Delinea

Server Suite

Mac Administrator's Guide

Version: 2024.x

Publication Date: 10/17/2024

Server Suite Mac Administrator's Guide

Version: 2024.x, Publication Date: 10/17/2024

Table of Contents

Administering macOS Systems

About Delinea Management Services for Mac

With Delinea Management Services for Mac, you can use Active Directory to centrally manage authentication, policy enforcement, single sign-on (SSO), and user self-service for popular endpoint devices running Mac operating systems.

A key component of Delinea Management Services for Mac is the *DirectControl agent* for Mac computers. You must install the agent on each computer that you want to integrate with Active Directory and manage through Delinea Access Manager.

After you install the agent on a Mac computer, you can perform many administration and configuration tasks on the computer to enable the computer to work with Delinea Management Services and with Active Directory.

Intended Audience

This guide is intended for Mac system administrators.

Topics Covered in this Guide

The following topics are covered:

The *Administrator's Guide for Mac* provides information about the administration and configuration tasks that you perform on a Mac computer after you install the agent so that you can manage users, groups, computers, and zones with Access Manager. Additional topics, such as installing the agent, optionally enrolling the computer in the Delinea Platform, and troubleshooting issues after the agent is installed are also covered.

Specific areas of focus are as follows:

- This guide provides installation instructions and step-by-step instructions for configuring Mac computers to join an Active Directory domain through Auto Zone, which creates one large zone for all Mac computers. Auto Zone requires minimal configuration and is appropriate for most Mac environments. If your environment is larger, or more complex, and doesn't easily fit into Auto Zone, you must consult the *Planning and Deployment Guide* for detailed information on how to move your Mac users and computers to Active Directory and use Delinea zones to structure your environment.
- This guide explains how to handle issues and tasks that are specific or unique to a Mac environment.

This guide does not cover planning or Access Manager tasks handled through the Access Manager console. For more information about those topics, see Where to go for more information.

This guide assumes you have a working knowledge of performing administrative tasks in a Mac environment.

Installing the DirectControl Agent for Mac

This section explains how to install the DirectControl Agent for a Mac computer.

Preparing to Install the DirectControl Agent for Mac

You must install the DirectControl Agent for Mac on each computer that you want to manage through Delinea and Active Directory. You can check the *Release Notes* included with the software, or visit the Delinea Web site (scroll to **Supported Platforms** and click the **Details** tab) to verify that each computer where you plan to install is running a supported version of the mac operating system.

Note: The installation package also contains a utility, ADCheck, which verifies that each of your Mac computers is ready for installation of the DirectControl agent. ADCheck confirms that a computer is running a supported OS, has sufficient disk space to install the DirectControl agent, and that the domain you intend to join has functioning domain controllers and DNS servers. Information about running ADCheck is included in this documentation.

Installing the Agent on Apple M1 Mac Computers

Depending on whether you using the graphical installer or the command line version to install the DirectControl Agent for Mac on Apple M1 Mac computers, you may need to install some additional software.

- If you install the DirectControl Agent for Mac on an Apple M1 Mac computer using the graphical user interface, you might be asked to install Rosetta.

  Click **Install**, then enter your user name and password to allow installation to proceed.

  For more information, see https://support.apple.com/en-us/HT211861.

- If you install the DirectControl Agent for Mac on an Apple M1 Mac computer using the install.sh script, or by installing remotely, you might need manually install Rosetta first. Please run the following command with root privileges to install Rosetta 2:

  ```
  /usr/sbin/softwareupdate --install-rosetta --agree-to-license
  ```

Verifying DirectControl Agent for Mac Installation Prerequisites

Before installing the DirectControl Agent for Mac on your Mac computers, be certain that you or another administrator has installed Delinea Management Services on a Windows computer in the domain. Delinea Management Services includes the Access Manager Console, which is the primary management console for performing ongoing operations, including the application of group policies.

For information about other Delinea Management Services components, such as Zone Provisioning Agent, see the *Planning and Deployment Guide* and the *Administrator's Guide for Linux and UNIX.*

Deciding When and How to Join a Domain

Following installation, you will be prompted to join a domain. Whether to join a domain depends primarily on how you intend to join. Delinea provides two ways to join a domain:

- Through Auto Zone, which is the recommended method for installations with 1500 or fewer users. When joined through Auto Zone, all users and groups defined in Active Directory for the forest – as well as all Active Directory users defined in a forest with a two-way, cross-forest trust relationship to the forest of the joined domain – automatically become valid users and groups on the Mac computer.
- By connecting to a specific Delinea zone, which is the recommended method for installations with 1500 or more users, or for installations in which fine-tuned access control is needed. A zone is similar to an Active Directory organizational unit (OU) and allows you to organize the computers in your organization in meaningful ways to simplify account and access management and the migration of information from existing sources to Active Directory.

The assumption of this guide is that you are joining Auto Zone. After installation, you can follow the instructions to join the domain and with a few configuration steps all your Active Directory users will be able to log into this computer.

Note: If you have a set of Apple Open Directory users, you should migrate them following installation but before joining a domain.

On the other hand, if your environment requires a zone structure, you must create that structure before joining a domain. Therefore, after installing the DirectControl agent, consult the *Planning and Deployment Guide* and the *Administrator's Guide for Linux and UNIX*, which explain in detail how to plan, create, and maintain an Active Directory installation of non-Windows computers with Server Suite.

Installing the DirectControl Agent

The DirectControl Agent for Mac can be installed in several different ways. The procedure in this section shows how do so by double-clicking the Delinea Installer package (DMG) and following the instructions displayed on the screen. This installation method is recommended for most users when installing on a single computer or a limited number of computers.

When you use the Delinea package installer, you will be prompted to join the domain. You may also join the domain after installation using either the adjoin command-line program or the Delinea Directory Access plug-in.

Delinea provides a number of other ways to install the DirectControl Agent for Mac

- By executing the DirectControl Agent for Mac installation script, `install.sh` in a Terminal window on a Mac computer and following the instructions displayed by the script.

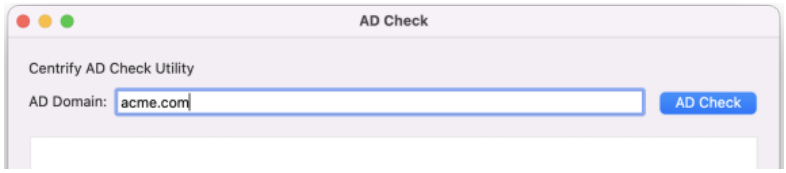
  If you are an experienced UNIX administrator and are familiar with UNIX command-line installations, running `install.sh` is a good method to use. When you install using the `install.sh` script, you can automatically join an Active Directory domain as part of the installation process; see Installing Using the install.sh Script for details.
- By installing remotely, without user interaction, using Apple Remote Desktop. This is a good method to use if you are using Apple Remote Desktop for software distribution. With Apple Remote Desktop you can add pre- and post-installation scripts that allow you to join the remote computer to a domain after installation; see Installing Silently on a Remote Computer for details.

To install the DirectControl Agent for Mac on a Mac computer using the graphical user interface:

1. Before installing the DirectControl Agent for Mac, disable Apple's built-in Active Directory plug-in, and remove Active Directory from the Authentication, and Contacts search paths. For more information, see Disabling the Apple Built-in Active Directory Plug-in.
2. In addition, be certain that the Apple Directory Utility is closed.
3. Log on with the Administrator account.
4. Navigate to the directory on the CD or your local network where the agent package is located. For example, if you are installing from the Delinea CD, open the MacOS directory.
5. Double-click the DMG file, for example:

   `centrifydc-release-mac10.10-x86_64.dmg`
6. Double-click ADCheck to open the ADCheck utility.

