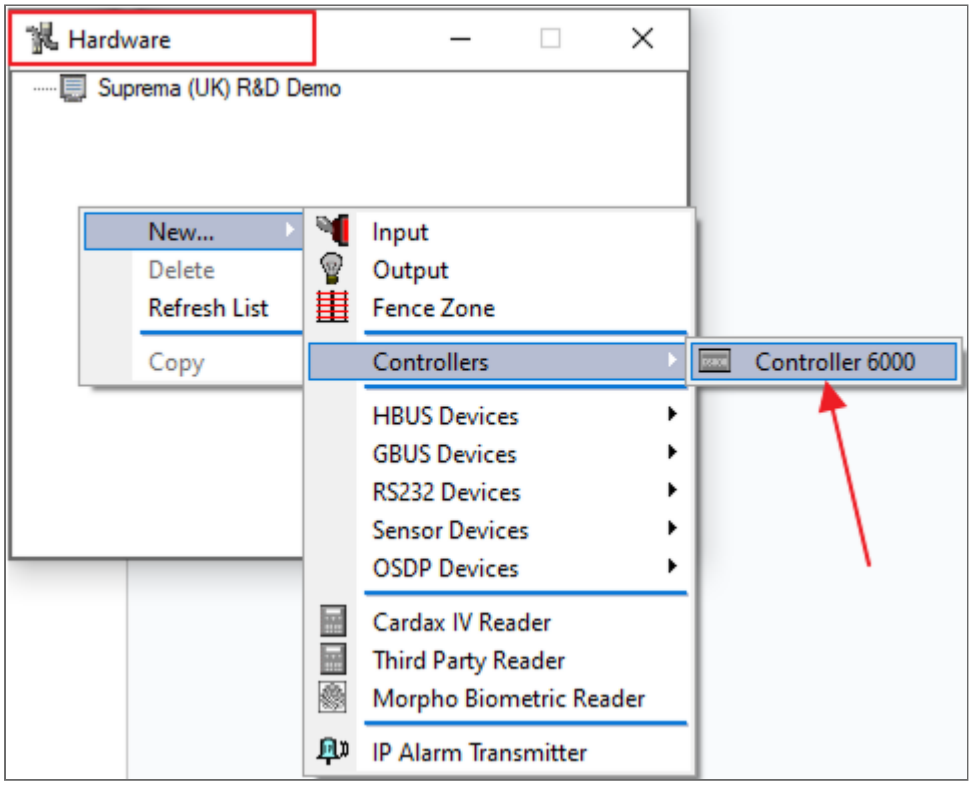
Información

- Salta a Configuración de BioStar 2 si el hardware ya se configuró.
- Usamos el controlador 6000 como referencia. Si tienes otro controlador, sigue los pasos según corresponda.

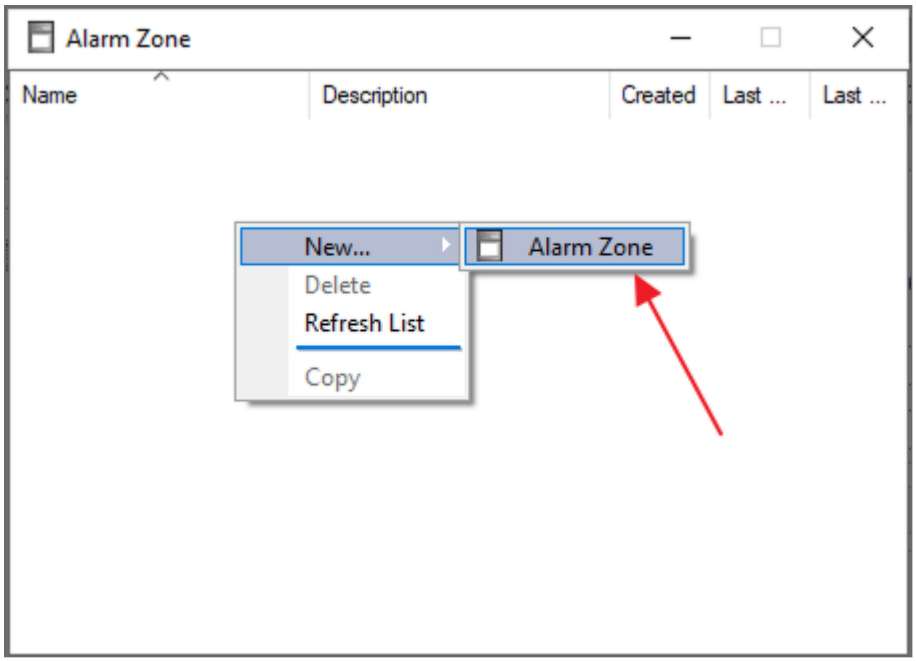
1. Primero, debemos crear el controlador 6000 (o cualquier otro controlador que tengas) para **conectarlo** al controlador Gallagher.

   Abre la ventana Gallagher Configuration Client y ve a Configure → Hardware.

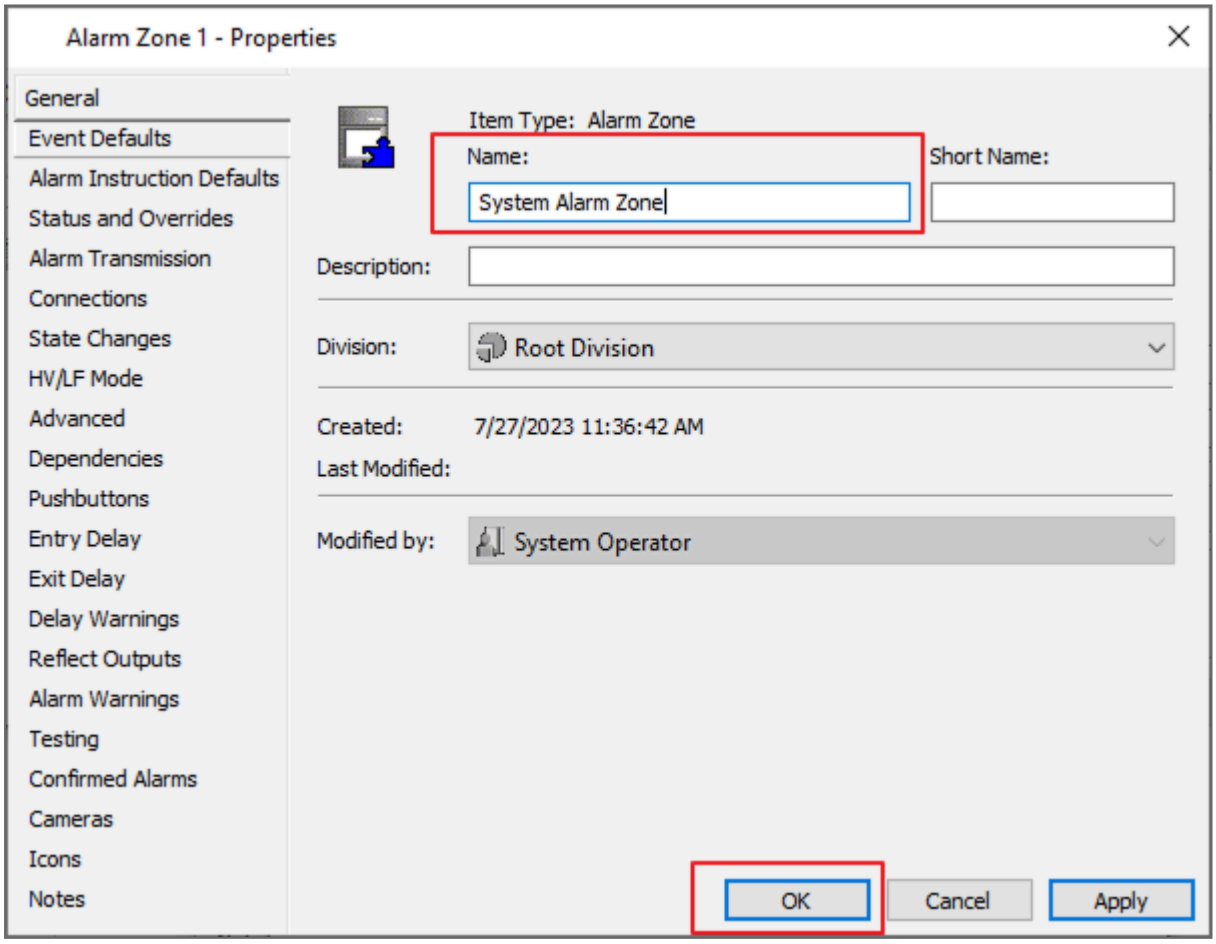
2. En la ventana de hardware, **haz clic derecho** y luego **New → Controllers → Controller 6000** (si tienes un controlador diferente, aparecerá aquí) y **presiona apply**. Esto creará un controlador en hardware.



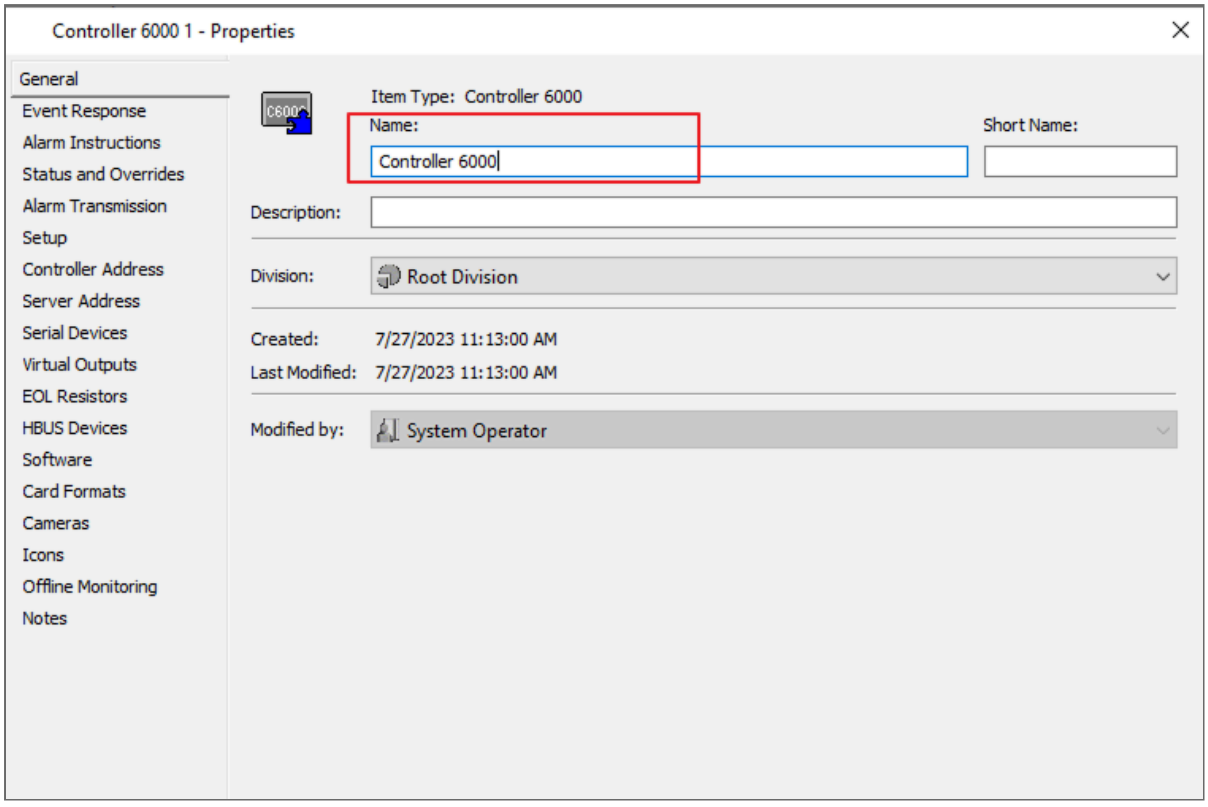
3. Luego **regresa** a Gallagher Configuration Client y ve a configure → Alarm Zones. Después, **haz clic derecho** para crear una nueva zona de alarma.



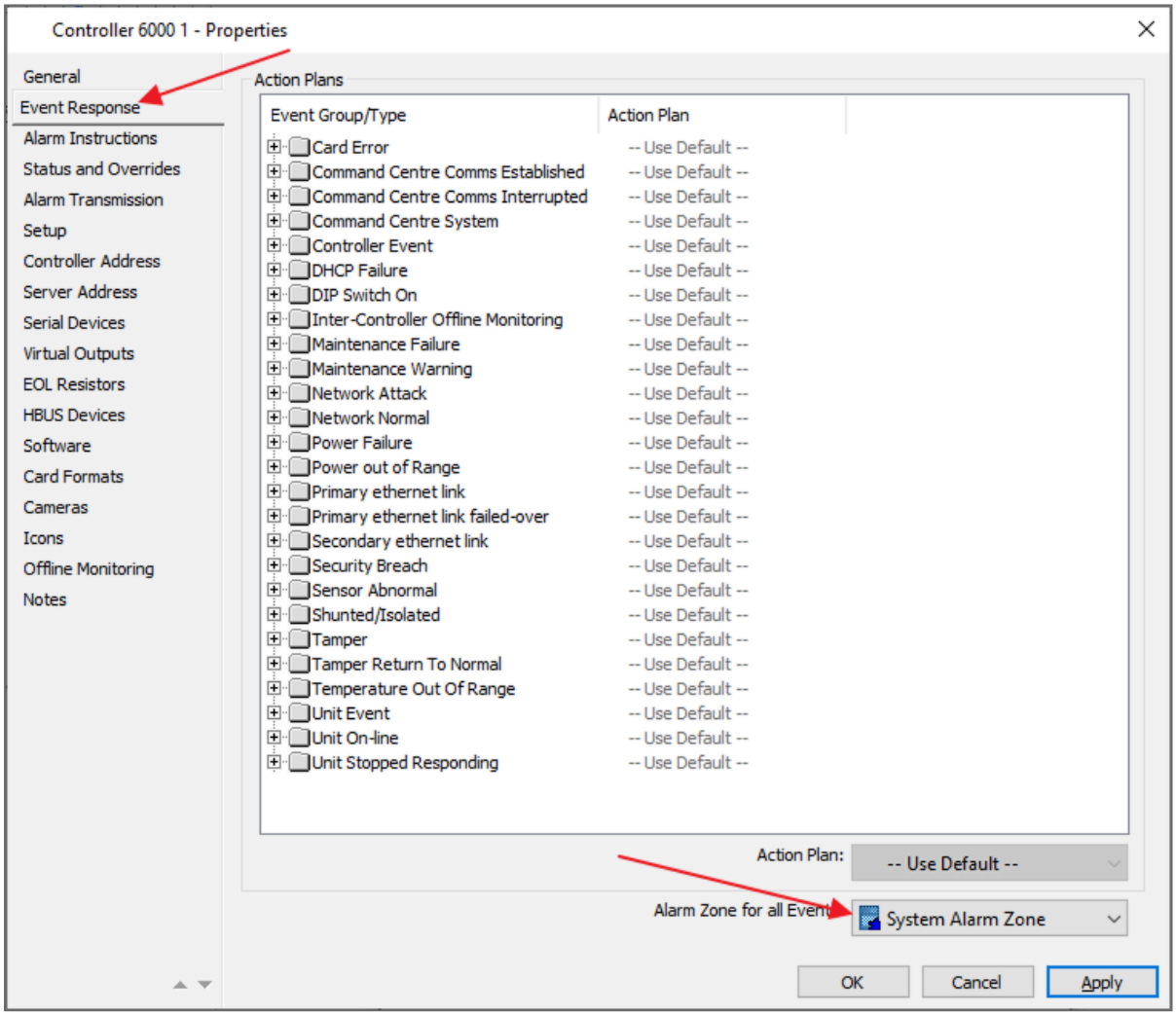
4. Para configurar la zona de alarma en General settings, cambia el nombre a **System Alarm Zone** y **presiona** el botón **OK**.



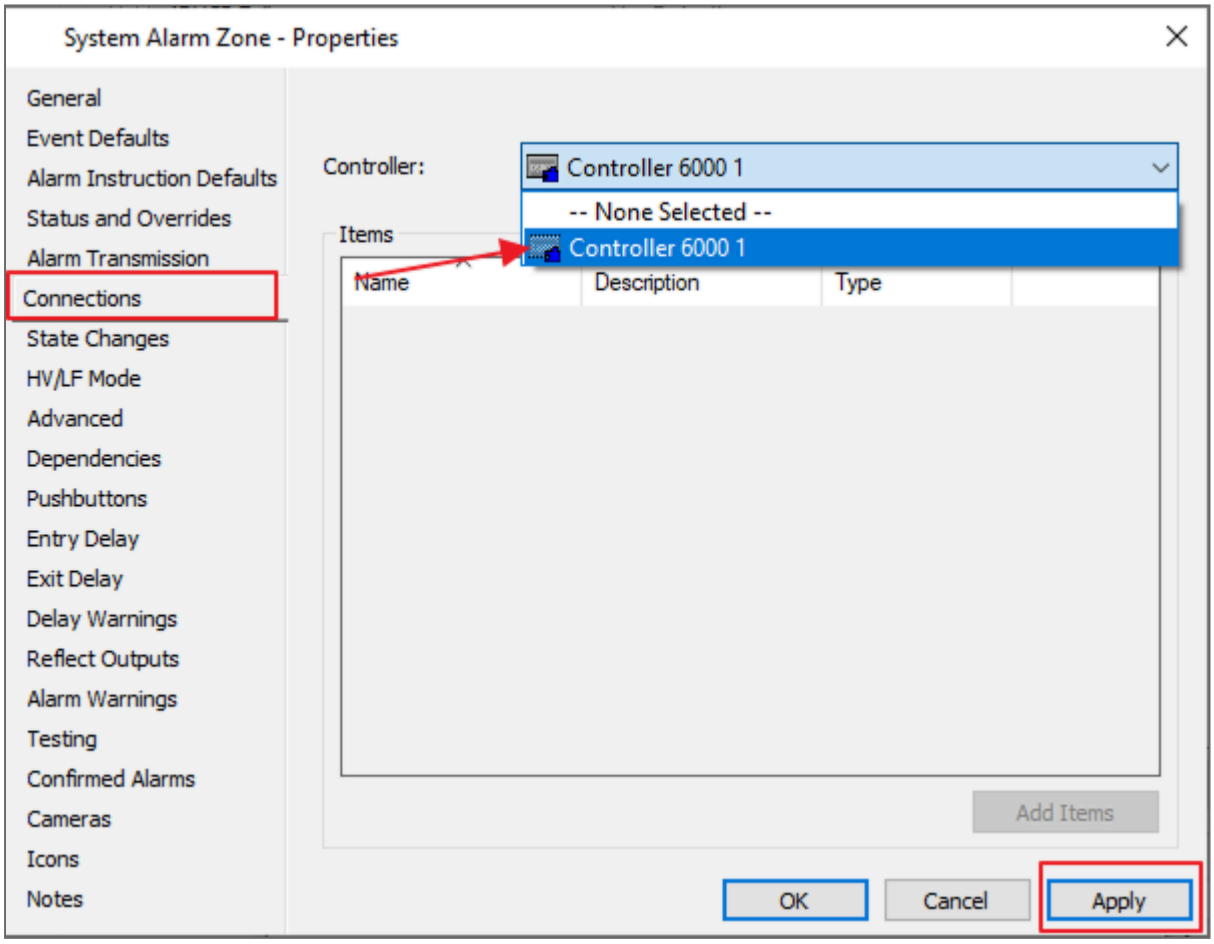
5. Configuremos el Controller 6000. En la configuración general, **establece** el nombre como **Controller 6000** (usa el mismo nombre que tu controlador).



6. Ahora **ve** a Event Response y selecciona Alarm Zone para todos los eventos y selecciona **System Alarm Zone**. Luego **presiona** el botón **Apply**.

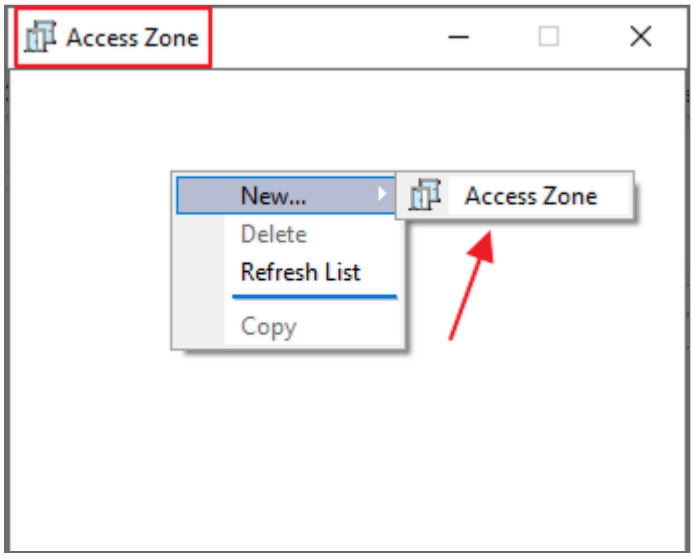


Ahora ve a System Alarm Zone Properties y **selecciona** Connections; en el menú desplegable del controlador, **elige Controller 6000**. **Presiona** el botón **OK** y **cierra** la ventana de Alarm Zone.

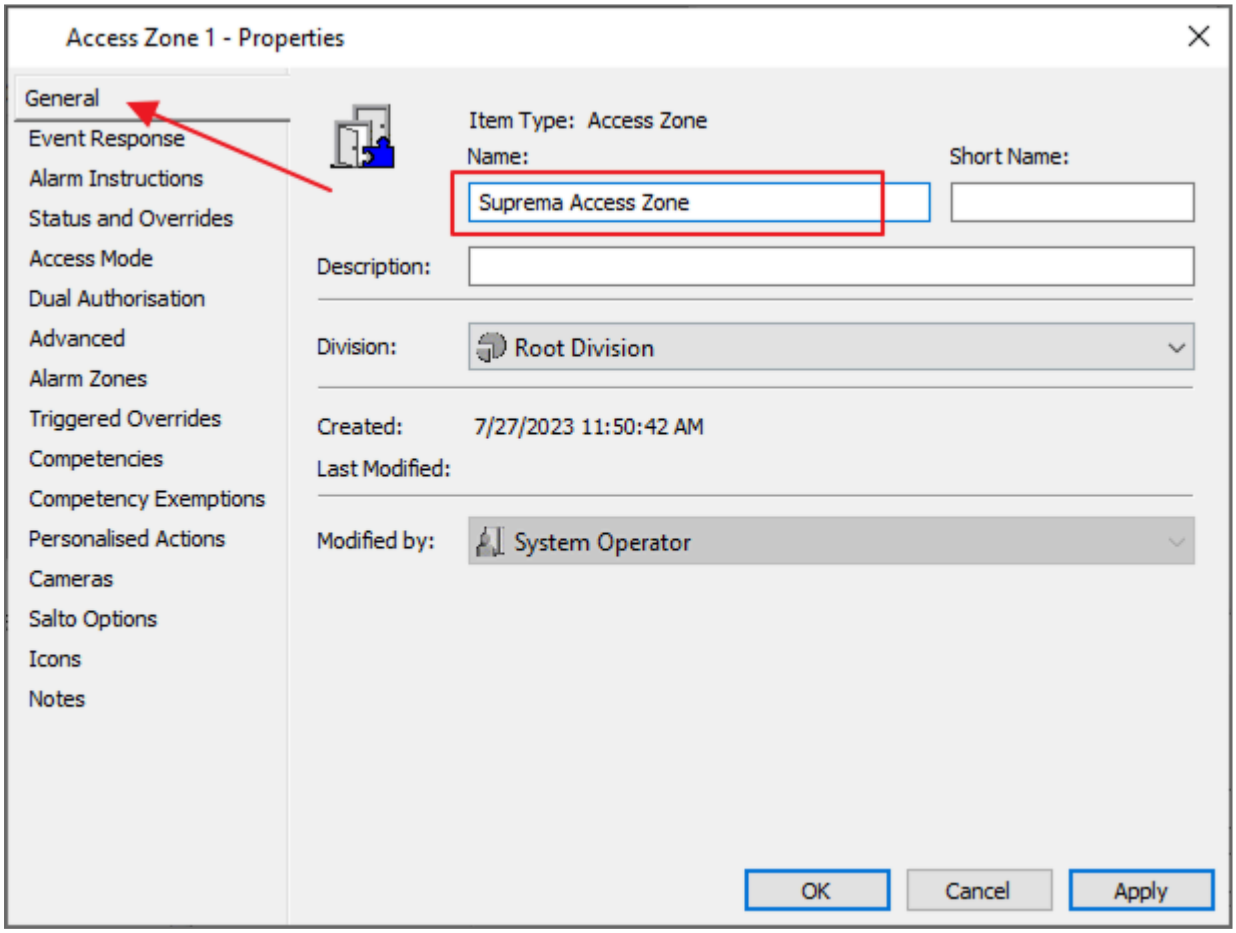


7. Ahora debemos **crear** una Access Zone en configure.

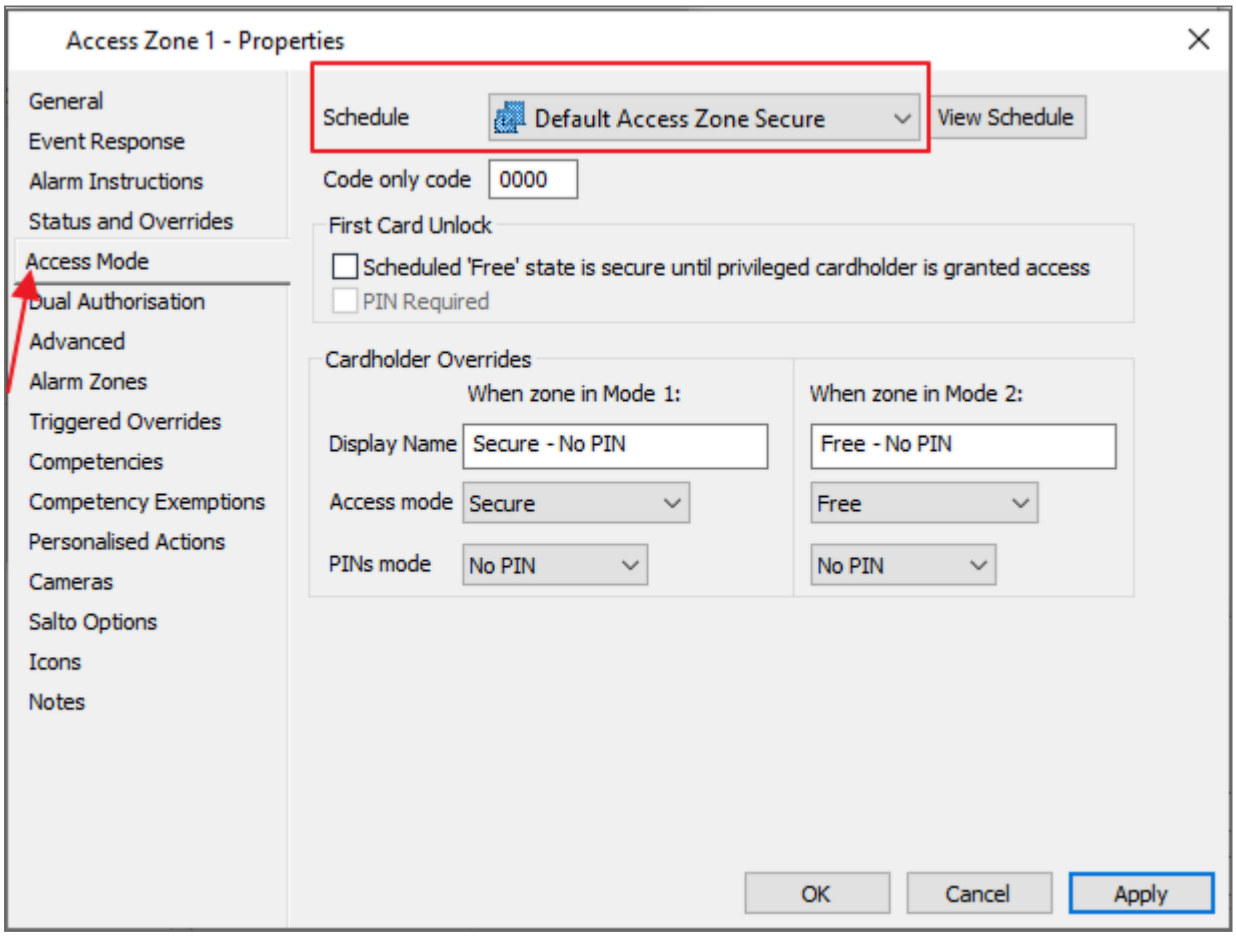
   Ve a Access Zone y se abrirá la ventana. Ahora **haz clic derecho** en la ventana de Access Zone y **selecciona** New → luego **haz clic** en Access Zone, y se creará una access zone.



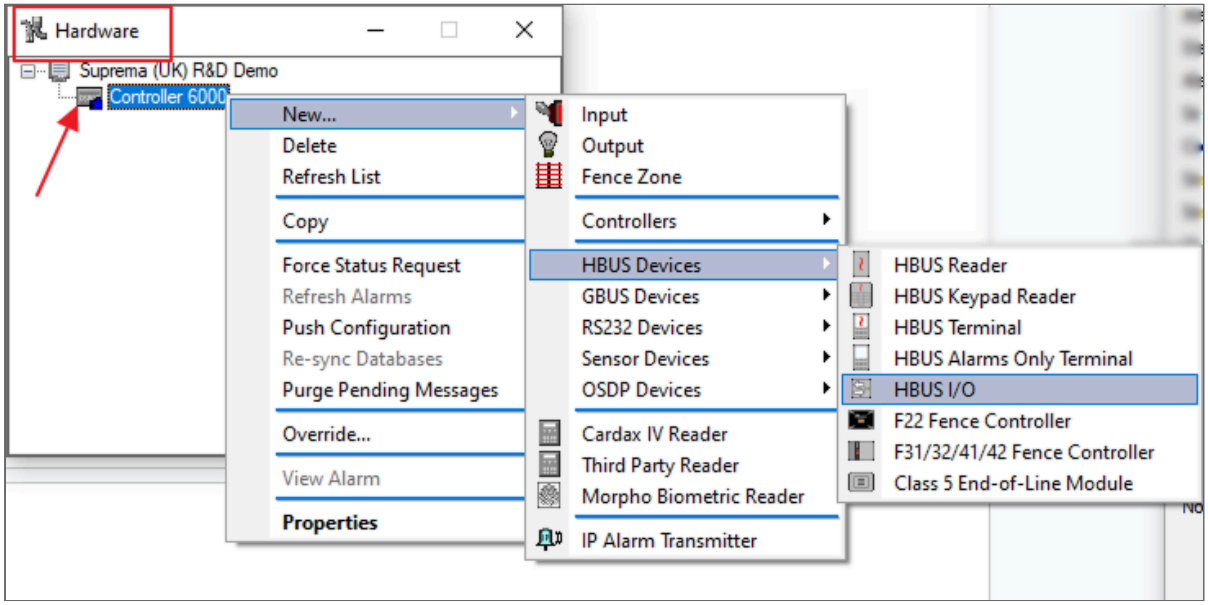
8. **Abre** las propiedades de Access Zone que creamos en General Setting. Luego **establece** el nombre como **Suprema Access Zone**.



9. **Ve** a la pestaña Access Mode. **Selecciona** Schedule como Default Access Zone Secure y **presiona** el botón **OK**.

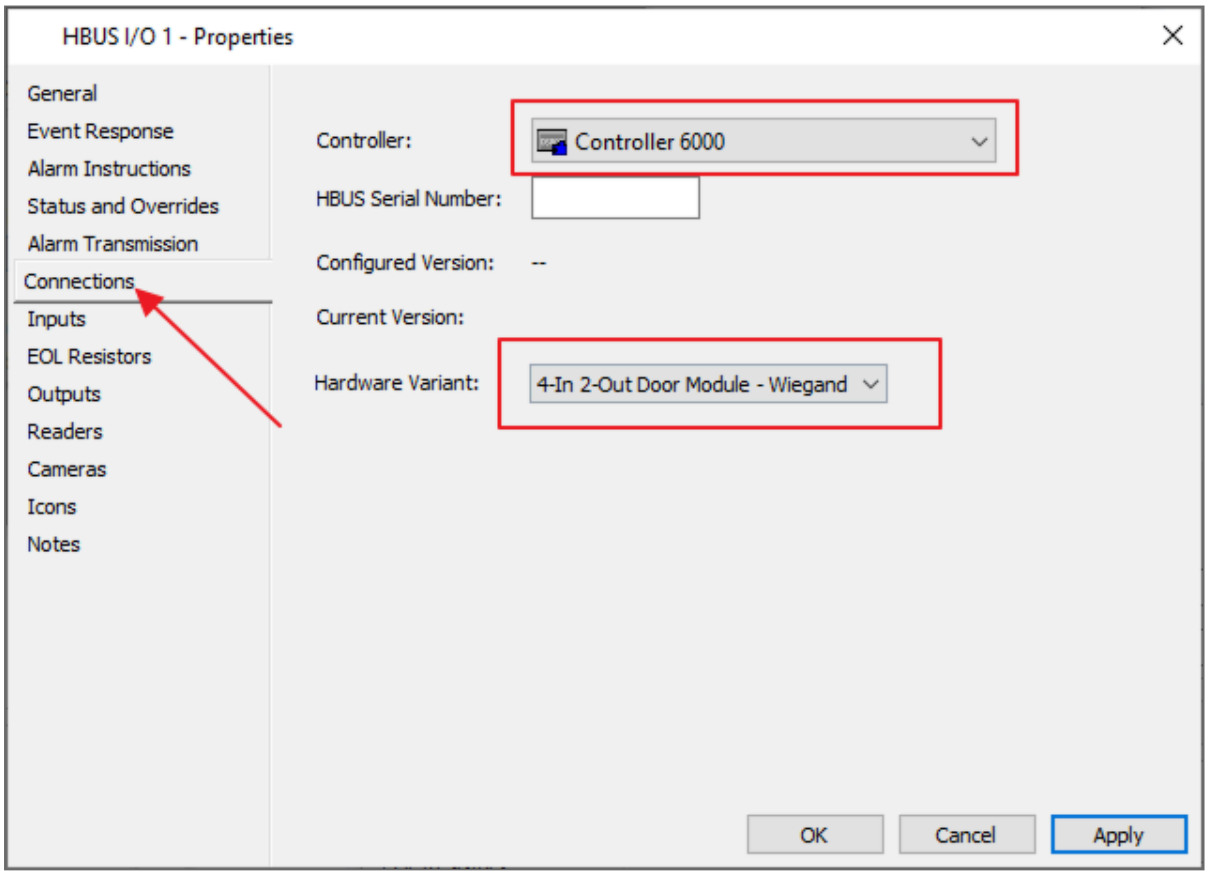


10. Ahora **ve** a la ventana de Hardware y luego **haz clic derecho** en Controller 6000. Selecciona New → HBUS Devices → HBUS I/O. Este paso creará HBUS dentro del controlador.

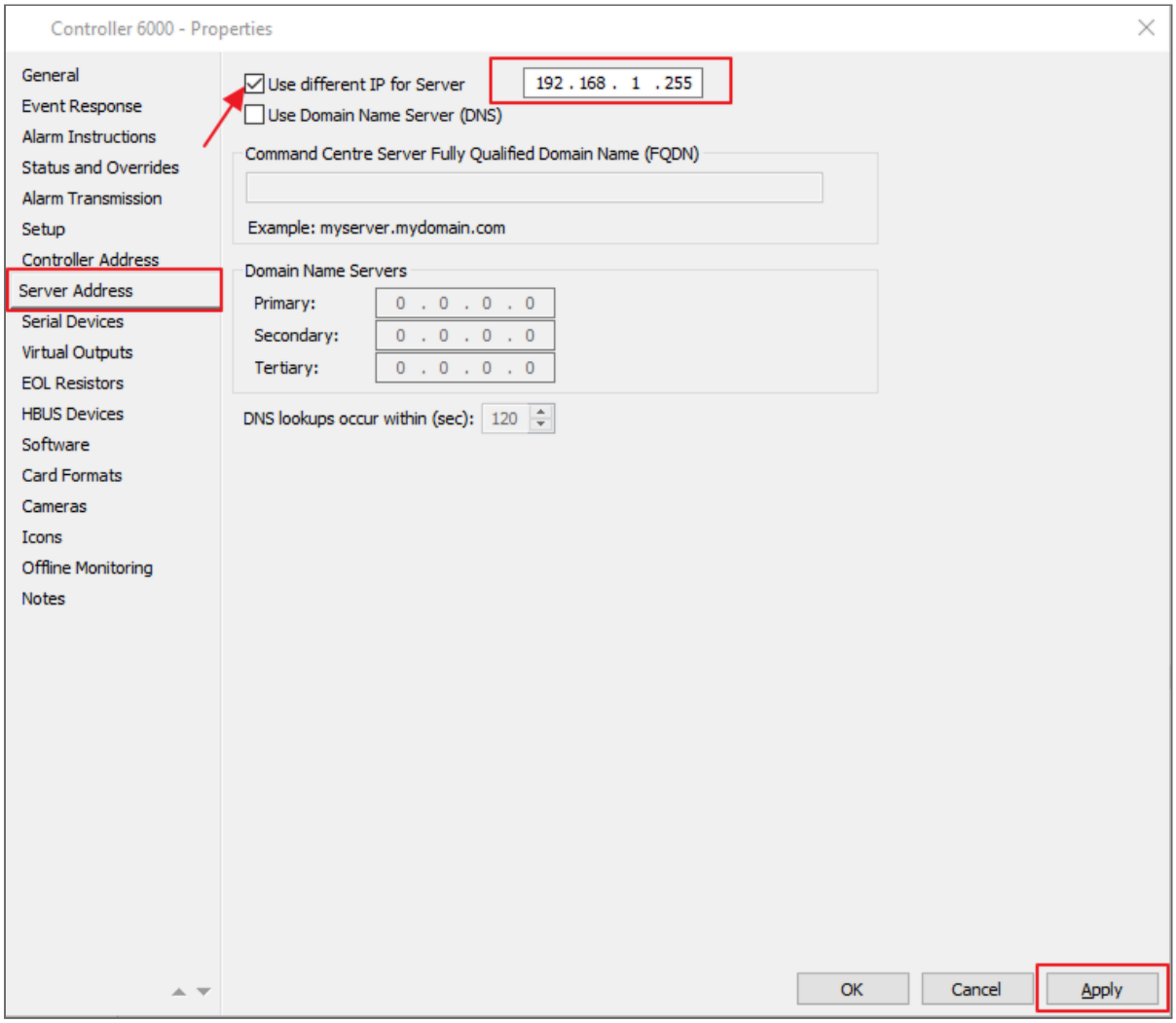


11. Configuremos el HBUS que creamos; para editar las propiedades, **haz doble clic** en él. En la configuración general, **establece** el nombre como **HBUS I/O Wiegand Module (Suprema)**.

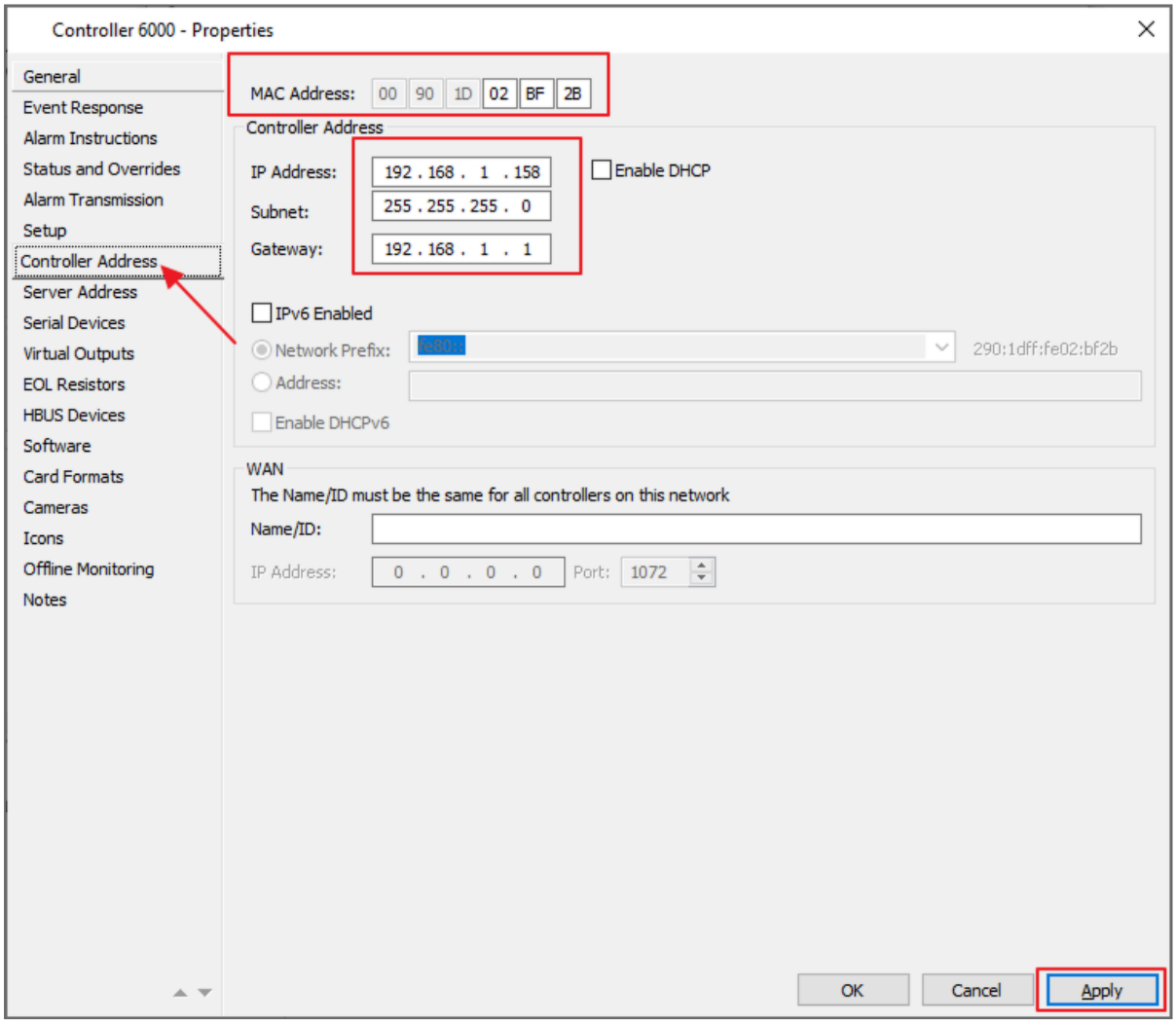
    Ve a la pestaña Connections y **elige** Controller como Controller 6000, establece Hardware Variant como 4 in 2 out y luego presiona el botón **OK**.



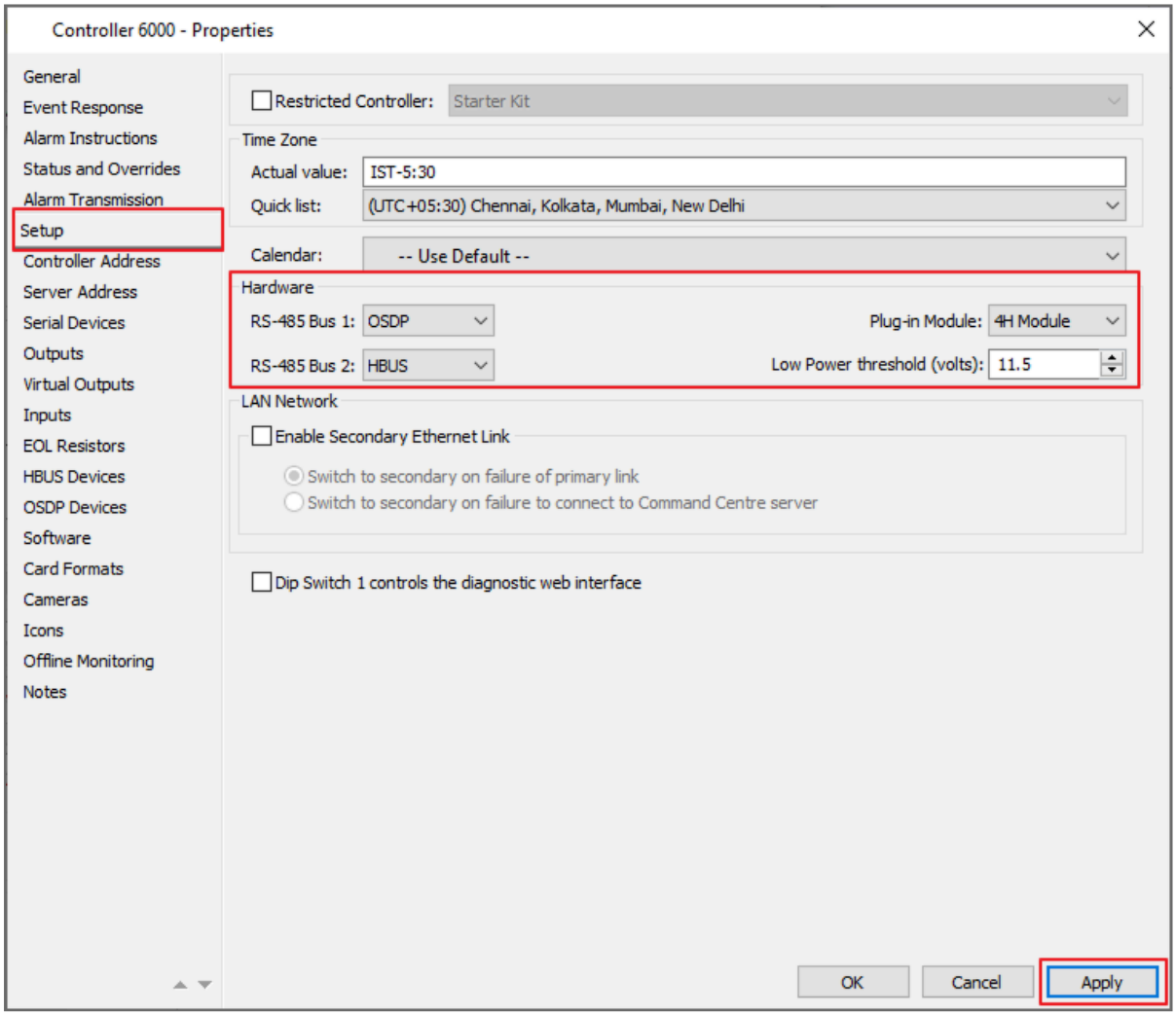
12. Para conectar tu controlador Gallagher al sistema, **abre** las propiedades de Controller 6000 y **haz clic** en la pestaña Server Address. Marca use different IP for the server y escribe la dirección IP de tu PC/servidor. Luego **presiona** el botón **Apply**.



13. En la configuración de Controller Address, establece la dirección MAC de tu controlador (consulta tu controlador C6000). Además, **establece** la dirección IP asignada para el controlador, la subred y la puerta de enlace. **Presiona** el botón **Apply**.



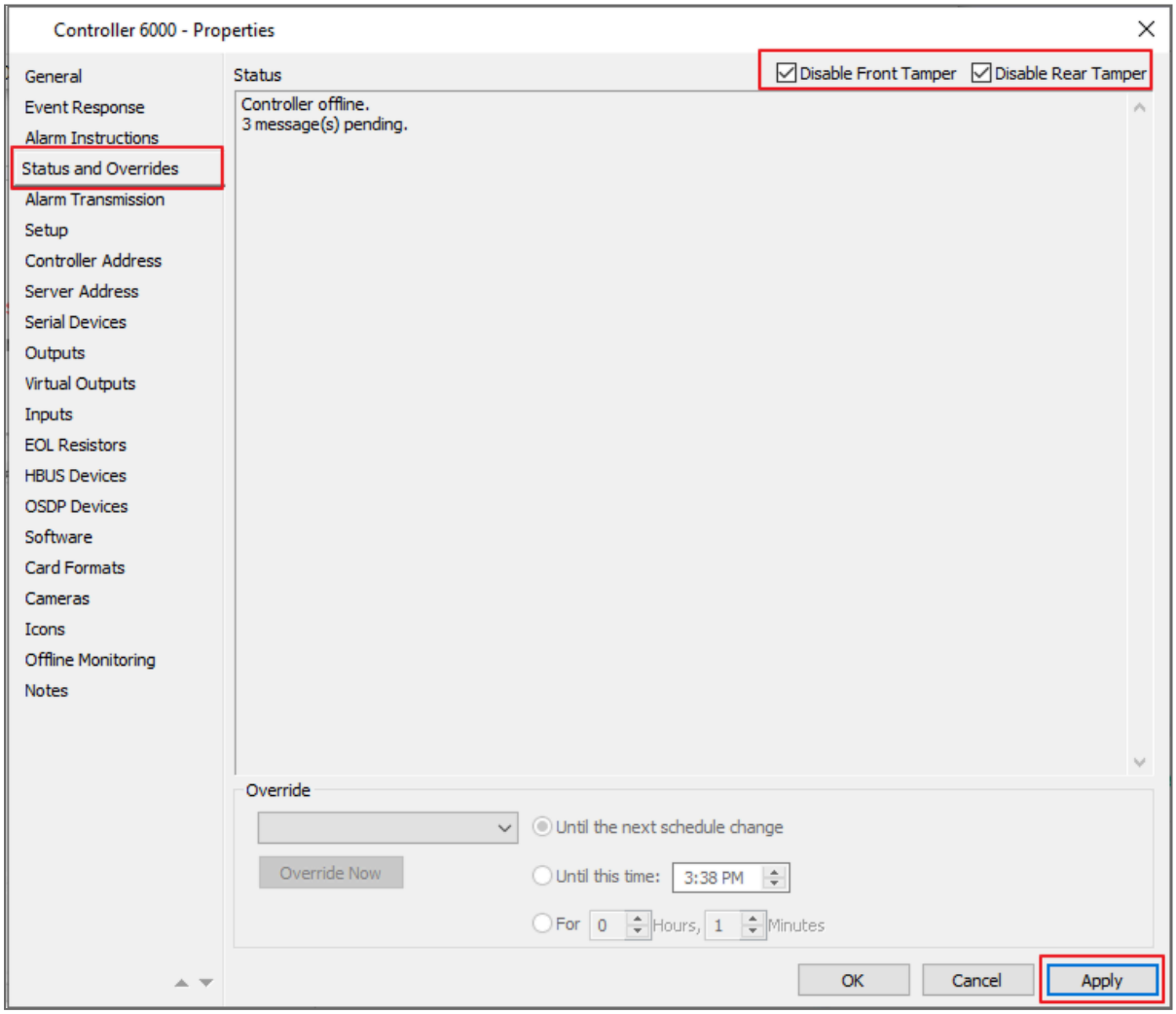
14. En la pestaña Setup, establece Plug in Module como **4H Module** (elige según tu controlador) y en Hardware RS485 Bus 1 como **OSDP** y RS485 Bus 2 como **HBUS**; luego presiona Apply.



Información

Tu configuración puede variar según tus dispositivos y componentes Gallagher.

15. En las opciones Status and Overrides, **marca** las dos casillas Disable Front Tamper y DisableRear Tamper.



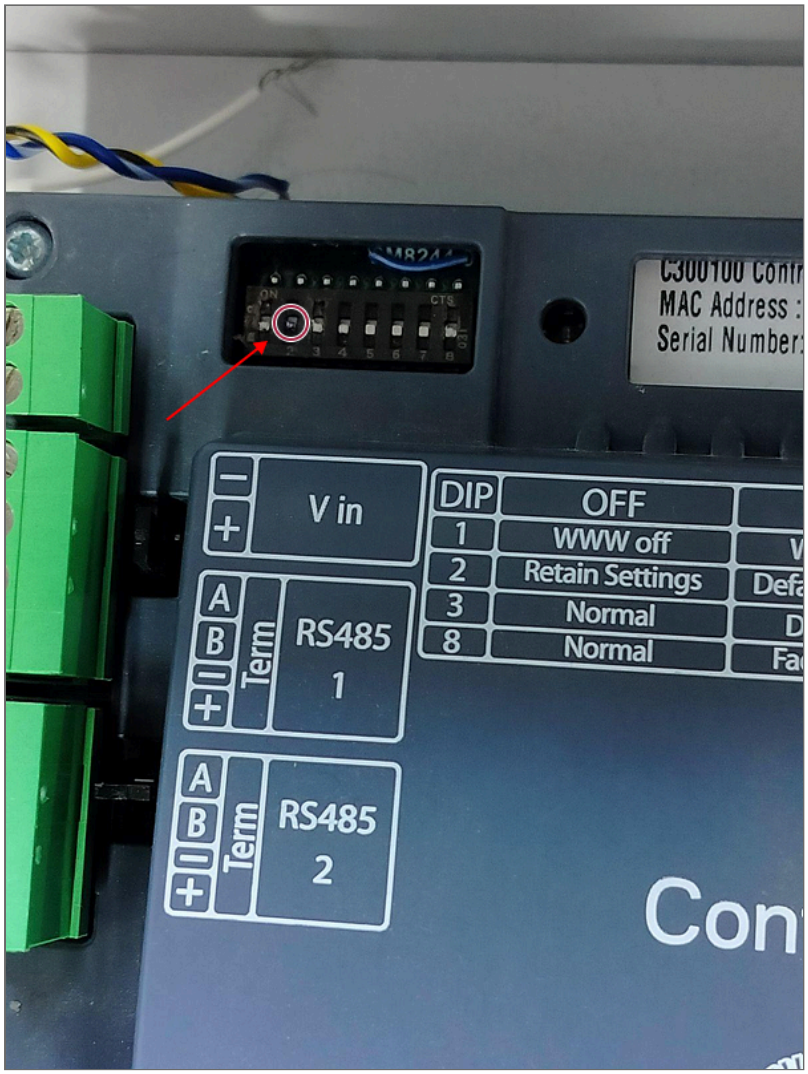
16. Para conectar tu controlador al sistema, **apaga** el controlador y espera hasta que la luz roja se apague. Luego **enciende** el segundo interruptor desde la izquierda.

> **Información**
> Antes de realizar este paso, asegúrate de que el firewall de tu PC esté desactivado.



17. Cuando el estado del controlador vuelva a normal, **apaga** el segundo interruptor (baja el segundo interruptor DIP).

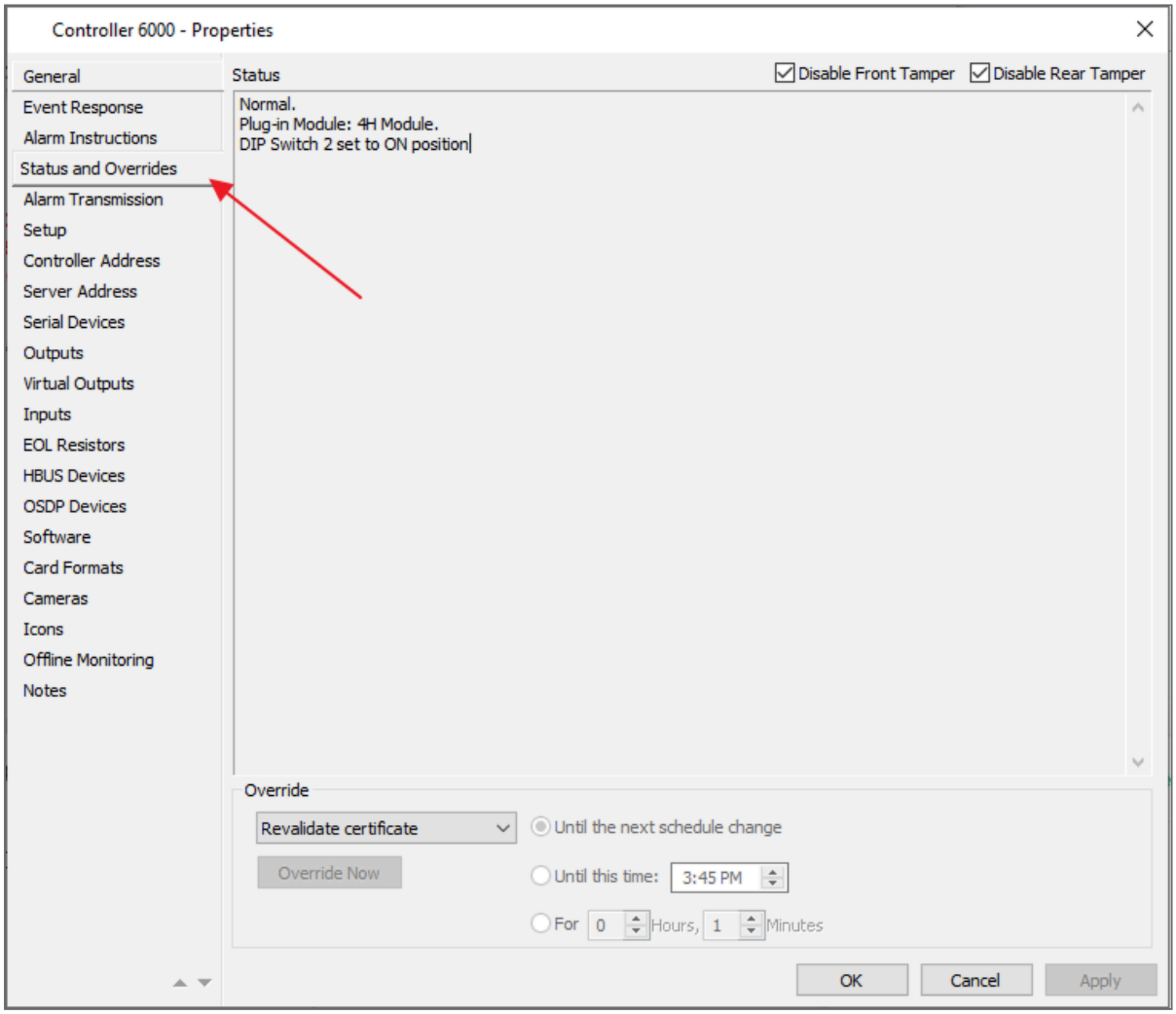
> **Información**
> Una vez que el controlador esté en línea y en estado normal, puedes apagar todos los interruptores DIP, incluido el 2.



Nota adicional: primer encendido y conexión de un controlador nuevo:

Solo necesitas activar el interruptor #2 cuando enciendas por primera vez un controlador nuevo y lo conectes a un servidor.

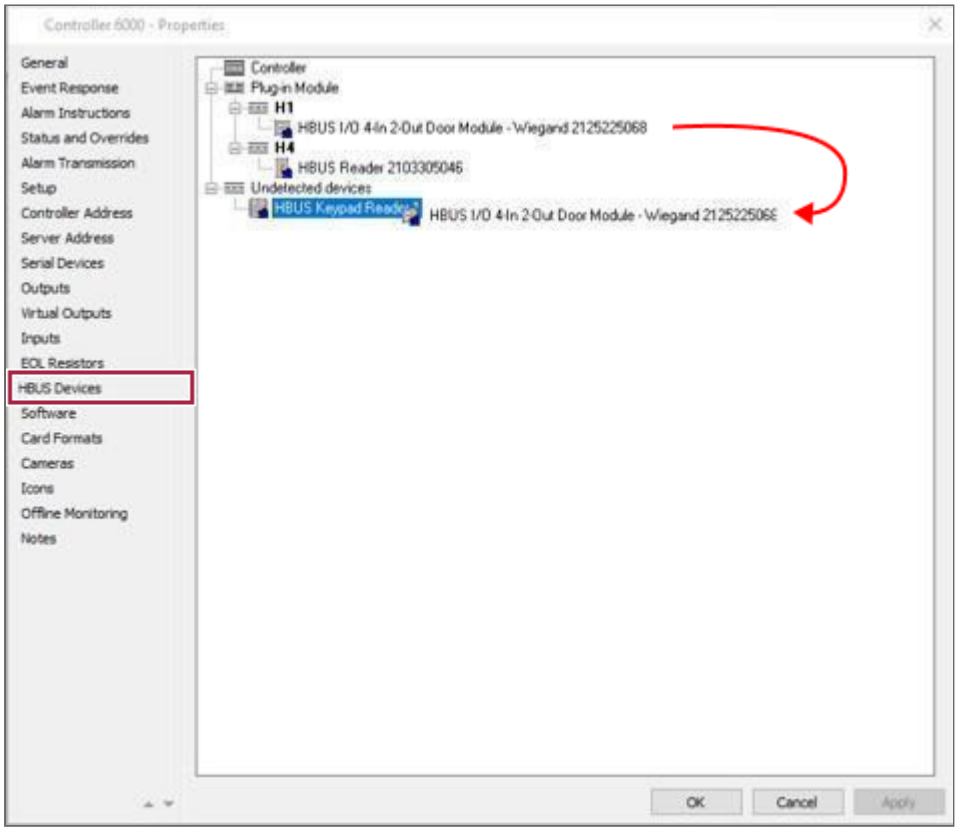
Además, el puente #2 puede usarse al realizar ciertos reinicios del controlador. Déjalo fijo si realizas actualizaciones en el controlador.



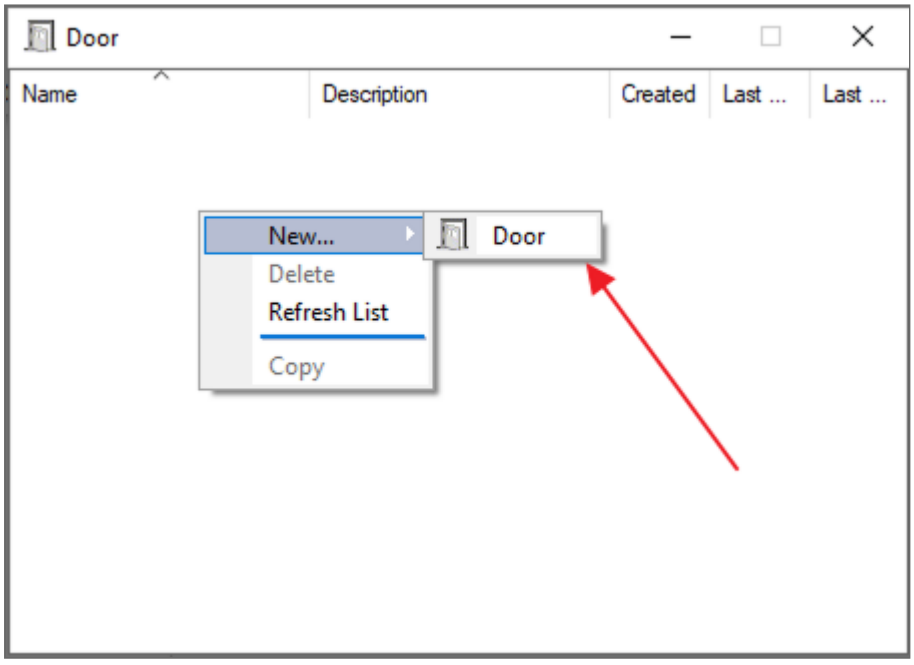
Información

Conecta dispositivos para acceder a HBUS en la configuración HBUS del controlador. (Para conectar dispositivos, consulta la configuración de BioStar 2.)

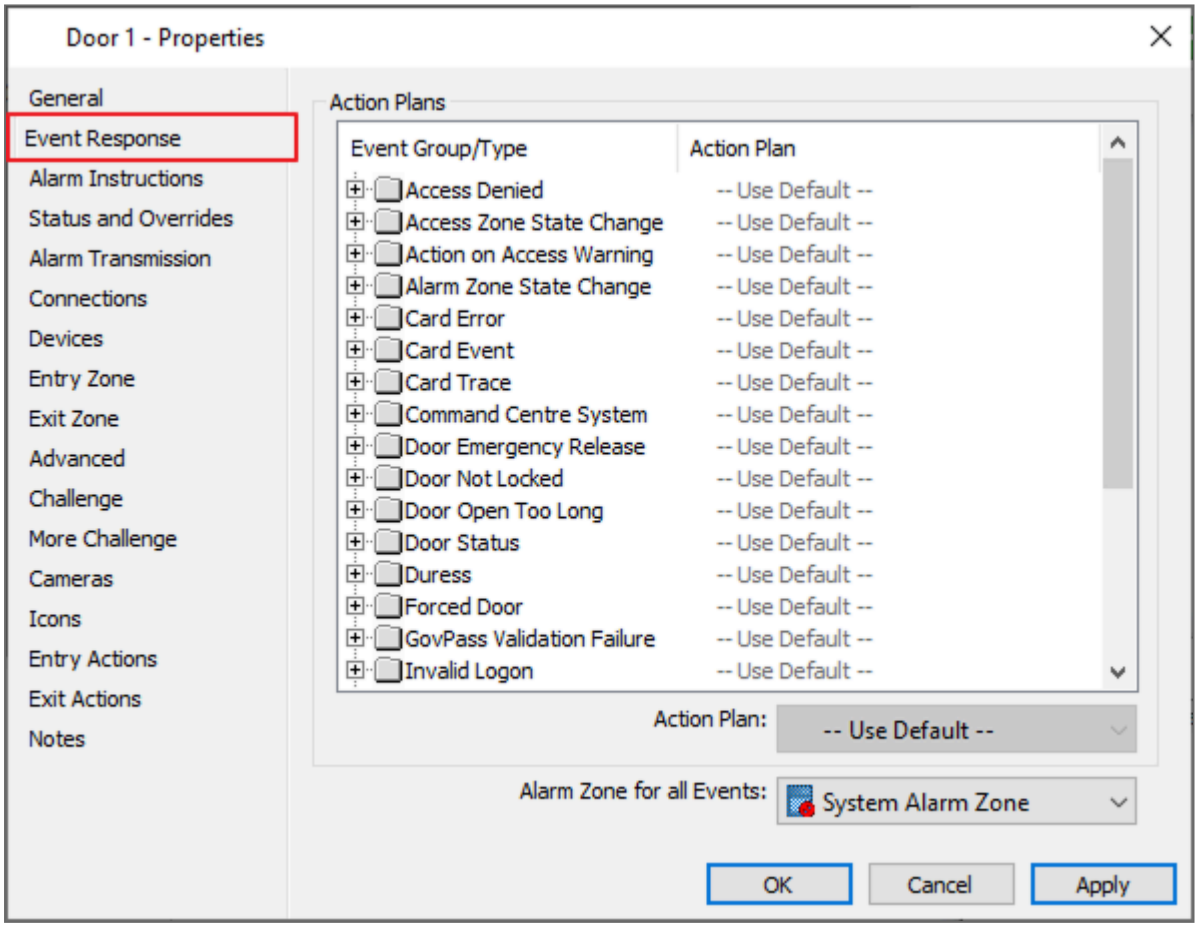
18. En la opción HBUS Devices de Controller 6000, **arrastra y suelta** el módulo HBUS I/O 4 in 2 Out - Wiegand desde **Plugin Modules** a **Undetected devices** HBUS I/O.



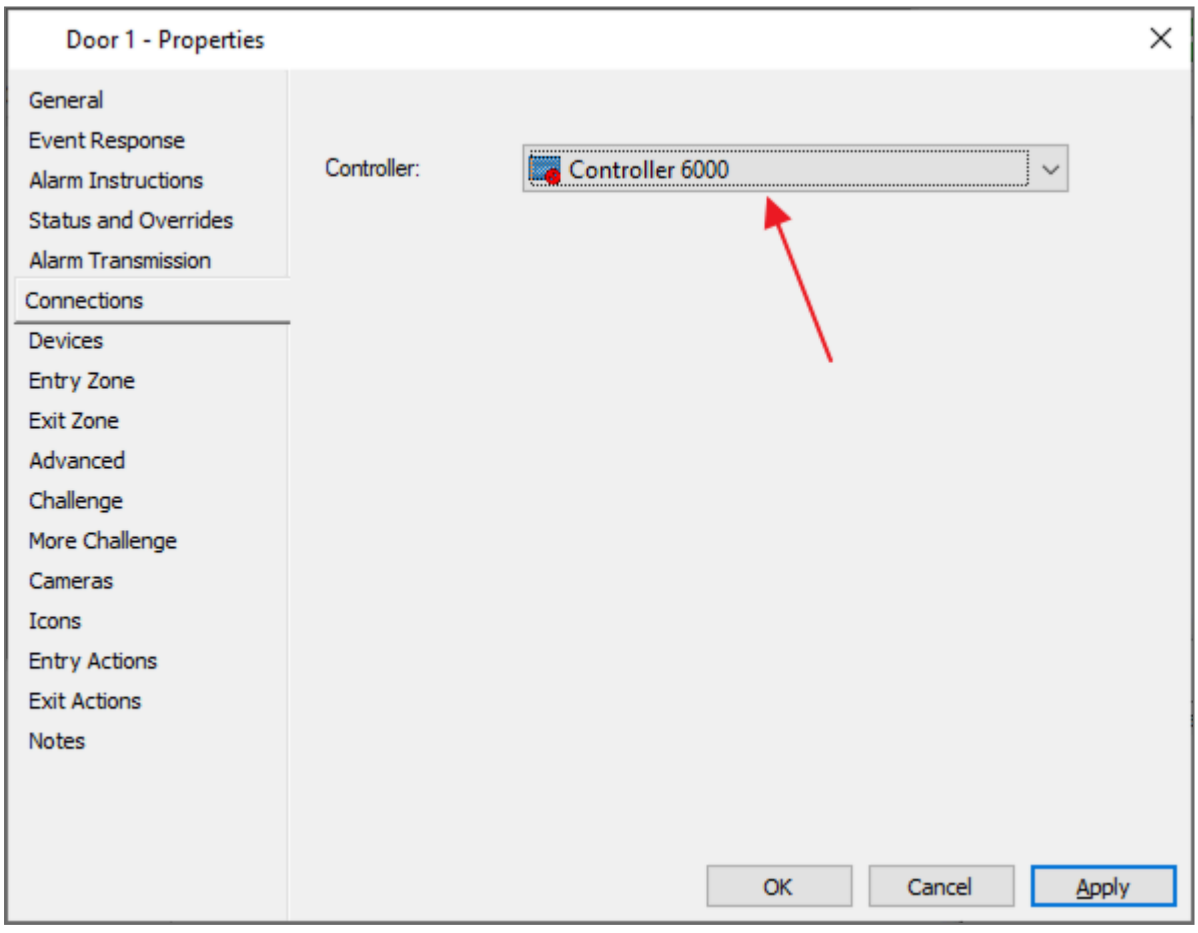
19. Para crear una puerta, ve a Configure, Door y luego **haz clic derecho** y crea una nueva puerta.



20. **Establece** el nombre de la puerta como **Suprema Door** y ve a Event Response y **elige** la alarma como System Alarm Zone.

