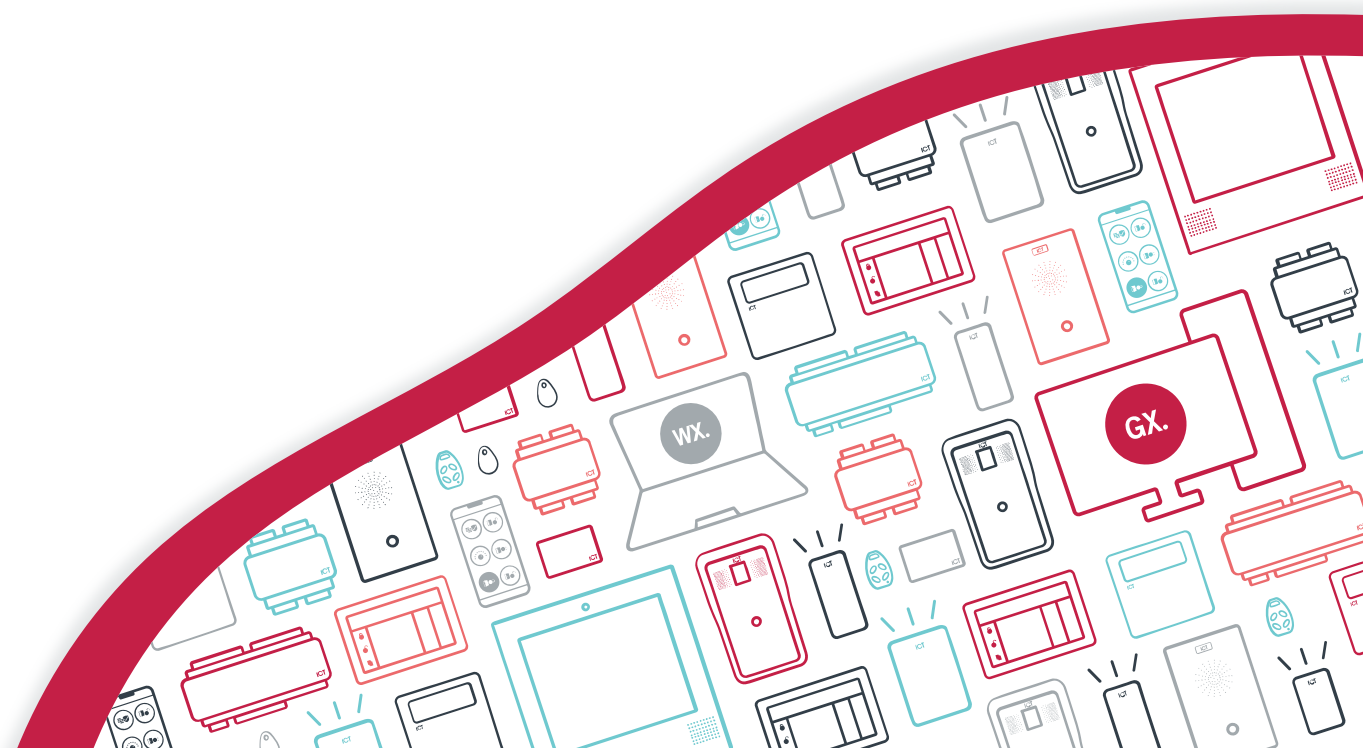
AN-309

Single Record Downloads in Protege GX

Application Note



Last Published: 19-Sep-25 3:44 PM

Contents

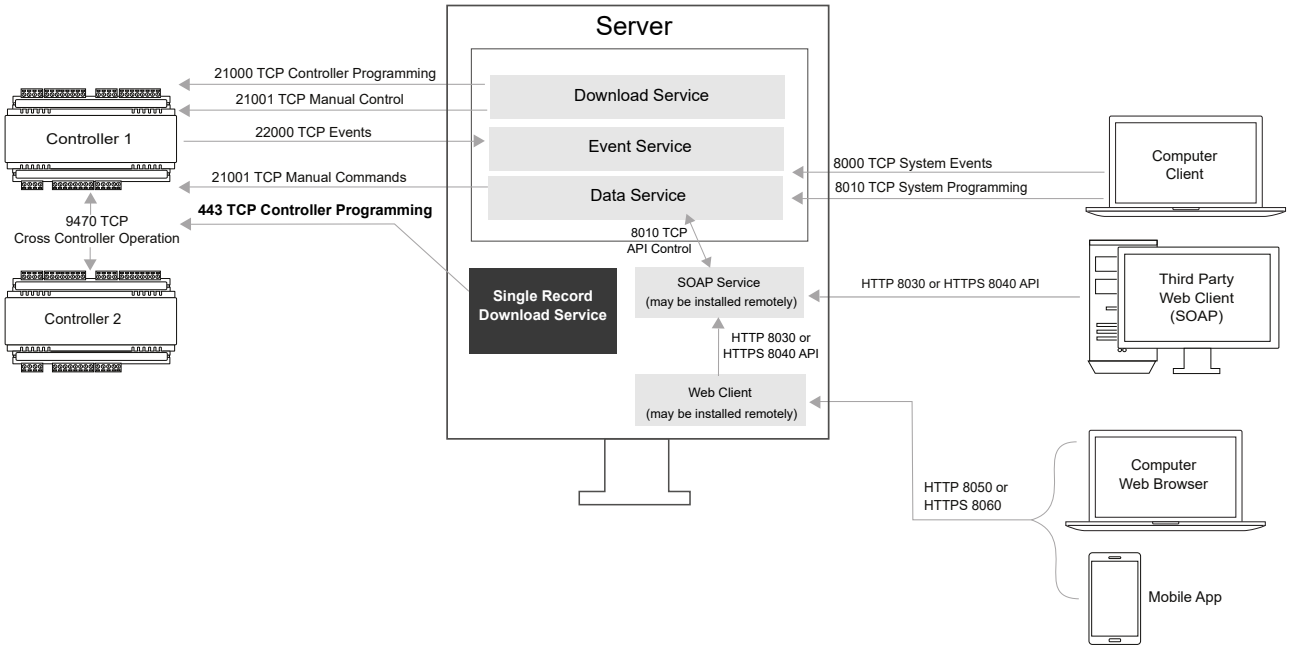
Introduction

Normally when you save a record in the Protege GX software, the Protege GX Download Service performs a full download to each controller that requires the change. In contrast, the Protege GX Single Record Download Service uses a differential download process, only downloading the specific records and fields that have changed in the database.

This service runs in parallel to the existing download service, providing an independent path for single-record changes that need to be downloaded to the controller in a timely fashion. Record changes downloaded by this service are typically received by a controller in under 30 seconds. This reduces download times considerably, especially on large sites with many controllers.

The single record download service monitors the data service for updates to users, access levels and schedules and sends these directly to controllers over HTTPS, independently of regular downloads by the download service. The service can send downloads to all controllers in the system, regardless of what site they are associated with.

After the single record download service has completed a download, it can automatically trigger a full download by the download service.



This application note contains instructions for installing and configuring the single record download service, and enabling and disabling single record downloads.

The single record download service is no longer recommended for new sites. Instead, we recommend the Protege GX Enterprise Download Server as a more powerful and scalable solution for controller downloads. For more information, contact your ICT representative.

Record Types

The single record download service can download changes to the following record types:

- Users
- Access levels
- Schedules

All other changes are handled by the standard download service as normal.

Software Prerequisites

To implement single record downloads, the following prerequisites are required.

Software	Version
