Xinet TechNote 218: Directory Services (Active Directory) Authentication with FullPress and WebNative – Mac OS X Server (Tiger)

By: Keigo Kiyohara, Hitesh Chhatrala

Last modified: 10/31/07

Note: these instructions were written for FP 15.03 / WNV 8.03. If you are running a older version, you may want to upgrade.

Overview

1) Bind your OS X Server to Active Directory.

2) Install FullPress and WebNative

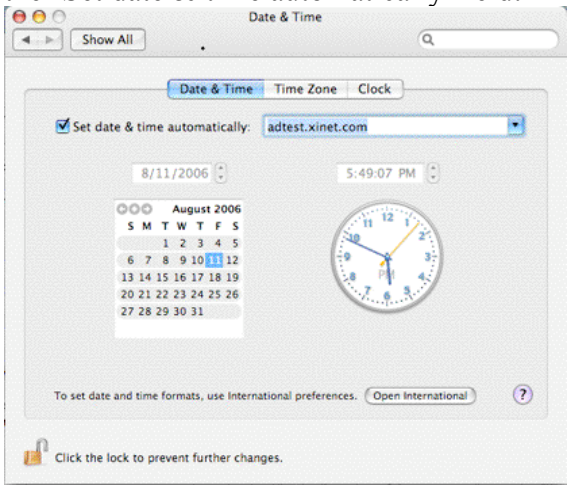
Binding Mac OS X Server (Tiger) to a Windows Server 2003 Active Directory

These directions are a rough guideline on how to bind a Mac OS X Tiger Server to Active Directory. Our test setup is a 10.4.7 Server and Windows Server 2003 Standard Edition Service Pack 1.

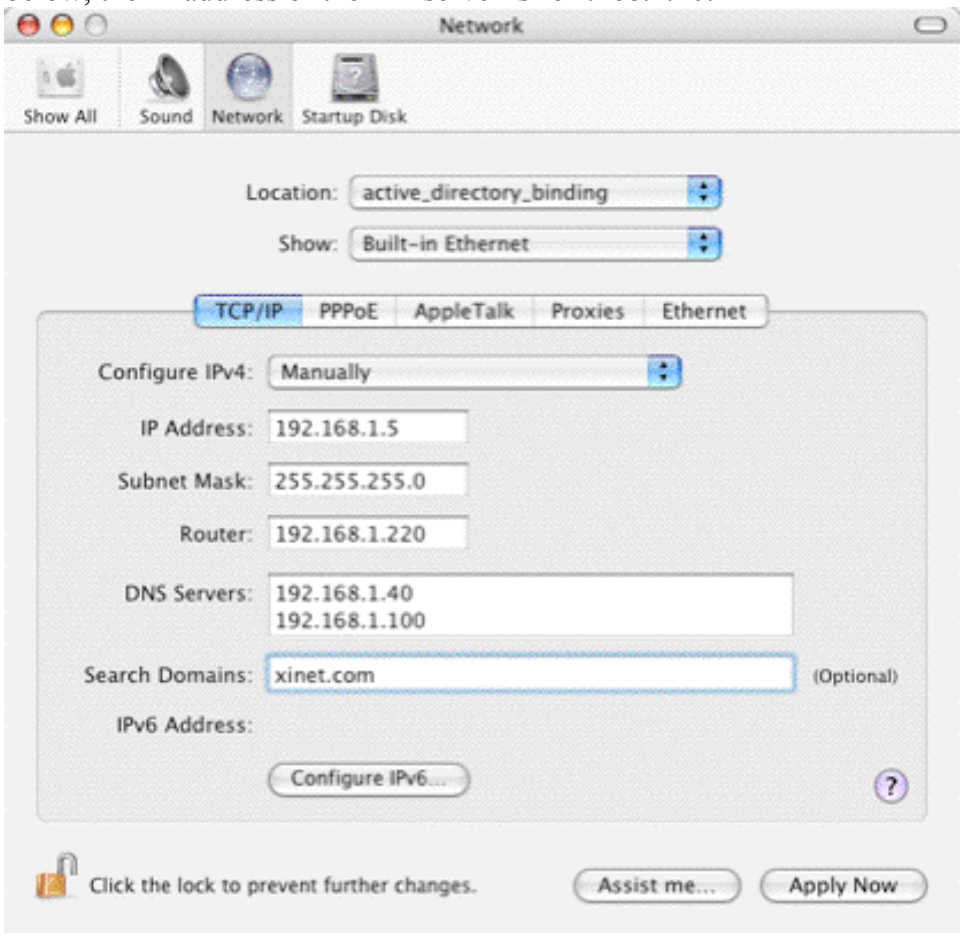
Be aware that versions prior to 10.4.7 sometimes had problems binding to an Active Directory server. We expect that 10.4.7 and all future releases will work correctly, but there is always the possibility that problems will arise in new operating system versions. We will add known problems to this technote in the "Potential Problems' section at the end of this document. Be sure to read that section before starting to install.