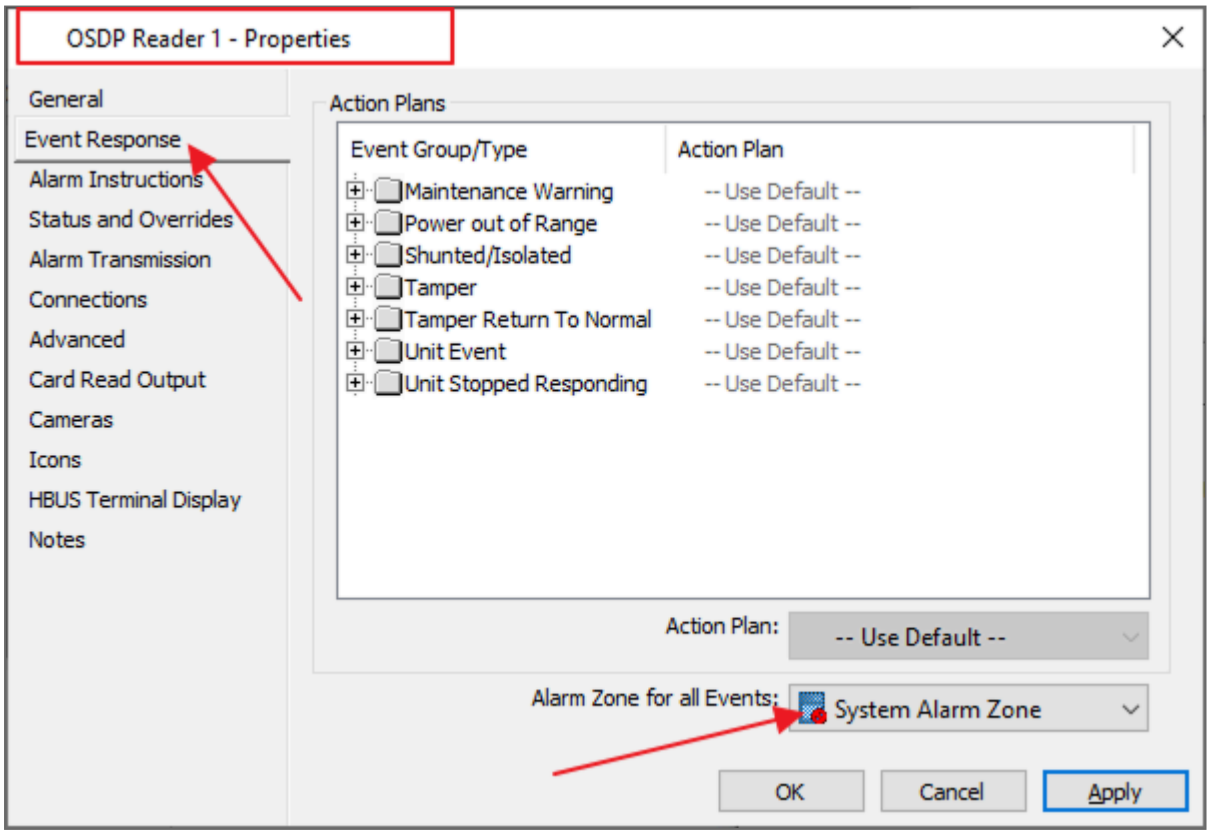


21. En **Connections, selecciona** Controller como Controller 6000 y presiona **Apply** y **OK**.



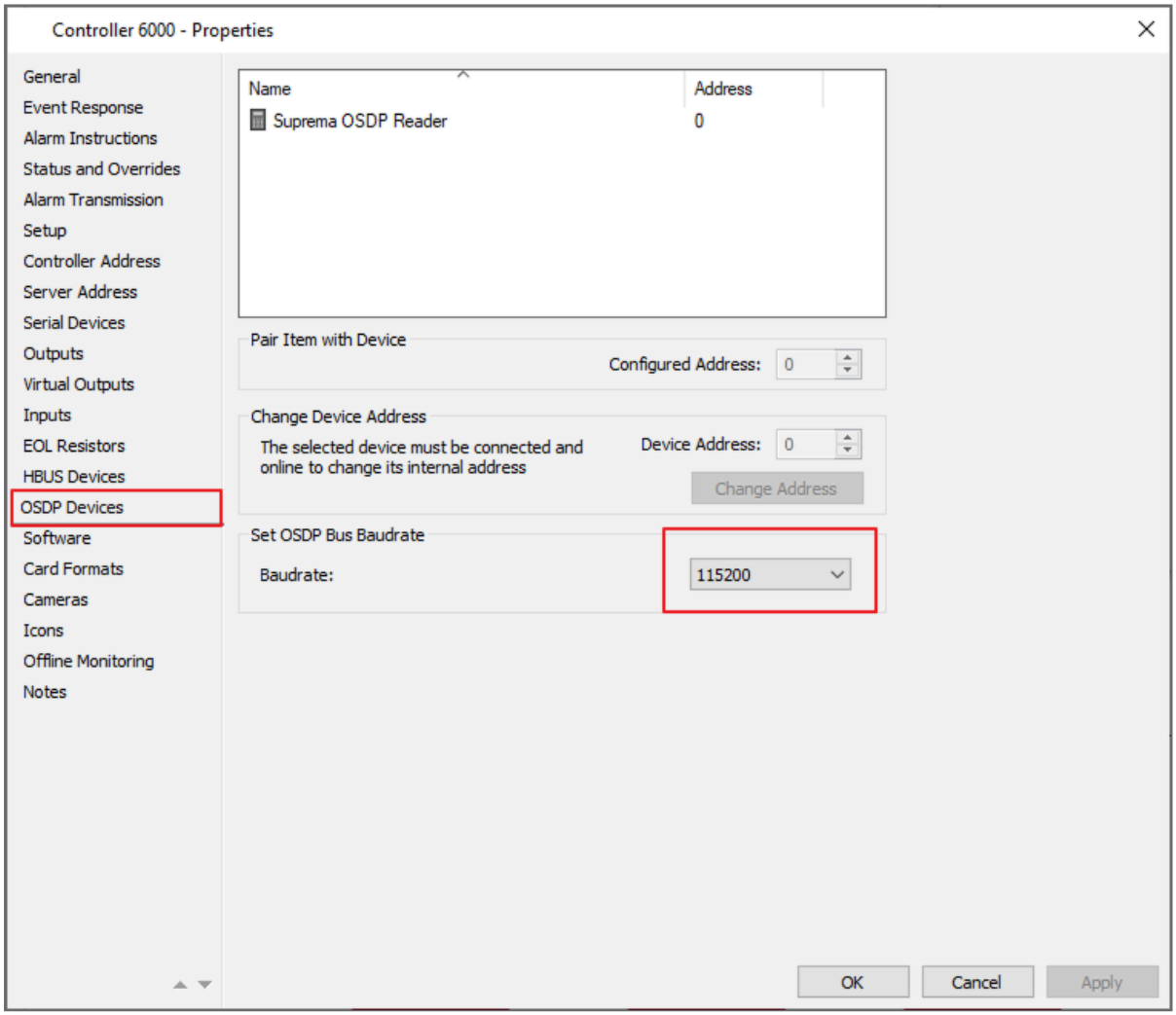
22. Para crear una conexión **OSDP**, haz clic derecho en la ventana de Hardware. Selecciona New** → **OSDP Device** → **luego haz clic en OSDP Reader** para crear OSDP Reader en Hardware.

    Se abre una nueva ventana. **Establece** el nombre como Suprema OSDP Reader y, en la pestaña de ajustes de Event Response, **establece** Alarm Zone for all events como System Alarm Zone. Luego **haz clic** en Apply y **presiona** OK para guardar los cambios.



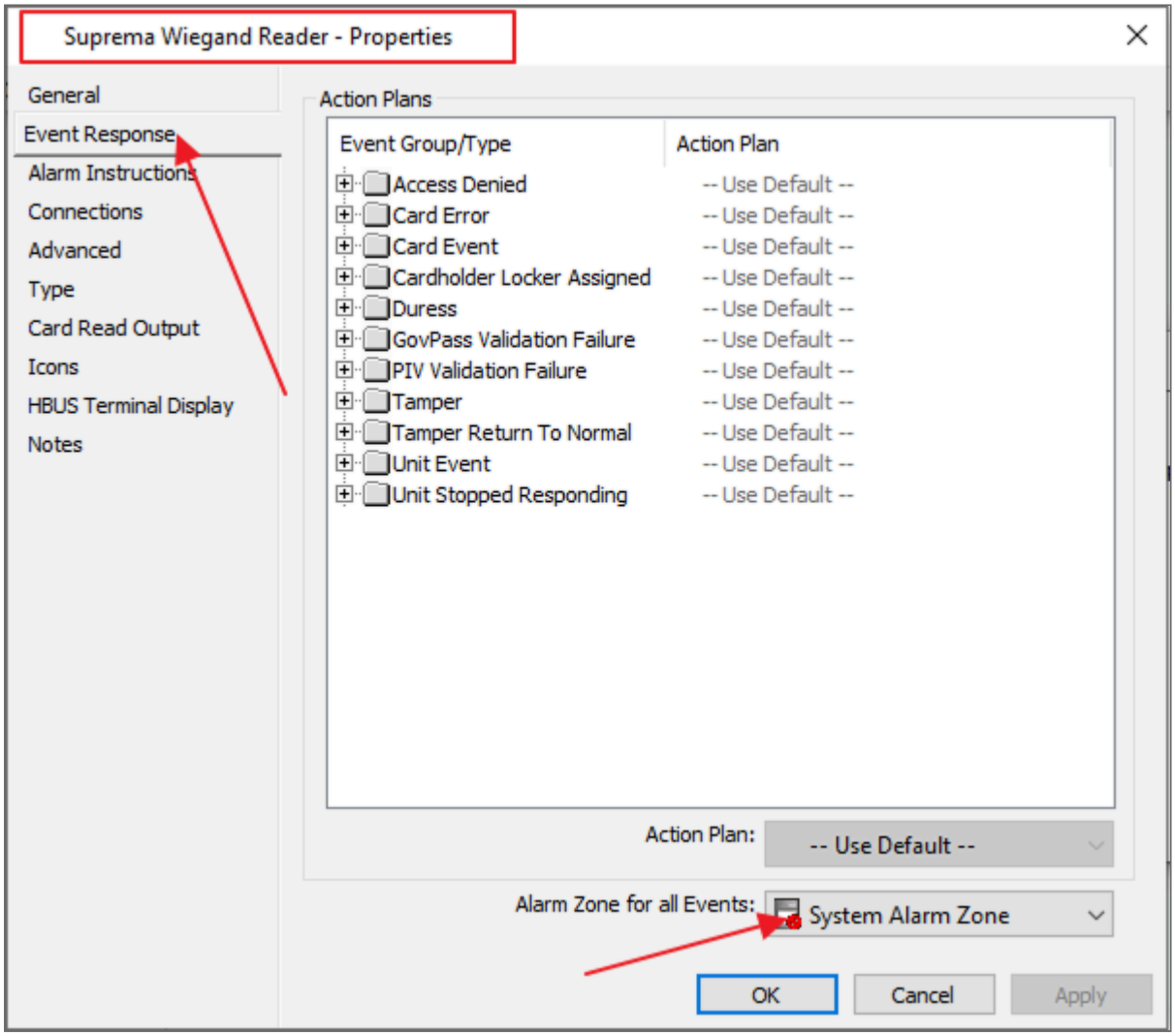
    Regresa a la ventana de Hardware. **Haz doble clic** en Controller 6000 para abrir las propiedades. **Haz clic** en la pestaña OSDP Devices.

23. **Arrastra** el lector OSDP desde la **ventana de Hardware** hasta las **propiedades del controlador** en la pestaña OSDP Devices. **Establece** Configured Address como 0, Suprema OSDP Device Address como 0 y Baudrate como **115200**.

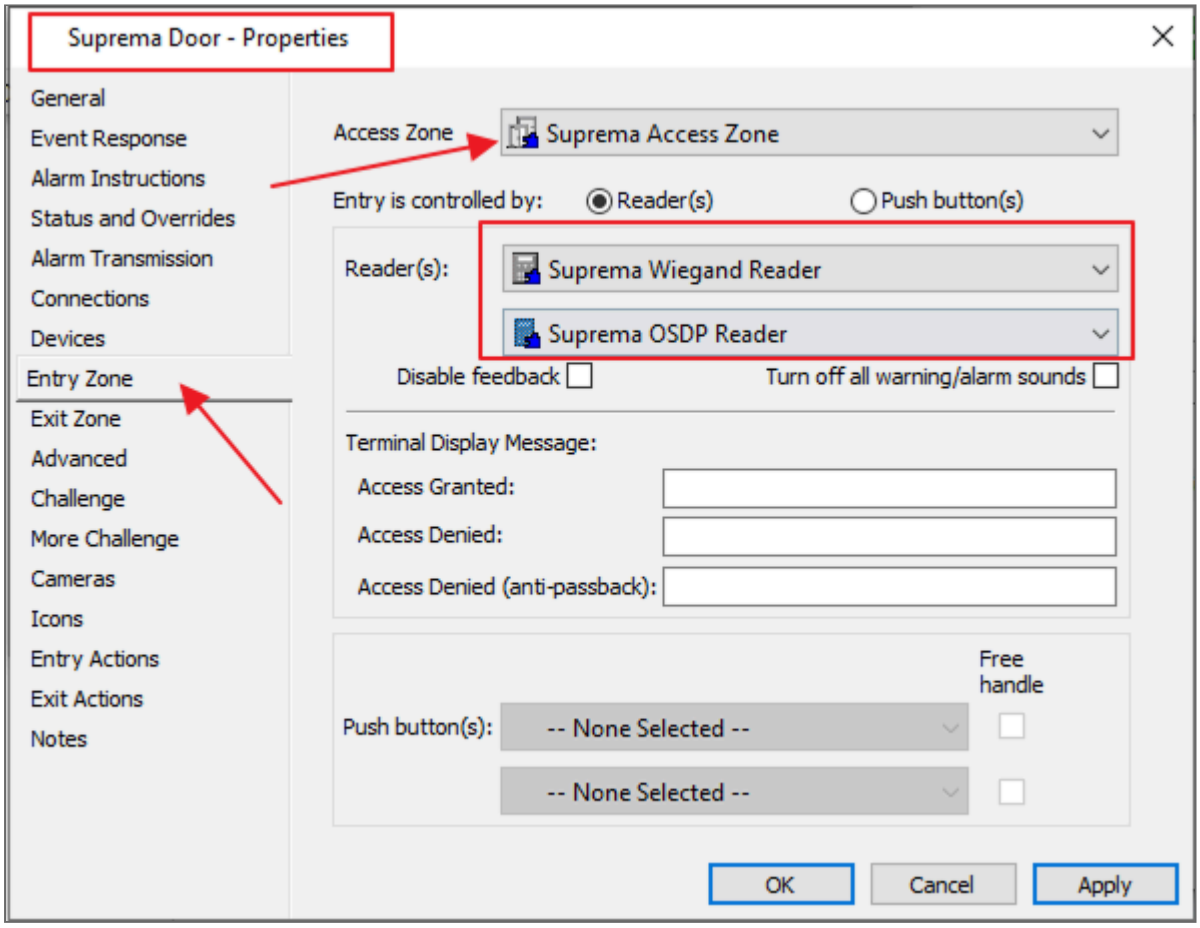


> **Información**
> Si tienes un lector OSDP 2x, cambia la dirección OSDP dentro de BioStar 2.

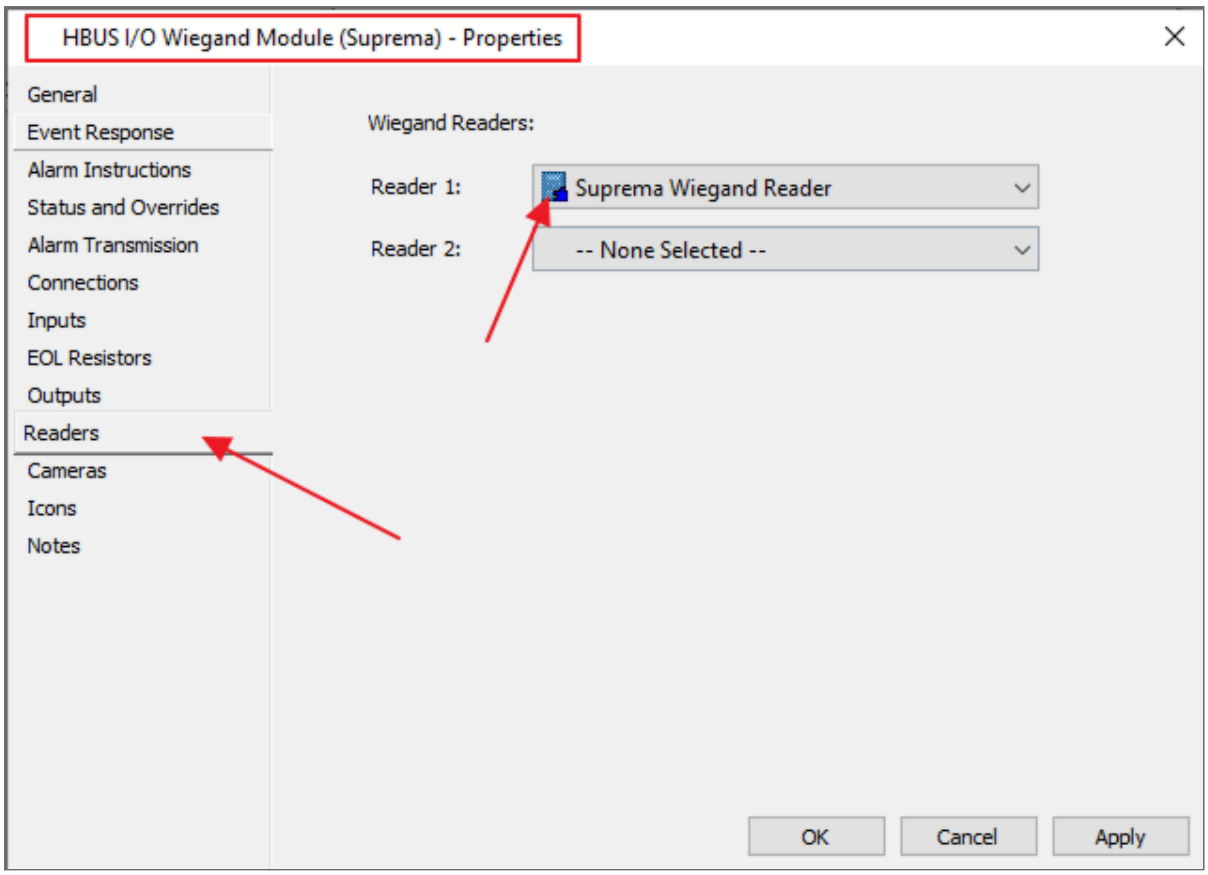
24. Para crear el lector Wiegand. **Haz clic derecho** en la ventana de Hardware. Haz clic en New → Third-Party Reader. Aparece una nueva ventana; **establece** el nombre como Suprema Wiegand Reader y luego ve a la pestaña Event Response. **Elige** Alarm Zone como System Alarm Zone y **presiona OK**.



25. **Ve** a la puerta que creamos en las propiedades. En **Entry Zone**, establece Access Zone como **Suprema Access Zone** y reader como **Suprema Wiegand Reader** y **Suprema OSDP Reader**; luego **presiona** el botón **OK**.



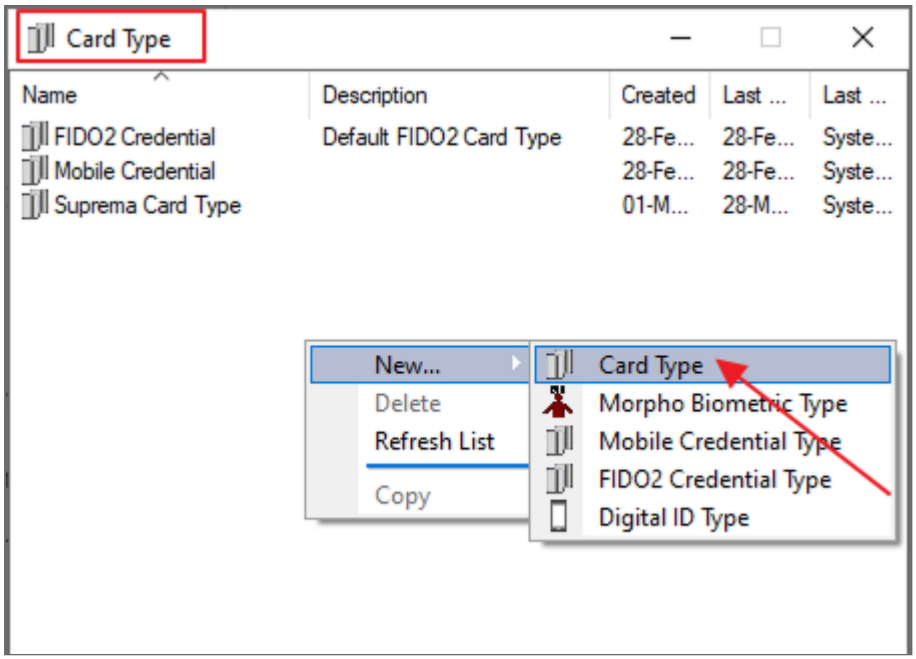
26. En las propiedades de **HBUS I/O**, ve a los ajustes de **Reader** y establece Reader 1 como Suprema Wiegand Reader; **presiona** el botón **OK**. **Cierra** la ventana de la puerta y del controlador.



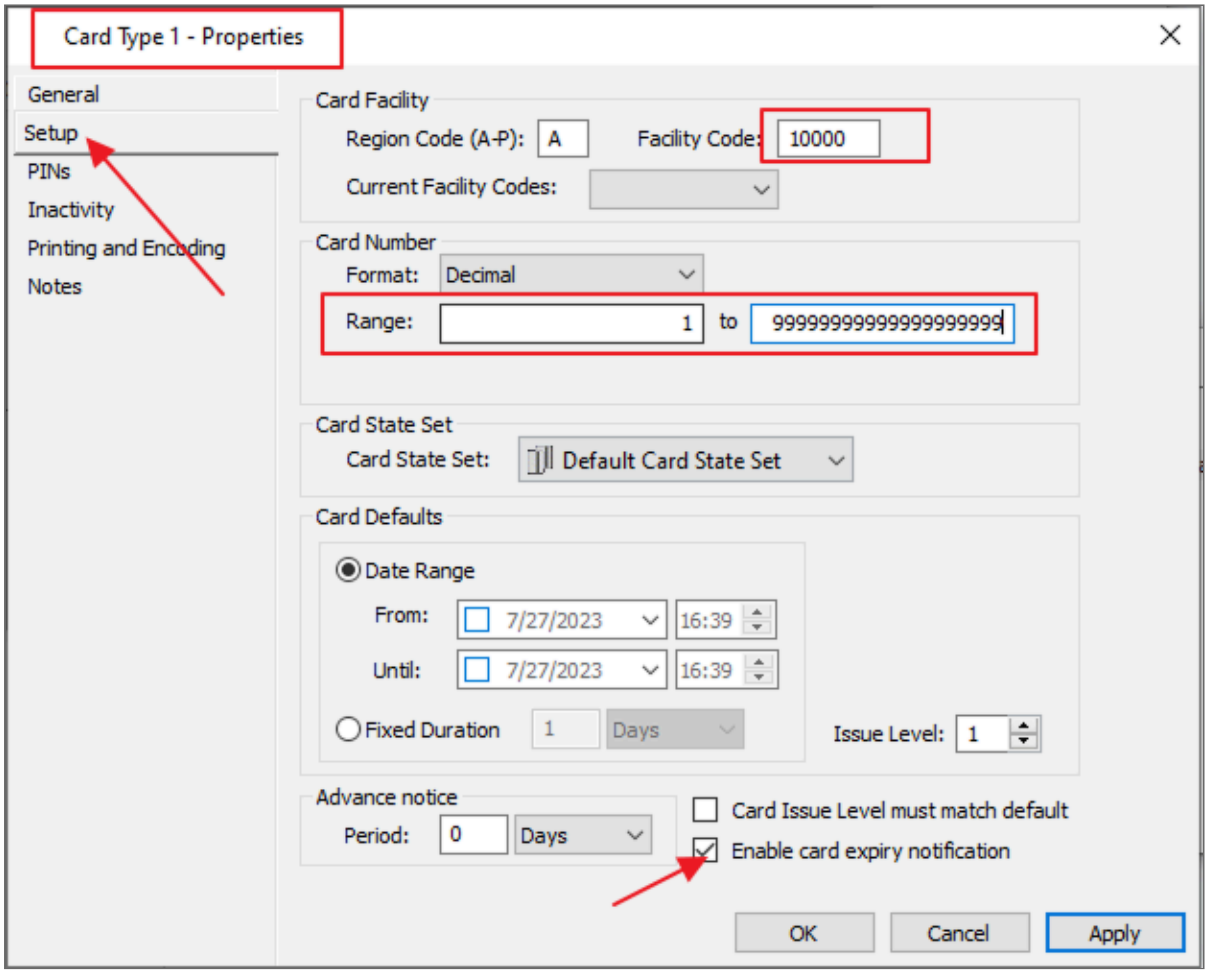
27. Para crear un tipo de tarjeta, ve a Configure → Card Type, **haz clic derecho** y crea un nuevo **Card Type**. **Establece** su

nombre como **Suprema Card Type**.

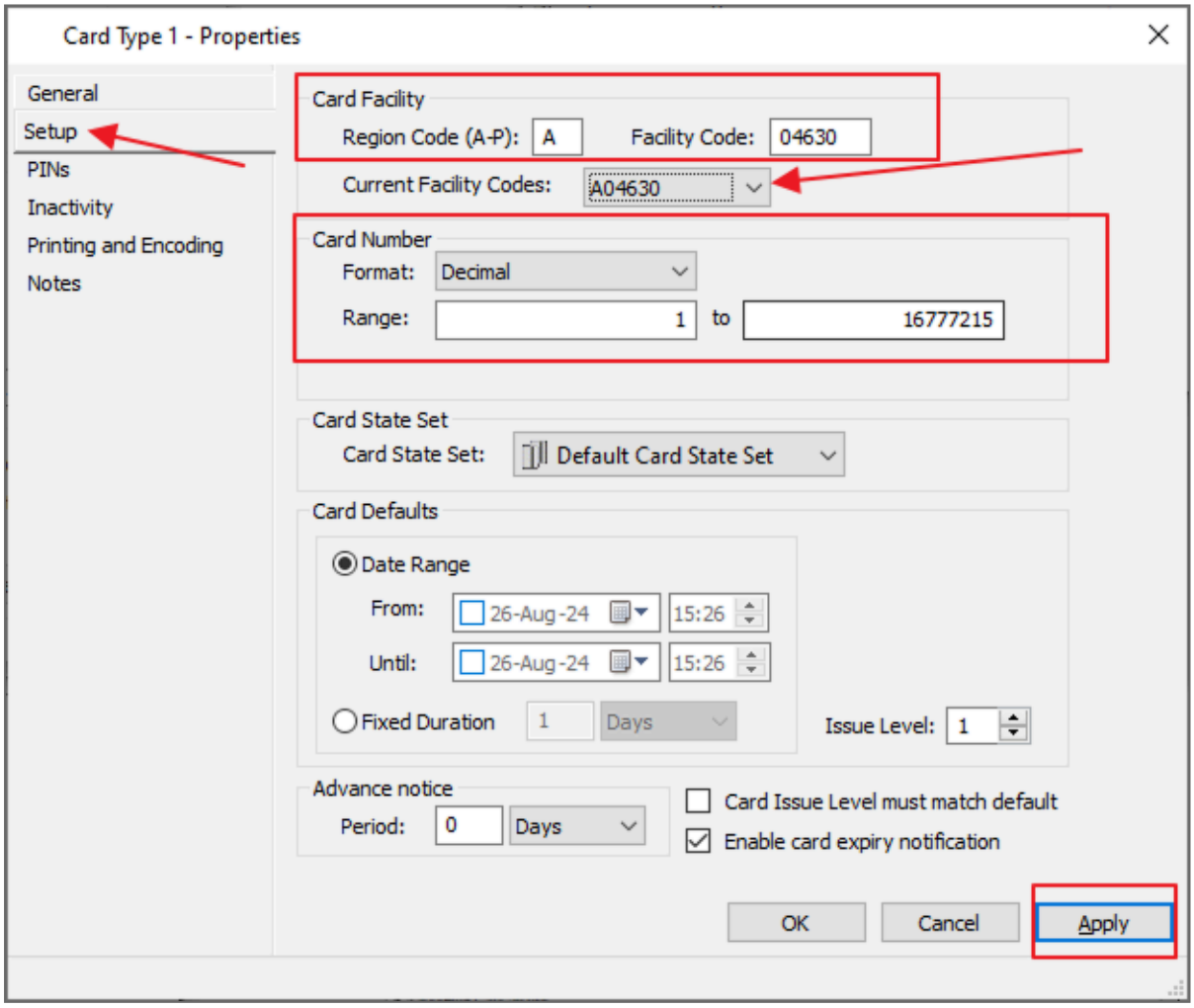
> **Información**
>
> - Se necesita una licencia QR Device para leer el código QR de Gallagher. Ponte en contacto con Suprema para obtenerla.
> - Usa los mismos términos mencionados para los campos.



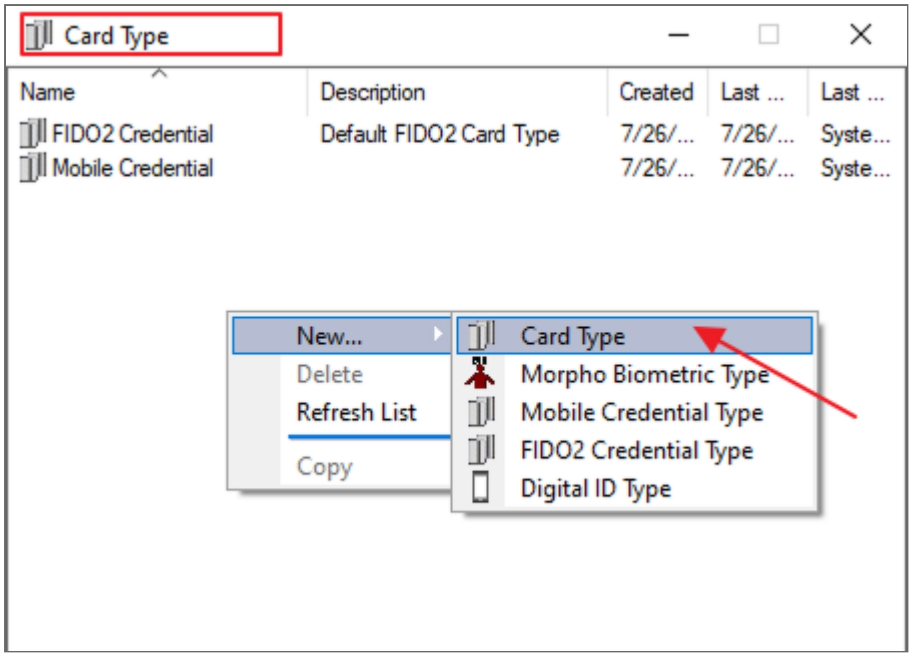
28. En las propiedades del tipo de tarjeta, **ve** a la opción setup y configura Region code como **A**, Facility code como **10000**, el rango de números de tarjeta como **1 a 99999999999999999999 (20 veces)** y habilita la notificación de vencimiento de la tarjeta. **Presiona OK**.



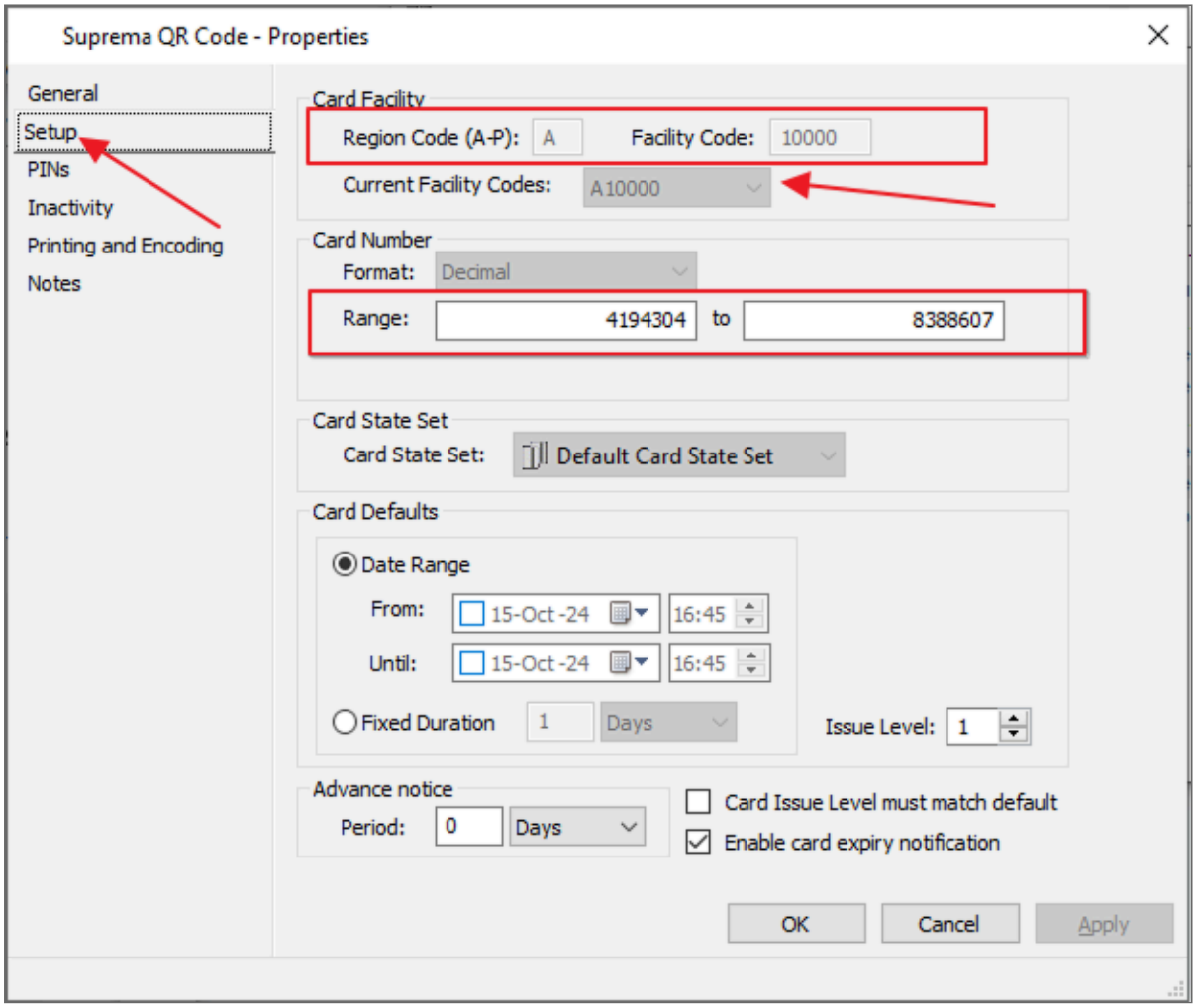
29. Crea otro tipo de tarjeta: ve a Configure → Card Type, **haz clic derecho** y crea un nuevo **Card Type**. Establece su nombre como **HID Seos Corporate**. Y **ve a** las propiedades (setup) para configurar el tipo de tarjeta. Usa la siguiente configuración para configurar la tarjeta y **presiona** Apply y **OK**.



30. Crea otro tipo de tarjeta: ve a Configure → Card Type, **haz clic derecho** y crea un nuevo **Card Type**. Establece su nombre como **Suprema QR Code**.

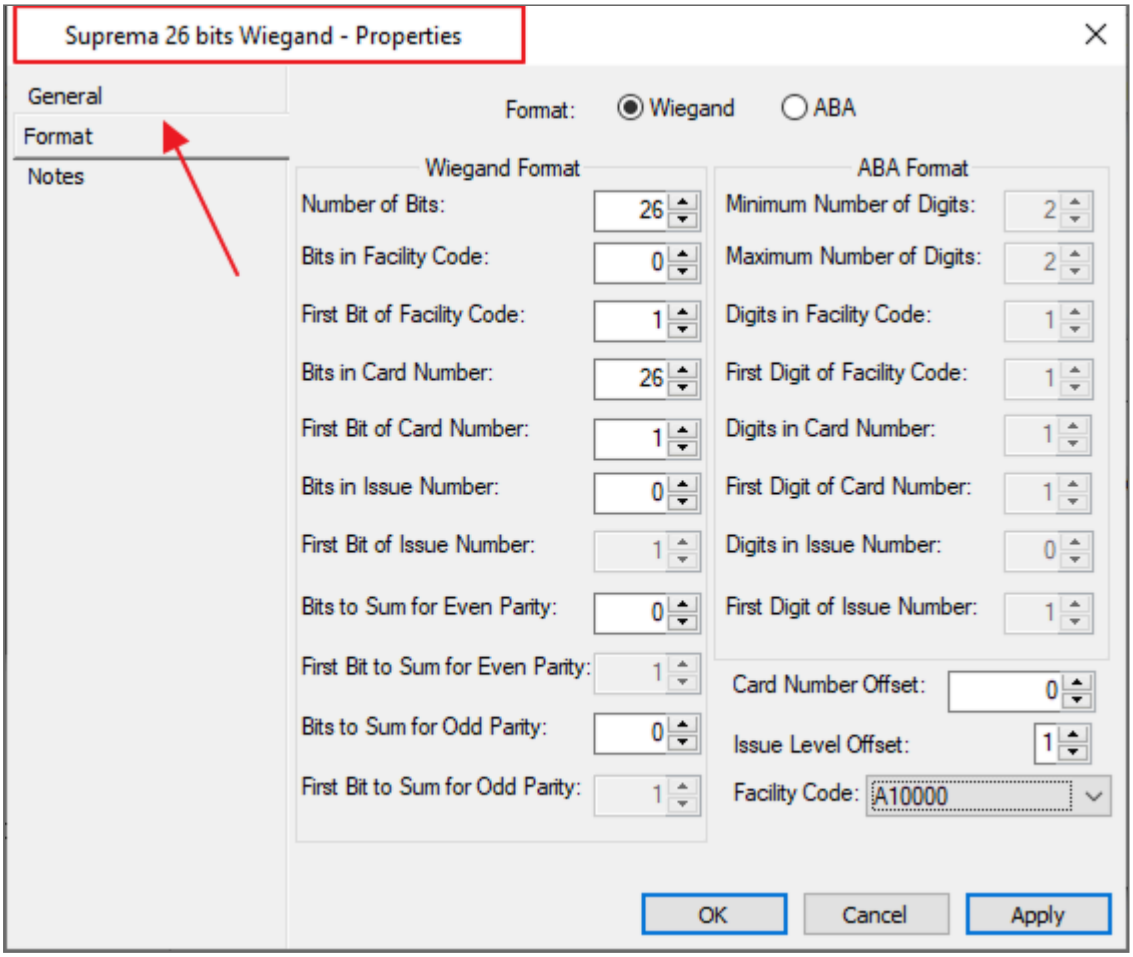


31. En las propiedades del tipo de tarjeta, **ve** a la opción setup y configura Region code como **A**, Facility code como **10000**, el rango de números de tarjeta como **4194304 a 8388607** y habilita la notificación de vencimiento de la tarjeta. **Presiona OK**.

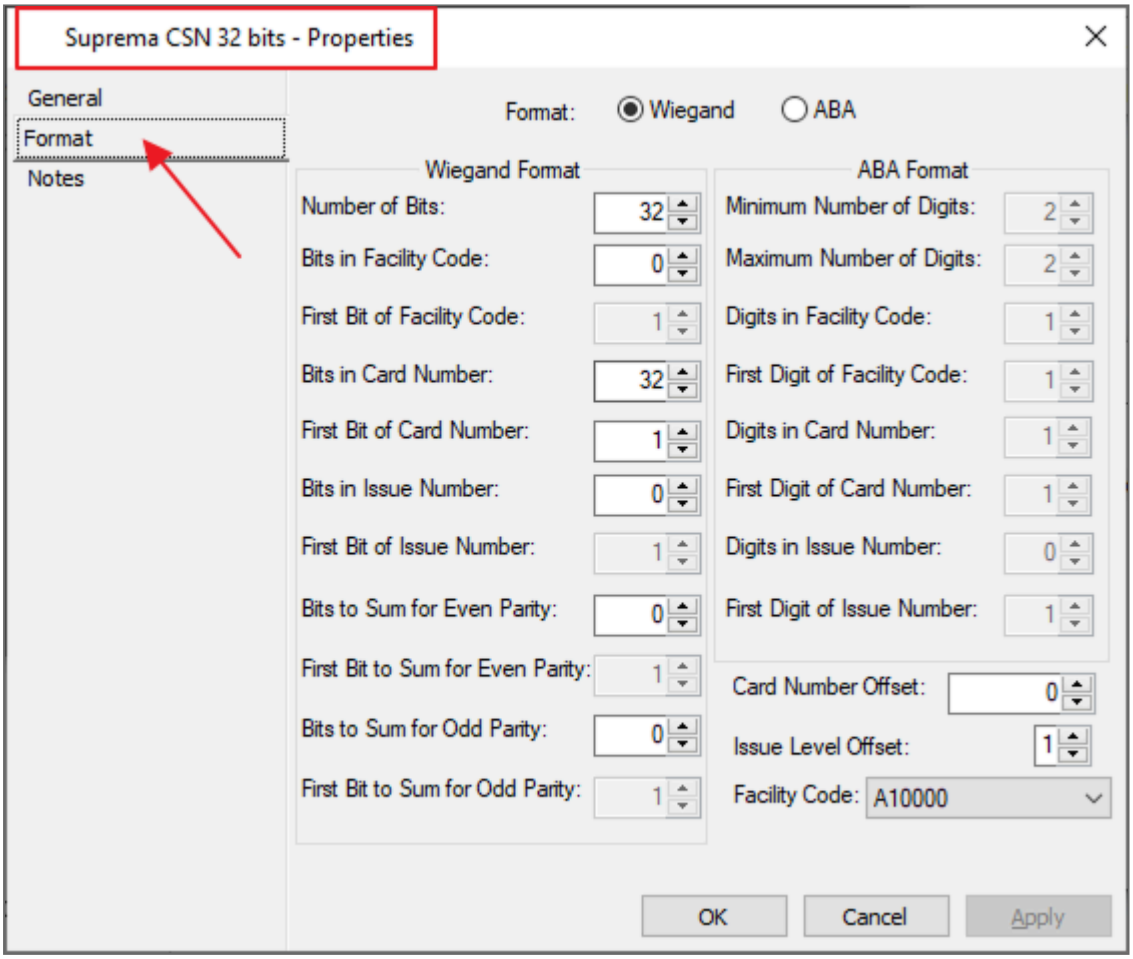


32. Para crear un tipo de tarjeta universal, ve a Configure → Universal Card Format, **haz clic derecho** y crea un nuevo formato de tarjeta universal. Debemos crear 4 formatos de tarjeta.

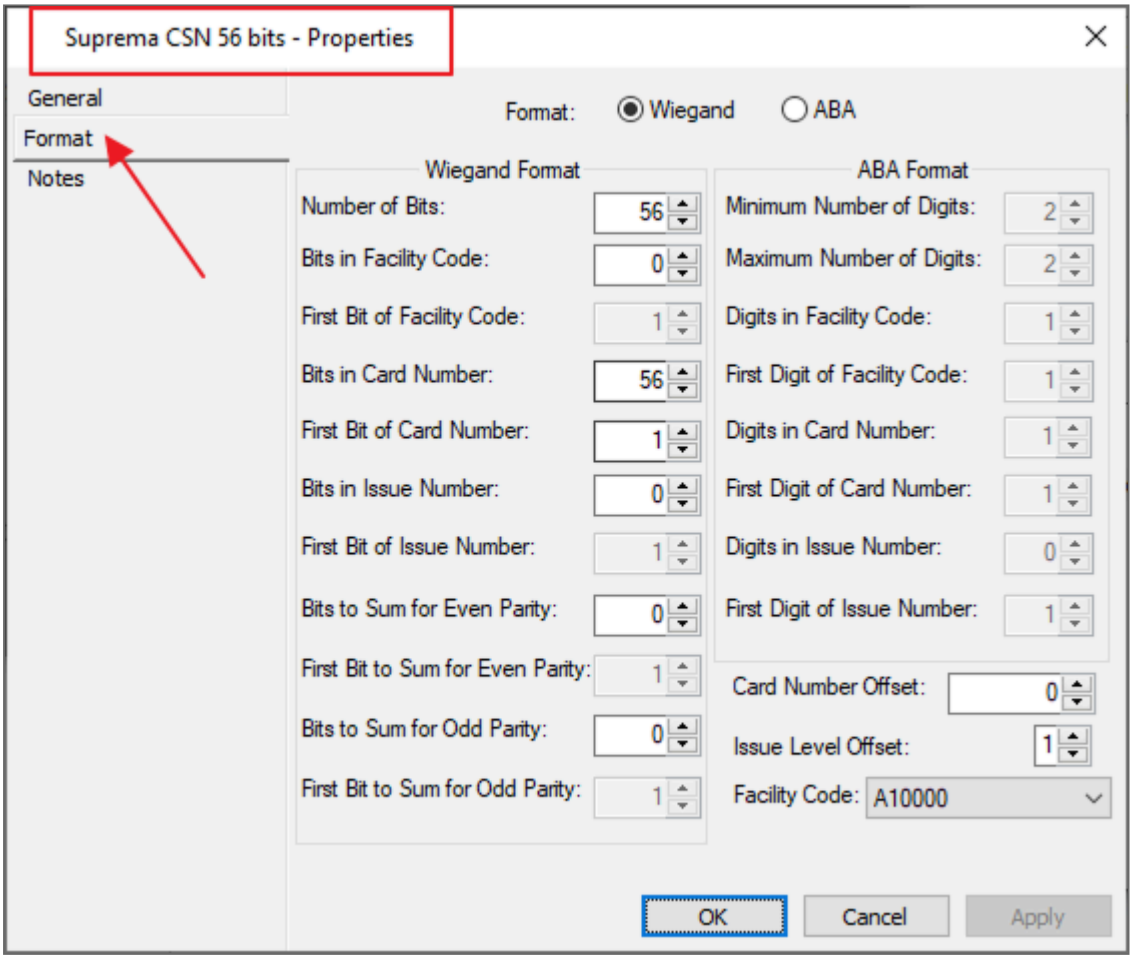
    1. **Crea** un nuevo formato con el nombre **Suprema 26 bits** Wiegand y establece el formato como en la imagen siguiente:



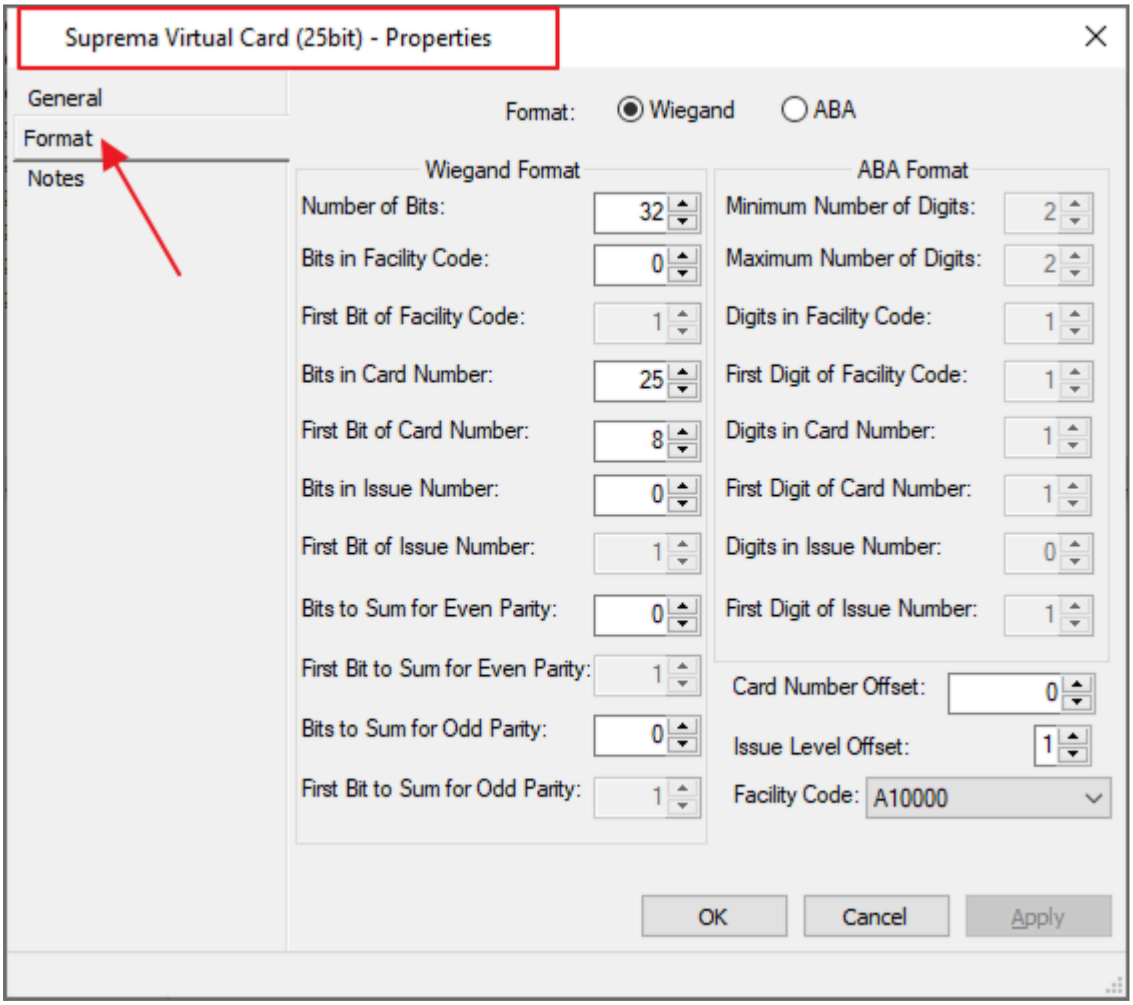
2. **Crea** un segundo formato de tarjeta como **Suprema CSN 32 bits** y establece el formato como se muestra abajo.



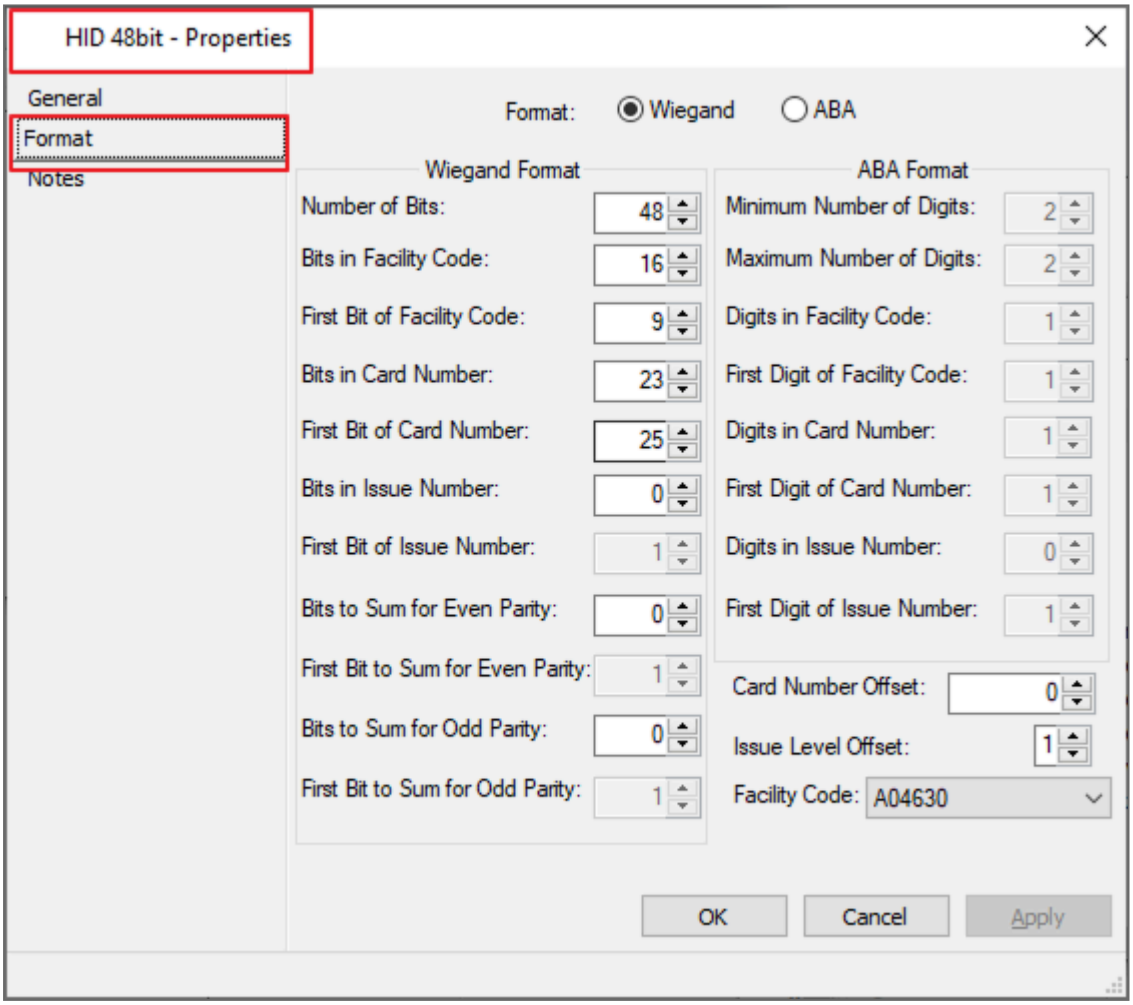
3. **Crea** un tercer formato de tarjeta como **Suprema CSN 56 bits** y establece el formato como se muestra abajo.



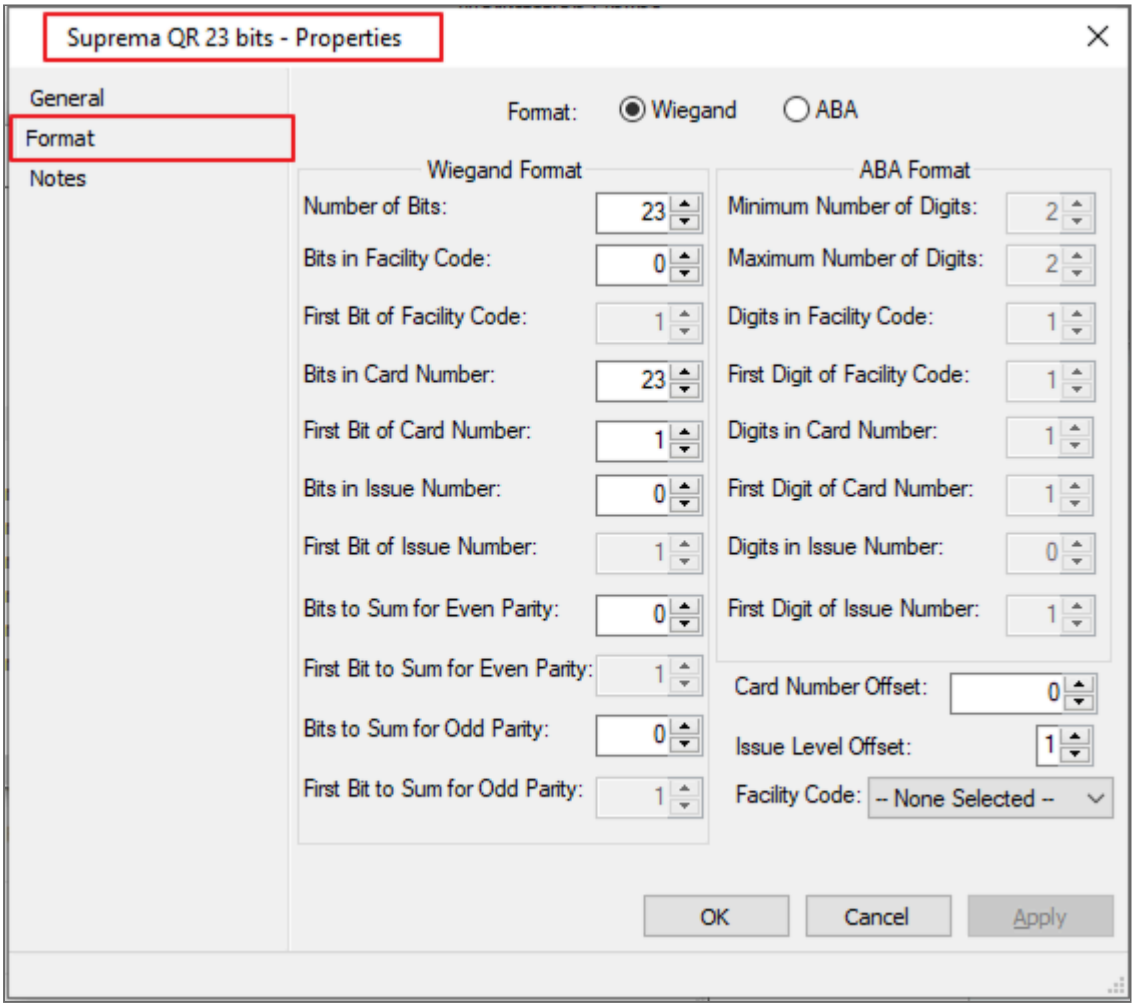
4. **Crea** un cuarto formato de tarjeta como **Suprema Virtual Card (25bit)** y establece el formato como se muestra abajo.



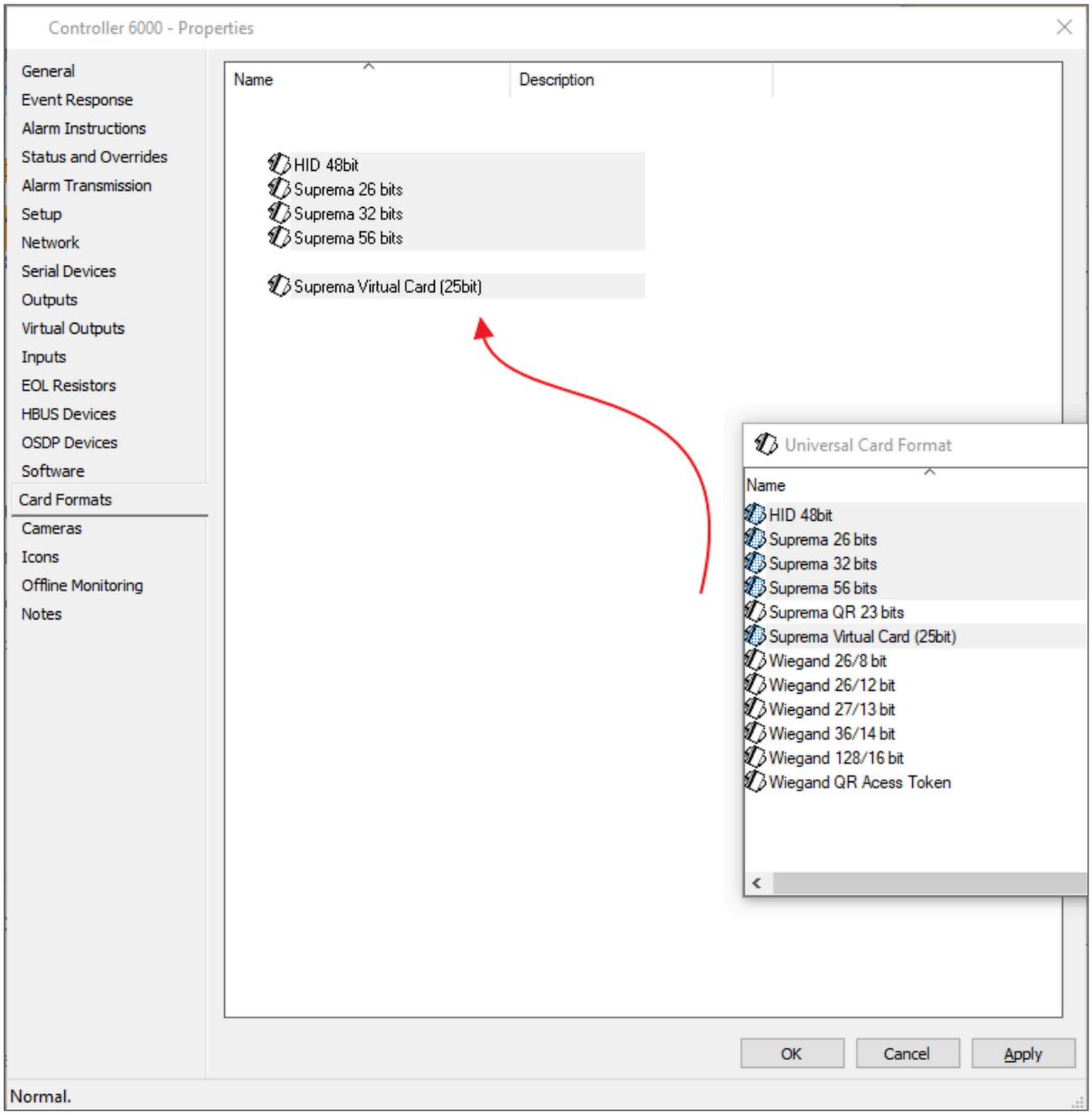
5. **Crea** un quinto formato de tarjeta como **HID 48bit** y establece el formato como se muestra abajo.



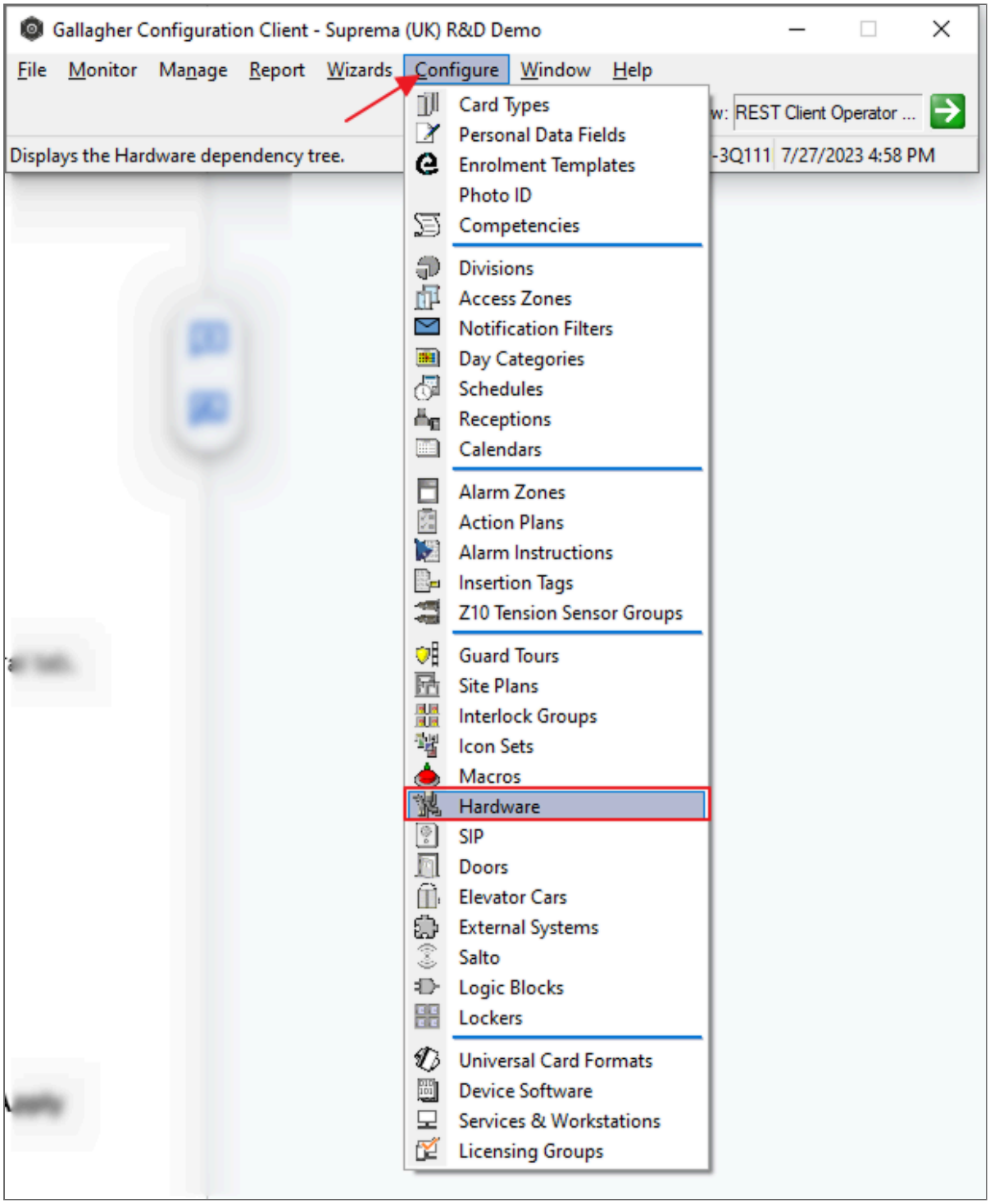
6. **Crea** un sexto formato de tarjeta como **Suprema QR 23 bits** y establece el formato como se muestra abajo.



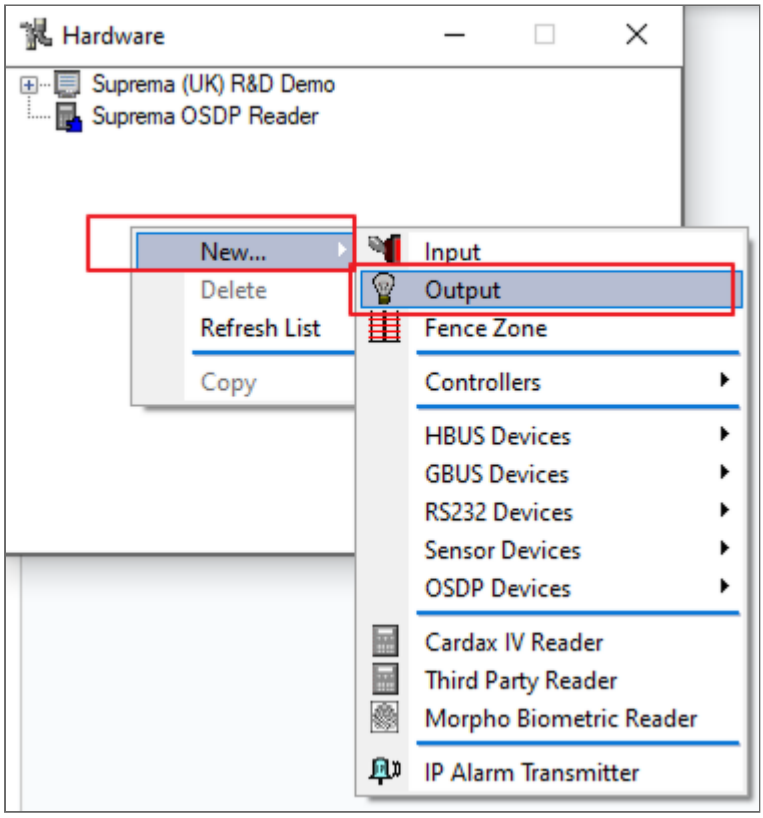
33. **Arrastra** los seis tipos de tarjeta y suéltalos en las propiedades del controlador, en Card Format Setting, y **aplica** la configuración. **Presiona OK** y **cierra** todas las ventanas de Gallagher Configuration Client.



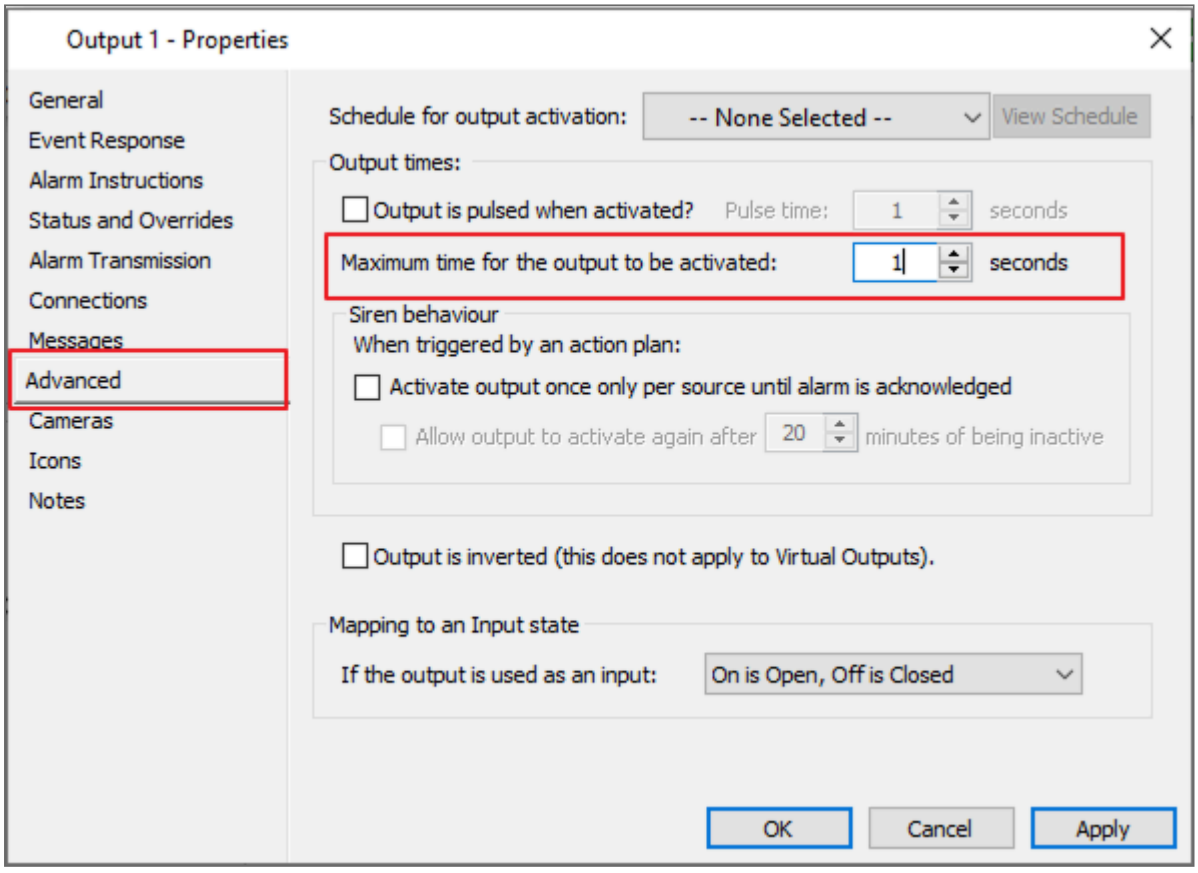
34. Ve a Config Client Configure → Hardware.



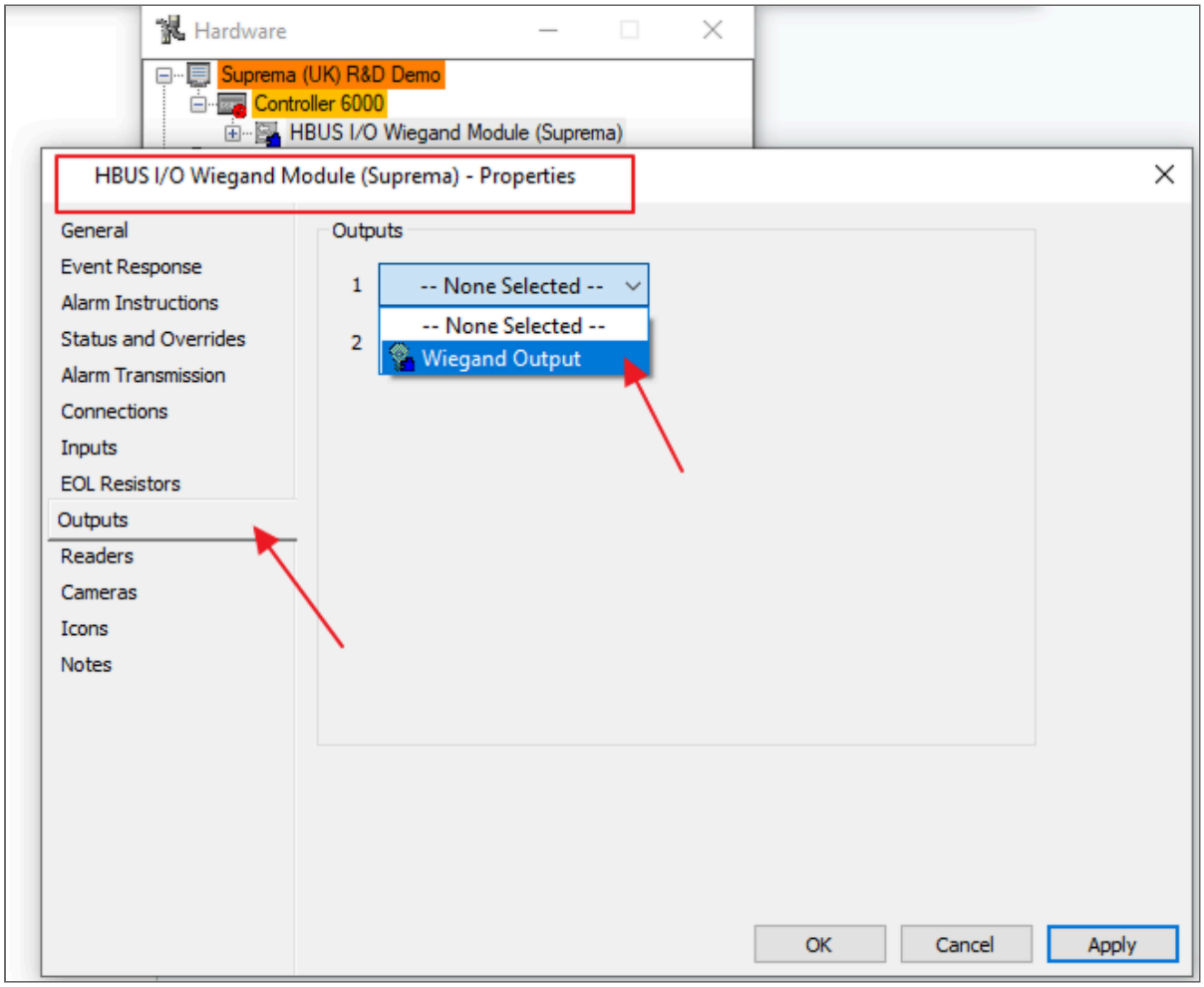
Luego **haz clic derecho** en la ventana y **crea** una salida y **establece** el nombre como **Wiegand Output** en la pestaña general.



