



PRT-GX-DB-SYNC

ICT Data Sync Service

Integration Guide



The specifications and descriptions of products and services contained in this document were correct at the time of printing. Integrated Control Technology Limited reserves the right to change specifications or withdraw products without notice. No part of this document may be reproduced, photocopied, or transmitted in any form or by any means (electronic or mechanical), for any purpose, without the express written permission of Integrated Control Technology Limited. Designed and manufactured by Integrated Control Technology Limited, Protege® and the Protege® Logo are registered trademarks of Integrated Control Technology Limited. All other brand or product names are trademarks or registered trademarks of their respective holders.

Copyright © Integrated Control Technology Limited 2003-2026. All rights reserved.

Last Published: 27-Feb-26 10:30 AM

Contents

Introduction	5
Use Cases	5
How it Works	6
Prerequisites	6
Operator Permission Requirements	7
Installing the Data Sync Service	8
Upgrading the ICT Data Sync Service	8
Security Configuration	9
Using a Third-Party Certificate for SOAP	9
Using a Self-Signed SSL Certificate for SOAP	10
Setup and Configuration	12
Data Target	12
Sync Options	13
Data Mapping	14
Data Source	14
Field Mapping	16
Target Field	16
Unique Field	16
Source Column	17
Original Value	17
Advanced Configuration	17
Result Value	19
Syncing Data to the Target System	20
Service Logs	21
Setting the Minimum Log Level	21
User Import Reference	22
User Name	22
User Start and Expiry Date	23
User PINs	24
Access Levels	25
Facility Code and Card Number	28
Credential Types	30
Custom Fields	31
Custom Field Formatting	31

Record Groups	34
User Photos	35
Importing to a Specific Site	37
Importing Schedules	38
Importing Controllers	40
Field Mapping Between Data Sync and Protege GX	41
Error Messages	50
Configuration Errors	50
Popup Messages	52
Import Errors	52
SOAP Error Codes	54
Release History	56
Disclaimer and Warranty	58

Introduction

The ICT Data Sync Service combines the power of Protege GX's enterprise level integrated access control, intrusion detection and building automation system with external data sources. The ability to synchronize data between the systems reduces management time and administration, while providing single data entry and enhancing accuracy and efficiency.

The ICT Data Sync Service incorporates the Protege GX SOAP Service to facilitate importing the required data. Using the Protege GX SOAP Service enables access to the power and functionality of Protege GX.

Ideally suited for a variety of applications, including 24-hour gym and fitness centers, sports clubs and facilities, university student databases, human resource systems and more, the data sync service provides a flexible approach to exchanging data between systems, allows you to synchronize user data and events, and makes automating membership and temporary visitor access simple.

If you were previously using the Protege GX Data Sync Service, you can easily upgrade to the ICT Data Sync Service using the Data Sync Upgrade Tool during initial configuration. For more information, refer to the [ICT Data Sync Service Upgrade Guide](#) available in the release package. We strongly advise that you read that document thoroughly before proceeding with the upgrade.

Use Cases

Visitor Management

The data sync service is ideal for administering temporary access for visitors, including tradespeople and contractors. Details are extracted from the visitor management system and are used to grant access for the duration the visitor will be on site.

HR Systems

HR databases store a wealth of user data including roles, departments and hours of work. Using data sync, this information can be used to create user records and assign the relevant access levels. This reduces data entry and administration time, since you no longer need to manage and update two separate databases.

Gyms and Fitness Centers

Many fitness centers have websites where members can sign up online. Data sync can use this data to automatically create user records, including access details and membership period. The site may also allow members to book facilities such as a squash court or private sauna. Data sync can manage these bookings by assigning a temporary additional access level for the duration of the booking to allow access to the area.

Freight / Delivery Services

In situations where delivery trucks are required to enter a controlled gate, data sync can be used to automate temporary visitor access for truck and courier drivers. Drivers won't have access cards, so the service is used to take booked jobs from the database and create users with PINs that match the job number. Access levels are assigned with an expiry date that matches the expected time on site.

University Campuses

Data sync can be used to generate access for students based on information stored in a student management system. Access levels are assigned to match the duration of the course the student is enrolled in and grant access to the areas they need entry to. When the study period ends, access is removed automatically.

How it Works

Data is extracted from the third party system and saved to a shared network folder.

Once configured, the data sync service monitors this folder and automatically imports the relevant data into Protege GX, creating records (including users, access levels, areas, doors, schedules, controllers and so on) for each matched entity. If information in the import file changes, the service updates the record in Protege GX.

Prerequisites

It is recommended that you use the latest versions of all software when using the ICT Data Sync Service. The minimum versions required are outlined below.

Software Requirements

Software	Version	Notes
Protege GX software	4.2.214 or higher	
ICT Data Sync Service	2.0.0.0 or higher	
Protege GX SOAP Integration Service	1.5.0.19 or higher	If using Protege GX SOAP version 1.5.0.17 only users and schedules can be synced.
* If using a version of the ICT Data Sync Service prior to 2.0.6.3 and a version of the Protege GX SOAP Service prior to 1.5.0.27, a Protege GX client connection must be available for use by the service.		

For information on how to install and configure the Protege GX SOAP Service, refer to the [Protege GX SOAP Service Installation Guide](#)

Licensing Requirements

License	Order Code	Notes
ICT Data Sync Service License	PRT-GX-DB-SYNC	1 license required per Protege GX server

Operator Permission Requirements

To access Protege GX data records, the data sync service requires a Protege GX operator login. This operator must meet specific minimum access permissions to provide the data sync service with access to the required Protege GX data. Without the correct access permissions, imports will fail.

You can create operators in **Global | Operators** and add roles with custom access permissions in **Global | Roles**. For more information and instructions, see Application Note 191: Programming Operator Roles in Protege GX.

It is recommended that a Protege GX operator is added solely for importing through data sync.

Minimum Data Sync Service Operator Permissions

- Read-only access to the **System** table.
- Read-only access to the site (or sites) the data sync is expected to import to.
- Full access to any record types the data sync is expected to import.
- Read-only access to any tables the data sync will reference.
(e.g. If assigning access levels to users, read-only access to the access levels table is required.)

Note: If the data sync service is importing users with a PIN assigned, the service operator requires full access to the **Generate PINs** option (**Sites | Security levels**).

Installing the Data Sync Service

1. Run the ICTDataSyncService.msi file to launch the install wizard.
2. Click **Next** to continue.
3. Select whether it is to be installed for everyone who uses the PC or just your user, then click **Next** to install to the default location (C:\Program Files (x86)\Integrated Control Technology\Data Sync Service).

If the service is to be installed in a different location, click **Browse** and navigate to the required directory.

4. Click **Next** to begin the installation.
5. Once the installation is complete, click **Close**.

Upgrading the ICT Data Sync Service

To upgrade the data sync service to a new version, simply uninstall the existing service and install the new version.

1. Before you begin, take a backup of your Protege GX database:
 - In Protege GX, navigate to **Global | Global settings**.
 - Ensure that the **Backup path** is set correctly.
 - Click **Backup now**.
2. In the Windows settings, navigate to the **Apps & features** section.
3. Locate the ICT Data Sync Service in the list of apps.
4. Click on the app and click **Uninstall**.
5. When the service has been uninstalled successfully, run the new installer provided by ICT.

Security Configuration

To achieve a secure connection between the Protege GX SOAP Service and the ICT Data Sync Service you must use a trusted SSL certificate.

A self-signed SSL certificate is automatically generated during installation of the SOAP service. However, this certificate is not inherently trusted by other computers and applications, so the connection may be refused or flagged as insecure. There are two methods for achieving a trusted connection:

- **Recommended:** Obtain and install a third-party certificate issued by a trusted certificate authority, such as:
 - **GoDaddy:** <https://www.godaddy.com/web-security/ssl-certificate>
 - **Network Solutions:** <https://www.networksolutions.com/>
 - **RapidSSL:** <https://www.rapidsslonline.com/>
 - **Let's Encrypt:** <https://letsencrypt.org/>
- Import a self-signed certificate into the trusted certificate store of each computer that will connect to each application. This can be either the certificate which was automatically generated during installation, or a custom self-signed certificate.

Using a Third-Party Certificate for SOAP

Once you have obtained a third-party certificate from a trusted certificate authority, you must install it in the **ProtegeGX** site in Internet Information Services (IIS) Manager. This secures the connection between the SOAP service and other applications.

This is the recommended method for securing the SOAP service on live sites.

Completing the Certificate Request

1. Open IIS Manager by pressing the **Windows + R** keys to open the **Run** prompt, then entering **inetmgr**.
2. In the **IIS** section, double-click **Server Certificates**.
3. From the **Actions** panel on the right, click **Complete Certificate Request...**
4. To locate your certificate file, click the ellipsis [...] button.
5. Select *.* as the file name extension.
6. Select the certificate and click **Open**.
7. Enter a **Friendly name** for the certificate file, then click **OK**.

Binding the Certificate to the ProtegeGX Site

1. In the **Connections** panel on the left of IIS Manager, expand the server where you installed the certificate.
2. Click the drop-down arrow next to **Sites** and select the **ProtegeGX** site.
3. In the **Actions** panel, click **Bindings...**
4. Select the https binding (port 8040) and click **Edit...**
5. Set the **SSL certificate** to the certificate you just installed. Click **OK**.
6. You will see a warning about overwriting the existing certificate. Click **Yes**.
7. Close the site bindings window and the IIS Manager window.

The SSL certificate installation is complete.

When the SOAP service is upgraded, the certificate will be reset to the default. Repeat the steps above to rebind the custom certificate.

Using a Self-Signed SSL Certificate for SOAP

As an alternative to a third-party certificate, you may use a self-signed certificate for the SOAP service. As self-signed certificates are not inherently trusted by other computers and applications, it is necessary to import the certificate to the trusted root store of each other computer that will connect to the SOAP service directly.

The instructions below cover creating a custom self-signed certificate, binding it to a site, and importing it as a trusted certificate on other computers.

For live sites, it is recommended that you use a third-party certificate or a trusted certificate issued by your IT department.

Creating and Exporting a New Self-Signed Certificate

There are multiple methods to create a self-signed certificate. The steps below describe how to create a certificate using IIS Manager. Alternatively, you may create a certificate using a utility such as [OpenSSL](#), or a certificate may be supplied by your IT department.

1. Open IIS Manager by pressing the **Windows + R** keys to open the **Run** prompt, then entering **inetmgr**.
2. In the **IIS** section, double-click **Server Certificates**.
3. From the **Actions** panel on the right, click **Create Self-Signed Certificate...**
4. Enter a name for the certificate.
5. Set the certificate store to **Personal**.
6. Click **OK**. Your new certificate will be added to the list.
7. Double-click on the new certificate to view it.
8. Navigate to the **Details** tab and select **Copy to File...** The certificate export wizard will open.
9. Complete the instructions in the wizard, selecting these options:
 - Do **not** export the private key.
 - **Format**: DER encoded binary X.509 (.CER)
 - Specify the name and location where you want to export the certificate.
10. Click **Finish** to complete the export.