Preparation notes:

- Be sure the date / time on your OS X server is synced to the AD server. One way to do this is to change System Preference | Date & Time. Use the domain name in the 'Set date & time automatically'field:

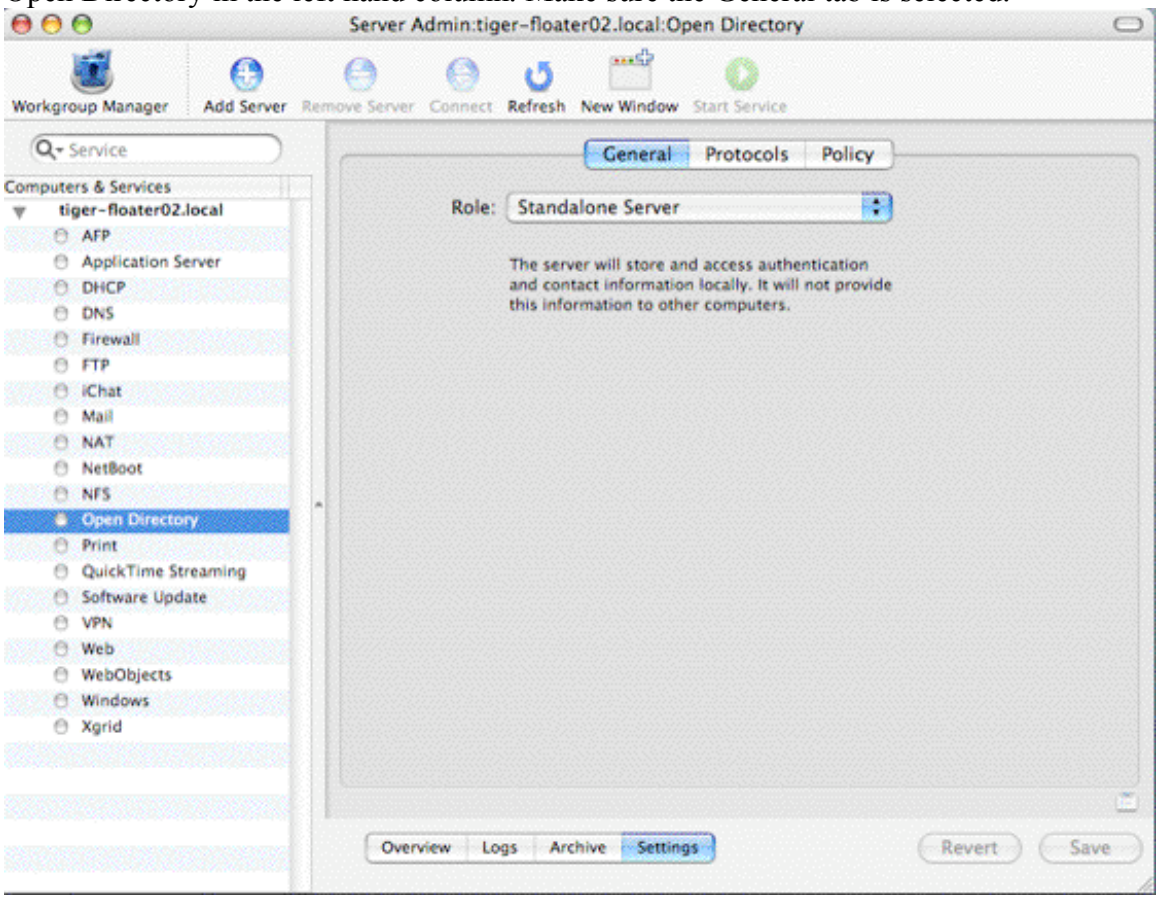


- Make sure you have DNS set up properly on your OS X server. In the screenshot below, the IP address of the AD server is 192.168.1.40.

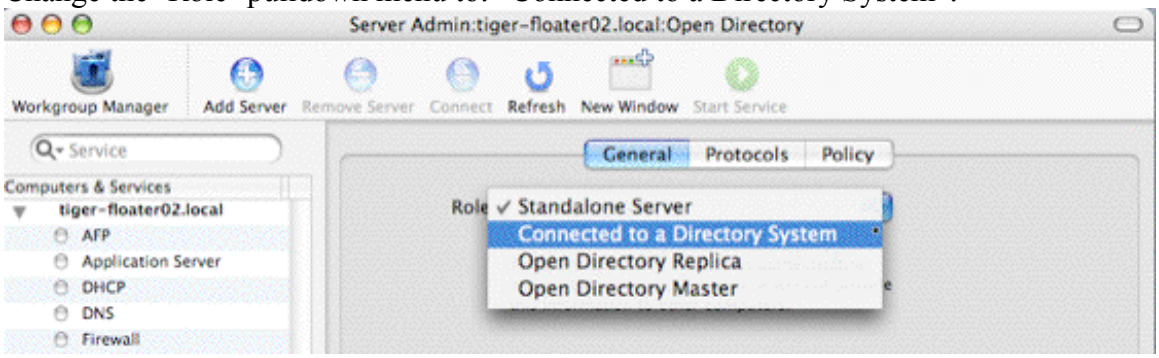


Once the preparation steps are complete, you are ready to bind your server to Active Directory.