35. Ahora **haz clic** en Advance en el lado izquierdo, **establece** 1 segundo en la opción Output times y **presiona Apply** y **OK**.

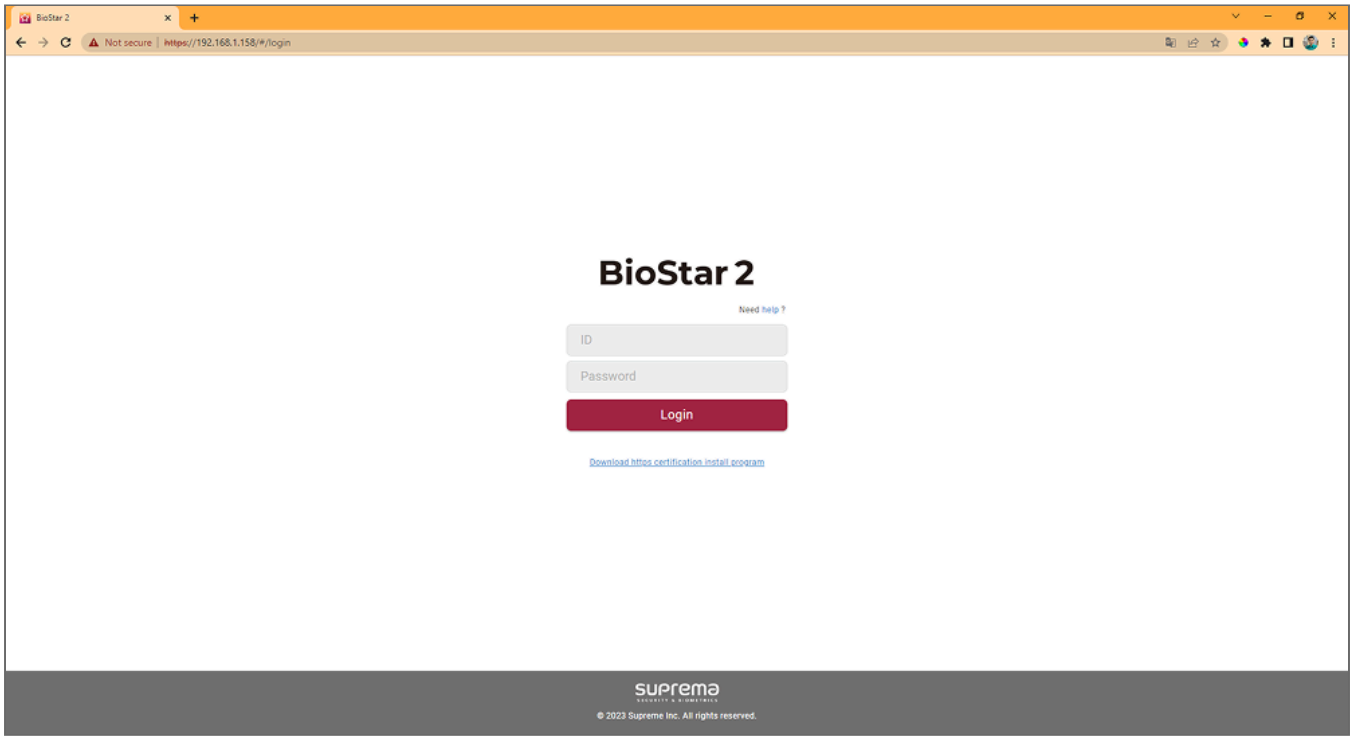


36. Ahora **ve** a la ventana de hardware → **haz doble clic** en HBUS I/O Wiegand Module (Suprema) en el lado izquierdo, **ve** a Outputs y **selecciona** Wiegand Output; **presiona Apply** y **OK**.

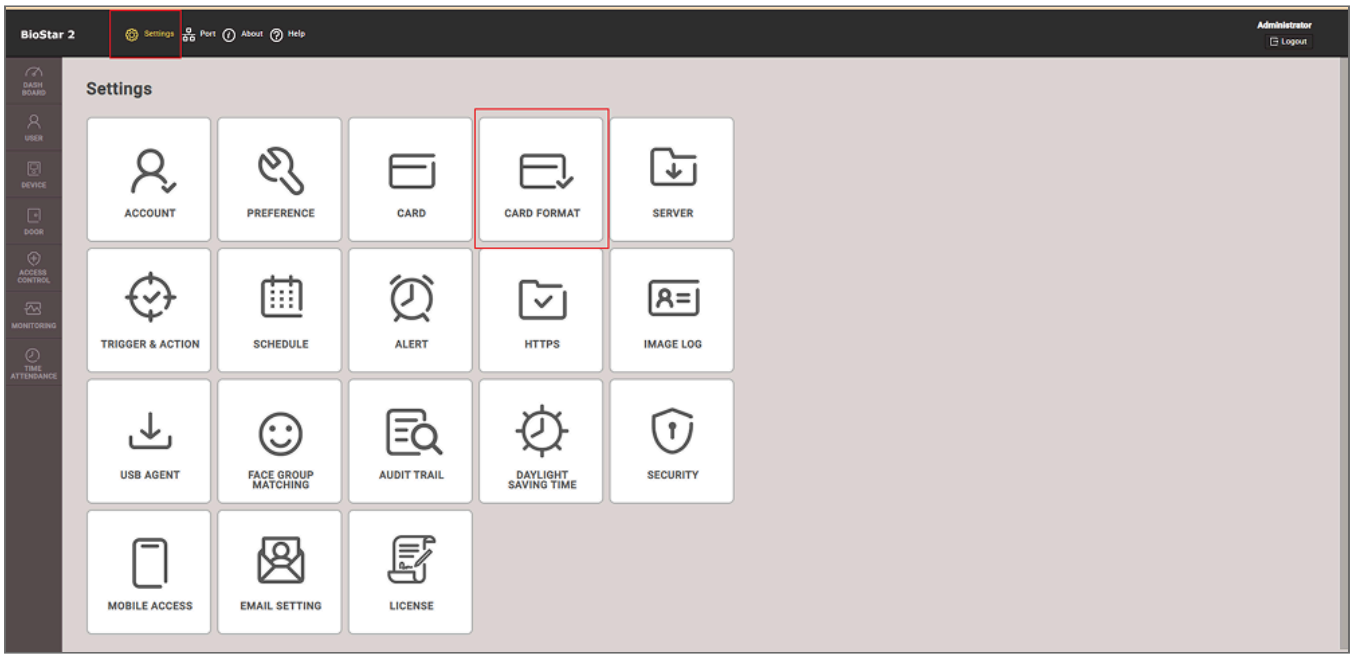


Configuración de BioStar 2

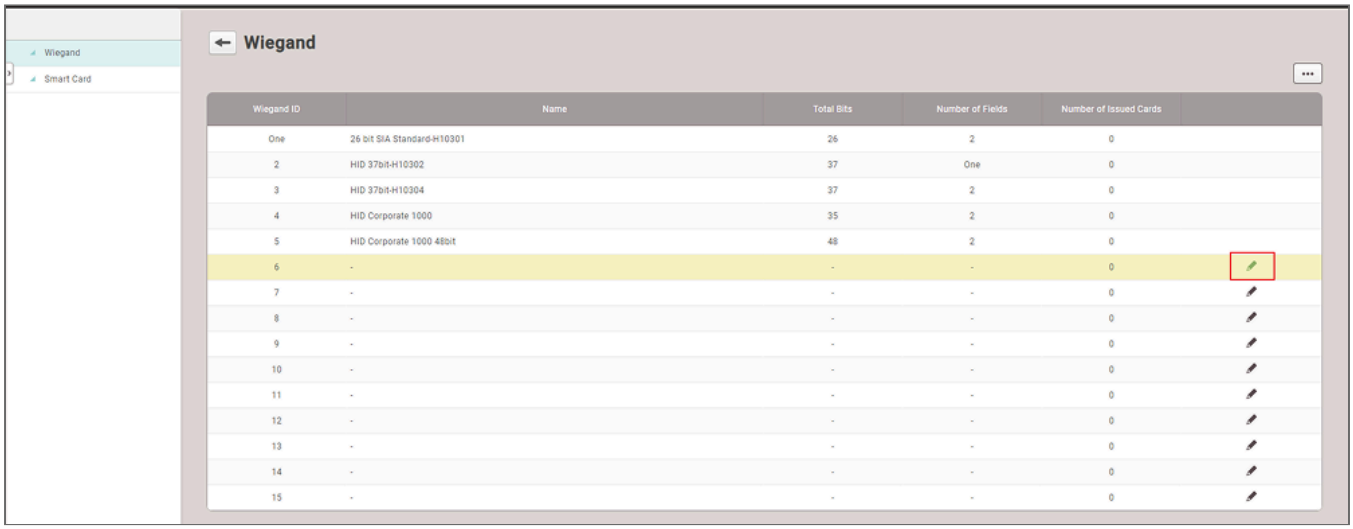
1. Para abrir BioStar 2, **escribe** https://[Your system IP Address]/#/login en tu navegador; se abrirá el formulario de inicio de sesión.



2. **Completa** tus credenciales de BioStar 2 para iniciar sesión, **ve** a la página de ajustes y **selecciona** Card Format.

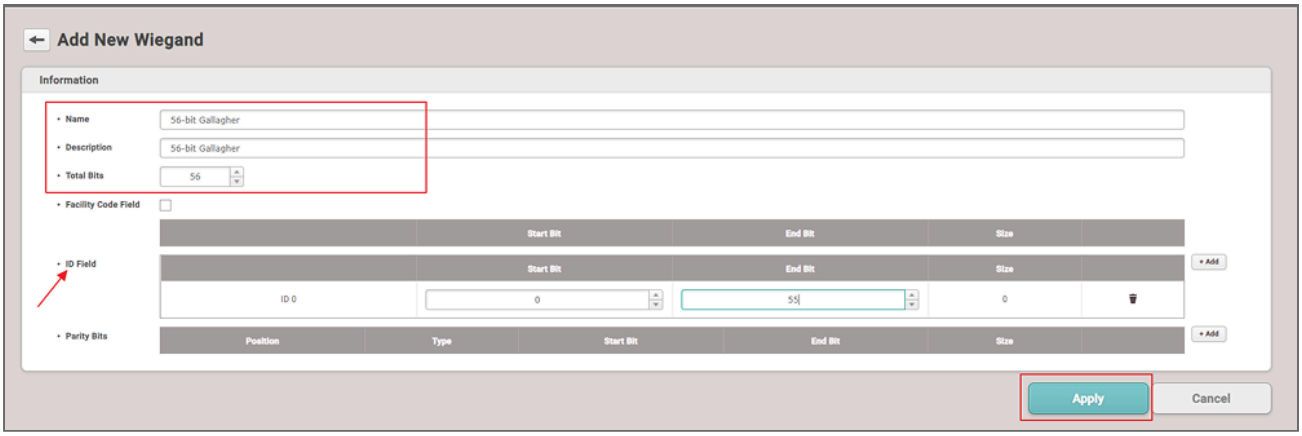


3. En el ajuste de la tarjeta, **haz clic** en el botón **edit** para crear un nuevo formato de tarjeta.

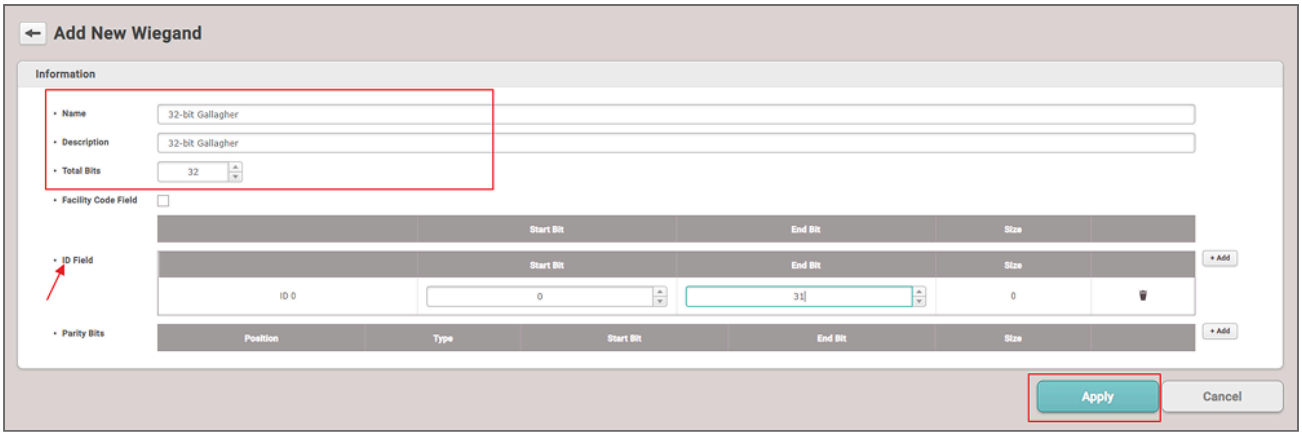


4. Aquí también debemos crear tres tipos de tarjeta: **56-bit**, **32-bit** y **26-bit**.

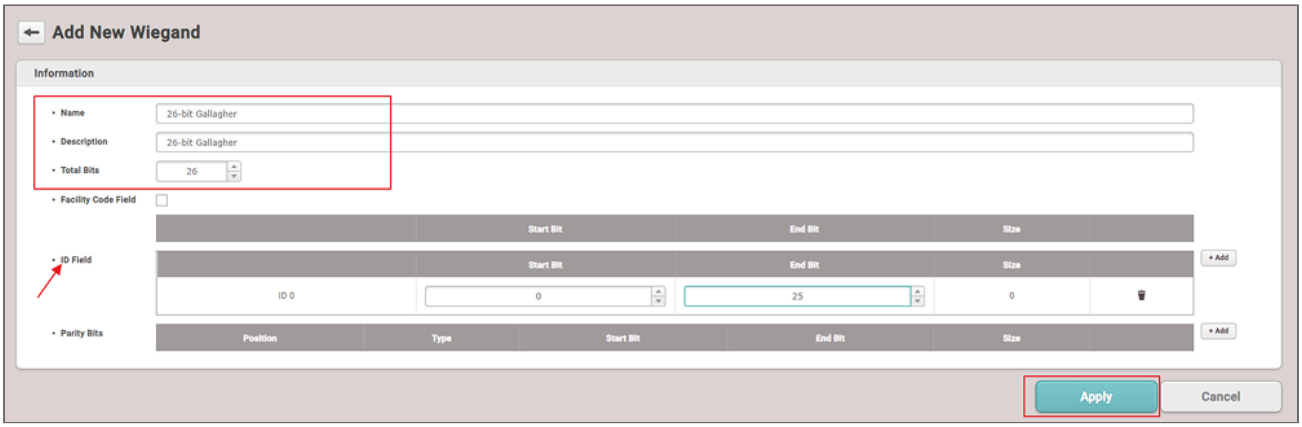
    1. **Establece** el nombre como **56-bit Gallagher**, los bits totales como 56 y, en el campo ID, **presiona** add, **establece** el bit inicial como 0 y el bit final como 55.



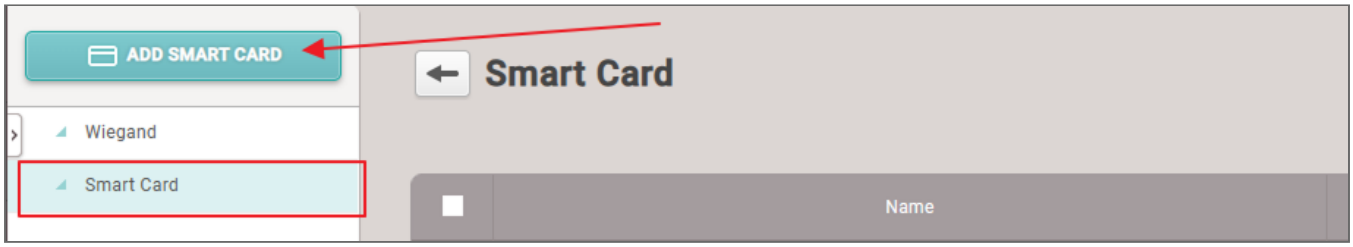
    2. **Establece** el nombre como **32-bit Gallagher**, los bits totales como 32 y, en el campo ID, **presiona** add y **establece** el bit inicial como 0 y el bit final como 31.



    3. **Establece** el nombre como **26-bit Gallagher**, los bits totales como 26 y, en el campo ID, **presiona** add y **establece** el bit inicial como 0 y el bit final como 25.

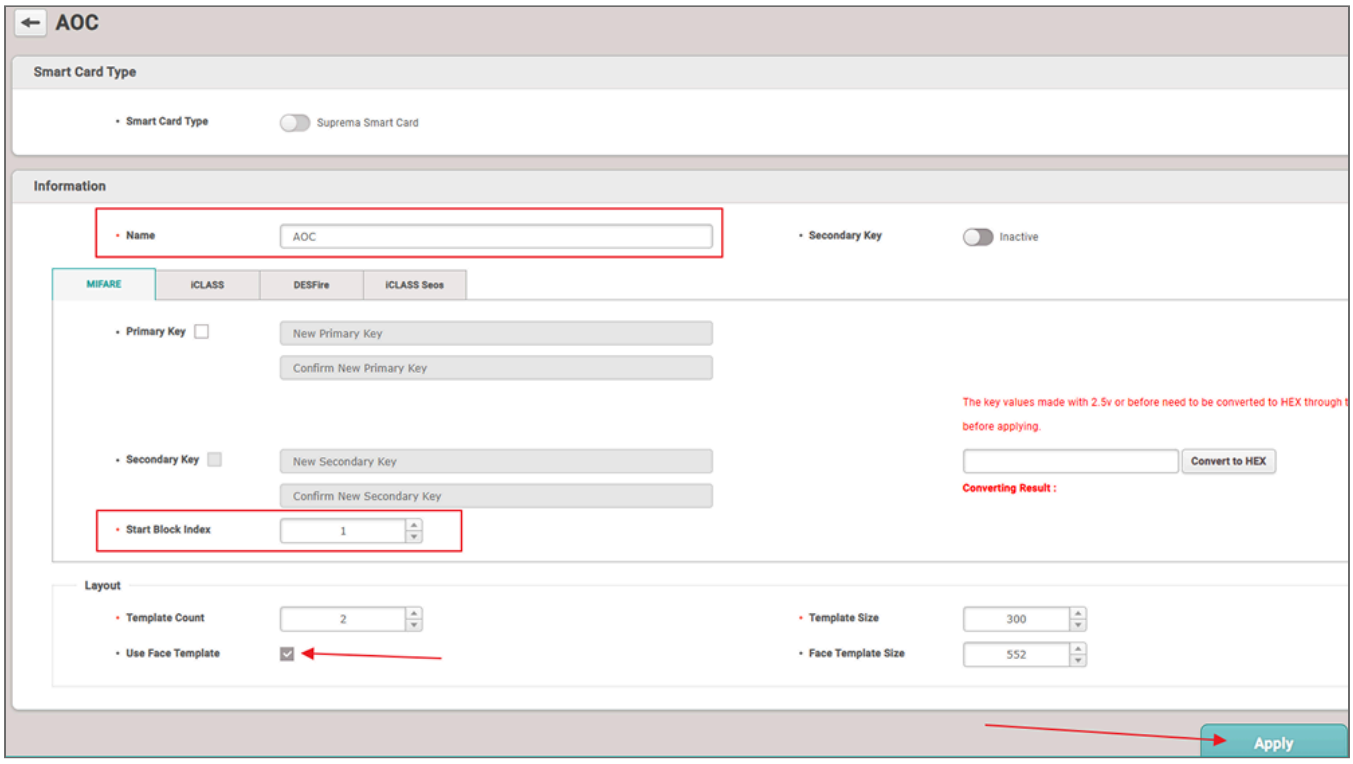


5. Ahora, dentro del formato de tarjeta, **ve** a la sección smart card presionando el botón smart card y **haz clic** en el botón ADD SMART CARD.

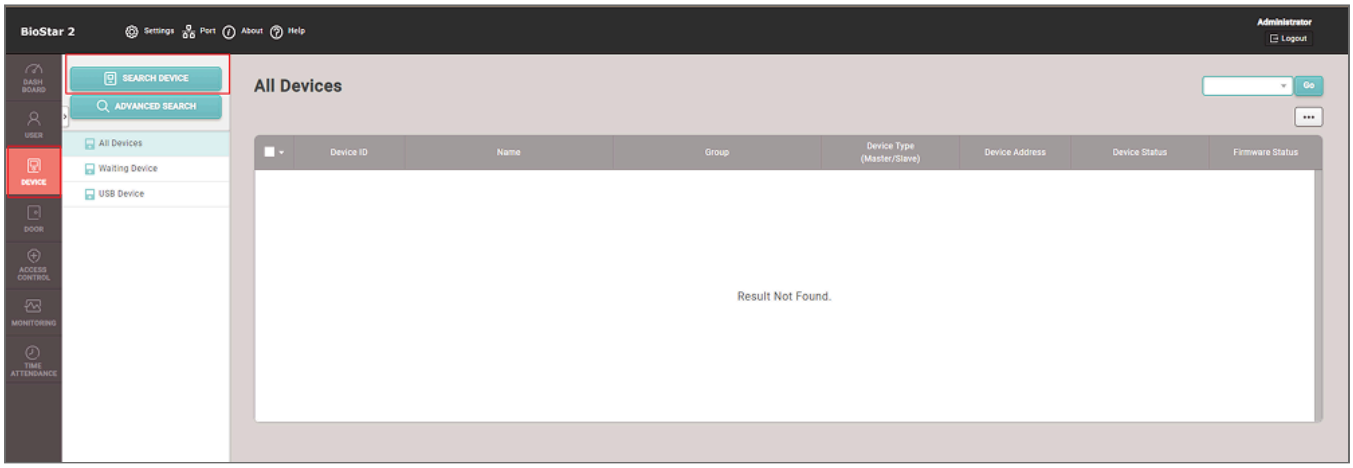


6. Ahora escribe el **nombre** como AOC Inside MIFARE, **ingresa 1** para Start Block Index, **marca** la casilla Use Face template y **presiona** el botón Apply.

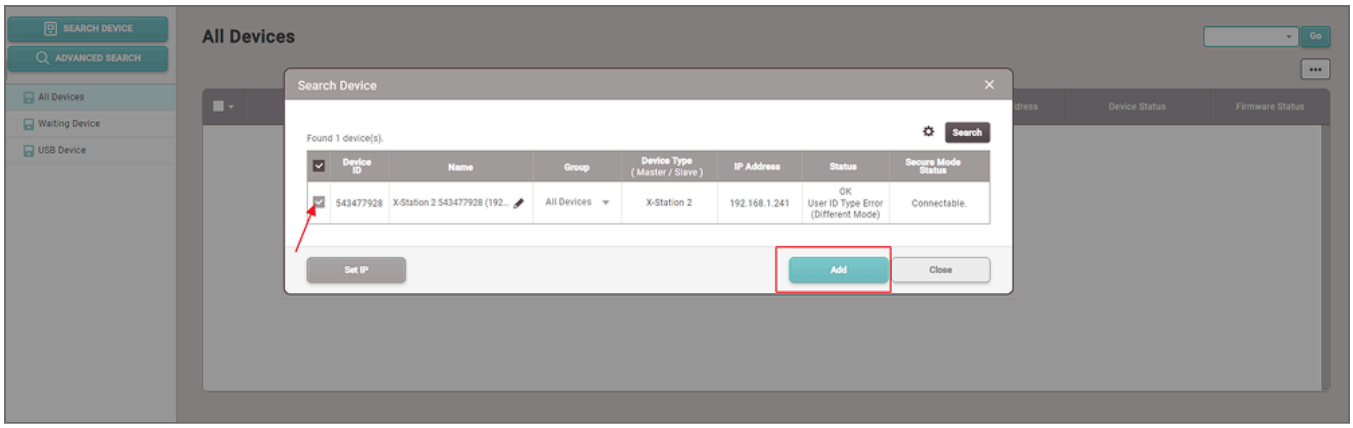
> **Información**
>
> Si no quieres usar un Visual Face y solo quieres usar una fingerprint en la smart card, puedes desmarcar la casilla.



7. Para conectar dispositivos al sistema, **ve** al panel de dispositivos y **presiona** el botón SEARCH DEVICE.



8. Ahora **presiona** el botón de búsqueda, **selecciona** el dispositivo y **presiona** el botón Add.



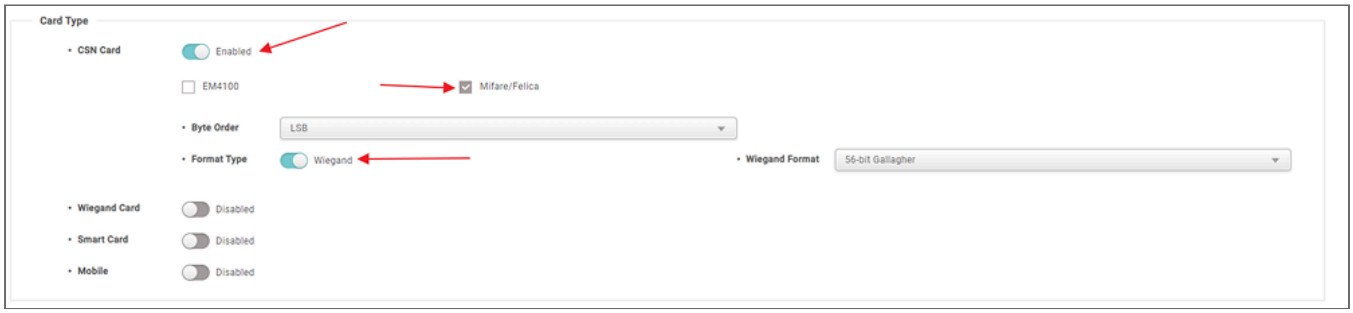
9. Los dispositivos conectados aparecerán en el panel de dispositivos del lado izquierdo.



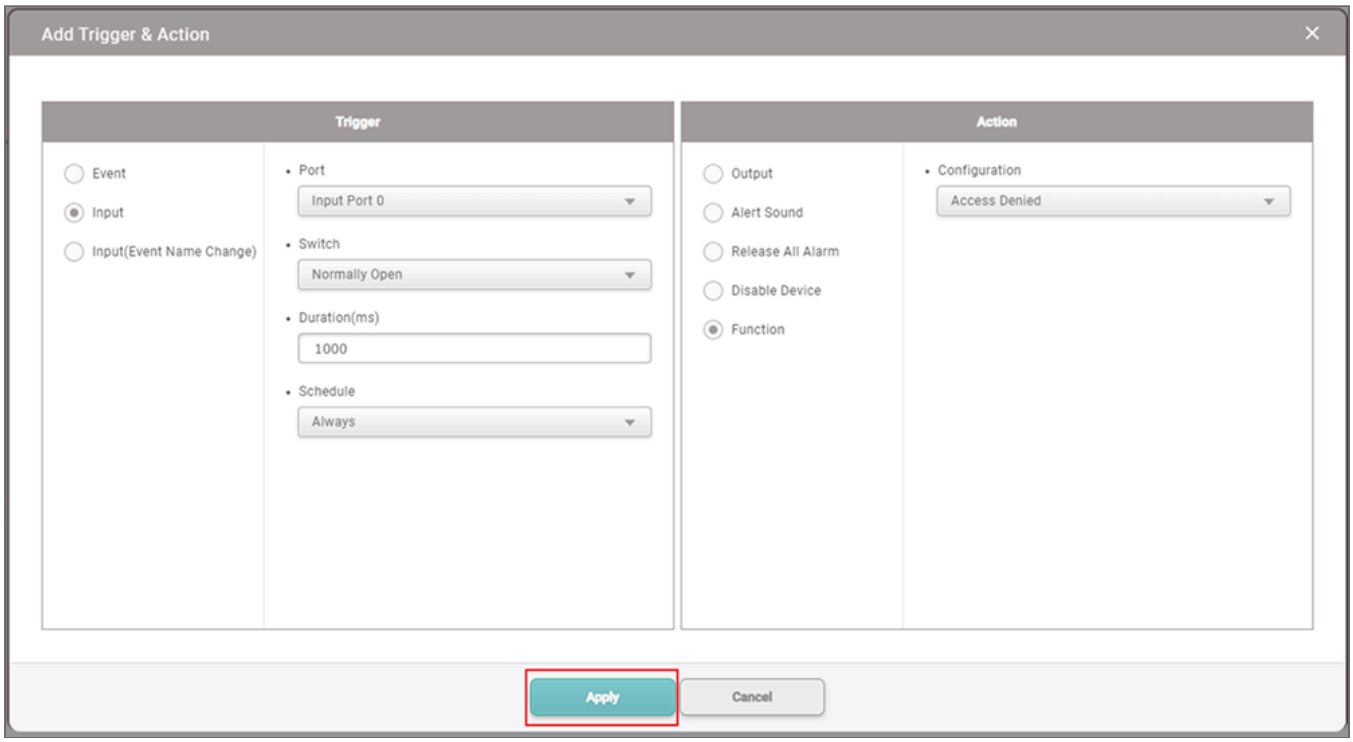
CONEXIÓN DEL READER Wiegand

1. **Haz clic** en el dispositivo que está conectado mediante la conexión Wiegand. **Desplázate hacia abajo** hasta ver Card Type.

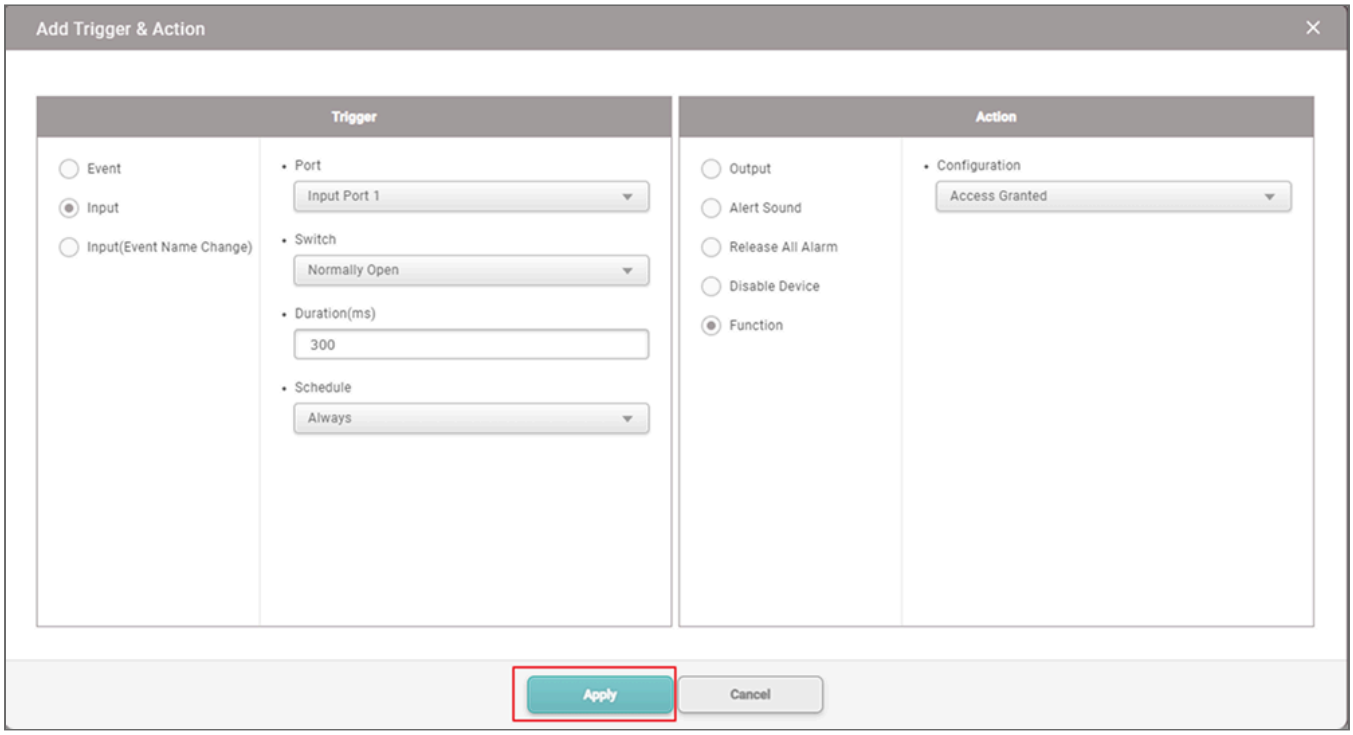
   Activa la **card CSN**, **marca Mifare/Felica**, **establece** el tipo de formato como **Wiegand**, el orden de bytes como **LSB** y el formato Wiegand como **56-bit Gallagher**.



2. Ahora **ve** a la configuración avanzada y desplázate hacia abajo hasta ver trigger and action; **presiona** el botón add y **establece** el campo como se muestra en la imagen.



3. Vuelve a **presionar** el botón add para agregar otro trigger and action.



4. En la sección Advanced, debajo de Trigger & Action: la configuración Wiegand debe establecer Input/Output como **Output**, Wiegand Input Format como Default, Pulse width como **40**, pulse interval como **10000**, output mode como **normal**, marca fail code y output info como **Card ID**.



CONEXIÓN DEL READER OSDP

1. Para la conexión OSDP, **haz clic** en el dispositivo conectado al panel OSDP y desplázate hacia abajo hasta ver Serial.

   Establece RS485 como Default y Baud rate como **115200**.



2. En intelligent slave expectation, configura code as **Enabled**, output info as Card ID y OSDP ID como **0**.

> **Información**
> Si tienes más dispositivos OSDP, cambia el OSDP ID a otro número y, para output, Info debe ser Card ID.

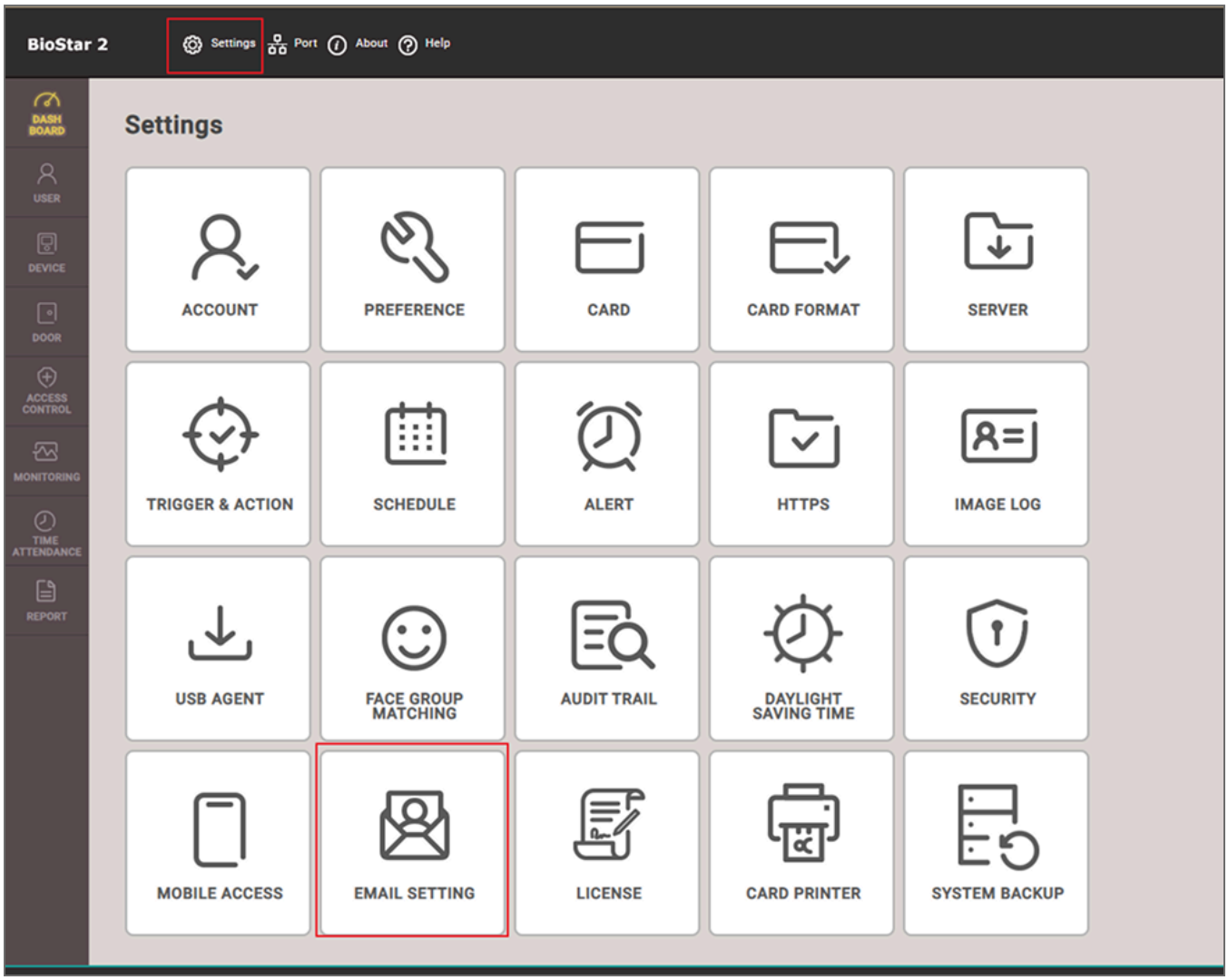


Configuraciones de correo electrónico para el código QR

Información

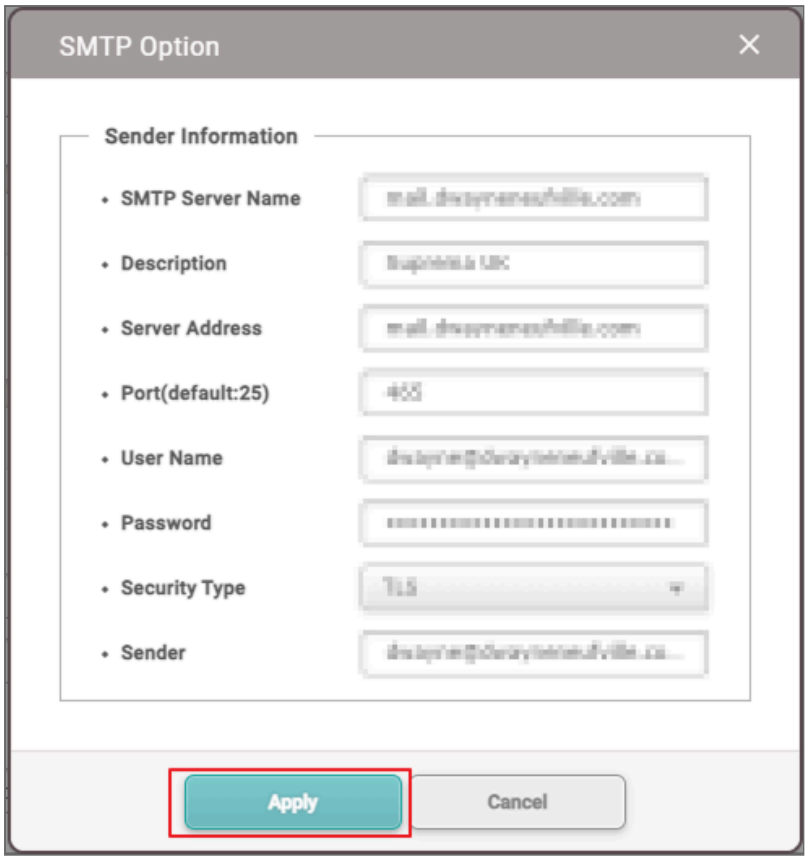
- Las confirmaciones por correo electrónico y los correos electrónicos para los perfiles de usuario son obligatorios para QR Code.
- Se requieren licencias para los correos electrónicos. Contacta al administrador para obtener la licencia necesaria.

1. **Ve** a la página de ajustes y **selecciona** Email Settings.



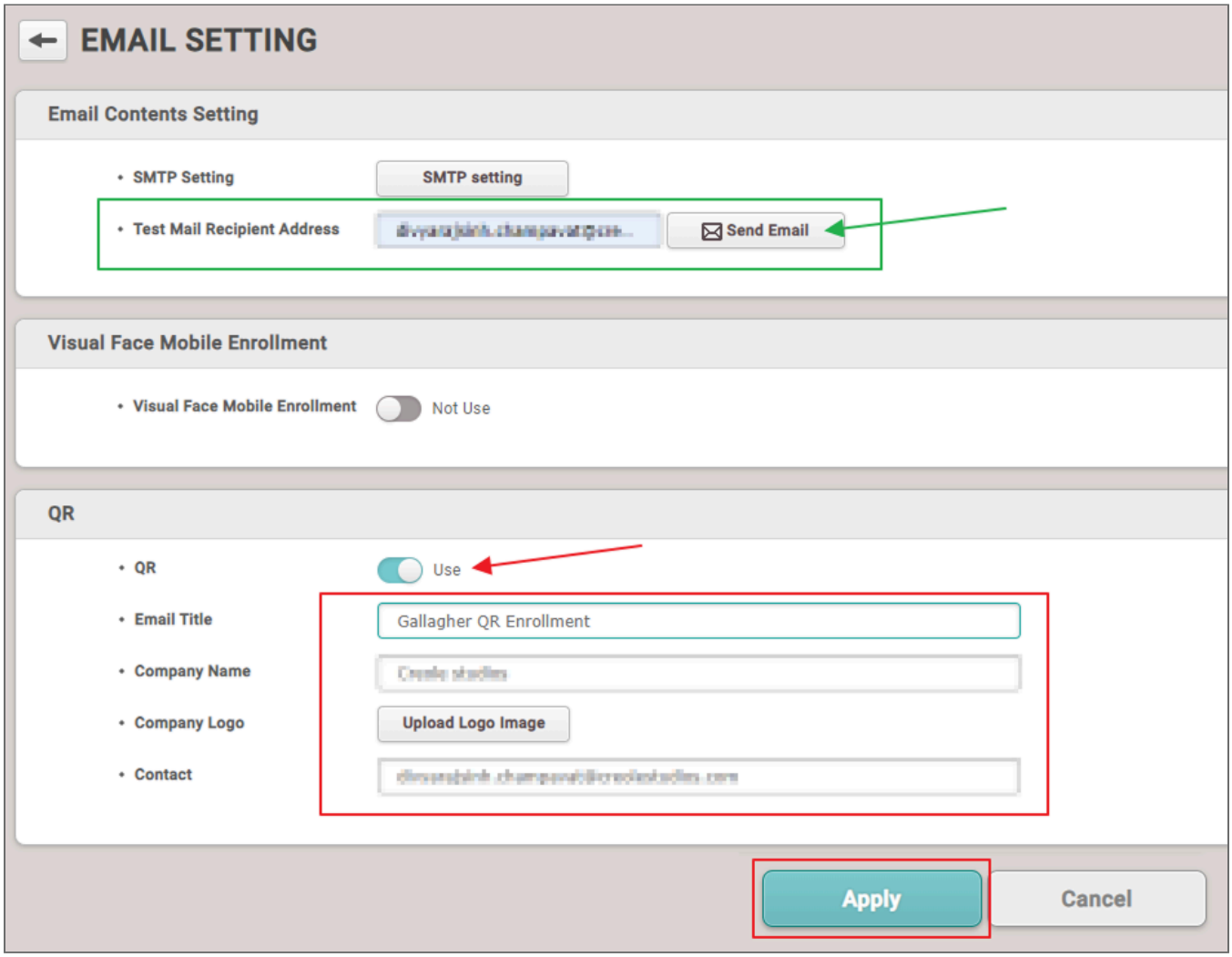
2. **Presiona** el botón de configuración SMTP dentro de Email Settings, completa los detalles de la opción SMTP y **presiona**

el botón Apply.



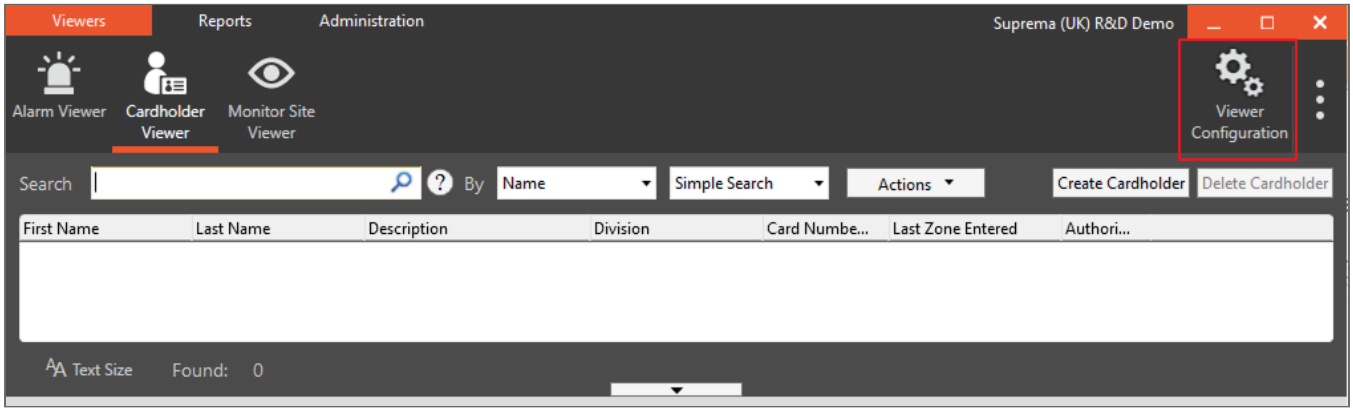
3. Para verificarlo, usa la función de correo de prueba: debes ingresar la dirección de correo que deseas probar y **presionar** el botón send email.

   Para usar la tarjeta QR Code, **habilita** la opción QR dentro de los ajustes, ingresa los detalles según los requisitos y **presiona** el botón Apply.



Integración de Suprema con Gallagher v2.0

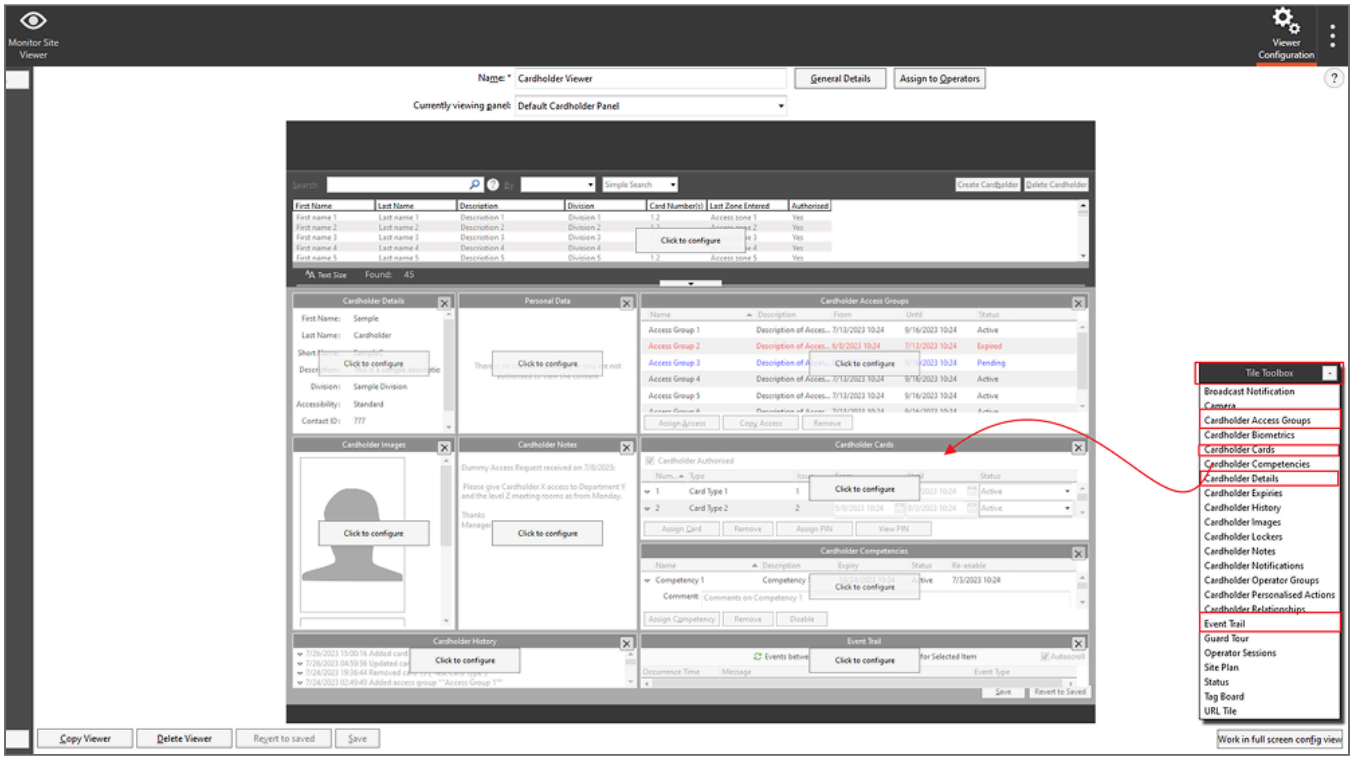
1. **Abre** Gallagher Command Centre en la opción Cardholder viewer y **ve** a viewer configuration.



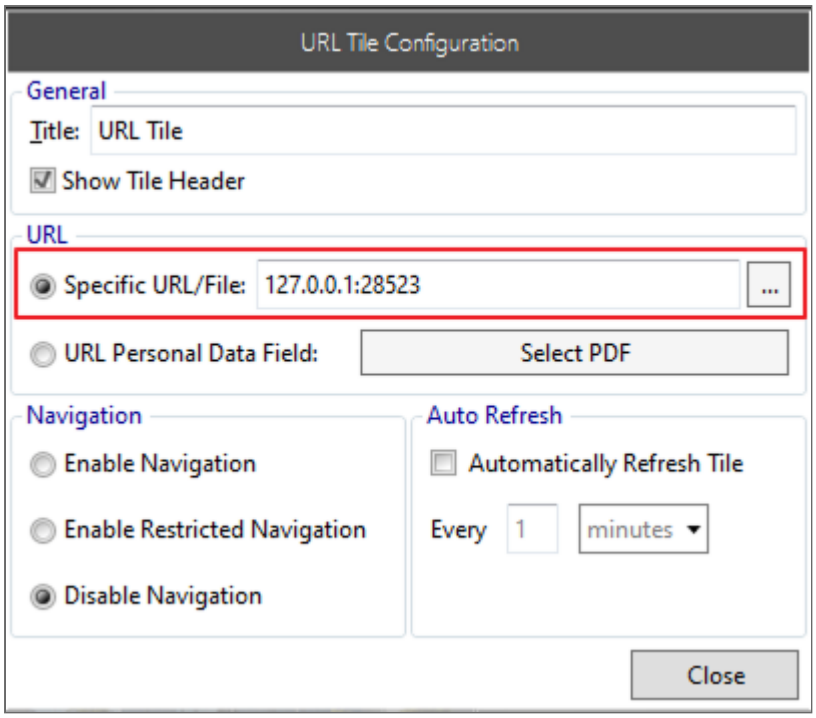
2. En Viewer Configuration, configura las ventanas como se muestra en la imagen siguiente y usa la ventana de herramientas para **arrastrar y soltar** ventanas.

   - Detalles del titular de la tarjeta
   - Grupos de acceso del titular de la tarjeta
   - Tarjetas del titular de la tarjeta

- Historial de eventos
- Elemento URL
- Imágenes del titular de la tarjeta



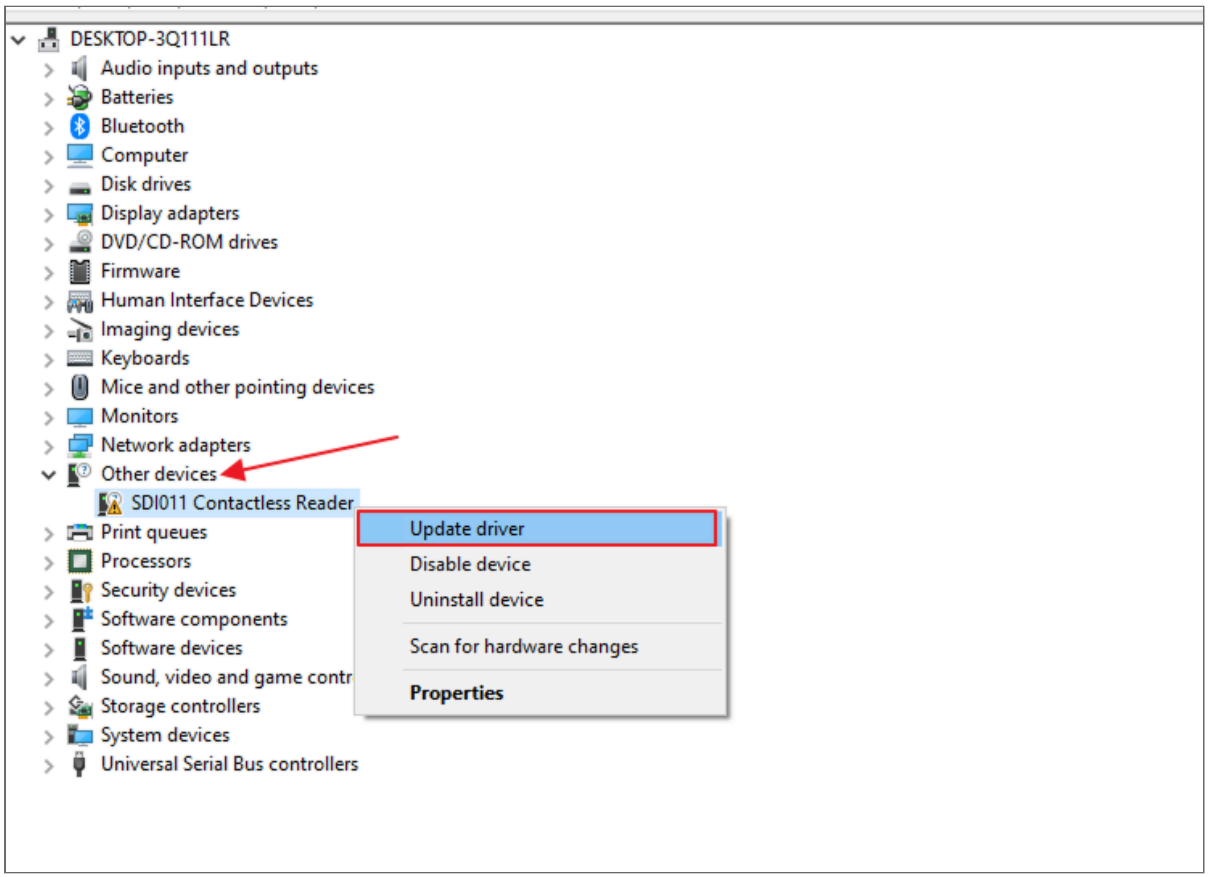
3. En la ventana URL, **haz clic** para configurar la URL específica en `<127.0.0.1>:28523` y elige navegación como Disable Navigation. Y **presiona** el botón de guardar para guardar la configuración.



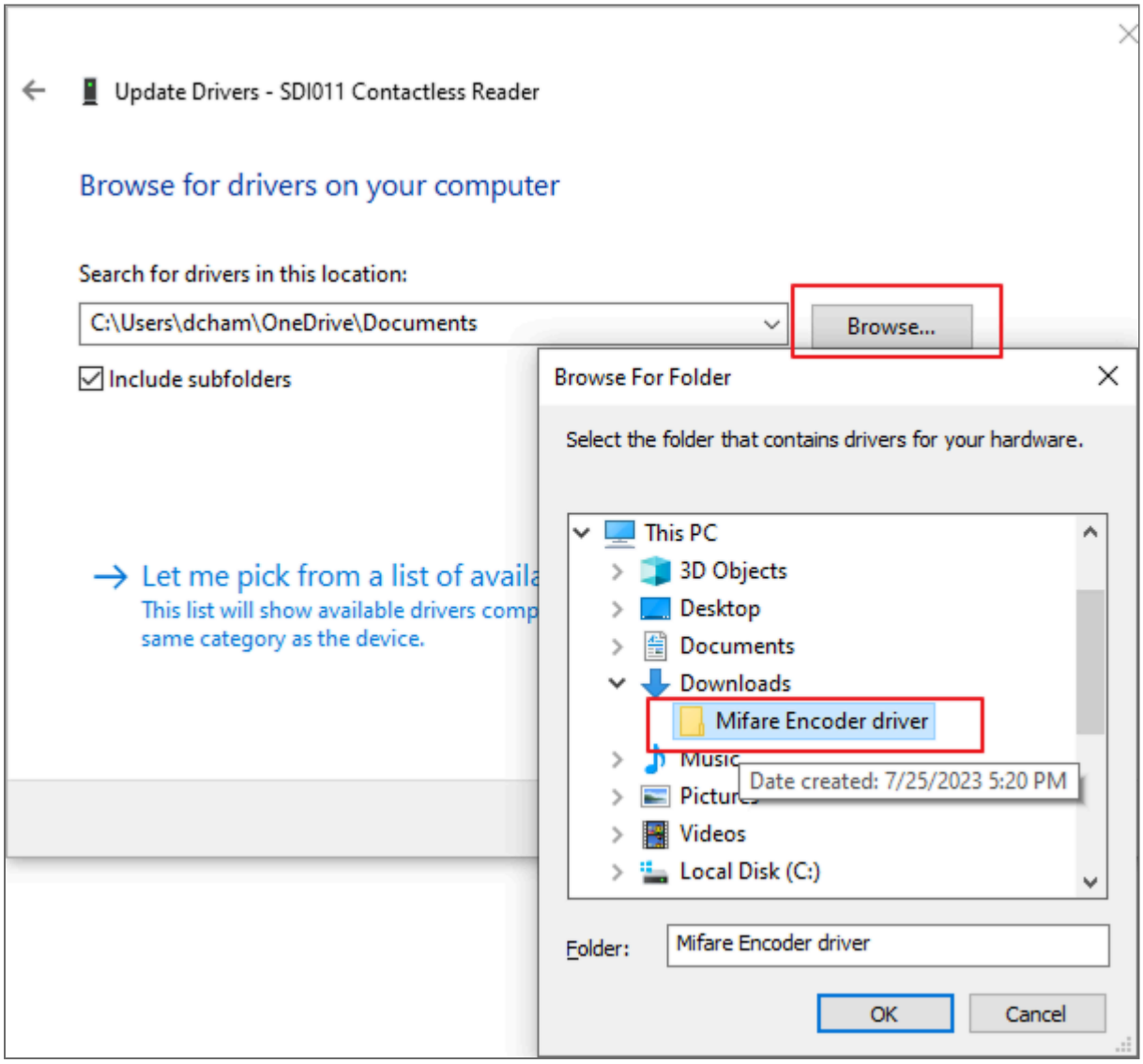
4. Después de completar la configuración, **presiona** el botón de guardar y luego **haz clic derecho** en viewer configuration y recarga el visor para ver el cambio.

5. **Conecta** el **Mifare Encoder** a la PC.

6. **Ve** al Administrador de dispositivos del sistema, en Otros dispositivos, **haz clic derecho** en SDI011 Contactless Reader (en tu caso puede ser un dispositivo diferente) y elige actualizar controlador.



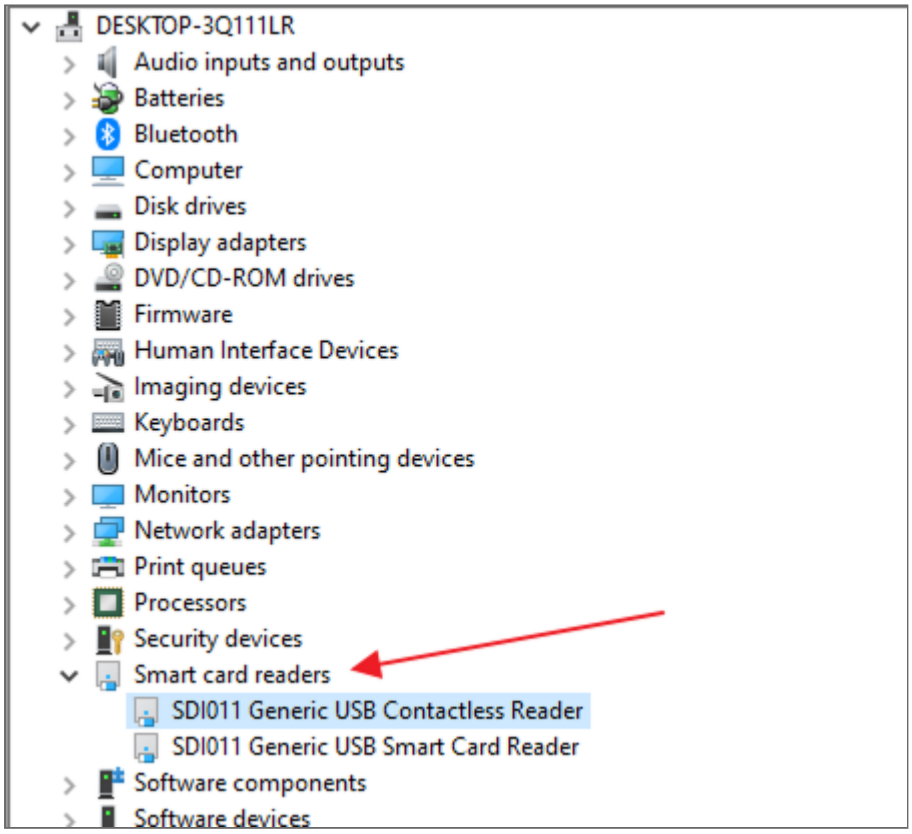
7. **Busca en mi equipo** el controlador y selecciona la carpeta que proporcionamos.



8. Cuando actualices el controlador por primera vez, estará disponible un lector de tarjeta inteligente.

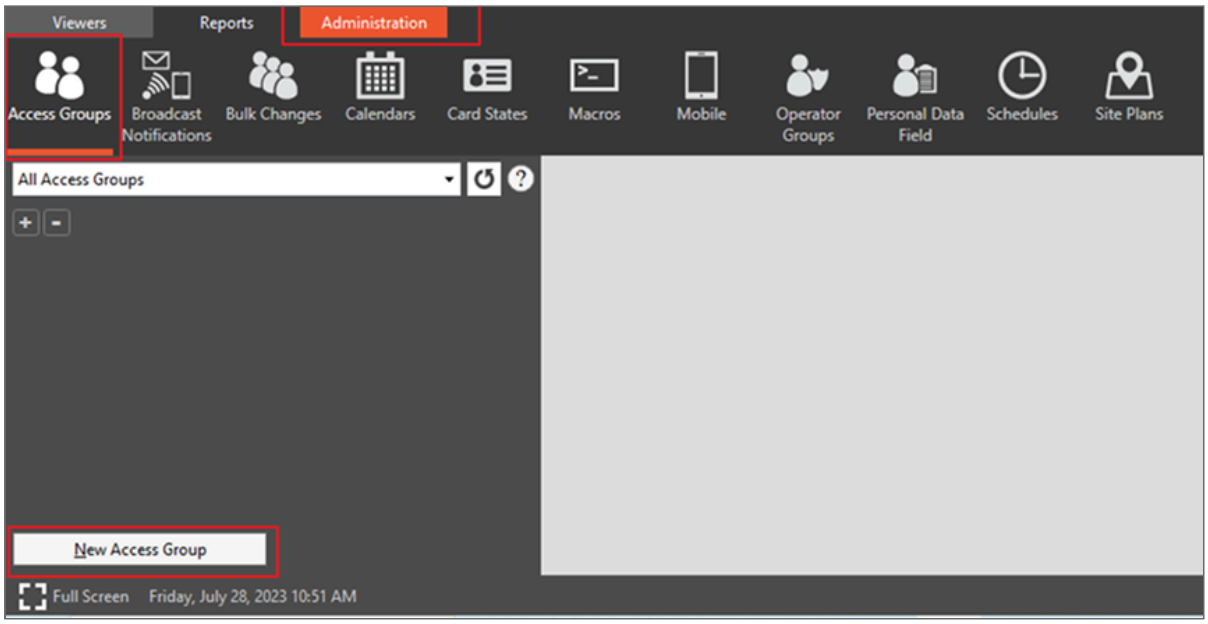
> **Información**
> El nombre del dispositivo USB puede diferir de un dispositivo a otro.

9. Ahora debemos actualizar de nuevo el controlador de Contactless Reader con el mismo archivo. Después verás que el nuevo controlador de tarjeta inteligente estará disponible.

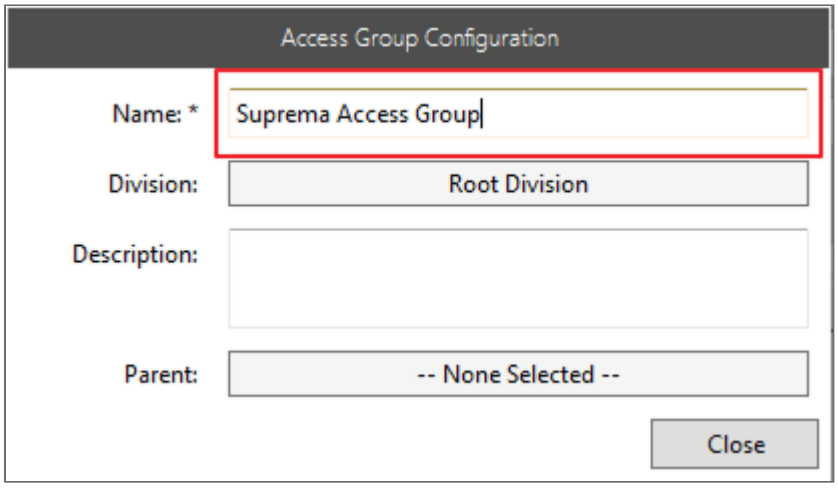


Agregar grupo de acceso

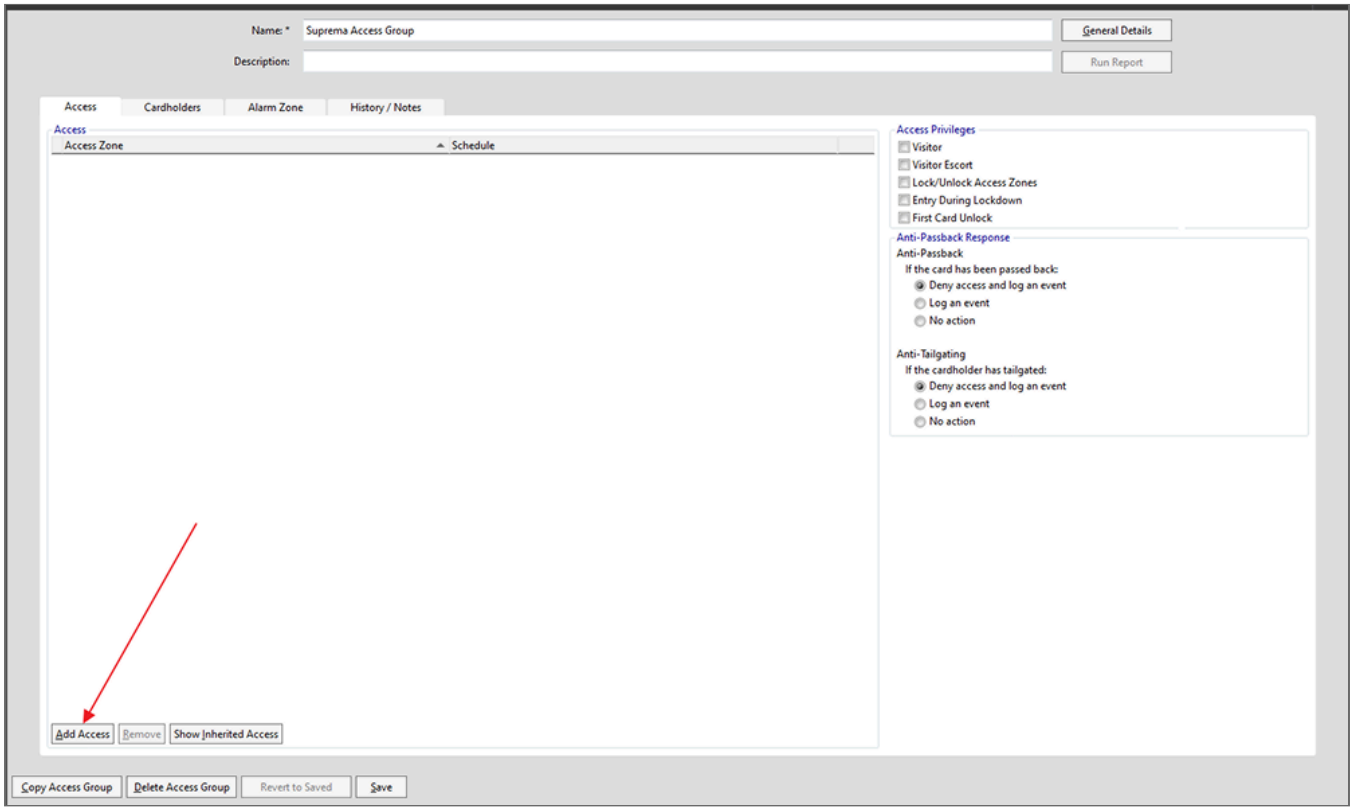
1. **Ve** a Administration, donde puedes ver **Access Groups** en la parte superior izquierda. **Haz clic** allí; luego verás el botón **New Access Group** en la parte inferior izquierda. **Haz clic** en ese botón.



