

Integrating Mac OS X With Active Directory

 **Apple Computer, Inc.**

© 2002 Apple Computer, Inc. All rights reserved.

Under the copyright laws, this publication may not be copied, in whole or in part, without the written consent of Apple.

The Apple logo is a trademark of Apple Computer, Inc., registered in the U.S. and other countries. Use of the “keyboard” Apple logo (Option-Shift-K) for commercial purposes without the prior written consent of Apple may constitute trademark infringement and unfair competition in violation of federal and state laws.

Apple, the Apple logo, and Mac are trademarks of Apple Computer, Inc., registered in the U.S. and other countries. Finder is a trademark of Apple Computer, Inc.

062-9329/02-27-02



Contents

Introduction	5
Directory Services	5
Prerequisites for Integrating Mac OS X With Active Directory	6
This Document	6
The Scenarios	7
Using Mac OS X Server as an AFP File Server	7
Using Mac OS X Server to Host Home Directories	9
Setting Up the Scenarios	11
Setting Up the AFP File Server Scenario	12
Setting Up the Windows Server	12
Modifying the Active Directory Schema	13
Creating User Records	13
Setting Up Mac OS X Directory Service Mappings	13
Enabling Secure LDAP Authentication	13
Setting Up Share Points and Permissions	13
Setting Up the Home Directories Scenario	14
Setting Up the Windows Server	15
Modifying the Active Directory Schema	15
Creating the mounts Class	16
Editing mounts Properties	18
Creating a mounts Search Base	20
Creating a mounts Record	21
Creating User Records	25
Setting Up Mac OS X Directory Service Mappings	26
Enabling Secure LDAP Authentication	26

Setting Up Home Directories	27
Logging In	28
The Remainder of This Paper	29
Updating Active Directory	29
Installing Windows 2000 Tools	29
Modifying the Active Directory Schema	30
Creating New Attributes	31
Creating User Records	34
Setting Up Mac OS X Directory Service Mappings	35
Enabling Secure LDAP Authentication	42



Integrating Mac OS X With Active Directory

Introduction

This document describes how you can use the information stored in Microsoft's Active Directory to authenticate Macintosh users and provide file services and home directories for them on Mac OS X Server. To do so, you'll take advantage of the Mac OS X directory services architecture.

Directory Services

A directory service provides a central repository for information about the systems, applications, and users in an organization. In education and enterprise environments, a directory service is the ideal way to manage users and computing resources. Organizations with as few as 10 people can benefit by deploying a directory service.

Directory services can be doubly beneficial. They centralize system and network administration, and they simplify a user's experience on the network. With a directory service, information about all the users—such as their names, passwords, and preferences—as well as printers and other resources on a network can be maintained in a single location rather than on each computer on the network. Using a directory service can reduce the system administrator's user management burden. In addition, users can log in to any authorized computer on the network, with their Desktop customized using their individual preferences, and easily locate and use authorized network resources.

Apple has built an open, extensible directory services architecture into Mac OS X and Mac OS X Server. This architecture directs system software and applications to either Apple's NetInfo (the directory that ships with Mac OS X Server) or an LDAP (Lightweight Directory Access Protocol) directory located on the network. NetInfo is an easy-to-deploy, scalable directory service for Macintosh networks. LDAP is an open standard commonly used in mixed environments. By adding LDAP support, Apple provides customers with the ability to easily integrate Mac OS X and Mac OS X Server systems into most managed networks.

In addition, it is now possible to integrate Mac OS X computers into environments based on Microsoft's Active Directory. This support lets you maintain Mac OS X user names and passwords in Active Directory, authenticate Mac OS X users with Active Directory, and allow users to mount their network home directory based on information stored in Active Directory.

Today, directory services are an essential part of any computing infrastructure. Directory services fill a number of critical roles, including managing workgroups, workflows, employee directories, and hardware and software resources. With Mac OS X's open directory services architecture and built-in support for open standards, Mac OS X desktops and servers can now leverage directory services wherever they reside—in a Macintosh NetInfo directory, in a Microsoft Active Directory, or in an enterprise LDAP directory.

Prerequisites for Integrating Mac OS X With Active Directory

For readers not familiar with Mac OS X directory services, we recommend the *Mac OS X Server Administrator's Guide* and the white paper entitled *Understanding and Using NetInfo*. Both are available at www.apple.com/macosx/server

The IETF and various LDAP Directory Service vendors have a number of valuable resources to help readers not familiar with the LDAP standard and associated schema.

Mac OS X uses the LDAP protocol, not Microsoft's proprietary Active Directory Services Interface (ADSI), to connect to Microsoft's Active Directory. This paper assumes that you have in-depth knowledge of Active Directory, especially the ways in which it needs to be configured to support standard LDAP schema definitions. Because the primary means of accessing Active Directory is ADSI, using LDAP as an alternative implies a thorough working understanding of the use and limitations of the LDAP support provided by Active Directory.

The instructions for working with the Windows server and Active Directory in this document assume that you are familiar with Windows 2000 and Active Directory. They do not show every step you use to update Active Directory. If you need additional assistance, consult an individual with Windows 2000 and Active Directory expertise, refer to the documentation for these products, or go to this Web site:

www.microsoft.com/support/

This Document

This document describes how information stored in Microsoft's Active Directory can be used to authenticate Mac OS X users and provide these users with network home directories and file services using Mac OS X Server and the Apple Filing Protocol (AFP).

The Scenarios

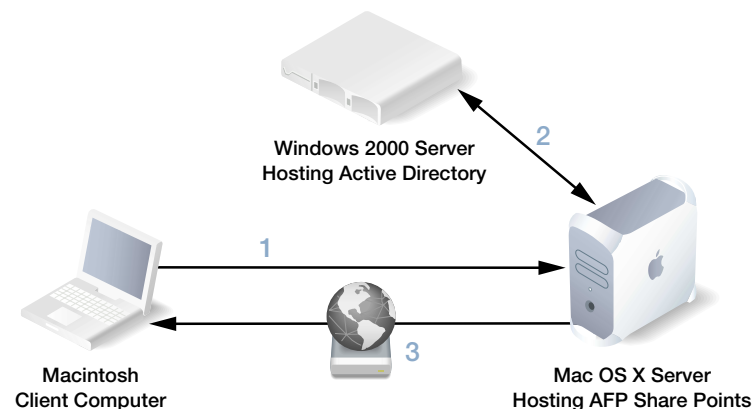
This paper presents two scenarios for Active Directory integration. In each scenario, Mac OS X Server is used to host files for Macintosh computer users:

- In one scenario, Mac OS X Server is an AFP file server.
When users connect to the server to access files, they are authenticated using Active Directory information and any share points the user is authorized to access are mounted. Recall that a share point is a hard disk (or hard disk partition), folder, or CD that contains files and folders you want particular users to share.
- In another scenario, Mac OS X Server hosts AFP home directories for Mac OS X users.
When users log in to Mac OS X computers, they are authenticated using Active Directory information and their home directories are mounted. After login is complete, they can access their home directories from the Finder by choosing Home from the Go menu or clicking Home in a Finder window. Their home directories are visible in the Finder under the Network globe.

In both scenarios, you set up three kinds of computers to provide authentication and file access: a Windows 2000 server hosting Active Directory, a Mac OS X Server hosting user files, and Macintosh computers at which users log in.

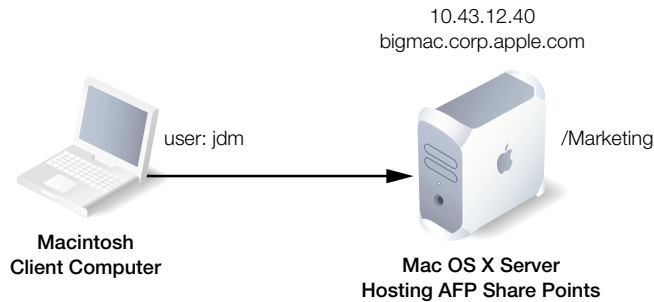
Using Mac OS X Server as an AFP File Server

In this scenario, a user connects to Mac OS X Server from a Mac OS 9 or Mac OS X computer to access files stored in a share point on the server.



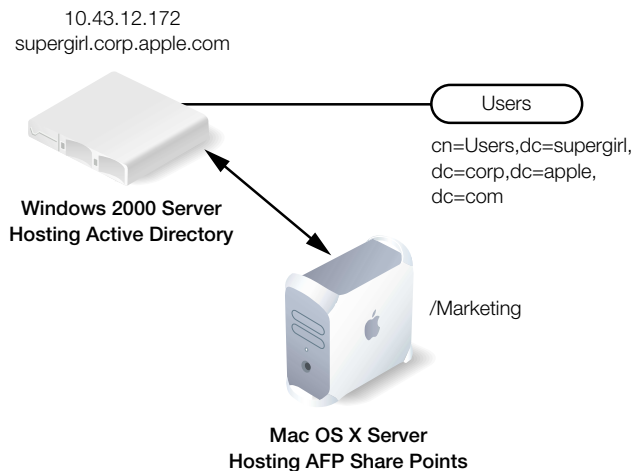
The numbers in this figure illustrate the sequence of interactions that occur between the time a user connects to Mac OS X Server and one or more share points are mounted on the user's computer:

- 1 Connecting to Mac OS X Server. After logging in to his Mac OS 9 or Mac OS X computer, the user requests a connection with Mac OS X Server. First, the user identifies the server, usually by using the Chooser on Mac OS 9 computers or choosing Connect to Server from the Go menu on Mac OS X computers. Then the user enters his user name and password.



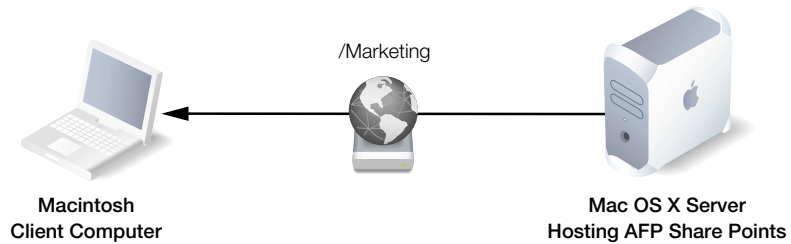
In this example, the Mac OS X Server has the IP address 10.43.12.40 and the name bigmac.corp.apple.com. The user has the short name “jdm,” and the share point he wants to access is named “Marketing.”

- 2 Setting up share point access. Next, the server retrieves the user’s Active Directory record and authenticates the user. The server uses the user ID (UID) and group ID (GID) in the record to set up file access permissions for the user.



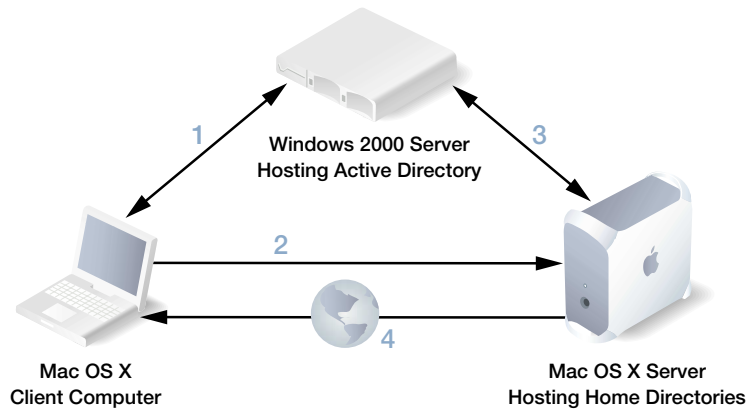
In this example, the user records reside in the search base indicated in Active Directory on a Windows 2000 Server. The name of the Windows server is supergirl.corp.apple.com, and its IP address is 10.43.12.172.

- 3 Accessing files. The share points the user is authorized to access are listed for the user, who selects the ones of interest. Selected share points are mounted on the user's desktop.



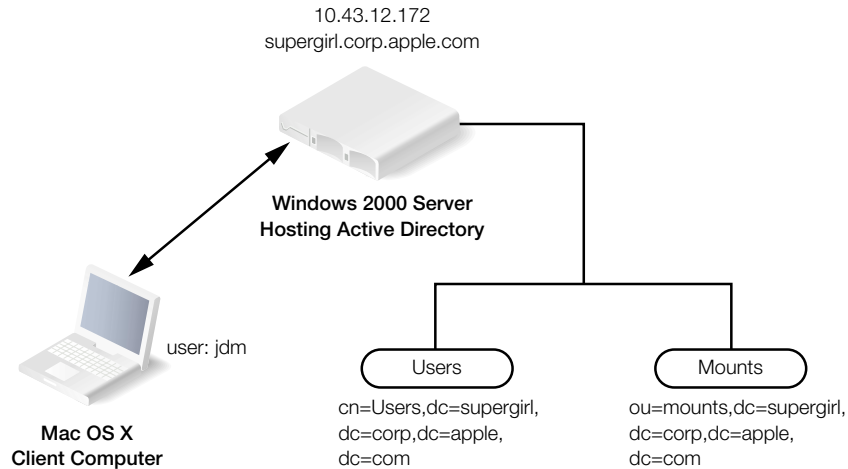
Using Mac OS X Server to Host Home Directories

In this scenario, a user has access to his home directory on Mac OS X Server after logging in to a Mac OS X computer and being authenticated using Active Directory information.



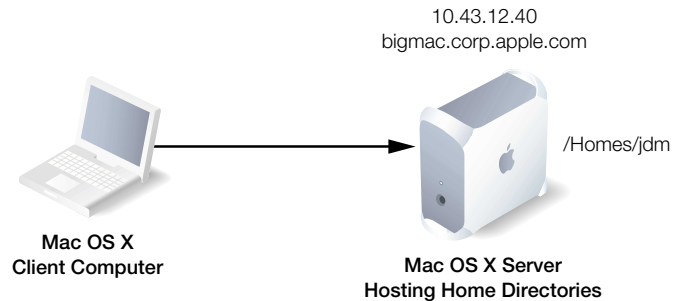
The numbers in this figure illustrate the sequence of interactions that occur between the time a user logs in to the Mac OS X client computer and can choose Home from the Go menu to access his home directory:

- 1 Retrieving user information. When the user logs in, the Mac OS X computer retrieves the user's record from Active Directory and authenticates the user. Home directory information in the user's record indicates that the home directory resides on the network, so a mount record for the home directory is retrieved from Active Directory. The mount record identifies the home directory share point and its access protocol—AFP in this case.



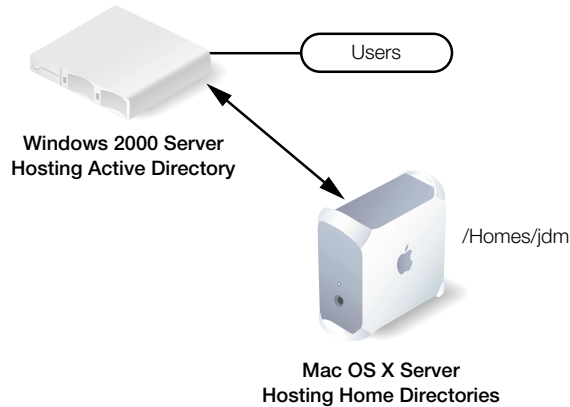
In this example, the user and mount records reside in the search bases indicated in Active Directory on the Windows 2000 Server.

- 2 Requesting authorization to mount the home directory. The Mac OS X client computer then sends the user's information to the Mac OS X Server hosting the home directory to request authorization to mount the home directory.

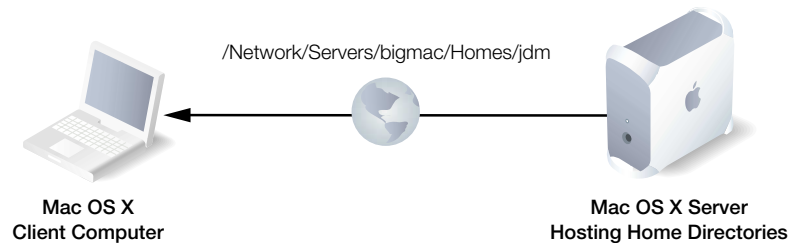


The home directories, named using the user short names, reside under the share point named "Homes" on Mac OS X Server.

- 3 Setting up home directory access. Next, the server retrieves the user's Active Directory record and authenticates the user. The server uses the UID and GID in the record to set up file access permissions for the user.



- 4 Accessing the home directory. The home directory is now mounted and visible on the user's computer in the Mac OS X Finder under /Network/Servers/bigmac/Homes, and login is complete.



Before setting up this scenario, install Mac OS X 10.1.3.

Setting Up the Scenarios

The remainder of this paper tells you how to set up each of the scenarios, which involves:

- Working with the Windows server to make sure Active Directory contains the necessary data
- Setting up Mac OS X directory service mappings using the Directory Setup application on Mac OS X computers so that those computers can access the Active Directory data
- Enabling secure LDAP authentication
- Setting up share points or home directories on Mac OS X Server

Some of the tasks you perform to set up these scenarios are the same for both scenarios. When this is the case, the tasks are documented in a single location toward the end of this paper, and the scenario-specific sections tell you exactly what that location is.

The instructions for working with the Windows server and Active Directory assume you are familiar with them. The instructions do not include every step you use to set up the Windows server and Active Directory for use in the scenarios. If you need assistance, consult an individual with Windows 2000 and Active Directory expertise, refer to the documentation for these products, or go to this Web site:

www.microsoft.com/support/

Setting Up the AFP File Server Scenario

The following tables summarize the Active Directory data needed to support this scenario by highlighting the record and data mapping you do using Directory Setup. The values in the far-right columns describe what an item is known as in the Active Directory database.

