Configuring Active Directory Binding for OS X (10.4.x) within Miami Dade Schools

1) Login to the Mac OS X (10.4.x) workstation with a local administrative account.

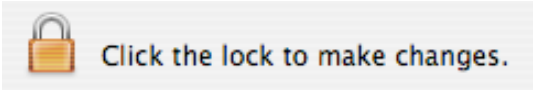
2) Open (double-click) the hard drive icon that appears on the desktop:

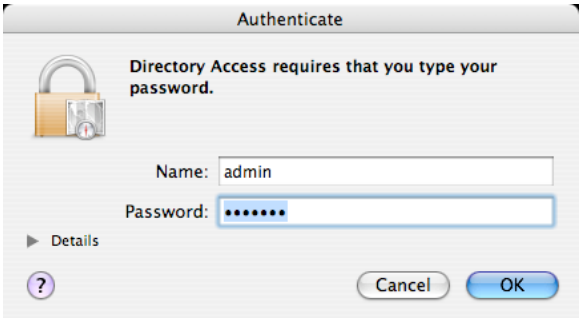
3) Open (double-click) the Applications folder within the Macintosh HD window

4) Open (double-click) the Utilities folder within the Applications window:

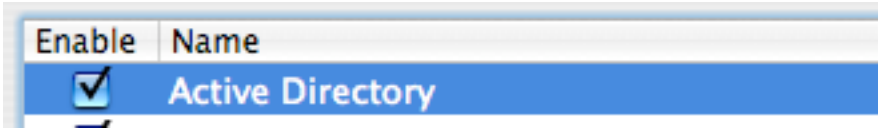
5) Open (double-click) the “Directory Access” program within the Utilities window:

6) Click the lock icon in the lower left of the window to ‘unlock’ the Directory Access window and enter the local administrator’s credentials:



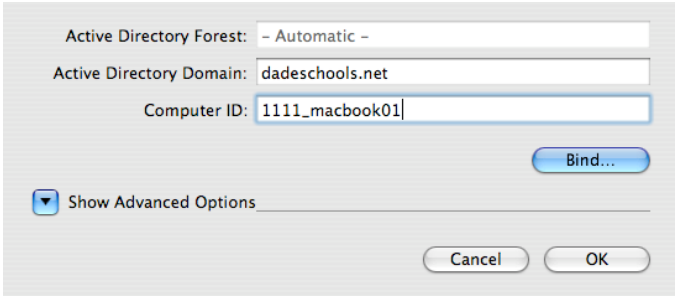


7) Click the Enable checkbox next to Active Directory in the list within the Services section of the Directory Access window:

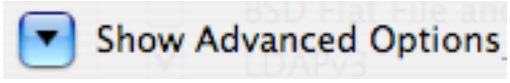


8) Click the Configure button at the bottom of the Services section of the Directory Access window:

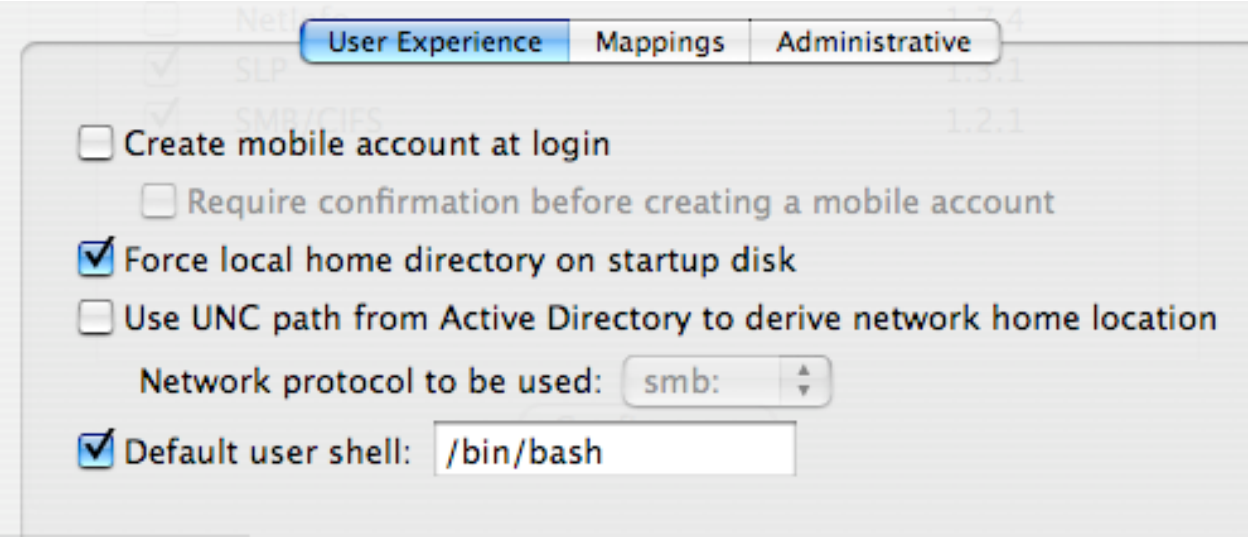
9) In the slip that appears, enter 'dadeschools.net' for the Domain and enter a computer ID that complies with the dadeschools.net naming standards (ie: Computer names start with site/location ID numbers. TIP: Avoid utilization of the '-' (hyphen) when naming your computer records as there are some underlying NetBios issues that can otherwise occur.



