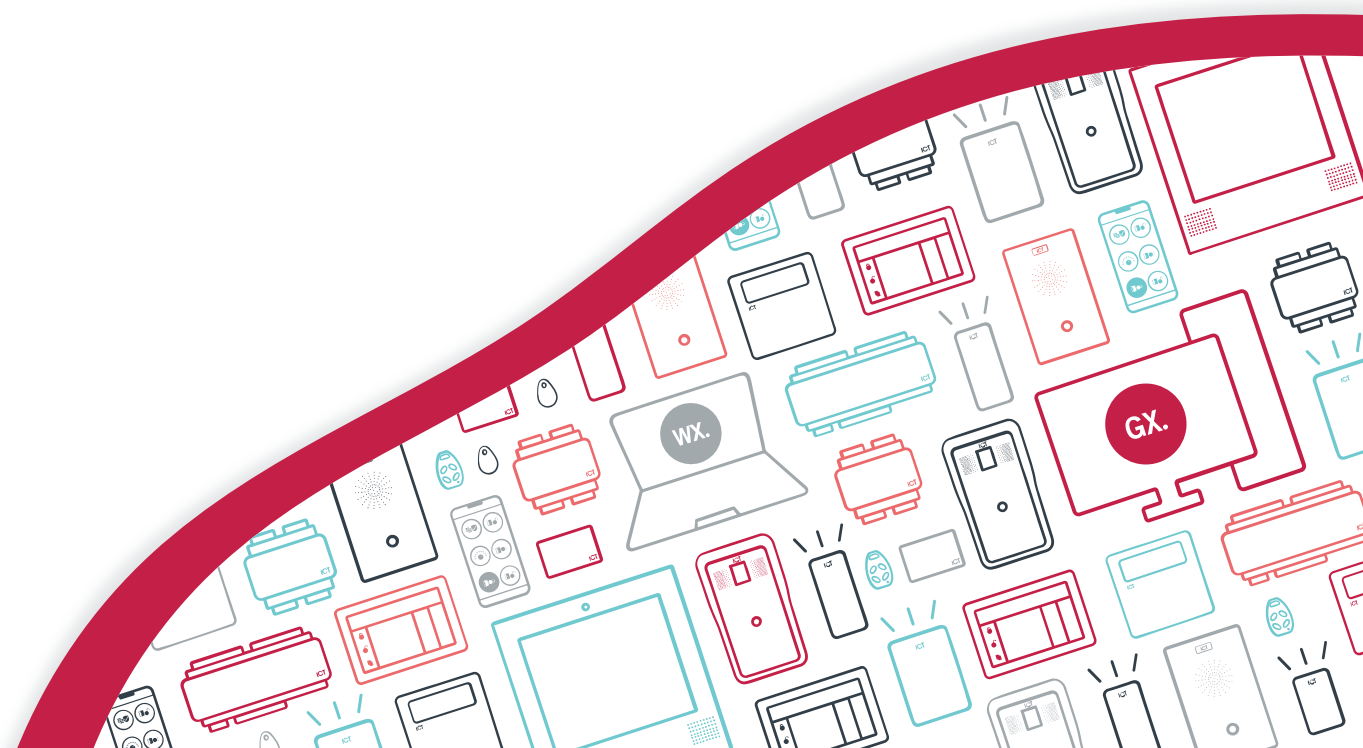
AN-360

# Protege GX IDEMIA MorphoManager Integration

Application Note



Last Published: 03-Feb-25 11:34 AM

# Contents

# Introduction

The Protege GX integration with IDEMIA MorphoManager combines the security and convenience of biometric identification with powerful access control functionality. Use any combination of fingerprint, face and card to access doors - all without the pain of duplicate data entry.

