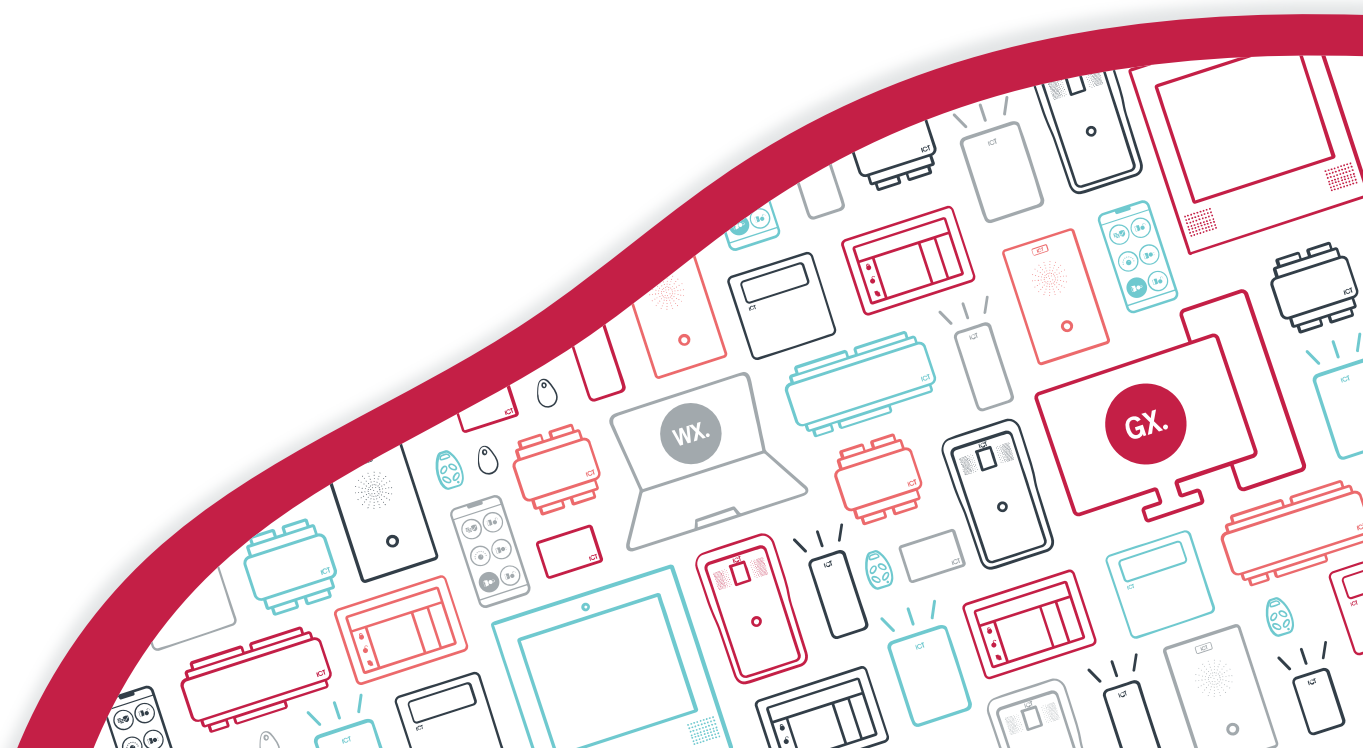
PRT-GX-SOAP

Protege GX SOAP Service

Installation Manual



Last Published: 29-Aug-24 1:32 PM

Contents

Introduction ____ 4
About this Manual ____ 4
Who This Manual is For ____ 4
What You Should Already Know ____ 4
Security ____ 4
Before You Begin ____ 5
System Requirements ____ 5
Prerequisites ____ 5
Installation ____ 6
Enabling the Required Windows Features ____ 6
Windows 8.1 and 10 ____ 7
Windows 11 ____ 8
Windows Server 2012 ____ 9
Windows Server 2016, 2019 and 2022 ____ 11
Enabling the Required Application Pool Settings ____ 12
Enable 32-Bit Applications ____ 12
Installation ____ 12
Installing on a Machine Not Hosting the Protege GX Database ____ 13
Installing the Protege GX SOAP Service ____ 13
Service Accessibility ____ 13
Security Configuration ____ 15
Using a Third-Party Certificate for SOAP ____ 15
Using a Self-Signed SSL Certificate for SOAP ____ 16
Disabling Insecure Cipher Suites and Protocols ____ 17
Enabling Mandatory ASLR ____ 17
Troubleshooting ____ 19
Disclaimer and Warranty ____ 20

Introduction

The Protege GX SOAP Service exposes the full functionality of Protege GX, providing a simple way to access Protege GX via a web platform, build your own application with a customized interface, or integrate with a physical device to unlock doors and disarm areas.