10) NOTE: DO NOT CLICK BIND YET, Instead, click the 'down arrow' to reveal Advanced options:



11) *User Experience:* The user experience section defines how the workstation will behave when a user authenticates with their Active Directory credentials.



Option A: Local Home Folders
With local home folders, each Active Directory user who logs in has a home folder on the Mac OS X startup disk. In addition, the user's network home folder, if defined in Active Directory, is mounted as a network volume, like a share point. The user can copy files between this network volume and the local home folder.

By default, binding to Active Directory will cause a local home directory to be placed into /Users on the workstation. This is done to provide storage for the user files, as the initial 'presumption' is that there is no defined user home directory within the users' record within Active Directory.

Option B: Mobile Accounts
You can start or stop using mobile Active Directory user accounts on a computer that is configured to use Directory Access's Active Directory plug-in. Users with mobile accounts can log in using their Active Directory credentials while the computer is not connected to the Active Directory server. The Active Directory plug-in caches credentials for a user's mobile account when the user logs in while the computer is connected to the Active Directory domain.

To enable mobile accounts, click "Create mobile account at login" and optionally click "Require confirmation before creating a mobile account."

- If both options are selected, each user decides whether to create a mobile account during login. When a user logs in to Mac OS X using an Active Directory user account, the user sees a dialog with controls for creating a mobile account immediately or logging in as a network user.

- If the first option is selected and the second option is unselected, mobile accounts are created automatically when users log in.
- If the first option is unselected, the second option is disabled.

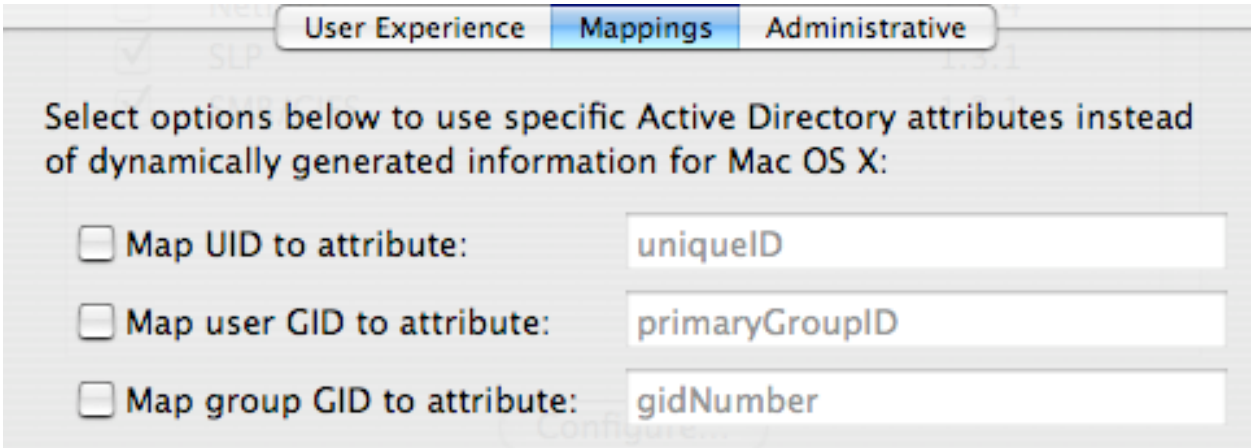
Option C: Network Home Folder
With network home folders, a user's Windows network home directory is mounted as the Mac OS X home folder when the user logs in. *NOTE:* This scenario requires a network home folder be defined in their user profile within Active Directory.

To use Active Directory's standard attribute for the home folder location, select "Use UNC path from Active Directory to derive network home location" and choose the protocol for accessing the home folder.

- If your home folders are located on a Windows file server, choose "smb:" to use the standard Windows protocol, SMB/CIFS.
- If your home folders are located on a MacOS X file server, choose "afp:" to use the standard Macintosh protocol, AFP.

12) Leave “Default User Shell” checked ‘on’ and set to /bin/bash

13) *Mappings:* On a computer that's configured to use Directory Access's Active Directory plug-in, you can specify an Active Directory attribute that you want mapped to Mac OS X's unique attributes. Usually the Active Directory schema must be extended to include an attribute that's suitable for mapping. As the Dadeschools.net domain schema has not been extended, the Mappings section of the Active Directory tools in Mac OS X should be left ‘unset’ as shown below:



14) *Administrative:* With the administrative options of the Active Directory settings, you may specify a preferred domain controller, what groups can administer the OS X Workstation, and allow cross domain authentication.

Preferred domain controller:
On a computer that's configured to use Directory Access's Active Directory plug-in, you can specify the DNS name of the server whose Active Directory domain you want the computer to access by default. If the server becomes unavailable in the future, the Active Directory plug-in automatically falls back to another nearby server in the forest. If this option is unselected, the Active Directory plug-in automatically determines the closest Active Directory domain in the forest.

To enable this option, select "Prefer this domain server" and enter the DNS name of the Active Directory server. (ie: 1111dc1.dadeschools.net)

Active Directory groups that can administer the OS X Workstation
You can identify Active Directory group accounts whose members you want to have administrator privileges for the computer. Users that are members of these Active Directory group accounts can perform administrative tasks such as installing software on the Mac OS X computer that you are configuring.

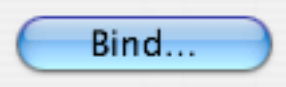
select "Allow administration by," then change the list of Active Directory groups accounts whose members you want to have administrator privileges.

- Add a group by clicking the Add button (+) and entering the Active Directory domain name, a backslash, and the group account name (for example, DADESCHOOLS\Domain Admins, DADESCHOOLS\Enterprise Admins, DADESCHOOLS\1111SiteAdmins).
- Remove a group by selecting it in the list and clicking the Remove button (-).

Controlling authentication from all domains in the Active Directory forest

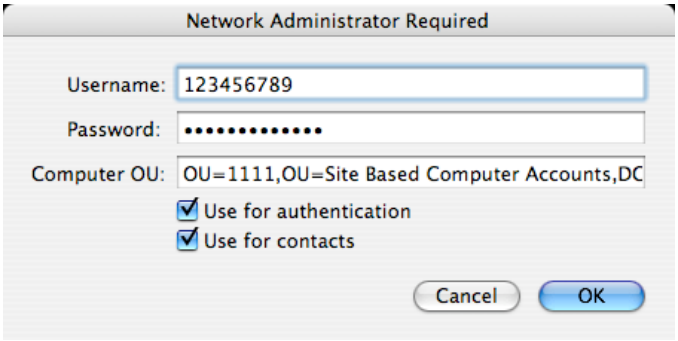
- If you select "Allow authentication from any domain in the forest," you can add the Active Directory forest to the computer's custom search policies for authentication and contacts. When adding to a custom search policy, the forest appears in the list of available directory domains as "/Active Directory/All Domains." (This is the default setting.)
- If you deselect "Allow authentication from any domain in the forest," you can add Active Directory domains individually to the computer's custom search policies for authentication and contacts. When adding to a custom search policy, each Active Directory domain appears separately in the list of available directory domains.

15) Click the BIND button in the middle of the Directory Access window:



16) If prompted, enter the local administrative credentials for the OS X Workstation:

17) Enter the credentials of an Active Directory account with binding rights to the domain in the Username and Password fields provided.



18) In the Computer OU field, enter the proper 'path' to the appropriate container within the dadeschools.net Active Directory structure:

In the sample screenshot above, this is:

"OU=1111,OU=Site Based Computer Accounts,DC=dadeschools,DC=net"

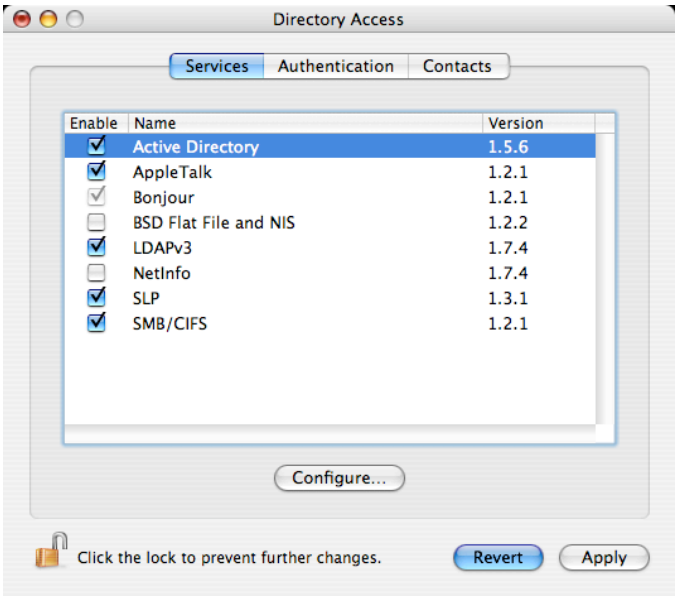
If you've created any sub-OUs within your site, ie: "Apple", then this entry would change slightly to:

"OU=Apple,OU=1111,OU=Site Based Computer Accounts,DC=dadeschools,DC=net"

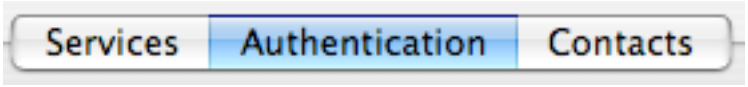
19) Click OK, and the Mac OS X workstation will proceed through 5 steps to bind to the Active Directory domain.

20) When complete, the "Bind" button will change state to "UnBind"

21) Click the OK button in the bottom right to return to the main Directory Access window view:



22) Click the Authentication tab at the center top:

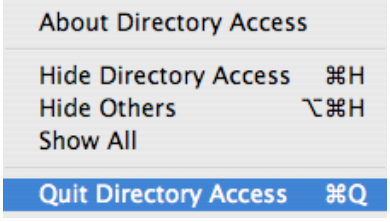


Beneath /NetInfo/DefaultLocalNode should be “Active Directory/All Domains” in the list.

This signifies that immediately after hunting the OS X local user database, the workstation will seek to authenticate against the Active Directory bindings just defined.

23) Click the Apply button in the bottom right of the Directory Access window to apply all your changes.

24) Exit/Quit the Directory Access program by choosing “Quit Directory Access” from the Directory Access menu in the upper menubar:



25) Log out of the OS X Workstation to the login window by choosing “Log out...” from the bottom of the Apple menu in the upper left corner of the screen:

26) At the login window, click a few times with the mouse on the grey colored text below “Mac OS X”

This technique reveals some basic status information about the workstation:

- Computer Name
- OS X Version
- OS X Build
- Serial Number of the workstation
- TCP/IP address of the workstation
- Network Account availability
- Current date and time of the workstation

If you see “Network Accounts Available” with a ‘green’ status indicator, you can enter an Active Directory user account and password to login to the workstation.

If you see “Network Accounts Unavailable” with a ‘red’ status indicator, you will only be able to login with the local user accounts on the workstation as there is a problem reaching the directory service.

This ‘feature’ is available on OS X and OS X Server login windows: