

Tutorial #3 - Merging Active Directory Trees

1 Overview

A common problem faced by users of Active Directory arises when users are stored within the Directory in separate organisational units, and a client application is only able to search a single tree for user data. For instance your Active Directory may be split up into the organisational units: Sales, Marketing, Accounts and Support. Users within each department are stored within their respective organisational units. Unfortunately, many applications will only use a single tree to perform a search for user data. If an application is authenticating against data stored in Active Directory, you may find that the application can only authenticate users from one department, as it is unable to recursively search through all of the other trees.

Symblabs LDAP Proxy is able to overcome this problem easily, using the Merge Trees plugin. Using the LDAP Proxy, you are able to merge all of the trees on the fly, so that a client application can be configured to search a virtual tree that includes all of the users from each organisational unit.

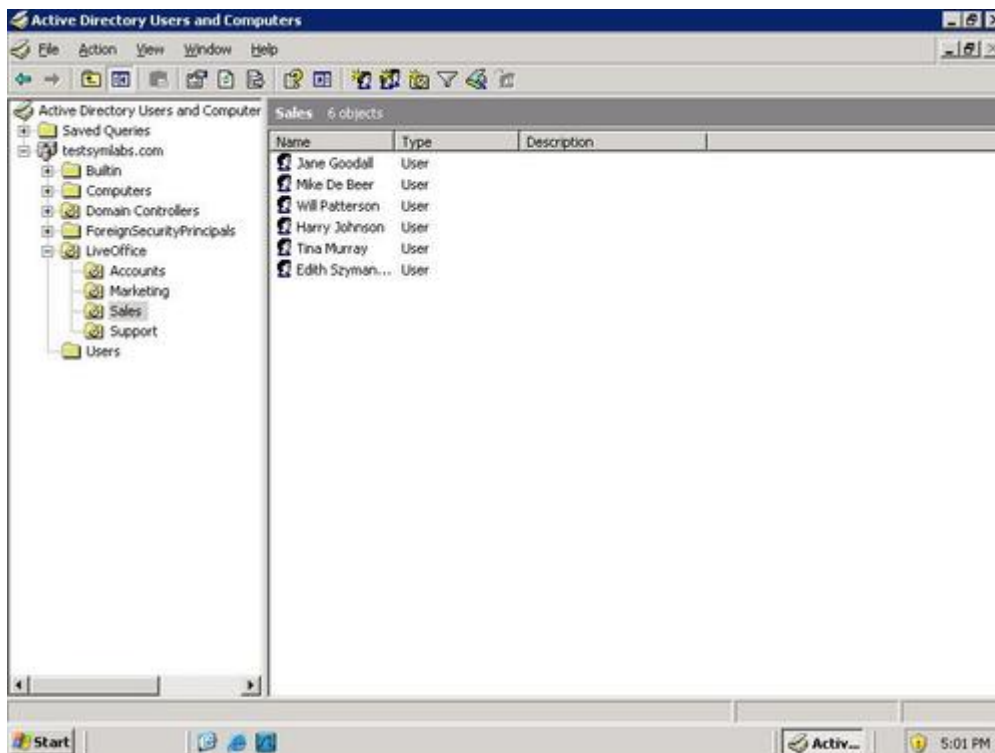


Fig-1: Active Directory can group users in different Organizational Units

2 Assumptions

LDAP Proxy is installed and configured properly; LDAP Proxy is currently running.

Active Directory is installed and is currently running and accessible to LDAP Proxy.

Active Directory is configured in such a way that there are a number of different organisational units and that each unit has been populated with differing user data.

Port 3890 is available on the computer in which LDAP Proxy is installed.

3 Create a New Configuration

Click File on the menu bar, then click New.

Click the OK button when asked which server you want to create the new configuration in (the default server is Local).

Enter MergeTreesTutorial for the filename when prompted, then click the Save button.

3.1 Server Group Configuration

Server Groups are the directories where your user information is stored. For this tutorial we will be creating one Server Group that contains a single directory pointing to your Active Directory server.

Click on the Output button on the left-hand side of the application to begin to configure a servergroup.

Click on the New Server Group button near the bottom of the screen.

Enter ActiveDirectory for your new Server Group and leave the Server Group Type as Automatic and then click the Okay button.

Click on the ActiveDirectory button on the left-hand side of the screen.

