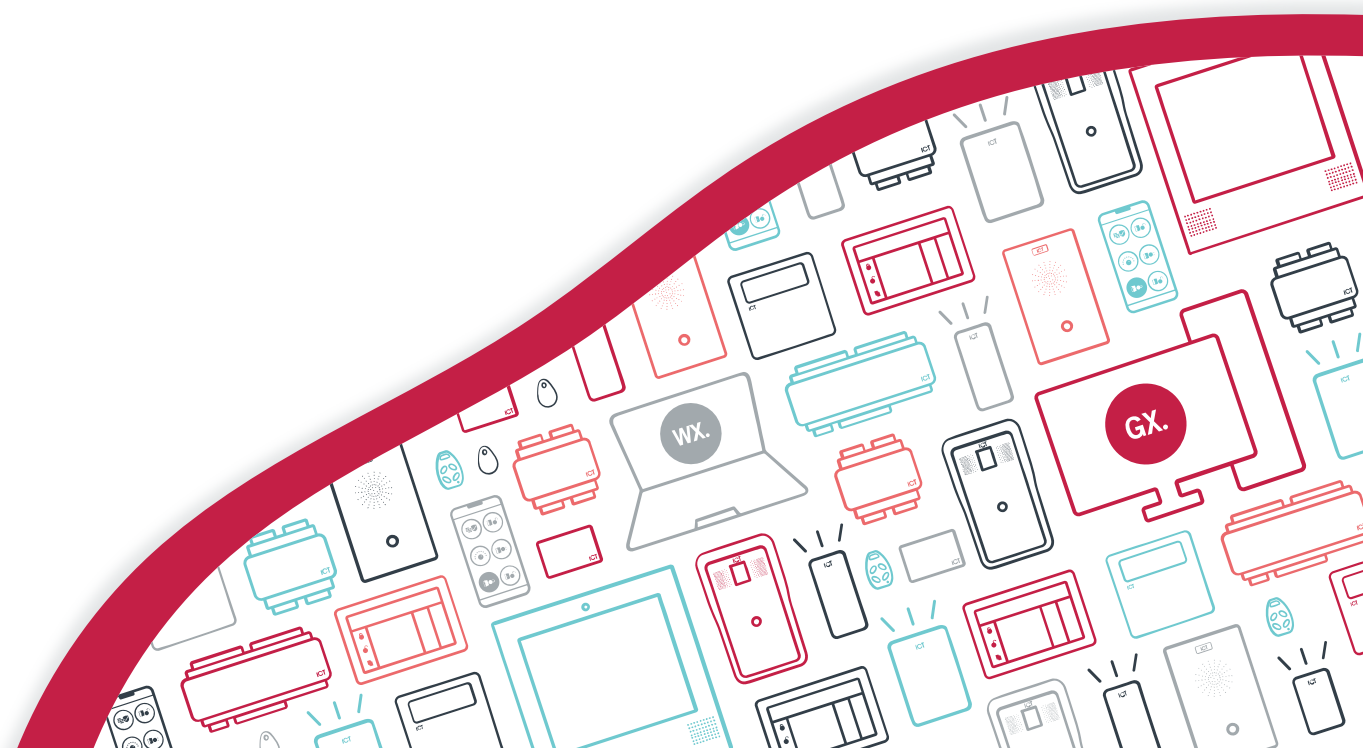
AN-290

Setting up a Secondary Protege GX Download Server

Application Note



Last Published: 22-Nov-23 8:56 AM

Contents

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: Edit the SQL Server Setup

When installed as part of a standard Protege GX installation, Microsoft SQL Server is configured to operate in Windows Authentication mode only. For a secondary download server to be able to connect to the database, this mode needs to be changed to Mixed Mode Authentication.

1. Open **Microsoft SQL Server Management Studio** and log in to the instance that hosts the Protege GX database.
2. At the top of the Object Explorer tree, right click the Instance name and select **Properties**.
3. Select the **Security** page, then under **Server authentication** select **SQL Server and Windows Authentication Mode**.
4. Click **OK**.
5. In the Object Explorer tree, expand **Security > Logins**, then right click the sa user account and select **Properties**.
6. Enter a **Password** for the sa user and click **OK**.

   It is highly recommended that this be a very strong password known only to authorized people.
7. Click on the **Status** page, and in the **Login** section select **Enabled**.
8. Click **OK**, then close SQL Server Management Studio.

