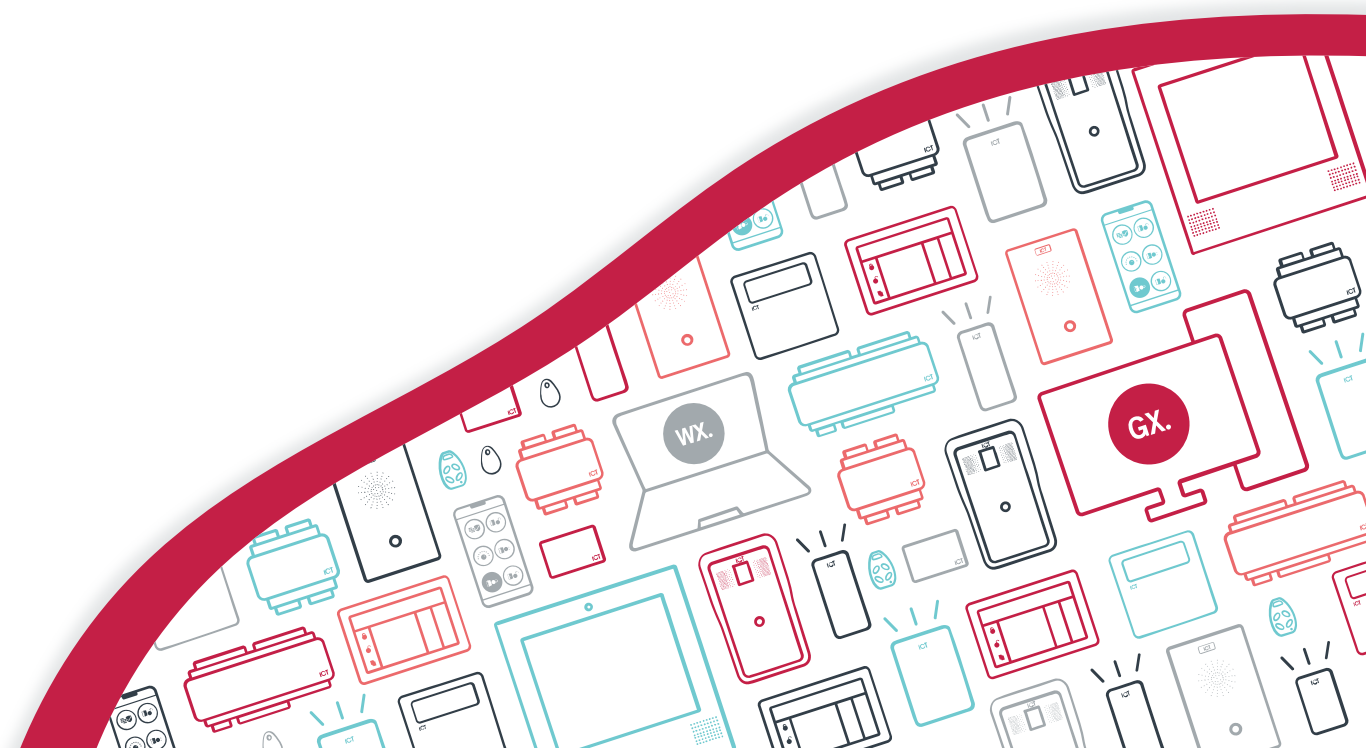
AN-277

Configuring Protege GX to use TLS 1.2

Application Note



Last Published: 17-Jun-22 3:47 PM

Contents

Introduction

As technology expands rapidly so does the possibility of security breaches or nefarious hackers attempting to break in and steal data. In order to keep systems safe and secure a number of protocols and security features are implemented to protect communications and the data being transferred.

Transport Layer Security (TLS) is a commonly used example of such protocols. However, several known vulnerabilities have been reported against earlier versions of Transport Layer Security (TLS). We recommend that you upgrade to TLS 1.2 for secure communication.

TLS 1.2 has been implemented in Protege GX and is now the default security setting for Protege GX software communication channels. This application note outlines the steps to fully configure Protege GX to use TLS 1.2.

