Client Management with Mac OS X Server

Mac OS X Server 10.3 Panther and connected clients
(9.2, 10.2.X and 10.3.X)

Version 1.2

I. Before you begin

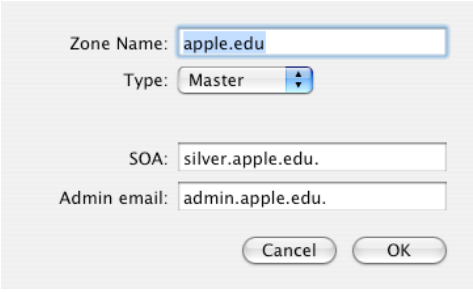
- DNS is key. You must have it available and running in your environment for Managed Client for X (MCX) to operate correctly.
- An MCX server must be acting as an Open Directory Master or an Open Directory Replica
- Yes, MCX computers (running Mac OS X 10.2.X and 10.3.X), and MacMgr computers (running Mac OS 8.6-9.2) can use the same login credentials to get to the same home directory.
- If you have Windows clients running Windows 98, 2000 or XP, they can also use the same credentials and home directory (although we won't be covering it in this document).

Note: After a clean installation of Panther Server, the server reboots to the setup assistant. Here are a few guidelines to follow while going through the setup assistant.

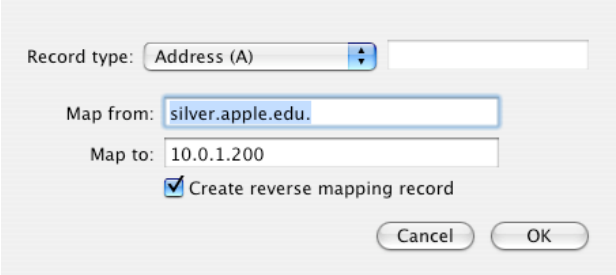
- When the setup assistant asks for a host name, be sure to put in the fully qualified domain name ("silver.apple.edu" instead of "silver").
- Do not turn on any services (AFP, Web, etc.) in the setup assistant. You can turn those on in Server Admin.
- Always establish your server as a standalone server and promote it later in Server Admin. It does not always work to set up your server as an Open Directory Master or Open Directory Replica in the setup assistant.
- As soon as you complete the setup assistant, run all applicable software updates (iCal, iPhoto, etc. are optional, of course).

A. DNS (Domain Name Service) is critical

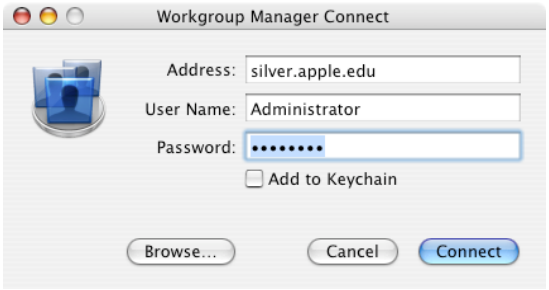
1. If you don't have DNS in your school, here's a quick and simple quide to getting it up and running so that your server and clients can appropriately resolve names.
2. In Server Admin, click on the DNS service and then click on "Settings" below.
3. In the left window, click on the plus sign go create a new zone.
4. In the window, name your zone so that it matches your naming scheme on the outside world. For example, if I were the technology coordinator for a school that owned the domain name "apple.edu," I create the same zone on the inside of my network. Here's a screen shot of how to create that new zone (note the trailing periods).



5. Once your zone is created, make a new record so that the server can resolve it's hostname to it's new IP address. Be sure to check the box to create a reverse record. This is what I would make after naming my server "silver.apple.edu" when going through the setup assistant on this server.



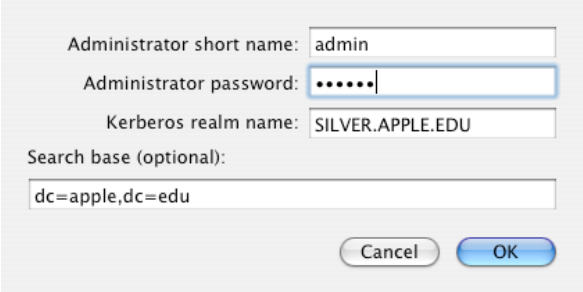
6. At the top of the Server Admin window, click "Start Service."
7. Be sure to add the DNS server into your TCP/IP settings.
8. Reboot your server.
9. If you still need assistance, review the documentation for network services and/or call Apple Tech Support at (800) 800-2775.
   (download PDF at http://images.apple.com/server/pdfs/Network_Services.pdf)
10. Once DNS is set up correctly, launching Workgroup Manager should result in a similar look as the screen shot below, as you'll see the fully qualified domain name instead of the .local address.



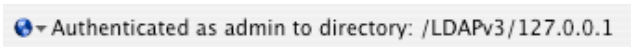
B. Setting your server as an Open Directory Master

Note: If you've already set up your server, no problem. If not, it's always a good idea to set up ANY 10.3 server as a Standalone Server when going through the setup assistant (the assistant that launches after you first install server software) because it is safer to set it up as an Open Directory Master in the Server Admin application. Also, when the setup assistant asks for the host name of the computer, always type in the fully qualified domain name ("silver.apple.edu" instead of "silver"). If your server is already set up and you missed the chance to put in the FQDN, then you can edit the entry in the /etc/hostconfig file.

