AN-368

Migrating Protege GX to a New Server

Application Note

Last Published: 26-Jun-26 1:21 PM

Contents

Introduction

Migrating the Protege GX system to a new server is a common maintenance task, especially when you take over an existing site. The new server might be a physical machine with modern hardware and operating system, or, perhaps more commonly these days, a virtual machine (VM) hosted by a cloud provider.

Regardless of the format, it is important to carry out the migration carefully to ensure that the system functions correctly afterwards. To assist with this process, this application note outlines the key requirements for migrating a Protege GX server to a new physical or virtual machine.

You should read this document alongside the Protege GX Installation Manual as you install the new server.

General Tips

- To perform the migration, you will need administrator rights on the existing server, the new server and the SQL Server instance.
- Always coordinate with the organization's IT administrator before you make any changes to the network or firewalls.
- This document assumes that the new Protege GX server is being installed on the same network as the existing server and controllers. This is usually the case, even when the new server is a VM. If the network architecture is changing, you should get assistance from the IT administrator.
- There will be some minor disruption to the site's operation during the migration process:
  - For most of the process, controllers will run in offline mode. They can still perform access control, intrusion and automation functions. However, it will not be possible to update access rights or system configuration.
  - Each controller can store up to 50,000 events while you bring the new event server online. If the site is very busy, we recommend performing the migration during a quiet period to avoid losing events.
  - Each controller will need to be restarted once to connect it to the new event server. The controller will not function for approximately 2 minutes while it restarts.
- We recommend performing the migration onsite to make it easier to troubleshoot issues.

Checklist

You can use this checklist to ensure that you complete everything required for the migration.

- ☐ **Validate the new server** (see next page)
- ☐ **Install the prerequisites** (see next page)
  - .NET Framework
  - SQL Server
- ☐ **Back up data from old server** (see next page)
  - Supporting files
  - Databases
  - Database encryption certificates
- ☐ **Migrate data to new server** (see page 8)
  - Database encryption certificates
  - Databases
  - Supporting files
- ☐ **Contact ICT to reset your server license** (see page 10)
- ☐ **Install Protege GX** (see page 10)
  - Install software
  - Complete security configuration
  - License software
  - Update computer name for download and event servers
- ☐ **Update the event server details on the controllers** (see page 11)
- ☐ **Update external applications** (see page 12)
- ☐ **Validate operator access** (see page 12)

Migrating the Protege GX Server

Validating the New Server

Before you begin, you should confirm that the new server is appropriate for your needs.

- Confirm that it meets the **Computer Hardware Requirements** in the Protege GX Installation Manual. For VMs, ensure that they have enough virtualized resources available.
- Confirm that the Windows operating system is listed in the **Supported Operating Systems** in the Protege GX Installation Manual. We recommend using the most recent available operating system.

You will need the following details about the new server:

- IP address
- Computer name

  The computer name must be 15 characters or fewer.

Installing the Prerequisites

Install the following prerequisite software on the new server:

Microsoft .NET Framework Version 4

Download and install the latest 4.x release from the Microsoft website.

Microsoft SQL Server

Review the supported SQL Server versions in the **Prerequisites** section of the Protege GX Installation Manual. Download a recent version from the Microsoft website.

Follow the instructions in the **Installing Microsoft SQL Server** section of the Protege GX Installation Manual.

Ensure that you set the **Named instance** and **Instance ID** to **PROTEGEGX**.

Backing Up Data

There are three types of data that you need to back up on the old server and migrate to the new one:

- SQL databases
- Encryption certificates
- Supporting files outside the database

Finding Supporting Files

Some files in the Protege GX system are stored outside the database. If the files are stored on the server computer, they must be migrated to the new server. If they are stored in a separate network drive, you just need to ensure that the new server can access that drive.

Check the following files in Protege GX:

- **Alarm sounds**: Review the alarm sounds saved in **Global settings | Sounds | Alarm sounds**.
- **Card template images**: User photos are stored in the Protege GX databases. However, other images on card templates such as the company logo may be stored on the server. Review the images used for card templates in **Users | Card template editor**.
- **Floor plan images**: Review the backgrounds and other images used for your floor plans in **Monitoring | Setup | Floor plan editor**.

- **Web links**: Sometimes web links are used to access HTML pages stored on the server. Review the web links in **Monitoring | Setup | Web links**.

Create a zip file containing any files that need to be migrated to the new server.

You should also consider whether there are any other files on the existing server that Protege GX needs. For example, if your system uses the ICT Data Sync Service, there may be a CSV file that you need to transfer to the new server.

Stopping the Protege GX Services

If any new changes enter the databases after you create the backups, those changes will be lost when you turn off the old server. To avoid this, you must stop the Protege GX services before taking the backups.

