AN-365

Restricting Protege GX Service Permissions

Application Note

Last Published: 13-Feb-26 4:01 PM

Contents

Introduction

In a standard Protege GX installation, the Protege GX services run on the server's local system account. This account has permission to perform any action on the server. In the rare event that one of the services were compromised, the attacker could potentially gain elevated access to the server.

You can harden the Protege GX server against attack by restricting the permissions of the Protege GX services. The services will run on a dedicated service account that is only permitted to perform the actions that Protege GX requires to function.

This application note provides a full list of the permissions required for the Protege GX services and instructions for setting up the service account.

In future, a PowerShell script will be provided to assist with setting up the account permissions.

Validated System

These permissions have been validated with Protege GX version 4.3.370.22.

The permissions outlined in this document are subject to change in future Protege GX versions. Ensure that you are using the most recent version of this document.

This document is only valid for the core Protege GX services, which are:

- Protege GX Update Service
- Protege GX Data Service
- Protege GX Download Service
- Protege GX Event Service
- Protege GX DVR Service A
- Protege GX DVR Service B

Further permissions may be required for extended services, integration services and other components.

Column Encryption

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

- PIN encryption
- ICT wireless locking

When you enable column encryption, Protege GX generates a new encryption certificate and uses it to encrypt the database column. This process requires some additional permissions for the certificate store and SQL Server.

After you have enabled column encryption, some of these additional permissions can be removed. However, Protege GX will still require some additional permissions to allow the services to read and write to the encrypted database column.

This document includes the additional permissions required in systems that use column encryption—see SQL Server Permissions and Certificate Store Permissions.

Restricting the Service Permissions

To restrict the service permissions, you will:

- Create a domain or local account for use by the services.
- Grant the service account the required permissions.
- Assign the account to the Protege GX services and start them.

Installing Protege GX

If you are installing Protege GX for the first time, ensure that you disable the **Start services after installation** setting in the installer. This prevents the services from automatically starting up using the local system account. When the service account is ready with the required permissions, you can assign it to the Protege GX services and start them (see page 17).

Creating the Service Account

Ask the site's IT team to create a dedicated account for the Protege GX services.

- This may be a local or domain account.
- **Run as service account** must be enabled.
- You will need the account's username and password.

SQL Server Permissions

The Protege GX services need the following permissions for its databases in SQL Server.

Database	Roles	Additional Permissions
ProtegeGX	db_datareader db_datawriter	CONNECT EXECUTE BACKUP DATABASE
ProtegeGXEvents	db_datareader db_datawriter	CONNECT EXECUTE BACKUP DATABASE

Column Encryption

Some additional permissions are required for systems that use column encryption (see page 4).

When you first enable column encryption, Protege GX requires access to encrypt the relevant database column:

Database	Additional Permissions
ProtegeGX	VIEW ANY COLUMN MASTER KEY DEFINITION VIEW ANY COLUMN ENCRYPTION KEY DEFINITION ALTER ANY COLUMN MASTER KEY ALTER ANY COLUMN ENCRYPTION KEY

After column encryption is enabled, Protege GX only requires the following permissions for reading the encrypted column. The ALTER permissions can be revoked.

Database	Additional Permissions
ProtegeGX	VIEW ANY COLUMN MASTER KEY DEFINITION VIEW ANY COLUMN ENCRYPTION KEY DEFINITION

Granting SQL Server Permissions

To grant permissions for the databases:

1. Log in to SQL Server Management Studio.
2. Click **New Query**.
3. Enter the following query. Replace `DOMAIN\username` with the domain and username for the service account.

```
-- Creating login for the service user
CREATE LOGIN [DOMAIN\username] FROM Windows;

-- Adding permissions for programming database
USE ProtegeGX;
CREATE USER [DOMAIN\username] FOR LOGIN [DOMAIN\username];
ALTER ROLE db_datareader ADD MEMBER [DOMAIN\username];
ALTER ROLE db_datawriter ADD MEMBER [DOMAIN\username];
GRANT EXECUTE TO [DOMAIN\username];
GRANT CONNECT TO [DOMAIN\username];
GRANT BACKUP DATABASE TO [DOMAIN\username];

--Optional: Adding permissions needed for column encryption
GRANT VIEW ANY COLUMN MASTER KEY DEFINITION TO [DOMAIN\Username];
GRANT VIEW ANY COLUMN ENCRYPTION KEY DEFINITION TO [DOMAIN\Username];
GRANT ALTER ANY COLUMN MASTER KEY TO [DOMAIN\Username];
GRANT ALTER ANY COLUMN ENCRYPTION KEY TO [DOMAIN\Username];

-- Adding permissions for events database
USE ProtegeGXEvents;
CREATE USER [DOMAIN\username] FOR LOGIN [DOMAIN\username];
ALTER ROLE db_datareader ADD MEMBER [DOMAIN\username];
ALTER ROLE db_datawriter ADD MEMBER [DOMAIN\username];
GRANT EXECUTE TO [DOMAIN\username];
GRANT CONNECT TO [DOMAIN\username];
GRANT BACKUP DATABASE TO [DOMAIN\username];

-- Flushing authentication cache
DBCC FLUSHAUTHCACHE;
```

4. Click **Execute**.

Revoking Column Encryption Permissions

After you enable column encryption, you can revoke several permissions from the service account. In SQL Server Management Studio, run the following query. Replace `DOMAIN\username` with the domain and username for the service account.

```
--Revoking ALTER Permissions
USE ProtegeGX;
REVOKE ALTER ANY COLUMN MASTER KEY FROM [DOMAIN\Username];
REVOKE ALTER ANY COLUMN ENCRYPTION KEY FROM [DOMAIN\Username];
```

Certificate Store Permissions

Protege GX needs permission to read any certificate that it will use for encrypted connections.

TLS 1.2

When Protege GX has TLS 1.2 enabled, it needs permission to read the **Data Service Certificate** (Personal certificate store). This allows it to create encrypted connections with client workstations using TLS 1.2.

Column Encryption

Some additional permissions are required in systems that use column encryption (see page 4).

When you first enable column encryption, Protege GX must have permission to generate an additional encryption certificate. This requires the following permissions:

- Read and write access to the Personal certificate store
- Read and write access to Trusted Root Certification Authorities

After column encryption has been enabled, you can disable some of these permissions. Going forward, Protege GX only needs the following permission:

- Read access to the **Data Service Encryption Certificate** (Personal certificate store)

Granting Certificate Permissions

To grant access to a certificate:

1. Press **Windows + R**. Enter **certlm.msc** and press **Control + Shift + Enter** to open the certificate manager.
2. Expand **Personal**, then **Certificates**.
3. Locate the relevant certificate.
4. Right click on the certificate and select **All tasks**, then **Manage private keys**.
5. Click **Add**.
6. Click **Object Types** and enable **Service Accounts**. Click **OK**.
7. Enter the name of the service account into the text field, then click **Check Names** to find the account.
8. Click **OK**.
9. Set **Full control** to Deny and set **Read** to Allow.
10. Click **OK**.
11. Repeat for any other certificates the services need access to.

Granting Certificate Store Permissions

When you enable column encryption, the Protege GX Data Service temporarily needs access to generate the column encryption certificate. The simplest way to achieve this is to run the data service under the local system account while you make the configuration change. Once the change is complete, you can return the data service to the dedicated service account.

When you need to enable column encryption, follow these steps:

1. Open **Services** as an administrator:
   - Press the **Windows + R** keys.
   - Type **services.msc** into the search bar.
   - Press **Control + Shift + Enter**.