1. Once DNS is set up correctly, it's time to promote your MCX server to an Open Directory Master.
2. Launch the Server Admin application and click on Open Directory.
3. Click on the Settings button below and change the server from a Standalone Server to an Open Directory Master.
4. Once selected, you will be prompted with the admin name and password below. A similar screen shot to the one below will confirm that things are looking good.



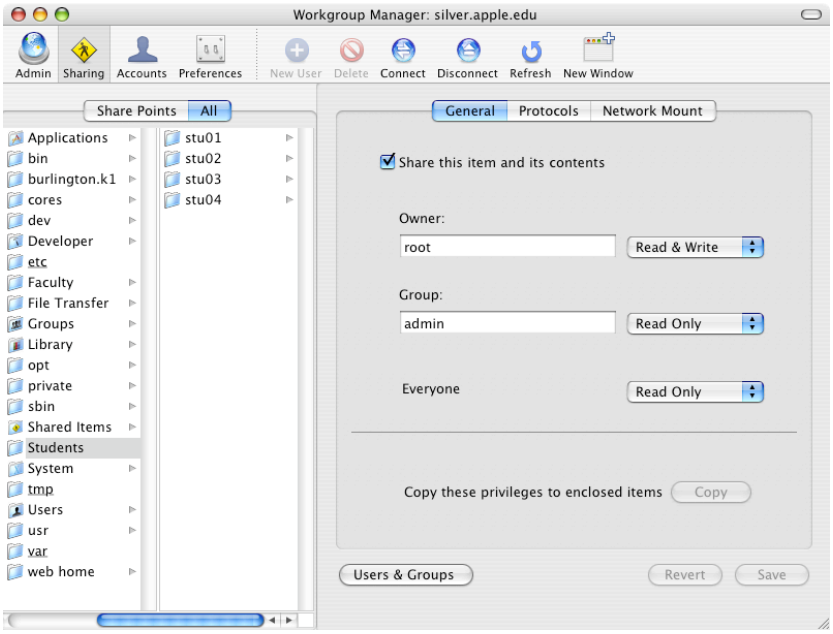
5. Put in the correct account information and click OK.
6. Click Save.
7. Launch Workgroup Manager (if it was already running, quit and relaunch).
8. You should see the following below the toolbar to confirm that you're utilizing the LDAP directory instead of NetInfo.



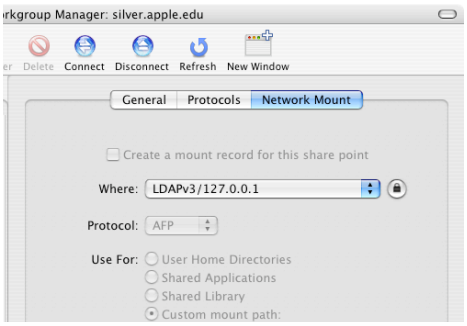
9. If these steps havn't worked for you, it's time for the "demote/promote" trick. In Server Admin, demote your Open Directory server to a Standalone server and click save.
10. Next, promote it right back to an Open Directory Master and click save.
11. Reboot your server and launch Workgroup Manager again. You should be all set.

C. Home Directories

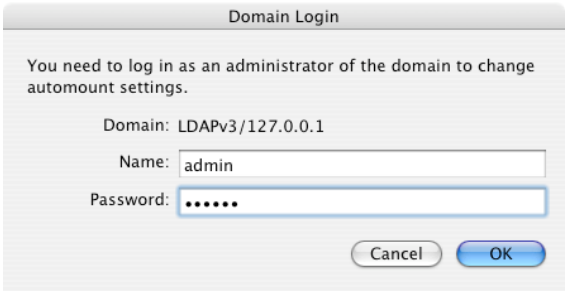
1. The whole home directory planning and implementation process could be a day-long class (and/or it's own 20 page manual). Here's a quick alternative lesson on creating a sharepoint for home directory storage.
2. Create a folder in the "Shared Items" location, at the root level of a server drive, or on your loaded Xserve RAID.
3. In WGM, click on Sharing and click on the "All" tab. You can then navigate to your new folder and check the box on the right to "Share this item and its contents."