Protege GX	4.3.307.2 or higher
Protege GX Single Record Download Service installer	1.0.1.1 or higher

Controller Support

Firmware

Controller	Firmware Version	Notes
Protege GX Controller	2.08.1098 or higher	Controllers must be online with Protege GX and successfully receiving downloads.

Operating System

In addition, the controller needs a specific operating system (OS) to establish the HTTPS connection with the single record download service. The supported operating systems depend on the hardware type of the controller, as older controller hardware does not support newer operating systems.

OS Version	Two-door with USB port	Two-door without USB port	One-door with USB port	One-door without USB port
2.0.25 or higher	✅	N/A	✅	N/A
2.0.20 - 2.0.24	☑	N/A	N/A	N/A
2.0.0 - 2.0.19	❌	N/A	N/A	N/A
1.33.145 or lower	N/A	❌	N/A	❌

✅ = Full support for single record downloads with TLS 1.2

☑ = Support for single record downloads with TLS 1.0. Some limitations apply (see below).

❌ = No support for single record downloads. It may be possible to upgrade the OS to a supported version.

N/A = OS and hardware versions not compatible

Before implementing single record downloads you should check each controller to ensure that it supports this feature. If you have a large number of controllers, you can use the compatibility check portal (see next page). To check individual controllers and determine the precise level of support, follow the process below.

First, identify the hardware type of the controller. Newer controllers have a USB port next to the ethernet port.

- Controllers with USB ports **may** support single record downloads (depending on the operating system).
- Controllers without USB ports **do not** support single record downloads and cannot be retrofitted.

To identify your controller's operating system version:

1. Log in to the web interface and navigate to **Application Software**.
2. Click on the **Current Version** number. This should expand to reveal additional versioning information.
3. Check and record the **OS** version.

If no additional versioning information is displayed when you click on the **Current Version**, the controller's OS is lower than 2.0.20.