On the old server:

1. Open **Services** as an administrator:
   - Press the **Windows + R** keys.
   - Type **services.msc**.
   - Press **Control + Shift + Enter**.
2. Locate the **Protege GX Update Service**.
3. Right click on the service and select **Stop**.

Backing Up the Databases

To back up the databases:

1. Run SQL Server Management Studio (SSMS) and connect to the PROTEGEGX instance.
2. Expand the **Databases** node. Right click on the ProtegeGX database and select **Tasks > Back Up...**
3. If a backup has been created previously, the file will be displayed in the **Destination** field. To use this file, click the **Media Options** tab and select whether you will append the current backup to the existing file or overwrite the existing file.

   To back up to a different file, click **Remove**. Then click **Add...** to enter the name and location of the new backup file. Click **OK**.

   The backup file must be in the .bak format.
4. Click **OK**.
5. Repeat to create a full backup of the ProtegeGXEvents database.

Exporting the Transparent Data Encryption Certificate

If your server instance has transparent data encryption enabled, it is critical that you migrate the encryption certificate to the new server.

If you do not migrate the TDE certificate, the new server will not be able to read the databases.

If you have not already exported the TDE certificate, do so now:

1. In SSMS, click **New Query** and enter the following query:

```
BACKUP CERTIFICATE TDECertificate TO FILE = 'c:\storedcerts\TDE
Certificate'
    WITH PRIVATE KEY ( FILE = 'c:\storedkeys\TDE Key' ,
    ENCRYPTION BY PASSWORD = '<UseStrongPasswordHere>' );
GO
```

2. Click **Execute**. SQL Server will export the certificate and private key files to the specified locations.

Exporting the Column Encryption Certificate

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

- PIN encryption
- ICT wireless locking

The certificate used for column encryption is the Data Service Encryption Certificate. It is stored on the machine where the Protege GX Data Service is installed. You must export this certificate and migrate it to the new server.

If you do not migrate the column encryption certificate, the new server will not be able to read some database columns.

To export the certificate:

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. Under **Certificates - Local Computer**, open **Personal**, then **Certificates**.
3. In the window displaying the certificates, scroll across to the **Friendly Name** column and locate the certificate called Data Service Encryption Certificate.
4. Right click the certificate and select **All Tasks > Export**.
5. The **Certificate Export Wizard** will open. Click **Next**.
6. Select **Yes, export the private key**, then click **Next**.

   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.

7. Select the following **Export File Format** options:
   - **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**.
8. On the **Security** page, select **Password**. Enter and confirm a strong password.

   Save this password to a password manager or other secure location.

9. Set **Encryption** to AES256-SHA256, then click **Next**.
10. Specify an export **File name** and path, then click **Next**.
11. Click **Finish** to complete the certificate export.

Migrating Data

Once you have exported the required data, transfer all of the files to the new server. Then you can deploy the certificates, databases and supporting files.

We recommend migrating all data before installing the Protege GX on the new server. If you migrate the databases after installing Protege GX, you may need to uninstall and reinstall the software to upgrade the databases.

Deploying the TDE Certificate

To install the TDE certificate on the new server:

1. Open SSMS on the new server and connect to the PROTEGEGX instance.
2. Click **New Query**.
3. Enter the following query:

```
USE master;
GO
CREATE MASTER KEY ENCRYPTION BY PASSWORD = '<UseStrongPasswordHere>';
GO
CREATE CERTIFICATE TDECertificate
    FROM FILE = 'c:\storedcerts\TDE Certificate.cer'
    WITH PRIVATE KEY (FILE = 'c:\storedkeys\TDE Key.pvk',
    DECRYPTION BY PASSWORD = '<EnterPrivateKeyPasswordHere>');
GO
```

4. Click **Execute**. The certificate will be uploaded to the server and encrypted using the Database Master Key.

Deploying the Column Encryption Certificate

To deploy the column encryption certificate to the new server:

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.
4. Right click on the **Certificates** sub-folder and navigate to **All Tasks**, then select **Import**.
5. The **Certificate Import Wizard** will open. Click **Next**.
6. 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).
7. Enter the **Password** that was created during the export process.
8. 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/back up 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.
9. Click **Next**.
10. Ensure the **Certificate store** is set to Personal, then click **Next**.
11. Click **Finish** to complete the certificate import.

Restoring Databases

To restore the databases to the new server:

1. Open SSMS on the new server and connect to the PROTEGEGX instance.
2. Right click on the **Databases** node and select **Restore Database...**
3. Set the **Source** to **Device**.

