AN-264

Suprema Biometrics Integration with Protege GX

Application Note

Last Published: 27-Aug-25 1:16 PM

Contents

Introduction

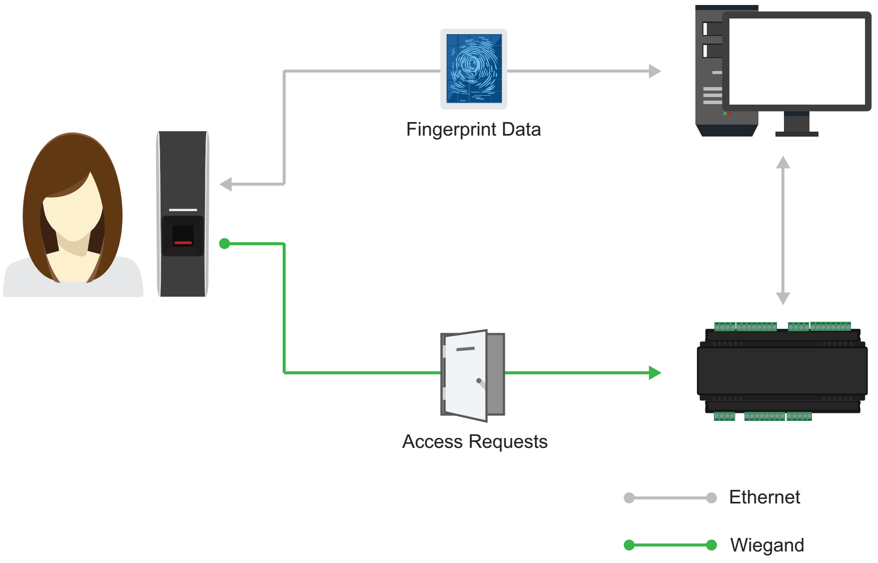
Integrating Suprema biometric devices with Protege GX combines the security and convenience of biometric identification with powerful access control and reporting functionality.

Enrollment is quick and easy: users simply scan their fingerprint or face at an enrollment reader, usually situated at the front desk of the building. Protege GX saves the biometric data and synchronizes it with other Suprema readers around the site. From then on, the user can access doors and areas throughout the building using their fingerprints and face, just like they would with an access card.

How It Works

Each user scans their face and/or fingerprints at an enrollment reader. The reader uses the scanned data to create a credential template, which it sends to the Protege GX server over ethernet. Protege GX generates a unique credential number for the biometric data and synchronizes it with all Suprema devices connected to the ethernet network.

Each biometric device is also wired to a Protege controller or reader expander using a standard Wiegand interface, just like a card reader. When a user presents their face or finger, the device authenticates them against the stored biometric scan and sends the associated credential number to Protege GX. Protege GX then validates the user's permissions and grants or denies access. Access events are logged in Protege GX for later reporting.



Biometric devices can be used on their own for door and area access, which is convenient for end users as they always have their credentials on hand. For added security, combine biometric devices with ICT card readers to provide dual factor authentication alongside a card or PIN code.

Prerequisites

The following software must be installed and operational.

Software	Version	Notes
Protege GX	4.3.393	This version supports the models listed below, but has deprecated support for some first-generation Suprema devices that were supported in previous Protege GX versions (see next page).
Suprema BioStar	-	Compatible with any version that supports the devices listed below.

Licensing

The following licenses are required for this integration.

License	Order Code	Notes
Protege GX Suprema Biometric Integration License	PRT-GX-BIO-SP	1 license per Suprema biometric reader connected to the system
Protege GX Suprema Biometric Integration Annual Care Plan	PRT-GX-BIO-SP-ACP	One annual care plan must be purchased for each Suprema biometric reader. It is charged annually for ongoing support and integration updates.
Protege GX Door License	PRT-GX-DOR-1	1 license per door record
	PRT-GX-DOR-10	
	PRT-GX-DOR-50	

Suprema DLL Files

Some additional DLL files are required to use this integration. These include the Suprema SDK and its prerequisites. Before you begin, you must acquire the following files from ICT (available on the ICT website):

- BS_SDK_V2.dll
- GXSV2.ThirdParty.dll
- libcrypto-1_1.dll
- libssl-1_1.dll

Even if your system already has these files from an earlier version of Protege GX, you must use the latest files from ICT. Make sure you update these files if you are upgrading from a version before 4.3.393.

