Apple Technical White Paper

Best Practices for Integrating OS X Lion with Active Directory

Updated November 1, 2011

Contents

Apple's Built-In Solution

Directory services are a core component of enterprise computing environments that allow organizations to centralize information about users, groups, and computing resources. In addition to consolidating resources and simplifying system management, directory services also provide benefits to users by enabling them to access enterprise resources from anywhere on the network with a single set of credentials. The full effectiveness of directory services is seen when a single directory services infrastructure is used across all the desktop, notebook, and server systems within a network.

A key advantage to this single-directory approach is that it allows organizations to centralize management of user, group and computing accounts. This approach alleviates problems caused by the proliferation of proprietary directory services solutions.

Apple's implementation of a centralized directory service is called Open Directory. Integrated into the foundations of OS X Lion, Open Directory is responsible for providing directory and network authentication services for both OS X clients and OS X Server. Open Directory uses open standard protocols such as LDAP, Kerberos, and SASL.

Although Apple provides its own native directory services platform through Open Directory, OS X supports access to a variety of other platforms including Microsoft's Active Directory. While every Active Directory installation is different, OS X integrates well with the vast majority of them with minimal effort.

OS X offers Active Directory integration through a directory service. With this support, the user doesn't need to maintain a separate directory or separate user records to support OS X systems. Users can move between different computers while still adhering to enterprise policies for strong authentication and password-protected access to network resources.

When fully integrated with Active Directory, OS X offers a complete managed environment where users can:

- Access any Mac in the integrated environment using the same credentials they would use to access Windows PCs.
- Be fully controlled by the Active Directory password policies.
- Have single sign-on access to Active Directory resources via Kerberos.

Users can have network-based home directories, local home directories, or a combination of the two called Portable Home Directories, which are similar to roaming profiles on Windows.

Users can be subject to client management policies enforced from the directory. For example, IT staff can specify that the screen saver requires a password via a policy from Active Directory. Apple's support for Active Directory extends to OS X Server as well. Integrating a server is just as easy as integrating a client system—in fact, the process is essentially the same. This allows Windows-based departments to take advantage of file sharing, web services such as wikis and blogs, and other services in OS X Server while using their existing Active Directory infrastructure for identification and authentication. Secure network services (including network home directories) hosted on OS X Server also support single sign-on for both OS X and Windows clients.

Address Book and Mail

The Address Book application in OS X Lion provides a flexible and convenient way to store contact information. Address Book can use common network technologies, such as LDAP, to query servers for contact information. This allows a Mac to look up contact information stored within Active Directory. Users can configure the use of an LDAP server (such as an Active Directory domain controller) even if their Mac hasn't been integrated into the Active Directory domain.

Users can select the "Directory Services" group in Address Book and search for a user by name or email address. Once the appropriate contact(s) have been located, users can then drag them into their local Address Book, which can be helpful if users who don't have permission to change Active Directory records want to add or modify information about a contact.

Address Book is integrated with Mail, iChat, and other applications in OS X. This allows these other applications to access the same set of contact information available to Address Book. Mail, for example, will search Active Directory for contact information as users type a contact's name and will offer matching contacts for autocompletion of the email address (provided email addresses are included in Active Directory for user accounts).

Address Book also offers the option for displaying phone numbers in large type for easy dialing, mapping of addresses using Google Maps, and easy copying of a correctly formatted address block ("Copy Mailing Label").

Additional information can be added to user accounts within Active Directory such as an instant messaging username or a blog address using Microsoft's management tools (or, if the environment is fully integrated, using Apple's Workgroup Manager). This information will appear in Address Book along with other contact information.

How to Integrate OS X with Active Directory

Getting Started

Using these simple steps, you can configure a Mac client to use DNS and Active Directory to determine the geometry of your Active Directory domain, find the nearest domain controller, and create a new computer account in the domain—if there is not an existing one with the computer ID that you have chosen.

On the Mac client, open the Accounts Pane within System Preferences, available from the Apple menu. Select Login Options, and then click Join under Network Account Server. Enter the name of your Active Directory domain. The sheet will expand so that you can enter any additionally required information. The computer's account in Active Directory will reflect the Client Computer ID—make sure it reads correctly before proceeding.

Computer accounts
Each Mac system has a unique computer account in Active Directory. If you clone a system or integrate NetBoot with Active Directory, all of the cloned systems are assigned the same computer account. This means that it's important to take care when changing a computer account, as any change will break authentication from all systems using that account.

Enter the user name and password of a user who has permission to join clients. This does not need to be an "admin" user—you may assign the privilege to any user. If you need to specify advanced options or a custom OU, click Directory Utility. If the standard options are fine, click OK, and the Mac will be bound to Active Directory.

Command Line Configuration

The functionality of the Directory Access graphical user interface is also accessible from the command line interface with the dsconfigad command. For example, the following command would join a system to Active Directory:

```
dsconfigad -preferred ads01.example.com -a COMPUTERNAME –
domain example.com
-u administrator -p "password"
```

Once you have bound a system to the domain, you can use dsconfigad to set the administrative options that are available in Directory Access:

```
dsconfigad -alldomains enable    -groups domain
admins@example.com, enterprise admins@example.com
```

When using dsconfigad in a script, you must include the cleartext password that was used to join to the domain. Typically, an Active Directory user with no other admin privileges is delegated the responsibility of joining clients to the domain. This user name and password pair is stored in the script.

In-depth Directory Service Information

Start by enabling directory services debug logging:

```
odutil set log debug
```

Now when you attempt to join Active Directory, you can look at the log to see what is occurring:

```
/var/log/opendirectoryd.log
```

When you have accomplished a successful join, use the same command to disable the debug logging:

```
odutil set log default
```

It may also be helpful to examine a packet trace of the client attempting to join to the domain. By default, the traffic is encrypted. To disable encryption:

```
/usr/sbin/dsconfigad -packetencrypt disable
```

To reenable:

```
/usr/sbin/dsconfigad -packetencrypt allow
```

When capturing traffic for the following ports:

UDP 53	- DNS
TCP 88	- Kerberos
TCP 389	- LDAP
TCP/UDP 464	- Kerberos Password Changes (KPasswd)

TCP 3268 - Global Catalog (LDAP)

For example, to capture traffic over the built-in Ethernet connection to a file called "capture.out," you could use the following syntax for tcpdump:

```
tcpdump –K -i en0 -s 0 -w capture.out port 88 or port 464
or port 53 or port 389 or port 3268
```

Enterprise Integration Challenges

DNS service

Since Active Directory relies on DNS SRV service records, the Mac client must be using the same DNS servers as all of the Windows clients on the network. Use the dig command to test that the Mac can read the proper DNS records. In the following example, replace example.com with the DNS of your Active Directory domain:

```
dig -t SRV _ldap._tcp.example.com
```

This should return the IP address of your domain controller. If it doesn't, your Mac systems are not using the same server for DNS as the Active Directory clients, or your DNS server is misconfigured.

OS X client will attempt to dynamically update DNS records hosted by Active Directory, both the forward (A) and reverse (PTR) records.

Passwords

Since OS X Lion leverages Kerberos, it inherently supports Active Directory password policies and enforces restrictions on the length and complexity of passwords on client systems. Mac users can also change their passwords using the Accounts preference pane in OS X.

In the days leading up to password expiration, users are notified that their password is about to expire, during login and other authentication events. This gives them the opportunity to change their password in Active Directory—which will reset the expiration timer—using the Accounts preference pane on the Mac client. When the password is within 24 hours of expiration, users cannot complete login until they have changed their password.

When a Mac system is bound to Active Directory, it sets a computer account password that is then stored in the System keychain. This computer account password is automatically changed by the client. The default is every 14 days, but you can use the dsconfigad command-line tool to set any interval that your policy requires.

Windows Server Versions
Joining a Mac system to Active Directory has been successfully tested with Windows Server 2000, 2003, 2003R2, 2008, and 2008R2. The domain can be in either native or mixed mode without any change in the functionality of the OS X clients.

Single Sign-On

Apple and Microsoft both support Kerberos to provide a secure single sign-on environment. When integrated into an Active Directory environment, OS X uses Kerberos exclusively for all authentication activities. The use of Microsoft's NT LAN Manager (NTLM) suite of protocols, including both NTLMv1 and NTLMv2, can be prohibited on the network as needed, with no impact on Mac computers or services provided by OS X Server within the Active Directory environment.

When a user logs into a Mac using their Active Directory account, the Active Directory domain controller automatically issues a Kerberos Ticket-Granting Ticket (TGT). When the user attempts to use any service on the domain that supports Kerberos authentication, the TGT generates a ticket for that service, without requiring the user to authenticate again.

You can use the Kerberos administration tools on a Mac to view tickets currently issued to a user both from the command line, where klist will display the current tickets, or by using the graphical Ticket Viewer utility located at /System/Library/CoreServices/Ticket Viewer.app, which allows you to view and work with Kerberos tickets.

Namespace Support

OS X offers the option of supporting multiple users with the same short names (or login names) that exist in different domains within the Active Directory forest. By enabling namespace support, using the dsconfigad command-line tool, a user in one domain can have the same short name as a user in a secondary domain. Both users will have to log in using the name of their domain followed by their short names (DOMAIN\short name), similar to logging in to a Windows PC.

Site awareness

Open Directory is site aware, able to use DNS service records and site information stored within Active Directory to locate and communicate with the most appropriate domain controllers (typically ones that are in close proximity in multi-site networks). By querying Active Directory for site information and polling the site's domain controllers, a Mac integrated in Active Directory can find not only the closest domain controllers but also the ones that respond the quickest. Using this information, Open Directory chooses domain controllers and Global Catalogs and communicates with them until a network change occurs, or until a domain controller stops responding.

Signed Connections

Open Directory is able to both sign and encrypt the LDAP connections used to communicate with Active Directory. Along with the signed Server Message Block (SMB) support that is present in OS X, you should have no need to downgrade your site's security policy to accommodate Mac clients. The signed and encrypted LDAP connections also eliminate any need to use LDAP over Secure Sockets Layer (SSL). If your site requires SSL connections, you can configure Open Directory to use SSL using the following command:

```
/usr/sbin/dsconfigad -packetencrypt ssl
```

Note that the certificates used on the domain controllers must be trusted for SSL encryption to be successful. If the domain controller certificates are not well-known certificates whose roots are installed by default in the System keychain, you must install and trust the root certificate in the System keychain. To manually install the root certificate, import it in Keychain Utility in /Applications/Utilities, or use the security command, as follows:

```
/usr/bin/security add-trusted-cert -d -p basic -k /Library/
Keychains/System.keychain <path to certificate file>
```

Deployment Strategies

Managed Preferences

OS X Lion offers a complete managed client environment where every aspect of the Mac user experience can be restricted or controlled. Although technically different from the way Windows group policies are implemented in Active Directory, the effect is very similar. When fully integrated, a user's access to any OS X components can be restricted and their user environment (including OS X features as well as third-party applications) can be preset or completely controlled.

Depending on the level of management your organization requires and the level of integration you want to use, there are several options for implementing client management for Mac computers:

Do nothing

Open Directory automatically enables authentication to Active Directory, including full support of password policies. It also allows you to set up network home directories for Mac users contained in Active Directory. Although this doesn't allow for client management, it does offer a fully functional environment in which standard users can be configured as non-admin users on Mac clients. This allows you to ensure that they will not be able to change any system settings.

Use Profile Manager

Profile Manager allows an administrator to configure policies outside of a directory service. In this scenario, a user would either opt-in to service configuration and policy settings via web interface or join the client to a profile manager server. The user would then authenticate against Active Directory, and the policies and settings would already exist locally on the Mac client. If the Mac is bound to a profile server, any changes to policies are triggered by an Apple Push notification, after which the Mac contacts the Profile Manager service to update policies and settings.

Extend the Active Directory schema to handle management

By adding Apple-specific attributes and object classes to the Active Directory schema, your Active Directory system can support all OS X management policies. Just use the management tools you would use to manage user and computer accounts stored on OS X Server and select the Active Directory domain as the target directory system. The details from this process are included in Appendix A and B.

Use a dual directory

This scenario adds OS X Server to the solution. Mac clients integrate with Active Directory and with an Open Directory domain hosted by OS X Server. In this scenario, clients still use Active Directory for user authentication, while Open Directory supplies client management only (often referred to as Manager Preferences). Active Directory users and groups are nested inside Open Directory groups. OS X further enhances this scenario with "augmented records" that allow information from a secondary directory to be added to information directly from Active Directory for the same record. This solution does not require any change to the Active Directory schema, but does require OS X Server.

Managed Client for OS X (Managed Preferences)

Because Windows and OS X handle preferences differently, the Mac is unable to use Group Policy Objects (GPOs) in Active Directory. Instead, Apple has a system called Managed Preferences that accomplishes the same task.

Managed Preferences can be stored locally on Mac clients that have been integrated into Active Directory, but this makes updates difficult because it involves each individual computer. It's also possible to host the Managed Preferences objects in Active Directory, which requires you to extend the schema. Another solution is to configure a secondary LDAP directory using OS X Server and Apple's Open Directory. In this scenario, clients still use Active Directory for user authentication, while Open Directory supplies Managed Preferences only.

Use a third-party solution

Products from Centrify, PowerBroker, Thursby, and Quest allow Managed Preferences to be stored in the Active Directory domain without requiring you to extend the schema. With the Thursby solution, you use OS X tools to create user preferences, while the Windows-based Centrify solution enables you to manage all the preferences using native Active Directory tools. PowerBroker Identity Services Enterprise Edition allows you to use both native Active Directory tools as well as Workgroup Manager to manage arbitrary preferences for many applications. QAS from Quest provides native Active Directory tool support as well as management for arbitrary preferences using preference manifests within the Active Directory Group Policy Editor.

Distributed File System (DFS)
OS X Lion also supports home directories and mounting of file shares via DFS. The Universal Naming Convention (UNC) path is the same as the SMB path, but if the name is hosted in a DFS namespace, the share will be mounted correctly.

AFP network homes
It's also possible to use an afp:// URL for your home directories. In Active Directory, the URL remains in the standard UNC. On the Mac, however, you can allow the client to translate the SMB path into an AFP path.

Home Directories

Regardless of your strategy for Managed Preferences, you can set up users with local homes, network homes, or a combination of the two called Portable Home Directories, which are similar to roaming profiles on Windows.

Local

With the default configuration of Apple's Active Directory in Directory Services, the user's home stays on the local system, without any change to the user record in Active Directory. If a network home is defined in the user record, that share will mount on the desktop when the user logs in.

Network

To define a network home in the Mac user's Active Directory record, use a URL in the form of \\server\share\user—just as you would for a Windows user. When interpreted by the Active Directory configuration on the Mac, the server name will be added to the Active Directory domain, forming a URL: smb://server.ad.domain/share/user.

Note: If the user's domain is different from the domain of the user's home folder, it may be necessary to put the fully qualified name of the server in the URL. So, instead of //server/share/user, you would use //server.userad.domain/share/home. Using a Mac friendly naming convention does not affect the Windows systems on the network.

The Mac user's network home can be hosted on either OS X Server or on a Windows server, using either AFP or SMB. You can even host home directories for both OS X and Windows clients on OS X Server, providing Mac services over AFP and Windows services over SMB.

Portable Home Directory

In this scenario, the Active Directory user record and the network home are cached locally on the client system, making it ideal for managing laptop users when they are away from the network. According to a sync policy, the local system synchronizes with the remote home folder. For laptops, this typically happens when they reconnect to the network. Portable Home Directories can also be useful for managing desktop users. You decide how often the client syncs and what files are included in the sync—and allow them to operate offline the rest of the time.

Conclusion

Apple's support for Active Directory within OS X Lion enables Mac clients and servers to integrate smoothly into existing Active Directory environments and provides the option of deploying a single directory services infrastructure that can support both Mac and Windows clients.

Because OS X and Windows handle preferences differently, the Mac uses Managed Preferences to accomplish the same task as Group Policy Objects in Active Directory.

Managed Preferences objects can be hosted in Active Directory, which requires you to extend the schema. To learn more about extending the schema, refer to *Appendix A: Modifying the Active Directory Schema to Support Mac System*.

And to integrate Mac computers into an existing Active Directory infrastructure using a combination of Workgroup Manager and Active Directory with extended schema, refer to *Appendix B: Managing Users and Policies on OS X With Workgroup Manager and Active Directory with Extended Schema*.

If you have any questions about the best practices discussed in this paper, or any other aspect of integrating OS X systems with Active Directory, please contact your Apple representative or Apple Authorized Reseller for assistance.

Appendix A: Modifying the Active Directory Schema to Support Mac Systems

Most Windows administrators are familiar with client management and directory services in the form of Active Directory Group Policy Objects (GPOs). By joining Mac computers to an existing Active Directory domain, you can also provide user authentication and policy directly to Mac computers centrally from Active Directory. This is an important capability given the growing adoption and popularity of the Mac within enterprises.

Group Policies that are well planned and executed can significantly ease setup, security, and support processes for new users and computers. . This appendix provides step-by-step instructions for extending the Active Directory schema to manage Mac systems.

Background

Just as Group Policies are a product of Active Directory, Managed Preferences are a product of Open Directory. Active Directory can be extended with Open Directory objects and attributes so that Mac computers can be integrated into an environment in which user and group records stored in Active Directory can have Managed Preferences associated with them, combining the best of both worlds.

To support Mac systems using Active Directory, Mac computers must be bound to the existing Active Directory infrastructure. Active Directory can also be used to store managed client preferences directly in Active Directory attributes, which requires modification of the Active Directory schema. Once the schema is modified, Open Directory in OS X can read the managed client preferences and apply them. Then administrators can use Workgroup Manager, a free user management tool from Apple, to populate the managed client settings within Active Directory. This white paper explains how to update the Active Directory schema to support the Mac.

Extending the schema for Apple-specific objects and attributes allows an organization to leverage its current Active Directory infrastructure without additional software for Mac computers. OS X systems can then be fully managed for security and organizational policy using a single directory service.

To integrate Mac computers into Active Directory, you need to start with built-in Windows-based tools to apply the initial schema modifications. After the schema modifications have been applied, you can use Workgroup Manager on a Mac to store policies in Active Directory that will be enforced on any Mac computers bound to Active Directory.

When joining OS X to Active Directory, OS X will authenticate against Active Directory. However, OS X does not recognize any Active Directory policies other than password policies. When Mac OS X is bound to Open Directory on OS X Server, it uses Managed Preferences from Open Directory to natively implement additional policies that are stored as XML files within Open Directory. For OS X to store and recognize objects and attributes within Active Directory, the Mac computers must be joined to

Active Directory, the Active Directory schema must be extended, and the administrator must populate Managed Preferences inside these objects and attributes. Once the Active Directory schema is extended, it will replicate any changes to the schema throughout the entire Active Directory forest.

Active Directory Schema Analyzer

To help integrate Mac computers into an existing Active Directory infrastructure, Microsoft provides the Active Directory Schema Analyzer, which connects to a preexisting directory service such as Open Directory and compares that schema to the schema in Active Directory. The Active Directory Schema Analyzer then generates custom LDAP Data Interchange Format (LDIF) files that can be used to modify the schema in Active Directory. By using the Active Directory Schema Analyzer to generate the schema modifications versus using stock LDIF files, system administrators will be made aware of any recent updates to the Active Directory schema from Apple, Microsoft, or third parties. For example, in Windows Server 2003, the RFC 2307 object classes and attributes were added to the Active Directory schema and were no longer required to be added for Managed Preferences.

Requirements

The following list outlines the components required to use the Active Directory Schema Analyzer to generate LDIF files and modify the schema in Active Directory:

- OS X Server v10.7 or later promoted to an Open Directory Master
- OS X v10.7 or later with Workgroup Manager installed to test schema modifications
- Windows XP with Service Pack 2 with .NET Framework 2.0 or later installed
- A test Active Directory domain controller with the specified organization’s current schema with Windows Server 2003 R2 schema or greater

Creating the LDIF Schema Modifications

Using the Active Directory Schema Analyzer to generate the required schema modifications is the first step in connecting Mac computers to both Active Directory and Open Directory. The following example shows how to accomplish this task.

1. On the Windows XP computer, download and install Microsoft’s Active Directory Application Mode (ADAM) directory services toolset. While ADAM provides much greater functionality than the Active Directory Schema Analyzer tool, it is the only tool required for generating the schema modifications. Note that ADAM does not currently run in Windows Vista or Windows 7.

2. If you do not have .Net Framework 2.0 or later installed, it must be installed in order to launch Active DirectorySchemaAnalyzer.

3. Choose Start > All Programs > ADAM> ADAM Tools Command Prompt.

4. Select the Active Directory Schema Analyzer tool by entering "Active DirectorySchemaAnalyzer" and pressing Return.

5. Choose File > Load Target Schema and enter the DNS name of the Open Directory Master.

6. Select Simple bind type and leave the other fields blank. Select a server type of Automatic and click OK.

7. Choose File > Load Base Schema. Enter the DNS name of the Active Directory domain controller, the Active Directory user name and password (an administrator's credentials are not required), and the domain where the Active Directory user's account resides. Select Secure bind type to enable the domain text box. Select server type of Active Directory and click OK.

8. Choose Schema > Hide Present Elements. The object classes and attributes contained in Open Directory, but absent from Active Directory, will be shown. Expand the Classes folder and then select the following classes and attributes. Note that you should not select all of the attributes because the other attributes may already be included within Active Directory or are not needed. For example, a user in Active Directory is composed of the following objectClasses: User, Person, and OrganizationalPerson. The User objectClass already contains the userCertificate and jpegPhoto attributes, so you do not need to include them in the apple-user objectClass. By adding apple-user to the objectClasses of the User objectClass in Active Directory, Apple-specific attributes will be added to a User. The object classes and attributes that are added are nearly all "apple-" specific. The "OS X Directory Data" appendix in the OS X Server Open Directory Administration guide describes the object classes and attributes selected in the following list.

```
[+] apple-computer-list
        [+] subclassOf: top
        [X] possSuperior: top
        [+] rdnAttId: cn
        [+] mayContain: apple-computer-list-groups
        [+] mayContain: apple-computers
        [X] mayContain: apple-generateduid
        [+] mayContain: apple-keyword
        [+] mayContain: apple-mcxflags
        [+] mayContain: apple-mcxsettings
        [X] mustContain: cn
```

Make sure that any other nonspecific attributes are deselected (contain an "x" in the checkbox). The only checkboxes that should be selected within the classes are shown above. When selecting schema classes and attributes, be sure to enable the desired class and then click to disable undesired attributes within a class.

For example, for the apple-computer-list, select apple-computer-list and then deselect mayContain: apple-generateduid, possSuperior: top, mayContain: apple-generateduid, and mustContain: cn.

The following is a list of objectClasses and attributes to select. Make sure that all of the objectClasses and attributes are selected, and deselect any attributes that are not contained in the list.

- apple-computer
  - subclassOf: top
  - rdnAttId: cn
  - mayContain: apple-category
  - mayContain: apple-computer-list-groups
  - mayContain: apple-hwuuid
  - mayContain: apple-keyword
  - mayContain: apple-mcxflags
  - mayContain: apple-mcxsettings
  - mayContain: apple-networkview
  - mayContain: apple-service-url
  - mayContain: apple-xmlplist
  - mayContain: macAddress
- apple-computer-list
  - subclassOf: top
  - rdnAttId: cn
  - mayContain: apple-computer-list-groups
  - mayContain: apple-computers
  - mayContain: apple-keyword
  - mayContain: apple-mcxflags
  - mayContain: apple-mcxsettings
- apple-configuration
  - subclassOf: top
  - rdnAttId: cn
  - mayContain: apple-data-stamp
  - mayContain: apple-keyword
  - mayContain: apple-xmlplist
- apple-group
  - subclassOf: top
  - rdnAttId: cn
  - mayContain: apple-group-homeowner
  - mayContain: apple-group-homeurl
  - mayContain: apple-keyword
  - mayContain: apple-mcxflags
  - mayContain: apple-mcxsettings
  - mayContain: apple-user-picture

```
apple-user
            subclassOf: top
            rdnAttId: cn
            mayContain: apple-imhandle
            mayContain: apple-keyword
            mayContain: apple-mcxflags
            mayContain: apple-mcxsettings
            mayContain: apple-user-authenticationhint
            mayContain: apple-user-class
            mayContain: apple-user-homequota
            mayContain: apple-userhomesoftquota
            mayContain: apple-user-mailattribute
            mayContain: apple-user-picture
            mayContain: apple-user-printattribute
            mayContain: apple-webloguri
mount
            subclassOf: top
            rdnAttId: cn
            mayContain: mountDirectory
            mayContain: mountDumpFrequency
            mayContain: mountOption
            mayContain: mountPassNo
            mayContain: mountType
```

9. Choose File > Create LDIF File and save the LDIF file. This LDIF file contains all the schema modifications required for Active Directory.

10. Verify that you receive the message, "LDIF file created: 27 attributes, 6 classes, 0 property sets, 0 updated present elements." If you did not export 27 attributes and 6 classes, recheck your selections and export again.

Modifying the Resulting LDIF File

Once you export the LDIF file from Active Directory Schema Analyzer, the file must be modified. Some of the object classes need to be changed, and some object classes require additional prefixes. You also need to specify where in Active Directory the required objects can be created.

Updating objectClassCategory.

The LDIF file from the Active Directory Schema Analyzer results in all objectClasses being assigned an attribute objectClassCategory with a value of 1. An objectClassCategory of 1 means that the object is a structural type, and an objectClassCategory of 3 is an auxiliary type. Structural objectClasses can be used to make objects within Active Directory, while auxiliary objectClasses can only be used to extend a structural object (or other auxiliary objects). User, Group, and Computer objectClasses exist within Active Directory already, so the Apple associated objectClasses that extend Users, Groups, and Computers need to be changed to the objectClassCategory of 3 (auxiliary).

1. Open the LDIF file in Wordpad.
2. Find the apple-user, apple-group, and apple-computer objectClasses in the Classes section of the LDIF file and change the objectClassCategory to 3, as shown for the apple-user objectClass:

```
# Class: apple-user
dn: cn=cls-apple-user,cn=Schema,cn=Configuration,dc=X
changetype: ntdsschemaadd
objectClass: classSchema
governsID: 1.3.6.1.4.1.63.1000.1.1.2.1
ldapDisplayName: apple-user
adminDescription: apple user account
objectClassCategory: 3
```

3. To effectively use auxiliary objectClasses, they need to be associated with current objectClasses in Active Directory. At the end of the LDIF file, add the following three sections to extend the User, Computer, and Group objectClasses in Active Directory with the apple-user, apple-computer, and apple-group auxiliary classes:

```
# Add the new class to the user object
           dn: CN=User,CN=Schema,CN=Configuration,DC=X
           changetype: modify
           add: auxiliaryClass
           auxiliaryClass: apple-user
           -

           # Add the new class to the computer object
           dn: CN=Computer,CN=Schema,CN=Configuration,DC=X
           changetype: modify
           add: auxiliaryClass
           auxiliaryClass: apple-computer
           -

           # Add the new class to the group object
           dn: CN=Group,CN=Schema,CN=Configuration,DC=X
           changetype: modify
           add: auxiliaryClass
           auxiliaryClass: apple-group
           -
```

Note: After each "-" line above, there must be a blank line, or the schema modifications will fail.

4. Save the LDIF file, but do not close the document.

Updating Prefixes.

The Active Directory Schema Analyzer adds a prefix of "cls" to all object classes and "attr" to all attributes. Because most of the object classes and attributes already have the "apple-" prefix, you need to remove the "attr-" and "cls-" prefix:

1. If you closed it after the previous action, open the LDIF file with Wordpad in Windows.
2. In the Edit menu, select Replace.
3. Search for "dn: cn=cls-" and replace it with "dn: cn=" (do not specify the quotes).
4. Search for "dn: cn=attr-" and replace it with "dn: cn=" (do not specify the quotes).

Microsoft recommends that all vendor-specific object classes and attributes include a prefix with the vendor's name. The majority of object classes and attributes already include the "apple-" prefix; however, the mount object class does not have a prefix and should be updated with the "apple-" prefix. Each of the following lines lists the addition of the "apple-" prefix to the start of the dn:

Replace: *dn: cn=mountDirectory,cn=Schema,cn=Configuration,dc=X*
With: *dn: cn=apple-mountDirectory,cn=Schema,cn=Configuration,dc=X*

Replace: *ldapDisplayName: mountDirectory*
With: *ldapDisplayName: apple-mountDirectory*

Replace: *dn: cn=mountDumpFrequency,cn=Schema,cn=Configuration,dc=X*
With: *dn: cn=apple-mountDumpFrequency,cn=Schema,cn=Configuration,dc=X*

Replace: *ldapDisplayName: mountDumpFrequency*
With: *ldapDisplayName: apple-mountDumpFrequency*

Replace: *dn: cn=mountOption,cn=Schema,cn=Configuration,dc=X*
With: *dn: cn=apple-mountOption,cn=Schema,cn=Configuration,dc=X*

Replace: *ldapDisplayName: mountOption*
With: *ldapDisplayName: apple-mountOption*

Replace: *dn: cn=mountPassNo,cn=Schema,cn=Configuration,dc=X*
With: *dn: cn=apple-mountPassNo,cn=Schema,cn=Configuration,dc=X*

Replace: *ldapDisplayName: mountPassNo*
With: *ldapDisplayName: apple-mountPassNo*

Replace: *dn: cn=mountType,cn=Schema,cn=Configuration,dc=X*
With: *dn: cn=apple-mountType,cn=Schema,cn=Configuration,dc=X*

Replace: *ldapDisplayName: mountType*
With: *ldapDisplayName: apple-mountType*

Replace: *dn: cn=mount,cn=Schema,cn=Configuration,dc=X*
With: *dn: cn=apple-mount,cn=Schema,cn=Configuration,dc=X*

Replace: *ldapDisplayName: mount*
With: *ldapDisplayName: apple-mount*

5. Save the LDIF file, but do not close the document.

Updating possSuperiors

Active Directory includes an attribute within each object class that specifies what parent an object can have in the directory. This does not apply to auxiliary classes; it applies only to the object classes used to create objects within the directory. You need to specify where the objects can be created by specifying the possSuperiors attribute. For all apple object classes that can be used to create objects in Active Directory, specify possSuperiors of "organizationUnit" and "container." If you wish to specify where objects can be created, find the following object classes, remove any possSuperiors if they exist, and add "organizationalUnit" and "container" as values for the possSuperiors attribute. The possSuperiors attributes can go anywhere within the appropriate object class sections.

```
apple-computer-list
        possSuperiors: organizationalUnit
        possSuperiors: container
apple-configuration
        possSuperiors: organizationalUnit
        possSuperiors: container
apple-mount
        possSuperiors: organizationalUnit
        possSuperiors: container
```

Verifying the LDIF File

To ensure that the LDIF file was correctly created, verify the following information:

- apple-user, apple-group, and apple-computer have an objectClassCategory of 3.
- The Attributes section contains 27 attributes, and all attributes have an attributeID that starts with 1.3.6.1.4.1.63.1000.1.1.1.
- The Classes section contains 6 classes, and all governsIDs start with 1.3.6.1.4.1.63.1000.1.1.2.
- All attributes and classes have an "apple-" prefix in their dn and ldapDisplayName.
- After each "-" line, there is a blank line.
- Every objectClass that does not have an objectClassCategory of 3 has organizationalUnit and container as possSuperiors.

Note: It is critical that there be exactly 27 attributes and six classes, and that all attributes and classes have the Apple prefix. If this is not true, do not proceed until you have resolved these issues.

If macAddress is in the list of attributes to be created, you may be using Windows Server 2000 or Windows Server 2003. macAddress was included in Windows Server 2003R2 and later, and is required for this whitepaper (note that Windows Server 2003 SP2 is not the same as Windows Server 2003R2). macAddress should be included in the apple-computer objectClass, but should not be listed under the Attributes section. This means that the apple-computer objectClass will have the macAddess attribute associated with it, but the macAddress attribute is not created when doing this schema modification. macAddress should already exist in Windows Server 2003R2 and later.

Updating the Schema on a Domain Controller in the Forest

The LDIF file created in the previous section can now be used to update the schema on a domain controller. The schema changes will be replicated to the rest of the forest during the next replication cycle. A domain controller must have the Flexible Single Master Operations (FSMO) role in order to apply schema modifications. See http://support.microsoft.com/kb/324801 for information on how to view and transfer FSMO roles.

The LDIF file can then be imported using the ldifde command.

1. Copy the LDIF file created in the previous section to the domain controller where you plan to implement the Active Directory schema modifications.
2. On the domain controller that has been designated the schema master, import the LDIF file using the ldifde command. The following command assumes that the LDIF file is named "apple-mods.ldf" and the domain name of the domain controller is EXAMPLE.COM:

```
ldifde /j . /k /i /f apple-mods.ldf /v /c "DC=X" "DC=EXAMPLE,DC=COM"
```

Note that /k will ignore errors if objectClasses or attributes already exist in the schema, /i will perform an import, /f specifies the file to import, /v is verbose output, /c will replace "DC=X" with the correctly formatted distinguishing name for the domain, and /j will send a copy of the output to ldif.err and ldif.log in the current directory. Also do not change "DC=X," as it produces the formatting required to use the /c option.

Additional Changes

Indexing and replicating to the Global Catalog

When an OS X system searches Active Directory for policy applied directly on a computer account or as part of a computer list, it looks for the MAC address and apple-hwuuid attribute in computer accounts in the Global Catalog. It searches for the MAC address of the primary interface of the system (usually the built-in Ethernet port or wireless port on a MacBook Air computer). The system does not have to communicate with Active Directory over this network port. The MAC address attribute is populated in a computer account when a Mac computer is bound to Active Directory.

Because a Mac will periodically search for policy applied to its computer account, the MAC address attribute should be indexed within Active Directory to improve search time and reduce overhead on domain controllers. Indexing the macAddress and apple-hwuuid attributes within Active Directory will provide greater responsiveness to searches and reduce CPU overhead on domain controllers. Also, since the Global Catalog is searched for the macAddress and apple-hwuuid, those attributes must be replicated to the Global Catalog in order for them to be found. Additionally, if you are populating uidNumber and gidNumber in user accounts and manually mapping those attributes, uidNumber and gidNumber must be indexed and replicated to the Global Catalog as well.

Visit http://support.apple.com/kb/HT4687 for more information.

Verifying the Changes

Once the schema modifications are complete, Workgroup Manager can create policy on Users, Groups, Computers, and Computer Lists. Use the following steps to verify that the schema modifications were successfully applied:

1. In Active Directory Users and Computers, create a security Group and populate it with Active Directory users who log in to Mac computers.
2. On an OS X client with Workgroup Manager installed, join Active Directory. If the client was bound before the schema changes were applied, you need to refresh the settings by either rebooting or restarting Open Directory on the client: sudo killall opendirectoryd
3. Launch Workgroup Manager, but do not authenticate. Click Cancel at the authentication window.
4. In the Server menu, select View Directories.
5. In the small globe in the upper right corner of the Workgroup Manager window, select Other. Select Active Directory and All Domains (or your specific domain if that is how you have configured the settings when joining Active Directory).
6. Select the Group tab and find the Group you created in step 1.

7. Click the Preferences button and select the System Preferences icon.
8. In the upper right corner, click the lock button and authenticate as an Active Directory Administrator who has write access to attributes of this Active Directory Group.
9. Change the Manage radio button to Always, click Show None, and click Apply.
10. Log out of the Mac and log in as an Active Directory user who is a member of the Group created in step 1. Go to System Preferences and note that all System Preferences panes are dimmed.

Support

Once the schema modifications have been applied to Active Directory, the AppleCare Protection Plan, a unique service and support solution that extends the complimentary coverage on the Mac, can assist you in integrating OS X clients into Active Directory. AppleCare representatives can help you validate the Apple-specific schema extensions. If there are any discrepancies, they can identify them. AppleCare personnel can also help you apply policy using Workgroup Manager to an Active Directory extended schema.

Note that AppleCare does not offer support for creating the schema modifications or extending the Active Directory schema. If you need assistance, Microsoft can provide support for extending the Active Directory schema.

Appendix B: Managing Users and Policies on OS X With Workgroup Manager and Active Directory with Extended Schema

To provide and enforce policies such as restricting access to specific applications or specifying when users' screen savers activate without installing additional software, administrators can modify the Active Directory schema to support OS X Lion. This appendix is a how-to guide for system administrators who want to use a combination of Workgroup Manager and Active Directory with extended schema to authenticate Mac users and apply policies to their actions, thereby fully integrating Mac computers into an existing Active Directory infrastructure.

Managed Preferences, Apple's own comprehensive client management architecture, are typically stored as records in Open Directory, the native directory services in OS X Server. However, to fully integrate Mac systems into Active Directory, administrators can store OS X policy information directly within Active Directory. OS X Server is not required to create Managed Preference-based policy in Active Directory. The easiest way to accomplish this is with Workgroup Manager, a free user management tool from Apple.

Workgroup Manager can be used to create Computer Lists in Active Directory and to apply policy to Users, Groups, Computers, and Computer Lists. Users, Groups, and Computers can be created in Active Directory using standard Microsoft tools. Workgroup Manager is one of the OS X Server Administration Tools and comes with OS X Server. Download the latest version of the OS X Server Administration Tools at www.apple.com/downloads.

Connecting Workgroup Manager to Active Directory

By joining Mac computers to an existing Active Directory domain, you can provide user authentication and policy directly to Mac computers centrally from Active Directory. Workgroup Manager communicates with Active Directory through the Active Directory configuration in Directory Services.

To join Mac systems to Active Directory:

1. Open Directory Utility in /System/Library/CoreServices.
2. Click the Services button.
3. If the lock in the lower left corner is not selected, click the lock and enter a local administrator's user name and password.
4. Enter the Active Directory domain, for example: "corp.example.com."
5. In the Computer ID field, enter the computer name.
6. Click Bind. Enter the user name and password of an Active Directory account that has the right to join computers to the domain. If the computer account is to be created in a different OU in Active Directory, the level at which administrative powers are commonly delegated, change the Computer OU.

7. Click OK to join.
8. Quit Directory Utility.

After joining Active Directory, use Workgroup Manager to view and edit Mac-specific policy in Active Directory.

To connect to Active Directory with Workgroup Manager:

1. Launch Workgroup Manager from /Applications/Server. It will prompt for authentication details. Click Cancel because the connection is not directly to Active Directory, but rather through the Active Directory configuration of Open Directory.
2. In the Server menu, choose View Directories. Ignore any warning messages about connecting to a local configuration database.
3. In the upper left corner, notice the domain selection globe. Select this globe and choose "Other..." Choose Active Directory > All Domains (or your specific domain).

The Users from within Active Directory should now appear in the user list, and Workgroup Manager should now be able to view data from within Active Directory.

Workgroup Manager can be used to apply policy to users, groups, computers, and computer lists. When using Workgroup Manager with Active Directory, users and groups can be created using Active Directory tools such as Active Directory Users and Computers. Workgroup Manager is then used to apply policy to these objects. Workgroup Manager should be used to create computer lists, a guest computer account, and to add computers to computer lists. These objects are created at the root of the domain in a container called "OS X." The following section outlines the steps required to optimize Workgroup Manager to work with Active Directory.

Limiting Search Results

When Workgroup Manager is first launched, it displays the Accounts section and the Users tab. It also displays a list of Users. In many Active Directory environments, the maximum number of Users that can be displayed is 1000. If you have a large number of Users, you may want to limit the number of displayed Users to the requested records.

The following steps will help to limit the search results to only the requested records:

1. In Workgroup Manager, choose Preferences in the Workgroup Manager menu.
2. Select the checkbox next to "Limit search results to requested records" (use "*" to show all).
3. Close the Preferences window.

Note that the list of Users is empty. To display a specific group of Users, enter a term in the search box above the User list. To view all Users, search by entering "*" in the search box.

Interface

The Workgroup Manager interface has two major sections: Accounts and Preferences. Under each section, there are four tabs: Users, Groups, Computers, and Computer Lists. The tabs determine the object, and the section determines the action being applied.

Creating Users, Groups, and Computers

As a standard practice, creating Users and Groups should be accomplished with Active Directory Users and Computers or another Windows-based tool. Workgroup Manager can then be used to apply policies to existing Users and Groups.

Creating computer accounts

When a Mac system is joined to Active Directory, a computer account is created that specifies the computer name in the settings specified when joining Active Directory, followed by "$". If the computer account was created in Active Directory prior to joining, or a Mac was not cleanly unbound, the computer name will be changed to match the computer account name found in Active Directory by searching for the MAC address of the primary interface.

Creating a Computer List using Workgroup Manager

OS X can manage computers using Computer Lists. The following example shows how to create a Computer List using Workgroup Manager:

1. Open Workgroup Manager and click Cancel when the authentication dialog appears.
2. Choose Server > View Directories from the menu bar.
3. Under the small globe in the upper left corner, select "Other..." and then select the Active Directory Node.
4. Click the lock in the upper right corner and authenticate as an Active Directory administrator.
5. Select the Computers Groups tab.
6. Click "Add Group"

Managing Policy with Managed Preferences

Workgroup Manager can create policy on Users, Groups, Computers, and Computer Lists. The following examples illustrate how to set policy at the User and the Computer level. These settings can also be applied to a User Group or Computer List. For more information on Managed Preference settings not specifically related to Active Directory, see the OS X Server User Management guide at www.apple.com/server/macosx/resources.

Common User-Level Settings

Application restrictions.

Workgroup Manager can be used to manage common user settings such as restricting access to specific applications. The following example illustrates how to accomplish this task.

1. Open Workgroup Manager and click the user in question. Although this policy will be deployed to a test user, it could just as easily be deployed to a Group or Computer List.
2. Authenticate to the directory using the Lock icon at the top of the right side of the screen.
3. Click the user and then click the Preferences button in the toolbar.
4. Once the Managed Preferences screen is open, click the Applications icon to set the application restriction. This will bring up the screen used to configure the policy. Click the Folders button at the top, then select the Applications tab in the "Restrict which applications are allowed to launch" section.
5. In this example, John Doe will only be allowed to open applications in the /Applications folder, but not from his home folder. To add the Applications folder to the list of allowed applications, click the Always radio button in the Manage field, and check the "Restrict which applications are allowed to launch" box. Next, click the plus button (+) to select /Applications and add it to "Allow applications within these folders." In the "Disallow applications within these folders" section, select the current home folder. Workgroup Manager will add "~/" to the disallowed folders.
6. Log in as John Doe to a workstation that has been bound to Active Directory. Attempt to drag an application to your home folder and launch it to test whether or not the policy was implemented correctly .

Screen Savers

Due to corporate policy or auditing requirements, it is important to specify when users' screen savers activate and whether or not a password is required to deactivate screen savers. To specify screen saver settings, do the following:

1. Select a Computer, or Computer List in Workgroup Manager and click Preferences.
2. Click the Details tab and select Screen Saver.
3. Click the Pencil icon to edit the Screen Saver preferences.
4. Select Always and click the disclosure triangle next to Always.
5. Click New Key to add a new managed preference.
6. Change the New Item to Require Password and set the value to true.
7. Select Often and click the disclosure triangle next to it.

8. Click New Key to add a new managed preference.
9. Change the New Item to Idle Time and set the value to the number of seconds of idle time until the screen saver activates.

Note that the idle time is an Often setting that the user can override by changing the value in the Screen Saver system preference. If users should not be able to override this setting, use Managed Preferences to prevent user access to the Screen Saver Preference pane.

Login window disclaimer and appearance

Many companies require that a disclaimer such as "Unauthorized use is not permitted" appear in the login window. To implement this disclaimer:

1. Go to the Login section of Overview in Workgroup Manager.
2. Select the Window tab and add the disclaimer text that will appear in the Login window. Note that this setting only applies at the Computer and Computer List level, since User-level settings would not apply when a user is not logged in.

Alternatively, you can use create a policy banner following http://support.apple.com/kb/HT4788. If you would like to include graphics or the policy banner is long, this may be the preferred option.

Mobile accounts

Mobile accounts allow a user's credentials to be cached at login and enable the user to authenticate when off the corporate network. These settings are specified in the Mobility section under the Account Creation tab. You can also specify whether to encrypt the user's home directory with FileVault in this same section. FileVault encrypts the information in a user's home folder. The data in the home folder is encrypted so that information is secure if a computer is lost or stolen.

Volume mounting at login

The home directory specified in the user's Active Directory profiles will automatically be mounted. If there are other file shares that need to be mounted at login, they can be specified in the Login section under Items. The volume can either be mounted via the Finder or created using a Favorite. To create a Favorite:

1. In the Finder, choose "Connect to Server" in the Go menu.
2. Enter the URL for the share (for example: smb://winserver.example.com/share/docs).
3. Do not click Connect. Click "+" to add as a Favorite.
4. Drag the newly created Favorite from ~/Library/Favorites to the Items list in Workgroup Manager.
5. Select "Mount Sharepoint with user's name and password" if required.

Restricting access to external storage

To safeguard intellectual property, many organizations have a policy to deny use of CDs, DVDs, USB flash drives, or USB/FireWire external hard drives to prevent users from copying files. It is also easy to use Workgroup Manager to apply a policy that prevents or limits external media from mounting.

Restricting access to login window

To prevent certain users from logging in to a computer, select a Computer or Computer List in Workgroup Manager and then go to the Login preferences. In the Access tab, add the users you want to allow or deny to the Access Control list.

Managing the Dock

You may also want to prepopulate the Dock with commonly used applications and allow users either to modify the Dock or to pin certain applications to the Dock. Even if some applications are pinned, users can be allowed to add and remove other items from the Dock.

To manage a user's Dock:

1. Select a User, Group, Computer, or Computer List in Workgroup Manager and click Preferences.
2. Click the Overview tab and then select Dock.
3. Under Dock Items, select Once if you want to apply the settings but allow the user to change the settings, or Always if you want to force the settings to remain.
4. Add the Applications and Documents and Folders to the lists provided, and select Merge with User's Dock to keep the user's current Dock settings.

Managing applications

Many application preferences can be managed. If an application has a manifest, it can be selected using the core services bundle mentioned in the "Screen savers" section. However, an application's preferences can be managed even if it does not have a manifest. To manage application preferences:

1. Select the preference from ~/Library/Preferences in the Preference editor in Workgroup Manager.
2. Remove any values and keys that do not need to be managed, and modify the ones that need to be managed.
3. In the following example, the preference for the format of a new document in TextEdit will be changed from rich text to plain text:
4. Open TextEdit and change the preference for New Documents to Plain Text. This will ensure that the preference key is stored in the

preference file. Be sure to quit TextEdit so that the preference file is saved to disk.

5. Select a User, Group, Computer, or Computer List in Workgroup Manager and click Preferences.
6. Authenticate by clicking the lock in the upper right corner.
7. Select the Details tab.
8. Click "+" to import the preference.
9. Select the TextEdit application in /Applications. Since the application does not have a preference manifest (a list of preferences that can be managed for that application), the preference file will be imported.
10. Click the Pencil icon to edit the newly imported preferences.
11. Disclose the triangle for Often, and remove all lines except "RichText" by selecting them and clicking Delete.
12. Set the value for RichText to false.
13. Force the preference by dragging the RichText line to the Always section.
14. Click Apply Now.
15. Log in as a user whose policy is affected by this setting. Open TextEdit and verify that the default format for a new document in TextEdit preferences is Plain Text. Change it to Rich Text, quit and relaunch TextEdit, and verify that the setting was changed back to Plain Text.

User Information

Once OS X is bound to Active Directory, Active Directory is automatically added to the Contacts Search Path in Directory Utility. This allows the Address Book and Mail features in OS X to automatically search for user information in Active Directory. The schema modifications add extra fields to user information, but the majority of information such as telephone numbers, addresses, and email are accessed from standard Active Directory attributes. Normally, these are set within the General and Address tabs in the Properties of an Active Directory user's profile.

Mail

Mail allows users to send, receive, and organize email messages. It is fully integrated with Address Book to look up contacts and autocomplete addresses to email messages. If a computer is joined to Active Directory and the Contacts search policy in the Active Directory configuration is specified, autocompletion will search Active Directory for contact information. Users typing an address into an email message will now have addresses automatically completed for them. This only works for users who have a populated email attribute within Active Directory.

Address Book

Address Book provides a flexible and convenient way to store contact information. Because Address Book is integrated with Mail, iChat, and other applications, users can enter contact information once and have instant access to it from multiple applications. Address Book can also be used to look up contact information in a directory service, such as Active Directory. Users can click the Directory group and search on a user's name or email address. If the computer is bound to Active Directory, contact information in Active Directory will be found. Users can then drag the contact into their local Address Book. Address Book also provides options for displaying phone numbers in large type for easy dialing, mapping addresses with Google Maps, or easy copying of a correctly formatted address block (Copy Mailing Label). All of these features can be accessed by searching on Active Directory Users and double-clicking the user's name.

Using Workgroup Manager, you can also specify a chat or weblog address within Active Directory. This information will appear in Address Book along with the other contact information.

To add chat or weblog addresses to Active Directory Users:

1. In Workgroup Manager, select the Active Directory domain.
2. Select the User tab and Account Section and find an Active Directory user.
3. Select the user and then select the Info tab.
4. Authenticate by clicking the lock in the upper right corner and entering an Active Directory administrator's user name and password.
5. Add a chat or weblog URL and click Save.

You can also select multiple users and enter a URL for a chat or weblog address. Workgroup Manager will automatically add the user's short name at the end of each URL when you click Save.

Printers

Printers advertised in Active Directory can be discovered and added easily to OS X. To discover a published printer, do the following:

1. Open System Preferences and select Print & Fax.
2. Click "+" to add a printer.
3. The printers that are advertised in Active Directory should appear under Default. Select a printer and then click Add.

Appendix C:
Third-Party Add-On Solutions

If your deployment requires DFS shares or GPOs, you can choose a third-party product to extend the capabilities of the Apple solution.

- **Group Logic ExtremeZ-IP**. www.grouplogic.com
  With this Apple Filing Protocol (AFP) server for Windows servers, Mac clients can access files on a Windows server using the native file-sharing protocol, AFP.
- **Centrify DirectControl**. www.centrify.com
  This Active Directory plug-in enables OS X to use Active Directory GPOs without requiring any schema modification. .
- **PowerBroker Identity Services Enterprise Edition.**
  www.beyondtrust.com
  This Active Directory plug-in enables OS X to use Active Directory GPOs and Workgroup Manager without requiring any schema modification.
- **Thursby ADmitMac.** www.thursby.com
  This directory services Active Directory plug-in and SMB client supports DFS shares.
- **Objective Development Sharity.** www.obdev.at/products/sharity
  This SMB client supports DFS shares.

Mention of third-party products is for informational purposes only and constitutes neither an endorsement nor a recommendation. Apple assumes no responsibility with regard to the performance or use of these products. All understandings, agreements, or warranties, if any, take place directly between the vendors and the prospective users. Every effort has been made to ensure that the information in this manual is accurate. Apple is not responsible for printing or clerical errors.

Because Apple periodically releases new versions and updates to its software, images shown in this white paper may be different from what you see on your screen.

11-14-2011