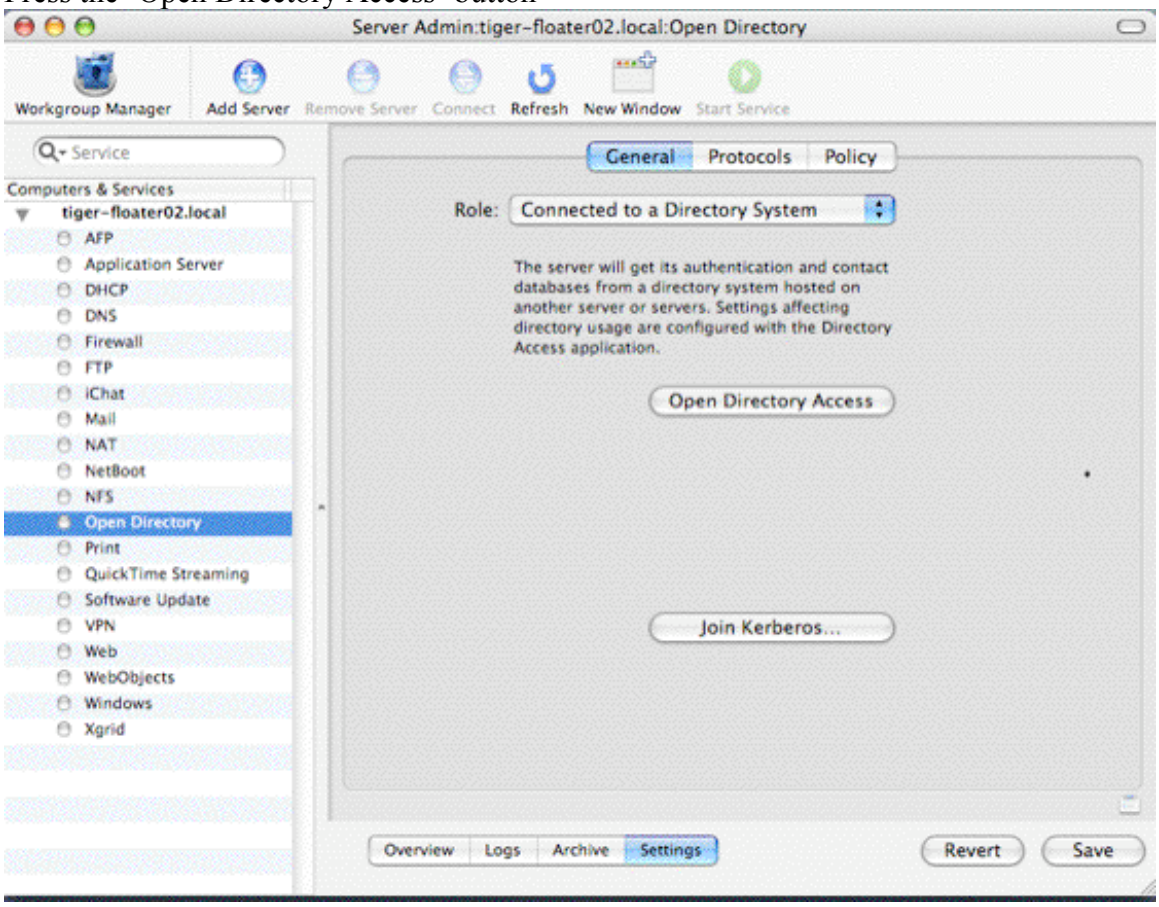
Launch Applications | Server | Server Admin. Authenticate with an admin account. Click Open Directory in the left hand column. Make sure the General tab is selected.



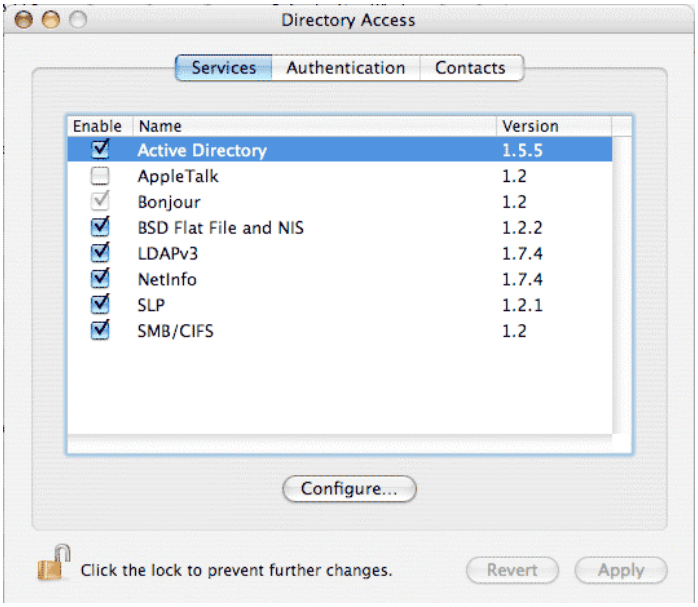
Change the 'Role' pulldown menu to: "Connected to a Directory System".