The web service sits between Protege GX and the third-party application and communicates using SOAP - an XML-based messaging protocol that is used to exchange information between systems. It is not limited to a specific operating system or programming language, enabling developers to build a solution for any system that can formulate and understand SOAP messages.

It is not advised to run this product in a production environment without loading a third party verified SSL certificate. ICT do not provide or install certificates. If there are concerns, an IT professional should install and administer IIS. For more information, see Security Configuration (page 15).

About this Manual

Who This Manual is For

This manual is intended for those that are required to install the Protege GX SOAP Service for the purpose of interfacing with the Protege GX Web Client, ICT Data Sync Service or other applications.

What You Should Already Know

This manual assumes that you are experienced with the configuration of the Microsoft Internet Information Server (IIS) application, the administration of ASP.NET and WCF and the general tasks associated with managing and maintaining an IIS installation. It is also assumed that you are proficient in using the Protege GX system and understand general security principles and policies.

This manual includes instructions for installing the Protege GX SOAP Service. It does not cover the installation of the Protege GX client/server, which are prerequisites for installation of the Protege GX SOAP Service.

For information on installing the Protege GX client/server refer to the Protege GX Installation Manual.

Security

The client communication security settings must be consistent between the Protege GX client and Protege GX SOAP Service installations. Any inconsistencies will result in a communication fault or error.

Before You Begin

This manual provides instructions on installing the Protege GX SOAP Service. This section includes information on system requirements and prerequisites.

Take a moment to read the material in this section before installation.

System Requirements

The following operating systems are supported by the Protege GX SOAP Service.

Operating System	Edition	Architecture
Microsoft Windows Server 2022	Standard, Datacenter	64-bit
Microsoft Windows Server 2019	Standard, Datacenter	64-bit
Microsoft Windows Server 2016	Standard, Datacenter	64-bit
Microsoft Windows 11	Pro, Business, Enterprise	64-bit
Microsoft Windows 10	Professional, Enterprise	32 / 64-bit

Prerequisites

Before installing the Protege GX SOAP Service, the following components are required:

- An operational Protege GX system.

It is recommended that you always use the latest versions of Protege GX and the Protege GX SOAP Service available from ICT.

You must also enable various Windows features and application pool settings. For your convenience, the configuration instructions are included in this manual.

Protege GX SOAP Web Service Software Development Kit (SDK)

If you are building your own interface or integration you will also require the Protege GX SOAP Web Service Software Development Kit (purchasing code: PRT-GX-SOAP-SDK).

The software development kit includes all the development tools necessary, including API documentation and sample code, to write a custom interface or build a custom integration to the Protege GX server.

Installation

Enabling the Required Windows Features

Before installing the Protege GX SOAP Service various Windows features need to be enabled.