4. Click the ellipsis **[...]**.
5. Click **Add**. Select the ProtegeGX backup, then click **OK**.
6. In the **Files** tab, enable **Relocate all files to folder**.
7. Click **OK**. SSMS will restore the ProtegeGX database to the new server instance.
8. Repeat to restore the ProtegeGXEvents database.

Supporting Files

Save all supporting files to appropriate locations on the new server. The most convenient method is to store them under the same filepath that was used on the previous computer.

If you change the filepaths, you will need to update the settings in Protege GX later.

Resetting the Server License

Protege GX licenses are tied to the server's hardware profile. Before you install the software on the new server, you must contact ICT Technical Support to reset your license.

You can find our contacts on the Help & Support page on our website.

After you reset your license, you can uninstall Protege GX on the old server.

Installing Protege GX

You can now install Protege GX on the new server:

1. Download the latest version of Protege GX from the ICT website.
2. Follow the instructions in the **Installing the Protege GX Server** section of the Protege GX Installation Manual.
   - If your previous installation was using a service account, disable the **Start services after installation** setting. You will start the services after configuring the service account (see below).
3. Install any additional applications that the site was previously using. This may include:
   - Protege GX SOAP Service
   - Protege GX Web Client
   - Protege GX Web App
   - ICT Data Sync Service
   - Integration services or video services

   See the relevant installation manuals or application notes for assistance with installing these services.

Security Configuration

The **Recommended Security Settings** section of the Protege GX Installation Manual contains important configuration for securing your site.

At minimum, you must complete the following security configuration:

- Allow the following services through the Windows Defender Firewall on the new server:
  - GXSV.exe
  - GXEvtSvr.exe
- If your installation was previously using custom TLS and HTTPS certificates, you must generate new certificates for the new server. Ask the site's IT administrator for assistance.
- By default, the Protege GX services run under the local system account. If your previous installation was running on a dedicated service account, you must reinstate this account on the new server. The key steps are:

- Grant the account all required permissions on the new server, including database permissions, certificate store permissions, etc.
- Assign the account to the Protege GX services.

See Application Note 365: Restricting Protege GX Service Permissions for more information and instructions.

Site Setup

You must activate your license in the new Protege GX installation:

1. Log in to Protege GX.
2. Navigate to **About | License**.
3. In the **License update** tab, use the automatic or manual process to activate your license.
4. When prompted, close and restart the Protege GX client.

You will also need to update the computer name in the software to allow controllers to connect:

1. Log in again and confirm that your configuration and event data is present.
2. Navigate to **Global | Download server**. Change the **Computer name** to the name of the new server. Click **Save**.
3. Navigate to **Global | Event server**. Change the **Computer name** to the name of the new server. Click **Save**.
4. Open **Services** as an administrator:
   - Press the **Windows + R** keys.
   - Type **services.msc**.
   - Press **Control + Shift + Enter**.
5. Locate the **Protege GX Download Service**. Right click and select **Restart**.
6. Restart the **Protege GX Event Service** as well.

Configuring Controllers

Each controller must be redirected to communicate with the new event server.

The encryption keys for server-controller communication are stored in the databases, so the controllers will be able to communicate with the new server. You do not need to default the controllers or restart encryption.

For each controller:

1. Log in to the controller's web interface.
2. Navigate to **System Settings**.
3. On the **General** tab, set the **Event Server 1** to the IP address or hostname of the new server.
4. Change the **Event Server 2** and **Event Server 3** if required. These should be alternative paths to the same event server.
5. Click **Save**.
6. Click **Restart**.
7. After the controller has restarted, check that its status in **Sites | Controllers** changes to Online.
8. Right click on the controller and select **Force download**. Open the **Download server diagnostic window** and confirm that the download complete successfully.

Repeat to redirect each controller to the new event server.

Access control, intrusion and automation will be unavailable for about 2 minutes as each controller restarts.

External Applications

If the server's IP address or hostname has changed, you must update the connection settings required for external applications. This includes any applications that connect to the SOAP service or web client, as these endpoints would also have changed.

As required, update the connection settings for any integration services or third-party platforms that connect to the Protege GX server.

Operator Access

Operators will need to make some changes to their workflow to log in to the new server:

- **Client Software**: When an operator logs in to the client software, they must enter the new server's IP address or hostname instead of the old one.
- **Web App and Web Client**: Operators must use the new server's IP address or hostname to access the web app and web client in their web browser. They may need to update bookmarks and password managers.
- **Mobile Apps**: If operators are connected to the Protege GX site in Protege Access+ or the Protege Mobile App, they must update their site settings to use the new IP address or hostname.

Before handover, we recommend validating that operators can access Protege GX from different computers on the network. If the connection fails, there may be an issue with the networking or certificates.

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