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 the **Services** snap-in by:
   - Pressing the **Windows + R** keys
   - Typing **services.msc** into the search bar and pressing **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

1. Open the **Services** snap-in by:
   - Pressing the **Windows + R** keys
   - Typing **services.msc** into the search bar and pressing **Enter**
2. Stop all Protege GX services on the secondary server by stopping the update service.
3. 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. Replace the existing connection strings with the modified connection strings shown below, updating the following variable fields as required:
   - Replace <PRIMARY_SERVER_IP> with the IP address of the Protege GX Primary Server.
   - Replace <SYS_ADMIN_PASSWORD > with the password you created for the system administrator account on the Protege GX Primary Server.

   The connection strings below are relevant for Protege GX software version 4.3.289.1 and later. For earlier versions, use the alternative connection strings provided below (see next page).

   GXSV2.exe.config Original Connection Strings:

```
<connectionStrings>
  <add name="MainConnection" connectionString="Provider=MSDASQL; Extended
Properties=&quot; Driver={ODBC Driver 17 for SQL Server}; Trusted_
Connection=yes; TrustServerCertificate=yes; Encrypt=yes;
Server=localhost\ProtegeGX; Database=ProtegeGX;"/>
  <add name ="EventConnection" connectionString="Provider=MSDASQL;
Extended Properties=&quot; Driver={ODBC Driver 17 for SQL Server};
Trusted_Connection=yes; TrustServerCertificate=yes; Encrypt=yes;
Server=localhost\ProtegeGX; Database=ProtegeGXEvents;"/>
</connectionStrings>
```

   GXSV2.exe.config Modified Connection Strings:

```
<connectionStrings>
  <add name ="MainConnection" connectionString="Provider=MSDASQL; Extended
Properties=&quot; Driver={ODBC Driver 17 for SQL Server};
TrustServerCertificate=yes; Encrypt=yes; Server=<PRIMARY_SERVER_
IP>\ProtegeGX; Database=ProtegeGX; Persist Security Info=False; UID=sa;
PWD=<SYS_ADMIN_PASSWORD>;&quot;"/>
  <add name ="EventConnection" connectionString="Provider=MSDASQL;
Extended Properties=&quot; Driver={ODBC Driver 17 for SQL Server};
TrustServerCertificate=yes; Encrypt=yes; Server=<PRIMARY_SERVER_
IP>\ProtegeGX; Database=ProtegeGXEvents; Persist Security Info=False;
UID=sa; PWD=<SYS_ADMIN_PASSWORD>;&quot;"/>
</connectionStrings>
```

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.

GXSV2.exe.config Original Connection Strings:

```
<connectionStrings>
  <add name="MainConnection" connectionString="Provider=MSOLEDBSQL; Trusted_
Connection=yes; TrustServerCertificate=yes; Encrypt=yes;
Server=localhost\ProtegeGX; Database=ProtegeGX;"/>
  <add name ="EventConnection" connectionString="Provider=MSOLEDBSQL;
Trusted_Connection=yes; TrustServerCertificate=yes; Encrypt=yes;
Server=localhost\ProtegeGX; Database=ProtegeGXEvents;"/>
</connectionStrings>
```

GXSV2.exe.config Modified Connection Strings:

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

User PIN Encryption

For sites with user PIN encryption enabled, some additional configuration is required for the **Encrypt User PINs** feature to work with secondary download servers.

As part of user PIN encryption a Data Service Encryption Certificate exists on the primary server. This certificate is the key to encrypting and decrypting PIN data in the database and must be installed on all secondary download servers in order for them to apply and recognize the same PIN encryption.

Secondary servers will not be able to read user PINs 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, press the **Windows + R** keys, then type **certlm.msc** into the search bar and press **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 with the assigned friendly name Data Service Encryption Certificate.
5. Right click the certificate and navigate to **All Tasks**, then select **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**.

   Ensure the password is recorded and stored securely with important site information.
10. Ensure that **Encryption** is set 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. The export wizard should verify that 'The export was successful'.
14. Confirm that the certificate backup .pfx file has been exported to the file path as specified.
15. The file should be stored securely in an alternate location to ensure that it is available if required.

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, press the **Windows + R** keys, then type **certlm.msc** into the search bar and press **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 selection 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. The import wizard should verify that 'The import was successful'.
15. Close the Certificate Manager tool.
16. Restart the Protege GX services.

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