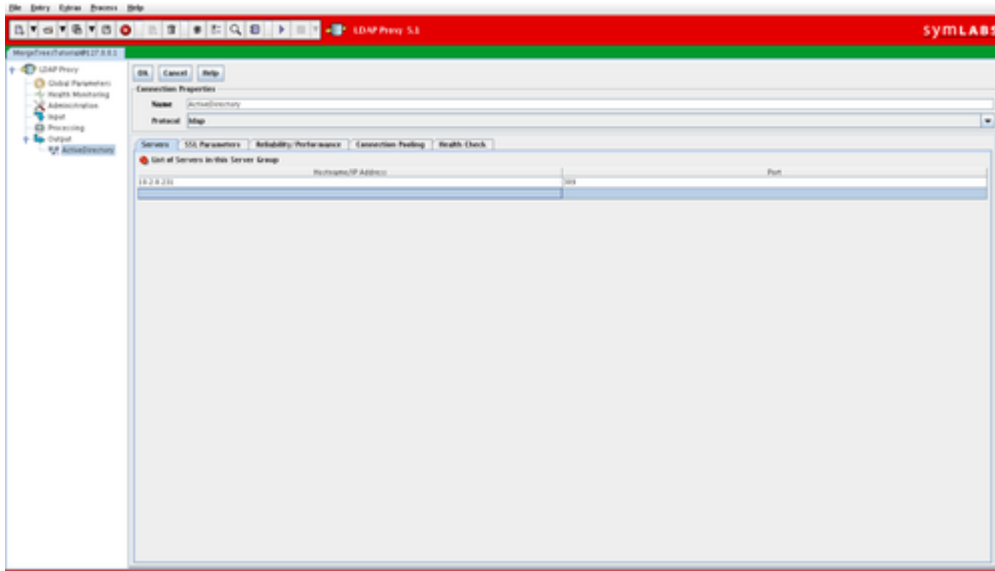


Fig-2: Configure a Server Group for your Active Directory server

Under the Servers tab, enter the Hostname / IP Address and the Port of your Active Directory server.

Click OK to save the change.

3.2 Listener Configuration

Click on the Input button on the left-hand side of the application.

Click on the New Listener button near the bottom of the screen.

Enter ActiveListener for the new input / listener and then click the OK button.

Click on the ActiveListener button on the left-hand side of the screen to begin configuring the listener.

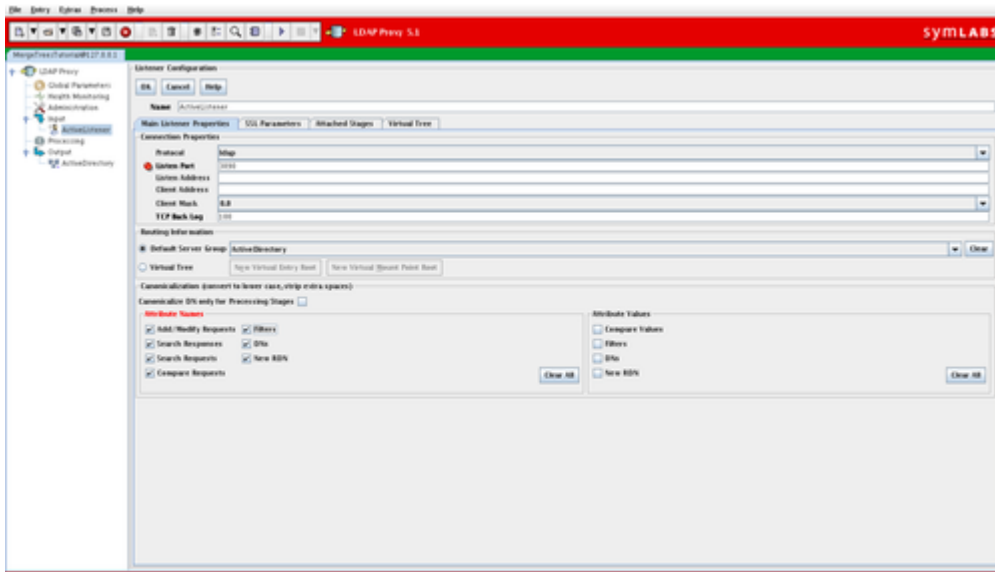


Fig-3: Configure a Listener for LDAP Proxy

Under the Main Listener Properties tab, make sure the Protocol is set to ldap.

