AN-288

Using Active Directory in Protege GX

Application Note

Last Published: 28-Jan-22 8:17 AM

Contents

Introduction ____ 4

What is Active Directory? ... 4

Active Directory and Protege GX ____ 5

Key Advantages ... 5

Active Directory for Operator Management ... 5

Active Directory User Integration ... 6

Data Sync Active Directory User Integration ... 7

Licensing ... 7

Active Directory Operator Integration ____ 8

Prerequisites ... 8

Programming ... 8

Configuring TLS 1.2 ... 9

- Requirements ... 9
- Configuration ... 9

Active Directory User Integration ____ 11

Prerequisites ... 11

Active Directory User Import Settings ... 11

Data Sync Active Directory User Integration ____ 12

Prerequisites ... 12

Data Sync Integration ... 12

PowerShell Script Sample ____ 14

Introduction

Organizations from almost all sectors – IT, manufacturing, healthcare, and finance to name just a few – use Microsoft Active Directory services to provide centralized management of their servers, workstations and users. This application note describes the Protege GX integration with Active Directory and gives instructions for its configuration.

What is Active Directory?

Active Directory (AD) is a Microsoft Windows directory service that allows IT administrators to manage users, applications, data, and various other aspects of their organization's network. It also helps organizations maintain a central administration over all the activities carried out in their networks.

User accounts, computer accounts, groups, and all related credential information are stored in Active Directory.

Organizations primarily use AD to perform authentication and authorization. The Domain Service domain controller authenticates and authorizes all users and computers in a network, assigning and enforcing security policies for all computers.

AD is contacted before a user is granted access to a resource or service. When a user logs into a computer that is part of a Windows domain, Active Directory checks the submitted password. Once the authenticity of the user is verified, AD helps to determine whether the user is authorized to use that particular resource or service. If the user checks out on both counts, access is granted.

Active Directory and Protege GX

Protege GX's Active Directory integrations provide synchronization and authentication for Active Directory users, enabling organizations to leverage the user management and security policies that AD provides.

For our purposes, the important aspects of AD are:

1. Active Directory stores all Windows user logons, passwords and access permissions.
2. Active Directory uses those credentials to control access to computers and programs.

Because AD stores user information, we can use it as a synchronized source of users for Protege GX. And because it controls access to programs, we can use it to control operator access to Protege GX.

Key Advantages

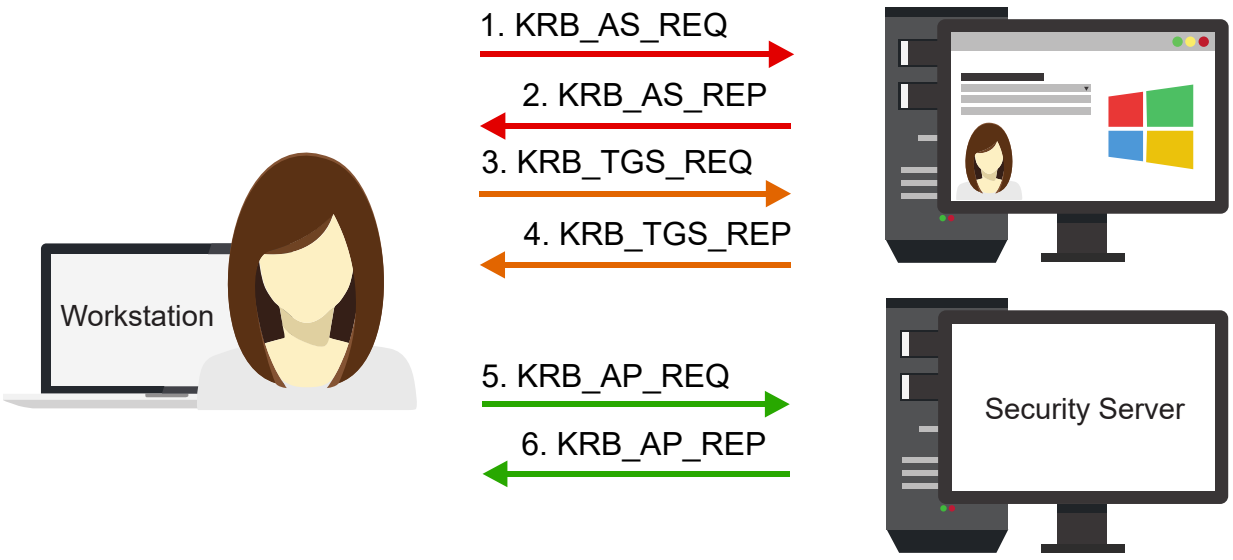
- Reduces administration and maintenance workload.
- Offers highly secure access through the usage of AD security policies.
- Provides centralized authentication while simplifying operator logon with single sign-on.
- Automatically creates and synchronizes Protege GX user accounts based on Active Directory users and groups.