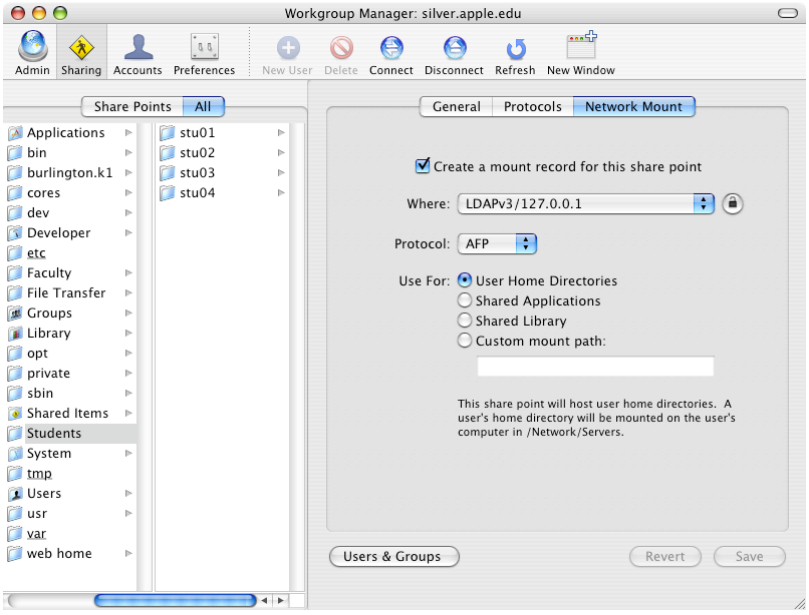
4. Once your sharepoint has been set, click on the "Network Mount" tab.
5. Click on the LDAPv3/127.0.0.1 menu and release on the same item (just click and release on the pulldown menu with your cursor).



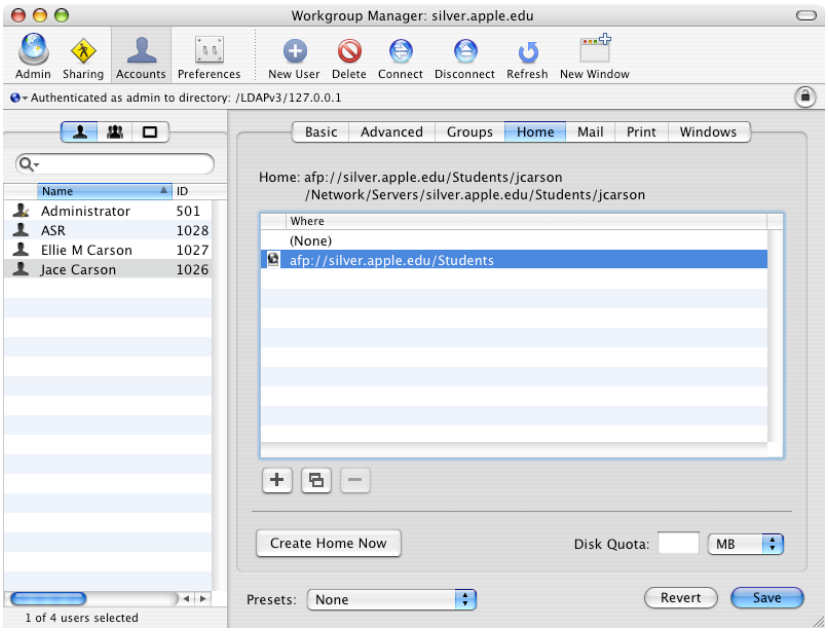
6. When prompted, enter your admin account and password information.



7. Once authenticated, check the box to "Create a mount record for this share point" and make sure it is set for use as a home directory sharepoint.



8. Now, when you go back to your user accounts, you'll see a new option under the home tab.
9. This is what we have to have in our managed environments; automounted home folders.



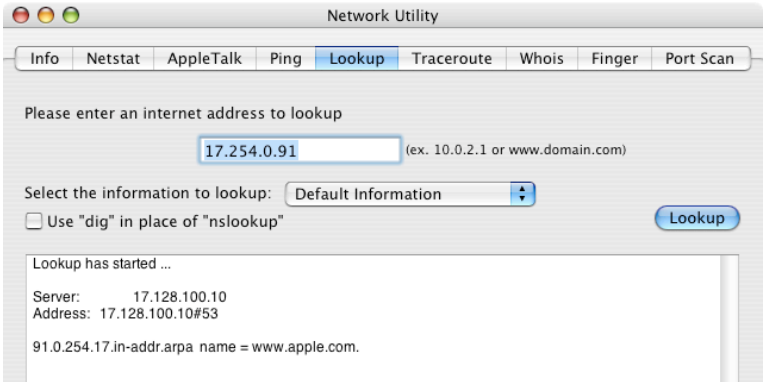
10. Yes, you can batch edit this. Highlight one account on the left, the hit command-A to select all, (deselect your admin account, of course) and point them to their new home location. Done!
11. If you want to create all home directories ahead of time, a quick visit to Terminal can fix this. Simply type the following at the command prompt:

    ```
    sudo createhomedir –a
    ```

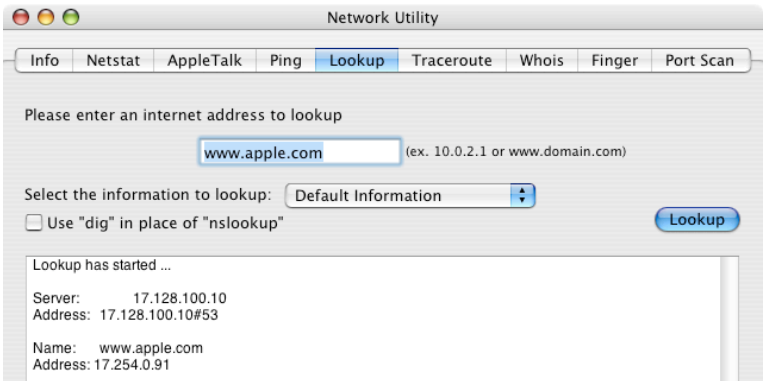
12. You'll then be prompted for the admin password, and you'll see all of them created for you automatically.