Under the Main Listener Properties tab, set the port to 3890.

Under the Main Listener Properties tab, select ActiveDirectory from the dropdown box to the right of Default Server Group.

Due to the varied way in which various browsers and servers present attribute information, it is good practice to make use of Canonicalization on Attribute Names to avoid incompatibilities down the line. Check all of the boxes in the Attribute Names window area.

Click the OK button near the top of the screen to save the Listener configuration.

4 Add Processing Stages

In this tutorial, we will also make use of the Add Entries plugin so that our merged trees are visible to browsers searching higher up in the tree, as the Merge Trees plugin will only come into action when the virtual tree that we create is requested. As a result, it will make sense to create two separate Processing Stages to hold these plugins.

Click on Processing in the Navigator on the left.

Click on the New Stage button, and name the stage addEntry.

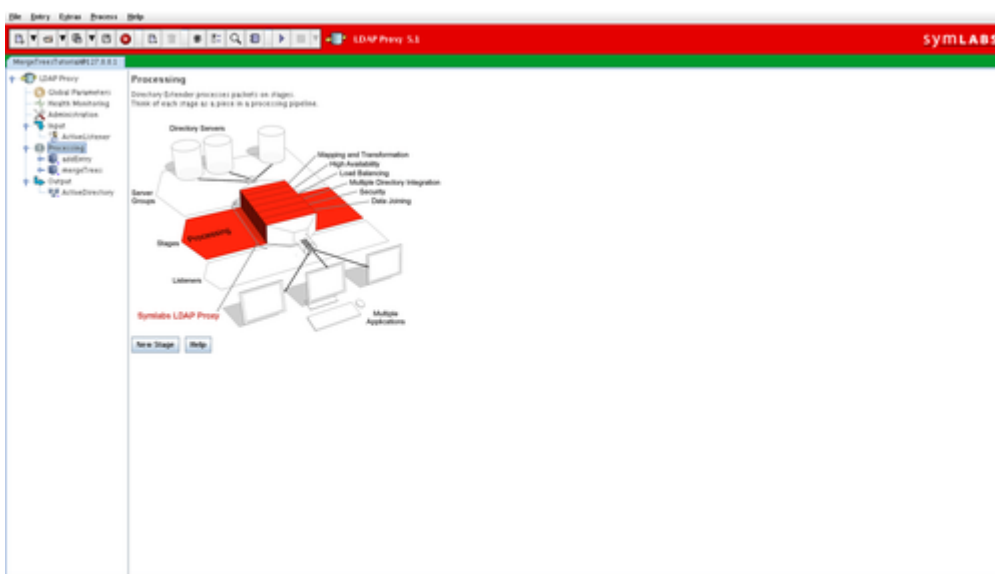


Fig-4: Add a Processing Stage for each plugin that you use

Click on the addEntry node that has been created in the Navigator tree, and click on the Add Plugin button.

A pop-up dialog will appear. Scroll through the list of plugins and select the Add Entries plugin. Click OK.

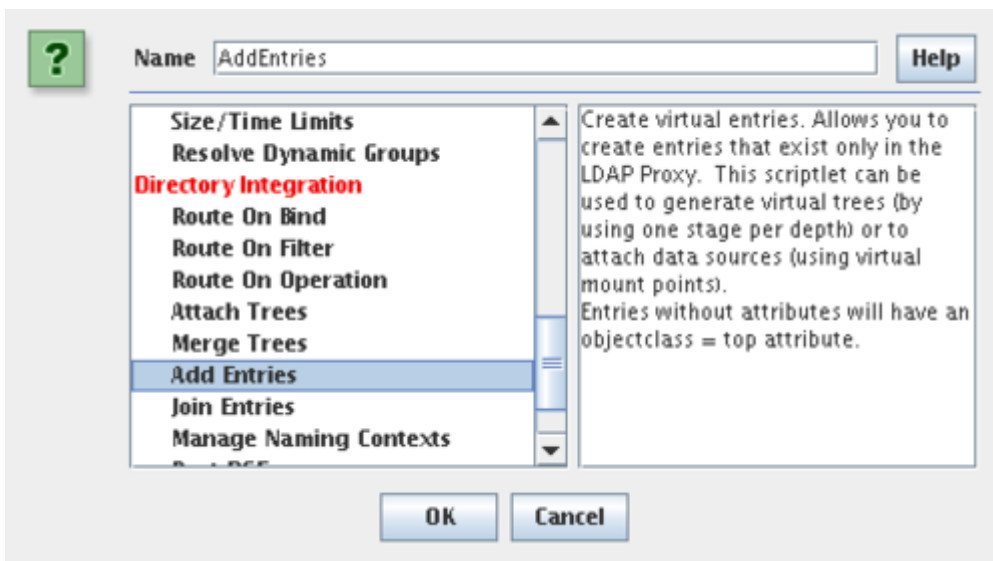


Fig-5: Attach the Add Entries plugin to the stage
Click on the Add Entries plugin listed in the Navigator Tree.