See Installing the Suprema DLL Files for instructions.

Supported Devices

This integration uses Suprema BioStar Device SDK version **2.9.8**. It is designed to support second-generation Suprema biometric devices.

Some first-generation devices can be upgraded to firmware versions that support BioStar Device SDK version 2. See the Suprema documentation, and contact your Suprema representative for assistance.

The following Suprema devices are supported by this integration. If the device you wish to use has not been validated by ICT, we recommend validating the integration on a test bench before deploying it to site.

Supported Suprema Device	Validated?	Firmware Version	Notes
BioEntry			
BioEntry W3	✓	1.0.0	
BioEntry P2	✓	1.4.3, 1.5.1	
BioEntry R2			
BioEntry W2			
BioEntry Plus	✓	2.3.4	Only devices with OC-4 sensors are supported. Must be upgraded to a firmware version that supports the BioStar 2 Device SDK.
BioEntry W			Only devices with OC-4 sensors are supported. Must be upgraded to a firmware version that supports the BioStar 2 Device SDK.
BioLite			
BioLite N2			
BioLite Net			Only devices with OC-4 sensors are supported. Must be upgraded to a firmware version that supports the BioStar 2 Device SDK.
BioStation			
BioStation 3	✓	1.1.1	
BioStation 2a			
BioStation 2			
BioStation A2			
BioStation L2			
FaceLite			
FaceLite	✓	1.1.0	
FaceStation			
FaceStation F2	✓	2.1.4	
FaceStation 2	✓	1.2.1, 1.5.3	
X-Station			
X-Station 2			

Unsupported Devices

This integration does not support the following devices:

- First-generation Suprema devices that cannot be upgraded to a firmware version that supports BioStar Device SDK version 2. This includes the following models:
  - BioLite Net (with OC-2 sensor)
  - BioEntry W (with OC-2 sensor)
  - BioEntry Plus (with OC-2 sensor)

  If you are already using these biometric devices on a site, they will continue to grant access to existing users. You can revoke access for the door by disabling or deleting the user record in Protege GX. However, you will not be able to add new users to these devices or modify the biometric credentials of existing users in Protege GX.
- The Biomini USB fingerprint scanner range.

Types of Suprema Face Readers

Suprema offers two types of face readers:

- Infrared face readers (e.g. FaceStation 2, FaceLite)
- Visual face readers (e.g. FaceStation F2, BioStation3, BioEntryW3)

Protege GX supports both types of face readers. However, be aware that the two types are not compatible: infrared face data cannot be used by visual face readers, and vice versa.

If a site has both types of face readers, each user must enroll their face twice (once at each type of reader). To prevent additional work for the end user, we recommend using only one type of face reader on each site.

Dual Authentication

This integration supports dual authentication using Suprema biometric readers alongside ICT card readers. To achieve this, wire the biometric device and card reader to the same reader port in Wiegand configuration. This allows you to use any combination of biometric, card and PIN credentials.

Capacity

Protege GX supports a maximum facility number of 2047 and maximum card number of 16,777,215 for this integration.

The actual number of users that can be enrolled at any time depends on the capacity of the Suprema devices used on the site. Consult the product specifications from Suprema before specifying sites with 50,000 or more active users.

Managing Biometric Data

This section explains how biometric data is captured, stored and handled. This may be useful for understanding the legal and privacy implications of using the Suprema biometric integration.

Capturing biometric data

When a user enrolls at a Suprema device, it creates the following data:

- **Finger and face**: Credential template
- **Visual face**: Photo of the user

This data is stored in the following locations:

- The ProtegeGX database
- The download files on the Protege GX server. These files are stored at: C:\ProgramData\ICT\Protege GX\Download_Biometric_X.dat
- The Suprema biometric devices on the site.

Suprema devices include measures to protect sensitive user data. See the Suprema website for more information.