D. Connecting a 10.3.X client to your server

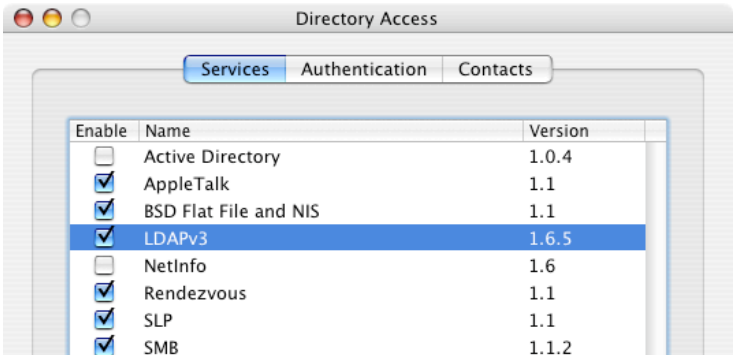
1. Now that your server is ready, it's time to connect a client and provide network logon capability for your users. I've heard a million times from many different customers, "How do I make my MCX environment look and feel like Macintosh Manager did?" Well, here you go.
2. First, be sure that your client is on the same page with your server in terms of DNS. From the client, launch /Applications/Utilities/Network Utility.
3. Click on the "Lookup" button and type in the IP address of your server. If it resolves to the fully qualified domain name of your server (ie www.apple.com), then you're on the right track.



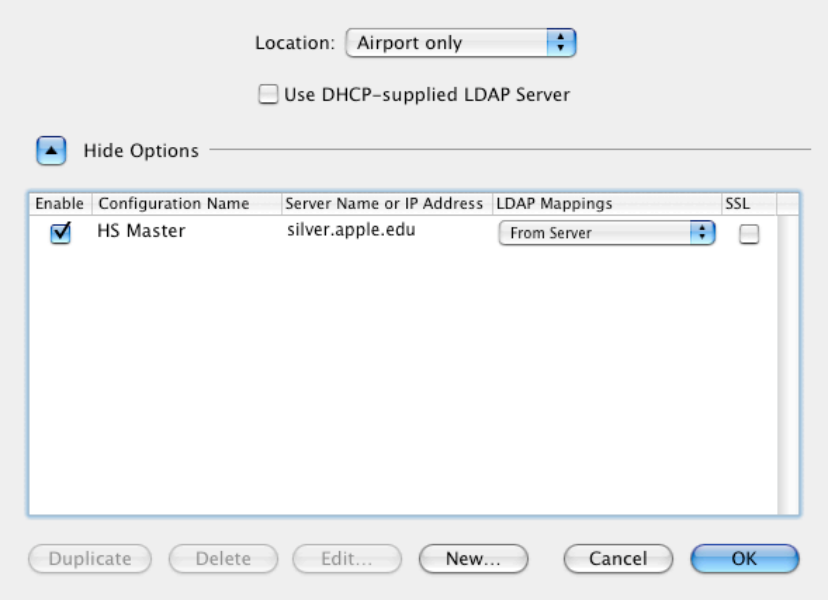
4. Now type in the fully qualified domain name of your server in the field and it should spit back your server IP address.



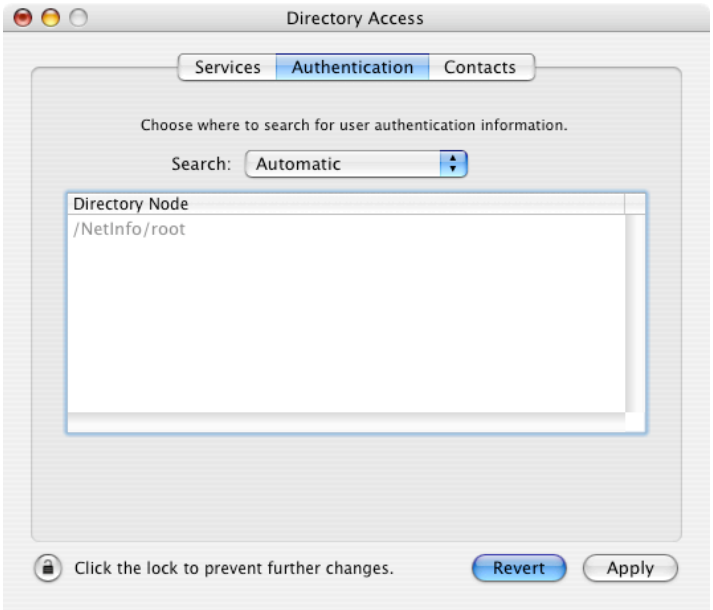
5. When these two lookups resolve, this is proof that your DNS has a correct forward and reverse entry for your server.
6. Now for the good part. Launch /Applications/Utilities/Directory Access.
7. We're going to use the LDAPv3 plugin for connectivity. Remember setting up your OD Master server? You were setting it up as an LDAP server.



