One Identity Authentication Services 4.1.3

Mac OS X/macOS Administration Guide

Copyright 2017 One Identity LLC.

ALL RIGHTS RESERVED.

This guide contains proprietary information protected by copyright. The software described in this guide is furnished under a software license or nondisclosure agreement. This software may be used or copied only in accordance with the terms of the applicable agreement. No part of this guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording for any purpose other than the purchaser's personal use without the written permission of One Identity LLC .

The information in this document is provided in connection with One Identity products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of One Identity LLC products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, ONE IDENTITY ASSUMES NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL ONE IDENTITY BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF ONE IDENTITY HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. One Identity make no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. One Identity do not make any commitment to update the information contained in this document.

If you have any questions regarding your potential use of this material, contact:

One Identity LLC.

Attn: LEGAL Dept

4 Polaris Way

Aliso Viejo, CA 92656

Refer to our Web site (http://www.OneIdentity.com) for regional and international office information.

Patents

One Identity is proud of our advanced technology. Patents and pending patents may apply to this product. For the most current information about applicable patents for this product, please visit our website at http://www.OneIdentity.com/legal/patents.aspx.

Trademarks

One Identity and the One Identity logo are trademarks and registered trademarks of One Identity LLC. in the U.S.A. and other countries. For a complete list of One Identity trademarks, please visit our website at www.OneIdentity.com/legal. All other trademarks are the property of their respective owners.

Legend

WARNING: A WARNING icon indicates a potential for property damage, personal injury, or death.

CAUTION: A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.

IMPORTANT, NOTE, TIP, MOBILE, or VIDEO: An information icon indicates supporting information.

Authentication Services Mac OS X/macOS Administration Guide
Updated - September 2017
Version - 4.1.3

Contents

Privileged Access Suite for Unix

Unix Security Simplified

Privileged Access Suite for Unix solves the inherent security and administration issues of Unix-based systems (including Linux and Mac OS X) while making satisfying compliance requirements a breeze. It unifies and consolidates identities, assigns individual accountability and enables centralized reporting for user and administrator access to Unix. The Privileged Access Suite for Unix is a one-stop shop for Unix security that combines an Active Directory bridge and root delegation solutions under a unified console that grants organizations centralized visibility and streamlined administration of identities and access rights across their entire Unix environment.

Active Directory Bridge

Achieve unified access control, authentication, authorization and identity administration for Unix, Linux, and Mac OS X systems by extending them into Active Directory (AD) and taking advantage of AD's inherent benefits. Patented technology allows non-Windows resources to become part of the AD trusted realm, and extends AD's security, compliance and Kerberos-based authentication capabilities to Unix, Linux, and Mac OS X. (See www.oneidentity.com/products/authentication-services/ for more information about the Active Directory Bridge product.)

Root Delegation

The Privileged Access Suite for Unix offers two different approaches to delegating the Unix root account. The suite either *enhances* or *replaces* sudo, depending on your needs.

- By choosing to enhance sudo, you will keep everything you know and love about sudo while enhancing it with features like a central sudo policy server, centralized keystroke logs, a sudo event log, and compliance reports for who can do what with Sudo.

  (See www.oneidentity.com/products/privilege-manager-for-sudo/ for more information about enhancing sudo.)
- By choosing to replace sudo, you will still be able to delegate the Unix root privilege based on centralized policy reporting on access rights, but with a more granular permission and the ability to log keystrokes on all activities from the time a user logs

in, not just the commands that are prefixed with "sudo". In addition, this option implements several additional security features like restricted shells, remote host command execution, and hardened binaries that remove the ability to escape out of commands and gain undetected elevated access.

(See www.oneidentity.com/products/privilege-manager-for-unix/ for more information about replacing sudo.)

Privileged Access Suite for Unix

Privileged Access Suite for Unix offers two editions - *Standard* edition and *Advanced* edition. Both editions include: **Management Console for Unix**, a common mangement console that provides a consolidated view and centralized point of management for local Unix users and groups; and, **Authentication Services**, patented technology that enables organizations to extend the security and compliance of Active Directory to Unix, Linux, and Mac OS X platforms and enterprise applications. In addition

- The *Standard* edition licenses you for Privilege Manager for Sudo.
- The *Advanced* edition licenses you for Privilege Manager for Unix.

One Identity recommends that you follow these steps:

1. Install Authentication Services on one machine, so you can set up your Active Directory Forest.
2. Install Management Console for Unix, so you can perform all the other installation steps from the mangement console.
3. Add and profile host(s) using the mangement console.
4. Configure the console to use Active Directory.
5. Deploy client software to remote hosts.

   Depending on which Privileged Access Suite for Unix edition you have purchased, deploy either:

   - **Privilege Manager for Unix** software (that is, Privilege Manager Agent packages)

     -OR-

   - **Privilege Manager for Sudo** software (that is, Sudo Plugin packages)

About this guide

The *Authentication Services Mac OS X Administration Guide* describes the port of the Authentication Services for Mac OS X product to the Mac OS X platform. Authentication Services for Mac OS X brings the enterprise functionality Authentication Services supplies on every other major Unix platform to Mac OS X.

Authentication Services supports both Mac OS X and Mac OS X Server versions 10.5 - 10.7. Authentication Services recommends that you install all the latest Apple system updates before installing Authentication Services.

In this guide you will find step-by-step instructions on installing, configuring, and uninstalling Authentication Services along with a detailed explanation of the Authentication Services components for Mac OS X.

In addition, the "Group Policy for Mac OS X" section documents each policy supported for this version of Authentication Services for Mac OS X.

This guide is not comprehensive and only describes those Authentication Services features specific to Mac OS X. Refer to the *Authentication Services Administration Guide*, located in the `docs` directory of the installation media for complete documentation on all other Authentication Services features.

NOTE: The term "Unix" is used informally throughout the Authentication Services documentation to denote any operating system that closely resembles the trademarked system, UNIX.

2

Installation

This section includes instructions for installing and configuring the Authentication Services agent on Mac OS X.

Authentication Services Mac OS X agent installation

Authentication Services Software is provided in a standard disk image located in the Mac OS X subdirectory on the Authentication Services installation disk. You can install the Authentication Services agent software through the graphical user interface or from the command line, more common in a mass deployment scenario.

Install Authentication Services using the graphical system installer

To install Authentication Services using the graphical system installer

1. Insert the Authentication Services installation disk and navigate to the Mac OS X folder for your operating system.

   There are three folders containing disk images: `macos-104`, `macos-106`, and `macos-107`. Select the VAS-<*version*>.<*build number*>.dmg file for your Mac OS X operating system where <*version*> is the version and <*build number*> is the build number of your Authentication Services release.

   NOTE: For Mac OS X 10.5, use the `.dmg` in the `macos-104` folder.

2. Mount the disk image by double-clicking the VAS-<*version*>.<*build number*>.dmg file.

   The .dmg contents mounts on your system. The .dmg contents are located in `/Volumes/VAS-Installer` and appear as a mounted volume in the *Finder* window.

Under the mounted disk image you find the Authentication Services metapackage (`VAS.mpkg`). This metapackage contains all Authentication Services client components.

Install Authentication Services with the system installer

To install Authentication Services with the system installer

1. Double-click the `VAS.mpkg` file from **Finder**.

   The Authentication Services installation wizard starts to guide you through the installation process.

2. On the Introduction (Welcome) screen, click **Continue** to proceed with the installation.

   The Software License Agreement displays.

3. On the License screen, if you agree to the terms, click **Agree**.

   NOTE: You must agree to continue.

4. On the Installation Type screen, click **Install** to install the standard components and accept the default installation location on the root volume. The standard components include Authentication Services Client and Quest Group Policy. To select additional components, click Customize. For more information, see Custom install on page 10.

   NOTE: You must install the Authentication Services packages on the root volume and you can not relocate them.

5. The system installer prompts you for local administrator credentials when the software installation begins.

   Enter administrator credentials and click **OK**.

   NOTE: If you do not have administrator rights for your system, contact your system administrator for assistance.

6. The Summary screen confirms a successful Authentication Services for Mac OS X installation. Click **Close** to exit the wizard.

Custom install

A custom installation includes the following options:

- Quest Authentication Services Software Development Kit (SDK)
- Quest Dynamic DNS Update — which supports authenticated A-record and PTR-

record updates to the Microsoft DNS servers

- Certificate Autoenrollment

To perform a custom install

1. On the Installation Type screen, click the **Customize** button to select additional components (besides Quest Authentication Services Client and Quest Group Policy) of the product you want to install.

   Once you have selected the additional components to be installed, click **Install**.
2. The system installer prompts you for local administrator credentials when the software begins to install.

   Enter administrator credentials and click **OK**.
3. The Summary screen confirms a successful Authentication Services for Mac OS X installation. Click **Close** to exit the wizard.

Command line install

You can either install the Authentication Services metapackage, which installs all of the Authentication Services packages, or you can install one or more of the individual Authentication Services packages contained in the Authentication Services metapackage using the system command line installer (`/usr/sbin/installer`).

NOTE: If you do not have administrator rights for your system, contact your system administrator for assistance.

You must launch a **Terminal.app** instance to complete the following tasks.

- Install the Authentication Services metapackage from command line
- Install a single Authentication Services package from command line
- Mount and unmount the Authentication Services .dmg from the command line

Install the Authentication Services metapackage from command line

To install all of the Authentication Services packages found in the Authentication Services metapackage

1. Open a `Terminal.app` window and execute the following commands
2. Change directories to the location where you mounted the Authentication Services.`dmg`:

   ```
   $ cd /Volumes/VAS-Installer
   ```

3. Execute the command line installer with the following arguments:

   ```
   $ sudo /usr/sbin/installer -pkg VAS.mpkg -target /
   ```

   This installs all of the Authentication Services packages contained in the Authentication Services metapackage.

4. Run the following command to install individual Authentication Services components.

   ```
   $ cd /Volumes/VAS-Installer/VAS.mpkg/Contents
   $ sudo /usr/sbin/installer -pkg Packages/vasclnt.pkg \ -target /
   ```

NOTE: You must install all Authentication Services components into the root file system, so the parameter to the target command line option must be /. Also, you must have local administrator rights to run commands using the sudo utility.

Install a single Authentication Services package from command line

To install a single Authentication Services package from command line

1. Change directories to the location where you mounted the Authentication Services agent `.dmg`:

   ```
   $ cd /Volumes/VAS-Installer/VAS.mpkg/Contents
   ```

2. Execute the following command to install the Authentication Services core components:

   ```
   $ sudo /usr/sbin/installer -pkg Packages/vasclnt.pkg \-target /
   ```

3. Execute the following command to install the Group Policy components:

   ```
   $ sudo /usr/sbin/installer -pkg Packages/vasgp.pkg \-target /
   ```

Mount and unmount the Authentication Services .dmg from the command line

To mount and unmount the Authentication Services .dmg from the command line

1. Mount the Authentication Services agent `.dmg` from the command line and run the following command:

   ```
   hdiutil attach /<path_to_dmg>/VAS-<version>.<build number>.dmg
   ```

   The `.dmg` contents mounts on your system, under

   ```
   /Volumes/VAS-Installer
   ```

2. To unmount the Authentication Services agent `.dmg` from the command line, run the following command:

   ```
   hdiutil detach /Volumes/VAS-Installer
   ```

Authentication Services agent upgrade

To upgrade Authentication Services, simply follow the normal installation steps for both the GUI process and the command line process. The Authentication Services installation scripts detect when an upgrade is being performed and automatically perform the proper steps to upgrade versions.

Authentication Services Mac OS X agent removal

Authentication Services provides an uninstaller that removes the Authentication Services packages from the system. The uninstaller is found in `/Applications/Uninstall QAS 4.n.n` (where *n.n* indicates the product version number.)

To uninstall Authentication Services, use the Finder, navigate to /Applications and double click the **Uninstall Authentication Services 4.n.n** application. The uninstaller displays the packages that you can remove. The uninstaller requires administrator credentials.

NOTE: When removing Authentication Services from your system, files owned by accounts supplied by the Authentication Services components appear as not having a valid owner since those accounts are no longer available to the system.

3

The Authentication Services Mac OS X components

The following Authentication Services Unix components are included in the Authentication Services Mac OS X port:

- The vastool command line utility
- The vgptool command line utility
- The uptool command line utility
- The pam_vas PAM module
- The One Identity Ownership Alignment Tool (OAT)

You can use these components inside a Terminal session the same way you use them on any other Unix platform. Man pages for each of these utilities are automatically installed and configured and you can view them with a standard man page viewer. The Authentication Services join process automatically configures Unix applications to use the `pam_vas` module where appropriate.

The components described in this section are specific to the Mac OS X platform.

Authentication Services startup items

A `launchd config plist` file is installed for each Authentication Services daemon under /Library/LaunchDaemons.

These `.plist` files are used to put the Authentication Services daemons under the control of `launchd`. You can use the `launchctl` utility to add or remove any one of these daemons from `launchd` control. For example, to remove the Authentication Services caching daemon (vasd) from `launchd` control, run the following command in a Terminal session:

```
$ sudo /bin/launchctl unload /Library/LaunchDaemons/com.quest.vasd.plist
```

You can also stop a daemon using `launchctl`, but the Authentication Services daemon configuration is such that `launchd` immediately restarts the stopped daemon unless you specify the `unload` command. If it is necessary to restart any one of the Authentication Services daemons, run a command similar to the following:

```
$ sudo /bin/launchctl stop com.quest.vasd
```

The Authentication Services join process automatically runs the necessary `load` commands at join time to put the Authentication Services daemons under `launchd` control. Typically, users do not need to directly interact with the Authentication Services startup items.

Authentication Services directory service plugin

Authentication Services provides a plugin for the system DirectoryService daemon.

The Authentication Services Directory Service Plugin uses the rest of the Authentication Services components to provide Active Directory group and user information to the rest of the system, and is installed at `/Library/DirectoryServices/Plugins/VAS.dsplug`.

The Authentication Services Directory Service Plugin also uses Kerberos authentication for Active Directory users. The plugin operates both when the system is connected to a network where Active Directory is available, and for disconnected scenarios where the Mac OS X system cannot contact Active Directory. The Authentication Services Directory Service Plugin provides secure authentication and performance identity lookups even in this disconnected mode.

Disconnected mode is available without having to create local Mobile Accounts on each Mac OS X system. The Authentication Services caching architecture also minimizes the impact that each Mac OS X system has on the Active Directory environment.

Authentication Services directory utility plugin

You use the Directory Utility application to configure the Directory Service Plugins that provide identity information for authenticating to the machine. When installed, Authentication Services is one of the plugins.

The Authentication Services Directory Utility plugin provides a GUI utility for joining and leaving Active Directory domains, and controlling the local Authentication Services configuration.

On Leopard (10.5), the Authentication Services Directory Utility Plugin is installed at:

```
/Applications/Utilities/Directory Utility.app/Contents/Plugins/VAS.daplug
```

On Snow Leopard (10.6) and Lion (10.7) it is installed at:

```
/System/Library/CoreServices/Directory Utility.app/contents/PlugIns/VAS.daplug
```

Authentication Services security server plugin

The system Security Server controls all authorization on the Mac OS X system.

To correctly initialize Authentication Services user login sessions, a VASMechanism Security Server plugin is installed and configured in the `/etc/authorization` file by the Authentication Services join process. This plugin is installed under `/System/Library/CoreServices/SecurityAgentPlugins/VASMechanism.bundle`. The Authentication Services mechanism initializes a Kerberos ticket cache for each Authentication Services user's login session with the Kerberos tickets obtained during DirectoryService authentication. Note that these ticket caches are fully compatible with the system `Kerberos.app` utility and the system MIT Kerberos command line utilities, so that the rest of the Mac OS X system components can reuse the Kerberos functionality.

4

Configuring the Authentication Services client

Before you can log in with Active Directory users and manage agent settings for users and computers, you must first join your Mac OS X/macOS machine to an Active Directory domain.

NOTE: For earlier versions of Mac OS X (prior to 10.11), use the Directory Utility application as explained in this chapter. For later versions of Mac OS X/macOS (10.11 and higher), use the QAS Join application.

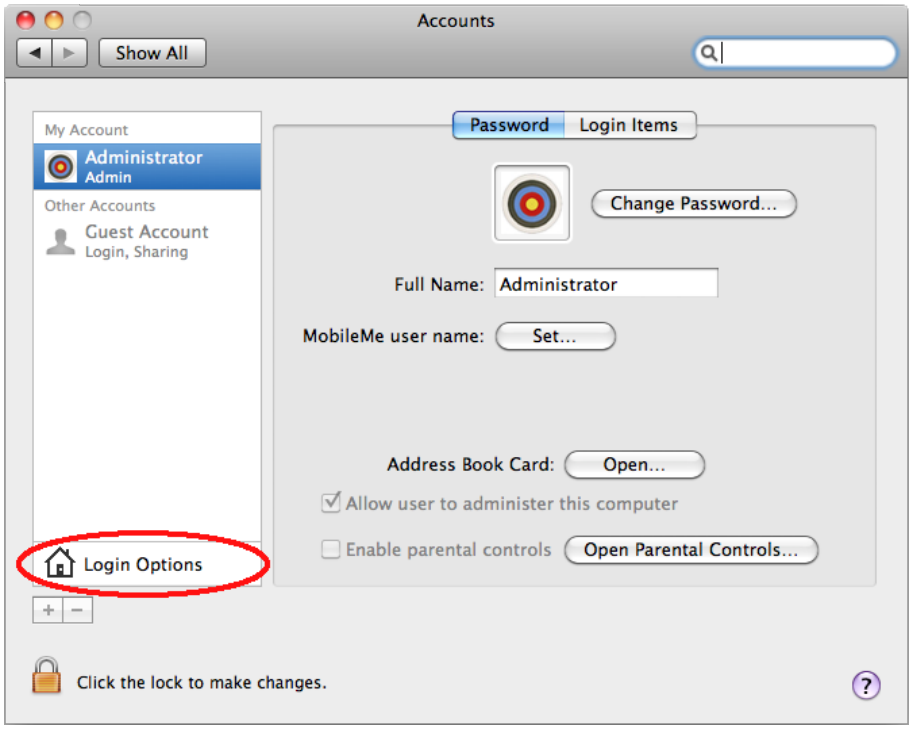
The following section guides you through the steps necessary to launch the Directory Utility application to configure your system for comprehensive Active Directory integration. When using the QAS Join application, you will notice that the screens are a bit different, but the procedure is similar to what is documented here.

