



**AN-290**

# Setting up a Secondary Protege GX Download Server

Application Note



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 2003-2025. All rights reserved.

Last Published: 30-May-25 11:58 AM

# Contents

Setting Up a Secondary Download Server .....	4
Prerequisites .....	4
Preparation .....	5
Server Configuration .....	8
Connection Strings prior to 4.3.289.1 .....	9
Notes on Secondary Download Server Operation .....	9
Encrypted Database Columns .....	10
Data Service Encryption Certificate Export .....	10
Data Service Encryption Certificate Import .....	11

# Setting Up a Secondary Download Server

As the Protege GX system grows, the time taken for data to be downloaded to controllers increases. In situations where it is important that changes are expedited (e.g. new user records created in a visitor management system), delays can be troublesome.

One effective solution is to implement a secondary Protege GX Download Server to share the load of performing the download to controllers. With a second server performing downloads to controllers, the same data is transferred twice as fast as when using a single download server.

Alternatively, the Protege GX Single Record Download Service can expedite downloads of users, access levels and schedules. For more information, see [Application Note 309: Single Record Downloads in Protege GX](#).

## Prerequisites

The following prerequisites, preparation and steps are required to set up a secondary Protege GX installation to function as a Secondary Download Server.

### Software Requirements

Software	Version
Protege GX software	4.3.279.1 or higher

### Hardware Requirements

- A new Windows Server (PC or VM) to be used as the secondary Protege GX download server.
- A functional network connection linking both servers to each other, and both servers to all Protege GX DIN rail controllers.

### Protege GX Licensing Requirements

Each additional download server requires a new Protege GX Software Serial Number (SSN) with exactly the same licensed items as the existing installation. ICT does not charge for the new SSN or duplicate licensed items.

# Preparation

---

Both servers require preparation before configuring the connection.

## Prepare the Primary Protege GX Server

---

### Step 1: Manage Authentication for SQL Server

The secondary download server must be able to log in to SQL Server to access the Protege GX databases. The server's account needs the following permissions for both databases:

- CONNECT
- EXEC
- db\_datareader
- db\_datawriter

There are two methods for achieving this:

- **SQL Server Authentication:** The second machine logs in to the SQL Server with a username and password.
- **Windows Authentication:** If both machines are joined to a Windows Active Directory domain, the secondary download server can connect with Windows Authentication. Contact the site's IT team for assistance.

The following instructions cover how to set up **SQL Server Authentication**:

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

It is highly recommended that you use a strong password. Save this password to a password manager or other secure location.

13. Disable **Enforce password expiration**. This prevents the service from periodically losing access to the database when the password expires.
14. Disable **User must change password at next login**.
15. In the **User Mapping** section, select **ProtegeGX**.
16. Enable **db\_datareader** and **db\_datawriter**.
17. Repeat for **ProtegeGXEvents**.
18. Click **OK**.
19. Click **New Query** and enter the following:

```
GRANT EXEC ON ProtegeGX TO [new_username]
GRANT EXEC ON ProtegeGXEvents TO [new_username]
```

20. Click **Execute**.
21. Right click on the instance name and select **Restart**.

This will also stop some Protege GX services.
22. To ensure that the new user is configured correctly, open a new instance of SQL Server Management Studio.
23. Set **Authentication** to SQL Server Authentication and attempt to log in with the new credentials. You should be able to log in successfully and view the ProtegeGX database.
24. Open the Services manager. Start the **Protege GX Data Service** and **Protege GX Download Service**.

### Step 2: Enable TCP/IP Protocol on the Primary SQL Server

1. From the Windows Start menu, launch **SQL Server Configuration Manager**.
2. Navigate to **SQL Server Network Configuration > Protocols for <INSTANCENAME>**.
3. Right click the **TCP/IP** Protocol and select **Enable**.
4. Navigate to **SQL Server Services**.
5. Restart the **SQL Server <INSTANCENAME>** service.
6. Close SQL Server Configuration Manager.

### Step 3: Enable SQL Server Browser Service

1. Open **Services** as an administrator:
  - Press the **Windows + R** keys.
  - Type **services.msc** into the search bar.
  - Press **Control + Shift + Enter**.
2. For the **SQL Server Browser** service, set the **Startup Type** to Automatic, then click **OK**.
3. Right click the SQL Server Browser service and select **Start**.
4. Close the Services window.

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.

## Prepare the Secondary Protege GX Server

---

Note: The secondary server will require SQL Server installed locally for the initial installation of Protege GX. However, this will not be used once Protege GX is reconfigured to operate as a secondary download server.

### Step 1: Install SQL Server

Install a supported version of SQL Server as per a standard Protege GX installation. No special changes are required for the secondary server.

### Step 2: Install Protege GX

Install the same version of Protege GX as installed on the primary server, using the newly issued SSN. Follow all the default settings and point to the locally installed SQL Server Instance on the secondary server.

### Step 3: License the Server

Log in to Protege GX on the secondary server and apply the appropriate server license.

### Step 4: Disable Protege GX Services

Open **Services** as an administrator:

- Press the **Windows + R** keys.
- Type **services.msc** into the search bar.
- Press **Control + Shift + Enter**.

1. Stop all Protege GX services on the secondary server by stopping the update service.
2. Open the **Properties** and change the **Startup Type** to Disabled for the following services only:
  - Protege GX Data Service
  - Protege GX Event Service
  - Protege GX DVR Service A
  - Protege GX DVR Service B

# Server Configuration

---

For the secondary Protege GX installation to connect to the primary SQL Server, additional configuration is required to allow remote connections.

## Step 1: Configuring the Protege GX Connection Strings on the Secondary Server

On the secondary Protege GX server:

1. Navigate to **C:\Program Files (x86)\Integrated Control Technology\Protege GX**.
2. Open the **GXSV2.exe.config** file using 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.

3. Locate the **<connectionStrings>** node. Replace it with the following:

```
<connectionStrings>
    <add name="MainConnection" connectionString="Provider=MSDASQL;Extended
Properties="Driver={ODBC Driver 17 for SQL Server};Server=<PRIMARY_
SERVER_IP>\ProtegeGX;Database=ProtegeGX
;UID=<USERNAME>;PWD=<PASSWORD>;TrustServerCertificate=yes;Encrypt=yes;Colu
mnEncryption=Enabled;" " />
    <add name="EventConnection" connectionString="Provider=MSDASQL;Extended
Properties="Driver={ODBC Driver 17 for SQL Server};Server=<PRIMARY_
SERVER_IP>\ProtegeGX;Database=ProtegeGXEvents
;UID=<USERNAME>;PWD=<PASSWORD>;TrustServerCertificate=yes;Encrypt=yes;Colu
mnEncryption=Enabled;" " />
</connectionStrings>
```

Notes:

- Replace **<PRIMARY\_SERVER\_IP>** with the IP address of the server where the databases are hosted.
- If you are using SQL Server authentication, replace **<USERNAME>** and **<PASSWORD>** with the login created above.
- If you are using Windows authentication, replace **UID=<USERNAME>;PWD=<PASSWORD>** with **Trusted\_Connection=yes**
- The connection strings above apply for Protege GX versions 4.3.289.1 and higher. For earlier versions, see Connection Strings prior to 4.3.289.1.

4. Save the config file.

## Step 2: Add Download Server in Protege GX

To configure the additional download server in the Protege GX database:

1. Open Protege GX on the primary server and log in.
2. Navigate to **Global | Download servers** and create a new download server record.
3. In the **Computer name** enter the PC hostname of the secondary Protege GX server.
4. Save the record.

## Step 3: Starting the Secondary Download Services

On the secondary server, start the **Protege GX Download Service**.

## Step 4: Verification

All necessary Protege GX services should now be running correctly. This includes all Protege GX services on the primary server, and the Protege GX download service on the secondary server.



1. Log in to Protege GX.
2. Navigate to **Sites | Controllers**.
3. Multi-select the controllers which should receive downloads from the secondary server and change their **Download server** setting to the secondary download server record created above.
4. Click **Save**.
5. Make a change to any record in Protege GX that will be downloaded to all controllers, and save that change.
6. Wait for the download to occur.
7. Once the controllers have downloaded, on the secondary server machine navigate to the **C:\ProgramData\Integrated Control Technology\Protege GX\Download** folder. You should be able to see the .dat file for the controllers that are configured to download via the Secondary Server, but not the .dat file for the controllers configured for the primary server.
8. Once this is confirmed, the secondary download server is fully operational.

## Connection Strings prior to 4.3.289.1

In Protege GX versions prior to 4.3.289.1, the following connection strings should be used.

```
<connectionStrings>
  <add name ="MainConnection" connectionString="Provider=MSOLEDBSQL;
TrustServerCertificate=yes; Encrypt=yes; Server=<PRIMARY_SERVER_IP>\ProtegeGX;
Database=ProtegeGX; Persist Security Info=False; User ID=<USERNAME>;
Password=<PASSWORD>; "/>
  <add name ="EventConnection" connectionString="Provider=MSOLEDBSQL;
TrustServerCertificate=yes; Encrypt=yes; Server=<PRIMARY_SERVER_IP>\ProtegeGX;
Database=ProtegeGXEvents; Persist Security Info=False; User ID=<USERNAME>;
Password=<PASSWORD>; "/>
</connectionStrings>
```

## Notes on Secondary Download Server Operation

- It is not possible to view the Download Server Diagnostic Window for additional download servers. When you open the diagnostic window from the controller programming it will provide diagnostics for the primary server, regardless of that controller's selected **Download server**.
- The primary download server restarts automatically once every 24 hours, but secondary download servers do not. If this is needed, it is recommended that you create a Windows scheduled task to restart the Protege GX Download Service on the secondary server.

# Encrypted Database Columns

---

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

- PIN encryption
- ICT wireless locking

When you restore the database to a secondary download server, you must also import the Data Service Encryption Certificate to allow that database to encrypt and decrypt those columns.

Secondary download servers will not be able to read or use encrypted columns until the certificate has been imported.

The required steps are:

1. Stop the Protege GX Download Service on all secondary servers.
2. Export the self-signed certificate from the primary server (see below).
3. Import the certificate to all Protege GX secondary download servers (see next page).
4. Start the Protege GX Download Service on all secondary servers.

## Data Service Encryption Certificate Export

To create a backup of the certificate you will need to access the Certificate Manager tool on the machine where the certificate exists, to create an **export** of the Data Service Encryption Certificate.

The certificate is created on the machine where the data service is installed, which may not be the same machine as the SQL server installation.

1. To open the Certificate Manager tool as an administrator, press the **Windows + R** keys, then type **certlm.msc** into the search bar and press **Control + Shift + Enter**.
2. The tool directory will display Certificates - Local Computer.
3. Open the **Personal** folder, then click the **Certificates** sub-folder.
4. In the window displaying the certificates, scroll across to the **Friendly Name** column and locate the certificate called Data Service Encryption Certificate.
5. Right click the certificate and select **All Tasks > Export**.
6. The **Certificate Export Wizard** will open. Click **Next**.
7. You must select the **Yes, export the private key** option.

The private key is the critical component in decryption. If you do not export the private key, when the certificate is imported it will not be able to decrypt the encrypted data.

Then click **Next**.

8. Ensure that the following **Export File Format** options are selected:
  - **Include all certificates in the certification path if possible**
  - **Enable certificate privacy**

The **Delete the private key if the export is successful** option **must be disabled**.

Then click **Next**.

9. On the **Security** page, enter and confirm a strong **Password**.

This should be saved securely with important site information.

10. Set **Encryption** to AES256-SHA256, then click **Next**.

11. Specify an export **File name** and path, then click **Next**.
12. Click **Finish** to complete the certificate export.
13. When the export is complete, confirm that the certificate backup .pfx file has been exported to the file path as specified.
14. The file should be stored securely in a separate location to ensure that it is available if required.

You must back up the certificate and the password used to encrypt the private key in a secure location. If these are lost, it will not be possible to restore database backups to another server.

## Data Service Encryption Certificate Import

To import the self-signed certificate you will need to access the Certificate Manager tool and **import** the .pfx backup of the Data Service Encryption Certificate.

1. Ensure that the .pfx backup file is accessible from the local PC.
2. Stop all Protege GX services before initiating the import.
3. To open the Certificate Manager tool as an administrator, press the **Windows + R** keys, then type **certlm.msc** into the search bar and press **Control + Shift + Enter**.
4. The tool directory will display Certificates - Local Computer.
5. Open the **Personal** folder.
6. Right click the **Certificates** sub-folder and navigate to **All Tasks**, then select **Import**.
7. The **Certificate Import Wizard** will open. Click **Next**.
8. Click **Browse...** and locate the .pfx backup file to import, then click **Next**.

You will need to change the file type dropdown to Personal Information Exchange (\*.pfx;\*.p12).

9. Enter the **Password** that was created during the export process.
10. Import Options:
  - **Mark this key as exportable. This will allow you to back up or transport your keys at a later time.**
    - This option must be selected if you want to be able to export/backup the private key with this certificate in the future. This option is slightly less secure.
    - The key is more secure if this option is not selected, however you will not be able to export the private key with the certificate in the future if you lose your current .pfx backup file.
  - Ensure that **Include all extended properties** is selected.
11. Click **Next**.
12. Ensure the **Certificate store** is set to Personal, then click **Next**.
13. Click **Finish** to complete the certificate import.
14. Close the Certificate Manager tool.
15. Restart the Protege GX services.

Designers & manufacturers of integrated electronic access control, security and automation products.  
Designed & manufactured by Integrated Control Technology Ltd.  
Copyright © Integrated Control Technology Limited 2003-2025. 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.