Client Management with Mac OS X Server

Mac OS X Server 10.4 Tiger and connected clients
(10.2.8, 10.3.8 and 10.4.X)

Version 1.3

I. Before you begin

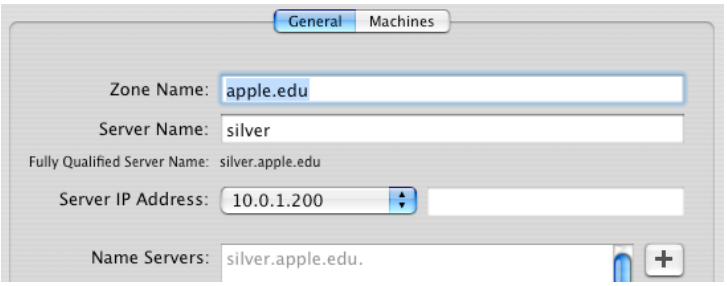
- DNS is key. You must have it available and running in your environment for Managed Client for X to operate correctly. If you ever need to call Apple's support hotline for assistance (800-800-2775), they'll expect the same.
- A client management server must be acting as an Open Directory Master or an Open Directory Replica
- Yes, managed computers (running Mac OS X 10.2.8, 10.3.X and 10.4.X) can use the same login credentials to get to the same home directory.
- If you have Windows clients running Windows 2000 or XP, they can also use the same credentials and home directory (although that won't be covered in this document).

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

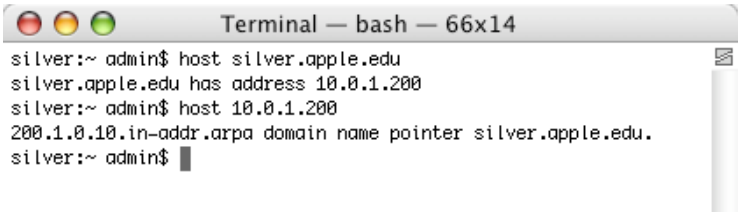
- The setup assistant no longer asks for a host name. The hostname data in /etc/hostconfig now handles this dynamically for you. Although you'll usually want to edit this file to put in the fully qualified domain name of the server.
- Do not turn on any services (AFP, Web, etc.) in the setup assistant. You can turn those on in Server Admin after you've determined that DNS is working correctly.
- Always establish your server as a standalone server and promote it later in Server Admin, again, after you've determined that DNS is working correctly.
- As soon as you complete the setup assistant, run all applicable software updates (iCal, iPhoto, etc. are not necessary, 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 guide 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 to 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 would create the same zone on the inside of my network. Here's a screen shot of how to create that new zone. A lot of guesswork has been eliminated since the Fully Qualified Server Name is dynamically updated as you type.



5. Once your zone is created, launch Terminal and type the following commands (with your IP and DNS information, of course). You should get feedback that looks similar to the screen shot below.



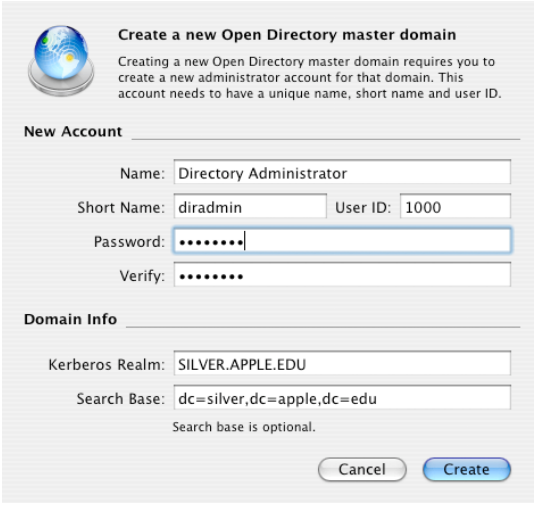
6. At the top of the Server Admin window, click "Start Service."
7. Be sure to add the DNS server into your TCP/IP settings.