Press the ‘Open Directory Access’ button



Select the Active Directory checkbox. Then, while it is highlighted, click the “Configure” button.



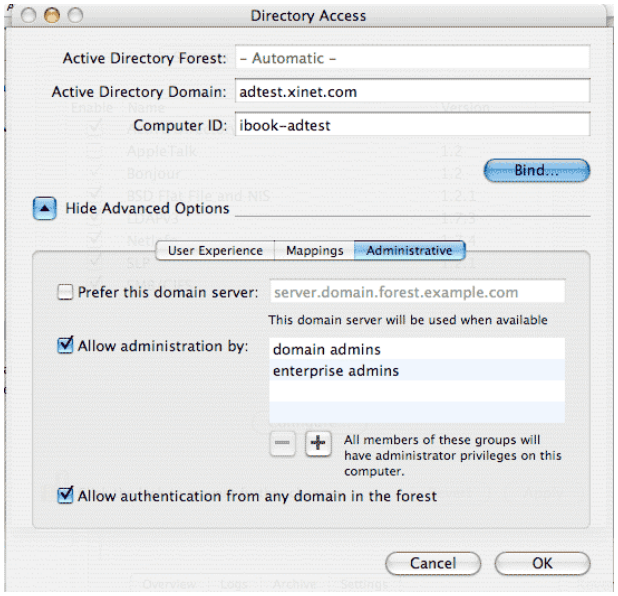
Press the arrow button next to ‘Show the Advanced Options’ and select the Administrative tab. Your screen should look similar to the one below.

Fill out the following fields:

Active Directory Domain: the FQDN (fully qualified domain name) of your AD domain. Note: It does not include the name of the actual AD server itself. In this example, we excluded the server name ‘2003svr’.

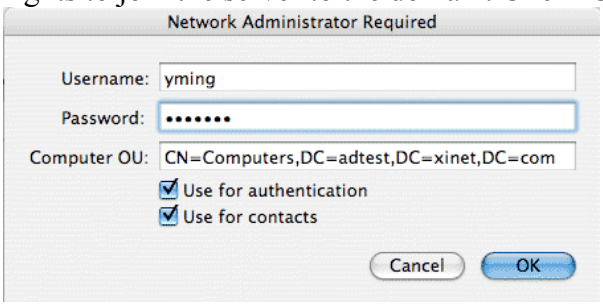
Computer ID: the hostname of the OS X server that is being bound to AD. This is listed in the Sharing System Preference pane or from the command line, when typing the hostname command.

Then, select the arrow next to ‘Show Advanced Options’ Select the boxes next to ‘Allow administration by’ and ‘Allow authentication from any domain in the forest.’ Click ‘Bind’.

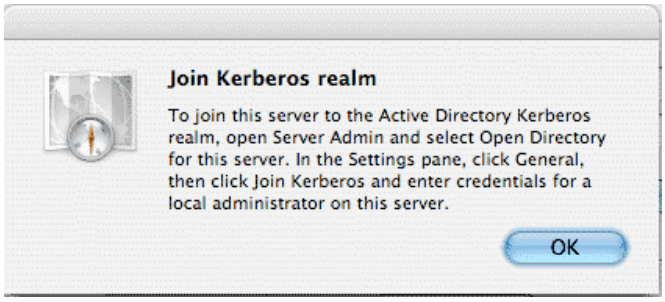


Then, you may be asked to authenticate as a System Administrator. This is an account on the OS X server. Enter the information, and click ok.

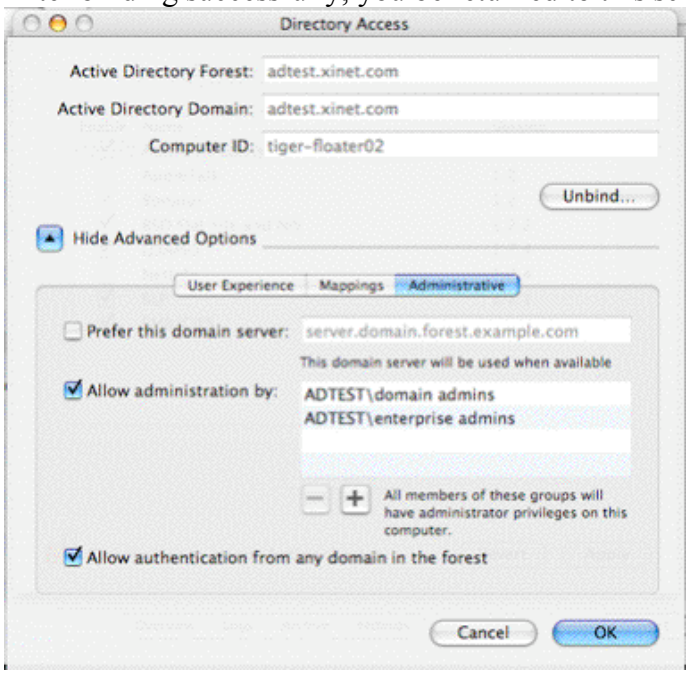
In the window that opens, enter the username / password for an AD account that has rights to join the server to the domain. Click ‘OK’.



