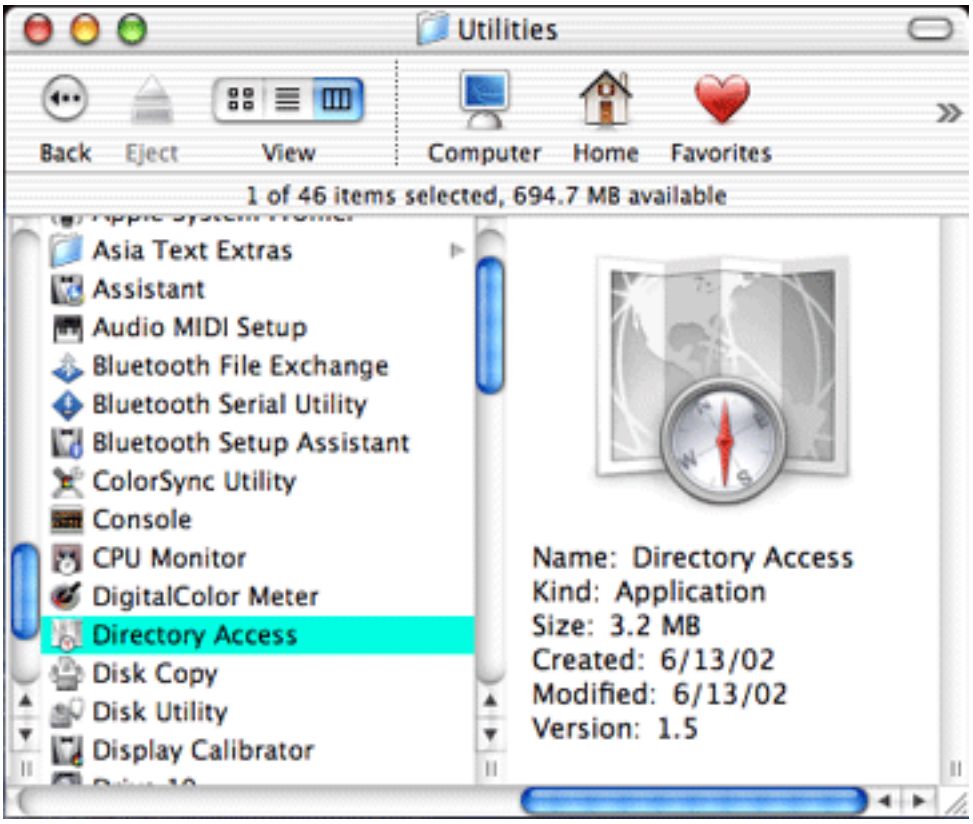
Enabling LDAPv3 for OS X 10.2 at the University of Michigan

