Windchill Active Directory Integration: Quick Start Guide

Plan

In the planning phase we will need to gather all the required information so we don't need to look for it while we are actually setting up the connection to Active Directory.

The first thing you will need is an Active Directory service account. This account will be used by Windchill to get user and group information from AD. I will try to supply sample information to help you understand the syntax however you should use the text file hand out for any copy and paste operations as the text file will not change formatting like Word.

Gather the following user information:

- User Name: "WindchillADServiceAccount"
- Password: "IWillNeverLetYouKnow"
- Distinguished Name: CN=WindchillADServiceAccount,OU=ServiceAccounts,DC=net,DC=Company,DC=COM

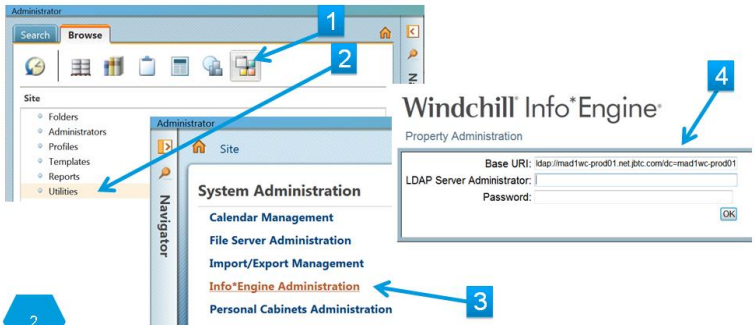
You will also need the following information:

- Administrator Login for the Windchill Directory Server
- Fully Qualified Domain Name (FQDN:) Active Directory Server
- Provider URL & Port "ldap://host:3268" Port may also be "389"
- Search Base In Active Directory
- Search Scope (Base | One Level | Subtree)

Here are the mapping parameters I recommend starting with:

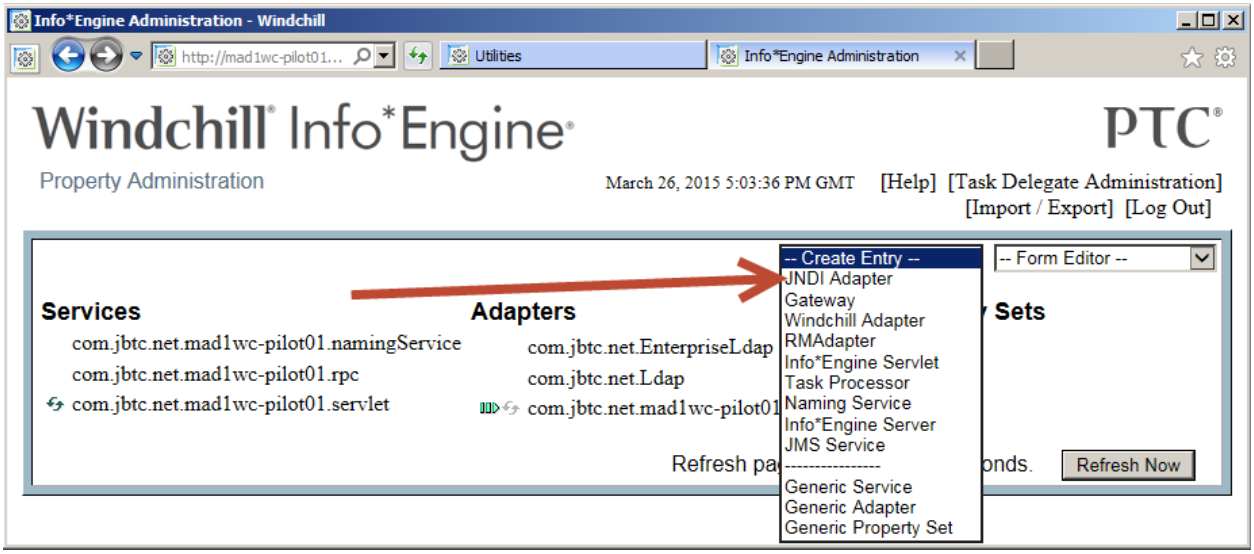
```
com.jbtc.net.ADLDAP.windchill.mapping.user.objectClass=user
com.jbtc.net.ADLDAP.windchill.mapping.user.uid=sAMAccountName
com.jbtc.net.ADLDAP.windchill.mapping.user.uniqueIdAttribute=sAMAccountName
com.jbtc.net.ADLDAP.windchill.mapping.user.member=memberOf
com.jbtc.net.ADLDAP.windchill.mapping.group.cn=cn
com.jbtc.net.ADLDAP.windchill.mapping.group.objectClass=group
com.jbtc.net.ADLDAP.windchill.mapping.group.uniqueIdAttribute=sAMAccountName
com.jbtc.net.ADLDAP.windchill.mapping.group.uniqueMember=member
com.jbtc.net.ADLDAP.windchill.config.directoryType=ADS
com.jbtc.net.ADLDAP.windchill.mapping.usersOrganizationName=JBT
```