   ADCheck performs a set of operating system, network, and Active Directory checks to verify that the Mac computer meets the system requirements necessary to install the DirectControl Agent for Mac and join an Active Directory domain.
7. Enter the domain you intend to join with the Mac computer and click **AD Check**; for example:

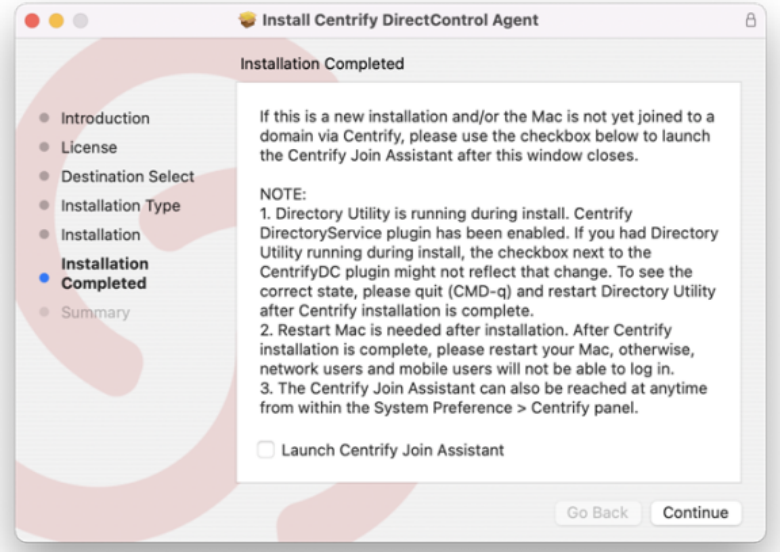


8. Review the results of the checks performed. If the target computer, DNS environment, and Active Directory configuration pass all checks with no warnings or errors, you should be able to perform a successful installation and join the specified domain. If you receive errors or warnings, correct them before proceeding with the installation; see the *Administrator's Guide for Linux and UNIX* for more information about ADCheck.
9. Double-click the Delinea DC package to open the Installer:

10. Review the information in the Welcome page, then click **Continue**.
11. Review or print the terms of the license agreement, then click **Continue**; click **Agree** to agree to the terms of the license agreement. Then click **Install** (note that you cannot change the volume on which the agent is installed – it must be on the same volume as Mac OS X).
12. If prompted, enter the administrator name and password, and click **Install Software** to install the DirectControl Agent for Mac.

If you see the following warning box, click **OK**. If you did not have Directory Utility running during the installation, you can ignore the warning. If Directory Utility was open, you can quit and restart it to show the correct status of the Delinea plug-in.

The installation process runs and presents the Installation Completed page once the DirectControl Agent for Mac is installed.



13. Select **Launch Delinea Join Assistant** if you want to join a domain, then click **Continue**.

    Note: If you know that you want to use Delinea zones in your environment, exit the installer now. You must create zones first, before you can join to one. Refer to Deciding When and How to Join a Domain for more information.

    If you chose not to launch the Delinea Join Assistant before clicking Continue, the installer presents a summary indicating that the installation was successful. You can now close the installer.

If you chose to launch the Delinea Join Assistant, you can start the process of **Joining an Active Directory Domain** described in the next section.

Note: If the Mac system is MacOS 11 or later, you must configure full disk access for the DirectControl Agent for Mac before you join the system to an Active Directory domain.

Joining an Active Directory Domain

This topic shows how to use the Delinea Join Assistant to join a domain. To join a domain, you must be a domain admin or a domain user with permission to create computer objects. If necessary, your domain administrator can use the Delegation Wizard to delegate permission to create computer objects. Refer to Who Can Add a Workstation to a Domain for more information.

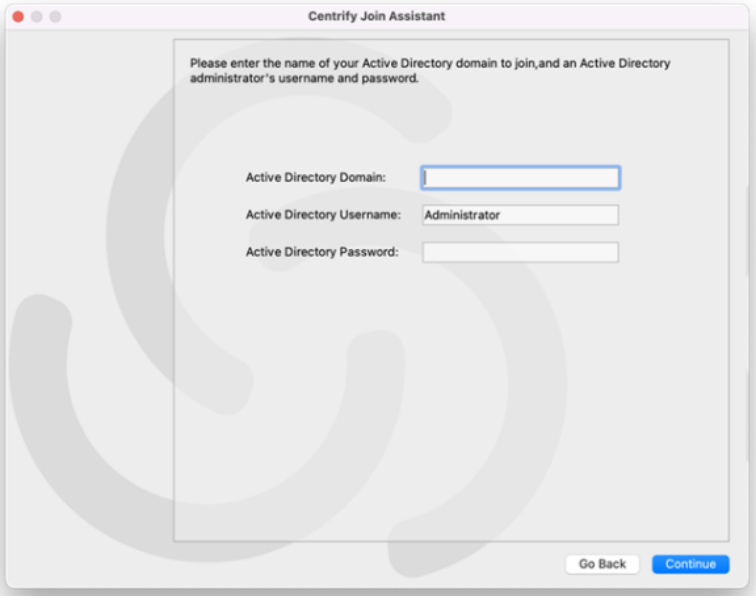
Note: Alternately, you may run the adjoin command-line utility, interactively or in a script, for each Macintosh computer you want to add to a domain in the forest. See the *Administrator's Guide for Linux and UNIX* for details.

To join the Mac to a domain:

1. Launch the Delinea Join Assistant.

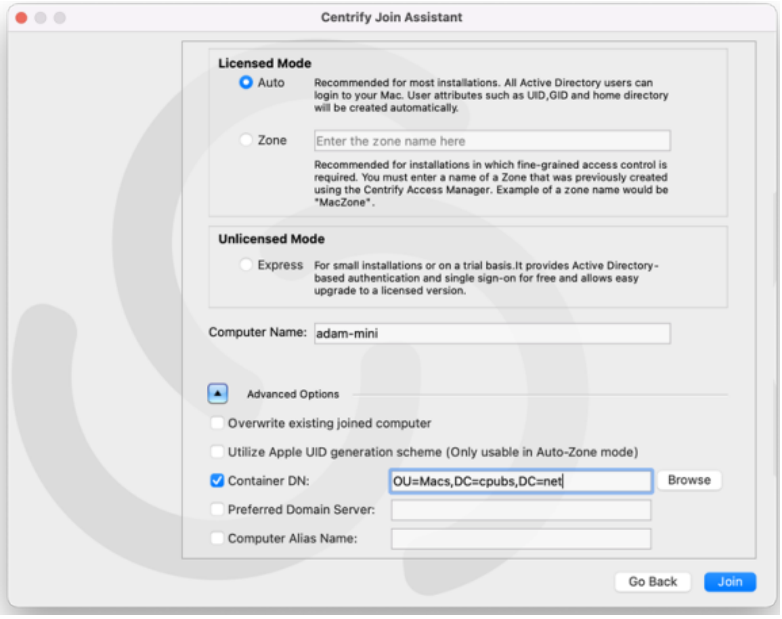
   There are two ways to launch the Delinea Join Assistant:

   - from the DirectControl agent installer, as described in Installing the DirectControl Agent for Mac.
   - click **Applications > Utilities > Delinea**, double-click **Delinea Join Assistant** to open it, then click **Continue** on the Welcome page



2. Enter the active directory domain that you want to join as well as administrator credentials for that domain, then click **Continue**.