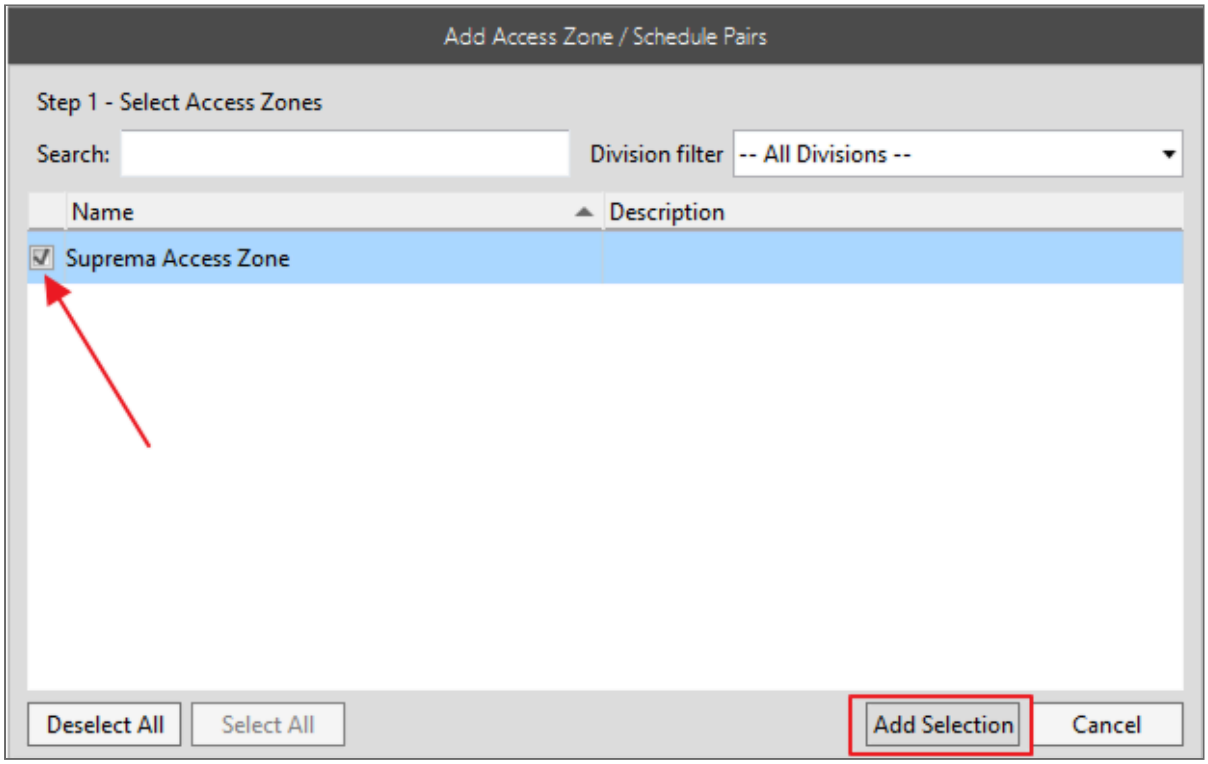
2. Después de **hacer clic en el botón New Access Group**, se abrirá una ventana emergente como se muestra en la imagen siguiente. **Establece** el nombre como **Suprema Access Group** y **haz clic** en el botón Close; luego la ventana emergente se cerrará.



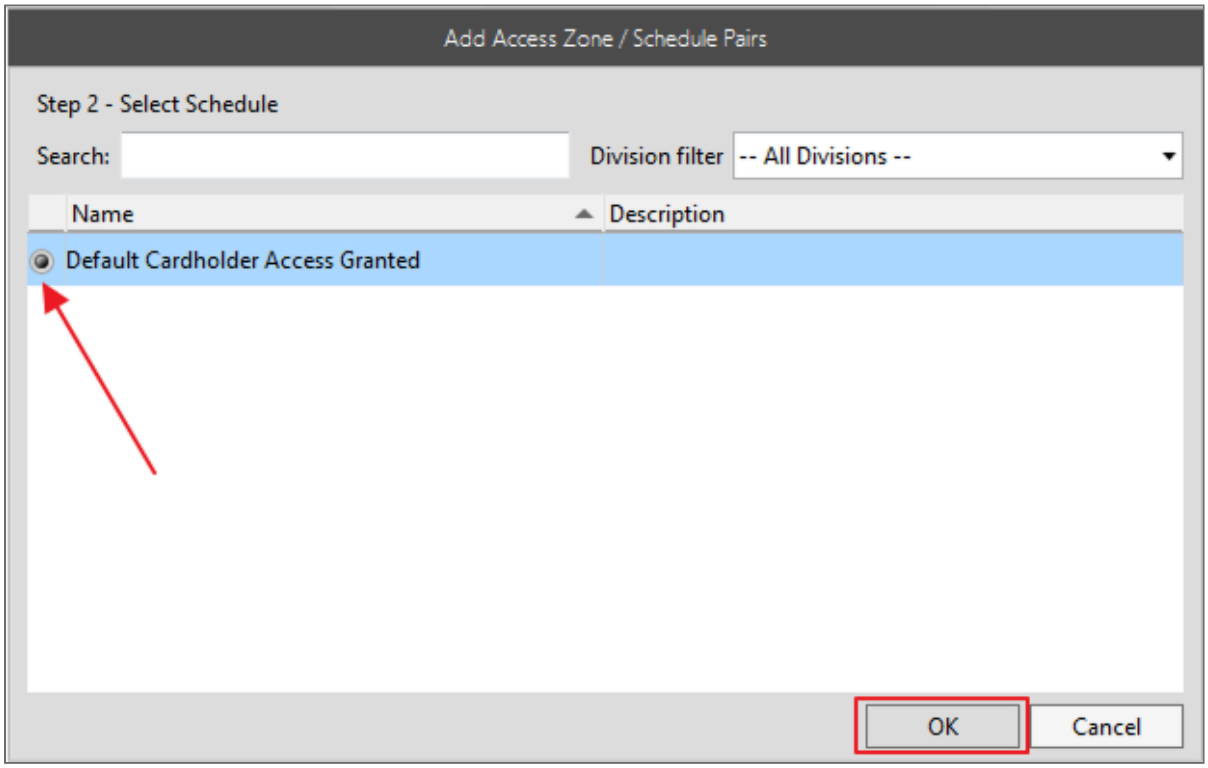
3. Después de **hacer clic** en el botón close, verás la pantalla que se muestra en la imagen siguiente; **haz clic** en el botón **Add Access** en la esquina inferior izquierda.



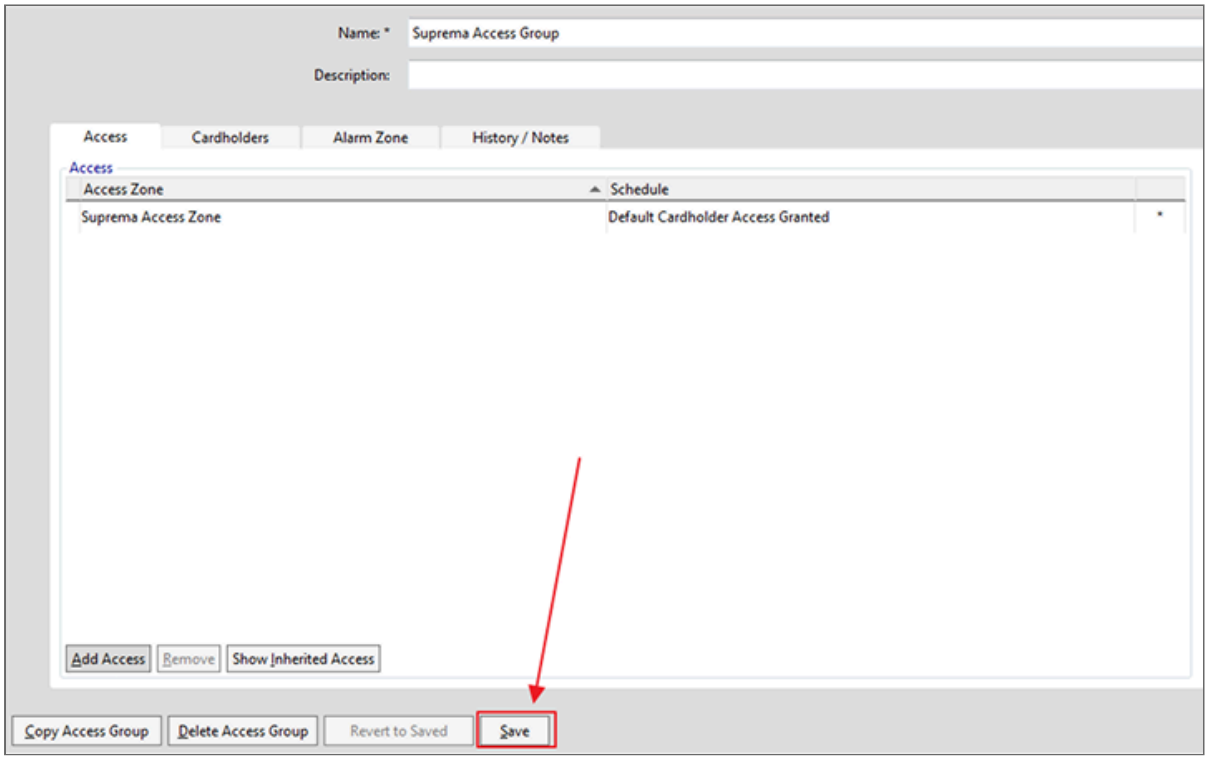
4. Después de **hacer clic en Add Access**, se abrirá una ventana emergente como se muestra en la imagen siguiente. Allí, **marca** la **casilla** y luego haz clic en el botón Add **Selection**.



Luego **marca** el botón de opción y haz clic en el botón **OK**; la ventana emergente se cerrará.

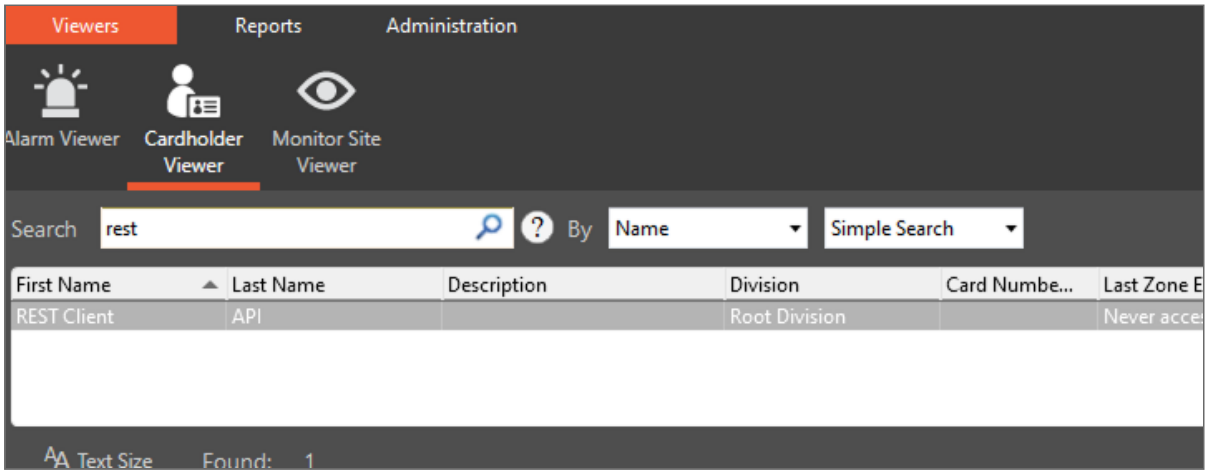


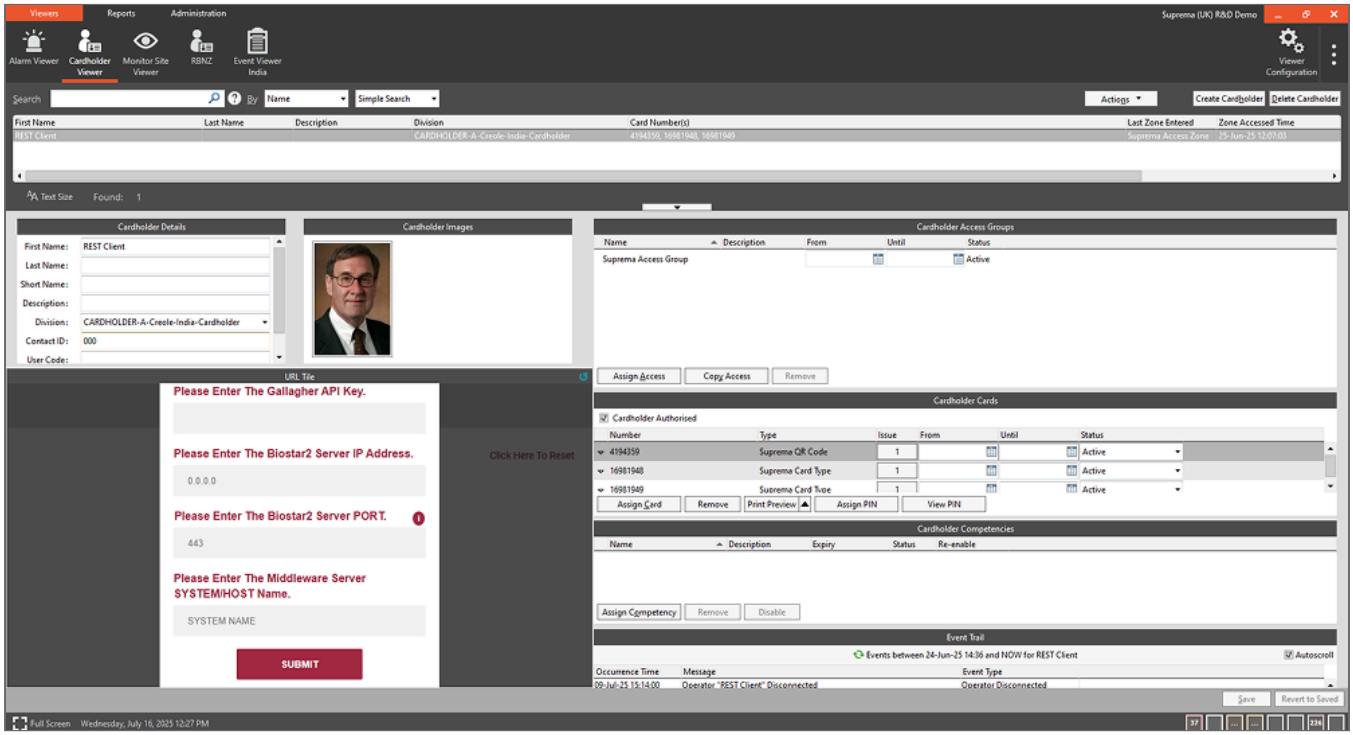
5. **Haz clic** en el botón **Save**; tu Access Group se agregará correctamente.


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

Integración de Suprema con Gallagher

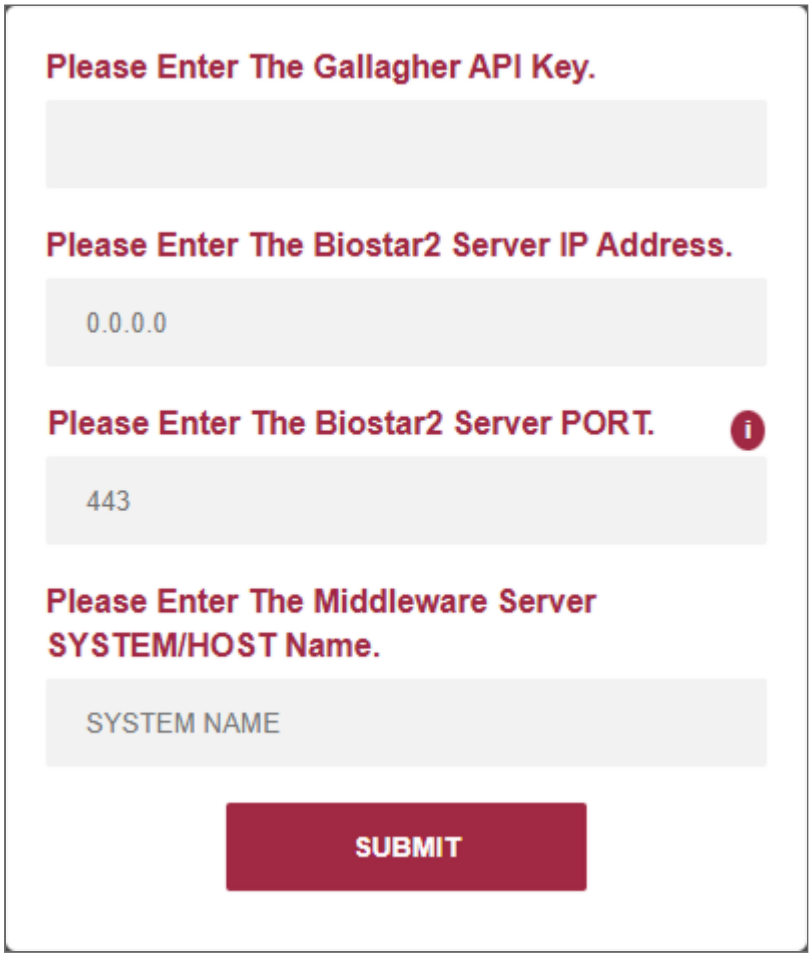
1. En Cardholder Viewer, busca rest y se cargarán todas las ventanas.



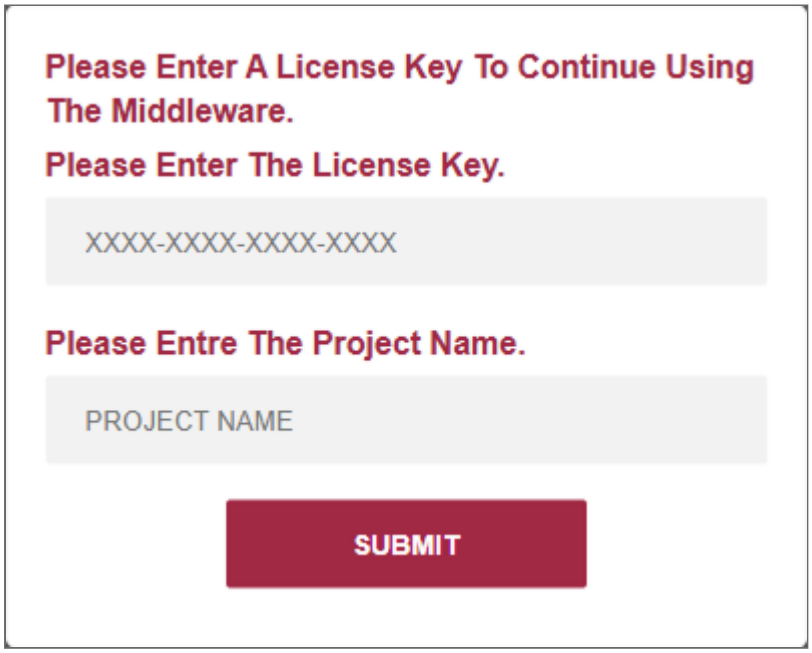


2. Primero, aparece la siguiente pantalla y debes **ingresar** la clave API de Gallagher, la IP del servidor BioStar 2, el puerto del servidor BioStar 2 y el nombre SYSTEM/HOST de la dirección del middleware para continuar.

> **Información**
>
> Si ejecutas el middleware en un puerto específico en dos servidores diferentes con direcciones IP particulares, consulta: Configura las reglas de entrada para el middleware.

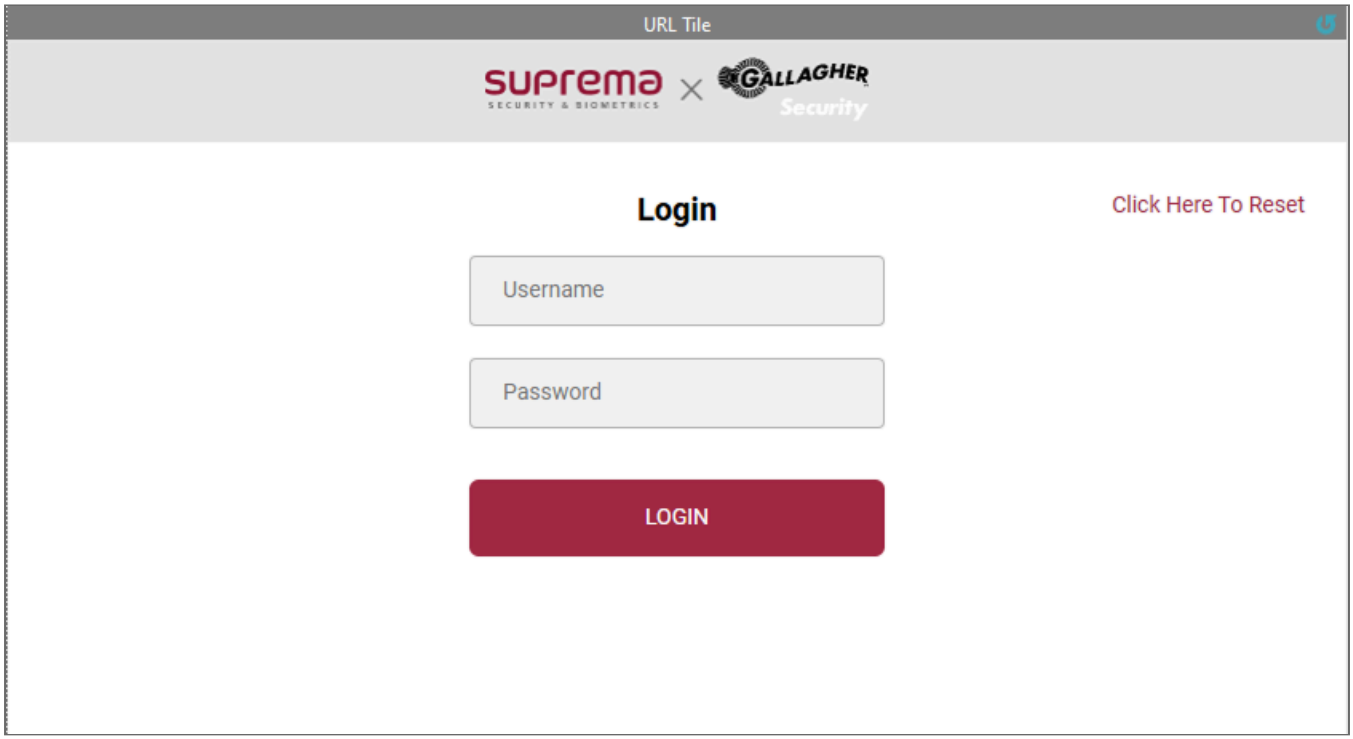


3. En la pantalla de licencia, **ingresa** la clave de licencia y el nombre de proyecto **exacto** que obtienes del administrador.

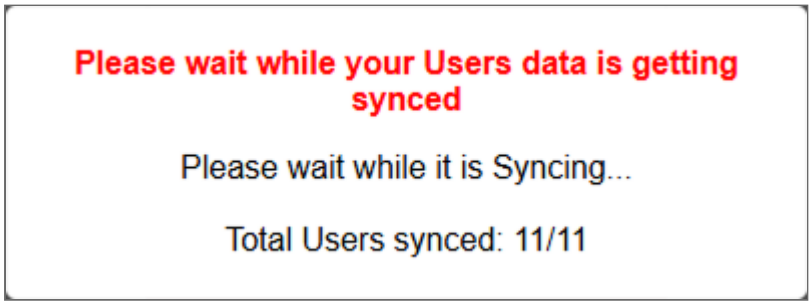


4. En la pantalla de inicio de sesión, **ingresa** las credenciales de Suprema BioStar 2.

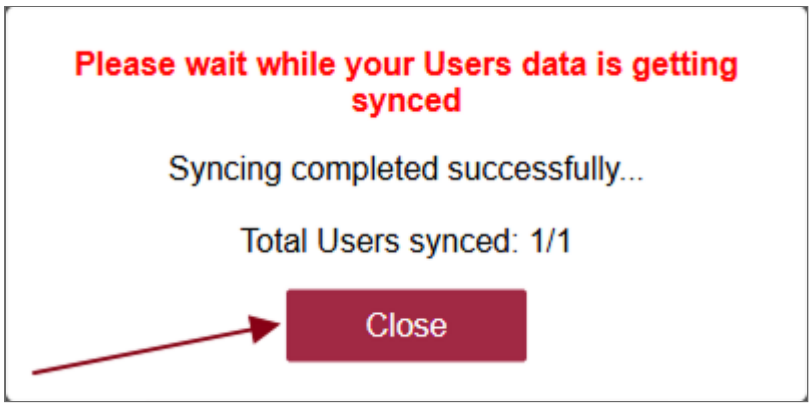
> **Información**
>
> En la pantalla de inicio de sesión, si obtienes un **error** por **LAN desconectada o IP cambiada para (dirección IP)**. Consulta: Solucionar error de la página de inicio de sesión.



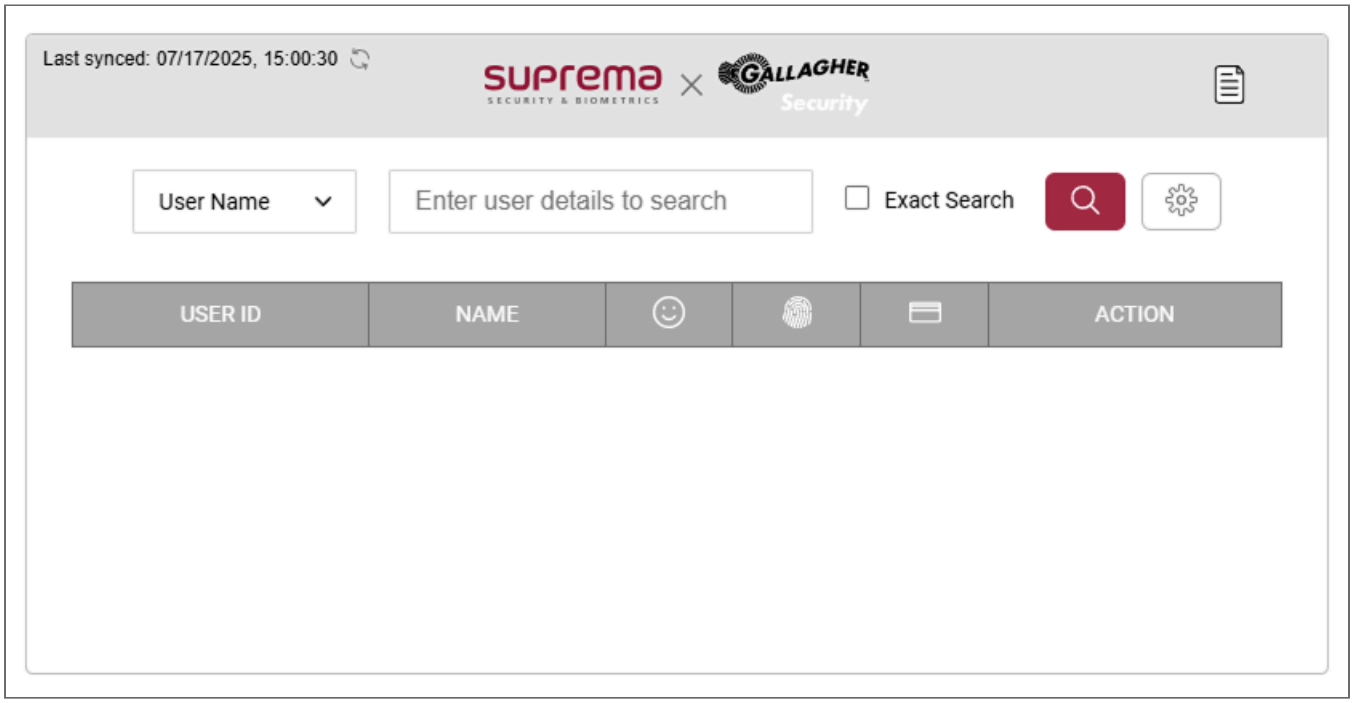
Después de ingresar las credenciales correctas, se abrirá la siguiente pantalla de sincronización de usuarios para la sincronización inicial.



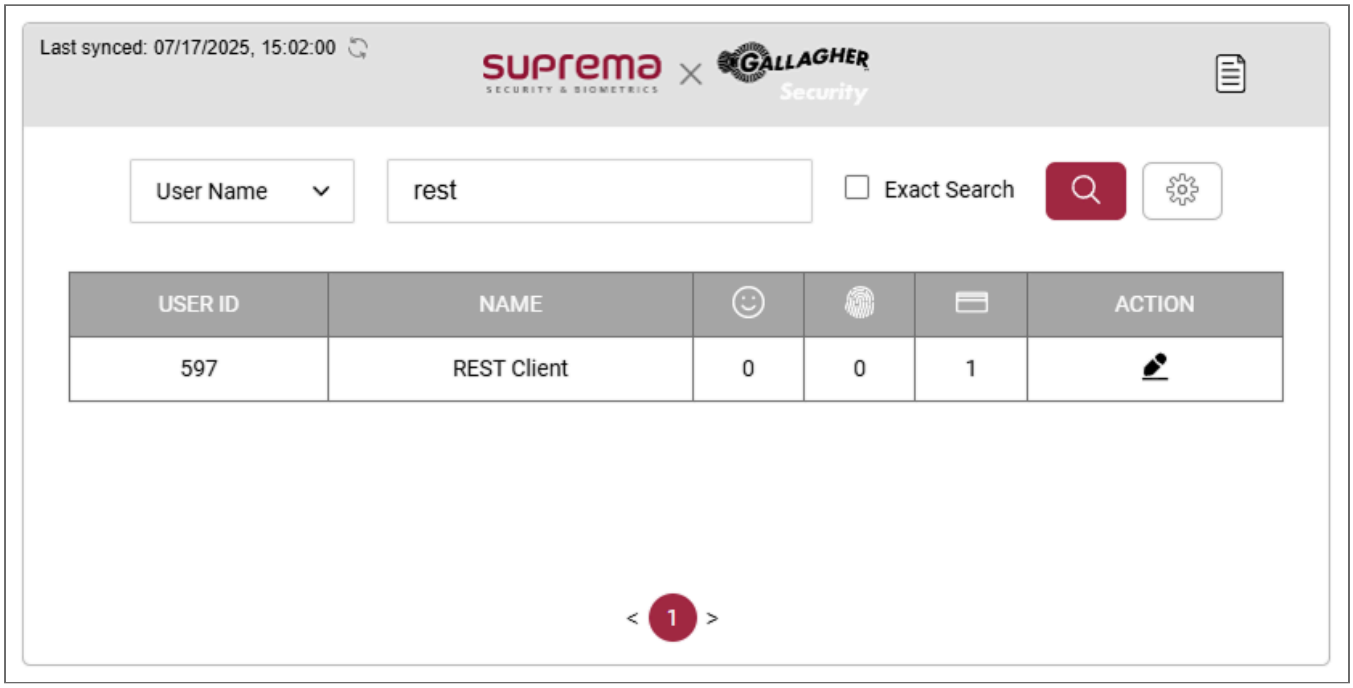
Después de sincronizar correctamente los usuarios, aparecerá el botón Cerrar en la pantalla, y al **presionar** el botón Cerrar podrás continuar.



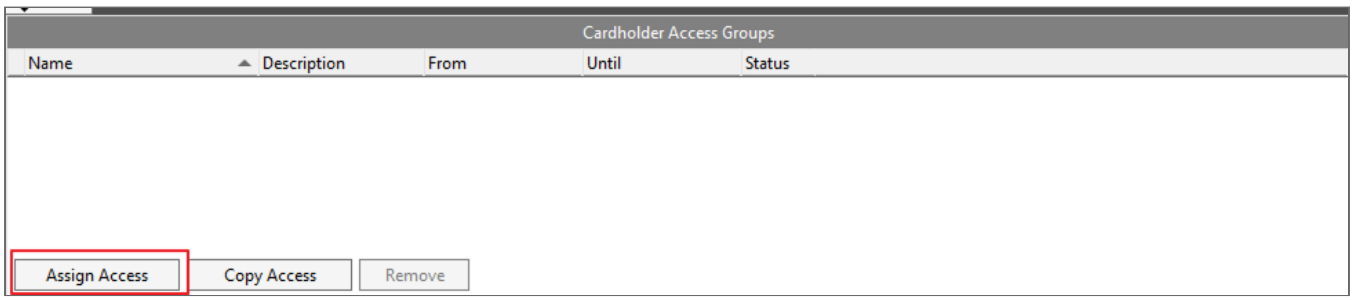
Después de sincronizar correctamente los usuarios, aparecerá la pantalla de búsqueda de usuarios.

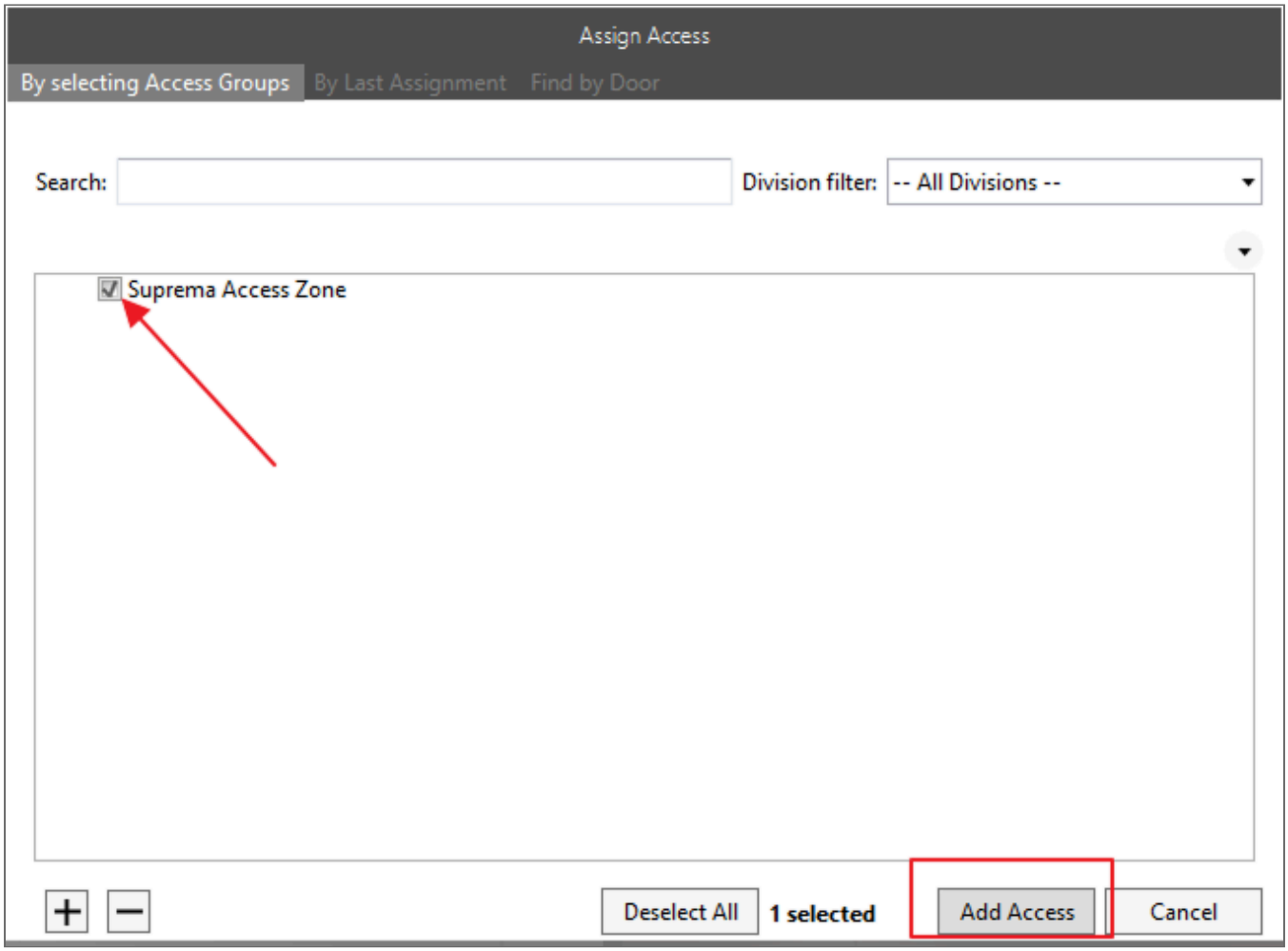


5. **Busca** rest y presiona el botón de búsqueda; el usuario buscado aparecerá en la tabla.



6. Ahora, conecta el codificador Mifare al sistema. **Presiona** el botón Asignar acceso, elige el grupo de acceso Suprema que creamos y **presiona** el botón Guardar.

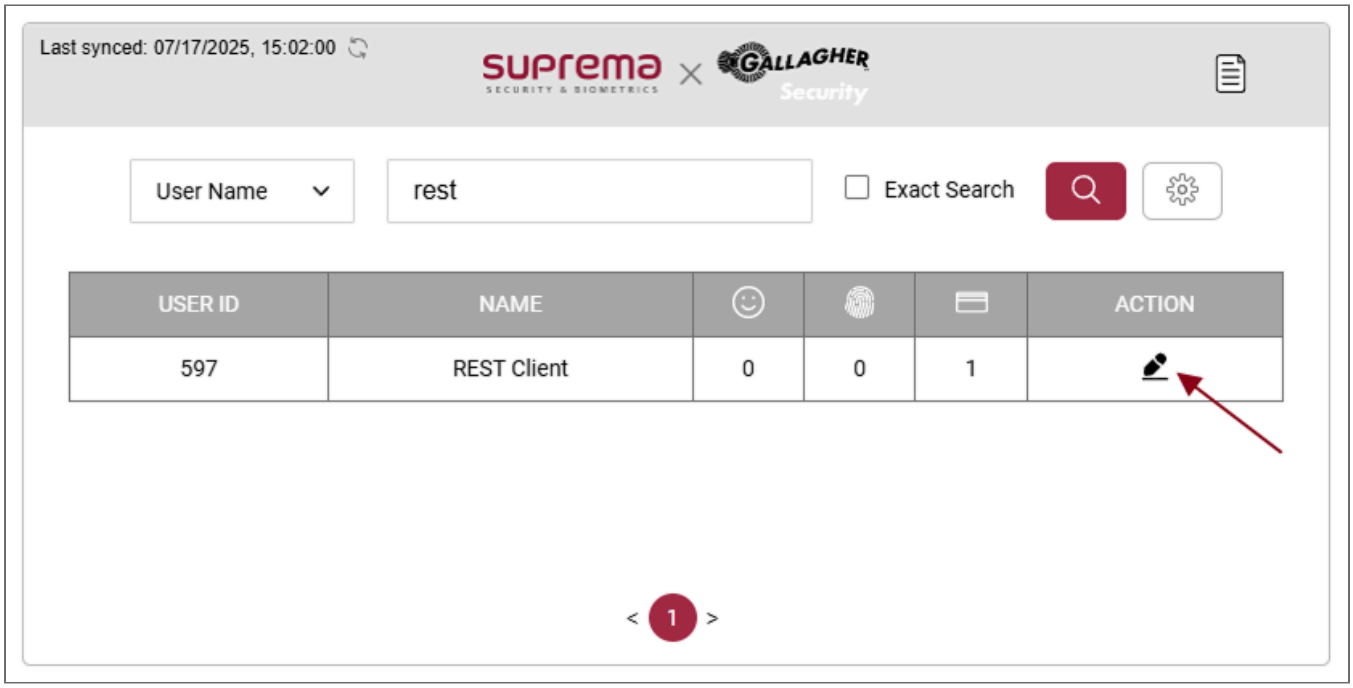




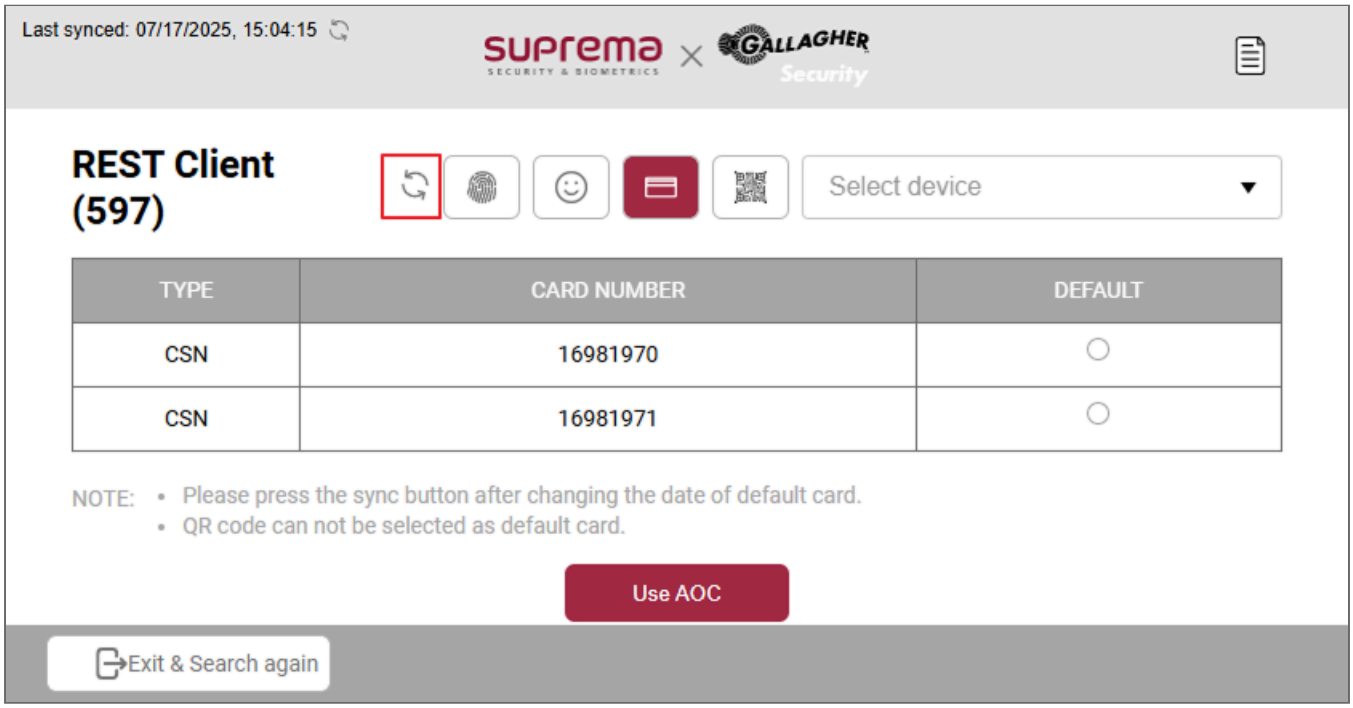
7. Después de agregar el grupo de acceso y conectar el codificador Mifare, haz **clic derecho** en Viewer Configuration y vuelve a cargar el visor.

8. Al **colocar** la tarjeta en el botón Assign Card del codificador, al **presionar** ese botón se asignará la tarjeta al usuario; después, **presiona** el botón **Guardar**. Luego **presiona** el botón **Editar** en el middleware.

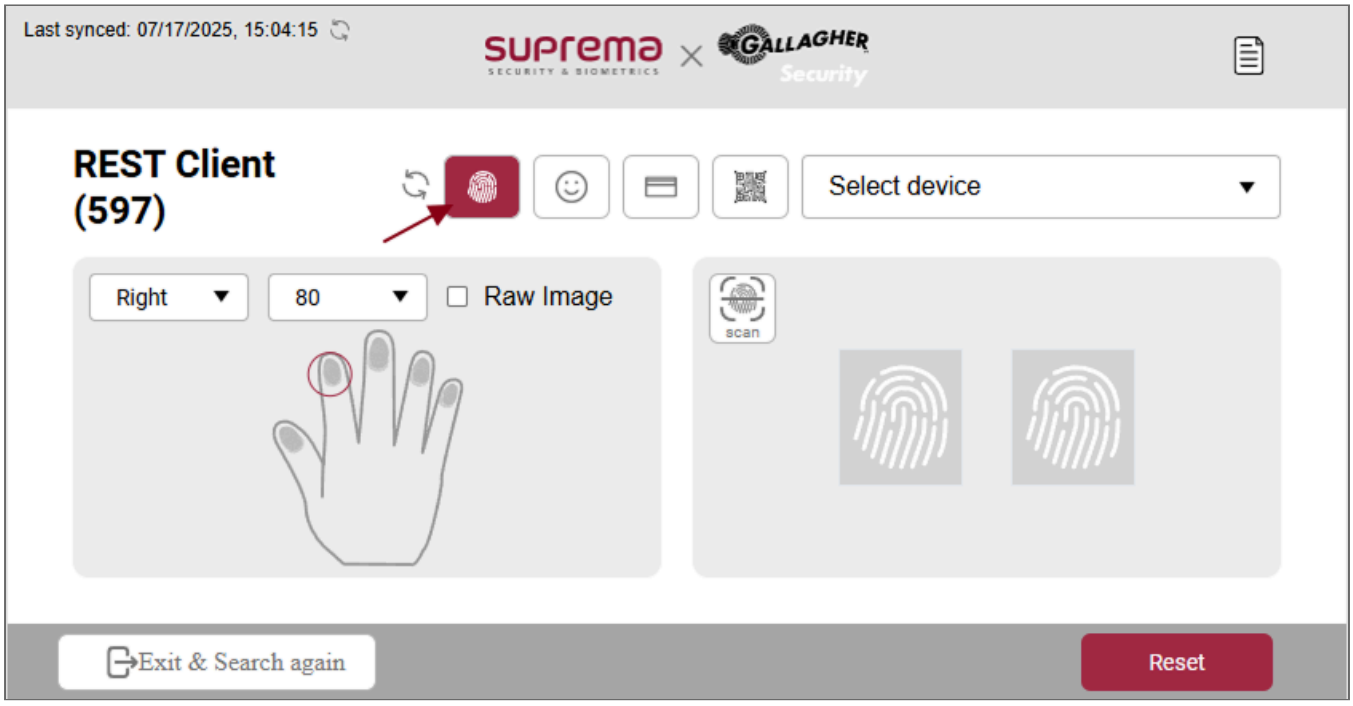
> **Información**
> Si solo quieres inscribir datos biométricos, no asignes ninguna tarjeta antes; solo **presiona** el botón Editar después de asignar la zona de acceso.



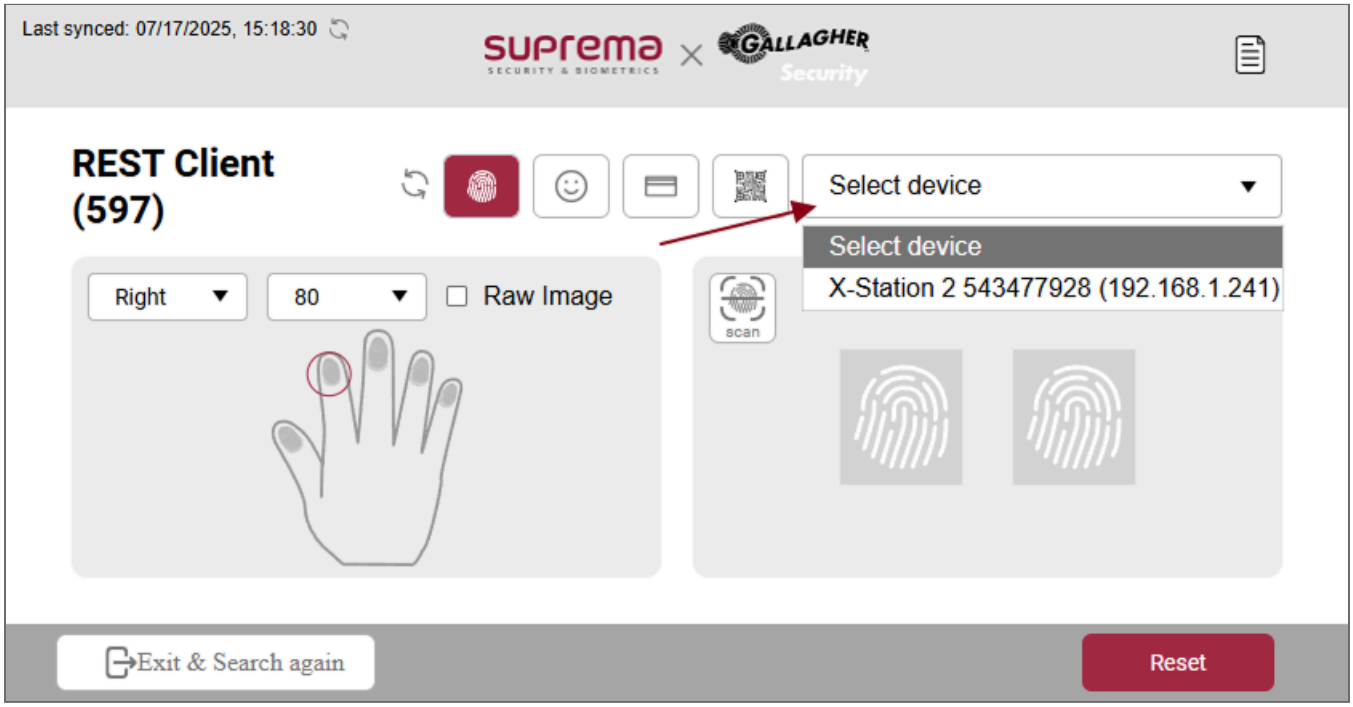
Puedes asignar varias tarjetas al usuario; cuando asignes la tarjeta y **presiones** el botón Guardar, **presiona** el botón verde de **sincronización** para sincronizar todos los datos de ese usuario.



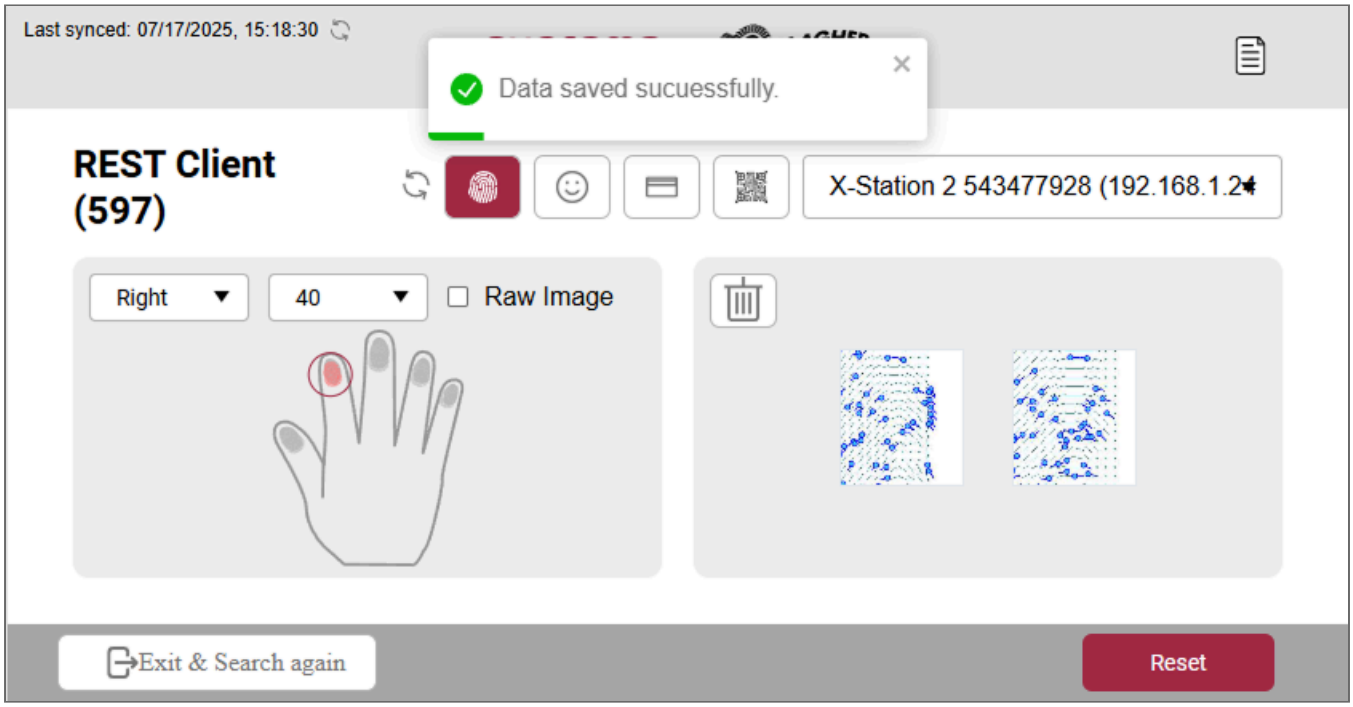
9. **Presiona** el botón Fingerprint y se cargará el módulo de huella dactilar.



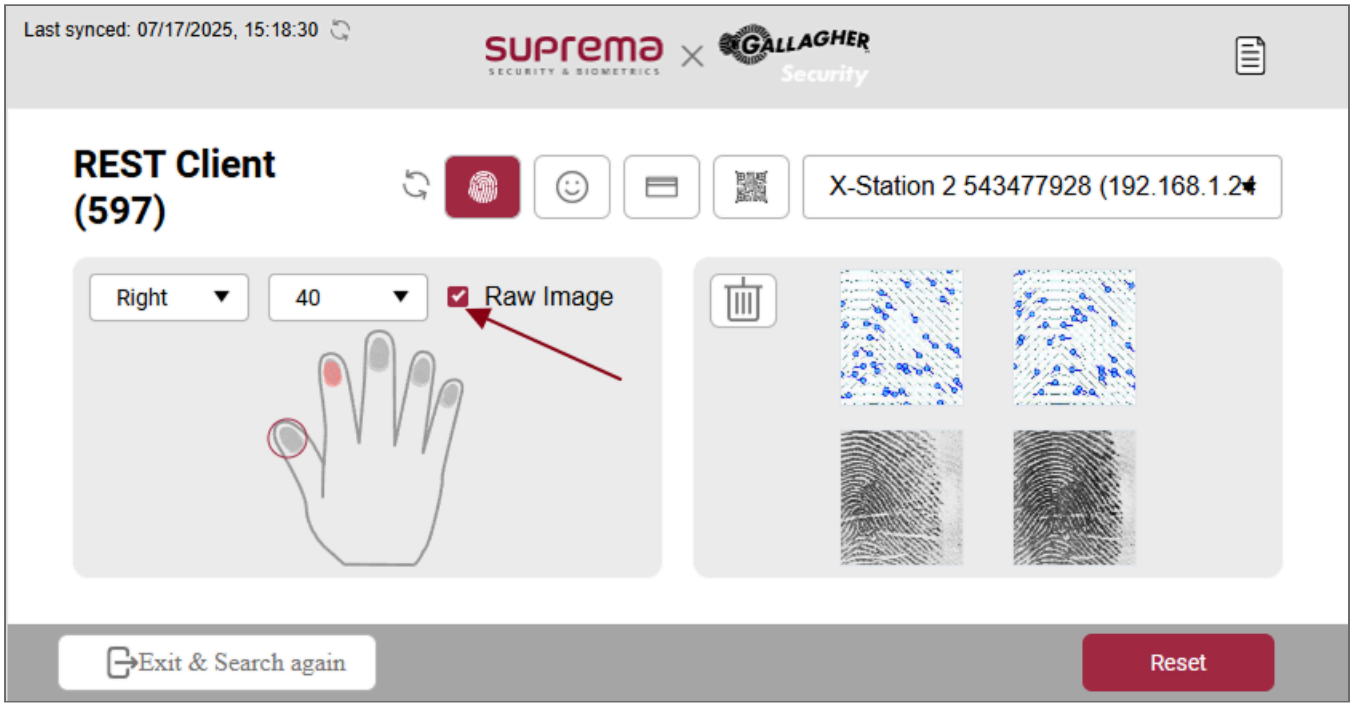
10. **Selecciona** el dispositivo de la lista.



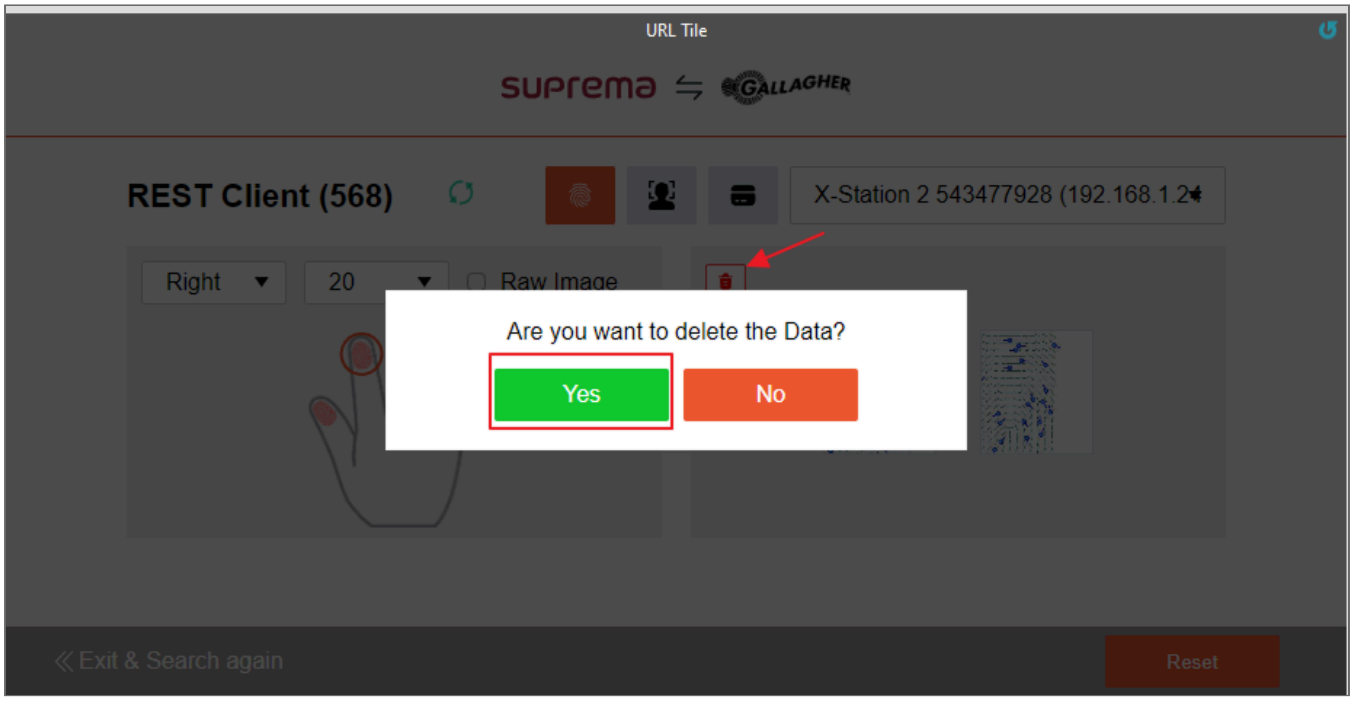
11. Puedes **seleccionar** la mano izquierda o derecha; después, elige la calidad de la huella dactilar y **presiona** el botón de escaneo para iniciar el escaneo. Cuando el escaneo se complete, el botón de escaneo cambiará al botón eliminar y la huella dactilar aparecerá en la pantalla. Los datos se almacenarán automáticamente; cuando se guarden correctamente, la huella dactilar guardada se mostrará en color.



12. Si necesitas una imagen sin procesar, marca la casilla Raw Image y luego **escanea** el dedo.

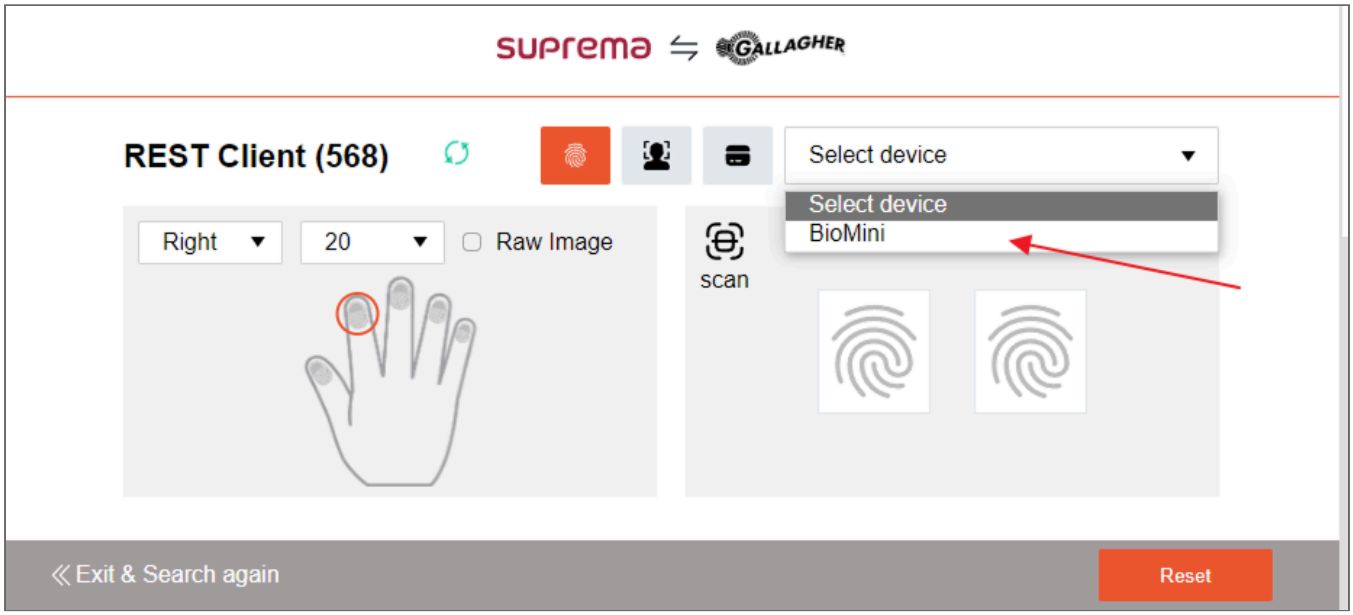


13. Para eliminar una sola huella dactilar, **presiona** el botón **Eliminar**; aparecerá una ventana emergente y luego **presiona** el botón **Sí**. Se eliminará esa huella dactilar.

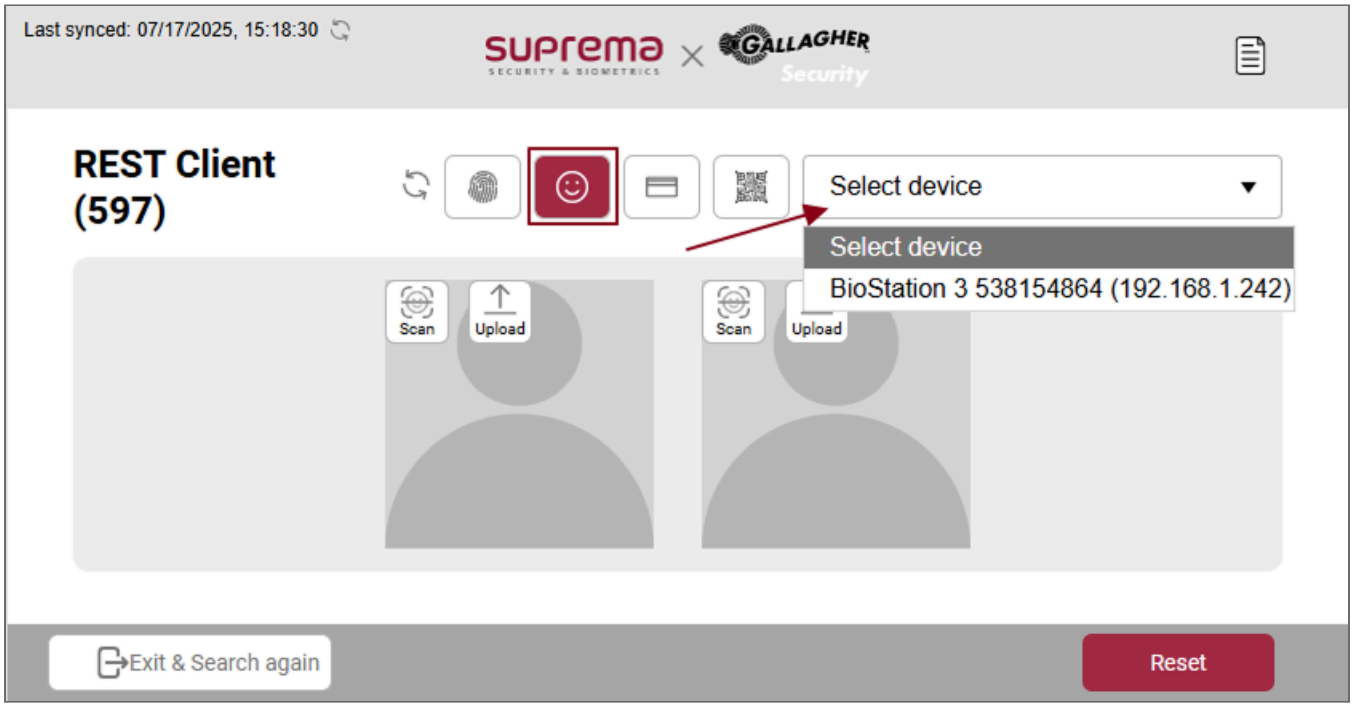


Para restablecer todos los datos de huellas dactilares, **presiona** el botón **Restablecer**; aparecerá una ventana emergente y luego **presiona** Sí. Se restablecerán todos los datos de huellas dactilares.

14. Podemos usar BioMini Plus 2 para inscribir datos de huellas dactilares de usuarios. Para ello, solo conecta el dispositivo y lo verás dentro de la **sección** de selección de dispositivos de huellas dactilares. **Selecciona** el dispositivo e inicia la inscripción de datos del usuario.



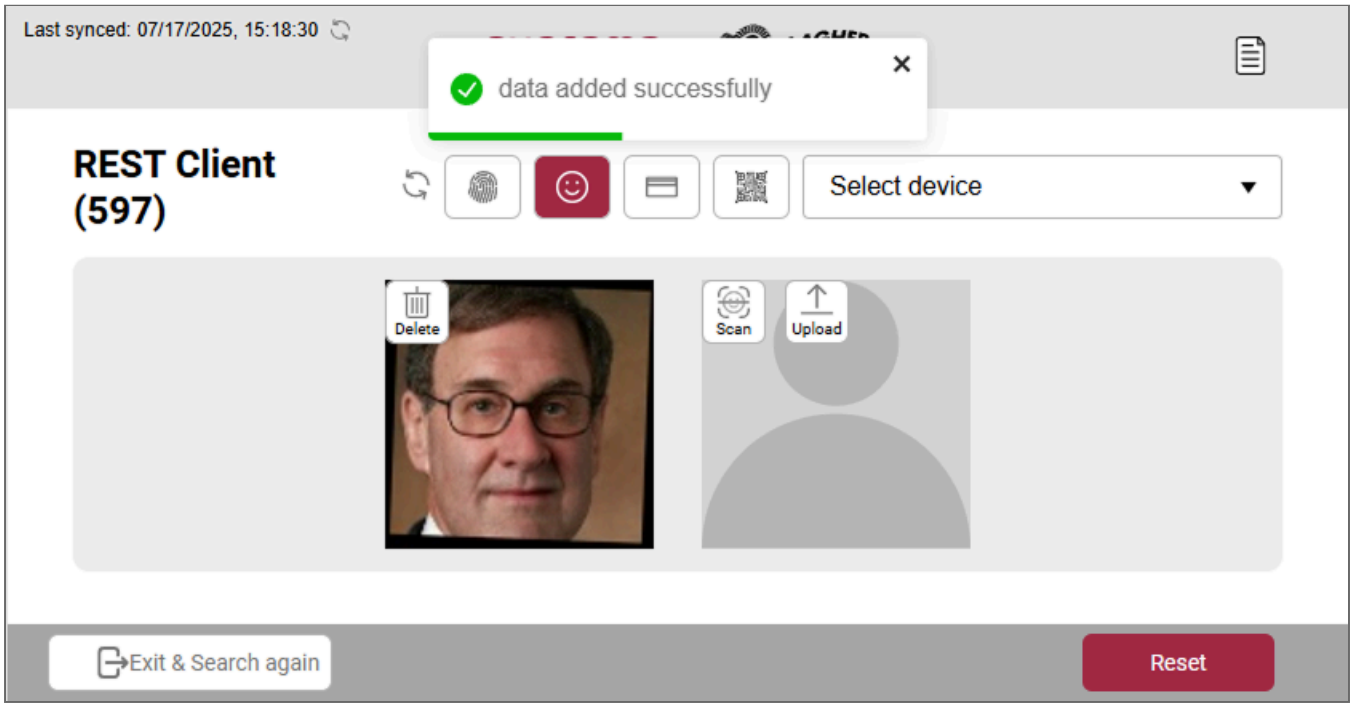
15. Para inscribir el rostro visual, **presiona** el botón junto a la huella dactilar; se cargará el módulo de rostro visual.



Hay dos métodos para escanear el rostro visual. Podemos cargarlo o escanear el rostro para inscribirlo.

16. **Presiona** el icono de **carga**; luego se abrirá una nueva ventana y podrás elegir la imagen que deseas cargar.

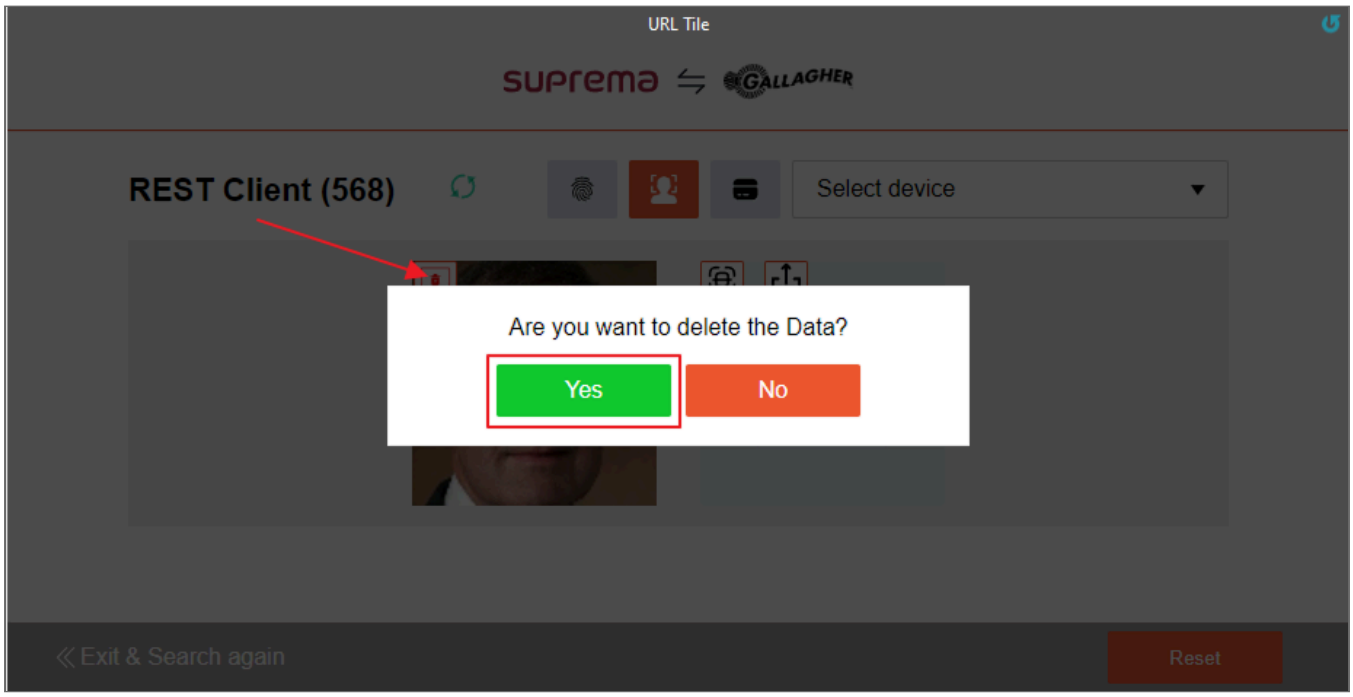
Si **presionas** el botón de **escaneo**, se activará el dispositivo que seleccionaste; usa ese dispositivo seleccionado para escanear tu rostro. Los datos se almacenarán automáticamente después de cargar o escanear el rostro visual, y luego aparecerá un mensaje de éxito.