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.
   http://images.apple.com/server/pdfs/Network_Services_v10.4.pdf

B. Setting your server as an Open Directory Master

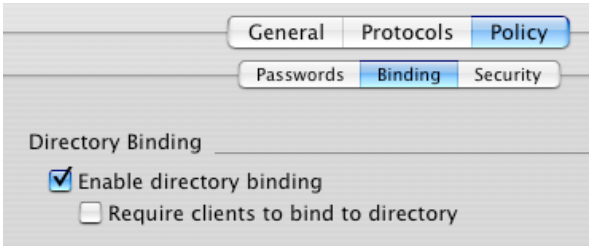
1. Once DNS is set up correctly, it's time to promote your client management server to an Open Directory Master.
2. Launch the Server Admin application and click on Open Directory.
3. Click on the Settings button below and change the server from a Standalone Server to an Open Directory Master.
4. Once selected, you will be prompted with a new, suggested Directory Administrator account. This is a great new "assistant" because it can help eliminate confusion later. If you set the administrative account as "admin" during the setup assistant, then that account will be used to make changes to the local NetInfo directory. What you should now use is the "diradmin" account for all of your LDAP administration. A similar screen shot to the one below will confirm that things are looking good.



5. A quick note about the search base. If you just want to go with a search base that reflects your domain (dc=apple,dc=edu, for example), then go right ahead. The main rule that you need to follow is to put the same search base in for your clients that will be connecting to this server for management. You can also do the same for the Kerberos Realm. It's required that you keep it in all caps however.
6. Put in the correct account information and click OK.
7. Click Save.

8. While in Settings, click on the Policy tab followed by the Binding sub-tab. Enable directory binding is already enabled, but you can also *require* clients to bind to the directory. ***However, if you require directory binding, it is a best practice to rename every computer to ensure that they have a unique computer name before binding.*** If you image your computers using NetInstall, NetRestore, multicast ASR, etc. you probably will want to avoid the "require binding" feature. If it's okay that all machines have the same name, you'll be fine. This is similar to how an AD-bound Mac client can be imaged and deployed after it is has been joined to AD.

   Note: The "require clients to bind to directory" checkbox is a new security feature that will not allow any user to intentionally or accidentally bind to another server in order to minimize their management and/or limitations.



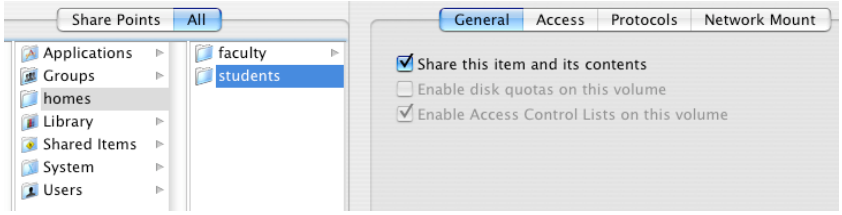
9. Launch Workgroup Manager (if it was already running, quit and relaunch) and authenticate as the "diradmin" account.



11. If these steps haven'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.
12. Next, promote it right back to an Open Directory Master and click save.
13. Reboot your server and launch Workgroup Manager again. You should be all set.

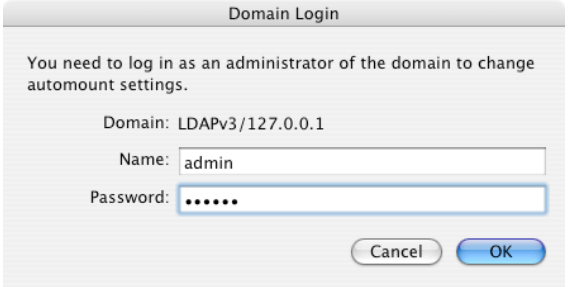
C. Home Directories

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."

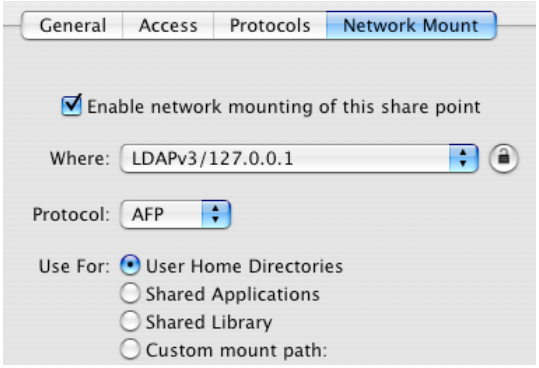


4. Once your sharepoint has been set, click on the "Network Mount" tab.

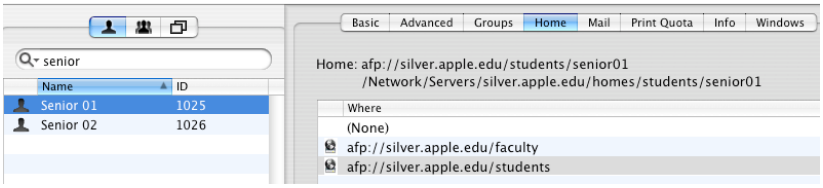
5. Click on the lock icon to unlock the settings.
6. When prompted, enter your admin account and password information.