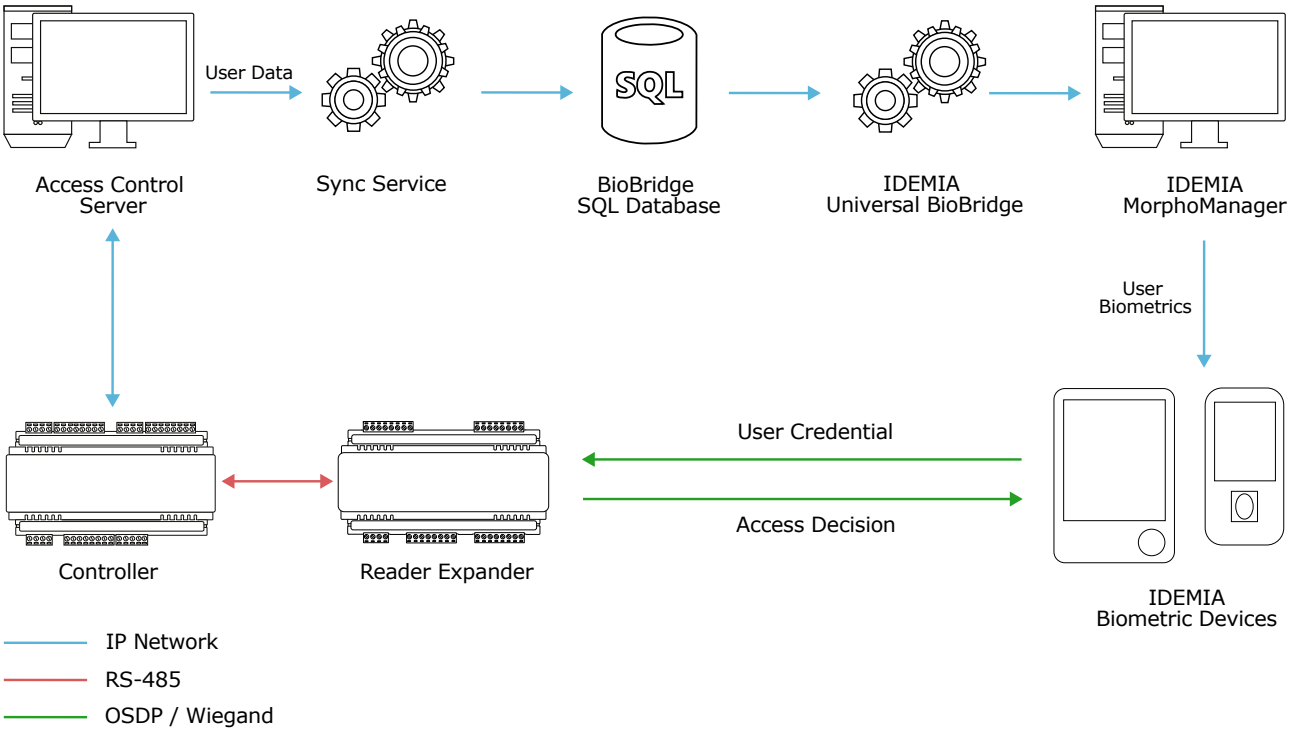
User records and access permissions are programmed in Protege GX and synchronized to MorphoManager. The user enrolls by scanning their fingerprints or face and their data is downloaded to biometric devices across the site. When they scan their biometrics at a door a unique credential number is sent to Protege GX to make the access decision - just like a normal card badge.

Integrating biometric devices with Protege GX unlocks a whole range of access control features that are normally available from card readers - such as multi-factor authentication, arming and disarming areas, activating automated processes and detailed reports.

This application note covers the requirements and instructions for setting up the IDEMIA MorphoManager integration with Protege GX and enrolling users for biometric access.

## Integration Architecture

This integration uses the IDEMIA Universal BioBridge interface to synchronize access data between Protege GX and IDEMIA MorphoManager.




It works as follows:

- Users and access levels are programmed in Protege GX.
- The Protege GX Idemia Sync Service synchronizes the users, access levels and credentials from Protege GX to the BioBridge database.
- An operator uses the BioBridge Enrollment Client to enroll face and fingerprint data against each user record, creating user records in MorphoManager.
- MorphoManager sends the user data to biometric devices via ethernet or WiFi.

- Biometric devices are connected to Protege GX controllers and reader expanders as OSDP or Wiegand readers. When the biometric device identifies a user, it sends a unique credential to the controller to request access.
- The controller makes the access decision based on the user's access levels and schedules and either grants or denies access.

# Prerequisites

The following software must be installed and operational.

| Component | Version | Notes |
|---|---|---|
| Protege GX | 4.3.377 or higher | |
| Protege GX SOAP Service | 1.7.0.0 or higher | |
| Protege GX Idemia Sync Service | 1.0.0.0 or higher | Instructions for installing this service are included in this document (see page 11). |
| Protege GX Controller | 2.08.1353 or higher | All controllers must be online with Protege GX. |
| Protege Reader Expander | 1.12.599 or higher | |
| IDEMIA MorphoManager Server | 16.4.2.0 | This is the **only** tested and supported version for this integration. Other MorphoManager versions 16 and higher are expected to work, but must be validated by the installer prior to installation. |
| IDEMIA MorphoManager Client | 16.4.2.0 | The BioBridge Enrollment Client is automatically installed alongside the main client software. |
| SQL Server | 2017 or higher | |

It is the responsibility of the installation professional to verify the version of the proposed third-party system and supported components with the version listed in this document. ICT will not accept responsibility for the failure to verify integrated system versions and requirements.