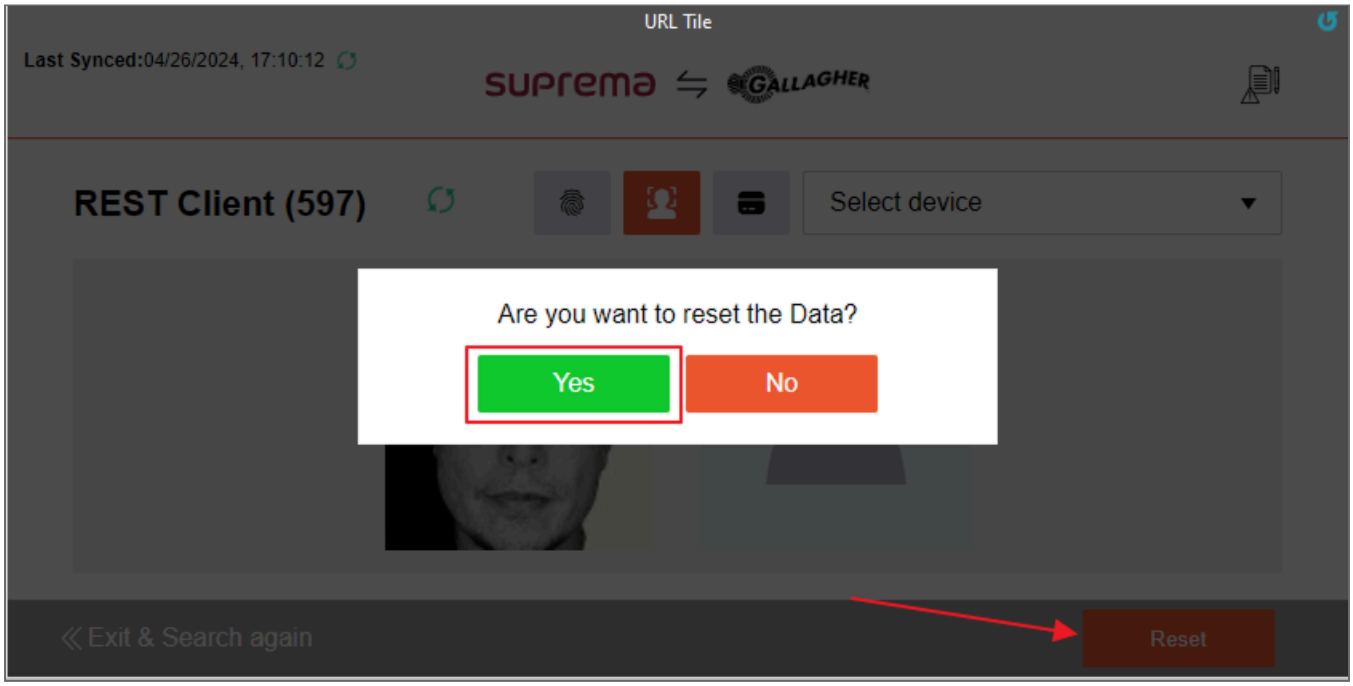
Información

- El tamaño admitido del archivo de imagen es de hasta 2 MB.
- Los formatos de archivo de imagen admitidos son JPG, JPEG y PNG.
- Si ocurre un error al inscribir un rostro visual con una imagen de perfil, usa una imagen más nítida.

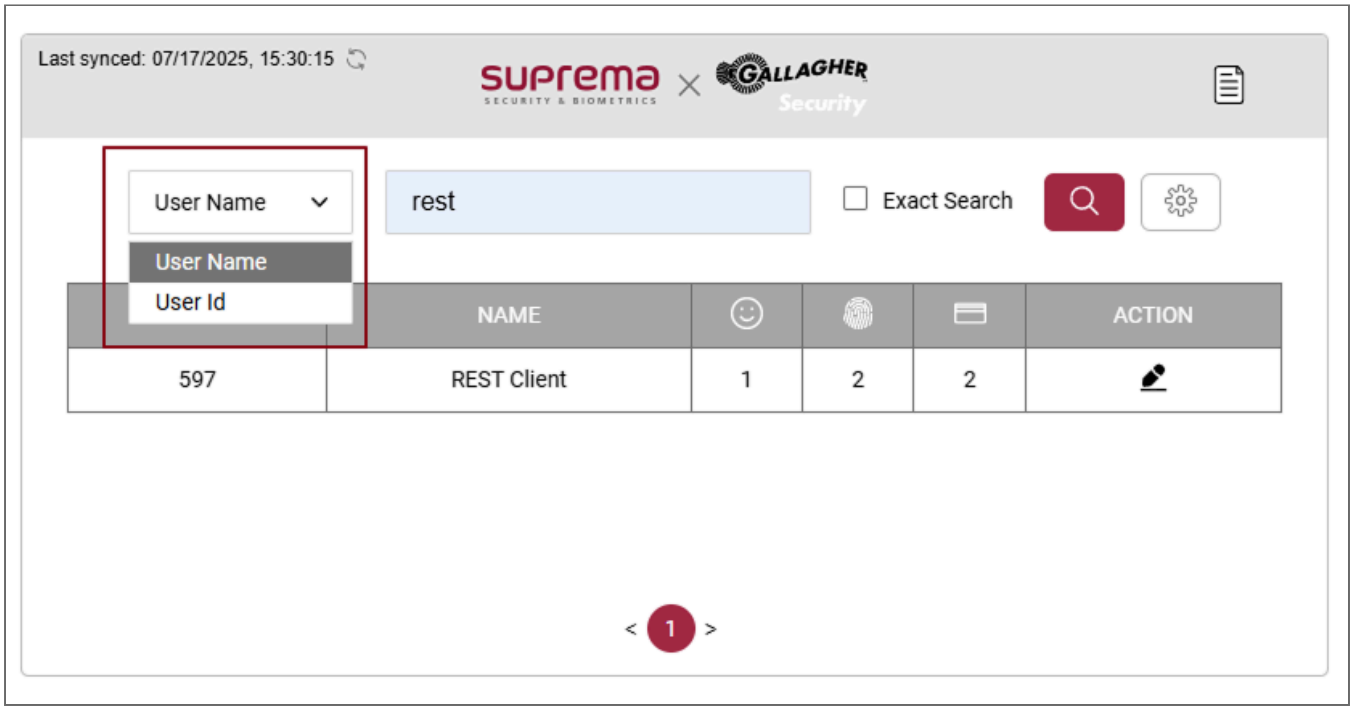
17. Si necesitas volver a escanear o volver a cargar los datos, debes eliminar los datos anteriores; **presiona** la ventana emergente del **botón rojo Eliminar** y **presiona Sí**. Se eliminará esa imagen.



18. Y si necesitas restablecer todos los datos de rostro visual, **presiona** el botón **Restablecer** y **presiona** Sí. Se restablecerán todos los datos.



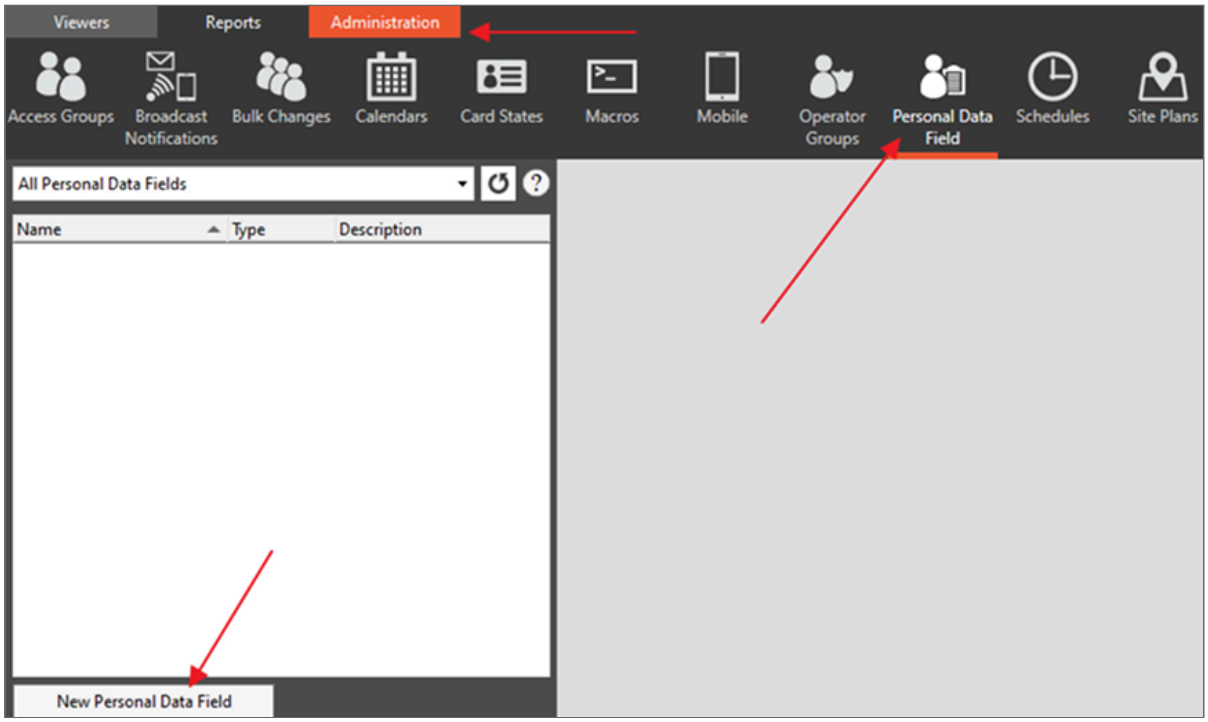
19. Si sales y buscas de nuevo al usuario, todos los datos guardados aparecerán en la tabla.



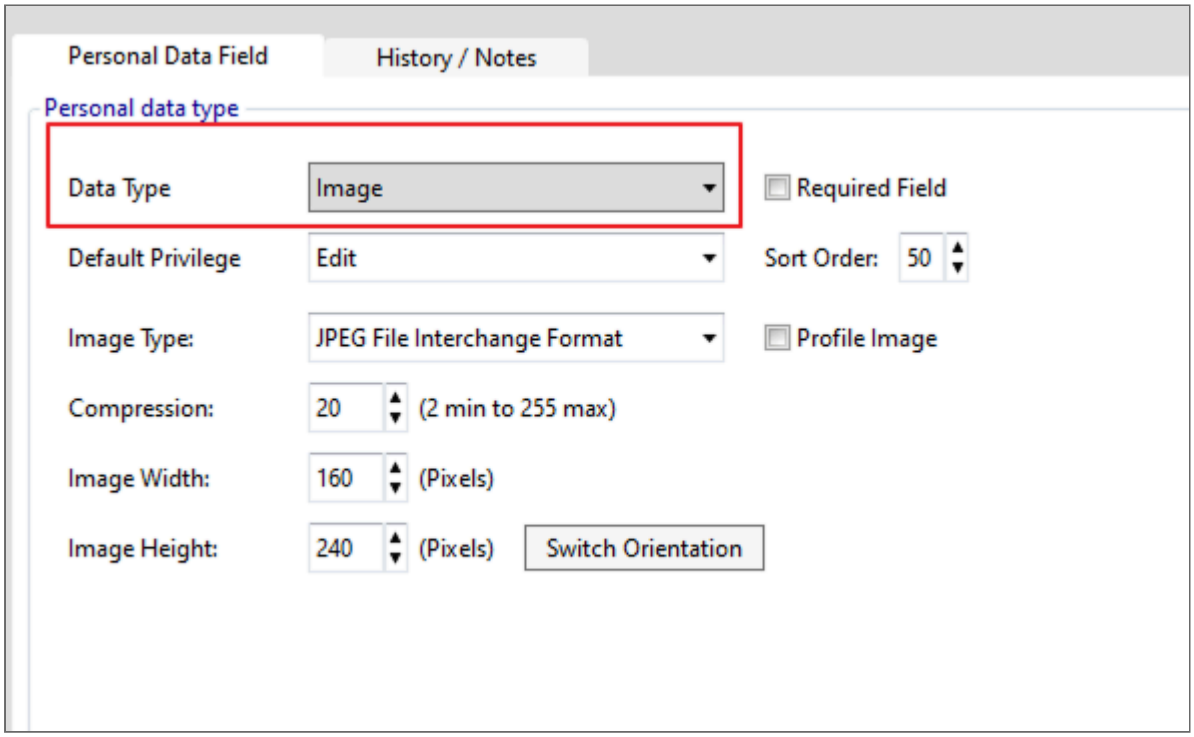
También puedes buscar al usuario por su id; **cambia** el nombre de usuario del menú desplegable a id de usuario y **busca** al usuario por id.

Inscribir la ID de foto del usuario en Command Center para la plantilla facial

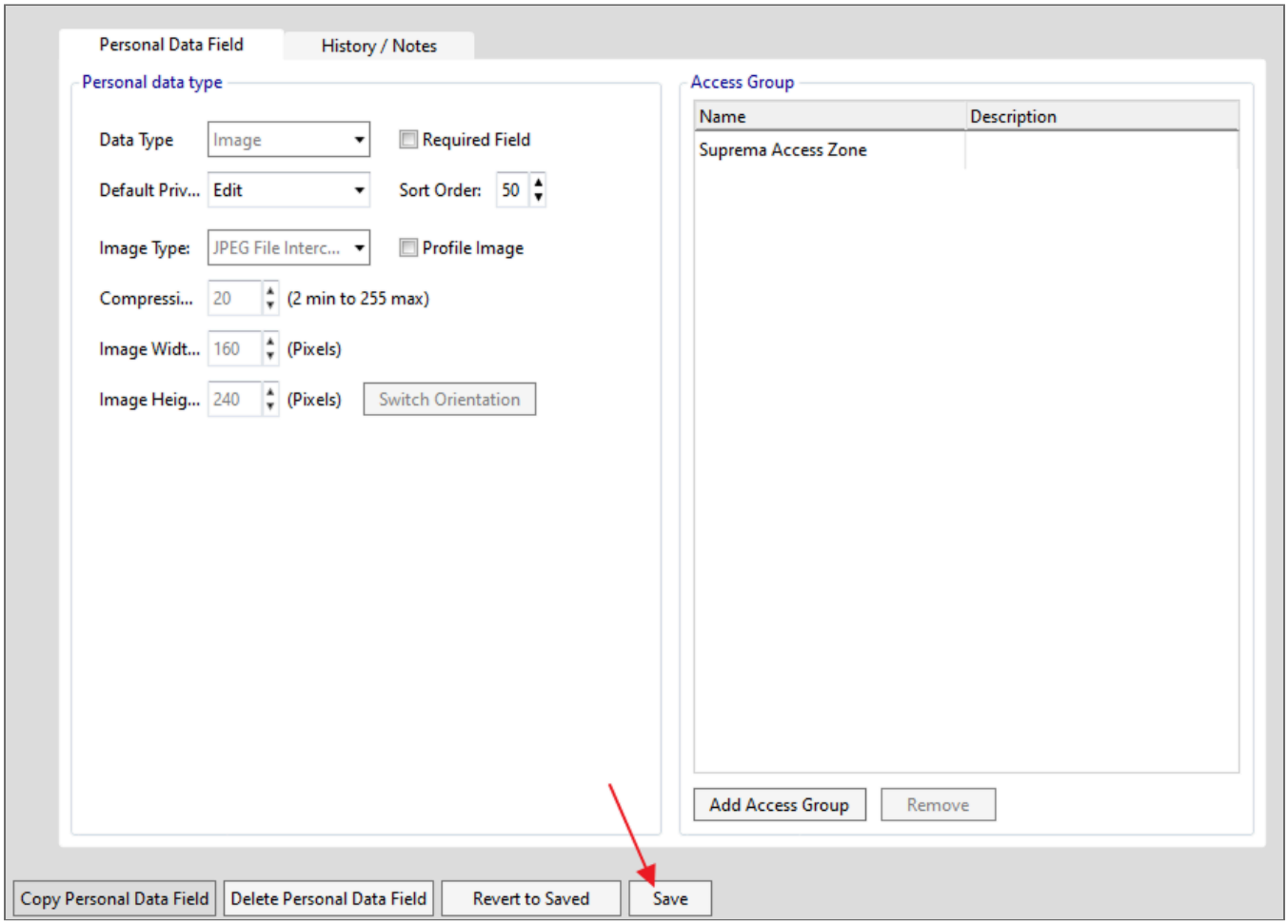
1. **Ve** a Administration, **haz clic** en Personal Data Field y **presiona** New Personal Data Field.



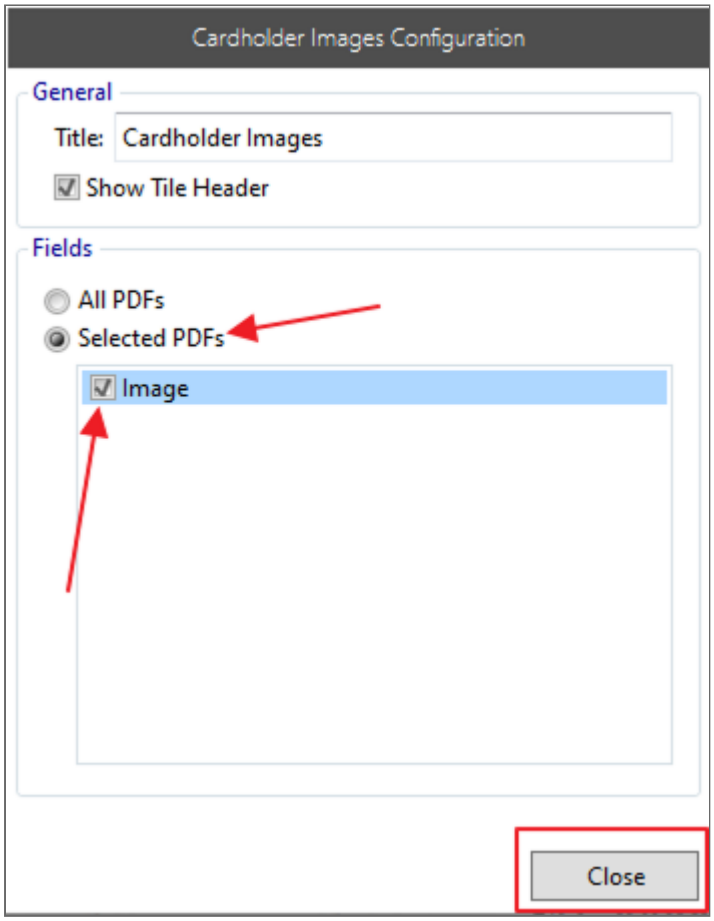
2. Ahora, dentro de la ventana emergente, **establece** el nombre como Image y **presiona** el botón Close. En el campo Data Type, **selecciona** Image como tipo de dato. No cambies nada aquí y asigna el grupo de acceso **presionando** el botón Add Access Group dentro de la sección Access Group y **seleccionando** Suprema Access Zone. Después de **seleccionar** Access Zone, **presiona** el botón Add Selection para el campo.



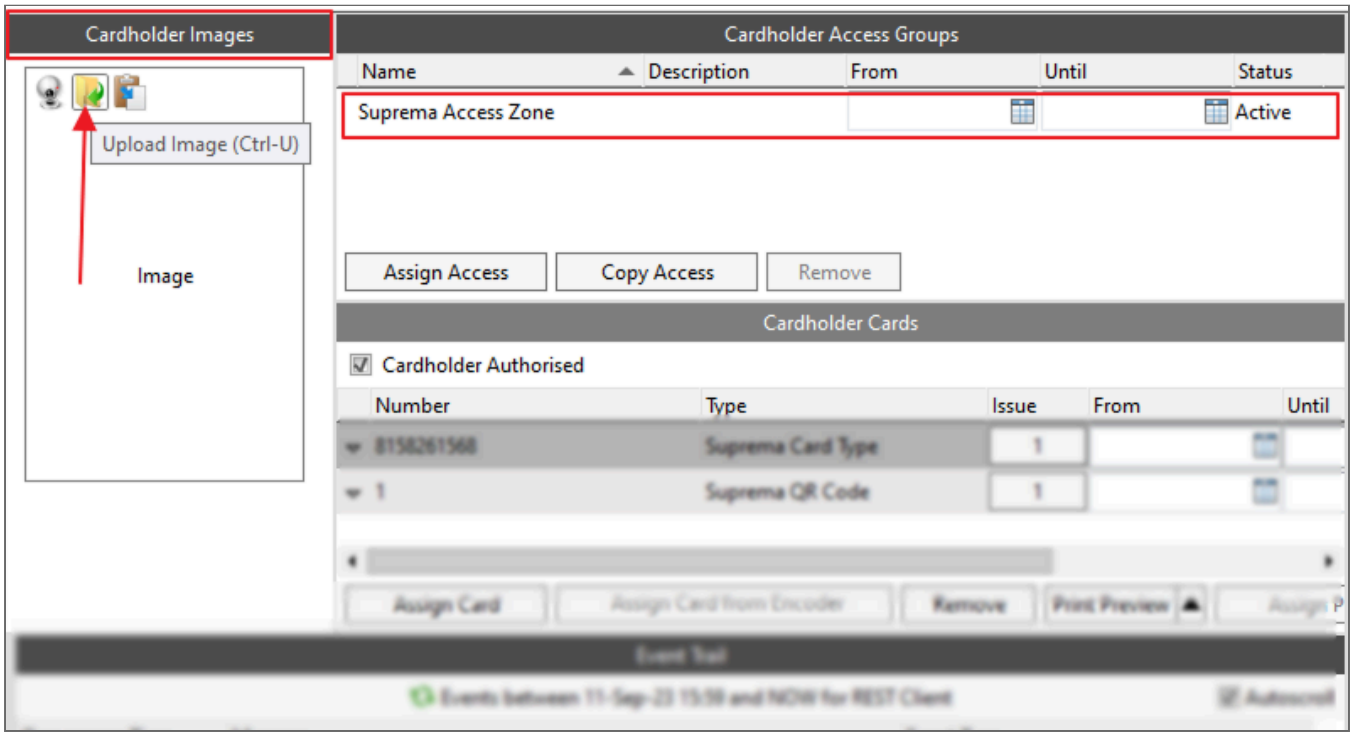
3. Después de asignar Access Zone, **presiona** el botón Guardar en la parte inferior.



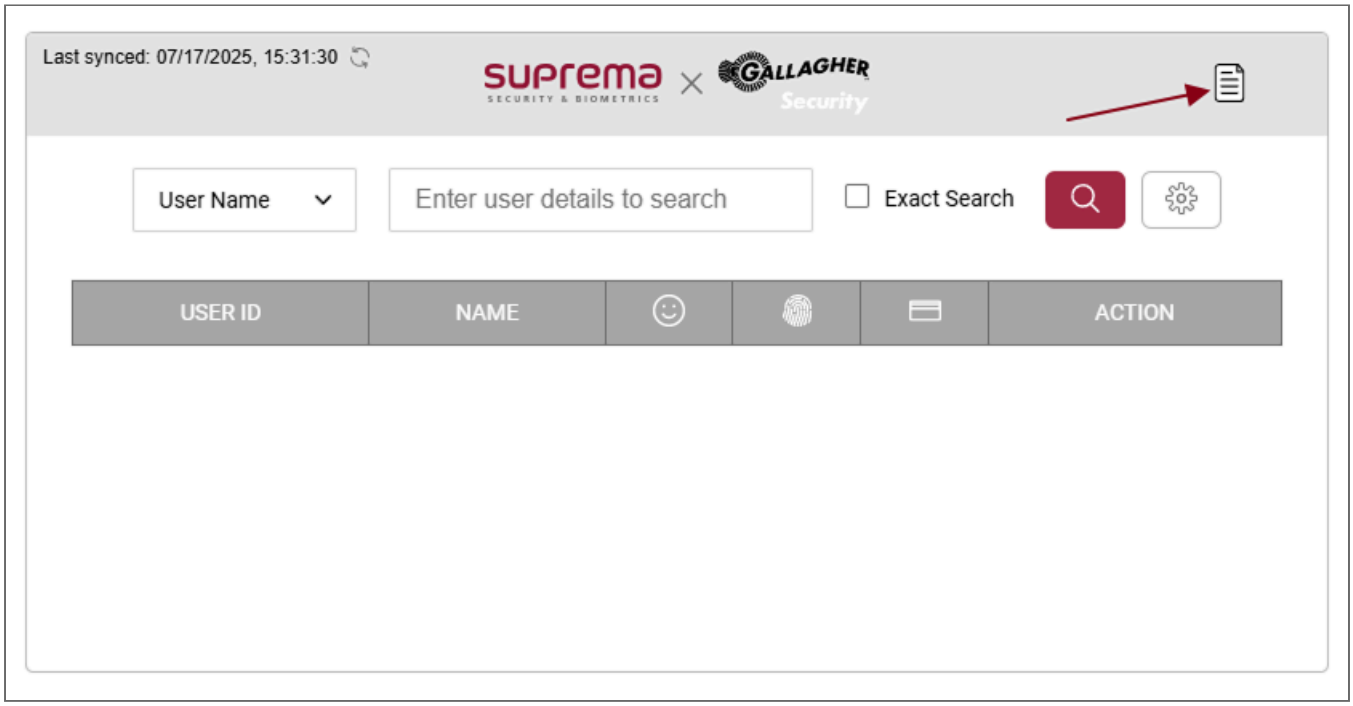
4. Ahora **ve** a Viewer Configuration y **haz clic** en Click to configure para Cardholder Images. Dentro de Cardholder Images Configuration, **elige** Selected PDFs, **selecciona** el campo Image y **presiona** el botón Close. Ahora **presiona** el botón Guardar en la parte inferior izquierda para guardar los cambios. Ahora haz **clic derecho** en Viewer Configuration y vuelve a cargar el visor para reflejar los cambios.



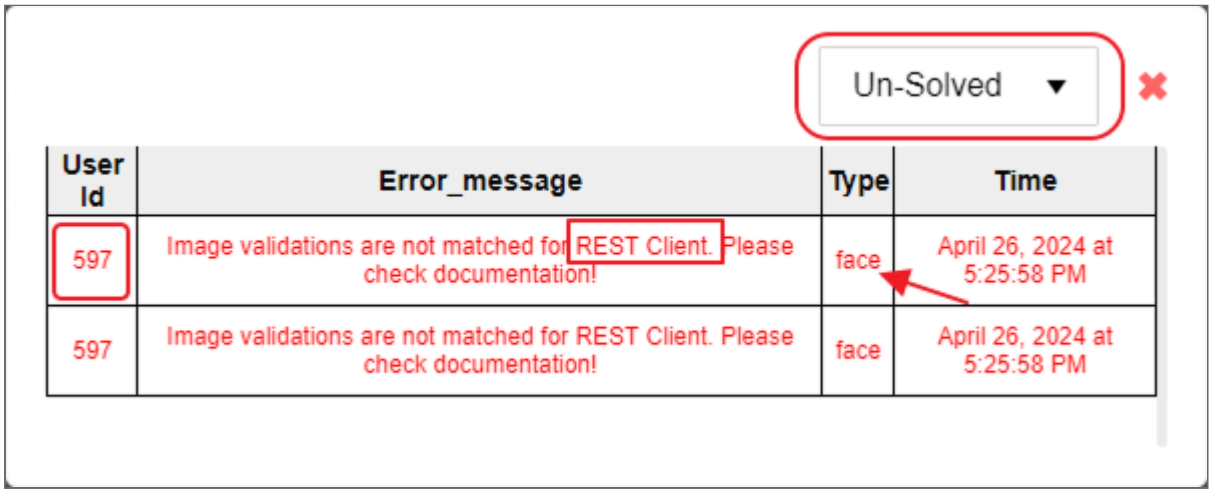
5. Ahora, dentro de Cardholder Viewer, puedes ver la pestaña Cardholder Images. Puedes cargar imágenes **haciendo clic** en el icono amarillo. Para ello, debemos asignar una zona de acceso al usuario. Después de cargar la imagen, **presiona** el botón Guardar.



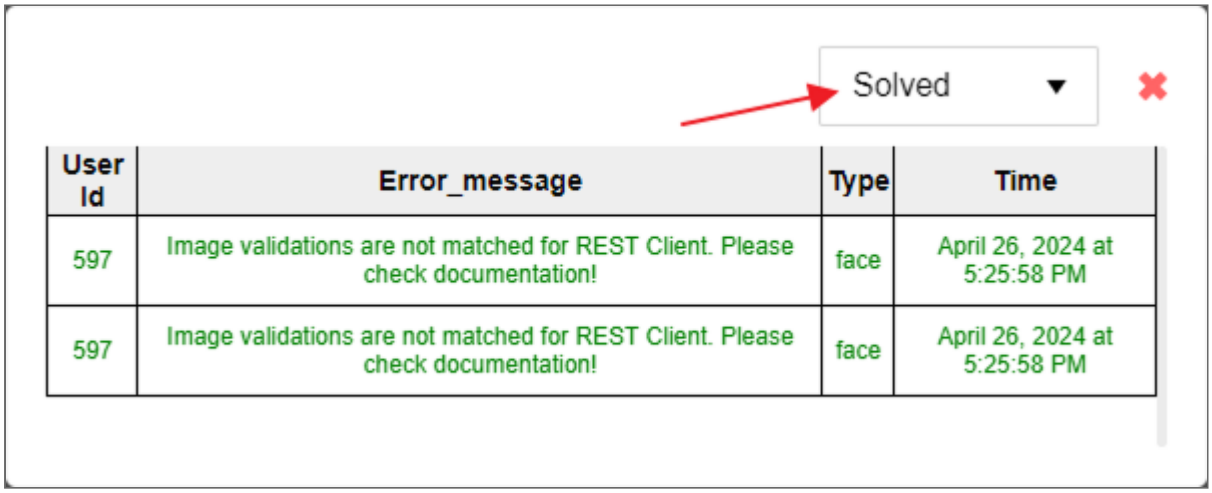
6. Si necesitas ver el mensaje de error que ocurre para los usuarios al actualizar la información del usuario, puedes encontrarlo en la sección ErrorLog **haciendo clic** en este icono. Se abrirá una ventana emergente que muestra diferentes errores del usuario.



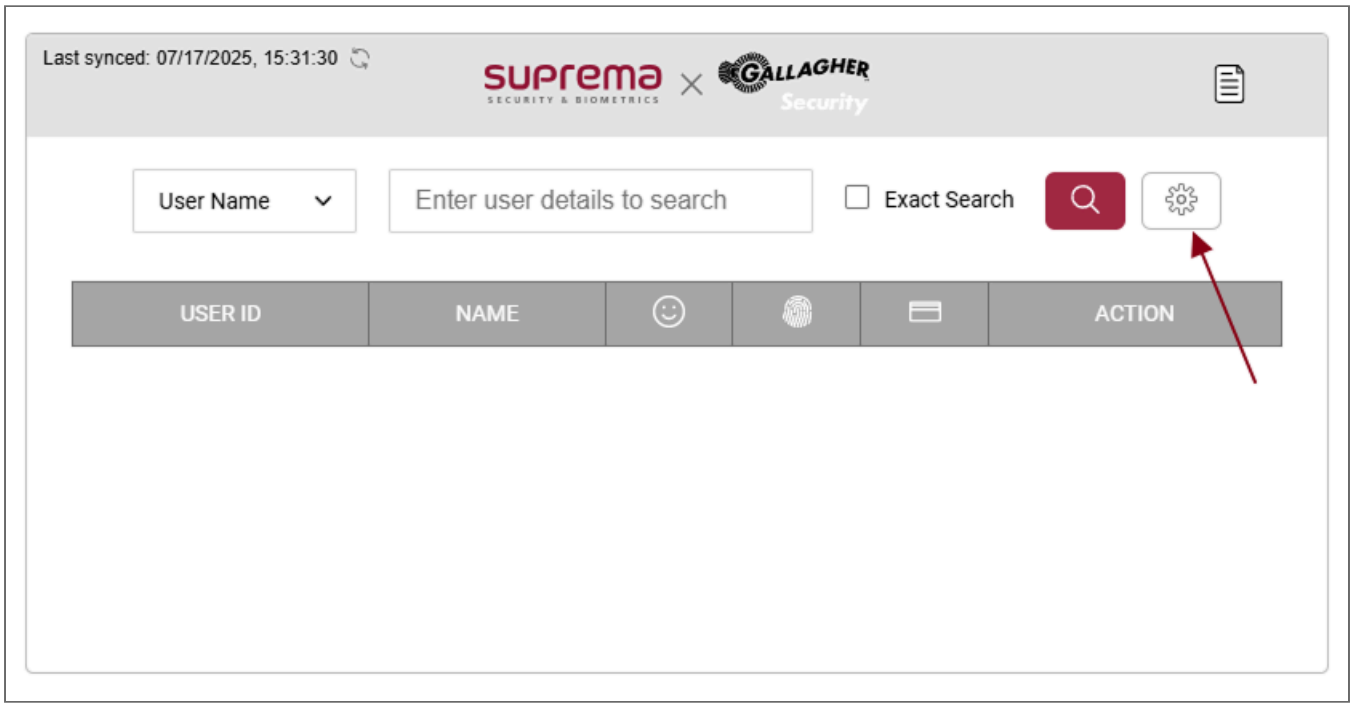
7. Como en la imagen siguiente, tenemos un error para un usuario. Aquí **Type** define qué tipo de error es, **Status** Un-solved significa que el error todavía no se ha resuelto para el usuario, y Solved indica que el error ya se resolvió para el usuario. Ahora el cuadro rojo indica el nombre del usuario y el otro cuadro rojo indica la ID del usuario.



8. La imagen siguiente muestra el resultado después de cambiar la imagen del usuario desde Gallagher Command Center, ya que obtenemos el error al inscribir el rostro del usuario; después de una inscripción exitosa, el color del mensaje de error también cambia y **Status** también cambia.

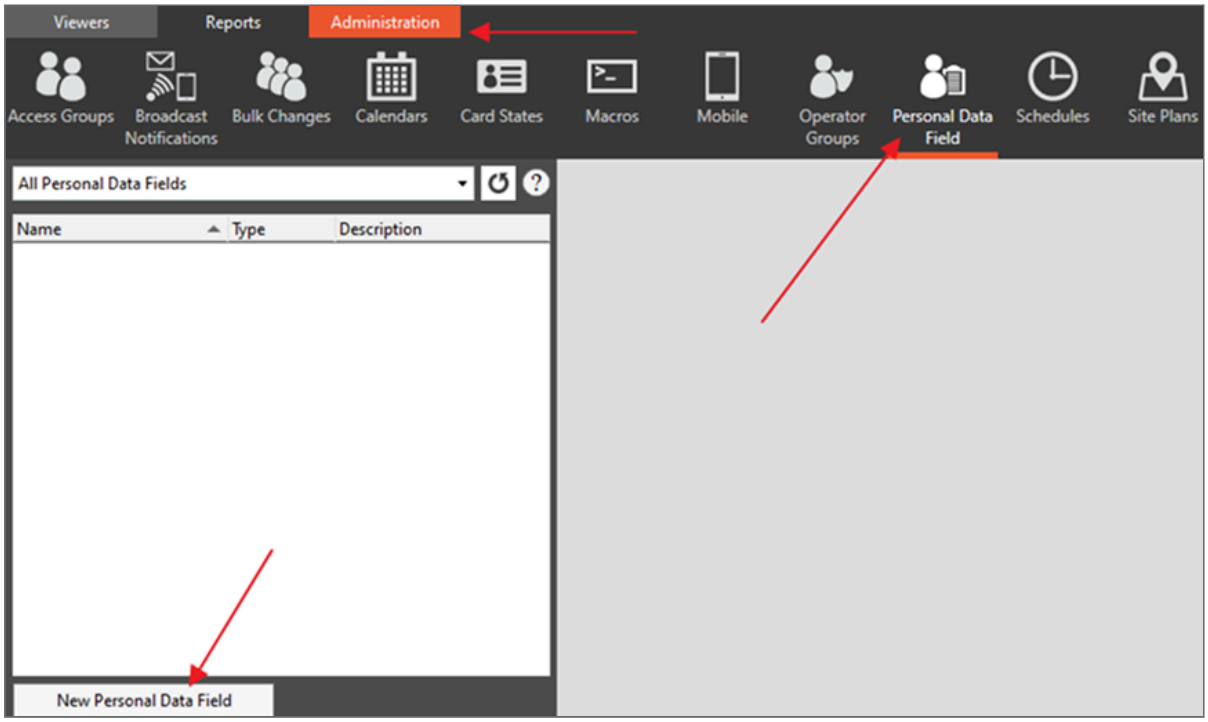


9. Si necesitas cambiar la configuración del dispositivo, **presiona** el botón **Configuración** y verás las siguientes pantallas:



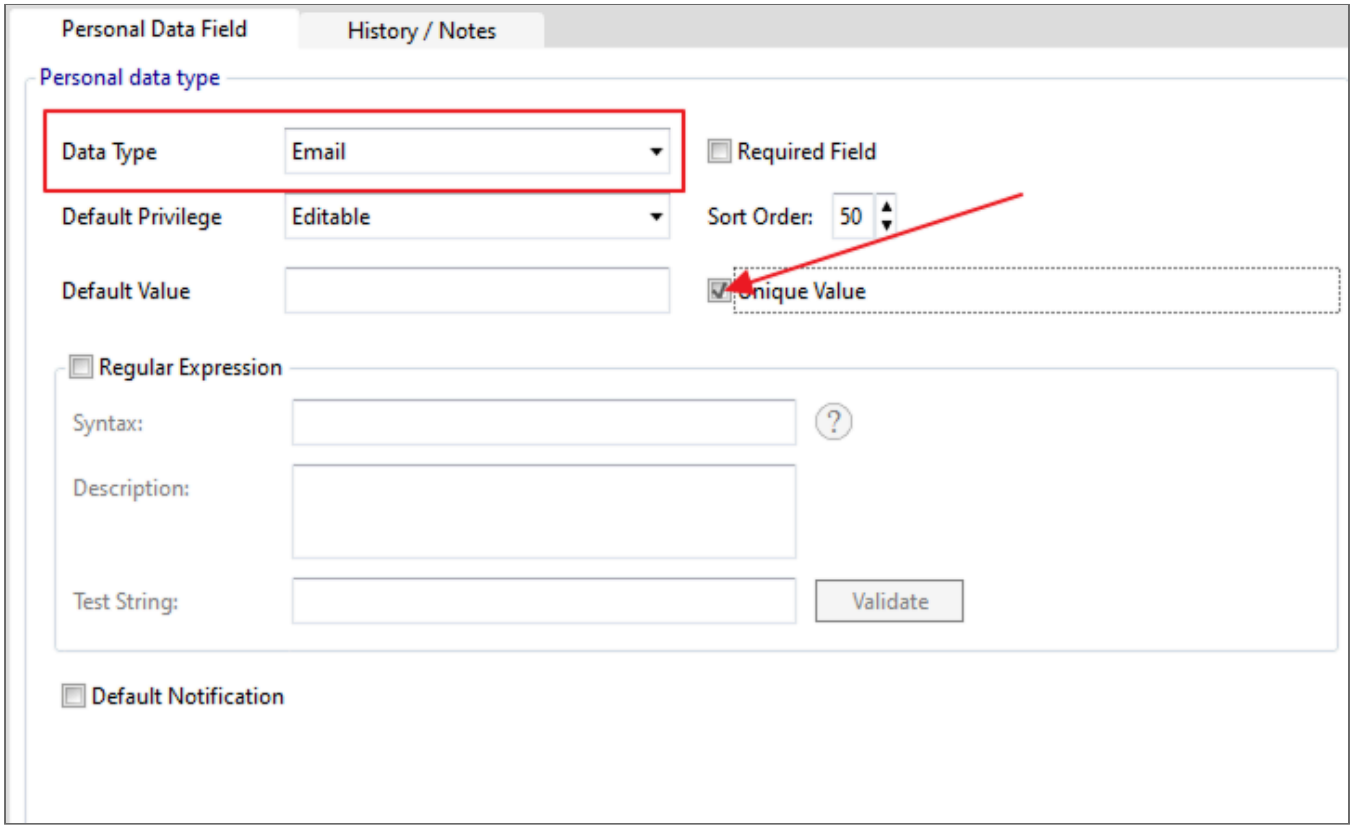
Inscribir la ID de correo electrónico del usuario en Command Center para el código QR

1. **Ve** a Administration, **haz clic** en Personal Data Field y **presiona** New Personal Data Field.

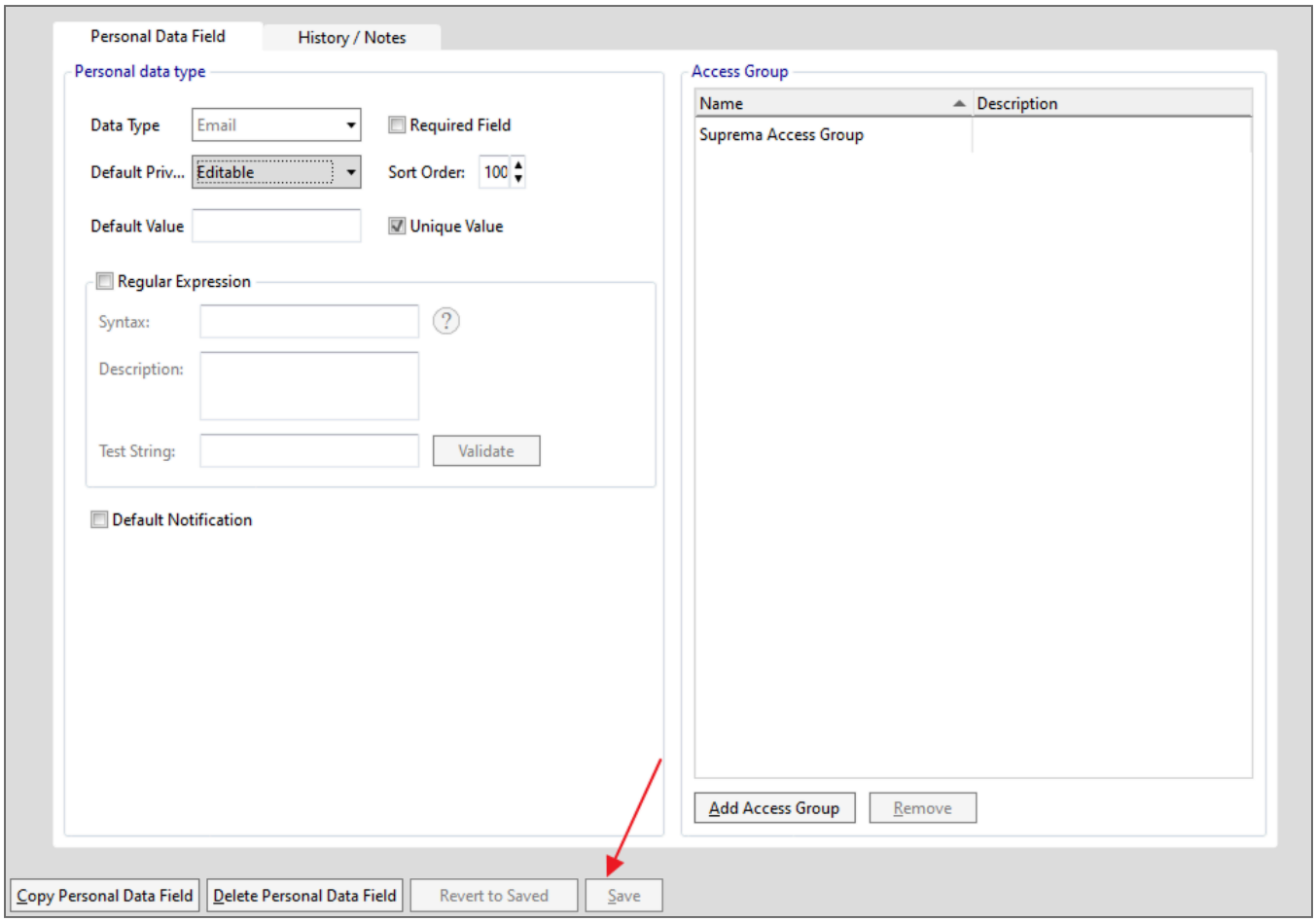


2. Ahora, dentro de la ventana emergente, **establece** el nombre como Email y **presiona** el botón Close. En el campo Data Type, **selecciona** Email como tipo de dato y **marca** la casilla Unique Value. No cambies nada aquí y asigna el grupo de acceso **presionando** el botón Add Access Group dentro de la sección Access Group y **seleccionando** Suprema Access Zone. Después de **seleccionar** Access Zone, **presiona** el botón Add Selection para el campo.

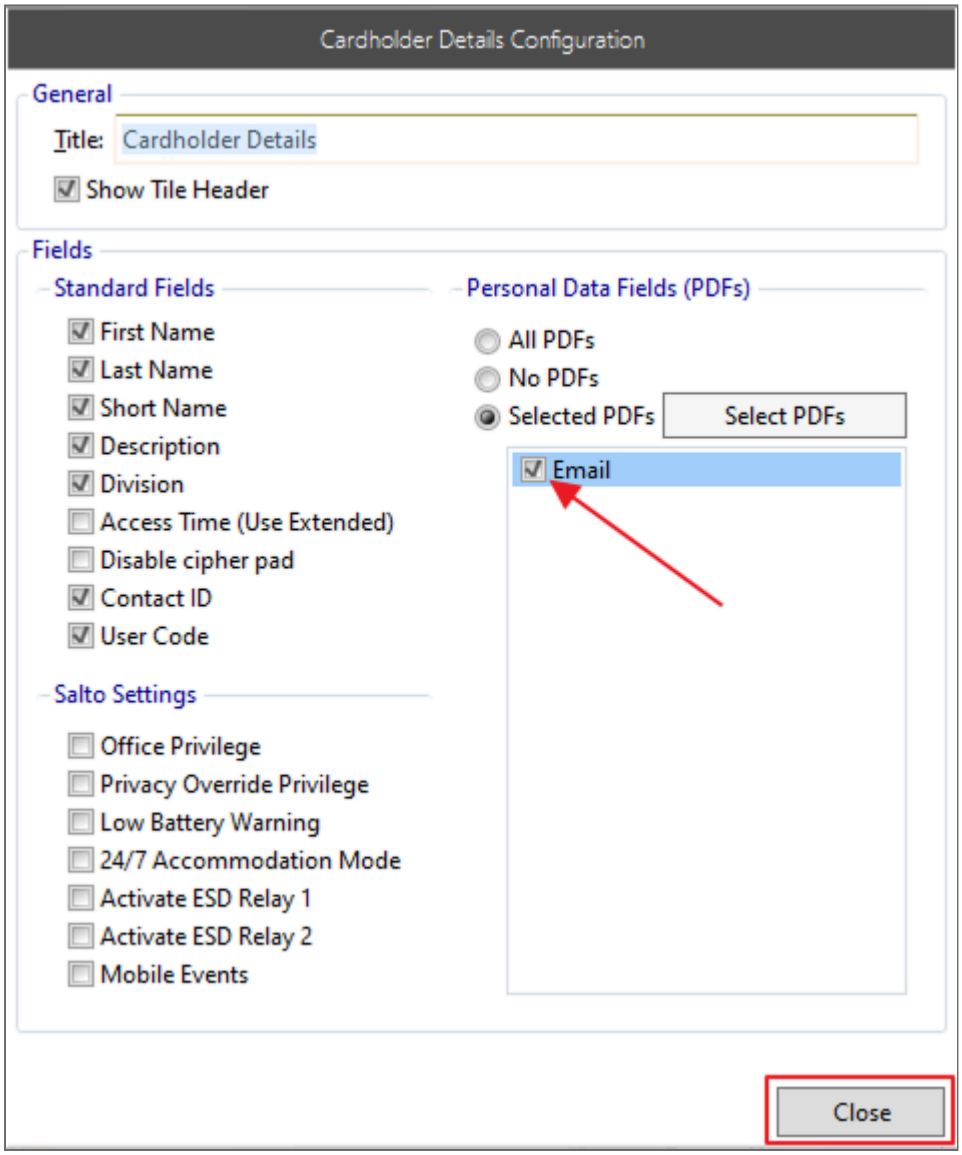
> **Información**
> Usa los mismos términos mencionados para los campos.



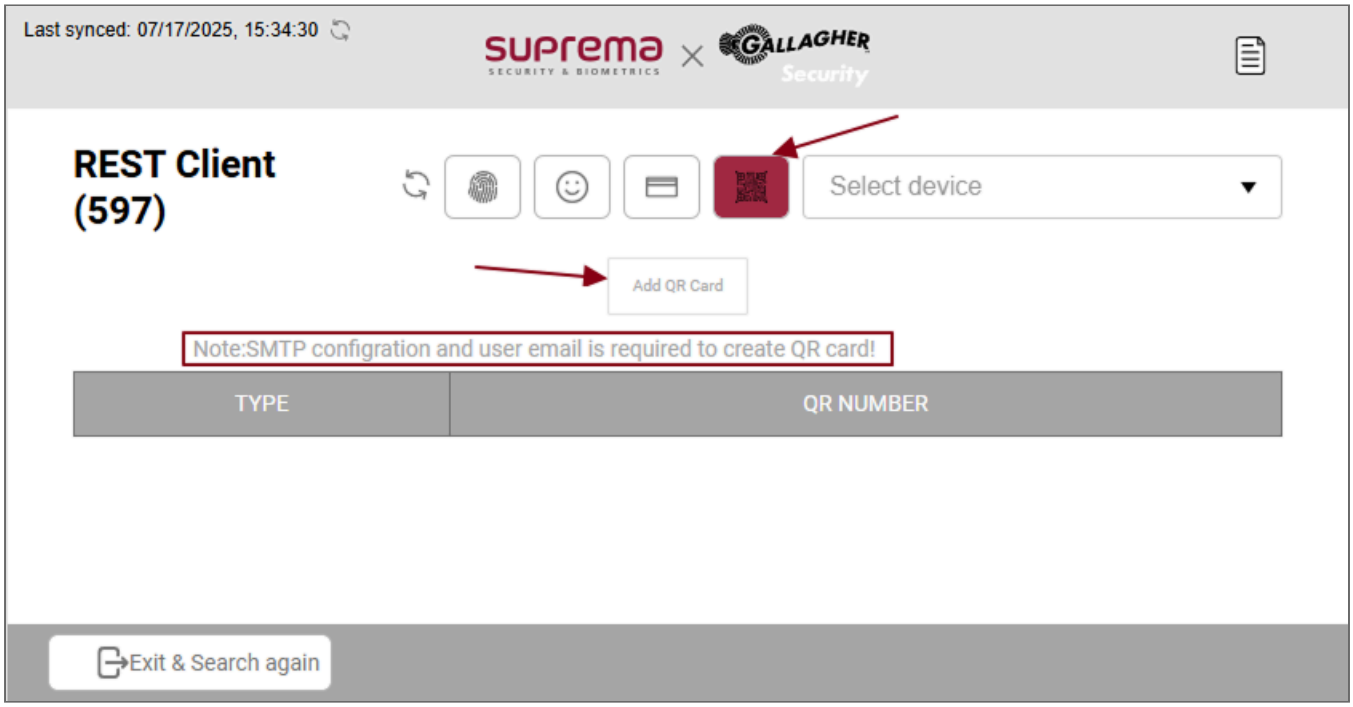
3. Después de asignar Access Zone, **presiona** el botón Guardar en la parte inferior.



4. Ahora **ve** a Viewer Configuration y **haz clic** en Click to configure para Cardholder Details. Dentro de Cardholder Details Configuration, **elige** Selected PDFs, **selecciona** el campo Email y **presiona** el botón Close. Ahora **presiona** el botón Guardar en la parte inferior izquierda para guardar los cambios. Haz clic derecho en Viewer Configuration y **presiona** Reload Viewer.



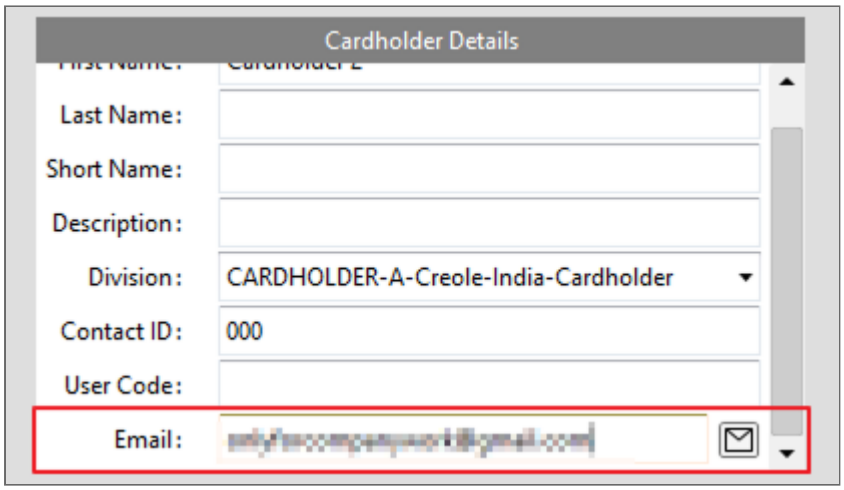
5. Para asignar el código QR, ve al perfil de usuario dentro del middleware y **haz clic** en el icono de QR. Como se muestra abajo, el botón Add QR está **deshabilitado**, y hay una nota que indica que el correo electrónico del usuario no se ha asignado en Gallagher.



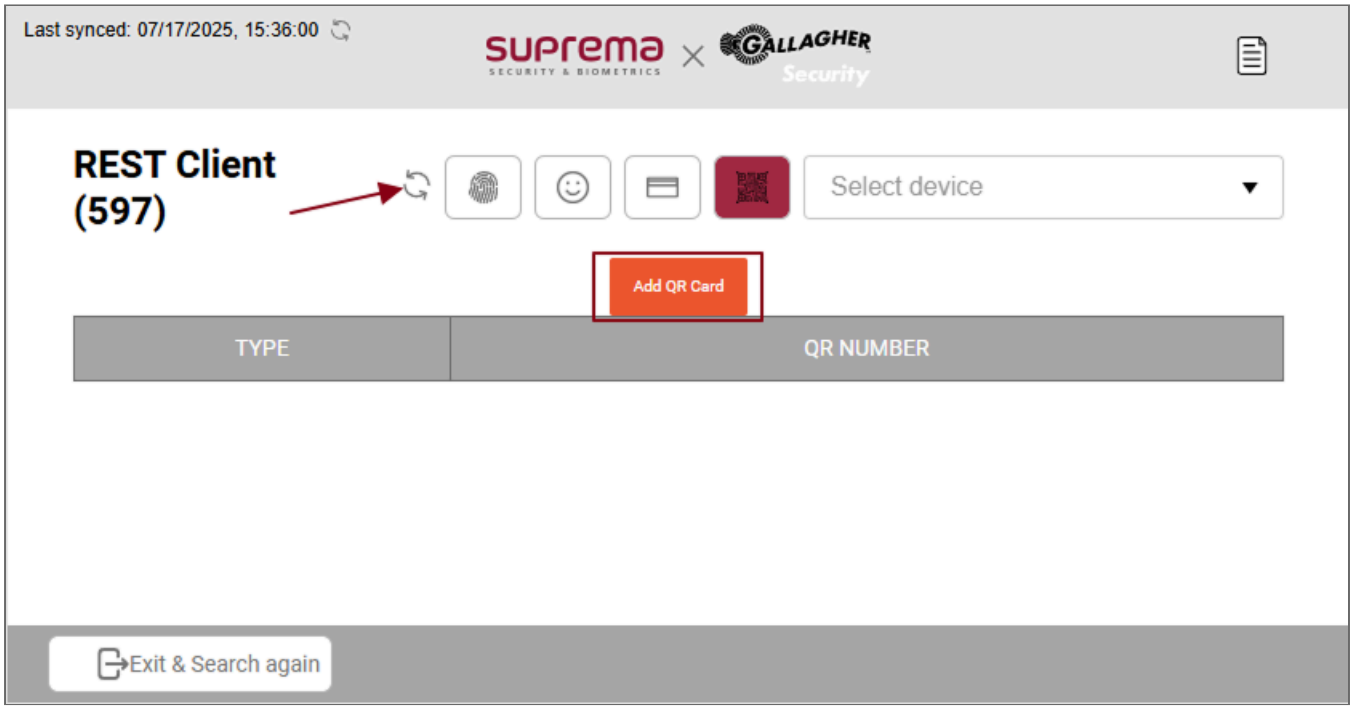
Información

- Para configurar las opciones de SMTP: Configurar SMTP para código QR.
- Para configurar la dirección de correo electrónico en Gallagher, configuración de correo electrónico en Gallagher.
- Configura el tipo de tarjeta QR en Gallagher: Crear tipo de tarjeta de código QR.

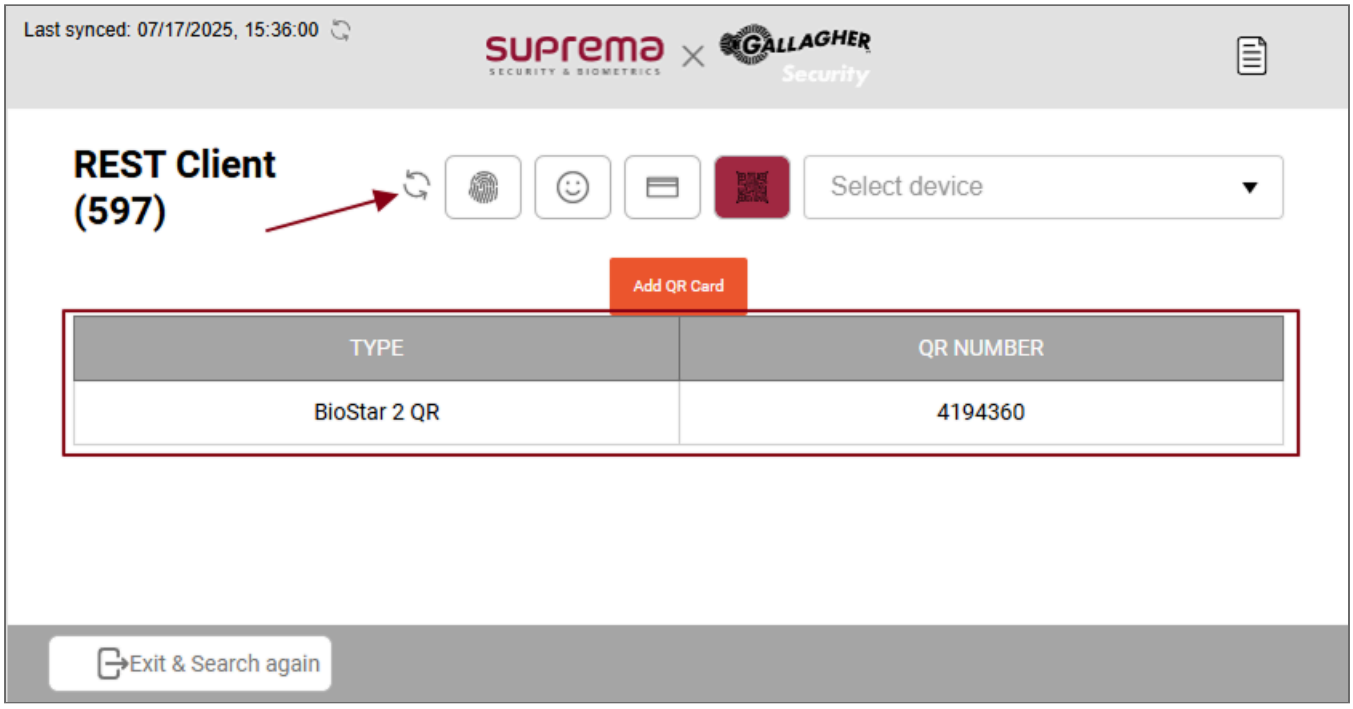
6. Para asignar una dirección de correo electrónico a un usuario, en Command Center ve a los detalles del usuario, coloca el correo electrónico del usuario en el campo de correo electrónico de Cardholder Details y **presiona** el botón Guardar.



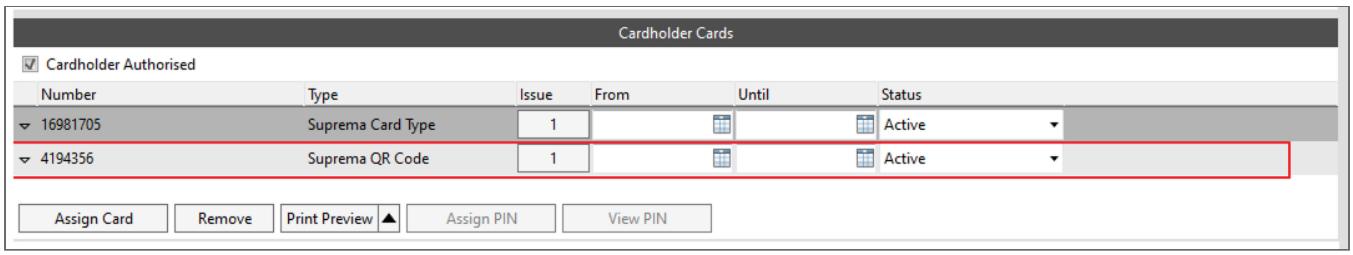
7. En el perfil de usuario del middleware, **presiona** el botón de sincronización, y el correo electrónico se asignará automáticamente al perfil de usuario en BioStar 2. El botón de correo electrónico ahora estará habilitado y la nota se quitará.



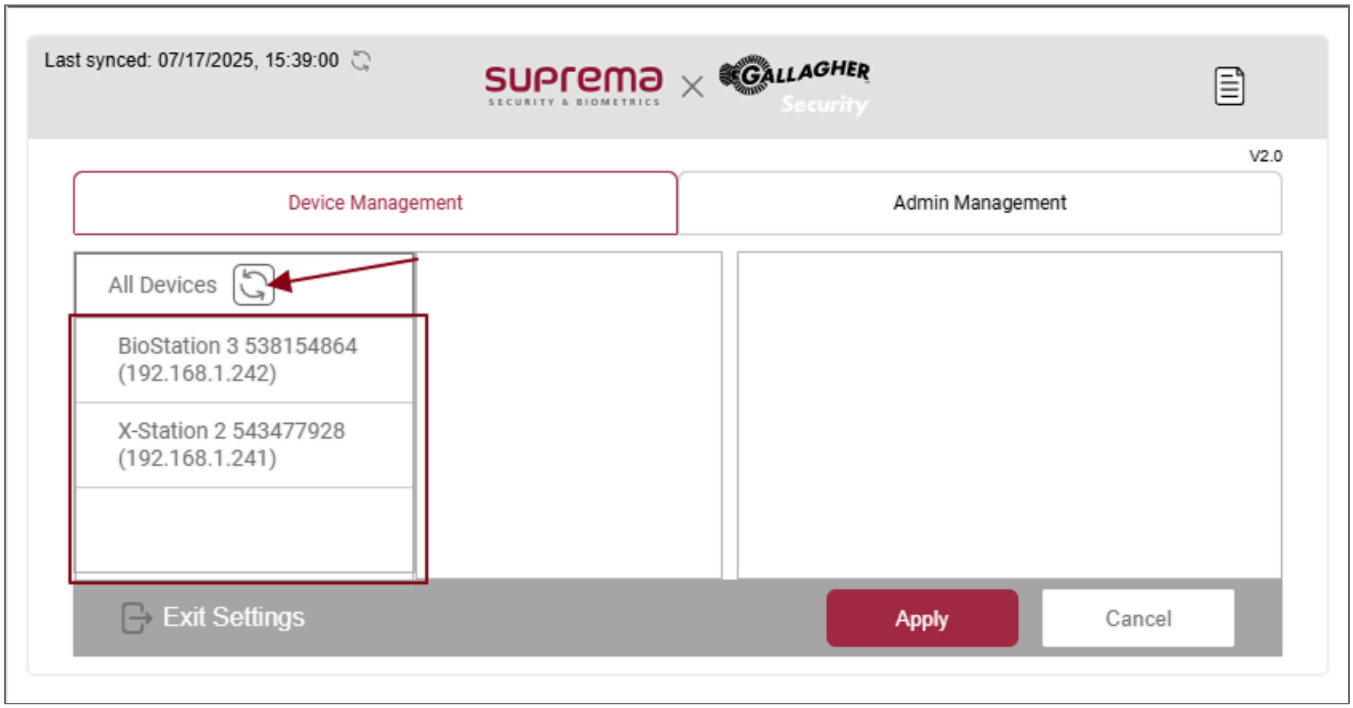
8. Ahora **presiona** el botón Add QR Code dentro de la sección QR del perfil de usuario; agregará el código QR a Gallagher y BioStar 2, y **enviará** el código QR a la dirección de correo electrónico que asignamos arriba.



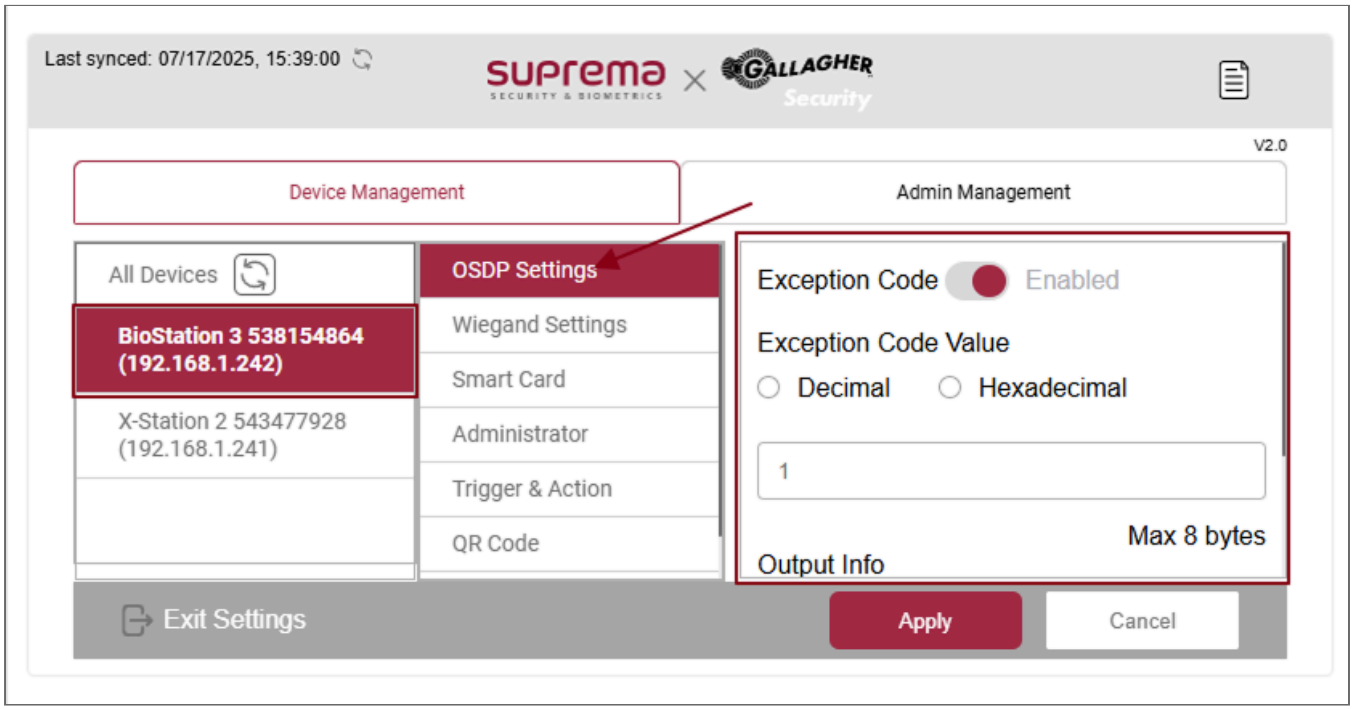
Una vez agregado el QR, puedes actualizar los datos **presionando** el botón de sincronización.



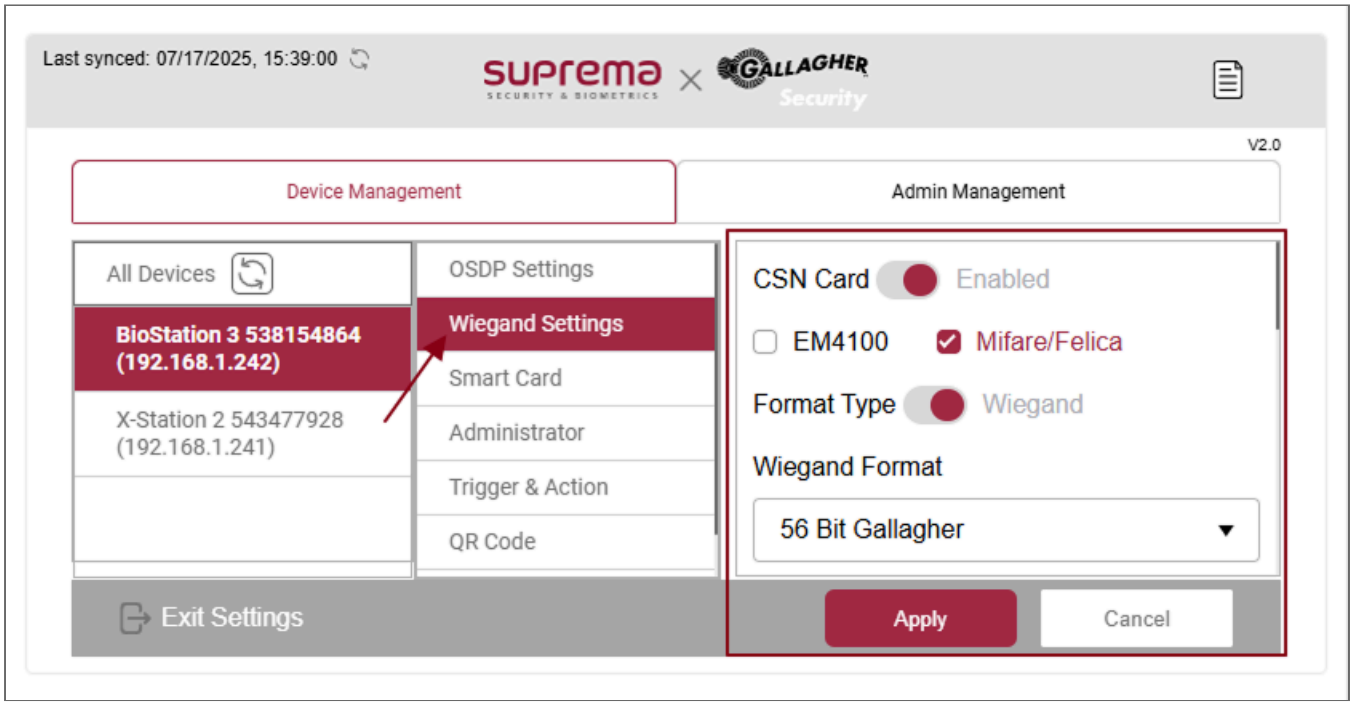
9. Debes **presionar** el botón de sincronización para sincronizar los dispositivos, y desde aquí puedes ver todos los dispositivos conectados y seleccionar cualquiera de ellos para ver la configuración del dispositivo.

