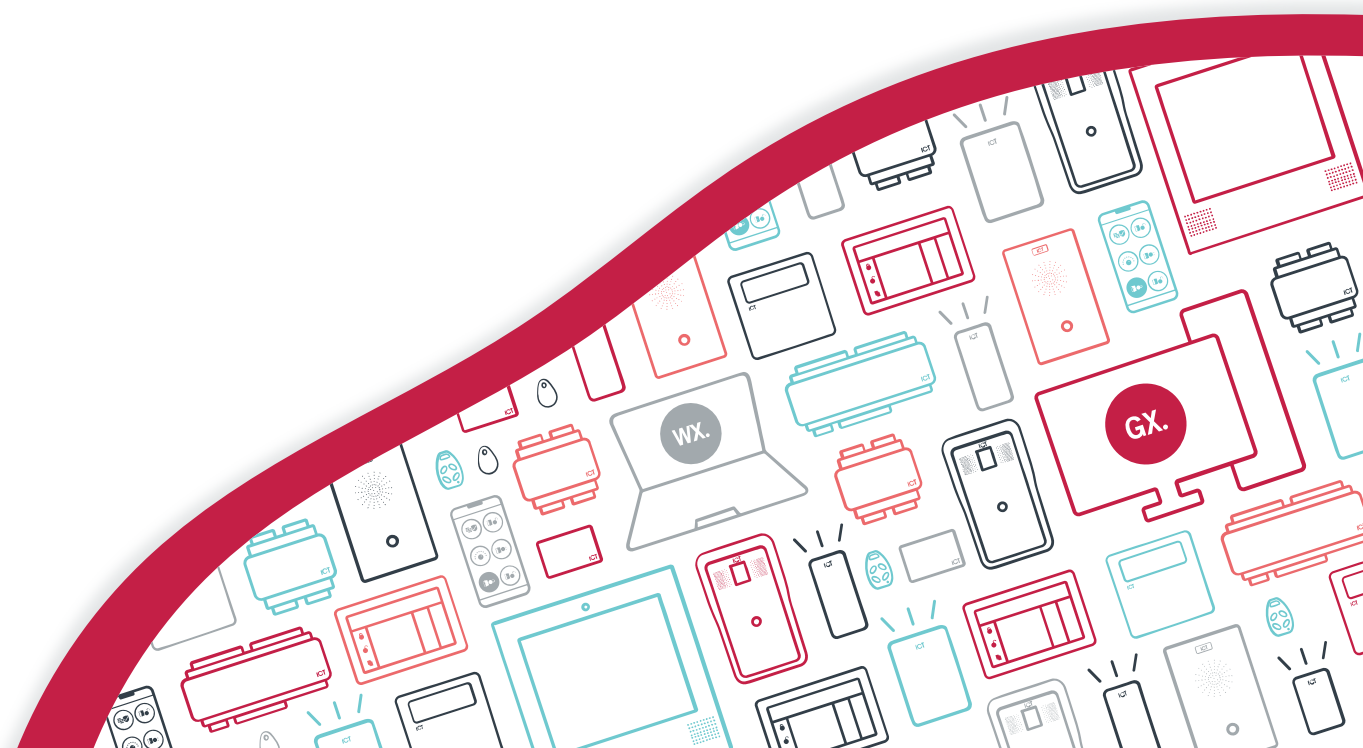
PRT-GX-WEB

Protege GX Web Client

Installation Manual



Last Published: 29-Aug-24 1:39 PM

Contents

Introduction

The Protege GX Web Client is a cross-platform solution that enables you to manage and monitor your Protege GX system from a web environment from any device with a modern web browser and an internet connection.

Installed on a web server, the web client uses the Protege GX SOAP Service to communicate with the Protege GX server. These components may be installed on the same machine as the Protege GX server, or on a separate physical server.

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 18).

About this Manual

Who This Manual is For

This manual is intended for those who are required to install the Protege GX Web Client in order to allow access to certain features of the Protege system via a web browser.

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 also assumes that readers are proficient in the use of the Protege system and understand general security principles and policies.

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

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 Web Client. 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 and Protege GX Web Client.

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 Web Client, the following components are required:

- An operational Protege GX system.
- For each operator that will concurrently log in, one Protege GX Web Client license (purchasing code: PRT-GX-WEB-OPR), applied to the installed Software Serial Number (SSN).

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

You must also enable various Windows features and application pool settings, and install the Protege GX SOAP Service. For your convenience, the files required are included in this distribution package and the configuration instructions are included in this manual.