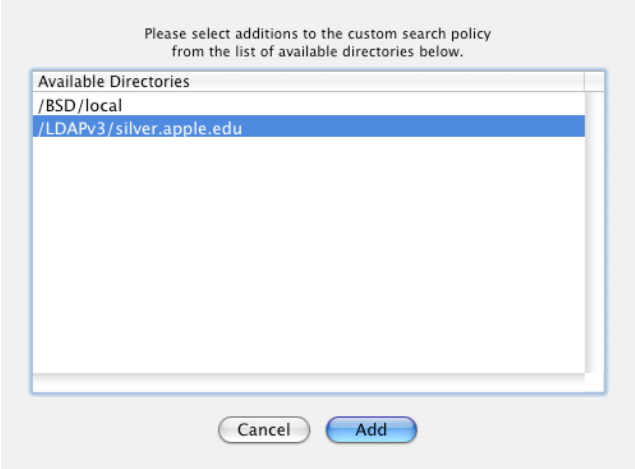
8. Double-click on the LDAPv3 plugin in order to configure it.
9. Click "New" in order to create a new connectivity configuration. It is here that you type a description and a server name or IP address. The description name can have spaces and doesn't really matter. Name it as if you were naming a file. In the server name/IP address field, be sure you type this accurately. One wrong character and it will not connect.



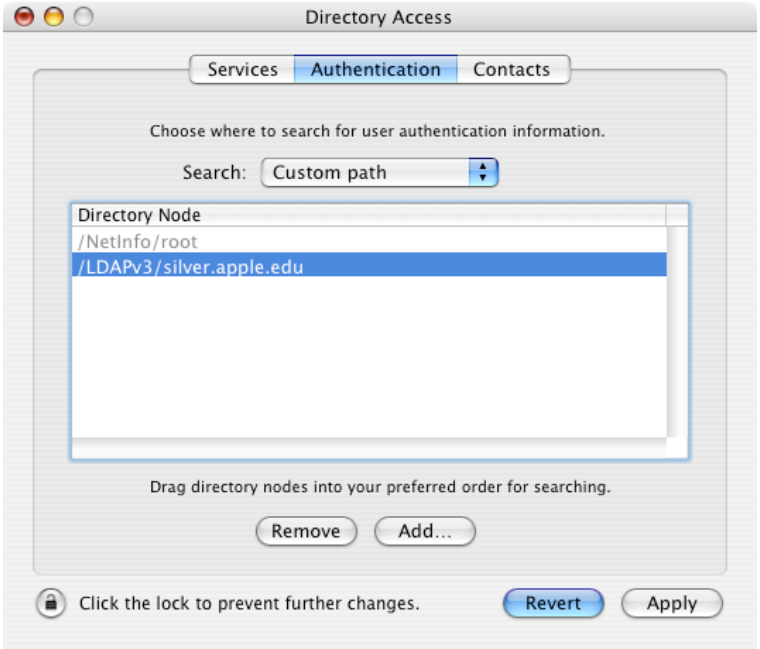
10. Don't forget to uncheck the box at the top so that you're not pulling LDAP info from a "DHCP-supplied LDAP Server."
11. There is no need to touch the "From Server" pull down menu under LDAP Mappings.
12. Click OK when you have everything set.
13. Now that your server information is in place, we need to place it in the authentication path. Click on the Authentication tab.



14. This is the default setting. Change the Search criteria from "Automatic" to "Custom path."
15. Click "Add" to add new authentication criteria.



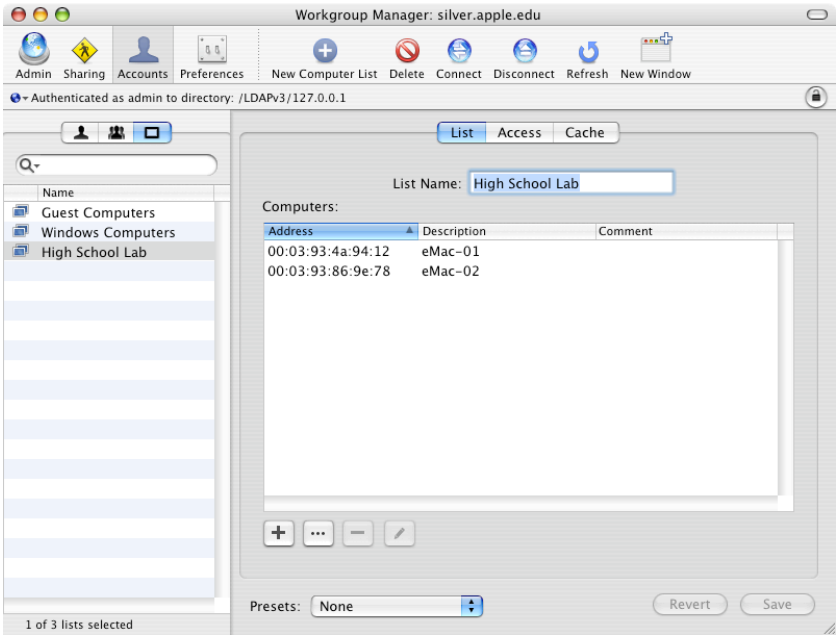
16. You now should see the option to add your LDAP directory. Highlight it and click the "Add" button.
17. Once you add it, your custom authentication path should look like this.