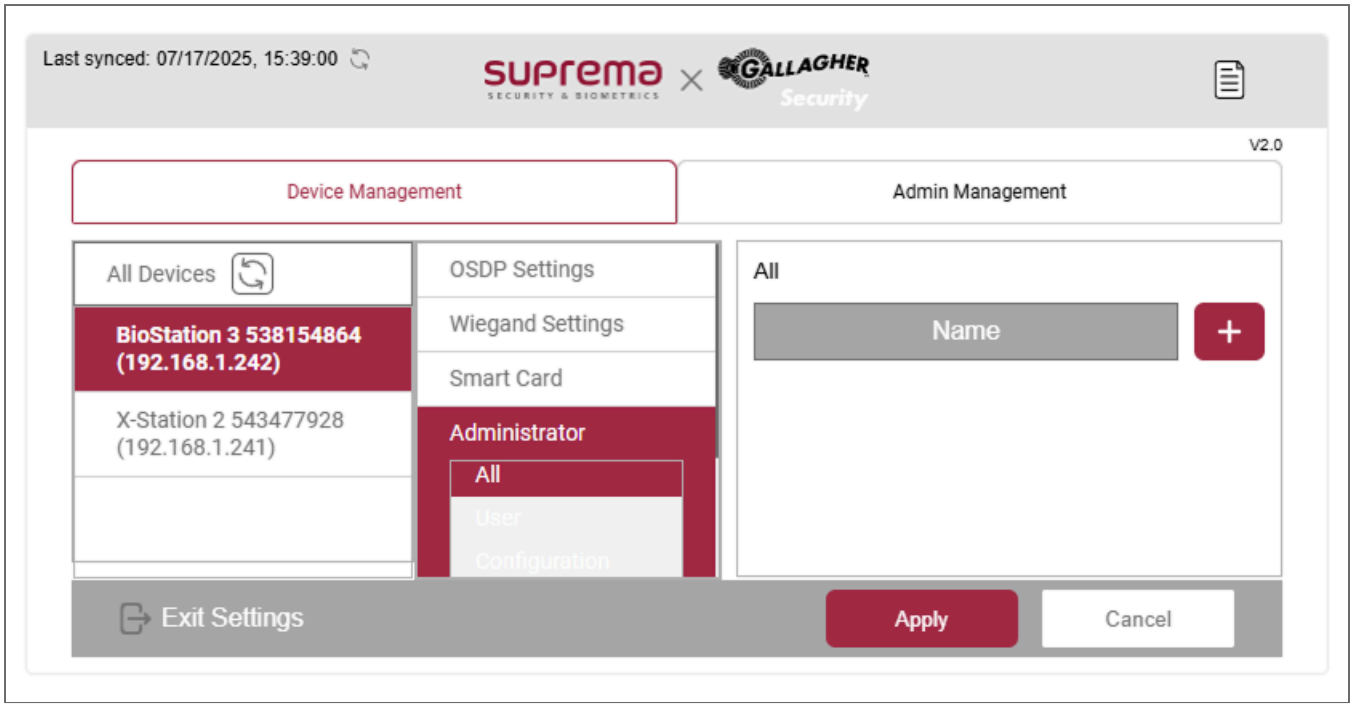


10. La imagen siguiente indica la configuración OSDP del dispositivo.

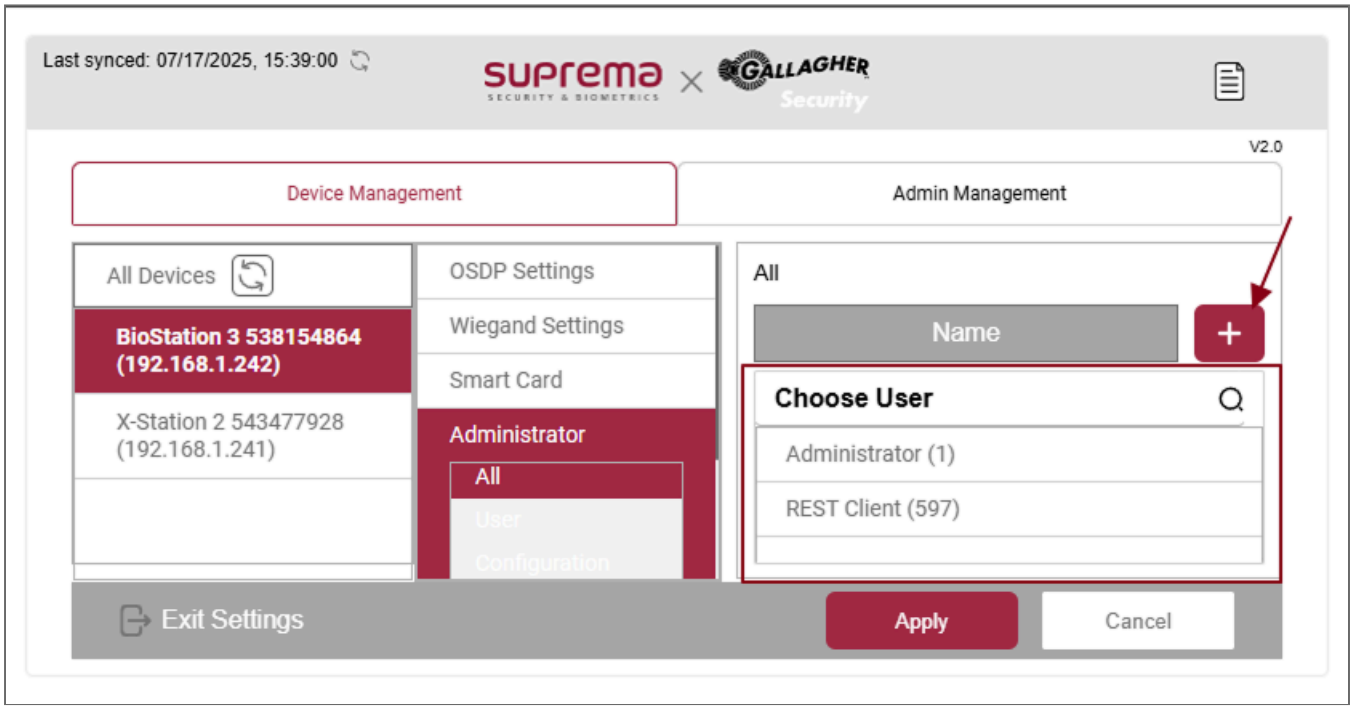


11. Las imágenes siguientes corresponden a la configuración Wiegand del dispositivo.

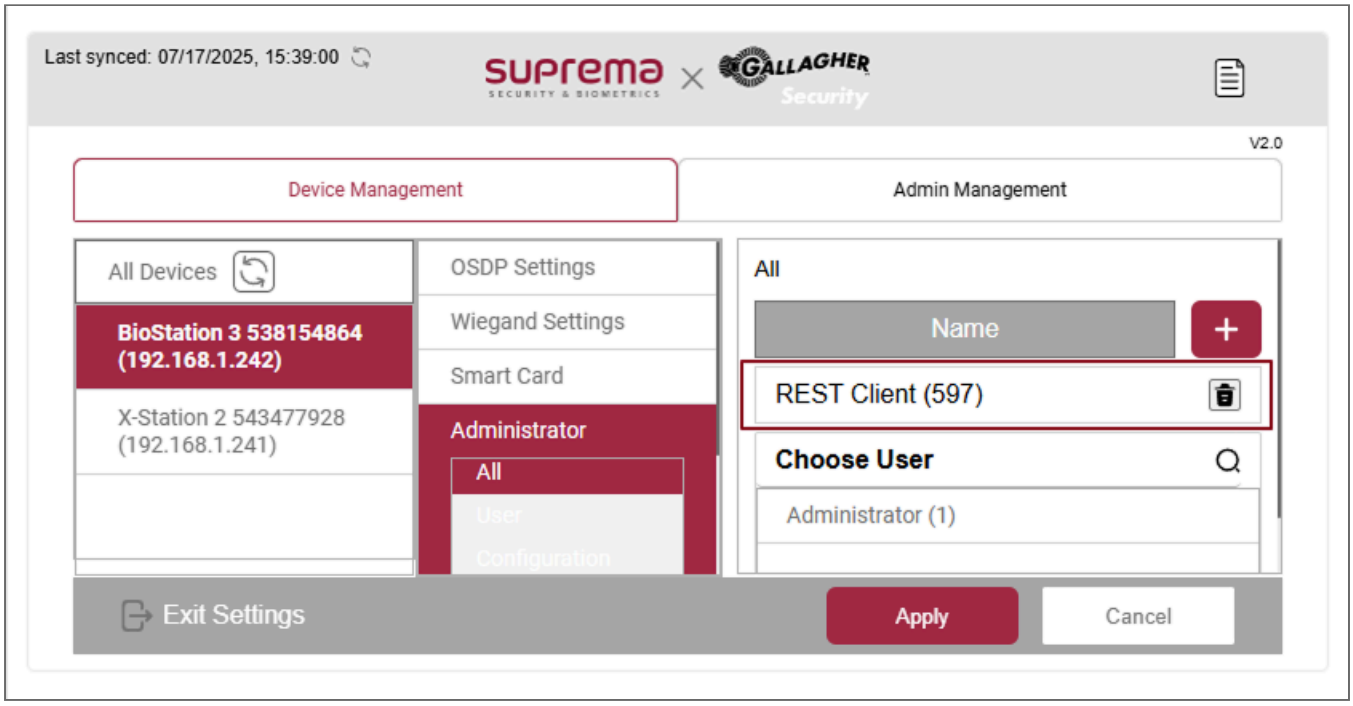




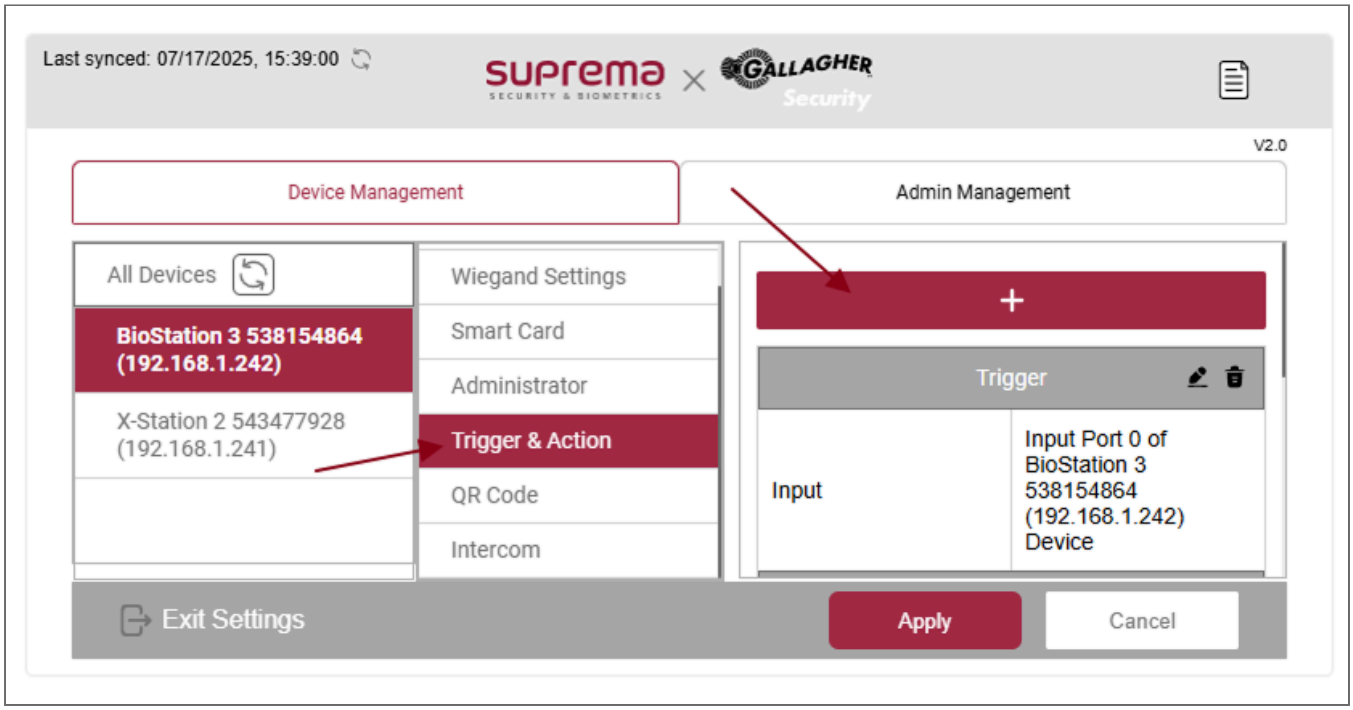
12. La imagen anterior corresponde al modo administrador, donde puedes elegir modos según tus necesidades. Como ves en la imagen siguiente, al **presionar** el botón + puedes seleccionar diferentes usuarios del menú desplegable.



13. Después de **seleccionar** el usuario, se puede mostrar como en la imagen siguiente; puedes eliminar al usuario de la lista **haciendo clic** en el botón eliminar.

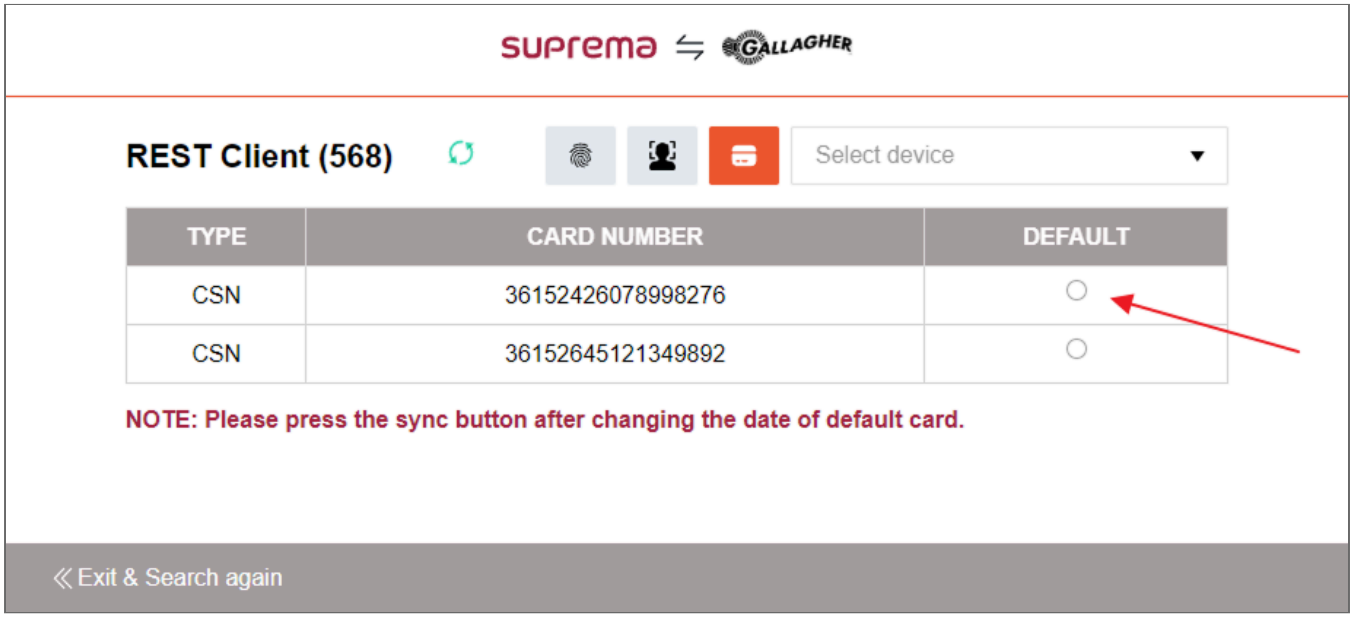


14. Este es el modo de activación y acción para el modo de salida del dispositivo. Puedes configurarlo **presionando** el botón +.

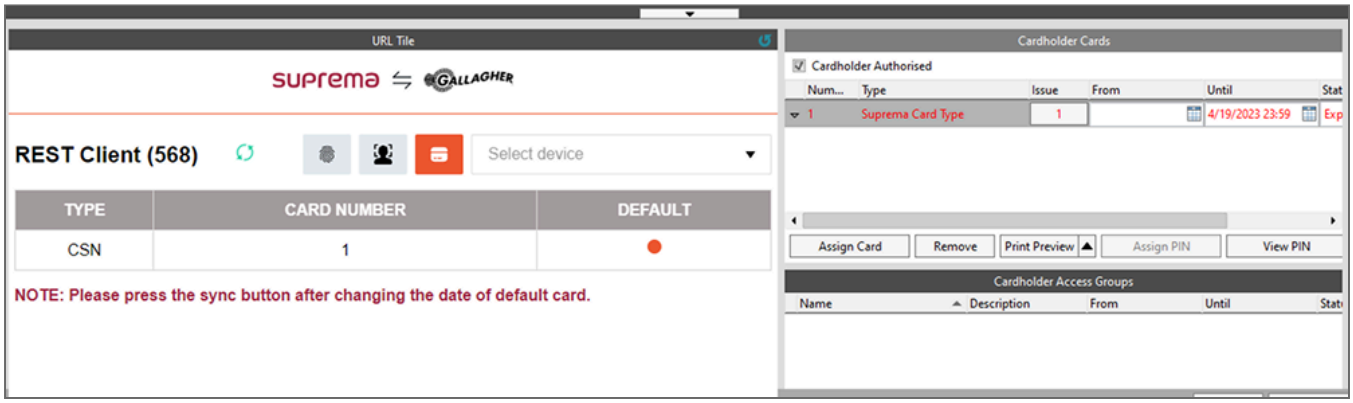


Selección de tarjeta predeterminada

1. Puedes seleccionar la tarjeta predeterminada **presionando** el botón de opción del usuario.



2. Puedes **establecer** el vencimiento del titular de la tarjeta configurando la fecha de vencimiento de la tarjeta predeterminada.



Información

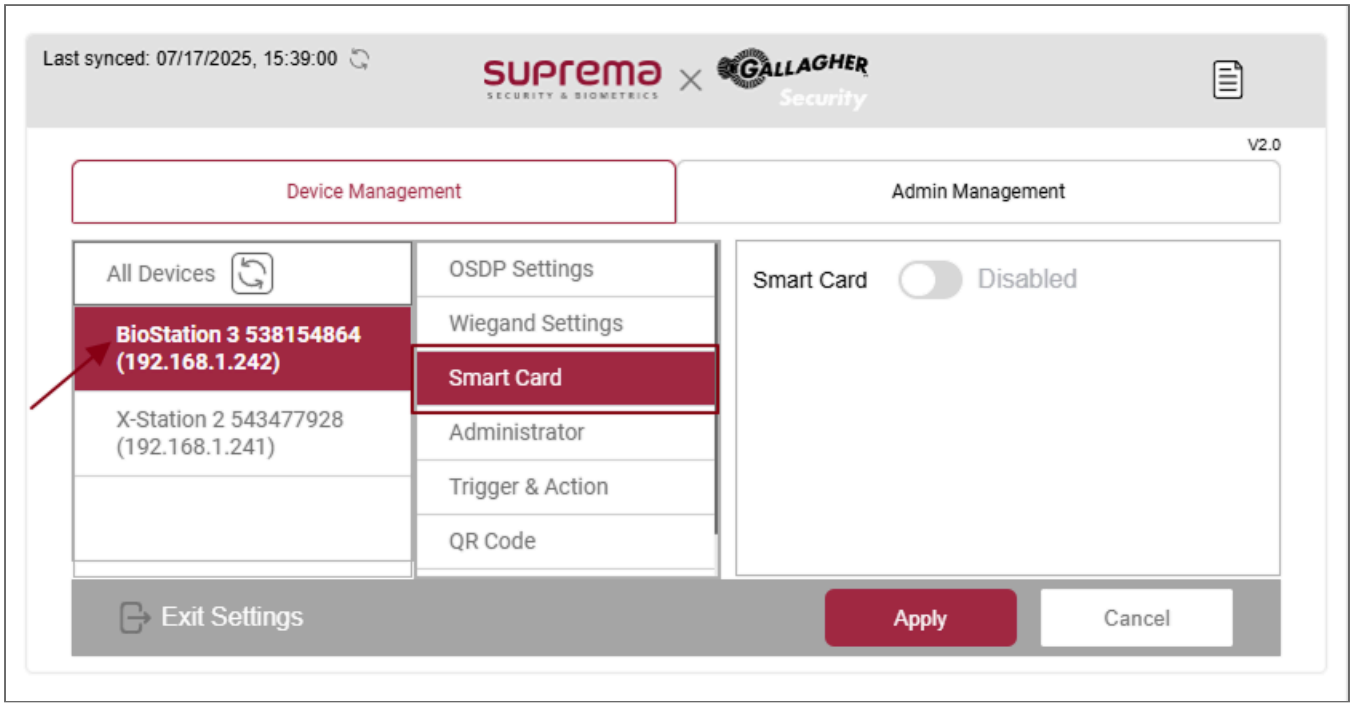
Si hiciste algún cambio en los detalles del titular de la tarjeta desde Command Centre. Debes abrir al mismo usuario en Suprema integration con middleware y presionar el botón de sincronización.

Tarjeta inteligente (AOC/TOC)

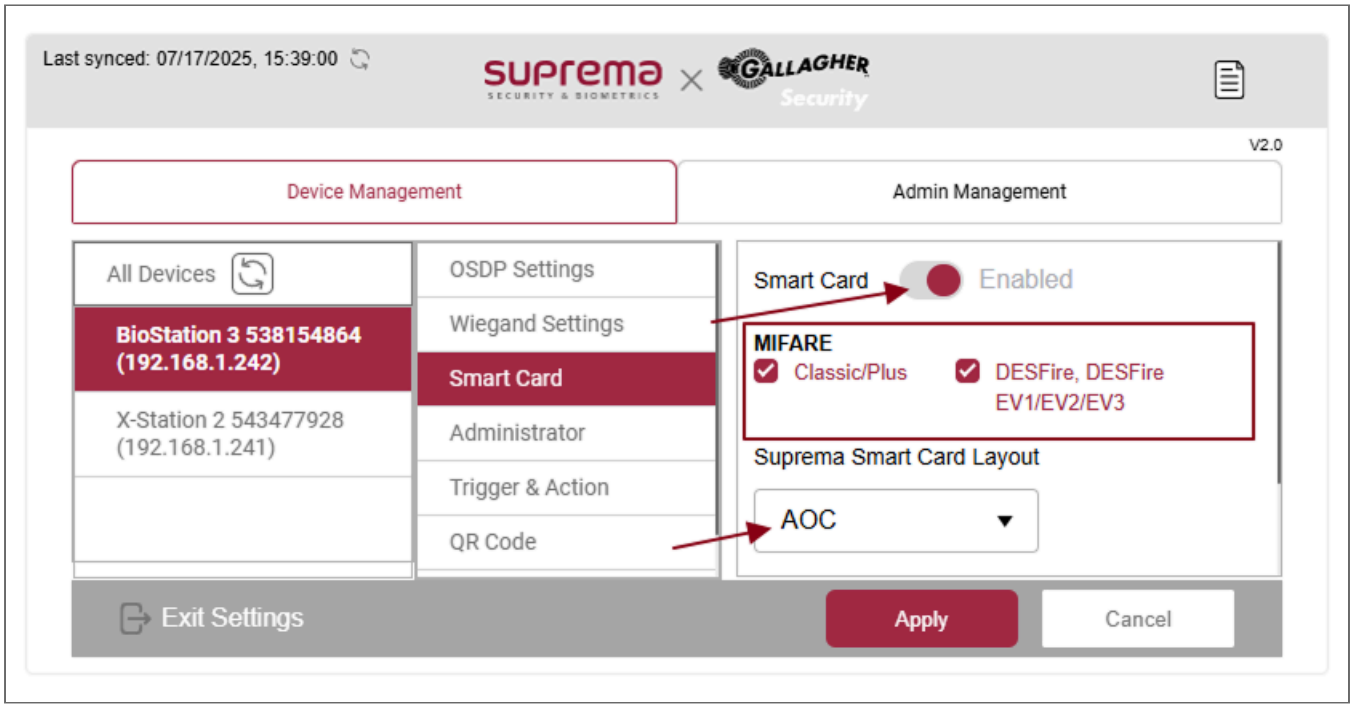
Información

Debes tener BioStar 2 versión 2.9.4 o superior para usar la función de tarjeta inteligente.

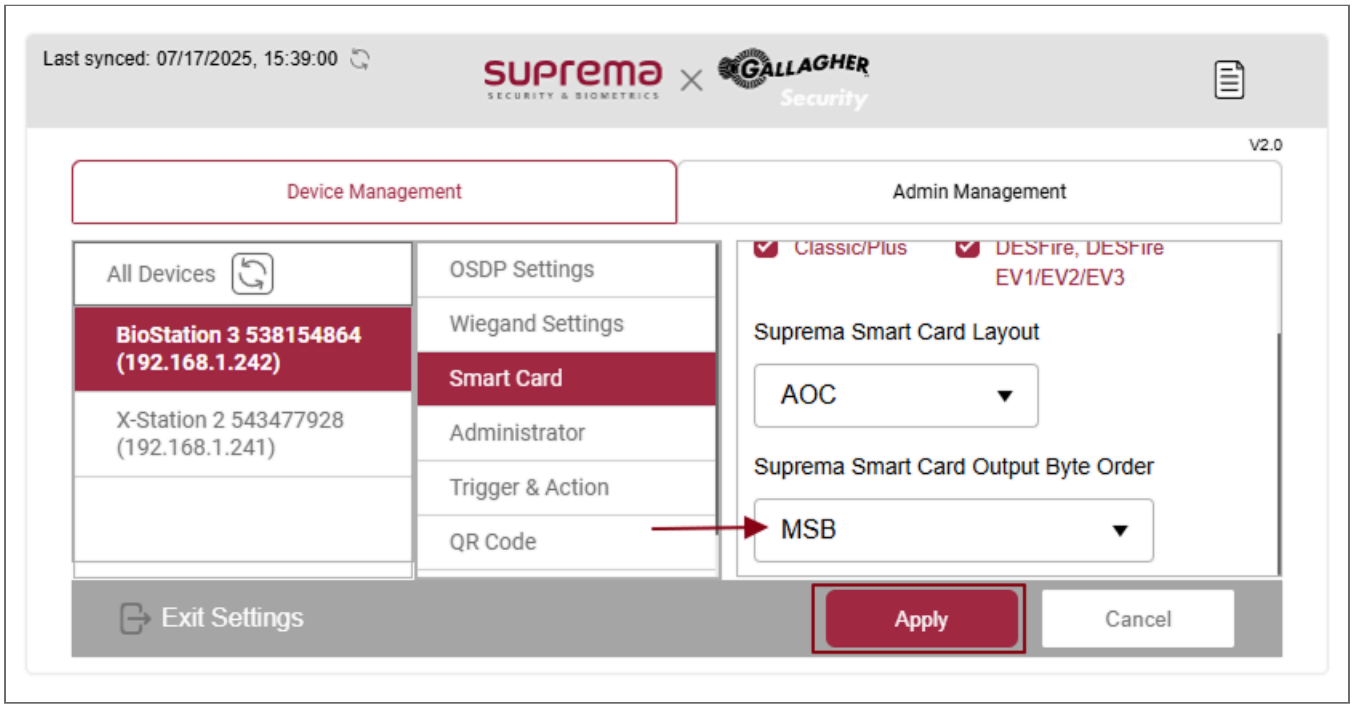
1. Si quieres usar la opción de tarjeta inteligente (AOC/TOC), ve a la configuración del dispositivo, **presiona** el botón **Configuración**, y dentro de Device Management **selecciona** el dispositivo que deseas configurar y **selecciona** la opción Smart Card.



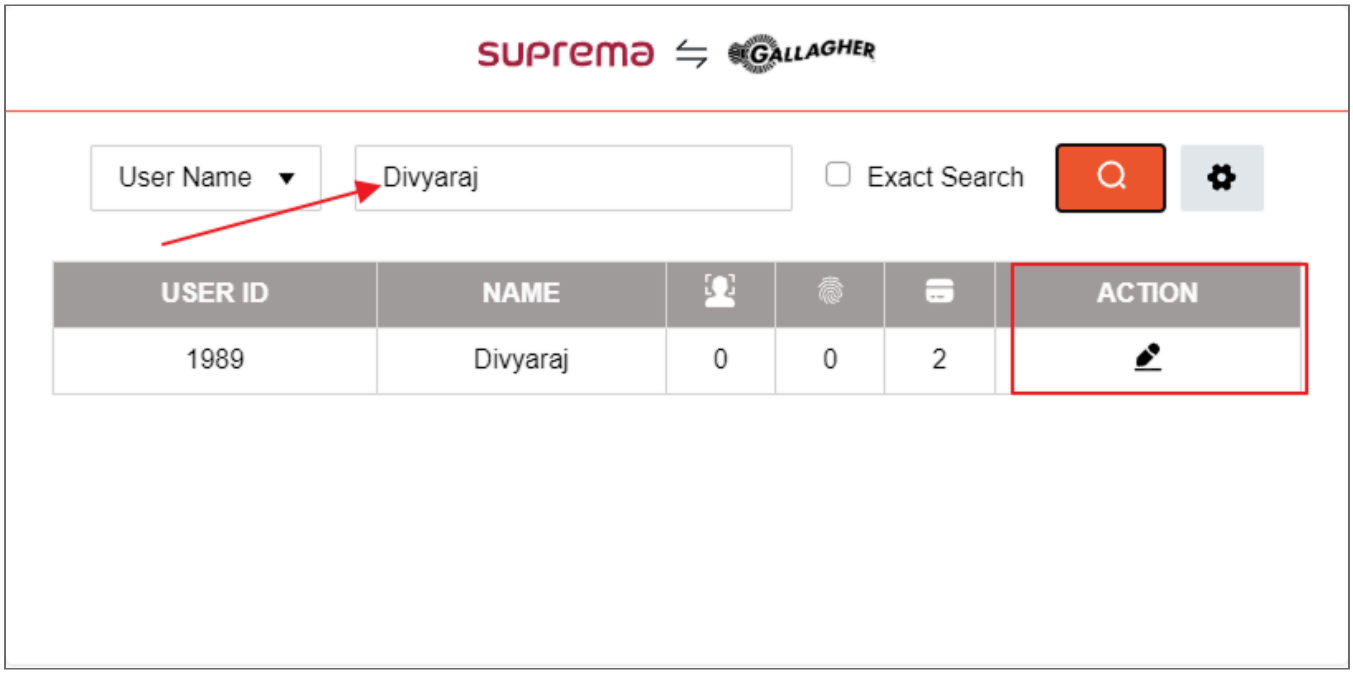
2. Ahora **habilita** el selector de Smart Card y realiza los siguientes ajustes como se muestra abajo.



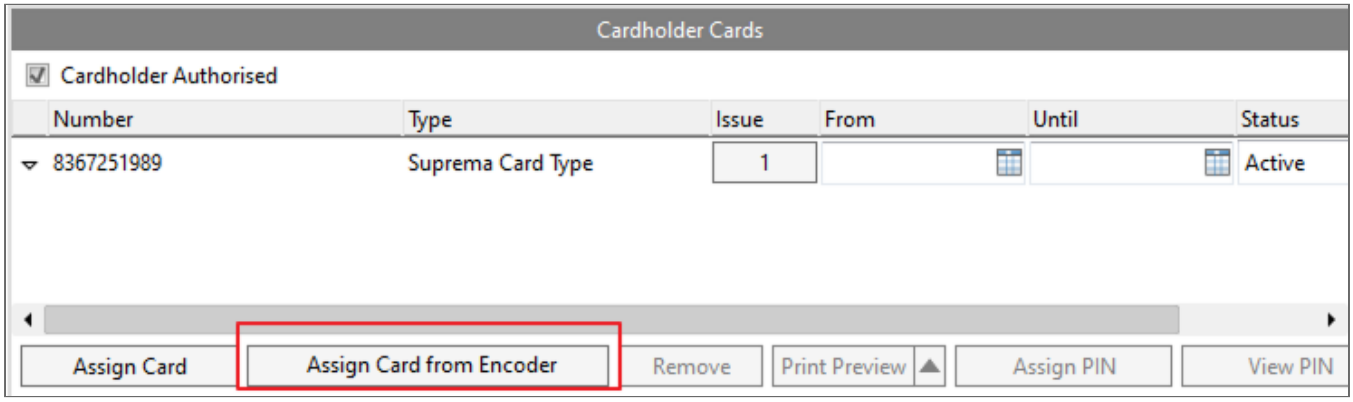
3. Después de cambiar todos los ajustes, **presiona** el botón Apply. Después de eso, **presiona** el botón Exit Settings en la esquina inferior izquierda para salir de la pestaña de configuración.



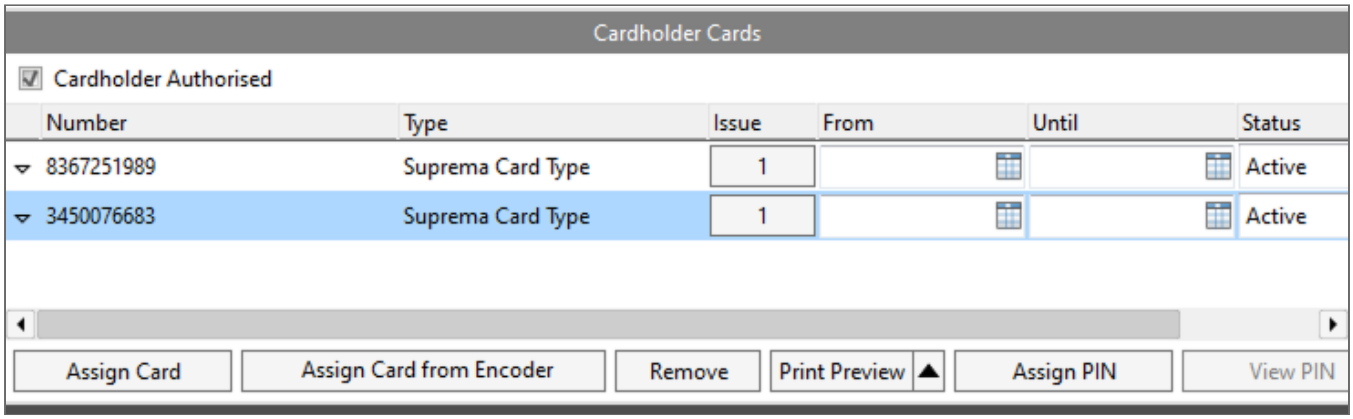
4. Ahora busca al usuario en la pantalla de búsqueda de usuarios; a quien deseas aplicar la tarjeta inteligente y **presiona** el botón editar para ver los detalles del usuario.



5. Ahora, para asignar la tarjeta inteligente, debes asignar una tarjeta desde el codificador en Gallagher dentro de la pestaña de tarjetas del titular.

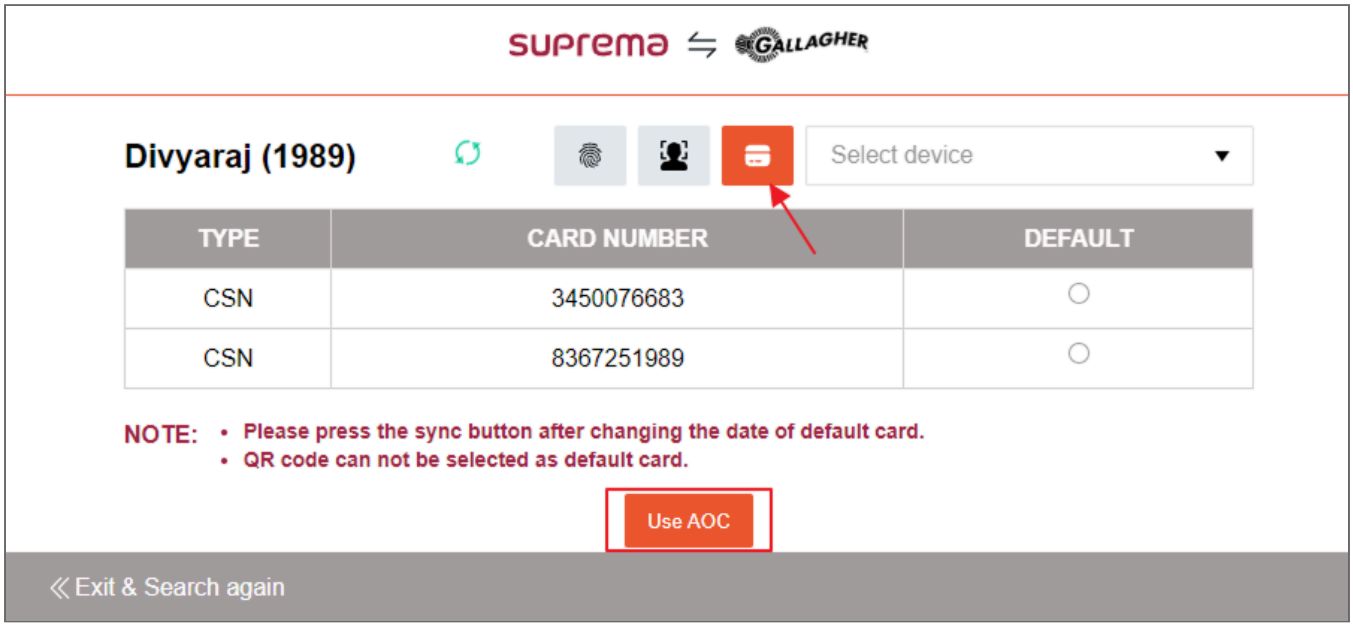


6. Después de presionar el botón, puedes ver el número de tarjeta; ahora debes **presionar** Guardar en Gallagher y verás la tarjeta recién asignada.

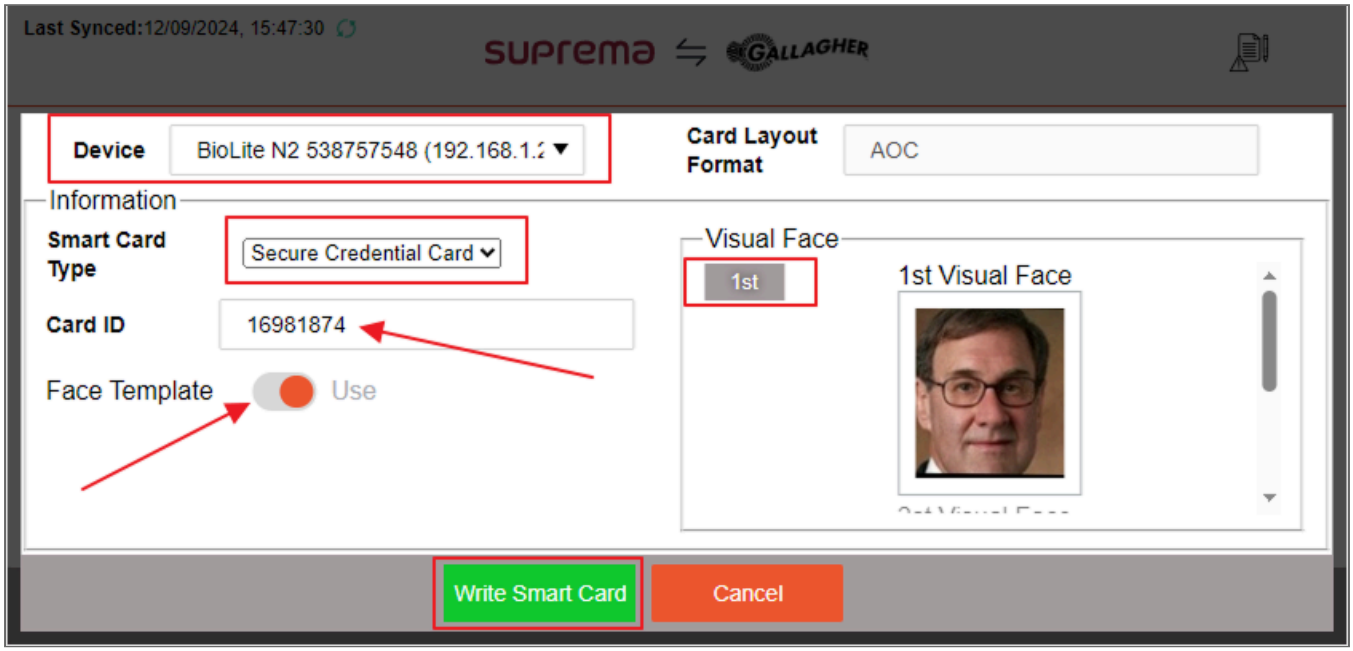


7. Ahora, dentro de la tabla de detalles del usuario, **ve** a la sección de tarjetas y **presiona** el botón Use AOC para asignar una tarjeta inteligente al usuario.

> **Información**
> Para asignar una tarjeta inteligente (AOC) al usuario, el usuario debe tener datos biométricos.



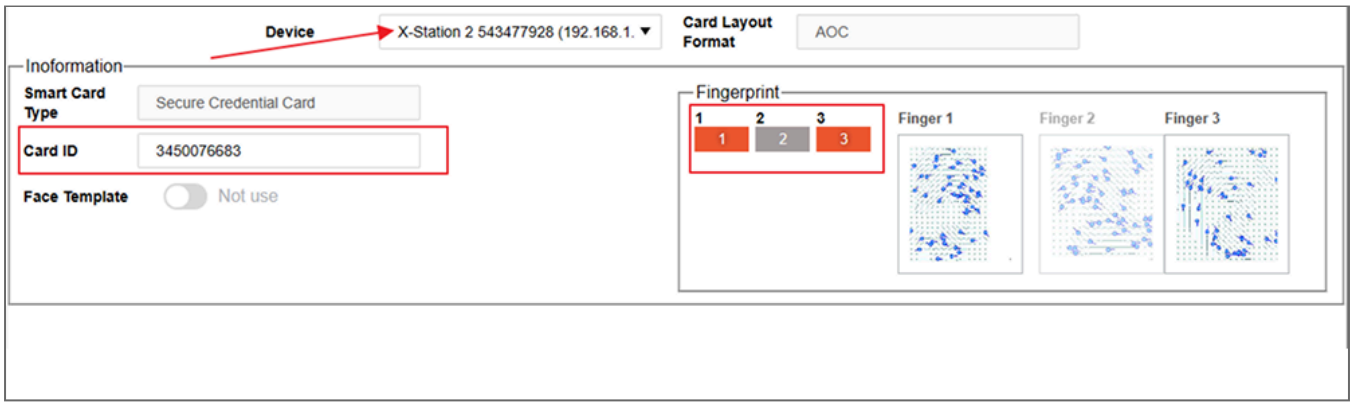
8. Ahora **selecciona** el dispositivo que usarás para AOC y **usa** el mismo número para la ID de tarjeta que obtuvimos al asignarla desde el codificador. **Selecciona** la plantilla facial y **elige** una imagen de la pestaña de rostro visual. **Presiona** el botón write smart card.



9. Ahora debes **escanear** la misma tarjeta en el dispositivo seleccionado para asignarla al usuario. Si no escaneas la misma tarjeta, obtendrás un mensaje de error; de lo contrario, escribirá la tarjeta para el usuario y borrará toda la información biométrica del usuario.

> **Información**
> Solo puedes asignar un dato biométrico a la tarjeta inteligente (AOC) del usuario.

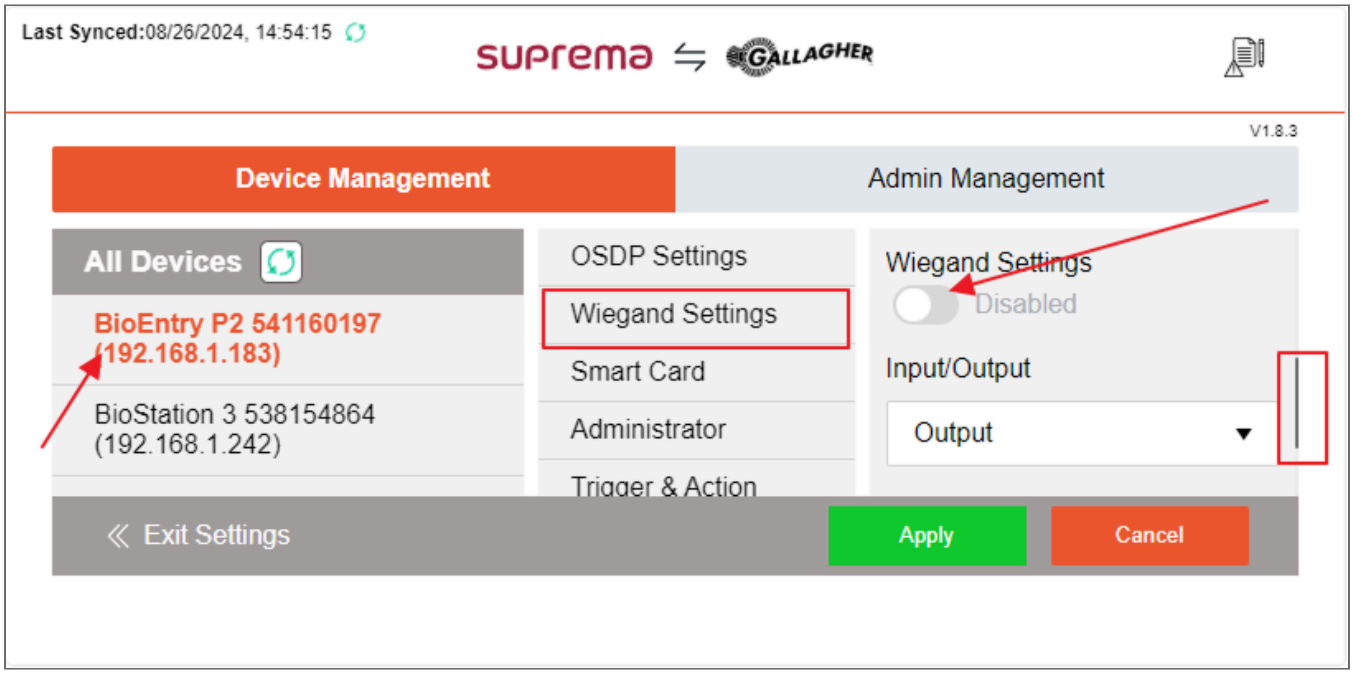
10. Para asignar la tarjeta inteligente con un usuario de huella dactilar, el usuario debe tener una huella dactilar; el usuario puede asignar hasta 2 huellas dactilares por tarjeta. Dentro de la sección de tarjetas del usuario, **presiona** el botón Use AOC y selecciona el dispositivo, **usa** el mismo número para la ID de tarjeta que obtenemos al asignar una tarjeta desde el codificador. **Selecciona** las huellas dactilares que deseas usar para la tarjeta inteligente. **Presiona** el botón write smart card.



11. Ahora debes **escanear** la misma tarjeta en el dispositivo seleccionado para asignarla al usuario. Si no escaneas la misma tarjeta, obtendrás un mensaje de error; de lo contrario, escribirá la tarjeta para el usuario y borrará toda la información biométrica del usuario.

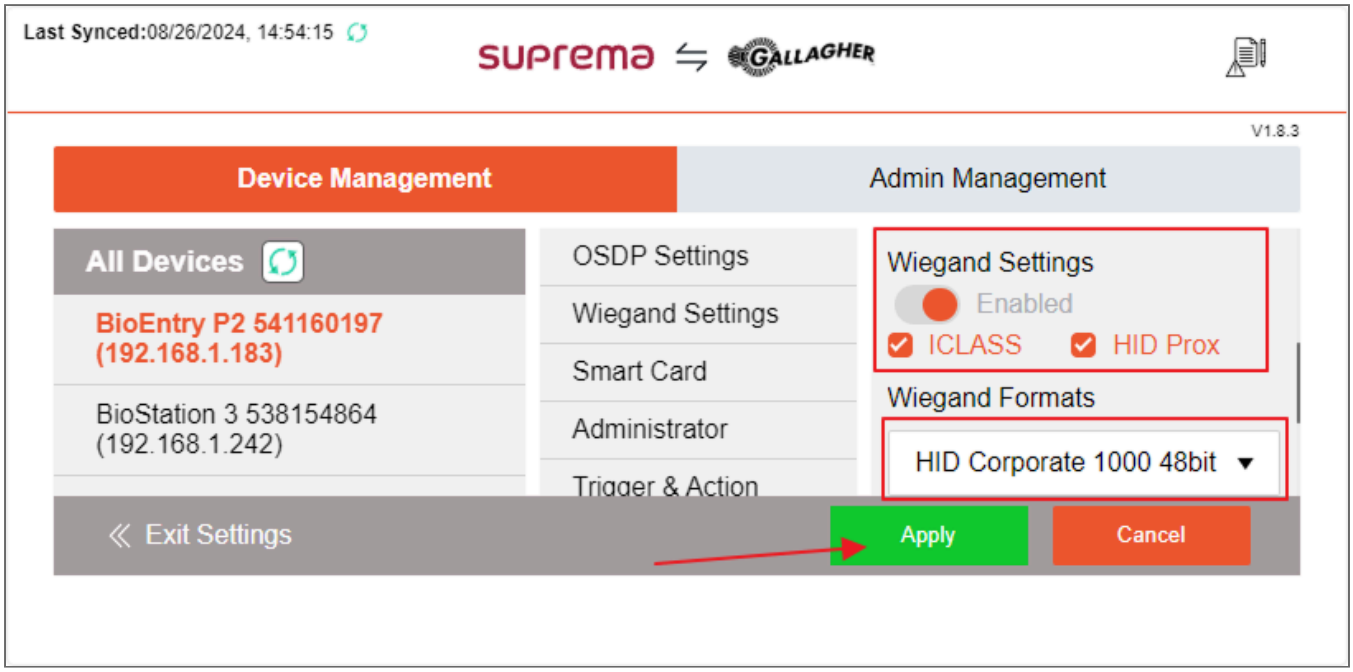
Tarjeta HID ICLASS

1. Si quieres usar la opción de tarjeta HID ICLASS, ve a la configuración del dispositivo, **presiona** el botón **Configuración**, y dentro de Device Management **selecciona** el dispositivo que deseas configurar y **selecciona** la opción Wiegand Settings; luego desplázate hacia abajo y busca la configuración de Wiegand.

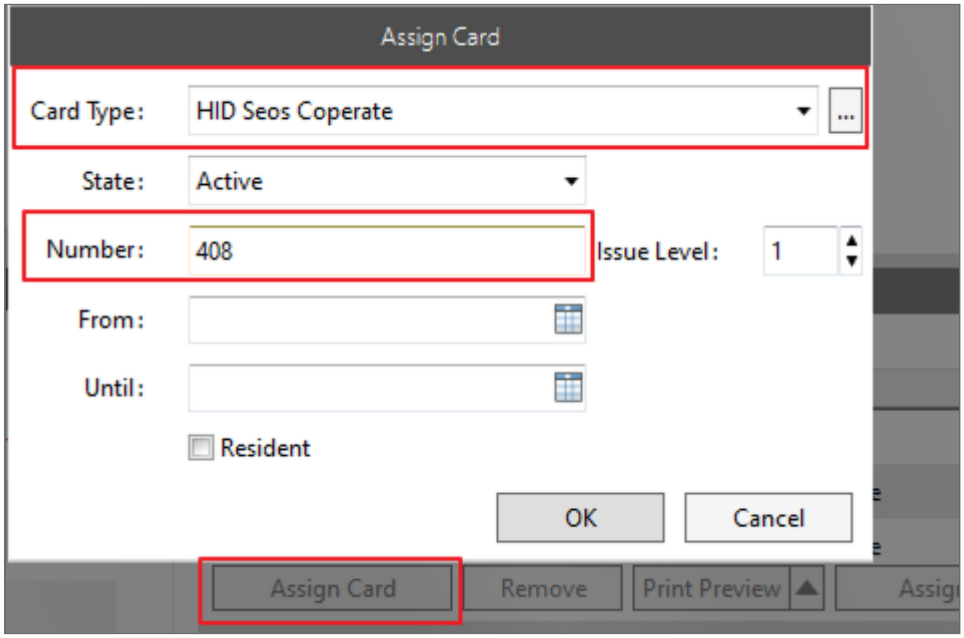


2. Ahora habilita la opción Wiegand Settings y **selecciona** las opciones ICLASS AND HID PROX. El formato Wiegand debe ser el mismo que el predeterminado seleccionado en el menú desplegable. **Presiona** el botón Apply para guardar los cambios.

> **Información**
> Para usar la tarjeta Wiegand, el usuario debe tener al menos un dato biométrico.

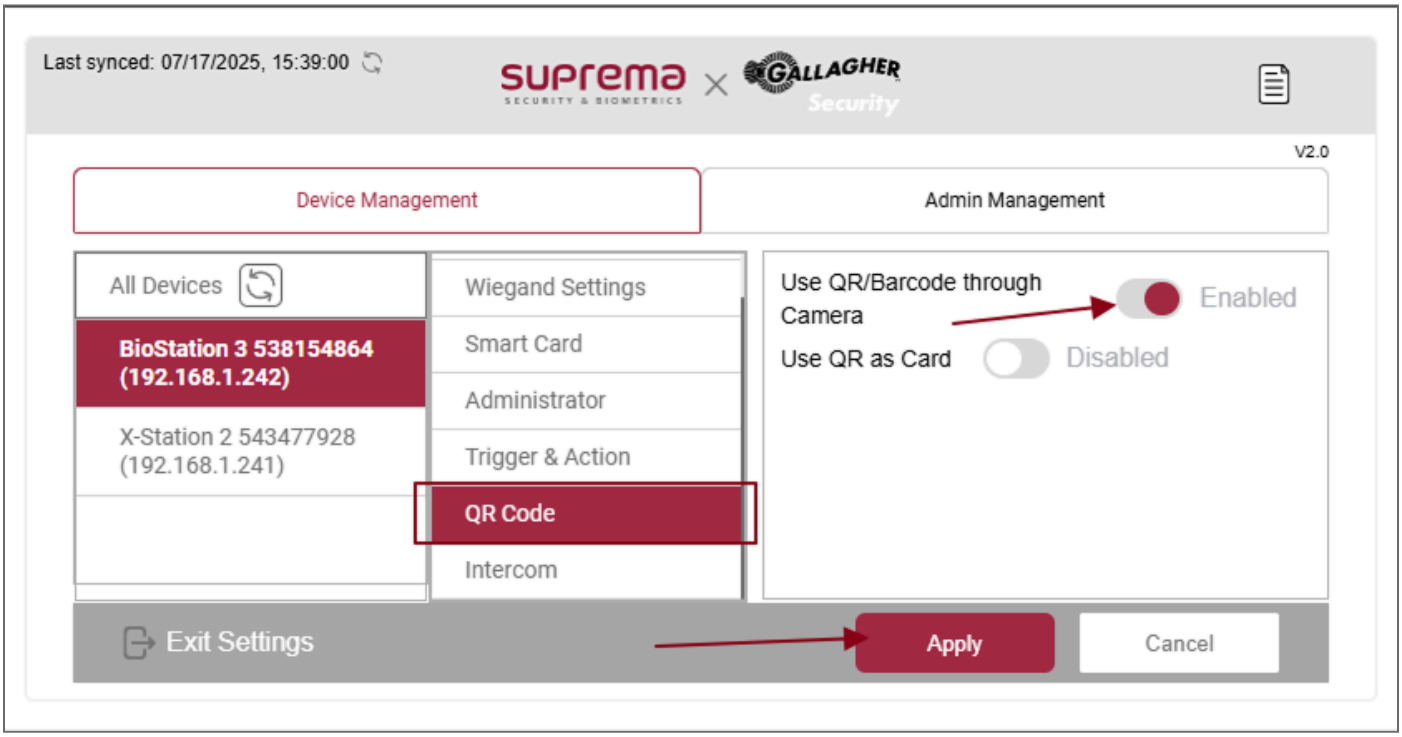


3. Para usar la función, debes asignar la tarjeta al usuario. Ve al Command Center de Gallagher, presiona el botón asignar tarjeta, **selecciona** HID Seos Corporate, **ingresa** el número, **presiona** el botón OK y **presiona** Guardar.



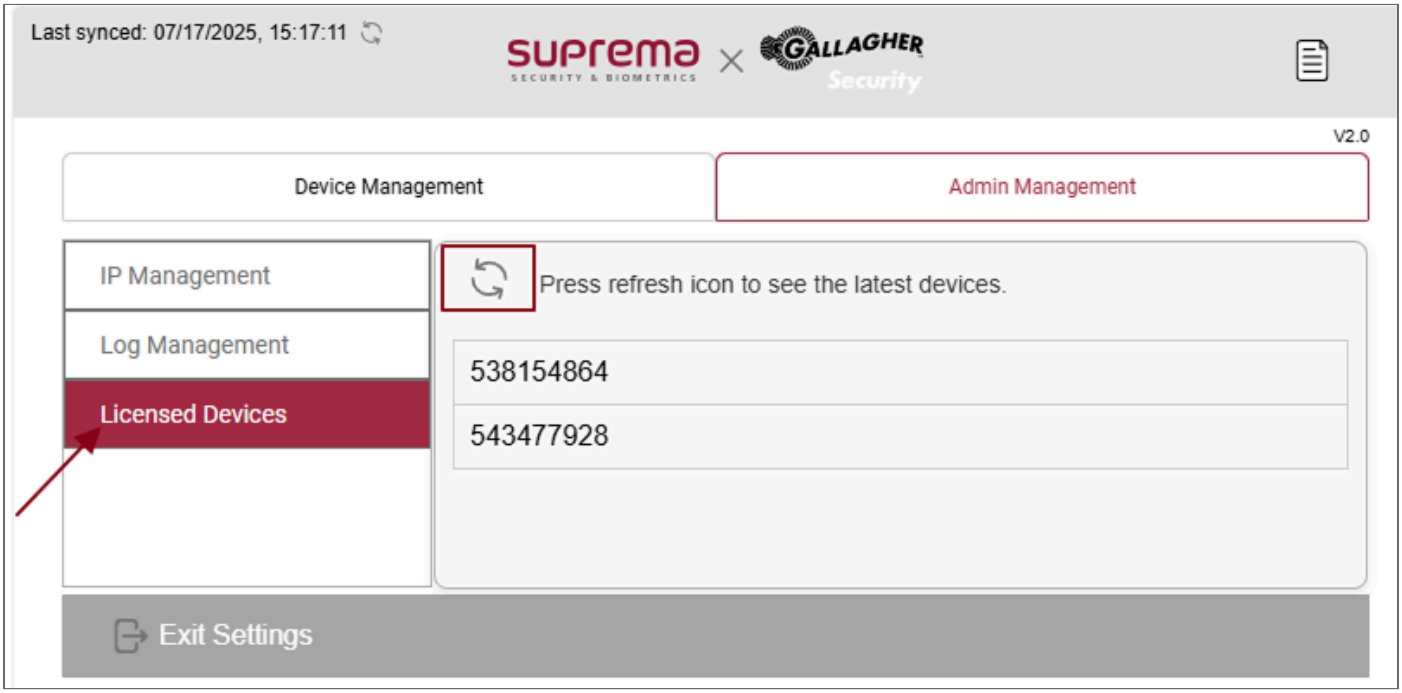
Tarjeta de código QR

Si quieres usar la opción de tarjeta de código QR, ve a la configuración **presionando** el botón **Configuración**, y dentro de Device Management, **selecciona** el dispositivo que deseas configurar. Luego, **selecciona** la opción QR Code Settings y **habilita** el uso de QR/Barcode mediante la configuración de la opción de cámara. **Presiona** el botón Apply para guardar los cambios.



Dispositivos con licencia

Si necesitas revisar los dispositivos asociados con la **licencia**, debes ir a **Admin Management** en **configuración** y **hacer clic** en Licensed devices; luego debes **presionar** el botón de sincronización. Mostrará la lista de los dispositivos más recientes asociados con tu licencia.



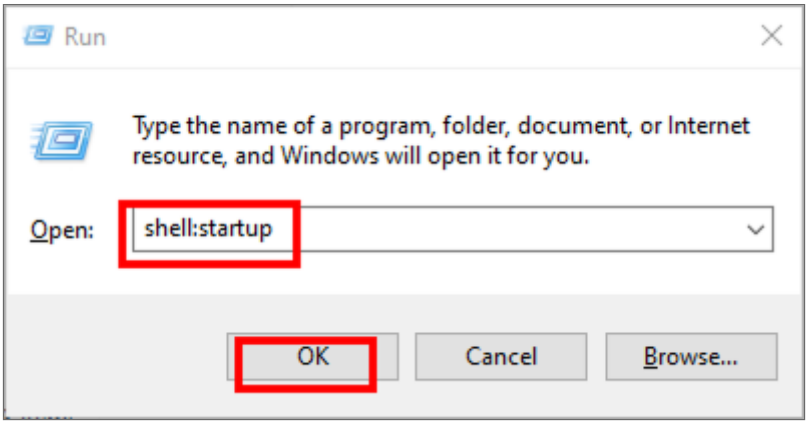
Solución de problemas y preguntas frecuentes

Configuración

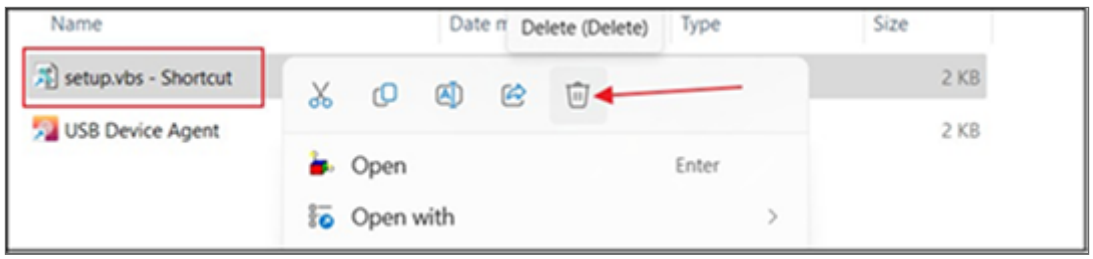
Q. Actualice solo el middleware a la nueva versión (proceso manual).

A. Si solo desea actualizar el middleware, solo necesita seguir los pasos que se muestran a continuación.

> **Información**
> Si está actualizando el middleware a la versión V1.8.3, consulte: Crear migración manualmente.

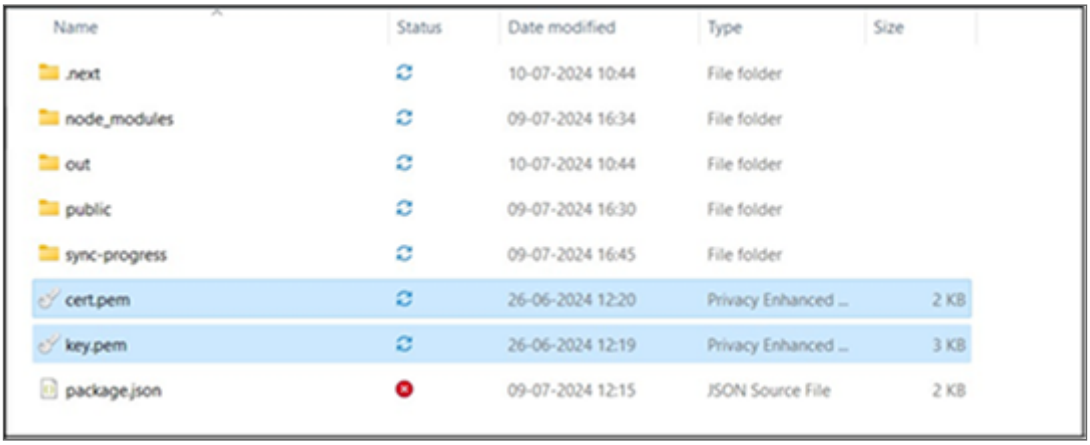


Elimine la versión anterior `setup.vbs - Shortcut`.



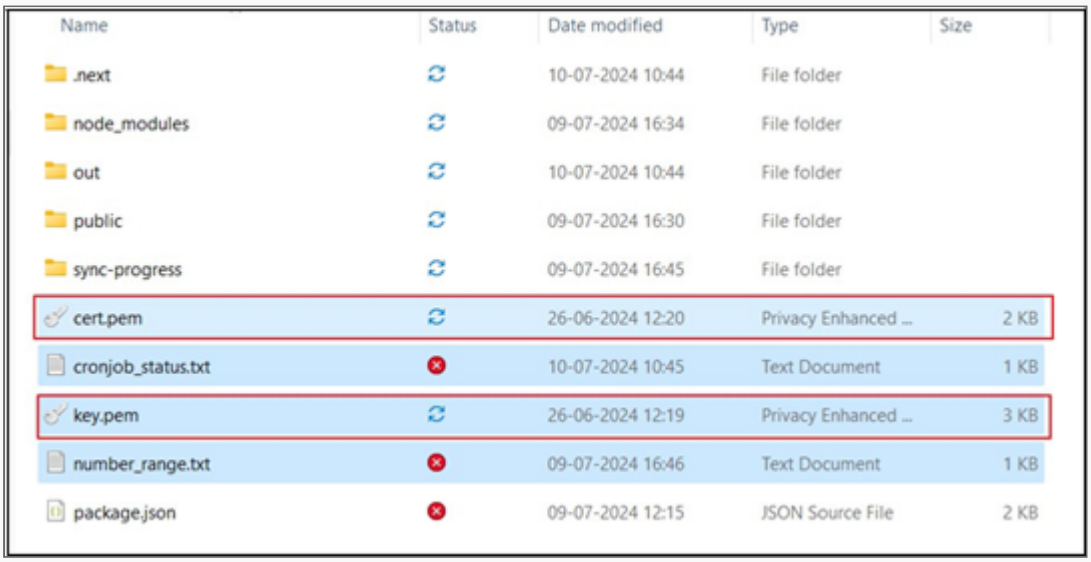
Corte los archivos de certificado y clave de la versión que usa actualmente, como se muestra en la imagen siguiente.

La ruta predeterminada sería: `C:\Program Files\Suprema Integration with Gallagher\Suprema Integration with Gallagher v(Current working version)\files`

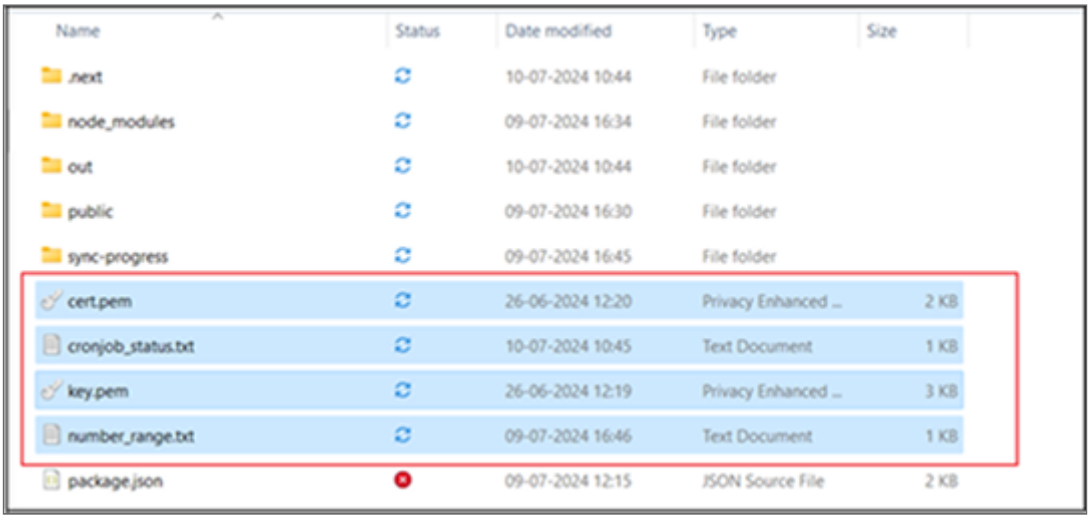


Información

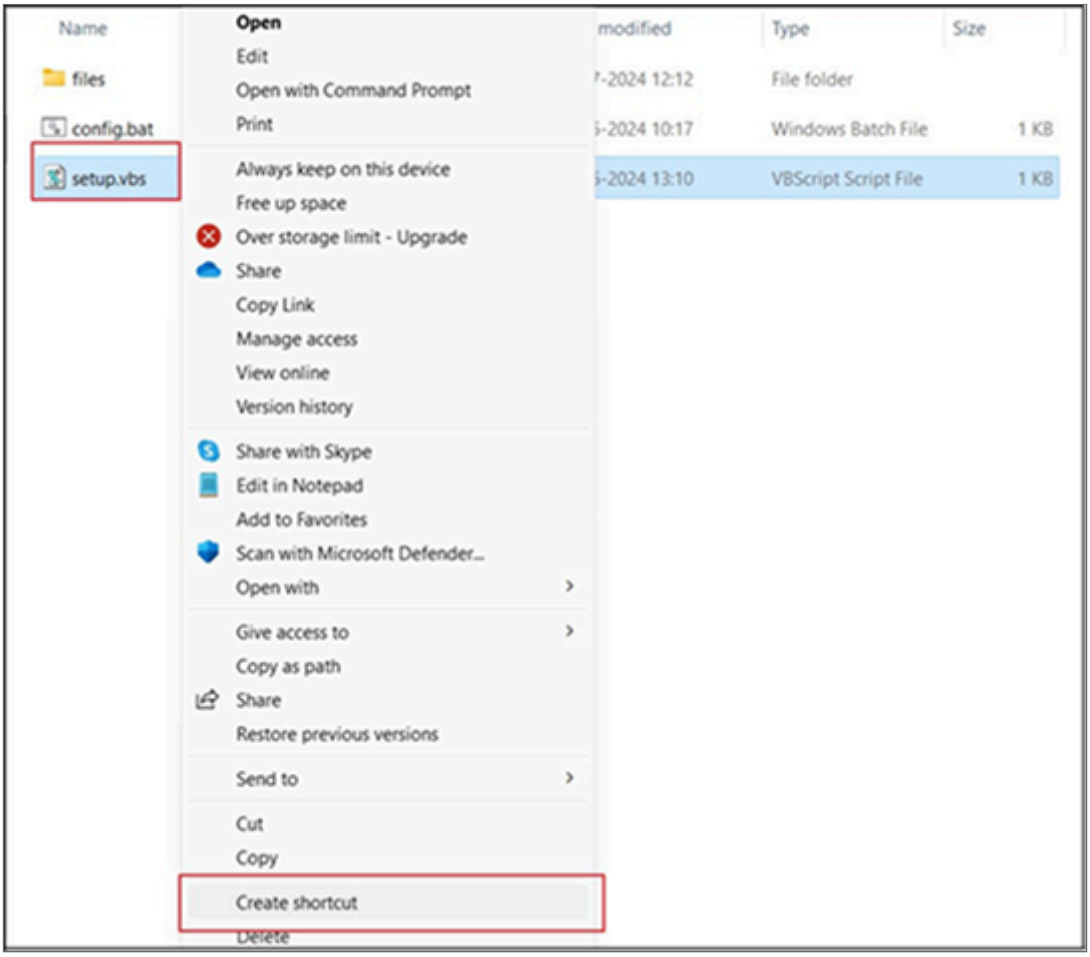
- Si está actualizando desde la versión 1.8.0 o superior, deberá cortar un total de cuatro archivos: `key.pem`, `cert.pem`, `cronjob_status.txt` y `number_range.txt`.
- En la versión 1.7.0, solo `number_range` no está disponible, así que corte los otros tres archivos.



Ahora **pegue** los archivos en la nueva versión de la integración de Suprema en `Gallagher V(new version)\files`. Como se mencionó antes, si está actualizando desde la 1.8.0 o superior, deberá cortar 4 archivos y la imagen siguiente muestra los archivos pegados en la nueva versión; así que, si no tiene 4 archivos, solo pegue 2 archivos de la versión anterior en la nueva versión.



Cree un acceso directo de `setup.vbs` de la última versión de la integración de Suprema con Gallagher y corte el archivo de acceso directo.



Vaya a `Win + R`, péguelo en `shell:startup` y después reinicie su escritorio.

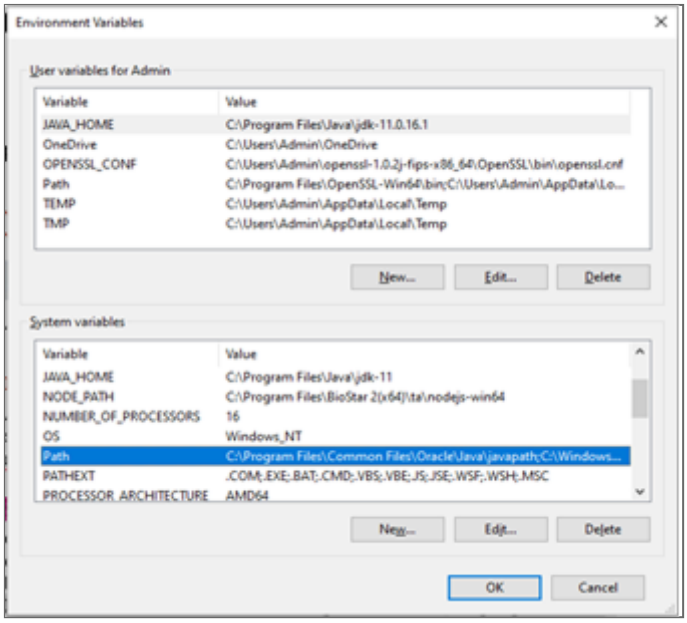
Q. Si el middleware no se inicia automáticamente.

A. Primero, asegúrese de que el acceso directo del archivo `setup.vbs` esté presente en `shell:startup`. Si `setup.vbs` no está presente, péguelo en `shell:startup` y reinicie el sistema.