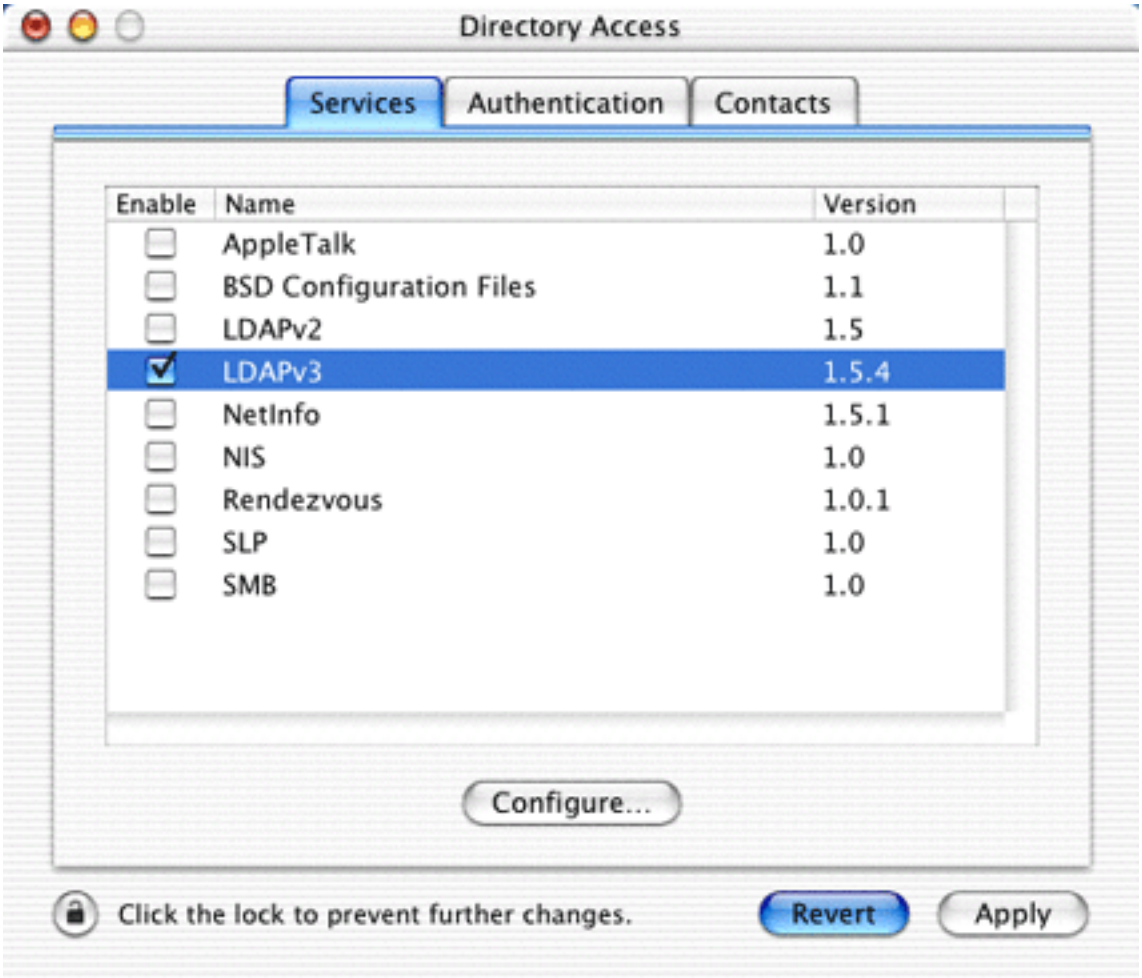
PDF version of this page

1. Log in to the computer using an account with administrative privileges.

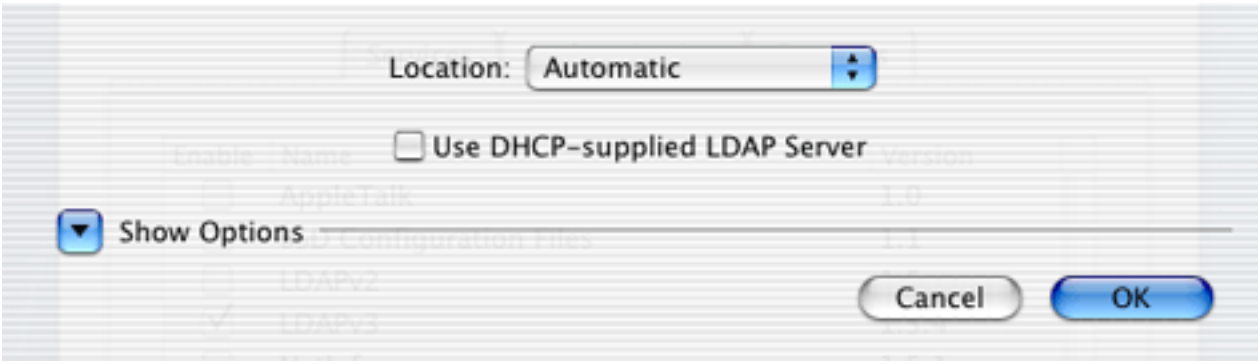
2. Open the **Directory Access** utility from the **Utilities** folder inside the **Applications** folder. You'll need to authenticate by clicking on the lock icon.



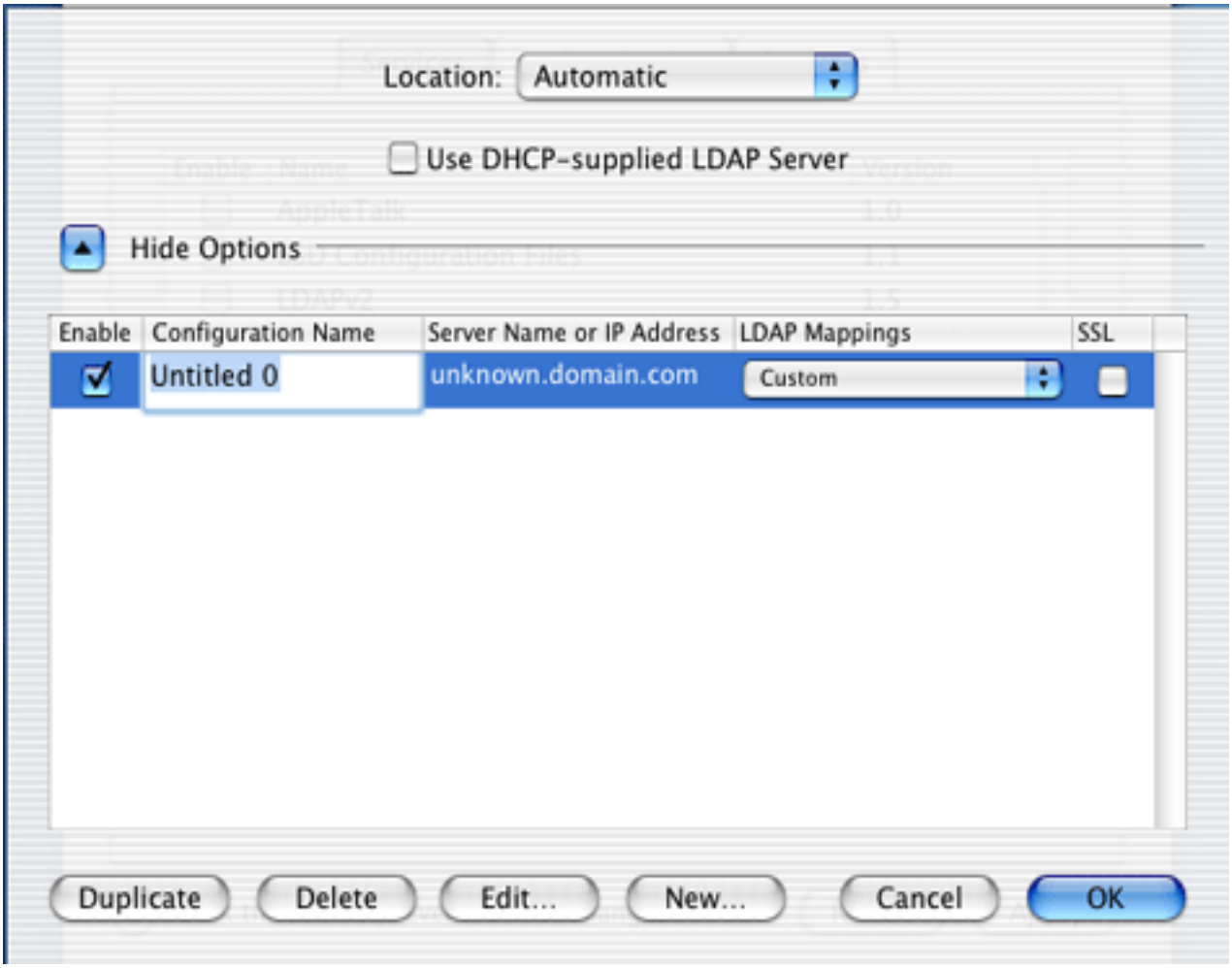
3. **LDAPv3** should already be enabled; if not, check the checkbox. It 's pretty likely that you won't need any of the other services selected, so deselect them now. Select the **LDAPv3** line and click the **Configure...** button.