Active Directory for Operator Management

Active Directory integration enables operators to log in to Protege GX automatically using their Windows credentials, providing centralized authentication and the convenience of single sign-on. Operators have one less password to remember, yet receive all the same password restrictions and security policies for that password as provided by Active Directory.

Active Directory details are configured under each operator record, and once defined the operator can select the option to use Windows Authentication. Protege GX then uses the operator's Windows network domain and user name automatically as authentication.

How it Works



When an operator attempts to log in using their Windows credential, the Kerberos network authentication service specifies six messages (five mandatory and one optional), grouped into three pairs of sub-protocols:

The Authentication Service (AS) exchange takes place at logon, and is concerned with giving clients the right to request tickets to access resources.

1. The client sends a **KRB_AS_REQ** authentication request to the KDC (Key Distribution Centre).
2. If approved, the KDC will generate a ticket granting ticket (TGT) which is returned to the client as part of the **KRB_AS_REP** authentication reply.

The Ticket Granting Service (TGS) exchange commences when the client requires access to a resource.

3. The client sends a **KRB_TGS_REQ** service ticket (ST) request to the KDC with the name of the service to which access is required.
4. The KDC will validate the authentication token within the TGT and, if permitted, return a service ticket which is valid for the requested service as part of the **KRB_TGS_REP** reply.

At this stage the client is not authenticated. The service ticket is only valid between the user and the service, but provides mutual authentication.

The Client/Server (AP) exchange is the authentication protocol, where the client presents a service ticket and an authenticator to a service to establish an authenticated communication session with the service.

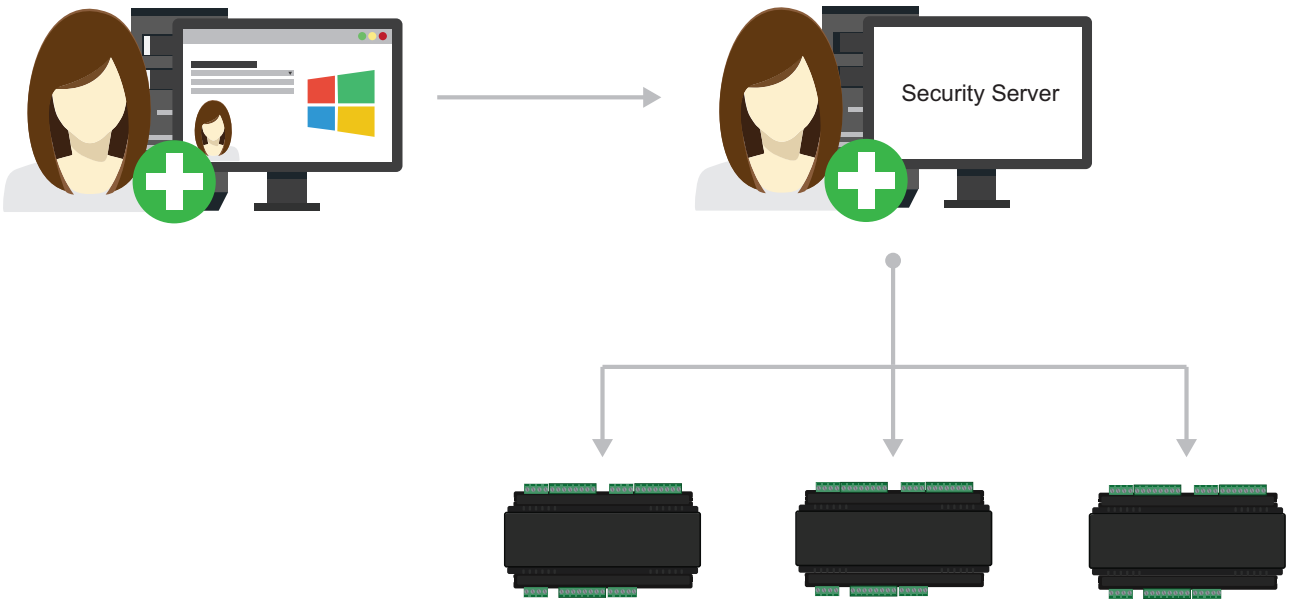
5. Only after the client has sent a **KRB_AP_REQ** request to the service server, and there is mutual authentication, will the client be authenticated and allowed access to the requested resource.
6. The service server may or may not send a **KRB_AP_REP** reply.