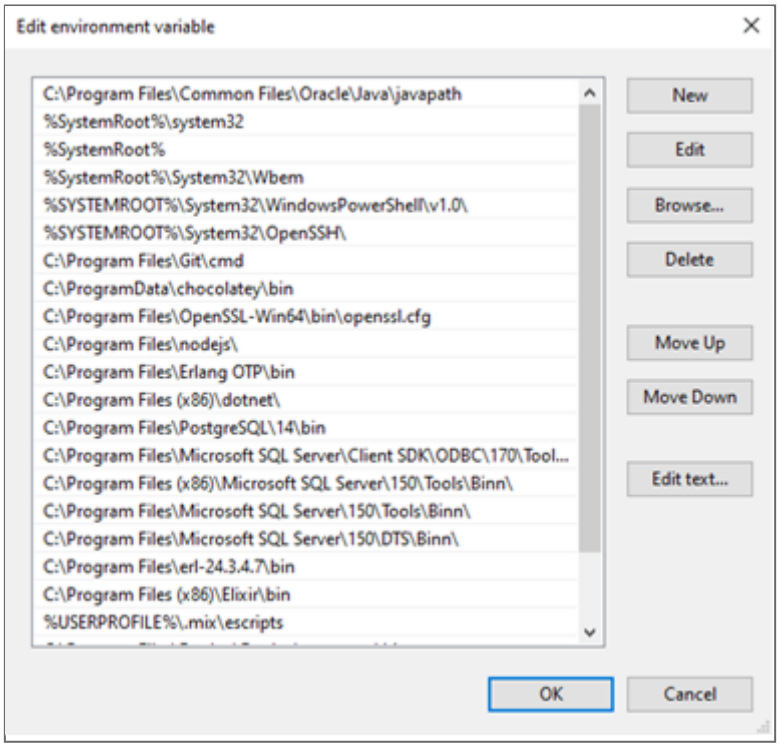
Si el middleware aún no se inicia automáticamente, revise la variable de entorno. Puede acceder a ella presionando

Inicio → Editar las variables de entorno del sistema → haga clic en la pestaña **Avanzado** → botón **Variables de entorno** cerca de la parte inferior de esa pestaña.

En la ventana *Variables de entorno* (mostrada abajo), seleccione la variable **Path** en la sección *Variables del sistema* y haga clic en el botón **Editar**.



Se abrirá la ventana de edición de la variable de entorno (mostrada abajo). Haga clic en el botón **Nuevo**, agregue la ruta `C:\Program Files\nodejs\` y presione el botón **OK**.



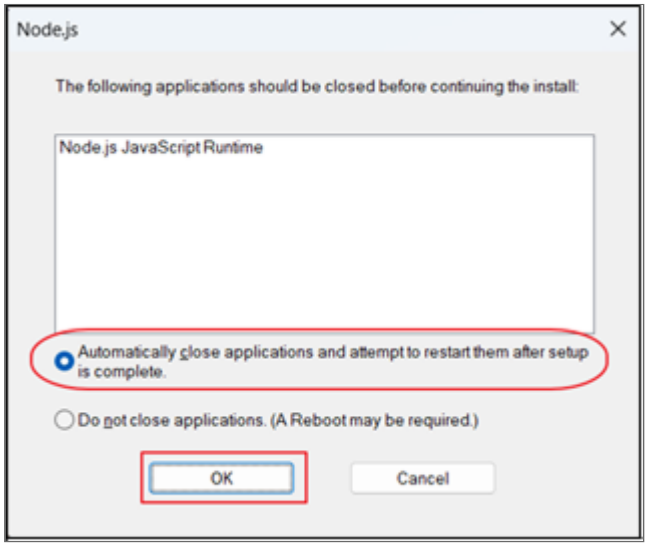
Presione el botón **OK** para la ventana *Variables de entorno* y luego presione el botón **OK** para las propiedades del sistema.

> **Información**
> Después de crear o modificar las variables de entorno, reinicie la computadora para que los cambios surtan efecto en Windows.

Q. Para desinstalar la lista de requisitos previos del middleware.

A. A continuación, se muestran los pasos para desinstalar los requisitos previos del middleware,

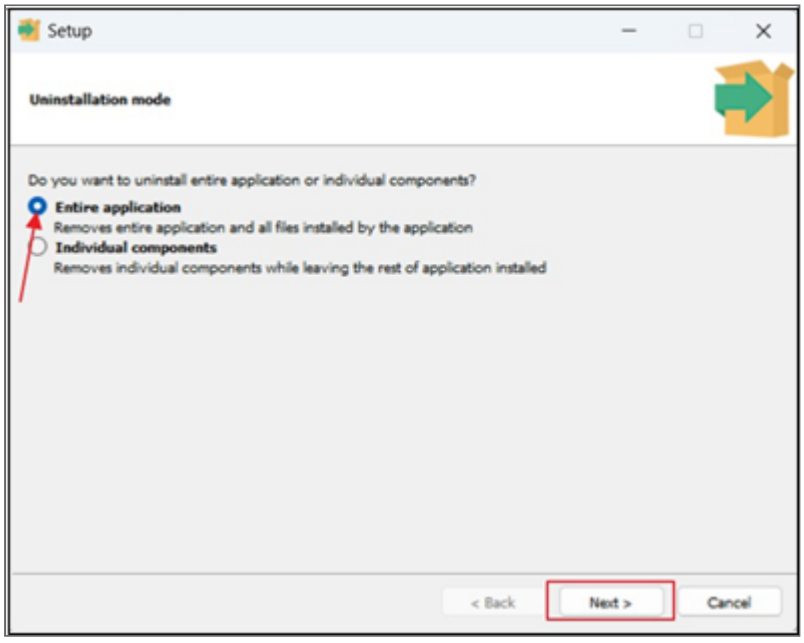
1. **Abra** el panel de control y vaya a la sección Programas y características.
2. Desplácese hacia abajo y **busque** Node.js. Haga clic derecho y **seleccione** Desinstalar.
3. Pide desinstalar Node.js, **presione** Sí y comenzará la desinstalación.
4. Después de un tiempo, cuando pida la aplicación Runtime, siga lo siguiente y **presione** OK. Omita este paso si no se aplica a su caso.



5. Ahora busque **OpenSSL**, haga clic derecho y **presione** desinstalar.
6. Pide desinstalar OpenSSL, presione **Sí** y comenzará la desinstalación.
7. Ahora busque **PgAdmin 4**, haga clic derecho y **presione** desinstalar.

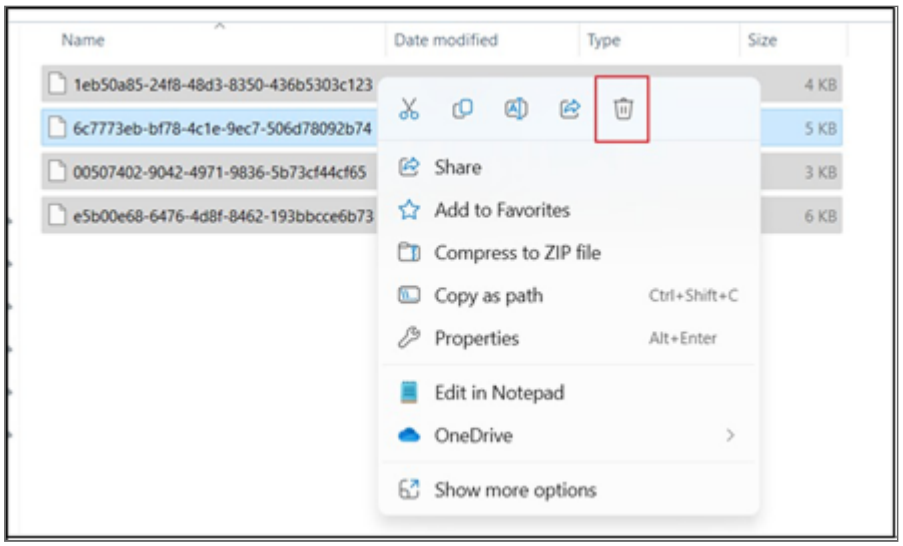
> **Información**
> Si no puede ver o desinstalar PgAdmin 4, omita el paso y siga los siguientes.

8. Pide desinstalar PgAdmin 4, presione **Sí** y comenzará la desinstalación.
9. Ahora **busque** PostgreSQL 14, haga clic derecho y **presione** desinstalar.
10. Pide desinstalar PostgreSQL 14, presione **Sí** y comenzará la desinstalación.
11. Cuando se abra el modo de desinstalación, **seleccione** el botón de opción Toda la aplicación y presione **Siguiente**.



12. Ahora **vaya** a `C:\Users\<YourUser>\AppData\Roaming\pgadmin\sessions` y elimine todos los archivos dentro de esta carpeta.

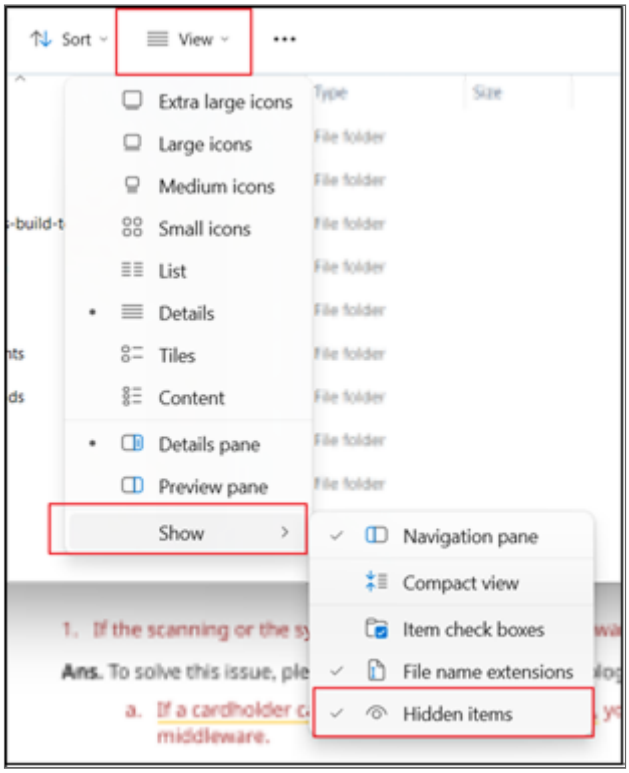
> **Información**
> Si no puede ver la carpeta AppData: Abra la carpeta AppData en Windows.



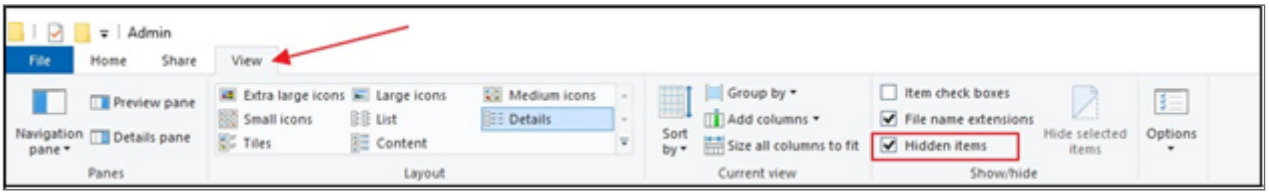
13. Ahora **vaya** a `C:\Users\<Your User>\AppData\Local`, seleccione las carpetas PgAdmin y PgAdmin4 y **elimine** las carpetas.
14. Ahora **vaya** a `C:\Program Files` y elimine la carpeta PostgreSQL.

Q. Cómo abrir la carpeta AppData en Windows.

A. Si usa Windows 11, dentro del administrador de archivos haga clic en la pestaña Vista, **seleccione** Mostrar y **haga clic** en Elementos ocultos.



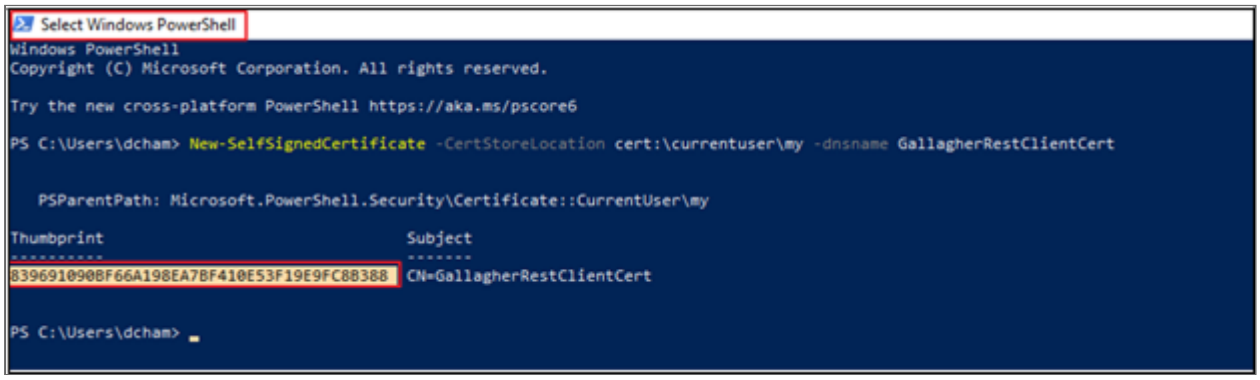
Si usa Windows 10, abra el Administrador de archivos y **haga clic en** Vista y **seleccione Elementos ocultos**.



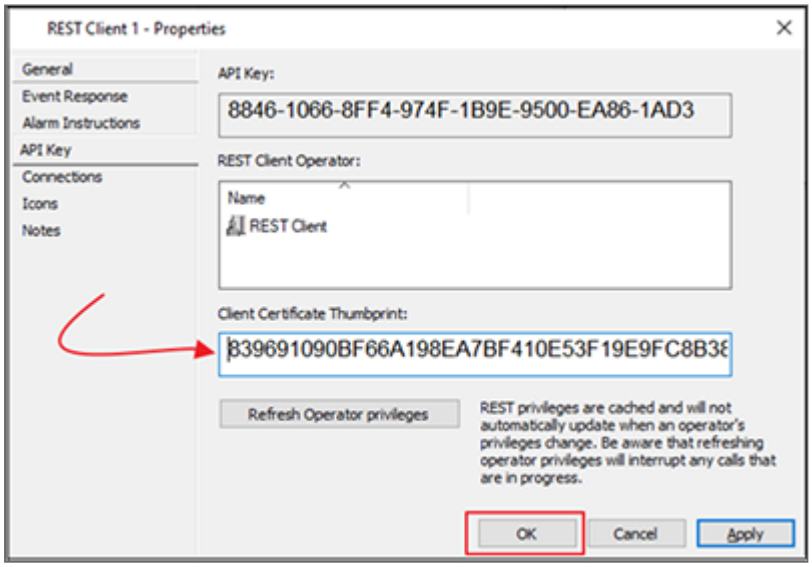
Q. Cómo generar manualmente el thumbprint y el certificado.

A. 1. Para generar el thumbprint del certificado del cliente, vaya a Windows PowerShell y ejecute este comando para obtener el thumbprint del certificado.

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

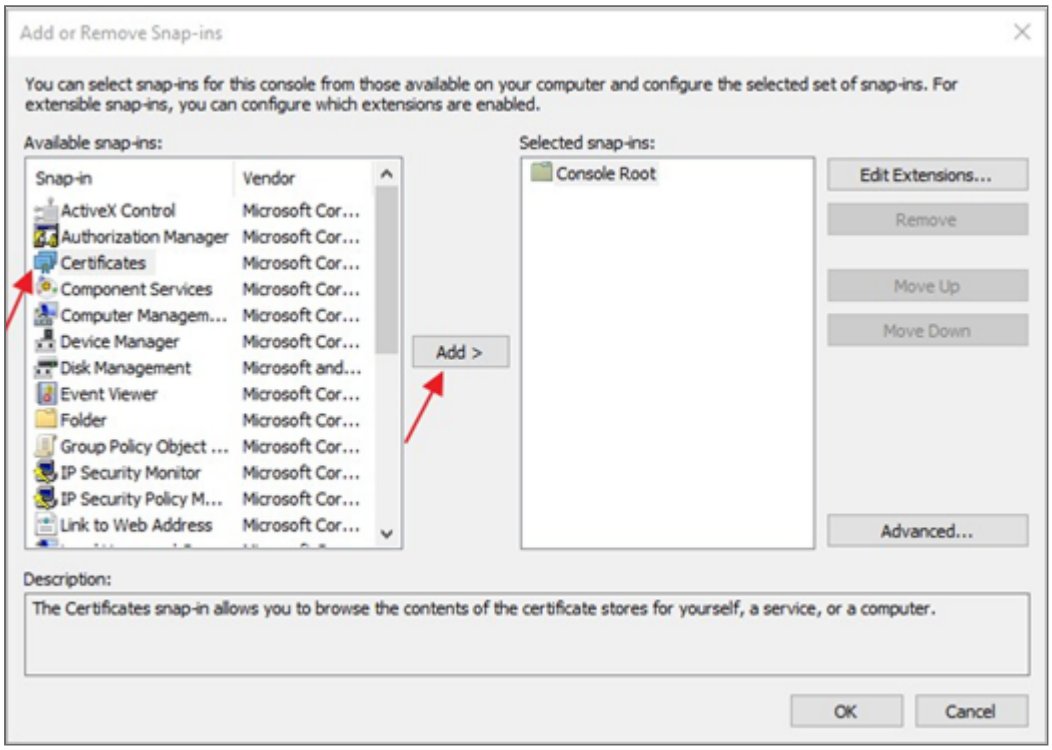


2. **Copie** el thumbprint y **pegue la clave del thumbprint del certificado del cliente** en la sección correspondiente. **Presione** el botón **OK** y también **cierre** Services and Workstations.

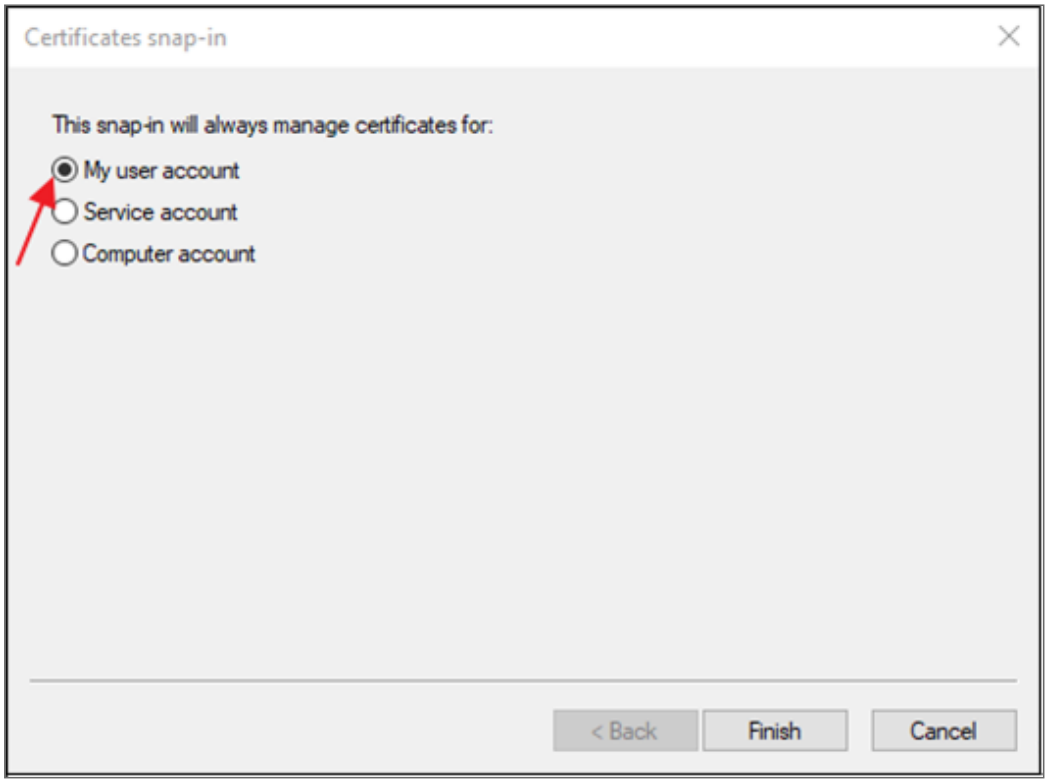


Generación de certificado SSL

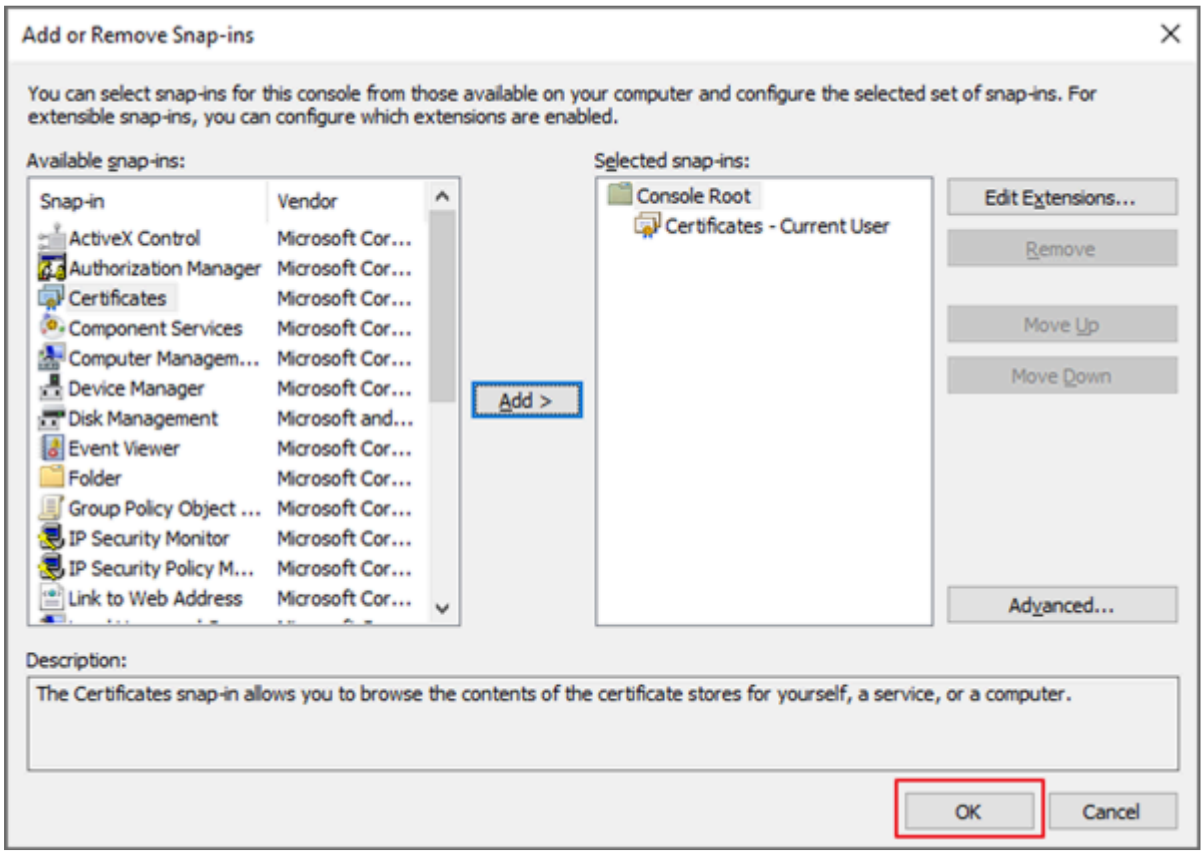
1. Vaya al menú Inicio y **abra** la aplicación **MMC**.
2. Vaya a **Archivo** → **Agregar o quitar complemento...** como se muestra en la pantalla siguiente.



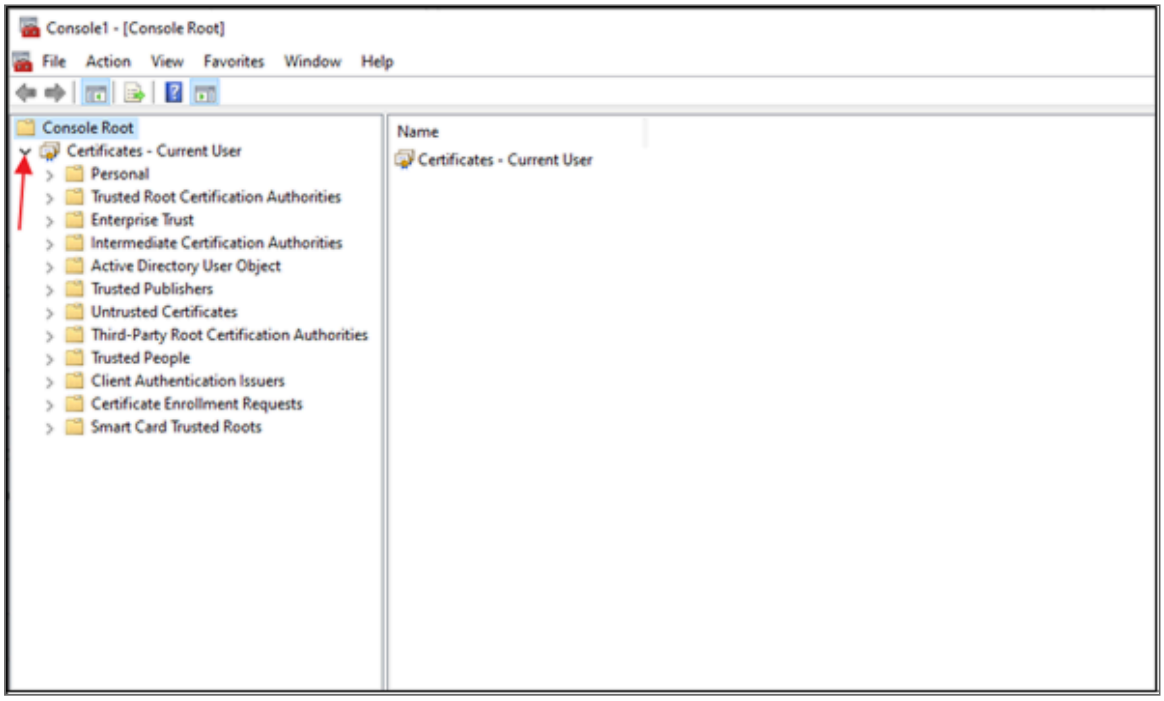
3. **Seleccione Certificados** y **haga clic** en el botón **Agregar**. Luego verá la pantalla siguiente, donde debe **seleccionar** la opción **Mi cuenta de usuario** y **hacer clic** en el botón **Finalizar**.

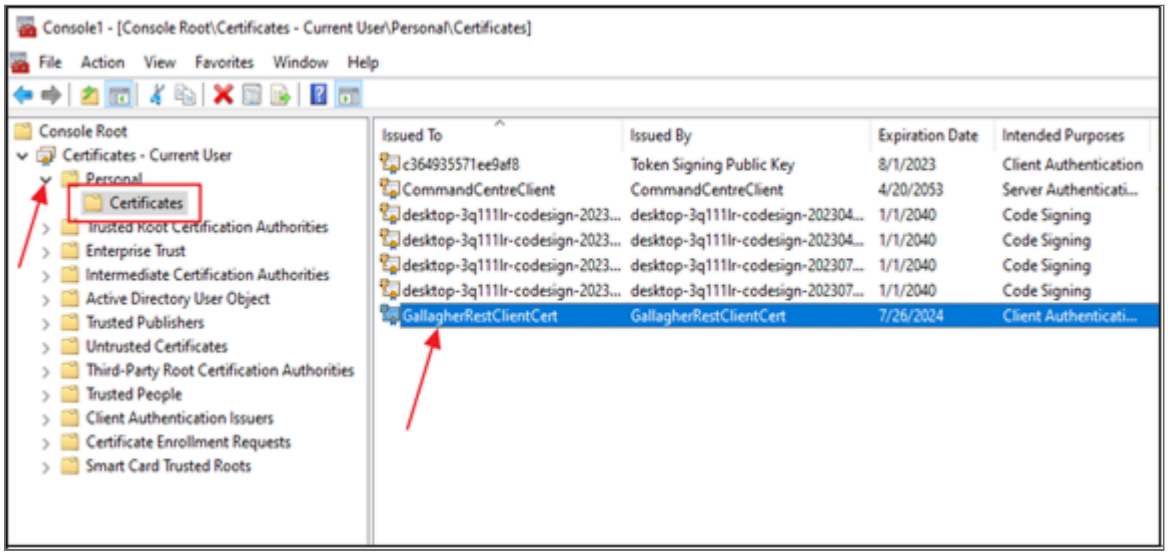


4. Después de hacer clic en Finalizar, verá la pantalla siguiente. Ahora **haga clic** en el botón **OK**. El certificado se agregará correctamente.

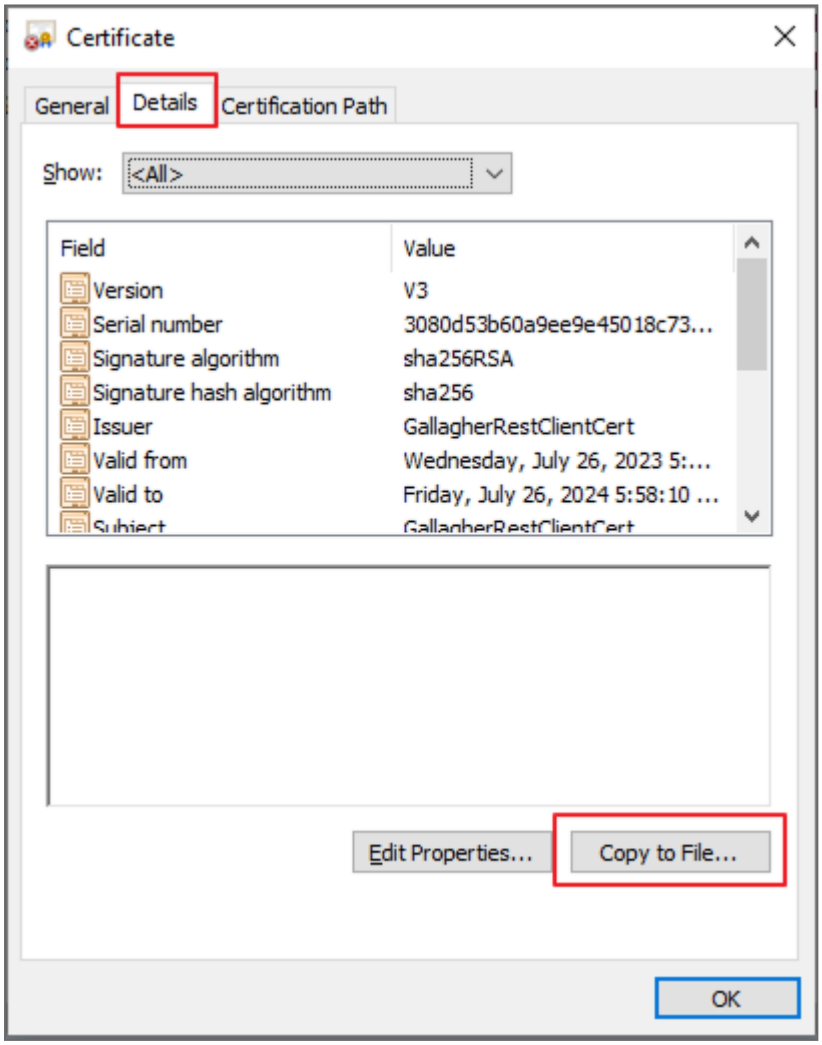


5. Ahora vaya a **Certificados - Usuario actual** → **Personal** → **Certificados** y seleccione el certificado **GallagherRestClientCert**.



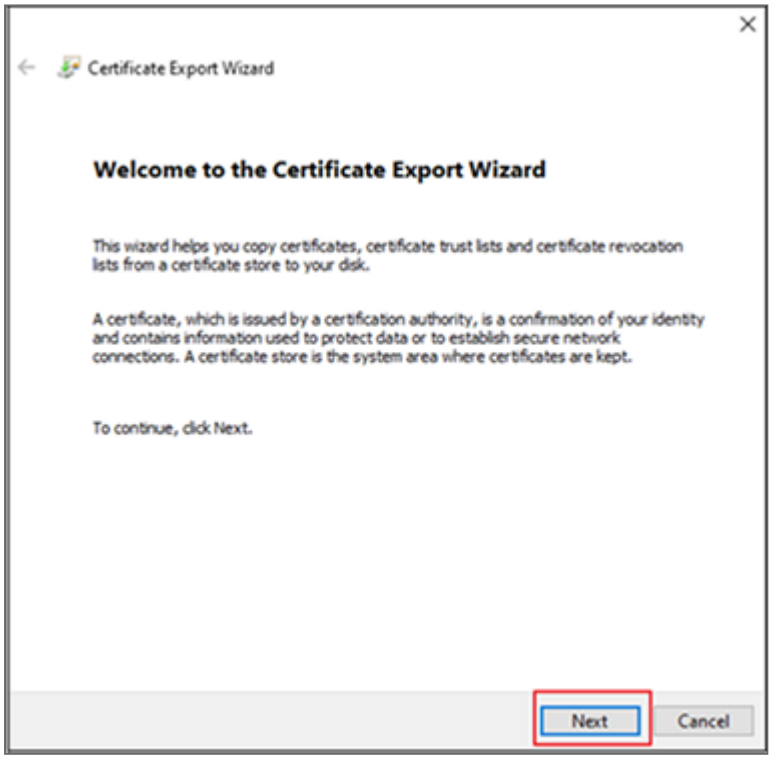


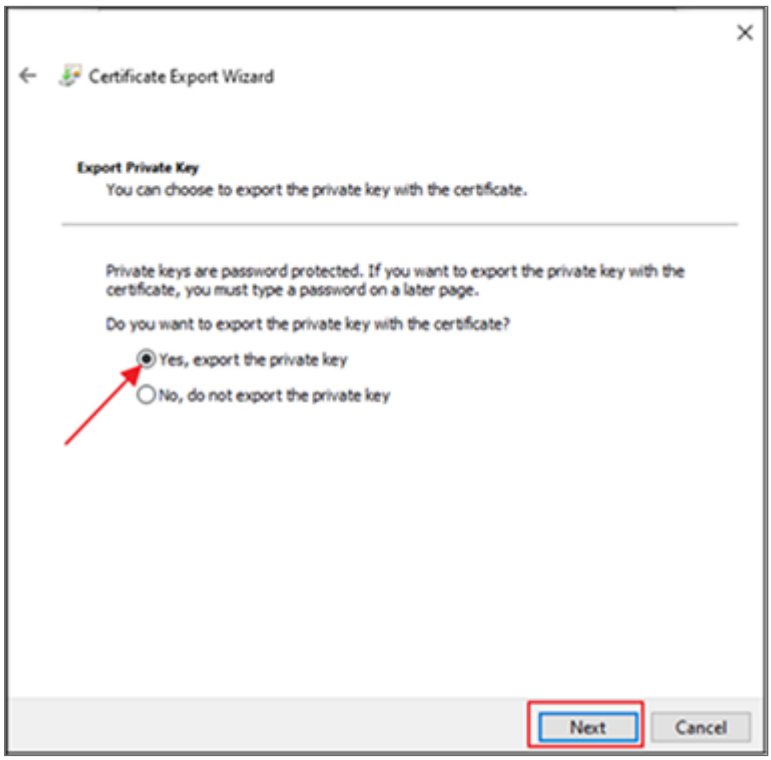
6. Vaya a **Detalles** y **haga clic** en **Copiar en archivo**.



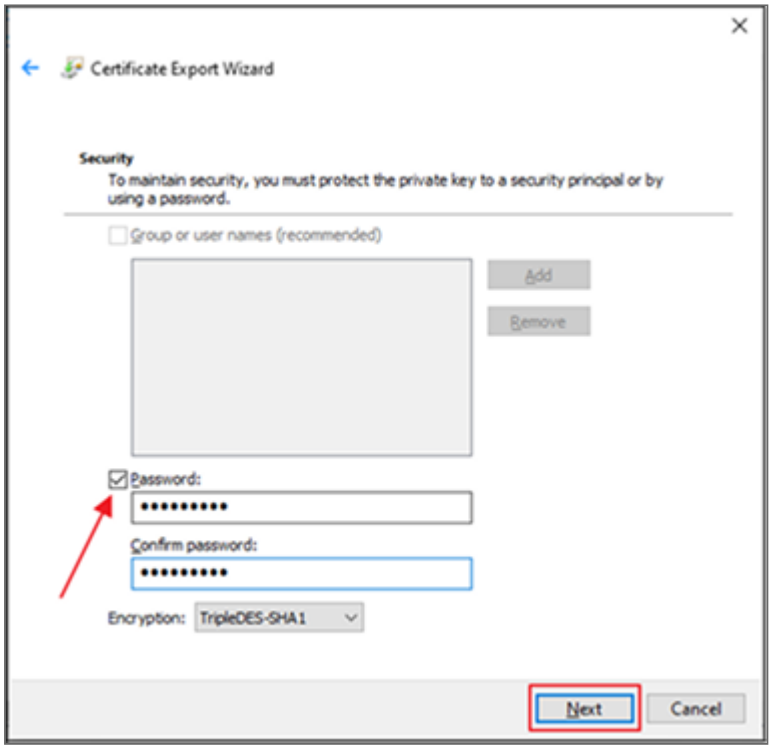
Ahora siga las capturas de pantalla siguientes y **haga clic** en **Siguiente** al mismo tiempo.

> **Información**
> Valide que el thumbprint sea correcto si tiene más de un certificado.

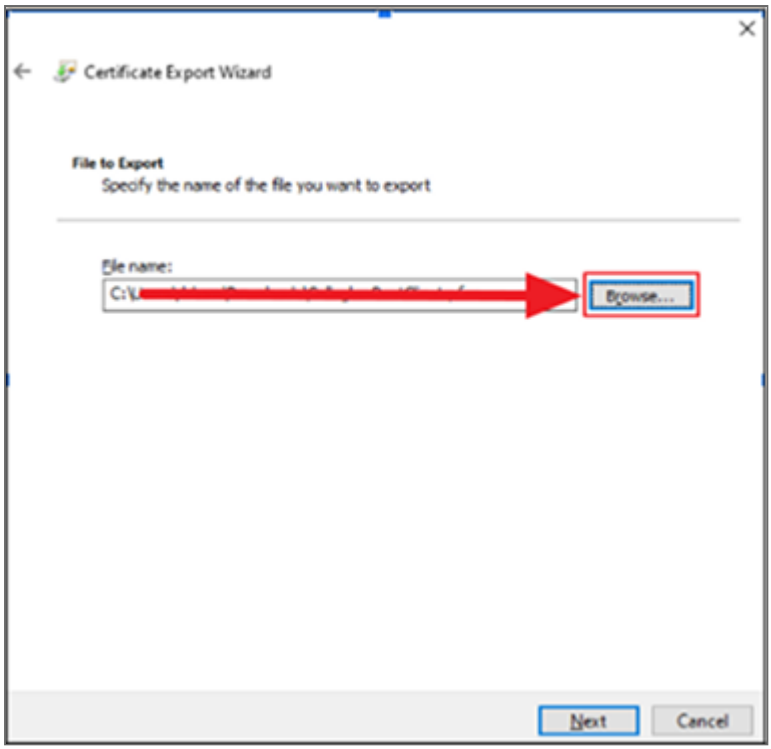


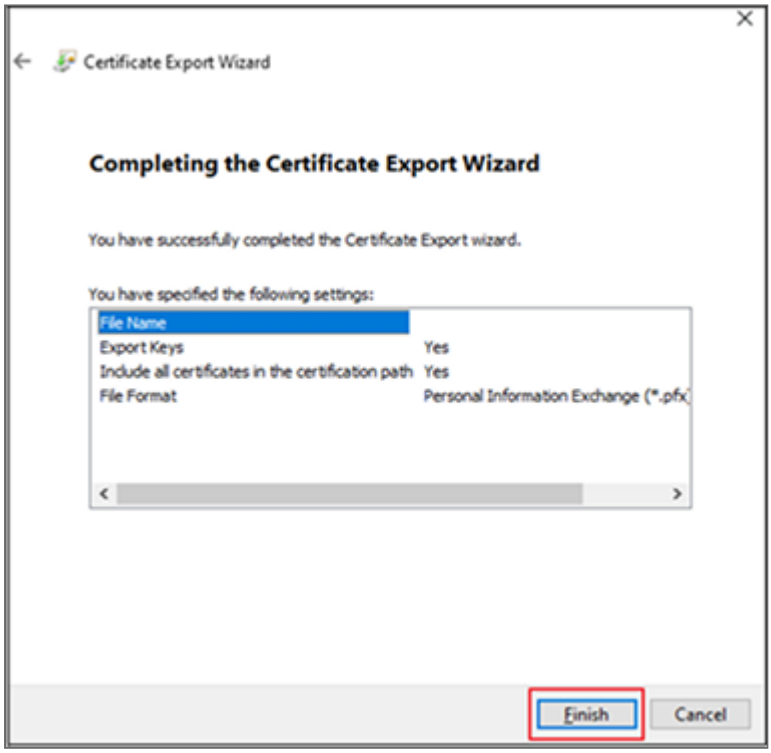


7. Ahora verá la pantalla siguiente. Marque la casilla de contraseña y **establezca** la contraseña siguiente: **G@ll@gher**



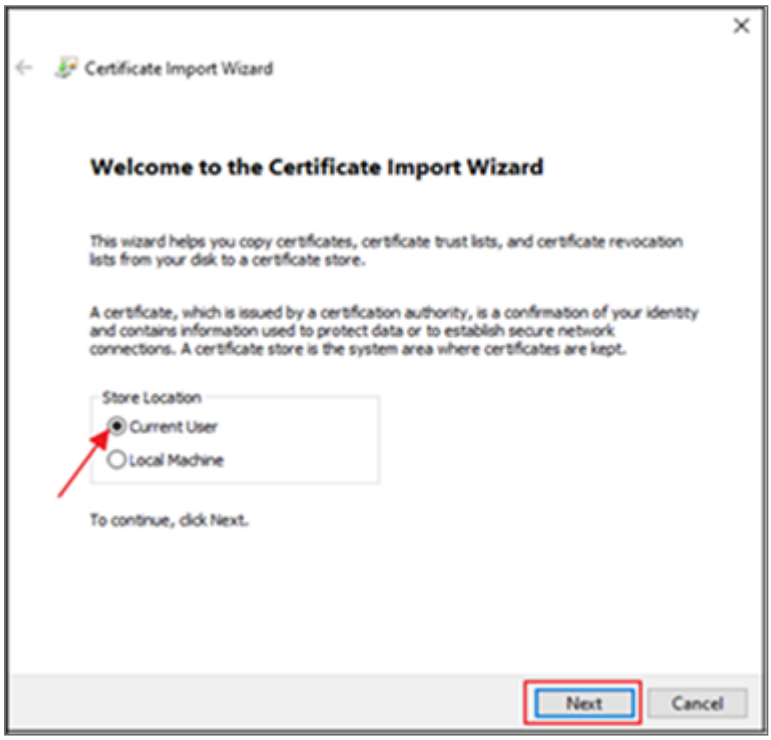
8. Ahora **busque** la ruta C:\Program Files\Suprema Integration with Gallagher\Prerequisites para exportar el archivo y **guarde** este archivo como **GallagherRestClient.pfx**. Luego **haga clic** en **Siguiente**.



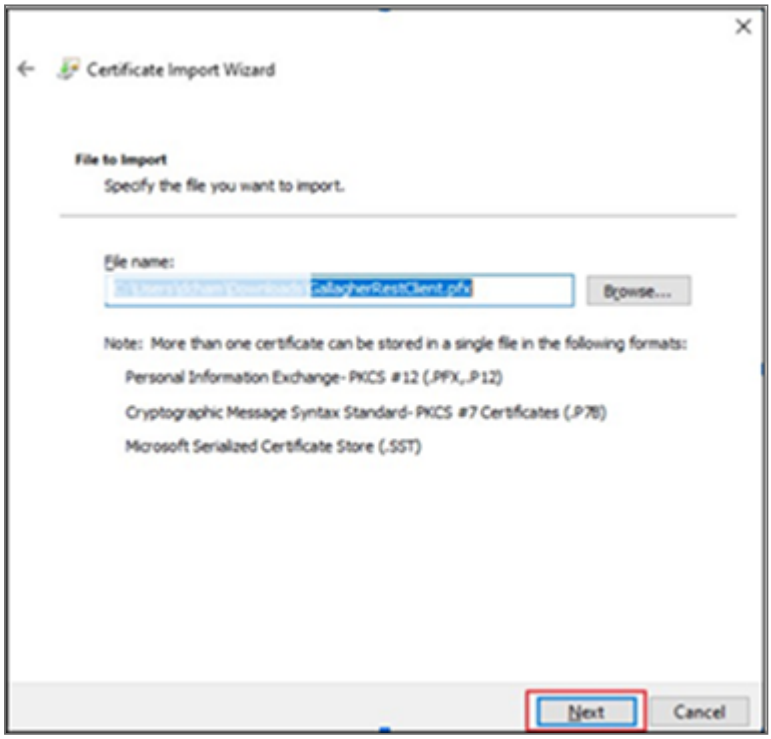


Haga clic en **Finalizar** y su certificado se exportará correctamente. Luego **cierre** el certificado y la ventana de MMC.

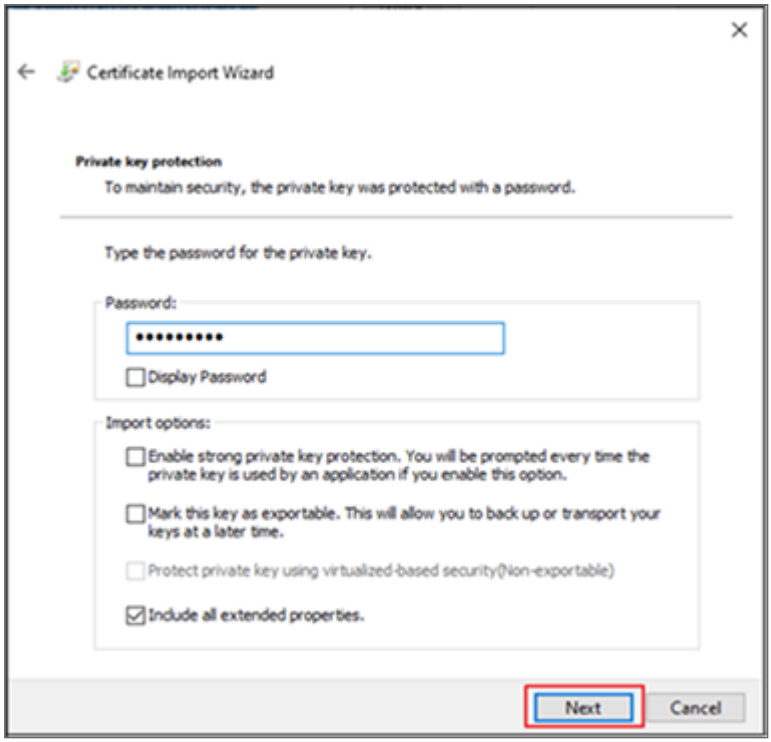
9. Ahora vaya a la ruta `C:\Program Files\Suprema Integration with Gallagher\Prerequisites`, donde exportamos el archivo de certificado **GallagherRestClient.pfx**, y haga **doble clic** en el archivo **GallagherRestClient.pfx**, **seleccione** la opción **Usuario actual** como se muestra en la imagen siguiente y luego **haga clic** en **Siguiente**.



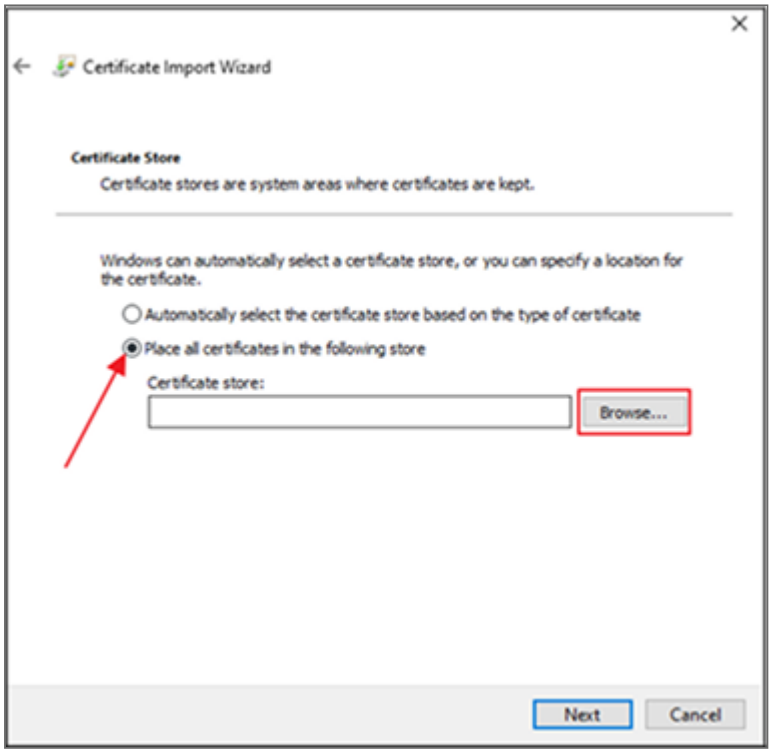
10. Ahora, **busque** `C:\Program Files\Suprema Integration with Gallagher\Prerequisites`, donde guardamos **GallagherRestClient.pfx**, y luego **haga clic** en **Siguiente**.

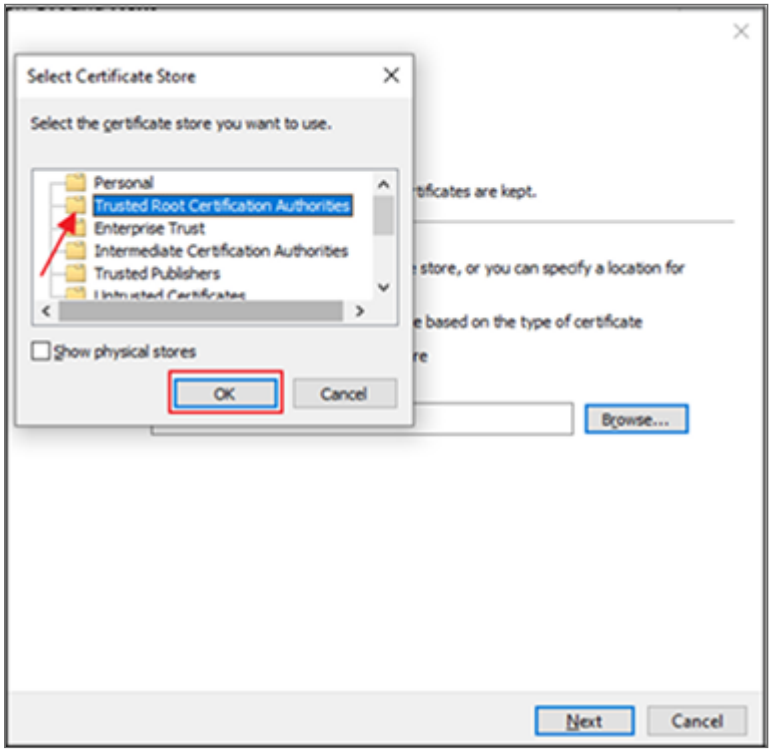


11. Ahora, **ingrese** la contraseña **G@ll@gher** y **marque** la casilla como se muestra en la imagen siguiente. Luego **haga clic** en **Siguiente**.

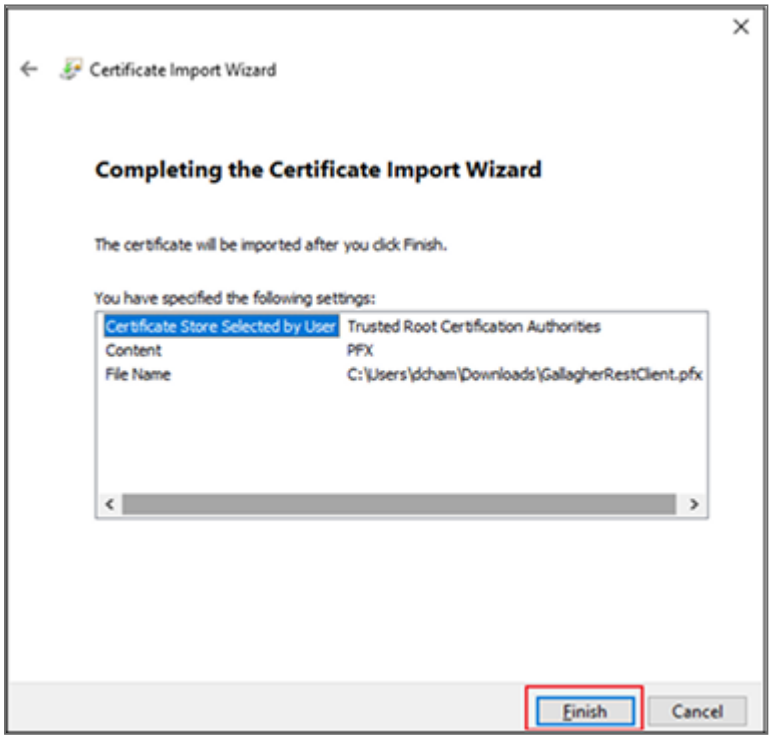


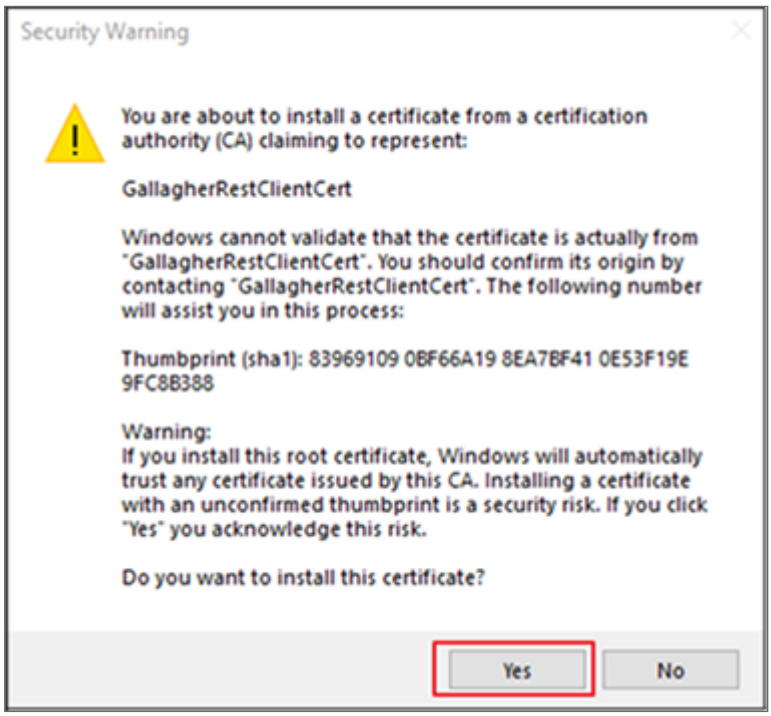
12. **Seleccione** la opción Colocar todos los certificados en el siguiente almacén y **busque** la carpeta **Trusted Root Certification Authorities**. Luego **haga clic** en **OK** y **Siguiente**.





13. **Haga clic** en **Finalizar**. Verá una advertencia de seguridad, **haga clic** en **Sí**.



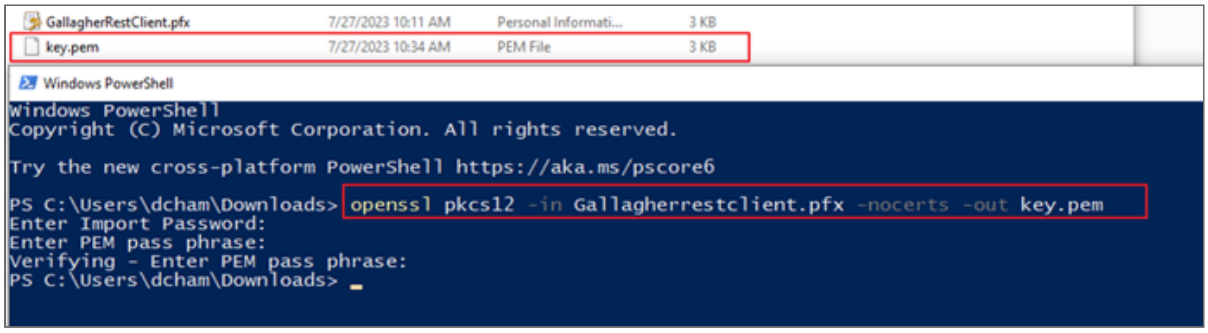


Ahora, **vaya** a la ruta `C:\Program Files\Suprema Integration with Gallagher\Prerequisites`, donde guardamos el archivo GallagherRestClient.pfx, **abra** Powershell aquí y **escriba PowerShell** en la URL de la carpeta para abrir PowerShell.

14. **Escriba** el siguiente comando para generar el archivo **key.pem**.

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

15. Después, pedirá la contraseña. Entonces **ingrese** la contraseña que configuró antes, es decir, **G@ll@gher**.

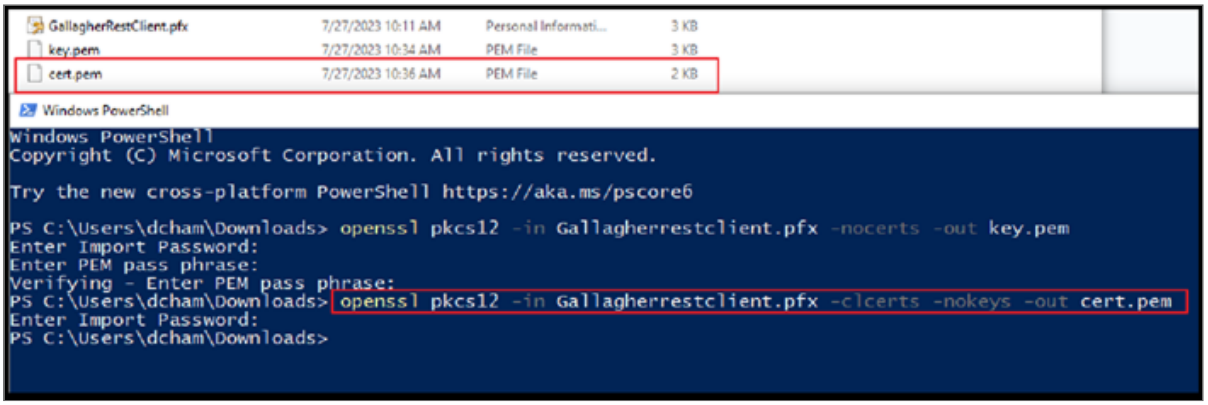


Su archivo **key.pem** se generará correctamente.

> **Información**
> Debe ingresar la contraseña tres veces aquí.

1. Luego, **escriba** el siguiente comando para generar un archivo **cert.pem**:

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

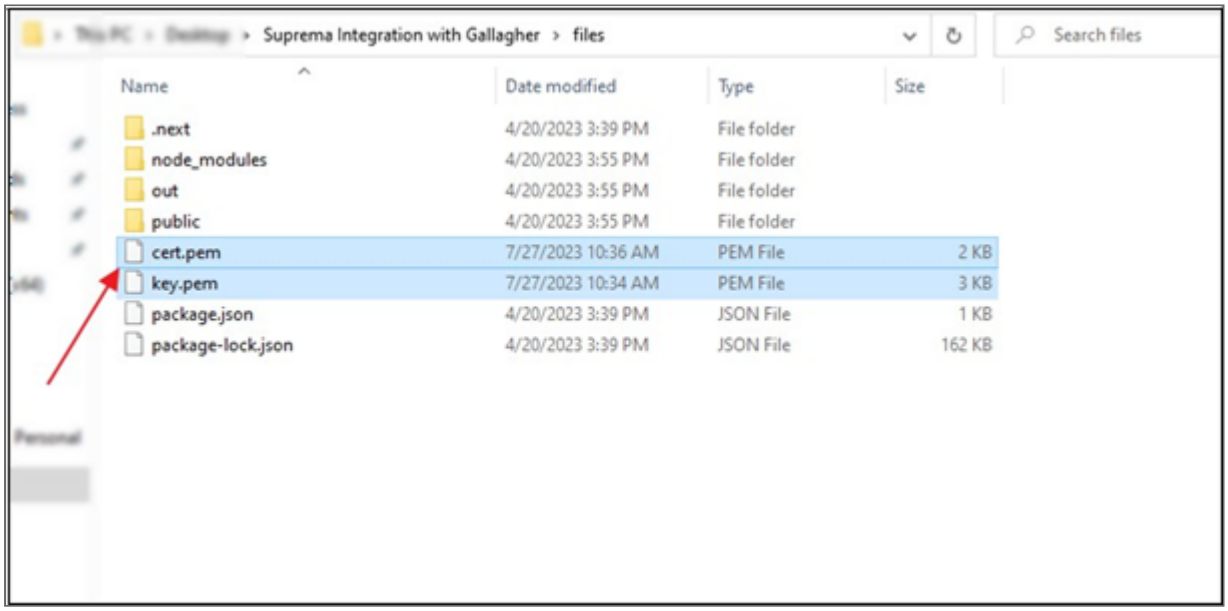
   

   Después, pedirá una contraseña. Entonces **ingrese** la contraseña que configuramos antes **G@ll@gher**.

   Su archivo **cert.pem** se generará correctamente.

   > **Información**
   > Debe ingresar la contraseña una vez aquí.

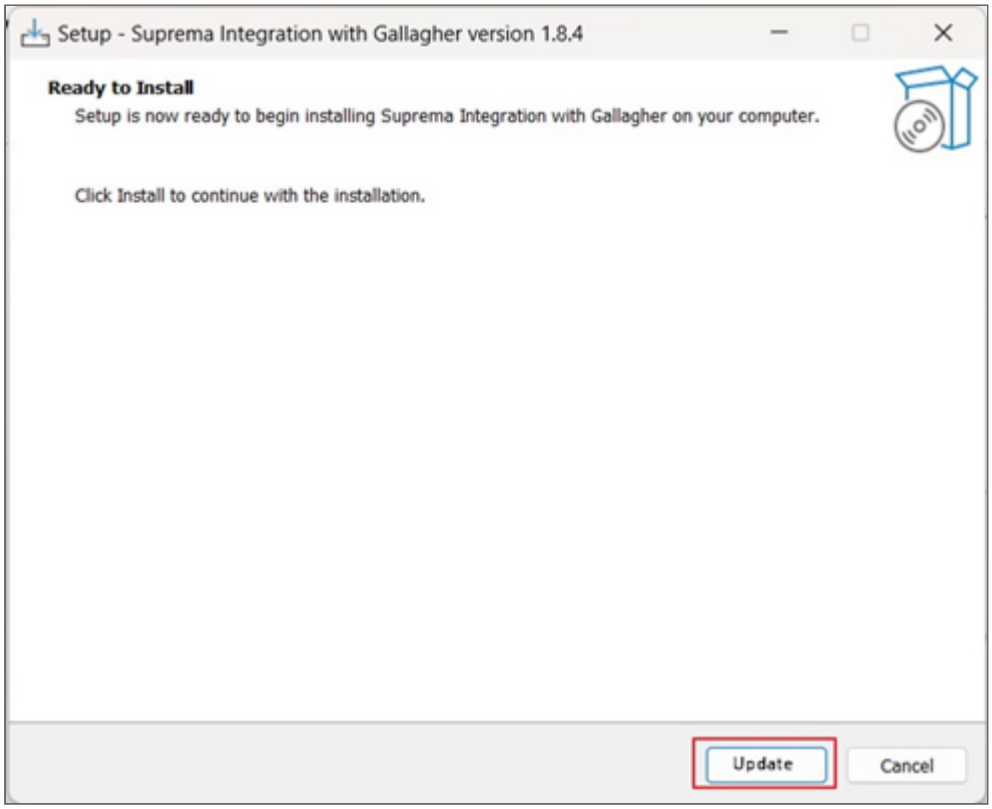
16. Luego **copie** ambos archivos, **key.pem** y **cert.pem**, y péguelos en la ruta siguiente `C:\Program Files\Suprema Integration with Gallagher\Suprema Integration with Gallagher v(lateast version)\files`.



Q. Actualización del middleware directamente desde la aplicación EXE.

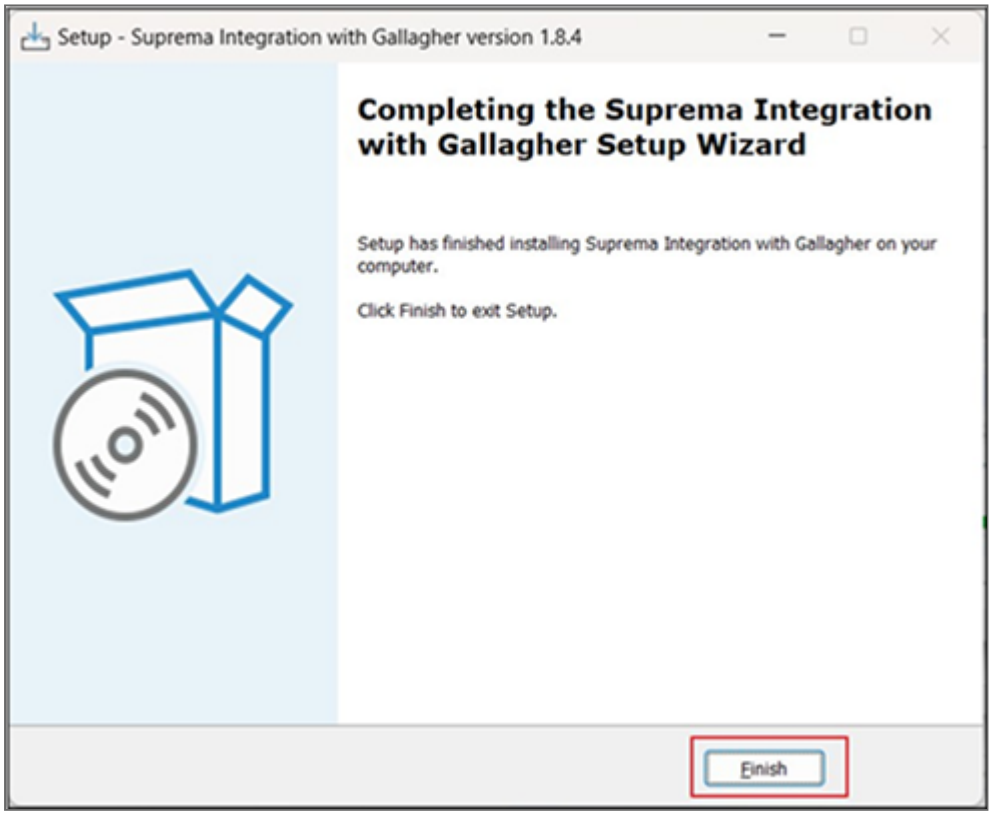
A.

1. Si está actualizando la versión, **presione** OK en la ventana emergente.
2. Luego **presione** el botón Actualizar.



3. Comenzará la actualización del middleware.
4. Después de instalar correctamente el middleware, debe **presionar** el botón Finalizar.

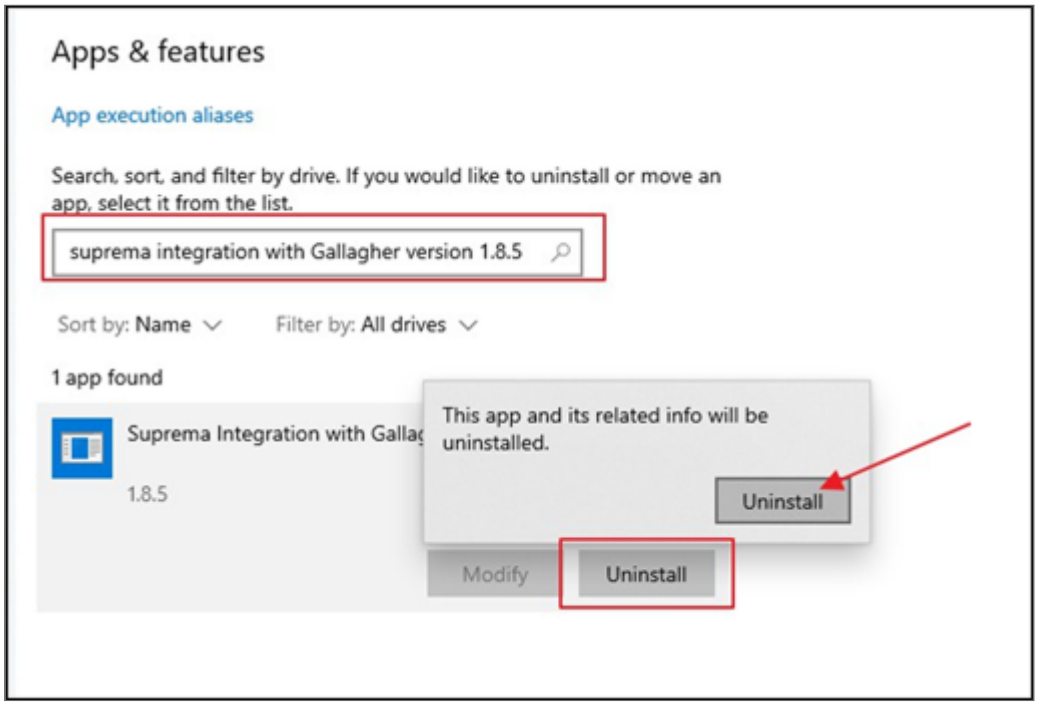
> **Información**
> Para aplicar los cambios más recientes, es necesario reiniciar el sistema.



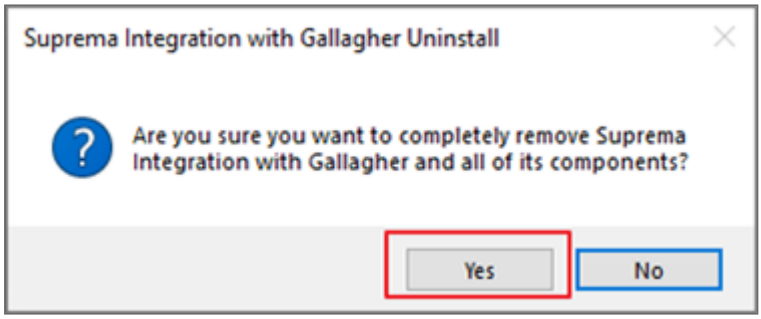
Q. Desinstalación del middleware directamente desde la aplicación EXE.

A.

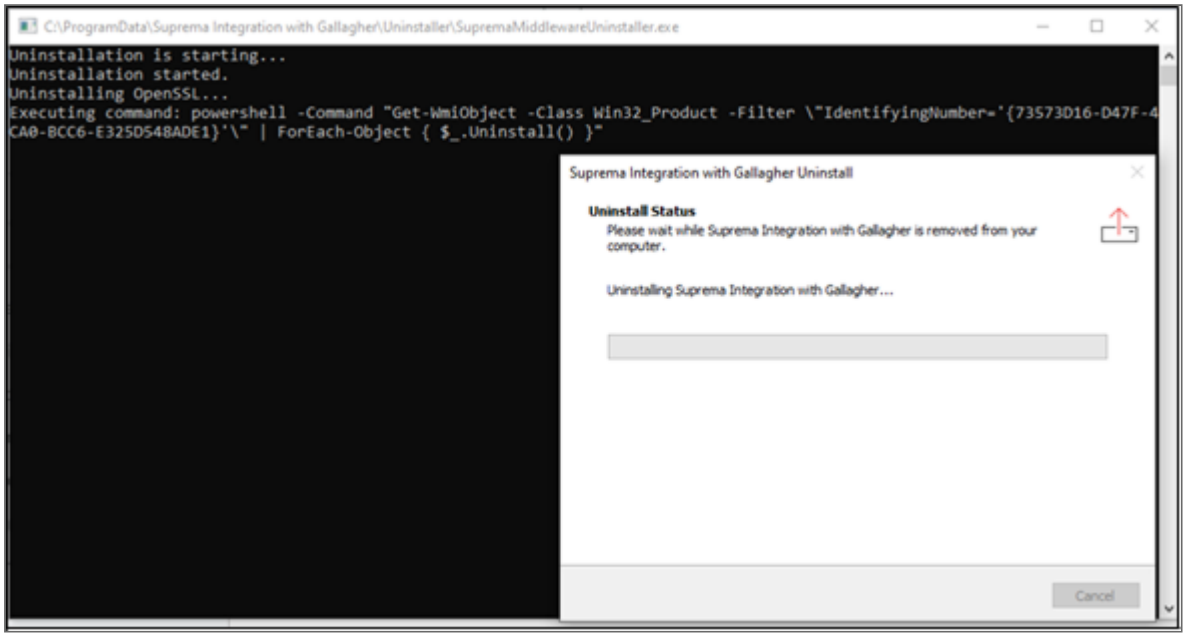
1. **Presione** el botón de Inicio de Windows Inicio , **busque** y **abra** Agregar o quitar programas.
2. En la lista de búsqueda de Aplicaciones y características, **busque** la integración de Suprema con la versión de Gallagher, seleccione la versión y **haga clic en** Desinstalar. Aparecerá una pequeña ventana emergente; **presione** Desinstalar otra vez.