2. Locate the Protege GX services.
3. Stop the **Protege GX Data Service**.
4. Right click the Protege GX Data Service and select **Properties**.
5. In the **Log On** tab, select **Local system account**.
6. Click **OK**.
7. Start the data service.
8. In Protege GX, enable the relevant column encryption feature:
   - **PIN Encryption**: **Encrypt user PINs** in **Global | Global settings | General**.
   - **Wireless Locks**: **Enable offline wireless locks** in **Global | Sites | Site defaults**.
9. When the software reports success, close the Protege GX client.
10. Return to the services manager and stop the Protege GX Data Service.
11. Right click the Protege GX Data Service and select **Properties**.
12. In the **Log On** tab, select **This account**.
13. Enter the name of the service account in the format: DOMAIN\username
14. Enter the **Password**.
15. Click **OK**.
16. Follow the instructions in Granting Certificate Permissions to give the service account read access to the **Data Service Encryption Certificate**.

COM Permissions

The Protege GX services need access to the following COMs (Component Object Models) on the server computer.

COM	Permissions
GXDVR1	Local Launch Local Activation Local Access
GXEvtSvr	Local Launch Local Activation Local Access
GXSV2	Local Launch Local Activation Local Access
GXSV3	Local Launch Local Activation Local Access

Granting COM Permissions

To set the COM permissions:

1. Press **Windows + R**. Enter **dcomdnfg** and press **Control + Shift + Enter** to open the Component Services manager.
2. Navigate to **Console Root > Component Services > Computers**.
3. Right click on **My Computer** and select **Properties**. Open the **COM Security** tab.
4. Under **Access Permissions**, click **Edit Limits**.
5. Add the service account to the list of users.
6. Select **Allow** for **Local Access** only. Click **OK**.
7. Under **Launch and Activation Permissions**, click **Edit Limits**.
8. Add the service account to the list of users.
9. Select **Allow** for **Local Launch** and **Local Activation**. Click **OK**.
10. Click **OK**.
11. Open **My Computer**, then **DCOM Config**.
12. Locate the following COMs:
    - GXDVR1
    - GXEvtSvr
    - GXSV2
    - GXSV3
13. Right click on each COM and select **Properties**. Open the **Security** tab.
14. Set the **Launch and Activation Permissions** to Customize and select **Edit**.
15. Add the service account and grant it **Local Launch** and **Local Activation** permissions. Click **OK**.
16. Set the **Access Permissions** to custom and grant the service access **Local Access**.

17. Click **OK**.
18. Repeat for all of the Protege GX COMs.

File System Permissions

Protege GX needs permissions for the following folders:

Directory	Default Location	Permissions Required
Installation folder	C:\Program Files (x86)\Integrated Control Technology\Protege GX	Full Control
Program data folder	C:\Program Data\Protege GX\ProtegeGX	Full Control
Database backup folder	Default backup folder for SQL Server. Configurable by the integrator. See **Global | Global settings | General** in Protege GX.	Full Control

Your Protege GX installation may also need access to read/write in other directories containing assets such as:

- Floor plan backgrounds
- Alarm sounds
- Exported reports
- Exported user images

These directories are configurable in Protege GX. Ensure that you grant the services access to all directories that are required for normal operation.

Granting File System Permissions

To grant the service account permission to a directory:

1. In the File Explorer, navigate to the parent directory.
2. Right click on the directory you will grant permission for and select **Properties**.
3. Open the **Security** tab and click **Edit**.
4. Click **Add** and select the service account.
5. Enable the permissions required, as per the table above.
6. Click **OK**.
7. Repeat for the other required directories.

Service Permissions

The Protege GX Data Service needs the following permissions to control other services:

Service	Permissions
GXDownloadService	Start Stop
GXEventService	Start Stop

Granting Service Permissions

The simplest way to grant service permissions is using PowerShell. To set the service permissions:

1. Open a PowerShell terminal as an admin.
2. Run the following command, replacing DOMAIN\username with the name of the service account:

   ```
   $account = "DOMAIN\username"; $sid = (New-Object
   System.Security.Principal.NTAccount($account)).Translate
   ([System.Security.Principal.SecurityIdentifier]).Value; Write-Output $sid
   ```

   Remove any line breaks before you run the command.