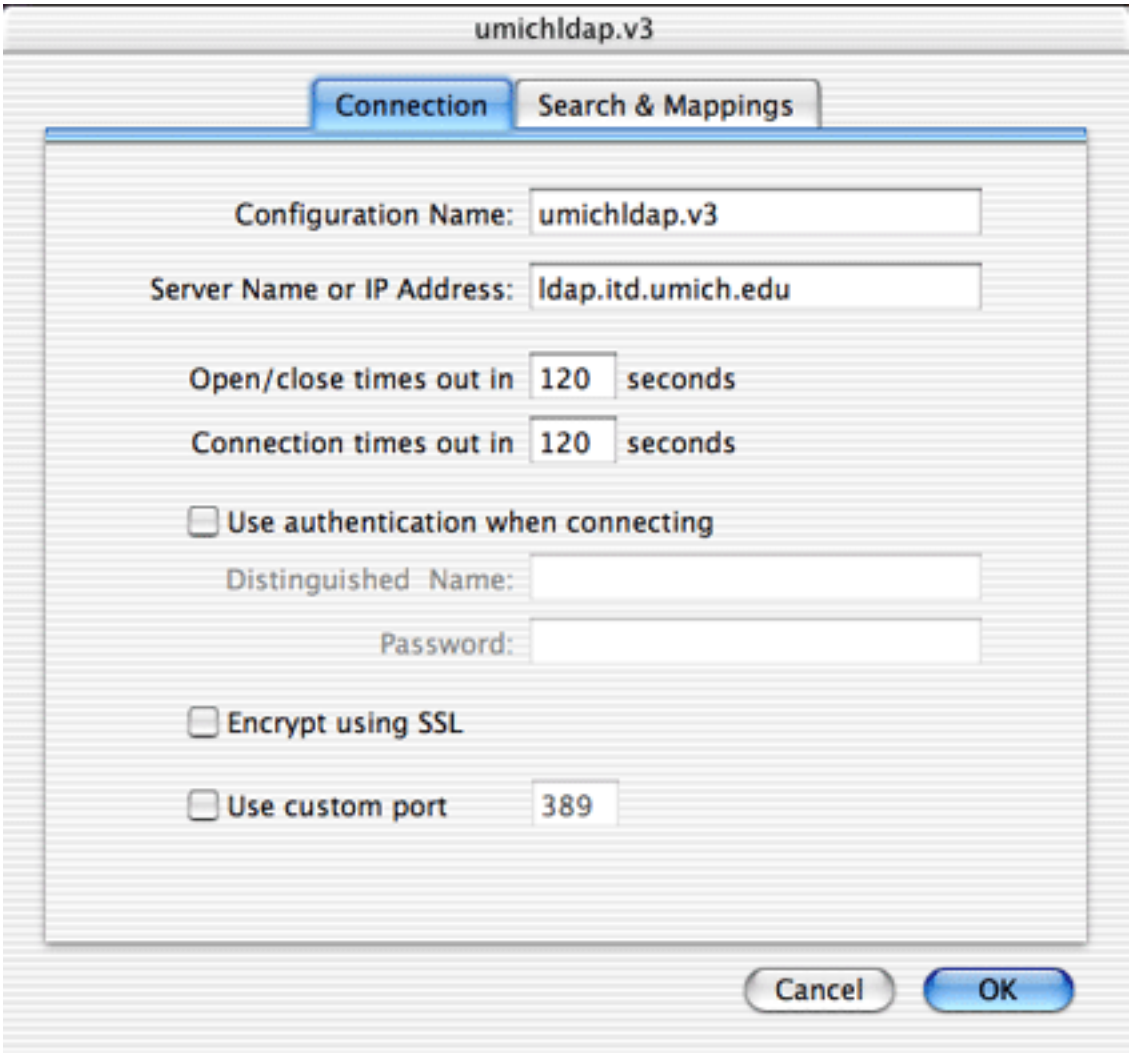
4. Select the location you want to configure, deselect **Use DHCP-supplied LDAP Server**, and click on the **Show Options** button.

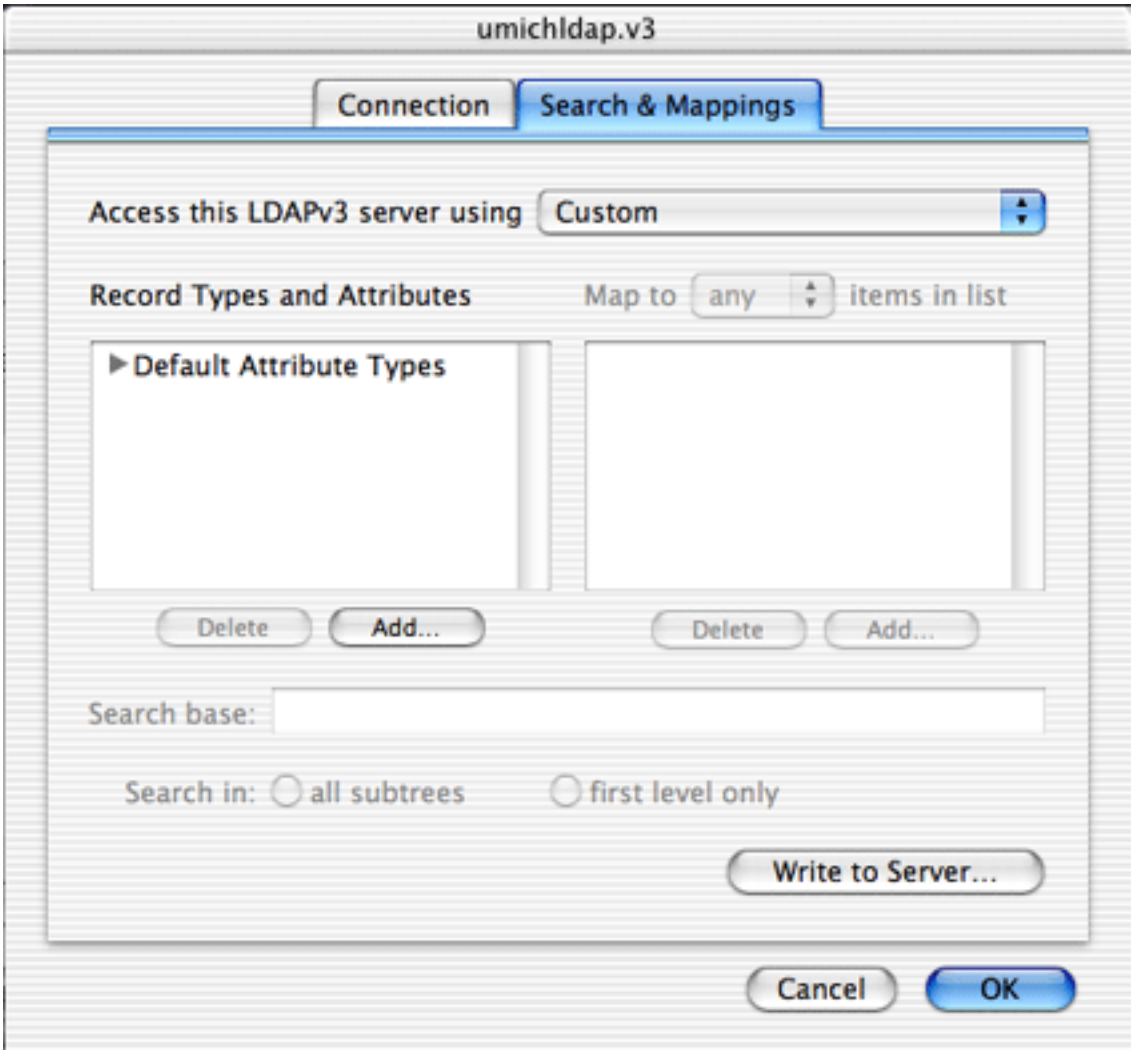


5. Click on the **New...** button. Double-click on **Untitled 0**, and change it to **umichldap.v3**,. Double-click on **unknown.domain.com** and change it to **ldap.itd.umich.edu.** Leave **LDAP Mappings** set to **Custom**. Currently, SSL is not supported (it will be soon); so for now, **don't** select the SSL checkbox. With the entire line highlighted, click on the **Edit...** button.

