ADmitMac®

Administration Guide

Mac Client for
Microsoft Active Directory
and NT Directory Services

Version 8.0

Mac Universal

THURSBY
Software

Copyright, Warranty and Trademark Notices

Thursby Software Systems, Inc. (TSS) warrants that at the time of delivery of the original software supplied to the Licensee, and for a period of ninety (90) days thereafter, that the original software will perform in accordance with the applicable Software Product Description (SPD). TSS does not warrant that the Software will meet all of Licensee's requirements or will operate uninterrupted or error-free.

The extent of TSS's liability under this warranty shall be limited to supplying, as soon as practicable, Code Corrections that TSS determines to be necessary, provided that written notice of a claimed problem is received by TSS within the warranty period.

THURSBY SOFTWARE SYSTEMS, INC. MAKES NO WARRANTIES, EITHER EXPRESSED OR IMPLIED, REGARDING THE ENCLOSED COMPUTER SOFTWARE PACKAGE, ITS MERCHANTABILITY OR ITS FITNESS FOR ANY PARTICULAR PURPOSE. THE EXCLUSION OF IMPLIED WARRANTIES IS NOT PERMITTED BY SOME STATES. THE ABOVE EXCLUSION MAY NOT APPLY TO YOU. THIS WARRANTY PROVIDES YOU WITH SPECIFIC LEGAL RIGHTS. THERE MAY BE OTHER RIGHTS THAT YOU MAY HAVE WHICH VARY FROM STATE TO STATE.

THURSBY SOFTWARE SYSTEMS, INC.
4901 South Collins Street
Arlington, Texas 76018 U.S.A.
http://www.thursby.com
sales@thursby.com

Contents

Overview

ADmitMac® is a software solution that enables Mac users to participate in Microsoft networks, taking advantage of the directory services provided by both Active Directory and NT Directory Services. ADmitMac allows administrators to manage their domain users in a consistent way without regard to what kind of computer they use. ADmitMac allows users to log into a Macintosh with their domain credentials and have access to files in their home directory. Users can log into any Macintosh equipped with ADmitMac and their desktop environment and documents will be preserved. ADmitMac provides secure access to both Active Directory and NT domains. Passwords are never sent over the network in plain text. Also, no security certificates are required.

For our Volume License Agreement (VLA) customers with large deployments, ADmitMac includes a deployment utility to create custom ADmitMac install packages to automatically configure the computers you administer with custom settings. By following the instructions in the panels, you can pick and choose the network configurations for your custom installer package depending upon your network needs. When you have completed configuring your settings, the ADmitMac Deployment utility automatically exports the package. The utility can even upload the settings to a web site for easy access during deployment.

With AD Commander, you can access and update the Active Directory contents on your Domain from your Macintosh. You may use Apple's Workgroup Manager with ADmitMac to allow you to integrate Apple's Mac OS MCX settings with your Active Directory domain server, or Windows Group Management Policy Management Console along with ADmitMac's ADM plugin to allow MCX settings integration.

ADmitMac Features and Benefits

- Administrators can easily manage Macs in their Microsoft Windows domain - without special training.
- Installs on the Mac with no Active Directory schema changes required.
- Provides secure access using Kerberos.
- Provides bi-directional file and printer sharing.
- Supports Windows login security restrictions.
- Allows users to easily change passwords.
- Support for Dfs - home directories can be mounted using Dfs, and Shares on the Mac support Dfs.
- Supports NTFS file format - does not create "dot-underscore" files.
- Supports Windows ACLs (Access Control Lists).
- Administrators can utilize MCX settings using Apple's Workgroup Manager or Windows Group Policy.
- Supports long share names.
- Preserves users' custom desktop and documents no matter which computer they log into.
- Offers complete interoperability with Services for Macintosh.
- Works with older NT directory services.
- Users can mount shared folders via the ADmitMac Browser or Connect to Server.
- Allows for user login with home directories located on the Macintosh client's local hard disk.
- Fully signed and sealed (encrypted) LDAP connections prevent disclosure of user's personal information and prevent man-in-the-middle attacks.
- Support for bi-directional SMB-signed connections, NTLM SSP, and NTLMv2.
- Expired and reset passwords are handled correctly when users log in to the Macintosh desktop.
- Caches user credentials for mobile user access when not connected to the network.
- Supports browsing for published shares.
- Print client can access shared printers. Printers may be configured by browsing the list of printers published in a domain, or manually.
- Kerberos credentials are set up automatically when a user logs in. No changes to /etc/authorization required.

- Cross-realm trust with MIT Kerberos.
- Administrators can limit domain search paths for users, groups, and published printers and shares.
- Administrators can give domain members administrative privileges based on username or group membership.
- Administrators can give administrative privileges to the user specified as the machine's manager in the domain's computer records.
- Supports Mac OS X Server service principal names.
- Home directories may be located at a path where the user does not have access to the parent folders.
- ADmitMac deployment utility (for VLA customers with large deployments) creates custom install packages for multi-computer installations.
- Dynamic DNS registration support: the Mac will register its IP addresses with DNS.
- AD Commander allows Administrators to edit Active Directory users and groups.

Security in ADmitMac

ADmitMac automatically configures the Macintosh to use Kerberos (for kerberized services), and obtains the necessary security keys from the domain. Kerberos is used to provide secure directory access that resists spoofing and "man-in-the-middle" attacks. All communications between the Macintosh and the directory service are encrypted. At login, ADmitMac authentication is performed using either Kerberos or NTLMv2. Older systems can be accessed with older LanMan methods depending on the security policy settings. ADmitMac can also utilize SMB message signing on its CIFS client and server for digitally signed communication when necessary (not required). You can configure ADmitMac to access shares using these services without having to re-enter your credentials (one-time login). ADmitMac allows for credential caching when disconnected from the network.

ADmitMac is compatible with Microsoft's Highly Secure Security templates for Windows 2003, and will operate in any domain where the HISECDC security template has been applied to the domain controllers. For more information about Microsoft's highly secure templates, visit Microsoft's Predefined Security Templates pages.

If you are printing this document, visit http://msdn.microsoft.com and search for HISECDC.

ADmitMac Requirements

ADmitMac requires the following hardware and software for the Macintosh client:

- Macintosh systems running OS X Mountain Lion or OS X Mavericks (10.8.x or 10.9.x with the latest updates)
- Any hardware required to use TCP/IP

ADmitMac requires at least one of the following servers:

- Microsoft NT (service pack 6) or later operating an NT domain
- Microsoft Windows 2000 (service pack 4) with Active Directory
- Microsoft Server 2003 with Active Directory
- Microsoft Server 2008 with Active Directory
- Microsoft Server 2012 with Active Directory

ADmitMac Conforms to the following RFCs:

1001,1002 Protocol standard for a NetBIOS service on a TCP/UDP transport
1510 The Kerberos Network Authentication Service (V5)
Kerberos features are based on MIT version 1.3.1
1777 Lightweight Directory Access Protocol (LDAP)
2743 Generic Security Service Application Program Interface Version 2
1964 The Kerberos Version 5 GSS-API Mechanism
2222 Simple Authentication and Security Layer
3244 Microsoft Windows 2000 Kerberos Change Password and Set Password Protocols

ADmitMac also conforms to Microsoft SMB/CIFS standards.

Planning and Deployment

Macintosh Computers in an Active Directory Network

Each organization will want to customize their deployment to meet their specific needs. ADmitMac supports a myriad of network settings for the most efficient configuration possible.

Planning is required to make sure ADmitMac is deployed with the least effort. We suggest you first think about the desired user experience with Active Directory after it is deployed, then work back to determine the details of how to deliver that experience.

Generally, we recommend starting with an ADmitMac test system and configuring the system manually. For VLA customers with large deployments, once you are familiar with ADmitMac's settings, you will want to use the ADmitMac Deployment utility to build your own custom install packages that will automatically configure your clients when installed.

Planning

The following sections cover typical Macintosh user experiences with Active Directory based networks followed by more detailed topics so that you will understand your specific deployment needs.

Planning for Home Folder Storage

Active directory users can have a network home folder attribute assigned that indicates where their home folder resides. Thursby recommends *Create Mobile Account at Login* to provide cached credentials for users who may work while disconnected from the domain. For users not needing cached credentials, ADmitMac supports the following modes for providing a user with their home folder:

- *Use Network Home Folder* to mount the user's network home folder.
- *Use Local Home Folder* to allow user to create and use a local home folder. This is an option for users in environments where network home folders are not supported, or users who always use the same Macintosh. If network home folders are present, they can be mounted as volumes on the desktop.
- *Use Either* to use a network home folder if provided, otherwise create and use a local home folder.
- *Create Mobile Account at Login* to provide an option for users who wish to use Apple's Home Sync feature.

Home Folder Location

The default location of a network user's home folder is **/Domain/<domainname>/Users/** on the local machine. You may elect to change that location by editing the above path in the following preferences file:

```
/Library/Preferences/com.thursby.CIFSPlugin.plist
```

First, make a copy of the file to the Desktop and convert it to a text file from a *Terminal* window, after using the cd (change directory) command to move to the Desktop:

```
cd /Users/Adminacct/Desktop <return>

sudo plutil -convert xml1 com.thursby.CIFSPlugin.plist <return>
```

Then open the file using *TextEdit*. Locate the following information:

```
<key>NFSHomeDirectoryFormat</key>

<string>/Domain/&lt;DOMAIN&gt;/Users/&lt;USERNAME&gt;</string>
```

Edit the second line to change the default Home Folder location. If, for example, you wished for the default location to be in /Users, the line would be edited as follows:

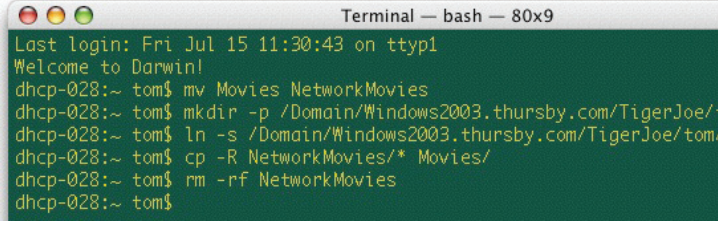
```
<string>/Users/&lt;USERNAME&gt;</string>
```

Save the file, close it, and drag it back to **/Library/Preferences**, overwriting the original file.

Hybrid Home Folders

You may want to provide network home folders to your users, but keep parts of their home folder on a local hard disk. For example, you might want to keep a user's Movies folder on the local disk and encourage them to keep their iMovie projects there to improve performance and reduce network storage needs. Symbolic links are used to point the Movies folder back to the local disk.

For example, you can direct a user's Movies folder to `/Domain/DomainName/LocalStorage/username/Movies/` using these steps:



```
Last login: Fri Jul 15 11:30:43 on ttyp1
Welcome to Darwin!
dhcp-028:~ tom$ mv Movies NetworkMovies
dhcp-028:~ tom$ mkdir -p /Domain/Windows2003.thursby.com/TigerJoe/
dhcp-028:~ tom$ ln -s /Domain/Windows2003.thursby.com/TigerJoe/tom
dhcp-028:~ tom$ cp -R NetworkMovies/* Movies/
dhcp-028:~ tom$ rm -rf NetworkMovies
dhcp-028:~ tom$
```

1. Log in as the user.
2. Launch the Terminal application.
3. Move the current folder out of the way:
   `mv Movies NetworkMovies`
4. Make a local storage folder:
   mkdir -p /Domain/*DomainName*/*LocalStorage*/*username*/Movies
5. Make a Symbolic Link to the local storage folder:
   ln -s /Domain/*DomainName*/*LocalStorage*/*username*/Movies Movies
6. Now copy the items to the new location, if you have any:
   `cp -R NetworkMovies/* Movies/`
7. Finally, remove the original folder:
   `rm -rf NetworkMovies`

Note: If the items have resource forks, you should move the contents of the NetworkMovies folder to the Movies folder using the Finder.

After testing your hybrid home folder, you will probably want to write a login script that will work for all users that will run from a login hook (see pg. 10 for more information).

Planning for the "User Experience" in Different Environments

Deploying ADmitMac to First Time Macintosh Users

Note: The following section on deployment is offered for our Volume License Agreement customers. The recommendations below will be of little use to customers who have purchased individual licenses.

The best way to deploy Macintosh computers for first time users is to use a master image that has been configured to use ADmitMac. Once the Macintosh is supplied to the user and they start the computer for the first time, it will be joined to the domain either manually or by using ADmitMac's automatic deployment features. See the **Installation** section below for methods of deploying ADmitMac on more than one computer.

Deploying ADmitMac to Existing Macintosh Users

Users are often required to log into computers using Active Directory domain credentials. Before installing ADmitMac, this may not have been possible for your Macintosh users. A local user will have a local account and password for their Macintosh and all files in their home folder will be owned by this local account.

After deploying ADmitMac, local user accounts may be *migrated* to domain accounts using the ADmitMac Home Mover Utility. A local user's home folder will be moved or copied from `/Users` to /Domain/*domainname*/Users, and all the file ownership will be changed so the files are owned by the domain account. Also, all resource data that points to files such as aliases and files in the Dock will be updated so that it points to the new folder location.

If a domain username and a local username are the same, the user will not be able to log into the Macintosh with their domain credentials. To prevent this problem, ADmitMac can rename the local user account when you run the Setup Assistant. Accounts are renamed by placing `local-` in front of the existing short name.

The user should log in at least one time while the Macintosh is still connected to the domain after an account is migrated to allow ADmitMac to cache information about the user. This will allow the user to continue to log in using their domain credentials even if the computer is disconnected from the domain.

To make sure users maintain local administrative privileges, follow the directions in the Give Domain Users Administrative Privileges section, pg. 6.

Deploying ADmitMac for Lab Use

Very often, the main factor determining user experience in a lab setting is the configuration of home folders, simply because a user's home folder contains preference settings and personal documents. Lab computers are often used by more than one person during any given day; therefore, the user's information will need to follow them from computer to computer. If the home folder is stored on a network, it is possible to give that user the same experience from all the computers in a lab or even in your network. However, it may not be possible to provide network home folders for thousands of users due to limited disk resources or network performance.

One Time Use Home Folders

If you want your users to have their desktop environment reset using a template you provide each time they log in, you can provide a login hook and script to handle this. When the user logs in, their home directory will be created from your template. When the user logs out, you can remove their home folder. An example script can be found in Sample Login Scripts, pg. 11.

Deploy ADmitMac to Laptop Users using ADmitMac-Local accounts

Notebook users frequently use their computers when they are not connected to the Active Directory services. When this happens, ADmitMac automatically switches to a cache mode, using information that it retrieved from the domain in the past. While ADmitMac is in cache mode, a user can log into the Mac a number of times set by the administrator (the default is 10) before they have to reconnect to the domain. In order for cache mode to be useful, the user must log into the Macintosh while connected to the domain at least one time.

> **Note:** Laptop users should always have ADmitMac configured to *Use Local Home Folder*, or *Create Mobile Account at Login*.

Deploy ADmitMac Using Mobile Accounts

ADmitMac supports using Apple's Mobile User accounts, with the *Create Mobile Account at Login* option on the Home Folders pane of ADmitMac's Directory Utility plug in.

Joining an Active Directory Domain

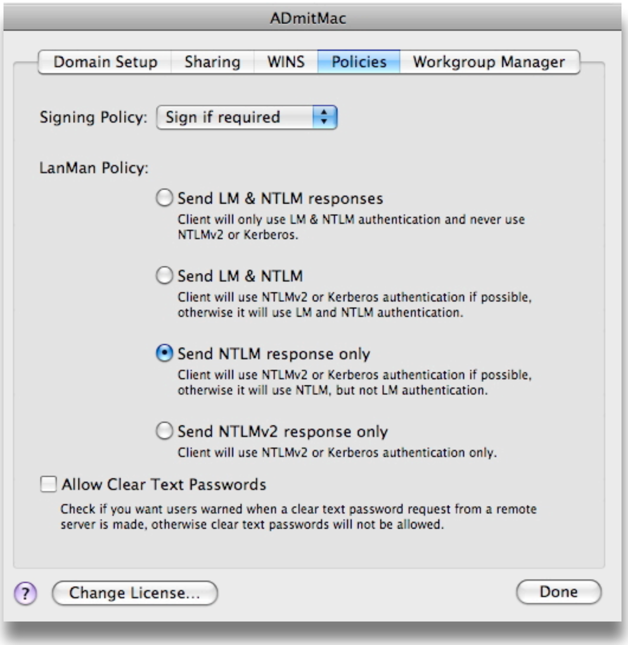
Computers that are members of an Active Directory domain need to have a computer account and password in the domain. The process of creating a computer account is often referred to as joining the domain. ADmitMac takes care of all the details of joining a Macintosh to the domain. All that is needed is a unique name for the computer, the name of the domain and a domain account that is authorized to create computer accounts.

The Macintosh computer will use its domain account to access directory information. This gives administrators the ability to prevent users from anonymously reading information about other users and information about the domain. In addition, the computer account allows the Macintosh to use encryption when retrieving domain information.

Determine Computer Account Naming

Many organizations already have a policy in place for naming domain member computers. Macintosh computers should be given names consistent with your existing policy. Computer accounts usually have names up to 15 characters long to support the older NetBIOS and WINS services that may be in use on your network.

However, this is not required and longer names up to 19 characters can be used. A computer name when appended with the domain name will become the DNS name for a domain computer. ADmitMac will automatically use dynamic DNS to add an A type record to the DNS server for the computer name.



Signing Policy: Sign if required

LanMan Policy:

○ Send LM & NTLM responses
Client will only use LM & NTLM authentication and never use NTLMv2 or Kerberos.

○ Send LM & NTLM
Client will use NTLMv2 or Kerberos authentication if possible, otherwise it will use LM and NTLM authentication.

● Send NTLM response only
Client will use NTLMv2 or Kerberos authentication if possible, otherwise it will use NTLM, but not LM authentication.

○ Send NTLMv2 response only
Client will use NTLMv2 or Kerberos authentication only.

□ Allow Clear Text Passwords
Check if you want users warned when a clear text password request from a remote server is made, otherwise clear text passwords will not be allowed.

Determine Client Policy

Home Folders

As discussed above under "Planning for Home Folder Storage," ADmitMac has four options for determining how a user's home folder will be configured.

- *Use Network Home Folder*
- *Use Local Home Folder*
- *Use Either*
- *Create Mobile Account at Login*

LanMan Security Level and SMB Signing

ADmitMac supports the latest authentication protocols used by Microsoft: Kerberos, GSSAPI, SPNEGO, NTLMSSP, NTLMv1 and NTLMv2. ADmitMac also supports SMB signing so each transaction with a file server is cryptographically signed to prevent man-in-the-middle attacks. In addition, you can prevent a user from giving out their plain text password to any SMB file server. To configure the ADmitMac security policy settings:

1. Launch *Directory Utility* in the **System** > **Library** > **CoreServices** folder and double click on *ADmitMac*.
2. Click on the *Policies* tab.
3. Choose the SMB signing policy you want to enforce. The *Always Sign* setting is equivalent to Windows "Microsoft network client: Digitally sign communications (always)." The *Sign if Possible* setting is equivalent to "Microsoft network client: Digitally sign communications (if server agrees)". ADmitMac will always sign if the server requires it.
4. Choose a LanMan Policy. These settings are equivalent to the Windows "Network security: LAN Manager authentication level." The most secure setting is *Send NTLMv2 response only* because it uses stronger encryption. The setting, *Send NTLM response only*, may provide the best operation when connecting to computers running Windows 95, 98, Me, and older third-party SMB services.

WARNING: Be aware that choosing Send LM & NTLM responses or Send LM & NTLM will allow ADmitMac to include a very weakly-encrypted hash of the user's password that can be cracked easily using widely available software. Thursby Software Systems does not recommend using these settings.

Credential Caching

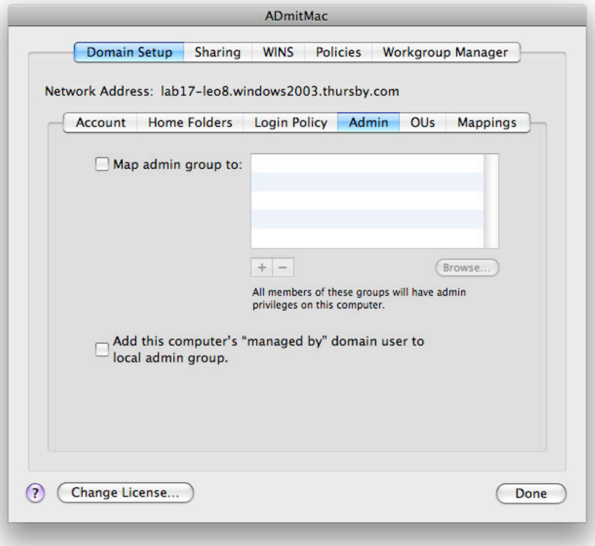
When a Macintosh can't communicate with the domain, ADmitMac will still allow users to log in by caching their password information. This feature is useful for users that have notebook computers. You can control how many times a user can log in using their cached credentials. The default number is 10. You can disable cached credentials by setting the number to 0.

User Shell

You may specify which terminal shell a user is given when starting the terminal application by checking the "Default user shell" checkbox and typing in the path to the desired shell.

Give Domain Users Administrative Privileges

You may want to give groups of domain users administrative privileges on the local Macintosh. For example, you may have a help desk group that needs to install or update software on a Macintosh. You can configure ADmitMac so that domain users in that group are added to the local "admin" group when they log in to a Macintosh. You may also include the name of a domain user. More than one group or user can be specified.



Network Address: lab17-leo8.windows2003.thursby.com

□ Map admin group to:

All members of these groups will have admin privileges on this computer.

□ Add this computer's "managed by" domain user to local admin group.

To tell ADmitMac what groups should have local administrative privileges:

1. Launch *Directory Utility* and double-click on *ADmitMac.*

2. Click on the *Admin* tab.

3. Make sure the check box next to *Map admin group to* is checked.

4. Click the '+' sign to add the names of groups or users in the *Map admin group to* text field.

NOTE: ADmitMac does not support groups with NT domains. Only usernames are allowed in the *Map admin group to* text field. Use principal names in Active Directory domains.

Give Domain Users Administrative Privileges On Their Primary Use Computer

You may want to give a domain user local administrative privileges for a particular Macintosh, but not for any other computer. You can control this from your Active Directory Users and Groups MMC plug-in by assigning a domain user to be the manager of a computer account. In addition, you must tell ADmitMac that the computer account manager is allowed to have local administrative privileges:

1. Launch *Directory Utility* and double-click on *ADmitMac.*

2. Click on the *Admin* tab.

3. Use one of the following methods:

   a) Make sure the check box next to *Map admin group to* is checked. lick the '+' sign and enter the name of the domain user that should have local admin rights in the *Map admin group to* field.

   b) Click on the *Mappings* tab. Make sure the check box next to *Add machine account manager to admin group* is checked.

NOTE: Since no specific user name is entered on the Macintosh, you may want to deploy with this setting on all your Macintosh clients. The setting will only be used if the computer account has a manager assigned. By default, managers are not assigned to computer accounts created by ADmitMac.

Map UNIX ID's to Active Directory Attributes

If your network has been customized to support other non-Macintosh UNIX systems such as Linux, Sun or AIX, you may want to consider providing those customized features to your ADmitMac users.

Don't use these mappings if any of the following are true of your network:

1. Your only UNIX systems are Macintosh computers.
2. Your other UNIX systems don't integrate with Active Directory to obtain user and group information.
3. You don't need to share files with or copy files to and from non-Macintosh UNIX systems.
4. Your network does not use Services for UNIX, or has not been customized to support UNIX id attri-

butes.

NOTE: Using these mappings incorrectly will result in users not being able to log in, or not have the proper group membership.

Some Active Directory networks may be customized to support UNIX users, or may be using Microsoft's Services for UNIX. ADmitMac can provide UNIX user and group IDs that are consistent with other UNIX platforms in your network. This is important if you use NFS, or directly share files between your Macintoshes and your other UNIX platforms, because ownership of the files will still match up with the user and group account from Active Directory.

By default ADmitMac derives UNIX user (UID) and group (GID) identity values from Active Directory using a method that does not require schema changes. The default ADmitMac method for doing this is not available on other UNIX systems. To make your Macintosh user and group identities match up, use the "Mappings" tab found in the Directory Utility as described above.

Your Active Directory must have special attributes for your UNIX user and group IDs. You may have up to four of these special attributes. ADmitMac does not create these special attributes for you. They get created by Microsoft's Services for UNIX, or by custom schema changes made by your organization.

To set the mappings, you will need to know the names of the attributes in Active Directory that represent UNIX user and group identities. For Microsoft's Services For UNIX v3.0 and later, these attributes are listed below:

Map UID to attribute:	msSFU30UidNumber
Map user GID to attribute:	msSFU30GidNumber
Map group GID to attribute:	msSFU30GidNumber
Map home directory to attribute:	msSFU30HomeDirectory

If you have a customized Active Directory schema, you will need to determine the corresponding attribute names from your schema definitions.

Note that not all domain users will have these attributes set, and additional administrative work is usually required. Consult your Microsoft Services for UNIX documentation for further information about Services For Unix:

http://www.microsoft.com/technet/interopmigration/unix/sfu

Partition a Domain for Security Reasons

You may not want just any domain user to be able to log into a Macintosh. You can configure ADmitMac to allow only users from a particular domain or organizational unit to log in. Users with accounts in that organizational unit or in other organizational units contained inside it will be allowed to log on.

To restrict user login by organizational unit:

1. Launch *Directory Utility* and double-click on *ADmitMac*.

2. Click on the *OUs* tab.

3. Enter the distinguished name of the organizational unit in the *Users OU* text field.

Restrict Managed Groups

Entering a distinguished name in the *Groups OU* field does NOT restrict logins to members with groups inside that OU. Instead, it will restrict which managed groups are available on that particular Macintosh. For example, if a user is in multiple managed groups, when they log in, they will only be able to choose from managed groups in the Groups OU you specify. This can be used to modify the user's desktop experience by location. Use this method only if you need to provide different management settings based on the location of a computer, but have managed group settings that would override managed computer list settings.

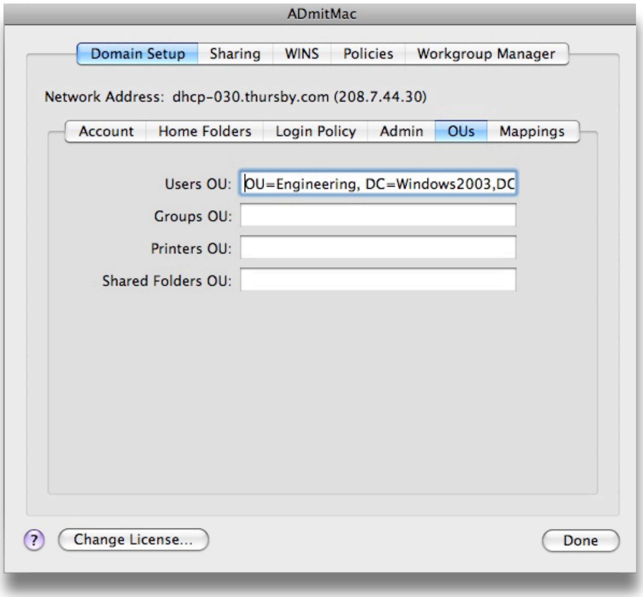
By default, the OU fields are left blank to allow login by any user in your forest of domains. If you do not want users from other domains in the forest logging in, enter the base DN for your domain in the *Users OU* field.

For example, if your domain is named `STUDENTS.MOOU.EDU`, you would enter:

`DC=STUDENTS,DC=MOOU,DC=EDU`

Restricting Published Folders and Printers by Physical Location

You may want users to only see published printers and shared volumes that are physically located near them. It does NOT prevent a user from using a printer or mounting a share in a different OU. When users browse the network, ADmitMac can be configured to only display published printers and shared volumes that are contained inside organizational units that you specify as follows:



Network Address: dhcp-030.thursby.com (208.7.44.30)

Users OU: OU=Engineering, DC=Windows2003,DC

Groups OU:

Printers OU:

Shared Folders OU:

1. Launch *Directory Utility* and double-click on *ADmitMac*.

2. Click on the *Domain Setup* tab if not currently selected.

3. Click on the *OUs* tab.

4. Enter the distinguished name of the organizational unit in the Printers OU and Shared Folders OU text field.

Performance

If your domain has a large number of users and computers, you may get better responsiveness by restricting where ADmitMac must look for account information. To accomplish this, enter more specific organizational units for the Users OU and Groups OU items.

Logging In for the First Time - Home Folder Templates

When users log in for the first time, and don't have a Library folder in their home folder, the Mac OS sets up their home folder using a template. This template is stored in `/System/Library/User Template/English.lproj`. Users with home folders stored on the local disk will always use this template.

You can provide a different template only for users that have network home folders. ADmitMac checks to see if their home folder has a Library folder in it. If no Library folder exists, ADmitMac will configure the user's home folder using the template in `/Library/Application Support/ADmitMac/User Template/English.lproj`. If this folder does not exist, ADmitMac will use the `/System/Library/User Template/English.lproj` folder instead. You may wish to customize the items in this template folder.

1. Create a new "default" local user.

2. Log in as that user and make any desired changes.

3. Log out and log back in as a local administrator.

If you want to use the template for a local home folder or mobile account:

4. Start Terminal and type,

```
sudo ditto -rsrc /User/Default "/System/Library/User Template/English.lproj"
```

(where "default" is the short name of the default account)

```
sudo chown -R root:wheel /System/Library/User Template/English.lproj
```

This will copy the default user template to this directory and apply the correct permissions.

5. If you want to use the template for a network home folder:

```
sudo ditto -rsrc /User/Default "/Library/Application Support/AdmitMac/
User Template/English.lproj"


sudo chown -R root:wheel /Library/Application Support/ADmitMac/User
Template/English.lproj
```

This will copy the default user template to the ADmitMac User Template directory and apply the correct permissions.

6. Exit Terminal.

7. Log into the user's account. The new template should be in effect.

Note that the ADmitMac user template is only used for network home folders. More information about creating Home Folder templates can be found by searching on the Apple Developer website: http://developer.apple.com/.

Custom Login/Logout Scripts

ADmitMac does not support Windows login scripts on a Macintosh. Such scripts would not be understood by the Macintosh operating system. However, Mac OS X does allow you to write scripts that run when users log in and out of the Macintosh desktop. These scripts will not run when users connect to the Mac using ssh. The primary scripts must *reside* on the Macintosh's local disk, but may *invoke* scripts copied from network servers at login time. Login scripts should be developed with care since they are used by all desktop logins. Flaws in the script logic may prevent anyone from logging in – even local user accounts. The best way to develop a login script is to create a local user account and test the login scripts with that account. Once they are working, you can make the scripts work for all user logins.

Login Scripts, Permissions and Parameters

WARNING: Login scripts must be written with care because they could possibly delete important system files without warning.

Login scripts run with root authority, meaning they are allowed to perform any operation. Logout scripts run with the permission of the user that is logging out and do not have root authority.

Your scripts will be run with the user name as the only argument. Login scripts do not have the current working directory set to the user's home directory, and don't have any useful information in the environment. ADmitMac will always have the user's home folder available (mounted if needed) and the user template will have already been copied if necessary before the login script executes. For domain users, the home directory will always be `/Domain/[domainname]/Users/$1`. Logout scripts do have the working directory set to the home directory, and do have the HOME environment variable set.

Testing Scripts with a Local User Account

Create a local test user account using the Macintosh System Preferences **Accounts** item.

1. Log in as the new test user.

2. Place your login and logout scripts in their desired location. For example, you may want to put your scripts in a folder named `/Domain/Scripts` and name them `admitmac_login.sh` and `admitmac_logout.sh`.

3. In the Terminal application, open a terminal window and use the following command to add the login script:

```
defaults write com.apple.loginwindow LoginHook /Library/Management/admitmac_
login.sh
```

Likewise, use this command to add the logout script:

```
defaults write com.apple.loginwindow LogoutHook /Library/Management/admitmac_
logout.sh
```

4. Log out and log in as the test user to test your scripts.

5. Once you are sure the scripts work as expected, copy the following file to /System/Library/Preferences.
   `/Users/testuser/Library/Preferences/com.apple.loginwindow`

Run Login Scripts With The Login User's Authority

If you want to make parts of your login script run with the privileges of the user logging in, you can use `/usr/bin/su` to run commands or another script as the user logging in.

For example, use the following line in the main login script to run `/Domain/Scripts/userLogon.sh`:

```
/usr/bin/su $1 /Domain/Scripts/userLogon.sh
```

Sample Login/Logout Scripts

Setting up a Macintosh for One-Time Login Use

Using this method, you can configure a Macintosh for one-time use. Any forest/domain user may log into the Macintosh. When they log out, any files created on the local disk will be removed. Users must be instructed to save files on the network before logging out.

The first step is to join the Macintosh to a domain and set the home folder policy. Choose *Use Local Home Folder* for this policy, since it gives the desired behavior. Next, you need to write a log out script that will clean up local resources when the user logs out. However, you must be careful that the script only removes files for domain users, and not local administrative users.

```
#!/bin/sh
  # remove a home folder for a domain user
  [ x$HOME = x ] && exit 0 # no home folder
  HOMEPATH='dirname $HOME'
  HOMEPATH='dirname $HOMEPATH'
  HOMEPATH='dirname $HOMEPATH'
  if [ $HOMEPATH = "/Domain" ]; then
  #remove the home folder
  cd /tmp/ # get us out of the way
  /usr/bin/logger "Removing home folder for $1 - $HOME"
  /bin/rm -rf $HOME # comment this out while testing
  fi
```

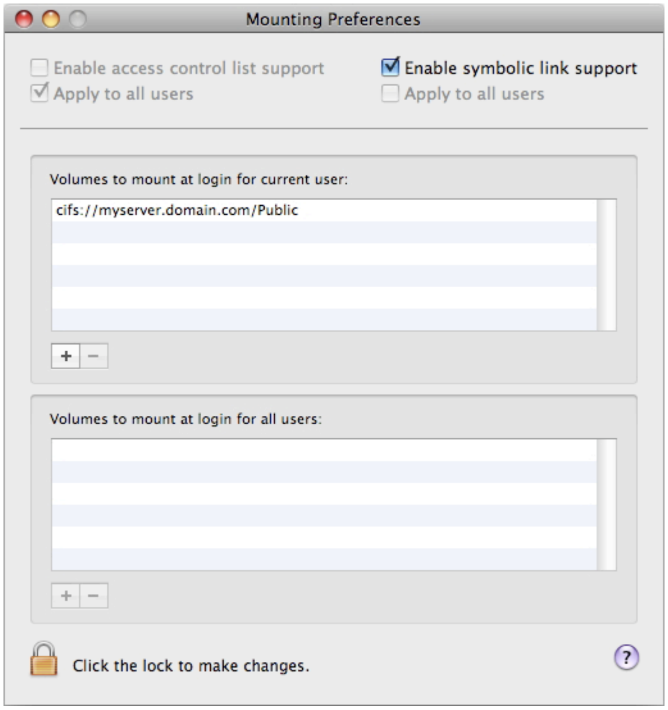
Create Symbolic Links for Hybrid Home Folders

Using this method, you can redirect a user's Movies, Pictures and other folders to different locations. You might want to redirect the Movies folder from a network home folder to a local disk.

```
#!/bin/sh
# Redirect Mac OS X Pictures folder to the Windows "My Pictures" folder
if [ ! -L Pictures ]; then
  if [ -e Pictures ]; then
    if [ ! -e Pictures.save ] ; then
      mv Pictures Pictures.save || \
                  (echo "Can't move Pictures out of the way." && exit 1)
    fi
  fi
  /bin/ln -s My\ Pictures Pictures || ([ -e Pictures.save ] && \
          /bin/mv Pictures.save Pictures)
fi
```

Mounting Folders Automatically

You can configure ADmitMac to automatically mount folders when a user logs into the Macintosh. You may configure volumes that mount for any user. Individual users can configure additional volumes that mount only when they log in. To configure volumes that mount automatically, launch the ADmitMac Browser application (in the Applications folder) and follow the steps below.



☐ Enable access control list support
☑ Apply to all users
☑ Enable symbolic link support
☐ Apply to all users

Volumes to mount at login for current user:

cifs://myserver.domain.com/Public

Volumes to mount at login for all users:

Click the lock to make changes.

1. Choose Mounting Preferences from the ADmitMac Browser menu.
2. Click the + button to add a volume to mount. Volumes will mount on the desktop. There are two different lists. One for volumes that should mount for all users, and another for volumes that mount for the current user. When the current user logs in, the volumes listed in both lists will be mounted.
3. Choose options that control support for access control lists and symbolic links as needed. When settings apply to all users, an individual user cannot override them.

Installation

When you deploy ADmitMac on a single Macintosh, follow these steps:

1. Install ADmitMac by double-clicking on the install package.
2. When the installer finishes, the ADmitMac Setup Assistant will launch automatically and guide you through the steps necessary to configure your settings and join your Macintosh to your domain.

When you deploy ADmitMac on a number of Macintosh computers, follow these steps:

1. Install ADmitMac on a test Macintosh and configure ADmitMac using the ADmitMac Setup Assistant.
2. Test ADmitMac to make sure you have the settings configured the way you need them to be.
3. Use the ADmitMac Deployment utility to build a custom ADmitMac installer package.
4. Install the custom installer package on your clients using one of the following methods:
   a. Install the package manually on each client by double-clicking on it.
   b. Install the package on a master disk image, and then restore that image onto your Macintosh clients.

Configure the Test Macintosh

Whether you are deploying ADmitMac on a large number of machines or on just a few, it is necessary to start with one test Macintosh. Once you have ADmitMac installed and working on one Mac, you have a number of options for deploying your working configuration.

1. Install ADmitMac using the installer from Thursby Software Systems, Inc. If you have a volume license agreement, you should have a custom install CD that already has the license information for your organization included on it. If you have a multi-pack license, you will need to have a license code for each Macintosh.
2. When the installer finishes, the ADmitMac Setup Assistant will launch automatically and guide you

through the steps necessary to configure your settings and join your Macintosh to your domain.

3. You may want to launch Directory Utility, then double-click on ADmitMac to review and modify settings.

4. Test your configuration by logging out (**Apple Menu > Log out**), then log in as a domain user. If you are satisfied with the ADmitMac configuration and want to deploy it on multiple Macintosh computers, the next step is to use the ADmitMac Deployment utility.

Deploy ADmitMac On Multiple Macintosh Computers

When you plan to use ADmitMac on more than a few machines, you will want to use the ADmitMac Deployment utility to create custom install packages.

Note: The following section on deployment is offered for our Volume License Agreement customers. The recommendations below will be of little use to customers who have purchased individual licenses.

Using the ADmitMac Deployment Utility you can:

- Automatically configure and join a client to your domain when installing.
- Keep a database of all your Macintosh clients so they can be joined to your domain using the same name each time. You can query your domain to get an up-to-date list of client names.
- Keep your settings on a web server so you can change them without having to build a new installer package.
- Write a simple NetRestore post-installation script to join a Macintosh client to the domain automatically, using the NetRestore name for the client. NetRestore is available from http://www.bombich.com.

Note: If your settings include the password for the account used to join clients to your domain, all your settings are encrypted. The encrypted data is either stored inside the installer package, or is stored on your web server. When you store the data on a web server, the encrypted password is not stored in the install package.

By stepping you through the installation process, the ADmitMac Deployment utility allows you to create a custom Apple Installer package. This package may then be installed on your master disk image (sometimes referred to as the perfect client image - an image made from the perfectly configured Macintosh client).

When clients are restored from the master disk image, you need to use the **amconfig** utility to configure the client with the settings you chose using ADmitMac Deployment Utility, and to join your domain automatically. **amconfig** is located in `/sbin`.

Custom Installation Configurations

There are two types of custom installations that can be configured using the ADmitMac Deployment Utility:

- For existing clients that you don't intend to re-image; and,
- For clients you are re-imaging using a tool such as NetRestore.

For Existing Clients

First, get the package to the clients via net share or e-mail. Installation will require local admin privileges. Double click to install. ***Setup Assistant*** will launch and configure the client.

For Re-imaging an Apple Install Package

In your deployment scripts, include the following lines to invoke the installer and **amconfig** tool (each command should be written on one line, with no carriage returns):

```
/usr/sbin/installer -pkg pathtoAdmitMacPackage -target \
     /Volumes/RealSystemVolume
```

and

```
/Volumes/RealSystemVolume/sbin/amconfig -A -R /Volumes/RealSystemVolume
```

or

```
/Volumes/RealSystemVolume/sbin/amconfig -A -R /Volumes/RealSystemVolume \
    -c clientname
```

Other Uses for amconfig:

- To reset ADmitMac configuration, just invoke amconfig. It will always re-join a domain and reconfigure the Directory Service settings even if the target client has already been configured in the past.
- You can also use the amconfig utility to manually join a domain:

  ```
  amconfig -a -d domain -u username [-p password] -c computername
  ```

- Remove a client from the domain using:

  ```
  amconfig -r -d domain -u username [-p password]
  ```

- Verify that the client is properly joined to the domain using: `amconfig -v -d domain`
- List the domains a client is joined to using: `amconfig -l`
- Specify which OU your Mac will join: `amconfig -a -d DOMAINNAME.COM -u username -p password -c CN=COMPUTERNAME,OU=OUNAME,DC=DOMAINNAME,DC=COM`
  NOTE: Nested OUs using the command above are specified from lowest level first to the highest.

Resolve Conflicts Between Local and Domain Accounts

The ADmitMac Setup Assistant will check for conflicts between local and domain accounts. When a local account name is the same as a domain account name, users might get confused and not be able to log into the correct account. Users should always be able to log into their domain account by entering their user name as "user@domain." The ADmitMac Setup Assistant will give the user the opportunity to rename local accounts that conflict by changing the local name to have "local-" in front of it.

Ignore Domain Controllers

ADmitMac allows the administrator to cause certain domain controllers to be ignored, or to be preferred over other domain controllers. To cause a domain controller to be ignored, the administrator may use this command in a terminal window (substitute your server.domain.extension for `server.domain.xxx`):

```
defaults write /Library/Preferences/com.thursby.ADmitMac.domainprefs \
server.domain.xxx ignore
```

To prefer a domain controller:

```
defaults write /Library/Preferences/com.thursby.ADmitMac.domainprefs \
server.domain.xxx prefer
```

To remove the setting for a domain controller:

```
defaults delete /Library/Preferences/com.thursby.ADmitMac.domainprefs \
server.domain.xxx
```

To view the settings:

```
defaults read /Library/Preferences/com.thursby.ADmitMac.domainprefs
```

Convert Local User Accounts

You may have Macintosh users who have local accounts on their machines, but you want them to use their domain accounts to log in instead. You can accomplish this by running the ADmitMac Home Mover utility's "Duplicate a Home Folder" function.

When Home Mover converts local user accounts, it completes the following:

- Move or copy the local home directory to `/Domain/domainname/Users`.

- Modify all resource fork and Finder aliases so they point to the new location of the home folder. Also update other preferences such as Finder sidebar and recent items, and Dock preferences.

- Change the user's files so they are owned by the user's domain account.

Using ADmitMac with Active Directory and MIT Kerberos

About Kerberos

Kerberos is an internet standard authentication system supported by Active Directory and Apple. Kerberos provides a single-sign-on architecture so that users should only have to type in their password once during their working day (about 10 hours by default). Instead of using plain-text passwords or cryptographic hashes, Kerberos keeps a set of credentials called tickets in a cache for the user. When the user first logs in, an initial ticket is placed in the cache known as a ticket-granting ticket.

ADmitMac automatically takes care of configuring Macintosh computers to use Kerberos. Kerberos is designed to authenticate a user to a network service, such as AppleShare or SMB. Network services that can operate using Kerberos are said to be kerberized. Not all services provided by Apple and Microsoft are kerberized. Some services provided by third party vendors may be kerberized.

> **Note:** Every user who logs in with a Macintosh to a forest must have an account in that forest — accounts from a different forest, trusted or not, will not work. The following section details mapping Active Directory Domain Accounts to User Principals in an MIT Kerberos realm.

ADmitMac and Active Directory with MIT Kerberos Realms

You may want to configure your Active Directory domain to work with a trusted MIT Kerberos realm. When you configure your domain, you can create user accounts that are mapped to user principals in the MIT realm. In fact, it is possible to map multiple user principals to these user accounts. Users from the MIT realm can then log into computers that are members of your domain. The steps to configure an MIT realm and an Active Directory domain are as follows:

1. Install and configure your Active Directory domain controllers.

2. Install and configure your MIT realm. To configure the MIT realm, you need to create two principals and set their passwords. Use the same password for both principals. You can choose any password you like, but longer, random passwords will be more secure. On your MIT realm KDC, use a shell to enter the following commands. Information you enter is displayed in bold face. Prompts or output from the utility are not displayed in bold. Enter the password you choose in place of "password" shown below:

```
% kadmin.local -r GRADUATE.EDU
kadmin.local: add_principal -pw password krbtgt/MOOU.EDU@GRADUATE.EDU
kadmin.local: add_principal -pw password krbtgt/GRADUATE.EDU@MOOU.EDU
kadmin.local: quit
%
```

   In the example above, the Active Directory domain is named "MOOU.EDU" and the Kerberos realm is named "GRADUATE.EDU." The names do not have to have any relationship to each other. Principals are now added to define the relationship between the MIT realm and the domain. The realm has a principal in the domain, and the domain has a principal in the realm.

3. Create the trust relationship between the Active Directory domain and the MIT realm. Now you need to configure the Active Directory domain so it knows about your MIT realm. Use the ksetup tool to do this in a command window. You should enter the DNS name of the KDC host for your realm instead of 'kdc_dns_name.geeks.org.' Enter the text in bold:

```
C:> ksetup /addkdc GRADUATE.EDU kdc_dns_name.graduate.edu
```

4. Set the password used for your trust relationship so that your Active Directory domain can communicate securely with your MIT realm. To do this, you need to use the "Active Directory Domains and Trusts" administrator tool on your Domain Controller.

a. Select your domain, then right click and choose *Properties* ..

b. Click on the *Trusts* tab.

c. Depending on the version of the Windows domain server, you need to use slightly different procedures as follows:

1) On Windows 2003 and 2008 servers, click the *New Trust* button and use the wizard to configure the trust. You will be asked for the password used when you configured your Kerberos V5 realm.

2) On Windows 2000 servers, click the *Add* button next to *Domains trusted by this domain*, and enter the domain name and password in the dialog that appears. If you want your Kerberos V5 realm to trust your domain, then click the *Add* button next to Domains that trust this domain.

d. Add mapped users to your Active Directory domain.

1) On the Windows system, launch *Active Directory Users and Computers*.

2) Select a user or create a new user account in an appropriate OU

3) Select the user, right-click and select *Name Mappings* from the contextual menu

4) In the dialog that appears, select the *Kerberos Names* tab.

5) Click *Add* and enter the Kerberos principal name of the corresponding user in your Kerberos V5 realm.

6) Click *OK* to dismiss the dialog.

e. One optional step can be used to add the name of your Kerberos V5 realm to the list of UPN (user principal name) suffixes that your domain will allow when you add or modify user account names. This step can make it easier to manage user accounts because the user account will have a user principal name suffix you choose. Management tools will be able to search for users in the domain that are mapped to your Kerberos V5 realm.

To add a UPN Suffix to a Forest:

1) On the Windows system, launch *Active Directory Domains and Trusts*.

2) Right-click *Active Directory Domains and Trusts* in the Tree pane, and then click *Properties*.

3) On the *UPN Suffixes* tab, type the new UPN suffix that you would like to add to the forest.

4) Click *Add*, and then click *OK*.

Now when you add users to the forest, you can select the new UPN suffix to complete the user's logon name.

Set the user account's logon name to match principal name

If you added a UPN suffix to your domain when you created the trust with your Kerberos V5 realm, you might want to set the user account's user logon name to match their principal name:

1. Right-click the desired user account and choose *Properties…*
2. Click the *Account* tab.
3. On the *Account* tab, the combo-box control next to the *User logon name* field and select the name of your Kerberos V5 realm.

Using ADmitMac with OS X Server

When you install ADmitMac on an OS X server, service principals are automatically created for common services such as AppleShare. This makes configuring your server for one-time login very simple. The following service principals are added to the server's `/etc/krb5.keytab` file: afpserver, ftp, http, cifs, smtp, pop, imap, and ldap.

Kerberizing OS X Services

Mac OS X servers come from Apple with a number of Kerberized services including AppleShare, FTP, SMTP, POP and IMAP. In order for these services to work with Kerberos, a service ticket must be stored in the server's `/etc/krb5.keytab` file. Service tickets are identified by a name known as a service principal name. For example, if your Mac OS X server name "osxserver" was joined to an Active Directory domain named "mydomain.com," the AppleShare service would have a service principal name of "afpserver/osxserver.mydomain.com@MYDOMAIN.COM."

In addition, the `/etc/krb5.keytab` file must contain a service ticket for this service principal name. ADmitMac will automatically put service tickets in the `/etc/krb5.keytab` file whenever the server is joined to a domain.

Configuring OS X Server for Single Sign-On

1) Install and configure ADmitMac

2) Your DNS must supply both a name to IP address resolution (A record) and IP address to name resolution (PTR record) for the name you used to join your Active Directory domain.

3) Use the amconfig tool from a command line to enable single sign-on for your domain:

```
/sbin/amconfig -enablesso -d MYDOMAIN.COM
```

The `-enablesso` may print out information that can be ignored. This command will configure the various Kerberized services on your OS X server.

4) Make sure AppleShare is configured and sharing volumes, then test to make sure you can mount an AppleShare volume from a client without having to enter a username or password

If you have trouble, try the following steps:

1) Test your DNS service using these commands:

```
dig myserver.mydomain.com
```

This should print out the IP address of the server in the answer section. Now test the IP address to name resolution using the IP address from above.

```
dig -x 192.168.1.100
```

The name in the answer section must match the Active Directory name for your server. For example: myserver.mydomain.com

2) Log out of the client Macintosh, then log back in using an Active Directory user account. If you attempt to use single sign-on from a client and then re-join the server to a domain within 10 hours, your client credentials will no longer be valid, so logging out and back in should correct this.

3) On the server using Directory Utility, open the ADmitMac plugin and delete the domain. Then, using the command line, type these commands to clean up Kerberos files:

```
sudo rm /Library/Preferences/edu.mit.Kerberos
sudo rm /etc/krb5.keytab
```

On a PC using Active Directory Users and Computers, make sure the server's computer account has been removed from the domain.

Now join the domain again using Directory Utility.

Windows Domain Management With AD Commander

Overview

AD Commander is a utility that lets Macintosh users perform administrative tasks for their Active Directory domain. It is useful to Macintosh users that have been delegated administrative authority for some part of their domain.

AD Commander is also handy for help desk personnel that need to reset user passwords and enable accounts that become disabled due to too many invalid login attempts.

With AD Commander you can perform the following tasks:

- Reset user account passwords
- Require that a user change their password when they next log in
- Enable or disable user accounts
- Create new organizational units
- Create new groups and add or remove users from groups
- Create new user accounts
- Modify user account information such as address, phone number, etc.
- Create home folders for user accounts - home folders can be created on any domain file server
- Create new computer accounts
- Remove organizational units, groups, user and computer accounts
- Move users and computers to different OUs

AD Commander uses fully encrypted, kerberized connections to communicate with the Active Directory domain. It does not require users to perform any special or complicated Kerberos or DNS configuration. The correct domain controllers are automatically located. Verify that you are connected to the network and you have administrator privileges to at least one domain.

Getting Started

AD Commander will use DNS to locate your Active Directory domain. This means that your Macintosh's DNS settings are important. If AD Commander can't find your domain, you should try to point your DNS settings at the same DNS server used by your domain controllers.

AD Commander is installed in **Library > Application Support > ADmitMac**. You may move it to any convenient location.

1. Once you locate AD Commander, simply double-click the application icon.
2. Enter the FULL domain name (not short name) of the domain you want to connect to (the last domain used will be remembered). For example, your domain may be named “`MYCOMPANY.COM`” and may have a short name “`MYCOMP`”. You must use the full name - “`MYCOMPANY.COM`”.

You may be asked to enter a user name and password to access the domain. AD Commander is Kerberized, and will first try to use your current credentials. Once you provide your credentials, you probably won't be asked for them again until they expire (usually in about 10 hours). You can also log into your domain using the Kerberos utility using Keychain Access (**Applications > Utilities** and selecting the menu item KeyChain Access > TicketViewer), if you have configured your computer to use Kerberos. You don't need to do any special Kerberos configuration to use AD Commander. It will automatically take care of the Kerberos details.

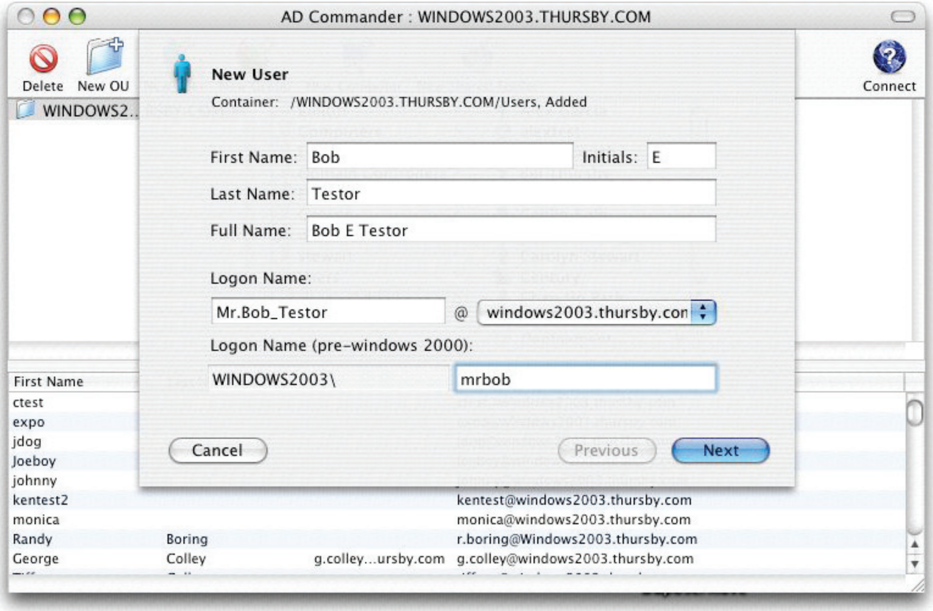
Note: About system-critical objects—some objects in the domain are very important to the operation of the domain, such as domain controller accounts. AD Commander will not allow you to modify or delete these objects in any way. You should use your PC management tools to modify system-critical objects.

Create or Delete a User

Using AD Commander, you can create or delete users on your Windows domain server from your Macintosh.

Complete the following to create or delete a user:

1. Open AD Commander and authenticate.
2. To create a new user, simply click the OU where you want the user to be created, click the *New User* icon from the tool bar, fill in the properties for the new object and then click *Finish*.
3. To view user information and access additional functions, control-click the user and select the desired function (select *Properties* to modify user information).



New User

Container: /WINDOWS2003.THURSBY.COM/Users, Added

First Name: Bob Initials: E

Last Name: Testor

Full Name: Bob E Testor

Logon Name:

Mr.Bob_Testor @ windows2003.thursby.con

Logon Name (pre-windows 2000):

WINDOWS2003\ mrbob

First Name			
ctest			
expo			
jdog			
Joeboy			
johnny			
kentest2			kentest@windows2003.thursby.com
monica			monica@windows2003.thursby.com
Randy	Boring		r.boring@Windows2003.thursby.com
George	Colley	g.colley...ursby.com	g.colley@windows2003.thursby.com

By control-clicking a user, you can:

- Get properties of a user;
- Enable or disable a user account;
- Reset a user's password;
- Send an Email to a user;
- Open a user's web page;
- Move the user to a new container;
- Delete a user

NOTES:

- To delete an item, select the item and click the *Delete* button from the tool bar.
- You can edit multiple items by clicking *Shift + select*.
- To find a user, select *Command + F* or select *Find* from the Edit file menu.
- To add a user to a group, you must perform a search. Also, check the search field pop-up after pressing return the first time. Make sure it is set to *Users*.

Create or Delete a Group

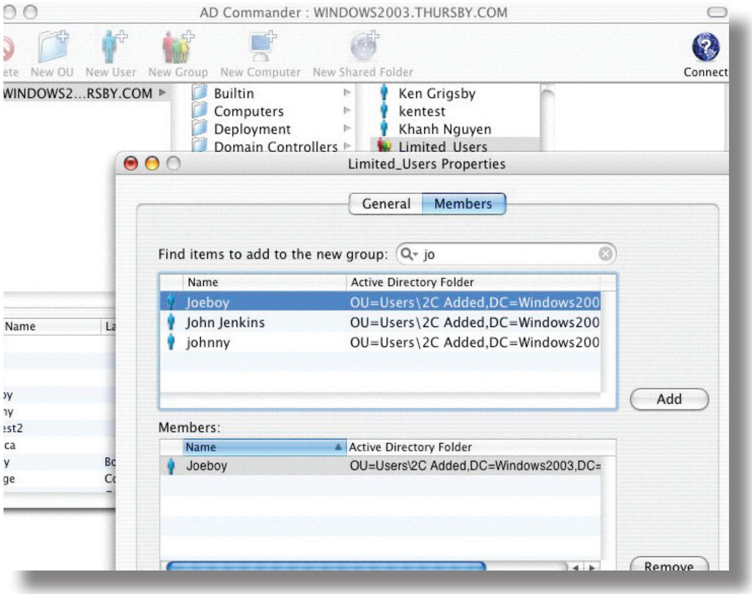
Complete the following to create or delete a group:

1. Open *AD Commander* and authenticate.
2. To create a new group, click the OU where you want the user to be created, click the *New Group* icon from the tool bar, fill in the properties for the new object and then click *Finish*.
3. To view group information and access additional functions, control-click the group and select the desired function (select Properties to modify group information). By control-clicking a group, you can view:
   - Group Scope.
   - Group Type.
   - Group Members.
4. To delete a group, select the group and click on the *Delete* icon.

Add a User to a Group

Complete the following to add a user to a group:

1. Open AD Commander and authenticate.
2. To add a user to a group, double-click the group icon to which you wish to add a user.
3. Click on the *Members* tab. To search for the user you wish to add to the group, begin typing in the search field next to *Find items to add to this group*. Press *Return* to begin the search.
4. When the user you wish to add to the group is located, highlight the user and click the *Add* button. Click the *close* button to exit the window. You will be prompted to save your changes.



AD Commander : WINDOWS2003.THURSBY.COM

Limited_Users Properties

Find items to add to the new group: jo

Name	Active Directory Folder
Joeboy	OU=Users\2C Added,DC=Windows200
John Jenkins	OU=Users\2C Added,DC=Windows200
johnny	OU=Users\2C Added,DC=Windows200

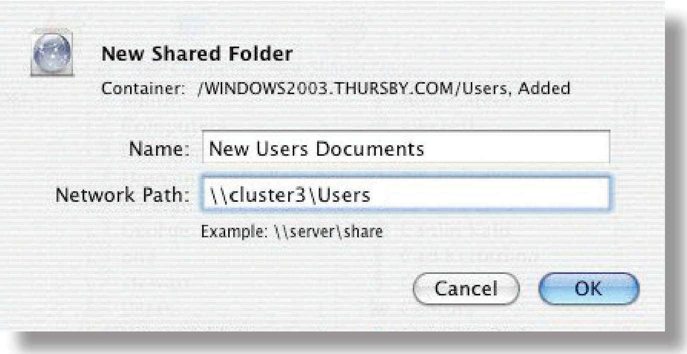
Members:

Name	Active Directory Folder
Joeboy	OU=Users\2C Added,DC=Windows2003,DC=

Create a New Shared Folder

You can use AD Commander to create a published share object to allow a shared folder to be located in the directory.

1. Open AD Commander and authenticate.
2. To create a new shared folder, simply click the OU where you want the shared folder to be created, click the *New Shared Folder* icon from the tool bar, enter the name as you would like for it to appear in the directory and the path to the existing share.
3. To view shared folder information and access additional functions, control-click the shared folder and select the desired function (select *Properties* to modify shared folder information). By control-clicking a shared folder, you can view its description, properties, and network path. You can mount a volume, move it and delete it.



New Shared Folder

Container: /WINDOWS2003.THURSBY.COM/Users, Added

Name: New Users Documents

Network Path: \\cluster3\Users

Example: \\server\share

Create or Modify Objects (OU)

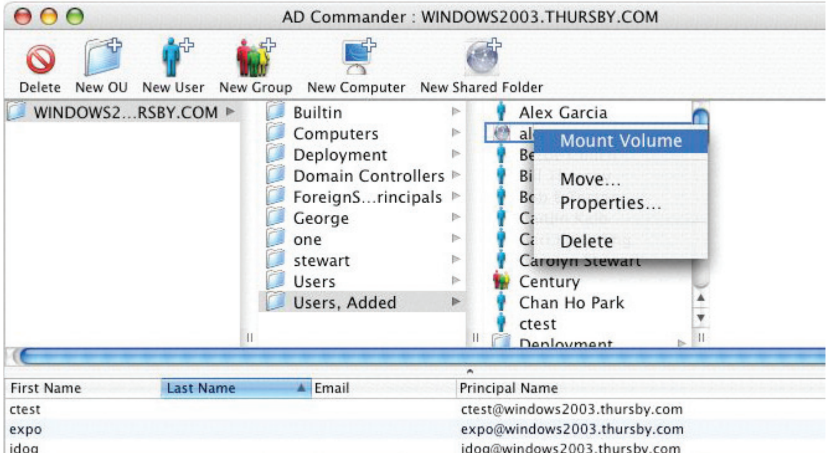
To Create and Modify Objects

NOTE: Some objects in the domain are very important to the operation of the domain, such as domain controller accounts. AD Commander will not allow you to modify or delete these objects in any way. You should use your PC management tools to modify system critical objects.

1. Open AD Commander and authenticate.
2. Click on the OU or CN where you want the new object created.
3. Click the new desired object type from the tool bar icons (*New OU, user, group* or *computer*).
4. Fill in the properties for the new object and click *Finish*.
5. To modify an object's attributes, double-click (or Control-click and select *Properties* and update the object's information or to move the object to a new container.
6. To delete an object, select the object and click the *Delete* button from the tool bar.

Mount a Published Folder

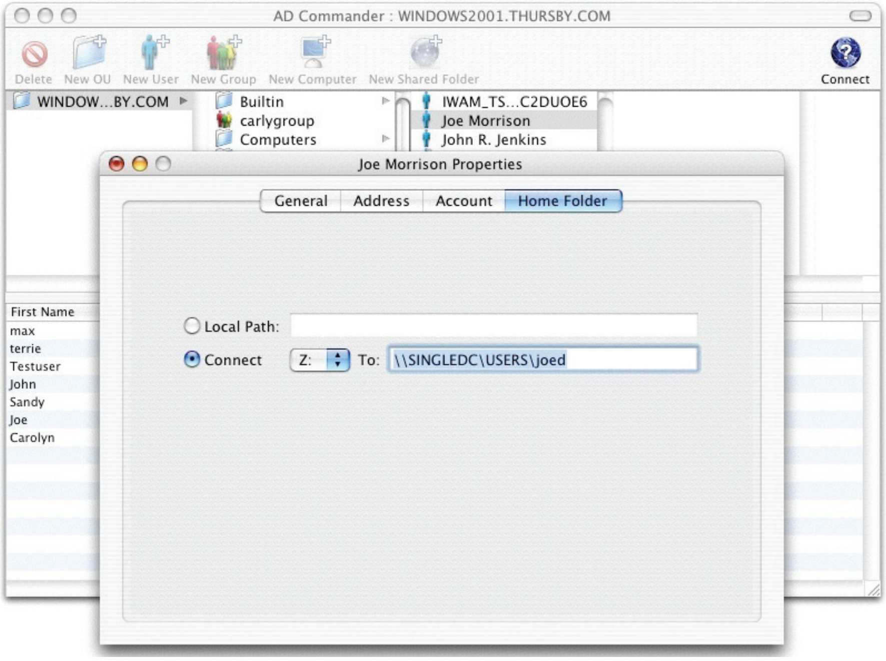
1. Open *AD Commander* and authenticate.
2. Select the published folder you wish to mount.
3. Control click and select *Mount Volume* from the contextual menu.
4. The published folder will be mounted on your desktop.



First Name	Last Name	Email	Principal Name
ctest			ctest@windows2003.thursby.com
expo			expo@windows2003.thursby.com
idog			idog@windows2003.thursby.com

Modify the Home Folder Path

1. Open *AD Commander* and authenticate.
2. To modify a home folder path, control-click the user you want modify and select *Properties...*
3. In the Home Folder tab, enter the new home folder location (UNC "\\server\share" format).



First Name
max
terrie
Testuser
John
Sandy
Joe
Carolyn

○ Local Path:

● Connect Z: To: \\SINGLEDC\USERS\joed

ADmitMac Home Mover

Overview

Home Mover is installed in **Library** > **Application Support** > **ADmitMac**.

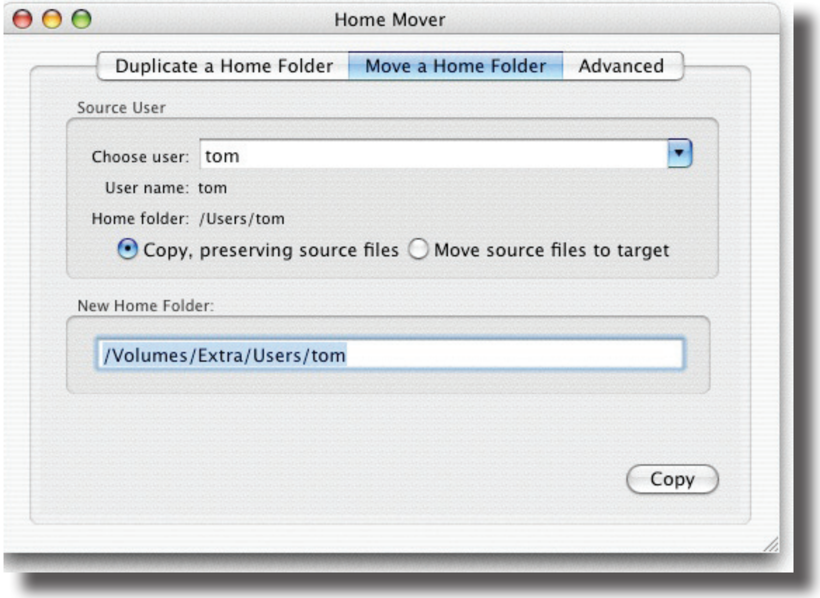
When you are deploying ADmitMac in your organization, you will often need to install it on Macintosh computers that are already being used. The user of such a computer has a local account and their files are stored on the local Hard Drive. It is often necessary to change the configuration so that the user will log in using domain credentials instead of local credentials.

Home Mover can help you convert the local user account files so that they can be used by the domain user account. Files are moved or copied to the domain account home folder (still on the local machine), and their ownership is changed. To perform this task see the section below entitled, "Making a Copy of a User's Home Folder for use by a Different User." Fill in the local user account as the source user, and the target user as the domain user.

If you have enough local disk space to copy the home folder, you should select *Copy*, preserving source files. This will allow you to make sure the user can log in using their domain credentials without disturbing the original files. Once you are sure everything is working, you may delete the local user account from the Macintosh. If you are short on local disk space, you should back up the user's data, then choose *Move source files to target*. Once you have tested to make sure everything works properly, you may then delete the local user account from the Macintosh.

Moving or Copying a Local User's Home Folder to a Different Location

1. Click on the *Move a Home Folder* tab.
2. Enter the name of the user you want to move in the *Choose User* field.
3. To move files instead of copying them, click on the *Move source files to target* radio button. Note that the source user will no longer have a home folder when you choose the *Move* option. Files in the home folder will only be usable by the target user. If the new home folder is on a different volume, files will be copied regardless of the radio button setting.
4. Enter the new location for the home folder. You may drag a folder to this field from the Finder, but if you do, you will need to type the last part of the new location's path.
5. Click the *Copy* or *Move* button.



Source User

Choose user: tom

User name: tom

Home folder: /Users/tom

● Copy, preserving source files ○ Move source files to target

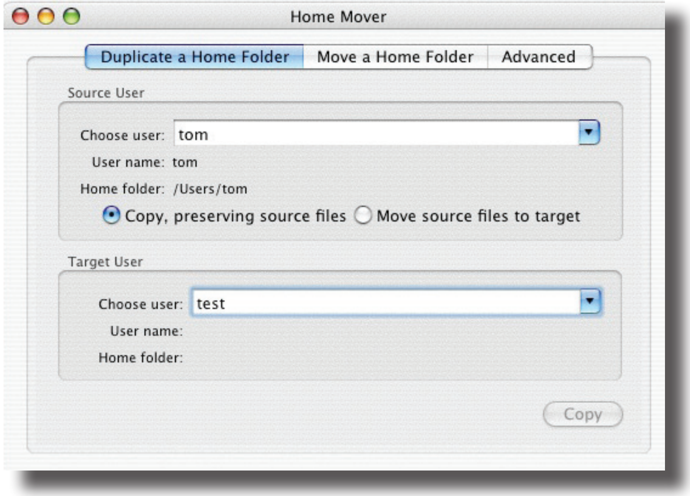
New Home Folder:

/Volumes/Extra/Users/tom

NOTE: You can't move an ADmitMac domain user's home folder. ADmitMac domain user home folders must always be in a specific path. Refer to the AD Commander section entitled, "Modify Home Folder Path" for information about storing domain user home folders on different volumes.

Making a Copy of a User’s Home Folder For Use By a Different User

1. Click on the *Duplicate a Home Folder* tab.
2. Enter the name of the user you want to move in the *Choose User* field inside the *Source user* box.
3. To convert the files for use by the new user without copying them, click on the Move source files to target radio button. If you have enough disk space to copy the source user’s home folder, you may choose the *Copy, preserving source files* radio button. Files will then be copied and converted for use by the target user. If the new home folder is on a different volume, files will be copied regardless of the radio button setting.



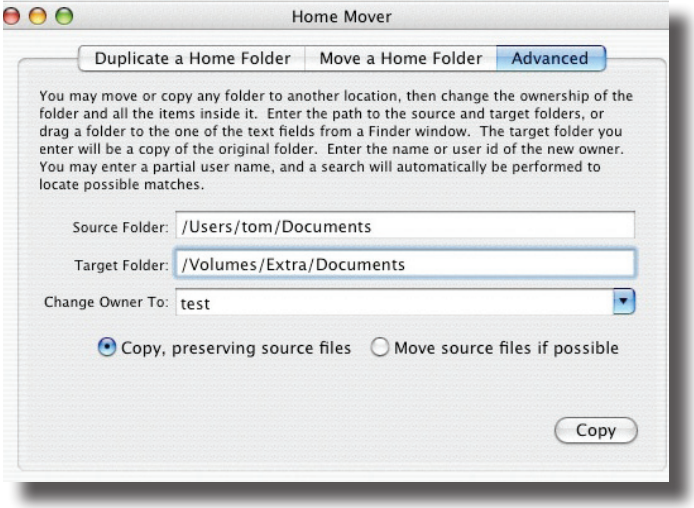
Choose user: tom
User name: tom
Home folder: /Users/tom
● Copy, preserving source files ○ Move source files to target

Choose user: test
User name:
Home folder:

4. Enter the name of the domain user that will own the copied or moved home folder in the *Choose User* field inside the Target user box.
5. Click the *Copy* or *Move* button.

Moving or Copying Any Folder to a New Location

1. Click on the *Advanced* tab.
2. Enter the name of the folder you wish to copy or move in the *Source Folder* field. You may also drag a folder to this field using the Finder.
3. Enter the name that the new folder should have after the copy or move is completed in the *Target Folder* field. The name you enter will be the copy of the original folder when copying or the new name of the original folder when moving. There must not be an existing item with this name. You may also drag a folder to this field using the Finder, and then add a slash character followed by the new name for the folder.



You may move or copy any folder to another location, then change the ownership of the folder and all the items inside it. Enter the path to the source and target folders, or drag a folder to the one of the text fields from a Finder window. The target folder you enter will be a copy of the original folder. Enter the name or user id of the new owner. You may enter a partial user name, and a search will automatically be performed to locate possible matches.

Source Folder: /Users/tom/Documents
Target Folder: /Volumes/Extra/Documents
Change Owner To: test
● Copy, preserving source files ○ Move source files if possible

4. Enter the name of the user that will be the owner of the files in the *Change owner to* field.
5. Click the *Copy* or *Move* button.

The current version of Home Mover works with local files only. If you are duplicating a local user so they can log in using their domain credentials, you must choose Local home folders as the ADmitMac home folder policy. If you have enough local disk space to copy the home folder, you should select Copy, preserving source files. This will allow you to make sure the user can log in using their domain credentials without disturbing the original files. Once you are sure everything is working, you may delete the local user account from the Macintosh. If you are short on local disk space, you should back up the user’s data, then choose Move source files to target. Once you have tested to make sure everything works properly, you may then delete the local user account from the Macintosh.

About Moving and Copying Folders

Files are copied and moved using administrative privileges. You must have administrative credentials to use Home Mover. When Home Mover does its work, it needs to modify some files that contain references to other files in a user's home folder. For example, when you drag a document from your Documents folder to your dock, a reference to the original document is placed inside the Dock application's preference file (`~/Library/Preferences/com.apple.dock.plist`). If you copy or move a home folder, the reference to the original document needs to be modified so it refers to the new location of the document.

Suppose you have a user named Tom with a home folder `/Users/tom`, and you wish to put Tom's home folder on a different volume. Tom has placed an alias to `/Applications/Calculator` on his desktop. He has also placed an alias to his `Sites/index.html` file on his desktop. If you use Home Mover to put Tom's home folder on `/Volumes/Extra/Users/Tom`, then the alias to `Tom's Sites/index.html` will be modified to point to `/Volumes/Extra/Users/Tom/Sites/index.html`. The alias to `/Applications/Calculator` will not be modified since it does not refer to a file in Tom's original home folder.

Differences between Moving and Copying Folders

When Home Mover moves a folder, the folder is simply renamed and put inside a different folder. Files inside the folder are not copied. If the target of an operation is on a different volume than the source folder, the folder can't be moved, and will be copied instead. **If a home folder is moved, the source user will no longer have a home folder.** If they log in, a new home folder will be created for them. If you are moving a local user's home folder, it is usually desirable to delete the local account after you have made sure that the home folder was successfully moved.

When Home Mover copies a folder, a copy is made of every item in the original folder. The original folder is not modified in any way. You can control whether Home Mover moves or copies folders using the radio buttons.

Conversion of File Data

When Home Mover finishes moving or copying items to the right place, it does some further conversion. First, all symbolic links that pointed to a file inside the original folder are changed to point to the new location for the moved or copied item. Second, all files that have a resource fork are scanned for alias resources. Alias resources are also updated to point to the new location for the moved or copied item. Lastly, Home Mover looks for a folder named `Library/Preferences` inside the folder being moved or copied. If it finds this folder, it looks inside all the preference files for alias data, and converts the data so that the alias points to the new location for the moved or copied item.

Using Home Mover as a Command Line Tool

The Home Mover application bundle contains a tool that can be used in shell scripts and from the command line. The tool should always be run as root because it changes file ownership.

Usage:

```
 Home\ Mover/Contents/MacOS/folderops -sourcePath source -targetPath tar-
get [-preserveSource YES] [-owner ownername] [-group groupname] [-modi-
fyUserHome accountname]
```

Where:

`source` is the path to the source folder of the copy/move operation

`target` is the path to the target folder of the copy/move operation

`-preserveSource YES` causes files to be copied instead of moved

`ownername` if supplied, target folder items owner will be changed to `ownername`

`groupname` if supplied, target folder items group will be changed to `groupname`

`modifyUserHome` if supplied, the account '`accountname`' will have its home folder changed to the target folder

Mac OS X Workgroup Management Using ADmitMac

Overview

ADmitMac integrates Apple's Workgroup Manager with Active Directory domains for increased workgroup management interoperability. When you install ADmitMac, you can complete the following tasks in Apple's Workgroup Manager using your Active Directory domain for authentication:

- Manage Macintosh User and Group MCX Settings (Preferences).
- Create computer groups.
- Add or delete Active Directory computer accounts to or from a computer group.
- Add or delete Active Directory users to or from an Active Directory or Open Directory group.

> **NOTE:** Workgroup Manager cannot be used to create Active Directory user accounts or Active Directory user groups. Use your PC tools for this or use AD Commander.

Getting Started

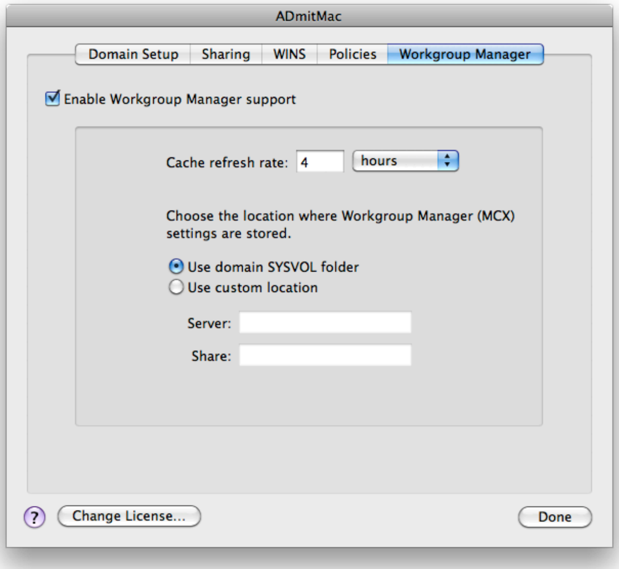
Before you begin using Workgroup Manager, you need to decide where ADmitMac will store workgroup management data. ADmitMac gives you flexibility that lets you choose the best approach. You can also turn off workgroup management support to improve performance when it is not needed. Control of workgroup management settings is done using the Directory Utility application.

Launch Directory Utility from the /System/Library/CoreServices folder, then do the following:

1. Click Services in the toolbar.
2. Click the padlock to unlock it. You will be prompted for an administrator password.
3. Double click on ADmitMac.
4. Click on the Workgroup Manager tab.

The window that appears lets you choose how often the local copy of Workgroup Manager settings are updated from the network store. You can also choose where the settings are stored on your network. ADmitMac lets you keep these settings in the same place you keep group policy for your domain - in the SYSVOL folder. You may also store them in any share that you choose.

You can choose to disable Workgroup Manager by unchecking "Enable Workgroup Manager support". This will improve client responsiveness when you don't need to manage Macintosh clients.



☑ Enable Workgroup Manager support

Cache refresh rate: 4 hours

Choose the location where Workgroup Manager (MCX) settings are stored.

● Use domain SYSVOL folder
○ Use custom location

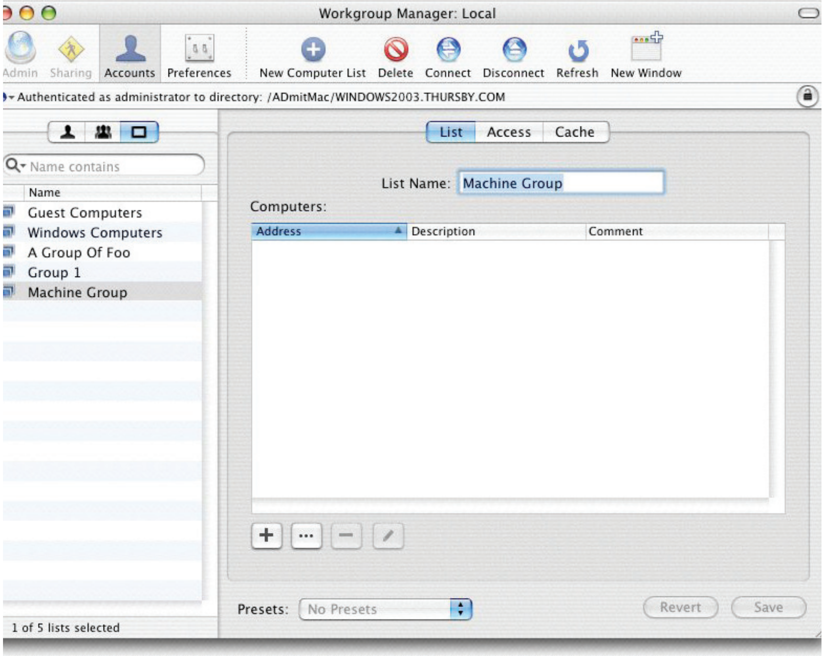
Server:

Share:

Manage Macintosh User and Group Preferences (MCX Settings)

To change Macintosh user or group preferences using Apple's Workgroup Manager:

1. Open the *Workgroup Manager* application and click *Command + D* to cancel out of the first authenticating window. The main Workgroup Manager window will display.
2. Verify that the desired domain displays in the authenticated domain list found immediately under the row of control icons. The domain should display automatically if you are joined to the domain and it is accessible.
3. To make changes to the groups and user preferences, click the *lock* and authenticate with credentials having authority to make changes to the Active Directory domain.



Authenticated as administrator to directory: /ADmitMac/WINDOWS2003.THURSBY.COM

Name
Guest Computers
Windows Computers
A Group Of Foo
Group 1
Machine Group

1 of 5 lists selected

List Name: Machine Group

Computers:

Address	Description	Comment

Presets: No Presets

4. Select the desired user or group then click the *Preferences* icon in the tool bar.
5. Click the icon of the particular preference for which you wish to modify.
6. Select *Always* or *Once* in the *Manage these settings* field for each preference change. For example, you can change user preferences for:

- Applications: determine which application a Macintosh user can use.
- Media Access: restrict user access to peripherals such as CD or DVD readers / writers.
- Finder: control user Finder access.
- Mobile Accounts: select universal access preferences for user disabilities.

6. Click Save.

Create a Macintosh Computer Group

Computer lists are useful when you want to supply preference settings based on a type of Macintosh, or its physical location. To create a Macintosh computer group, complete the following:

1. Open the *Workgroup Manager* application and click *Command + D* to cancel out of the first authenticating window. The main Workgroup Manager window will display.
2. Verify that the desired domain displays in the authenticated domain list. It should display automatically if you are joined to the domain and it is accessible.
3. Click the *lock* and authenticate with credentials with the authority to make changes to the Active Directory domain.
4. Click on the *Computer Groups* tab (looks like overlapping rectangles) and select the *Accounts* icon in the tool bar.

5. Click on the *New Computer Group* icon in the tool bar to create a new computer group.

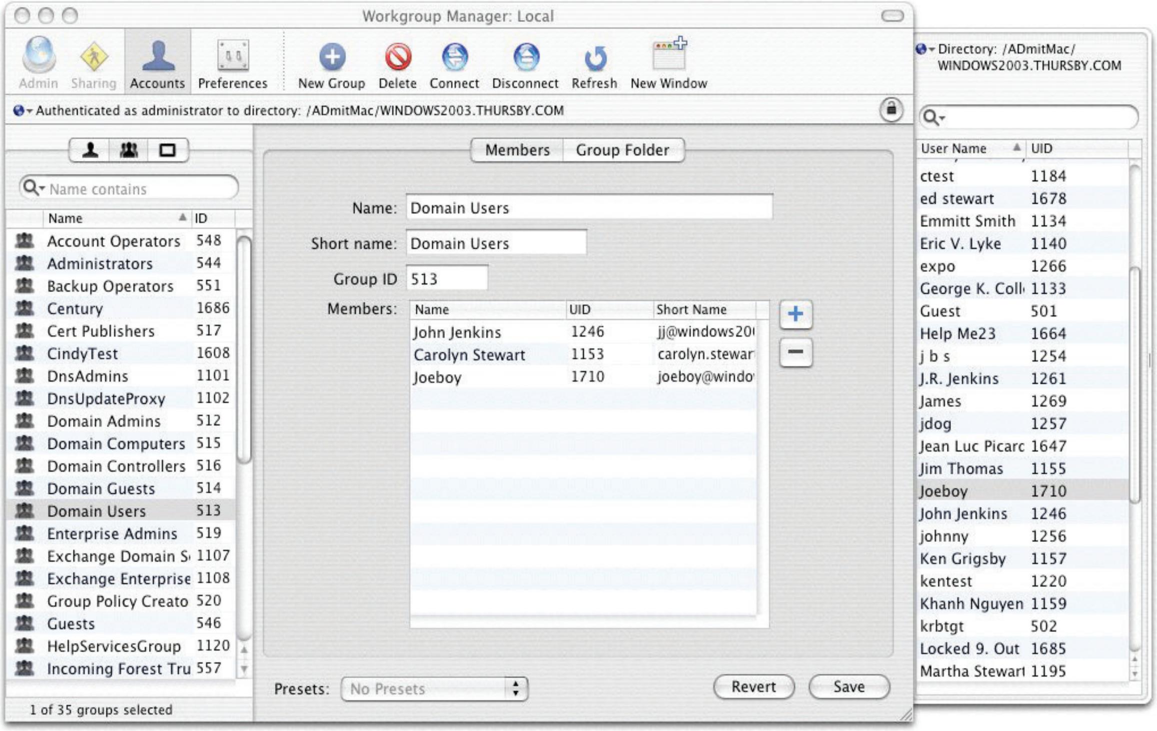
6. To add a computer account to the list, click the + at the bottom of the field and enter the computer's Ethernet ID (found in **System Preferences** > **Network** > **Show Built-in Ethernet** > **Ethernet** tab.).

7. Click *Save*.

Add Users to a Group, Delete Users from a Group

If you would like to put an Active Directory user into a pre-existing group complete the following:

1. Open the *Workgroup Manager* application and click *Command + D* to cancel out of the first authenticating window. The main Workgroup Manager window will display.



Authenticated as administrator to directory: /ADmitMac/WINDOWS2003.THURSBY.COM

Name	ID
Account Operators	548
Administrators	544
Backup Operators	551
Century	1686
Cert Publishers	517
CindyTest	1608
DnsAdmins	1101
DnsUpdateProxy	1102
Domain Admins	512
Domain Computers	515
Domain Controllers	516
Domain Guests	514
Domain Users	513
Enterprise Admins	519
Exchange Domain S	1107
Exchange Enterprise	1108
Group Policy Creato	520
Guests	546
HelpServicesGroup	1120
Incoming Forest Tru	557

1 of 35 groups selected

Name: Domain Users

Short name: Domain Users

Group ID: 513

Members:

Name	UID	Short Name
John Jenkins	1246	jj@windows20
Carolyn Stewart	1153	carolyn.stewar
Joeboy	1710	joeboy@windo

User Name	UID
ctest	1184
ed stewart	1678
Emmitt Smith	1134
Eric V. Lyke	1140
expo	1266
George K. Coll	1133
Guest	501
Help Me23	1664
j b s	1254
J.R. Jenkins	1261
James	1269
jdog	1257
Jean Luc Picarc	1647
Jim Thomas	1155
Joeboy	1710
John Jenkins	1246
johnny	1256
Ken Grigsby	1157
kentest	1220
Khanh Nguyen	1159
krbtgt	502
Locked 9. Out	1685
Martha Stewart	1195

2. Verify that the desired domain displays in the authenticated domain list. It should display automatically if you are joined to the domain and it is accessible.

3. To make changes to a group, click the *lock* and authenticate using credentials with the authority to make changes to the Active Directory domain.

4. Select the *Groups* tab (multiple silhouettes). Choose the group you wish to change, or search for it using the search field.

5. Click the *Members* tab in the right-hand pane. Click the + icon to add users, or select a user and click the - icon to remove them from the group. When adding users to a group, a drawer will appear that lets you choose a user to add.

6. Click *Save*.

Change the Location of Workgroup Manager MCX Settings on the Domain

You may want to store MCX settings in a location other than your domain SYSVOL folder. This can be done using the ADmtiMac directory service plug-in found in the Directory Utility application.

Step 1: Create a New Shared folder

a. Select the server on the domain that will host the share where the MCX settings will be stored (for example, `bigserver`, in a domain named `tango.thursby.com`).

b. Create a shared folder on this server (for example, `Public`).

c. Inside the shared folder create a new folder with the same name as the domain (in this case it would be `TANGO.THURSBY.COM`).

d. Set the permissions on the new folder so that the account that will be setting up Workgroup Manager in the following step has Read/Write Access to the folder.

Step 2: Configure the Macintosh Client

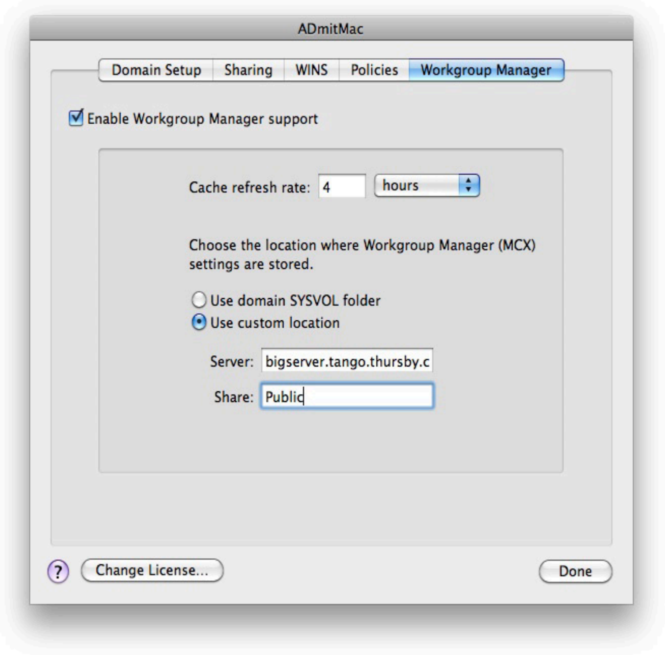
a. Launch Directory Utility from the /System/Library/CoreServices folder, then do the following:

b. Click Services in the toolbar.

c. Click the padlock to unlock it. You will be prompted for an administrator password.

d. Double click on ADmitMac.

e. Click on the Workgroup Manager tab, check "Enable Workgroup Manager support", select the "Use custom location" radio button, and enter the FQDN of the server (the NetBIOS name may also be used) and the share name in the fields provided.



☑ Enable Workgroup Manager support

Cache refresh rate: 4 hours

Choose the location where Workgroup Manager (MCX) settings are stored.

○ Use domain SYSVOL folder
● Use custom location

Server: bigserver.tango.thursby.c

Share: Public

Step 3: Confirm the changed location of WorkGroup Manager MCX settings:

a. Restart the Macintosh.

b. Log in and launch *Workgroup Manager.*

c. Make changes to the *Workgroup Manager* settings and click the *Done* button.

d. The MCX settings should now be in the new location.

e. To verify this, go to the new server and open the folder with your domain name and there should be a new folder called `ADmitMac`.

Bugs Associated with Workgroup Manager

There are some Workgroup Manager attributes that you will not be able to edit. Unfortunately, because of OS limitations at this time, we cannot display an error message for every problem or incompatibility. However, we do display three main bug numbers that are associated with most problems you may have using Workgroup Manager. If you get error number 14121, then you were attempting to change a read-only attribute. We don't allow you to change read-only attributes, e.g. changing your username.

These are typically bugs, or the SYSVOL mount was lost for some reason.

14350: An error occurred writing data to the SYSVOL.

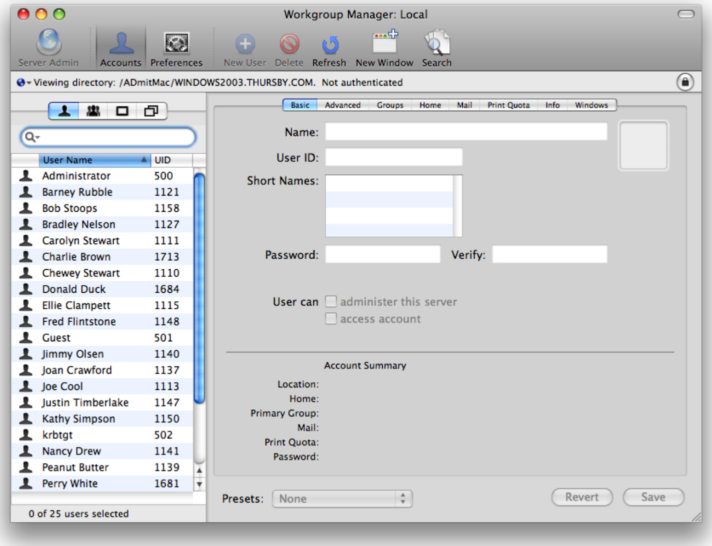
14351: An error occurred reading data from the SYSVOL.

Setting Up Group Folders using Workgroup Manager

Workgroup Manager may also be used in conjunction with ADmitMac to set up group folders to be mounted when a member of the group logs into their Macintosh.

After you have verified that you have set up a share on a server and that it is accessible to members of the group, proceed with the following steps on the client Macintosh:

1. Open the Workgroup Manager application and type "Command + D" to cancel out of the first authentication window. The main Workgroup Manager will display. Verify that the desired domain is displayed in the authenticated domain list in the viewing area. It should display automatically if you are joined to the domain and it is accessible.

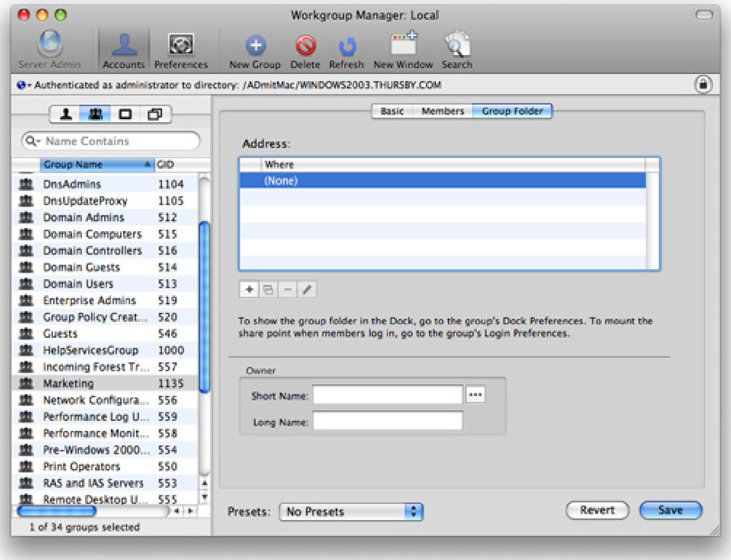


Viewing directory: /ADmitMac/WINDOWS2003.THURSBY.COM. Not authenticated

User Name	UID
Administrator	500
Barney Rubble	1121
Bob Stoops	1158
Bradley Nelson	1127
Carolyn Stewart	1111
Charlie Brown	1713
Chewey Stewart	1110
Donald Duck	1684
Ellie Clampett	1115
Fred Flintstone	1148
Guest	501
Jimmy Olsen	1140
Joan Crawford	1137
Joe Cool	1113
Justin Timberlake	1147
Kathy Simpson	1150
krbtgt	502
Nancy Drew	1141
Peanut Butter	1139
Perry White	1681

0 of 25 users selected

2. Authenticate to the domain controller by clicking on the lock icon and typing the administrator username and password. Select the Groups tab (multiple silhouettes) and select the group you wish to use (you may also use the Search field at the top of the list). Click on the "Group Folder" tab in the right pane.



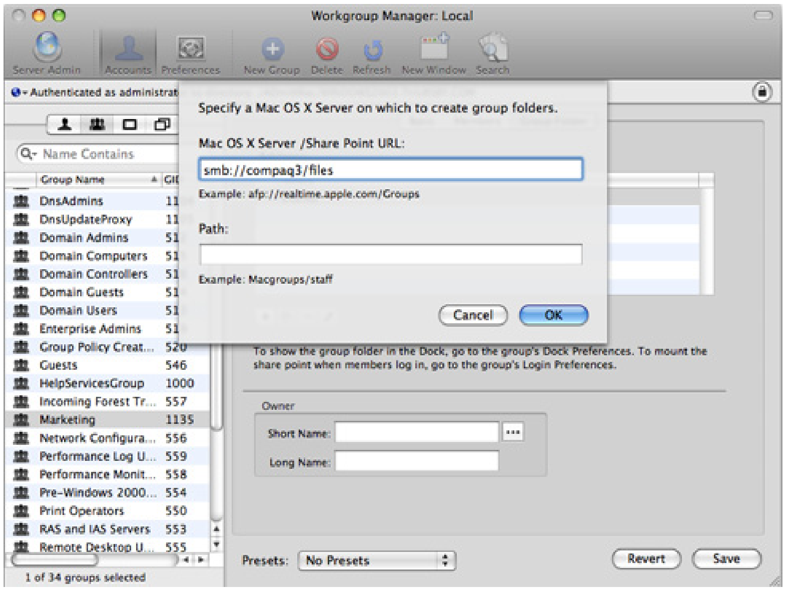
Authenticated as administrator to directory: /ADmitMac/WINDOWS2003.THURSBY.COM

Group Name	GID
DnsAdmins	1104
DnsUpdateProxy	1105
Domain Admins	512
Domain Computers	515
Domain Controllers	516
Domain Guests	514
Domain Users	513
Enterprise Admins	519
Group Policy Creat...	520
Guests	546
HelpServicesGroup	1000
Incoming Forest Tr...	557
Marketing	1135
Network Configura...	556
Performance Log U...	559
Performance Monit...	558
Pre-Windows 2000...	554
Print Operators	550
RAS and IAS Servers	553
Remote Desktop U...	555

1 of 34 groups selected

To show the group folder in the Dock, go to the group's Dock Preferences. To mount the share point when members log in, go to the group's Login Preferences.

3. Click on the "+" icon and enter the URL of the group folder on your server and the path to the share. Click the "OK" button.



Authenticated as administrat

Specify a Mac OS X Server on which to create group folders.

Mac OS X Server /Share Point URL: smb://compaq3/files

Example: afp://realtime.apple.com/Groups

Path:

Example: Macgroups/staff

Group Name	GID
DnsAdmins	11
DnsUpdateProxy	11
Domain Admins	51
Domain Computers	51
Domain Controllers	51
Domain Guests	51
Domain Users	51
Enterprise Admins	51
Group Policy Creat...	520
Guests	546
HelpServicesGroup	1000
Incoming Forest Tr...	557
Marketing	1135
Network Configura...	556
Performance Log U...	559
Performance Monit...	558
Pre-Windows 2000...	554
Print Operators	550
RAS and IAS Servers	553
Remote Desktop U...	555

1 of 34 groups selected

To show the group folder in the Dock, go to the group's Dock Preferences. To mount the share point when members log in, go to the group's Login Preferences.

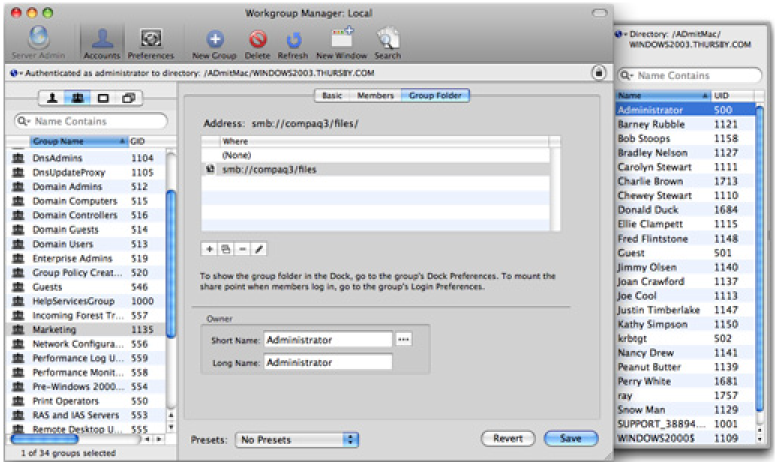
Owner

Short Name:

Long Name:

Presets: No Presets

4. Click the ". . ." icon to select the owner of the folder. A list of users will appear on the right side of the panel. Drag the name of the owner to the short name field. Click the "Save" button. The Groups folder will now be added to the list.



Authenticated as administrator to directory: /ADmitMac/WINDOWS2003.THURSBY.COM

Group Name	GID
DnsAdmins	1104
DnsUpdateProxy	1105
Domain Admins	512
Domain Computers	515
Domain Controllers	516
Domain Guests	514
Domain Users	513
Enterprise Admins	519
Group Policy Creat...	520
Guests	546
HelpServicesGroup	1000
Incoming Forest Tr...	557
Marketing	1135
Network Configura...	556
Performance Log U...	559
Performance Monit...	558
Pre-Windows 2000...	554
Print Operators	550
RAS and IAS Servers	553
Remote Desktop U...	555

1 of 34 groups selected

Address: smb://compaq3/files/

Where
(None)
smb://compaq3/files

To show the group folder in the Dock, go to the group's Dock Preferences. To mount the share point when members log in, go to the group's Login Preferences.

Owner

Short Name: Administrator

Long Name: Administrator

Presets: No Presets

Directory: /ADmitMac/WINDOWS2003.THURSBY.COM

Name	UID
Administrator	500
Barney Rubble	1121
Bob Stoops	1158
Bradley Nelson	1127
Carolyn Stewart	1111
Charlie Brown	1713
Chewey Stewart	1110
Donald Duck	1684
Ellie Clampett	1115
Fred Flintstone	1148
Guest	501
Jimmy Olsen	1140
Joan Crawford	1137
Joe Cool	1113
Justin Timberlake	1147
Kathy Simpson	1150
krbtgt	502
Nancy Drew	1141
Peanut Butter	1139
Perry White	1681
ray	1757
Snow Man	1129
SUPPORT_38894...	1001
WINDOWS2000$	1109

5. You can now set group folders to automatically mount when a member of the group logs in. To do this access the Perferences pane by clicking the Preferences icon, then click the "Login" icon, then the "Items" tab. Check the boxes "Authenticate selected sharepoint with user's login name and password" and "Add group share point". Click the "Apply Now" button. Quit Workgroup Manager.

Managing Macintosh Clients using Active Directory Group Policy

Overview

ADmitMac supports two ways to manage Macintosh clients joined to an Active Directory domain. You can use Active Directory group policy using Macintosh specific administrative templates provided with ADmitMac. You can also use Apple's Workgroup Manager utility, saving the data it generates on your domain. In either case, it is important to know that ADmitMac always uses some group policies when a Macintosh is joined to a domain because Workgroup Manager does not have support for all the settings ADmitMac needs to operate. When you use Workgroup Manager, it's settings override the same settings provided by a group policy object. For more information on Workgroup Manager, see page 25.

Active Directory group policies help administrators configure settings for one group of settings for one or more computers and users. ADmitMac extends group policy support to Macintosh clients to make administration more seamless because there are no new tools to deploy or learn how to use. ADmitMac never requires schema changes or any other changes that affect the whole forest. If you plan to use group policy to manage Macintosh clients, you will need a good understanding of Active Directory group policies. There are some basic concepts that will be helpful if you are unfamiliar with group policy that will help you get started.

Administrators make effective use of group policies by creating group policy objects (GPO) containing basic settings for users and computers. Group Policy objects are then linked to one or more organizational units (OU) in Active Directory so that the GPO settings affect all the user and computer objects contained in the OU. GPOs do NOT apply directly to groups of users or computers in the same way that Apple's Workgroup Manager does. However, GPOs can be applied to specific groups of users because access to a GPO is moderated by access control lists. The following example illustrates these concepts.

Consider a school where users are either staff members or students. You want to restrict applications a student can launch, but staff members will not be restricted. The most straightforward way to do this would be to group users into organizational units as follows:
OU=STAFF,DC=MYSCHOOL,DC=EDU contains all staff members
OU=STUDENTS,DC=MYSCHOOL,DC=EDU contains all students

You would use the Microsoft Active Directory tools to create a GPO that restricts applications a Macintosh user can launch. That GPO would then be applied to the STUDENTS ou. The next time a student logs into a Macintosh, the restrictions will be enforced.

Consider a situation where you want to remove the application restriction for one student only. You could move the student account into the STAFF OU, but there may be other policies that you don't want applied to the student. One solution to this would be to place an access control list (ACL) on the GPO that restricts applications. The ACL would give everyone read permission to the GPO, but would deny access to the one particular student. Since the student account can't read the GPO, its settings will not apply when the student logs in. At a future time, the ACL DENY access entry can be removed, restoring the GPO restrictions for the student.

How Group Policy Settings affect the Macintosh

When you install ADmitMac, you are asked to configure a number of settings. These settings are stored in a local policy database on the Macintosh client. The same settings can be configured in a Group Policy Object. Settings from a GPO will always override the local policy settings. When using the Directory Service ADmitMac plugin, you may find that some settings cannot be changed. This happens when the setting is provided by a GPO. There are three categories of settings that can be applied using the ADmitMac templates. First, you may configure Macintosh managed client settings (MCX) such as the appearance of the Dock. Second, you may configure settings that change the behavior of the ADmitMac software itself, such as the home folder policy. Finally, you can configure settings that apply to both Windows and Macintosh clients such as the LanMan or signing policy.

The following table gives a comprehensive list of settings you can make using the templates supplied with ADmitMac.

Policy	Setting
Applications	Applications which are allowed to be launched §
	Disallow applications within these folders §
	Allow applications within these folders §
	Dashboard widgets which are allowed to run §
	Allow Front Row
Dock	Dock Size
	Dock screen position
	Dock minimization effect
	Automatically hide and show the Dock
	Animate opening applications
	Enable Dock magnification
Finder	Preferences: Show servers on desktop
	Preferences: Show hard disks on desktop
	Preferences: Show removable media (such as CDs) on desktop
	Preferences: Set new window target
	Preferences: Always open folders in new window
	Preferences: Always open windows in column view
	Preferences: Show warning before emptying the Trash
	Preferences: Always show file extensions
	Command: Disable 'Burn Disc'
	Command: Disable 'Connect to Server'
	Command: Disable 'Eject'
	Command: Disable 'Go to Folder'
	Command: Disable 'Go to iDisk'
	Command: Disable 'Restart'
	Command: Disable 'Shut Down'
	Desktop View settings
	Default View settings
	Computer View settings
Login	Items: User may press Shift to keep items from opening
	Items: User may add and remove additional items
	Items: Visible auto-launched applications
	Items: Hidden auto-launched applications
	Window: Login window heading
	Window: Show list of users able to use this computer
	Window: Show Restart button
	Window: Show ShutDown button

Policy	Setting
Media Access	Eject all removable media at logout
	Allow CDs & CD-ROMs
	Allow DVDs
	Allow Recordable Discs
	Allow Internal Discs
	Allow External Discs
	Allow Disk Images
	Allow DVD-RAM
Mobility	Preference Sync Rules: Sync in the background
	Preference Sync Rules: Sync manually
	Preference Sync Rules: Merge with user's settings
	Preference Sync Rules: Folder to sync
	Preference Sync Rules: Folders to not sync
	Preference Sync Rules: Sync at login
	Preference Sync Rules: Sync at logout
	Home Sync Rules: Sync at login
	Home Sync Rules: Sync at logout
	Home Sync rules: Sync in the background
	Home Sync Rules: Sync manually
	Home Sync Rules: Merge with user's settings
	Home Sync Rules: Folders to sync
	Home Sync Rules: Folders to not sync
	Rules Options: Sync in background
	Rules Options: Show status in menu bar
	Account Creation: Create mobile account when user logs into network account
	Account Creation: Require confirmation before creating mobile account
	Account Creation: Show Don't ask me again checkbox
	Account Creation Options: Encrypt contents with FileVault
	Account Creation Options: Home Folder location
	Account Expiry: Delete mobile account
Network	Proxies: Use Passive FTP Mode (PASV)
	Proxies: Enable FTP Proxy
	Proxies: Enable Web Proxy (HTTP)
	Proxies: Enable Secure Web Proxy (HTTPS)
	Proxies: Enable Streaming Proxy (RTSP)
	Proxies: Enable SOCKS Proxy
	Proxies: Enable Gopher Proxy
	Proxies: Automatic Proxy Configuration
	Proxies: Bypass proxy settings for these Hosts & Domains
	Sharing & Interfaces: Disable Internet Sharing
	Sharing & Interfaces: Disable Airport
	Sharing & Interfaces: Disable Bluetooth

Policy	Setting
Software Update	Software Update Server
System Preferences	Items to be shown in System Preferences
ADmitMac *	Home Folders: Set home folder location
	Home Folders: Require confirmation before creating a mobile account
	Home Folders: Mount network home folder on desktop
	Home Folders: Set home folder protocol
	Login Policy: Set default user shell
	Admin: Add this computer's manager domain user to local admin group
	Admin: Set admin group mapping
	OUs: Set users OU
	OUs: Set groups OU
	OUs: Set printers OU
	OUs: Set shared folders OU
	Mappings: Map UID to attribute
	Mappings: Map user UID to attribute
	Mappings: Map user GID to attribute
	Mappings: Map group GID to attribute
	Mappings: Map home directory to attribute
	WINS: enable and configure WINS
Time Machine*	Backup server
	Backup startup volume only
	Skip system files
	Backup automatically
	Limit total backup storage

* For computer OUs only.

§ Restriction or allowance on applications and widgets require their name with the extension (e.g. Safari.app or iCal.wdgt), whereas applications within folders are specified by their full paths (e.g. /Applications/Microsoft Office 2011/).

The following settings in a GPO also apply to PC and Macintosh clients using Window's Registry Editor (regedit.exe):

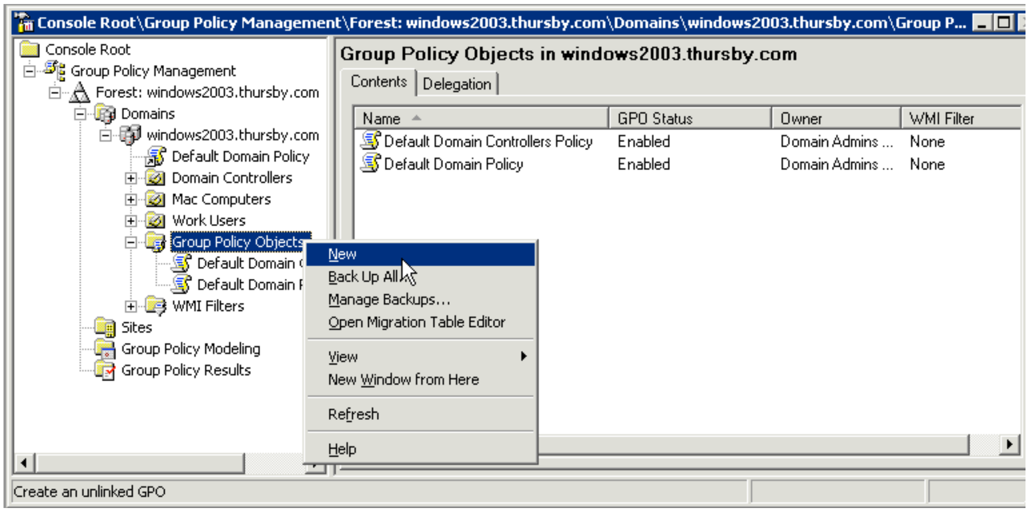
Policy	Setting
SYSTEM\\Current-ContolSet\\Services\\LanManWorkStation\\Parameters	RequireSecuritySignature
	EnableSecuritySignature
	EnablePlainTextPassword
SYSTEM\\Current-ContolSet\\Services\\NetLogon\\Parameters	MaximumPasswordAge
SYSTEM\\Current-ContolSet\\Services\\Tcpip\\Parameters	NV Hostname
SYSTEM\\Current-ContolSet\\Control\\Lsa	LM compatibilitylevel

Getting Started

Be sure that the latest version of ADmitMac is installed on all Macintosh computers and that they are joined to an Active Directory domain. Insert the ADmitMac CD into the drive of the Windows server (if you have down-loaded a .iso image of ADmitMac, you must first burn an installer CD from the image). If the installer does not automatically run, double-click the "ThursbyADMInstaller.exe file".

The first step is to add ADmitMac's administrative templates in the GPO. In the GPO Management Utility:

1. Right-click on Group Policy Objects, then select "New".



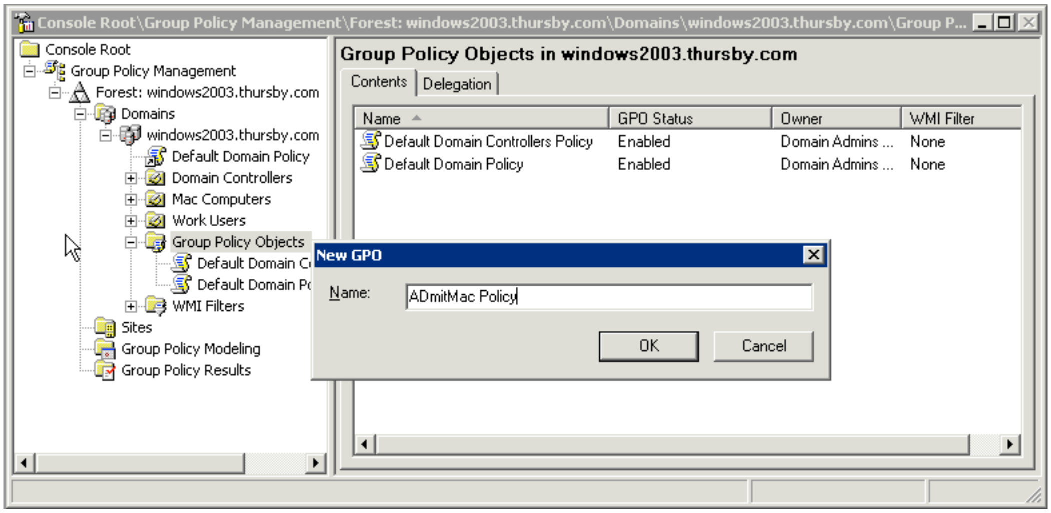
Console Root\Group Policy Management\Forest: windows2003.thursby.com\Domains\windows2003.thursby.com\Group P...

Group Policy Objects in windows2003.thursby.com

Name	GPO Status	Owner	WMI Filter
Default Domain Controllers Policy	Enabled	Domain Admins ...	None
Default Domain Policy	Enabled	Domain Admins ...	None

Create an unlinked GPO

2. Type in a name for the new GPO.



Console Root\Group Policy Management\Forest: windows2003.thursby.com\Domains\windows2003.thursby.com\Group P...

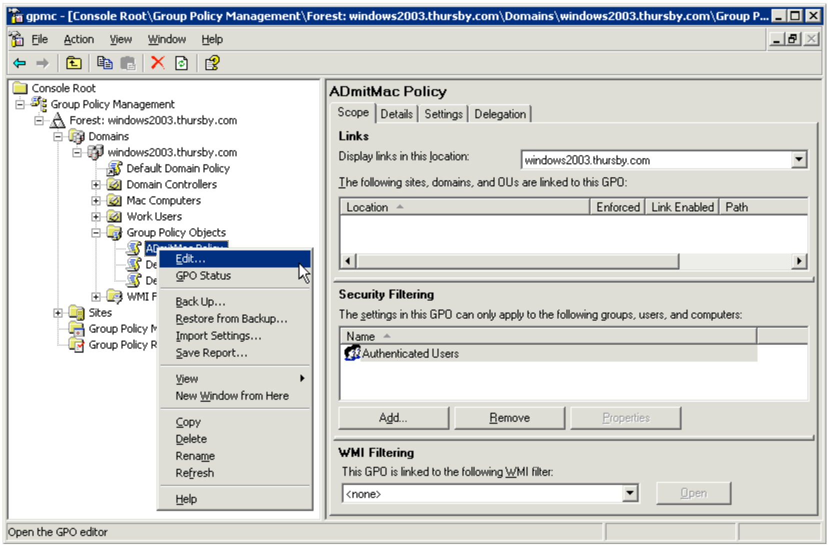
Group Policy Objects in windows2003.thursby.com

Name	GPO Status	Owner	WMI Filter
Default Domain Controllers Policy	Enabled	Domain Admins ...	None
Default Domain Policy	Enabled	Domain Admins ...	None

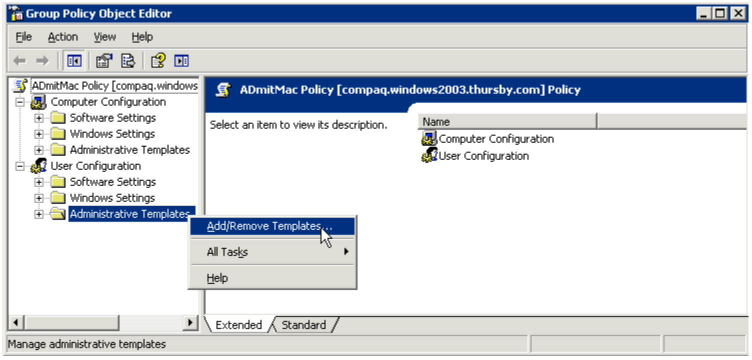
New GPO

Name: ADmitMac Policy

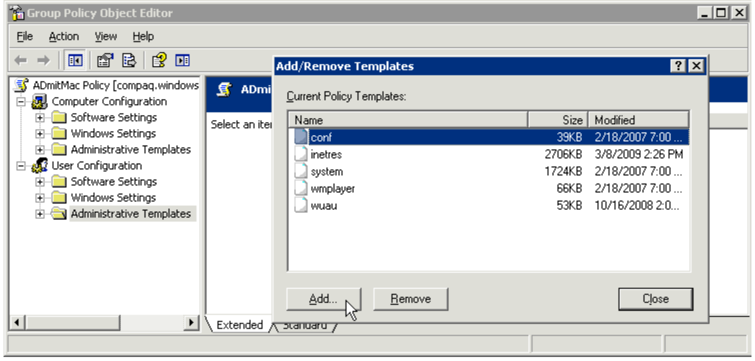
3. Right-click the newly created GPO and select “Edit”.



4. The GPO Object Editor window will appear. Expand either the User settings or the Computer settings in the GPO. Then go to the Administrative Templates (either under User Configuration or Computer Configuration) and right-click. Then select “Add/Remove Templates”.

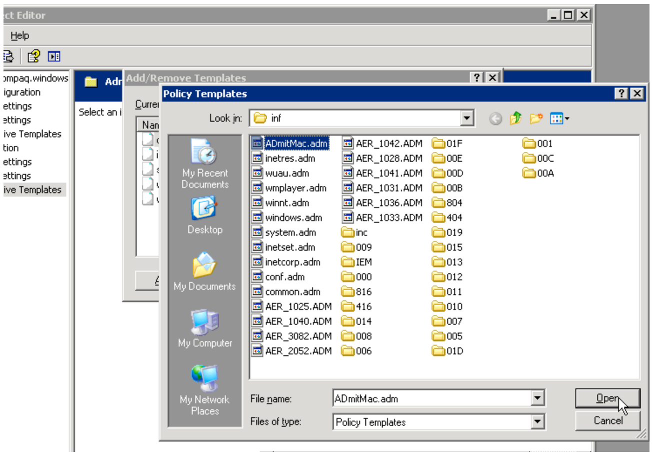


5. The Add/Remove Templates window will appear. Click “Add”.



Name	Size	Modified
conf	39KB	2/18/2007 7:00 ...
inetres	2706KB	3/8/2009 2:26 PM
system	1724KB	2/18/2007 7:00 ...
wmplayer	66KB	2/18/2007 7:00 ...
wuau	53KB	10/16/2008 2:0...

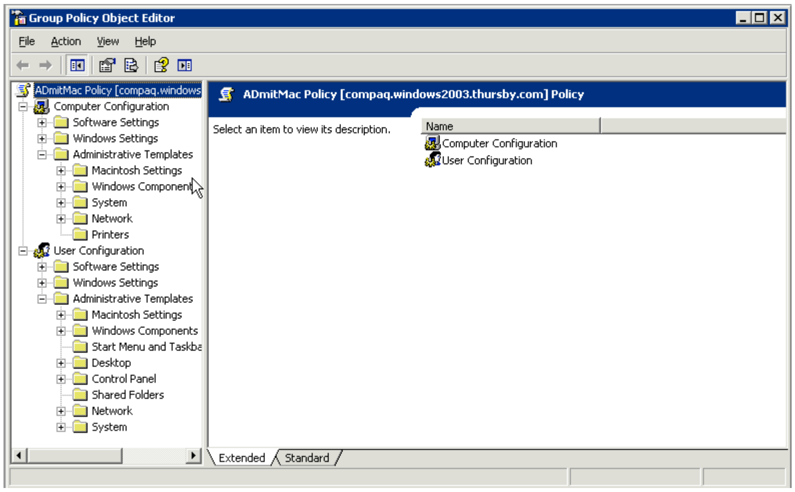
6. Select the ADmitMac .ADM file (located in C:\WINDOWS\inf) and click "Open".



7. The Add/Remove Templates window will now show the newly added ADmitMac template. Click the "Close" button.

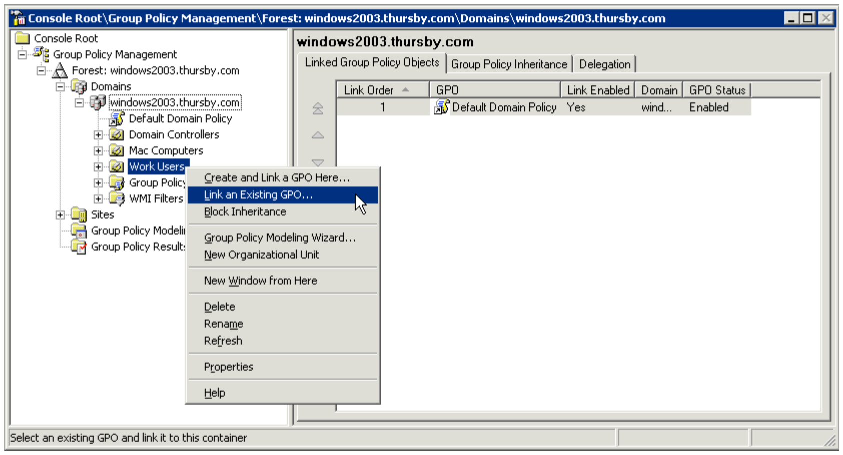
8. Expand the Administrative Templates tree under both the Computer Configuration and User Configuration The .ADM templates should appear as Macintosh Settings under both.

NOTE: On Windows Server 2008, the .ADM templates will appear under the Administrative Templates tree in "Classic Administrative Templates".



Once ADmitMac's ADMs are installed on the server, the Group Policy Management Console is used to link a new GPO by the following steps:

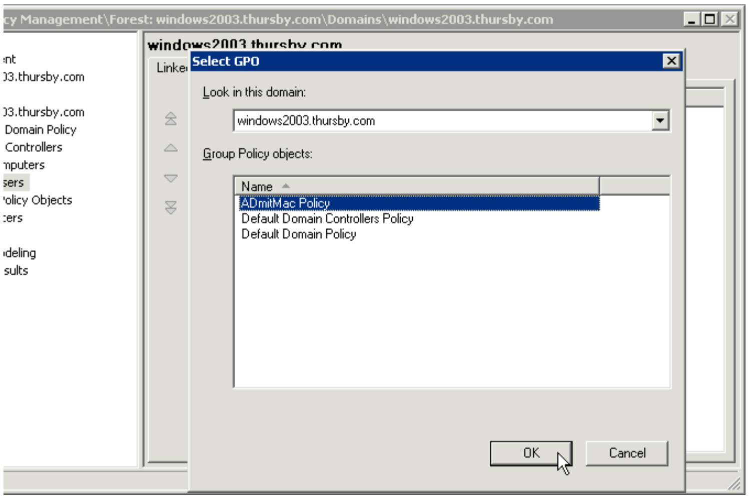
1. Access the OU you want to use with the Group Management Console. Right-click the OU node, and select "Link an Existing GPO..." (you may create a new OU here or in Active Directory before linking).



Link Order	GPO	Link Enabled	Domain	GPO Status
1	Default Domain Policy	Yes	wind...	Enabled

Select an existing GPO and link it to this container

2. Select the Group Policy Object that was created in Step 2 and click "OK".

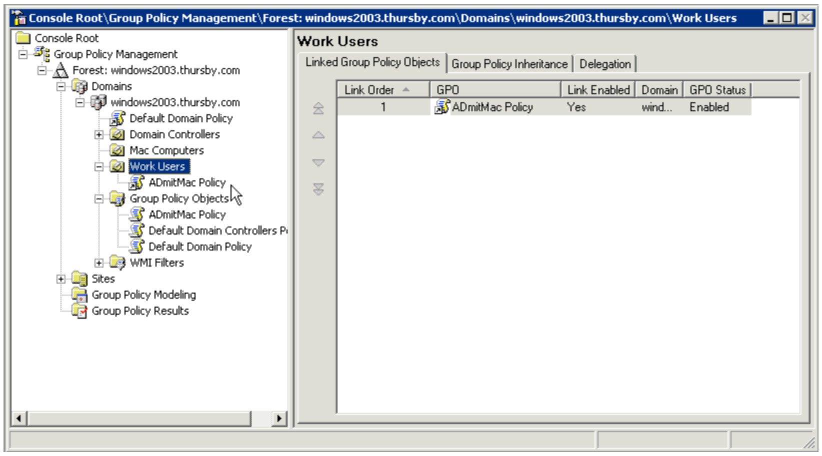


Look in this domain: windows2003.thursby.com

Group Policy objects:

Name
ADmitMac Policy
Default Domain Controllers Policy
Default Domain Policy

3. The newly added Group Policy Object will now appear under the appropriate OU tree. ADmitMac management may now be applied.



Link Order	GPO	Link Enabled	Domain	GPO Status
1	ADmitMac Policy	Yes	wind...	Enabled

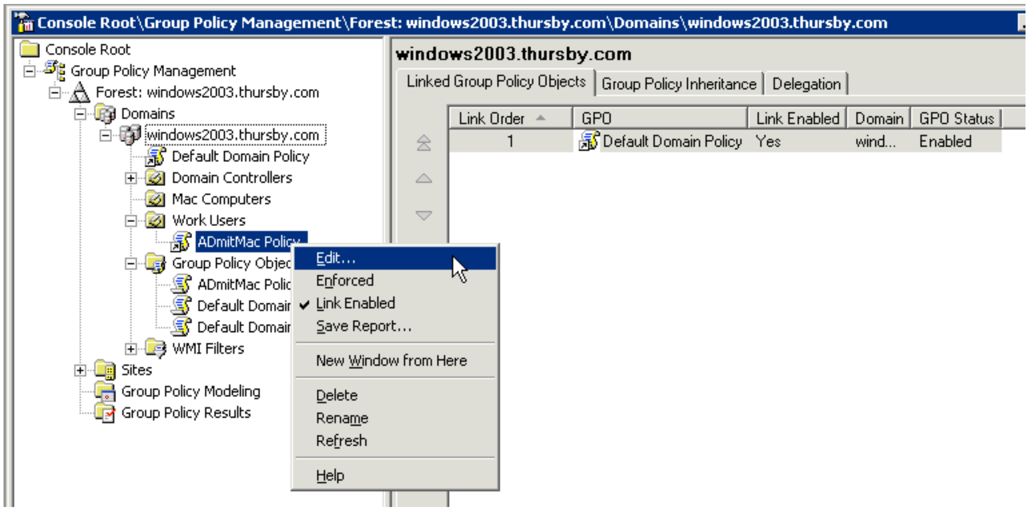
ADmitMac Group Policy Management

Now that ADmitMac's administrative templates are installed and linked to a particular OU, the system administrator can manage Macintosh OS components and applications for user/computer configurations for members of that OU. There are ADmitMac templates common to both users and computers, whereas there are additional templates that apply to computers only (for example, configuring and enabling WINS). In cases where the same settings are applied in both, the computer configuration overrides the user configuration.

User Configuration

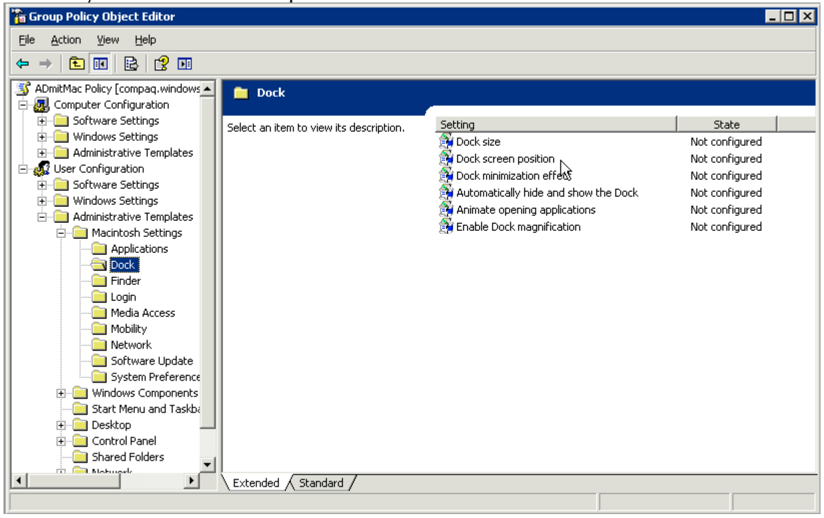
To configure users in an OU, do the following:

1. Right-click on Group Policy Object under the appropriate OU tree (in this example, Work Users) and select "Edit..."



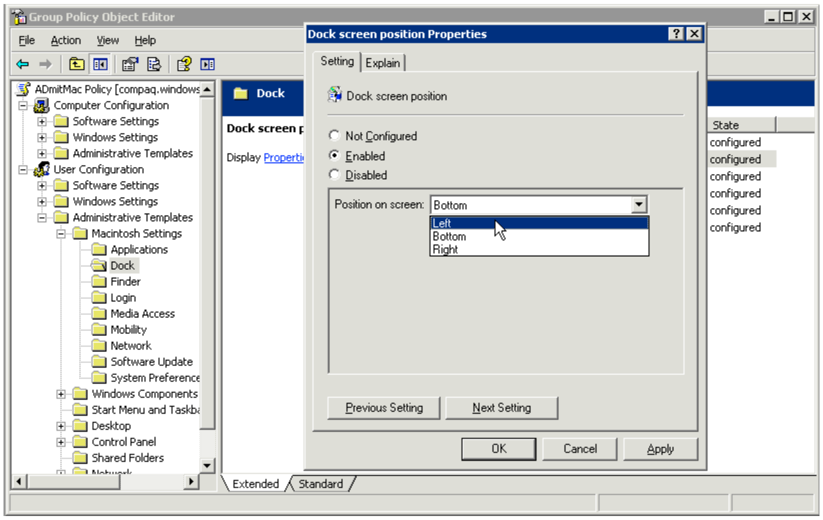
Link Order	GPO	Link Enabled	Domain	GPO Status
1	Default Domain Policy	Yes	wind...	Enabled

2. The GPO Editor window will open. Expand the Administrator Templates under the User Configuration tree. Then expand the Macintosh settings to reveal Applications, Dock, Finder, Login, Media Access, Mobility, Network, Software Update, and System Preferences templates to be configured. As an example, we will select the Dock template and modify the Dock screen position for all users in the Work Users OU.



Setting	State
Dock size	Not configured
Dock screen position	Not configured
Dock minimization effect	Not configured
Automatically hide and show the Dock	Not configured
Animate opening applications	Not configured
Enable Dock magnification	Not configured

3. Double-click (or right-click and select "Properties") on the Dock Screen Position. The properties of the setting will be displayed. Click the "Enable" radio button and select Left from the drop-down menu. Click "Apply" or "OK". Close the GPO Editor.



Dock screen position Properties

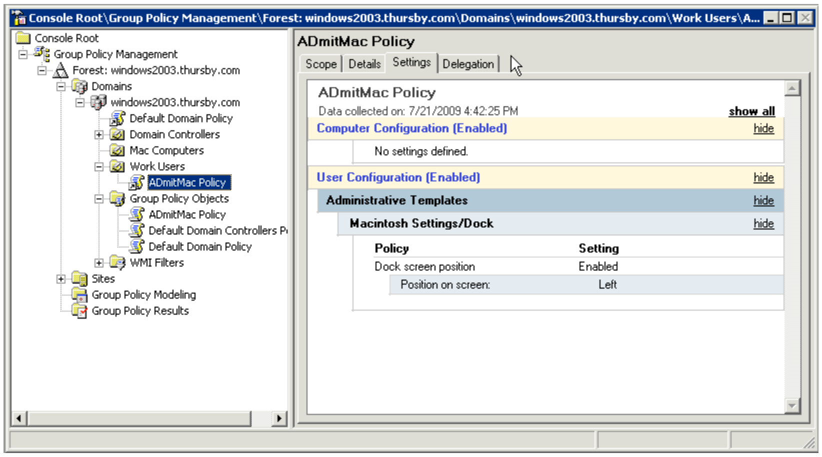
Dock screen position

○ Not Configured
● Enabled
○ Disabled

Position on screen: Bottom

Left
Bottom
Right

4. Group Policy Management will now show the GPO with the Dock position set to the left for all users in the Work Users OU.



ADmitMac Policy

Data collected on: 7/21/2009 4:42:25 PM

Computer Configuration (Enabled)

No settings defined.

User Configuration (Enabled)

Administrative Templates

Macintosh Settings/Dock

Policy	Setting
Dock screen position	Enabled
Position on screen:	Left

The group policy for the user in the OU will take effect 15 minutes after the last time the policy was updated from the domain controller. If you wish to have the policy take effect immediately, run the following command from Terminal (located in the /Applications/Utilities folder) logged in as a local administrator:

```
sudo /Library/FileSystems/DAVE/ReplicatePolicy --user <principle> --force
```

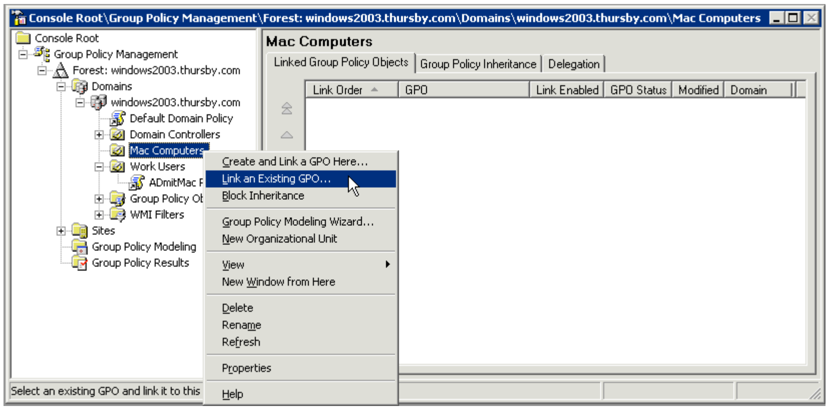
Type the password for the user at the prompt. Alternatively, in the Finder, delete the Policies folder located in `/Library/Caches/com.thursby.sysvol/`. Type in the local administrator password at the prompt. This second option is useful in the case where an OU has a large number of users. Performing either of these two options will ensure that the group policy settings will be replicated to the Macintosh immediately.

The steps listed above may be used to configure other ADmitMac policies for users in an OU.

Computer Configuration

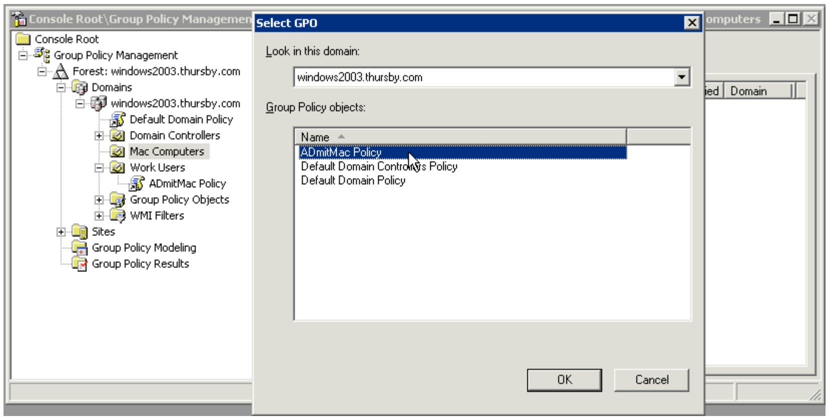
All of the settings for User Configuration are available for Computer Configuration. Additionally, there are a set of specific ADmitMac templates that only apply to computers. Since we have already created a GPO in the Work Users OU, we can link it to a computer OU.

1. In the following example, we have created a Mac Computers OU comprised of a group of Macintosh computers. Right-click on the appropriate computer OU and select "Link an Existing GPO..." (alternatevely, a new GPO can be created by selecting "Create and Link a GPO Here...")



Select an existing GPO and link it to this

2. Select the already created GPO (created in the last section) and click "OK".

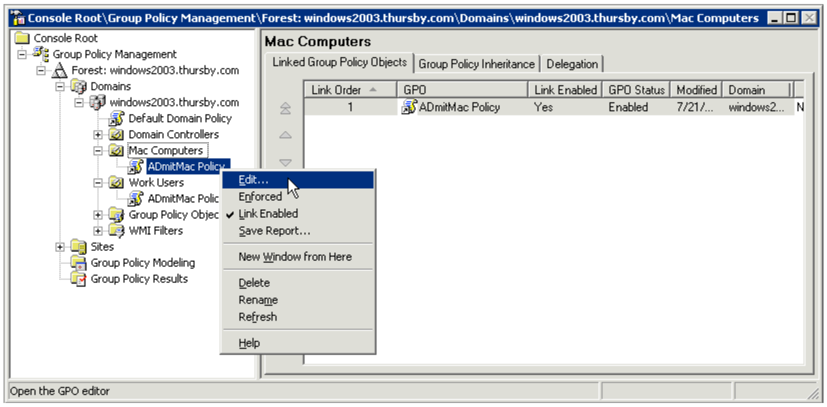


Look in this domain: windows2003.thursby.com

Group Policy objects:

Name
ADmitMac Policy
Default Domain Controllers Policy
Default Domain Policy

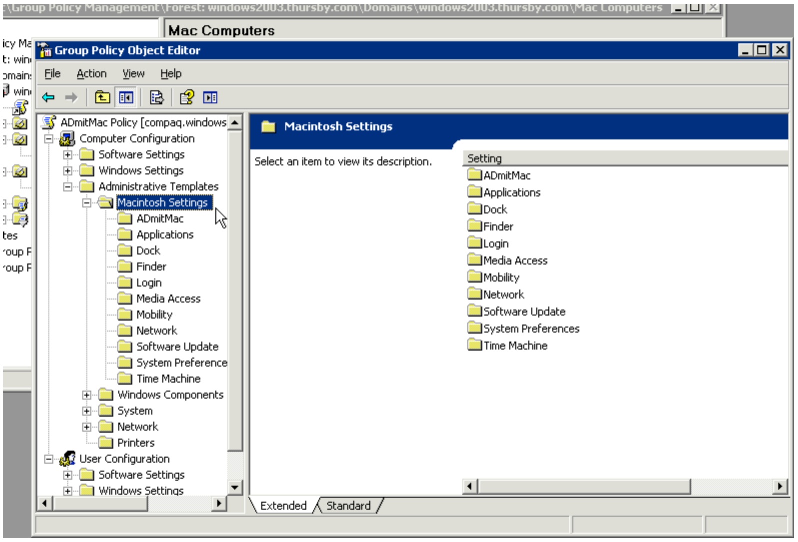
3. Right-click on the Group Policy Object under the appropriate OU tree (in this example, Mac Computers) and select "Edit..."



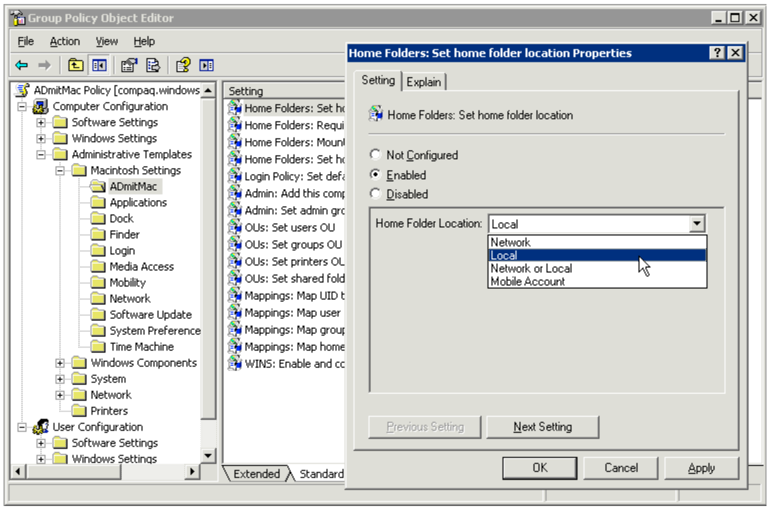
Link Order	GPO	Link Enabled	GPO Status	Modified	Domain
1	ADmitMac Policy	Yes	Enabled	7/21/...	windows2...

Open the GPO editor

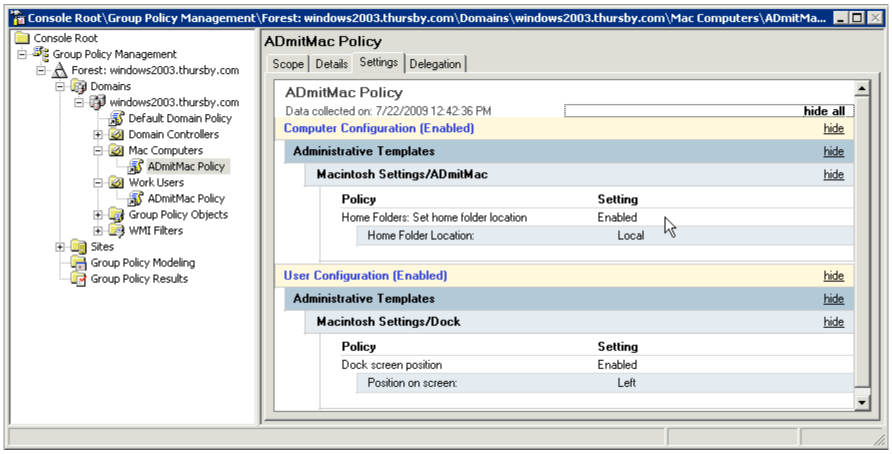
4. The GPO Editor window will open. Expand the Administrator Templates under the Computer Configuration tree. Then expand the Macintosh settings to reveal theADmitMac templates. In addition to the templates for User Configuration, there are two additional templates that only apply to computer groups: ADmitMac and Time Machine.



5. As an example, the ADmitMac template will be used to modify the computer OU's Home Folder location. Select the ADmitMac template, then double-click (or right-click and select "Properties") on the "Home Folders: Set home folder location". The properties of the setting will be displayed. Click the "Enable" radio button, then select "Local" from the pop-down menu. Click "Apply" or "OK". Close the GPO Editor.



6. Group Policy Management will now show the GPO with the Home Folder Policy set to Local for all computers in the Mac Computer OU.



ADmitMac Policy

Data collected on: 7/22/2009 12:42:36 PM

Computer Configuration (Enabled)

Administrative Templates

Macintosh Settings/ADmitMac

Policy	Setting
Home Folders: Set home folder location	Enabled
Home Folder Location:	Local

User Configuration (Enabled)

Administrative Templates

Macintosh Settings/Dock

Policy	Setting
Dock screen position	Enabled
Position on screen:	Left

7. The computer settings for all Macintosh computers in the OU will take effect 15 minutes after the last time the policy was updated from the domain controller. If you wish to have the settings take effect immediately, run the following command from Terminal (located in the /Applications/Utilities folder) logged in as a local administrator:

```
sudo /Library/FileSystems/DAVE/ReplicatePolicy --gp --force
```

Alternatively, in the Finder, delete the Policies folder located in `/Library/Caches/com.thursby.sysvol/`. Type in the local administrator password at the prompt. Performing either of these two options will ensure that the group policy settings will be replicated to the Macintosh immediately.

More on Application Access Management

You can use GPO settings from ADmitMac's ADM template to allow users to launch certain applications or applications in approved folders, while at the same time deny user access to other applications or applications located in unapproved folders. Although access for Apple specific applications is straightforward, care should be taken with regard to third-party applications, and especially third-party suites that have "helper applications" or other interdependencies (such as Microsoft Office for Mac and Adobe InDesign), to prevent erratic behavior.

To allow or prevent the launching of an application, three templates can be utilized.

"Always allow these applications" lists applications which should be allowed.

"Disallow applications within these folders" lists applications and folders which contain applications that are disallowed. This takes precedence over all subfolders.

"Allow applications within these folders" lists applications within the specified folder which are allowed.

If an application or its folder is not in either of these lists, they cannot be executed. This implies that any helper application(s) that some applications may depend on that are installed in other areas of the directory will not run unless explicitly listed. For example, listing /Applications/Microsoft Office 2011 will allow all programs in the Office Suite to run except Microsoft's AutoUpdate application, located in /Library/Application Support/Microsoft directory. Another example is Adobe Bridge, in which it is necessary to use the "Allow Applications within these folders" ADM template, specifying /Application/Adobe Bridge CS5 directory instead of the Adobe Bridge CS5.app itself.

If there is sporadic behavior involving an allowed application, check the dependencies of its helper applications or check if there are additional directories in /Library/Application Support/.

Troubleshooting

Common Problems

- Active directory domain names need to be fully qualified. For example, use "engineering.education.com" instead of "engineering").
- Verify that a DNS server with a valid address is specified in the Network preference pane (Apple > System Preferences).
- For best results, the Macintosh should be using the same DNS servers as the Active Directory servers. To verify your DNS server settings, open the Network preference pane (Apple > System Preferences).
- You cannot join a domain in the *Directory Utility* ADmitMac plug-in unless you have privileges to join a domain.
- If you cannot mount the network home directory and have selected "Use Network Home Folder" in *Directory Utility* under ADmitMac, then verify (on the PC server) that a valid, fully qualified (for example: \\server\share\home_directory) home directory path is entered in the user's Home Directory > Profile field.
- If there is too great a time difference (more than 5 minutes) between the domain controller and the client Macintosh computer, Kerberos cannot pre-authenticate and an error will be given. Try using a network time server: open Apple > System Preferences > Date and Time preference panel. In the Network Time tab, check the Set Date & Time Automatically button.
- Make sure the user's home directory is accessible. If ADmitMac can't get to a user's home directory, the user cannot log in. The default home folder setting is to use a network home directory. To change this setting to local (or use either), see Configure ADmitMac.

Tips for Verifying a Domain

Verify a Macintosh is configured for a domain:

1. Open the **System > Library > CoreServices** folder and double-click *Directory Utility*.
2. In the Services tab, double-click ***ADmitMac*** in the list to open the ADmitMac plug-in (you will need to enter administrator credentials).
3. Select a domain in the list and click *Verify* to make sure the domain is available.

Verify User Account information:

1. Enter the following in the terminal window and click *enter*:

```
id username
```

The user name information will display if:

- The account is configured correctly on the domain server.
- ADmitMac services are configured correctly in the *Directory Utility* > **Search Policy** tab.

2. If the user name fails, verify ADmitMac authentication is configured:

   a. In the **System > Library > CoreServices** folder, double-click *Directory Utility*.

   b. In the Authentication tab, verify that your Windows domain is listed. (a Custom path directory node should be listed, for example: `/ADmitMac/THURSBY.COM`).

   c. If ADmitMac is not listed, click *Add...* and select an Active Directory or NT domain from the list.

Edit or Recreate Kerberos Preference File

To edit the `edu.mit.kerberos` file in the Terminal, complete the following:

1. Launch the terminal application (**Applications** > **Utilities** > **Terminal**).
2. In the terminal window, enter the following command exactly:

```
sudo vi /Library/Preferences/edu.mit.kerberos
```

The text of the edu.mit.kerberos file should display. If not, you should recreate the file (see procedure below).

Recreate the edu.mit.kerberos and /etc/krb5.keytab files:

NOTE: These steps will remove your Kerberos settings completely.

1. Log into the Macintosh with a local administrator account.
2. Launch the Terminal Application and type:

```
sudo rm /Library/Preferences/edu.mit.kerberos
```

3. Enter the administrator password if necessary.
4. Type:

```
sudo rm /etc/krb5.keytab
```

5. Launch Directory Access or Directory Utility**,** double-click on *ADmitMac* and join your domains again. See that new `edu.mit.kerberos` and `/etc/krb5.keytab` files are created.

Unable to Join Domain

An error is reported when ADmitMac cannot communicate with a remote computer's resources. Here are some specific causes for this error message:

- If you see this error when trying to join a computer to the network in the ADmitMac Configuration Directory Access or Directory Utility plug-in, you must use a user account with join privileges to join the computer to the domain.
- This can also happen when you have a pre-existing computer account left over from a previous domain join or one that has the same name as the computer you're attempting to join. Either change the name of the computer or find the computer account in the Computers container on the domain and delete it.
- This error can occur if you are attempting to join to the Active Directory domain controller, but there is a problem with the DNS records on your DNS server for the domain controller (i.e. the name of the domain controller does not match the DNS record). This can also happen if you are using WINS and the WINS server is in a different subnet from the domain controller you are trying to join.
- The remote computer is down.
- The remote computer's name has changed.
- The remote computer name is mis-typed.
- The remote computer is no longer reachable using TCP/IP.

Resolution:

Try one or more of the following:

- Verify reverse DNS exists and is configured correctly for the "joining" domain controller.

  To make sure DNS is working properly:

  1. Launch Network Utility (**Applications > Utilities**).
  2. Click the *Lookup* tab at the top of the pane.
  3. Type in the Domain Controller name or IP address and select *Name Server* in the Drop Down menu.
  4. Press *enter* or click *Lookup*.

     If you don't see a domain controller in the results box, then your domain controller is probably using a different DNS server than your Macintosh.
- Verify that you have sufficient privileges to join a computer to the domain.
- Verify there isn't a computer account name conflict.
- Verify the remote computer name you entered is correct and is reachable using TCP/IP.

Joined Domain but Cannot Log In

- Check that you've added a custom authentication path in Directory Utility. Without it, OS X won't use your Active Directory connection for account authentication. If you get the window shake immediately without pause check this first. See Configure ADmitMac.
- Make sure the user's home directory is accessible. If ADmitMac can't get to a user's home directory, the user cannot log in. The default home folder setting is to use a network home directory. To change this setting to local see Configure ADmitMac.
- Use the short name (login name) for your user name when logging in.
- Verify ADmitMac uses a local home directory or if a network home directory is specified, make sure the path has been configured into the user account (**Properties > Profile** tab).
- Verify the username and password are correct by logging into a PC on the same domain. You may also try resetting the password.

Cannot join .local domains

This error occurs because Apple's DNS resolver always attempts to look up names ending with .LOCAL using multicasting if the name can't be found using DNS servers.

Resolution:

Add two SRV records to the DNS server of the form:

```
_kerberos-master._udp.XXXXX.LOCAL
_kerberos-master._tcp.XXXXX.LOCAL
```

where `XXXXX` is the name of the domain.

Cannot Find or Mount Home Directory

Unable to find the home directory

If you cannot find the home directory in `/Domain/domainname/Users`, first try rebooting and logging in again. If you still cannot find the home directory folder, verify that the authenticating server is available and if that is not the issue then try recreating the Domain directory. To recreate `/Domain`, move it out of the way by renaming it, then log out and log in as with domain credentials.

Cannot mount home directory from the server.

When you configure the user's *Profile* tab, select *Connect in the Home Folder* section.

> **NOTE:** entering a drive letter is an option if the user will also log into the network from a PC. Enter a path to the home directory CIFS share, (for example: `\\server\share\home_directory`). ADmitMac will create a folder in the `/Domain/domainname/Users` folder. Also, verify you can mount a share in the *Connect to Server* window.

DNS could not resolve primary or secondary WINS.

Primary and Secondary WINS addresses should be entered in IP dotted-decimal (e.g. "192.168.3.38") form or IP DNS (Domain Name System) form. If the address is not dotted-decimal, ADmitMac attempts to find the address in DNS form (e.g. "wins.thursby.com"). It does this by requesting the information from DNS using the TCP/IP settings. If the request fails this error is reported.

Resolution:

Verify that you are entering the correct WINS information. Also verify that the correct DNS information is entered in the of the **System Preferences > Network > TCP/IP panel**.

The Volume "NAME" mounted from server "SERVER NAME" has been lost.

This error occurs when ADmitMac cannot access the remote volume. ADmitMac will attempt to unmount the inaccessible volume, but if there are any open files, then the user will have to unmount the volume.

Resolution:

Try to re-mount the volume. If this still fails, verify that the remote server is still available and the share still exists.

Unknown Domain. The domain "NAME" could not be found to verify your name and password. Please specify a different domain.

ADmitMac could not find a Primary Domain Controller (PDC) or a Backup Domain Controller (BDC) in the domain entered.

Resolution:

In Directory Utility, double click *ADmitMac* and verify that the domain name you entered is correct.

More Information — Frequently Asked Questions

Visit our FAQ online at http://www.thursby.com/support/faq.lasso

For more information, please refer to our websites:

www.thursby.com

www.admitmac.com

THURSBY Software