Based on the controller's OS version, you will have one of three results:

1. **Version 2.0.25 or higher**: Single record downloads are fully supported with TLS 1.2.
   - No action is required.
2. **Version 2.0.20 - 2.0.24**: Single record downloads are supported with TLS 1.0. This is an older version of HTTPS security which has known vulnerabilities and is not supported by web browsers.
   - **Recommended**: Contact ICT Technical Support for information about upgrading your controller's operating system to a version with full support.
   - If you do implement single record downloads with this OS version, most web browsers will block you from accessing the controller's web interface. You will need to temporarily default the IP address to access the interface. For more information, see Accessing the Controller's Web Interface (page 13).
   - If your Protege GX server blocks earlier versions of TLS, you may need to downgrade the server's security to allow the single record download service to connect to this controller.
3. **Version 2.0.0 - 2.0.19**: Single record downloads are not supported.
   - Contact ICT Technical Support for information about upgrading your controller's operating system to a supported version.

SRDS Compatibility Check Portal

To check large numbers of controllers for compatibility with single record downloads, use the compatibility check portal at https://www.ict.co/SRDS-Compatibility. You will need to provide the serial numbers of the controllers you want to check.

A valid ICT website login is required to access the compatibility check portal.

1. For manual entry, enter controller serial numbers into the search window.

   Each serial number must be entered on a separate row.
2. To upload a TXT or CSV file, click **Choose File** and select the file to upload.
3. Click **Search** to check SRDS compatibility. Results will be displayed in a table below.
   - **Yes** if the controller is compatible.
   - **No** if the controller is incompatible.
   - **Invalid serial number** if the entry is not a recognized serial number.
4. Click **Export** to export the results in a CSV file to your **Downloads** folder.

The portal does not specify what level of support each controller has. To determine this you must check the operating system versions (see previous page).

If compatible the controller will still need to meet the firmware prerequisite as specified above.

Additional Requirements

To complete the installation, you will also need the following information:

- The instance name of the SQL server that contains the Protege GX databases.
- Any networking requirements which may need to be configured for the single record download service. For example, additional configuration may be required if the default HTTPS port (443) is not available, there is port forwarding between the server and controllers, or communications are blocked by a firewall.

  Contact your system administrator to determine all networking requirements.

To communicate with the SQL Server Browser service on a server behind a firewall, you will need to open UDP port 1434, along with the TCP port used by SQL Server (e.g., 1433). This must be done in Windows Firewall and/or your system/network firewalls.

Recommendations for Large Sites

The single record download service typically runs alongside the standard download server. Each time there's a change to users, access levels or schedules, the single record download service quickly sends only that change to all controllers. It then requests a full download from the download server to delete records that are not needed on that controller.

However, during the full download the controller blocks any further access changes from the single record download service. For large sites with frequent access changes, this can cause considerable delays in updating access.

If you are installing the single record download server on an enterprise site, we recommend you estimate how frequently operators will make access changes. Compare this frequency to the time it takes to complete a full download to one controller (using the download server diagnostic window in **Sites | Controllers | General**). **If the time to complete a full download is much longer than the estimated time between access changes, you likely need to use the method outlined below.**

For large sites with frequent access changes, we recommend the following method:

- Use the Windows Task Scheduler to stop the Protege GX Download Service during normal business hours. Only the single record download service will run during these hours. Changes to users, access levels and schedules are downloaded immediately, but changes to other types of records (e.g. configuration changes to doors) will not be sent to controllers.

  Disable the `force_download_after_success` setting (see page 12).

- After business hours, start the Protege GX Download Service. If there have been any changes to records other than users, access levels and schedules, the download service will download them now. It will clean up unneeded records on the controller at the same time.
- If you need to make changes to a very large number of users at once (e.g. adding an access level to 1000 users), do this outside of business hours or run the standard download service temporarily.
- If your site has multiple standard download servers, you can use a maintenance download server to send full downloads to controllers promptly. The maintenance server is running at all times, but usually has no controllers assigned to it. When you need an urgent full download you can assign only the necessary controller to that server to complete the download immediately.

This provides a good balance of updating access quickly, while allowing the system to clean up unneeded records and update configuration overnight.

Setting up Single Record Downloads

Installing the Service

The single record download service is not included with the normal Protege GX installation and must be installed using the separate installer file provided.

1. Open the single record download service installer file provided.
2. The installation wizard will open. Click **Next**.
3. Review the installation directory. Click **Next** to use the default location, or **Change...** to select an alternative directory (if required).
4. Click **Next**.
5. Enter the **Database server**. This is the instance name of the SQL server that contains the Protege GX databases.
   Click **Next**.
6. Click **Install**.
7. You will be prompted to grant administrator permissions. Click **Yes** to begin the installation.
8. Click **Finish** to complete the installation.
9. If there is port forwarding or a firewall in place, you must allow the Protege GX Single Record Download Service to communicate on the network.