   The response is the SID for the service account, in the following format:

   ```
   S-1-5-21-2937585081-1717772430-3299410257-5012
   ```

3. Run the following command to get the existing control permissions for the download service:

   ```
   sc sdshow GXDownloadService
   ```

   This will return a string of characters similar to that below. Note that there is a `D:` section followed by several parentheses, then an `S:` section followed by several parentheses.

   ```
   D:(A;;CCLCSWRPWPDTLOCRRC;;;SY)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)
   (A;;CCLCSWLOCRRC;;;IU)(A;;CCLCSWLOCRRC;;;SU)S:
   (AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)
   ```

4. Copy the existing control permissions to a text document. At the end of the `D:` section, but before the `S:`, insert the new permission. Replace `SID` with the SID you found above.

   ```
   (A;;SWSDRPWPLOLCRC;;;SID)
   ```

   For example, using the SID from above:

   ```
   D:(...)(...)(...)(...)(A;;SWSDRPWPLOLCRC;;;S-1-5-21-2937585081-1717772430-
   3299410257-5012)S:(...)
   ```

5. In the PowerShell terminal, enter the following command. Insert your new permission string between the double quotes.

   ```
   sc sdset GXDownloadService "D:(...)S(...)"
   ```

6. If successful, the result should be:

   ```
   [SC] SetServiceObjectSecurity SUCCESS
   ```

7. Repeat the above steps for the **GXEventService**, starting from step 3.

To validate the permissions, log in to the server using the service account. Open the Services Manager, right click on the Protege GX Download Service and check that the **Start** and **Stop** controls are available (not grayed out). Repeat for the Protege GX Event Service.

Registry Permissions

The service account used by Protege GX needs the following permissions:

Registry Directory	Permission
HKEY_CLASSES_ROOT\CLSID	Read
HKEY_CLASSES_ROOT\Interface	Read
HKEY_CLASSES_ROOT\WOW6432Node	Read
HKEY_CLASSES_ROOT\WOW6432Node\AppID	Advanced (see below)
HKEY_CLASSES_ROOT\WOW6432Node\CLSID	Advanced (see below)
HKEY_CLASSES_ROOT\WOW6432Node\Interface	Advanced (see below)
HKEY_CLASSES_ROOT\GXSV2.DLSVRControl	Full Control
HKEY_CLASSES_ROOT\GXSV2.DLSVRControl.1	Full Control
HKEY_CLASSES_ROOT\GXSV2.SGL	Full Control
HKEY_CLASSES_ROOT\GXSV2.SGL.1	Full Control
HKEY_CLASSES_ROOT\GXSV3.LicenceComCOM	Full Control
HKEY_CLASSES_ROOT\GXSV3.LicenceComCOM.1	Full Control
HKEY_CLASSES_ROOT\GXSV3.Restraints	Full Control
HKEY_CLASSES_ROOT\GXSV3.Restraints.1	Full Control
HKEY_CLASSES_ROOT\TypeLib\{00020430-0000-0000-C000-000000000046}\2.0	Full Control
HKEY_CURRENT_USER	Read
HKEY_USERS	Read
HKEY_LOCAL_MACHINE\SOFTWARE	Read
HKEY_LOCAL_MACHINE\HARDWARE\Description	Read
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft	Read
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control	Read
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services	Read
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\TCPIP	Read
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W3SVC	Read
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventLog\Security	Read
HKEY_LOCAL_MACHINE\SYSTEM\WOW6432Node\Description\Microsoft\Rpc\UuidTemporaryData	Read
HKEY_LOCAL_MACHINE\SYSTEM\WOW6432Node\ODBC\ODBC.INI	Read
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node	Advanced (see below)
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\GXDataService	Full Control

Registry Directory	Permission
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\GXDownloadService	Full Control
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\GXDVRServiceA	Full Control
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\GXDVRServiceB	Full Control
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\GXEventService	Full Control
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\GXUpdateService	Full Control
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventLog\ICT Protege GX	Full Control

Granting Standard Registry Permissions

To set standard permissions (i.e. Read or Full Control) for registry directories:

1. Press **Windows + R**. Enter **regedit** and press **Control + Shift + Enter** to open the Registry Editor.
2. Locate each registry folder from the table above.
3. Right click on the folder and select **Permissions**.
4. Click **Add** and select the service account.
5. Enable the permissions required, as per the table above.
6. Click **OK**.
7. Repeat for all required registry folders.

Troubleshooting

You may receive an 'Access Denied' message when you attempt to update the following registry folder:

```
HKCR\TypeLib\{00020430-0000-0000-C000-000000000046}\2.0
```

By default, the owner of this registry key's security settings is SYSTEM. If your own permissions allow, you can temporarily change this to allow you to update the permissions:

1. In the **Permissions** window for this key, click **Advanced**.
2. Next to **Owner**, click **Change**.
3. Select your own user, then click **OK**.
4. Update the permissions for the Protege GX service account as described above.
5. Once you have completed these changes, revert the **Owner** to SYSTEM.

Granting Advanced Registry Permissions

The following registry directories require advanced permissions:

- HKEY_CLASSES_ROOT\WOW6432Node\AppID
- HKEY_CLASSES_ROOT\WOW6432Node\CLSID
- HKEY_CLASSES_ROOT\WOW6432Node\Interface
- HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node

To set advanced permissions:

1. Right click on each folder and select **Permissions**.
2. Click **Add** and select the service account.
3. Click **Advanced**.

4. Click **Enable inheritance** (if it is not already enabled).
5. Double click on the service account.
6. Click **Show advanced permissions**.
7. Enable all permissions except for:
   - Full control
   - Create Link
   - Delete
   - Write DAC
   - Write Owner
8. Click **Close**, then **OK**.

Reserved URL

The Protege GX DVR B service needs a reserved URL to function correctly.

1. Open a command prompt as an administrator.
2. Run the following command. Replace **DOMAIN\username** with your domain and the service account username.

```
netsh http add urlacl url=http://+:8020/GXDVR2/GXDVR2Service/
user=DOMAIN\serviceAccount
```

Assigning the Account to the Protege GX Services

Finally, you can assign the service account to the Protege GX services:

1. Open **Services** as an administrator:
   - Press the **Windows + R** keys.
   - Type **services.msc** into the search bar.
   - Press **Control + Shift + Enter**.
2. Locate the Protege GX services.
3. Stop any services that are currently running.
4. Right click the **Protege GX Data Service** and select **Properties**.
5. In the **Log On** tab, select **This account**.
6. Enter the name of the service account in the format: DOMAIN\username
7. Enter the **Password**.
8. Click **OK**.
9. Repeat for the other Protege GX services.
10. Open the Windows Event Viewer to monitor any errors or warnings that occur when you start the services.
11. Start the Protege GX Data Service. Most other services will start automatically.
12. Start the Protege GX Download Service.

Troubleshooting—Data Service

When you attempt to start the Protege GX Data Service, you may see one of the following warnings or errors in the event viewer:

- System.UnauthorizedAccessException: Retrieving the COM class factory for component with CLSID {...} failed due to the following error: 80070005 Access is denied.
- Warning - Failed to Initialize License Data - Running in demo mode
- Error has occurred. Background Service exiting with ExitCode 1
- CoCreateInstance(CLSID_Restraints...) Failed

If you see one of these errors, the data service does not have sufficient COM and registry permissions to start up. Ensure that all of the permissions in COM Permissions and Registry Permissions have been granted.

Troubleshooting—DVR Service

The following error may occur when you attempt to start the Protege GX DVR Service B:

- Application: GXDVR2.exe Framework Version: v4.0.30319 Description: The process was terminated due to an unhandled exception.

In this case, ensure that the URL has been reserved for this service (see previous page).

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

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.