Updating Biometric Data

To update the user's biometric data, repeat the user enrollment process (see page 17).

Erasing biometric data

To erase the user's biometric data, simply delete the user record from Protege GX. This will also delete the biometric data from connected Suprema devices.

Biostar and Protege GX Services

The BioStar software and Protege GX Download Service use the same port (51211) to communicate with the biometric devices. This means that the services cannot connect to the devices at the same time.

- If you are using BioStar to configure the devices, you must stop the Protege GX Download Service.
- If you are using Protege GX to enroll users, you must stop **all** BioStar services.

To start and stop the services:

1. Open **Services** as an administrator:
   - Press the **Windows + R** keys.
   - Type **services.msc** into the search bar.
   - Press **Control + Shift + Enter**.
2. Locate the service or services you wish to stop. Right click on each service and select **Stop**.
3. Locate the service or services you wish to start. Right click on each service and select **Start**.
4. It is recommended that you set the BioStar services to manual mode, so that they do not automatically start when the computer boots up.
   - Right click on each BioStar service and select **Properties**.
   - Set the **Startup type** to Manual.
   - Click **Ok**.

When you switch from using BioStar to Protege GX, you should delete the readers from BioStar and power cycle them. This is because each reader can only support one open IP connection at a time, and the power cycle helps it refresh that connection so it can connect to Protege GX. For more information, see Disconnecting Devices from BioStar (page 10).

Connecting the Biometric Devices

Each Suprema device has two wiring connections:

1. Ethernet connection to the network, allowing Protege GX to send biometric data to all devices when a user is enrolled. You may need assistance from the IT team if the biometric devices are not on the same network as the Protege GX server.
2. Wiegand connection to the Protege GX controllers and reader expanders. When a user scans their face or fingerprint at a door, the biometric device sends a facility and card number over the reader port, in the same way as a standard card reader.

Dedicated enrollment readers that are not used for door access only need an ethernet connection.

Wiegand Connection

To connect the biometric device over Wiegand, use the **Wiegand output cable** supplied with the unit.

Biometric Reader Port	Pin on Protege Reader Port
WG 0 / WG OUT0	Wiegand D0
WG 1 / WG OUT1	Wiegand D1
WG GND	V-

Some devices have separate Wiegand output and input ports, whereas others have combined output/input ports. Ensure that you use the output port. Consult the installation manuals for the specific Suprema devices you are installing.

If the reader uses 12V power, you can also power the device from the controller or reader expander's auxiliary ports using the **power cable**.

Configuring Devices in BioStar

You can configure Suprema biometric devices using Suprema BioStar software.

1. Stop the Protege GX Download Service and start the BioStar service (see page 8).
2. Open the BioStar software and navigate to the **Device** section.
3. Click **Search Device** to perform a network scan for the devices on the local subnet. Alternatively, click **Advanced Search** and enter the IP Address and Device Port settings of the device you wish to configure.
   - Most Suprema devices have DHCP enabled by default. If your network has DHCP, these devices will be found automatically.
   - If your network does not have DHCP, the devices will assign themselves IP addresses. In this case, use a network scanner to find each device's IP address and enter it into the **Advanced Search** field.
   - If the IP address has previously been set on the device and you do not know what it is, default the device to return it to DHCP mode. Refer to the Suprema documentation for instructions for your devices.
4. Open each device from the **All Devices** list.
5. Do **not** enable the **Device > Server Connection** setting. This setting prevents the devices from connecting to Protege GX.
6. In the **Network** section, update the network settings as required.

   The biometric devices should use a static IP address so that Protege GX does not lose connection to them. There are two ways to achieve this:
   - Uncheck **Use DHCP** and enter a new **IP Address**.
   - Alternatively, configure the DHCP server to keep IP addresses constant.

   Make a note of the **IP Address** for later.
7. In the **Advanced** section, configure the following **Wiegand** settings:
   - Set the **Input/Output** to Output.
   - Set the **Wiegand Format** to 26 Bit SIA Standard.
   - Set the **Output Mode** to Normal. This allows the biometric device to authenticate the user and pass the Wiegand credential associated with that user to Protege GX.
   - Set the **Pulse width** to 20 microseconds.
   - Set the **Pulse Interval** to 200 microseconds.
   - Set the **Output info** to Card ID.
8. Click **Apply**.
9. Repeat to program the other biometric devices that will be connected to the system.