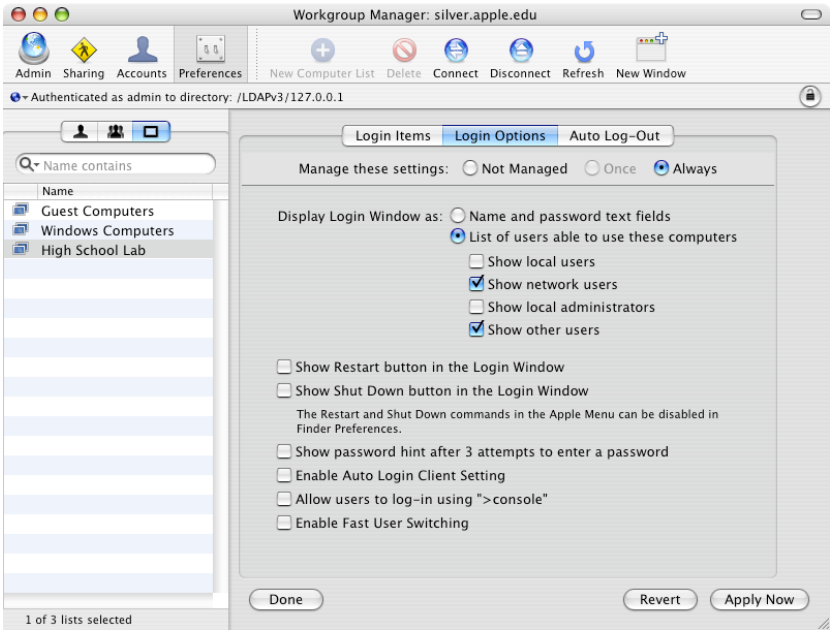
18. Click the apply button. The above screen shot can be translated to the following. "Hey, Mr. 10.3.X client computer. When somebody logs into this computer, I want you to first check the local user database to see if the account name and password match. You know, check the users that the admin person set up under Accounts in System Preferences on this local HD. If you can't find the account in that directory, check on the server silver.apple.edu. There is an LDAP directory that the account might be in. If neither occur, shake the login screen at them and enjoy looking at the puzzled face of the students and teachers." See? Easy stuff.
19. Reboot your client computer. At the login screen, you will either be looking at name/password fields or a user list that now has "Other…" at the bottom. Login with a network account and that account should be properly mapped to a network-based home directory.

E. Matching what users used to see in the Macintosh Manager world

1. This part is pretty straightforward. The request I hear the most when visiting with customers is that they want their users to be able to choose their name from a list in the Mac OS X environment.
2. In Workgroup Manager, create a computer list for each individual lab or group of computers. An example would be a typing or multimedia lab.



3. Once you have your computer list built, click on Preferences while you have that computer list highlighted.
4. Click on the Login preference and then the "Login Options" button.



5. Choose to always manage these settings and pick the details that you wish. I like to utilize the list of users feature. In addition, I like to take advantage of the "other" user so that I can hide local users and admins that the kids need not be concerned with.

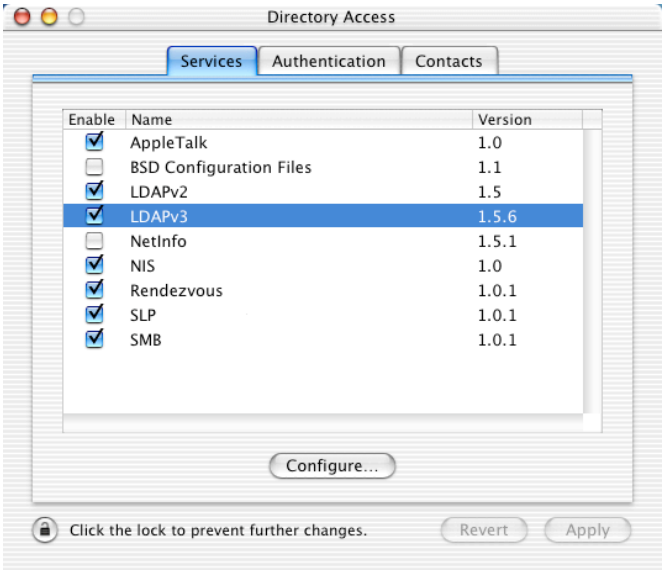
6. If your client isn't showing the list, then you might need to refresh the cache. This updates itself every 2 days by default on computer lists (click on the computer list your modifying and then click on the "Cache" button to manually update it).
7. You should now see the following (screen shot on next page), although your list is probably a lot longer.