Protege GX SOAP Web Service Software Development Kit (SDK)

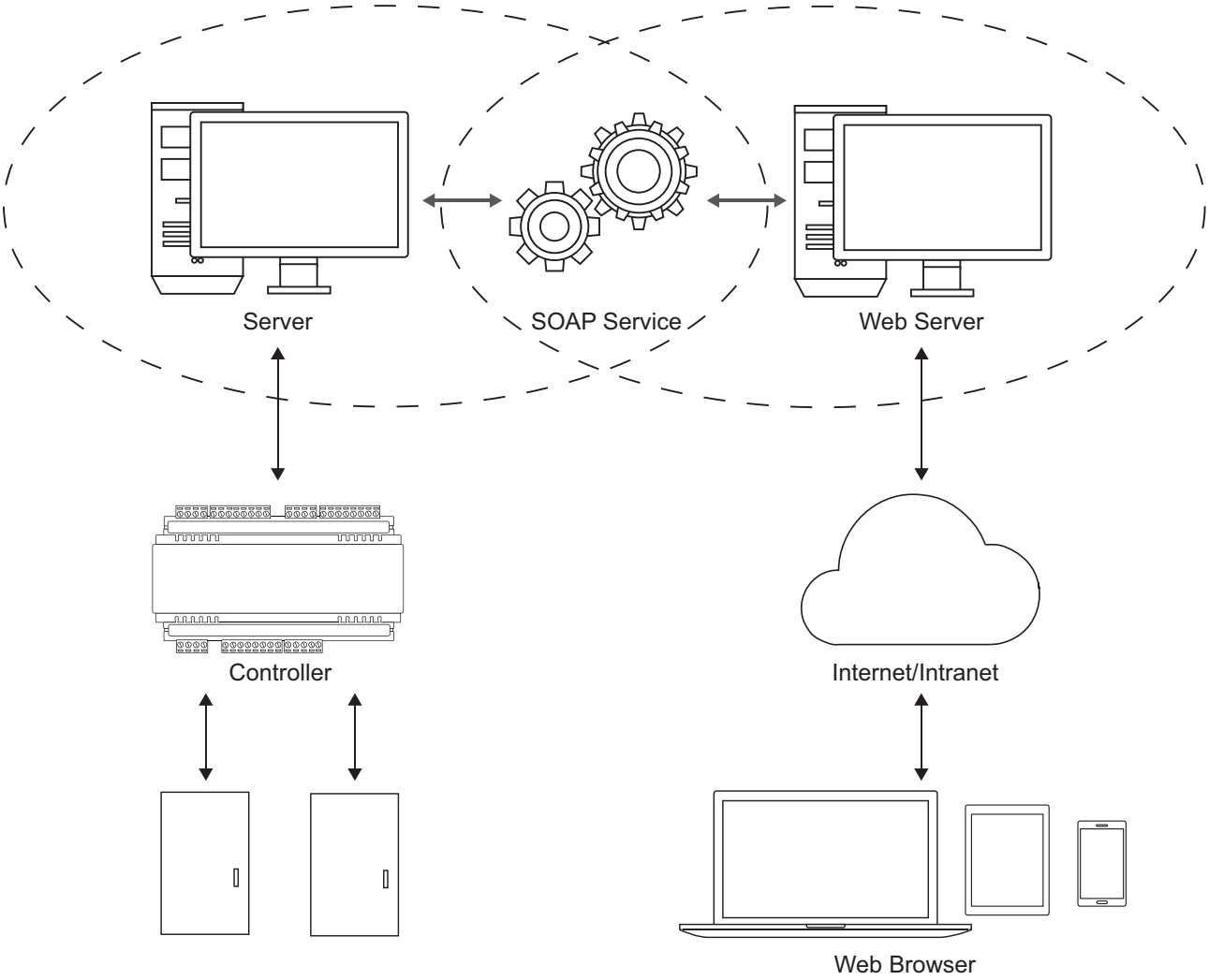
If you are building your own interface or integration you will also require the Protege GX SOAP Web Service Software Development Kit (purchasing code: PRT-GX-SOAP-SDK).

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

Installation Overview

Installed on a web server, the web client uses the SOAP service to communicate with the Protege GX server. These components may be installed on the same machine as the Protege GX server, or on a separate physical server.



Installing the Protege GX SOAP Service

In order to use the Protege GX Web Client, the Protege GX SOAP Service must be installed separately. If you have already completed this setup, proceed to the Installing the Protege GX Web Client section (see page 16).

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.

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

Enabling the Required Windows Features

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

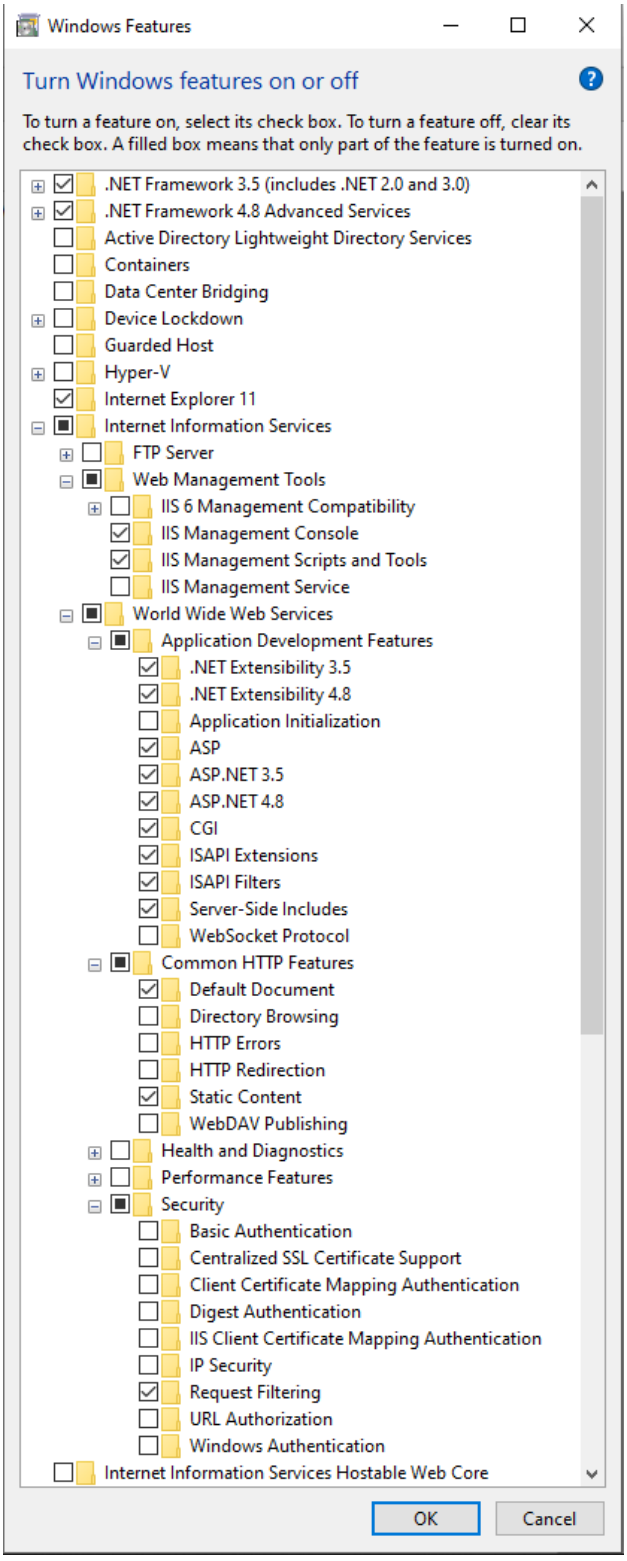
See the following pages for instructions for the operating system (Windows version) you are using.

- Windows 8.1 and 10 (see next page)
- Windows 11 (see page 10)
- Windows Server 2012 (see page 11)
- Windows Server 2016, 2019 and 2022 (see page 12)

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.

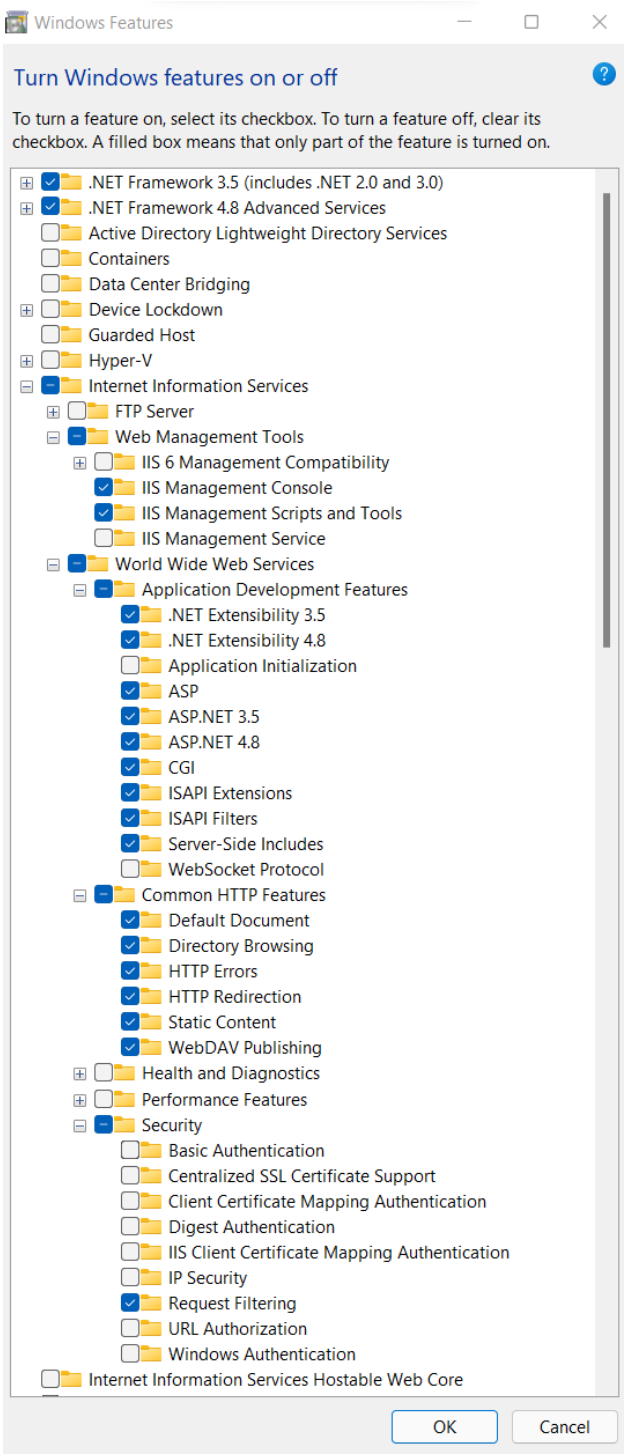


3. Click **OK**.

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.

