AN-299

Using Windows Authentication with the Protege GX Web Client

Application Note

Last Published: 11-May-22 10:45 AM

Contents

Introduction

Protege GX integration with Windows Active Directory provides the convenience and security of Windows Authentication, allowing operators to automatically log in to Protege GX with their domain credentials.

This Application Note describes how to implement Windows Authentication for use with the Protege GX Web Client, using the Kerberos Protocol.

For more information about integrating Active Directory with Protege GX, see Application Note 288: Using Active Directory in Protege GX.

Prerequisites

Configuring Windows Authentication requires the KRBStub.zip file to implement the Kerberos Protocol on the Web Client. This file is available from ICT on request.

The following applications and configurations are required to implement Windows Authentication with the Protege GX Web Client:

- The Protege GX server, SOAP Service and Web Client must be installed and functional. The prerequisites for installing all of these applications also apply to this feature.

  For installation instructions and prerequisites, see the relevant installation manual.
- Protege GX Web Client version 1.47.034 or higher is required.
- The **Use Windows Authentication** option must be enabled during installation of the Protege GX server and SOAP Service.
- The **Use HTTPS to Communicate with SOAP Service** option must be enabled during the installation of the Protege GX Web Client.
- The Protege GX Data Service, SOAP Service, and Web Client must be joined to the same Windows domain.
- The Protege GX Active Directory Operator Integration must be configured and functional for the Protege GX thick client. This is a licensed feature (product code: PRT-GX-AD-OPR).

  To set up the Active Directory Integration, see Application Note 288: Using Active Directory in Protege GX.

Required Web Client IIS configuration:

- The Protege GX Web Client IIS Application must have network access to the Protege GX Data Service. Some configuration may be required if the Web Client and SOAP Service are installed on different machines.
- The Protege GX Web Client IIS Website must be using HTTPS. This can be achieved by removing the http binding from the site in the IIS manager, or by adding an HTTP-to-HTTPS redirect in the Web Client's web.config file.

Required Active Directory configuration:

- The Service Principal of the Protege GX Web Client IIS Application must have an appropriate Service Principal Name (SPN) for requesting client credentials. The following formats may be appropriate for SPNs:
  - HOST/servername.domainname.local
  - HTTP/servername.domainname.local
  - HTTP/servername

  For more information, see the Microsoft Support article on using SPNs. The Kerberos Configuration Manager utility may assist with diagnosing SPN related issues.

Configuring Windows Authentication

Adding the Kerberos (KRBStub) Application to IIS

Using Window Authentication with the Web Client requires the KRBStub Service to be deployed under the Protege GX Web Client application in Microsoft Internet Information Services (IIS). Its root URL should be /ProtegeGXWebClient/KRBStub/.

The KRBStub.zip file is available from ICT on request.

1. Open the **Internet Information Services Manager** by:
   - Pressing the **Windows + R** keys to open the run dialogue
   - Typing **inetmgr** into the search bar and pressing **Enter**
2. In the **Connections** pane on the left side, expand the following nodes:
   - Server (PC Name)
   - Sites
   - ProtegeGXWeb
   - ProtegeGXWebClient
3. Click on the **ProtegeGXWebClient** node. In the **Actions** on the right side, click the **Explore** action to open the program files in Windows Explorer.
4. Extract the KRBStub.zip file to a new KRBStub directory within the ProtegeGXWebClient directory. Ensure that the following path is valid: C:\inetpub\wwwroot\ProtegeGXWebClient\KRBStub\bin\KRBStub.dll.
5. Return to IIS. In the **Connections** pane on the left, right click on the **ProtegeGXWebClient** node. Select **Add Application**.
6. Fill in the following Application details:
   - **Alias**: KRBStub
   - **Physical path**: C:\inetpub\wwwroot\ProtegeGXWebClient\KRBStub

   Click **OK**.

Configuring Windows Authentication in IIS

To use Windows Authentication with the Web Client, all authentication options except for **Windows Authentication** should be disabled. The Windows Authentication option should only have the **Negotiate** provider available (or it must be the first in the list).

1. Select the **ProtegeGXWebClient** node in IIS as above. In the central **Features** pane, double click **Authentication**.
2. Right click on **Anonymous Authentication** and select **Disable**.
3. Right click on **Windows Authentication** and select **Enable**.
4. In the **Actions** pane on the right, select **Providers...**.
5. Ensure that **Negotiate** is the first or only provider in the list. If Negotiate is not in the Enabled Providers list, select it from the **Available Providers** dropdown and click **Add**.

   Click **OK**.