Click on the New Virtual Entry button and name the new entry "allusers".

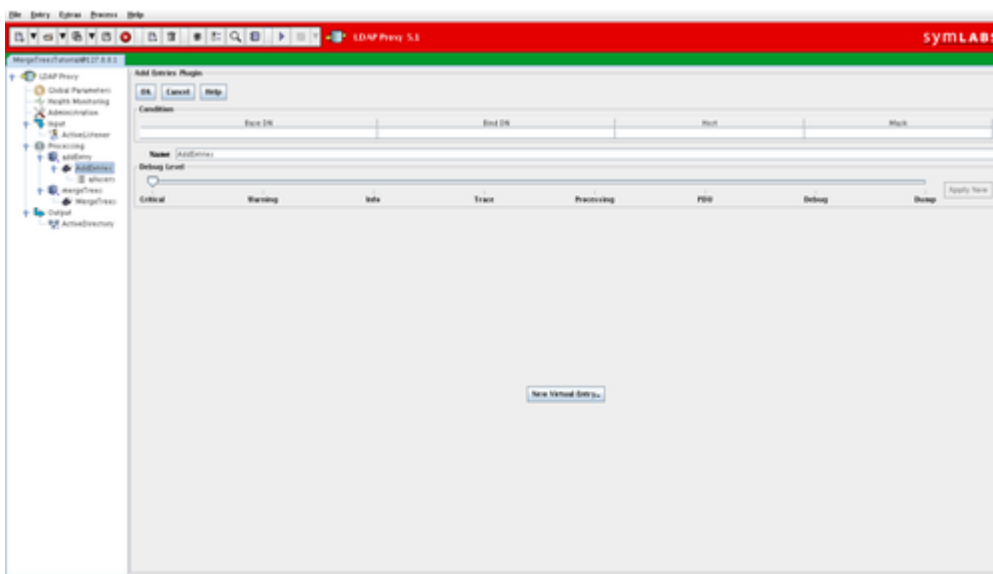


Fig-6: Click on the Add Entries plugin to create a New Virtual Entry
Click on the "allusers" node in the Navigator tree.

In the Entry Dn field, provide the DN that you wish to use to refer to the virtual tree. In our example, we will use ou=allusers,ou=LiveOffice,dc=testsymlabs,dc=com. In order to keep our configuration consistent, and because we are using canonicalization, note that all of the Attribute Names in the DN are entered in lower case.