8. Notice the "Other…" account. This is my back door to get in as the local admin account of this computer.

F. Connecting a 10.2.8 client to your MCX Server.

1. Notice that the title of this section is not "Connecting your 10.2.X client." This is because your 10.2 clients must be updated to 10.2.8 for this to work.
2. At your client workstation, you'll need to again visit /Applications/Utilities/Directory Access.
3. We will be modifying the LDAPv3 plugin once more.

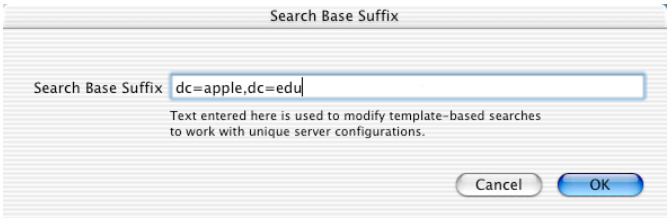


3. Click "Configure" to modify this plugin.
4. This next screen shot should look familiar. Add a new configuration and put in a name and server address for your MCX server.

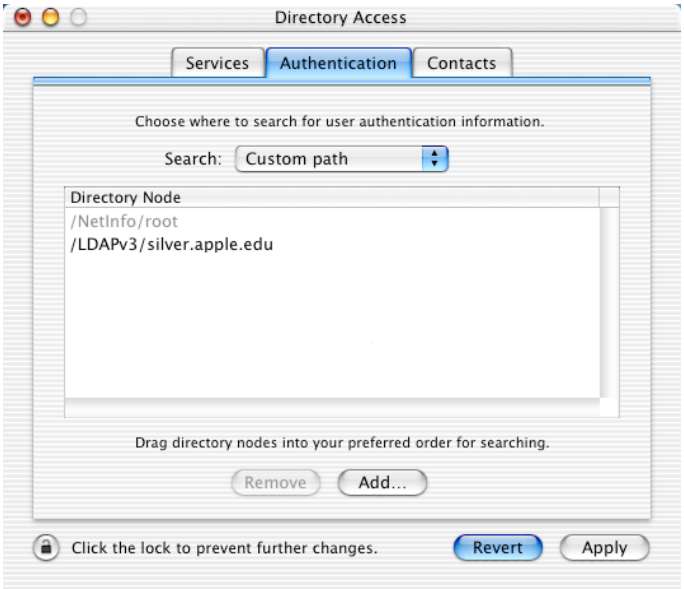
5. Before clicking OK, you want to click on the "From Server" pull down menu and choose "Open Directory Server."



6. You will be prompted to put in a search base suffix. This is where people usually get confused and pick up the phone. However, we've seen this information before when creating our OD Master server (see screen shot on page 3), so we put in that same information.



7. For my server, my search base suffix was based on my domain name, which was apple.edu. If your domain is "school.k12.ks.us," then you would have a search base suffix of: **dc=school,dc=k12,dc=ks,dc=us**
8. Notice that there are no spaces in the search base suffix. Again, one wrong character and you're not going to resolve properly to your server.
9. Once this is entered click OK and click OK again at your LDAPv3 configuration window.
10. Now click on the Authentication tab and add your new custom authentication path. Your results should look similar.

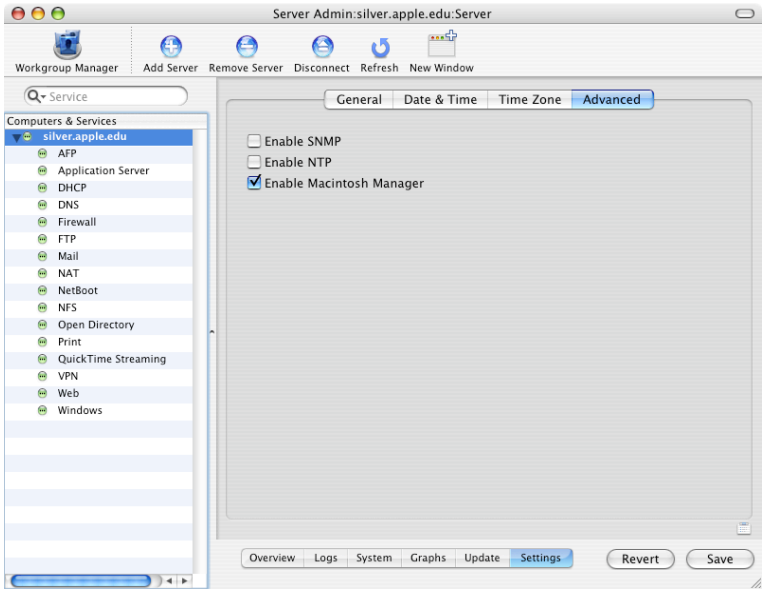


11. Click Apply and reboot your client workstation. You should see a login screen that looks a lot like your 10.3 client.



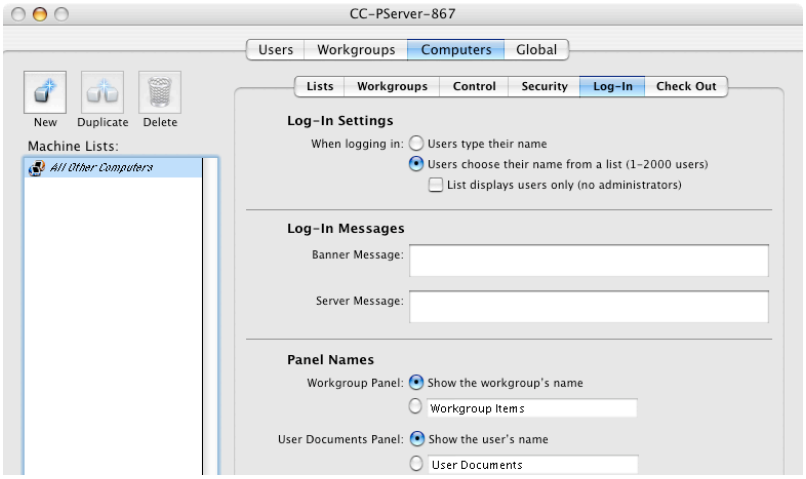
F. Connecting a Mac OS 9/Macintosh Manger client to your MCX Server.

1. If your Mac OS 9 clients are still humming along and you don't want to leave them out of the mix, here's the steps involved so that your Macintosh Manager clients can use the same username and password to login and get to the same home folder that they see from the Mac OS X environment
2. First, you need to enable Macintosh Manager (MM) on the server. In Server Admin, click on the server name and click on Settings. In settings, click on the Advanced tab and check the appropriate box to enable MM.



3. Now that that is done, you can launch the MM Admin program (from your admin workstation, not on the server itself), and authenticate with your admin name and password.
4. Now that MM Admin is launched, launch Workgroup Manager as well and authenticate to your MCX server with your admin name and password.

5. Here's the fun part. Drag your two open windows (WGM and MM Admin) so that they are offset and you can see the User lists for both interfaces.
6. Select all of your users that you want in WGM and drag them into your user list in MM Admin. Those that you select should only be those users who need to login from a Mac OS 9 workstation.
7. Once the MM Admin import is done, it is usually helpful to show your MM clients a list of users so that it appears similarly to your Mac OS X login screens. To do this, click on the "Computers" tab followed by the "Log-In" sub-category. Choose the option so that users choose their name from a list.



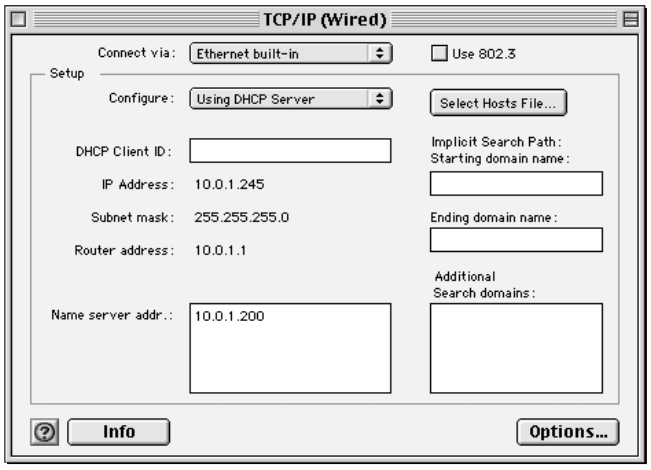
8. Now that your MM Server is ready, it's time to update your MM client workstation.
9. Open the Extensions Manager control panel and make sure your client has version 2.2.2 of the MM software. If not, you can download the latest version at http://www.apple.com/support (search for "macintosh manager 2.2.2").



10. Once rebooted, your client workstation may be looking for the MM server that it used to connect to. Select to "Pick a different server" and type in the new destination.



11. If the Mac OS 9 client says that it cannot find that server, you may not be pointing to the appropriate DNS server so that it can resolve the name to the IP address. Since my lab DNS server is 10.0.1.200, I have the TCP/IP settings look like the screen shot below.



12. Once your workstation can resolve the server name and can attach via MM, restart the workstation. Your resulting login screen should look similar to the one below.



13. Notice that I have the server name that resolves correctly and the same user list as my 10.2.8 and 10.3.X clients (actually, I deleted my ASR user somewhere in the process of collecting these screen shots, so don't let that bother you that the ASR user is missing from the 10.2.8 and MM login screens).

Remember that this is just a quickstart guide. It's sole intention is to get you up and running quickly with MCX and network-based home directories. Further details are available in the server manuals and other resources such as John DeTroye's Tips and Trick series (http://homepage.mac.com/johnd). As always, Apple's support website and hotline phone support (800-800-2775) are your first line of defense when troubleshooting. Comments on this document as well as tips for future documentation are welcome. Send me a line at ccarson@apple.com.

Thanks!