Prerequisites

To enable TLS 1.2 the following are required:

Software Component	Version	Notes
Protege GX	4.3.264.9 or higher	
Microsoft SQL Server	**32-bit installations:** 2012 SP4, 2014 SP2, or a later edition that supports TLS 1.2 **64-bit installations:** 2016 SP2 or a later edition that supports TLS 1.2	For the SQL server editions that support TLS 1.2, see the Microsoft Documentation. For the SQL server editions supported by Protege GX, see the Protege GX Server Installation Manual.

TLS 1.2 Setup

TLS 1.2 is the default security option in the Protege GX installation process, and required items are automatically set up in the background unless a different option is selected. If TLS 1.2 is not currently enabled in your installation, you can enable it by reinstalling the application and ensuring that TLS 1.2 is selected.

To check whether TLS 1.2 was enabled during installation, navigate to the installation directory (C:\Program Files (x86)\Integrated Control Technology\Protege GX) and open GXSV.exe.config in a text editor. If the file contains the text `sslProtocols="Tls12"`, then TLS 1.2 was enabled.

As part of the Protege GX install process a number of items are installed or configured. These include:

- Installing Microsoft .NET Framework 4.6.2.
- Installing OLE DB Driver 18.
- Creating a self-signed certificate on the local PC.
- Adding configuration entries into the Windows registry.
- Adding required configuration entries into the Protege GX config files.

In addition to the above the following manual steps are required to fully enable TLS 1.2 for Protege GX.

Different configuration is required to use TLS 1.2 with Windows Authentication. For more information, see Logging in with Windows Authentication (page 10).

Enabling Force Encryption and TCP/IP

1. Open SQL Server Configuration Manager:
   - Press **Windows + R** to open the run dialogue.
   - Type sqlservermanager<version>.msc, replacing <version> with the version number of the application corresponding to your SQL Server installation (see this page).
   - Click **OK**.
2. Open the **SQL Server Network Configuration** section from the left-hand pane.
3. Right click on **Protocols for ProtegeGX** (or the SQL instance name that holds the Protege GX database), and select **Properties**.
4. In the Properties window set **Force Encryption** to Yes and click **OK**.
5. Open **Protocols for Protege GX**.
6. Double click **TCP/IP** and set **Enabled** to Yes. Click **OK** to close the window.
7. Open **SQL Server Services** from the left-hand pane.
8. Right click on **SQL Server (ProtegeGX)** in the right-hand pane and select **Restart** to restart the Protege GX SQL Server Service.
9. When complete, close the SQL Server Configuration Manager.

Enabling the IIS Management Console

1. Enable the IIS Management Console by navigating to: **Control Panel > Programs and Feature > Turn Windows Features On or Off**.
2. In the feature list, navigate to **Internet Information Services > Web Management Tools > IIS Management Console**. Check the box to enable this feature.
3. Click **OK**.
4. Restart all Protege GX services.

Using a Custom Certificate

In some systems, it is preferred to use a custom TLS/SSL certificate instead of the self-signed certificate generated by Protege GX during installation. Some additional configuration is needed to install the custom certificate.

This is required when there are Protege GX clients connecting to the server from outside the router/firewall and port forwarding is in place. The custom certificate must refer to the external hostname of the Protege GX server.

The exact process may vary depending on your operating system. Consult your IT provider for more detailed instructions.

Obtaining the Server Certificate

An SSL certificate in the form of a .pfx file must be obtained from your IT provider. This can be self-signed or provided by a trusted certificate authority. You will also require the password used to generate the file, in order to install the certificate.

Installing the Server Certificate

1. Copy the .pfx file to the Protege GX server you are installing the certificate on.
2. Double click the certificate to initiate the **Certificate Import Wizard**.
3. Set the **Store Location** to Local Machine.
4. Do not change the **File to Import**.
5. Enter the password used to generate the .pfx file. The person who generated the certificate should know this.
6. Set the place where you wish to store the certificate as the **Personal folder**.
7. Complete the import.

Configure Protege GX to use the Certificate

Once the certificate is installed you will need to configure Protege GX to use that certificate for its connections.

1. Open **Microsoft Management Console** by pressing **[WIN + r]**, typing mmc and pressing enter.
2. Once the console is open, open **Add or Remove Snap-ins** by pressing **[CTRL + m]**, or via the **File** menu.
3. Double click **Certificates**, select **Computer Account** and click **Next**.
4. Select **Local Computer** and click **Finish**.
5. Click **OK** to close the snap-ins window.
6. Navigate to **Certificates (Local Computer) > Personal > Certificates**.
7. You should be able to see your installed certificate here. Double click on it.
8. Find the field named **Thumbprint** and copy the data from it to a safe place.
9. Open **GXSV.exe.config**, located in the installation directory (C:\Program Files (x86)\Integrated Control Technology\Protege GX).