Kind of record	To access a record that	Map this LDAP record type	To this Active Directory element
user	Identifies authorized users	Users	cn=Users, dc=supergirl, dc=corp, dc=apple, dc=com

Kind of record	To access this information	Example values	Map this LDAP data type	To this Active Directory element
User	User's login names	jdm JD Mankovsky	RecordName	sAMAccountName name or displayName
	UID	155	UniqueID	UniqueID
	User's full name	JD Mankovsky	RealName	name or displayName
	User's primary group ID	20	Primary GroupID	primaryGroupID

To set up the file server scenario, follow the directions in this section.

Setting Up the Windows Server

See "Installing Windows 2000 Tools" on page 29 for instructions.

Modifying the Active Directory Schema

See “Modifying the Active Directory Schema” on page 30 and “Creating New Attributes” on page 31 for instructions.

Creating User Records

See “Creating User Records” on page 34 for instructions.

Setting Up Mac OS X Directory Service Mappings

See “Setting Up Mac OS X Directory Service Mappings” on page 35 for instructions.

Enabling Secure LDAP Authentication

See “Enabling Secure LDAP Authentication” on page 42 for instructions.

Setting Up Share Points and Permissions

To set up share points and permissions for them on Mac OS X Server:

- 1** In a Finder window, open the folder in which you want to create the share point. Choose New Folder from the File menu. Name the share point.
- 2** In Server Admin, click the File & Print tab and make sure that Apple file service is turned on (a globe appears on the service icon if it is running).
- 3** Click the General tab, then click Sharing and choose Set Sharing Attributes.
- 4** Select the folder you want to share and click Choose.
- 5** Configure the share point for AFP access. Click “Share this item and its contents” in the General pane.
- 6** Set privileges. To list a user or group to assign privileges to, click Users & Groups in the General tab of Server Admin and choose Find Users & Groups from the pop-up menu. In the find window, choose “Selected directories” from the pop-up menu, then select the LDAP server or a NetInfo domain containing the user or group and click Done. Drag a user or group to the appropriate field in the sharing window.
- 7** Click Copy if you want all files and folders within the share point to have the same privileges as the share point.
- 8** Click Save.

Setting Up the Home Directories Scenario

The following tables summarize the Active Directory data needed to support this scenario by highlighting the record and data mapping you do using Directory Setup. The values in the far-right columns describe what an item is known as in the Active Directory database.

Kind of record	To access a record that	Map this LDAP record type	To this Active Directory element
mount	Identifies a home directory share point	Mounts	ou=mounts, dc=supergirl, dc=corp, dc=apple, dc=com
user	Identifies authorized users	Users	cn=Users, dc=supergirl, dc=corp, dc=apple, dc=com

Kind of record	To access this information	Example values	Map this LDAP data type	To this Active Directory element
mount	Share point name	bigmac:/Homes	RecordName	cn
	Home directory mount point in user's Finder	/Network/Servers	VFSLinkDir	vfmdir
	URL to mount	net url==afp://; AUTH=NO%20USER%20 AUTHENT@bigmac.corp. apple.com/Homes	VFSOpts	vfsopts
	How to interpret vfsopts	url (the value for AFP share points)	VFSType	vfstype
User	User's login names	jdm JD Mankovsky	RecordName	sAMAccountName name or displayName
	UID	155	UniqueID	UniqueID
	Path to AFP home directory	<home_Dir> <url> afp://bigmac.corp.apple.com/ Homes</url> <path>jdm </path> </home_Dir>	Home Directory	homeDirectory

Kind of record	To access this information	Example values	Map this LDAP data type	To this Active Directory element
	Path to home directory on user's computer	/Network/Servers/bigmac/Homes/jdm	NFSHome Directory	userSharedFolderOther
	User's full name	JD Mankovsky	RealName	name or displayName
	User's primary group ID	20	Primary GroupID	primaryGroupID

To set up the home directories scenario, follow the directions in this section.

Setting Up the Windows Server

See “Installing Windows 2000 Tools” on page 29 for instructions.

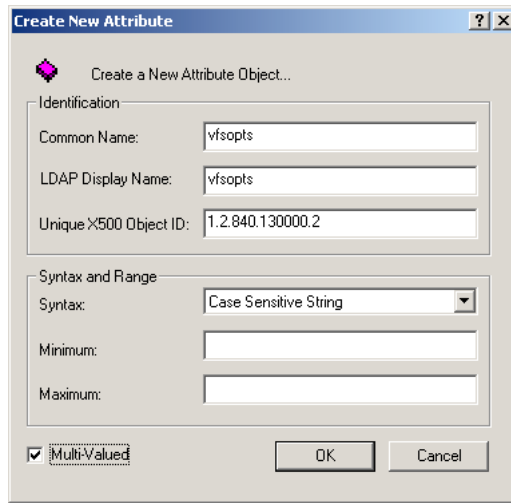
Modifying the Active Directory Schema

See “Modifying the Active Directory Schema” on page 30 and “Creating New Attributes” on page 31 for instructions.

Then create new attributes for the mounts class:

- 1 First, create vfsdir as shown here, then click OK.

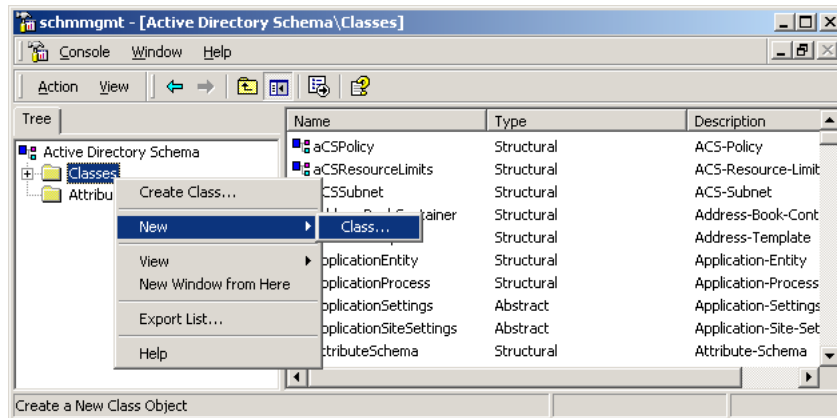
- 2 Next, create vfstype. Enter “vfstype” in the Common Name and the LDAP Display Name fields, then specify “1.2.840.30000.3” for the OID. As in the case of vfstype, choose “Case Sensitive String” as the Syntax value. Click OK.
- 3 Now, create vfopts. Make sure that the Multi-Valued checkbox is checked before clicking OK. (The vfopts attribute is a multi-valued attribute.)



Creating the mounts Class

To create a mounts class:

- 1 Choose the New Class command.



- 2 Enter information describing the class, then click Next.

Create New Schema Class

Identification

Common Name:

LDAP Display Name:

Unique X500 Object ID:

Inheritance and Type

Parent Class:

Class Type:

< Back Next > Cancel

- 3 Add the three attributes defined earlier, then click Finish.

Create New Schema Class

Mandatory:

Add...
Remove

Optional:

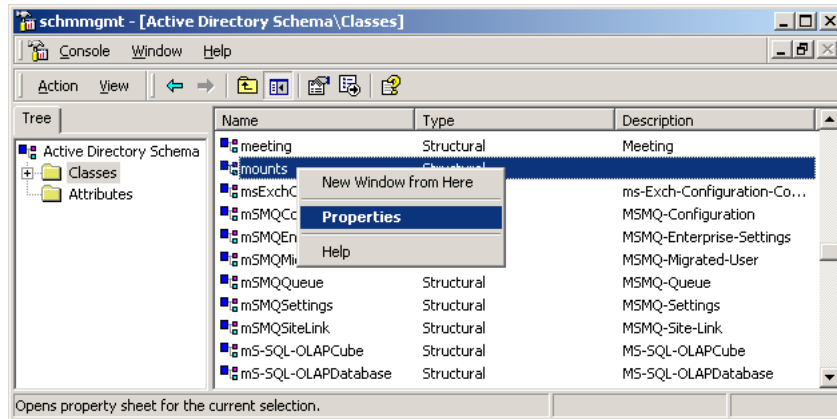
Add...
Remove

< Back Finish Cancel

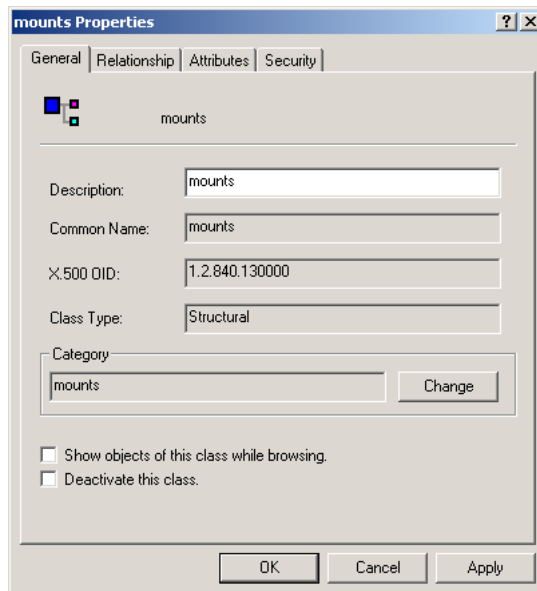
Editing mounts Properties

Edit the mounts properties to make sure all the values are correct.