Configuring the Controllers

There is some configuration required for each controller before the single record download service can connect to it and begin sending downloads.

For **each** controller that will receive single record downloads, complete the following steps.

In the controller's web interface:

1. In a web browser, log in to the controller's web interface.
2. The single record download service will use an operator login to connect to each controller. Navigate to the **Operators** page and **Add** a new operator.
3. Enter a **Name** (e.g. Single Record Download Service), **Username** and **Password**.
   You will need this Username and Password below.
4. Click **Save**.
5. If you are not using the default HTTPS port (443), update the port that the controller will use to receive communications from the single record download service:
   - Navigate to the **Settings** page.
   - If not already enabled, enable **Use HTTPS** to reveal the HTTPS options.
   - Enter the required **HTTPS Port**.
   - If HTTPS was not previously enabled, disable **Use HTTPS**.
   - Click **Save**.
   - Click **Restart** or power cycle your controller.

In the Protege GX software:

1. Open Protege GX and log in as an administrator operator.
2. Navigate to **Sites | Controllers** and select the controller that you are configuring.
3. Enter the **Username** and **Password** for the new controller operator that you created above.

   The controller's web interface only allows lowercase letters in operator usernames. Ensure that you enter the username here using **all lowercase letters**, otherwise the connection will fail.

4. If you are not using the default HTTPS port (443), enter the **Single record download port** that the single record download service will use to communicate with the controller.
5. Click **Save**.

Repeat the steps above for every controller that will use the single record download service.

Confirming the Service Operation

The single record download service begins communications with controllers as soon as there is a change to one of the supported record types.

To test the single record download service:

1. Navigate to **Users | Users** and add a new user with any settings. Save the record and take note of its **Database ID**.
2. Open the Windows Event Viewer:
   - Press the Windows key + R
   - Type **eventvwr** into the run window.
   - Press **OK**.
3. In the event viewer, open **Windows Logs > Application**.
4. To view logging messages for the single record download service, click **Filter Current Log...** in the right pane. Set the **Event sources** to Protege GX Single Record Download Service and click **OK**.
5. A number of messages will be displayed, showing the actions of the single record download service as it detects the change, initiates communications with each controller, downloads the new record and triggers a full download.

   If the download is successful, you should see a message similar to the following:

   ```
   Record: Table: Users, ID: 1013, Site: 1: Response from
   'https://192.168.1.2/': OK
   ```

6. If the download attempt fails, the single record download service will retry the connection several times. You should see the following message:

   ```
   Error Occurred A task was canceled for Controller 'https://192.168.1.2/'
   ```

When the single record download service is connecting to a controller for the first time, you may see some error messages where the service initially fails to connect to the controller. This is an expected part of the initialization process and does not indicate that the service is not functioning.

Upgrading the Service

To upgrade the single record download service to a new version, simply uninstall the existing service and install the new version.

1. In the Windows settings, navigate to the **Apps & features** section.
2. Locate the Protege GX Single Record Download Service in the list of apps.
3. Click on the app and click **Uninstall**.
4. When the service has been uninstalled successfully, run the new installer provided by ICT.

Additional Operations

This section outlines some additional operations and configuration which might be required when the single record download service is in use.

Enabling and Disabling Single Record Downloads

If you need to enable or disable single record downloads, simply start and stop the Protege GX Single Record Download Service in the Windows Services Manager.

Uninstalling the Service

To uninstall the service, navigate to the Windows Apps & features page. Locate the Protege GX Single Record Download Service in the list, click on it and select **Uninstall**. Follow the instructions to remove the service.

Logging Service Activity

The single record download service provides comprehensive logs to enable you to troubleshoot any issues. Logs are available in the Windows Event Viewer or a separate log file.

To enable logging to a file:

1. Stop the Protege GX Single Record Download Service in the Windows Services Manager.
2. In the File Explorer, navigate to the installation directory of the single record download service.
   The default installation directory is: C:\Program Files (x86)\Integrated Control Technology\Protege GX.
3. Open **GXSV2B.exe.config**.

   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 settings under `<appSettings>`:

   ```
   <add key="sv2b:infrastructure.logging.test.enabled" value="false" />
   <add key="sv2b:logging.level" value="1" />
   ```

5. Set the `logging.test.enabled` value to `true`.
6. Set the `logging.level` to a value from 1 to 3, where 1 provides fewer details and 3 provides more details. It is helpful to start at the lowest value and increase the logging level for more information if required.

   This also affects the level of logging in the Windows Event Viewer.

7. Save the config file.
8. Start the Protege GX Single Record Download Service in the Windows Services Manager.
9. Add or modify a user record to generate some logs.
10. In the File Explorer, browse to C:\temp\SRDS\logs to locate the logs that are generated. You can open these in any text editor. The logs will show the steps the service is taking to connect to the controller and any errors that occur (e.g. incorrect username or password).
11. Once you have finished troubleshooting, it is recommended that you disable logging.
    - In the config file, set `logging.test.enabled` to `false`.
    - Restart the single record download service.

When the single record download service is connecting to a controller for the first time, you may see some error messages where the service initially fails to connect to the controller. This is an expected part of the initialization process and does not indicate that the service is not functioning.

Troubleshooting HTTPS Issues

If the event log indicates an issue with HTTPS, first check that the controller meets the requirements in the prerequisites (see page 5).

In some cases, the single record download service may fail to connect to a controller because it did not successfully restart the controller after enabling HTTPS.

To identify and resolve this issue:

1. Log in to the controller's web interface using the standard HTTP URL. For example: http://192.168.1.2
2. In the **System Settings**, check whether the **Use HTTPS** option is now enabled. If so, the service has partially enabled HTTPS but failed to restart the controller.
3. In the top toolbar, click **Restart**.
4. Make a change to a user record and monitor the Windows event viewer. This time the service should successfully connect and download the change.

Optional Settings

The config file for the single record download service has some optional settings which may improve the performance of the service. The available settings are:

- `access_levels_enable`: When this is `true` (default setting), the single record download service will download access levels to controllers. Change this setting to `false` to exclude access levels from single record downloads and only send them using the standard download service. This may be required when access levels contain a very large number of relationships (e.g. 1000+ doors), as this can cause downloads to partially fail.

  If you enable this setting, you must also upgrade your controller firmware to 2.08.1514 or higher. This resolves an issue where very large access levels fail to download from the standard Protege GX Download Service.

- `force_download_after_success`: When this is `true` (default setting), the service will trigger a full download to each controller after every successful single record download. Change this setting to `false` to disable these additional downloads.
- `only_download_to_online_controllers`: When this is `true` (default setting), the service will download only to controllers that are currently online with Protege GX. Change this setting to `false` to attempt to download to every controller, regardless of whether they are currently online or offline.
- `maximum_message_without_delay`: This setting determines how many messages the service can send to each controller without imposing a delay between messages. The recommended (default) setting is 5.
- `delay_in_milliseconds`: After the service reaches the message limit set above, it will delay each subsequent message for this number of milliseconds after the last response from the controller. The recommended (default) setting is 2000.
- `reset_time_in_milliseconds`: If this time passes without any new messages, the message limit will reset so that the next messages can be sent without delay. The recommended (default) setting is 10000.

If changes are being made by an automated integration, for best performance set the maximum change frequency to 1 second more than the service throttling (e.g. set the `delay_in_milliseconds` to 1 second and the change frequency to 2 seconds).

To edit these settings:

1. Stop the Protege GX Single Record Download Service in the Windows Services Manager.
2. In the File Explorer, navigate to the installation directory of the single record download service.
   The default installation directory is: C:\Program Files (x86)\Integrated Control Technology\Protege GX.
3. Open **GXSV2B.exe.config**.

   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 settings under **<appSettings>** and set each value as required:

```
<add key="sv2b:ingress.database.access_levels.enable" value="true" />
<add key="sv2b:egress.comms.controller.force_download_after_success"
value="true" />
<add key="sv2b:egress.comms.controller.only_download_to_online_
controllers" value="true" />
<add key="sv2b:egress.comms.throttling.maximum_message_without_delay"
value="5" />
<add key="sv2b:egress.comms.throttling.delay_in_milliseconds" value="2000"
/>
<add key="sv2b:egress.comms.throttling.reset_time_in_milliseconds"
value="10000" />
```

5. Save the config file.
6. Start the Protege GX Single Record Download Service in the Windows Services Manager.

Accessing the Controller's Web Interface

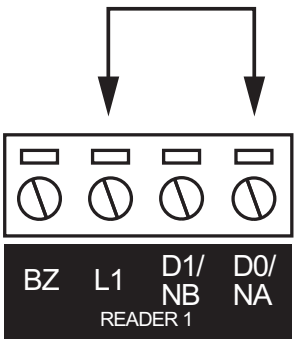
When the single record download service connects it enables HTTPS on the controller so that they can communicate over a secure connection. After setting up single record downloads you must use HTTPS to access the controller's web interface (e.g https://192.168.1.2).

Controllers with older operating systems use TLS 1.0, which is an older, unsupported communication protocol (see Controller Support). In this case most web browsers will block your connection to the web interface.

In this situation you can temporarily default the controller's IP settings. This will revert the controller to HTTP operation until it is next power cycled, allowing you to access the controller and make any required configuration changes.