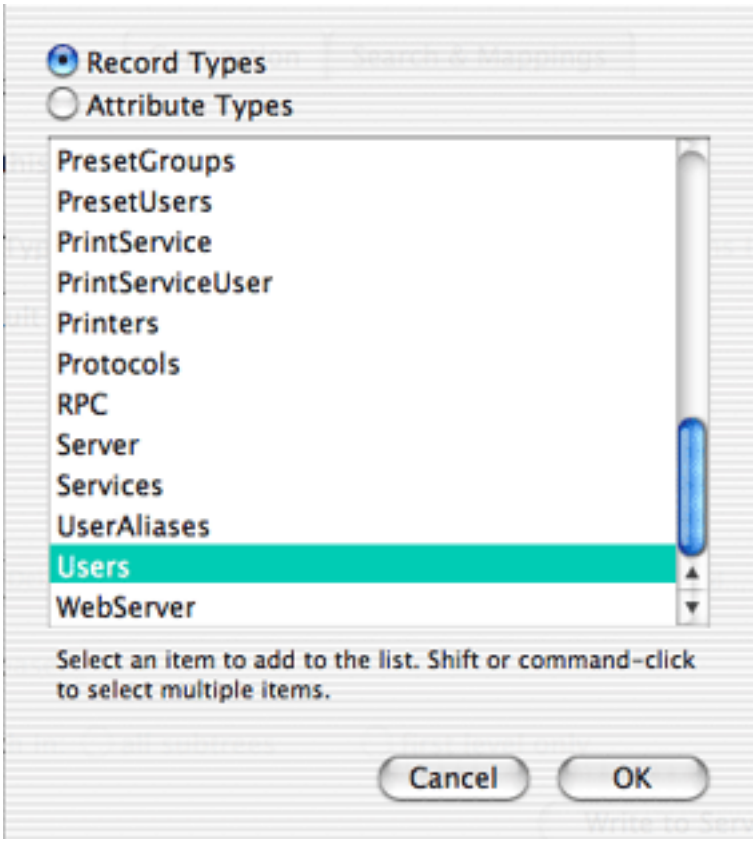


6. Under the **Connection** tab, you shouldn't need to make any changes, so click on the **Search & Mappings** tab. Under the **Record Types & Attributes** box,click on the **Add** button.

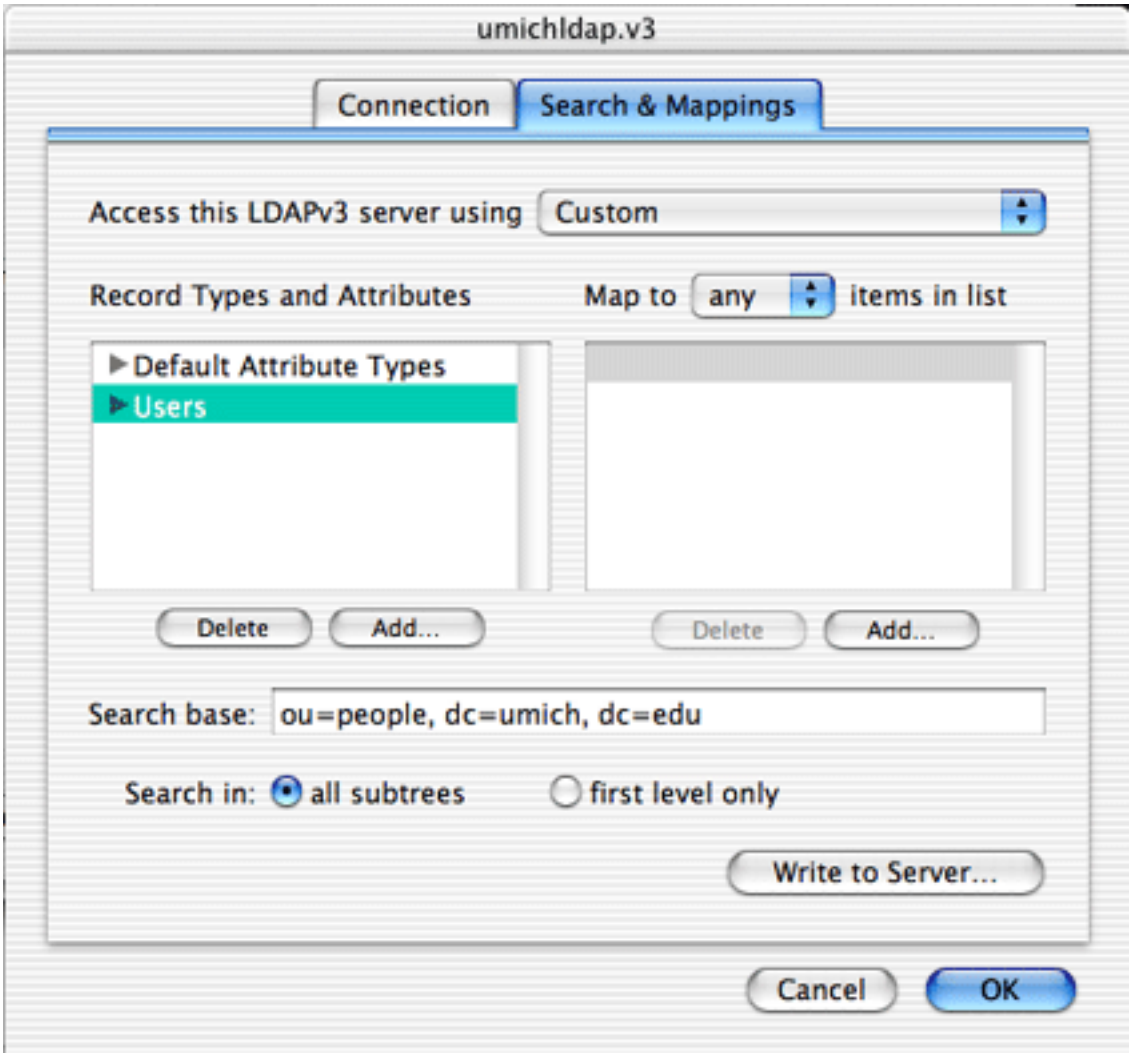

umichldap.v3
Connection
Search & Mappings
Configuration Name:
umichldap.v3
Server Name or IP Address:
ldap.itd.umich.edu
Open/close times out in
120
seconds
Connection times out in
120
seconds
Use authentication when connecting
Distinguished Name:
Password:
Encrypt using SSL
Use custom port
389
Cancel
OK