Launch the directory utility application

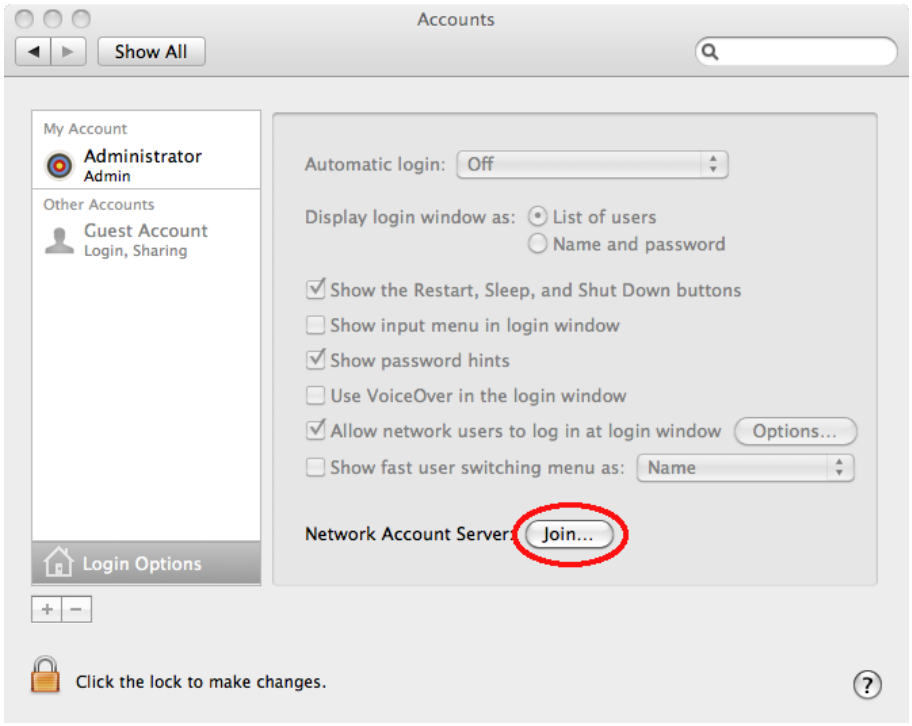
To launch the Mac OS X 10.7 (or higher) Directory Utility Application

1. Open **System Preferences** and select the **Users & Groups** preferences.

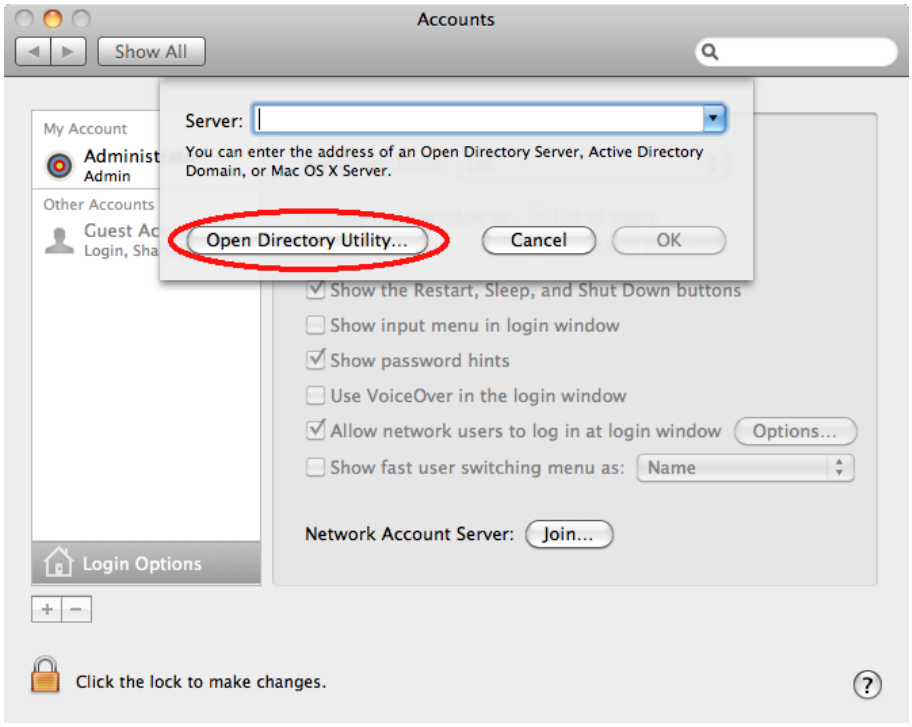
2. Select **Login Options** on the bottom left side of the view.



3. Select the **Network Account Server Join...** button on the bottom right side.



4. Click the **Open Directory Utility** button.

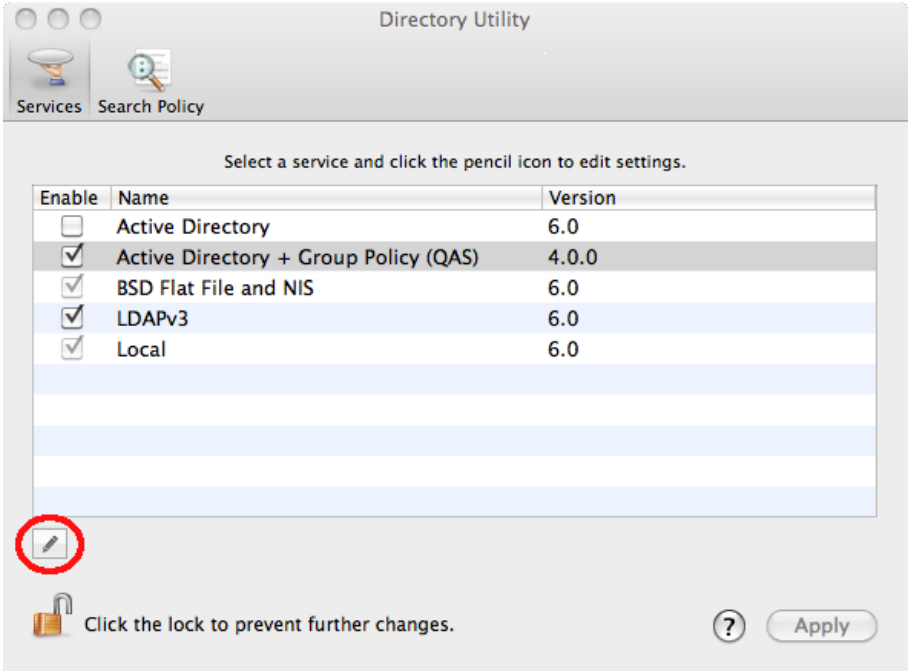


CAUTION: Do not enter the name of your domain and click OK from this dialog. If you do, you will join using the native Apple Active Directory plugin which has no support for Active Directory group policies. You must open the Directory Utility application to join the domain using Authentication Services.

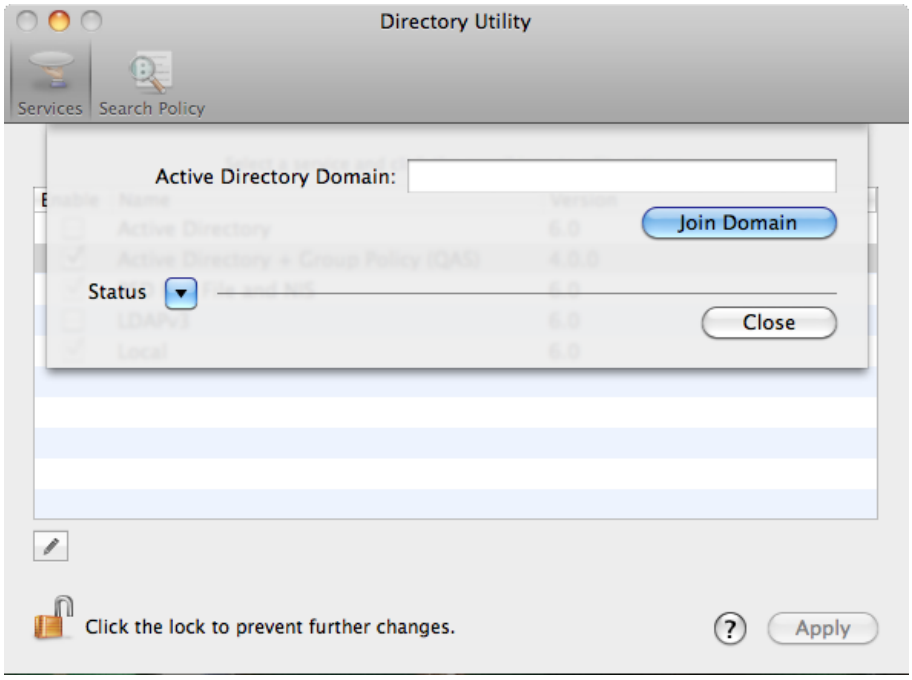
Configure the Authentication Services node

To configure the Authentication Services node

1. Click the **Lock** icon in the bottom left corner of the Directory Utility application to be authorized as an administrator. Until you do this, you will be unable to modify the system's Directory Access configuration.
2. Click **Services** to display configurable services.
3. Select **Active Directory + Group Policy (QAS)**, and click the *Pencil* icon to configure this node.



The Authentication Services Directory Utility plugin interface displays.



Adding, checking, and verifying Authentication Services licenses

To utilize the complete Authentication Services functionality, you must have a Authentication Services product license installed. This license provides basic functionality such as Active Directory authentication.

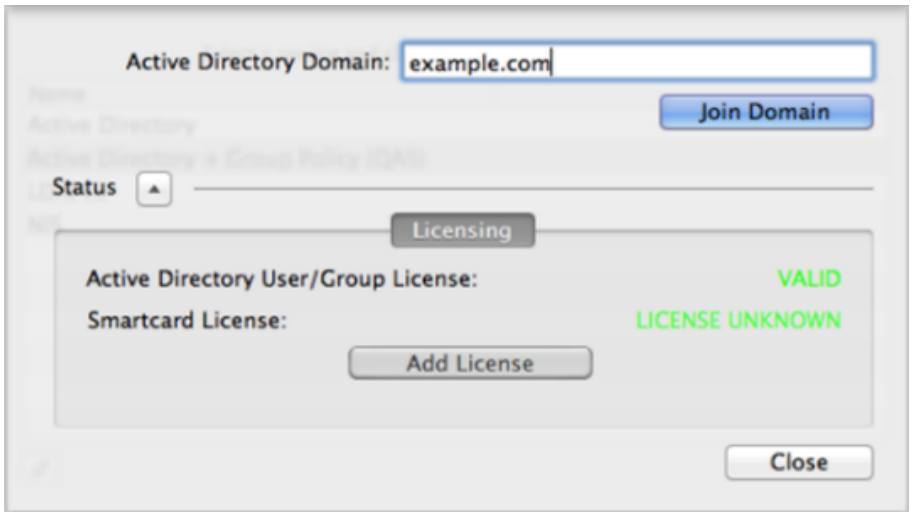
Complete the following steps to install the license using the Authentication Services Directory Utility plugin before continuing with the join process.

NOTE: For scripted or command-line configuration, copy the licenses to `/etc/opt/quest/vas/.licenses`

Add, check, and verify licenses

To add, check, and verify licenses

1. From the Authentication Services Directory Utility plugin, click the **Status Disclosure Triangle** to check for valid licenses.



If the license is missing or expired, click **Add License**.

NOTE: Most Authentication Services deployments have Authentication Services licenses available through an Active Directory group policy or installed through the Authentication Services application configuration that automatically applies to the system when you perform the Authentication Services join. If you have a license policy configured in Active Directory, you can skip these manual install instructions. Instead return to this screen after joining to verify proper license installation.

2. Once the license has been added, verify that it is valid and click **Close**.

Joining the Active Directory domain

Authentication Services provides both a graphical option and a command line option for joining the domain.

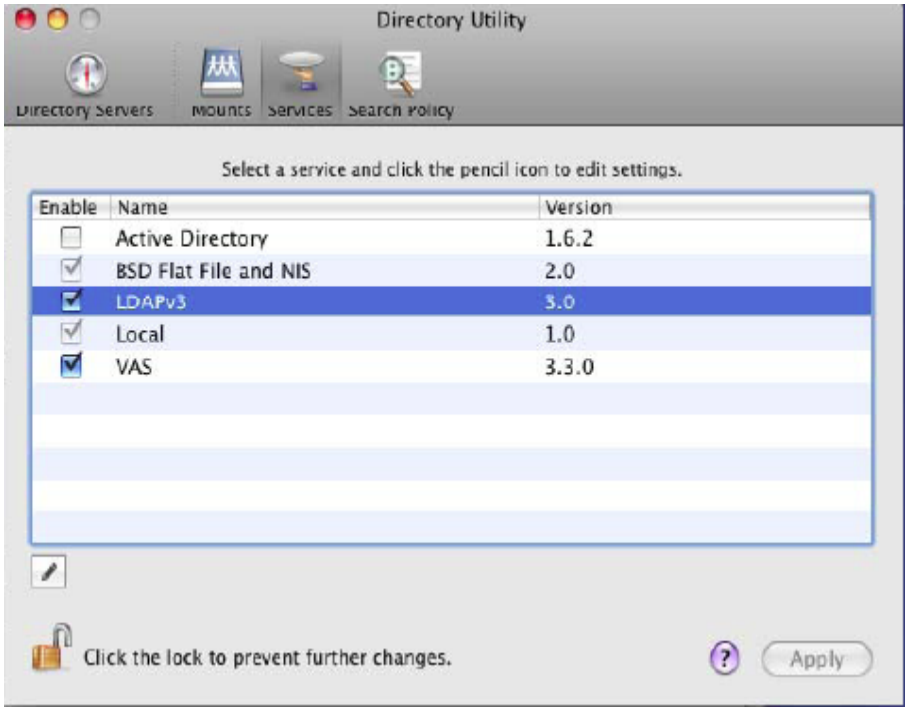
NOTE: You cannot manage agent settings by means of Authentication ServicesGroup Policy if you have joined with the Apple-provided Active Directory plug-in. If you are currently bound to the domain using Apple components, unbind before proceeding.

Unconfigure local LDAPv3

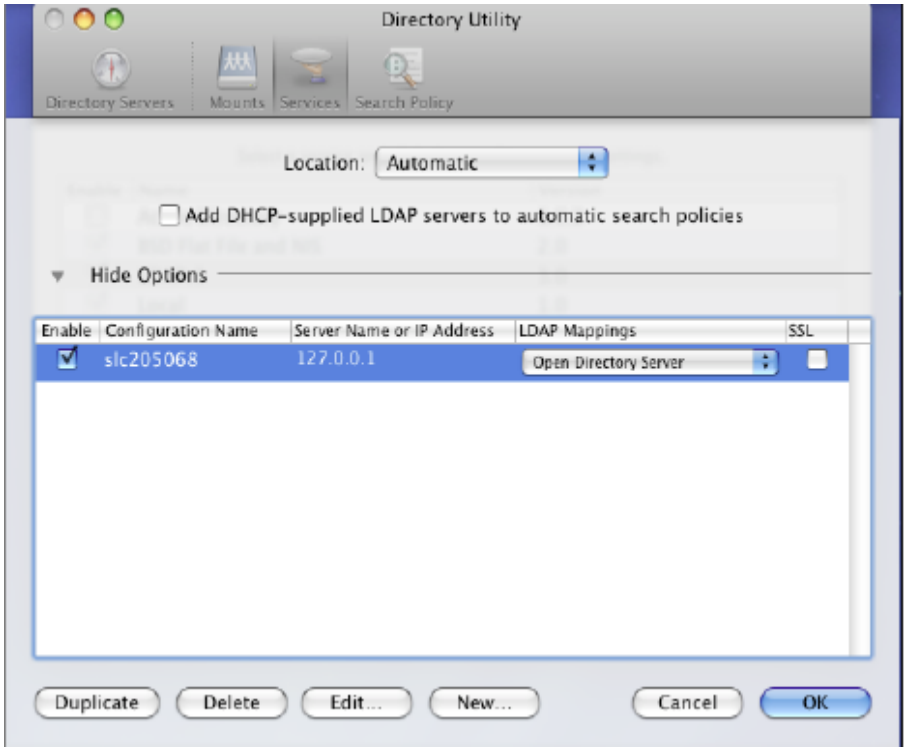
If you are running Mac OS X 10.5, you must unconfigure the local LDAPv3 node before joining to Authentication Services by means of Active Directory. Problems arise with application of machine policy if you do not do this. If you are replacing an existing OpenDirectory or LDAP instance with Active Directory, unconfigure the corresponding LDAP node at this time.

To unconfigure an LDAPv3 node

1. From the Directory Utility screen, select the **LDAPv3** box.



2. Click the *pencil* icon to edit the service.
3. On the Search Policies screen, click **Delete** and then click **OK**.

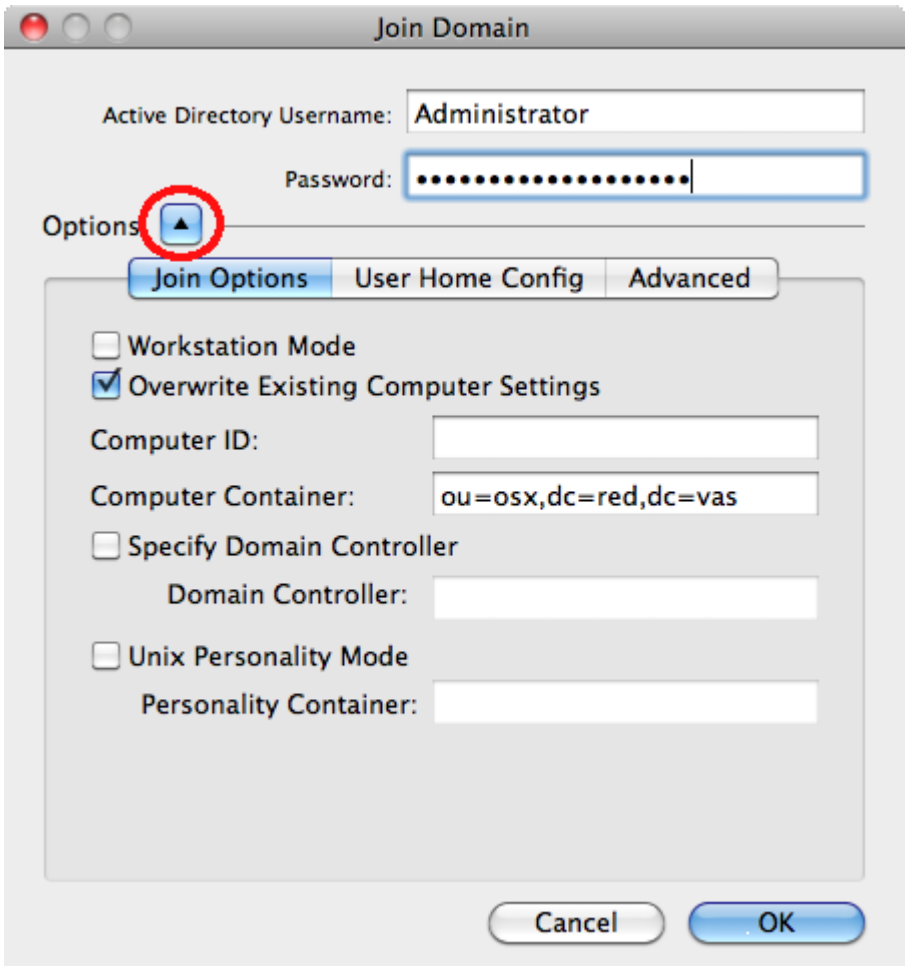


Graphically join the domain

To graphically join the domain

1. Enter the name of the Active Directory Domain you want to join and click **Join Domain**.
2. In the Join Domain dialog that appears, supply Active Directory credentials to join the domain.

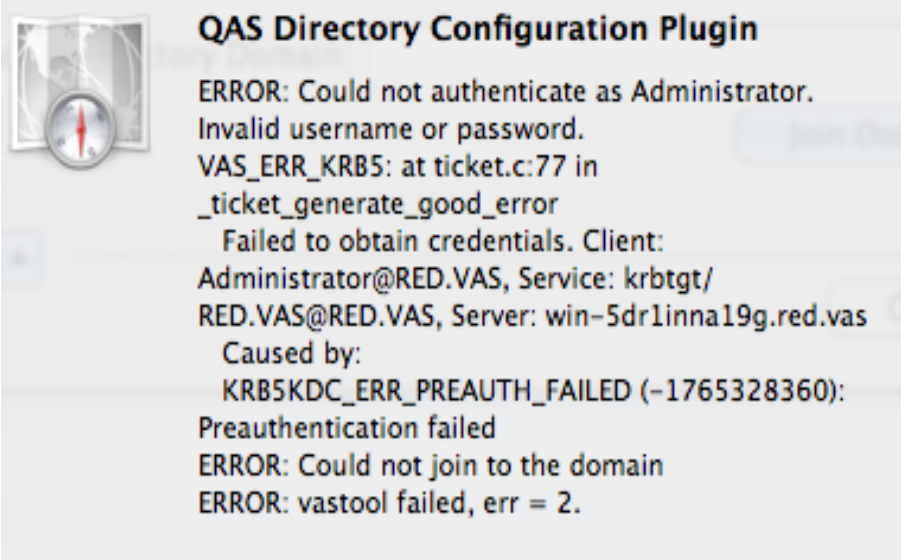
   From this dialog you can also specify a number of optional join arguments before continuing with the join operation. For example, you can specify a specific Active Directory container in which you want to create the new computer object. (By default it is created in the Computers Container). For a detailed explanation of each join option, see the *vastool man page* located in the `docs` directory of the installation media.