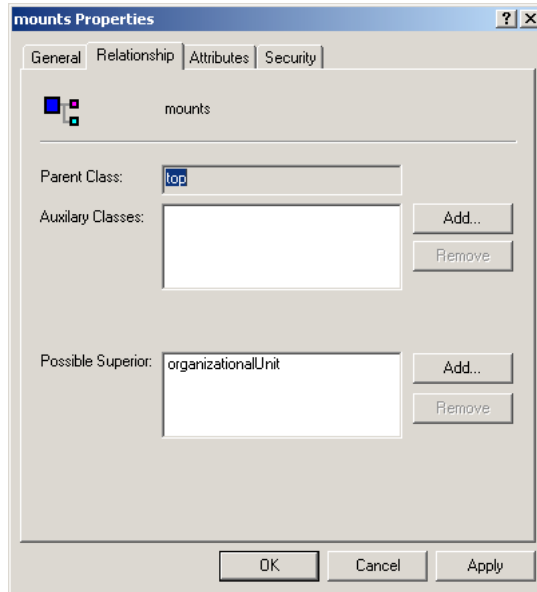
- 1 Select “mounts” and choose the Properties command.



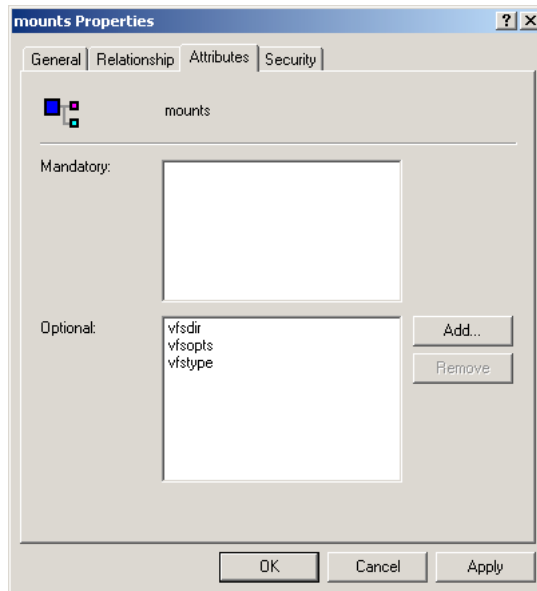
- 2 Ensure that the general properties for mounts look like this:



- 3 In the Relationship tab, ensure the Parent Class is set to “top” and that the Possible Superior value is organizationalUnit.



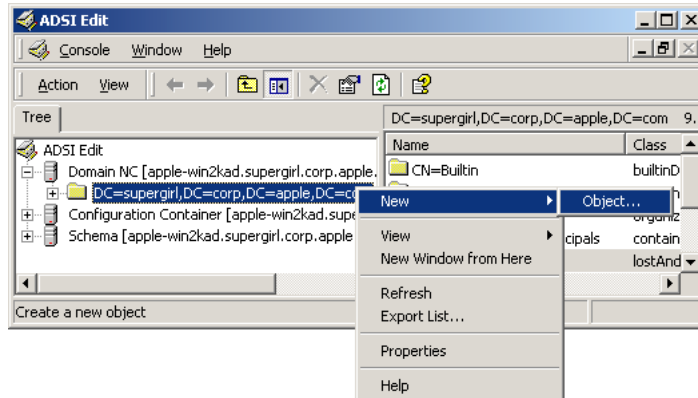
- 4 In the Attributes tab, ensure that vfsdir, vfsopts, and vfstype are listed as optional attributes.



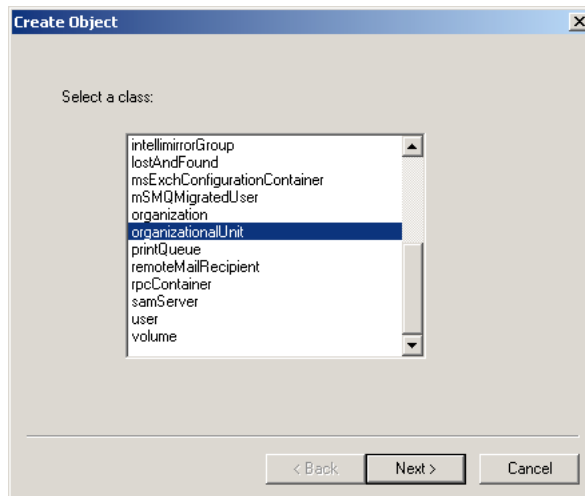
Creating a mounts Search Base

To create a search base for mount records:

- 1 Open the ADSI Edit tool located in Programs/Windows 2000 Support Tools/Tools/.
- 2 Create a new mounts object.



- 3 Map the mounts object to the organizationalUnit class.

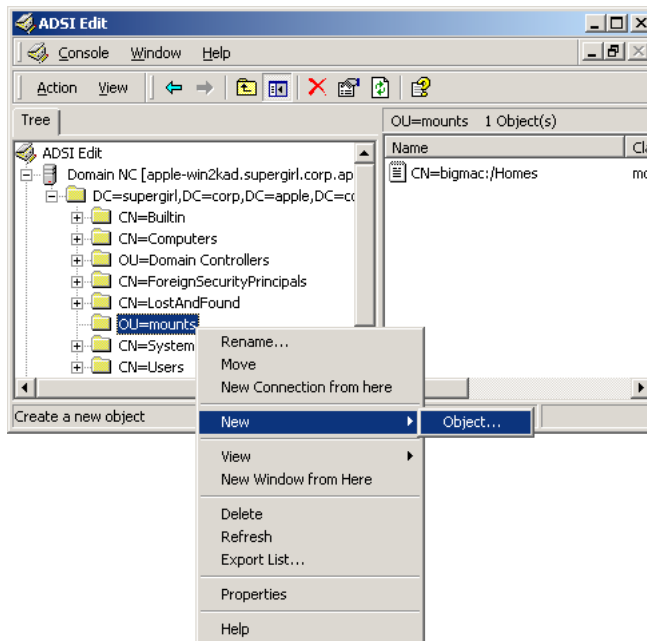


- 4 Name the organizationalUnit "mounts." Click Next, then click Finish.

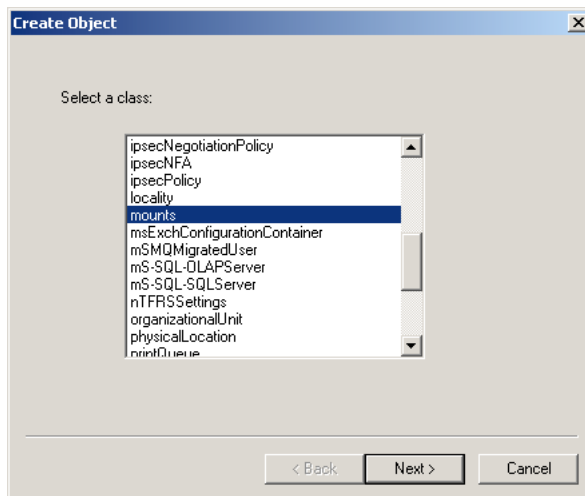
Creating a mounts Record

To create a record describing the home directory share point, follow these steps:

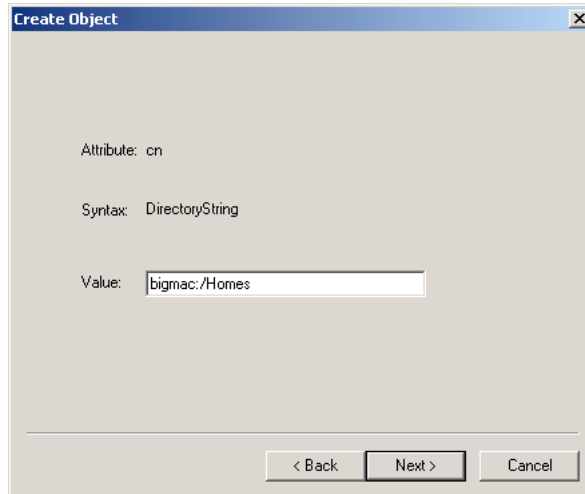
- 1 Create a new mounts object that describes the home directory share point.