Disconnecting Devices from BioStar

After you complete all required device configuration in BioStar, you must disconnect the devices from BioStar and power cycle them. This refreshes the network connection, allowing Protege GX to connect to the biometric devices.

To disconnect the devices:

1. Take a backup of the BioStar database.
2. Open the settings for each biometric device. In the **Server** section, disable the **Device > Server** setting.
3. Click **Apply**.
4. Delete the device from the BioStar software.
5. Repeat for each biometric device you have configured.

6. Stop the BioStar services and start the Protege GX Download Service (see page 8).
7. Power cycle all devices.

Installing the Suprema DLL Files

To enable the integration, you must copy the Suprema DLL files provided by ICT onto the Protege GX server and each client machine. There is also an additional DLL file that needs to be registered on client workstations.

If your system already has these files from a Protege GX version prior to 4.3.393, acquire the latest DLL files from ICT and replace the existing files.

You will need administrator access to the computers where you are performing these actions.

Protege GX Server

First, install the DLL files on the Protege GX server.

1. Navigate to the Protege GX installation directory. By default this is:
   C:\Program Files (x86)\Integrated Control Technology\Protege GX
2. Paste the following DLL files into this directory.
   - BS_SDK_V2.dll
   - GXSV2.ThirdParty.dll
   - libcrypto-1_1.dll
   - libssl-1_1.dll

   Grant admin permissions when requested.
3. The **Suprema.dll** file in this folder will be needed for client installations. Copy this file into a shared directory with the other DLL files.
4. Open **Services** as an administrator:
   - Press the **Windows + R** keys.
   - Type **services.msc** into the search bar.
   - Press **Control + Shift + Enter**.
5. Locate the **Protege GX Download Service**. Right click on it and select **Restart**.

Protege GX Clients

You must complete the following instructions on all workstations that will be used for enrolling users.

1. On each client workstation, navigate to the installation directory. By default this is:
   C:\Program Files (x86)\Integrated Control Technology\Protege GX
2. Copy and paste the Suprema DLL files into this directory:
   - BS_SDK_V2.dll
   - GXSV2.ThirdParty.dll
   - libcrypto-1_1.dll
   - libssl-1_1.dll
   - Suprema.dll
3. Open a command prompt as an administrator:
   - Press Windows + R.
   - Type cmd and press Ctrl + Shift + Enter.
   - Click Yes to grant administrator permissions.
4. Type the following command and press Enter:

   ```
   cd C:\Windows\SysWOW64
   ```

5. If you have a 64-bit machine, type the following command and press Enter:

   ```
   regsvr32.exe "C:\Program Files (x86)\Integrated Control Technology\Protege
   GX\Suprema.dll"
   ```

   If you have a 32-bit machine, type the following command and press Enter:

   ```
   regsvr32.exe "C:\Program Files\Integrated Control Technology\Protege
   GX\Suprema.dll"
   ```

6. You should see a popup saying that the DLL was registered successfully.
7. If the client was running, close and reopen it.
8. Repeat for each other Protege GX workstation that will be used to enroll users.

Setup in Protege GX

To set up the integration in Protege GX, you must enable the integration and create one biometric reader for each Suprema device. You can then set up the doors with Wiegand readers.

Preparation

Before you begin configuring the integration in Protege GX, you should:

- Bring all controllers and reader expanders online
- Create the reader expanders and doors that will have biometric devices connected to them

Enabling the Integration

The Suprema Biometrics integration must be enabled for each Protege GX site that will use it.

1. Stop the BioStar service, if you have not already (see page 8).
2. Navigate to **Global | Sites** and select the site that will use this integration.
3. Select the **Biometrics** tab and check **Enable Suprema integration**.
4. Configure the following settings as required:
   - **Default facility number**: This is the facility number that will be used when you enroll new biometric credentials. Set this to any value from 1-2047 that is not already used by cards on this site.
   - **Default enrollment reader**: The biometric reader that will be used by default for enrolling user credentials. Set this after adding the biometric readers.