## Licensing

| License | Order Code | Notes |
|---|---|---|
| Protege GX IDEMIA Integration License | PRT-GX-IDEMIA | 1 per Protege GX server. |
| Protege GX IDEMIA Integration Annual Care Plan | PRT-GX-IDEMIA-ACP | The annual care plan must be purchased alongside the base integration license. 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 | |

## Biometric Devices

This integration supports any IDEMIA biometric device that can connect to MorphoManager, including fingerprint, handwave and facial recognition devices.

Ensure that the device firmware is compatible with the MorphoManager software version you have installed.

### Cards

IDEMIA readers can read MIFARE Classic and MIFARE DESFire cards encoded by ICT. MIFARE DESFire credentials are strongly recommended to provide higher security.

This application note provides instructions for configuring standard ICT 26 bit or 34 bit cards on IDEMIA readers. Before you begin, contact ICT Customer Services or Technical Support (Contact Us) to obtain the following information about your cards:

- Wiegand Format
- For MIFARE DESFire cards:
  - Application ID of the open Wiegand file
  - MIFARE DESFire read key
- For MIFARE Classic cards:
  - Read/Write Key for the open sector (sector 12)

## Limitations

Before you begin, please be aware of the following limitations in this integration:

- User records that will be synchronized to IDEMIA must have a **First name** and **Last name**.
- IDEMIA BioBridge does not support user and access level names longer than 70 characters. Before you begin, ensure that the **First name** and **Last name** fields for users and the **Name** field for access levels do not exceed 70 characters. Otherwise the service installation will fail.

  If you need to add notes to the record, you can use the **Display name** and **Name (Second language)** fields as these are not synchronized to BioBridge.
- User records are synchronized between Protege GX and the BioBridge database almost instantly. However, the BioBridge Enrollment Client's cache is only updated on the hour. This means that new users added in Protege GX may take up to an hour to appear in the BioBridge Enrollment Client.
- Every access level in Protege GX must be mapped to a user distribution group in MorphoManager. If any access levels are not mapped, the user records will fail to synchronize.
- Duress activation is not supported.

# System Preparation

Before you set up this integration, you must complete some basic configuration in your Protege GX and MorphoManager systems.

In Protege GX, you should:

- Bring all controllers and reader expanders online.
- Create all reader expanders and doors that will have biometric readers connected to them.
- Create all required access levels.
- Create users and assign access levels to them.

If you plan to use IDEMIA devices for card reading, you will need use a custom credential type for Protege doors. You may wish to set this up now: see Configuring Card Reading in Protege GX.

In MorphoManager, you should bring all biometric devices online, including a desktop enrollment reader.

# Setting Up Users in MorphoManager

Before installing the sync service, you must set up the templates for user records in MorphoManager.

## User Distribution Groups

User distribution groups determine which biometric readers each user record is downloaded to.

You must create:

- One user distribution group for every access level that includes biometric doors. This must contain all the biometric devices that are used by the access level.
- One additional 'dummy' user distribution group to map to access levels that do not include biometric doors.

To create user distribution groups:

1. Navigate to **Administration | User Distribution Groups**.
2. Click **Add**.
3. Enter the **Name** of this group. For ease of programming, this should be the same name as the corresponding access level in Protege GX. Click **Next**.
4. Select the biometric devices that are needed for the doors in this access level.
5. Click **Finish**.
6. Repeat to create all groups required for biometric doors.
7. Add another user distribution group called Unused Distribution Group or similar.
8. Click **Next**. Do not add any biometric devices. Click **Finish**.

## User Configuration

The user configuration provides the template for user records synchronized from Protege GX.

1. Navigate to **Administration | User Configuration**.
2. Click **Add**.
3. Enter a descriptive name (e.g. Protege GX Users).
4. Set the **Access Mode** to Per User.
5. Set the **Wiegand Profile** to Standard 26 bit.
6. Leave the **User Authentication Mode** as Biometric (1:Many). Click **Next**.
7. Set the finger, face and wave settings as required for your biometric devices.
8. Set the **Preferred Duress Finger** to None.
9. Click **Finish**.

# Synchronizing Protege GX with MorphoManager

After a few initial setup steps, we can install the Protege GX Idemia Sync Service and connect MorphoManager to the BioBridge database.

## Enabling SQL Server Communication

To ensure that SQL Server can communicate with the sync service:

1. Open SQL Server Configuration Manager as an administrator.
2. Under **SQL Server Network Configuration**, select **Protocols for ProtegeGX**.
3. Double click on **TCP/IP**.
4. Ensure that **Enabled** is set to Yes.
5. In the **IP Addresses** tab, scroll down to the **IPAll** section. Ensure that the **TCP Port** is set to 1433.
6. Click **Ok**.
7. Open **Services** as an administrator:
   - Press the **Windows + R** keys.
   - Type **services.msc** into the search bar.
   - Press **Control + Shift + Enter**.
8. Locate SQL Server (ProtegeGX). Right click on the service and click **Restart**.