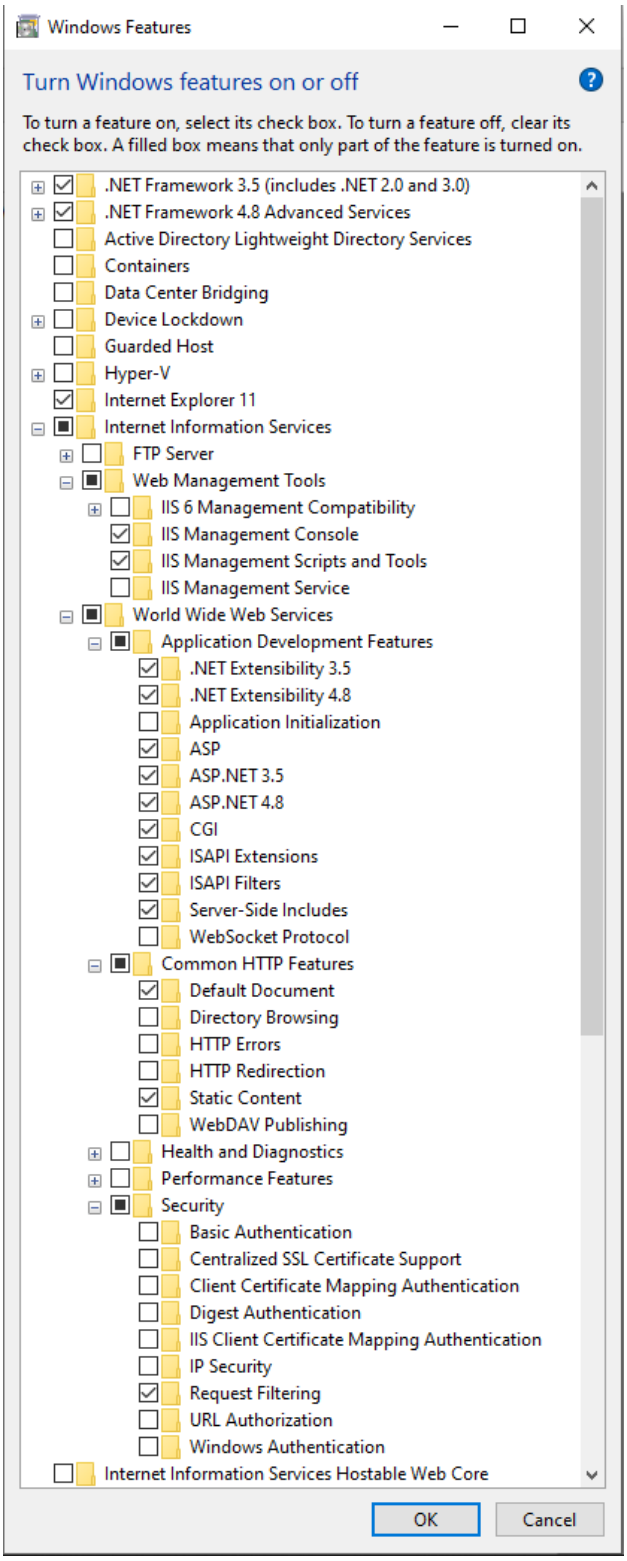
See the following pages for instructions for the operating system (Windows version) you are using.

- Windows 8.1 and 10 (see next page)
- Windows 11 (see page 8)
- Windows Server 2012 (see page 9)
- Windows Server 2016, 2019 and 2022 (see page 11)

Windows 8.1 and 10

1. Open the **Control Panel** and navigate to **Programs | Turn Windows Features On or Off** for Windows 8, and **Programs and Features | Turn Windows Features On or Off** for Windows 10.
2. In the dialog box, ensure that the selections shown in the image below are enabled.

   Where an expandable check box is ticked, you need to expand it and enable all features and sub-features.

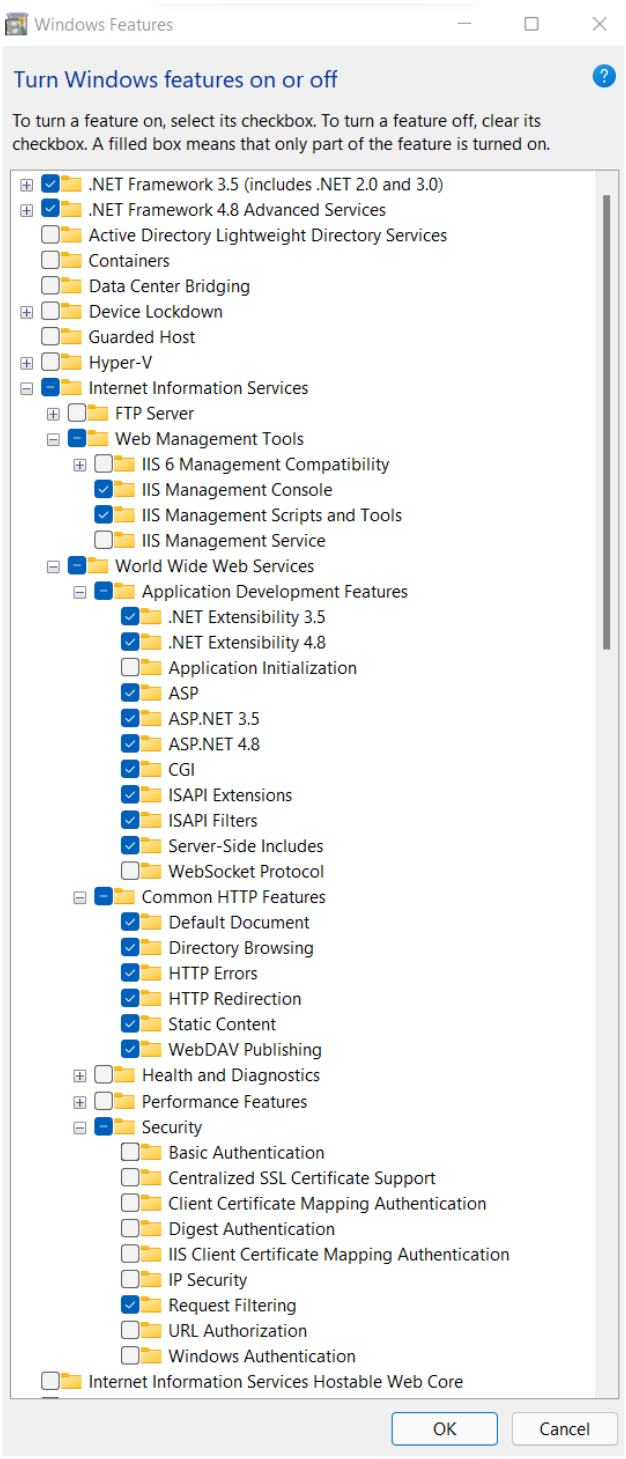


3. Click **OK**.

Windows 11

1. Open **Settings**.
2. Open the **Optional features** section.
3. Click **More Windows features** to open the Windows Features dialog.
4. Ensure that the following settings are enabled:

   Where an expandable check box is ticked, you need to expand it and enable all features and sub-features.

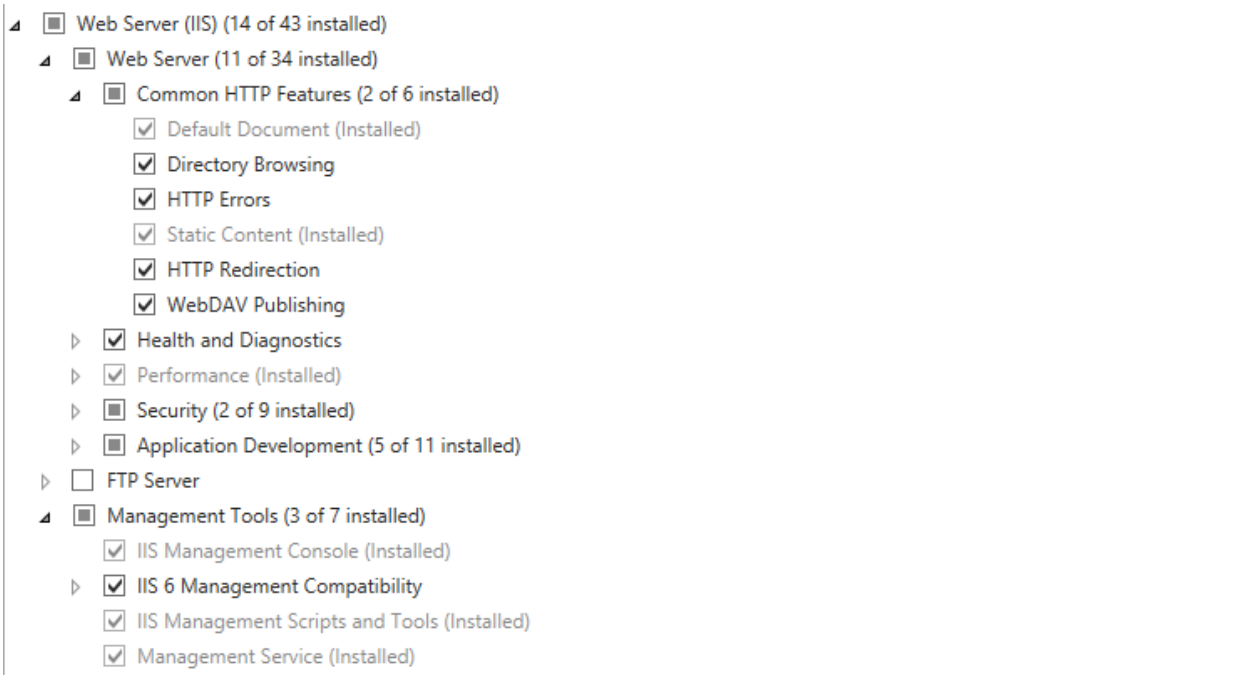


5. Click **OK**.

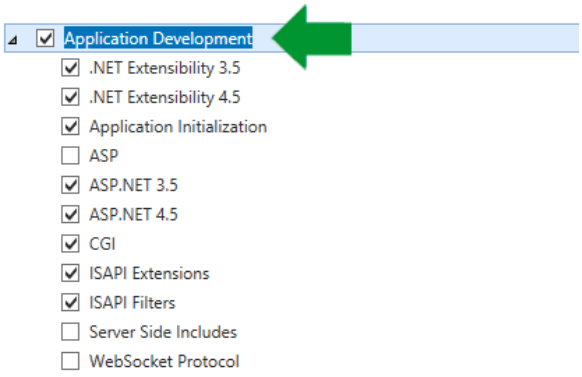
Windows Server 2012

1. Launch the **Server Manager**.
2. From the **Manage** menu, select **Add Roles and Features**. This launches the Add Roles and Features Wizard.
3. From the **Server Roles** page, ensure that the following fields are enabled:

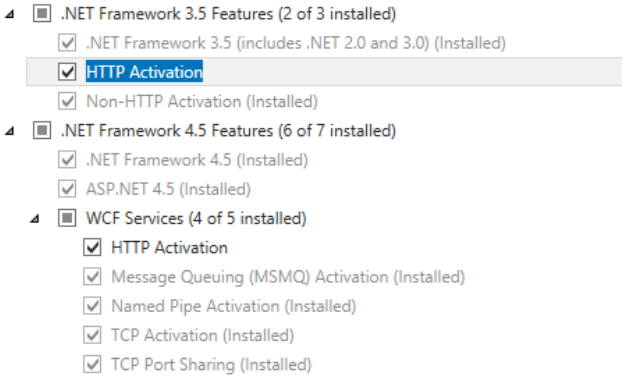
   Where an expandable check box is ticked, you need to expand it and enable all features and sub-features.

4. Expand the **Application Development** menu and ensure that the following fields are enabled:

5. Click **Next**.
6. From the **Features** page, ensure that the following .NET framework features are enabled.

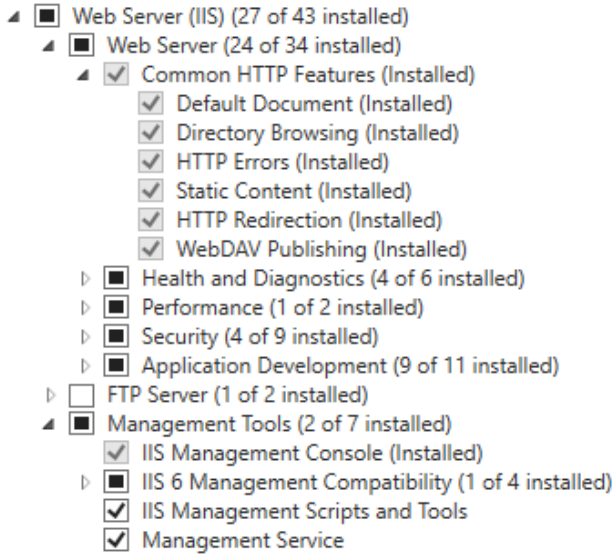


7. Click **Next** to complete the setup and install the features.

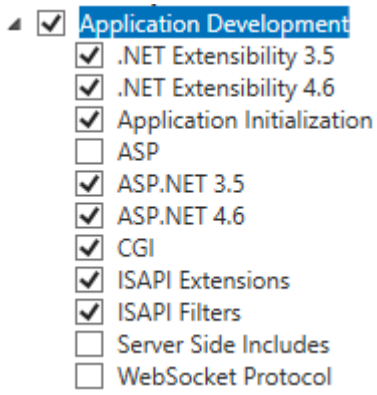
Windows Server 2016, 2019 and 2022

1. Launch the **Server Manager**.
2. From the **Manage** menu, select **Add Roles and Features**. This launches the Add Roles and Features Wizard.
3. From the **Server Roles** page, ensure that the following fields are enabled:

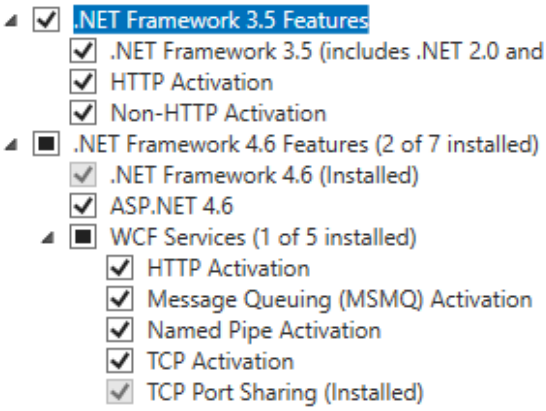
   Where an expandable check box is ticked, you need to expand it and enable all features and sub-features.

4. Expand the **Application Development** menu and ensure that the following fields are enabled:

5. Click **Next**.
6. From the **Features** page, ensure that the following .NET framework features are enabled.

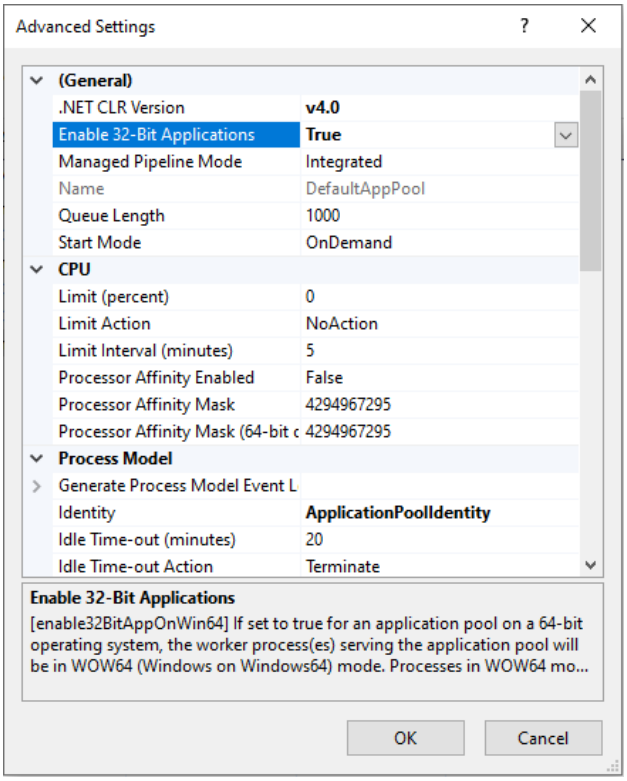
7. Click **Next** to complete the setup and install the features.

Enabling the Required Application Pool Settings

Before installing the Protege GX SOAP Service the following application pool settings need to be enabled.

Enable 32-Bit Applications

1. Launch **Internet Information Services (IIS) Manager**.
   - Press the **Windows + R** keys to open the run prompt.
   - Type **inetmgr** into the search bar and press Enter.
2. Under IIS Manager's **Connections** menu, expand the node for the current server then click **Application Pools**.
3. In the **Application Pools** pane click **DefaultAppPool**.
4. In the **Actions** pane on the right click **Advanced Settings**.
5. In the **General** section , ensure that **Enable 32-Bit Applications** is set to True, as displayed below.



6. Click **OK**. Then close IIS Manager.

Note: If this setting is not enabled, the Protege GX SOAP Service installation will fail. InstallShield Wizard will display a message advising that the installation was interrupted.

Installation

The following section outlines the steps you need to take to install the Protege GX SOAP Service so you can get up and running quickly. Note that there are additional steps to carry out if you are installing the SOAP service on a machine that does not also host the Protege GX databases.

You must have local administrative privileges on the server and workstation(s) you are performing the installation on.

Installing on a Machine Not Hosting the Protege GX Database

If you are installing the Protege GX SOAP Service on a machine that does not contain the SQL instance hosting the Protege GX database, follow the steps below in SQL Server Management Studio.

1. Open SQL Server Management Studio and connect to the relevant server.
2. Right-click on the SQL instance name (the top level icon) and select **Properties**.
3. Click on the **Security** tab and ensure that **SQL Server and Windows Authentication Mode** option is enabled.
4. Close the **Server Properties** window.
5. From the **Object Explorer**, navigate to **Security | Logins**.
6. Right-click **NT Authority/System Login** and select **Properties**.
7. Select **User Mapping** and enable the map checkboxes for the **ProtegeGX** and **ProtegeGXEvents** databases.
8. Assign the required **Database Role** for both the **ProtegeGXEvents** and **ProtegeGX** database by selecting both databases and enabling the **db_owner** checkbox.
9. Click on the **Status** tab, ensure that **Login** is Enabled.
10. Click **OK** to close the Login Properties window.
11. Restart the SQL server instance from the Windows Services Manager to apply the changes.

Installing the Protege GX SOAP Service

1. Run the supplied **setup.exe** file to launch the Protege GX SOAP Service Install Wizard.

   If the required .NET version is not installed, the wizard will prompt you to install or update .NET.

2. Click **Next** to continue.
3. Read and accept the license agreement, then click **Next**.
4. Click **Next**.
5. In the **Data Server installed PC name** field provide the name of the machine that hosts the Protege GX data service.

   Do not use localhost as the service will fail to operate.

6. If required, enable Windows Authentication for the Protege GX data server/web server communications and configure the WCF/IP port.

   You can use the default WCF TCP/IP port, or specify the ports used by entering the new details. These options should be changed if another application on the target machine uses the default port, as this will cause the services to fail to start.

   The **Enable Windows Authentication on Protege GX Data Server/Web Server Communications** option must match the selection made when installing the Protege GX server. For example, if Windows Authentication is enabled when installing the Protege GX server, Windows Authentication must also be enabled when installing the SOAP service.

7. Click **Next**.
8. Click **Install**.
9. When the installation is complete, click **Finish**.

Service Accessibility

To confirm that the service is accessible and ready to use:

1. Open a web browser and enter the following link into the URL bar:
   https://<pcname>.<domainname>:<portnumber>/ProtegeGXSOAPService/service.svc

   The default port number is **8040**. You can use localhost instead of the PC name and domain name, but this causes the HTTPS certificate to load incorrectly.

2. Press the **Enter** key.
3. Most web browsers will present you with a security warning because the SOAP service is using a self-signed certificate. Click the **Advanced** button and proceed to the site.

   For more information see the Security Configuration section below.

4. You should see a default page with the following text:

   Service1 Service
   You have created a service.

   This confirms that SOAP is accessible on the HTTPS endpoint.

Security Configuration

It is important to secure the connection between the SOAP service and other applications it is communicating with, such as the Protege GX Web Client, ICT Data Sync Service and custom integrations. To achieve this, the SOAP service must use a trusted SSL certificate to encrypt communications (using the HTTPS protocol).

A self-signed SSL certificate is automatically generated during installation of the SOAP service. However, this certificate is not inherently trusted by other computers and applications, so the connection may be refused or flagged as insecure. There are two methods for achieving a trusted connection:

- **Recommended**: Obtain and install a third-party certificate issued by a trusted certificate authority, such as:
  - **GoDaddy**: https://www.godaddy.com/web-security/ssl-certificate
  - **Network Solutions**: https://www.networksolutions.com/
  - **RapidSSL**: https://www.rapidsslonline.com/
  - **Let's Encrypt**: https://letsencrypt.org/
- Import a self-signed certificate into the trusted certificate store of each computer that will connect to each application. This can be either the certificate which was automatically generated during installation, or a custom self-signed certificate.

Once a trusted certificate has been installed, applications can connect to the HTTPS endpoint of the SOAP service (see page 13) and achieve secure communications.

Using a Third-Party Certificate for SOAP

Once you have obtained a third-party certificate from a trusted certificate authority, you must install it in the **ProtegeGX** site in Internet Information Services (IIS) Manager. This secures the connection between the SOAP service and other applications.

This is the recommended method for securing the SOAP service on live sites.

Completing the Certificate Request

1. Open IIS Manager by pressing the **Windows + R** keys to open the **Run** prompt, then entering **inetmgr**.
2. In the **IIS** section, double-click **Server Certificates**.
3. From the **Actions** panel on the right, click **Complete Certificate Request...**
4. To locate your certificate file, click the ellipsis **[...]** button.
5. Select ***.*** as the file name extension.
6. Select the certificate and click **Open**.
7. Enter a **Friendly name** for the certificate file, then click **OK**.

Binding the Certificate to the ProtegeGX Site

1. In the **Connections** panel on the left of IIS Manager, expand the server where you installed the certificate.
2. Click the drop-down arrow next to **Sites** and select the **ProtegeGX** site.
3. In the **Actions** panel, click **Bindings...**.
4. Select the https binding (port 8040) and click **Edit...**.
5. Set the **SSL certificate** to the certificate you just installed. Click **OK**.
6. You will see a warning about overwriting the existing certificate. Click **Yes**.
7. Close the site bindings window and the IIS Manager window.

The SSL certificate installation is complete.

When the SOAP service is upgraded, the certificate will be reset to the default. Repeat the steps above to rebind the custom certificate.

Using a Self-Signed SSL Certificate for SOAP

As an alternative to a third-party certificate, you may use a self-signed certificate for the SOAP service. As self-signed certificates are not inherently trusted by other computers and applications, it is necessary to import the certificate to the trusted root store of each other computer that will connect to the SOAP service directly.

The instructions below cover creating a custom self-signed certificate, binding it to a site, and importing it as a trusted certificate on other computers.

For live sites, it is recommended that you use a third-party certificate or a trusted certificate issued by your IT department.

Creating and Exporting a New Self-Signed Certificate

There are multiple methods to create a self-signed certificate. The steps below describe how to create a certificate using IIS Manager. Alternatively, you may create a certificate using a utility such as OpenSSL, or a certificate may be supplied by your IT department.

1. Open IIS Manager by pressing the **Windows + R** keys to open the **Run** prompt, then entering **inetmgr**.
2. In the **IIS** section, double-click **Server Certificates**.
3. From the **Actions** panel on the right, click **Create Self-Signed Certificate...**
4. Enter a name for the certificate.
5. Set the certificate store to Personal.
6. Click **OK**. Your new certificate will be added to the list.
7. Double-click on the new certificate to view it.
8. Navigate to the **Details** tab and select **Copy to File...** The certificate export wizard will open.
9. Complete the instructions in the wizard, selecting these options:
   - Do **not** export the private key.
   - **Format**: DER encoded binary X.509 (.CER)
   - Specify the name and location where you want to export the certificate.
10. Click **Finish** to complete the export.