Optionally, you can require SSL for the KRBStub application to receive more meaningful error messages (instead of e.g. 404 or WCF Activation Failure messages). In IIS, select the **KRBStub** application in the left pane. In the central pane, double click the **SSL Settings** icon and check **Require SSL**.

Editing the KRBStub Config File

If the Protege GX Web Client is hosted on a different machine to the Protege GX Data Service, it is necessary to manually edit the web.config file so that it points at the Data Service.

1. Locate the web.config file in the /ProtegeGXWebClient/KRBStub/ directory and open it with 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.

2. Locate the connection string for the client endpoint:

   ```
   <client>
     <endpoint address="...">
   ```

3. Replace `localhost` with the hostname of the PC where the Protege GX Data Service is hosted.
4. Save the file.

Browser Configuration (Optional)

To prevent security warnings when accessing the Web Client, you can mark it as a trusted site. This should be done for every PC that will log in to the Web Client.

To add a Trusted Site to Internet Explorer, Microsoft Edge and Google Chrome:

1. Open the **Windows Control Panel**. Double click **Internet Options** to open the Internet Properties dialogue.
2. Open the **Security** tab and select **Trusted Sites**.
3. Enter the URL for the Web Client: https://<host>:<port>/ProtegeGXWebClient/KRBStub and click **Add**.

For Firefox, you can disable Enhanced Tracking Protection:

1. In Firefox, browse to https://<host>:<port>/ProtegeGXWebClient.
2. Click on the **Shield** icon to the left of the browser bar.
3. Click the toggler to disable **Enhanced Tracking Protection**.
4. To view the sites which have Enhanced Tracking Protection disabled, navigate from there to **Protection Settings > Manage Exceptions** .

Disable NTLM (Optional)

You may wish to disable use of the legacy NT LAN Manager (NTLM) authentication protocol, either 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.

To disable NTLM, make the following change to the following files:

- The **GXSV.exe.config** file on the server
- The **GXPI.exe.config** file on all clients

These config files are located in the installation directory. Default location:

C:\Program Files (x86)\Integrated Control Technology\Protege GX.

1. Locate and open the config file for editing.

   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. In the config file XML, locate the following section:

   ```
   /configuration/system.serviceModel/behaviors/endpointBehaviors/behavior
   [@name="md0"]/clientCredentials/
   ```

3. Add the following configuration line as a child of the **<clientCredentials>** element:

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

4. Save the config file.

5. You must **restart** the Protege GX Data Service for changes to GXSV.exe.config to take effect.

Configuring Windows Authentication and TLS1.2

Some additional configuration is required to continue using Windows Authentication to log in to the Web Client when TLS 1.2 is used for authentication on data service/client communications.

Prerequisites

- Windows Authentication login should be tested and confirmed to be working prior to enabling TLS 1.2.

  This provides a known starting point if troubleshooting becomes necessary.

- The machine running the Protege GX Data Service (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 must be enabled and configured correctly on the server and all workstation clients. See Application Note 277: Configuring Protege GX to use TLS 1.2.

  When following on from the instructions to configure Windows Authentication (see page 5), Protege GX must be uninstalled and then reinstalled (selecting the option for TLS1.2 during installation).

- TLS 1.2 should be enabled and configured correctly for the SOAP Service.

  When following on from the instructions to configure Windows Authentication (see page 5), The Protege GX SOAP Service must be uninstalled and then reinstalled (selecting the option for TLS1.2 during installation).

Edit the Configuration Files

Server and Client Config Files

The following configuration changes must be made to:

- The **GXSV.exe.config** file on the server
- The **GXPI.exe.config** file on all clients

These config files are located in the installation directory. Default location:

C:\Program Files (x86)\Integrated Control Technology\Protege GX.

Note: If the Protege GX workstation client software is **not** installed on a client PC, and the PC will only be using the **Web Client** to log in, then omit the GXPI.exe.config changes for that PC.

GXSV.exe.config

1. Open the config file for editing.

   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. In the config file XML, locate the following section:
   ```
   /configuration/system.serviceModel/client/identity
   ```
3. Replace the node <dns value="localhost"/> with:
   ```
   <ServicePrincipalName value="host/servername.domainname.local" />
   ```
4. In the config file XML, locate the following section:
   ```
   /configuration/system.serviceModel/bindings/netTcpBinding/bindingname="Bin
   ding1"/security
   ```
5. Replace the existing security node with the code below:
   ```
   <security mode="TransportWithMessageCredential"><transport
   clientCredentialType="None" protectionLevel="EncryptAndSign"
   sslProtocols="Tls12"/><message clientCredentialType="Windows"/></security>
   ```
6. Save the config file.