If the BioBridge database will be hosted on a separate server instance, repeat the above steps on the other instance.

## Creating the SQL Server Login

When you run the sync service installer, it will create a new BioBridge database and pull data from the Protege GX server into it. For this it needs access to the relevant SQL Server instances.

1. Run SQL Server Management Studio on the machine with the Protege GX databases installed.
2. Connect to the ProtegeGX server instance.
3. Right click on the instance name in the Object Explorer and select **Properties**.
4. Make a note of the **Name** displayed on the **General** page.
5. Navigate to the **Security** page.
6. Set **Server authentication** to **SQL Server and Windows Authentication mode**.
7. Click **OK**.
8. In the Object Explorer, expand the **Security** folder and right click on **Logins**.
9. Select **New Login...**
10. Enter a **Login name**.
11. Select **SQL Server authentication**.
12. Enter a secure **Password** and repeat it to confirm.
13. In the **Server Roles** tab, enable the **public** and **sysadmin** roles.
14. Click **OK**.

15. Right click on the instance name and select **Restart**.

    This will also stop some Protege GX services.

16. To ensure that the new user is configured correctly, open a new instance of SQL Server Management Studio.
17. Set **Authentication** to SQL Server Authentication and attempt to log in with the new credentials. You should be able to log in successfully and view the ProtegeGX database.
18. Open the Services manager. Start the **Protege GX Data Service** and **Protege GX Download Service**.

The BioBridge database can be created in the same server instance as Protege GX or a different one. If you plan to use a different server instance, repeat the instructions above to create an SQL login for the other instance.

# Installation

The installer provided by ICT will install the Protege GX Idemia Sync Service, create the BioBridge SQL database and add/edit some records in Protege GX to set up the integration.

It is recommended to run the installer on the Protege GX server to avoid communication issues.

1. Run the installer file provided by ICT.
2. Click **Next**.
3. Select **I accept the terms in the license agreement** and click **Next**.
4. Enter the site information:
   - **Site ID**: The Database ID of the Protege GX site that will be synchronized (1 by default).
   - **Facility Number**: The facility number that will be used for biometric credentials. This can be any number that is not already used for other access credentials on site.
5. Enter the SOAP connection details:
   - **API URL**: The endpoint for the SOAP service WSDL. By default this is: https://<pcname>:8040/ProtegeGXSOAPService/service.svc?wsdl
   - **Username**: The username of any Protege GX operator.
   - **Password**: The password of the Protege GX operator.

   Click **Next**.
6. Enter the Protege GX database details:
   - **Database Server**: The name of the Protege GX server instance that you copied above (see previous page).
   - **Database Name**: The name of the Protege GX programming database (ProtegeGX by default).
   - **User Name**: The name of the SQL login created above.
   - **Password**: The password of the SQL login created above.
7. Enter the details for the new BioBridge database that will be created by the installer:
   - **Database Server**: The name of the server instance where the BioBridge database will be created. This can be the same as the Protege GX server instance, or a different server.
   - **Database Name**: BioBridge.
   - **User Name**: The name of the SQL login created above.
   - **Password**: The password of the SQL login created above.
8. Select the **Complete** setup type and click **Next**.
9. Click **Install**.
10. Once the installation is complete, click **Finish**.

The installer creates the BioBridge database in the specified SQL Server instance and populates it with user data from Protege GX. The sync service will run in the background to synchronize changes and new user records from Protege GX to BioBridge.

After installing the sync service, you will see the following changes in Protege GX:

- A new Idemia download server has been added in **Global | Download server**. Do not change any settings of this record, including the name.
- A new Idemia credential type has been added in **Sites | Credential types**. Do not change the name of this record.
- Every existing user in the system has a credential from the new credential type assigned. The format is:
  - **Facility number**: The number assigned during installation of the sync service.
  - **Credential number**: The user's Database ID + 1.

## Troubleshooting

- **Error message**: "The given value of type String from the data source cannot be converted to type nvarchar of the specified target column."

  **Solution**: At least one user or access level has a name that is too long. Ensure that the **First name** and **Last name** fields (for users) and the **Name** field (for access levels) do not exceed 70 characters.

# Configuring ODBC

The Universal BioBridge integration uses the Open Database Connectivity (ODBC) interface to synchronize data between the BioBridge and MorphoManager databases. Some configuration is required to allow the connection.