A page appears that allows you to select how to join the domain with an option to enroll in the Privileged Access Service.



3. Select from the following options:

Select this option	To do this
Auto	Joins the computer through Auto Zone, which allows joining a computer with little or no configuration. This option is recommended for most installations.
Zone	Joins to the zone that you type in the box. Note that you must have created at least one zone before you can use this option.
Computer name	Defaults to the name of the computer on which you are running the join assistant, but you can change it if you want to use a different name for the local host in Active Directory.

Note: Enrollment is no longer supported.

4. (Optional) Click the arrow to expand the Advanced Options and select any Advanced Options that you want to use to join the device.

Select this option	To do this

Overwrite existing joined computer	Overwrite the information stored in Active Directory for an existing computer account. This option allows you to replace the information for a computer previously joined to the domain. If there is already a computer account with the same name stored in Active Directory, you must use this option if you want to replace the stored information. You should only use this option when you know it is safe to force information from the local computer to overwrite existing information. Checking this option is the same as running the adjoin command with the `--force` option.
Container DN	Specify the distinguished name (DN) of the container or Organizational Unit in which you want to place this computer account. By default, computer accounts are created in the domain's default Computers container. Click **Browse** to browse Active Directory and select the container to use, or click Container DN and enter the name of the container in distinguished name format; for example, if the domain suffix is acme.com and you want to place this computer in the paris.regional.sales.acme.com organizational unit, you would type: `ou=paris, ou=regional, ou=sales` Checking this option is the same as running the adjoin command with the `--container` option.
Preferred Domain Server	Specify the name of the domain controller to which you prefer to connect. You can use this option to override the automatic selection of a domain controller based on the Active Directory site information. Checking this option is the same as running the adjoin command with the `--server` option.
Computer Alias Name	Specify an alias name you want to use for this computer in Active Directory. This option creates a Kerberos service principal name for the alias and the computer may be referred to by this alias. Checking this option is the same as running the adjoin command with the `--alias` option.

5. Click **Join**.

   Delinea Join Assistant informs you that you have successfully joined your Mac to your Active Directory domain at <mydomain.com>.

6. Click **Done** to close the Delinea Join Assistant.

   Your Active Directory users can now log on to the joined Mac computer, as described in Logging onto the Mac after Joining a Domain.

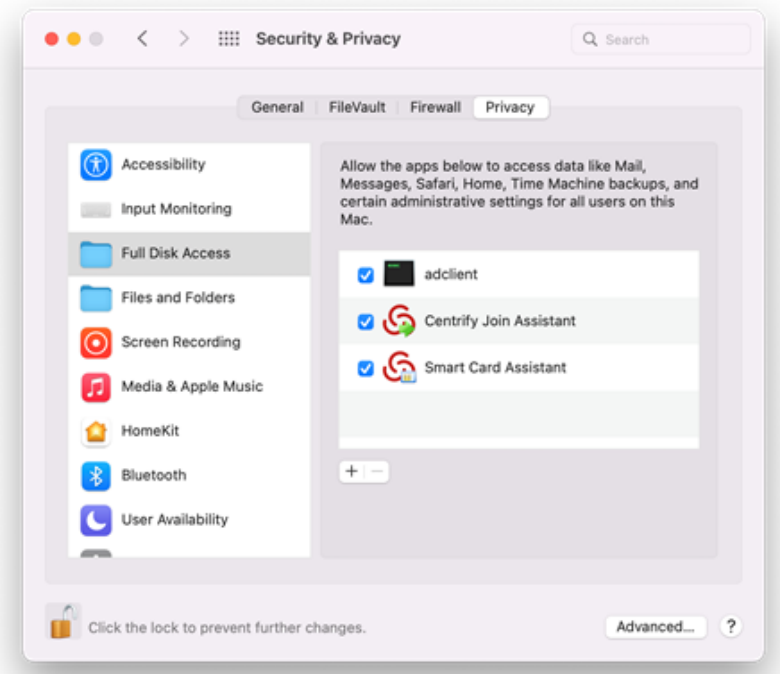
Configuring Full Disk Access for the DirectControl Agent for Mac

Due to a limitation of MacOS 11.x and MacOS 12.x, "Full Disk Access" is required for the DirectControl Agent for Mac. You can configure this yourself if you're an administrator on the computer, or you can set it by way of your MDM (Mobile Device Management) provider.

To configure full disk access as an administrator:

1. Log in to the Mac computer as an administrator user.
2. Open **System Preferences**.
3. Click **Security & Privacy.**

4. Click **Privacy**.
5. Click **Lock** and then enter the password or use TouchID to unlock.
6. In the left pane, scroll down and select **Full Disk Access**.
7. Click **+** (the plus button).
8. Press and hold these three keys together: Shift + Command + G.
9. Enter the path "/usr/local/sbin/adclient" and click **GO**, then click **Open** to add the path.
10. Repeat step 7 and 8, then input the path "/Applications/Utilities/Centrify/Centrify Join Assistant.app" and click **GO**, then click **Open** to add the path.
11. Repeat step 7 and 8, then input the path "/Applications/Utilities/Centrify/Smart Card Assistant.app" and click **GO**, then click **Open** to add the path.
12. Click **Lock** again to lock the system preferences.



Configuring Full Disk Access Through Your MDM Provider

Contact your MDM provider for more information. Your MDM provider will need the following information:

```
% codesign -dv /usr/local/sbin/adclient
Executable=/usr/local/sbin/adclient
Identifier=adclient
...
% codesign -dr - /usr/local/sbin/adclient
Executable=/usr/local/sbin/adclient
designated => identifier adclient and anchor apple generic and certificate 1
[field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf
[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] =
"64CT837G5Z"
% codesign -dv /Applications/Utilities/Centrify/Centrify\ Join\ Assistant.app
```

```
Executable=/Applications/Utilities/Centrify/Centrify Join
Assistant.app/Contents/MacOS/Centrify Join Assistant
Identifier=com.centrify.cdc.centrifyjoinassistant
...
% codesign -dr - /Applications/Utilities/Centrify/Centrify\ Join\ Assistant.app
Executable=/Applications/Utilities/Centrify/Centrify Join
Assistant.app/Contents/MacOS/Centrify Join Assistant
designated => identifier "com.centrify.cdc.centrifyjoinassistant" and anchor apple generic
and certificate 1[field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf
[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] =
"64CT837G5Z"
% codesign -dv /Applications/Utilities/Centrify/Smart\ Card\ Assistant.app
Executable=/Applications/Utilities/Centrify/Smart Card Assistant.app/Contents/MacOS/SCTool
Identifier=com.centrify.cdc.smartcardassistant
...
% codesign -dr - /Applications/Utilities/Centrify/Smart\ Card\ Assistant.app
Executable=/Applications/Utilities/Centrify/Smart Card Assistant.app/Contents/MacOS/SCTool
designated => identifier "com.centrify.cdc.smartcardassistant" and anchor apple generic and
certificate 1[field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf
[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] =
"64CT837G5Z"
```

Configuring Full Disk Access for Apple Remote Desktop

If your organization uses Apple Remote Desktop to run any DirectControl Agent for Mac commands (such as adjoin, adleave, and so forth), you need to also set Full Disk Access for Apple Remote Desktop. You can do this either as an administrator user or through your MDM service, following the same procedures as mentioned earlier.