3. Click **OK** to execute the join operation.

   The join operation may take several seconds, to several minutes depending upon your domain configuration. Domain Join progress is continuously updated as progress proceeds.

4. If any errors occur during join, an error dialog opens with a detailed error message as well the option to view and save the join process log. As an example, the error message below is seen if you specified an incorrect password for the account you are using to join to the domain.



Unjoin an Active Directory domain

To leave the Active Directory Domain, repeat the join steps, except click **Leave Domain** instead. You do not have to supply Active Directory credentials when unjoining if you do not delete the Active Directory computer object. This option is available in the Leave Domain dialog options.

1. After modifying the Authentication Services configuration, click **Apply** in the main Directory Access or Directory Utility dialog (depending on your version of Mac OS X) to ensure that your changes take effect.

Command line join

Use the **vastool** utility to perform a command line join.

At the command line, enter `vastool join` to join the Mac OS X system to an Active Directory domain.

Using Terminal.app to join and unjoin

You can access the same functionality that is available through the Authentication Services Directory Utility Plugin through the Authentication Services command line utilities.

There are two ways to join your Mac OS X system to an Active Directory domain:

- Run the `vasjoin.sh` script.

  ```
  $ sudo /opt/quest/libexec/vas/scripts/vasjoin.sh
  ```

  This script prompts you for information needed to perform the join operation without requiring you to know the syntax of the `vastool join` command.

  -OR-

- Run the `vastool join` command.

  ```
  $ sudo /opt/quest/bin/vastool -u Administrator join -f example.com
  ```

To leave an Active Directory Domain from a Terminal session, use the `vastool unjoin` command.

NOTE: See the *vastool man page* located in the `docs` directory of the installation media for more information about the `vastool join` or `vastool unjoin` commands.

System changes made by the join process

When joining an Active Directory Domain, Authentication Services automatically modifies the following system configurations:

- Authentication Services is added to the DirectoryService search path.
- The Authentication Services startup items are configured to startup automatically
- The system MIT Kerberos configuration file is configured to use the Active Directory servers that Authentication Services detects.
- The system authorization rules contained in `/etc/authorization` are modified to use the VASMechanism for Authentication Services logins.
- Group Policies configured for the Mac OS X system are applied by the Group Policy components if they are installed.

Once you have successfully completed the Authentication Services join process, you are immediately able to log into the Mac OS X system through both the Mac OS X Login Window and remotely through SSH.

When leaving a domain, the Authentication Services unjoin process reverts the above changes that were made by the Authentication Services join process. Also, uninstalling Authentication Services automatically reverts the above changes as well.

NOTE: You can re-join on top of existing computer accounts created with the Mac OS X Active Directory Plugin by default using the Authentication Services Active Directory plugin, but we recommend disabling the Mac OS X Active Directory plugin so that the domain will not appear in the *Directory Servers* window as not responding.

Verify the installation and configuration

It is important to verify that your system is configured correctly to use the Active Directory account information provided by Authentication Services.

To verify the Authentication Services installation and configuration

1. Run the following shell commands.
    - To show a list of the available Unix-enabled Active Directory users, enter

      `dscl /VAS list /Users`
    - To show a list of the available Unix-enabled Active Directory groups, enter

      `dscl /VAS list /Groups`
    - To ensure that the system can read user information for Authentication Services users, enter

      `dscl /Search read /Users/<Username>`

      where `<Username>` is the username of a Authentication Services user.
    - To perform an authentication for a Authentication Services user, enter

      `dscl /Search auth <Username>`

      where `<Username>` is the username of a Authentication Services user.

    If any of the previous commands do not work, capture debug information from the Authentication Services Directory Service plugin.
2. Add the following items to the `vas.conf` [`vas_macos`] section:

    ```
    [vas_macos]
       dslog-mode = /Library/Logs/vasds.log
       dslog-components = plugin,auth
    ```
3. After adding those items, run the following shell command in a Terminal session to trigger the Authentication Services Directory Services Plugin to reload its logger configuration:

    ```
    $ sudo /opt/quest/libexec/vas/macos/vasdsreload
    ```
4. Execute the previous verification commands that failed and send the contents of `/Library/Logs/vasds.log` to One Identity Support who will assist in resolving the problems.

Logging in with Active Directory accounts

Authentication Services for Mac OS X allows you to authenticate to your Mac OS X system, but before you can use any given account for authentication, you can prepare it for Mac OS X authentication from a Windows Administrative Console through a process called Unix-enabling. However, if you do not have access or permissions to modify user account information in Active Directory, you can join and specify that you want the Authentication Services client to locally generate Unix identity information.

To locally generate Unix identity information, select the **Generate Unix Identity Attributes** option when you join (or, if you are joining using the command line utility, specify the `--autogen-posix-attrs` flag). This allows you to use all the features of the Authentication Services client, without requiring any modification to user information in Active Directory. If you plan to manage identity data in Active Directory globablly, proceed to the *Unix-enable a User* section.

Unix-enable a user

You Unix-enable a user by entering the Unix attributes on the Unix Account tab in Active Directory Users and Computers (ADUC) MMC Snapin.

To Unix-enable a user

1. Logon to a Windows Administrative workstation.
2. Start ADUC.
3. Locate the user object that you would like to Unix-enable.
4. Right-click on the user and select **Properties**.
5. Select the **Unix Account** tab.
6. Select the **Unix-enabled** check box.

   Default values are generated for the user.
7. Adjust values as necessary and click **OK**.

Troubleshooting connections to Windows SMB shares

There are some known issues connecting to Windows shares using Finder. If you log in as a domain user, Authentication Services obtains Kerberos credentials for your login session. Finder *should* use these credentials to automatically authenticate when connecting to

Windows shares. Instead, Finder promptd you for your password. The two possible causes for these issues are explained in the following topics:

- Connecting to SMB shares on domain controllers
- The DNS domain name differs from the Kerberos realm

Connecting to SMB shares on domain controllers

When connecting to SMB shares on a domain controller, settings on the default domain controller policy can force a Mac OS X client to Digitally Sign all traffic. Since Mac OS X clients do not support digitally signing SMB traffic, this can lead to a failure when attempting to mount an SMB share.

This issue is related to two settings in the Default Domain Controllers Policy.

To disable the policies and allow Mac OS X machines to connect to SMB shares

1. Open **Active Directory Users and Computers**, select the domain, right-click, and select **Properties**.
2. Click the **Group Policy** tab.

   NOTE: If you are using MS Server 2008, there is an additional menu item, **Policies**, added between **Computer Configuration** and **Windows Settings** in the following sequence.

   a. If the default Domain Controllers Policy is linked to this domain, navigate to **Edit | Computer Configuration | Windows Settings | Security Settings | Local Policies | Security Options**, then double-click and disable the following two policies:
      - Microsoft network server: Digitally sign communications (always)
      - Microsoft network server: Digitally sign communications (if client agrees)

   b. If the Default Domain Policy is linked to this domain, navigate to **Edit | Computer Configuration | Windows Settings | Security Settings | Local Policies | Security Options**, then double-click and disable the following two policies:
      - Microsoft network server: Digitally sign communications (always)
      - Microsoft network server: Digitally sign communications (if client agrees)

      If these group policies are not currently defined, you can leave them unconfigured. If either policy is enabled and linked to the domain, however, the Mac OS X computer is not be able to use SMB connections to mount the Windows file shares.

3. If you change these policies on the domain controller, run the `gpupdate` command to refresh the group policies before logging on to Mac OS X computers.

The DNS domain name differs from the Kerberos realm

Problem:

A network trace reveals if a Kerberos TGS request for the CIFS service ticket was sent to a domain controller. If a MAC never attempts to get a CIFS service ticket for SSO, it is usually a problem where the machine is not able to connect the host name you are contacting with a Kerberos realm. When this happens Finder, or any other mounting application, assumes that the host is not a part of any Kerberos domain for which you have credentials and prompts you for a user name and password.

This can easily happen if your DNS domain name is not the same as your Kerberos realm (often referred to as a disjoint DNS name space). It might also happen if you were trying to connect to the server using a short-name or some other alias.

Workaround:

Add a domain to realm mapping for your DNS domain, short-name, or alias under the "[domain_realm]" section of the `/Library/Preferences/edu.mit.kerberos` file.

Authentication Services automatically adds a mapping similar to the following at join time:

```
[domain_realm]
.example.com = EXAMPLE.COM
```

This maps any DNS names ending in `.example.com` to the KRB5 realm `EXAMPLE.COM`. You must always specify the destination domain realm in upper case. And, when attempting to connect to the share, you must specify the source exactly as the DNS name is specified.

If you are connecting to a share using an alias that does not have a domain suffix, you can explicitly map that name to a KRB5 realm using a domain realm:

```
[domain_realm]
shortname = EXAMPLE.COM
```

Automatically mount network home folders

When you Unix-enable an Active Directory user with Authentication Services, the default configuration for that user is that he or she will use a local home directory. The home directory path is populated with a Unix path (`/home/<username>`).

On Mac OS X systems, `/home` is replaced with `/Users`, aligning with the Mac OS X standard location for local home directories. Authentication Services supports the automatic mounting of network shares (SMB or AFP) using Active Directory credentials, but you must specify a server path. You can store this server path in the directory on each user as a UNC path, or as a per machine setting.

You can configure your home folder strategy globally for the entire domain using Group Policy extensions for Unix, or you can configure it on a per machine basis at the time you join your Mac OS X machine to the domain.

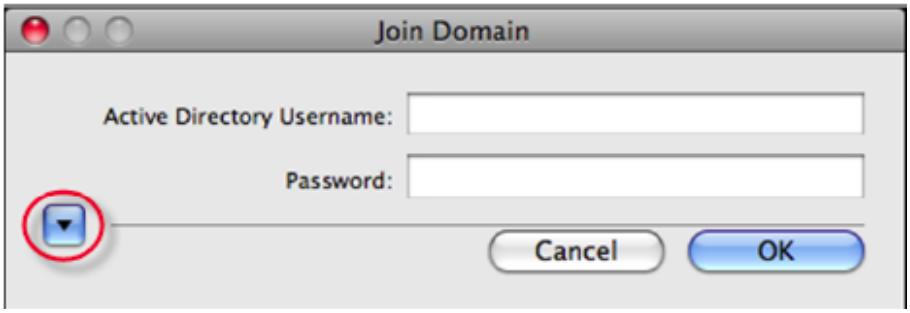
Configure automatic home folder mounting at join time

To configure automatic home folder mounting at join time

1. When you are prompted for your administrative username and password, click the disclosure triangle.

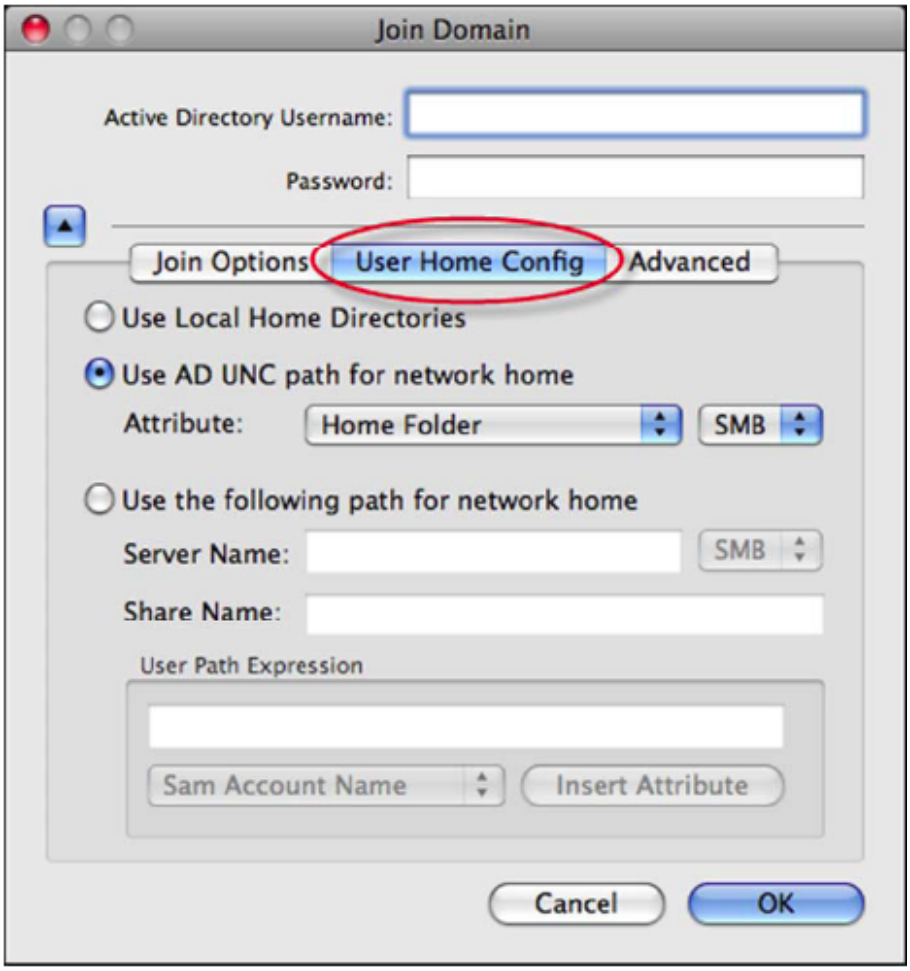
   

   The Join Domain dialog displays:

2. Select the **User Home Config** tab to expose all of the home folder mounting

options:

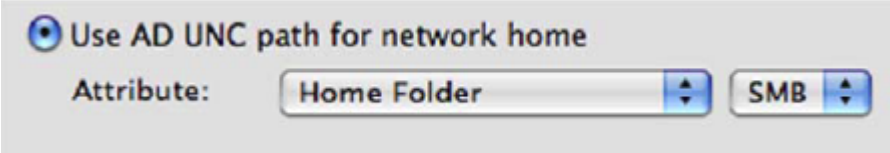


Mount the Windows home folder or profile path

You can configure Authentication Services to mount a share that is specified as a UNC format path and stored on a user. The two most commonly used paths are found on the users Profile tab in ADUC.

To mount the Windows Home Folder or Profile Path

1. Use Authentication Services to mount either the Home Folder or Profile Path on a Mac OS X agent at log in by selecting **Use Active Directory UNC path for network home** from the User Home Config properties.

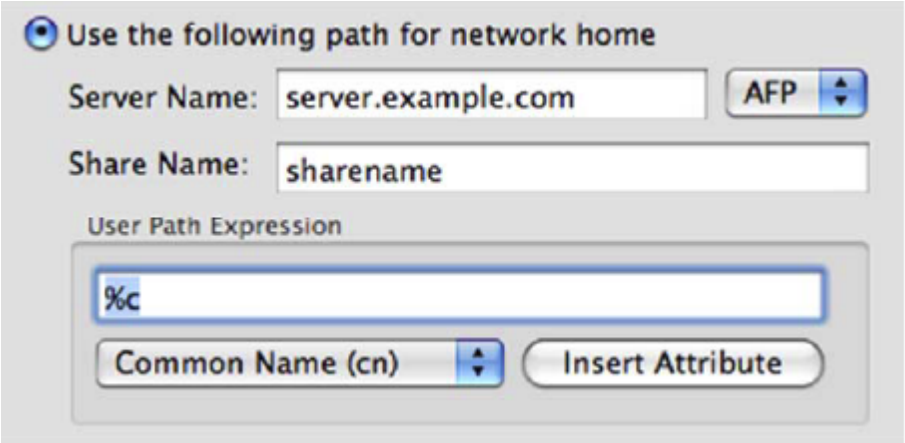


Mount an alternate share at login

If you cannot use the shares specified in Profile Path or Home Folder for some reason (for example, if your Windows home shares are DFS shares), you can specify an alternate share at join time by specifying a network home path expression.

To specify a network home path expression

1. Select **Use the following path for network home** from the User Home Config tab.



Selecting this option configures the network home for all users on the machine. Because of this you must specify how the path name will be resolved for each user.

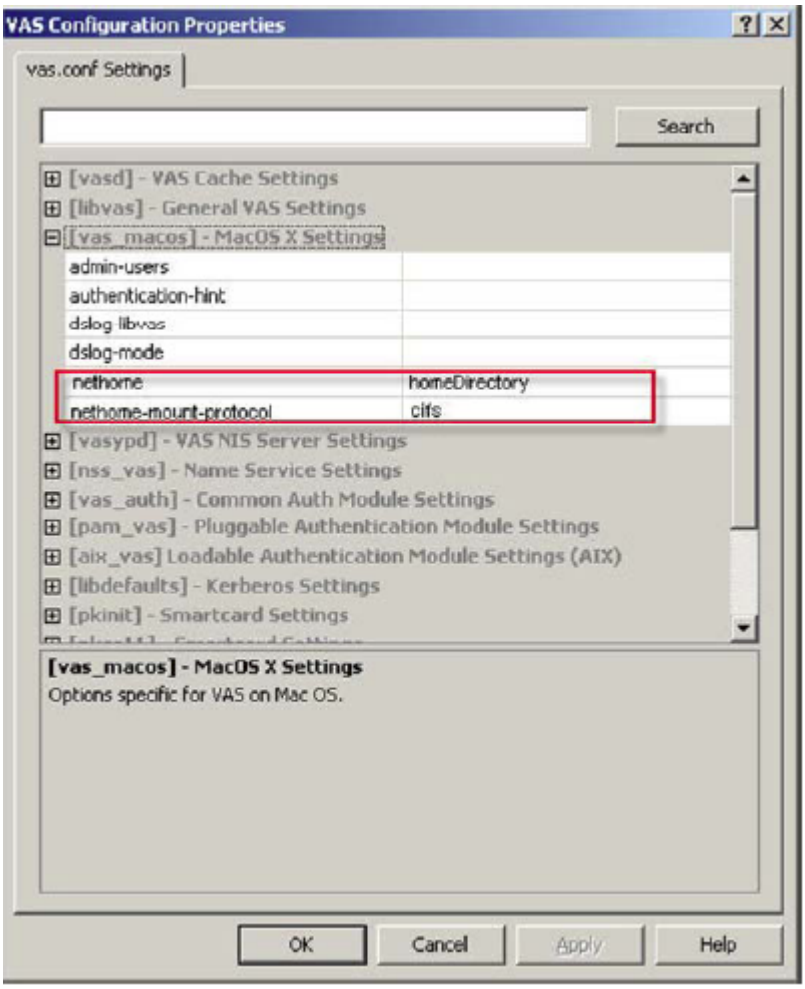
2. Under **User Path Expression**, specify the appropriate user attributes in the path portion of the server URL.

   For example, if you selected **Common Name** and then clicked **Insert Attribute**, the expansion macro for Common Name (%c) is inserted into your path expression. The path expression may have text and expansion macros, or it may just be a single expansion macro with no other text.

Configure automatic home folder mounting using Group Policy

During deployment, installation and join usually happen in a scripted fashion from the command line. It is still possible to configure home folder mounting without using the graphical join interface, either through modification of the `vas.conf` file or by setting the appropriate options in group polices that apply to your Mac OS X machines.

The two options that have bearing upon home directory mount behavior are `nethome` and `nethome-mount-protocol`. These options are set in the `vas.conf` policy.



The `nethome` is either the name of the user attribute where the UNC path is stored ("homeDirectory" or "profilePath"), or it is the server URL expression for all users (that is, `cifs://servername/sharename/%c`).

If the `nethome` is specified as an attribute name, you can specify whether the path is mounted by means of AFP or CIFS using the "nethome-mount-protocol" setting.

Setting either of these options has no effect on any Authentication Services platform other than Mac OS X, so you can safely set it on a domain-wide Unix settings policy. Creation or modification of group policies is accomplished using the Microsoft GPOE on any Windows administrative workstation.

Group permissions on auto-mounted home directories

For Authentication Services to resolve to a Windows SID to a Unix UID or GID, the user or group to whom that SID belongs must have had a UID or GID manually assigned to them. Or, in other words, you must Unix-enable the user or group on the *Unix Account* tab in

Active Directory Users and Computers. If a group or user has not been Unix-enabled, the Mac OS X machine will still assign a UID or GID to the user or group, but the Authentication Services agent software will not be able to resolve the a UID or GID.

To log into an Mac OS X machine, all users must be Unix-enabled so this normally only causes problems when dealing with group permissions on SMB-mounted home directories. It is not uncommon for the group owner of a network home location to be a group WITHOUT a Unix GID assigned. When a user's ability to access this directory relies on correct group membership, problems can arise. It is, therefore, best practice to Unix-enable all groups that are used for SMB File level permissions on network mounted home directories.

Mounting AFP shares

To mount AFP shares, you must have an AFP file server that knows about all your Active Directory users and credentials. You can easily accomplish this using third-party software that shares files from a Windows machine joined to your domain.

5

Special Mac OS X features

This section details two special Mac OS X features:

- Local Administrator Rights for Authentication Services Users
- Active Directory User Password Hint

Local administrator rights for Authentication Services users

Authentication Services allows you to give local administrator rights to Authentication Services users on individual Mac OS X systems. This gives a user the ability to administer his own system while still using Active Directory for authentication. It also allows Mac OS X system administrators "admin" access on Mac OS X systems without a shared local account.

Grant Authentication Services accounts administrator rights

To grant Authentication Services accounts administrator rights

1. Modify the `/etc/opt/quest/vas/vas.conf` file and add the following section to the Authentication Services configuration using a text editor:

   ```
   [vas_macos]
   admin-users = johnd@example.com
   ```

   For example, with the pico text editor, enter:

   ```
   $ sudo pico /etc/opt/quest/vas/vas.conf
   ```

NOTE: If there is already a [vas_macos] section in the `vas.conf` file, just add or modify the `admin-users` key following the existing section. You can also manage this option through Group Policy.

For the value of the admin-users key, use a comma-separated list of Active Directory User Principal Names (UPN) for Authentication Services users with administrator rights. The Domain Users option also supports groups of users.

2. Specify the group in the form, Domain\groupname.

   Either step ensures that Authentication Services processes the new configuration.

3. Verify that the configured users have administrator rights by checking their group memberships using the following command line (the example is for a user called *jdoe*):

   ```
   $ groups jdoe
   ```

   If jdoe was correctly configured to have local administrator rights, you see the *local admin*, *appserveradm*, and *appserverusr* groups listed in the output. The jdoe user is then able to use his user credentials for authorizing administrative tasks started from the System Preferences application.

Active Directory user password hint

The password hint is displayed for all Active Directory users when you have Mac OS X configured to provide password hints. The password hint is used to notify a user of a website where they can reset their password, or to remind a user that the account they are using requires a domain password. The default value for the authentication-hint is "Windows Domain Password".

Before Mac OS X will display authentication hints, you must enable the "Show password hints" option through the log in options.

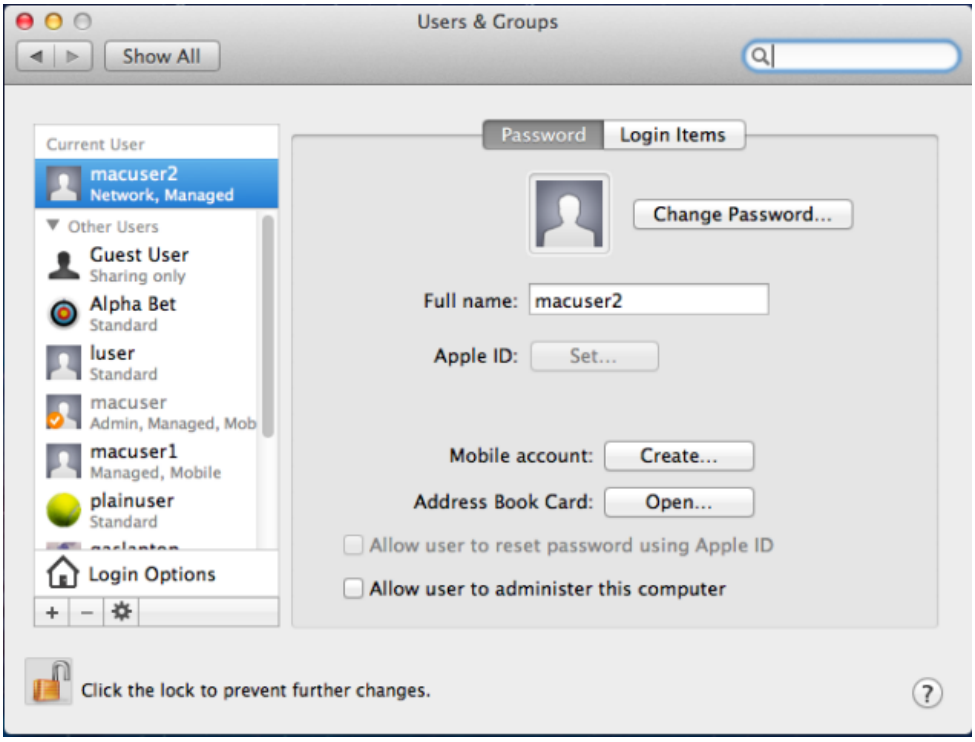
After enabling password hints, after several incorrect login attempts, the password hint displays.

You can manage this hint centrally on the domain controller through Group Policy.

NOTE: For security reasons, if a mapped user changes his password hint, it is intentionally reset to the generic Windows domain password hint the next time he logs in.

Configuring Apple FileVault disk encryption

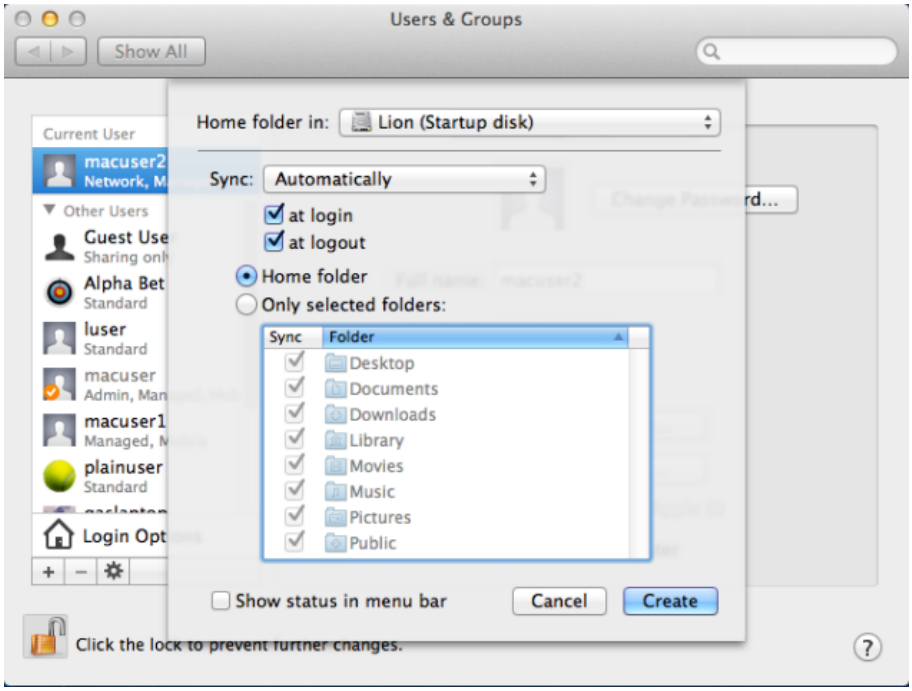
Authentication Services is compatible with Apple's FileVault disk encryption, introduced in Mac OS X 10.7. In order to use FileVault with an Active Directory user, you must first create a mobile account for that user on the Mac OS X client. A Mac OS X mobile account has a local home directory that can automatically sync with the user's network home directory.



To encrypt your disk

1. As an Active Directory user, open **System Preferences** and navigate to **Users & Groups**.
2. Click the **Lock** icon and enter administrator credentials to enable preference changes.

3. Click the **Create** button next to **Mobile account**.



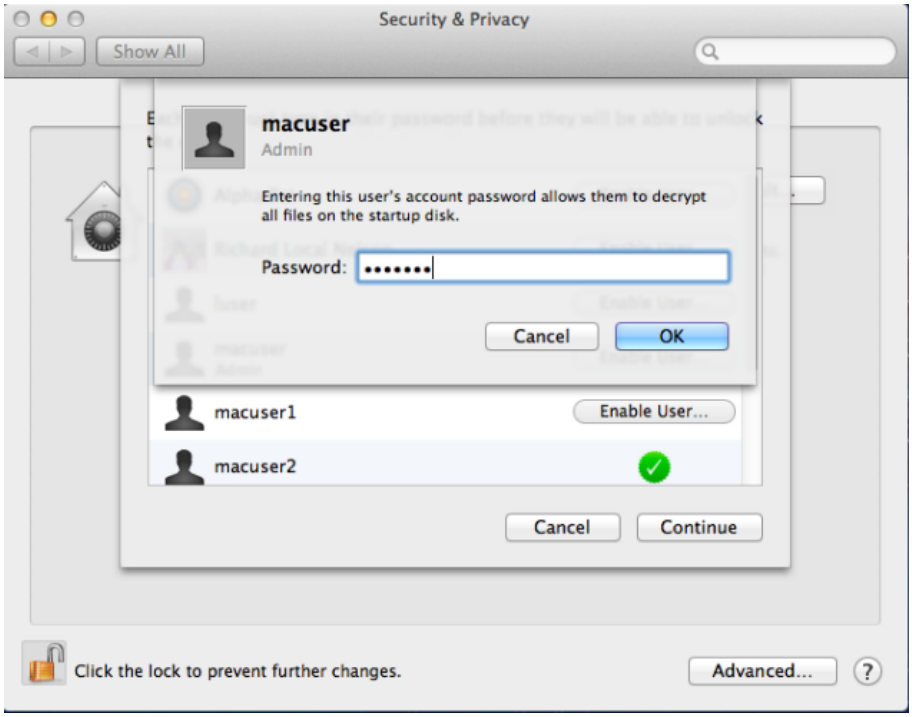
4. Select your preferred syncing and home folder location preferences in the pop-up menu and click **Create**.

   A popup message displays explaining that you must log out and log back in to create the local home folder.

5. Click **Create** and enter your password at the prompt.

6. Log back in and configure FileVault encryption.

7. From *System Preferences*, navigate to **Security & Privacy** and open the **FileVault** tab.
8. Click **Turn on FileVault** to begin the encryption process.



9. Select users (local users and mobile accounts) to enable them to unlock the encrypted disk at system startup.

   NOTE: Once you enable FileVault unlock for a user account, if you subsequently delete the account from Active Directory, you must also delete the local user account to disable FileVault unlock for that user.

10. Enter a password for each user you enable.

11. Take note of the recovery key on the following screen; store it somewhere yourself, and store it with Apple Support.

12. Restart your system to begin encrypting the drive.

    The encryption can take several hours, depending on the size of your disk, during which time you can continue using your computer. You can monitor the encryption process by returning to the **FileVault** tab in **Security & Privacy** preferences.

    After you enable FileVault, your Mac OS X will initially boot to an unencrypted disk partition and ask for your password to unlock the encrypted partition. Because this separate partition does not have access to Authentication Services and Active Directory, you must use your most recent locally cached password. Before the local cache is updated, if you need to unlock the encrypted disk after a password change, either use your old password or click the **Recover Key** to unlock the drive. Once the drive is unlocked, although it says you must reset your password, you can ignore the prompt and log in with your recently changed account password.

    You can find more information about FileVault in these articles by Apple Support:

    - *OS X Mountain Lion: Create and configure mobile accounts*
    - *OS X: About FileVault 2*

6

Authentication Services limitations on Mac OS X

There is some Authentication Services functionality that is limited by the Mac OS X system.

Limitations lists

- When using the command line su utility to become a Authentication Services user, the Authentication Services PAM module will not create a ticket cache for the new session because Authentication Services uses the CCacheServer process for Kerberos ticket cache management. Creating this ticket cache would inadvertently destroy any existing Kerberos tickets.
- If Authentication Services users who have custom home directory paths log into the system through the system login window and the parent directories for their home directory do not exist, the system home directory creation code incorrectly sets the ownership mode of all the home directory parent directories. This causes subsequent Authentication Services user logins to fail if they share the same home directory path. Their home directory will be created but it will be inaccessible to the user.

  Administrators should ensure that if they are using custom home directory paths, the parent directories are pre-created with a valid ownership and mode that allows all Authentication Services users to access those paths.
- The automatic ticket feature of Authentication Services does not currently work with non-file-based ccaches. Because Mac OS X uses API based ccaches, the ticket renewal utility will not work.

  NOTE: You can manually renew tickets with any utility that supports renewing tickets, such as Apple's Ticket Viewer.
- When using the Authentication Services mapped user feature, if a local user is mapped to a Authentication Services user and, at some point the user is unmapped (returned to a local account) you must reset the user's password.

7

Authentication Services Group Policy for Mac OS X

With Authentication Services you can manage your Mac OS X clients using Group Policy. Authentication Services includes Group Policy extensions to manage preferences just as you would with Workgroup Manager. In addition, Authentication Services supports custom policies based on Preference Manifests.

Authentication Services Group Policy includes support for Mac OS X. Using Authentication Services you can manage your Mac OS X through Group Policy. This eliminates the need to set up additional Mac OS X Servers for Mac OS X client management. Mac OS X policy settings are applied using Profile-based policies.

Profile-based policy takes advantage of the Configuration Profile infrastructure provided by Apple. Policy settings are defined in Group Policy and downloaded to Mac OS X clients where the settings are assigned to Configuraiton Profiles, which apply the settings to various configuration files on the Mac OS X.

Profile-based policy

Profile policy settings are divided into two categories: Workgroup Manager Settings and Preference Manifest Settings.

The Workgroup Manager settings are designed to look and feel like the Workgroup Manager application. If you are familiar with Workgroup Manager from Mac OS X server, it should be easy to transition to Group Policy. Settings for Applications, Classic, Dock, Energy Saver, Finder, Login, Media Access, Network, Parental Controls, Printing, Software Update, System Preferences, Time Machine and Universal Access are included. Authentication Services supports the *Never*, *Always* and *Once* policy application options. You can apply settings to users or computers. With standard Group Policy security filtering, you can restrict settings to specific groups of users or computers.

Authentication Services also includes support for Preference Manifest files. Preference Manifest files describe application settings you can manage centrally. Many standard Mac OS X Preference Manifest files are included by default such as iChat, Mail, Sidebar, Time Zone and iTunes. You can import additional Preference Manifest files at any time, increasing the number of applications and features that you can manage.

On the Mac OS X agent, Group Policy integrates with the Configuration Profile subsystem according to Mac OS X best practices. This ensures that policy settings are applied correctly and appropriately to each new release of Mac OS X.

Mac OS X management modes

The following management modes exist for Mac OS X policy settings:

Table 1: Mac OS X: Management modes

Mode	Description
Never	This mode means that the settings do not apply. This is equivalent to disabling the policy. This is the default mode.
Once	In this mode, policy settings are applied one time. Users can remove the Configuration Profile. This mode functions as a default value.
Always	In this mode, policy settings will always apply. Users cannot remove the Configuration Profile.

Workgroup Manager settings

Authentication Services provides Group Policy extensions that mirror the functionality available in Apple Workgroup Manager console. Workgroup Manager Settings are located in the `Mac OS X Settings` folder (or in the `Policies` folder, if you are using the new **Group Policy Management Editor**.)

For additional information about any of the topics covered in this section, refer to Chapter 10: *Managing Preferences* in the Mac OS X Server User Management manual available from Apple. Apple's User Management guide is written for Workgroup Manager, but most of the settings and information also apply to Group Policy for Mac OS X.

To open the properties of the various settings described in this section

1. Start the Group Policy Management Editor and navigate to the `Mac OS X Settings` directory under either `Computer Configuration` or `User Configuration`.
2. Double-click the **Workgroup Manager Setting** to open its properties.

Applications properties

The *Applications Properties* settings allow you to control access to specific applications and paths to applications using digital signatures. The *Applications*, *Widgets*, and *Front Row* tabs apply only to users of Mac OS X 10.5 or later. The *Legacy* tab applies only to users of Mac OS X 10.4.

You can apply *Application Properties* settings under both `Computer Configuration` and `User Configuration`.

Applications tab

The Application tab settings control which applications are allowed to execute on Mac OS X and support the following management modes: *Never*, *Always*. The Applications settings apply only to Mac OS X 10.5 and later.

Application restrictions are controlled by means of folder paths. Group Policy does not currently support application management using digital signatures, therefore to allow or prevent users from launching an application, add the application or the path to the application to one of two lists:

- **Disallow applications within these folders**.

  Add folders containing applications that you want to prevent users from opening. All applications in sub-folders of disallowed applications are also disallowed.

- **Allow applications within these folders**.

  Add folders containing applications that you want users to launch. If an application or path to the application appears in both the *disallow* and the *allow* lists, then the *disallow* list takes precedence and the user is not allowed to launch the application.

If an application does not appear in either of these lists, the user can not launch the application.

Click **Add** to open the New Application Item dialog. You can type the absolute Unix path or you can click **Remote Browse** to log into a remote Mac OS X machine (by means of SSH) and browse for the target folder. It displays recently specified paths. To reuse a recently specified path, double-click the item in the list.

NOTE: Both disallow and allow paths support the %HOME% macro-expansion to the user's Unix home directory. For example, to restrict a user from running applications in their home directory, specify %HOME%. This macros is only supported by user policies; machine policies do not support this macro type.

Front Row tab

Front Row is media center software for Mac OS X. Front Row tab settings allow you to control whether or not Front Row is allowed to execute and supports the following management modes: *Never*, *Always*.

Select **Allow Front Row**, to allow Front Row to execute on Mac OS X.

Legacy tab

The Legacy tab settings control which applications are allowed to execute on Mac OS X 10.4 systems and supports the following management modes: *Never*, *Always*.

To control application restrictions on newer systems use the settings on the Applications tab. Legacy Application settings support a single list of Unix paths. Applications residing in a path in the list are allowed to execute if you select the **User can open only these applications** option, or prevented from executing if you select the **User can open all applications except these** option. The path list functions as a deny list or an allow list, but not both.

The following options are also supported:

- **User can also open all applications on local volumes**

  Select to allow users to execute all applications on local volumes. When not selected, the application must be allowed through the application path list configuration.

- **Allow approved applications to launch unapproved applications**

  Select to allow approved applications to execute unapproved applications. When not selected, approved applications fail if they attempt to launch unapproved applications.

- **Allow Unix tools to run**

  Select to allow users to execute standard Unix command line tools. When not selected, you must explicitly allow Unix tools to run through the path list configuration.

Widgets tab

Widgets tab settings allow you to configure which Dashboard widgets are allowed to execute on Mac OS X clients. By default Authentication Services enables a set of common Dashboard widgets for management. If you want to customize the set of available Dashboard widgets you can edit the `widgets.xml` file which is installed into the Authentication Services installation directory. Widgets settings supports the following management modes: *Never*, *Always*.

If you select the **Allow only the following Dashboard widgets to run:** option, only the listed widgets are allowed. Click **Add** and **Remove** to configure the set of allowed widgets.

Classic Properties

The *Classic Properties* settings allows you to set Classic startup options, assign a `Classic System` folder, set sleep options for the Classic environment, and make specific Apple menu items available to users.

You can apply *Classic Properties* settings under both `Computer Configuration` and `User Configuration`.

NOTE: Classic configuration settings apply only to computers running Mac OS X 10.4.

Startup tab

Classic is the Mac OS 9 emulator for Mac OS X. Classic allows legacy Mac OS 9 applications to run on Mac OS X. Startup tab settings supports the following management modes: *Never*, *Always*.

