Instructions for Adding a MacOS 10.4.x Client to ASURITE

Before beginning, it would be prudent not to have an account with the same username as your Active Directory account. If an account with the same name exists, the local account will not be able to login due to mismatched permissions.

For DHCP Workstations:
You **must** hard code a "DHCP Client ID:" in System Preferences\Network. (Ex, Make up a highly unique name..Room #, Prop Control Number, etc). *Make sure you have propagated DNS Servers and Search Domains Fields.*

For Static Workstations:
Verify that all of your pertinent network information is filled out in System Preferences\Network. (Ex. DNS,Subnet, Search Domains, etc)

Open up the Macintosh HD on the desktop
Click on **Applications**
Then **Utilities**
And finally **Directory Access**
Next click on the picture of the Padlock and type in your Admin login and password for the local machine. (If applicable)

Put a checkmark next to SMB/CIFS to enable the service
Highlight SMB/CIFS then click on "**Configure…**"
Change Workgroup to "**ASURITE**" without the quotes.
Next to WINS server type in "**129.219.17.11**" without the quotes

Note: The MacOS 10.4 GUI client will not accept more than one WINS entry. However, if you really want a secondary or tertiary WINS Server then edit the /etc/smb.conf and change the entry from "wins server = 129.219.17.11" to "wins server = 129.219.17.11 129.219.13.105 129.219.17.194" without the quotes. The GUI interface on the server version does not have this problem.

Click OK
Type in your local administrator Login and Password if necessary.

Note: These configurations are added to /etc/smb.conf file
See http://developer.apple.com/documentation/Darwin/Reference/ManPages/man5/smb.conf.5.html

Put a checkmark next to **Active Directory** to enable the service
Highlight Active Directory then click on "**Configure…**"
Click on the down arrow next to "**Show Advanced Options**"

For the following options:

Active Directory Forest: *leave blank*
Active Directory Domain: **asurite.ad.asu.edu**
Computer ID: *enter the name of your computer*

Note: The ComputerID will be the name of this computer in Active Directory. Anything past 16 characters will be truncated.

Unchecked Create mobile account at login

Unchecked Require confirmation before creating a mobile account

Note: The mobile account option caches the user's identification data and authentication credentials allowing the user to login when disconnected from the Active Directory.

Checked Force local home directory on startup disk

Note: If this is a lab environment, you may not want to force home directories.

Checked Use the UNC path from Active Directory to derive network home location

Network protocol to be used: **smb:**

Note ***smb:*** *is using samba which is compatible with Windows network mappings*

afp: *is used for connecting to Apple shares*

Checked Default user shell: **/bin/bash**

Under Mappings

Unchecked Map UID to attribute: *leave blank*

Unchecked Map user GID to attribute: *leave blank*

Unchecked Map group GID to attribute: *leave blank*

Under Administrative

Checked Prefer this domain server: **asurite.ad.asu.edu**

Checked Allow administration by: **domain admins**

enterprise admins

Note: you should type in your ASURITE admin groups or user id's here for administration. It is also recommended that you remove "domain admins".

Unchecked Allow authentication from any domain in the forest

Click on **Bind**.

Enter your local login and password if prompted

In the Network Administrator Required window

Type in your ASURITE Username and Password

Note: you must be an OU admin to do this.

Computer OU: **OU=***Your OU name***,DC=asurite,DC=ad,DC=asu,DC=edu**

Note: If you want to put this in your sub OU, then do something like this

*OU=m.MyOU.MySubOU,OU=m.MyOU,****DC=asurite,DC=ad,DC=asu,DC=edu***

Checked Use for authentication

Unchecked Use for Contacts

Note: Data from these configurations are written in: /Library/Preferences/DirectoryService/ActiveDirectory.plist If something appears to be corrupted, you can delete this file and reconfigure Active Directory.

Save the file, exit, reboot, and you should now have an SSO (Single Sign On) and be able to map to the servers without a FQDN.

Note: A list of kdc's and admin servers will automatically be generated in:
/Library/Preferences/edu.mit.Kerberos
Note: You may notice a significant jump in network activity and may have problems logging in immediately after this configuration.
This is because the Apple is reading the entire Active Directory forest and contact information.

Configuring Active Directory through the terminal/ Darwin:

The following commands activate the Active Directory Service in the GUI:
defaults write /Library/Preferences/DirectoryService/DirectoryService "Active Directory" "Active"
plutil -convert xml1 /Library/Preferences/DirectoryService/DirectoryService.plist
sudo killall DirectoryService
sudo killall lookupd

This command binds the computer to Active Directory:
dsconfigad –a *currentcomputername* **–u** *ouadminusername* **–p** *ouadminuserpassword* **-ou "OU=***m.MyOU***,DC=asurite,DC=ad,DC=asu,DC=edu" –domain asurite.ad.asu.edu -status -lu** *localusername* **-lp** *localuser_password*

You should see the following output:
Step 1 of 5: Searching for Forest/Domain information
Step 2 of 5: Finding nearest Domain controllers
Step 3 of 5: Verifying credentials
Step 4 of 5: Searching for existing computer
Step 5 of 5: Binding computer to Domain
Computer was successfully Added to Active Directory.

This command configures the admins and preferences:
dsconfigad –localhome enable –preferred asurite.ad.asu.edu –groups "ASURITE\enterprise admins,ASURITE*myadmingroup***" –alldomains disable -lu** *localusername* **-lp** *localuser_password* **–status**

You should see the following output:
Settings changed successfully

This command sets up the authentication to Active Directory:
sudo dscl /Search -create / SearchPolicy CSPSearchPath
sudo dscl /Search -append / CSPSearchPath "/Active Directory/asurite.ad.asu.edu"
Note: If you're having trouble with the previous command, verify the Active Directory service is started (aka checkmarked) in Directory Access.

Shows the current Active Directory configuration
dsconfigad –show

See http://developer.apple.com/documentation/Darwin/Reference/ManPages/man8/dsconfigad.8.html for details

Setup WINS:
sudo pico /etc/smb.conf

Note: UNIX pro's can use VI and grep. They can also create a script to do everything.

Scroll down to where it says "**workgroup = Workgroup**"
Change "workgroup = Workgroup" to "workgroup = **ASURITE**" without the quotes
Press enter
Type in the following without the quotes "wins server = 129.219.17.11"

Note: you can optionally type in"wins server = 129.219.17.11 129.219.13.105 129.219.17.194", however the GUI interface will display the WINS server as blank. (An Apple bug?)

Hold down the **control** key then depress the **X** key.
Depress the **Y** key.
Depress the **Enter** key

Other notes of interest:

Go to the terminal and into the /Network directory
You'll find the whole forest there.

As of 10.4.2 Tiger has been patched so you can edit the tty files and create login hooks
See http://docs.info.apple.com/article.html?artnum=301722 for patch information
See http://docs.info.apple.com/article.html?artnum=301446 for setting up hooks

If you want to set this up in a script, then check out http://www.bombich.com/mactips/scripts.html
(I of course found the link after I wrote all this up (bangs head against desk))

FAQS for MacOS 10.4.x

When I try to sudo in terminal, it doesn't work. Why?

You are most likely logged into an account not associated with root. Log in as the primary administrator account or alternately you can modify /etc/sudoers to associate your account with root. I suggest you do a **man sudoers** in terminal before editing that file.

I want to use SWAT (Samba Web Administration Tool) to administer users, groups, and shares on the Apple.

There seems to be a problem with SWAT recognizing the proprietary Apple encryption scheme. You can enable SWAT, however this will disable the root password and give everyone the capability to administer your Apple. If you're feeling foolhardy or want to experiment, then this is how you would enable SWAT.
First you should know that the man page totally wrong!!
Swat is already compiled on your workstation at /usr/sbin/swat. It does not need to be installed and compiled at /usr/local/samba/bin/swat like the man file says.

In Terminal go to /System/Library/LaunchDaemons/ and edit the swat.plist
Change the line under /usr/sbin/swat from -d 10 to –a
Note: The "-d 10" is the highest mode of debugging and "-a" puts SWAT info demo mode.
Save the file.
Next go to the /etc/ and edit the hostconfig
Change SMBSERVER=-NO- to SMBSERVER=-YES-
Save the file.
Next go to the /etc/ and edit the services
Find the line where port 901 is defined
Delete the line where it says 901/udp
Change the 901/tcp line to "swat 901/tcp" without the quotes.
Add spacing to make it look appropriate
Save the file.
In Terminal type "/sbin/service swat start" without the quotes
Reboot your Apple
Now you can Access SWAT through http://127.0.0.1:901 or through http://localhost:901
(If you know a fix, then please let me know!!)

I've heard that you can put some 3rd party SAMBA software on the Apple to get SWAT to work.

There is a 3rd party software package called Xamba at http://xamba.sourceforge.net. However, this has not been developed since MacOS 10.2.x and is incompatible with the higher versions of MacOS.

What is CUPS??

(Common UNIX Printing System) CUPS is used to manage your printers and printer shares through a web based interface. You can access this through your web browsers at http://127.0.0.1:631 or through http://localhost:631. On previous versions or upgrades, the CUPS password encryption system is broken.

If you want to know more see http://www.cups.org/.

Can I use CUPS to manage my printers with Active Directory?

Only on the server version of 10.4.x and then….Good Luck!!

Hey, this is UNIX based OS! Can't I setup shares that are authenticated through Active Directory on my stand alone workstation?

In short no, it only has one way authentication. Apple has modified the winbind NTLM_auth tool to fit their needs. Adding winbind parameters to the /etc/smb.conf file will not work. On the server version they put the winbind options in the /Library/Preferences/DirectoryService/winbindd.conf file. This is definitely not a standard configuration! You will need to purchase the server version to setup shares through Active Directory. Another option would be to download and recompile the SAMBA, but at the risk of breaking other applications (Good Luck!!).

I changed the Apple Computer name in Open Directory (or in the /etc/smb.conf), but it keeps going back to the previous name.

The /etc/smb.conf file is constantly updated with other preference files. You probably have a different computer name setup in System Preferences/Sharing.

I want to use my Windows Print server in Active Directory to manage print jobs from Apple Clients. What do I do?

Go to **\Applications\Utilities** and open the "**Printer Setup Utility**"
Click on **Add**
Hold down the "**Alt**" key and click on **More Printers…**

Note: Using the "Alt" key will give you an additional selection on the next screen called Advanced in the next screen.

On the top drop down menu click on **Advanced**
In the Device: drop down menu, select "**Windows Printer via SAMBA**"
In the Device name type in a Descriptive name the user will understand.
In the **Device URI:**
Type in one of the following

smb://username:password**@**server[:port]/printer
smb://username:password**@**workgroup/server[:port]/printer
smb://domain\username:password**@**server/printer

Note: This is highly insecure. The login and password are stored in /etc/cups/printers.conf

Note: The port setting is optional. A username and password are required because of a bug in the authentication process.
The smbpool does not support Kerberos authentication. However there is a patch out there. See the following URLs for information:

http://lists.samba.org/archive/samba-technical/2005-June/041321.html
http://lists.samba.org/archive/samba-technical/2005-April/040492.html

If you have problems connecting try the following troubleshooting methods suggested on multiple forums:

Install “UNIX File and Print Services” on the Windows server.
Verify you have a compatible PPD file on your printer.
Change the entry "client ntlmv2 = no" to read "yes" in the /etc/smb.conf file.
Note: Changing ntlmv2 to yes, will break SSO (Single Sign On) with the Active Directory Plug-in.

***** **Update**: I figured out how to Kerberize CUPS so the user can print to the *****
***** Windows server with pass through authentication. See me offline for assistance *****

The Mac doesn’t prompt me to type in my login, it just automatically logs in.

Click on **System Preferences\Accounts** (click the picture of the lock if necessary)\Login Options\

Unchecked Automatically log in as:

Display login window as:
Unchecked List of users
Checked Name and password

I want to automatically map drives when the users login. How do I do that?

Multiple Drives

Open the Applescript Editor located in Applications\AppleScript\Script Editor
In the bottom half of the window, type the following text:

```
tell application "Finder"
try
mount volume "cifs://servername/location"
delay 1
end try
end tell
```

Replace servername/location with the appropriate share name.

Press the "**Check Syntax**" button on the right to verify the syntax is correct.
Next click the "Run" button.
Save the script as an application by choosing the **File menu\Save As...** In the save dialog box choose "**Application**" for the Format and click the "**Never Show Startup Screen**" box. Make sure that is will be saved as "**Run Only**" - this will make the script more difficult to view. Name the app and click "**Save**".
Once you save the file to your preferred location go to **System Preferences\Accounts\User Account\Login Items** and click **+**. Next browse and add the script.

Note: **cifs** is used for Windows Shares (a.k.a. Common Internet File System)
(Enhance version of SMB with Microsoft extensions)

smb is the standard used to connect to UNIX Shares (a.k.a. Server Message Block)
(Can be used to connect to Windows Shares)

afp is used for Apple Shares (a.k.a. AppleTalk Filing Protocol)

ftp is used to connect to remote sites (a.k.a. File Transfer Protocol)
(Unsecured Protocol)

http is used to connect to a WebDav server (HyperText Transfer Protocol)

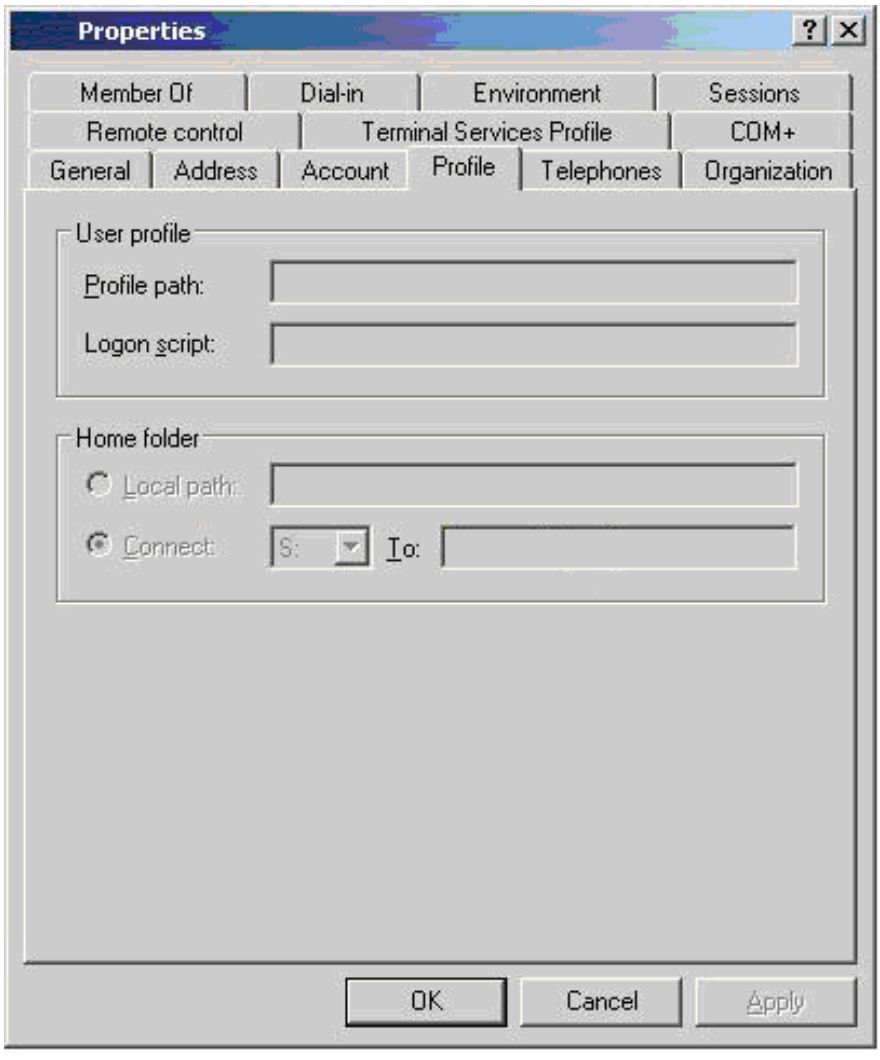
nfs is typically used by UNIX variants (Network File System)
(Developed by SUN)

Every user in Active Directory has the ability to login, but I want to filter who can and cannot login.

In order to filter users you will need to utilize Apple Managed Client for X, or MCX for short. MCX can be implemented two ways. The first is to have U.T.O. modify their Active Directory schema (Ha!!! Chuckles ☺). The second option is to put a Apple server on your network.

Users Home Directory

Contact Central IT and have an Enterprise Admin edit the users account and add your servers "Home folder". Make sure you have them put in a FQDN for your server, otherwise you will have issues with Apples DNS weirdness. (Example: \\myservername.myorg.asu.edu\johndoe)



Error messages received when attempting to join ASURITE:

You most likely typed in the wrong domain. If you have a static IP address, check your DNS and WINS.

Check your computers time. If it is off by more than 5 minutes, then you will receive this error.

Note: I believe that ASU uses the following time servers:

Colorado Springs, CO: Schriever AFB
204.34.198.40: navobs1.usnogps.navy.mil; CNAME: tick.usnogps.navy.mil
204.34.198.41: navobs2.usnogps.navy.mil; CNAME: tock.usnogps.navy.mil
Service area: U.S. pacific and mountain time zones

This indicates that you do not have the ability to add computers to Active Directory. Verify you have typed in the correct account information.

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