If you're configuring full disk access as an administrator, the application path to add is as follows:

```
/System/Library/CoreServices/RemoteManagement/ARDAgent.app
```

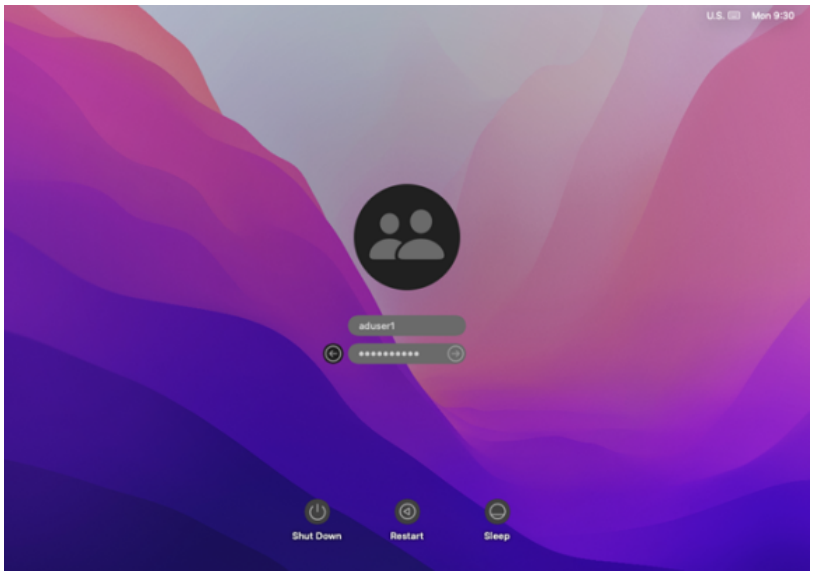
If you're configuring full disk access through your MDM provider, here's the information that your provider needs:

```
% codesign -dv /System/Library/CoreServices/RemoteManagement/ARDAgent.app
Executable=/System/Library/CoreServices/RemoteManagement/ARDAgent.app/Contents/MacOS/ARDAgent
Identifier=com.apple.RemoteDesktopAgent
...
% codesign -dr - /System/Library/CoreServices/RemoteManagement/ARDAgent.app
Executable=/System/Library/CoreServices/RemoteManagement/ARDAgent.app/Contents/MacOS/ARDAgent
designated => identifier "com.apple.RemoteDesktopAgent" and anchor apple
```

Logging onto the Mac After Joining a Domain

When using Auto Zone, all Active Directory users in the domain become valid users on a joined computer. To verify that the software is working properly, you can simply log into the Mac computer by using an Active Directory account.

On the Mac login screen, select **Other** and enter an Active Directory user name and password:



Upgrading The DirectControl Agent for Mac

In most cases, you can update agents on Mac computers by simply installing the new agent either directly or remotely on top of an existing agent. As a best practice, you should perform in-place upgrades using a local Mac administrative (`admin`) account or any other user account that has local administrative rights and reboot the computer after completing the upgrade. In most cases, you should not perform the upgrade while you are logged on as an Active Directory user in a currently active session.

In rare cases, you might be advised to run `adflush` to clear the Active Directory cache before performing an in-place upgrade. For example, if you are updating agents from version 4.x, or earlier, to 5.1.x, run `adflush` first to ensure a smooth upgrade. It is highly unusual for an upgrade to require you to leave and rejoin a managed Mac computer to the domain.

Creating Home Directories

This section explains how to create different types of home directories for a Mac computer.

Understanding Home Directories

Whenever an Active Directory user logs in to a Mac computer, a home directory is created for the user. Mac provides three styles of home directory, which can be configured by an administrator to fit the type of user who will be using the computer, the type of computer, and the use to which the computer will be put. Auto Zone supports each of these styles:

- Local home directory – The user's home directory is created on the local computer in the Users folder with the user's login name (`/Users/username`).
- Network shared directory – The user's home directory is created on a network share.

- Portable home directory – The user's home directory is created on a network share and copied and synchronized to the local computer. This type of directory is also called a *mobile* home directory.

When you join a computer to a domain by connecting to Auto Zone, the home directory is created based on the following:

- Active Directory user settings; for example, an administrator can specify a network home directory in the Profile for an Active Directory user.
- Auto Zone default values; by default, Auto Zone is configured to support the creation of home directories in the Users folder on the local computer.
- Auto Zone parameters set in the configuration file, `/etc/centrifydc/centrifydc.conf` by an administrator or by a group policy. See the *Configuration and Tuning Reference Guide* for a description of all Auto Zone parameters.

The following sections explain in detail how to set up each type of user home directory.

Configuring a Local Home Directory

In general, you do not need to explicitly configure local home directories for your Active Directory users because Auto Zone is configured to work for Active Directory users exactly as if they were local users. That is, by default, an Active Directory user who logs in to a Mac computer that is joined to a domain through Auto Zone is given a local home directory at `/Users/username`. For example, for a user, Glen Morris, whose login name is gmorris, the local home directory is set to: `/Users/gmorris`.

Although it isn't necessary to explicitly configure the agent for local home directories, in some situations you might want to do so. For example, if a Windows user has a local home directories defined in their Active Directory profile, that home directory will be assigned when the user attempts to log in and may prevent the user from logging in. The agent provides a configuration parameter (`auto.schema.use.adhomedir`)that you can set to ignore home directories in an Active Directory profile and always set the home directory to the default (`/Users/username`).

To explicitly configure a computer for local home directories:

1. On the Mac computer, edit the configuration file, `/etc/centrifydc/centrifydc.conf`.
2. Add the following two parameters:

   ```
   auto.schema.use.adhomedir: false
   auto.schema.homedir: /Users/%{user}
   ```

   - Setting `auto.schema.use.adhomedir` to false configures the local computer to ignore any home directories that are set for users in Active Directory. This parameter is set to true by default.
   - Setting `auto.schema.homedir: /Users/%{user}` configures the local computer to set the home directory to `/Users/username`, where *username* is the user logon name defined in the user's Active Directory account. Note that this parameter is set to this value by default on all Mac computers.

     Note: If you plan to configure network-home or portable-home directories for this computer, you must set `auto.schema.use.adhomedir` to true, the default value, otherwise, the agent will ignore the network home directories that you specify for users in Active Directory.

3. Save and close the file.

Configuring a Network Home Directory

For each user whom you want to have a network home directory, you must specify the location in Active Directory.