Startup tab settings are used to configure the following behaviors of Classic:

- **Start up Classic at login**

  Normally Classic starts when a legacy application is launched. If you enable this option, Classic starts at login, making legacy applications appear more responsive when launched.

- **Warn at Classic startup**

  Select to trigger a warning when an application starts Classic.

- **Use this System Folder when Classic starts**

  Classic requires a full Mac OS 9 system installation. Select this option to specify which folder you want to contain the Mac OS 9 system. Specify the folder as an absolute path. Click **Remote Browse** to log into a remote Macintosh system by means of SSH and browse for a folder.

Advanced tab

Classic is the emulator for Mac OS 9. Advanced settings supports the following management modes: *Never*, *Always*.

The Advanced tab settings allow you to configure the following features of Classic:

- **Allow special startup modes**

  Select this option to allow users to explicitly start or restart Classic from the Classic preference pane.

- **Allow user to rebuild Desktop**

  Classic uses a Desktop environment cache to improve performance. Select this option to allow users to rebuild the Desktop environment. This can be helpful to resolve issues with icons and application associations. Leave this option deselected to disallow users from rebuilding the Mac OS 9 Desktop.

- **Use preferences from home folder**

  Select to store Classic-related preferences in each user's home directory rather than in the Classic system directory. The first time Classic starts after you select this option, users will see the following message: "Would you like the contents of these folders copied from your Classic system folder?" This is asking if you want to copy Preferences (and other folders) from the Mac OS 9 System Folder to your home directory. The process of copying may require a few minutes, and there is no indication of progress. Classic continues to start when this is finished.

- **Hide Chooser and Network Browser**

  Select to hide Chooser and Network Browser from users.

- **Hide Control Panels**

  Select to hide Control panels from users.
- **Hide other Apple Menu Items**

  Select this option to hide Apple Menu Items from users.
- **Put Classic to sleep when it is inactive for**

  Select to cause Classic to sleep (release OS resources) after a specified period of inactivity.

Dock properties

On Mac OS X the Dock is similar to a tool bar on other operating systems. In addition to showing which applications are running, the dock provides quick shortcuts to applications, folders and documents as well as system controls. Dock settings allow you to adjust the behavior of the user's Dock and specify which items appear in it.

You can apply Dock Properties settings under both `Computer Configuration` and `User Configuration`.

Dock Items tab

Dock Items tab settings control the applications, files and folders that are displayed on the user's Dock and support the following management modes: *Never*, *Once*, *Always*.

You can insert three types of items into the user's Dock: Applications, Documents and Folders. The **Applications** list controls which applications are inserted. The **Documents and Folders** list controls documents and folders that are inserted into the user's Dock. Click **Add** to select the items to insert in the Dock. You can drag the items within the list to change the order in which they appear on the Dock.

In addition to standard Unix paths, you can specify a network share by using the following syntax:

```
cifs://<server hostname>/<share name>
```

Folder paths support two types of macro-expansions. First, the %@ macro expands to the user's Unix name. Additionally, you can expand any active directory attribute using the %<*attributename*>% macro. For example, to add the user's network home directory to the dock, specify %homeDirectory%. You can get the value for any user attribute using the %<*attributename*>% macro. These macros are only supported by user policies; machine policies do not support either of these macro types.

NOTE: When adding a Dock icon for Documents and Folders on Mac OS X 10.4, it only opens a window to the mount point and not to sub-folders.

The following options are also supported:

- **Merge with the user's Dock**

  Select to merge the specified items into the user's Dock. If you do not select this option, the specified items replace the user's Dock.

- **Add other folders:**

  Select to add predefined folders to the user's Dock. Authentication Services supports `My Applications` and `Documents`.

Dock Display tab

Dock Display tab settings allow you to configure options that affect the visual display of the user's Dock and support the following management modes: *Never*, *Once*, *Always*.

The following options are supported:

- **Dock Size**

  Select to control the size of the *Dock* window on the user's Desktop.

- **Magnification**

  Select to control the size of magnification when the mouse cursor hovers over an item on the Dock.

- **Position on screen**

  Select this option to control where on the screen the Dock is anchored. Options include Bottom, Left and Right.

- **Minimize Using**

  Select to control the visual effect used when applications are minimized to the Dock. Options include Genie and Scaled.

- **Animate opening applications**

  Select to animate (bounce) the application icons on the Dock as the application loads.

- **Automatically hide and show the dock**

  Select to hide the Dock automatically. When you position the cursor over the Dock it displays itself automatically. Leave this option deselected leave the Dock visible at all times.

Energy Saver Properties

The Energy Saver Properties settings helps you save energy and battery power by managing wake, sleep, and restart timing.

You can apply Energy Saver Properties settings only under `Computer Configuration`.

Desktop tab

Desktop tab settings control energy usage settings for Mac OS X and supports the following management modes: *Never*, *Always*.

You can use preset settings by moving the slider anywhere from **Minimum Energy Usage** to **Maximum Performance**. When you set the slider to **Custom** you can customize all aspects of the energy usage settings.

The following Desktop Settings options are supported for both Mac OS X and Mac OS X Server. Settings on the *OS X* tab apply to Mac OS X workstations. Settings on the *OS X Server* tab apply to Mac OS X Servers.

- **Put the computer to sleep when it is inactive for**

  Configure how long you want the system to wait before putting the computer to sleep to save power. Inactivity means no keyboard or mouse input.
- **Put the display to sleep when the computer is inactive for**

  Select to control how long you want the system to wait before putting the display to sleep. Inactivity means no keyboard or mouse input.
- **Wake when the modem detects a ring**

  Select to configure the computer to wake from sleep when the modem detects a ring.
- **Wake for Ethernet network administrator access**

  Select to configure the computer to wake from sleep if an administrator attempts remote access.
- **Restart automatically after a power failure**

  Select to configure the computer to automatically start when power is restored after a power failure.
- **Put the hard disks to sleep when possible**

  Select to configure the system to attempt to power down hard disks.
- **Allow the power button to sleep the computer**

  Select to configure the computer to go to sleep when a user presses the power button.

Portable tab

Portable tab settings control energy usage settings for Mac OS X portable devices and support the following management modes: *Never*, *Always*.

You can use preset settings by moving the slider anywhere from **Minimum Energy Usage** to **Maximum Performance**. When you set the slider to **Custom** you can customize all aspects of the energy usage settings.

Authentication Services supports the following Portable Settings options for both Adapter and Battery powered situations. Settings on the Adapter tab apply when the portable device's power adapter is plugged in. Settings on the Battery tab apply when the portable device is running on battery power.

- **Put the computer to sleep when it is inactive for:**

  Select to control how long you want the system to wait before putting the computer to sleep to save power. Inactivity means no keyboard or mouse input.
- **Put the display to sleep when the computer is inactive for:**

  Select to control how long you want the system to wait before putting the display to sleep. Inactivity means no keyboard or mouse input.
- **Wake when the modem detects a ring**

  Select to configure the computer to wake from sleep if the modem detects a ring.
- **Wake for Ethernet network administrator access**

  Select to configure the computer to wake from sleep if an administrator attempts remote access.
- **Restart automatically after a power failure**

  Select to configure the computer to automatically start when power is restored after a power failure.
- **Put the hard disks to sleep when possible**

  Select to configure the system to attempt to power down hard disks.
- **Processor Performance**

  Select to control the processor performance. The higher the performance setting the more power used. Options include: Highest, Automatic and Reduced. Automatic will attempt to use reduced power when the computer is running on battery power.

Battery tab

Battery tab settings control battery status display and support the following management modes: *Never*, *Always*.

To show the battery status in the menu bar select the **Show battery status in the menu bar** option.

Schedule tab

Schedule tab settings control automatic startup and shutdown for Mac OS X workstations and servers; and, support the following management modes: *Never*, *Always*.

Schedule Settings allow you to configure managed computers to start up and/or shutdown according to a specific schedule. For example, you might configure certain computers to sleep on Friday night and wake up early Monday morning.

To force the computer to start up or wake, select the **Startup or wake** option and set the frequency and the time of day.

To force the computer to shut down or sleep check the box and select either **Shutdown** or **Sleep** option from the dropdown then set the frequency and time of day.

Finder properties

Finder is the Mac OS X Window manager and file system browser. Finder Settings allow you to configure the way Finder works.

You can apply Finder Properties settings under both `Computer Configuration` and `User Configuration`.

Preferences tab

Preferences tab settings control features and functionality of Finder and support the following management modes: *Never*, *Once*, *Always*.

Finder can operate in normal mode or simple mode. In simple mode, users cannot launch applications or files from a Finder window. They are limited to what is accessible from the Dock. In addition, users cannot create folders, delete files or mount network volumes in simple mode. To enable normal mode, select **Use Normal Finder**. To enable simple mode, select **Use Simple Finder**. If you select **Use Simple Finder**, you can not specify any other options because they do not apply to a simplified Finder environment.

The following options are supported:

- **Show these items on the desktop**

  Configures Authentication Services to display an icon on the user's Desktop for each selected item. Options include: **Hard disks**, **Removable media** and **Connected servers**.

- **New Finder window shows**

  Set the default view for *New Finder* windows. To show the user's home directory, select **Home**. To show the computer view including mounted volumes select **Computer**.

- **Always open folders in a new window**

  Select to configure Authentication Services to open a *New Finder* window each time a user opens a new window.

- **Always open windows in column view**

  Select to configure Authentication Services to automatically open new windows in column view.

- **Show warning before emptying the Trash**

  Select to configure Authentication Services to prompt users to confirm before moving items to the Trash.

- **Always show file extensions**

  Select to display file extensions in Finder views.

Commands tab

Commands tab Settings control which commands users are allowed to execute and support the following management modes: *Never*, *Always*.

The following options are supported:

- **Connect to Server**

  Select to enable users to launch a dialog to find servers on the network. If disabled, this functionality is not allowed.

- **Go to iDisk**

  Select to enable users to open their iDisk. If disabled, this functionality is not allowed.

- **Eject**

  Select to enable users to eject removable media and mounted volumes. If disabled, this functionality is not allowed.

- **Burn Disk**

  Select to enable users to write permanent information to CD or DVD. If disabled, this functionality is not allowed.

- **Go to Folder**

  Select to enable users to navigate to specific folders by typing a path name. If disabled, this functionality is not allowed.

- **Restart**

  Select to display the **Restart** command in the Apple Menu. If disabled, the **Restart** command is not available.

- **Shut Down**

  Select to display the **Shut Down** command in the Apple Menu. If disabled, the **Shut Down** command is not available.

Views tab

Views tab settings controls icon size and display in Finder and support the following management modes: *Never*, *Once*, *Always*.

You can configure three different types of views:

- **Desktop view**

  Controls the size and arrangement of icons on the desktop.

- **Default view**

  Controls the view settings of *Finder* windows.

- **Computer view**

  Controls the view settings of the *Computer* view which shows available volumes in Finder.

The following options are supported:

- **Icon Size**

  Select to control the size of icons displayed in Icon view.

- **Icon arrangement**

  Select to control the way icons display in Icon view. The following options are supported:

  - **Name** - arranges icons alphabetically by name.
  - **Modification Date** - Icons are arranged according to the last time the file was modified.
  - **Creation Date** - arranges icons according to when the file was created.
  - **Size** - arranges icons by file size.
  - **Kind** - groups icons according to file extensions.
  - **Snap to Grid** - arranges icons into a grid arrangement.

- **Use relative dates**

  In List View, specifies file dates relative to the current date.

- **Calculate folder sizes**

  Select to calculate folder sizes "on the fly".

- **Icon Size**

  In List View, icons can be displayed as either small icons (16x16 pixels) or large icons (32x32 pixels). Select this option to control which size to use in List View mode.

Login properties

The Login settings control the appearance and behavior of the Mac OS X login window.

You can apply Login Properties settings under both `Computer Configuration` and `User Configuration`. However, the Items tab is only available in `Users Configuration`.

Window tab

The Window tab settings of the Login Properties control the appearance of the login window such as the heading, message, which users are listed if the "List of users" is specified, and the ability to restart or shut down. Window tab settings supports the following management modes: *Never*, *Once*, *Always*.

The following options are supported:

- **Heading**

  Select an item to display at the top of the login window.

- **Message**

Enter a message to display in the login Window.

- **Style**

  Set the following options to modify the login window style:

  - **Name and password text fields**

    To only display the user name and password text boxes.

  - **List of users able to use these computers**

    To display a graphical list of users that are allowed to log in.

    NOTE: Users can click the account to use for log in and will be prompted for a password. You can set additional options to control which users are displayed in the list.

  - **Show Other**

    To allow users to log in using the name and password text fields.

  - **Show Restart**

    To display the restart button in the login window.

  - **Show Shut Down**

    To display the shut down button in the login window.

Options tab

The Options tab of the Login Properties controls miscellaneous login-related options and support the following Manage Modes: *Never*, *Always*.

The following options are supported:

- **Show password hint when needed and available**

  All Authentication Services users always have a password hint of "Active Directory Domain Password" by default. This hint is configurable in the Authentication Services configuration policy. Users are never allowed to set a password hint on a Authentication Services account. Local or non- Authentication Services accounts may have a password hint which was intentionally set by the user to remind them of their password.

- **Enable automatic login**

  Select to configure the operating system to boot directly to the desktop without presenting the user with a login screen. The operating system boots using the automatic login account configured locally under **System Preferences**, **Accounts**.

- **Enable console login**

  By default users can type **>console** at the login window to drop to a terminal login. This setting allows you to disable the ability to drop to a terminal login.

- **Enable Fast User Switching**

  Select to display the logged in user's name in the right-hand corner of the desktop. Selecting on the user name allows the user to switch to another account without logging out of their current desktop session.

- **Log out users after X minutes of inactivity**

  Select to automatically log out a user if he has been inactive for the specified number of minutes.

- **Local administrators may refresh or disable management**

  Select to allow administrators to disable or refresh login window management settings.

- **Set computer name to computer record name**

  This setting affects the computer's Bonjour name. The new Bonjour name is name-#.local where name is the computer record name you specify and # uniquely identifies the computer if there are several computers with the same Bonjour name.

- **Enable external accounts**

  Select to store external accounts on removable storage devices such as a thumb-drive. You must insert the removable device before an external account can log in.

- **Enable guest account**

  Select to enable a guest account to log in without a password. When the guest user logs out, the home directory, documents and settings are removed from the system.

- **Start screen saver after X minutes**

  Select to modify your screen saver setting.

Access tab

The Access tab settings of the Login Properties control which users are allowed to log in and support the following management modes: *Never*, *Always*.

Authentication Services provides unified access control across all supported Unix platforms including Mac OS X. Because of this, you should use the Authentication Services access control policies to manage access control. The access control policies are found in the `Access Control` node in the Quest Software folder under **Unix Settings.**

The following option is supported:

- **Local-only users may login**

  Select to allow local users to log in; leave this option deselected to only allow Active Directory users to log in.

Scripts tab

The Scripts tab settings of the Login Properties control scripts that run at login and logout; and, support the following management modes: *Never*, *Always*.

You can specify shell scripts that you want to execute when a user logs in or out on Mac OS X. Scripts are stored in the policy settings so you can browse to local files or remote hosts to select the script to use. Scripts configured through Group Policy run as root with the trust value of FullTrust.

NOTE: Test scripts thoroughly before deploying them with Group Policy.

The following options are supported:

- **Login script**

  Specify the script to execute when the user logs in.

- **Also execute the client computer's LoginHook script**

  Select to allow the LoginHook script to execute. The LoginHook script is a locally configured script that runs at login.

- **Log-Out script**

  Specify the script to execute when the user logs out.

- **Also execute the client computer's LogoutHook script**

  Select to allow the LogoutHook script to execute. The LogoutHook script is a locally configured script that runs at log-out.

Items tab

The Items tab settings of the Login Properties, control items that are started automatically when a user logs in and support the following management modes: *Never*, *Once*, *Always*.

NOTE: The Items tab is only available in `Users Configuration`.

Refer to Add login items to run items automatically when a user logs in.

The following options are supported:

- **User may add and remove additional items**

  Select to allow users to add and remove additional items by means of local configuration. You can only configure this option if the management mode is set to **Always**.

- **User may press Shift to keep items from opening**

  Select to allow users to press shift to prevent items from opening automatically. You can only configure this option if the management mode is set to **Always**.

- **Merge with user's items**

  Select to merge the configured items with the user's items. You can only configure this option if the management mode is set to **Once**.

Add login items

NOTE: This procedure shows you how to add an item that starts automatically from the *Items* tab.

To add login items

1. Click **Add** to type the full path to the volume, document, folder or application. Alternatively, you can click **Browse** to browse for the path to the item on a remote Mac OS X system. Items open in the order they are listed.
2. Select the **Hide** option and to start the item in a minimized state on the Dock. This prevents screen clutter when starting several items while still making the items easily accessible.
3. Click **Apply**.

Media Access Properties

The Media Access Properties settings allows you to control settings for and access to CDs, DVDs, the local hard disk, and external disks (for example, floppy disks and FireWire drives).

You can apply Media Access Properties settings under both `Computer Configuration` and `User Configuration`.

Media Access tab

The Media Access tab settings control access to media devices and support the following management modes: *Never*, *Always*.

The following options are supported:

- **Disc Media**

  Select which removable disc media devices you want to allow users to access. If you select **Require Authentication**, the user needs to provide credentials before he can access the disc media.

- **Other Media**

  Select other media devices you want to allow users to access. If you select **Require Authentication**, the user needs to provide credentials before he can access the media. If you select **Read-Only**, the user cannot write to the media.

- **Eject all removable media at logout**

  Select to automatically eject all removable media when the user logs out.

Network properties

Network Properties settings allow you to configure settings for hosts and domains to bypass and disable Internet Sharing, AirPort, and Bluetooth.

You can apply Network Properties settings under both `Computer Configuration` and `User Configuration`. However, you can only apply the Sharing & Interfaces functionality in the `Computer Configuration` node.

Sharing & Interfaces tab

The Sharing & Interfaces tab settings of the Network Properties control access to network features and support the following management modes: *Never*, *Always*.

Sharing & Interfaces settings are only configurable in the `Group Policy Computer Configuration` node.

The following options are supported:

- **Disable Internet Sharing**
- **Disable AirPort**
- **Disable Bluetooth**

Parental Controls Properties

The Parental Controls Properties allow you to hide profanity in Dictionary, limit access to websites, or set time limits or other constraints on computer usage.

You can apply Parental Controls Properties settings under both `Computer Configuration` and `User Configuration`.

Content Filtering tab

The Content Filtering tab settings of the Parental Controls Properties control websites that users are allowed to access and support the following management modes: *Never*, *Always*.

Content Filtering settings apply to Mac OS X 10.5 and higher only.

The following options are supported:

- **Hide profanity in Dictionary**

  Select to hide profanity in the Dictionary application.
- **Limit access to websites by**

  Select to filter websites explicitly or by using the built-in adult content filter.

Filter content explicitly

NOTE: This procedure shows you how to set up the Parental Controls content filter to allow access only to websites you specify.

To filter content explicitly

1. Open the **Parental Controls Properties** and select the **Content Filtering** tab.
2. Select the **Always** management mode.
3. Check **Limit access to websites by**.

4. Select **allowing access to the following websites only** from the drop-down box.

   The view now shows a single box with buttons on the right side.
5. Allowed websites will be displayed in the user's browser. You can organize the websites using folders. Click **Add folder** to add a folder. Type the name of the folder and press **Enter**.
6. Click **Add website**.

   The Web Site dialog appears. Here you can type the display name for the web site and the Web address.
7. Type the web site display name in the box labeled **Web site title** type the web site URL in the box labeled **Address**.
8. Click **OK**.

   The new website is displayed under the folder. You can drag items to move them to different folders.
9. Add additional folders and websites as needed, then click **OK** to save settings and close the Parental Controls dialog.

Filter content with the built-in adult content filter

To filter content with the built-in adult content filter

1. Open the **Parental Controls Properties** and select the **Content Filtering** tab.
2. Select the **Always** management mode.
3. Check **Limit access to websites by**.
4. Select **trying to limit access to adult websites** from the drop-down box.

   The view now shows two list boxes with buttons on the right.
5. The system tries to limit access to adult websites using a built-in algorithm. You can override the behavior of the system filter by specifying websites that should always be allowed or always be denied.
6. To allow a site, click the **Add** button under the *Always allow sites at these URLs* heading. Type the URL of the website and press **Enter**.

   A new website is added to the allow list.
7. To deny a site, click the **Add** button under the *Never allow sites at these URLs* heading. Type the URL of the website and press **Enter**.
8. Click **OK** to save settings and close the Parental Controls Properties dialog.

Time Limits tab

The Time Limits tab settings of the Parental Controls policy, control the amount of time and time of day that users are allowed to access the system. Time Limits settings supports the following management modes: *Never*, *Always*.

Time Limits settings apply to Mac OS X 10.5 and higher only.

The following option is supported:

- **Enforce limits**

  Select to enforce the configured time limits on all client computers.

  NOTE: You can configure the number of hours the computer may be accessed as well as the time window that the computer is available for use.

Configure time allowances

NOTE: This procedure shows you how to configure the number of hours the host computer may be used each day.

To configure time allowances

1. Open the **Parental Controls Properties** and select the **Time Limits** tab.
2. Select the **Always** management mode.
3. Click the **Enforce limits** option.
4. Select the **Allowances** tab.
5. To limit computer usage during the week, click the **Limit computer use to** option in the **Weekdays** box and move the slider to the maximum number of hours the host can be used during the week. You can specify any amount of time between 30 minutes and 8 hours in half-hour increments.
6. To limit computer usage on the weekend, click the **Limit computer use to** option in the **Weekends** box and move the slider to the maximum number of hours the host can be used on weekends. You can specify any amount of time between 30 minutes and 8 hours in half-hour increments.
7. Click **OK** to save settings and close the Parental Controls Properties dialog.

Configure time curfews

NOTE: This procedure shows you how to configure the number of hours the host computer may be used each day.

To configure time curfews

1. Open the **Parental Controls Properties** and select the **Time Limits** tab.
2. Select the **Always** management mode.
3. Click the **Enforce limits** option.
4. Select the **Curfews** tab.
5. To set the window of time that the computer cannot be accessed during the week click the **Sunday through Thursday** option. Set the window start time in the **From** box and the end time in the **to** box.

   Users will not be able to access the computer during the configured time window during the work week.

6. To set the window of time that the computer cannot be accessed on weekends click the **Friday and Saturday** option. Set the window start time in the **From** box and the end time in the **to** box.

   Users will not be able to access the computer during the configured time window on the weekends.
7. Click **OK** to save settings and close the Parental Controls Properties dialog.

Printing properties

Printing properties allow you to specify network printers you want to configure for use on client computers.

You can apply Printing Properties settings under both `Computer Configuration` and `User Configuration`.

Printers tab

The Printers tab settings of the Printing Properties, control printers that are configured for use on client computers and support the following management modes: *Never*, *Always*.

Printers tab settings allow you to set up printers that will be available on client computers.

The following options are supported:

- **Allow printers that connect directly to user's computer**

  Select to allow printing to printers that connect directly to the user's computer through FireWire or USB ports etc.
- **Require an administrator password**

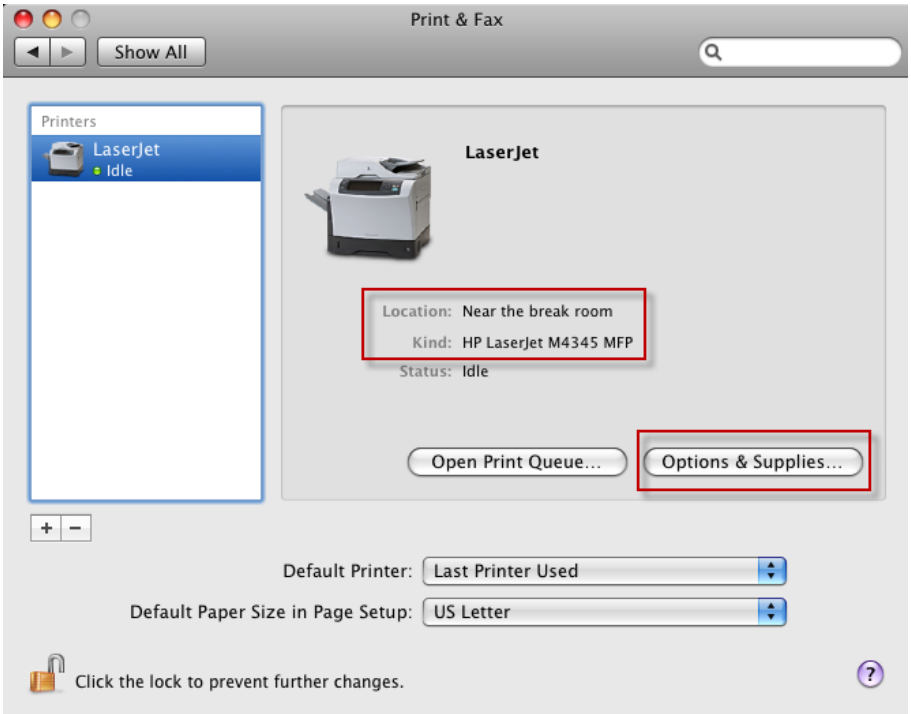
  If you have selected the **Allow printers that connect directly to user's computer** option, select this option to require an administrator password in order to print to a printer that is connected directly.

Add a printer

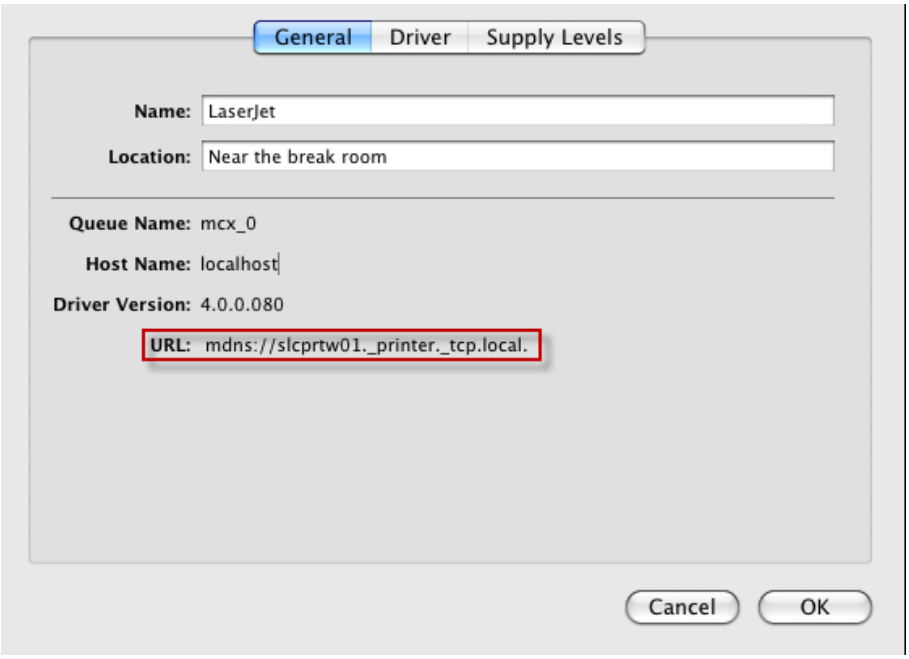
NOTE: This procedure shows you how to add a printer that will be available on Mac OS X clients.

To add a printer

1. In order to determine the proper printer settings the best practice is to first configure the printer on a single Mac OS X host system. Add the printer as instructed in the Mac OS X documentation and verify that you can print to it. Once you have set up the printer open the printer properties and make a note of the following settings: Name, Location, Kind and URL. The following screen shots show where to find these settings:



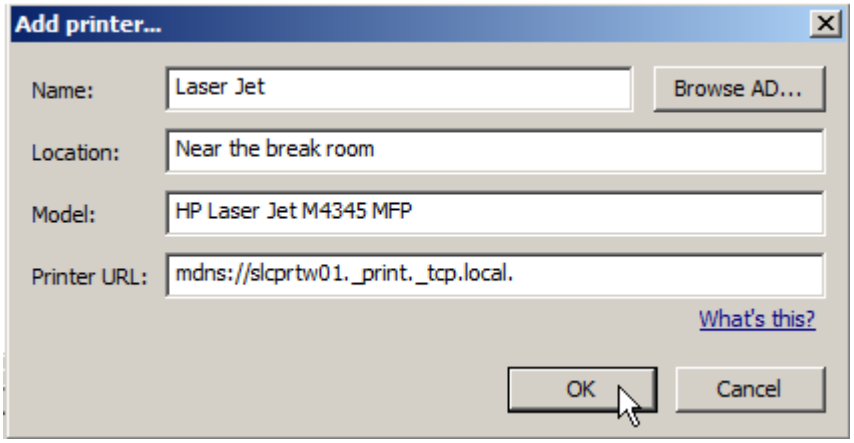
Click the **Options & Supplies** button to determine the URL:



This is all of the information you will need in order to configure the printer for all of your Mac OS X systems using Group Policy.

2. In Group Policy Management Editor, open the **Printing** policy (**Computer Configuration** | **Policies**| **Mac OS X Settings** | **Workgroup Manager Settings**) and select the **Printers** tab.
3. Select the **Always** management mode.

4. Click **Add** to add a new printer to the policy. The Add printer dialog appears. Enter the Name, Location, Model and Printer URL, then click **OK**. The best way to determine the printer URL is to configure a printer on a Mac OS X client and enter the URL specified in the Options and Settings dialog. (See step 1.)



   You can also add SMB printers by browsing for the printer in Active Directory.
5. If you want the selected printer to be the default printer click **Make Default**.
6. If you want to require the user to enter an administrator password before printing to the selected printer, click the **Require an administrator password** option.
7. Click **OK** to save settings and close the Printing dialog.

Footer tab

The Footer tab settings of the Printing Properties control footer display and formatting; and, support the following management modes: *Never*, *Always*.

Footers are additional information appended at the bottom of each printed page containing the date and the name of the user that initiated the print job.

The following options are supported:

- **Print Page Footer**

  Select to enable page footers.
- **Include MAC address**

  Select to include the client computer's network card MAC address in the footer information when page footers are enabled.
- **Font name**

  Select the page footers font name.
- **Font size**

  Select the page footers font size.

Software Update properties

The Software Update policy allows you to configure the Software Update server that managed clients use for downloading updates.

You can apply Application Properties settings under both `Computer Configuration` and `User Configuration`.

Software Update tab

The Software Update tab settings of the Software Update Properties control the Software Update server that managed clients use to download updates. Software Update settings supports the following management modes: *Never*, *Always*.

You can cache software updates on your local intranet using a local Software Update server. This can help reduce network bandwidth usage and speed update deployment in your network. Use this setting to instruct managed clients to use the local Software Update server.

The following option is supported:

- **Software Update server to use**

  Specify the URL of the software update server. The URL must be in the form http://<*server hostname*>:< *port* >/index.sucatalog

System Preferences properties

The System Preferences Properties allow you to control which items appear in the System Preferences of managed clients. This allows you to restrict which System Preferences configurations users can access.

You can apply System Preferences Properties settings under both `Computer Configuration` and `User Configuration`.

System Preferences tab

The System Preferences tab settings of the System Preferences Properties control which items appear in System Preferences on managed clients. System Preferences settings supports the following management modes: *Never*, *Always*.

You can control which items appear in System Preferences on managed clients. The System Preferences tab displays a list of System Preferences items. Select to place or clear the check mark in the **Show** column next to the item that you want to show or hide. Click **Show All** to select all items or **Show None** to clear all items.

Time Machine properties

The Time Machine Properties allow you to control the Time Machine application which provides network backups of installed applications, preferences, documents and local account data. For more information about Time Machine, refer to documentation provided by Apple.

You can apply Time Machine Properties settings only under the `Computer Configuration`.

Time Machine tab

The Time Machine tab settings control the Time Machine application and support the following management modes: *Never*, *Always*.

Time Machine is an application that performs network backup of local machine applications and data.

The following options are supported:

- **Backup Server**

  Specify the URL of the Time Machine backup server in the form: afp://someserver.company.com/Backups/. (Refer to the Apple documentation for more information about AFP and Time Machine backup servers.)

- **Back up**

  Specify which volumes to back up. You can choose to back up **Startup volume only** or **All local volumes**.

- **Skip system files**

  Select to skip system files. System files are operating system files installed when you install Mac OS X. Selecting this option significantly reduces the amount of storage space used for backups. However, if you do not back up system files, you will need to install the operating system when performing a full restore.

- **Backup automatically**

  Select this option to force automatic backups.

- **Limit total backup storage to**

  Enter the backup storage limit in megabytes. If the backup limit is reached, no more data is backed up.

Universal Access properties

The Universal Access settings allow you to set up and manage settings for users with special needs.

You can apply Universal Access Properties settings under both `Computer Configuration` and `User Configuration`.

Seeing tab

The Seeing tab setting of the Universal Access Properties control visual display and desktop zooming and support the following management modes: *Never*, *Once*, *Always*.

Options on the Seeing tab help users with visual impairments work more effectively. To further customize the user's display, you can set Finder Views preferences to control the size of icons in Finder windows, and use Dock Display preferences to enlarge or magnify icons in the user's Dock.

The following options are supported:

- **Turn on Zoom**

  Select to enable Zooming. You can control the **Min Zoom** and **Max Zoom** levels. Select the **Show preview rectangle when zoomed out** option to display a preview window on the user's desktop. Select the **Smooth images** option to improve the graphical quality.

- **Switch to**

  Select to switch the visual display to **White on Black** or **Grayscale**.

  The Preview shows an example of what the user's desktop will look like when you select one of these options.

Hearing tab

The Hearing tab settings of the Universal Access Properties control visual alerts and support the following management modes: *Never*, *Once*, *Always*.

The following option is supported:

- **Flash the screen whenever an alert sound occurs**

  Select to configure the screen to flash whenever an audible alert sounds. This feature is designed to aid hearing-impaired users or users that don't have an audio device enabled.

Keyboard tab

The Keyboard tab settings of the Universal Access Properties control keyboard functionality and support the following management modes: *Never*, *Once*, *Always*.

Keyboard tab settings are available to help users cope when they have difficulty pressing more than one key at a time or repeated keystrokes.

The following options are supported:

- **Sticky keys**

  Select to treat a sequence of modifier keys as a key combination. For example, press **Shift** then **A** to simulate Shift + A. Press a key twice to simulate holding it down.

Press **Shift** twice, then press **Command** then press **O** to simulate Shift + Command + O.

- **Beep when a modifier key is set**

  Select to sound an audible alert when a modifier key is set.

- **Display pressed keys onscreen**

  Select this option to display active modifier keys on screen.

- **Slow keys**

  Slow keys help users who press keys for too long or accidentally press keys. If you enable Slow Keys, you must hold the key down for the duration of the acceptance delay in order for the computer to accept a keystroke.

- **Use click key sounds**

  Select this option to play a sound when you press a key and play a different sound when the computer accepts the keystroke.

- **Acceptance delay**

  Move the slider to control the duration you must press a key down before the computer accepts the keystroke.

Mouse tab

The Mouse tab of the Universal Access Properties controls mouse functionality. Universal Access settings supports the following management modes: *Never*, *Once*, *Always*.

The following options are supported:

- **Mouse Keys**

  Select to allow users to use the arrows on the keypad in place of the mouse. This option is for users that have difficulty using the mouse.

- **Initial Delay**

  Move the slider to adjust how soon the mouse pointer begins to move.

- **Maximum Speed**

  Adjust the slider to control the maximum speed of the mouse pointer.

Options tab

The Options tab of the Universal Access Properties controls miscellaneous Universal Access options and support the following management modes: *Never*, *Always*.

NOTE: The Options tab is only available under the `Computer Configuration`.

The following option is supported:

- **Enable access for assistive devices**

  Select to enable managed users to turn on assistive devices such as text readers.

Wireless User Profile properties

Wireless settings allow you to configure networks and profiles used by AirPort on Mac OS X systems.The Wireless Profile Properties settings allow you to control wireless user profiles for Mac OS X.

To open the Wireless Profile properties page

1. In the Group Policy Object Editor, navigate to **User Configuration | Policies | Mac OS X Settings | Profile Manager Settings**.

   Wireless Networks apply only to users.
2. Double-click the **Wireless Networks** node.

Add wireless profiles

The Wireless Profiles tab settings control user options associated with wireless networks.

To add wireless profiles

1. From the Wireless Networks tab, click **Add** to open the Wireless Network dialog.
2. Enter the name of the wireless profile in the **Name** box.
3. Enter the SSID of the wireless network to which this profile applies in the **SSID** box.
4. Select the type of wireless network from the **Type** drop-down list.
5. Select the authentication type options that apply to this profile from the **Authentication** list.
6. If you want users to be prompted for their password each time they connect to a wireless network, select the **Always prompt for password** option.
7. Click the **Up** or **Down** buttons to reorder the wireless profiles.

   Wireless profiles are added to the user profiles list on Mac OS X systems in the order listed in the policy.

Preference Manifest settings

The Preference Manifests node lists applications and settings that you can manage using preference manifests. Policy items contained in this node are specific to the Macintosh operating system. A preference manifest is a file that describes application settings and makes them manageable. Application developers create preference manifest files to make their application's settings available for management through the **Preference Manifests** node.

When you install Group Policy console extensions, it creates preference manifests in `sysvol` at the following location:

```
Policies\Quest Software\Preference Manifest
```

In order to reduce GPO size, Preference Manifest files are stored in the GPT under the `Policies\Quest Software\Preference Manifest` folder. All of the Preference Manifest files found there are displayed in the **Preference Manifests** node. If the folder does not exist in the GPT, Preference Manifest files are loaded from the local installation directory.

Apple provides preference manifests for many built-in applications and systems. Group Policy includes preference manifests for Microsoft Office applications and other common third-party applications. You can also import custom preference manifests for policy configuration. The Authentication Services installation process adds Mac OS X, Workgroup Manager, and Preference Manifest Settings nodes to both the Computer Configuration and User Configuration nodes and stores all the Authentication Services for Mac OS X Desktop policies there.

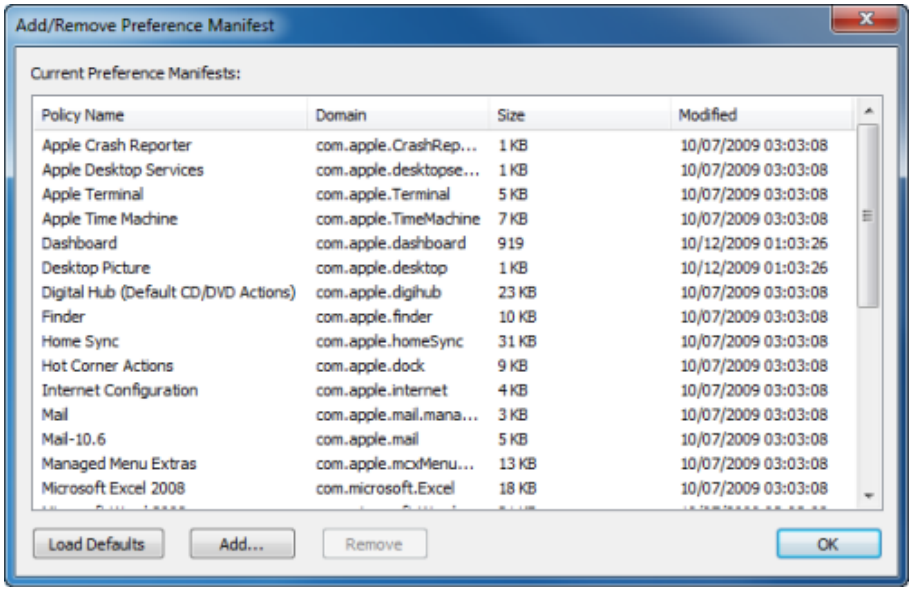
Add a preference manifest

You can add a preference manifest file to the Preference Manifests node in Group Policy Object Editor (GPOE)

To add a preference manifest

1. Right-click on the **Preference Manifests** node and select **Add/Remove Preference Manifests** from the menu.

   The Add/Remove Preference Manifest dialog is displayed.



2. Click **Add** to browse for the preference manifest file that you want to load.
3. Click **Load Defaults** to reset the list to the default set of preference manifests.
4. Click **Remove** to remove the selected preference manifests.
5. Click **OK** to save changes and close the Add/Remove Preference Manifest dialog.

   The Preference Manifest view is updated to reflect the changes.

8

Certificate Autoenrollment

Certificate Autoenrollment is a feature of Authentication Services 4.1 based on Microsoft Open Specifications. Certificate Autoenrollment allows Mac OS X/macOS® clients to take advantage of existing Microsoft infrastructure to automatically enroll for and install certificates. Certificate policy controls which certificates are enrolled and what properties those certificates will have.

With Certificate Autoenrollment, a public/private key pair is automatically generated according to certificate template parameters defined in Group Policy. The public key is sent to the Certification Authority (CA) and the CA responds with a new certificate corresponding to the public key which is installed along with the private key into the appropriate system or user keychain on the Mac client.

You can use Group Policy to automatically configure which certificate enrollment policy servers to use for Certificate Autoenrollment and to periodically run Certificate Autoenrollment.

This section explains the system requirements for Certificate Autoenrollment and walks you through policy setup as well as client-side usage and troubleshooting.

Certificate Autoenrollment on Mac OS X/macOS

Most of the Certificate Autoenrollment code is implemented in Java. After this code has successfully requested a certificate from a CA, it invokes platform-specific code to store the private key and certificate in a suitable way for the operating system or for particular applications. This platform-specific code is implemented as a shell script, `certstore.sh` in the `/var/opt/quest/vascert/script` directory.

The `certstore.sh` script is a platform-agnostic front end that chooses and loads a platform-specific back end script. For Mac OS X®/macOS®, the back end script is `certstore-mac.sh`. This script provides a fully functional implementation that uses the `/usr/bin/security` tool to integrate with Max OS X/macOS keychains.

Certificate Autoenrollment requirements and setup

Prior to installing One Identity Certificate Autoenrollment, ensure your system meets the following minimum hardware and software requirements:

Table 2: Certificate Autoenrollment: Minimum requirements

Component	Requirements
Operating system	Mac OS X®/macOS® 10.8.3 or higher
Java unlimited strength policy files	See Java requirement: Unlimited Strength Jurisdiction Policy Files on page 75
Authentication Services	One Identity Authentication Services version 4.1.2
Additional software	Certificate Autoenrollment depends on services provided by a Microsoft Enterprise Certificate Authority (CA) in your environment. In addition to Active Directory and an Enterprise CA, you must install the following software in your environment: • Microsoft Certificate Enrollment Web Services In order for Certificate Autoenrollment to function on client computers, you must configure the following policies: • Certificate Services Client - Auto-Enrollment Group Policy • Certificate Services Client - Certificate Enrollment PolicyGroup Policy • Certificate Templates Additionally, you must configure Java 1.6 or higher as the default JVM for your system. NOTE: Install JRE (Java Runtime Environment) on all platforms other than macOS; macOS requires JDK (Java Development Kit). Typing `java` on the command line provides instructions. • For Linux/UNIX operating systems, install JRE 1.6 or higher. • For Mac OS X (that is, your operating system tells you to get it from Apple), install what Apple provides (JRE). • For macOS (that is, your operating system tells you to get it from Oracle), install the JDK.

Component	Requirements
Rights	Enterprise Administrator rights to install software and configure Group Policy and Certificate Template policy (only if Certificate Autoenrollment is not already configured for Windows hosts in your environment.)

Java requirement: Unlimited Strength Jurisdiction Policy Files

By default, most JRE and JDK implementations enforce limits on cryptographic key strengths that satisfy US export regulations. These limits are often insufficient for Certificate Autoenrollment and may lead to "java.security.InvalidKeyException: Illegal key size" failures. The "Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files" can be installed to remove these limits and enable Certificate Autoenrollment to function properly.

Do I need the Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files?

In general the answer is: Yes, these files are needed.

Java 9 and above do not require these files, but Java 6, 7 and 8 rely on these files.

In some environments, Certificate Autoenrollment may be able to function correctly without these files. Typically, these are older environments such as Windows Server 2008 R2 with Java 6 on Mac OS X 10.9. However, even if one of these environments works now, it may no longer work in the future when its components are upgraded to newer releases. Therefore, it is prudent to install the policy files even if they are not needed at present.

Obtaining and installing the policy files

For Java implementations from IBM, the policy files are usually bundled with the JDK but not the JRE, so it may be more convenient to install the JDK rather than just the JRE. Once the JDK is installed its `demo/jce/policy-files/unrestricted` directory should contain two JAR files:

- `local_policy.jar`
- `US_export_policy.jar`

Use these files to replace the corresponding JAR files in the `jre/lib/security` directory of the JDK. Alternatively, the "Unrestricted SDK JCE policy files" can be downloaded from ibm.com.

For Java implementations from Sun, Oracle and Apple and for OpenJDK implementations, the policy files must be downloaded from Oracle. Each major Java version requires its own policy files:

- Java 6: http://www.oracle.com/technetwork/java/javase/downloads/jce-6-download-429243.html
- Java 7: http://www.oracle.com/technetwork/java/javase/downloads/jce-7-download-432124.html
- Java 8: http://www.oracle.com/technetwork/java/javase/downloads/jce8-download-2133166.html

Each of these downloads is a zip file that includes a README.txt and two JAR files, `local_policy.jar` and `US_export_policy.jar`. Use these JAR files to replace the corresponding files in the JRE or JDK:

- JRE: The `lib/security` directory usually holds these files.
- JDK: The `jre/lib/security` directory usually holds these files.

Installing certificate enrollment web services

The following procedures walk you through the installation and configuration of the required components. If Certificate Autoenrollment is already configured for Windows hosts in your environment, you can skip to Using Certificate Autoenrollment on page 79.

To perform these procedures, you need Enterprise Administrator rights to install software and configure Group Policy and Certificate Template policy.

NOTE: Microsoft has documented all of the steps to install and configure certificate enrollment Web services.

To set up certificate enrollment web services

1. Review the requirements as specified by Microsoft at: http://technet.microsoft.com/en-us/library/dd759243.aspx.
2. Follow the instructions at: http://technet.microsoft.com/en-us/library/dd759241.aspx to install the Certificate Enrollment Web Service.
3. Follow the instructions at: http://technet.microsoft.com/en-us/library/dd759214.aspx to install the Certificate Enrollment Policy Web Service.
4. Follow the instructions at: http://technet.microsoft.com/en-us/library/dd759140.aspx to configure server certificates for HTTPS.

Certificate enrollment Web services are now installed. Next, you will configure policy settings to enable Certificate Autoenrollment.

Configuring Certificate Services Client - Certificate Enrollment Policy Group Policy

If you are using Group Policy, you must configure the Certificate Enrollment Policy Web Service group policy setting to provide the location of the Web service to domain members. Otherwise, you must manually configure the server URL on each system as explained in Using Certificate Autoenrollment.

To configure certificate enrollment policy

1. On the Web server that hosts the Certificate Enrollment Policy Web Service, open Server Manager.
2. In the console tree, expand **Roles**, and then expand **Web Server (IIS)**.
3. Click **Internet Information Services (IIS) Manager**.
4. In the console tree, expand **Sites**, and click the Web service application that begins with *ADPolicyProvider_CEP*.

   NOTE: The name of the application is ADPolicyProvider_CEP_ *AuthenticationType* where *AuthenticationType* is the Web service authentication type.
5. Under **ASP.NET**, double-click **Application Settings**.
6. Double-click **URI**, and copy the URI value.
7. Click **Start**, type `gpmc.msc` in the **Search programs and files** box, and press **ENTER**.
8. In the console tree, expand the forest and domain that contain the policy that you want to edit, and click **Group Policy Objects**.
9. Right-click the policy that you want to edit, and then click **Edit**.
10. In the console tree, navigate to **User Configuration | Policies | Windows Settings | Security Settings** and click **Public Key Policies**.
11. Double-click **Certificate Services Client – Certificate Enrollment Policy**.
12. Click **Add** to open the Certificate Enrollment Policy Server dialog.
13. In the **Enter enrollment policy server URI** box, type or paste the certificate enrollment policy server URI obtained earlier.
14. In the **Authentication type** list, select the authentication type required by the enrollment policy server. (Kerberos)
15. Click **Validate**, and review the messages in the **Certificate enrollment policy server properties** area.
16. Click **Add**.

    The **Add** button is available only when the enrollment policy server URI and authentication type are valid.

17. In the Group Policy Object Editor, navigate to **Computer Configuration | Policies | Windows Settings | Security Settings** and click **Public Key Policies**.
18. Repeat steps 11-16 for machine configuration.

Configuring Certificate Services Client - Auto-Enrollment Group Policy

If you are using Group Policy, you must enable Certificate Autoenrollment in Group Policy otherwise, Group Policy may disable Certificate Autoenrollment. If you are not using Group Policy, Certificate Autoenrollment is enabled on each host by default.

To enable Certificate Autoenrollment using Group Policy

1. On a domain controller running Windows Server 2008 R2 or Windows Server 2008, open the **Start** menu and navigate to **Administrative Tools | Group Policy Management**.
2. In the console tree, double-click **Group Policy Objects** in the forest and domain containing the Group Policy Object (GPO) that you want to edit.
3. Right-click the GPO, and click **Edit**.
4. In the Group Policy Object Editor, navigate to **User Configuration | Policies | Windows Settings | Security Settings** and click **Public Key Policies**.
5. Double-click **Certificate Services Client - Auto-Enrollment**.
6. Next to **Configuration Model**, select **Enabled** from the drop-down list to enable autoenrollment.
7. Click **OK** to accept your changes.
8. In the Group Policy Object Editor, navigate to **Computer Configuration | Policies | Windows Settings | Security Settings** and click **Public Key Policies**.
9. Repeat steps 5-7 for machine configuration.

Configuring Certificate Templates for autoenrollment

Certificate enrollment is based on templates which define the properties of certificates generated by the Certificate Authority (CA) when clients request certificates.

To create a new certificate template

1. On the server hosting your Enterprise CA, click **Start**, select **Administrative Tools**, and click **Certification Authority**.

2. In the console tree, expand the CA root node, select **Certificate Templates**, and click **Manage**.
3. In the **Certificate Templates** console, select the template that you would like to enable for autoenrollment, or create a new template.
4. Double-click the template to open its properties and select the **Security** tab.
5. Add the users and machines that you want to automatically enroll for the certificate and select the **Autoenroll** permission option.
6. Click **Apply**.

Using Certificate Autoenrollment

Certificate Autoenrollment is an automatic process which runs as-needed on client systems according to Group Policy or according to manual configuration if you are not using Group Policy. Certificate Autoenrollment typically requires no user interaction. After Certificate Autoenrollment is complete, certificates appear in the user's keychain for user-based enrollment or in the system keychain for machine-based enrollment.

Certificate Autoenrollment runs when:

- a user logs in
- Group Policy machine processing occurs (at machine startup and periodically thereafter)
- `vascert trigger` runs manually (for machine-based enrollment)

If Group Policy is in use and a **Certificate Services Client - Auto-Enrollment** Group Policy indicates that Certificate Autoenrollment should occur, then the Certificate Autoenrollment client runs. The Certificate Autoenrollment client then downloads and evaluates Certificate Autoenrollment policy and uses this information to determine whether any certificates should be enrolled.

Each of these steps can be invoked manually for testing and troubleshooting. To start Group Policy manually, use the `vgptool` command. To run Certificate Autoenrollment, use the `vascert` command. These command are installed in `/opt/quest/bin`.

Configuring Certificate Autoenrollment manually

Once Certificate Autoenrollment is installed, you must configure your machine to use it. If you are using One Identity Authentication Services with Group Policy, then skip the manual configuration described in this section as Group Policy performs these tasks automatically.

NOTE: Group Policy functionality is not available when used with the Apple Directory Services plug-in. When Group Policy is not available, you must manually configure certificate enrollment policy servers and schedule machine certificate enrollment to run on an interval if desired.

Configure a machine for Certificate Autoenrollment

Use the `vascert` command line utility to configure your machine for Certificate Autoenrollment. Your computer must be joined to the Active Directory domain where your certificate enrollment policy server resides.

NOTE: Unless you are using Group Policy, machine processing must be triggered manually using the `vascert trigger` command. You can schedule this command to run at an interval.

To configure your machine for Certificate Autoenrollment

- As `root` (or using sudo), run the following command to configure a machine for Certificate Autoenrollment:

  `/opt/quest/bin/vascert server add -r <policy server URL>`

  Where `<policy server URL>` is the actual http URL for your certificate enrollment policy server.

  For example: `https://example.com/ADPolicyProvider_CEP_Kerberos/service.svc/CEP`

  NOTE: You can configure more than one certificate enrollment policy server. Certificate Autoenrollment will choose the most appropriate server automatically when performing certificate enrollment.

Configure a user for Certificate Autoenrollment

Use the vascert command line utility to configure a user for Certificate Autoenrollment. The user must be an Active Directory user. Certificate Autoenrollment is not supported for local users. Your computer must be joined to the Active Directory domain where your certificate enrollment policy server resides.

NOTE: Certificate Autoenrollment will run automatically when users log in based on the `/Library/LaunchAgents/com.quest.qcert.UserApply.plist` file. You can change this behavior by modifying this file.

To configure a user for Certificate Autoenrollment

- As `root` (or using sudo), run the following command to configure a user for Certificate Autoenrollment:

```
/opt/quest/bin/vascert server add -u <username> -r <policy server URL>
```

Substitute the actual http URL for your certificate enrollment policy server for example:

```
https://example.com/ADPolicyProvider_CEP_Kerberos/service.svc/CEP
```

NOTE: You can configure more than one certificate enrollment policy server. Certificate Autoenrollment will choose the most appropriate server automatically when performing certificate enrollment.

Trigger machine-based Certificate Autoenrollment

Normally Group Policy triggers Certificate Autoenrollment. If you are not using Group Policy, use the `vascert` command line utility to manually trigger Certificate Autoenrollment processing for the machine. This will result in certificates being added to the System.keychain according to enrollment policy. You can schedule this command to run periodically if desired.

To manually trigger Certificate Autoenrollment

- As `root` (or using sudo), run the following command to manually trigger Certificate Autoenrollment:

  ```
  /opt/quest/bin/vascert trigger
  ```

Certificate Autoenrollment will proceed in the background. When complete, newly enrolled certificates will be installed in the System.keychain automatically. To troubleshoot Certificate Autoenrollment, run the `vascert pulse` command as `root`.

Troubleshooting Certificate Autoenrollment

To help you troubleshoot Certificate Autoenrollment, One Identity recommends the following resolutions to some of the common errors, and methods for finding and correcting configuration problems.

Enable full debug logging

You can enable full debug logging for all Certificate Autoenrollment components using the `vascert` command line utility.

If debug logging is configured, Group Policy extensions, the vascert tool, and `launchd` write log files in /Library/Preferences/com.quest.X509Enrollment/log for machine enrollment and ~/Library/Preferences/com.quest.X509Enrollment/log for user enrollment. You can enable debug logging for all of these components.

To enable debug logging

1. As `root`, run the following command to configure debug logging for all users:

   ```
   /opt/quest/bin/vascert configure debug
   ```

2. To configure debug logging for a specific user, log in as that user and run the same command.

   NOTE: Enabling debug logging causes the `vascert` command to write debug messages to a file in addition to `stdout`. Even after you enable debug logging, you must set the debug level using the `-d` command line option when running `vascert` commands manually.

3. When you are finished debugging, run the following command as `root` to turn off debug logging for all users. One Identity recommends that you turn off debug logging to improve performance and conserve disk space.

   ```
   /opt/quest/bin/vascert unconfigure debug
   ```

4. To turn off debug logging for a specific user, log in as that user and run the same command.

Pulse Certificate Autoenrollment processing

Use the `vascert` command line utility to manually perform Certificate Autoenrollment.

To perform Certificate Autoenrollment processing manually

1. Decide whether you want to pulse Certificate Autoenrollment for the machine or a specific user.
2. To pulse Certificate Autoenrollment for the machine, run the following command as `root` (or using sudo):

   ```
   /opt/quest/bin/vascert pulse
   ```

   NOTE: To pulse certificate enrollment for the machine, you must run the command with `root` privileges. This is mostly useful for troubleshooting. In some cases (such as when logging in by means of SSH), this will not result in successful certificate enrollment because the System.keychain cannot export existing private keys required for certificate renewal processing. If you just want to run Certificate Autoenrollment processing for the machine and you are not interested in the output, use `vascert trigger` instead.

3. To pulse Certificate Autoenrollment for a specific user, log in as that user and run the following command:

   ```
   /opt/quest/bin/vascert pulse
   ```

NOTE: Use the GUI to log in as the user. This ensures that the user's keychain is unlocked so that enrolled certificates can be exported and imported. Logging in by other means, such as SSH, is generally not sufficient and may lead to errors when the `certstore-mac.sh` script invokes the `/usr/bin/security` tool.

Manually apply Group Policy

If you are using One Identity Authentication Services 4.1 or higher, Certificate Autoenrollment is configured automatically by Group Policy. Use the `vgptool` command line utility to manually apply Group Policy.

To manually apply Group Policy

1. Decide whether you want to apply machine policy or user policy.

   NOTE: Machine policy affects the entire system; User policy only affects the specified user.

2. To apply machine policy, enter the following command as `root` (or using sudo):

   ```
   /opt/quest/bin/vgptool apply
   ```

   The terminal displays policy processing results.

3. To apply user policy, enter the following command as `root` (or using sudo):

   ```
   /opt/quest/bin/vgptool apply -u <username>
   ```

   The terminal displays policy processing results.

Command line tool

`vascert` is the Certificate Autoenrollment command line tool for certificate enrollment. With `vascert` you can configure various aspects of Certificate Autoenrollment. You can manually trigger certificate enrollment processing. `vascert` is also helpful for troubleshooting various network and authentication problems that may occur.

This command reference details the command line usage for `vascert`.

`vascert` command reference

vascert is the Certificate Autoenrollment processor.

Name

vascert

Synopsis

```
vascert [-d <debug level [1-6]>] [-b] [-h <command>] <command [command options]>
```

Overview

`vascert` is the Certificate Autoenrollment processor for Unix clients.

Commands

To run `vascert`, specify one or more general options, then specify a specific command which may have further options and arguments.

Table 3: `vascert` commands

Command	Description
clean	Clears certificate enrollment state information.
configure	Allows you to configure Certificate Autoenrollment settings.
importca	Imports trusted root CA certificates based on policy.
info	Dumps the contents of a policy template.
list	Lists all configured policy template names.
pulse	Performs Certificate Autoenrollment processing.
renew	Renews an existing certificate based on a policy template.
server	Manages local policy server configuration.
trigger	Triggers machine-based Certificate Autoenrollment policy processing.
unconfigure	Allows you to un-configure Certificate Autoenrollment settings.

Common Options

The following options can be passed to all `vascert` commands. Specify these options before the command name.

`[-d <debug level [1-6]> ]`

Prints additional information according to debug level, higher debug level prints more output.

`[-b]`

Do not display banner text.

`[-h <command>]`

Display help for a particular command.

vascert commands and arguments

The following is a detailed description of all the available `vascert` commands, their usage and arguments.

vascert clean

Clears certificate enrollment state information.

`vascert [common options] clean [-u <username>] [-x]`

Arguments:

`[-u <username>]` is the name of the user to perform the operation.

`[-x]` removes all local state information.

Additional Information:

This command causes Certificate Autoenrollment to remove all previous configuration and downloaded policy. When run as root with the `-x` option, this command removes all local state information returning the system to the state it had just after package install.

vascert configure

Allows you to configure Certificate Autoenrollment settings.

`vascert [common options] configure <sub-command> <command>`

Sub-commands:

debug enables debug logging for all Certificate Autoenrollment components.

Debug command arguments:

`vascert [common options] configure debug [-u <username>]`

`[-u <username>]` is the name of the user to perform the operation.

vascert importca

Imports trusted root CA certificates based on policy.

`vascert [common options] importca [-u <username>] [-p]`

Arguments:

[-u <username>] is the name of the user to perform the operation.

[-p] simulates policy-based CA import.

vascert info

Dumps the contents of a policy template.

`vascert [common options] info <policy template name>`

vascert list

Lists all configured policy template names.

`vascert [common options] list [-p]`

Arguments:

[-p] lists pending enrollment requests.

vascert pulse

Performs Certificate Autoenrollment processing.

`vascert [common options] pulse [-p]`

Arguments:

[-p] simulates policy-based pulse.

vascert renew

Renews an existing certificate based on a policy template.

`vascert [common options] renew -t <template name>`

Arguments:

-t <template name> is the name of the policy template for which certificates are to be renewed.

vascert server

Manages local policy server configuration.

`vascert [common options] server <sub-command>`

Sub-commands:

`remove` removes a policy server configuration by URL.

`list` lists policy servers that are configured locally.

`add` adds a new local server configuration.

Remove command arguments:

`vascert [common options] server remove [-u <username>] [-a] <URL>`

`[-u <username>]` is the name of the user to perform the operation.

`[-a]` removes all server configurations.

List command arguments:

`vascert [common options] server list [-u <username>]`

`[-u <username>]` is the name of the user to perform the operation.

Add command arguments:

`vascert [common options] server add [-u <username>] [-c <cost> ] -r <URL> [-n <name> ]`

`[-u <username>]` is the name of the user to perform the operation.

`[-c <cost>]` specifies the cost associated with this server. Servers with lower cost are preferred when performing server selection.

`-r <URL>` specifies the service endpoint to contact to object enrollment policy.

`[-n <name>]` specifies the display name of this server.

vascert trigger

Triggers machine-based Certificate Autoenrollment policy processing.

`vascert [common options] trigger`

vascert unconfigure

Allows you to un-configure Certificate Autoenrollment settings.

`vascert [common options] unconfigure <sub-command> <command>`

Sub-commands:

`debug` disables debug logging for all Certificate Autoenrollment components.

Debug command arguments

`vascert [common options] unconfigure debug [-u <username>]`

[-u <username>] is the name of the user to perform the operation.

About us

Contacting us

For sales or other inquiries, visit https://www.oneidentity.com/company/contact-us.aspx or call +1-800-306-9329.

Technical support resources

Technical support is available to One Identity customers with a valid maintenance contract and customers who have trial versions. You can access the Support Portal at https://support.oneidentity.com/.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. The Support Portal enables you to:

- Submit and manage a Service Request
- View Knowledge Base articles
- Sign up for product notifications
- Download software and technical documentation
- View how-to-videos
- Engage in community discussions
- Chat with support engineers online
- View services to assist you with your product

Glossary

A

access control
A set of procedures performed by hardware, software, and administrators to monitor access, identify users requesting access, record access attempts, and grant or deny access. Compare with authorization. See also ACL.

Access Control List (ACL)
A set of data that informs a computer's operating system which permissions, or access rights, that each user or group has to a specific system object, such as a directory or file. Each object has a unique security attribute that identifies which users have access to it, and the ACL is a list of each object and user access privileges such as read, write, or execute.

ACE
Acronym for Access Control Entry.

ACL
Acronym for Access Control List.

ACL Filtering
Access Control Lists can be applied to Group Policy objects which determine whether or not the policy will be applied on a system.

Active Directory
Microsoft's network directory service for computers.

ADAM
Active Directory Application Mode, a Windows 2003 service in which LDAP runs as a user service rather than as a system service.

ADSI
Active Directory Services Interface, an editor (browser), scripting language, and so forth.

ADUC
Active Directory Services Interface, an editor (browser), scripting language, etc.

affinity
With respect to a directory, the organization of the accounts relies on properties they have in common. This similarity may be due to departmental structure or geographical location of the people that use the accounts.

ARC4
See RC4.

ARCFOUR
See RC4.

ARS
ActiveRoles Server, a product installed on a Windows server and uses SQL Server for configuration data and publishing itself as a connection point object within Active Directory. A cross-platform, roles-based provisioning system that allows additional attributes to be stored for an object. For example, ARS can put a newly hired engineer into all the appropriate groups on all platforms relevant to the job description.

authentication
Authentication is the process of determining whether someone or something is, in fact, who or what it is declared to be. In private and public computer networks (including the Internet), authentication is commonly done through the use of log on passwords. Knowledge of the password is assumed to guarantee that the user is authentic. Each user registers initially (or is registered by someone else), using an assigned or self-declared password. On each subsequent use, the user must know and use the previously declared password. The weakness in this system for transactions that are significant (such as the exchange of money) is that passwords can often be stolen, accidentally revealed, or forgotten. Logically, authentication precedes authorization (although they may often seem to be combined).

authoritative source
In migrating identities from disparate NIS domains, identities from the first source repository are migrated without any changes to their internal identity (ID) and the first repository becomes the authoritative source. In case of ID conflict or mismatch, IDs in all remaining sources are changed to match those in the first source.

authorization
Authorization is the process of giving someone permission to do or have something. In multi-user computer systems, a system administrator defines for the system which users are allowed access to the system and what privileges of use (such as access to which file directories, hours of access, amount of allocated storage space, and so forth). Assuming that someone has logged in to a computer operating system or application, the system or application may want to identify what resources the user can be given during this session. Thus, authorization is sometimes seen as both the preliminary setting up of permissions by a system administrator and the actual checking of the permission values that have been set up when a user is getting access. Logically, authorization is preceded by authentication.

B

Block Inheritance
When Block Inheritance is set on a GPO link all GPOs above the link level are excluded from GPO processing unless the GPO is enforced.

C

CAC
Common Access Card, a smart card issued by the United States Department of Defense (DoD) for active-duty military, civilian employees and contractors.

canonical name
Essentially the distinguished name in reverse, generally, a software-internal representation, such as acme.com/engineering/jim.

CIFS
Common Internet File System, a Microsoft technology. See also SMB.

CN
Common Name, a component of a distinguished name (DN).

COM
Component Object Model, a Microsoft technology that enables components to communicate, used by developers to create reusable software components, link components together to build applications and take advantage of Windows services like Active Directory.

credential
A proof of qualification or competence attached to a user or session, an object verified during an authentication transaction. In Kerberos parlance, a message containing the random key along with a service name and the user's long-term key.

D

DC
Domain Controller.

disconnected authentication
Provisory authentication based on prior login and used in case of network failure. The maximum duration of a stored password hash is configurable.

DN
Distinguished Name.

domain
In Active Directory, a centrally-managed group of computers.

domain controller (DC)
The server that responds to security authentication requests in the Active Directory domain.

DSE
Directory-specific entry in an LDAP environment.

E

Enforced
If a GPO is enforced, then it will be applied regardless of block inheritance settings.

F

firewall
A piece of hardware and/or software that sets rules about what network traffic can cross it. These rules can focus on the protocols used by the traffic and ports in use. Authentication Services, for instance, requires a set of ports by which it implements its services. Those ports must not be blocked. However, if a host has access to Active Directory, to its domain controllers, and so forth., then the ports needed by Authentication Service are open. For Authentication Services specifically, this means 88 (TCP/UDP for Kerberos ticket services), 389 (LDAP queries and ping), 464 (TCP/UDP for Kerberos passwords) and 3268 (TCP for Global Catalog access), optionally, 53 (UDP for DNS SRV records), 123 (UDP for time-synchronization with Active Directory). For Authentication Services Group Policy, port 445 (TCP for Microsoft DS).

forest
The collection of all objects and their attributes and rules in Active Directory. It is named "forest" because it holds one or more trust-linked trees, allowing users in one domain to access resources in another domain.

FQDN
Fully Qualified Domain Name, a domain name specified exhaustively such as CN=jim,OU=engineering,DC=acme,DC=com.

FSMO
Flexible Single Master Operations, a multi-master-enabled database such as Active Directory provides the flexibility of allowing changes at any domain controller in the enterprise, but also gives rise to the possibility of conflicts and the need to resolve them, especially for certain tasks. Collectively, FSMO tasks are used where standard data transfer and update methods on multiple peer domain controllers are ill adapted to multi-master replication, to wit: schema update and modificationdomain naming (addition or removal of domains in the forest)relative ID assignment (including SIDs)infrastructure (security) maintenance (including GUIDs, SIDs and reference object DN in cross-domain references)and PDC emulation These tasks are handled in a single master model by Windows 2000/2003.

G

GC
Global Catalog.

GECOS
(also in lower case) A field in the Unix /etc/passwd file that contains general information about the user including things like full name, telephone number, and so forth, depending completely on the host implementation.

gid
group identity, standard C library object, represented by gid_t, identifying a group.

GID
Group identity, broad term referring to the underlying number that identifies a group of users or other objects in a directory service.

GPMC
Group Policy Management Console, a Microsoft tool.

GPO
Group Policy Object, an actual directory object tied to system volume instance. The group policy object is a collection of settings that define what a system looks like and how it behaves for a defined group of users. A GPO is created, using the Group Policy Management Console (see above), when there are such settings. GPOs are associated with a container such as a site, domain or organizational unit (OU). GPOs are very powerful and can be used even to distribute software and updates à la Tivoli (IBM). See also group policy.

group policy
A Microsoft technology that reduces the cost of supporting Windows users by providing centralized management of computers and user in Active Directory. Group Policy controls various aspects of an object including security policy, software installation, login, folder redirection and software settings. Such policies are stored on group policy objects (GPOs).

GSS
generic security service, security services provided atop underlying, alternative cryptographic mechanisms such as Kerberos. According to RFC 2744, the GSS API allows a caller application to authenticate a principal identity associated with a peer application to delegate rights to another peer, and to apply security services such as confidentiality and integrity on a per-message basis.

GUID
Globally Unique Identifier, a number, address or other cookie used to represent an object uniquely in a directory service, file system, and so forth. In Active Directory, the GUID is a unique, unchanging 128-bit string used for search and replication.

J

joining
Describes the action of a Unix or Linux workstation being incorporated into an Active Directory domain by means of the vastool join command.

K

KDC
The Key Distribution Center in Kerberos. Part of a cryptosystem to reduce the intrinsic risk of exchanging keys, basically consisting of the authentication server (AS) and the ticket-granting server (TGS).

Kerberized application
A software application that requires or performs Kerberos authentication.

Kerberos
A computer network authentication protocol that proves the identity of intercommunicating points on an insecure network like a LAN or the Internet in a secure manner. Guards against eavesdropping and replay attacks. There are different Kerberos encryptions including DES and ARC4, the latter being more secure as well as the default in Authentication Services since release 2.6 SP4.

Kerberos authentication
An authentication system developed at the Massachusetts Institute of Technology (MIT). Kerberos is designed to enable two parties to exchange private information across an otherwise open network. It works by assigning a unique key, called a ticket, to each user that logs on to the network. The ticket is then embedded in messages to identify the sender of the message.

keytab
A file containing authentication credentials used, usually in place of a password, for authentication

L

LAM
Loadable Authentication Module, IBM's precursor to PAM on the AIX (Unix) operating system. Authentication Services provides a LAM-based implementation on AIX. LAMs are configured in /usr/lib/security/methods.cfg.

LDIF
LDAP Data Interchange Format. See also Lightweight Directory Access Protocol (LDAP)

Lightweight Directory Access Protocol (LDAP)
A software protocol for enabling anyone to locate organizations, individuals, and other resources such as files and devices in a network, whether on the public Internet or on a corporate intranet. LDAP is a "lightweight" version of Directory

Access Protocol (DAP), which is part of X.500, a standard for directory services in a network. Netscape includes it in its latest Communicator suite of products. Microsoft includes it as part of what it calls Active Directory in a number of products including Outlook Express. The Novell NetWare Directory Services inter-operates with LDAP. Cisco also supports it in its networking products.

M

Mapped Users

Mapped User allows Authentication Services to authenticate against Active Directory while taking identity and Unix attributes from local files. It is implemented by replacing the 'x' placeholder in /etc/passwd with the user principal name (UPN) (Linux and Unix only), or by creating a local-to-AD user map file and specifying the location of that file in /etc/opt/quest/vas/vas.conf (Linux, Unix, or Mac).

MIIS

Microsoft Identity Integration Server, a server that manages the flow of data between all connected data sources and automates the process of updating identity information (for example, of employees, and so forth) in the implementing environment.

MMC

Microsoft Management Console, for which Authentication Services has a snap-in used when browsing users or groups and getting their properties.

N

NAS

Network-Attached Storage, file-level data storage connected, often remote, but not appearing as a local volume/disk. This is in opposition to SAN.

Native Mode

Native Active Directory mode refers to a network being serviced completely by either Windows 2000 or Windows 2003 servers but not both. If servers from both versions are present, the services offered can only be a common subset of the two. If all servers are running Windows 2003 Server, then all the features that this operating system offers over its predecessor are available. Not being in native mode has ramifications for various components, that is, local groups are not added to the PAC of the Kerberos ticket; group membership is not available.

NIS

Network Information Services, a Unix client-server directory service protocol, originally Sun Microsystems' "Yellow Pages". It provides centralized control over many types of network objects including users, groups and network services like printers. NIS arose as a solution to each Unix host having its own /etc/passwd and groups files as the resident authority on users and groups when these notions needed to be extended over a network. NIS domains are flat (no hierarchy), use no authentication and the NIS map files are limited to 1024 bytes in size.

nscd
name service caching daemon, provides a cache for the most common name service request on Linux and Unix from the passwd, group, and hosts databases through standard C library interfaces including getpwnam, getpwuid, getgrnam, getgrgid, gehostbyname, and others. The configuration file is /etc/nscd.conf

NSS
Name Service Switch, interface to nsswitch.conf that controls how look-ups are done for users (/etc/passwd), groups (/etc/grps), hosts (/etc/hosts), and so forth. For example, getpwnam goes through NSS, which is extensible and configurable (just as is PAM), to reach variably passwd, vasd, NIS or LDAP.

NTP
Network Time Protocol, as implemented by a server that keeps time on the network and is accessible to other nodes for the purpose of all keeping the same notion of time.

O

Organizational Unit (OU)
An Active Directory container object used within domains. An organizational unit is a logical container into which users, groups, computers, and other organizational units are placed. It can contain objects only from its parent domain. An organizational unit is the smallest scope to which a group policy object can be linked, or over which administrative authority can be delegated.

OU
Organization Unit. See also Personality container.

Override
If a GPO specifies a policy and another GPO further down in the GPO application chain is allowed to overwrite the previously specified policy, then the policy supports override.

P

PAC
Privileged Attribute Certificates, used by Kerberized applications for fine-grained access control to services, a feature of Microsoft's Kerberos implementation.

PAM
Pluggable Authentication Module, an architecture and shared libraries created by Sun Microsystems for the Solaris operating system that permits intervention into and specialization of the authentication process. PAMs are configured in /etc/pam.conf or in individual files off /etc/pam.d/.

PDC
Primary Domain Controller, an NT concept, emulated on Windows 2000/2003, that performs a number of crucial tasks in an enterprise including time

synchronization, password replication, recording of password failures, account lock-out, and modification or creation of GPOs.

Personality container
An Active Directory organization unit (OU) designated to contain user and group personalities. Unix clients specify a Unix personality container (vastool join -p) in order to join the domain in Unix Personality Management (UPM) mode.

Personality scope
Consists of a primary Personality container, along with any secondary Personality containers. Only the Personalities, Active Directory users, and Active Directory groups that reside within that Personality scope will be usable on the Unix system.

PKI
Public Key Infrastructure; a way to ensure secure transactions over the wire; an arrangement providing for third-party vetting of user identities typically placing any keys within a certificate. Not yet a standard; there are myriad implementations.

POSIX
The Portable Operating System Interface, the open operating interface standard accepted world-wide. It is produced by IEEE and recognized by ISO and ANSI.

principal
In Kerberos, this is basically a simple account including name, password and other information stored in the database and encrypted using a master key.

provisioning
The process of providing customers or clients with accounts, the appropriate access to those accounts, all the rights associated with those accounts, and all of the resources necessary to manage the accounts. When used in reference to a client, provisioning can be thought of as a form of customer service.

R

RC4
(pronounced "arcfour") the most widely used stream cipher in such popular protocols as secure sockets layer (SSL). RC4 generates a pseudo random stream of bits XOR'd with the clear-text password, for example. RC4 is more secure than DES.

realm
A Kerberos term that usually maps to an Active Directory domain, not because they are the same thing, but because for implementation, it is a natural alignment.

S

Samba
A free software implementation of Microsoft's networking protocol that runs on *nix systems and is capable of integrating with an Active Directory (Windows)

domain as either a primary domain controller or as a domain member. See also SMB.

SAN

Storage Area Network, an architecture for attaching remote storage devices (disk arrays, tape libraries, optical jukeboxes, and so forth) to servers in such a way that to the operating system these appear as locally attached. This is in opposition to NAS where it is clear that the storage is remote.

Sarbanes Oxley Act (SOX)

Reference to legislation enacted in response to recent and spectacular financial scandals, to protect shareholders and the general public from accounting errors and fraudulent practices. The act is administered by the Securities and Exchange Commission, which sets deadlines for compliance and publishes rules on requirements. SOX defines which records are to be stored and for how long. It also affects IT departments whose job it is to store electronic records.

schema master

A domain controller that holds the schema operations master role in Active Directory. The schema master performs write operations to the directory schema and replicates updates to all other domain controllers in the forest. At any time, the schema master role can be assigned to only one domain controller in the forest.

Secure Sockets Layer (SSL)

The Secure Sockets Layer (SSL) is a commonly-used protocol for managing the security of message transmission on the Internet. SSL uses a program layer located between the Internet's Hypertext Transfer Protocol (HTTP) and Transport Control Protocol (TCP) layers. SSL is included as part of both the Microsoft and Netscape browsers and most Web server products. Developed by Netscape, SSL also gained the support of Microsoft and other Internet client/server developers, becoming the de facto standard until evolving into Transport Layer Security (TLS). The sockets part of the term refers to the sockets method of passing data back and forth between a client and a server program in a network or between program layers in the same computer. SSL uses the public/private key encryption system from RSA, which also includes the use of a digital certificate.

security principal

An entity that can be positively identified and verified by means of a technique known as authentication.

Simple and Protected GSS-API Negotiation Mechanism (SPNEGO)

A GSSAPI mechanism that allows the secure negotiation of the mechanism to be used by two different GSSAPI implementations. In essence, SPNEGO defines a universal but separate mechanism, solely for the purpose of negotiating the use of other security mechanisms. SPNEGO itself does not define or provide authentication or data protection, although it can allow negotiators to determine if the negotiation has been subverted, once a mechanism is established.

Single Sign-On (SSO)

An authentication process in a client/server relationship where the user, or client, can enter one name and password and have access to more than one application or access to a number of resources within an enterprise. Single sign-on removes the need for the user to enter further authentications when switching between applications.

SMB

Server Message Block, a protocol that exists primarily for trust relationships, the concept upon which NetBIOS is based and hence, used by DOS and Windows. The message format is used for sharing files, directories and devices. CIFS (Common Internet File System) is a synonym for SMB. See also Samba.

T

Tattooing

When files or settings are left on the system after group policy has been un-applied, the files and settings are said to be tattooed. Unless otherwise documented a policy should remove all associated settings and files when the policy is unlinked. A policy that supports non-tattooing will not leave any files or settings behind after it is un-applied.

Index

E

F

G

H

I

J

K

L

M

N

O

P

R

S

T

U

V

W