Binding the Certificate to the ProtegeGX Site

1. In the **Connections** panel on the left of IIS Manager, expand the server where you installed the certificate.
2. Click the drop-down arrow next to **Sites** and select the **ProtegeGX** site.
3. In the **Actions** panel, click **Bindings...**
4. Select the https binding and click **Edit...**
5. Set the **SSL certificate** to the certificate you just installed. Click **OK**.
6. You will see a warning about overwriting the existing certificate. Click **Yes**.
7. Close the site bindings window and the IIS Manager window.

When the SOAP service is upgraded, the certificate will be reset to the default. Repeat the steps above to rebind the custom certificate.

Importing the Certificate to Another Computer

This section must be completed on each computer that will connect directly to the SOAP service.

1. Open the certificate manager by pressing **Windows + R**, then entering **certlm.msc**.
2. Browse to **Certificates - Local Computer > Trusted Root Certification Authorities > Certificates**.

3. Right click on the Certificates folder and select **All Tasks > Import....** This will open the certificate import wizard.
4. Click **Next**.
5. Browse to and select the certificate file that you exported.
6. Select the option to **Place all certificates in the following store** and enter Trusted Root Certification Authorities as the certificate store.
7. Click **Finish** to complete the import.

Setup and Configuration

To run the ICT Data Sync Service Configuration Tool, double click on the ICT Data Sync Service shortcut on the desktop. Alternatively, navigate to the install location (if you accepted the defaults during installation, this will be C:\Program Files (x86)\Integrated Control Technology\Data Sync Service) and open the DataSyncServiceConfig.exe file.

When opening the application for the first time, you will be presented with the following message: "If you were previously using the Protege GX Data Sync Service (version 1.X.X) and wish to import the previous settings into the ICT Data Sync Service, click YES. Alternatively, if you wish to use the ICT Data Sync Service from new, click NO."

If you are upgrading from the Protege GX Data Sync Service (1.X.X) to the ICT Data Sync Service (2.X.X), refer to the ICT Data Sync Service Upgrade Guide available in the release package for more information on the upgrade tool.

Click **NO** to continue to the configuration tool.

Data Target

The **Data Target** section contains details on the system being synced to.

- **Target System:** The system that the data is to be imported to. This should be Protege GX.
- **SOAP Server Address:** The Protege GX SOAP Service address. This must be the HTTPS endpoint for the SOAP service, by default:

```
https://<pcname>.<domainname>:<HTTPSPORTNUMBER>/ProtegeGXSOAPService/Service.svc
```

The default HTTPS port is 8040. The computer's name and domain name must be used instead of localhost.

- **Data Server Address:** If the data sync service is installed on a different machine to the Protege GX Data Service, this field must contain the IP address and port number of the Protege GX Data Service, separated by a colon (e.g. 10.2.14.15:8005).
 - **IP Address:** If SOAP is installed on the local machine you can use localhost before the colon. If SOAP is installed on a different machine, use the IP address of the machine the SOAP service is installed on.
 - **Port Number:** The Protege GX Data Service Net TCP port number. The default port used during installation of Protege GX is port 8000.

This field does not need to be configured when using ICT Data Sync Service version 2.0.6.3 or higher with Protege GX SOAP version 1.5.0.30 or higher, as all communication with Protege GX is configured within the SOAP service.

- **Username:** The operator username required to access the target system (by default this is set to admin).

Operators require specific minimum permissions for the necessary data sync access (see page 7). It is recommended that a Protege GX operator is added solely for importing through data sync (and that this operator is assigned a secure password). This ensures that you can easily identify the records that have been added/modified/deleted by data sync.

- **Password:** The password associated with the **Username** entered above.
- **Site:** The site that the records are to be imported to. All sites that have been added in Protege GX will be available in the dropdown list.

If the records in the import file(s) are to be imported to more than one site you can override the global **Site** selection by mapping the SiteID field for each record type. This allows different records to be imported to multiple sites within a single sync.

The remaining fields in the **Configuration** window are disabled until a valid **Server Address, Username, Password** and **Site** have been entered.

Sync Options

The **Sync Options** section allows you to configure how data sync synchronizes the selected import file.

- **Resynchronize Every <value> <units>**: Data is synchronized repeatedly for the selected time interval (the default is 1 minute). After a sync has finished the service will wait for the selected time to elapse before restarting. If any changes have been made in the import file the updated data will be synced to the target system when the service restarts.
- **Delete Import File When Complete**: When enabled, the import file is deleted after every row in the file is synced successfully.
 - **Move Files on Error**: When this option is enabled, files that generate an error during the sync will be moved to a separate file directory, so that they will not be resynced until the operator addresses any problems.
- **Import Expired Records**: When enabled, records are imported to the target system even if the mapped end date is in the past.
- **Delete Expired Records**: When enabled, records that have expired (based on the end date in the import file) are deleted from the target system.

For examples of usage of the **Import Expired Records** and **Delete Expired Records** options, refer to the User Start and Expiry Date section (see page 23).

- **Enable Event Logging**: When enabled, events are logged in the Windows Event Viewer and written to a text file in the logs folder of the installation directory.
- **Open Log Folder**: Click this button to open the log file directory.
- **Log Errors Only**: When enabled, only errors are logged. Events at an 'Information' or 'Warning' level will not be logged.
- **Enable Time Zone**: This option is only required when the Protege GX server is located in a different time zone to where the data sync service is installed. If this is the case, enable this option and select the time zone in which the server is located.

Data Mapping

The **Data Mapping** section allows you set which type of record will be imported to the target system.

- **Record to Sync:** Select which type of Protege record is being imported to the target system.
 - Multiple record types can be configured to import within a single sync by saving one configuration, then changing the option selected in this field to enter another configuration. Ensure the current mapping is saved before proceeding to the next.
 - Different record types are synced in the order in which they are saved. If multiple record types are being synced and the data in one record type references another, care must be taken in the order in which each record type is saved. For example, if both access levels and users are configured for import, the access levels must be saved before the users so that the access levels exist in Protege GX before the user sync begins.

If using Protege GX SOAP version 1.5.0.17 only users and schedules can be synced.

Data Source

The **Data Source** section defines the file(s) used for import.

- **File Directory:** Defines the location of the import file(s). Click on the ellipsis button and navigate to the path where the import files are located.
- **Import File:** When enabled, this option is used to import a single file. This field can accept a regular expression, provided there is a double slash (//) on both sides of the regular expression.

To import all files in a particular file directory, leave the **Import File** setting disabled.

- **File Format:** Defines how the file is to be split into individual records and fields.
 - **Delimited:** A file where each value within the import file is separated by some delimiter (symbol). For example, a CSV file is a delimited file where the column delimiter is a comma.
 - **Row Delimiter:** The character that separates rows in the import file.

To view the row delimiters, you can open the file with Notepad++ and navigate to **View | Show Symbol | Show All Characters**. The row delimiter will be shown at the end of each row. Common line ending options are provided in the dropdown menu; however, any row delimiter can be entered into this field.
 - **Column Delimiter:** The character that separates columns in the import file. If data is being imported from a CSV, select {Comma}.
 - **Fixed Width:** A file where each field is a fixed width and the column width is measured in units of characters.
 - **Row Delimiter:** Same as above for the delimited format.
 - **Column:** A series of numbers separated by commas, where each number represents the length of each respective column in the import file.
- **Text Qualifier:** If the import data contains a text qualifier, enable this option and select the qualifier from the dropdown menu. This option is only available for files using a delimited file format. A text qualifier is placed around a field so that the content within the qualifier is interpreted as a single field. For example, the field "4 Example Avenue, Erewhon, Metropolis, 1234" contains double quotation marks as the text qualifier so that the entire address is interpreted as one field and is not separated into several fields by the commas.
- **Group Data Before Import:** When enabled, data is grouped by the **Unique Field**. This option should be used when the import file contains entries for the same record in one or more rows. For example:

```
Unique Field,Name,Access Level
100,Joe Bloggs,Office
101,John Doe,Office
100,Joe Bloggs,Warehouse
```

The record with a **Unique Field** of 100 is entered twice in the import file, with a different access level in each row. To import both access levels for this user (rather than overwriting the first access level), enable the **Group Data Before Import** option.

This option cannot be used in conjunction with the **Validate Against Last Sync** option.

- **Start Import:** If you do not need to import the entire file, enable this option to skip data at the beginning of the file.
 - **At Row:** The import will include data in the specified row number and all of the rows that follow.
 - **After:** The import will exclude data before and within the specified text and only sync the data that follows.
 - **With:** The import data will begin at the line where the specified text is found.
- **End Import:** If you do not wish to import the entire file, enable this option to skip data at the end of the file.
 - **Before:** End the import before the specified text is found.
 - **With:** End the import at the location where the specified text is found.
- **Skip Rows That Contain:** When enabled, this option allows you to skip rows within the import file. This option is useful when the import file contains comments. Once enabled, enter the character that the row begins with (e.g. a hash). This field can also accept a regular expression.
- **Validate Import Files Contain:** When enabled, data sync validates that the text entered in this field is present in the import file. If this check fails the data is not imported and an event is logged.
- **Validate Against Last Sync:** When enabled, the data that is currently being imported is compared to the data that was imported on the last sync. This results in a faster sync process because every time the service restarts, any rows in the import file(s) that have not been modified are not processed.

When this option is enabled, records that are deleted from Protege GX will not be re-imported, even if the record remains in the import file. This option cannot be used in conjunction with the **Group Data Before Import** option.

- **Delete Sync History:** Click this button to delete the sync history generated by the **Validate Against Last Sync** option. This allows you to perform a fresh import of the entire dataset.
- **Delete Records Not Present in Import File:** When enabled, if there are any records that were in the import file on the previous sync but not in the current sync, these records are deleted from Protege GX. This provides a simple solution for removing outdated records.

If the data source is directed to a different file which has some users missing, those users will not be deleted from Protege GX. Instead of redirecting the data source, update the same file with the changes you need.

Field Mapping

The field mapping panel enables you to configure which line of the import data maps to a specific field in the target system.

The most efficient way to map data is to:

1. Select a **Target Field**.
2. Check the **Unique Field** option for the field that is to be used to identify the record.
3. Select the corresponding **Source Column** which contains the data for the assigned field.
4. Configure any **Advanced** options if required.

Target Field

The **Target Field** is the field in Protege GX that the specified column in the import file will be imported to. Click on a blank button in the **Target Field** column to begin.