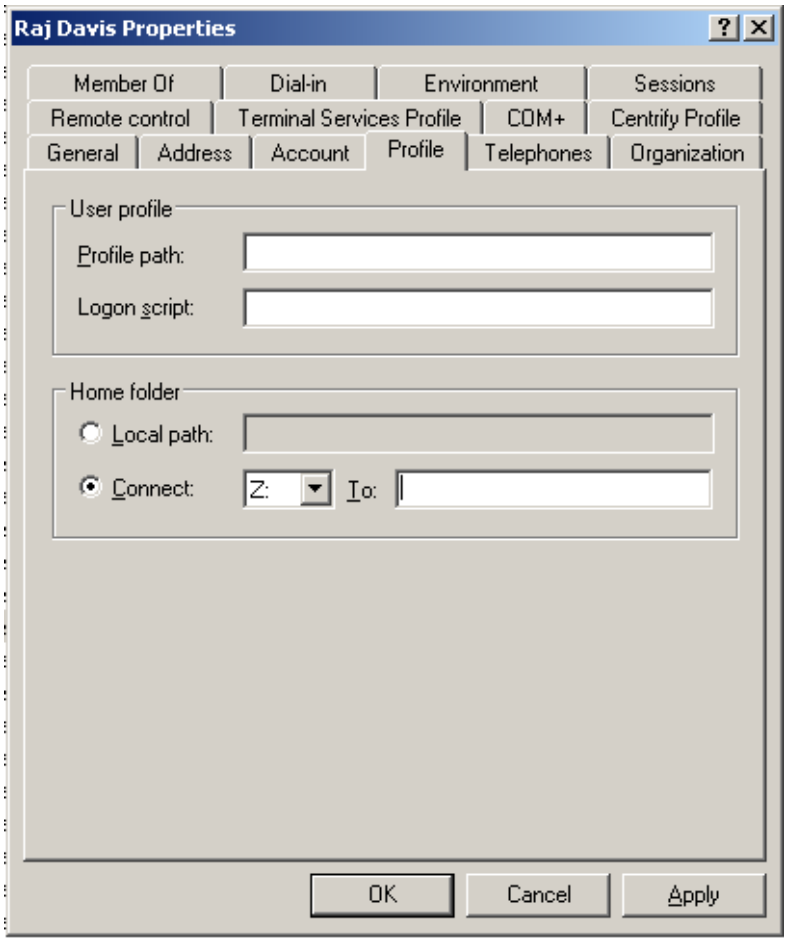
> **Note:** In earlier releases you had to first create a network home directory for a user if you planned to also create a portable home (mobile home) directory for that user. With the current release, you can create portable home directories for users without first creating network home directories for those users.

To configuring a network home directory for a user connected to Auto Zone:

1. Create a network share to host the home directory.

   For example, on the dc-demo server (`acme.com` domain), create a network share called MacUsers.

   You must assign appropriate permissions to the network shared directory so the Active Directory account is able to write to the user's home directory. One way to do this is to assign read/write permissions to Authenticated Users on the network share. Each home directory that is created inherits permission from the network share so the account of the logged-in user is granted write permission its network home directory. See Setting Shared Directory Permissions for more details about properly setting and fine-tuning network share permissions.
2. On a domain controller in the forest to which the Mac OS computer is joined, open Active Directory Users and Computers.
3. Select **Users**, select the user, then right-click the user and click **Properties**.
4. Click the **Profile** tab, then under **Home folder** select **Connect**.



5. In **Connect...To** type the location of the share you created in Step 1 by using the following format:

   `//*Server/share/path`

   For example:

   `//dc-demo.acme.com/MacUsers/rdavis`

6. Click **OK** to save the user profile.
7. (Optionally) By default, the agent is configured to use the Active Directory home folder if one is specified in a user's profile. However, to be explicit, you can edit the configuration file and add the following parameter:

   `auto.schema.use.adhomedir: true`

   Save and close the file.

8. Specify the type of share to mount for the network home directory on the Mac computer, SMB, or AFP.

   By default, the Mac computer will attempt to mount an SMB share for the network home. If you specified an AFP share, you must set the following parameter in the configuration file:

   `auto.schema.remote.file.service:AFP`

Or enable the **Computer Configuration > Policies > Centrify Settings > DirectControl Settings > Adclient Settings > Auto Zone remote file service** group policy to specify SMB (the default) or AFP for all Mac computers.

9. Optionally, if you want the network home directory to be mounted automatically on the user's computer, enable the following group policy: **User Configuration > Policies > Centrify Settings > Mac OS X Settings > Automount Settings > Automount user's Windows home**.

When the specified user next logs onto the Mac computer, the home directory will be created on the specified share. On the Mac computer, you should see the server and share under **SHARED** in the Finder.

Configuring a Portable Home Directory

You can create a portable home directory for a user and synchronize that directory with the share defined in the user's Centrify Profile. You can synchronize to `/SMB/`, `/AFP/`, or `/Network/Servers` (NFS) shares.

Advantages of a Portable Home Directory

- If a user does not have a portable home directory and the computer becomes disconnected from the domain controller (and therefore disconnected from Active Directory), the user can log in with Active Directory credentials only if the user's information exists in the Centrify cache. If there is any issue with the Centrify cache (for example, if the adflush --force command was issued to flush the cache immediately before the computer was disconnected from the domain), Active Directory users cannot log in unless they have portable home directories.
- Active Directory users without portable home directories are required to log in at least once in connected mode to populate their account information in the Centrify cache. If the computer is not connected to the domain controller, the Centrify cache is not updated with the initial set of Active Directory user data, and Active Directory users cannot log in.

  You use group policies to configure synchronization. These group policies perform the same function as the Mobility preferences that you can manage through Workgroup Manager.

The following sections describe the process of specifying the options for creating mobile accounts, and for specifying the options for synchronizing mobile accounts with the network home directory.

Before you begin you should have the following in place:

- A Group Policy Object that applies to a domain or OU that includes Mac users.
- A good understanding of the synchronization rules that you want to apply. The procedures in the following sections explain the group policies and options that you can enable, but you should consult the Mac OS X Server documentation for strategies about which options to apply.

Working with Macs

This section describes the unique characteristics or known limitations that are specific to using Delinea Management Services on a Mac computer.

Specifying the Macintosh User's Home Directory Location

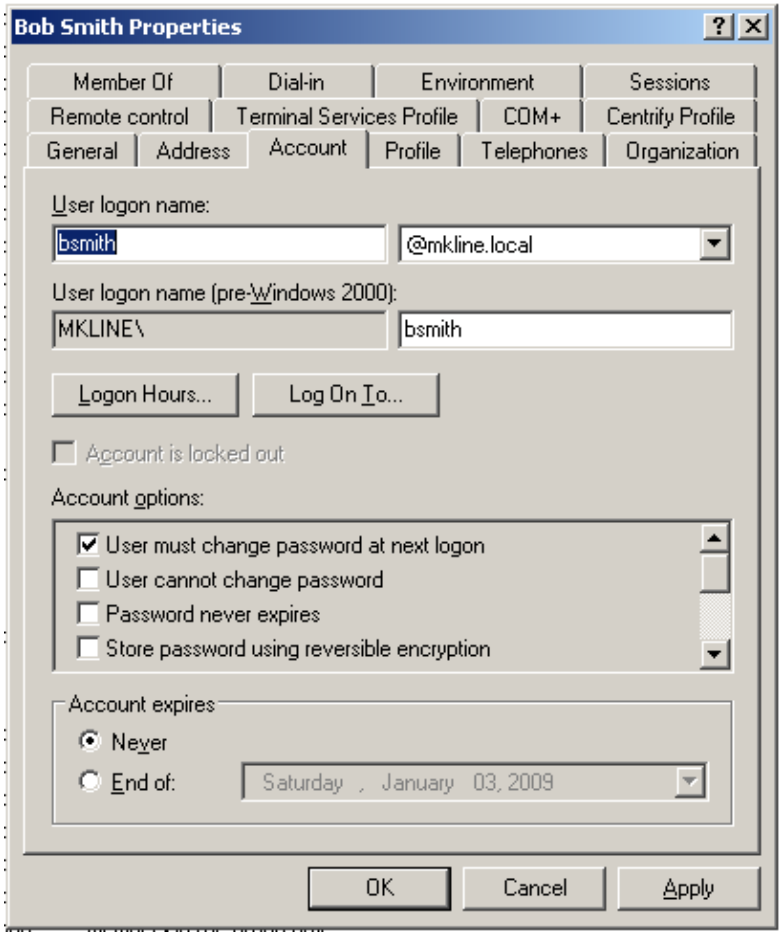
If you configure NFS, SMB, or AFP network file sharing for your Mac OS X computers, you can automatically mount and log on to file shares using Active Directory credentials.