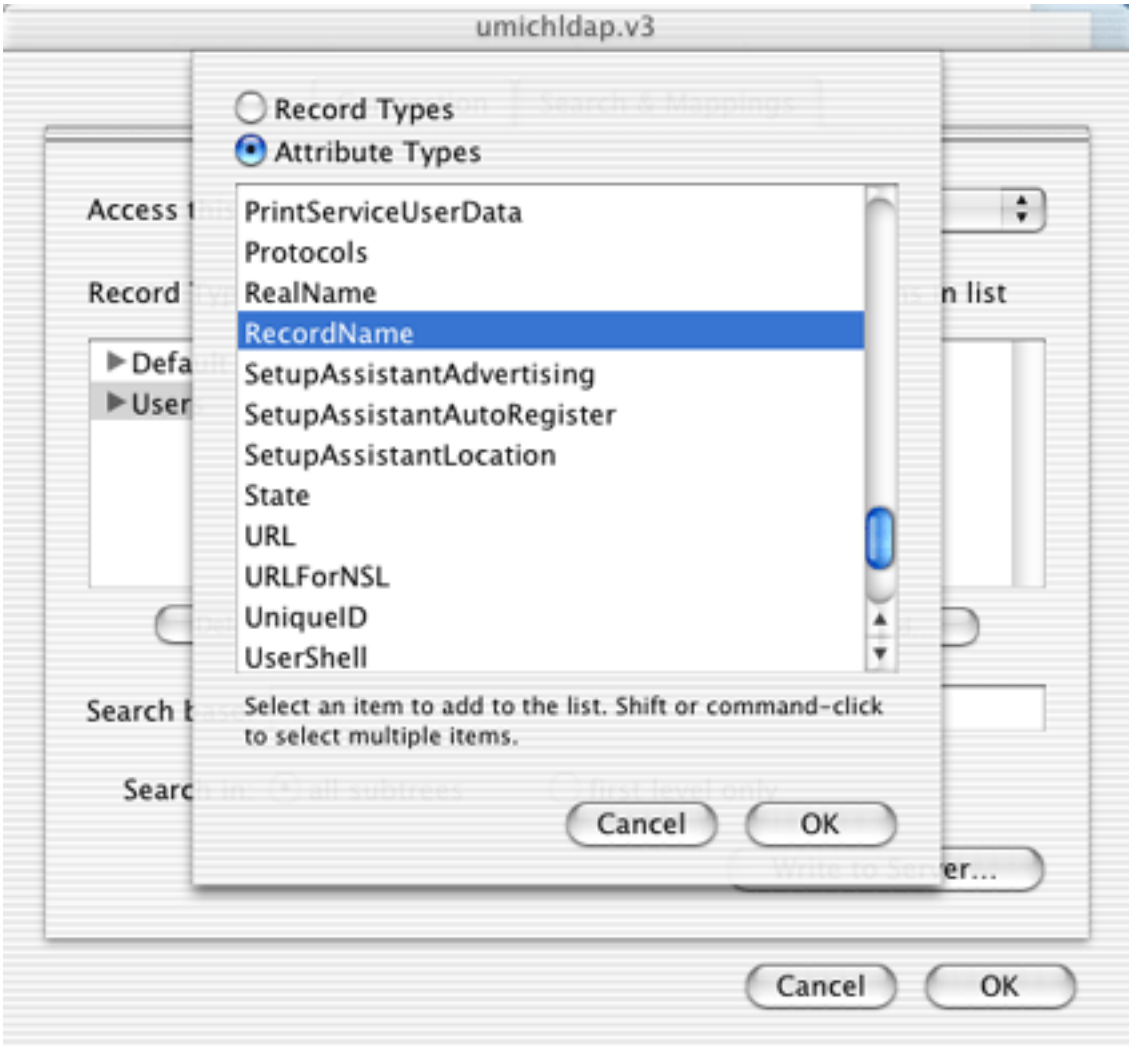
7. Make sure the **Record Types** radio button is selected, select **Users** and then click the **OK** button.

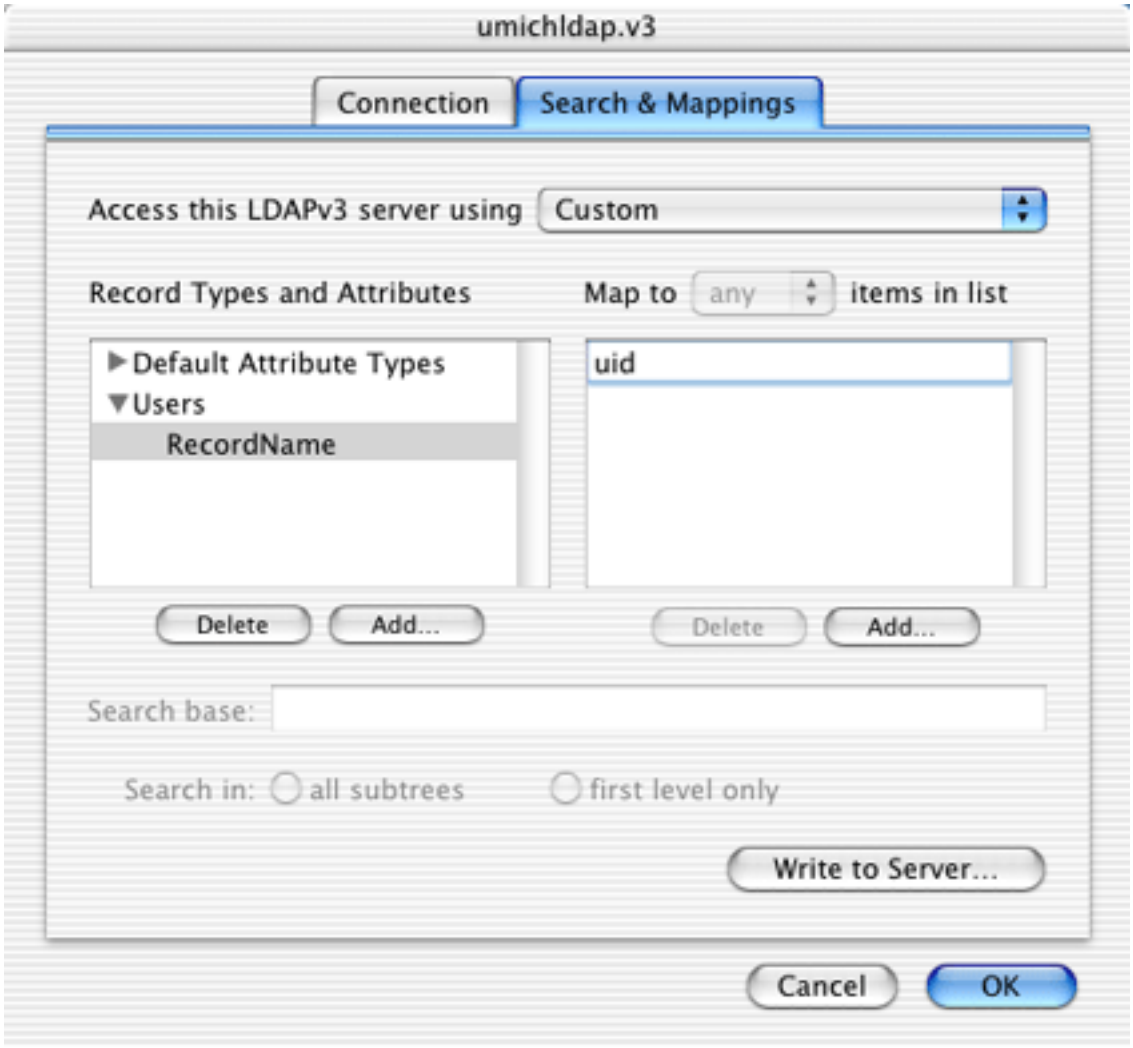


8.Click inside the **Search base** text box. Type in **ou=people, dc=umich, dc=edu** .