- The **Target Fields** window is populated with fields based on the **Record to Sync** and are retrieved from the SOAP service.
- If there is a column in the import data that you do not wish to import, leave the **Target Field** blank. If you have already chosen a **Target Field** but do not wish to import it to the target system, click **Do Not Import** and it will be removed.
- You cannot select fields ending in GroupData as they are only group headings for a set of data.
- Fields ending in GroupDataData select an entire group of data and you cannot select the linked fields individually. If there is a field within the selected group that is not required for import, set the corresponding **Source Column** value to Skip.
- Data sync does not allow you to select the same field more than once, unless it is a field ending in GroupDataData. These fields can be mapped multiple times as they allow assignment of a record in a one-to-many relationship (e.g. one user can be assigned many access levels).

Users can be assigned the same access level twice if the schedule is different. In this case, enable the **Use This Field As The Group Data Identifier** option in the advanced configuration (see next page) on both the **AccessLevel** and **Schedule** fields. Failing to do so will result in only the second instance of the access level being assigned to the user.

Delete Record

- The **DeleteRecord** field deletes the record from the target system when prompted by the import file. For example, the import file may contain the following row:

101,Jay Gatsby,false

If the entry in the third column is changed to true (in lower case) the record is deleted from the target system when the service restarts.

- If this field does not contain a true or false (e.g. contains a Y or N or is in upper case) you must use a conversion. For information on **Conversions**, refer to the Advanced Configuration section (see next page).

To configure a conversion for the **DeleteRecord** field you only need to map the field that results in true as data sync searches the file for true and if it is not found it is assumed the record is not to be deleted.

- If a column mapped to the **DeleteRecord** field contains a true flag on the first sync the record will not be imported and a record already deleted event will be logged.

Unique Field

Each record type must contain a minimum of one **Unique Field** for the import to be successful.

- The **Unique Field** is used by the service to identify which record is to be added/updated/deleted.
- By default this option is enabled on:

- **CustomField1 (for users):** For files that have been exported from third-party systems there is often a unique numeric ID associated with each user that can be used to populate this field.
- **Name (for every other record type):** When importing doors for example, it is convenient to refer to each door by its name.
- You can select more than one **Unique Field**. This configuration would be used in a situation where a single field cannot be guaranteed to be unique, so multiple fields together must be used to identify the record. For example, when syncing areas there may be areas with the same name that are linked to different controllers. In this scenario **Unique Field** should be enabled on both the **Name** and **ControllerID**.

Any records where the **Unique Field** contains a duplicate in the import file will result in the record being overwritten and an event being logged. Only the last instance of the record with that unique field will remain in the target system once the sync is complete.

Source Column

This is a numeric field that corresponds to each column in the import file.

- Set the **Source Column** to the numeric value for the column that corresponds to the data for the associated **Target Field**.
- You can set a default value for data that does not exist in the import file by:
 - Selecting a **Target Field**.
 - Setting the **Source Column** to Not From Import File.
 - Setting the **Default Value** (in the **Advanced Configuration** window) to the value to be assigned to that **Target Field** for every record.
- Setting the **Source Column** to Skip will result in that field being ignored during the sync process.

Original Value

This column is read-only and provides a preview of the data in the import file to ensure the **Target Field** is mapped to the correct **Source Column** or **Default Value**.

Advanced Configuration

To open the advanced configuration window, click the ellipsis [...] button in the **Advanced** column. It provides a series of options for configuring date/time fields, grouped data and conversions.

You cannot open the advanced configuration window before selecting a **Target Field** and **Source Column**.

Default Value

This field is used to sync data that is not in the import file and it is assigned to every record that is synced.

To configure a default value for a field:

1. Select the **Target Field** to import the data to in Protege GX.
2. Set the **Source Column** to Not From Import File.
3. Set the **Default Value** to the required data.

This field is often used to sync custom fields where the **CustomFieldID** has its **Default Value** set to the name of an existing custom field, or credential types where the **UserCredentialType** has its **Default Value** set to the name of an existing credential type in Protege GX. This allows the data in the import file to be assigned to a custom field or a credential type that may not be relevant to the third-party system that the file is exported from.

Pattern

This field uses a regular expression to handle special cases in the import data. For example, a field that is padded with characters or text such as F UniqueID ^1677^^ requires a **Pattern** to strip the unnecessary characters from the data.

Conversion

This option is often used when the import data contains a field that data sync is not expecting, and is most often used to set the state of a checkbox or assign a value to the **DeleteRecord** field.

Where a Boolean value is being assigned, data sync expects a true or false result. **This is case sensitive.**

For example, if the **DisableUser** column in the import file contains a Y this must be converted to true. In the **Original Value** field, enter the data contained in the import file and in the **Resulting Value** field enter the value that data sync is expecting. Some common conversions that may need to be configured include:

Original Value	Resulting Value
Y	true
Yes	true
Delete	true
1	true
N	false
No	false
0	false

Group Data Options

Use This Field as the Group Data Identifier

This option must be enabled for the field that should be used to uniquely identify a linked record, and is used to determine whether to update a record or assign a new record on resync. Consider the following example:

- Assigning Credentials to a User.

If the value of a user credential is modified in the import file:

- To update an existing credential for a user, the **Use This Field as the Group Data Identifier** option should be enabled for the UserCredentialType field.
- To assign a new credential to a user, the **Use This Field as the Group Data Identifier** option should be enabled for both the UserCredentialType and UserCredential fields.

Grouping Type

This section handles import data where a single column contains data that is to be imported to more than one field. In the **Delimiter** fields you can select an option from the dropdown or enter the symbol directly.

These settings are only available for target fields that belong to a GroupDataData field.

There are three different **Grouping Type** options:

- Singular Data:** Default configuration where the column in the import file maps to a single **Target Field**.
- Paired Data:** Assigns multiple records that are mapped to a single **Target Field**.

For example, if a column contains the data **Office;Warehouse** where both the Office and Warehouse access levels are to be assigned to a user:

- In the advanced data configuration window for the **UserAccessLevel** field, the **Grouping Type** should be set to Paired Data and the **Pair Delimiter** should be set to a semicolon character. When the user is

imported to Protege GX they will be assigned both access levels.

- **Grouped Paired Data:** Assigns multiple records that are mapped to one or more **Target Fields**.

If a column contains the data **1:15;true;1:16;true** where both cards are to be assigned to a user:

- In the **Advanced Data Configuration** window for the **FamilyNumber**, **CardNumber** and **CardDisabled** fields, the **Grouping Type** should be set to Grouped Paired Data, the **Group Delimiter** should be set to a semicolon character, and the **Pair Delimiter** should be set to a colon character. Additionally:
 - For the **FamilyNumber**, the **Index** should be set to 1.
 - For the **CardNumber**, the **Index** should be set to 2.
 - For the **CardDisabled**, the **Index** should be set to 3.

Find ID

Enable this option if the data in the associated **Target Field** is another record in Protege GX and the value supplied is the **Name** of the record to be assigned. For example, if assigning an access level to a user, the **UserAccessLevel** would need this option enabled with the dropdown set to **Access Levels**. This tells the data sync service to locate an access level by the **Name** provided in the data and assign it to the user record being synced.

If the value provided is the Database ID of the access level, this option does not need to be configured.

Date Time Options

- **Date and Time Format:** If the field contains date/time data, enable the **Date and Time Format** option and enter the date/time format of the data in the import file. The dropdown provides a few common date/time configurations; however, if the format contained in your import data is not displayed, simply enter it.
- **Use This Field for Expiry Date Check:** This option must be enabled when the **Import Expired Records** or **Delete Expired Records** options are enabled. This tells data sync to check the date/time data in this field to calculate if the record is expired, and determine if the record is to be imported or deleted.

Data Preview

Provides a preview of the original and resulting data if any configuration has been set up that affects the data in the selected field.

For example, if a **UserAccessLevel** has been configured as Paired Data, the following will be displayed:

- **Original Value:** Office;Warehouse
- **Resulting Value:** Office || Warehouse

Where the pipe character denotes that the data has been split correctly.

Result Value

This column is a read-only field that provides a preview of the data that will be imported to the target system.

Syncing Data to the Target System

1. Once the required settings and field mapping have been configured, click **Save**.
2. To begin the data import, click on the **Start** button at the bottom of the Configuration window.
3. Data will begin importing to the **Target System**. Data is synchronized repeatedly for the selected time interval. After a sync has finished, the service will wait for the **Resync Time** to elapse before restarting. If any changes have been made in the import file the updated data will be synced to the target system when the service restarts.

Note: If any necessary data is missing from the import file (for example, if a user is assigned an access level that does not exist in Protege GX), the import will 'soft fail': an error will be logged and the file will be imported with the faulty field left unassigned (e.g. the user will be imported without an assigned access level).

Service Logs

If the **Enable Event Logging** option has been enabled, all events that are generated by the data sync service are logged to both the Windows Event Viewer and a log file.

- In the Windows Event Viewer, navigate to **Application and Services Logs | ICT Protege GX** to locate the events logged by the data sync service.
- Log files containing the same events are saved to the **logs** folder in the installation directory (by default, C:\Program Files (x86)\Integrated Control Technology\Data Sync Service). Click **Open Log Folder** to view the logs.

Setting the Minimum Log Level

The log levels provided by the service are:

ID	Log Level
0	Debug Debug messages are added to the log files only, not the Event Viewer.
1	Information
2	Warning
3	Error

The default minimum log level is **1 - Information**, so the service logs all information, warning and error messages. You may wish to change the minimum log level in some circumstances:

- Set the minimum log level to **0 - Debug** to capture more information for troubleshooting. This can fill up disk space quickly, so only use this setting during initial setup or when investigating issues.
- Set the minimum log level to **2 - Warning** to exclude information messages and only capture warnings and errors, saving disk space.

To change the minimum log level:

1. Open the data sync service configuration tool and click **Stop** (or stop the service from the Windows Services Manager).
2. Navigate to the installation directory (by default C:\Program Files (x86)\Integrated Control Technology\Data Sync Service).
3. Open **settings.xml** in a text editor.

Files in this directory require administrator permissions to edit. You may need to open the file as an administrator using an application like Notepad++, or make a copy in a different directory to edit and replace the original.

4. Locate the following line in the XML and modify as required:
`<EnableLogging MinimumLogLevel="1">true</EnableLogging>`
5. Save the file.
6. Start the data sync service again.

If you subsequently edit any settings in the configuration tool and click **Save**, the minimum log level will be reset to 1.

User Import Reference

This section outlines the steps required to map common user import fields using the ICT Data Sync Service Configuration Tool.

User Name

Protege GX contains separate fields for a user's **First name**, **Last name** and **Name** (full name or display name). You can configure each of these separately in the import.

1. Click on a blank button in the **Target Field** column and select **FirstName**.
2. Set the **Source Column** to the first name column in the import file.
3. Click on a blank button in the **Target Field** column and select **LastName**.
4. Set the **Source Column** to the last name column in the import file.
5. There are two methods for setting the **Name** for imported users:
 - If you do not have a display name field in the import file, Protege GX will automatically populate the display name in the format **[FirstName] [LastName]**.