To enable Mac OS X users to log on to file shares when the network is configured with NFS, SMB, or AFP network sharing:

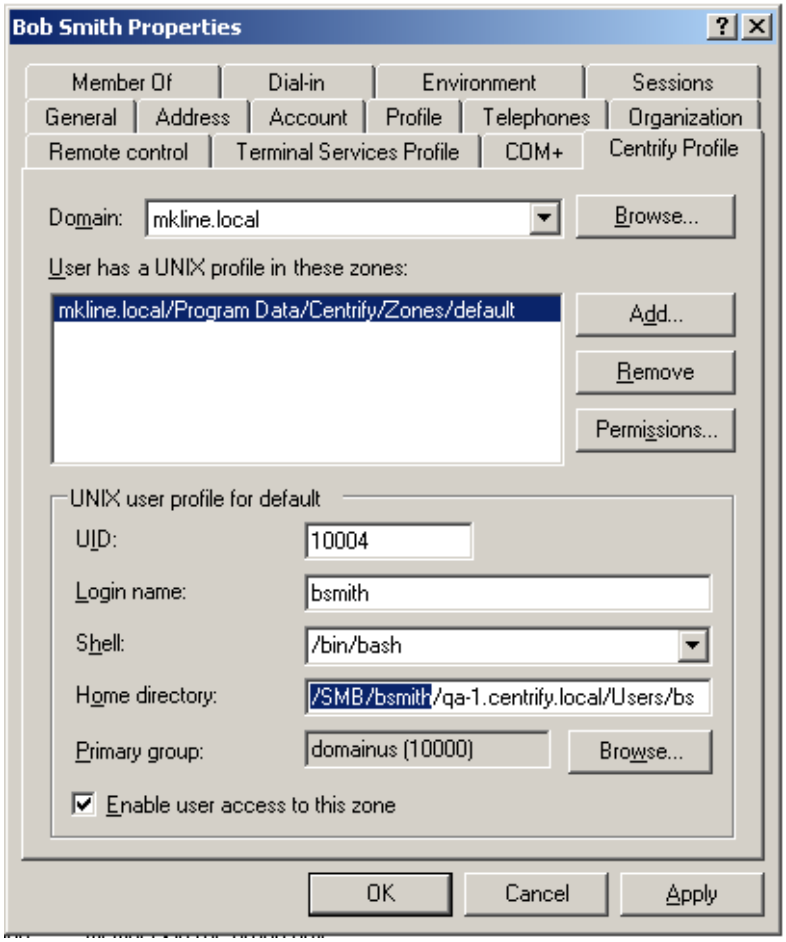
1. Open Active Directory Users and Computers or the Access Manager console.
2. Select the user account for which you want to enable automounting, right-click, then click **Properties**.
3. Click the **Delinea Profile** tab and set the **Home directory** path to use one of the following formats:
   - `/Users/user_login_name` to set the user's home directory to the default home directory location for all user home directories on Mac OS X computers.
   - `/SMB/server_name/share[/path]` to automount a file share on the SMB *server_name* you specify. Be certain to use the fully-qualified domain name for *server_name*, or the IP address. The short name does not work. For example:
     `/SMB/myHost.acme.com/Users/isuzuki`
   - `/SMB/unix_username/server_name/share[/path]` to automount a file share when you are using Fast User Switching on the SMB *server_name* you specify. Be certain to use the fully-qualified domain name for *server_name*, or the IP address. The short name does not work. For example:
     `/SMB/isuzuki/myHost.acme.com/Users/isuzuki`
   - `/AFP/server_name/share[/path]` to automount a file share on the Apple *server_name* you specify.
   - `/AFP/unix_username/server_name/share[/path]` to automount a file share when you are using Fast User Switching on the Apple *server_name* you specify.

     In specifying the remote SMB or AFP file share, you must use the uppercase letters SMB or AFP at the beginning of the path. If you use lowercase letters (smb or afp), automounting fails.

     Note: If you plan to use Fast User Switching to switch between Active Directory users on the same computer, you should use the `/SMB/unix_username/server_name/share[/path]` or `/AFP/unix_username/server_name/share[/path]` format to specify the user's home directory to prevent conflicts between users logging on using the same share. If you want to automount a share on an Apple file server using the Apple File Protocol (AFP), however, you must use Delinea 3.0.1 or later.
4. In Step 3, if you specified a network directory, make sure the Active Directory user logon name (pre-Windows 2000), also known as the samAccountName, matches the Mac login name (UNIX name). Otherwise, the login is not guaranteed to work on all Mac systems. The name must be eight characters or fewer because the UNIX name is automatically truncated to eight characters and won't match if the Active Directory name is longer. The Active Directory name is defined on the **Accounts** tab. To see an example, open the **Properties** page for a user and select **Account**.



Then select the **Delinea Profile** tab to see the UNIX name.



5. For the shared directory you specified in Step 3 (for example, Users), set 'full' permissions for authenticated users. See the section, Setting Shared Directory Permissions, for details on how to do this.
6. Verify that the computer on which the shared directory resides is configured on the DNS server with forward and reverse lookup zones by running the following commands in a terminal window:

   `nslookup computerName.domainName`

   for example:

   `nslookup QA1.acme.com`

   Server: acme.com

   Address: 192.168.1.139

   Name: QA1.acme.com

   Address: 192.168.1.139

   nslookup ipAddress

   for example:

```
nslookup 192.168.1.139
```

Server: acme.com

Address: 192.168.1.139

Name: QA1.acme.com

Address: 192.168.1.139

If you get an error message such as this:

```
Can't find server name for address 192.168.1.139
```

it means a reverse lookup zone is not configured for the specified server. To configure DNS forward and reverse lookup zones, see the Microsoft Support Article 816518.

Populating the Home Directory on a Network Share

If you configure users to automount a network share when they log on, you must determine whether a home directory already exists on the network share for those users. If the individual user's home directory does not exist on the network share, Access Manager creates the home directory automatically the first time the user logs on.

Note: For NFS shares, Access Manager cannot create the home directory on the network share, so you must create the directory before users log in for the first time.

For example, assume you have defined the home directory in a user's Delinea Profile as: `/SMB/demo-dc.acme.com/home/thomas`, indicating that there is an SMB share on the server `demo-dc` and a shared folder named `home` where the user `thomas` has permission to list and create folders.

Note: For the server name, be certain to use the fully-qualified domain name, such as `demo-dc.acme.com`, and not the short version `demo-dc`.

When the zone user `thomas` logs on for the first time, Access Manager creates the new home directory `thomas` and populates it with the standard Mac OS X files and folders.

If the home directory specified in the Delinea Profile for a zone user exists prior to the user's first logon, Access Manager assumes that the directory is valid and contains the appropriate files, and it does not populate the directory with additional Mac-specific folders.