9. Back in the **Record Types & Attributes** box, make sure **Users** is selected and click the **Add** button again. Make sure the **Attribute Types** radio button is selected. Select **RecordName** and click the **OK** button. Again, back to the **Map to** box and click the **Add** button. Type in **uid**.


umichldap.v3
Record Types
Attribute Types
PrintServiceUserData
Protocols
RealName
RecordName
SetupAssistantAdvertising
SetupAssistantAutoRegister
SetupAssistantLocation
State
URL
URLForNSL
UniqueID
UserShell
Select an item to add to the list. Shift or command-click to select multiple items.
Cancel
OK
Cancel
OK



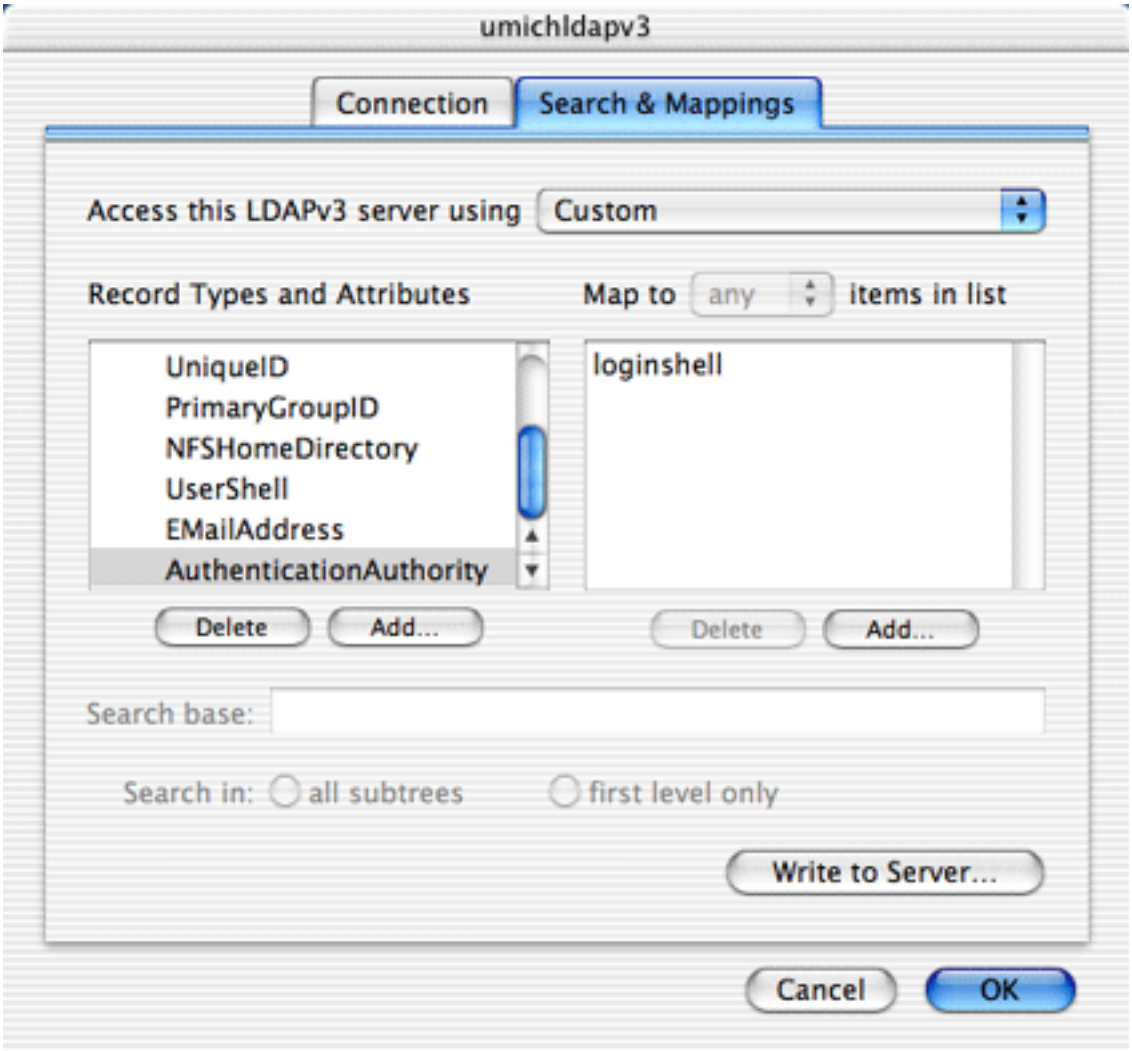
10. Repeat the same steps using the following information:

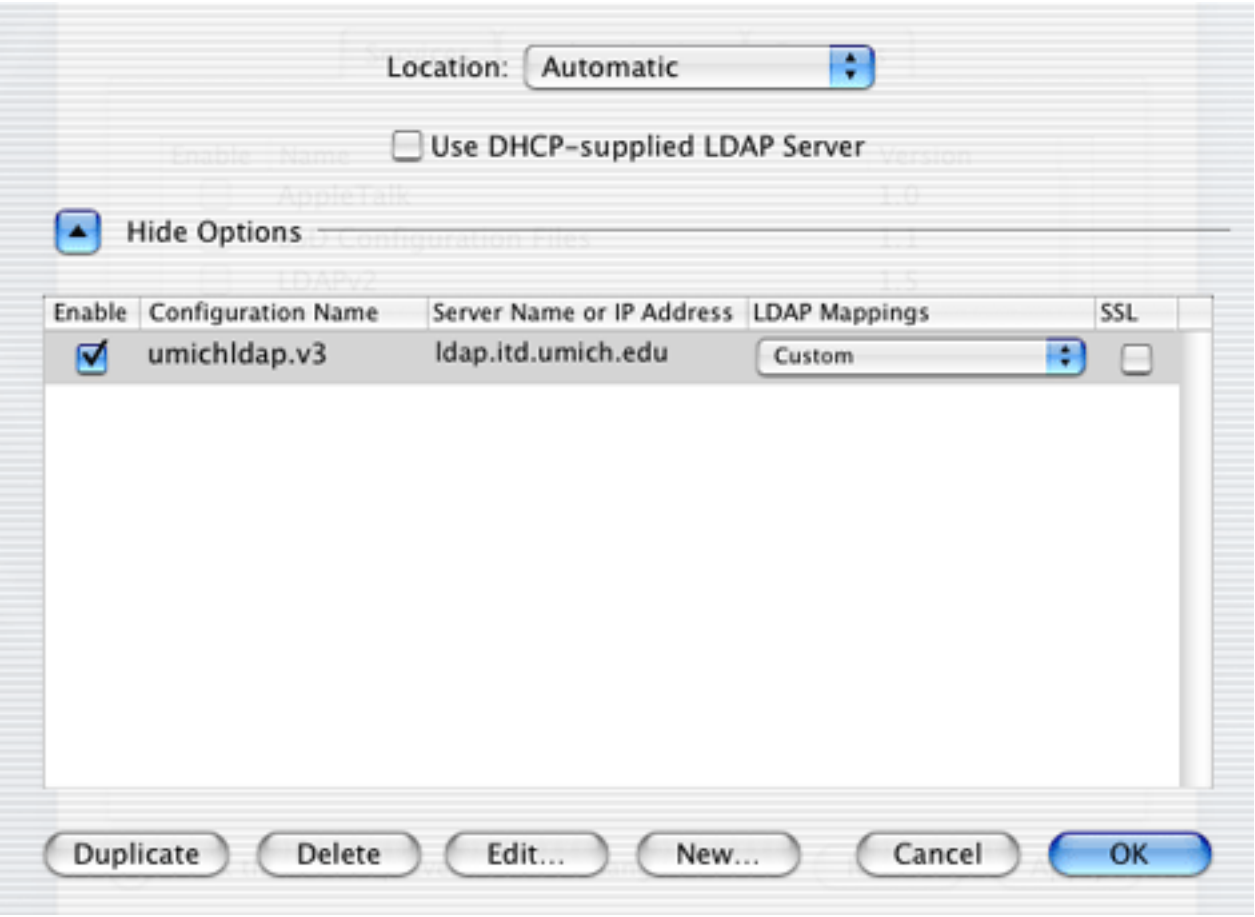
Make sure to include AuthenticationAuthority mapping; it's a recent addition for security!

Attribute Type:	Maps to:
RecordName	uid
RealName	cn
UniqueID	uidnumber
PrimaryGroupID	gidnumber
NFSHomeDirectory	homedirectory
UserShell	loginshell

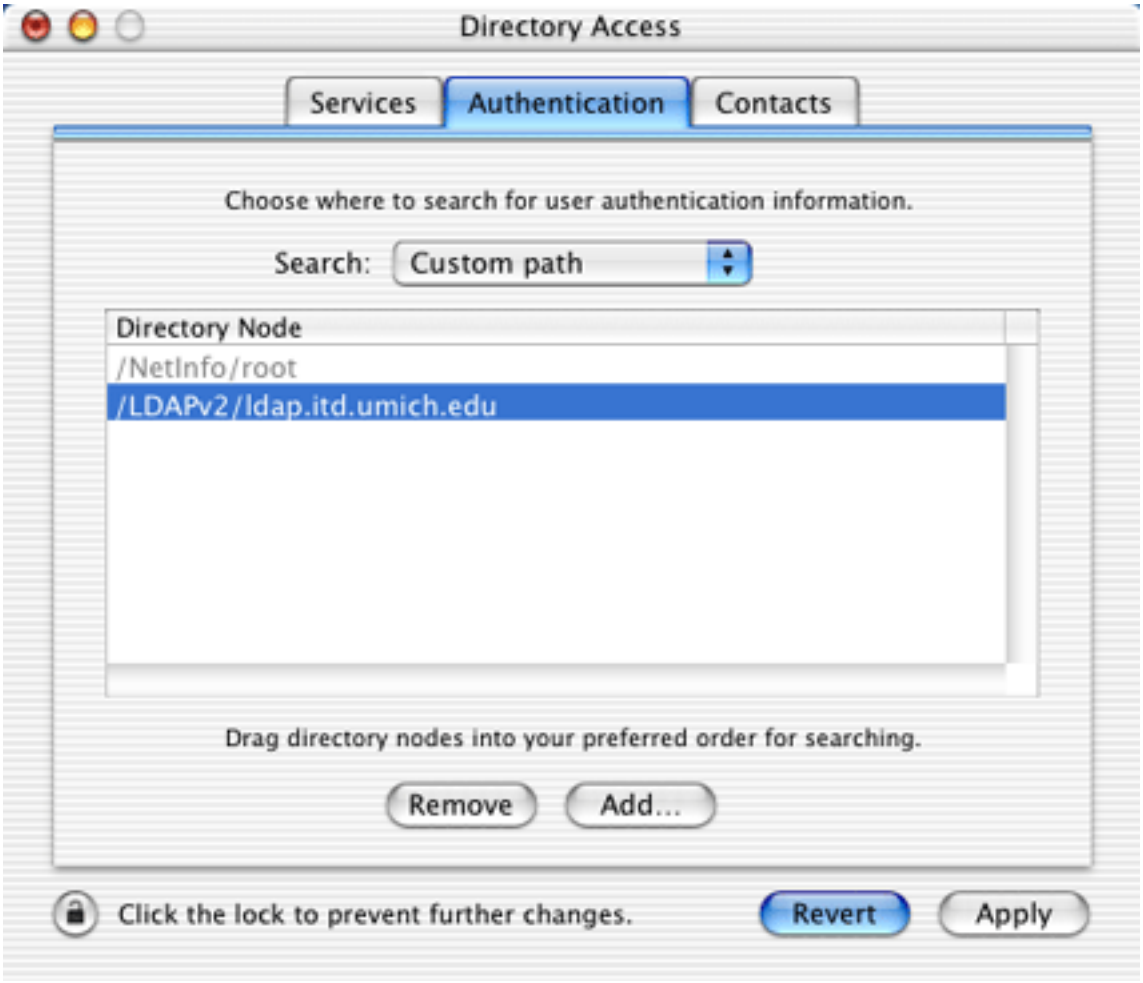
EmailAddress	mail
AuthenticationAuthority	loginshell