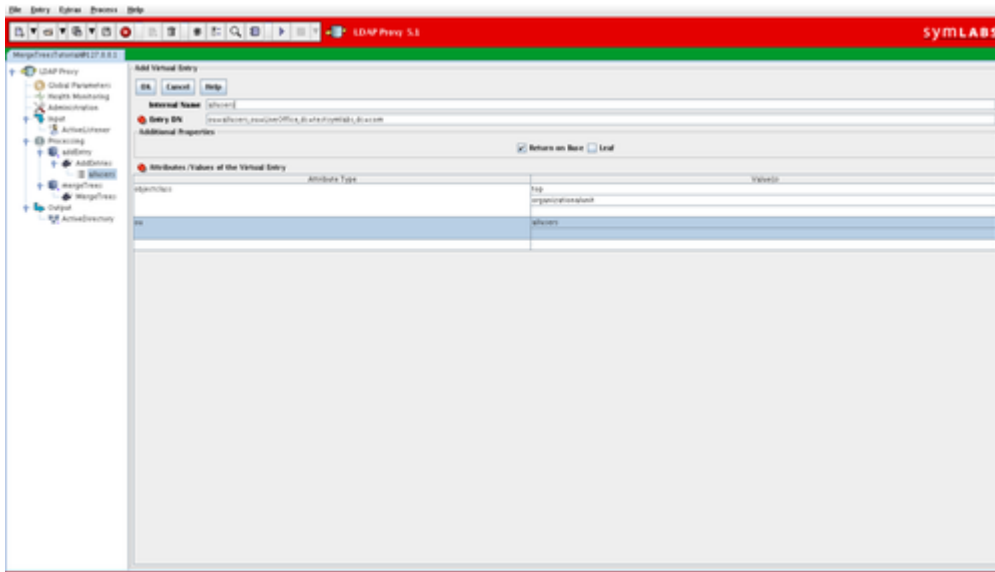


Fig-7: Configure the allusers entry for the virtual tree

You will now need to provide some attributes for the virtual DN that you are creating. In the Attribute Type column of the table, create an attribute type called "objectclass". In the Attribute Values column, enter a value of "top" and a second value of "organizationalunit".

Create a second Attribute type called "ou" and assign it the value "allusers".

Click on the Processing node in the Navigator panel again, and then on the New Stage button. Name the new stage MergeTrees, as this stage will contain the Merge Trees plugin.

Click on the Add Plugins button and scroll through the list of plugins until you can select the Merge Trees plugin. Click OK.

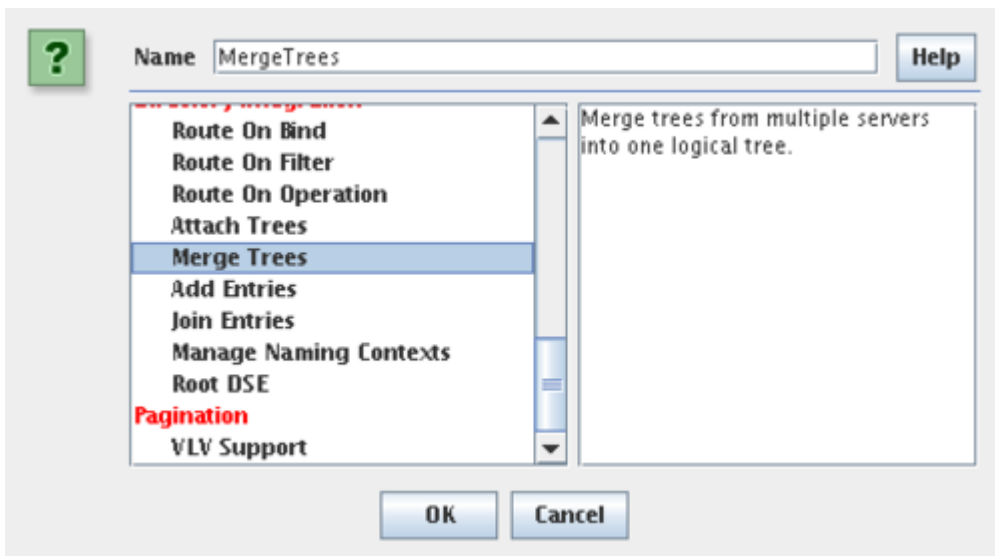


Fig-8: Add the Merge Trees Plugin to the new Processing Stage

Click on the Merge Trees plugin node in the Navigator panel.

In the Condition section of the panel on the right, add a rule to only process if the Base DN matches our virtual tree DN. So in our example, we will enter ou=allusers,ou=LiveOffice,dc=testsymlabs,dc=com. Once again, note that all of the Attribute Names that make up the DN are specified in lowercase in order to take advantage of canonicalization.

In the Joined Tree DN field, enter the DN for the virtual tree that you intend to create. Once again, in our example, we will enter ou=allusers,ou=LiveOffice,dc=testsymlabs,dc=com. And again we have specified all Attribute Names in lower case.

Finally, in the table, enter the DNs for each of the trees that you wish to merge. So, for our example, we will add the following entries:

ou=Accounts,ou=LiveOffice,dc=testsymblabs,dc=com
ou=Sales,ou=LiveOffice,dc=testsymblabs,dc=com
ou=Marketing,ou=LiveOffice,dc=testsymblabs,dc=com
ou=Support,ou=LiveOffice,dc=testsymblabs,dc=com
And for each of these entries we will use the Server Group, VirtualDirectory which we created earlier.