Adding the Biometric Readers

For each Suprema biometric device connected to the system, add one biometric reader record.

1. Navigate to **Sites | Biometric readers**.
2. **Add** a new biometric reader with a relevant name (e.g. Front Door FaceStation).
3. Enter the device's **IP address** and **IP port** details.
4. Set the **Type** to Suprema.
5. Set the **Secondary type** to Biostar 2.

   Biostar 1 is no longer supported.

6. Select the **Biometric type** for this reader:
   - Fingerprint reader
   - Visual face reader
   - Face reader
   - Fingerprint and visual face reader

   Visual face readers and standard infrared face readers capture different types of data that are not compatible with each other. Ensure that you select the correct type of face readers that are used on site. For more information, see Types of Suprema Face Readers (page 7).

7. If the device will be used for door access, enable **Automatically download users to this reader**.

   If the device will only be used for enrollment, do not enable this setting.

8. Click **Save**.

9. Repeat to add all other biometric readers.
10. Optionally, return to **Global | Sites | Biometrics**. Set the **Default enrollment reader** to a convenient reader (e.g. at the reception desk).

Creating the Custom Reader Format

The biometric reader sends credentials to the controller using a custom Wiegand data format. This must be configured in the controller programming and applied to the relevant reader expanders.

1. Navigate to **Sites | Controllers** and select the controller that will be used in this integration.
2. Select the **Custom reader format** tab.
3. Set the following **Custom reader configuration** settings:
    - **Custom reader type**: Wiegand
    - **Bit length**: 37
    - **Site code start**: 1
    - **Site code end**: 11
    - **Card number start**: 12
    - **Card number end**: 35
    - **Data format**: 32 Bit Data
    - **Parity type (1-4)**: Odd Parity
    - **Parity location (1-4)**: 255
    - **Parity start (1-4)**: 255
    - **Parity end (1-4)**: 255
    - **Set bit (1-4)**: 255
    - **Clear bit (1-4)**: 255
    - **Card data AES encryption key**: Blank
4. Click **Save**.
5. Repeat the above for all controllers used in this integration.

Configuring Wiegand Readers

For each Suprema device that is connected in Wiegand mode, you must configure the reader expander port it is connected to. Setting the reader format allows the reader expander to recognize the custom 37 bit format created above.

1. Navigate to **Expanders | Reader expanders** and select the reader expander that the biometric reader(s) will be connected to.
2. Select the appropriate **Reader 1/2** tab.
3. Set the **Reader 1/2 format** to Custom format.
4. Set the **Reader 1/2 secondary format** to 26 bit.
5. Click **Save**. Wait for the programming to download to the controller, then right click on the reader expander record and click **Update module**.
6. Repeat the above for all reader expanders used in this integration.

Creating Door Types

Each door with a biometric device needs a door type that uses biometric credentials.

1. Navigate to **Programming | Door types**.
2. Click **Add** and give the door type a descriptive name (e.g. Biometric reader).
3. Under **Entry**, set the **Entry reading mode**:
   - If the door is only using biometrics, use Card only.
   - If the door is using both biometrics and a card reader, set to Card and biometric or Card or biometric.
   - For other credential combinations, set the **Entry reading mode** to Custom and select the **Entry credential types** (e.g. Bio and PIN).
4. If the doors have exit readers, set the **Exit reading mode** as required.
5. Set any other options that are required for this door type, such as antipassback.
6. Click **Save**.
7. Repeat to create any other biometric door types that are required.

Finally, set the door type for the doors with biometric devices connected:

1. Navigate to **Programming | Doors**.
2. Select each door controlled by a biometric reader and set the **Door type**.
3. Click **Save**.

Adding and Enrolling Users

Enrolling biometric credentials using Protege GX is a straightforward process. Once this is complete, the user can use their face or fingerprint at any biometric device that they have access to.