Binding the Certificate to the ProtegeGX Site

1. In the **Connections** panel on the left of IIS Manager, expand the server where you installed the certificate.
2. Click the drop-down arrow next to **Sites** and select the **ProtegeGX** site.
3. In the **Actions** panel, click **Bindings...**.
4. Select the https binding and click **Edit...**.
5. Set the **SSL certificate** to the certificate you just installed. Click **OK**.
6. You will see a warning about overwriting the existing certificate. Click **Yes**.
7. Close the site bindings window and the IIS Manager window.

When the SOAP service is upgraded, the certificate will be reset to the default. Repeat the steps above to rebind the custom certificate.

Importing the Certificate to Another Computer

This section must be completed on each computer that will connect directly to the SOAP service.

1. Open the certificate manager by pressing **Windows + R**, then entering **certlm.msc**.
2. Browse to **Certificates - Local Computer > Trusted Root Certification Authorities > Certificates**.
3. Right click on the Certificates folder and select **All Tasks > Import...**. This will open the certificate import wizard.
4. Click **Next**.
5. Browse to and select the certificate file that you exported.
6. Select the option to **Place all certificates in the following store** and enter Trusted Root Certification Authorities as the certificate store.
7. Click **Finish** to complete the import.

Disabling Insecure Cipher Suites and Protocols

We recommend that you follow best practice by disabling old and insecure cipher suites and communication protocols on the Protege GX server and SOAP server. This requires editing the registry settings on the computer where the Protege GX server is installed, as well as the computer hosting the SOAP service if this is installed separately. For more information about the relevant settings, see the Microsoft documentation and contact your IT provider.

Always back up (export) the registry settings before editing the registry.

IIS Crypto by Nartac Software is a useful tool for managing security settings. It allows you to apply security settings to the server without needing to manually edit the registry.

A standard Protege GX installation has been validated with the **PCI 3.2** and **Best Practices** settings from IIS Crypto 3.2. PCI 3.2 provides stricter security and is the recommended setting.

To apply these settings:

1. Download IISCrypto.exe from the link above.
2. Run the program and click **Yes** to allow it to make changes to your computer.
3. Navigate to the **Templates** tab.
4. Select the PCI 3.2 template from the dropdown, then click **Apply**.
5. Restart the computer to implement the new settings.

Protege GX supports a wide range of integrations, which may not all be compatible with best-practice security settings. In addition, older hardware may not support more recent encryption protocols. In some situations, it may be necessary for you to enable less secure cipher suites and communication protocols. It is the responsibility of the installer to ensure that appropriate security settings are applied.

Enabling Mandatory ASLR

Address space layout randomization (ASLR) is a memory-protection process which randomizes the location where system executables are loaded into memory. This helps to guard against buffer-overflow attacks by making it more difficult for an attacker to predict target addresses and exploit memory corruption vulnerabilities.

The Mandatory ASLR option available in Windows Security can be used to ensure that all EXEs and DLLs on the operating system are forcibly randomized at runtime. For more information about Mandatory ASLR see the Microsoft documentation or contact your IT provider.

To maintain legacy compatibility this feature is disabled by default on all Windows operating systems. We recommend that you follow best practice by enabling Mandatory ASLR on your Protege GX server, SOAP server, and for maximum security all Protege GX client workstations.

You will require administrator permissions to enable this feature.

To enable Mandatory ASLR:

1. Open **Windows Security**.
2. Navigate to **App and browser control**.
3. Under the **Exploit protection** section, select **Exploit protection settings**.
4. Under **System Settings**, go to the **Force randomization for images (Mandatory ASLR)** option and change the setting to On by default.
5. Restart the computer to implement the new settings.

Troubleshooting

It is not possible to access SOAP over the HTTP endpoint (port 8030)

The SOAP service no longer supports unencrypted HTTP connections from version 1.7.0.0. Use the HTTPS endpoint instead (see page 13).

When I start the application, I receive the error: "Operator Logon Failed. Password Change Required."

The operator used by the SOAP application needs to change their password. Use the operator's current credentials to log in to a Protege GX client and change the operator's password, then update the login credentials in the SOAP application.

Disclaimer and Warranty

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.

For warranty information, see our Standard Product Warranty.

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