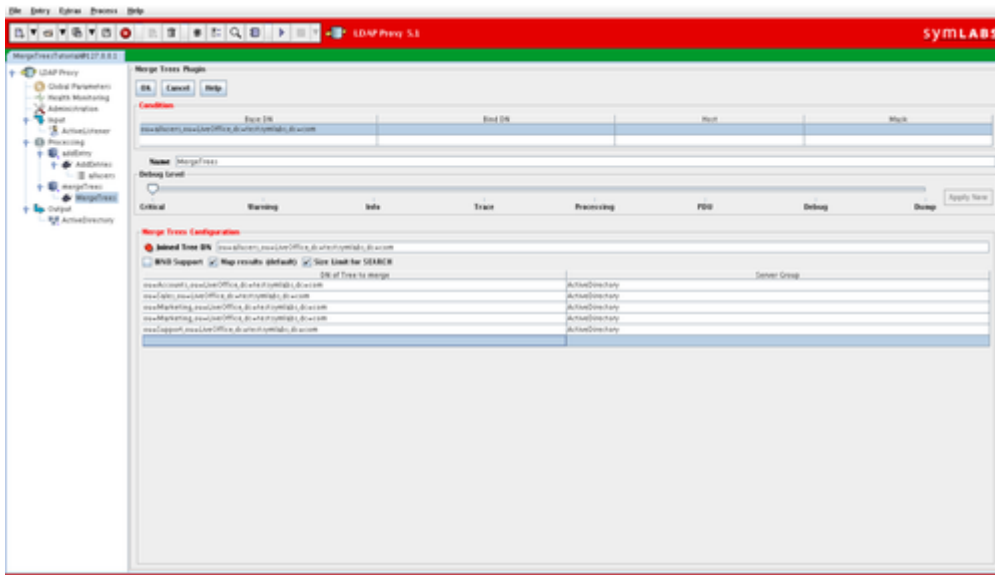


Fig-9: Configure the Merge Trees Plugin
Click OK to save this part of the configuration.

5 Attach the Processing Stages to the Listener

Now go back to the Listener node in the Navigator panel, and click on the ActiveListener that we created earlier.

Click on the Attached Stages tab.

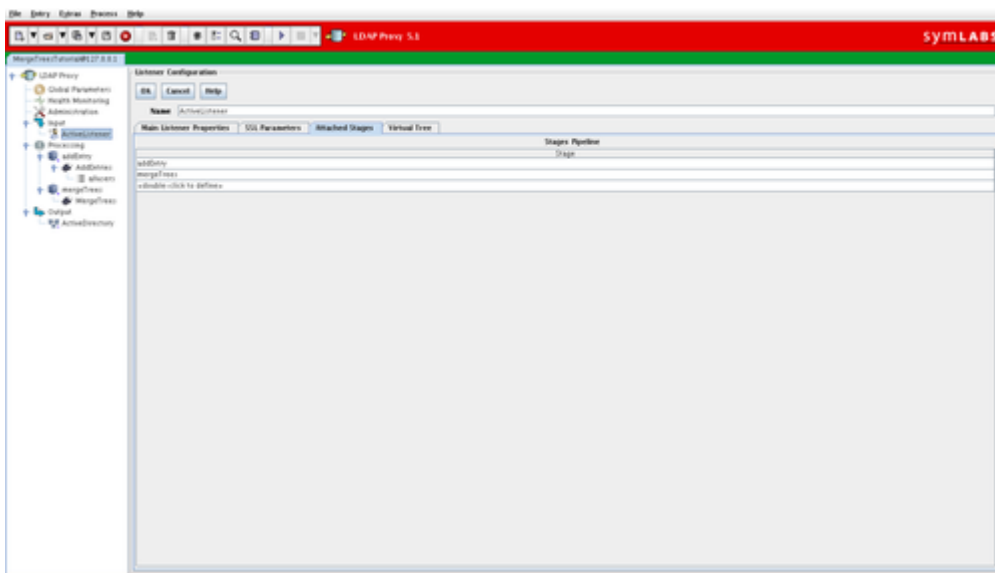


Fig-10: Attach the Processing Stages to the Listener
In the Stages list, double click on the first line and select the AddEntry stage.
A new line will appear, double click on it and select the MergeTrees stage.
Click OK to save this change.
Finally click on the Save button in the toolbar, or choose the option to Save Config from the File menu.

6 Testing the configuration.

All rights reserved. Copyright © 2008 Symblabs, Inc.