1. Navigate to **Users | Users**.
2. Add a new user, or select an existing user.
3. **If you are adding a new user**, enter the user's name, access card details, access levels and other settings, then click **Save**.

   > You must save the new user to generate the Database ID, which is needed for the biometric credential.

4. Open the **Biometrics** tab. This displays all the types of biometric data that are used on your site.
5. Select an **Enrollment device**. The **Biometric data** section will show what types of data need to be enrolled and what has been enrolled already.
6. Click **Scan** to enroll finger or face data.
   - For fingerprint scans, make sure you leave your finger in place long enough for a good scan. Take your finger off the reader between the first and second scan.
   - For face scans, follow the instructions on the device.
   - **Visual face** and **Face** are different types of data. If you have both types of readers on your site, each user must enroll their face twice.
7. If you are using a fingerprint reader, you can scan an additional finger (e.g. in case the first finger is injured).
8. You can change the **Enrollment device** to scan different types of data, if necessary.
9. Once you have enrolled all the biometric data you need, click **Save**.

When you save the user, Protege GX will automatically generate a credential number in the **Facility/Card number or biometric data** field (**General** tab). It then downloads the biometric data and credential number to all Suprema biometric readers.

If you need to update a user's biometric credential, simply repeat the scanning process above.

Revoking Access

There are three ways to revoke access from doors with biometric readers:

- **Disable access in Protege GX**: Disable the user record or remove their access levels to prevent Protege GX from granting access to the user.
- **Disable the biometric data**: Select the user and open the **Biometrics** tab. Check the **Disable** box next to the types of biometric data you wish to disable. This disables the user's biometric data in the Suprema devices, so no Suprema device will grant access to that user.
- **Delete the user record**: Delete the user record in Protege GX to remove their data from both Protege GX and the biometric devices.

Troubleshooting

Biometric Device Issues

The BioStar software and Protege GX Download Service cannot be used at the same time. If you are experiencing configuration issues with the readers, make sure that only one of these services is running at a time. For more information, see Biostar and Protege GX Services (page 8).

If the devices will not come online with Protege GX, ensure that you have correctly disconnected them from BioStar (see page 10).

Download Issues

Downloads to the biometric devices are managed by the Protege GX Download Service. Downloads occur every 1 minute. To verify whether a download has occurred, Wireshark your server and filter the capture by the TCP port being used to communicate with the biometric reader (e.g. `tcp.port==51211`).

If your biometric device is configured correctly, restarting the Protege GX Download Service will bring it online and force a download to it.

> The Protege GX Enterprise Download Server does not download data to biometric devices. The standard download server will continue to handle these downloads even when the enterprise download server is installed.

Resolving Known Issues

The user with Database ID 0 cannot access Suprema devices

When biometric devices are connected to the BioStar software, BioStar overwrites the user record with a Database ID of 0. This will prevent the user from gaining access at biometric readers. There are a few options for working around this issue:

- Create a copy of this user record, then delete the original record. The copy will have a higher Database ID, avoiding this issue.
- Avoid connecting biometric devices back to the BioStar software.
- If the user record has been overwritten, when you reconnect the device to Protege GX delete the C:\ProgramData\ICT\Protege GX\Download_Biometric_X.dat file to initiate a complete download and restore the user record.

Client workstations cannot enroll users, display "Failed to invoke the Protege GX Suprema component"

You must register the Suprema.dll file on the client machine. Follow the instructions in Installing the Suprema DLL Files.

Additional Notes

- Protege GX always inserts the biometric facility/card code into position 2 in the user's Card Numbers list. If position 2 contains existing data, this will automatically be moved down the list.
- If the user has no facility/card entries, Protege GX will fill position 1 with arbitrary data. You can delete this to add a standard card number for the user later.

Designers & manufacturers of integrated electronic access control, security and automation products.
Designed & manufactured by Integrated Control Technology Ltd.

Disclaimer: Whilst every effort has been made to ensure accuracy in the representation of this product, neither Integrated Control Technology Ltd nor its employees shall be liable under any circumstances to any party in respect of decisions or actions they may make as a result of using this information. In accordance with the ICT policy of enhanced development, design and specifications are subject to change without notice.