Defaulting the IP Address of a Two Door Controller

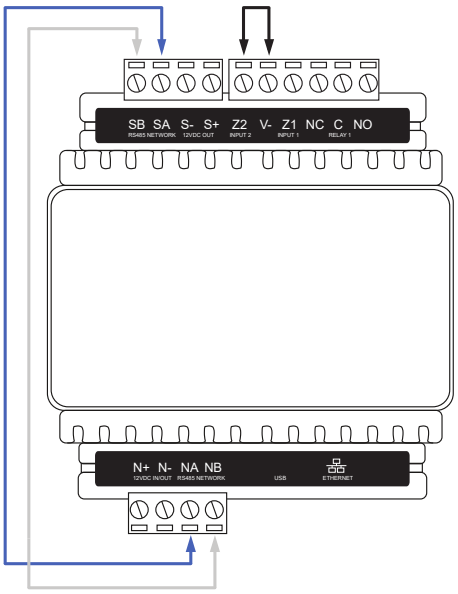
1. Remove power to the controller by disconnecting the 12V DC input.
2. Wait until the power indicator is off.
3. Connect a wire link between **Reader 1** D0 input and **Reader 1** L1 output.



4. Power up the controller. Wait for the status indicator to begin flashing steadily.

Defaulting the IP Address of a Single Door Controller

1. Remove power to the controller by disconnecting the 12V DC input.
2. Wait until the power indicator is off.
3. Connect a wire link between **NA** of the module network and **SA** of the reader network, and between **NB** of the module network and **SB** of the reader network.
4. Connect **Input 2** to ground.



5. Power up the controller. Wait for the status indicator to begin flashing steadily.

Accessing the Controller

5. When the controller starts up it will use the following temporary settings:
   - **IP Address**: 192.168.111.222
   - **Subnet Mask**: 255.255.255.0
   - **Gateway**: 192.168.111.254
   - **DHCP**: Disabled
   - **Use HTTPS**: Disabled
6. Connect to the controller by entering http://192.168.111.222 into the address bar of your web browser, and view or change the IP address and other network settings as required.

   Remember to change the subnet of your PC or laptop to match the subnet of the controller.

7. Remove the wire link(s) and power cycle the controller again.

   The controller will now use the configured network settings.

Using Custom HTTPS Certificates

The single record download service may be used with custom HTTPS certificates, including those obtained from a third-party certificate authority.

If the controller already has a custom certificate installed when the single record download service connects for the first time, the service automatically uses the certificate to communicate via HTTPS. There is no configuration required.

If you wish to use a new custom HTTPS certificate on the controller after the single record download service has connected, complete the following steps:

1. Generate the certificate and load it onto the controller, following the procedure in Application Note 314: Configuring HTTPS Connection to the Protege GX Controller.
2. In Protege GX, navigate to **Sites | Controllers | Configuration**.
3. Expand the **HTTPS public key** section.
4. Delete the existing public key.
5. **Save** the record.

The next time the single record download service connects to the controller, it will use the new certificate to connect.

Defaulting the Controller

After defaulting the controller, you must log in to the web interface and restore any custom network settings to allow it to come online with Protege GX. You will also need to recreate the operator username and password used by the single record download service (see page 8).

In addition, any user-created HTTPS certificates loaded on the controller are deleted when it is defaulted, and the factory certificate is reloaded. If the controller does not have a factory default certificate, it reverts to HTTP operation.

If you are using the factory default certificate, no further changes are required. The single record download service should reconnect to the controller automatically.

If you are using a custom HTTPS certificate, reload the same custom certificate onto the controller via the web interface, following the instructions in Application Note 314: Configuring HTTPS Connection to the Protege GX Controller. The single record download service will connect to the controller using this certificate next time there is a change that needs to be downloaded.

If you are using an automatically generated certificate, there are some additional steps you must complete to prompt the single record download service to generate a new certificate:

1. You must delete the existing public key from the Protege GX server. If the public key in the server does not match the controller's certificate, or the controller does not have a certificate, the single record download service will not connect to the controller.
   - Navigate to **Sites | Controllers | Configuration**.
   - Expand the **HTTPS public key** section.
   - Delete the existing public key.
   - **Save** the record.
2. Due to a known issue, the single record download service will not generate a new certificate if it has connected to this controller over HTTPS previously. To work around this issue, restart the single record download service. The next time the service sends a download, it will install a new certificate on the controller.

Protecting Controller Credentials

The username and password for each controller are stored in plain text in the Protege GX database. To prevent attackers from obtaining these credentials we recommend that you implement Transparent Data Encryption (TDE). This SQL Server security feature encrypts the databases and backup files on the disk, then decrypts them when they are accessed by an authorized application such as the Protege GX software.

For more information and instructions for enabling TDE, see the Protege GX Server Installation Manual.