Defining a Home Directory in the Active Directory Profile

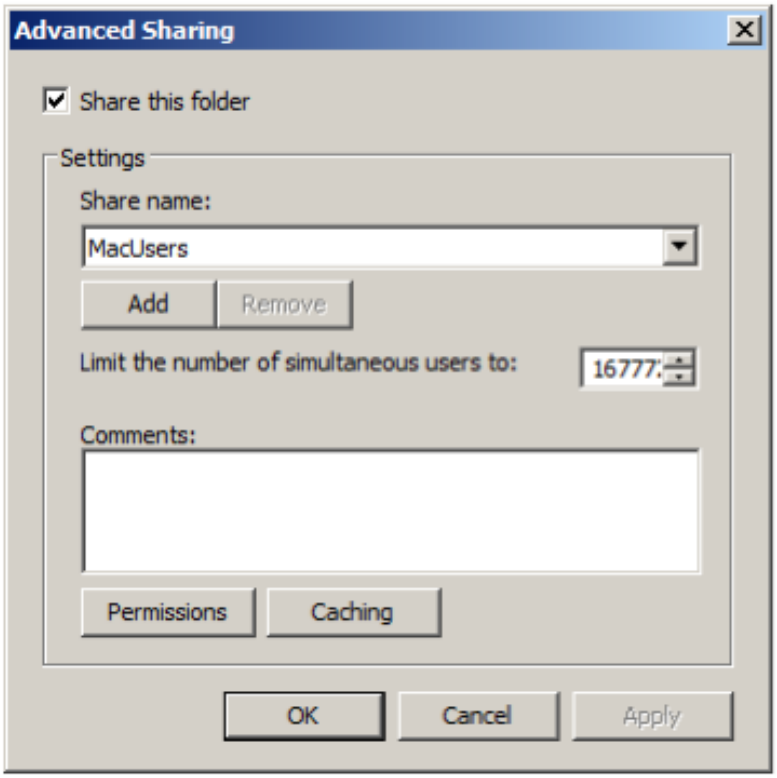
When you are configuring a network home directory for remote Mac users, the home directory is created automatically when users first log; it should not exist prior to that initial log on unless you want to prevent Access Manager from creating the home directory. Therefore, you should not define a home directory connection point in the Profile properties for new Active Directory users or new mobile user accounts. Instead, you should allow Access Manager to create and populate the remote home directory. However if you need to synchronize a network home directory from a local home directory as part of your migration process, the network home directory must exist prior to migration. If you are synchronizing from a local home directory to a remote share, you can create the remote home directory manually, or click the **Profile** tab and set the connection path.

Setting Shared Directory Permissions

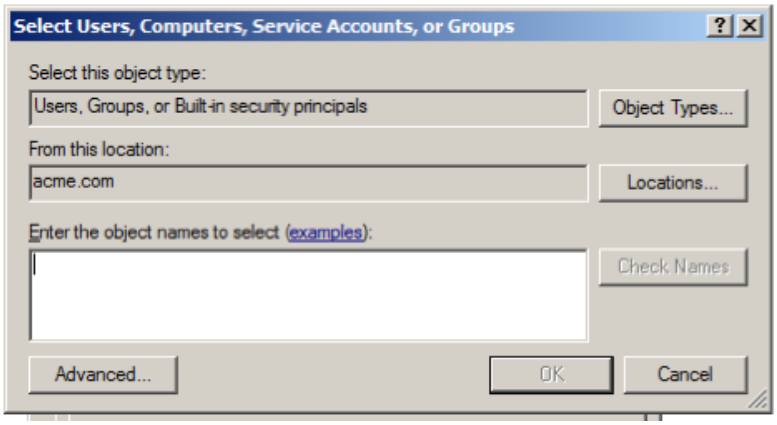
All users who are set up with a network home or portable home directory must have proper permissions to the shared directory in which the home directories are created. Initially, you can provide access to the shared directory through the Windows built-in security group, Authenticated Users. Later, you can fine tune permissions for this group based on your company's file-sharing needs. For example, if an administrator pre-creates home directories for each user before they log in, users only need Read access to the shared directory to access their home directories.

To set permissions for the shared directory for network home and portable home directories:

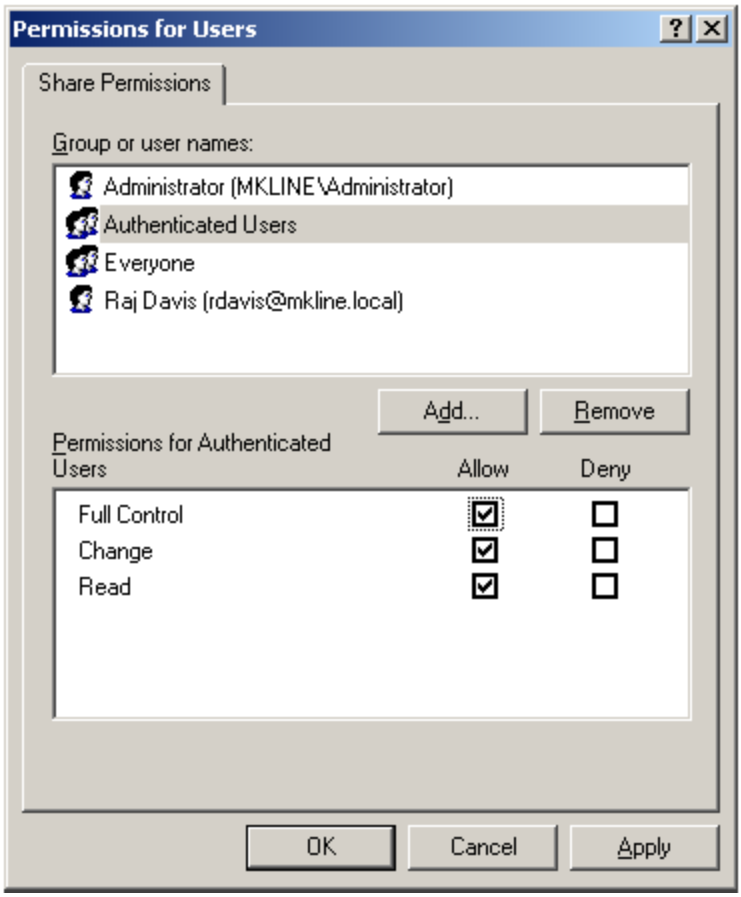
1. On the network share computer, select the directory to share (for example, MacUsers). Right-click, click **Properties** and click the **Sharing** tab; then click **Advanced Sharing**; for example:



2. Make sure **Share this folder** is selected. Click **Permissions**, then click **Add**:



3. Type `auth` and click **OK** to return the Authenticated Users group. Select **Authenticated Users**, then click **Allow** for **Full Control**. Click **OK** to set permissions for authenticated users, then click **OK** again to close the properties page.



4. Verify that Authenticated Users have proper permissions on the **Security** tab as well as on Share Permissions. Ordinarily, these permissions are applied automatically because the Active Directory Users group, which

includes authenticated users, inherits Full Control to the shared folder, but if permissions were altered on the Security tab and they are insufficient, users may be unable to log in.

Click the **Security** tab and select **Authenticated Users** (or if it is not already in the Group or user names box, click **Add** to add it).

5. Select **Full control** and click **OK** to save and close the Properties page.

   Assigning permissions to Authenticated Users on the network home share directory means that each home folder will inherit permissions that enable logged-in users to access their home directories. It also means that every user will have access to every other user's home directory. To change this access, you can set permissions on the individual home directories. For information about fining tuning permissions for individual users, see the next section, **Limiting Users Access to Other Users' Home Folders**.

Limiting Users Access to Other Users' Home Folders

The previous section explained how to assign permissions to a network-home shared folder, which are consequently inherited by the home folders created in the shared folder. Because permissions are inherited, each user has equal access to every other user's home folder. This section explains how to fine tune permissions to limit user's access to their own home folder.