You should now have completed configuring an instance of LDAP Proxy that will be able to merge different trees within Active Directory to present them as a single virtual tree. To test the new configuration, we will start the LDAP Proxy instance and then connect to it using an LDAP browser. Using the browser, we will be able to see the RDN `ou=allusers` listed, because the Add Entries plugin will make this available to the browser. When we actually browse this portion of the tree, all of the users that are listed in the other trees will be listed as users within the `ou=allusers` RDN, because the Merge Trees plugin will make this information available on the fly. Once you are certain that everything is working as expected, you will be able to configure your application to query this virtual tree to access the details of users in all of the DNs that you have configured to be merged by the Merge Trees plugin.

Click on the Start button in the toolbar, to launch an instance of LDAP Proxy using the current configuration.

Once the configuration is running, click on the LDAP Browser icon in the toolbar to launch the LDAP Browser. You could test this using another LDAP Browser if you have a preference, but the built-in browser will let you quickly determine whether your configuration is working as expected.

In the dialog that opens up, enter the relevant details to access the instance of LDAP Proxy that you have just configured. So, in our example, we will enter:

Hostname: localhost
Port: 3890
Root Suffix: DC=testsymlabs,DC=com
Bind DN: CN=Administrator,CN=Users,DC=testsymlabs,DC=com
Password: secret

Select a server from the list, or enter a new one below

mergetreestut

Name: mergetreestut

Hostname: localhost

Port: 3890

Root Suffix: dc=testsymlabs,dc=com

Bind DN: CN=Administrator,CN=Users,DC=testsymlabs,DC=com

Password: ***** Show Password

Suffixes... Test...

OK Cancel Help

Fig-11: Enter the details to connect to LDAP Proxy into the LDAP Browser

Click the Test Connection button.

If the test connection was successful, click OK.

Use the browser to navigate your way through the tree until you have opened the DN that should contain your virtual tree. In our example, this would be: `ou=LiveOffice,dc=testsymlabs,dc=com`. You should now see the virtual tree listed in the browser. This is available to browse because the Add Entries plugin has inserted the DN into the tree.

Expand the virtual tree (`ou=allusers,ou=LiveOffice,dc=testsymlabs,dc=com`) and you will now see all of the users listed from the original DNs that have been merged.

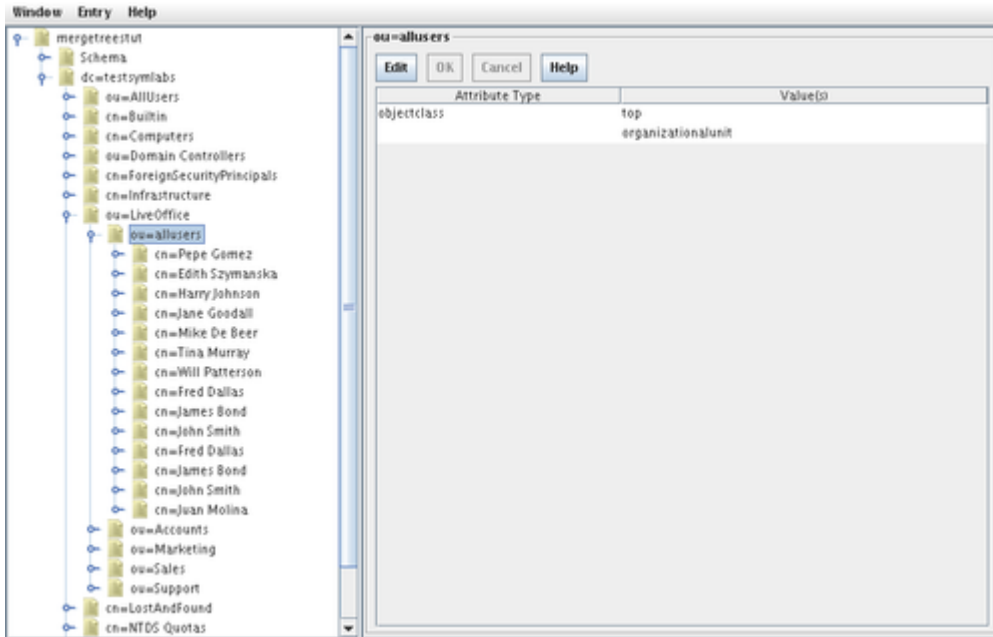


Fig-12: The allusers DN should now show all of the users from the merged DNs
 You can now confidently configure your application to search this new virtual tree in the LDAP Proxy to find all users.

"