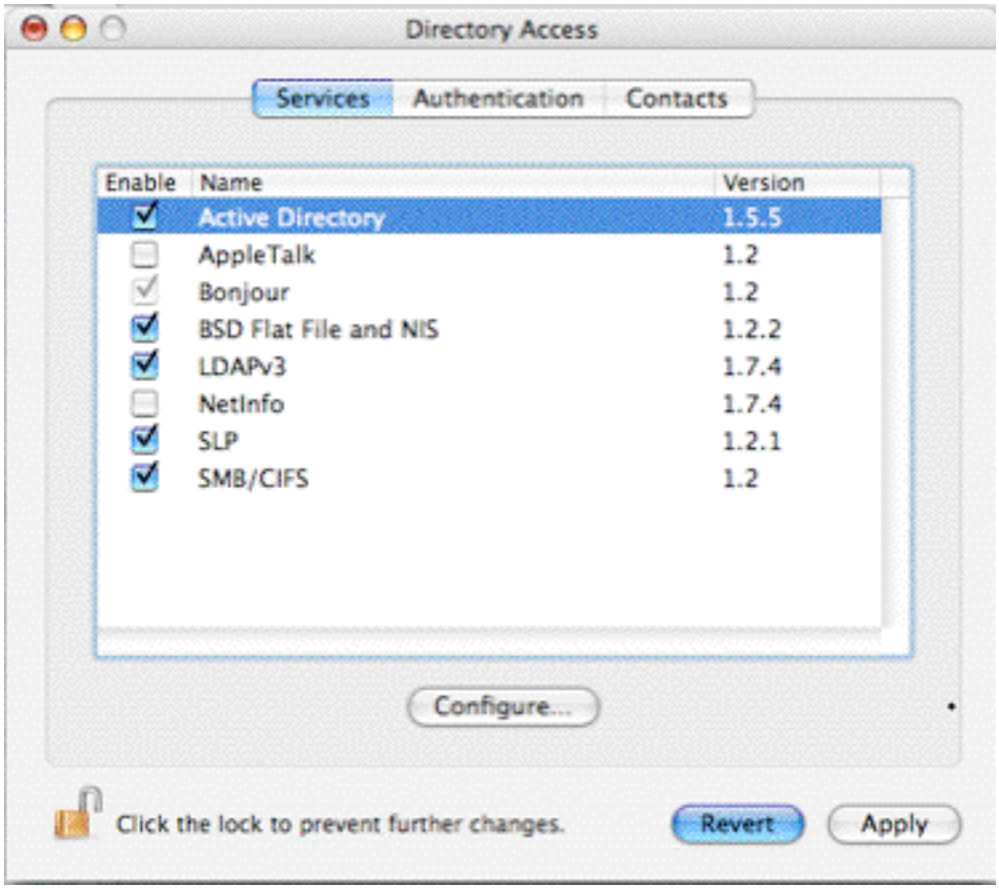
You will see the server go through a five step process as it binds to the AD server. If you are successful, you should get the result shown below. Click ‘OK’.



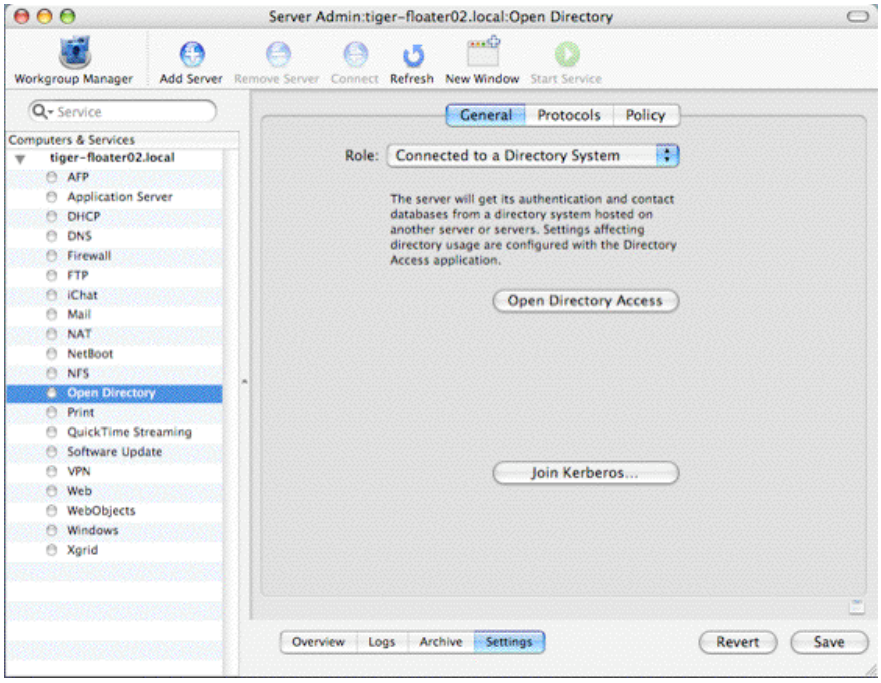
After binding successfully, you be returned to this screen. Click ‘OK’.