Multiple Download Servers

If your site has multiple standard download servers, there are two options for using the single record download service:

1. Use one single record download service installation for the entire system. This service sends downloads to every controller.
2. Install a separate single record download service instance for each standard download server that needs single record downloads. Each instance only sends downloads to the controllers connected to one of the download servers.

By default, the single record download service sends records to all controllers (option 1). Do not set the **Download server parent** when using this method.

If you wish to use multiple service instances (option 2), set the download server parent for each instance as follows:

1. Install one instance of the single record download service per download server that needs one (see page 8).
2. In Protege GX, navigate to **Global | Download server**.
3. Select the Single Record Download Server record. This record was created when the first single record download service was installed.
4. Set the **Download server parent** to the primary standard download server. This restricts the single record download service to only send records to the controllers managed by this download server.
5. Click **Save**.
6. Add a new download server record for each single record download service installed, with the following settings:
   - **Download server type**: Single record
   - **Download server parent**: Set to the corresponding standard download server.

Column Encryption

Some features in Protege GX use encrypted database columns to keep your data secure:

- PIN encryption
- ICT wireless locking

Some additional configuration is required to enable the single record download service to read encrypted columns.

1. Stop the Protege GX Single Record Download Service in the Windows Services Manager.
2. In the File Explorer, navigate to the installation directory of the single record download service.
   The default installation directory is: C:\Program Files (x86)\Integrated Control Technology\Protege GX.
3. Open GXSV2B.exe.config.

   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 connection string:

```
<add name="Main" connectionString="Trusted_Connection=yes;
TrustServerCertificate=yes; Encrypt=yes; Server=[DatabaseServer];
Database=[MainDatabase]; max pool size=2000;" />
```

5. Add the text in bold:

```
<add name="Main" connectionString="Trusted_Connection=yes;
TrustServerCertificate=yes; Encrypt=yes; Server=[DatabaseServer];
Database=[MainDatabase]; max pool size=2000; Column Encryption
Setting=Enabled;" />
```

6. Save the config file.
7. Start the Protege GX Single Record Download Service in the Windows Services Manager.

Azure Deployment

If you have deployed the Protege GX server to Microsoft Azure, you will need to modify the config file for the single record download service to allow it to connect.

For more information, see Application Note 281: Deploying Protege GX on Microsoft Azure.

1. Stop the Protege GX Single Record Download Service in the Windows Services Manager.
2. In the File Explorer, navigate to the installation directory of the single record download service.
   The default installation directory is: C:\Program Files (x86)\Integrated Control Technology\Protege GX.
3. Open GXSV2B.exe.config.

   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 connection string:

   ```
   <add name="Main" connectionString="Trusted_Connection=yes;
   TrustServerCertificate=yes; Encrypt=yes; Server=[DatabaseServer];
   Database=[MainDatabase]; max pool size=2000;" />
   ```

5. Replace this connection string with the following example, replacing the terms in square brackets with the information for your installation:

   ```
   <add name="Main" connectionString="Trusted_Connection=no; User ID=
   [SQLUsername]; Password=[SQLPassword]; TrustServerCertificate=no;
   Encrypt=yes; Server=tcp:[SQLServerName].database.windows.net,1433;
   Database=ProtegeGX; max pool size=2000;" />
   ```

6. Save the config file.
7. Start the Protege GX Single Record Download Service in the Windows Services Manager.

Appendix: Service Capabilities

Notes and Limitations

- To avoid overwhelming the controller, the service throttles the number of changes it can send over a certain time period. It can send up to 5 changes without any delay between them, then delays each new change by 2 seconds after the controller's last successful response. If there are no new changes for 10 seconds, the cycle resets so that the next changes can be sent without delay.

  These values can be modified in the config file for the service (see page 12).

- If the single record download service fails to download changes to a controller, it will try to send the data 6 more times, waiting a few seconds between each attempt. If these attempts fail, it will resend the data every 5 minutes until it is successful.
- The single record download service downloads all records to all controllers that it services, regardless of whether the controller will use that record. For example, a user record will be downloaded to all controllers even if it does not have an access level set.

  When the controller next receives a full download, any unnecessary records will be deleted.

- The download server diagnostic window in **Sites | Controllers | General** does not display information for the single record download service. You can enable logging for the service if required (see page 11).
- The single record download service can only download supported records (see page 4). Any unsupported records will only be downloaded by the standard download service, even if they are used by a supported record.

  For example, if a new door is created then added to an access level, the access level will not grant access to the door until the new door record has been downloaded by the standard download service.

Validated Items

The following items have been validated to be working correctly with the single record downloads feature.