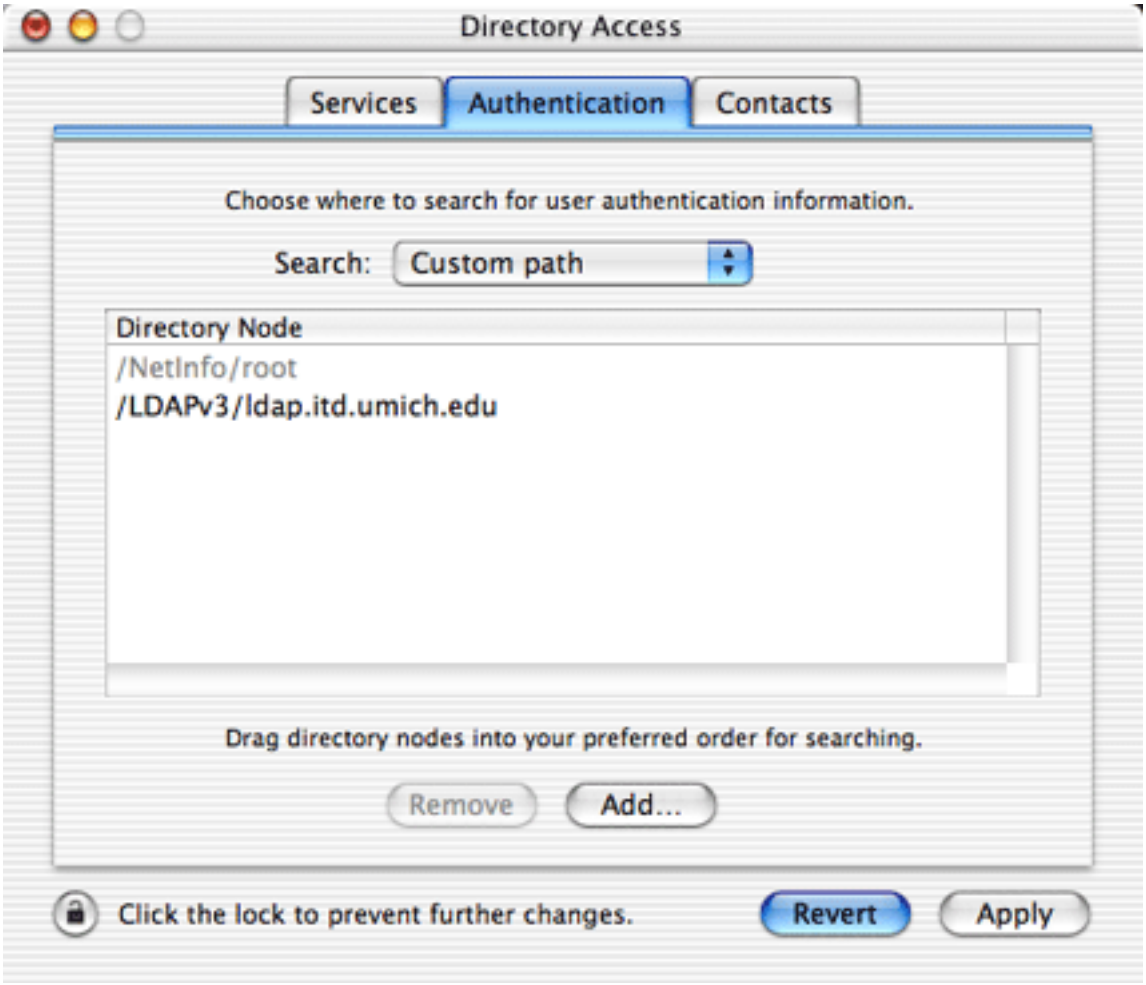
11. When you are finished, click the **OK** button. At the next screen, click the **OK** button there as well.





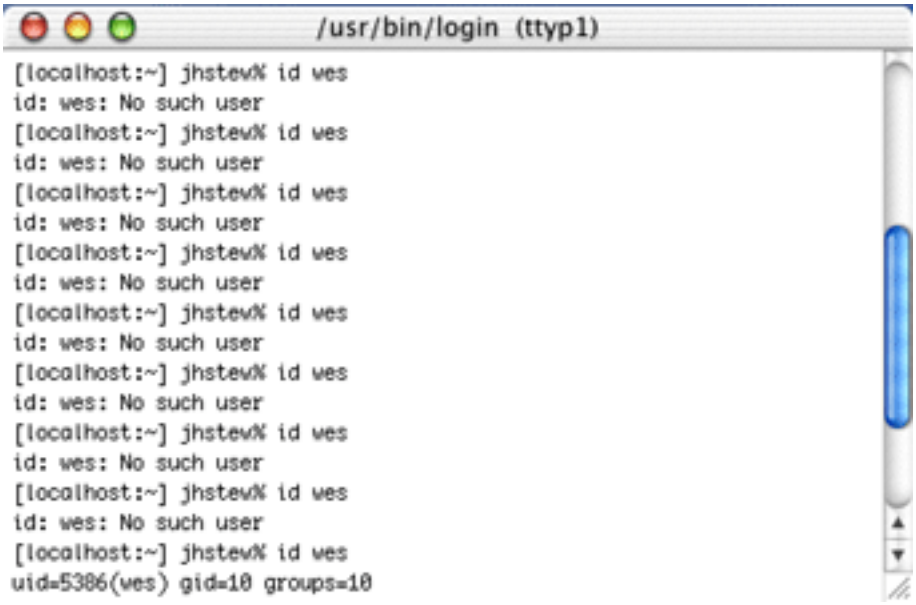
12.Click on the **Authentication** tab. You can remove any previous custom paths by selecting them and clicking the **Remove** button. Then click the **Add** button, and select **/LDAPv3/ldap.itd.umich.edu**. Then click the **Add** button. Nothing under the **Contacts** tab needs to be configured, so you can click on the **Apply** button. Click on the red close-window button , **Save** the changes, and you are done!


Directory Access
Services
Authentication
Contacts
Choose where to search for user authentication information.
Search:
Custom path
Directory Node
/NetInfo/root
/LDAPv2/ldap.itd.umich.edu
Drag directory nodes into your preferred order for searching.
Remove
Add...
Click the lock to prevent further changes.
Revert
Apply



13. Start the **Terminal** application from the **Utilities** folder in the **Applications** folder.

14. Type **id *uniquename* <Enter>**, where uniquename is a "Michigan Person" who does not have a local user account on the computer. The reply will come back `id: uniquename: No such user` until the changes come through; then you should get the uid, gid, and groups values for that unquename. That indicates that everything is working correctly.



Additional sites for your UM OS X Configurating pleasure:

http://www.umich.edu/~arosenbl has pages on configuring both MIT Kerberos and OpenAFS
http://www.itd.umich.edu/macos/macosx_more.html The "more" page has all the good stuff.
Well, more is **MORE** , isn't it?
Reloading a lab? You need Radmind... http://rsug.itd.umich.edu/software/radmind/macosx.html
Running logout scripts, or other scripts that want a gui? http://rsug.itd.umich.edu/software/ihook
Setting up a lab in the first place? http://www.macosxlabs.org is where you need to go. No, trust me; you need to go there.
How about a free **secure** ftp client? http://rsug.itd.umich.edu/software/fugu