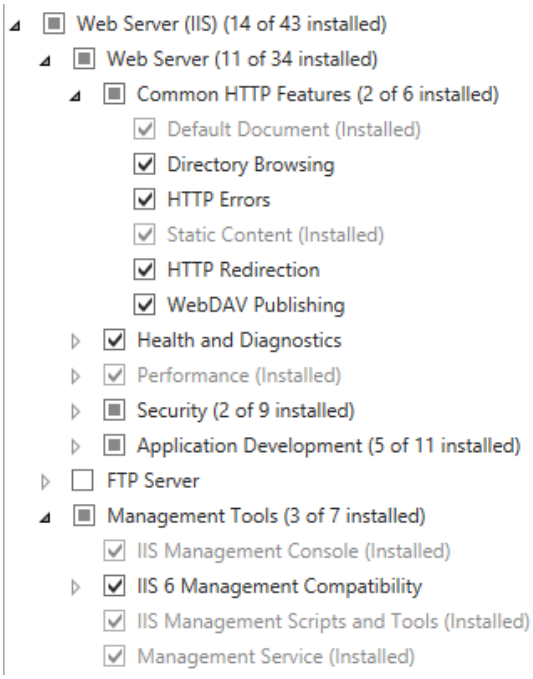


5. Click **OK**.

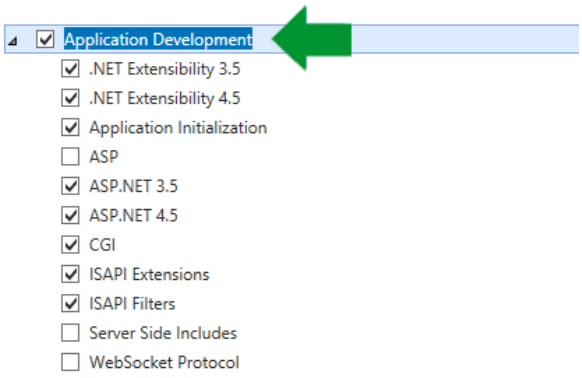
Windows Server 2012

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:

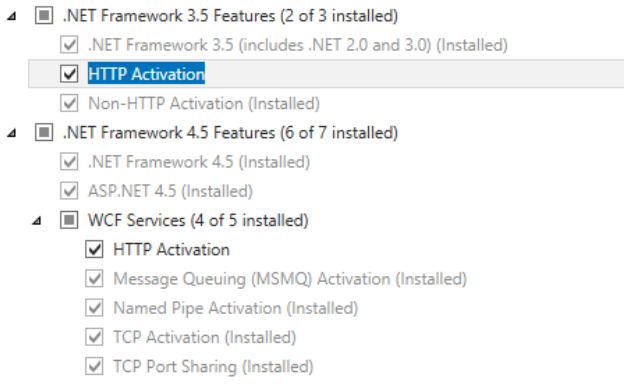
   Where an expandable check box is ticked, you need to expand it and enable all features and sub-features.



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.

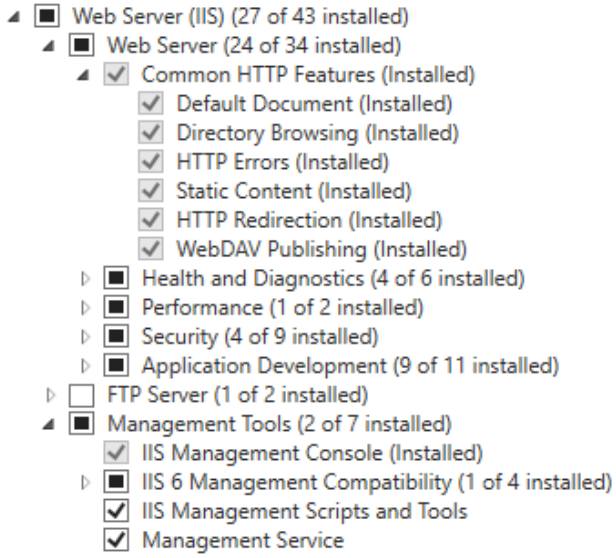


7. Click **Next** to complete the setup and install the features.

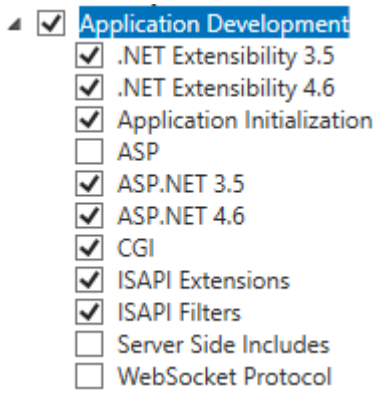
Windows Server 2016, 2019 and 2022

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:

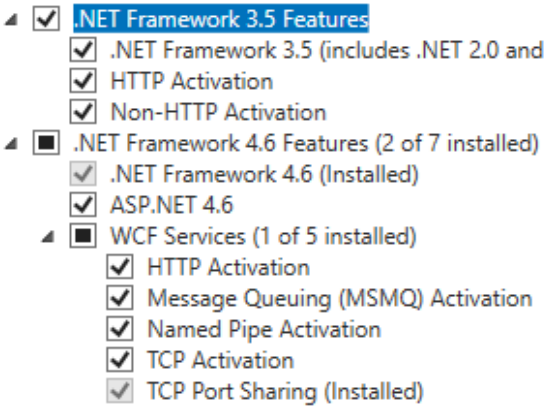
   Where an expandable check box is ticked, you need to expand it and enable all features and sub-features.

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.

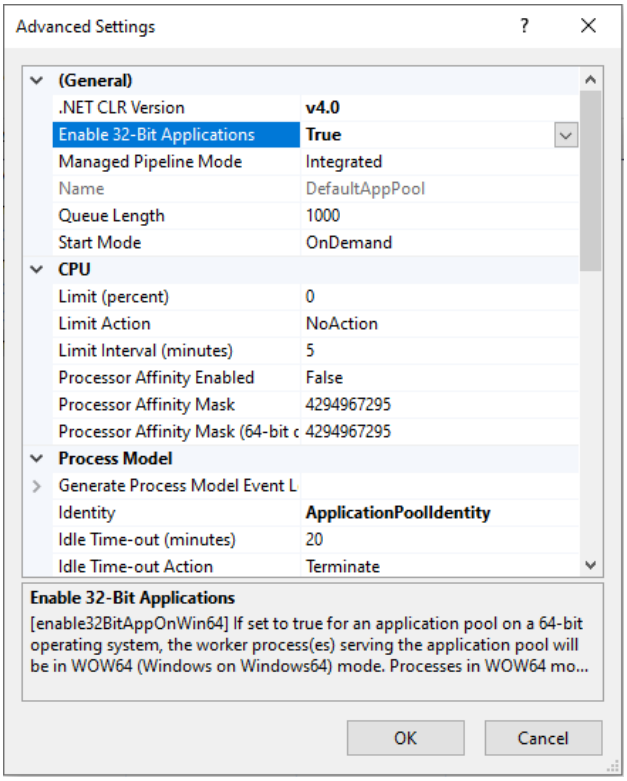
7. Click **Next** to complete the setup and install the features.

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.

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.

Installing the Protege GX Web Client

Following the prerequisite installations, you are able to install the web client. The web client must be installed on the same machine as the SOAP service.

Protege GX Web Client Installation

1. Run the supplied web client installer by right clicking and selecting **Run as Administrator**.
2. This launches the install wizard. Click **Next** to continue.
3. Read and accept the license agreement, then click **Next**.
4. By default, the install wizard installs the web client and a tool used to export reports to PDF. Click **Next** to confirm the installation of both features.

   To install only the web client, expand the drop-down menu for the **Export reports to PDF** feature and select **This feature will not be available**.

5. Click **Next** to accept the default PC name and port numbers. The default PC name should be changed if the Protege GX SOAP service is installed on another PC or remote server. The port numbers should be changed if there are other devices or services on the network that use the default ports.
6. Click **Install** to begin installation.
7. Click **Finish**.

Correct Time Zone Fix

In some instances, the time displayed on the web client's index page is inaccurate. This is because PHP handles time zones differently to Windows. If you don't configure your PHP server with a time zone, it attempts to default to the Windows system time zone, but it doesn't always get this right. For example, in Australia if you set your PC to Brisbane time, the web client thinks the time zone should be 'Australia/Melbourne'. This is incorrect because daylight saving is observed in Melbourne, Victoria, but not in Brisbane, Queensland.

This can be fixed by editing the **`php.ini`** configuration file.

1. Locate the **`php.ini`** config file which, by default, is found in C:\Program Files (x86)\PHP on 64-bit machines, and C:\Program Files\PHP on 32-bit machines.
2. Open the **`php.ini`** file in 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. Press **CTRL+F** and enter **date.timezone** in the field to locate the line that needs changing.
4. You should see the line:

   ```
   ;date.timezone =
   ```

5. Remove the semicolon before date.timezone and enter a supported time zone from the list available on the PHP website.
6. Once you have saved the **`php.ini`** file, open the Internet Information Services Manager and restart the Protege GX Web site.
7. The web client should display the correct time the next time you log in.

Accessing the Web Client

To access the web client:

1. Open a web browser and enter the following link into the URL bar:
   https://<pcname>.<domainname>:<portnumber>/ProtegeGXWebClient/login.php

   The default port number is **8060**. 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 web client 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. The link should present a login page.
5. Log in with your Protege GX username and password.

Security Configuration

Secure communications require end-to-end encryption: that is, every connection between services or applications must be encrypted. To achieve this, each stage in the path must be secured by a trusted SSL certificate, which allows the applications to communicate using the HTTPS protocol. For the web client, there are two connections to consider:

- Connection between the SOAP service and the web client
- Connection between the web client and the user's web browser (or another application such as the Protege GX mobile app)

Both the SOAP service and the web client automatically generate a self-signed SSL certificate during installation. However, these certificates are not inherently trusted by web browsers and other applications, so the connection may be refused or flagged as insecure. There are two options to achieve 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 both the SOAP service and the web client have a trusted SSL certificate installed, you can securely connect to the web client via the HTTPS endpoint (see page 16). This will remove the security warning which appears in the web browser when you navigate to the web client.

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.

Using a Third-Party Certificate for the Web Client

Once you have obtained a third-party certificate from a trusted certificate authority, you must install it in the **ProtegeGXWeb** site in Internet Information Services (IIS) Manager. This secures the connection between the web client and web browser or mobile app, and will remove any security warnings.

This is the recommended method for securing the web client 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 ProtegeGXWeb 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 **ProtegeGXWeb** site.
3. In the **Actions** panel, click **Bindings...**.
4. Select the https binding (port 8060) and click **Edit...**.

   Alternatively, you can add a new binding for the default HTTPS port of 443. This removes the need to enter the port number in the URL when connecting to the web client.
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 web client is upgraded, the certificate will be reset to the default. Repeat the steps above to rebind the custom certificate.

Using a Self-Signed Certificate for the Web Client

As an alternative to a third-party certificate, you may use a self-signed certificate for the web client. 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 and mobile device that will connect to the web client.

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 ProtegeGXWeb 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 **ProtegeGXWeb** site.
3. In the **Actions** panel, click **Bindings...**.
4. Select the https binding (port 8060) and click **Edit...**.

   Alternatively, you can add a new binding for the default HTTPS port of 443. This removes the need to enter the port number in the URL when connecting to the web client.
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 web client 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 to the web client.

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.

The SSL certificate installation is complete. This should remove the security warning which appears when you access the web client in a web browser. If the security warning is still present, consult the documentation for your web browser for any additional requirements.

Setting the Secure Flag for Session Cookies

Setting the secure flag for session cookies can prevent certain kinds of attacks by allowing the cookie to be sent over HTTPS only.

Setting the secure flag will prevent the web client from accepting HTTP connections. It will only be accessible via HTTPS.

1. Navigate to the web client's installation directory, which is by default C:\Program Files (x86)\Integrated Control Technology\Protege GX Web Client.
2. In the php directory, open the php.ini file.

Administrator permissions are required to edit files in this location. You must open the file as an administrator (using a text editor such as Notepad++). Alternatively, you can copy the file to a different location, edit and save the file, then paste into the original location, granting administrator permission to replace the original file.

3. Locate the line that reads:

```
;session.cookie_secure =
```

4. Remove the comment **;** and add the value **1**, so that the line reads:

```
session.cookie_secure = 1
```

5. Save the file.
6. Open the IIS Manager by pressing the **Windows + R** keys to open the **Run** prompt, then entering **inetmgr**.
7. In the pane on the right side, click **Restart** to restart the web server.

Updating the PHP Version

New versions of PHP are released regularly with security patches, bug fixes and new features. For improved security, you may wish to update the PHP version used by the Protege GX Web Client more frequently than new web client versions are released.

PHP has three version numbers: a major, minor and patch version (e.g. 8.1.19). Typically it is possible to update the patch and minor versions without affecting the system. The major version should not be updated manually.

1. Web browse to https://windows.php.net/download
2. Locate and download the required version of PHP. This must be a **Non Thread Safe** version.
3. Open Internet Information Services Manager. In the **Actions** pane, click **Stop**.
4. In the File Explorer, navigate to C:\Program Files (x86)\Integrated Control Technology\Protege GX Web Client\php
5. Rename the **php** folder to **php_old**.
6. Create a new folder called **php** at the same location.
7. Extract the zip file and copy all of the files into the new folder.
8. Copy the **php.ini** file from the old php folder to the new one.
9. In Internet Information Services Manager, click **Start**.
10. Browse to the web client and confirm you can log in and perform all expected functions.

ICT cannot guarantee that the web client will function correctly with any version of PHP that was not installed with the software. Test the system carefully after updating the PHP version. If any issues arise, roll back to the previous PHP version or contact ICT Technical Support.

Troubleshooting

This section deals with some common problems related to the Protege GX SOAP Service and Web Client installation, their causes, and potential solutions.

Cannot Access the Web Client over HTTP

Problem:

When you attempt to browse to the web client over HTTP (port 8050), the page does not load.

Cause:

The web client is no longer available over unencrypted HTTP from version 1.48.0.0. Only HTTPS is available.

Solution:

Use the HTTPS URL instead (see page 16). You may need to configure the web client's security certificate to allow the connection (see page 18).

Page Not Found

Problem:

A blank page, or a page with rectangular boxes with cross symbols, or a static content handler error is displayed.

Cause:

This frequently occurs when IIS has not been installed correctly due to missing prerequisites.

Solution:

1. Enable the required fields shown in the topic Enabling the Required Windows Features (see page 7).
2. Uninstall and reinstall the Protege GX SOAP Service.

OR

1. Navigate to **Control Panel | Programs and Features | Turn Windows Features On/Off**.
2. Locate and enable **Static Content** under **Internet Information Services | World Wide Web Services | Common HTTP Features**.
3. Restart IIS.

Communication Fault/Failure

To view a communication fault/failure, open the **Windows Event Viewer**.

Problem:

Communication error when attempting to log in to the Protege GX Web Client.

Cause:

This issue is commonly caused by security binding inconsistencies between the Protege GX Data Service and the Protege GX SOAP Service.

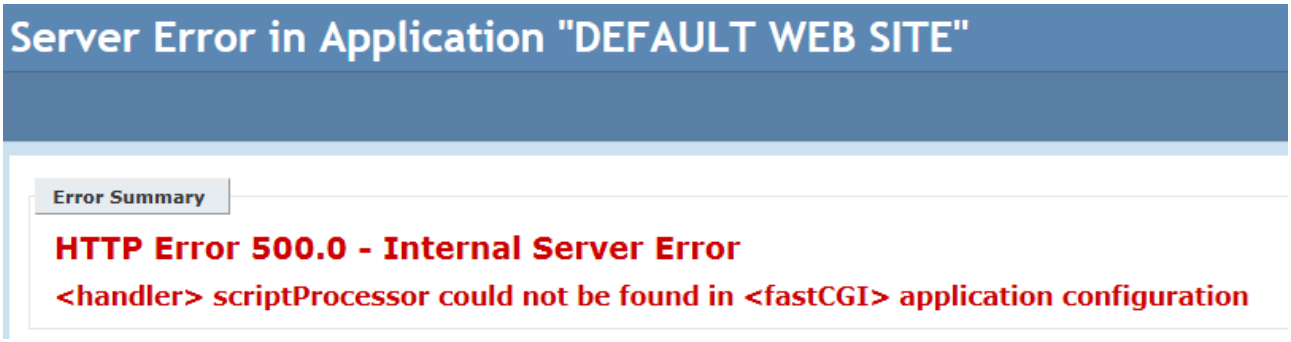
Solution:

1. Navigate to the Protege GX installation folder and open the **GXSV.exe.config** file.
2. Search for the following tag:
   ```
   <security mode="None" />
   ```
3. In a new file explorer window, navigate to **C:\inetpub\wwwroot\ProtegeGXSOAPService**,
4. Open the **web.config** file and search for the same tag:
   ```
   <security mode="None" />
   ```
5. If the tag is not found in the **GXSV.exe.config** file but is found in **web.config** file, remove the tag from the web.config file.
6. If the tag is found in the **GXSV.exe.config** file but is not found in **web.config** file, add the tag to the web.config file, in the same location as it appears in the GXSV.exe.config file.

CGI Failure

Problem:

When attempting to access the Protege GX Web Client, you are presented with the following page:



Cause:

The FastCGI settings may not be properly enabled in IIS during installation.

Solution 1:

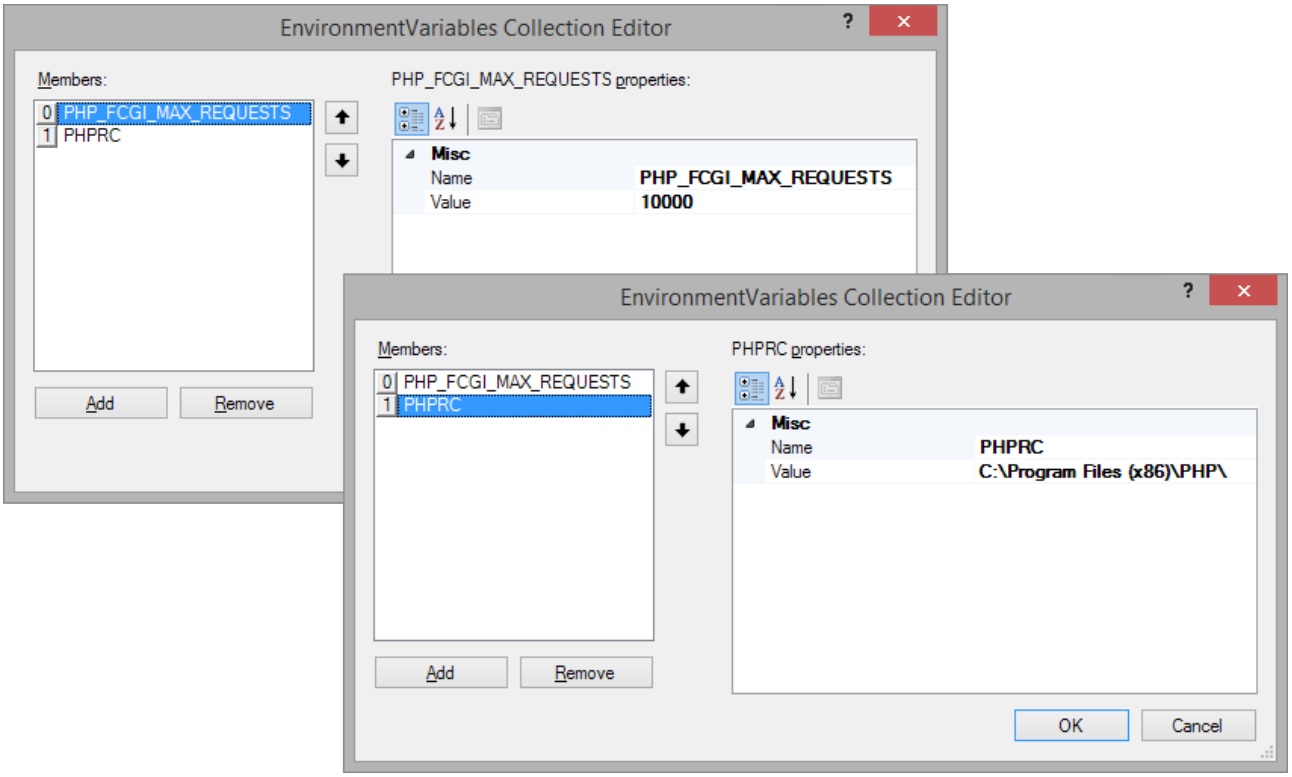
If PHP was already installed before running the Protege GX SOAP service installation, ensure that the PHP CGI executable is available in the PHP installation folder. If you are unsure of this, re-run the PHP installation and select **FastCGI** as the web server.

Solution 2:

1. Launch the Internet Information Services (IIS) Manager and select the top-level server node in the left-hand pane.
2. Select **Fast CGI Settings**.
3. Check whether there is an entry with the following parameters:
   - **Full Path**:
     - **C:\Program Files (x86)\Integrated Control Technology\Protege GX Web Client\php\php-cgi.exe** for 64-bit Windows
     - **C:\Program Files\Integrated Control Technology\Protege GX Web Client\php\php-cgi.exe** for 32-bit Windows
   - **Arguments**: (blank)

- **Max. Instances**: 0
- **Instance Max. Requests**: 10000

4. If the record is present, click the ellipsis button in the **Environment Variables** line.
5. Ensure that the following parameters match:
   - **PHP_FCGI_MAX_REQUESTS**: 10000
   - **PHPRC**: **C:\Program Files (x86)\PHP** for 64-bit Windows or **C:\Program Files\PHP** for 32-bit Windows



6. If this record does not exist, click **Add Application** to create it with the parameters shown above.
7. Navigate back to the main window and select **Handler Mappings**.
8. In the list, locate **PHP_via_FastCGI** and ensure that it has the following parameters:
   - **Path**: *.php
   - **Handler**: FastCgiModule
   - **State**: Enabled
9. If the record exits, double-click to open it and ensure that **Executable (optional)** field is set to the same path as the FastCGI application as in step 2.1.
10. If the record doesn't exist, click **Add Module Mapping** to create it.
11. Set the fields to the following:
    - **Request path**: *.php
    - **Module**: FastCgiModule
    - **Executable**: **C:\Program Files (x86)\PHP\php-cgi.exe** for 64-bit Windows or **C:\Program Files\PHP\php-cgi.exe** for 32-bit Windows
    - **Name**: PHP_via_FastCGI
    - **Request Restrictions**:
      - **Mapping**: Enable the **Invoke handler only if request is mapped to** option and select File or Folder
      - **Verbs**: All verbs
      - **Access**: Script

Cannot Save Records

Problem:

In the Protege GX Web Client it is impossible to save certain records, even though they can be saved in the Protege GX thick client. This especially effects records that involve a lot of data (e.g. users with multiple credentials or multiple access levels assigned).

Cause:

The maximum query string length is incorrectly configured in IIS. This value should be set to 65536 during installation. The above issue may occur when this value has not been set correctly and so is too small.

Solution:

1. Open the IIS Manager by pressing the **Windows + R** keys to open the **Run** prompt, then entering **inetmgr**.
2. Open **Request Filtering** from the central pane.
3. In the pane on the right, click **Edit Feature Settings**.
4. Set the **Maximum query string (Bytes)** to 65536.
5. Click **Ok**.

Web Client Hangs on Users Page

Problem:

When you load the **Users | Users** page of the web client, the client does not immediately load any user records. If you attempt to navigate to a different page before the user records have been loaded, the web client will hang instead of loading the new page.

Cause:

This is a known issue which may occur when using the HTTPS version of the web client.

Workaround:

This issue can be resolved by changing some settings within IIS.

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 on **FastCGI Settings**.
3. Right click on Protege GX Web Client line and select **Edit...**.
4. Set **Standard error mode** to TerminateProcess.
5. Set **Activity Timeout** to 20 (seconds).
6. Click **OK**.
7. In the left-hand pane, navigate to **Application Pools**.
8. Right click on **DefaultAppPool** and select **Set Application Pool Defaults...**.
9. Set **Maximum Worker Processes** to 3.
10. Click **OK**.

These settings should prevent the web client from hanging on the users page.

SSL Key Usage Incompatible

Problem:

When you attempt to browse to the web client, you receive one of the following error messages:

- **Chrome**: SSL_KEY_USAGE_INCOMPATIBLE
- **Edge / Firefox**: An exception occurred retrieving operator details

Cause:

This is caused by a conflict with TLS 1.3 on newer versions of Internet Information Services.

Solution:

Disable TLS 1.3 on the SOAP and web client sites.

1. Open Internet Information Services Manager.
2. Locate the ProtegeGX site in the sidebar.
3. Right click on the site and select **Edit Bindings...**
4. Select **HTTPS** and click **Edit...**
5. Select **Disable TLS 1.3 over TCP**.
6. Click **OK**, then **Yes**.
7. Click **Close**.
8. Repeat for the ProtegeGXWeb site.

Known Issues

This section explains some known limitations related to the Protege GX Web Client operation.

User Reports

- In the web client it is not possible to filter the columns on user reports with the standard Yes/No filter selections. As a workaround user report columns with Yes/No selections can be filtered by entering into the report's filter editor a value of **T** or **True** for Yes and **F** or **False** for No.
- The web client is unable to display credential type data on user reports. There is no workaround for this limitation.

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.