1. On the machine with the BioBridge database installed, press the **Windows** key and search for ODBC.
2. Right click on ODBC Data Sources (64 bit) and select **Run as administrator**.
3. Select the **System DSN** tab.
4. Click **Add**.
5. Select **SQL Server**.
6. Click **Finish**.
7. Enter the name BioBridge.
8. In the **Server** field, enter the name of the server instance that the BioBridge database is installed on.
9. Click **Next**.
10. Select **With SQL Server authentication**.
11. Enter the **Login ID** and **Password** that you created for this server instance in Creating the SQL Server Login.
12. Click **Next**.
13. Enable **Change the default database to** and select BioBridge.
14. Click **Next** twice, then **Finish**.
15. Click **OK**.
16. Click **OK**.

# Enabling Universal BioBridge

Once the sync service has been installed, you can enable the Universal BioBridge integration in MorphoManager.

1. Navigate to **Administration | System Configuration**.
2. Select the **BioBridge** tab.
3. Set the **System** to MorphoManager Universal BioBridge.
4. Click **Configure Connection**.

- Set the **DSN** to BioBridge.
- Under **Logon details**, enter the SQL user credentials created above (see page 10).
- Click **OK**.

5. Set the **Grouping Mode** to Manual.
6. Select **Enable Forced User Configuration** and set the user configuration record created above.
7. The **Access Groups** section shows the access levels that have been synced from Protege GX.
   - For each access level that uses biometric doors, select the corresponding user distribution group.
   - For any access levels that do not use biometric doors, select the Unused Distribution Group.
8. Click **Save**.

You can now open the BioBridge Enrollment Client and see the users synchronized from Protege GX.

# Configuring Biometric Devices

Biometric devices are configured in MorphoManager and receive programming and user data over the network. They are also connected to Protege controllers and reader expanders to send credential data, much like card readers.

The supported wiring configurations are:

- OSDP with secure channel
- Wiegand

OSDP wiring is strongly recommended, as it is securely encrypted, provides better feedback to the user and has simpler cabling requirements.

The integration also supports several options for credential reading:

- Biometrics (fingerprint or face)
- ICT cards (MIFARE DESFire or MIFARE Classic)

Any combination of wiring method and reading mode can be used.

## Wiring

First you must connect your IDEMIA devices to the reader ports on Protege controllers and reader expanders, following the RS485 or Wiegand instructions in the relevant IDEMIA installation manual.

Please note:

- You can connect up to two biometric devices to each reader port for entry and exit. In Wiegand configuration, you must wire OUT1 of the exit device to D1 of the other reader port (see the relevant controller or reader expander installation manual for more information).
- To give correct feedback to the user in Wiegand mode, wire LED1 of the biometric reader to L1 (green LED) of the controller or reader expander.

## Setting Up Biometric Devices in MorphoManager

To begin with, we will set up the profiles and basic configuration for biometric devices in MorphoManager.

### Wiegand Profile for Biometrics

The Wiegand profile defines the data format that is sent to the Protege reader expander when the user scans their biometrics. This can be any desired format as long as you program the same format into the Protege GX credential type and set up the fixed element to match the facility number in Protege GX.

This step is required regardless of whether you are using Wiegand or OSDP wiring.

In this document we will use the Standard 26 bit format as a simple example.

1. In the MorphoManager Client, open the **Administration** tab.
2. Navigate to **Wiegand Profiles**.
3. Double click the Standard 26 bit profile.
4. Click **Next**.
5. Select **Fixed** and click **Edit**.
6. Set the **Value** to the facility number of the biometric credentials (selected during sync service installation).

7. Click **Next**.
8. Click **Finish**.

# Biometric Device Configuration

The biometric device configuration section enables you to set up templates for biometric devices connected to MorphoManager. This determines what kinds of credentials they read and what data they send to the Protege reader expander.

## OSDP Configuration

1. Navigate to **Administration | Biometric Device Configuration**.
2. Click **Add**.
3. Enter a descriptive name (e.g. Protege GX OSDP). Click **Next**.
4. Set the **Wiegand Profile** to Standard 26 bit. Click **Next**.
5. Adjust the biometric threshold settings if required, then click **Next**.
6. Leave **Multi-Factor Mode** set to Biometric Only, then click **Next**.
7. Set the following access control mode settings:
   - **Access Control Mode**: Integrated By OSDP
   - **Duress Wiegand Mode**: Disabled

     Protege GX does not support duress activation from IDEMIA biometrics.
   - **OSDP Secure Channel**: Enabled
   - **Baud Rate**: 38400

   Click **Next**.
8. Program any additional settings that are required for your biometric readers.
9. Click **Finish**.