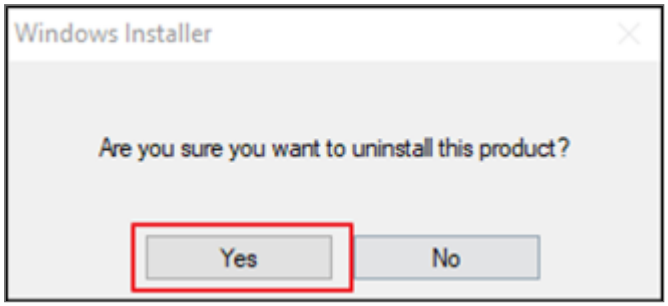
3. **Presione** Sí en la ventana emergente para quitar todos los componentes de la integración.



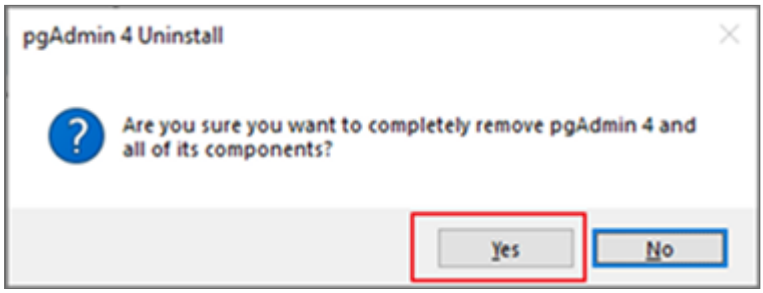
4. Comenzará la desinstalación y verá algo como las pantallas siguientes.



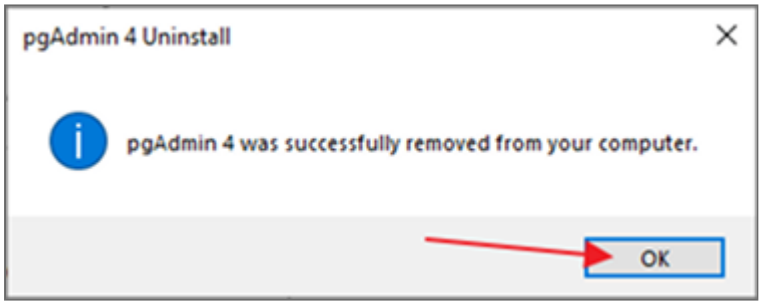
5. **Presione** Sí en la ventana emergente siguiente.



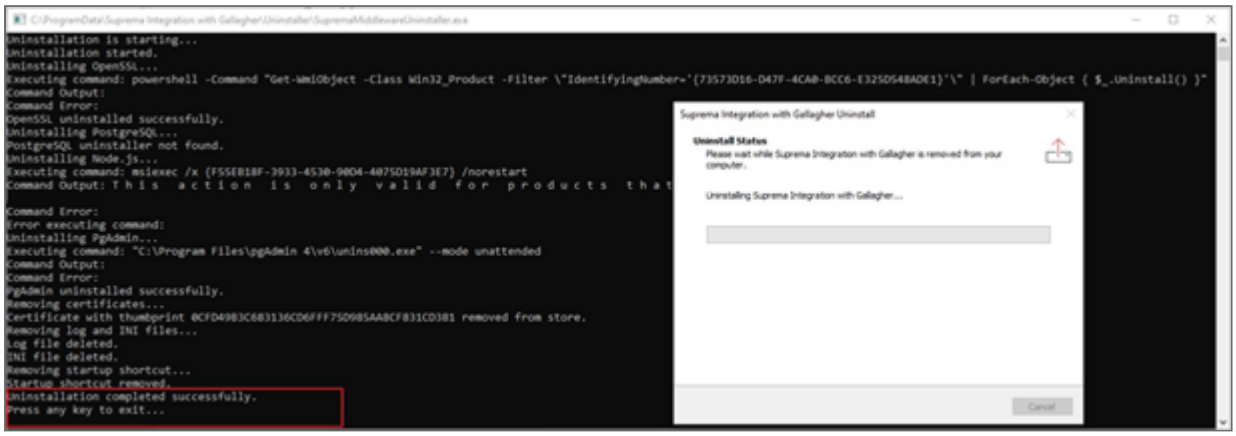
6. **Presione** Sí en la ventana emergente siguiente.



7. **Presione** OK.

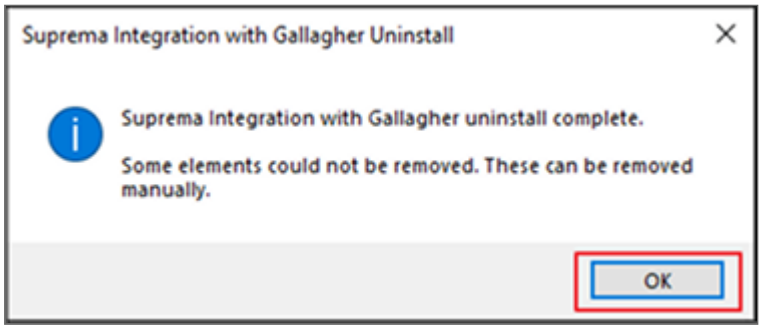


8. Ahora haga clic dentro de la terminal y **presione** Enter para completar el proceso de desinstalación.



9. **Presione** OK en la ventana emergente siguiente y el middleware se habrá eliminado correctamente.

> **Información**
> Debe reiniciar el sistema para que los cambios surtan efecto.

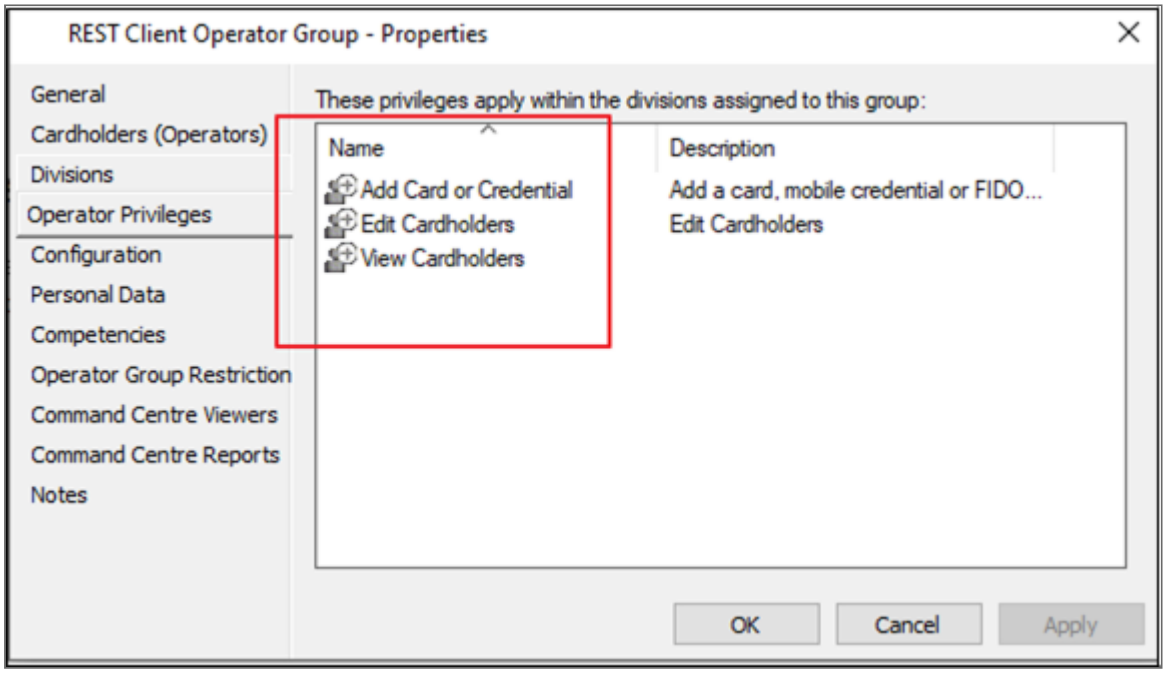


Middleware

Q. Si el escaneo o la sincronización de datos en el middleware es extremadamente lenta.

A.

- Para resolver este problema, haga clic aquí y consulte el blog.
  - No verá ninguna tarjeta en el middleware si no se crea automáticamente la tarjeta del titular.
- Debe agregar 3 privilegios al grupo de operador.



Después de agregar estos tres privilegios, reinicie el sistema.

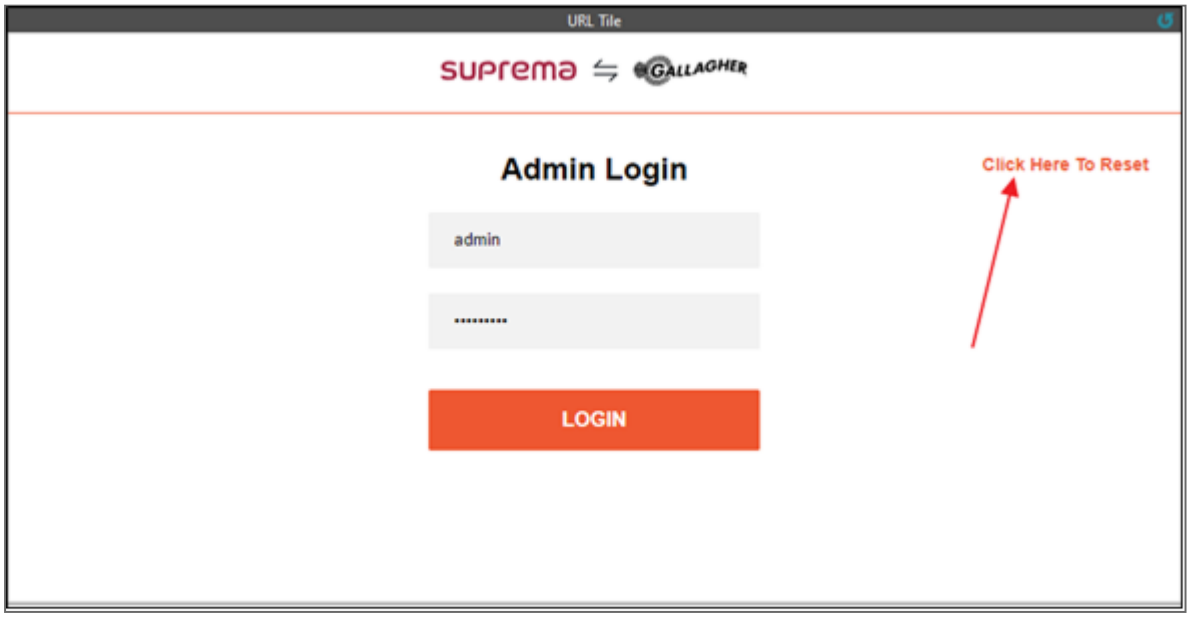
Q. Hay un error en la página de inicio de sesión que indica "LAN está desconectada o la IP ha cambiado para (IP Address)".

A.

- Para resolver este problema, revise los siguientes escenarios de solución de problemas:

  1. Asegúrese de que el cable LAN esté conectado.
  2. Verifique que la IP no haya cambiado y que la dirección IP sea la misma para el servidor BioStar 2. Si ingresó una dirección IP incorrecta.

- Si recibe el error **LAN está desconectada o la IP ha cambiado para (IP Address)** en la pantalla de inicio de sesión, debe **presionar** el **botón click here to Reset** en el middleware.



Pide permiso para restablecer el middleware; **presione** el botón Sí.



Una vez restablecido, verá la pantalla inicial del middleware y podrá seguir los pasos posteriores.

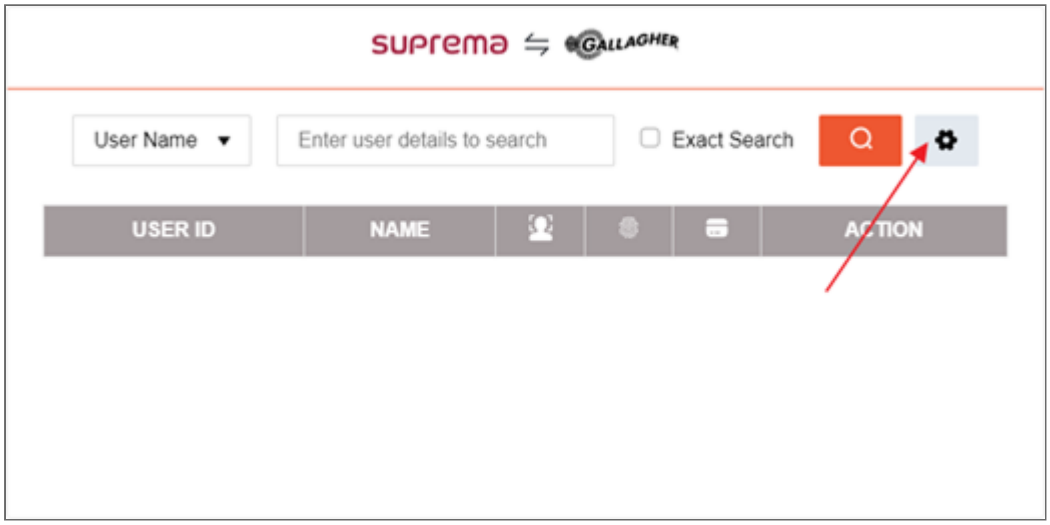
Q. Si obtiene el error "LAN está desconectada o la IP ha cambiado para (IP Address)" mientras ejecuta el middleware en cualquier página.

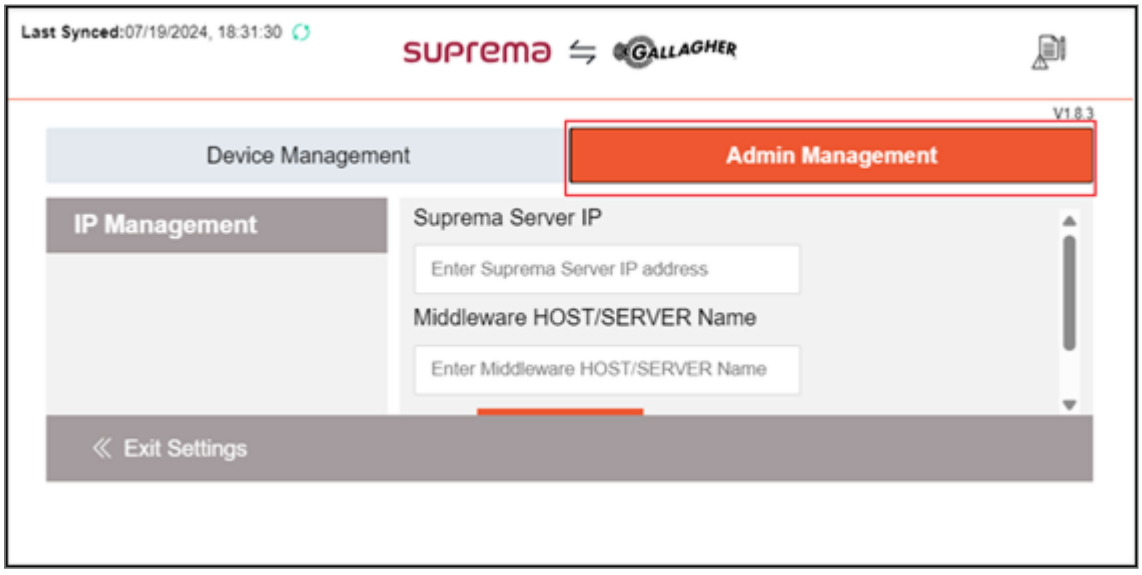
A.

- Para resolver este problema, revise los siguientes escenarios de solución de problemas:

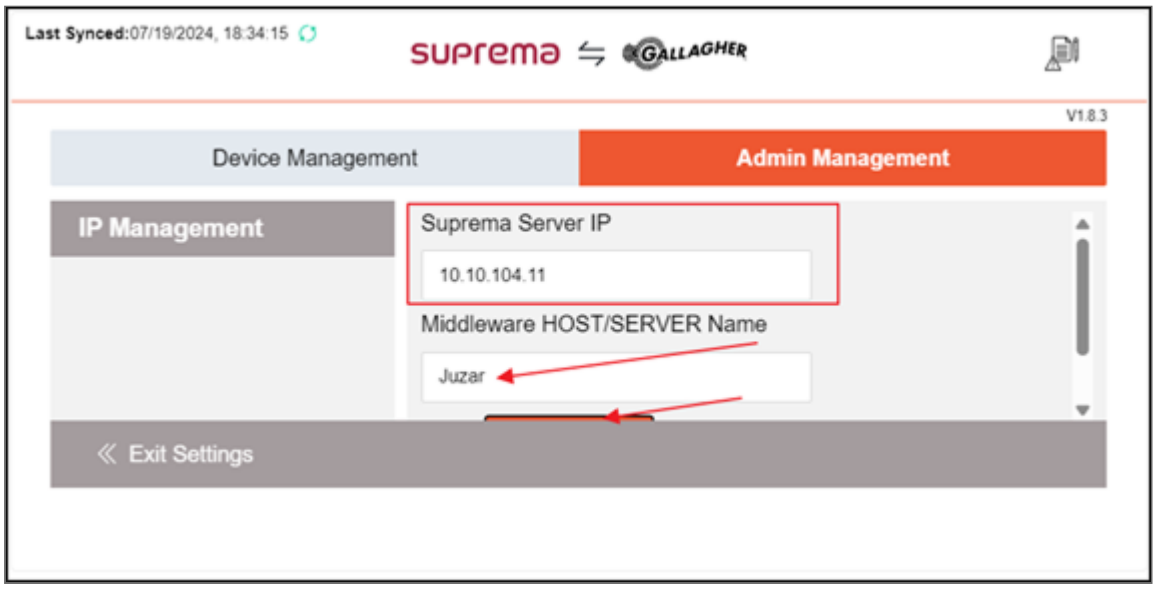
  1. Asegúrese de que el cable LAN esté conectado.
  2. Verifique que la IP no haya cambiado y que la dirección IP haya cambiado para el servidor BioStar 2.

- En este caso, vaya a la sección Settings → Admin Management → IP management dentro del middleware.





Ahora, dentro del cuadro de texto, ingrese la dirección IP del servidor BioStar 2 y el nombre HOST/SERVER del middleware. Presione el botón Submit para iniciar los servicios de BioStar 2 para el middleware.



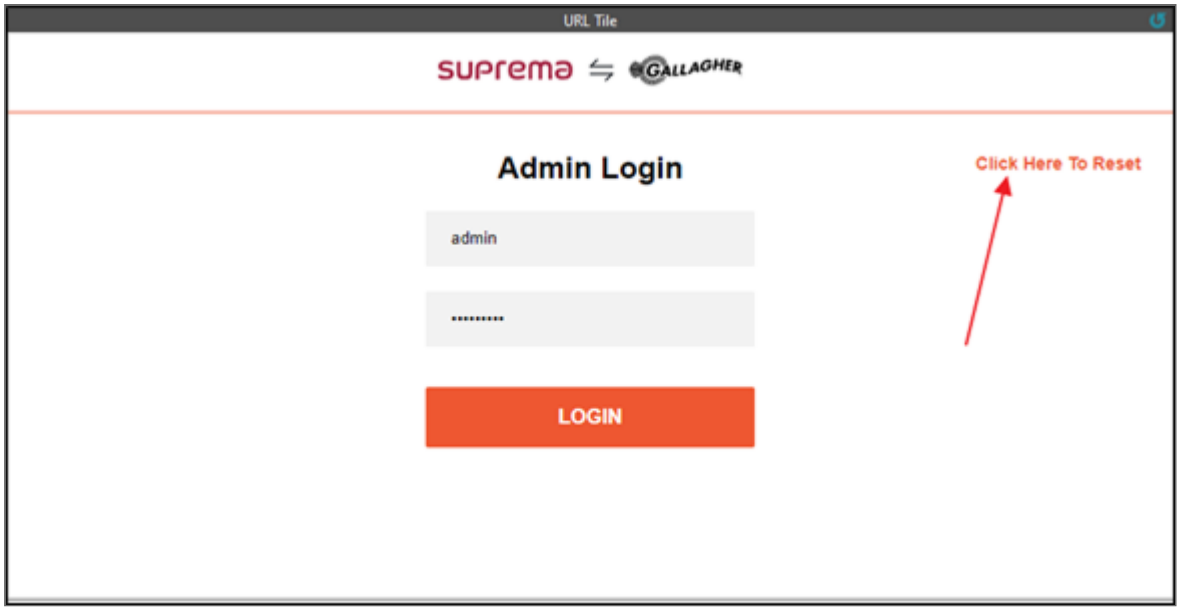
Después de **presionar** el **botón** Submit, obtendrá el mensaje de éxito por el cambio de IP y **presione** el **botón** Exit setting para salir de la pantalla de configuración.

Q. Cómo usar el middleware en varios servidores en versiones anteriores.

A. Desde la versión 1.7.0 agregamos una pantalla separada para obtener la dirección IP del servidor BioStar 2. Esta es la solución para usar el middleware en versiones anteriores a la 1.7.0.

A continuación, se muestran los pasos para cambiar la dirección IP,

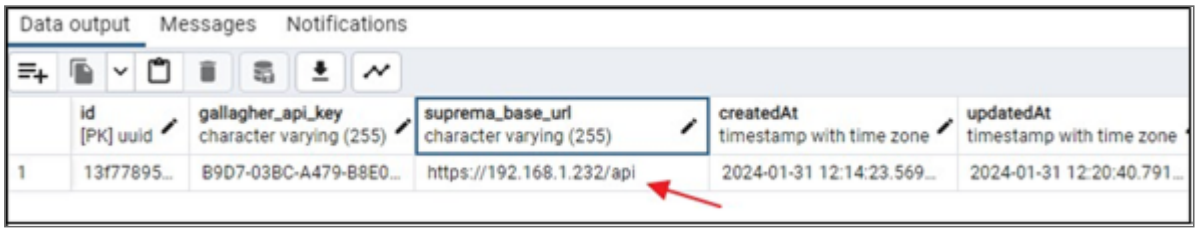
1. Vaya a Pgadmin → tables y haga clic derecho en la tabla y Tuncate → Truncate Restart Identity (para las tres tablas).
2. Ingrese al centro de comando de Gallagher si no ve la ventana de la clave API y solo puede ver la pantalla de inicio de sesión. **Haga clic en** el enlace reset middleware y restablezca el middleware.



3. Después de ingresar la clave API para el middleware, inicie sesión y abra Pgadmin, haga clic derecho en la tabla de

credenciales y vaya a ver/editar datos → Todas las filas.

4. Se cargará la información de la tabla. Ahora cambie la dirección IP según la IP de su servidor BioStar y presione el botón F6 para guardar los cambios.



5. Después de esto, debe truncar la tabla globaluserrecord dentro de Pgadmin.
6. Reinicie el sistema para que los cambios surtan efecto.

Q. Ejecute el middleware en un puerto específico en dos servidores diferentes con direcciones IP específicas / Configure las reglas de entrada para el middleware.

A. A continuación, se indican las instrucciones para ejecutar el middleware en un puerto específico en dos servidores diferentes con direcciones IP específicas.

Encontramos que nuestro middleware usa el puerto 28523 para llamar al backend de la aplicación (middleware-backend). Dentro del backend llamamos las API del servidor BioStar 2, así que para eso el único puerto usado es 443, ya que es el puerto HTTPS predeterminado del servidor web.

Para esto, dentro de server2, que es el servidor BioStar 2, configuramos el tipo de protocolo como TCP y proporcionamos los puertos 443 y 8081 para el puerto local. Deje la opción de puerto remoto como Todos los puertos.

Server 1 tiene Gallagher y Middleware dentro,

- Dirección IP: 192.168.1.68
- Máscara de subred: 255.255.255.0
- Puerta de enlace predeterminada: 162.168.1.1

Server 2 tiene BioStar 2 dentro,

- Dirección IP: 10.10.104.13
- Máscara de subred: 255.255.254.0
- Puerta de enlace predeterminada: 10.10.104.1

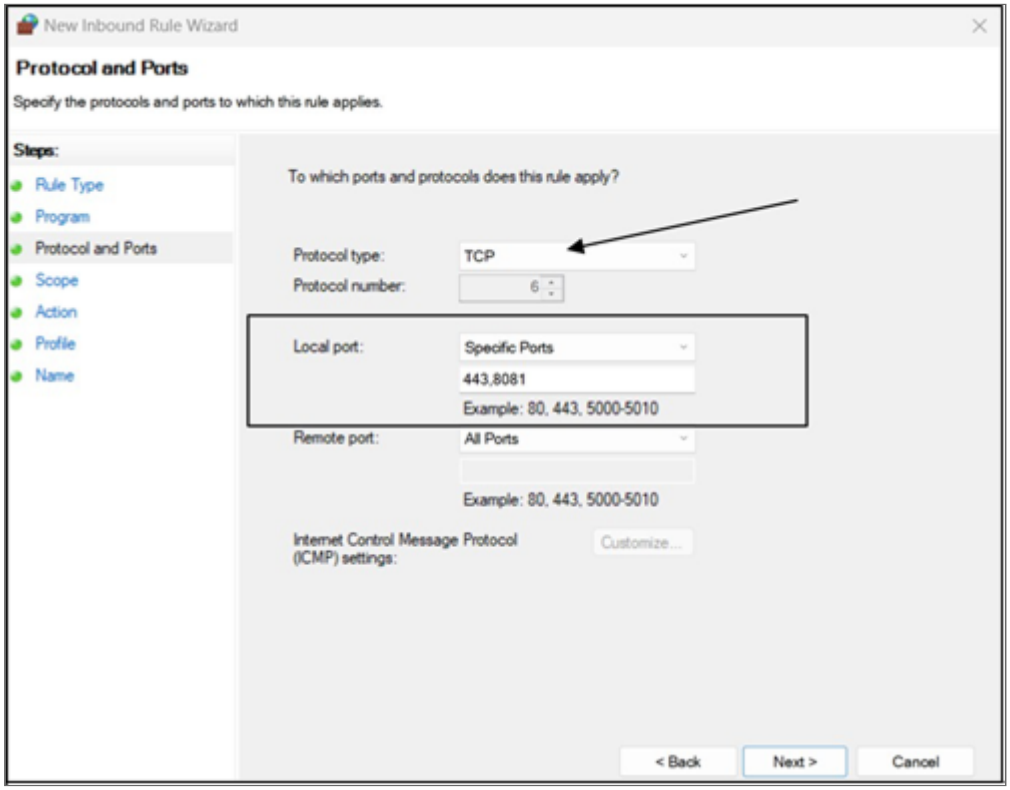
Estos son los pasos para crear reglas de entrada:

> **Información**
> Los pasos siguientes deben ejecutarse en el servidor BioStar 2.

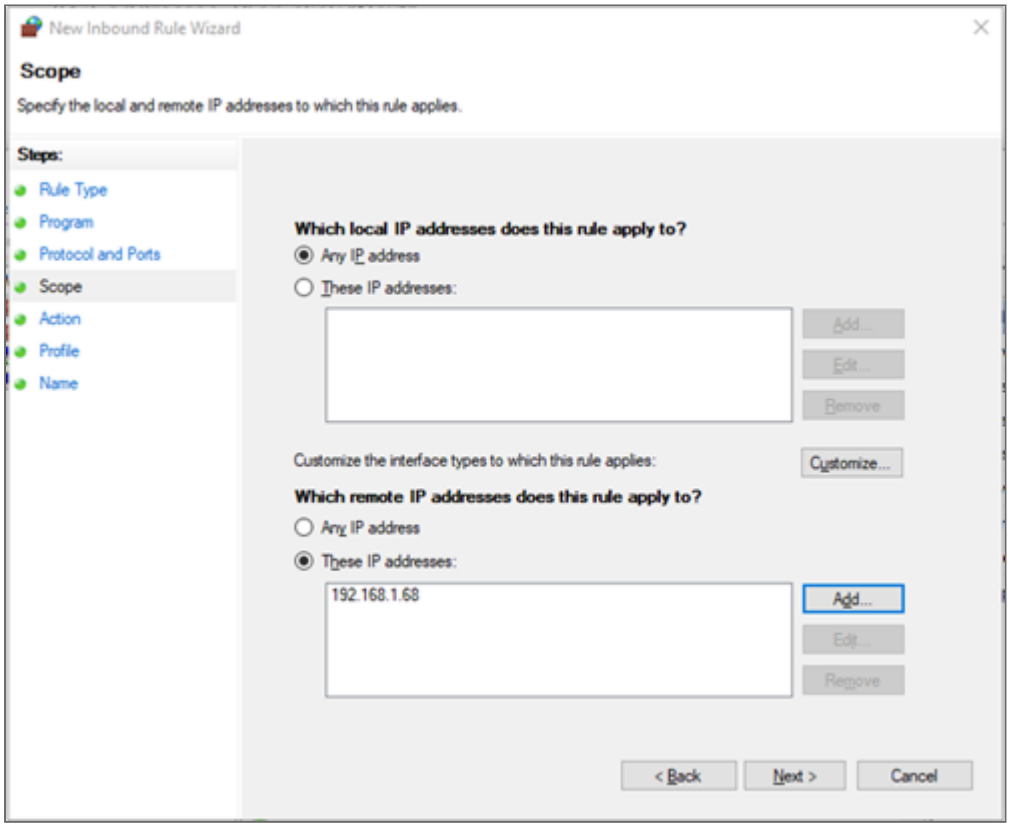
1. Abra la configuración del Firewall de Windows Defender:
   - Presione `Win + R` para abrir el cuadro de diálogo Ejecutar.
   - Escriba `control firewall.cpl` y presione Enter. Esto abrirá la configuración del Firewall de Windows Defender.
2. Acceder a la configuración avanzada:
   - En la ventana del Firewall de Windows Defender, verá opciones en el lado izquierdo. Haga clic en **Configuración avanzada**. Esto abre la consola de Firewall de Windows Defender con seguridad avanzada.

3. Crear nueva regla de entrada:
   - En la consola del Firewall de Windows Defender con seguridad avanzada, verá opciones en el lado izquierdo, incluidas **Reglas de entrada** y **Reglas de salida**.
   - Haga clic en **Reglas de entrada**.
   - En el panel derecho, haga clic en **Nueva regla...**. Esto abre el Asistente para nueva regla de entrada.
4. Seleccionar tipo de regla:
   - En el Asistente para nueva regla de entrada, seleccione **Personalizada** y haga clic en **Siguiente**.
5. Configurar programa:
   - Si desea aplicar esta regla a un programa específico, especifíquelo aquí. Como estamos trabajando con tráfico ICMP, deje esto como **Todos los programas** y haga clic en **Siguiente**.
6. Configurar protocolo y puertos:
   - En la ventana Protocolo y puertos, seleccione **TCP**, ya que trabajaremos con puertos específicos. Ahora, dentro del puerto local, debemos seleccionar Puertos específicos e ingresar los puertos 443 y 8081. Deje el puerto remoto como Todos los puertos. Luego haga clic en **Siguiente**.

> **Información**
> Aquí asignamos el puerto 8081 a BioStar 2, que lo usa para dispositivos USB.



7. Configurar ámbito:
   - En la ventana Ámbito, puede especificar qué direcciones IP tienen permitido enviar tráfico ICMP al servidor. Para las direcciones IP locales, déjelo como está y, para las direcciones IP remotas, complete la dirección IP del servidor Gallagher y Middleware. Ahora elija Estas direcciones IP: Haga clic en el botón Agregar y luego, en el asistente de dirección IP, ingrese la dirección IP del servidor Gallagher y Middleware, y presione OK. Consulte la imagen siguiente como referencia.



8. Configurar acción:
   - En la ventana Acción, seleccione **Permitir la conexión** y haga clic en **Siguiente**.
9. Configurar perfil:
   - En la ventana Perfil, seleccione los perfiles a los que se aplicará esta regla. Por lo general, conviene habilitarla para todos los perfiles (Dominio, Privado, Público). Luego haga clic en **Siguiente**.
10. Nombre y descripción:
    - Asigne un nombre y una descripción a la regla. Por ejemplo, puede nombrarla **Permitir solicitud de eco ICMP para middleware**. Luego haga clic en **Finalizar**.
11. Habilitar la regla:
    - Después de crear la regla, debería verla en la sección Reglas de entrada de la consola Firewall de Windows Defender con seguridad avanzada.
    - Haga clic derecho en la regla que acaba de crear y seleccione **Habilitar regla** si no se habilitó automáticamente. Esto garantiza que la regla esté activa y permita tráfico ICMP.

Q. Si la IP del servidor BioStar cambia y el middleware se vuelve lento.

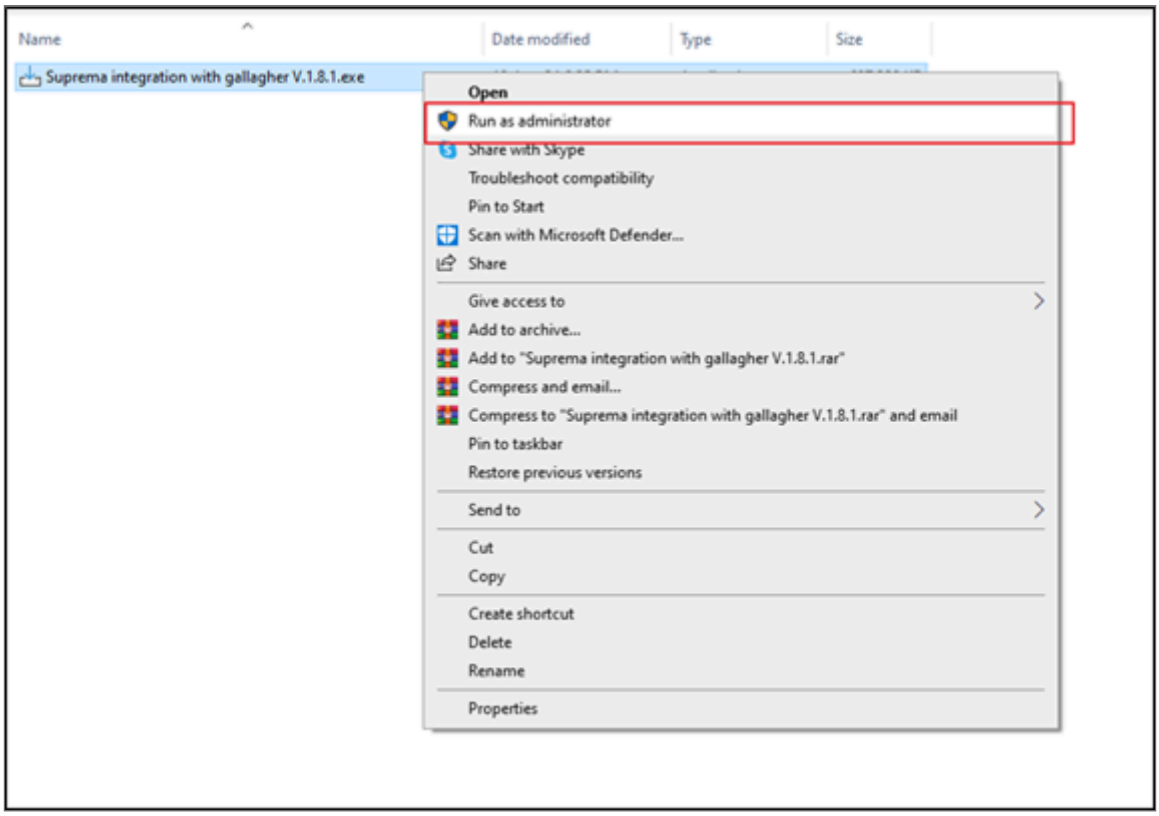
A. Si tiene el error en el que su IP cambió, consulte el siguiente enlace: https://support.supremainc.com/en/support/solutions/articles/24000041659--biostar-2-troubleshooting-when-the-server-ip-changed.

Q. Si no se genera un thumbprint al ejecutar el archivo EXE.

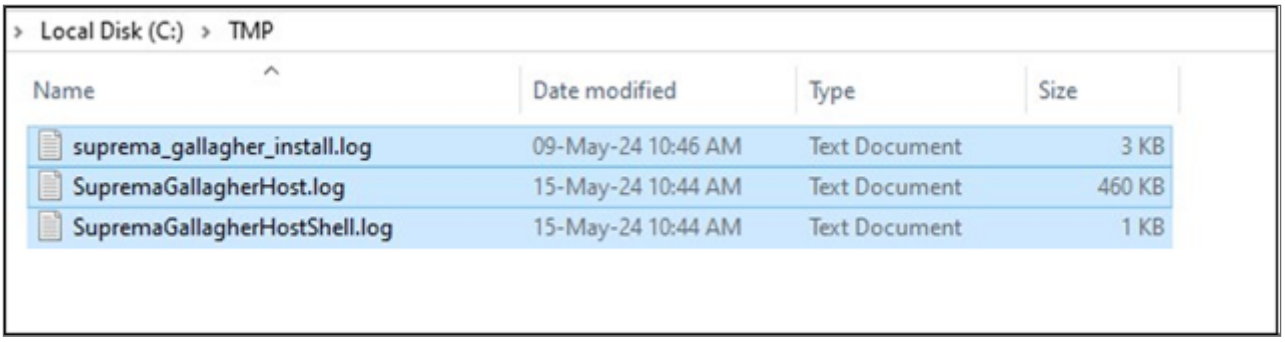
A. Si instaló el middleware y no se genera un thumbprint, vuelva a ejecutar nuestro archivo EXE con permisos de administrador. Siga las instrucciones siguientes.

Haga clic derecho en el archivo Suprema integration with the gallagher.exe y **seleccione** la opción Ejecutar como administrador, como se muestra en la captura siguiente. Ahora solicita permiso; **haga clic** en Sí para ejecutar nuestro

archivo EXE.



Si aún no se genera el archivo thumbprint, vaya a `C:\TMP` y comparta todos los archivos de registro con el equipo de desarrollo.



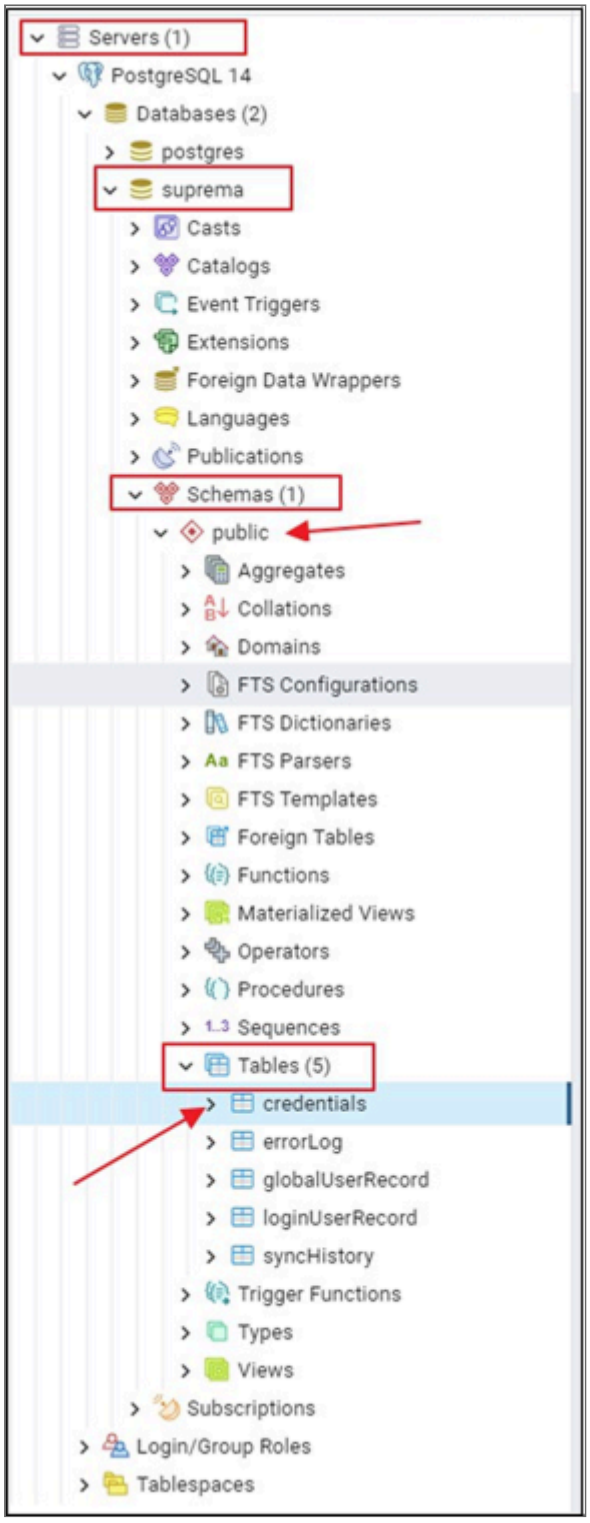
Mientras tanto, consulte el artículo que ayuda a generar manualmente el thumbprint. Consulte: Cómo generar el thumbprint manualmente.

Q. Crear migración manualmente.

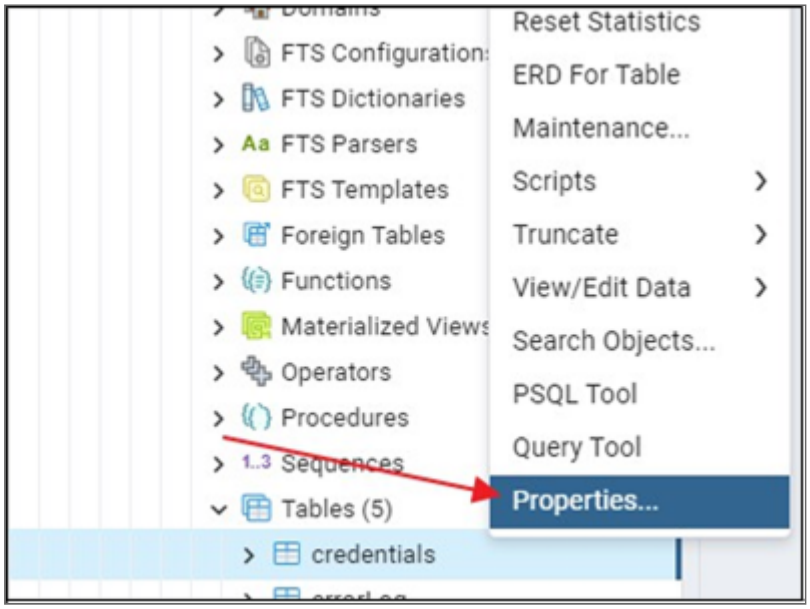
A. Hacemos las migraciones porque, desde el middleware V1.8.3, se admite el nombre de host, así que podemos usar el middleware mediante el cliente de estación de trabajo de Gallagher.

Para crear la migración manualmente, siga los pasos siguientes:

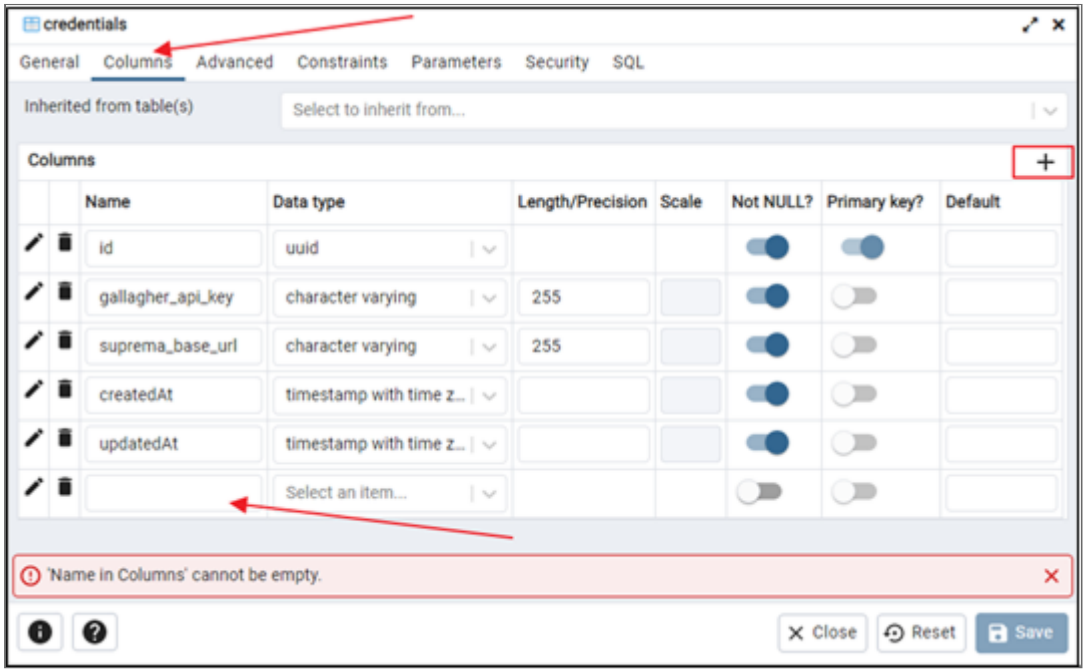
1. Vaya a Pgadmin. Pide la contraseña. Escriba la contraseña **G@ll@gher**, que es la contraseña predeterminada que configuramos durante la instalación.
2. Ahora **haga clic en** Servers. Si pide la contraseña, use la misma **G@ll@gher** como contraseña. Luego **haga clic en** Databases y **expanda** Suprema → Schemas → public → Tables. Ahora **seleccione** la tabla de credenciales.



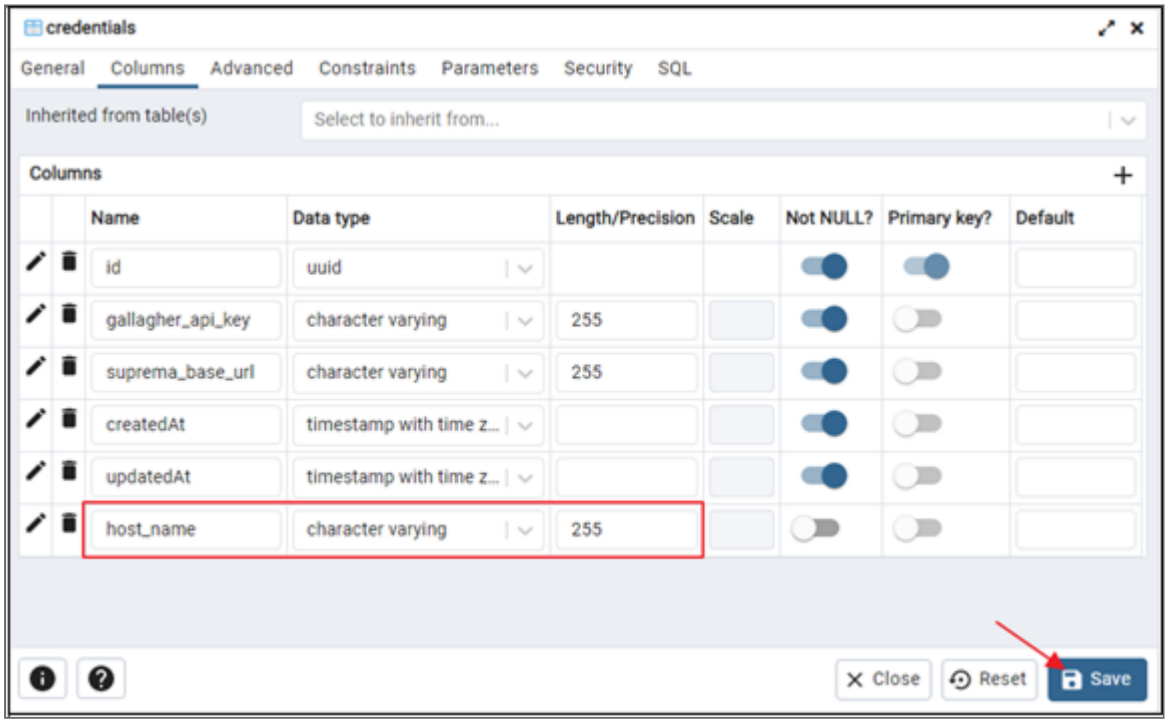
3. Ahora **haga clic derecho en** la tabla de credenciales y **seleccione** la opción Properties de la lista.



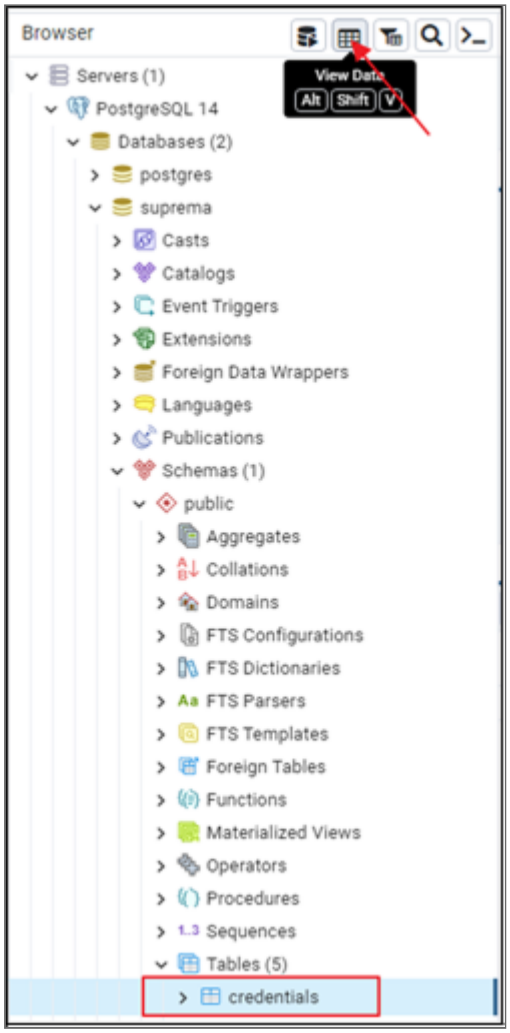
4. Ahora, dentro de la ventana, **seleccione** la opción Columns y luego **haga clic en** el icono +. Se generará la nueva opción de columna, como se muestra en la imagen siguiente.



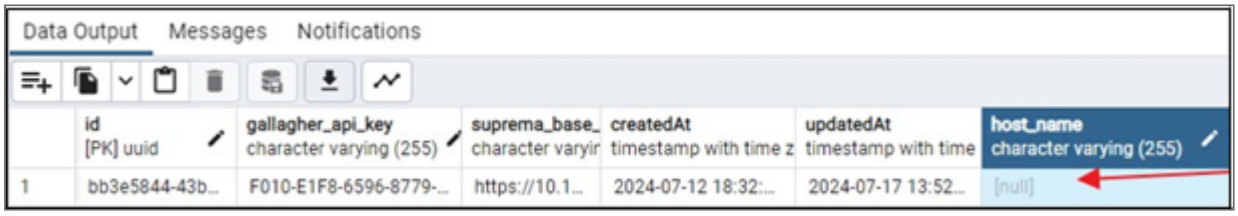
5. Ahora, dentro de la opción Columns, **establezca** el nombre como host_name, y **establezca** el tipo de dato como character varying, **establezca** Length/Precision como 255 y **presione** el botón Save.



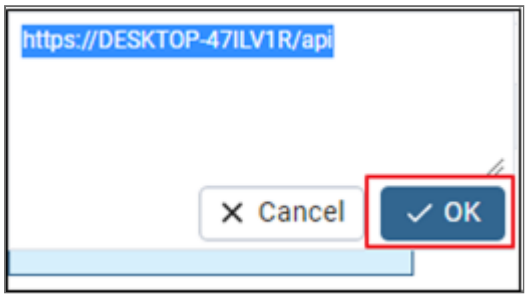
6. Ahora **seleccione** la tabla de credenciales y **haga clic en** el botón View Data.



7. Ahora, dentro de la columna host_name, **haga doble clic** en la celda y se abrirá la ventana emergente.



8. En la ventana emergente, escriba `https://[YOUR-HOST/SYSTEM-NAME]/api` y **presione** OK.



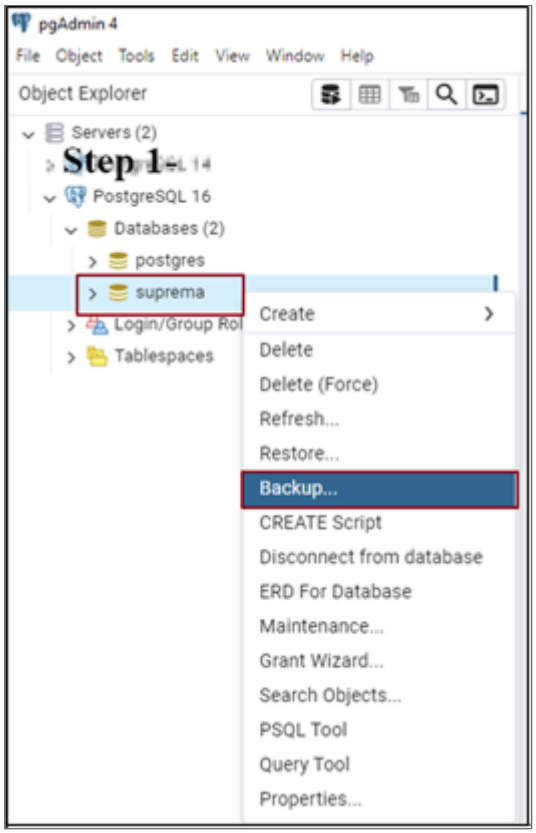
9. Ahora **presione** `F6` para guardar los cambios.

Q. Pasos para respaldar la base de datos PostgreSQL 14, actualizar a la versión 16 y restaurar la base de datos.

A. Respaldo de la base de datos en PostgreSQL 14

1. Abra pgAdmin 4:

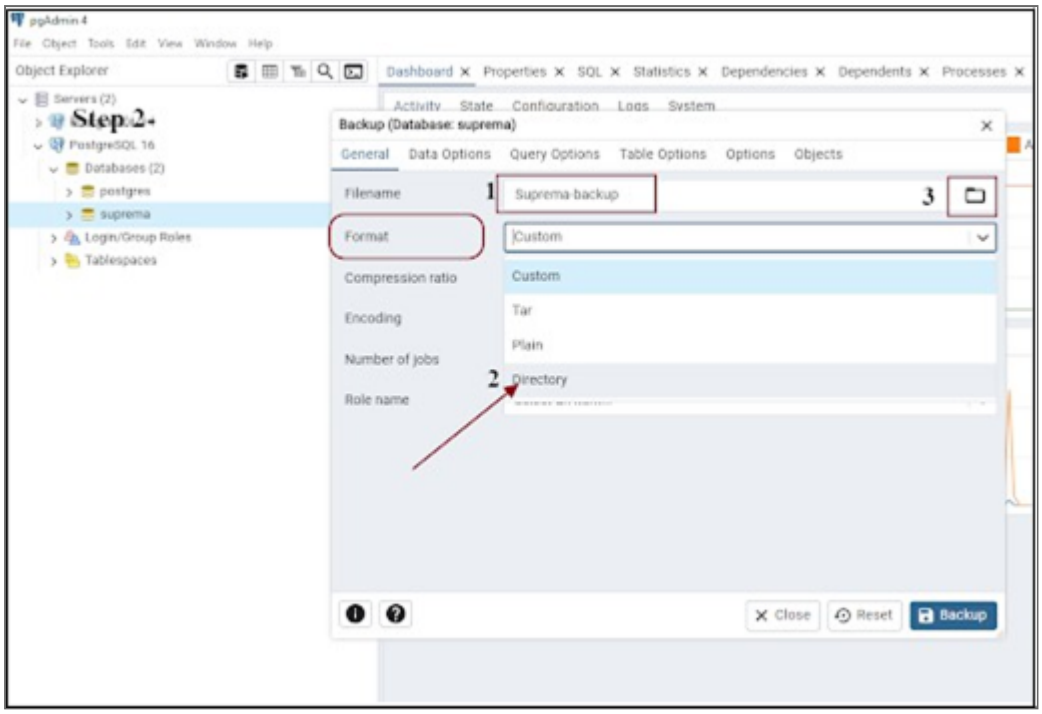
   - Haga clic derecho en la base de datos **Suprema** en la sección **Databases** y seleccione **Backup**.



2. Establecer nombre y formato del archivo de respaldo:

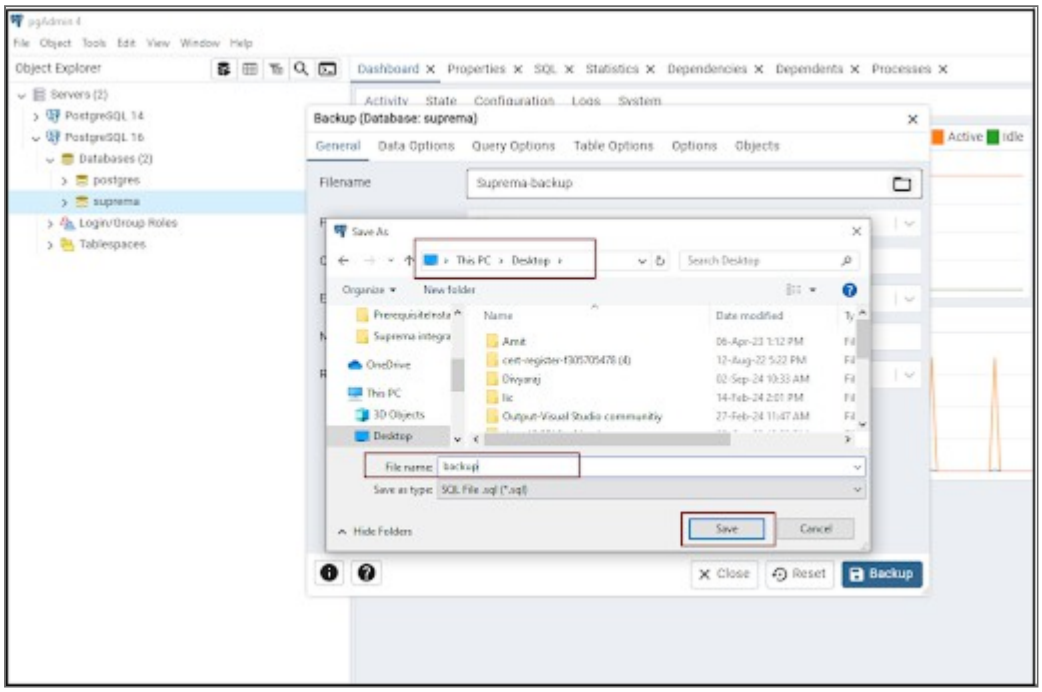
   - En el campo **File name**, escriba **Suprema-backup** como nombre y elija **Directory** como formato.

- **Haga clic** en el icono del archivo para seleccionar una ubicación de guardado.



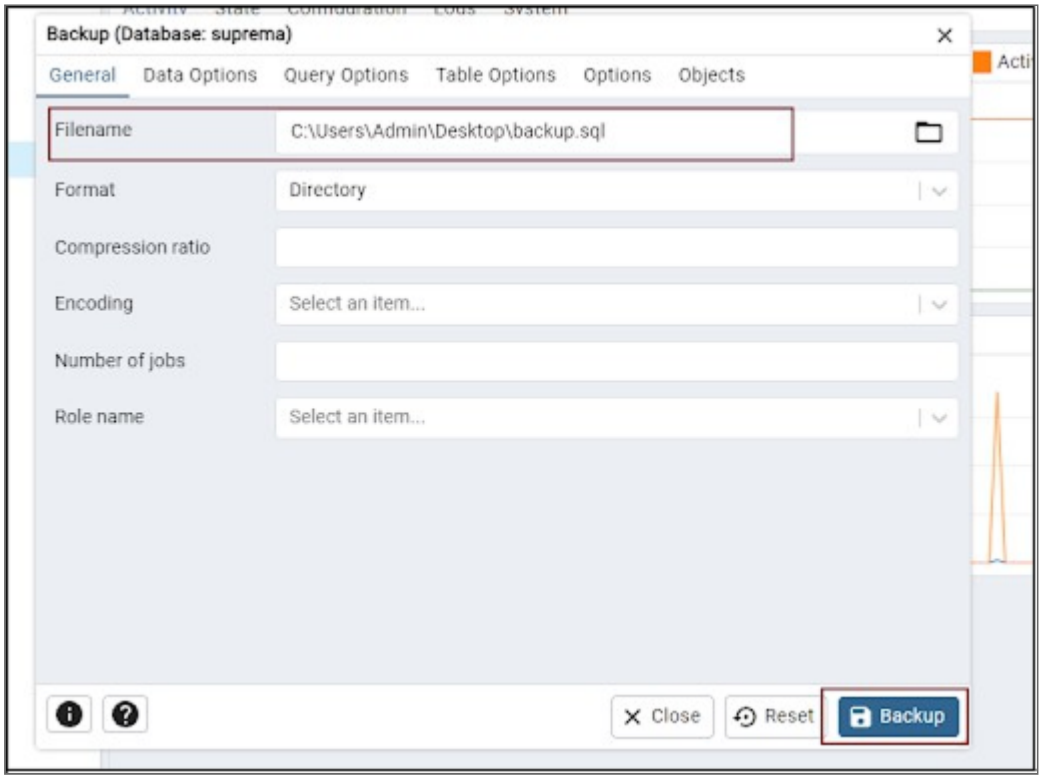
3. Elegir ubicación de guardado:

- Seleccione el directorio donde desea guardar el respaldo (por ejemplo, Escritorio). Ingrese el nombre del archivo y presione **Save**.



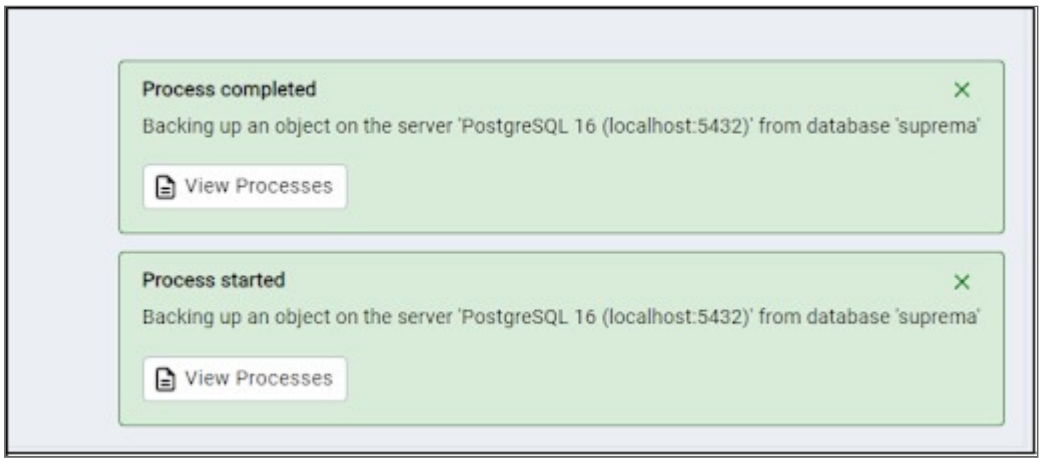
4. Iniciar respaldo:

- Verá que el nombre del archivo se actualiza con la ubicación que seleccionó. Presione el botón **Backup**.



5. Confirmar finalización del respaldo:

   - Aparecerá una notificación cuando termine el respaldo. Ahora su base de datos ya cuenta con un respaldo seguro.



Actualizar PostgreSQL a la versión 16

1. Detener el middleware y los servicios de PostgreSQL:
   - Detenga el middleware en ejecución y finalice los servicios de PostgreSQL deteniendo los procesos en los puertos 28523 y 5432.
2. Actualizar contraseña (si es necesario):
   - Establezca la contraseña en **G@ll@gher** para garantizar la compatibilidad durante la actualización.
3. Instalar PostgreSQL 16:
   - Descargue e instale PostgreSQL 16 desde el sitio web oficial de PostgreSQL, siguiendo los pasos de instalación para su sistema operativo, o consulte el enlace para obtener directamente la versión V16.4.1: https://drive.google.com/file/d/17ehlTpedaGeWezOHZiMd6-ircQhTqBAJ/view?usp=drive_link.
4. Migrar datos (opcional):
   - Consulte la restauración de Database in Postgresql 16.
5. Desinstalar PostgreSQL 14 (opcional):

- Después de confirmar la actualización, puede desinstalar PostgreSQL 14 si ya no lo necesita. Consulte: Desinstale postgresql14 después de actualizar a la versión 16.

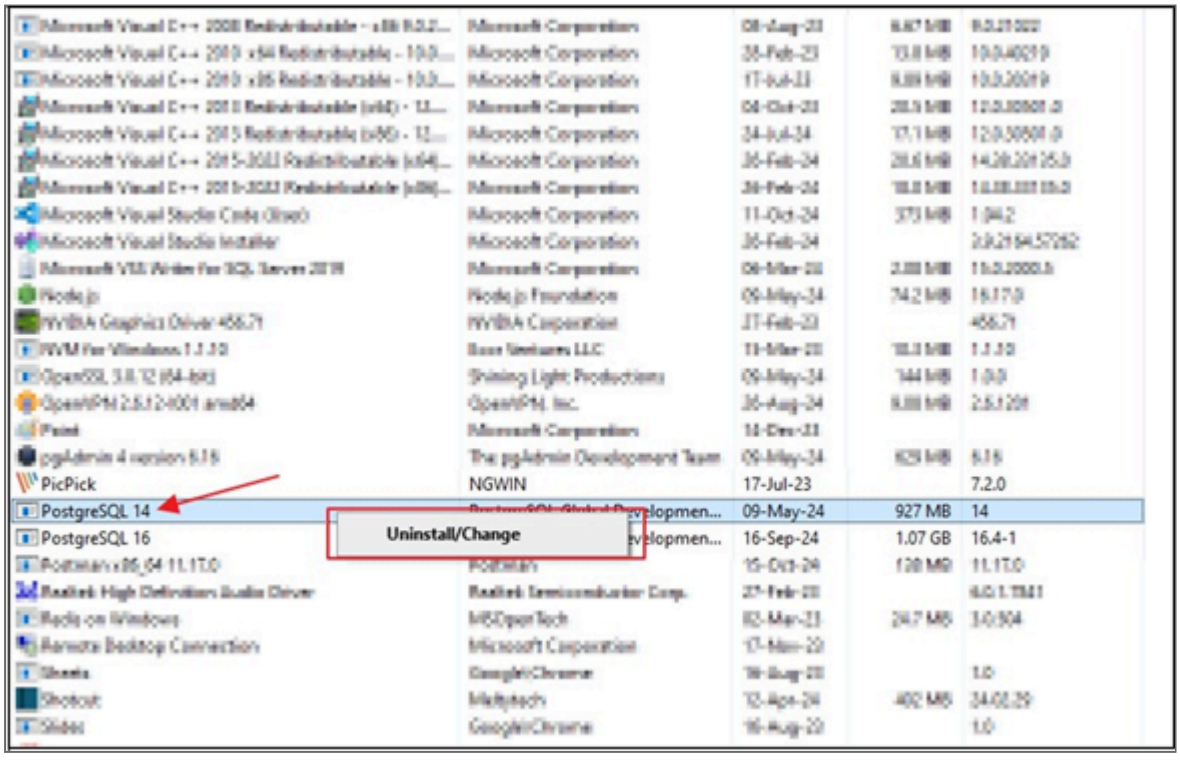
Restaurar la base de datos en PostgreSQL 16

1. Abra pgAdmin 4 (conectado a PostgreSQL 16).
2. Crear una base de datos nueva:
   - En pgAdmin, haga clic derecho en **Databases** y seleccione **Create** → **Database**.
   - Asigne el nombre **Suprema** a la base de datos y guarde.
3. Restaurar el respaldo:
   - Haga clic derecho en la base de datos **Suprema** recién creada y seleccione **Restore**.
4. Seleccionar archivo de respaldo:
   - En el campo **Filename**, seleccione el archivo de respaldo del directorio (**Suprema-backup**) que creó antes.
5. Iniciar restauración:
   - Haga clic en **Restore**. Espere a que se complete el proceso.
6. Verificar finalización de la restauración:
   - Una vez que termine la restauración, debería ver un mensaje de éxito. Ahora puede acceder a sus datos y verificarlos en PostgreSQL 16.

Q. Desinstale PostgreSQL 14 después de actualizar PostgreSQL a la versión 16.

A. Para desinstalar PostgreSQL 14, siga los pasos siguientes,

1. Vaya a **Panel de control** → **Programas** → **Programas y características**.
2. Busque **PostgreSQL 14** en la lista de programas instalados.
3. Haga clic derecho en **PostgreSQL 14** y seleccione **Desinstalar**. Siga las indicaciones para completar la desinstalación.



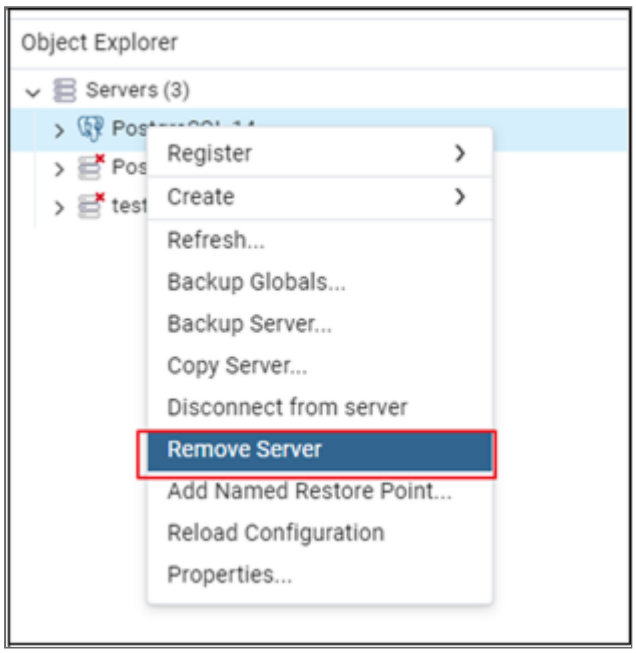
4. Revise el directorio de instalación (por lo general, en `C:\Program Files\PostgreSQL\14`) y elimine los archivos o carpetas

restantes.

> **Información**
> Si PostgreSQL 14 sigue apareciendo en pgAdmin incluso después de desinstalarlo, es probable que pgAdmin aún conserve su configuración del servidor.

Puede eliminarlo manualmente de pgAdmin siguiendo estos pasos:

1. **Haga clic derecho** en **PostgreSQL 14** en el panel Object Explorer de pgAdmin.
2. **Seleccione** Delete/Remove Server en el menú contextual.



3. **Confirme** la eliminación cuando se le solicite.



Esto eliminará la configuración del servidor PostgreSQL 14 de pgAdmin sin afectar la instalación de PostgreSQL 16.

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

Para obtener más información sobre las sucursales globales de Suprema,
visite la página web a continuación escaneando el código QR.
http://www.supremainc.com/en/about/contact-us.asp

© 2026 Suprema Inc. Suprema y los números y los nombres que identifican productos mencionados en este documento son marcas comerciales registradas de Suprema, Inc. Todas las marcas y los nombres de productos que no pertenecen a Suprema son marcas comerciales o marcas comerciales registradas de sus respectivas compañías. La apariencia del producto, el estado de la estructura o las especificaciones están sujetas a cambio sin previo aviso.