Configure Adapter



Open Windchill click on Site > Utilities > Info*Engine Administration > Log in with Windchill Directory Server Admin Credentials.

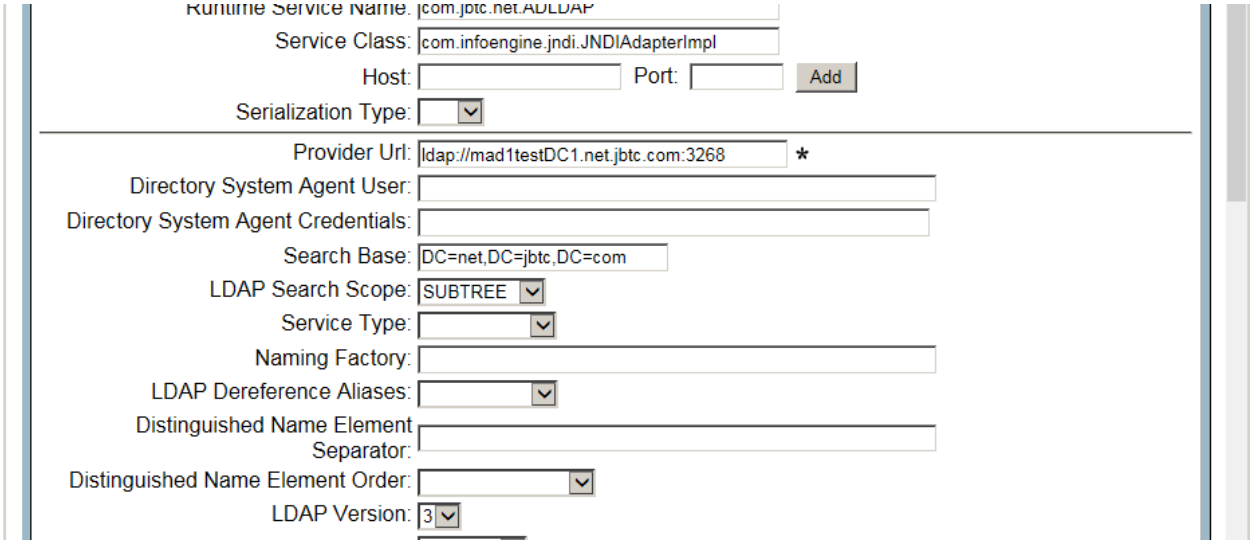
From the Create Entry dropdown select JNDI Adapter:



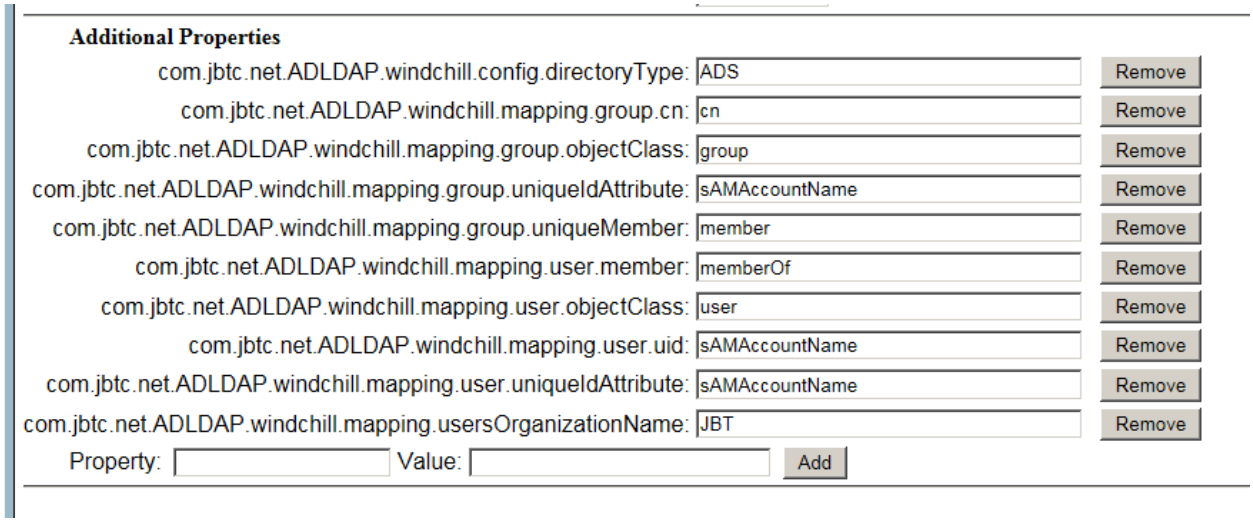
Enter the Service name. Recommended value is FQDN: of Windchill Server and an adapter name. The reason for this is to ensure unique adapter names.

Make sure the Runtime Service Name is the same as the service name.

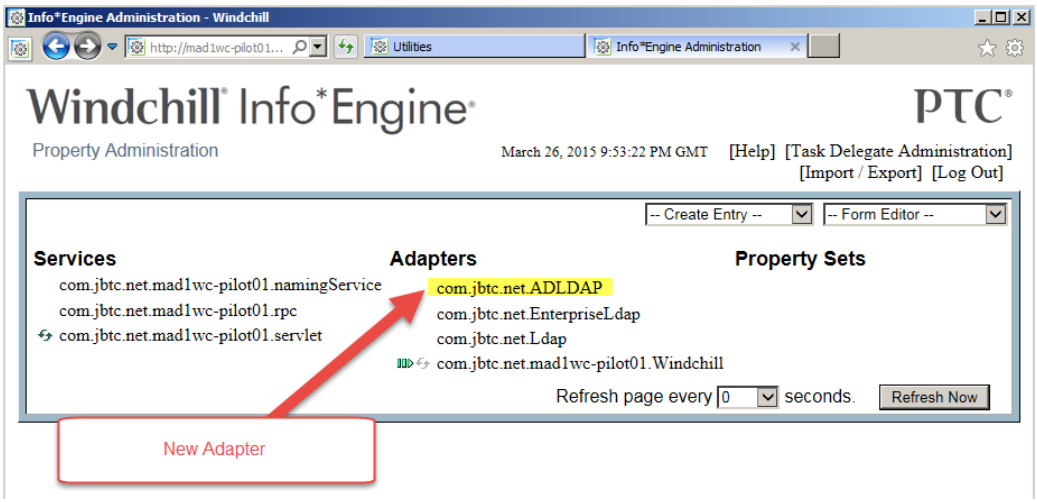
- Enter the Provider URL
- Search base
- Set LDAP Search Scope
- Set LDAP Version to 3



Enter the additional properties listed in the first section. I would start with these properties make sure the adapter works and then add additional properties if desired. This will reduce the amount of troubleshooting required to resolve LDAP issues.