## Wiegand Configuration

1. Navigate to **Administration | Biometric Device Configuration**.
2. Click **Add**.
3. Enter a descriptive name (e.g. Protege GX Wiegand). Click **Next**.
4. Set the **Wiegand Profile** to Standard 26 bit. Click **Next**.
5. Adjust the biometric threshold settings if required, then click **Next**.
6. Leave **Multi-Factor Mode** set to Biometric Only, then click **Next**.
7. Set the following access control mode settings:
   - **Access Control Mode**: Integrated By Wiegand / Panel Feedback
   - **Panel Feedback Mode**: LED Feedback (2 Wire)
   - **Panel Feedback No Response Timeout**: 1000

     If there is no access granted response from the reader expander within 1 second, the biometric device will show an "access denied" message. This value may need to be adjusted after testing the system.
   - **Duress Wiegand Mode**: Disabled

     Protege GX does not support duress activation from IDEMIA biometrics.

   Click **Next**.
8. Program any additional settings that are required for your biometric readers.
9. Click **Finish**.

## Biometric Devices

Finally, you must apply the new templates to the biometric devices:

1. Navigate to **Biometric Device**.
2. Select each biometric device.
3. Select the appropriate **Biometric Device Configuration** as configured above.
4. If the device is connected via OSDP, set the **OSDP Serial Address**. Program this as 0 for an entry reader and 1 for an exit reader.

   You will need this value for setting up the OSDP readers in Protege GX later.

5. Click **Finish**.

# Configuring ICT Cards in MorphoManager

Once the basic biometric device configuration has been set up, we can add card reading for MIFARE DESFire or MIFARE Classic if required.

## Key Policies

To enable IDEMIA readers to read ICT cards, you will need to set up a key policy for the cards you are reading.

Before you begin, ensure that you have all the card details outlined in the Prerequisites.

If you use both MIFARE DESFire and MIFARE Classic cards on your site, combine both sets of instructions below into a single key policy record.

### MIFARE DESFire Key Policy

To create the key policy:

1. Navigate to **Administration | Key Policy**.
2. Click **Add**.
3. Enter a descriptive name (e.g. ICT MIFARE DESFire).
4. Click **Next**.
5. Click **Next**.
6. Click **Set Desfire AID**.
7. Set **Contact Fingerprints Application ID** to the Application ID of the open Wiegand file. Click **Next**.
8. Next to **Contact Fingerprints**, set the **DESFire FID** to 1.
9. Under **Mifare DESFire AES**, enter the **Read Key**.
10. Enable the following settings:
    - Disable Morpho Key Derivation on Master Key
    - Disable Morpho Key Derivation on Application Key
    - Do Not Authenticate With Master Key
11. Click **Next** until you reach the end of the process.
12. Click **Finish**.

### MIFARE Classic Key Policy

To create the key policy:

1. Navigate to **Administration | Key Policy**.
2. Click **Add**.
3. Enter a descriptive name (e.g. ICT MIFARE Classic).
4. Click **Next**.
5. Beside **Contact Fingerprints**, set the following:
   - **Start Write Sector**: 12
   - **Start Write Block**: 1
6. In the **Read/Write Keys** table, select Sector 12, Key A. Enter the read/write key for the ICT open sector.
7. Click **Next** until you reach the end of the process.
8. Click **Finish**.

## Biometric Device Configuration for Cards

You must apply the key policy and some additional custom settings to the biometric device configuration template.

1. Navigate to **Administration | Biometric Device Configuration**.
2. Select a configuration or add a new one.
3. Give the configuration a descriptive name (e.g. Protege GX OSDP with MIFARE DESFire).
4. Set the **Key Policy** to the key policy created above. Click **Next**.
5. Set the **Wiegand Profile** to Standard 26 bit. Click **Next**.
6. Adjust the biometric threshold settings if required, then click **Next**.
7. Set **Multi-Factor Mode** to Custom.
8. Enable **Biometric** and either **Mifare Classic** or **Mifare DESFire AES**, depending on the cards you are using. Click **Next**.
9. Under **Access Control Mode Settings**, enter the settings required for either OSDP or Wiegand configuration (see page 14).
10. Click **Next** until you reach the **Custom Parameters** page.

11. Enter the following custom parameters:

| Name | Value |
|---|---|
| sc.verify_user_id | 3 |
| sc_binary_read.data_length_num_bytes | 4 |
| sc_binary_read.data_length_add_bits | 2 |
| sc_binary_read.data_offset_num_bytes | 1 |
| sc_binary_read.data_offset_add_bits | 0 |
| ucc.per_user_rules | 0 |
| wiegand.custom_format_slot1 | 0000000049435420<br>3334626974000000<br>0000000000000000<br>0000000000000000<br>0000000022000000<br>0000000022000000<br>0000000000000000<br>0000000000000000<br>0000000000000000 |
| wiegand.event_identify_pass | 10 |
| wiegand.event_verify_pass | 11 |

12. Click **Finish**.

If you have added a new biometric device configuration, navigate to **Biometric Device** and assign it to the devices that will be used to read cards.

# Configuring the Biometric Devices in Protege GX

Now we can set up the biometric devices in Protege GX as either OSDP or Wiegand readers. We also need to program the Idemia credential type and enable doors to accept it as a valid credential.

We recommend that you set up and validate biometric reading first before adding the configuration for card reading.

## Idemia Credential Type

The Idemia credential type represents the data that will be sent by the biometric device when it matches a user's credential. For this example we will use the Standard 26 Bit profile.

1. Navigate to **Sites | Credential types** and select the Idemia credential type.
2. In the **Wiegand or TLV format** field, enter the following format code:

```
#Standard26bit__#Variables__A,FACILITY,8,MSB,BIN__B,CARD,16,MSB,BIN__
#Format__PAAAAAAAABBBBBBBBBBBBBBBP__#Parity__EXXXXXXXX................._
_........XXXXXXXXXXXXXXXXO
```

3. Click **Save**.

## OSDP Biometric Devices

Each OSDP biometric device is programmed as a smart reader in Protege GX:

1. Navigate to **Expanders | Reader expanders**.
2. Select a reader expander with a biometric device connected.

3. Set the **Port 1/2 network type** to OSDP.
4. Click **Save**.
5. Navigate to **Expanders | Smart readers**. The software has automatically created two smart readers to represent entry and exit biometric devices.

   You can identify which biometric device each smart reader corresponds to using the **Expander address**, **Expander port** and **Configured address**. The **Configured address** is equivalent to the **OSDP Serial Address** in MorphoManager plus 1 (i.e. 1 for entry and 2 for exit).
6. Delete any smart readers that do not have biometric devices connected (e.g. delete any exit readers that are not used).
7. Give each smart reader a descriptive name (e.g. Front Door IDEMIA Sigma Reader).
8. In the **Reader** tab, set the **Reader one format** to Custom credential.
9. Set the **Reader one location** to Entry or Exit.
10. Select the **Reader one door** that this device will control.
11. Click **Save**.
12. Return to **Expanders | Reader expanders**. Right click on the reader expander and select **Update module**.
13. Right click on the reader expander and select **Activate OSDP install mode**.
14. Repeat to program all other biometric devices.

## Wiegand Biometric Devices

1. Navigate to **Expanders | Reader expanders**.
2. Select a reader expander with a biometric device connected.
3. Set the **Port 1/2 network type** to Wiegand.
4. If there are two biometric devices connected for entry and exit, enable **Multiple reader input port 1/2**.
5. In the **Reader 1** tab, set the **Reader 1 format** to Custom credential.
6. In the **Reader 2** tab, set the **Reader 2 format** to Custom credential.
7. Click **Save**.
8. Wait for the changes to be downloaded to the controller, then right click on each reader expander and select **Update module**.
9. Repeat for all other reader expanders with biometric devices connected.

## Door Types

To program a door type for biometric reading only:

1. Navigate to **Programming | Door types**.
2. Add a new door type called IDEMIA Biometric.
3. Set the **Entry reading mode** to Custom.
4. Under **Entry credential types**, add the Idemia credential type.
5. Repeat for the **Exit reading mode** if exit readers are required.
6. Click **Save**.

Finally, set the door types for your doors:

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

3. Click **Save**.

We recommend that you validate biometric reading (see next page) before setting up card reading (if applicable).

# Configuring Card Reading in Protege GX

Some additional configuration is required in Protege GX for sites that are using card reading on biometric devices.

Be aware that it is not possible to use the default Protege GX card formats alongside biometric reading on IDEMIA devices. For consistency, the best thing to do is set up a custom credential type for ICT cards and use it for all readers across the site, both biometric devices and standard card readers.

These instructions are only required if you are reading cards on IDEMIA devices.

## ICT Card Credential Type

To set up a credential type for ICT cards:

1. In **Sites | Credential types**, add a new ICT Card credential type.
2. In the **Wiegand or TLV format** field, enter the format code for your cards. The most common formats for ICT cards are HID 26 bit and HID 34 bit:
   - `#HID26bit__#Variables__A,FACILITY,8,MSB,BIN__B,CARD,16,MSB,BIN__ #Format__PAAAAAAAABBBBBBBBBBBBBBBP__#Parity__ EXXXXXXXX.................__.........XXXXXXXXXXXXXXXXO`
   - `#HID34bit__A,FACILITY,16,MSB,BIN__B,CARD,16,MSB,BIN__ PAAAAAAAAAAAAAAAABBBBBBBBBBBBBBBP__EXXXXXXXXXXXXXXX.................__.................XXXXXXXXXXXXXXXXO`
3. Click **Save**.

If your cards use a different Wiegand format, program it following the instructions in Application Note 276: Configuring Credential Types in Protege GX.

## Card Readers

You must configure all standard ICT or third-party card readers on site to recognize the ICT Card custom credential type programmed above.

For ICT RS-485 readers:

1. Navigate to **Expanders | Reader expanders** and select each reader expander with standard card readers connected.
2. Set the **Port 1/2 network type** to Wiegand temporarily.
3. In the **Reader 1** tab, set the **Reader 1 format** to Custom credential.
4. Repeat in the **Reader 2** tab.
5. Return to the **General** tab and change the **Port 1/2 network type** back to ICT RS485.
6. Click **Save**.
7. Wait for the changes to download to the controller, then right click on the reader expander and select **Update module**.

For OSDP readers:

1. Navigate to **Expanders | Smart readers** and select each smart reader with a standard card reader connected.
2. In the **Reader one** tab, set the **Reader one format** to Custom credential.
3. Click **Save**.

For Wiegand readers:

1. Navigate to **Expanders | Reader expanders** and select each reader expander with standard card readers connected.
2. In the **Reader 1** tab, set the **Reader 1 format** to Custom credential.
3. Repeat in the **Reader 2** tab.
4. Click **Save**.
5. Wait for the changes to download to the controller, then right click on the reader expander and select **Update module**.

## Door Types

You will also need a door type for reading the custom credentials:

1. Add a new door type called ICT Card.
2. Set the **Entry reading mode** to Custom.
3. Under **Entry credential types**, add the ICT Card credential type.
4. Repeat for the **Exit reading mode**.
5. Click **Save**.

You can program additional door types for different combinations of credentials:

| Door Type | Fallback door type | Entry/Exit reading mode | Entry/Exit credential types |
|---|---|---|---|
| Card and Biometric | | Custom | Idemia<br>ICT Card |
| Card or Biometric | ICT Card | Custom | Idemia |

Once you have created all the door types, navigate to **Programming | Doors** and select the **Door type** for each door.

# Validating Devices

Any users that were already programmed in Protege GX before you installed the sync service are now available to enroll. Open the **BioBridge Enrollment Client** and follow the instructions to enroll users with a desktop enrollment device.

To test each biometric device, open a status page or floor plan in Protege GX. Scan a user's finger or face, or badge their card.

If access is granted, you should see:

- The door unlocks
- The biometric device displays an "Access Granted" message
- Protege GX displays an "Access Granted" event in the event log

If access is denied due to a schedule, expired access level or similar:

- The biometric device displays an "Access Denied" message
- Protege GX displays an event that indicates why access is denied

If the user never has access to this door, the biometric reader will fail to identify the user.

# Adding and Syncing Users

The synchronization rules are as follows:

- Only one Protege GX site is synchronized.
- Only users with **both** an Idemia credential and an access level are synchronized to the BioBridge database.

To add a new user and synchronize them to BioBridge:

1. In **Users | Users**, click **Add**.
2. Enter the user's **First name** and **Last name**.

   Ensure that these fields do not exceed 70 characters.
3. In the **Access levels** tab, add one or more access levels that grant access to biometric devices.
4. Program any other required settings.
5. Click **Save**.
6. In the **General** tab, scroll down to the **Credentials** section.
7. Enter the Idemia credential in the format **FacilityNumber:CredentialNumber** (e.g. 100:9).
   - The Facility Number should match the one entered during installation of the sync service.
   - The Credential Number is the user's Database ID + 1. You can see the Database ID in the user list.
8. If you are using the ICT Card credential type, enter the facility and card number separated by a colon (e.g. 20453:121).
9. Click **Save**.

The new user will sync to the BioBridge database and become available to enroll in the BioBridge Enrollment Client.

Because BioBridge only refreshes its user cache once an hour, it may take up to an hour for new users in Protege GX to appear in the BioBridge Enrollment Client. Changes to existing users will be passed through immediately.

## Adding Access Levels

When you add a new access level after synchronizing the integration, you must map it to a user distribution group in MorphoManager. If you do not map all access levels, the integration will not sync.

If the access level uses biometric doors:

1. In MorphoManager, navigate to **Administration | User Distribution Groups**.
2. Click **Add**.
3. Enter the **Name** of this group (ideally the same as the access level's name). Click **Next**.
4. Select the biometric devices that are needed for the doors in this access level.
5. Click **Finish**.
6. Navigate to **System Configuration**, **BioBridge** tab.
7. Under **Access Groups**, map the new access level to the matching user distribution group.
8. Click **Save**.

If the access level does not use biometric doors:

1. In MorphoManager, navigate to **Administration | System Configuration**, **BioBridge** tab.
2. Under **Access Groups**, map the new access level to the Unused Distribution Group.

3. Click **Save**.

# Release History

**Version 1.0.0.0**

Initial release of the Protege GX Idemia Sync Service.

**Version 1.0.2.0**

- Fixes for SOAP certificate validation.

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