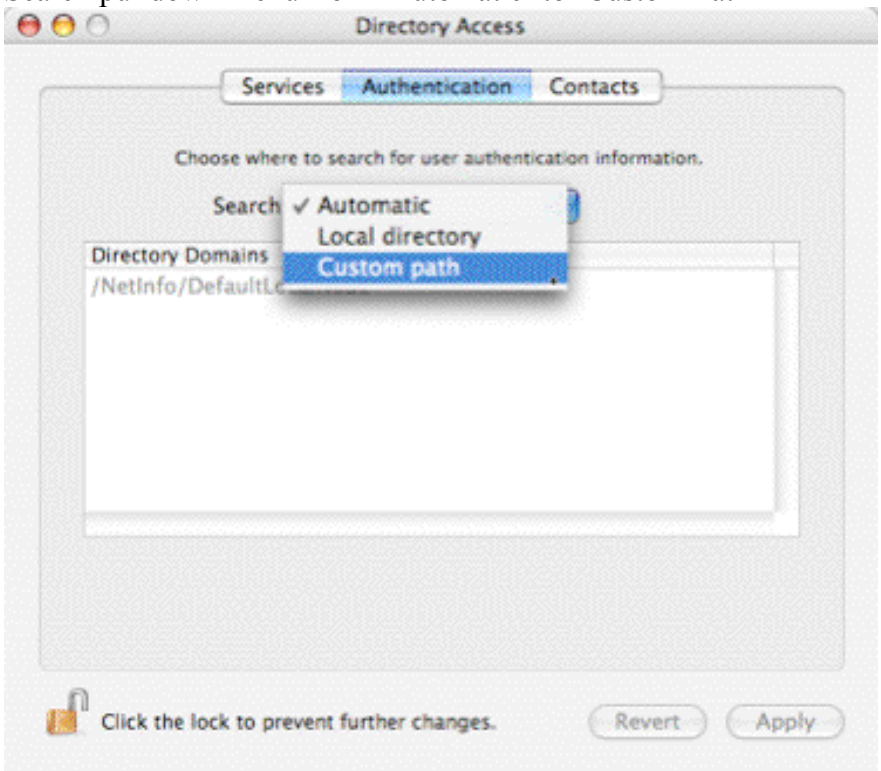
You will be returned to the ‘Directory Access’ window. Click ‘Apply’ then close the window.



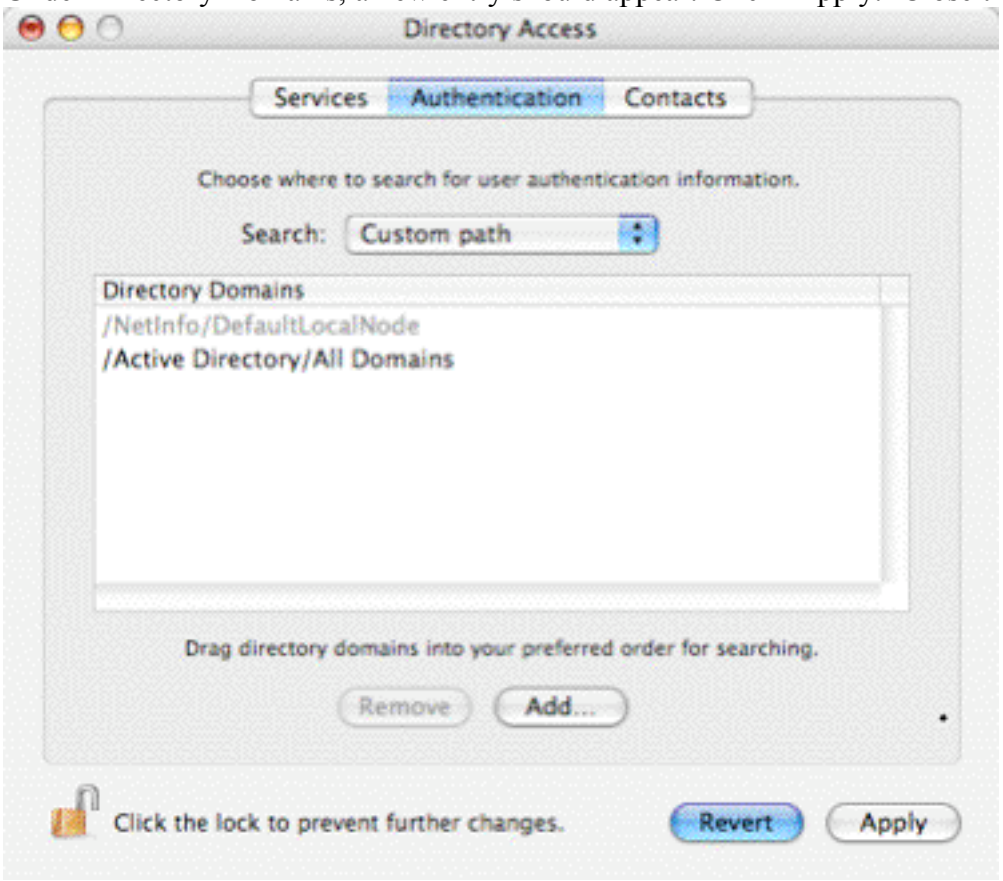
Click the ‘Save’ button in the next screen.