   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.

10. Locate the following section in the XML:
    /configuration/system.serviceModel/behaviors/serviceBehaviors/behavior[@name="md"]/serviceCertificate

    If this section does not exist it is because you did not install Protege GX with TLS enabled.

11. In the **<serviceCertificate>** tag, change the **findValue** to the thumbprint of the new certificate you installed. The result will look similar to the following:

```
<serviceCertificate
storeLocation="LocalMachine" storeName="My" findValue="CERTIFICATE_
THUMBPRINT" x509FindType="FindByThumbprint" />
```

12. **Save** the config file and **restart** the Protege GX Data Service for the changes to take effect.

Custom Wildcard Certificates

It is possible to install custom wildcard TLS certificates in the same way as the standard custom certificates above. However, due to bugs in the Windows Communication Foundation (the service framework used by the Protege GX Data Service), some additional configuration is required to install a wildcard certificate.

In particular, it is necessary to change the hostname in **GXPI.exe.config** and **GXRpt.exe.config** from localhost to the hostname you will actually be connecting to.

This should be completed for both config files for **each client installation**. However, the same configuration files can simply be copied to other machines as necessary.

The following sections need to be updated in each file:

- **configuration/system.serviceModel/client/endpoint@address** - this should be the full hostname that you are actually connecting to.
- **configuration/system.serviceModel/client/endpoint/identity/dns@value** - this should be the first entry listed in the certificate's Subject Alternative Names section.

Example:

```
<endpoint address="net.tcp://security.other.domain.bits:8000/GXSV/GXService"
behaviorConfiguration="md0" binding="netTcpBinding"
bindingConfiguration="Binding1" contract="ServiceReference2.IGXService">
    <identity>
        <dns value="*.other.domain.bits" />
    </identity>
</endpoint>
<endpoint address="net.tcp://security.other.domain.bits:8010/GXSV/GXService2"
behaviorConfiguration="md0" binding="netTcpBinding"
bindingConfiguration="Binding1" contract="GXServiceRef2.IGXService2">
    <identity>
        <dns value="*.other.domain.bits" />
    </identity>
</endpoint>
```

After this change has been made, when connecting from the client it is necessary to leave the **Server** field on the login page blank. If this field is filled the client will fail to connect correctly.

Enabling Certificate Validation on the Client

When a custom trusted certificate is in use, it is recommended to enable service certificate validation to harden the connection between the Protege GX server and client. This protects against man-in-the-middle attacks during the initial connection.

This is only available when a third-party certificate provided by a trusted authority is used, or a self-signed certificate that has been installed as a trusted certificate on client workstations. If the same client workstation is used to connect to multiple Protege GX servers, this setting requires all servers with TLS enabled to use a trusted certificate.

To enable service certificate validation, complete the following configuration on all client workstations:

1. Open **GXPI.exe.config**, located in the installation directory (C:\Program Files (x86)\Integrated Control Technology\Protege GX).

   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.

2. Directly after the **<configSections>** node, add the **<appSettings>** node as shown below:

```
<configSections>
    <section
name
="microsoft.scripting"
 type="Microsoft.Scripting.Hosting.Configuration.Section,
Microsoft.Scripting, Version=1.0.0.0, Culture=neutral,
PublicKeyToken=null" requirePermission="false" />
</configSections>
<appSettings>
    <add key="client.validateServiceCertificate" value="true" />
</appSettings>
```

3. Save the config file.

The customized config file may be overwritten when the software is upgraded. You may be required to add the **<appSettings>** node to each client again after the upgrade.

Configuring the Protege GX SOAP Service

This section describes the additional configuration required to deploy the Protege GX SOAP Service for TLS 1.2.

1. When installing the Protege GX SOAP Service, ensure that you install with **TLS enabled**.

   On the **Customize WCF TCP/IP Port** page, point the SOAP service to the Protege GX server:
   - **Protege GX Data Server installed PC name**: the DNS name or hostname of the Protege GX server
   - **Data Server Port**: 8000 (or as configured)
   - **Report Server Port**: 8010 (or as configured)

   For instructions on installing the SOAP Service, see the Protege GX SOAP Service Installation Manual.