This format is used regardless of the **User display name auto format** setting in **Global | Global settings**. This is a known issue.
 - If you want to import a custom display name for each user, create a display name column in the import file with the relevant data and map it to the **Name** target field. Click on a blank button in the **Target Field** column and select **Name**, then set the **Source Column** to the display name column in the import file.
6. Click **Save**.

User Start and Expiry Date

The steps below outline how to configure the user expiry date/time for a user import to Protege GX.

1. Click on a blank button in the **Target Field** column and select **StartDate**.
2. Set the **Source Column** to the column in the import file that contains the relevant date/time data.
3. Click on the **Advanced** button [...] to open the advanced data configuration window.
4. Enable the **Date and Time Format** option and enter the date/time format of the import data into the text box (by selecting from the dropdown or typing it in manually).
5. Click **OK** to exit the advanced data configuration window.
6. Click **Save**.
7. Repeat the process for the **ExpiryDate** field.

Preventing Import of Expired Records

- In the advanced data configuration window for the **ExpiryDate** field, enable the **Use This Field for Expiry Date Check** option.

Allowing Import of Expired Records

- In the advanced data configuration window for the **ExpiryDate** field, enable the **Use This Field for Expiry Date Check** option.
- In the **Sync Options** section of the main window, enable the **Import Expired Records** option.

Deleting Expired Records

- In the advanced data configuration window for the **ExpiryDate** field, enable the **Use This Field for Expiry Date Check** option.
- In the **Sync Options** section of the main window, enable the **Delete Expired Records** option.

User PINs

The steps below outline how to configure a user **PIN** import to Protege GX.

1. Click on a blank button in the **Target Field** column and select **PINNumber**.
2. Set the **Source Column** to the column in the import file that contains the relevant user PIN data.
3. Click **Save**.

Rules for Syncing User PINs

- Syncing the **PINNumber** field is prohibited when the **Encrypt user PINs** option (**Global | Global settings**) is enabled in Protege GX.
If PIN encryption is enabled and the PINNumber field is added to the field mapping, a warning is displayed. The import will continue, but PIN records will be ignored.
- User PINs will be updated on every sync when the **Require dual credential for keypad access** option (**Global | Global settings**) is enabled.
This is because operators cannot view user PINs when dual credentials are enabled, so the data sync service does not have access to compare PINs to check whether an update is required.
A warning is displayed at the start of the sync and recorded in the log file.
- User PINs will be updated on every sync if the data sync service operator does not have the **Show PIN numbers for users** option (**Global | Operators**) enabled, as the operator does not have access to compare PINs to check whether an update is required.
A warning is displayed at the start of the sync and recorded in the log file.
- Duplicate PINs are not allowed when the **Allow PIN duplication** option (**Global | Sites | Site defaults**) is not enabled. Duplicate entries will fail to import and a 'Duplicate PIN' error will be generated (see page 54).

Access Levels

The steps below outline how to set up data mapping to assign access levels to users for import to Protege GX.

A Single Access Level in a Single Column

Take the following import data as an example:

105,John James,Main Office,Warehouse

1. Click on a blank button in the **Target Field** column and select **UserAccessLevelGroupDataData**. The **Source Column** is automatically set to Group and the linked fields are displayed.
2. Set the **Source Column** value for the **UserAccessLevel** field to the column in the import file that contains the name of the access level that will be assigned to the user.
3. Click on the **Advanced** button [...] to open the advanced data configuration window for the **UserAccessLevel** field.
4. Enable the **Use This Field as the Group Data Identifier** option.
5. Enable the **Target Field Record Type** option and set the dropdown to Access Levels.
6. Click **OK**.
7. Click **Save**.

The **UserAccessLevelGroupDataData** field can be mapped more than once, allowing multiple access levels to be assigned to a user. If the access levels are in separate columns in the import file simply repeat the steps above and set the **Source Column** accordingly. If the access level data is grouped and is in a single column in the import file, see the instructions below.

Multiple Access Levels in a Single Column

Take the following import data as an example:

105,John James,Main Office;Warehouse

1. Click on a blank button in the **Target Field** column and select **UserAccessLevelGroupDataData**. The **Source Column** is automatically set to Group and the linked fields are displayed.
2. Set the **Source Column** value for the **UserAccessLevel** field to the column in the import file that contains the access level name. In this example the **Source Column** would be set to 3.
3. Click on the **Advanced** button [...] to open the advanced data configuration window for the **UserAccessLevel** field.
4. Enable the **Use This Field as the Group Data Identifier** option.
5. Set the **Grouping Type** to Paired Data.
6. Set the **Pair Delimiter** to a semicolon (;). This states that each access level within the column is separated by a semicolon.
7. Enable the **Target Field Record Type** option and set the dropdown to Access Levels.
8. Click **OK**.
9. Click **Save**.
10. You will see the **Result Value** column displays only the access level name(s).

Multiple Access Levels with an Assigned Schedule in a Single Column

Take the following import data as an example:

105,John James,Main Office:General Access 9AM-5PM Mon-Fri;Main Warehouse:Extended Access 5AM-10PM Mon-Fri

1. Click on a blank button in the **Target Field** column and select **UserAccessLevelGroupDataData**. The **Source Column** is automatically set to Group and the linked fields are displayed.
2. Set the **Source Column** value for the **UserAccessLevel** field to the column in the import file that contains the access level data. In this example the **Source Column** would be set to 3.
3. As the access level and schedule are in a single column in the import file, set the **Source Column** value for the **UserAccessLevelSchedule** field to the same as that assigned to the **UserAccessLevel**. In this example the **Source Column** would be set to 3.
4. Click on the **Advanced** button [...] to open the advanced data configuration window for the **UserAccessLevel** field.
5. Enable the **Use This Field as the Group Data Identifier** option.
6. Set the **Grouping Type** to Grouped Paired Data.
 - Set the **Group Delimiter** to a semicolon (;). This states that each group of access level data within the column is separated by a semicolon.
 - Set the **Pair Delimiter** to a colon (:). This states that each field within the group is separated by a colon.
 - Set the **Index** to 1. This states that the access level name is the first value in the pair.
7. Enable the **Target Field Record Type** option and set the dropdown to Access Levels.
8. Click **OK**.
9. You will see the **Result Value** column displays only the access level name(s).
10. Click on the **Advanced** button [...] to open the advanced data configuration window for the **UserAccessLevelSchedule** field.
11. Set the **Grouping Type** to Grouped Paired Data.
 - Set the **Group Delimiter** to a semicolon (;). This states that each group of access level data within the column is separated by a semicolon.
 - Set the **Pair Delimiter** to a colon (:). This states that each field within the group is separated by a colon.
 - Set the **Index** to 2. This states that the schedule assigned to the access level is the second value in the pair.
12. Enable the **Target Field Record Type** option and set the dropdown to Schedules.
13. You will see the **Result Value** column displays only the schedule name(s).
14. Click **OK**.
15. Click **Save**.

This structure provides a simple way to assign multiple access levels to each user.

Adding Start and End Dates

As a follow-on to the two scenarios above, if you also wish to import an **Expiry start** and **Expiry end** for the access level:

You must have both an expiry start and expiry end for the access level for a successful import. You cannot assign just one.

1. Set the **Source Column** for the **UserAccessLevelStart** to the column in the import file that contains the access level start data.
2. Click on the **Advanced** button [...] beside the **UserAccessLevelStart** field to open the advanced data configuration window.
3. Enable the **Date and Time Format** option and enter the date/time format of the import data into the combo box (by selecting from the dropdown or typing it in manually).
4. Click **OK** to exit the advanced data configuration window.
5. Set the **Source Column** for the **UserAccessLevelEnd** to the column in the import file that contains the access level end data.

6. Click on the **Advanced** button [...] beside the **UserAccessLevelEnd** field to open the advanced data configuration window.
7. Enable the **Date and Time Format** option and enter the date/time format of the import data into the combo box (by selecting from the dropdown or typing it in manually).
8. Click **OK** to exit the advanced data configuration window.
9. Set the **Source Column** to Not From Import File for the **UserAccessLevelExpire** field.
10. Click on the **Advanced** button [...] beside the **UserAccessLevelExpire** field to open the advanced data configuration window.
11. Set the **Default Value** to true.

This field must be entered **exactly as shown**. It is case sensitive.

12. Click **OK**.
13. Click **Save**.

Facility Code and Card Number

The steps below outline how to configure a facility code and card number in a user import to Protege GX.

The import does not require both a card number and facility code to succeed. Either is acceptable.

Each Facility Code and Each Card Number in Separate Columns

Take the following import data as an example:

105,John James,1,15,1,25

1. Click on a blank button in the **Target Field** column and select **UserCardNumberGroupDataData**. The **Source Column** is automatically set to Group and the linked fields are displayed.
2. Set the **Source Column** value for the **FamilyNumber** field to the column in the import file where the facility code is located. In this example the **Source Column** would be set to 3.
3. Click on the **Advanced** button [...] beside the **FamilyNumber** field to open the advanced data configuration window.
4. Enable **Use This Field as the Group Data Identifier**.
5. Click **OK**.
6. Click on a blank button in the **Target Field** column and select **UserCardNumberGroupDataData**. The **Source Column** is automatically set to Group and the linked fields are displayed.
7. Set the **Source Column** value for the **CardNumber** field to the column in the import file where the card number is located. In this example the **Source Column** would be set to 4.
8. Click on the **Advanced** button [...] beside the **CardNumber** field to open the advanced data configuration window.
9. Enable **Use This Field as the Group Data Identifier**.
10. Click **OK**.
11. Click **Save**.

The **UserCardNumberGroupDataData** field can be mapped more than once (and up to eight times as supported by Protege GX), allowing multiple cards to be assigned to a user. To import the second facility code and card number in the example above, simply set the **Source Column** for **FamilyNumber** and **CardNumber** to 5 and 6 respectively.

Multiple Facility Codes and/or Card Numbers in a Single Column

Take the following import data as an example:

105,John James,1:15;1:25

1. Click on a blank button in the **Target Field** column and select **UserCardNumberGroupDataData**. The **Source Column** is automatically set to Group and the linked fields are displayed.
2. Set the **Source Column** value for the **CardNumber** field to the column in the import file that contains the card number for the user. In this example the **Source Column** would be set to 3.
3. As the card number and facility code are a single field in the import file, set the **Source Column** value for the **FamilyNumber** field to the same as that assigned to the **CardNumber**. In this example the **Source Column** would be set to 3.
4. Click on the **Advanced** button [...] to open the advanced data configuration window for the **FamilyNumber** field.
5. Enable the **Use This Field as the Group Data Identifier** option.
6. Set the **Grouping Type** to Grouped Paired Data.