- 2 Map the OU=mounts object to the mounts class, then click Next.



- 3 Identify the share point using the short DNS name of the home directory server (rather than an IP address), then click Next.



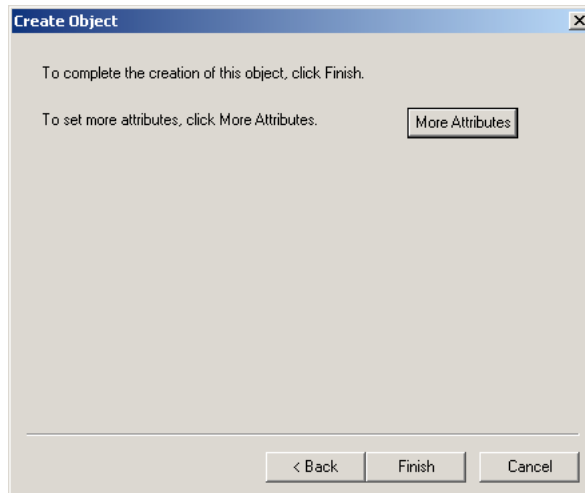
Attribute: cn

Syntax: DirectoryString

Value: bigmac:/Homes

< Back **Next >** Cancel

- 4 Click More Attributes to continue.

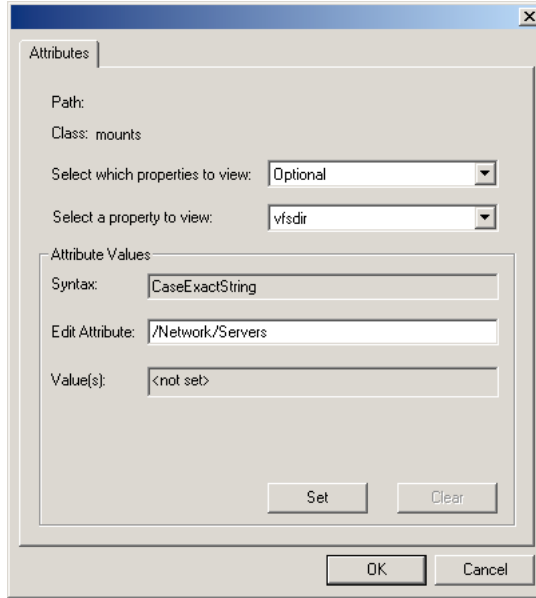


To complete the creation of this object, click Finish.

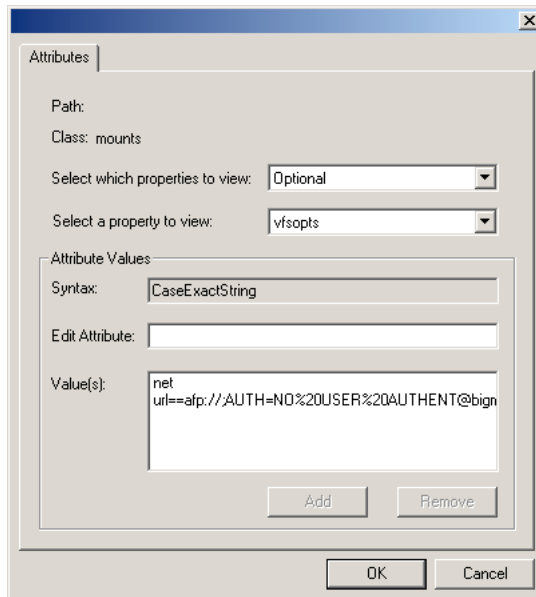
To set more attributes, click More Attributes. **More Attributes**

< Back Finish Cancel

- 5 Enter “/Network/Servers” in the Edit Attribute field to assign a value to vfsdir for the share point, then click Set.

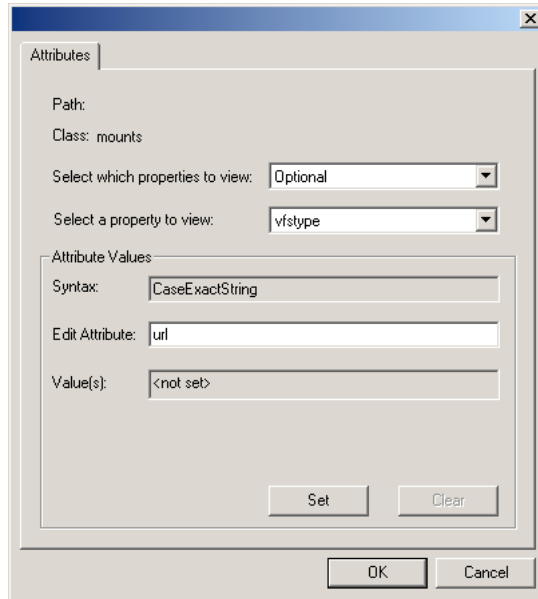


- 6 To set the values for vfsopts (the multi-valued attribute), enter “net” in the Edit Attribute field, click Add, enter the URL value in the Edit Attribute field, then click Add again.



The URL value (url= =afp://;AUTH=NO%20USER%20AUTHENT@bigmac.corp.apple.com/Homes) indicates that the home directory share point (Homes) is an AFP share point. It includes the DNS name of the home directory server where the share point resides and authorization information that supports an AFP guest connection.

- 7 Now set the value of the vfstype attribute.

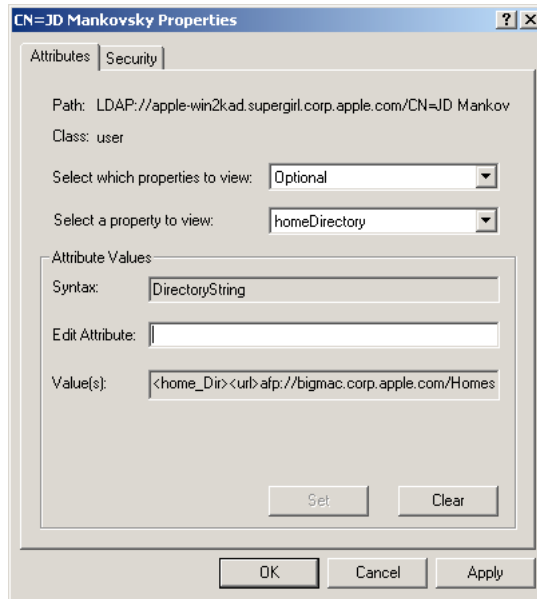


- 8 Repeat steps 1 through 7 when you need to define an additional share point.

Creating User Records

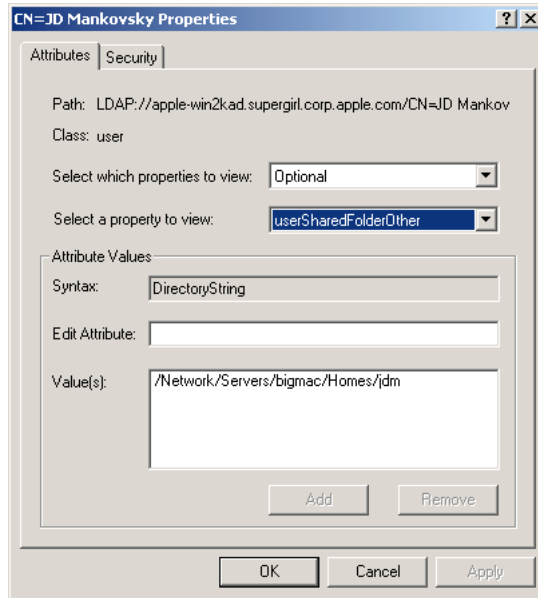
See “Creating User Records” on page 34 for instructions. Then follow these steps to assign values to home directory attributes of a user record:

- 1 Set the user’s homeDirectory attribute, which provides information required for AFP home directories, by entering the path to the home directory on the Mac OS X Server. In the example, the path is `<home_Dir> <url>afp://bigmac.corp.apple.com/Homes</url> <path>jdm</path> </home_Dir>`.



The value identifies the DNS name of the Mac OS X Server, the location of the share point (Homes), and the user’s home directory relative to the share point (jdm).

- 2 Set the userSharedFolderOther attribute, which provides information required for both AFP and NFS home directories. It includes the name of the mount object—“bigmac” in this example—as well as the path to the share point and the user’s home directory.



Setting Up Mac OS X Directory Service Mappings

See “Setting Up Mac OS X Directory Service Mappings” on page 35 for instructions.

Enabling Secure LDAP Authentication

See “Enabling Secure LDAP Authentication” on page 42 for instructions.