GXPI.exe.config

1. Open the config file for editing.

   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. In the config file XML, locate the following section:
   ```
   /configuration/system.serviceModel/bindings/netTcpBinding/bindingname="Bin
   ding1"/security
   ```
3. Replace the existing security node with the code below:
   ```
   <security mode="TransportWithMessageCredential"><transport
   clientCredentialType="None" protectionLevel="EncryptAndSign"
   sslProtocols="Tls12"/><message clientCredentialType="Windows"/></security>
   ```
4. Save the config file.

Web Config Files

The following configuration change must be made to the **Web.config** file in the **ProtegeGXSOAPService** folder of the IIS website on the server. Default location:

C:\inetpub\wwwroot\ProtegeGXSOAPService

1. In the config file XML, locate the following section:
   ```
   /configuration/system.serviceModel/bindings/netTcpBinding/bindingname="Bin
   ding1”/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.

The following configuration change must be made to the **Web.config** file in the **KRBStub** folder of the IIS website on the server. Default location:

C:\:\inetpub\wwwroot\ProtegeGXWebClient\KRBStub

1. In the config file XML, locate the following section:
   `/configuration/system.serviceMode1/bindings/netTcpBinding/bindingname="NetTcpBinding_IGXService"`
2. Replace the entire binding node with the following code.

   This inserts the security settings and closes the binding node correctly.

   ```
   <binding name="NetTcpBinding_IGXService"><security
   mode="TransportWithMessageCredential"><transport
   clientCredentialType="None" protectionLevel="EncryptAndSign"
   sslProtocols="Tls12"/><message
   clientCredentialType="Windows"/></security></binding>
   ```
3. Replace all references to **localhost** with the **Fully Qualified Domain Name** of the Protege GX server.
   e.g. `SERVERNAME.DOMAINNAME.LOCAL`
4. Save the config file.

Restart Services

When all the above configuration steps are complete, you need to restart:

- The Protege GX Data Service
- The IIS web service

Restarting the Services

1. Navigate to **Control Panel | System and Security | Administrative Tools**.
2. Open the **Services** snap-in.
3. Right click on the **Protege GX Data Service** and select **Restart**.
4. Close the Services snap-in.
5. Open the **Internet Information Services (IIS) Manager**.
6. In the **Connections** pane on the left, left click to select the **server**.
7. In the **Actions** pane on the right, under **Manage Server** click **Restart**.
8. Close the Internet Information Services (IIS) Manager.

Using Windows Authentication with the Web Client

Logging in with Windows Authentication

The following are required for an operator to log in to the Web Client using Windows Authentication:

- The client browser machine must be joined to the relevant Windows domain.
- The end user must be logged in to the PC using a domain account.
- The end user's Windows domain account must be connected to an operator in Protege GX.
- The Protege GX Web Client must be accessed via https://<hostname>:<port>/ProtegeGXWebClient/, not via localhost.

The steps for an operator to log into the Web Client with Windows Authentication are as follows:

1. Log in to a PC on the domain network using an Active Directory account.
2. Access the Web Client via a web browser using the URL: https://<host>:<port>/ProtegeGXWebClient/.
3. On the login page, enable **Use Windows Authentication** and click **Login**. You should be logged in to the Web Client as the operator associated with that Windows domain account.

Using the Service to get a Session (Optional)

The following API request can be used to get a session for debugging or use with the SOAP service:

```
HTTP GET https://<host>:<port>/ProtegeGXWebClient/KRBStub/KRBStub.svc/SOAPLogin
```

This service must be accessed over HTTPS only.

If it succeeds, the request will return a session cookie similar to the below:

```
{"Cookie":51806696,"OperatorID":22,"RoleID":0,"Username":"DOMAIN\\userlogin"}
```

The cookie provided may be passed to the SOAP service in place of the usual username/password credentials:

- `LD.LogonType`: 3
- `LD.Password`: The cookie obtained above.

Troubleshooting

If Windows Authentication is not working, check the following:

- Review the prerequisites (see page 4) to ensure that they have all been met.
- Check and confirm that there are sufficient Client licenses installed.
- You should be connecting to the Web Client via HTTPS.
- The Web Client should be connecting to the SOAP Service via HTTPS.
- You should be able to log in to the Protege GX thick client using Active Directory on the same machine.

  If you are getting the following message, you may not have a Protege GX operator configured for the current domain account: "The server encountered an error processing the request. The exception message is 'Failed to log on: 0x00002711'".
- If you have performed a Web Client upgrade or reinstall recently, the IIS configuration in the document may need to be reapplied.

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