- Set the **Group Delimiter** to a semicolon (;). This states that each group of card data is separated by a semicolon.
 - Set the **Pair Delimiter** to a colon (:). This states that the field within the group are paired by a colon.
 - Set the **Index** to 1. This states that the **Target Field** (in this example, the **FamilyNumber**) is the first value in the pair.
7. Click **OK**.
 8. You will see that the **Result Value** field contains the facility number only.
 9. Click on the **Advanced** button [...] to open the advanced data configuration window for the **CardNumber** field.
 10. Enable the **Use This Field as the Group Data Identifier** option.
 11. Set the **Grouping Type** to Grouped Paired Data.
 - Set the **Group Delimiter** to a semicolon (;). This states that each group of card data is separated by a semicolon.
 - Set the **Pair Delimiter** to a colon (:). This states that the fields within the group are paired by a colon.
 - Set the **Index** to 2. This states that the **Target Field** (in this example, the **CardNumber**) is the second value in the pair.
 12. Click **OK**.
 13. Click **Save**.

In this scenario there can be up to eight pairs of data separated by a colon (eight card numbers are supported in Protege GX).

Credential Types

The steps below outline how to set up the data mapping to assign credential types to users for import to Protege GX.

Take the following import data as an example where a license plate is being imported as a credential type:

105,John James,ABC123

1. Click on a blank button in the **Target Field** column and select **UserCredentialGroupDataData**. The **Source Column** is automatically set to Group and the linked fields are displayed.
2. To define the credential type to which the data is going to be imported to, set the **Source Column** of the **UserCredentialType** to Not From Import File.
3. Click on the **Advanced** button [...] to open the advanced data configuration window for **UserCredentialType**.
4. In the **Default Value** field, enter the name of an existing credential type to which the data is be imported to. In this example we would set the **Default Value** to License Plate.
5. Select the **Target Field Record Type** option and set the dropdown to Credential Types.
6. Enable the **Use This Field as the Group Data Identifier** option.
7. Click **OK**.
8. Set the **Source Column** value for the **UserCredential** field to the column in the import file that contains the data to be assigned to the credential type. In this example the **Source Column** would be set to 3.
9. Click **Save**.

The **UserCredentialGroupDataData** field can be mapped more than once, allowing multiple credentials to be assigned to a user. Simply repeat the steps above and set the **Source Column** accordingly.

If the user credential data is grouped in a single column in the import file, refer to the Advanced Configuration section (see page 17).

Custom Fields

Custom fields are a powerful component of Protege GX that allow customization of user data and related programming. Being able to import custom data provides an effective link to other systems and operations. The steps below outline how to map import data to Protege GX custom fields.

Any custom field that you want to import to must already exist within Protege GX before importing.

1. Click an available **Target Field** button and select **UserCustomFieldGroupDataData**. The **Source Column** is automatically set to Group and the linked fields are displayed.
2. To specify importing the data to a custom field, set the **Source Column** of the **CustomFieldID** target field to Not From Import File.
3. Click the **Advanced** button [...] to open the advanced data configuration window for the **CustomFieldID** target field.
4. Set the **Default Value** to the name of the Protege GX custom field to import to.

This must **exactly** match the name of the custom field in Protege GX or the data cannot be imported.

5. Enable the **Target Field Record Type** option and set the dropdown to Custom Fields.
6. Enable the **Use This Field as the Group Data Identifier** option.
7. Click **OK**.
8. Next, configure the **CustomFieldType** to define the type of data held in the custom field, and the way new data will be imported.

For information on custom field type configuration, refer to Custom Field Formatting (see below).

The **UserCustomFieldGroupDataData** field can be mapped more than once, allowing multiple custom fields to be assigned to a user. Simply repeat the steps above and set the **Source Column** accordingly.

If user custom field data is grouped in a single column in the import file, refer to the Advanced Configuration section (see page 17).

Custom Field Formatting

When importing data to custom fields in Protege GX, the data sync service needs to know what type of data is held in each custom field.

Refer to the table and configuration information below:

Protege GX Custom Field Type	ICT Data Sync Service Custom Target Field	ICT Data Sync Service Custom Field Type Default Value
Text	CustomFieldTextData	0
Numerical	CustomFieldNumericalData	1
Time	CustomFieldDateTimeData	2
Date	CustomFieldDateTimeData	3
Time and Date	CustomFieldDateTimeData	4
Option	CustomFieldBooleanData	5
Link	CustomFieldTextData	6
Dropdown Box	CustomFieldTextData	7
Image	N/A	N/A

Text

1. Set the **CustomFieldType** to Not From Import File and assign a **Default Value** of 0.
2. To assign a value to the custom field, set the **Source Column** value for the **CustomFieldTextData** field.

This should correspond to the column in the import file where the custom field is located.

Numerical

Leading zeros are removed during the import. If leading zeros are required (e.g. for a phone number), you must use the **CustomFieldTextData** field.

1. Set the **CustomFieldType** to Not From Import File and assign a **Default Value** of 1.
2. To assign a value to the custom field, set the **Source Column** value for the **CustomFieldNumericalData** field.

This should correspond to the column in the import file where the custom field is located.

The numerical field is limited to a maximum value of 2147483647. The sync will fail if any record in the data set exceeds this value, so for longer numbers (such as some phone numbers) a text field must be used.

Time and Date

1. Set the **CustomFieldType** to Not From Import File and assign a **Default Value** of 4.
2. To assign a value to the custom field, set the **Source Column** value for the **CustomFieldDateTimeData** field.

This should correspond to the column in the import file where the custom field is located.

3. You must also set the **Date and Time Format** in the advanced data configuration window.

Time

If you are importing a time you must still enter the time and date in full. Protege GX will trim the date/time field and only place the required data into the custom field. Follow the directions in the Time and Date section but set the **CustomFieldType Default Value** to 2.

Date

If you are importing a date you must still enter the time and date in full. Protege GX will trim the date/time field and only place the required data into the custom field. Follow the directions in the Time and Date section but set the **CustomFieldType Default Value** to 3.

Option

1. Set the **CustomFieldType** to Not From Import File and assign a **Default Value** of 5.
2. To assign a value to the custom field, set the **Source Column** value for the **CustomFieldBooleanData** field.

This should correspond to the column in the import file where the custom field is located.

Link

A link is added to a custom field in the same way that text data is. Refer to the section on importing a **Text** field.

The link used must use the format of www.google.com. You cannot include the prefix https:// in the link if you are required to access the URL using the link button in Protege GX.

Dropdown Box

To import to a dropdown box into Protege GX, the dropdown box must already exist and contain all of the dropdown items that are to be assigned from the import file.

1. Set the **CustomFieldType** to Not From Import File and assign a **Default Value** of 7.
2. To assign a value to the dropdown, set the **Source Column** value for the **CustomFieldTextData** field.
This should correspond to the column in the import file where the custom field is located.
3. In order for the dropdown field to import correctly, you must add the required conversions. Open the advanced data configuration window for the **CustomFieldTextData** field.
In the **Conversions** table, the **Original Format** is the **Display Text** in Protege GX, and the **Resulting Format** is the **Value** of the dropdown item in Protege GX.
4. You will see that the data mapping has been updated to show you that the **Original Value** maps to the correct **Resulting Value** based on the conversion.

Record Groups

The steps below outline how to map record groups. Note that the record group you wish to import to must already exist within Protege GX.

1. Click on a blank button in the **Target Field** column and select **RecordGroup**.
2. Set the **Source Column** value for the **RecordGroup** field to the column in the import file that contains the name of the record group.
3. Click the **Advanced** button [...] to open the advanced data configuration window for the **RecordGroup** field.
4. Enable the **Target Field Record Type** option and set the dropdown to Record Groups.
5. Click **OK**.
6. Click **Save**.

User Photos

Photos can be imported and assigned to Protege GX users via the data sync service.

There are two methods which can be used for importing user photos:

1. From a single defined directory
2. From individual file paths

In both instances the **ImageID** field is added to the data sync data mapping to provide a link between the user record from the CSV import file and the image file to be assigned as the user's photo.

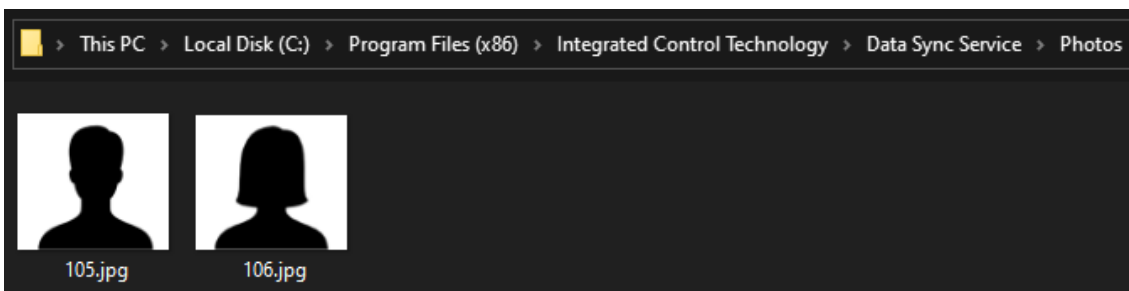
Prerequisites

- ICT Data Sync Service version 2.0.10 or higher.
- The data sync service must have access to any directory the photos are stored in.
- Each photo image file must have a unique file name. This will be referenced to link the file to the user.
- Only .jpg / .jpeg file formats are supported.
- All other user field data mapping should be completed before mapping user photos.

Importing all Photos from a Single Directory

When the import file does not contain a column that holds the file path for each user image, user photos can be imported from a single defined directory.

- All user photos must be stored in a folder named Photos (this is case sensitive).
- The Photos folder must be in the data sync service installation directory:
C:\Program Files (x86)\Integrated Control Technology\Data Sync Service\Photos



- The CSV import file must contain a column which includes the file names, to reference each user's photo file in the specified directory folder. For example:

105, Jim James

106, Alex Reader

- Add the **ImageID** field to the **Data Mapping**, and set the **Source Column** to the column in the import file that contains the files names of the images in the Photos folder.

In the above example the **Source Column** would be 1.

Importing Photos with Individual Paths

User photos can be imported from any directories that the data sync service has access to, if the CSV import file contains a column which includes the file path for each user image.

- The path to each image file can be formatted as any of:
 - A fully qualified path
 - A relative path
 - A UNC (Universal Naming Convention) path
- A single DSS import can import files from multiple directories, but all file paths must be in the same column in the import file. For example:

Jim James,C:\DataSync\Images\105.jpg

Alex Reader,C:\Photos\Staff\AR_Photo.jpg

- Add the **ImageID** field to the **Data Mapping**, and set the **Source Column** to the column in the import file that contains the file paths to the images.

In the above example the **Source Column** would be 2.

Importing to a Specific Site

Data sync allows you to import users to different sites within a single import.

1. Click on a blank button in the **TargetFields** column and select **SiteID**.
2. Set the **Source Column** value for the **SiteID** field to the column in the import file that contains the name of the site.
3. Click the **Advanced** button [...] to open the advanced data configuration window for the **SiteID** field.
4. Enable the **Target Field Record Type** option and set the dropdown to Sites.
5. Click **OK**.