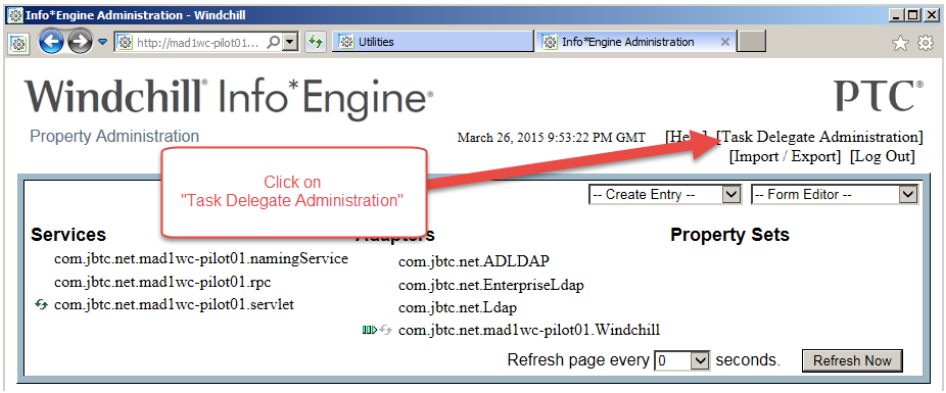


Commit changes. The new adapter should now be listed with the other adapters:

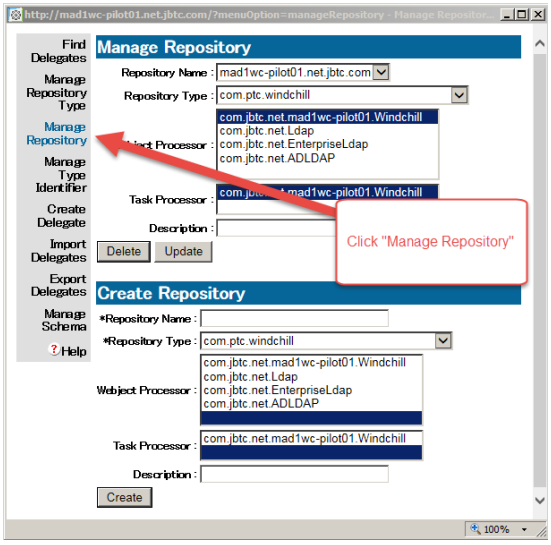


Create Repository

From the Windchill Info*Engine page click on Task Delegate Administration:



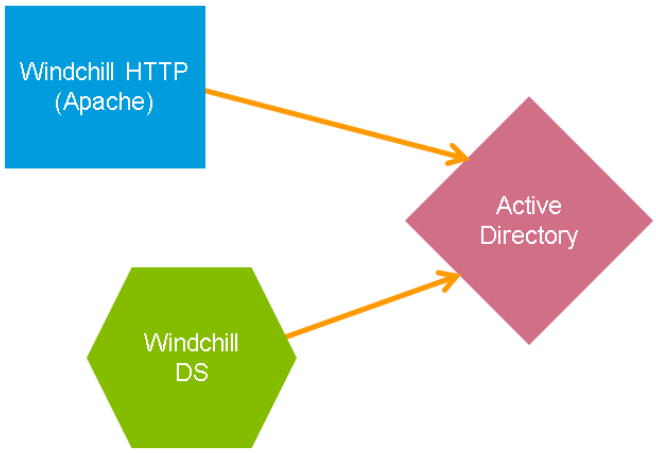
Click Manage Repository from the popup Window:



The repository name is the reverse of the adapter name created in the last section.

The Repository type is com.ptc.windchill weject processer is the one ending in Windchill and the same is used for task processor. You can also add a description. Click the create button. You now have an adapter and a repository.

Map Credentials



Windchill and apache will need the credentials for the Active Directory Bind account in order to search active directory and authenticate users. To map credentials we need to open a Windchill Shell and run an xconfmanager command:

The xconfmanager command is: -mapcredentials.admin.adapters

The Parameters are:

- Service Name
- Bind User DN
- Password

Example command:

Xconfmanager -mapcredentials.admin.adapters -com.jbtc.net.ADLDAP CN=UserName,OU=OU,DC=COM -“NeverInAMillionYears”

We need to configure Windchill to use the adapter. So let’s get a list of current adapters:

Xconfmanager –d wt.federation.org.directoryServices

The results will include something like this:

$(wt.federation.org.defaultAdapter),$(wt.federation.org.enterpriseAdapter)

Append the new adapter to this list:

$(wt.federation.org.defaultAdapter),$(wt.federation.org.enterpriseAdapter),com.jbtc.net.ADLDAP

Then run this command (all one line):

xconfmanager -p -s "wt.federation.org.directoryServices=$(wt.federation.org.defaultAdapter),$(wt.federation.org.enterpriseAdapter) , com.jbtc.net.ADLDAP"