2. Locate and edit the following file: **C:\inetpub\wwwrootProtegeGXSOAPService\Web.config**.
   - Under **/configuration/system.serviceModel/**, comment out or remove this line: **<serviceHostingEnvironment multipleSiteBindingsEnabled="true" />**.
   - When using TLS security (recommended) on the data service:
     - Under **/configuration/system.serviceModel/client/endpoint@address**, set the endpoint hostname to the DNS name or hostname of the Protege GX server.
     - Under **/configuration/system.serviceModel/client/endpoint/identity/dns@value**, set the endpoint DNS-identity to one of the 'Subject Alternative Names' in the data service's TLS Certificate.
     - The following node should not exist when using a custom certificate. Remove if present: **/configuration/system.serviceModel/behaviors/endpointBehaviors/behavior[@name=md0]/clientCredentials/serviceCertificate/authentication**.

Renewing TLS Certificates

Sometimes it is necessary to renew or update the TLS certificate associated with a Protege GX installation. This can happen when:

- The existing certificate expires.
- The server's IP address or hostname changes so that the existing certificate is no longer valid.

If you are using the default self-signed certificate generated by your Protege GX installation, you must uninstall and reinstall Protege GX to generate a new self-signed certificate.

If you are replacing a custom certificate, you will need to install and configure the new certificate as described above (see page 6). To complete the process, restart the Protege GX Data Service.

Logging in with Windows Authentication

Protege GX's Windows Active Directory integration allows operators to use Windows Authentication to log in to Protege GX. Some additional configuration is required to continue using Windows Authentication alongside TLS 1.2.

Windows Active Directory integration is a licensed feature which must be purchased separately for operators (order code: PRT-GX-AD-OPR) and users (order code: PRT-GX-AD-USR).

Requirements

- Windows Authentication login should be tested and working prior to enabling TLS 1.2. It can be enabled for each operator under **Global | Operators**. This gives a known starting point if troubleshooting is necessary.
- The Protege GX Data Service machine (i.e. the Protege GX server) must be joined to the Windows domain.
- All workstation clients must access the system from a logged in domain account on the same Windows domain as the Protege GX Data Service.
- TLS 1.2 should be enabled and configured correctly on the server and all workstation clients.
- The Protege GX Data Service must run under the NT AUTHORITY\SYSTEM account (default). It cannot be run under a domain account or a local machine account.

Once the following changes have been applied, when logging into Protege GX it will be necessary to specify the **machine name** of the Protege GX server. This is required even when logging on to the server machine: leaving the field blank or entering localhost will no longer function.

Configuration

The following configuration is required to use TLS 1.2 with Windows Authentication (Active Directory).

Edit the Configuration Files

The following configuration change **must** be made to the **GXSV.exe.config** file on the server, and the **GXPI.exe.config** file on all clients.

The above files are located in the installation directory, by default C:\Program Files (x86)\Integrated Control Technology\Protege GX.

1. Locate the following section in the XML:
   /configuration/system.serviceModel/bindings/netTcpBinding/binding[@name="Binding1"]/security
2. **Replace** the existing security node with the code below:

```
<security mode="TransportWithMessageCredential">
    <transport clientCredentialType="None"
protectionLevel="EncryptAndSign" sslProtocols="Tls12"/>
    <message clientCredentialType="Windows"/>
</security>
```

3. **Save** the config file. You must **restart** the Protege GX Data Service for any changes to GXSV.exe.config take effect.

Disable NTLM

You may wish to disable use of the legacy NTLM authentication protocol in order to test that the configuration will work on other machines, or for better security. When NTLM is disabled, authentication will occur via the Kerberos protocol. Make the following change to the **GXSV.exe.config** file on the server, and the **GXPI.exe.config** file on all clients:

1. Locate the following section in the XML:
   /configuration/system.serviceModel/behaviors/endpointBehaviors/behavior
   [@name="md0"]/clientCredentials/
2. Add the configuration line below as a child of the **<ClientCredentials>** element:

   ```
   <windows allowNtlm="false"/>
   ```

3. **Save** the config file. You must **restart** the Protege GX Data Service for any changes to GXSV.exe.config to take effect.

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