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 is primarily utilized in managed environments; automounted home folders.



10. Yes, you can batch edit this. Highlight one account on the left, then 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, and the "Create Home Now" button doesn't create all home directories at once, 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 10.4.X client to your server

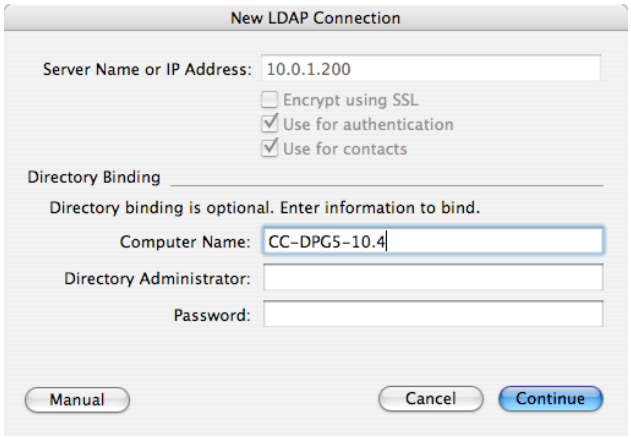
1. Now that your server is ready, it's time to connect a client and provide network logon capability for your users.
2. First, be sure that your client is on the same page with your server in terms of DNS. From the client, launch /Applications/Utilities/Terminal.

3. Use the commands from page 2 of this document to ensure that DNS is resolving as expected. When these two lookups resolve, this is proof that your DNS has a correct forward and reverse entry for your server.
4. Now for the good part. Launch /Applications/Utilities/Directory Access.
5. 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.
6. Double-click on the LDAPv3 plugin in order to configure it.
7. Click "New" in order to create a new connectivity configuration. Now you can simply type in the IP address or the FQDN of your server and be done. It will put the search base in for you (dc=silver,dc=apple,dc=edu). Just be sure to check the box for authentication (contacts is very cool, but optional).

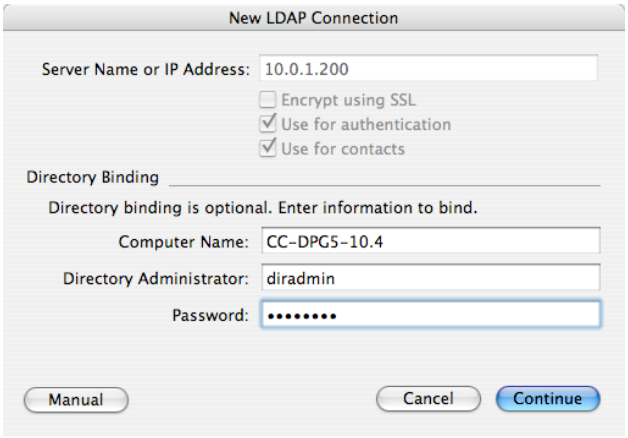
   What you do with the SSL checkbox when binding is up to you, but now in Tiger Server it's not as necessary. This is due to the fact that the Kerberos session key encrypts the data being transferred for the binding and the user authentication. If you do use SSL, the server is doing double encryption, which puts a lot of load on the server.



8. If you followed the steps on page 4 and are requiring that clients bind to your directory, then you'll need to follow the second screen shot below. If you chose not to require binding due to your dependency on imaging and/or ease of setup, then you can leave the second and third fields blank.



Joining without binding

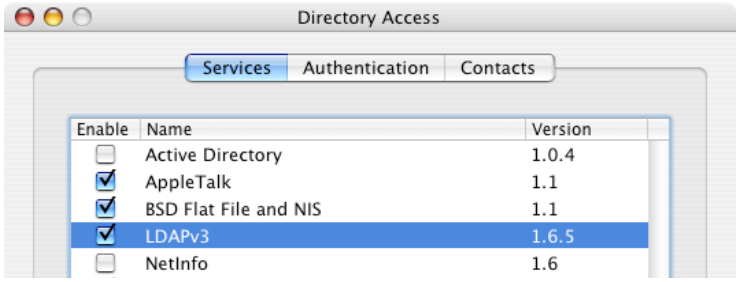


Joining and binding

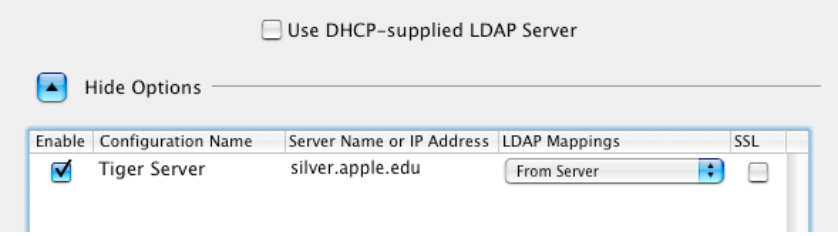
9. Reboot your client computer. At the login screen, you will either be looking at name/password fields or a user list that now has "Other…" at the bottom. Login with a network account and that account should be properly mapped to a network-based home directory.

E. Connecting a 10.3.8 client to your server

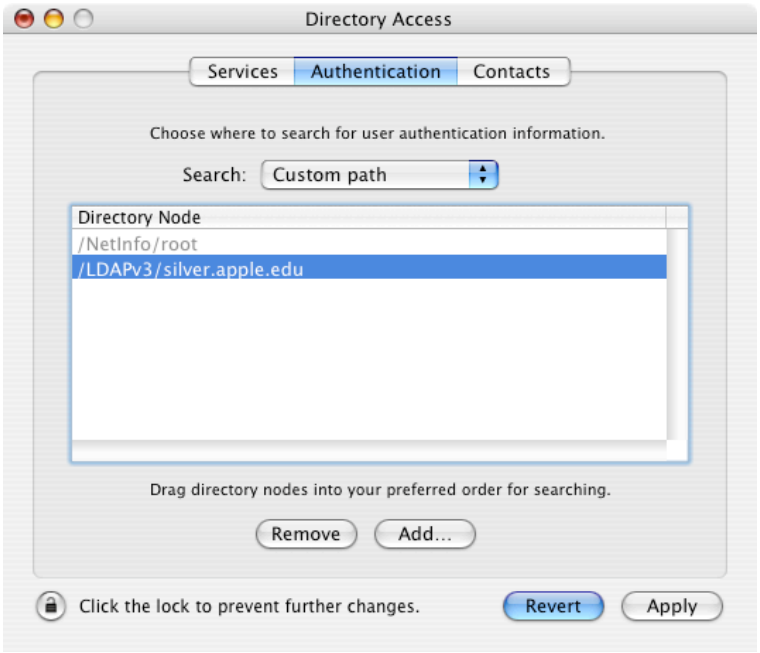
1. Connecting a 10.3.8 client to your Tiger Server requires the exact same steps that you have probably already taken when connecting to your Panther Server (10.3). Version 10.3.4 or higher is required to make this work, with 10.3.8 appearing to be the most stable.
2. First, be sure that your client is on the same page with your server in terms of DNS. From the client, launch /Applications/Utilities/Terminal.
3. Use the commands from page 2 of this document to ensure that DNS is resolving as expected. When these two lookups resolve, this is proof that your DNS has a correct forward and reverse entry for your server.
4. Launch /Applications/Utilities/Directory Access.
5. We're again going to use the LDAPv3 plugin for connectivity.



6. Double-click on the LDAPv3 plugin in order to configure it.
7. 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.



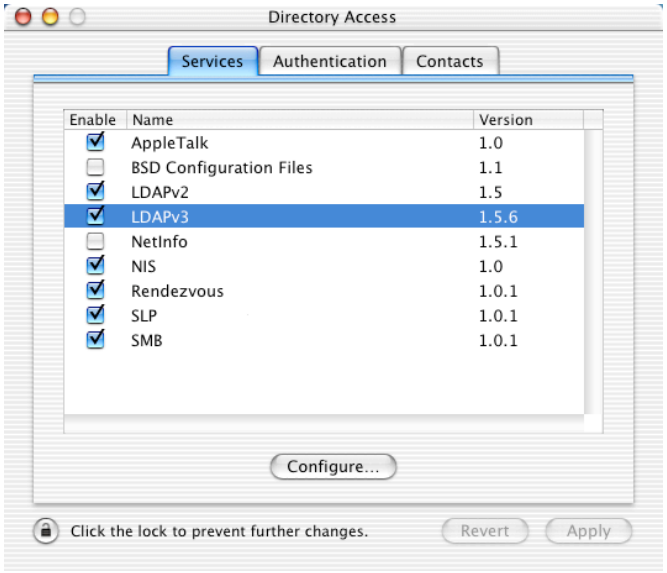
8. Don't forget to uncheck the box at the top so that you're not pulling LDAP info from a "DHCP-supplied LDAP Server."
9. There is no need to touch the "From Server" pull down menu under LDAP Mappings.
10. Click OK when you have everything set.
11. Now that your server information is in place, we need to place it in the authentication path. Click on the Authentication tab.
12. This is the default setting. Change the Search criteria from "Automatic" to "Custom path."
13. Click "Add" to add new authentication criteria.
14. You now should see the option to add your LDAP directory. Highlight it and click the "Add" button.
15. Once you add it, your custom authentication path should look like this.



16. Click the apply button.
17. 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.

F. Connecting a 10.2.8 client to your client management server.

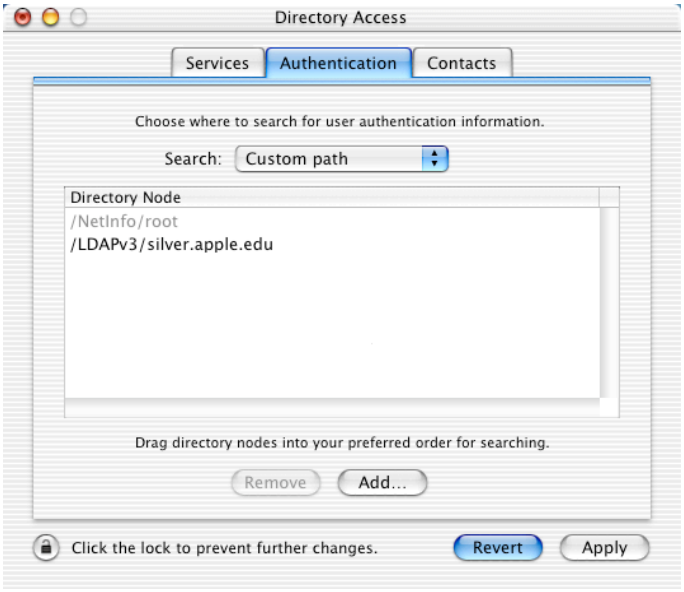
1. Notice that the title of this section is not "Connecting a 10.2 client." This is because your 10.2 clients must be updated to at least 10.2.4 for this to work. Unless something is preventing you from further updates, going to 10.2.8 can only help.
2. At your client workstation, you'll need to again 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 client management 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, which is "dc=silver,dc=apple,dc=edu" without the quotes around it.
7. For my server, my search base suffix was based on my fully qualified domain name, which was silver.apple.edu. If your domain is "school.k12.ks.us," and you want your search base to match that, 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.
12. All done!

Remember that this is just a quickstart guide. It's sole intention is to get you up and running quickly with client management 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 (available now at http://www.afp548.com). Some excellent new books are available that will greater strengthen your knowledge of Mac OS X Server. For those that are fairly new to the server scene, the following books will be of great value (Amazon.com has these now).

"Mac OS X Server Essentials" by Schoun Regan
"Mac OS X Server 10.4 Tiger" by Schoun Regan
"Mac OS X Server 10.3 Panther" by Schoun Regan

You veterans that love spending the majority of your time at the command line and knowing everything that goes on "under the hood" should consider Michael Bartosh's new book. It covers planning, deployment and security in great depth.

"Essential Mac OS X Panther Server Administration" by Michael Bartosh

This document was written with greater accuracy due to the fact that a good pal took the time to read it carefully and test the same steps in his environment. I owe a big thanks to Jeff Ochsner for his time and attention to detail. Joel Rennich, thanks to you as well for clarifying some points that needed, well, some clarifying.

Comments and corrections for this document are welcome. Send me a line at ccarson@apple.com.