At all stages, only the KDC can read the TGT and only the service can read the ST.

Active Directory User Integration

Active Directory integration enables you to leverage the user data already contained in your Microsoft Windows Domain to create and maintain Protege GX users.

This integration works by obtaining a list of users based on the defined Active Directory security group, importing the user names and current AD status (active or disabled), then synchronizing them as frequently as desired.



New users are automatically added to Protege GX as they are added to Active Directory without the need for administrators to intervene.

Synchronization ensures that if there are any changes made to the Active Directory profile, then the Protege GX user record is updated, and if a user is disabled or deleted within Active Directory, their Protege GX user account is also disabled.

Data Sync Active Directory User Integration

Active Directory integration using Data Sync provides a more sophisticated level of user integration, with fully customizable access to the user data already contained in your Microsoft Windows Domain.

This feature can be used to import and update access levels, departments, car registration, even sporting teams. Any user data in Active Directory can be mapped to any field in Protege GX, existing or custom, to create and maintain Protege GX users with selected AD properties.

The integration works by running a configured ICT Data Sync Service import, with customized user data synchronized from Active Directory as often as required. User data is retrieved from AD and exported to a CSV file. The ICT Data Sync Service then reads the data in the CSV file and uses the Protege GX SOAP Service to import the records to Protege GX.

Licensing

The Active Directory Operator and User integrations are all optional licensed features that add functionality to an existing Protege GX system. Each requires a specific license, which is applied to the server.

Each integration option is licensed separately.

- PRT-GX-AD-OPR : Active Directory Operator Integration License.
- PRT-GX-AD-USR: Active Directory User Integration License.
- PRT-GX-DB-SYNC: Data Sync License for Data Sync User Integration.

Active Directory Operator Integration

The Active Directory operator integration enables the use of Active Directory security properties for operator management, allowing operators to log in automatically using their windows credentials.

Prerequisites

Active Directory operator integration is an optional licensed feature that requires a Protege GX Active Directory Operator Integration license applied to the server.

- PRT-GX-AD-OPR : Active Directory Operator Integration License.

The **Enable Windows Authentication on Data Service / Client Communications** option must be selected during installation of Protege GX to enable this feature.

If this option has not been selected during installation, Windows Authentication logons will fail, with no notifications or event viewer errors. If this is the case, Protege GX will need to be uninstalled, and reinstalled with the above option selected as the WCF TCP/IP Port, on the server and all workstations.