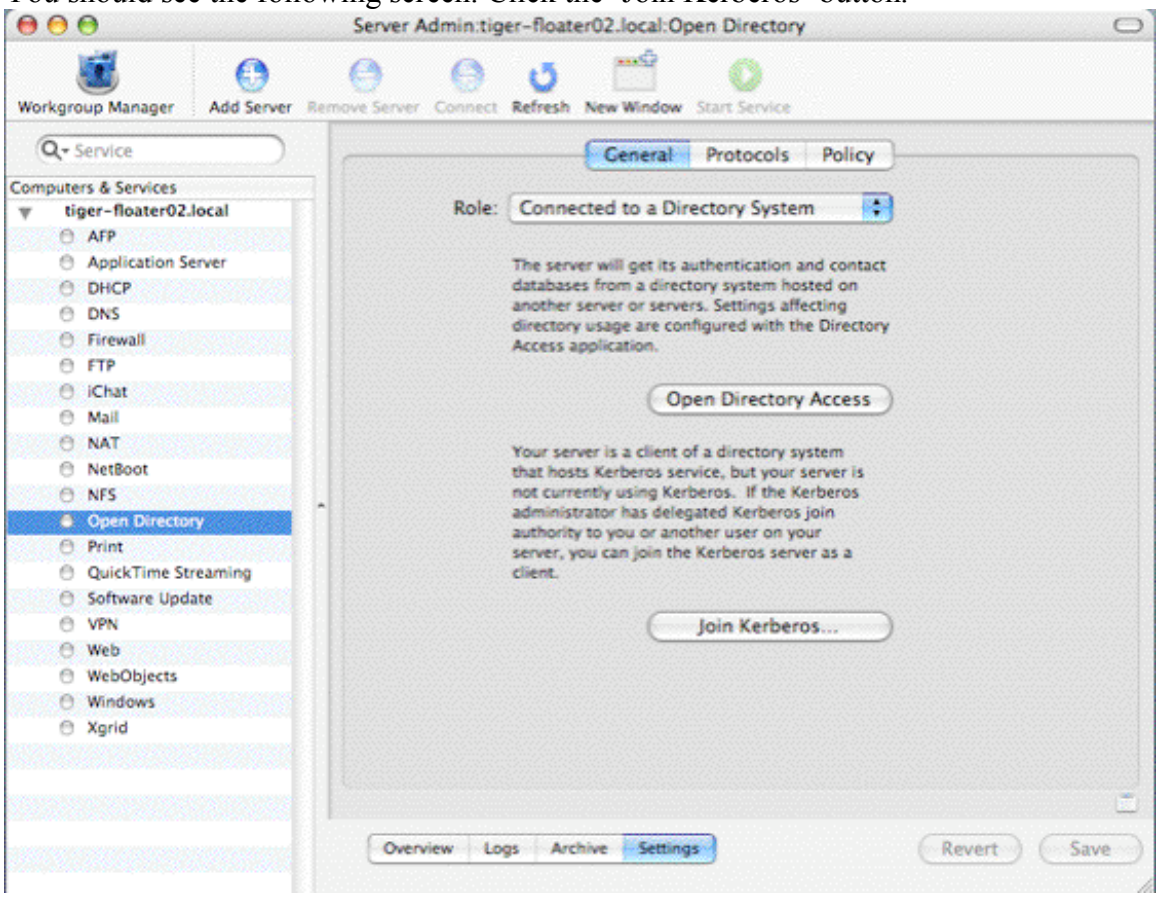
Click the ‘Open Directory Access’ Button. Click on the ‘Authentication’ tab. Change the Search pulldown menu from ‘Automatic’ to ‘Custom Path’