Importing Schedules

If you were previously using the Protege GX Data Sync Service (version 1.X.X) and have upgraded to the ICT Data Sync Service, contact ICT Support before carrying out an import that includes schedules.

This section outlines how to import schedules into Protege GX.

- The **Name** is assigned as the **Unique Field** by default.
- Just like the user import process, schedules can be imported to more than one site from a single import file:
Weekend Schedule 08:00 - 12:00,31/03/2019 08:00,31/03/2019 12:00

It is important to note that if the schedule import data exceeds the 8 periods allowed in a single schedule as enforced by Protege GX, **only the first 8 periods** in the import file will be imported. A warning will be logged advising that there are more than 8 periods and some have not been imported.

Importing a Schedule

1. Click on a blank button in the **Target Field** column and select the **SiteID** field.
2. Set the **Source Column** to the column in the import file that contains the name of the site the schedule is to be imported to.
3. Click the **Advanced** button [...] to open the advanced data configuration window.
4. Enable the **Target Field Record Type** option and set the dropdown to Sites.

Importing Schedules Where Periods Have a Date

- Only periods within the next seven days are imported. If this is not the case, the period will not be imported and a warning will be logged.
- Periods that are in the past will not be imported.
- Each start time must have a corresponding end time mapped in order for the import to be successful.

For this example take an import file in the following format:

Monday to Friday 08:00 - 16:30,25/03/2019 08:00,25/03/2019 16:30

Monday to Friday 08:00 - 16:30,26/03/2019 08:00,26/03/2019 16:30

Monday to Friday 08:00 - 16:30,27/03/2019 08:00,27/03/2019 16:30

Monday to Friday 08:00 - 16:30,28/03/2019 08:00,28/03/2019 16:30

Monday to Friday 08:00 - 16:30,29/03/2019 08:00,29/03/2019 16:30

Weekend Schedule 08:00 - 12:00,30/03/2019 08:00,30/03/2019 12:00

To set up the schedule import:

1. Set the **Record to Sync** to Schedules.
2. Enable the **Group Data Before Import** option in the **Data Source** section.
3. Click on a blank button in the **Target Field** column and select **Name**.
4. Set the **Source Column** to the column in the import file that contains the name of the schedule. In this example the **Source Column** would be set to 1.
5. Click on a blank button in the **Target Field** column and select **StartTime1**.
6. Set the **Source Column** to the column in the import file that contains the start time for the schedule period. In this example the **Source Column** would be set to 2.
7. Click the **Advanced** button [...] to open the advanced data configuration window.

8. Enable the **Date and Time Format** option and enter the date time format of the import data into the text box (by selecting from the dropdown or typing it in manually).
9. Click **OK**.
10. Click on a blank button in the **Target Field** column and select **EndTime1**.
11. Set the **Source Column** to the column in the import file that contains the end time for the schedule period. In this example the **Source Column** would be set to 3.
12. Click the **Advanced** button [...] to open the advanced data configuration window.
13. Enable the **Date and Time Format** option and enter the date time format of the import data into the text box (by selecting from the dropdown or typing it in manually).
14. Click **OK**.
15. Click **Save**.

Importing Controllers

This section outlines how to import controllers into Protege GX.

Binary Blob

When importing controllers, binary blob data can also be imported and linked with controller records. The binary data can be imported from a file or as a data string. The file path or data string can be included in the import **data source**, or can be supplied in the advanced data configuration of the assigned **target field**.

When imported into Protege GX the controller will access and reference the linked binary blob data. This data cannot be viewed or edited in the user interface, but successful linking can be confirmed by checking the **Download binary blob** section of the controller programming. If a binary blob has been successfully linked to the controller the **Database data length (bytes)** field will display a value greater than zero, representing the associated binary bytes .

Importing binary data is available in ICT Data Sync Service version 2.0.10.7 or higher, and requires Protege GX version 4.3.285.18 or higher.

Importing a Controller

1. In the **Data Mapping** section, set the **Record to Sync** to **Controllers**.
2. Define the **Data Source** by selecting the **File Directory** where the source file(s) will be found, or specifying the **Import File** containing the controller records.
3. Click on the blank **Target Field** button corresponding to the **Source Column** that contains the controller name and select **Name** from the target fields list.

The **Name** is assigned as the **Unique Field** by default.

4. If not already correctly mapped, set the **Source Column** to the column in the import file that contains the name of the controller.
5. Map other target fields according to the source file data.
6. To link binary blob data, click on a blank **Target Field** button and select **DownloadBinary**.

The **DownloadBinary** target field is only available when the **Record to Sync** is set to **Controllers**.

If the binary blob file path or data string is contained within the import data source:

- Set the **Source Column** to the column in the import file that contains the file path or data string.

If the binary blob file path or data string is not contained within the import file:

- Set the **Source Column** for the **DownloadBinary** target field to **Not From Import File**.
- Click the **Advanced** button [...] to open the advanced data configuration window.
- In the **Default Value** field, enter the file path to the binary blob file (either a full path or relative path) or the data string.
- Click **OK**.

Binary blob data can be added and updated, however deletion is currently not supported.

7. Click **Save**.

Field Mapping Between Data Sync and Protege GX

The table below outlines the user based fields, their names in Protege GX, their names in data sync, and how to configure them for import.

By default, some fields are not visible as they are associated with an integration that is not enabled.

Some fields are absent from the table as these are fields that do not need to be mapped, currently cannot be synced, or are read-only in Protege GX.

SOAP Name	Protege GX Display Name	Protege GX Menu Location	Protege GX Option Type
AcknowledgeSystemTroubles	Acknowledge system troubles	Users Users Options	Checkbox
ArmOn3BadgeEnabled	Arm on 3 badge enabled	Programming Apartments Users	Checkbox
AuditOpeningsInTheKey	Audit openings in the key	Users Users Salto	Checkbox
Badge3LatchDoor2Hours	Badge 3 latch door 2 hours	Programming Apartments Users	Checkbox
Badge3LatchDoor4Hours	Badge 3 latch door 4 hours	Programming Apartments Users	Checkbox
Badge3LatchDoor8Hours	Badge 3 latch door 8 hours	Programming Apartments Users	Checkbox
Badge3LatchDoorToggle	Badge 3 latch door toggle	Programming Apartments Users	Checkbox
BadgeNumber	Badge number	Users Users Extended	Textbox
BadgeType	Badge type	Users Users Extended	Textbox
Calendar	Calendar	Users Users Salto	Dropdown
CardNumber	Card number	Users Users Extended	Textbox
CardType	Card type	Users Users Extended	Textbox
CardCanArmSystemOnly	Code can arm system only	Programming Apartments Users	Checkbox

SOAP Name	Protege GX Display Name	Protege GX Menu Location	Protege GX Option Type
CustomField4	Custom field 4	Users Users Extended	Textbox
CustomField5	Custom field 5	Users Users Extended	Textbox
CustomNoteField1	Custom note field 1	Users Users Extended	Textbox
CustomNoteField2	Custom note field 2	Users Users Extended	Textbox
DateOfBadgeExpiration	Date of badge expiration	Users Users Extended	DateTime
DaysOrHours	Period	Users Users Salto	Dropdown
DefaultLanguage	Default language	Users Users General	Dropdown
DeleteRecord	Deletes user from Protege GX when set to true		
DisabledVisitorCard	Visitor card disabled	Users Users Visitor	Checkbox
DisableUser	Disable user	Users Users Options	Checkbox
DisableOnSingleBadgeEnabled	Disable on single badge enabled	Programming Apartments Users	Checkbox
DualCustodyMaster	Dual custody master	Users Users Options	Checkbox
DualCustodyProvider	Dual custody provider	Users Users Options	Checkbox
Duress1	Duress	Users Users Biometrics	Checkbox
Duress2	Duress	Users Users Biometrics	Checkbox
EmployeeFunction	Employee function	Users Users Extended	Textbox
EnableRevalidationOfKeyExpiration	Enable revalidation of key expiration	Users Salto	Checkbox
EnrollmentDevice	Enrollment device	Users Users Biometrics	Dropdown
ExpirationDateOfBadge	Expiration date of badge	Users Users Extended	Textbox
ExpiryDate	End date time field	Users Users General	DateTime

SOAP Name	Protege GX Display Name	Protege GX Menu Location	Protege GX Option Type
ExpiryDateValid	End date checkbox	Users Users General	Checkbox
Finger1	Enable	Users Users Biometrics	Checkbox
Finger2	Enable	Users Users Biometrics	Checkbox
FirstName	First name	Users Users General	Textbox
GoDirectlyToTheMenuOnLogin	Go directly to the menu on login (no area control)	Users Users Options	Checkbox
HLIEnableCartService	Enable cart service	Users Users Options	Checkbox
HLIEnableCIMOverride	Enable CIM override	Users Users Options	Checkbox
HLIEnableSplitGroup	Enable split group operation	Users Users Options	Checkbox
HLIEnableVertigo	Enable Vertigo	Users Users Options	Checkbox
HLIEnableVertigo2	Enable Vertigo 2	Users Users Options	Checkbox
HLIIsVIPUser	User is a VIP	Users Users Options	Checkbox
ImageID	Binary data of image	Users Users Photo	Image
KabaKeyID	Cencon key ID	Users Users General	Numeric
KabaKeyInitialised	Initialise key	Users Users General	Button
KeyAssigned	Key assigned	Users Users Salto	Textbox
LastName	Last name	Users Users General	Textbox
LicenseNumber	License Number	Users Users Extended	Textbox
Name	Name	Users Users General	Textbox
Name2	Name (second language)		
NotificationAddress	Notification email address	Users Users Visitor	Dropdown
Office	Office	Users Users Salto	Checkbox

SOAP Name	Protege GX Display Name	Protege GX Menu Location	Protege GX Option Type
OverrideLockdown	User can override lockdown	Users Users Salto	Checkbox
OverridePrivacy	User can override privacy	Users Users Salto	Checkbox
PhotoIDTemplate	Card template	Users Users Photo	Dropdown
PIN	PIN	Users Users Salto	Checkbox
PINNumber	PIN	Users Users General	Numeric
RearmAreaInStayMode	Rearm area in stay mode	Users Users Options	Checkbox
RecordGroup	Record group	Users Users General	Dropdown
ReportingID	Reporting ID	Users Users General	Numeric
SalaryNumber	Salary number	Users Users Extended	Textbox
SaltoLockdownEnabled	User can lockdown door	Users Users Salto	Checkbox
SaltoOverrideLockdown	User can override lockdown	Users Users Salto	Checkbox
SaltoOverridePrivacy	User can override privacy	Users Users Salto	Checkbox
ServiceName	Service name	Users Users Extended	Textbox
ServiceNumber	Service number	Users Users Extended	Textbox
Showagreetingmessagetouser	Show a greeting message to user	Users Users Options	Checkbox
ShowAlarmMemoryOnLogin	Show alarm memory on login	Users Users Options	Checkbox
Site	Site	Users Users Extended Fields	DateTime
SiteID	Can be mapped when syncing data in a single file to multiple sites.		
StartDate	Start date time field	Users Users General	DateTime
StartDateValid	Start date checkbox	Users Users General	Checkbox

SOAP Name	Protege GX Display Name	Protege GX Menu Location	Protege GX Option Type
SupportVMS	User supports visitors	Users Users Visitor	Checkbox
TreatUserPINLess1AsDuress	Treat user PIN plus 1 as duress	Users Users Options	Checkbox
TurnOffthePrimaryArealfUserHasAccessOnLogin	Turn off the primary area If user has access on login	Users Users Options	Checkbox
TurnOfftheUserAreaonLoginifUserhasaccess	Turn off the user area on login if user has access	Users Users Options	Checkbox
Union	Union	Users Users Extended	Textbox
UpdatePeriod	Update period	Users Users Salto	Numeric
UseAntipassback	Use antipassback	Users Users Salto	Checkbox
UseExtendedOpeningTime	Use extended opening time	Users Users Salto	Checkbox
UserAccessLevelGroupData			
UserAccessLevelGroupDataData			
UserAccessLevelGroupDataID	Automatically assigned		
Site	Automatically assigned		
• UserAccessLevel	Name	Users Users Access levels	Read-Only
• UserAccessLevelStart	Expiry start	Users Users Access levels	DateTime
• UserAccessLevelEnd	Expiry end	Users Users Access levels	DateTime
• UserAccessLevelExpire	Access level expires	Users Users Access levels	Checkbox
UserArea	User area	Users Users General	Dropdown
UserAreaGroupGroupData			
UserAreaGroupGroupDataData			
• UserAreaGroupGroupDataID	Automatically assigned		
• UserID	Automatically assigned		
• Site	Automatically assigned		
UserAreaGroup	Name	Users Users Area groups	Read-Only
UserCanAcknowledgeAlarmMemory	User can acknowledge alarm memory	Users Users Options	Checkbox

SOAP Name	Protege GX Display Name	Protege GX Menu Location	Protege GX Option Type
UserCanLogInRemotely	User can edit user settings from keypad	Users Users Options	Checkbox
UserCanModifyOtherUsers	User can modify other users	Programming Apartments Users	Checkbox
UserCanModifyTheirOwnCode	User can modify their own code	Programming Apartments Users	Checkbox
UserCardNumberGroupData			
UserCardNumberGroupDataData			
• CardLastUsed	Automatically assigned		
• CardLastUsedValid	Automatically assigned		
• CardInactivityPeriodInMinutes	Inactivity period	Users Users General	Numeric
• CardInactivityPeriodsActive	Inactivity period	Users Users General	Checkbox
• CardInactivityPeriodAction	Inactivity period (minutes/hours/days)	Users Users General	Dropdown
• UserCardNumberGroupDataID	Automatically assigned		
• Site	Automatically assigned		
• FamilyNumber	Facility code	Users Users General	Numeric
• CardNumber	Card number	Users Users General	Numeric
• CardDisabled	Disabled	Users Users General	Checkbox
UserCredentialGroupData			
UserCredentialGroupDataData			
• DBUserCredentialGroupDataID	Automatically assigned		
• UserCredentialGroupDataID	Automatically assigned		
• Site	Automatically assigned		
• UserCredential	Credential	Users Users General	Textbox
• UserCredentialType	Credential type	Users Users General	Dropdown
• FollowedByNext	Disabled	Users Users General	Checkbox
UserCustomFieldGroupData			
UserCustomFieldGroupDataData			

SOAP Name	Protege GX Display Name	Protege GX Menu Location	Protege GX Option Type
• UserCustomFieldGroupDataID	Automatically assigned		
• Site	Automatically assigned		
• CustomFieldID	ID of the custom field		
• CustomFieldType			
• CustomFieldTextData			
• CustomFieldDateTimeData			
• CustomFieldBooleanData			
Userhassuperrightsandcanoverrideantipassback	User has super rights and can override antipassback	Users Users Options	Checkbox
UserInactivityDeletionPeriodAction	Delete Period (Minutes/Hours/Days)	Users Users General	Dropdown
UserInactivityDeletionPeriodInMinutes	Delete period	Users Users General	Numeric
UserInactivityDeletionPeriodsActive	Delete period	Users Users General	Checkbox
UserInactivityPeriodAction	Disable period (minutes/hours/days)	Users Users General	Dropdown
UserInactivityPeriodInMinutes	Disable period	Users Users General	Numeric
UserInactivityPeriodsActive	Disable period	Users Users General	Checkbox
UserisaDuressUser	User is a duress user	Users Users Options	Checkbox
UserKabaLockGroupData			
UserKabaLockGroupDataData			
• UserKabaLockGroupDataID	Automatically assigned		
• UserKabaLock	Name	Users Users Cencon locks	Read-Only
• UserKabaLockSerialNumber	Lock serial number	Users Users Cencon locks	
UserKabaLockGroupGroupData			
UserKabaLockGroupGroupDataData			
• UserKabaLockGroupGroupDataID	Automatically assigned		
• Site	Automatically assigned		
• UserKabaLockGroup	Name	Users Users Cencon lock groups	Read-Only

SOAP Name	Protege GX Display Name	Protege GX Menu Location	Protege GX Option Type
UserKeyWatcherID	Third party user ID (Key cabinet integration)	Users Users General	Textbox
UserLoiterExpiryCountEnabled	User loiter expiry count enabled	Users Users Options	Checkbox
UserOperatesADAFFunction	User operates extended door access function	Users Users Options	Checkbox
UserPhotoPlaceholderHeightPixels	Pixels ____ high	Users Users Photos (Photo Settings)	Numeric
UserPhotoPlaceholderWidthPixels	Pixels ____ wide	Users Users Photos (Photo Settings)	Numeric
UserRoomGroupData			
UserRoomGroupDataData			
• UserRoomGroupDataID			
• Site			
• UserRoom			
• ArrivalDateTime			
• DepartureDateTime			
• TempUserName			
UserSaltoDoor			
UserSaltoDoorGroup			
UserSaltoDoorGroupData			
UserSaltoDoorGroupDataData			
• UserSaltoDoorGroupDataID	Automatically assigned		
• Site	Automatically assigned		
• UserSaltoDoor	Name	Users Salto door groups	Read-Only
• Schedule	Schedule	Users Users Salto door groups	Dropdown
UserSaltoDoorGroupGroupData			
UserSaltoDoorGroupGroupDataData			
• UserSaltoDoorGroupGroupDataID	Automatically assigned		
• Site	Automatically assigned		
• UserSaltoDoorGroup	Name	Users Users Salto door groups	Read-Only

SOAP Name	Protege GX Display Name	Protege GX Menu Location	Protege GX Option Type
<ul style="list-style-type: none"> Schedule 	Schedule	Users Users Salto door groups	Dropdown
<ul style="list-style-type: none"> UserSaltoOutput 			
VisitorAccessLevel	Visitor access level	Users Users Visitor	Dropdown
VisitorNotificationMode	Visitor notification mode	Users Users Visitor	Dropdown
VMSCheckedIn	Checked in	Users Users Visitor	DateTime
VMSCheckedOut	Checked out	Users Users Visitor	DateTime
VMSExpectedLeaveDate	Expected departure	Users Users Visitor	DateTime

Error Messages

Configuration Errors

Configuration errors are displayed at the bottom of the ICT Data Sync Service Configuration Tool window and relate to operator-assigned settings and options. Some of the errors that relate to populating fields are displayed beside the field that is configured incorrectly.

To view more information about the error, hover the mouse over the red error icon.

The table below provides a list of inline errors and solutions to the corresponding errors.

Error Message	Cause	Solution
A Data Sync Service license is not enabled on this SSN therefore the sync is limited to 10 records only.	A purchased data sync service license cannot be found.	This may be due to the product being unlicensed or a missing license update in Protege GX.
Failed to find Operator where Username = __.	An existing Protege GX operator with the username entered cannot be found.	Check that the operator Username has been entered correctly and is an existing operator in Protege GX.
Incorrect username or password, or the operator does not have access.	Failed to locate a valid operator in Protege GX.	Either the Username or Password for the operator is incorrect, or the operator does not have the correct role assigned in Protege GX (Global Operators).
The "Show PIN numbers for Users" option for the Data Sync Operator (__) must be switched ON.	The operator with the entered Username does not have the Show PIN numbers for users option enabled in Protege GX.	In Protege GX, navigate to Global Operators and select the operator mentioned in brackets in the error message. Enable the Show PIN numbers for users option.
The "Import File" cannot be left blank. If you do not wish to use this option, deselect the checkbox.	The Import Filename option has been enabled but the corresponding textbox has been left blank.	Disable this option if you do not wish to use it. If you wish to use this option, select an import file by either entering the filename in the checkbox or using the file browser.
You must select at least one Unique Field.	A Unique Field has not been selected.	For the configuration to save successfully, you must select at one or more unique fields.
File Directory __ is empty.	The file path entered in the File Directory points to a folder which does not contain any files.	Ensure that the selected File Directory contains at least one file with only files of the same format. Additionally, the files must be of a format that are accepted by data sync such as CSV, TXT or XML.
File Directory __ does not exist.	The file path is incorrect.	This may be due to a spelling error, or the directory having been deleted.
"File Format" selection is incorrect	The option selected in the File Format field is incorrect for the type of data in the import file(s).	Select the file format that matches the import file (s).

Error Message	Cause	Solution
File not found for "Import File Name" setting".	For example, the selected File Directory does not contain a file with the specified name.	Ensure that the selected File Directory contains a file with the name entered in the Import Filename field. This error can arise from a spelling error.
Source Column does not exist in this row.	The selected source column cannot be found.	There are a mismatched number of columns in the import file and mapped columns in data sync.
Select a Target Field to proceed.	The Advanced button [...] has been selected before a Target Field has been assigned.	You must assign a Target Field before attempting to set up the advanced configuration.
Please provide a valid start point for your data import. If you do not wish to use this option, deselect the checkbox.	The Start Import option has been enabled but the corresponding textbox has been left blank.	Disable this option if you do not wish to use it. If you wish to use this option, enable it and enter the desired text in the textbox.
Please provide a valid end point for your data import. If you do not wish to use this option, deselect the checkbox.	The End Import option has been enabled but the corresponding textbox has been left blank.	Disable the option if you do not wish to use it. If you wish to use this option, enable it and enter the desired text in the textbox.
Please provide text that is to be skipped. If you do not wish to use this option, deselect the checkbox.	The Skip Rows That Contain option has been enabled but the corresponding textbox has been left blank.	Disable the option if you do not wish to use it. If you wish to use this option, enable it and enter the desired text in the textbox.
The "Validate Import Files Contain" field cannot be left blank. If you do not wish to use this option, deselect the checkbox.	The Validate Import Files Contain option has been enabled but the corresponding textbox has been left blank.	Disable the option if you do not wish to use it. If you wish to use this option, enable it and enter the desired text in the textbox.
No file(s) containing text ___ found for "Validate Import Files Contain" setting.	The text entered in the Check Import File Contains field cannot be found in any of the import files.	Ensure that the correct import files have been placed in the File Directory selected. If you do not wish to use this option, disable it to clear the error.
The column delimiter cannot be left blank	The File Format has been assigned but the Column Delimiter has been left blank.	You must enter a Column Delimiter for data sync to read the import file. Either select a value from the dropdown or enter it in the textbox.
The column delimiter contains an invalid regular expression: ___	The Column Delimiter entered is incorrect for the data in the import file(s).	Check what the column delimiter is in the import file(s). For more information, see Data Source (page 14).
The row delimiter cannot be left blank.	The File Format has been assigned but the Row Delimiter has been left blank.	You must enter a row delimiter for data sync to read the import file. Either select a value from the dropdown or enter it in the textbox.
The row delimiter contains an invalid regular expression: ___	The Row Delimiter entered is incorrect for the data in the import file(s).	Check what the row delimiter is in the import file(s). For more information, see Data Source (page 14).

Error Message	Cause	Solution
Row ___ is blank, non-existent or the setup is invalid.	The numeric value selected in the Start At Row setting is invalid.	Check that the number of rows in the import file is greater than the number selected for this option.

Popup Messages

The popup messages are used to inform you that something has been configured incorrectly and must be immediately corrected to proceed.

Message	Explanation
'_' is not a valid selection as it is only a group heading.	This appears when you attempt to add a Target Field in grey which is a heading only. Click OK to return to the Target Fields window. If you wish to add group data, select the green heading which will add the entire group of data to the mapping.
Do you want to delete " _ " field mapping?	This appears when you remove the selection in the File Directory field. If you do not wish to delete the current mapping, click No . If you click Yes , the current configuration will be deleted for that record.
'_' is not a valid selection as it is part of a group. Did you meant to select _GroupData?	This appears when you attempt to add a Target Field that is a part of a group of data that is an invalid selection. You must add the entire group data if you wish to map to a field within the group. Click Yes to add the group data to the mapping, or click No to return to the Target Fields window.

Import Errors

Import errors can arise during the sync process. Some of the more common errors and how to solve them are provided in the table below.

Level	Message	Explanation
Error	The "Use this Field as the Group Data Identifier" option in the Advanced Data Configuration window must be enabled for at least one child field of '_' that has a unique value.	See the Group Data Options heading in the Advanced Data Configuration section (see page 17).
Error	Import file ___ cannot be found in directory ___	The file selected in the Import Filename field cannot be located in the directory provided in the File Directory field.
Error	___ will not be synced as the Unique Field(s) ___ for the following row is blank:	The column that has been configured as the Unique Field is blank for the row stated in the error message.
Error	The "FindID" option in the Advanced Data Configuration is not configured for the SiteID field.	A SiteID has been mapped as a Target Field but the Target Field Record Type in the advanced data configuration window has not been set to Sites.

Level	Message	Explanation
Error	Cannot find Site where Name = ___	The value mapped to the SiteID is not an existing valid site in Protege GX.
Error	Cannot find Controller where Name = ___	The value mapped to the ControllerID is not an existing valid controller in Protege GX.
Error	The ControllerID field must be mapped for ___	The ControllerID has not been mapped – it must be set to the controller that the record is to be assigned to.
Error	The HostControllerRef field must be mapped for ___	The HostControllerRef has not been mapped – it must be set to the controller that the record is to be assigned to.
Error	The "FindID" option in the Advanced Data Configuration is not configured for the ControllerID.	The ControllerID has been mapped as a Target Field but the Target Field Record Type in the advanced data configuration window has not been set to Controllers.
Error	Cannot find ID for ___ where Name = ___	An item with the Name as mapped in the import file cannot be located in Protege GX. For example, Cannot find ID for Access Levels where Name = Warehouse indicates that an access level named Warehouse cannot be found in Protege GX. Check that the access level exists in Protege GX and is assigned to the correct site as mapped in data sync.
Error	Failed to add record ___ where ___ = ___	The AddRecord request sent to SOAP has returned false. For more information, see SOAP Error Codes (next page).
Error	Failed to update ___ where ___ = ___	The UpdateRecord request sent to SOAP has returned false. For more information, see SOAP Error Codes (next page).
Warning	Duplicate ID found: ___ has been overwritten.	Advises the user the record has been overwritten because a record with a duplicate Unique ID has been found in the import file.
Warning	Found more than one ___ where Name = ___. The first instance (ID ___) will be used.	The Find ID option has been assigned for a field that contains more than one record by the name in that field. For example, this error may occur when there are two access levels by the same name. Data sync cannot determine which access level the field is referring to and so the first instance of the access level by that name is used.
Warning	Some rows have not been added correctly - import file(s) will not be deleted.	Occurs when the Delete Import File When Import Completed option is selected and for some other reason (check the other events in the event viewer) one or more rows were not imported and as a result the import file will not be deleted. The import file will only be deleted when every record is imported successfully.
Warning	User PINs will not be synced as the Global setting "Encrypt User PINs" is switched ON in Protege GX.	Occurs when the PINNumber field is mapped while Encrypt User PINs is enabled. The encrypted PINs feature prevents operators from viewing or assigning PINs. Data sync cannot assign a PINNumber when this option is enabled as there is no way to return the system generated PIN while obeying the inherent security feature. Note that all fields with the exception of PINNumber can still be synced.
Warning	User PINs will be updated on every sync as the Site setting "Require Dual Credential for Keypad Access" is switched ON in Protege GX.	Occurs when the PINNumber field is mapped while Require dual credential for keypad access is enabled. When this feature is enabled, operators are not permitted to view user PINs. Because data sync views the existing PIN as '*****' this does not match the numeric PIN in the import file, which triggers an update of the user. A warning will be logged at the beginning of the sync.

Level	Message	Explanation
Warning	User PINs will be updated on every sync as the Operator setting "Show PIN numbers for Users" is switched OFF in Protege GX.	Occurs when the PINNumber field is mapped while Encrypt user PINs and Require dual credential for keypad access are disabled, and Show PIN numbers for users is disabled for the data sync operator. Because the data sync operator is not permitted to view user PINs, data sync views the existing PIN as '****', which does not match the numeric PIN in the import file and triggers an update of the user. A warning will be logged at the beginning of the sync.

SOAP Error Codes

The Failed to add record to table error indicates that the SOAP service has been unable to import one or more users to the target system.

The data sync service identifies which SOAP error has occurred by providing the error code:

Code	Description
-6	Download server is not running
1	Duplicate facility/card number on user
2	Deleting event failure (SQL execution error)
3	Duplicate PIN
4	Duplicate record related to Active Directory
5	Access denied
7	License failure
8	Connection lost/not logged on
10	Clear controller firmware version failed
11*	XML parsing error or empty data in XML string
13	Failed to connect to database
14	Database initialization failed
15	Database report of query failed
47	Duplicate booking (related to Cencon)
50	Data is associated with an invalid record group
53	Failed to get parent record
108	Error in creating download server object or server is not running
201	Event report result set not found
202	Failed to get Event ID range
10000	Duplicate credential
10001	Smart readers over license limitation (Wiegand)
10002	Smart readers over license limitation (RS485)
10003	Smart readers over license limitation (Salto SALLIS)

Code	Description
10004	Smart readers over license limitation (Aperio)
10005	Smart readers over license limitation (Third Party Generic)
16777216	Data parse error
16777217	Date/Time parse error
16777218	Integer parse error
33554432	PIN policy error
33554433	PIN length is less than minimum length
33554434	PIN exceeds maximum sequential digits
33554435	PIN length is less than minimum length and exceeds maximum sequential digits
33554436	PIN exceeds maximum repetitive digits
33554437	PIN length is less than minimum length and exceeds maximum repetitive digits
33554438	PIN exceeds maximum sequential digits and maximum repetitive digits
33554439	PIN length is less than minimum length, exceeds maximum sequential digits and maximum repetitive digits

*Error Code 11 arises from the XML data being incomplete due to the advanced data configuration being incorrect. In many cases this is from the **Find ID** or **Date Time** options being incorrectly configured in Advanced Configuration (see page 17).

Release History

Version 2.0.10.17

- Removed log4net dependency.
- Resolved an issue where the event log file was not being created, causing the service to continually restart without syncing any data.
- Added a warning to advise the operator that user PINs are updated on every sync when the **Require dual credential for keypad access** option is enabled.
- Resolved an issue where duplicate user records were being created when a custom field was used as the unique ID.

Version 2.0.10.18

- Resolved an issue where duplicate user records were being created when two instances of the data sync service were running at the same time. Improved error handling in the data sync service.

This fix requires Protege GX version 4.3.320.1.

Version 2.0.10.19

- Resolved an issue where multiple instances of the same access level assigned to a user with overlapping schedules were not imported correctly.

Version 2.0.10.22

- Resolved an issue where schedules with multiple Unique IDs were duplicated instead of being correctly matched to existing records.
- Resolved an issue where schedules would be imported even if all periods were in the past or more than 7 days in the future.
- Resolved an issue where clicking the **Open Log Folder** button caused a permission error.
- Resolved an issue where switching between record types would cause the **Delete Records Not Present In Import File** setting to be enabled incorrectly.
- Resolved an issue where the service would delete access levels and cards which had been manually added to a user if the import file contained an empty string for those settings.

Version 2.0.10.23

- Improved cybersecurity by removing an unnecessary third-party component.

Version 2.0.10.24

- Resolved an issue where restarting the service would cause a full resync of the data, even when the **Validate Against Last Sync** option was enabled.
- The data sync service will now check the Last Modified date/time of the import file before attempting to resync the data. If the file has not been modified since the last sync, the data sync service will not attempt to resync the data.
- Reduced the delay between the end of one sync and the start of the next, which could cause delays when syncing 100,000+ records.
- Resolved an issue where the **Validate Against Last Sync** and **Delete Records Not Present In Import File** settings were not working together.
- The **Delete Records Not Present In Import File** setting now works when importing multiple files from a specified directory, whereas before it could only be used with single file.
- The data sync service can now generate detailed logs for debugging purposes. For more information, see [Setting the Minimum Log Level \(page 21\)](#).

Version 2.0.10.25

- Resolved an issue where the data sync service could consume excessive CPU resources.

Version 2.0.10.26

- Resolved an issue where the data sync service did not detect changes in an import file when a new version was copied over from another server.

Disclaimer and Warranty

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.

For warranty information, see our [Standard Product Warranty](#).

Designers & manufacturers of integrated electronic access control, security and automation products.
Designed & manufactured by Integrated Control Technology Ltd.
Copyright © Integrated Control Technology Limited 2003-2026. All rights reserved.

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.