Setting Up Home Directories

To set up home directories for Active Directory users on the Mac OS X Server, follow these steps:

- 1** If you have not already done so, configure the server's directory services connection to the Windows computer, as described under "Setting Up Mac OS X Directory Service Mappings" on page 35.
- 2** Create the home directory share point.
 - a** Log in to the server as a user with administrator privileges.
 - b** Create the Homes directory.
 - c** Open Server Admin and use the Sharing module to make Homes a share point. Click the General tab, then click Sharing. Choose Set Sharing Attributes, select the Homes folder, then click Choose.
 - d** In the General pane, click "Share this item and its contents" to set up the share point for access using AFP. Ensure that the share point Owner has Read & Write privileges and that Group and Everyone have Read privileges.
- 3** Use the Server Admin Apple module to enable AFP Guest access. Click the File & Print tab, then click Apple. Choose Configure Apple Service. Click the Access tab, and click "Allow guest access." Click Save.
- 4** Set up home directories for each user defined in the Active Directory database:
 - a** Click the General tab in Server Admin, then click Users & Groups. Choose Home Directories Defaults. Click Local, choose Homes from the share point pop-up menu, and click Save.
 - b** List all the Active Directory users for whom you need home directories. Click Users & Groups, then choose Find Users & Groups. In the Find window, choose "Selected directories" from the pop-up menu, then select the LDAP server and click Done. Click More Choices, and set up criteria for the users you want to list. For example, you might want to list all the Active Directory users with UIDs greater than 99. To do so, ensure that Name is not checked but that Kind is checked and set to "Is User." Also check ID and set it to "Greater than 99." Click Find.
 - c** Examine the values for a few of the users to ensure that the mappings you used are correct. To view a user's values, double-click the user in the U&G Find Results window, and select the Advanced tab. Make sure the values for User ID, Primary Group ID, and home directory are correct.
 - d** Create an export file describing the users. In the U&G Find Results window, select all users for whom you want to create a home directory. Click Export, specify a location and filename, and click Save.

- e Click Users & Groups, then choose Import. Select the file saved in step 4d, and click Choose. Server Admin automatically creates a home directory for the user in the local Homes directory and names it after the user's short name. All the expected folders are created in the home directory, and the proper permissions are set up (Owner privileges are Read & Write and Group and Everyone privileges are Read Only).
- f Delete the users created in step 4e to remove their local NetInfo user records but retain their home directory folders. Click Users & Groups, then choose Show Users & Groups List, selecting the local NetInfo domain. Select the Active Directory users, then click Delete.

Logging In

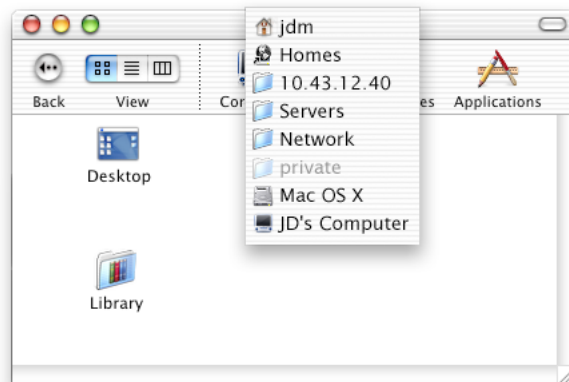
After all the Active Directory changes are complete, the directory services mappings set up, and the home directories created, your Active Directory users should do the following:

- Ensure that their Mac OS X computers are set up so that users not defined locally can log in. Click the Login Window tab in the Login pane of System Preferences. Ensure that “Automatically log in” is not checked. Then either select “Name and password entry fields” or select “List of users with accounts on this computer” and ensure that there is a checkmark in the box labeled “Show “Other User” in list for network users.”
- Restart their Mac OS X computers and log in.

After users log in, they can access their home directories from the Finder in one of the following ways:

- Choose Home from the Go menu.
- Click Home in a Finder window.

To see the complete path to the home directory, click the title bar in the home directory window while holding down the Command key:



The Remainder of This Paper

The remaining sections of this paper contain procedures you must complete while following the instructions in “Setting Up the AFP File Server Scenario” on page 12 and “Setting Up the Home Directories Scenario” on page 14.

Updating Active Directory

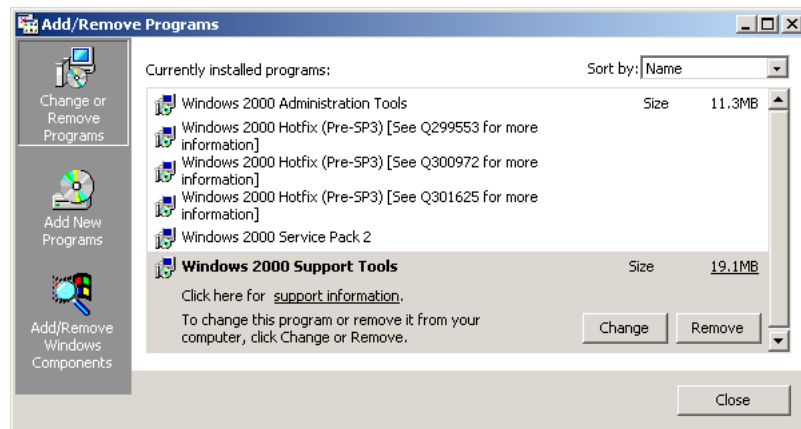
To ensure that Active Directory contains the information required to support either scenario, you may need to modify the Active Directory schema and add users to the Active Directory database.

Installing Windows 2000 Tools

On a Windows 2000 server with Service Pack 2 installed, install the Microsoft Active Directory Schema Manager snap-in. The Active Directory Schema Manager snap-in is installed when you install the full set of Windows 2000 Administration Tools (the AdminPak):

- 1 Open Add/Remove Programs and select “Windows 2000 Administration Tools.”
- 2 Click Change.
- 3 Click Next, then select “Install all of the Administrative Tools.”
- 4 Complete the installation.

Here is a screen shot of a Windows 2000 server showing the tools necessary for the Mac OS X integration:



The Windows 2000 Support Tools, available on the Windows CD, also contain some useful utilities. To install the support tools:

- 1 Navigate to Support\Tools\Setup.exe.
- 2 Click Start, point to Programs, point to Windows 2000 Support Tools, then point to Tools.
- 3 Click Active Directory Administration Tool.

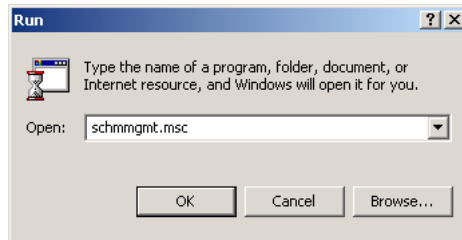
Modifying the Active Directory Schema

Setting up Active Directory to provide the required data for the scenarios is relatively simple. Most of the data is supported by built-in classes, properties, and attributes. To supplement these:

- In either scenario, you may want to define a new property of the organizationalPerson class to provide the UID. Alternatively, you can use a predefined property (such as employeeID) to obtain this information, if it provides only integer values ranging from 100 to 2^{31} .
- For the home directory scenario, you create a new class to provide mount data.

This document demonstrates how to create new schema attributes by using the Schema Manager. To allow changes to be made to the Active Directory schema, do the following:

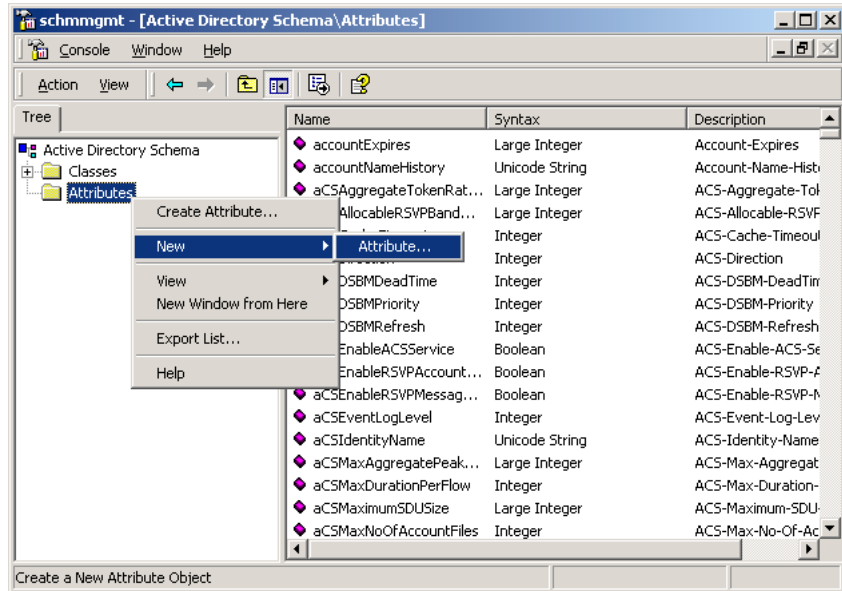
- 1 Use the Windows “run” command to enter schmmgmt.msc.



- 2 From the Schema Manager console, select the Active Directory Schema. Right-click and choose Operations Master.
- 3 Click to put a checkmark in the box labeled “The Schema may be modified on this Domain Controller.”

Creating New Attributes

To create new attributes, you use the schmmgmt.msc tool.



Note: When you create attributes, assign them names that make sense to you. You do not need to use the names used in this paper. Whatever names you assign are the names you use when setting up the LDAP mapping on the Mac OS X computers.

If you want to create a new property for UID, create an attribute (named UniqueID in this example) using schmmgmt.msc.

The screenshot shows a dialog box titled "Create New Attribute" with the following fields and values:

- Identification:**
 - Common Name: unixid
 - LDAP Display Name: UniqueID
 - Unique X500 Object ID: 2.5.4.45
- Syntax and Range:**
 - Syntax: Integer
 - Minimum: 100
 - Maximum: 2000000000
- Multi-Valued
- Buttons: OK, Cancel

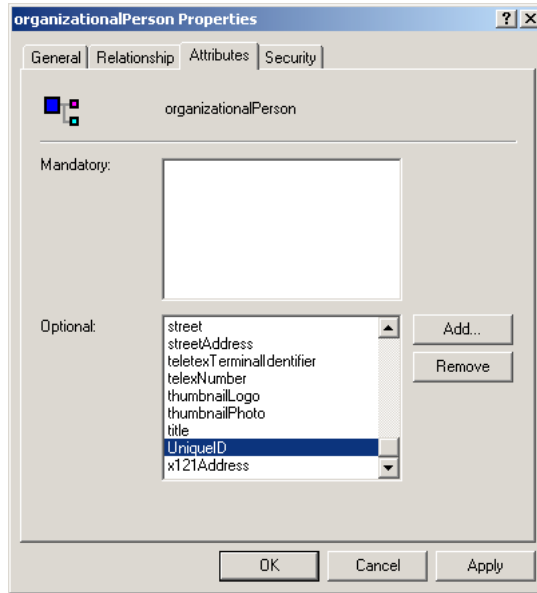
The UniqueID is the Mac OS X UID. The UID should be unique for each user, because it is used to manage file ownership. The UID is an integer that ranges from 100 to 2^{31} , making 2 billion unique identifiers available for use.

The object identifier (OID) for an attribute—which you enter in the Unique X500 Object ID field when you create an attribute—must also be unique. To find values that are not already used, consult this Web site, substituting your object name for “UniqueID” and an OID prefix for “2.5”:

www.alvestrand.no/cgi-bin/hta/oidwordsearch?text=UniqueID&prefix=2.5

All the OIDs used in this paper are examples of unique OIDs derived by using this Web site.

If you add UniqueID, you also need to edit the organizationalPerson class and add the UniqueID to it as an optional attribute.



When you are setting up the home directories scenario, you need to make additional schema changes. See “Modifying the Active Directory Schema” on page 15 through “Creating a mounts Record” on page 21 for details.

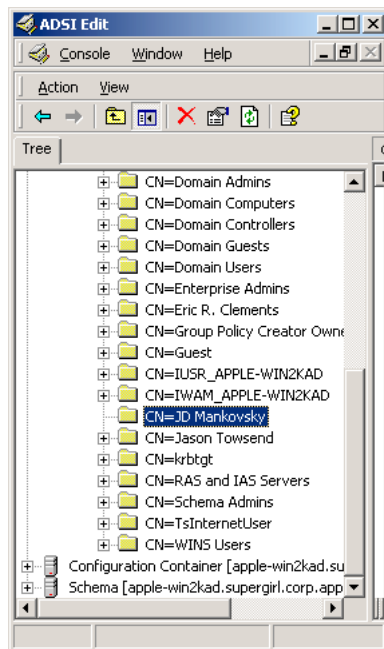
Creating User Records

You can add users to the Active Directory database and set their attributes by using the Active Directory Users And Computers application in the Administrative Tools (available in the Start menu) and the ADSI Edit tool.

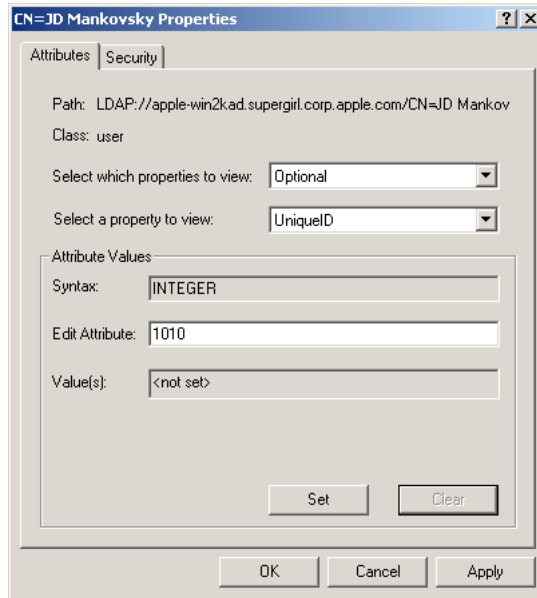
Two of the tools are the LDAP Data Interchange Format (LDIFDE) utility and Csvde.exe. These command-line tools can be used to assign values to user attributes in a batch process. Information about these tools can be found by searching at the Microsoft support site (www.microsoft.com/support) for the article numbers indicated:

- Q237677, *Using LDIFDE to Import and Export Directory Objects to the Active Directory*
- Q263991, *How to Set a User's Password with LDIFDE*
- Q300409, *How to Use Csvde.exe to Import Contacts Into the Active Directory*

This example presumes that a user named JD Mankovsky has just been created with the Users And Computers tool, which was also used to set the user's password value as well as values for the user's short name (sAMAccountName), full name (name or displayName), and group ID (primaryGroupID).



Now, you can use the ADSI Edit tool to set the values of other required attributes. For both scenarios, ensure each user has a valid UID.



For the home directories scenario, also set home directory attribute values, as “Creating User Records” on page 25 describes.

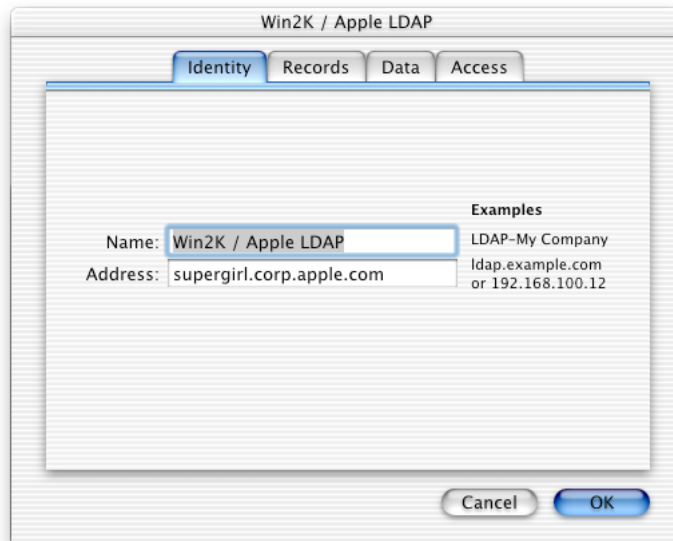
Setting Up Mac OS X Directory Service Mappings

To set up Mac OS X computers so they can access the Active Directory data, you use the Directory Setup application on Mac OS X computers.

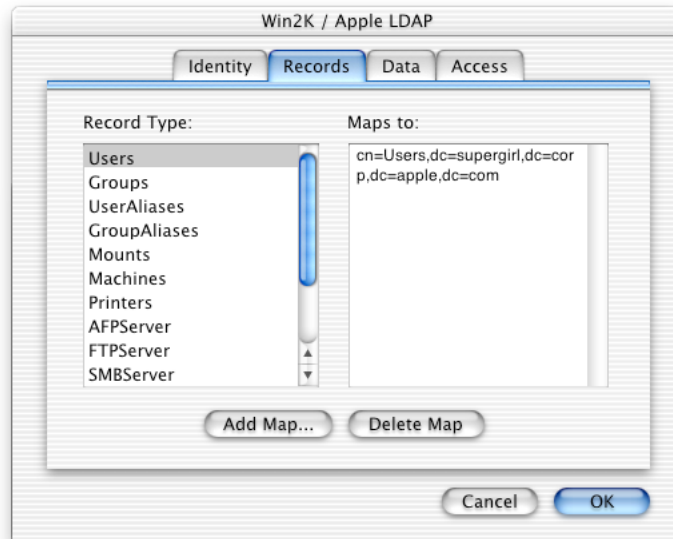
For the file server scenario, follow these steps on Mac OS X Server. For the home directories scenario, follow them on all Mac OS X computers that Active Directory users will use and on the Mac OS X Server that hosts the home directories:

- 1 Open Directory Setup, located in /Applications/Utilities.
- 2 Click the lock to log in as administrator.
- 3 Select LDAPv2, then click Configure.
- 4 Click New.