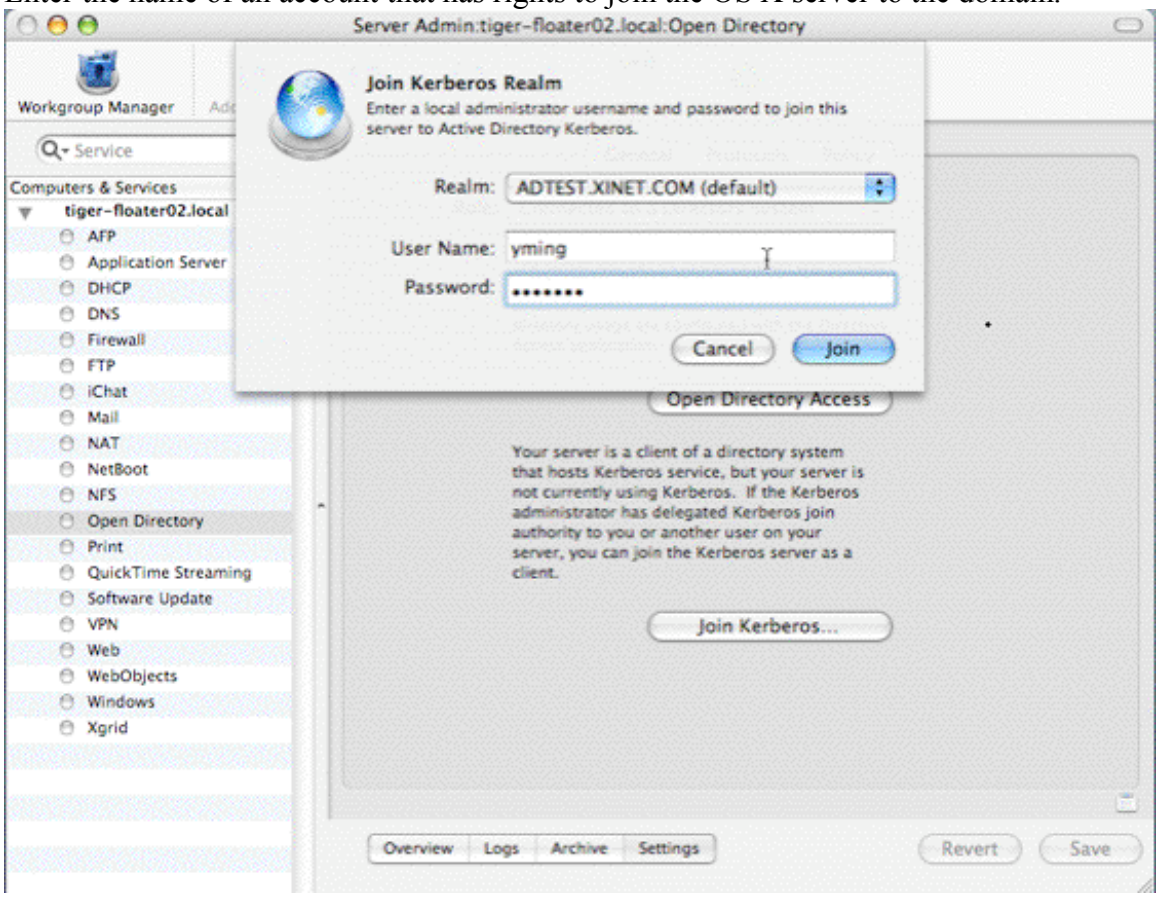
Under Directory Domains, a new entry should appear. Click ‘Apply.’ Close the window.



You should see the following screen. Click the ‘Join Kerberos’ button.



Enter the name of an account that has rights to join the OS X server to the domain.



Once that happens, your OS X server should be bound to Active Directory.

To test it, enable ssh (System Preferences | Sharing | Remote Login) on the OS X server. Then, from a separate unix workstation, you should be able to login to the OS X FullPress server via ssh using an AD account.

Install FullPress and WebNative

Install and license FullPress and WebNative. At this point, FullPress will be pulling user information from Active Directory.

In order for WebNative to pull the user information from Active Directory, you will need to create a blank file named system.userlist by running this command in the terminal:

FPServer# touch /usr/etc/webnative/system.userlist

Once you do this, any local accounts on the OS X server will no longer appear in WebNative Administration. Only accounts from the AD server will appear.
Also, the "New Users" and "Delete Users" tabs will no longer be accessible under the "Users" tab. This is because all administration of users should be done on the AD Server.

Note:
In the past, creating a file called system.grouplist was an option to help speed up the time it took to display users. However, that functionality has been incorporated into system.userlist. If you are upgrading from past versions to 8.03, we recommend you to log in WebNative as nativeadmin and visit the 'Groups' tab; any editing, such as a simple save, will prompt the system to incorporate groups information into system.userlist file.

As of 15.03, in some cases FullPress will also consult system.userlist file to filter out groups that are not in it. If you don't want this behavior, you can modify the xinet services file and add this option '-groupfile no' as the first option to ksd.

Possible Issues

- There might be an issue re-binding a machine with a name that was used previously. For instance, say a machine called "XYZ" was bound to an AD server. XYZ is then removed from the network. Then another machine is named "XYZ" and made to bind to the AD server. At this point, we encountered significant problems making the binding work. We haven't found the true source of this problem.

- There was 10.3.9 OS X servers when domain name included ".local" in the suffix. We haven't confirmed if this problem still exists in 10.4.7.

- There is an issue with hostnames longer than 20 characters. This includes the .local suffix added to the name by OS X. For example, tiger-svr-intel-mini appears in Server Admin as tiget-svr-intel-mini.local.

  If you have a hostname longer than 20 characters, you may get a misleading error when binding: