AN-264

Suprema Biometrics Integration with Protege GX

Application Note

Last Published: 21-Dec-23 8:41 AM

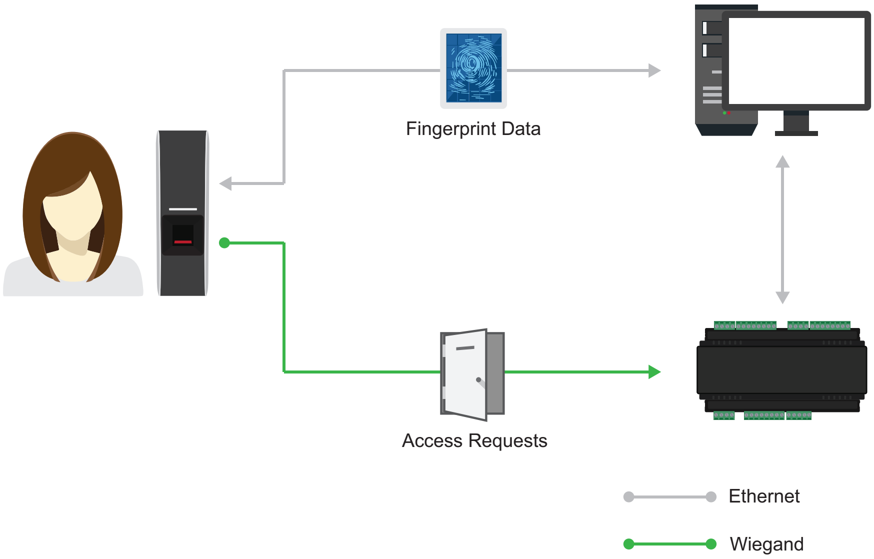
Contents

Introduction

Once thought to be the domain of top secret government agencies and James Bond films, biometric technology has become mainstream and is now used by businesses every day. Protege GX integrates with Suprema BioEntry, BioEntry Plus and FaceStation devices, putting security literally at your fingertips (or right in your face).

Enrollment is both quick and easy. Users simply scan their fingerprint or face at an enrollment reader to create their biometric record. The reader uses the scanned data to create a credential template, including a card number, which it sends to the Protege GX server. Protege GX stores this data in the database and then sends the template over IP to all other Suprema readers attached to the system, so the user needs to enroll only once.

The integration also allows a second fingerprint template to be stored against a user. This is typically used as a backup in case the first finger cannot be read, however it can also be used to provide a duress function.



Suprema Biometric readers are connected to Protege reader expanders using a standard open Wiegand interface. When a user presents their face or finger to any of the connected biometric readers, the reader authenticates the scanned data against the stored template and sends the associated card number to Protege GX. Protege GX then validates the user's access based on their programming, and unlocks the door.

Biometric readers can be used on their own, where only a single authentication factor is required, which is convenient for end users as they always have their credentials on hand. For added security, biometric readers can be combined with ICT access control readers to require dual factor authentication.

Prerequisites

The following software must be installed and operational.

Software	Version	Notes
Protege GX	4.2.247.4 or higher	Versions below 4.3.285 support a smaller number of users for use with this integration. For more information, see Limitations (page 6).
Suprema BioStar	-	

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 Door License	PRT-GX-DOR-1	1 license per door record
	PRT-GX-DOR-10	
	PRT-GX-DOR-50	

Suprema DLL Files

Some additional Suprema DLL files are required to use this integration. Before you begin you must acquire the following files from ICT (available on the ICT website):

- BS_SDK.dll
- BS_SDK_V2.dll
- GXSV2.ThirdParty.dll

Prior to version 4.3.336.1, these files were installed alongside the Protege GX software. After this version the files must be acquired and installed manually (see page 8).

Supported Devices

The following Suprema devices have been tested and are supported in Protege GX with their listed device firmware version and the necessary integration prerequisites:

Suprema Device	Firmware Version
BioLite N2	1.0.1
Face Station 2	1.1.0
BioEntry Plus	1.5
BioEntry P2	1.1.0
BioEntry W	2.2.3
BioEntry W2	1.2.0

Dual Authentication

The Protege GX integration with Suprema supports dual authentication using Suprema biometric readers alongside ICT card readers. The biometric reader and card reader are wired to the same reader port in Wiegand configuration to allow any combination of biometric, card and PIN credentials.

Reading cards from Suprema devices is outside the scope of this integration, as Suprema devices with inbuilt card readers are not capable of decrypting ICT MIFARE and DESFire credentials. As a workaround it is possible to use CSN reading alongside a custom credential format in Protege GX, but ICT Technical Support cannot assist with this process.

Limitations

As of Protege GX version 4.3.285, the Suprema Biometrics integration supports 16,777,215 users. The maximum available facility number is 2047. This is dependent on the Custom Reader Format configuration (see page 9).

The number of supported users is based on the total number of users that have been created in the database. This includes user records that have been deleted and users that do not have enrolled biometric credentials. If a user has a Database ID of 16,777,215 or higher, they cannot use the Suprema Biometrics integration.

If the Protege GX version is earlier than 4.3.285, or the custom reader format is not configured as specified (see page 9), the maximum number of users is 65,535 and the maximum facility number is 255.

Biostar and Protege GX Services

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

- If you are using BioStar to configure the readers, 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 the **Services** snap-in by:
   - Pressing the **Windows + R** keys
   - Typing **services.msc** into the search bar and pressing **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.

Configuring the Biometric Readers

The Suprema readers can only be configured through Suprema's BioStar software, which is freely downloadable from the Suprema website. The current supported version is BioStar 2 and SDK version 2.6.1

1. Stop the Protege GX Download Service and start the BioStar service.
2. Open the BioStar software and navigate to the **Device** section.
3. Click **Search Device** to perform a network scan for the reader 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 come with DHCP enabled by default. When using a network with a DHCP server you should have no problem discovering these devices. If you are not using DHCP the device will fail to obtain an IP address and assign itself an address in the 169.254.0.0 range. In this case you will need to discover the IP address of the device using a network scanner and enter this into the **Advanced Search** field.

4. If the IP address has previously been set on the device and you do not know what it is, you can default the reader to DHCP. To default a Suprema fingerprint reader, hold down the small button on the back of the reader until the reader beeps and restarts. This puts the reader into DHCP mode. You will need to scan the network for the Suprema device using either BioStar software or a network scanner as detailed above.
5. Once you have the biometric reader online with the BioStar software you can configure the IP address settings to be static at the address you require, through its **Network** settings.
6. In the **Authentication** section, configure the **Format** settings:
   - Set the **Format** or **Format Type** to Wiegand.
   - Set the **Byte Order** to MSB.

   Reader configuration options will vary depending on reader model and firmware version. Some settings may be defaulted, and others may be unavailable. Refer to the appropriate Suprema documentation for the correct configuration of your particular reader.

7. In the **Advanced** section, configure the following **Wiegand** settings:
   - Set the **Input/Output** to Output.
   - Set the **Pulse width** to 20.
   - Set the **Pulse Interval** to 200.
   - Set the **Wiegand Format** to 26 Bit SIA Standard.
   - Set the **Output Mode** to Normal. This allows the biometric reader to authenticate the user and pass the Wiegand credential associated with that user to Protege GX.

     If you are using the card reader on a Suprema device, it is possible to set the **Output Mode** to Bypass to allow the biometric reader to send the credential template in addition to the Wiegand data for cards. Protege GX can then use a custom credential type to interpret and authenticate the credential. However, ICT Technical Support cannot assist with this process (see page 5).

8. When the reader configuration in BioStar is complete and saved/applied:
   - Delete the reader from the BioStar software.
   - Stop the BioStar services.
   - Power cycle the reader.

Installing the Suprema DLL Files

To enable the integration you must copy the Suprema DLL files acquired from ICT into the Protege GX installation directory on the Protege GX server and each client machine.

These files may already exist if you have upgraded from a previous version of Protege GX, but they are no longer included in the installation by default.

1. Locate and copy the **GXSV2.ThirdParty.dll**, **BS_SDK.dll** and **BS_SDK_V2.dll** files.
2. Navigate to the Protege GX installation directory. By default this is:
   C:\Program Files (x86)\Integrated Control Technology\Protege GX
3. Paste the DLL files into this directory. Grant admin permissions when requested.
4. Repeat this process on the server and each client installation of Protege GX.

Setup in Protege GX

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.
2. Navigate to **Global | Sites** and select the site you want to use biometric readers in.
3. Select the **Biometrics** tab and check **Enable Suprema integration**.
4. Configure the following settings as required:
   - **Default facility number**: This field sets the Facility Number for all new Suprema biometric credentials. When a user enrolls a new biometric credential, it will use this number. Changing the default facility number will not affect existing user credentials.

     > The maximum facility number available for Suprema Biometric credentials is 2047, subject to the controller's Custom Reader Format configuration (see below).

   - **Default enrollment reader**: This field sets the biometric reader that will be used by default for enrolling user credentials. This can be set after the biometric readers have been added.

Adding the Biometric Readers into Protege GX

1. Navigate to **Sites | Biometric readers**.
2. **Add** a new reader record and enter the relevant **IP address** and **IP port** details.
3. Set the **Type** to Suprema.
4. Set the **Secondary type** to the version of integration you need to use.
   - If you used BioStar 2 to set up your readers you should select Version 2.
   - If you used BioStar 1 then select Version 1.
5. Check the box for Protege GX to **Automatically download users to this reader**.

   > The only time you would not select this is for a dedicated enrollment reader not performing access control.

Setting the Custom Reader Format

The Protege GX controller communicates with the biometric reader using a custom Wiegand data format. This must be configured in the controller programming and applied to the relevant reader expanders.

The custom reader format described below increases the number of users supported by the integration to 16,777,215. The maximum available facility number is 2047.

> The **Reader 1/2 format** can also be set to HID 26/34 Bit. However, with this configuration the maximum card number supported by the integration will be 65,535, with a maximum facility number of 255.

Configuring the Custom Reader Format

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 the Reader Expanders

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 the Door Type

A door type is needed to instruct the doors which credentials they will use.

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 some **Entry credential types**, including Bio.
4. If the door has an exit reader, set the **Exit reading mode** as required.
5. Set any other options that are required for this door type.
6. Click **Save**.
7. In **Programming | Doors**, assign this door type to any doors which are using biometric readers.

Enrolling Users

Enrolling user biometric credentials using Protege GX is a straightforward process.

You must add and save the user record in Protege GX prior to enrolling a biometric credential. The integration uses the user's database ID as a reference and if the record is not saved the ID is 0, creating a duplication error.

1. Navigate to **Users | Users** and select the user to register a credential for.
2. Select the **Biometrics** tab and set the biometric reader to use as the **Enrollment device**.
3. For fingerprints, check the **Enable** option for Finger one and (if required) Finger two, then click **Scan** and follow the instructions to register the fingerprint.

   Be sure to leave your finger in place long enough for an adequate read quality, and remember to take your finger off the reader between the first and second read.
4. For the FaceStation, click **Scan** and complete the Face enrollment by following the instructions on the screen of the FaceStation device.
5. **Save** the user. This will automatically generate a Wiegand credential and download the user changes to the controller and all biometric readers that require the data.

If it becomes necessary to update a user's biometric credential, simply repeat the scanning process above.

Protege GX will insert 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, arbitrary data will be written to populate position 1 and the biometric data will be written to position 2.

Notes

- The same face or finger data cannot be registered to more than one user in Protege GX.
- It is acceptable to register both finger and face data to a user.
- New biometric credentials use the **Default facility number** set in the site programming (see page 9). This number can be changed if necessary, but changes are not downloaded to the biometric readers unless the C:\ProgramData\ICT\Protege GX\Download_Biometric_X.dat files are deleted to force a fresh download.
- The card number for the biometric credential is based on the user's Database ID. This number should not be changed, or duplicate credential errors can occur.
- When biometric readers are connected to the BioStar software, the user record with a Database ID of 0 is overwritten. 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 with a higher Database ID, then delete the original record.
  - Avoid connecting biometric readers back to the BioStar software.
  - If the user record has been overwritten, when you reconnect the reader 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.