Programming

The main programming steps are:

- Enabling the **Use Windows Authentication** setting
- Logging In with Windows Authentication
- Configuring TLS 1.2

Enabling the Use Windows Authentication setting

1. To enable Windows Authentication for an operator, navigate to **Global | Operators**.
2. In the Configuration settings, enable **Use Windows Authentication**.
3. Click the ellipsis **[...]** beside the **Username** to search for the Active Directory users record for the operator.
4. Enter the operator's **Username** or name and click **Search**.
5. Select the **Domain** from the drop-down list if required.
6. Select the operator's user record from the list of AD Usernames displayed below, then click **OK**.
7. The operator's AD user credentials should now be displayed in the Username.
8. Once the operator's AD credentials have been verified, click **Save**.

Logging In with Windows Authentication

Once your credentials are verified and you are logged in to your computer, you can automatically log in to Protege GX with your Windows credentials, without needing an additional Protege GX logon or password.

1. Start Protege GX.
2. When the login window is displayed, select the **Use Windows Authentication** option.
3. Unless you are logging in on the Server PC, you will need to specify the Protege GX **Server** to connect to.
   When logging in within your network domain, you can simply enter the computer name or IP address of the Protege GX server. If you are connecting from outside your domain, you will need to enter a valid FQDN (Fully Qualified Domain Name).
4. Click **Log in**. You will be logged in with your Windows user credential, as long as it is valid.

Configuring TLS 1.2

Additional security configuration is necessary to use Windows Authentication when using TLS 1.2.

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.

Active Directory User Integration

The Active Directory user integration enables the import of Active Directory users into the Protege GX system based on the active directory group that has been selected.

Prerequisites

Active Directory user integration is an optional licensed feature that requires a Protege GX Active Directory User Integration license applied to the server.

- PRT-GX-AD-USR: Active Directory User Integration License.

Active Directory User Import Settings

Enabling the Active Directory user integration requires configuration of the Active Directory user import settings. This allows Protege GX to import and synchronize Active Directory user records with Protege GX users. Navigate to **Global | Sites | Active Directory**.

- **Import users from Active Directory**: Select this option to import user details from Active Directory to the Protege GX database.
- **Active Directory domain**: Defines the Windows Active Directory domain being used.
- **Windows group**: The Windows group containing the users to import.

  Only one selected Windows security group can be synchronized with this integration.
- **Synchronization period (minutes)**: Defines the frequency of synchronizing users with Active Directory.
- **Disable users if AD users are disabled**: Disables Protege GX user access if the Active Directory account is disabled.
- **Disable users if AD users are deleted**: Disables Protege GX user access if the Active Directory account is deleted.

Data Sync Active Directory User Integration

The Data Sync Active Directory user integration provides an advanced customized import and synchronization of Active Directory users into the Protege GX system, including multiple AD groups and custom user criteria.

Any field that exists in Active Directory can be mapped to any field that exists in Protege GX. Even if the field is not automatically included in Protege GX it can be added as a custom field, bringing great power to utilize AD user data.

PowerShell Script

A customized Windows PowerShell script will be required to retrieve the necessary Active Directory user data and export it to a suitably configured CSV file. This is a complex script requiring knowledge of Windows PowerShell and your network domain and security configuration.

The attached sample (see page 14) provides a basic indication of the type of process and fields required, but there is potential for far more complex and useful user criteria to be synchronized. Please consult your IT professional for assistance with this process.

The PowerShell script should always contain at least a Unique Identifier, First Name, Last Name, and a Status field to identify whether users are enabled or disabled.

Prerequisites

Data Sync Active Directory user integration is an optional licensed feature that requires a Protege GX Data Sync license applied to the server, along with specific software and licensing requirements.

Software Requirements

All software must be installed and operational.

Software	Version
Protege GX	4.2.214 or higher
Protege GX SOAP Integration Service	1.5.0.19 or higher
ICT Data Sync Service	2.0.0.0 or higher

Licensing

License	Order Code	Notes
ICT Data Sync Service License	PRT-GX-DB-SYNC	1 per server
Protege GX Client Connection License	PRT-GX-CLNT	If using a version of the ICT Data Sync Service prior to 2.0.6.3 and a version of the Protege GX SOAP Service prior to 1.5.0.27, a Protege GX client connection must be available for use by the service.