- 5 Identify the LDAP server in the Identity tab:
 - a In the Name field, enter a descriptive name for the Active Directory server.
 - b In the Address field, enter the server's domain name or IP address.

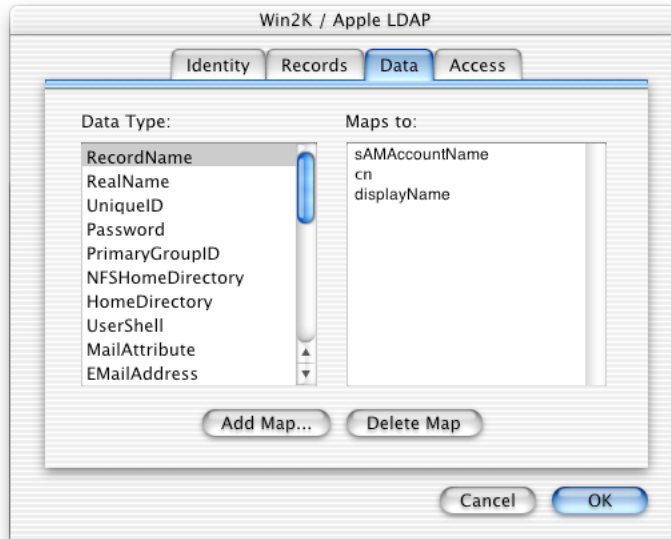


- 6 Define the Active Directory search base.
 - a Click the Records tab.
 - b Select Users in the Record Type list. Edit the default “Maps to” value to specify the search base for Active Directory user information. The exact search base value to enter can be interpreted from the ADSI Edit tool (see step 2 on page 20).



- c For the home directories scenario, you also provide mapping to the Active Directory mounts record. Select Mounts in the Record Type list. Set the “Maps to” value to “ou=mounts,dc=supergirl,dc=corp,dc=apple,dc=com.”

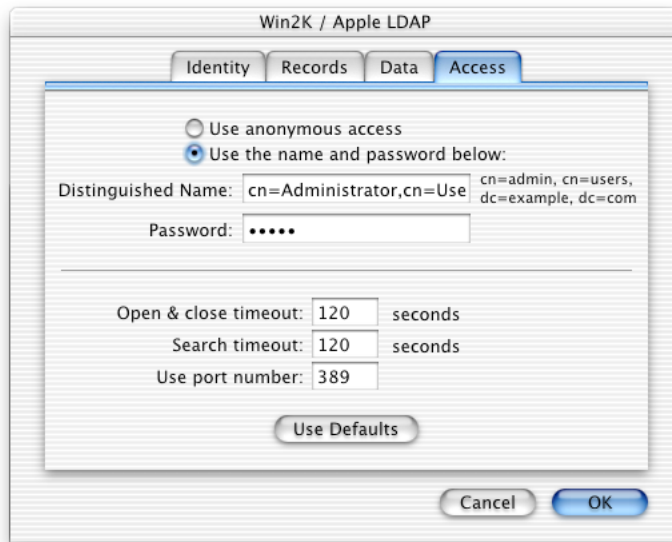
- 7 Map user attributes and, for the home directories scenario, map home directory attributes.
 - a Click the Data tab.



- b Select data types and enter, in the “Maps to” field, the name of the Active Directory attribute that provides its value.

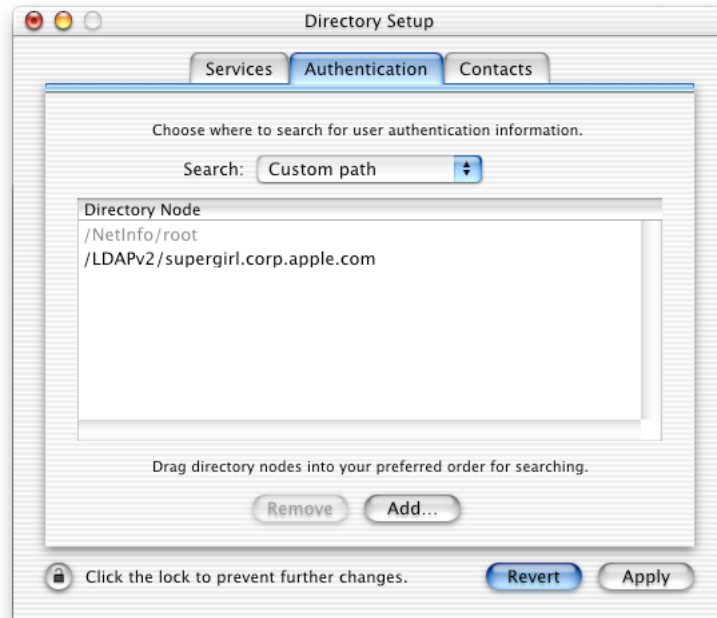
Data Type	Maps To	Comments
RecordName	sAMAccountName cn name or displayName	<p>For the home directories scenario, sAMAccountName and cn are required; they identify the user's short name and the home directory share point. The name or displayName, which identifies the user's long or full name, is optional.</p> <p>For the file server scenario, sAMAccountName and cn, name, or displayName are required.</p> <p>Map all the values the user should be able to use to log in to a Mac OS X computer. Directory services uses any of the RecordName attributes for authentication.</p> <p>For the home directories scenario, the first value you enter should be the short name, since the Server Admin Users & Groups module uses the first name entered when creating a user's home directory.</p>
RealName	name or displayName	<p>Map RealName to the user's long name. Typically, this name duplicates the long name mapping for RecordName.</p>
UniqueID	UniqueID	<p>If you are using a predefined Active Directory attribute such as employeeID, supply that attribute's name as the "Maps To" value.</p>
Password	a blank value	
PrimaryGroupID	primaryGroupID	
NFSHomeDirectory	userSharedFolderOther	Not required for the file server scenario.
HomeDirectory	homeDirectory	Not required for the file server scenario.
VFSType	vfstype	Not required for the file server scenario.
VFSLinkDir	vfmdir	Not required for the file server scenario.
VFSOpts	vfsopts	Not required for the file server scenario.

- 8 Define the attributes of the connection between the Mac OS X computer and the Windows 2000 computer.
 - a Click the Access tab.



- b Select "Use the name and password below" and enter the distinguished name and password the Mac OS X computer should use to establish a connection with the Windows server. In this example, the distinguished name is cn=Administrator,cn=Users, dc=supergirl,dc=corp,dc=apple,dc=com.
- c Click OK.
- d Select the Enable checkbox to make the connection you just configured available for use by directory services, then close the window and click Save.
- e In the Services pane, make sure the LDAPv2 box is checked. If you need to check the box, click Apply after you do so.

- 9 Add the Active Directory server to the Mac OS X computer's search policy.
 - a Click the Authentication tab.



- b Choose "Custom path" from the Search pop-up menu.
- c Click Add.
- d In the Add Nodes window, select the LDAP entry you just created, and click Add.
- e Close the Add Nodes window and click Apply.
- f Click the lock to safeguard your changes.

Enabling Secure LDAP Authentication

You can configure the Mac OS X LDAP plug-in to use SSL for communication with the Windows server. When you do so, information is not transmitted between Mac OS X computers and the Windows server in clear text form. To learn about third-party applications that let you set up LDAP connections that use SSL on Mac OS X computers, go to:

www.apple.com/downloads/macosx/

One such application, SSL Enabler, lets you set up secure authentication by mapping the LDAP port on a Mac OS X computer (port 389 by default) to the SSL port on a Windows server (636 is the standard LDAP over SSL port). To set up secure authentication, follow these steps:

- 1** On the Windows server, ensure that SSL is enabled. For more information, search for article Q247078, *How to Enable Secure Socket Layer (SSL) Communication Over LDAP For Windows 2000 Domain Controllers*, located at:
www.microsoft.com/support
- 2** On the Mac OS X computer, search for and download SSL Enabler at:
www.apple.com/downloads/macosx/
- 3** Run SSL Enabler, installing the stunnel utility it uses when prompted. Click Add and enter the Local Port value (usually 389), the Remote Server IP value (the IP address of the Windows server), and the Remote Port value (usually 636). Click Save.
- 4** Run Directory Setup to change the IP address of the LDAP entry for the Windows server.
 - a** Click the lock to log in as administrator, select LDAPv2, then click Configure.
 - b** Select the LDAP entry you configured earlier (Apple LDAP), and click Edit. Change the Address field value to the loopback address, 127.0.0.1, then click OK.
 - c** Click the Authentication tab to update the search path. Choose “Custom path” from the Search pop-up menu. Delete the old LDAP entry by selecting it, then clicking Remove. To add the new entry, click Add, select the updated LDAP entry, close the Add Nodes window, then click Apply.