Troubleshooting Downloads and Online Status

Capturing biometric data: When a user is scanned at a Suprema enrollment reader the reader encrypts the scanned data and creates a credential template which it sends over IP to the Protege GX server. Protege GX stores this data in the database and then sends the template over IP to all other Suprema readers attached to the system.

- Data downloaded to the biometric readers is written to the following files:
  C:\ProgramData\ICT\Protege GX\Download_Biometric_X.dat
  (where X is the Database ID of the biometric reader)
- Information on Suprema cybersecurity and encryption can be found on the Suprema website:
  https://www.supremainc.com/en/solutions/gdpr-privacy-protection.asp

Authentication: The authentication process depends on the configuration of the reader (see page 7).

- In Normal output mode the reader performs the authentication process and, if a match is found, sends an access request to Protege GX via Wiegand to the connected reader expander, just like a regular card reader.
- With Bypass mode enabled the reader will send the credential template in addition to the Wiegand data for cards, relying on Protege GX to authenticate the user and determine whether the access credential is valid.

Updating biometric data: If it becomes necessary to update a user's biometric credential, simply repeat the enrollment process (see previous page).

Erasing biometric data: Biometric data is stored in the Users table in the Protege GX SQL database in the following columns:

Enabled/Disabled Flags	Finger1, Finger2 (0=Finger Disabled, 1 = Finger Enabled)
Fingerprint Data	FingerData, FingerData2
Face Data	BiometricFaceData

- If a user's biometric credential is disabled within Protege GX (i.e. Finger1, Finger2 and/or BiometricFaceData is set to 0), the user will no longer be included in the .dat file, but the fingerprint or face will still be recognized by the biometric reader. If the credential is altered (either by completing a new scan or by manually updating the database record), the credential that was overwritten will no longer be valid at the biometric reader.
- The options for removing a credential from your biometric reader are:
  - Overwrite the database record by performing a fingerprint or face scan.
  - Alternatively, stop the Protege GX Download Service and sync the biometric reader to a Suprema BioStar server. Then, when you bring the reader back online with Protege GX, the reader will have a blank database and only receive finger data from the current .dat file from Protege GX.

Viewing Reader Data: The data stored on a Suprema reader can be viewed using the Biostar software.

For further information, consult the relevant Biostar documentation.

If data is edited or deleted in the Biostar software these updates will not be sent back to Protege GX.

Protege GX Download Service: 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 6).

Status: The online status of the biometric reader and downloads to the device are managed by the Protege GX Download Service. Downloads occur every 1 minute. If your biometric reader is configured correctly, restarting the Protege GX Download Service will bring the biometric reader online and force a download to it. 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`).

Resolving Known Issues

User Data Cannot be Enrolled at Client Machines

One required Suprema DLL file is not registered when the Protege GX client is installed. This prevents operators from enrolling user data at client machines. User registration will fail with the error "Failed to invoke the Protege GX Suprema component."

To resolve this issue, the DLL file must be manually registered on each client machine.

1. In the File Explorer navigate to the Protege GX installation directory. By default this is:
   C:\Program Files (x86)\Integrated Control Technology\Protege GX
2. Check that the Suprema.dll file is present. If not, copy and paste the file from the server installation into this directory.
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"
   ```
6. 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"
   ```
7. You should see a popup saying that the DLL was registered successfully.
8. Close and re-open the Protege GX client and ensure that you can enroll a user's fingerprint.

Updated Fingerprints are not Downloaded to Controllers

Updating the fingerprint data on a user record may not trigger a download to relevant controllers. This may occur when replacing an existing fingerprint, or adding a second fingerprint after the first was already saved.

As a workaround, navigate to **Sites | Controllers**, right click on the controller record and select **Force download**.

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.