Data Sync Integration

The following steps are required to program Active Directory user synchronization using the ICT Data Sync Service.

- It is assumed the ICT Data Sync Service is installed and configured, with the appropriate license applied.
- It is assumed Protege GX SOAP Service is installed and configured, with the appropriate license applied.

- It is assumed that the customized PowerShell script has been supplied (see next page).

Programming

The main programming steps are:

- Export Active Directory users to a CSV file, using a customized Windows PowerShell script
- Import Active Directory users from the CSV file into Protege GX, using the data sync service

Export Active Directory Users to a CSV File

1. Right click the Windows PowerShell script file and **Run with PowerShell**.
   This process may take seconds or minutes, depending on the file size.
2. Locate the CSV file created by the above process. It is recommended to check the file to ensure that the export has completed as expected and the data is correct before continuing.

Import Active Directory Users from the CSV file into Protege GX

1. Open the **Data Sync Service Configuration Tool**.
2. Select the **Target System**. This would typically be Protege GX but will depend on your system configuration.
3. Enter the **SOAP Server Address**. This is the server where your Protege GX SOAP Service is installed.
4. Enter the **Username** and **Password** for this Data Sync synchronization.

   A unique **Operator** should be created specifically for this process to enable targeted event reporting.
5. Select the **Site** to synchronize.
6. Under **Data Mapping** select the **Record to Sync**. This is the Protege GX database table that you want to map and import AD user records into. This would typically be the Users table but it is possible to create more customized integrations.
7. Specify the **Data Source** to be imported by selecting the **File Directory** (folder location) and **Import File**.
8. The **Start Import At Row** setting will usually need to be changed to **Row 2**, as Row 1 typically contains the file headers and is not user data to be imported.
9. In the mapping window below, map each **Source Column** from the AD users CSV file to the appropriate **Target Field** in the Protege GX **Record to Sync**.

   The unique identifier must be mapped to a **Unique Field**. This would generally be a custom field (CustomField1 is recommended).
10. Any fields that contain true or false values, such as a Disabled User field, will typically be exported to the CSV file in ALL CAPS. These must be converted to lower case.
    - Click the **Advanced** button in the row of the required Target Field.
    - In the **Conversion** table, enter the Original Value of TRUE, with a Resulting Value of true.
    - In the second row, enter the Original Value of FALSE, with a Resulting Value of false.
    - Click **OK** to save.
11. **Save** the configuration.
12. Then **Start** the data sync import.
13. Under **Sync Options** set the **Resynchronize Every** setting to the required number of minutes or hours for the synchronize process to run and update user records.
14. Click **Save** to update the configuration

Imported results and user details can be viewed in Protege GX under **Users | Users**.

PowerShell Script Sample

```
Import-Module ActiveDirectory
# CSV path for exported users
$CSVpath = "C:\DataSync\ADusers.csv"

$users = Get-ADGroup -Server "svr1.yourdomain.local" -Filter * -SearchBase
"OU=Building Security,OU=Security Groups,OU=Users,DC=Domain Users" | Get-
ADGroupMember | Sort | Get-Unique | Get-ADUser

$myData = $users | Select-Object -Property @{Name="UniqueID";Expression={ -
join ($_.ObjectGUID.ToByteArray() | foreach { $ofs="" } { "{0:X2}" -f $_})}},
@{Name="FirstName";Expression={$_.GivenName}},
@{Name="LastName";Expression={$_.Surname}},
@{Name="FullName";Expression={$_.name}},
@{Name="DisableUser";Expression={ !($_.Enabled)}}

$myData | Export-csv -path $CSVpath -notype

$a = "<SOF>"
$b = Get-Content "C:\DataSync\ADusers.csv" | Where { $_ -notmatch "UniqueID" }
$b = $b  -replace ";\s", ";"
$c = "<EOF>"

Set-Content "C:\DataSync\ADResults.csv" $a, $b, $c
Move-Item "C:\DataSync\ADResults.csv" "C:\DataSync\Output\ADResults.csv" -
force
```

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