Configure Apache / HTTP Server

Option 1:

Navigate to the Apache/HTTP server folder and run the required ant command:

Here is the structure of the command:

ant -f webAppConfig.xml addAuthProvider -DproviderName=<NAME> "-DldapUrl=ldap://<LDAP Host>:<LDAP Port>/<SearchBase>" "-DbindDn=<Bind User DN>" "-DbindPwd=<Password>"

Here is an example command with values filled in:

ant -f webAppConfig.xml addAuthProvider -DproviderName=ADLDAP "-DldapUrl=ldap://mad1testDC1.net.jbtc.com:3268/DC=net,DC=JBTC,DC=COM" "-DbindDn=CN=WindchillLDAPUser,OU=Service Accounts,OU=Users,OU=Madera,OU=FPSD,DC=net,DC=jbtc,DC=com" "-DbindPwd=ImNotTelling“

<Name> is a unique name for this adapter : CorpLdap

<LDAP Host> is the hostname of the LDAP server

<LDAP Port> is the port used by LDAP (optional)

<SearchBase> is the search base. Should match the base set in the JNDI Adapter, eg, ou=users,dc=mydomain,dc=com

<Bind User DN> is the full DN of the user that will connect to LDAP to perform the searches. Should match the DN used in step 3

<Password>Is the password for the AD bind user account.

Option 2: (You only need option 1 OR option 2 NOT BOTH)

EDIT A TEXT FILE:

1. Edit Apache\conf\extra\app-Windchill-AuthProvider.xml

2. Add an additional provider section in the form,

```
<provider>
 <name>Windchill-<adaptername></name>
 <ldapUrl>ldap://<ldaphostname>:<ldapport>/<searchbase></ldapUrl>
 <bindDn><Bind User DN></bindDn>
 <bindPwd><Password></bindPwd>
</provider>
```

Where

<adaptername> is a unique name for the adapter, e.g. CorpLdap

<ldaphostname> is the hostname of the LDAP server which should match the LDAP hostname in step 1

:<ldapport> is an optional port number if the LDAP server is not using port 389

<searchbase> is the search base for the LDAP server which should match the search base in step 1

<Bind User DN> is the user DN used to connect to LDAP which should match the DN used in step 3

<Password> is the password for this user which should match the password used in step 3

For example,

```
<provider>
<name>Windchill-CorpLdap</name>
<ldapUrl>ldap://corpldap.mydomain.com/ou=users,dc=mydomain,dc=com</ldapUrl>
<bindDn>cn=WCAccess,ou=users,dc=mydomain,dc=com</bindDn>
<bindPwd>manager</bindPwd>
</provider>
```

3. From a Windchill shell in the Apache directory run

```
ant -f webAppConfig.xml regenWebAppConf
```

Testing

Open Windchill go to participate administration and try to search for an AD user.

Additional Resources – Great Resources From PTC Support:

- CS29445, CS29454 – Overview of Full Process
- CS24211 – Filter LDAP Users
- CS37358 – Filter on 'Disabled' flag in AD
- RFC 2254 – LDAP Filter Syntax Examples
- CS60955 – Windchill Last Name, First Name
- CS158333 – Failover Protection for LDAP

Additional Considerations

Active Directory Groups

One of the things you will need to decide is how you want to manage groups in Active Directory. You can pull your groups from active directory or you can simply create groups in Windchill and assign users to those groups. There are tradeoffs and it will depend on how your business operates.

For example if Active Directory groups our maintained by your IT department and you have no control over who is added to those groups you may want to create your own groups in Windchill and not us AD groups so you can maintain control of what users are given access to Windchill. However if your IT Department allows you to create your own groups and control who is placed in those groups new users can automatically have access to Windchill without your intervention.

Bind Account

Another point to think about is where the AD Bind account is located and who has access to unlock the account. In some organizations first tear support may not have access to unlock service accounts this can result in downtime if the account becomes locked.

Port Number

The standard port number for Active Directory is 389. However you can use the alternate port 3268 but, check with your IT department to make sure that all the parameters you need are available when using that port number. CS29445, CS29454 have more information on this.