Sites | Schedules

- Add schedule
- Delete schedule
- **Configuration** tab
  - Name
  - Period 1
  - Period 2
  - Period 3
  - Period 4
  - Period 5
  - Period 6
  - Period 7
  - Period 8
- **Options** tab
  - Validate schedule if qualify output on
  - Validate schedule if qualify output off
  - Qualify output
- **Holiday groups** tab
  - Add
  - Delete
  - ID

Users | Users

- Add user
- Delete user
- **General tab**
  - Name
  - Default language
  - PIN
  - PIN expiry time
  - Facility
  - Card number
  - Facility (biometric)
  - Card number (biometric)
  - User expiry date/time start
  - User expiry date/time start value
  - User expiry date/time end
  - User expiry date/time end value
  - User area
  - Reporting ID
  - Credentials add
  - Credentials delete
  - Credential type

    - Credentials disabled
    - Credential value
    - Credentials start
    - Credentials start value
    - Credentials end
    - Credentials end value
- **Access levels** tab
    - Add
    - Delete
    - ID
    - Access level expires
    - Expiry start
    - Expiry end
    - Schedule
- **Options** tab
    - Show a greeting message to user
    - Go directly to the menu on login (no area control)
    - User can acknowledge alarm memory
    - Show alarm memory on login
    - Turn off the primary area if user has access on login
    - Turn off the user area on login if user has access
    - Acknowledge system troubles
    - Treat user PIN plus 1 as duress
    - User has super rights and can override antipassback
    - User operates extended door access function
    - User loiter expiry count enabled
    - User can edit user settings from keypad
    - User is a duress user
    - Rearm area in stay mode
    - Dual custody master
    - Dual custody provider

Users | Access Levels

- Add access level
- Delete access level
- **General** tab
    - Name
    - Operating schedule
    - Time to activate output (seconds)
    - Reader access activates output
    - Keypad access activates output
    - Activate output until access level expiry
    - Toggle access level output
    - Enable multi-badge arming
    - Use access level door type
    - Enable usage restriction

    - Commands
    - Elevator destination floor
- **Doors** tab
    - Add
    - Delete
    - ID
    - Schedule
    - Access direction
- **Door groups** tab
    - Include all doors
    - Add
    - Delete
    - ID
    - Schedule
- **Floors** tab
    - Add
    - Delete
    - Schedule
- **Floor groups** tab
    - Add
    - Delete
    - Schedule
- **Elevator groups** tab
    - Add
    - Delete
    - Schedule
- **Menu groups** tab
    - Add
    - Delete
    - Schedule
- **Arming area groups** tab
    - Add
    - Delete
    - Schedule
- **Disarming area groups** tab
    - Add
    - Delete
    - Schedule
- **Outputs** tab
    - Add
    - Delete
    - ID
- **Output groups** tab
    - Add
    - Delete
    - ID

Release History

This release history covers changes to the single record download service beginning from version 1.0.0.2.

Version 1.0.0.4

- Resolved an issue where adding and immediately deleting a user record while a full download was in progress could cause the single record download service to fail and not recover.
- Resolved an issue where the service could not successfully install a self-signed certificate on the controller in environments with older operating systems.

  This fix requires Protege GX version 4.3.320.9 or higher.

Version 1.0.0.5

- Added an option to disable the full download which occurs after a single record download (see page 12).
- Added an option to disable downloads to controllers that are not currently online (see page 12).
- Resolved an issue where the single record download service would trigger a download when a user record was saved without any changes, or with changes only to fields that are not downloaded to the controller. Now user downloads are only triggered when there are changes to fields which need to be downloaded to the controller.

  This fix requires Protege GX software version 4.3.344.1.

Version 1.0.0.7

- Resolved an issue where the **Access direction** settings in access levels were being downloaded with incorrect values, which could prevent users from accessing doors.

Version 1.0.1.0

- Increased the rate at which the service can send downloads to the controller. The service applies progressive throttling to avoid overwhelming the controller. For more information, see Notes and Limitations (page 18).
- Logs can now be written to a log file as well as the Windows Event Viewer. For more information, see Logging Service Activity (page 11).

Version 1.0.1.1

- Updated the single record download service to support controllers on firmware version **2.08.1403 and higher**. If you upgrade the controller firmware, you **must** also upgrade the single record download service.

  The service is still back-compatible with previous controller firmware versions.

Version 1.0.1.2

- Resolved an issue where the PendingRecordsForController table grew continuously.

Version 1.0.1.3

- Resolved an issue where single record downloads were delayed because they were regularly failing with the error <Invalid Session><invalid session id>.

Version 1.0.1.5

- You can now disable access level downloads from the single record download service. This may be required when access levels contain a very large number of relationships (e.g. 1000+ doors), as this can cause downloads to partially fail. For more information, see Optional Settings (page 12).

  If you enable this setting, you must also upgrade your controller firmware to 2.08.1514 or higher. This resolves an issue where very large access levels fail to download from the standard Protege GX Download Service.

- The single record download service will no longer attempt to download to controllers that are using the enterprise download server.

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