Windows 2003 Administrators Guide to Files Shares for Mac Clients

Deciding on the Network Protocol

Here are the choices most Administrators are faced with:

	AFP over TCP	CIFS/SMB	AppleTalk
Characters in Filename	31*	255	31*
Supports Illegal Windows characters	Yes**	No	Yes**
Password Encrypted	Yes***	Yes	No
Logon Banners Supported	Yes	No	Yes

* Remember, Window 2003 adds an extension to certain files, so the filename may only appear to be 27 characters

** All are valid characters (/\?<>*|") except for a colon **:**

*** This is dependent on the client and authentication you use.

WARNING

Before doing anything to your server, always follow best practices!!
Perform testing in a test environment.
Backup all data before performing any of these operations in a production environment.
If you have question about best practices, contact U.T.O.

AFP over TCP—*requires installation of "Services for Macintosh"*

Definition:
AFP over TCP—AppleTalk Filing Protocol over Transmission Control Protocol

Use:
MacOS X users will click **Go\Connect to Server…** and type in the server address and sharename.
Example: *servername*/*sharename*
Optionally: they can type in afp://*servername*/*sharename*
Note: MacOS assumes you are using afp by default

	MacOS 10.3 and Below	Microsoft UAM Module Add-on	MacOS 10.4
Supports # of characters in Passwords	8	14	???*
Encryption	sent in clear text	encrypted	encrypted
Ports used on Windows Server	TCP / 548	dynamic**	TCP / 548

* Apple has not published their specifications for 10.4.

** These appear to be using ports in the 49000 range, but I haven't verified this on multiple servers.

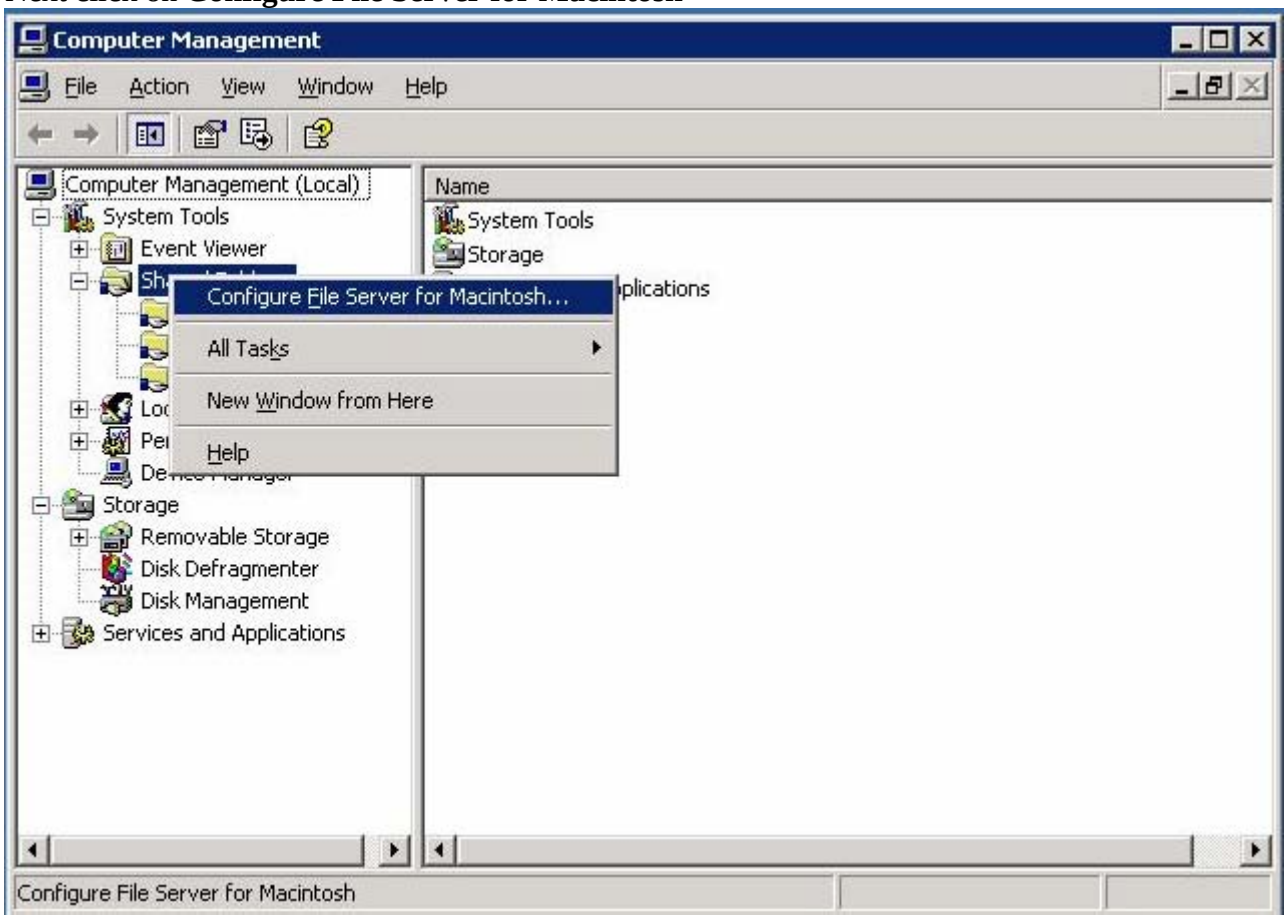
MacOS 10.**3** and below has a huge security hole in how it authenticates users to Windows Servers. Microsoft came out with the "Services for Macintosh" networking component and an installable security module for the Mac Operating systems for interoperability and security. I recommend supplementing the encryption with CheckPoints VPN software and the Microsoft UAM module. MacOS 10.4 has the encryption module built-in and the Microsoft UAM module is optional on this OS.

Installing AFP over TCP on Windows 2003 server

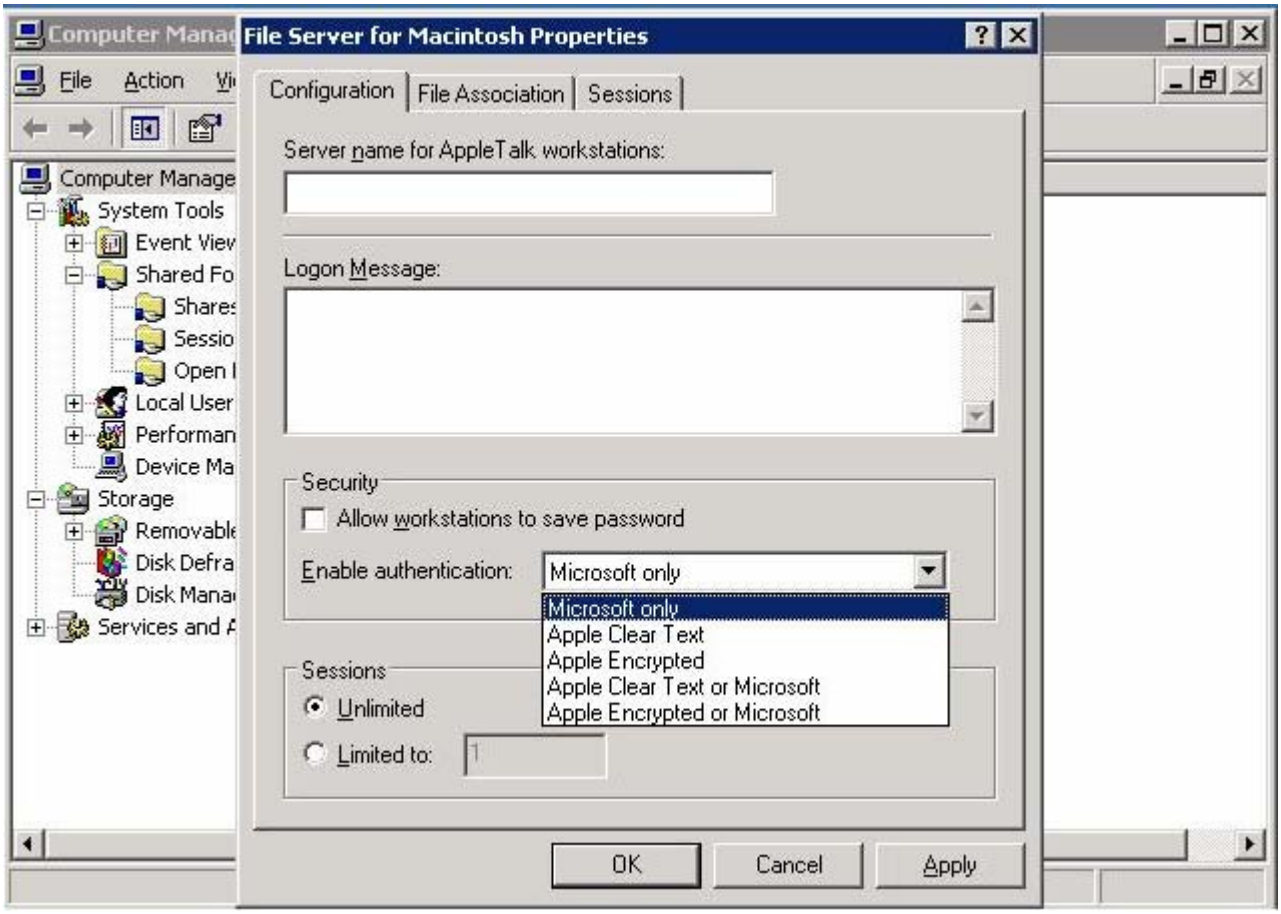
Open **Add Remove or Programs**
(or type "**appwiz.cpl**" without the quotes in **Start\Run**).
Click on **Add/Remove Windows Components**
In the **Windows Components Wizard**, highlight **Other Network File and Print Services**
Click on **Details…**
Put a checkmark next to **File Services for Macintosh**
Click **OK**
Click **Next**
Click **Finish**

Configuration of File Services for Macintosh:

In the **Control Panel \ Administrative Tools** click on **Computer Management**
(or type "**compmgmt.msc**" without the quotes in **Start\Run**).
Expand **System Tools** and right click on **Shared Folders**
Next click on **Configure File Server for Macintosh**



In the **Configuration** index tab, you need to click on the drop down menu under **Enable authentication:**



Microsoft: offers an additional level of security because the password is used as a key to encrypt a random number.

Note: This requires the client to download and install the MS UAM Client.
This can be at two places: The UAM share that was automatically created on your server's C drive or at http://www.microsoft.com/mac/otherproducts/otherproducts.aspx?pid=windows2000sfm.

Apple Encrypted: specifies that passwords will be sent in an encrypted format compatible with the version 8.3 of the AppleShare software (requires version 8.3 or higher of the AppleShare client).

Note: User passwords are saved in clear text format!! You must also open up port 548 TCP on your firewall.

Apple Clear Text: sends the user password over the network in clear text.

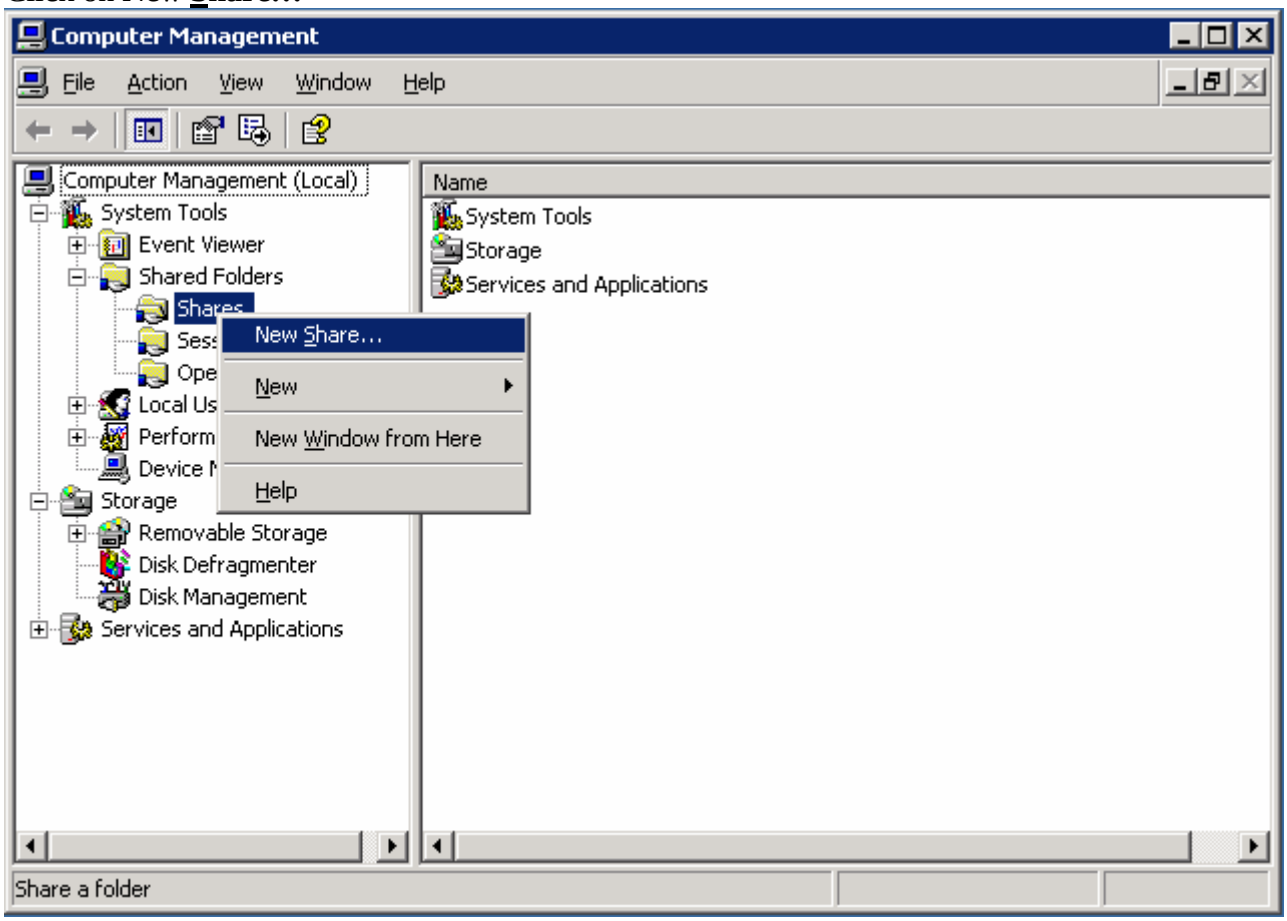
Note: User passwords are sent in clear text across the network when they authenticate to your server. (I don't recommend using this for file sharing!)

Note: if the Apple client is in Active Directory, SSO (Single Sign On) will not occur on any of these selections.

Creating the Apple/Window Shares

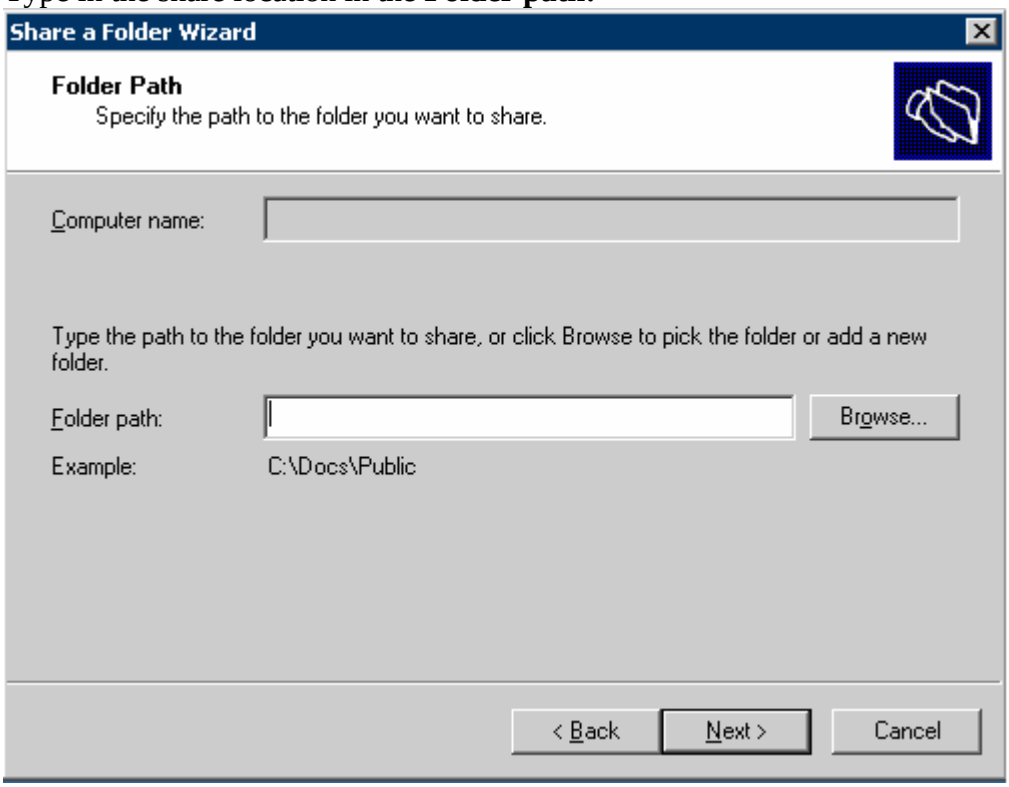
In the **Control Panel \ Administrative Tools** click on **Computer Management**
(or type "**compmgmt.msc**" without the quotes in **Start\Run**).
Expand **System Tools**
Expand **Shared Folders**
Right click on **Shares**

Click on **New Share…**



Click **Next**

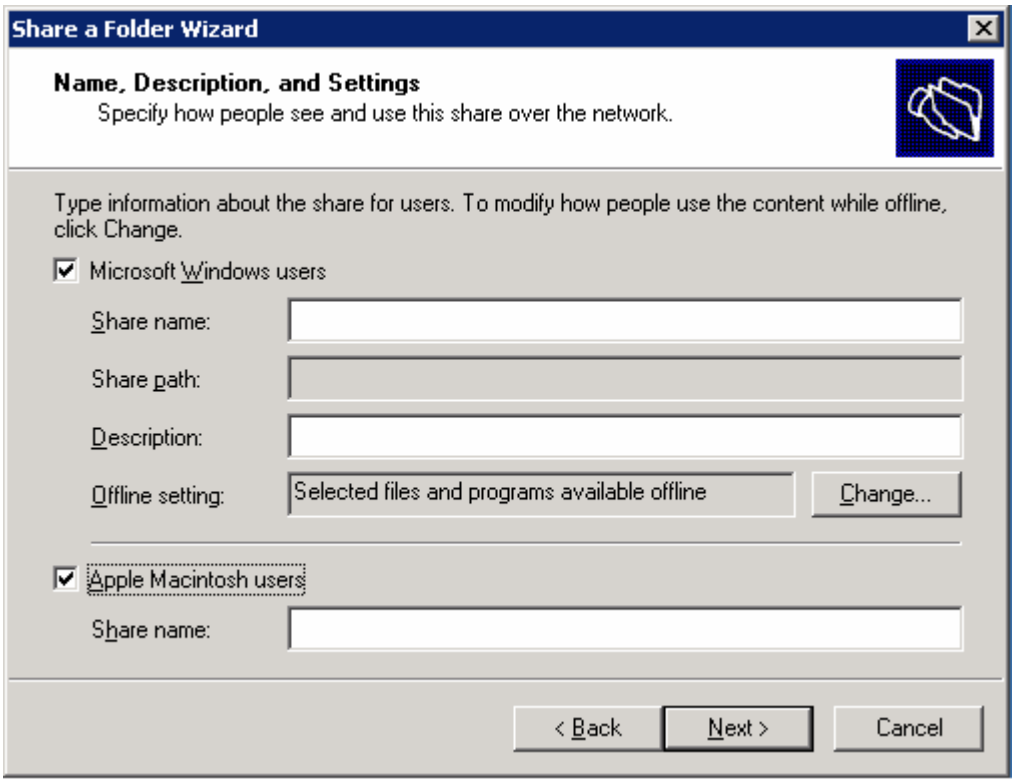
Type in the share location in the **Folder path:**



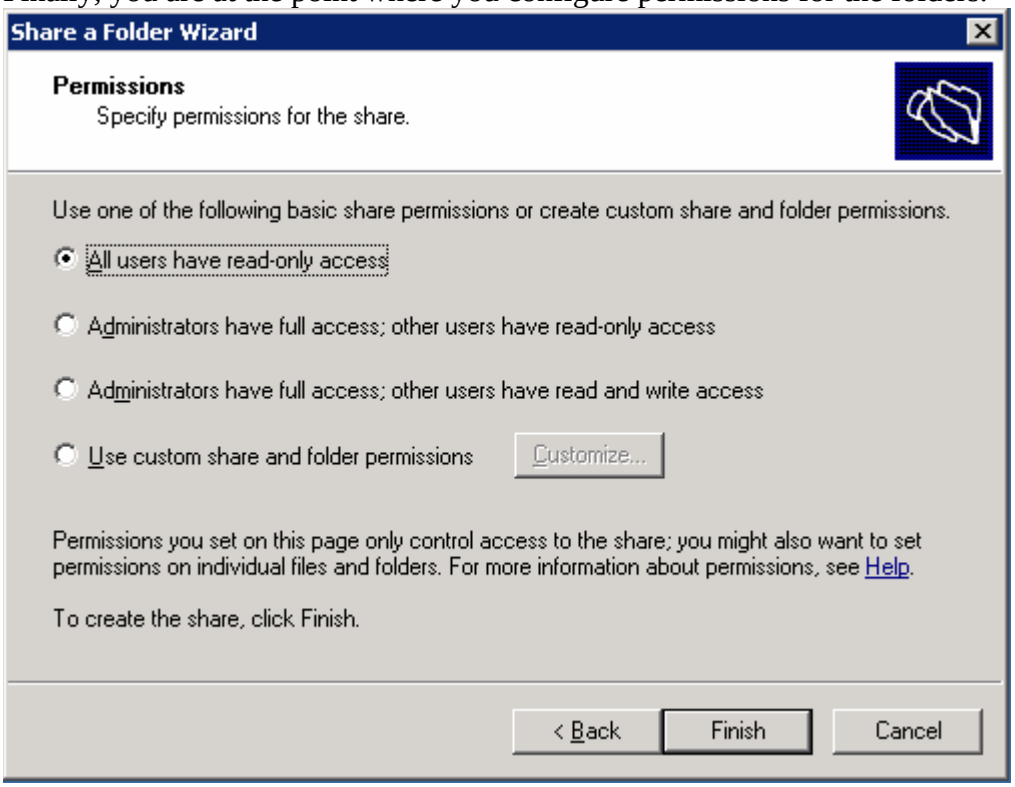
In the **Share a Folder Wizard**, put a check by **Apple Macintosh users**

Next type in the share names, paths, descriptions of your shares on your server.

Click **Next**



Finally, you are at the point where you configure permissions for the folders.



SMB/CIFS Connection

Definition:
SMB: Server Message Block
CIFS: Common Internet File System

Use:
MacOS X users will click **Go\Connect to Server…** and type in either **smb://** or **cifs://** followed by the server address and sharename.
Example: **smb://***servername/sharename*
cifs://*servername/sharename*

This is a standard connection that does not require installation of additional software, but there are some caveats. Samba based clients such as Linux and MacOS do not recognize a security feature in Windows 2003 called Digital Signing. As of Windows 2003 Service Pack 1, Digital Signing is set as a requirement for all SMB communication.

Windows 2003 digital signing is used to prevent SMB session hijacking. This prevents a hacker from using a session interjection on an already established connection. As with most security features, you sacrifice performance for security. A 10% to 15% performance hit will take place if this is enabled.

SMB Signing See Windows Networking
http://www.windowsnetworking.com/nt/registry/rtips206.shtml

Many files beginning with "._" (called the “Apple Double” format) are created by Mac OS X when connecting to the Windows server via SMB or CIFS (essentially Windows file sharing). The "._" is the "resource fork" of the Apple file, but SMB/CIFS doesn't know how to handle resource forks. Therefore Mac OS X compensates by splitting the Mac file in two and placing it this way on the server. If you were to copy the file back to the Mac, Mac OS X would knit the two files back together.

References

Apple Double Format: See Apple Knowledgebase article 106510
http://docs.info.apple.com/article.html?artnum=106510

SMB Digital Signing: See Microsoft Knowledgebase article 887429
http://support.microsoft.com/?kbid=887429

CIFS Protocol: See Microsoft MSDN
http://msdn.microsoft.com/library/en-us/cifs/protocol/cifs.asp

AppleTalk

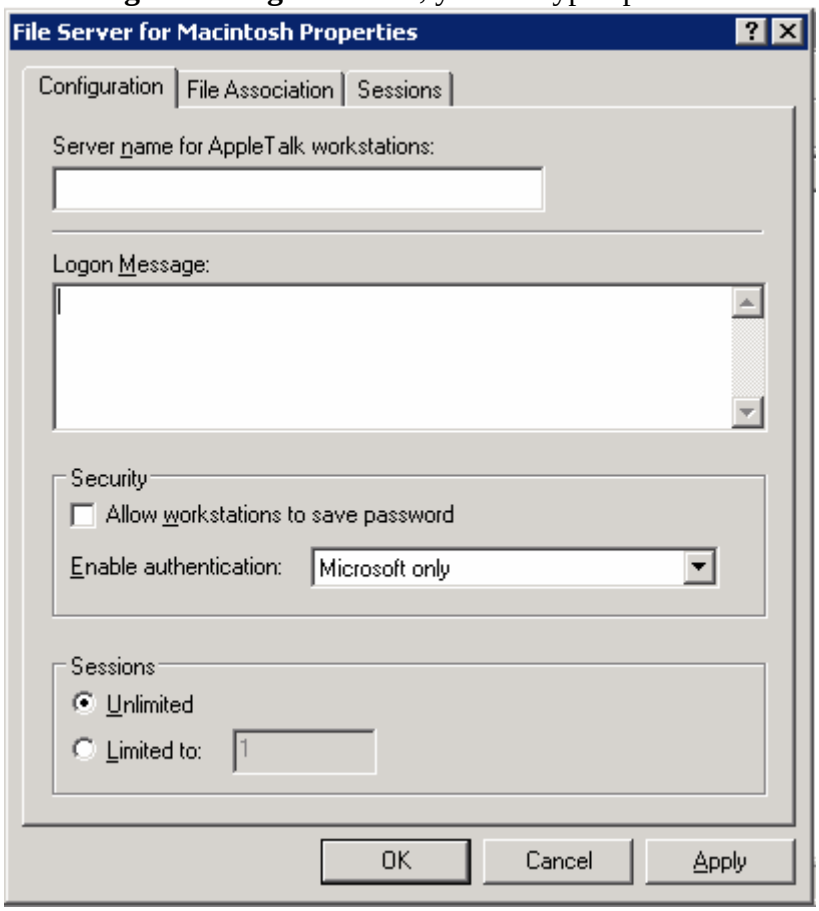
AppleTalk is being shutdown at ASU per U.T.O.’s edict! Therefore, I won’t go into any details.

FAQ Section

Can I put a logon banner on my Apple Shares?

Of course!

In **Computer Management**, click **System Tools**
Right click on **Shared Folders**, then click on **Configure File Server for Macintosh…**
In the **Logon Message:** window, you can type up to 199 characters.



How can I tell if the client is using the Microsoft UAM module?

There are two ways to check.

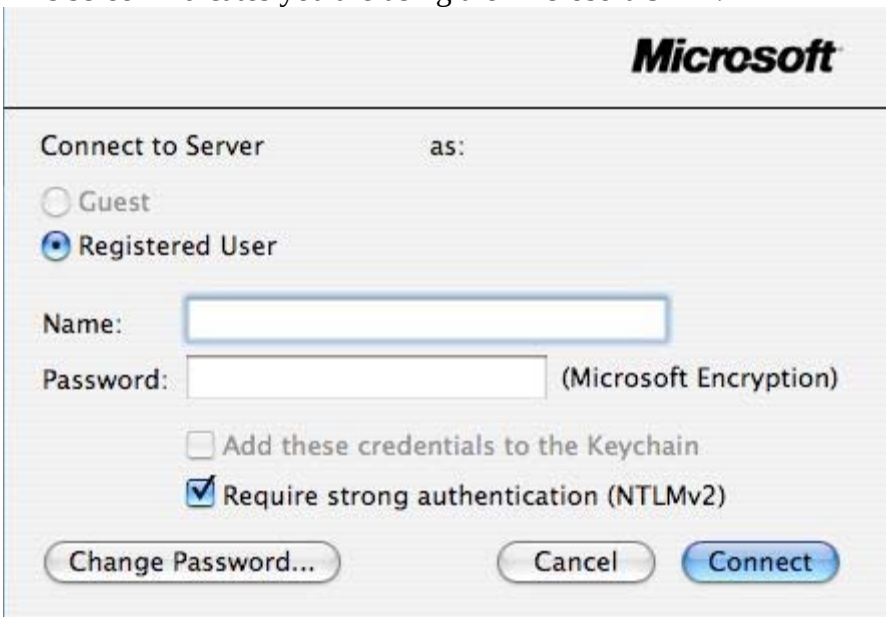
Option 1:
On the Mac client, Click on (Desktop hard drive Icon)\Applications\Utilities\Terminal
Type the following: **cd /Library/Filesystems/AFP over TCP/Authentication** <*enter*>
Type the following: **ls** <*enter*>
If you see a file call MS UAM, the module is installed.

Option 2:

When attempting to connect to the network share from the client, you will see one of two screens:

This screen indicates, you are using the default authentication module by Apple. This is NOT the Microsoft UAM!

This screen indicates you are using the Microsoft UAM.



Preventing .DS_Store files from being written to the servers

This can be extremely annoying, especially when Apple clients browse to the Windows shares.
On the MacOS X client, start the **Terminal** application located in /Application/Utilities
Type the following:
sudo defaults write com.apple.desktopservices DSDontWriteNetworkStores true

Note: The DS_Store tells the Apple Explorer how to present the files to the users (Thumbnails, positions, list, details, etc, etc)

.DS_Stores: See Apple Article 301711
http://docs.info.apple.com/article.html?artnum=301711

Security Warning: A hacker can discern what files are in the directory structure by viewing the .DS_Store files. This would be applicable on an FTP site, Web Server, etc, etc.

Any recommendations on Windows/Apple Server Migration Utilities?

Check out the RsyncX utility

See: http://archive.macosxlabs.org/rsyncx/intro.html
http://xnews.soad.umich.edu/RsyncX_v1.7/docs/rsyncx_v1.7/intro.html

Should the clients use either SMB or CIFS when connecting to the Windows Shares?

The SMB file sharing protocol was developed first through the aid of Microsoft and IBM. Later on, Microsoft developed a newer standard with their extensions and sent it to the IETF committee. The CIFS standard has better file synchronization and locking. However the CIFS draft has expired. If someone has a good answer to this question, then let me know!!!

Troubleshooting Section

Clients can't connect to Windows 2003 Server using AFP over TCP.
Problem:
MacOS 10.4.5 clients have problems connecting to AFP shares via AFP over TCP/IP.

Solution 1:
Update the client to MacOS 10.4.6 which includes the following fixes:
-login and authentication in a variety of network environments
-file access and byte range locking with AFP file sharing
Note: The 10.4.6 update may break some AppleTalk connections with 10.3.9 Apple Servers (ex, File locks)
As of this writing, Apple has not acknowledged this problem.

Solution 2:
Add the Microsoft UAM module to the client computer.

Problem:
All Apples clients have problems connecting to my server.

Solution 1:
Check your firewall settings and verify you have opened port 548 TCP on your firewall and open the port if needed.

Solution 2:
Verify you have setup the appropriate permissions on the Apple share. Remember, the permissions are not the same as the SMB/CIFS/Windows share.

Clients can't connect to my Windows cluster via AFP over TCP:

Problem:
Microsoft has confirmed this to be a problem in Knowledgebase article 243839
See http://support.microsoft.com/kb/243839/en-us

Bad Solution:
As a work-a-round have them explicitly connect to an individual server, not the cluster name.

Better solution:
Have the clients connect via SMB to their shares. Still can't see the cluster? Then try connecting to an individual server.

Apple Clients are getting the following Error message:
An error has occurred (error = -5000)

or

An error has occurred (error = -5023) (if password is left blank)

Problem:
This error occurs when SMB signing is enabled on a Windows server.

Solution 1:

Disable SMB Digital Signing

Type "**secpol.msc**" without the quotes in **Start\Run**
In the Local Security Settings Navigate to the following directory:
Security Settings\Local Policy\Security Options
Highlight **Microsoft network client: Digitally sign communications (always): Enabled**
Double click on this and select the **Disabled** Radio button

or

Edit the Windows 2003 registry
HKEY_LOCAL_MACHINE/SystemCurrent/ControlSetServices/LanManServerParameters/RequireSecuritySignature
Change the key from 1 to 0

Note: You are disabling a security feature.

SMB Digital Signing: See Microsoft Knowledgebase article 887429
http://support.microsoft.com/?kbid=887429

Note: If you need SMB signing for other services, then check out this article
See Microsoft KB http://support.microsoft.com/kb/839499/en-us

Solution 2:

Use a 3rd Party Application

Example: Sharity supports SMB signing

Note: This application is free for student personal use. See http://www.obdev.at/products/sharity/buy.html

Apple Clients are getting the following Error message:

Connection to the server broken unexpectedly

or

The server unexpectedly terminated the session

Problem: If you are running Symantec Antivirus on your server

Solution:
Microsoft has a workaround listed in Knowledgebase 883409
See http://support.microsoft.com/kb/883409/en-us

My desktop support team can't install the Microsoft UAM module on the Mac's.

Solution 1:
Hire more qualified desktop support people!

Solution 2:
When you installed Services for Macintosh, it created a UAM share of the root of your Windows 2003 server's C drive. Copy the **C:\Microsoft UAM Volume\MS UAM for AFP over TCP 3.6\AFP over TCP Folder\MS**

UAM file to the Macintosh. Place the "MS UAM" file in the following directory **/Library/Filesystems/AFP over TCP/Authentication**

> Note: The **C:\Microsoft UAM Volume\MS UAM for AFP over TCP 3.8** directory is used for MacOS 9 clients. Alternately, you can copy this module from another MacOS X computer that already has it installed. Remember to run the Disk Utility/Repair Permissions afterwards. *I personally do not like any shares on the C: drive of my server and would recommend removing the UAM share or moving it to another location.*

I can't delete files on my Windows Server that Apple clients created/updated!

Problem:
Windows will act as if the file is in use or missing even after the client has disconnected. This appears to be an issue with the implementation of oplocks (Opportunistic locking) and/or the state information in paged pool memory. Windows oplocks in the cache become corrupted and some admins have stated that after a reboot, they are able to delete the files. Services for Macintosh maintains state information in memory. Neither Apple nor Microsoft has acknowledged this bug.

Opportunistic Locking: See Microsoft Article ID: 129202
http://support.microsoft.com/?id=129202

Services for Macintosh State Memory: See Microsoft Article ID: 243839
http://support.microsoft.com/kb/243839/en-us

Solution:
Connect via an Apple client and delete the files.

I didn't do any extensive testing and performed these operations on my server in production. Now my users can't access anything!

Solution:
I hear they're hiring at McDonalds.

Instructions by Jason Wulf
(Don't ask me questions, I just wrote up what I found out)
"I know nothing!!" – (Schultz-- Hogans Heroes)