To limit users access to their own home folder:

1. Select the network share you assigned permissions to in the previous section.
2. Select one of the user home directories in the network share.
3. Click the **Security** tab.
4. Click **Advanced** and **Change Permissions**.
5. Deselect **Include inheritable permissions from the object's parent**.
6. Click **Remove** when prompted.
7. Click **Add**.
8. Type `users` and click **Return**.
9. Select the following permissions for Users:
   - Traverse folder / execute file
   - Read Attributes
   - Read Extended Attributes
   - Create files / Write Data
   - Create Folder / Append Data
10. Click **OK**, and **OK** again until you have saved all open dialogs and closed the Properties page.

Enabling Users to Manage Their Print Queues

On Mac computers, Delinea Active Directory users are unable to manage their own print jobs. For example, if they attempt to pause, stop, or resume one of their own print jobs, they are prompted to supply the name and password of a user in the "Print Operator" group, otherwise, they cannot continue. Delinea supplies the group policy, *Map*

zone groups to local group, that you can use to enable all Mac users authenticated through Active Directory to manage their printers.

This policy gives members of a specified zone group (an AD group, or AD group that has been added to a Delinea zone) the privileges that belong to members of a local group on the local group. For example, as explained in the following procedure, mapping an AD group to the local `_lpoperator` and `_lpadmin` groups, provides members of the AD group with the privileges to manage print jobs on the local Mac computer when they log in.

To map a zone group to local `_lpoperator` and `_lpadmin groups`:

For purposes of illustration, this procedure asks you to create a **MacPrint** group and then add specific users to the group to provide them with printing privileges on Mac computers. You could also map an existing AD group to the local `_lpoperator` and `_lpadmin` groups, or create a new group with a different name.

1. On a Windows computer, open Active Directory Users and Computers
2. Select **Users**, right-click and select **New > Group**.
3. Enter a name for the group, such as MacPrint and select **Global** and **Security**.
4. Double-click the group and select the **Members** tab
5. Click **Add** and select the AD users who you want to provide with printing privileges on Mac computers.
6. Open the Access Manager Console
7. Expand the zone hierarchy as well as the zone containing Mac computers.
8. Expand **UNIX Data**, select **Groups**, then right-click and select **Create UNIX Group**.
9. Find and select the AD group you created (MacPrint) and click **OK** to add it to the zone.
10. Open the Group Policy Management Editor and select the GPO that you use for Mac OS X computers.
11. Click **Computer Configuration > Policies > User Configuration > Policies > Delinea Settings > Mac OS X Settings > Accounts**.
12. Double-click **Map zone groups to local group**.
13. Click the **Policy** tab and click **Enabled**.
14. Click **Add** and do the following:
    a. In **Local Group**, type `_lpoperator` to add the printer operators group.
    b. In **Zone Group** click **Browse**.
    c. Find and select the AD zone group you created (MacPrint), then click **OK** to map MacPrint to the printer operators group.
    d. Click **Add** again and in **Local Group** type `_lpadmin` to add the printer admin group.
    e. In **Zone Group**, click **Browse** then find and select MacPrint again to map MacPrint to the printer admin group.
15. Click **OK** to save the policy.

The first time users attempts to manage their printer, for example by pausing the printer, they will be prompted for credentials for a user in the “Printer Operator” group. They can simply enter their own name and password. Subsequently, they can manage the printer without supplying credentials.

Setting Up Authenticated Printing

In a Windows Active Directory environment that requires authentication for printing services, Mac users who are already authenticated must provide credentials again when using a Windows network printer. To provide single-sign on when using printers, the Delinea DirectControl Agent for Mac includes an authenticated printer plug-in that enables users to send print jobs to printers on the Windows network without requiring them to enter credentials again. This plug-in uses the user identifier (UID) of the user printing a job to find the user account to authenticate, then validates the user's Kerberos credentials through Active Directory. If the user's credentials are not available, the print job will fail.

Understanding Printing on Mac OS X

Mac uses the Common UNIX Printing System (CUPS) to manage printing services. Although you can access the CUPS facility directly to manage printers, in general you do not need to do so. Printers are managed through the Print and Scan system preference, which uses the CUPS facility. For example, when you add a printer through Print and Scan, the CUPS facility does the following:

- Creates a Postscript Printer Description (PPD) file that defines the printer. The file is given the name of the printer and resides in the `/etc/cups/ppd directory`; for example, `/etc/cups/ppd/laserjet2.ppd`.
- Modifies the CUPS configuration file, `/etc/cups/printers.conf`, with information about the new printer.

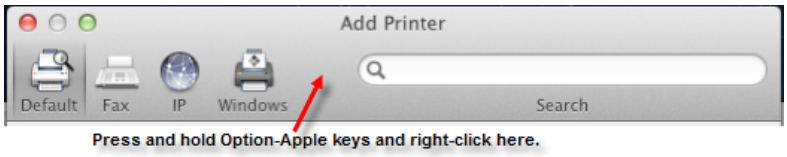
One method to set up authenticated printing for all Mac computers in your environment is to configure an authenticated printer on one (template) computer, then export the files that CUPS creates to define this printer (*printerName*.ppd and printers.conf) to each of your Mac computers. You can use group policy to export these files to all your Mac computers.

You can also configure printing directly with CUPS commands.

To set up authenticated printing for multiple printers using the Delinea plug-in, first identify the printer to configure, including the server that hosts it; for example, `HPLaserJet2.@dc01`.

1. On the Mac computer that you will use to define an authenticated printer template, open **System Preferences > Print & Scan** (**Print & Fax** on older systems), then click the plus sign (+) and select **Add Other Printer or Scanner**.
2. Double-click the **Advanced** icon in the toolbar.

   Note: If the Advanced option is not showing, press and hold the **Option** and **Apple** keys and right-click in the open area in the toolbar next to the Windows icon and select **Customize Toolbar**. Drag the Advanced icon to the toolbar and click **Done**. Then double-click it.



3. Scroll in the **Type** drop-down list and select **Windows Printer via Delinea** from the list.

   Note that after you make this selection, the URI scheme in the Device URI window changes to `cdcsmb://`, which specifies the Delinea plugin.

4. Type the complete URI specification for the printer in the form:

   `scheme://servername/sharename`

   for example:

   `cdcsmb://printserver.acme.com/hplaserjet2`

   Note: A URI specification does not accept spaces. If the printer share name contains spaces, you must replace them with %20 (ASCII code for space); for example, to specify the **HP Color LaserJet 4** printer:

   `cdcsmb://printserver.acme.com/HP%20Color%20LaserJet%204`

5. Type a name for the printer; for example HPLaserJetMac.

   When you type the URI for the printer, the first part of the name automatically appears in the **Name** field. You can change that name now. This is the name that will appear in the list of printers in the Print and Scan system preference and in the list of available printers when a user prints a document. It is also the name of the PPD (Postscript Printer Description) file that the CUPS facility creates for each printer that is added to your Printer preferences.

   Type an optional description in **Location** to assist users in locating the printer.

6. In the **Print Using** window, specify the type of the printer, which enables you to properly manage the printer.

   For example, if you have drivers installed for the printer, click **Select Printer Software** and select the appropriate item such as **HP Laserjet 4300**, then click **OK**.

   You can also specify **Generic Postscript Printer**, or click **Other** to browse for drivers or printer software.

   Click the **Add** button to add the printer to the list of available printers.

7. Repeat this procedure for as many printers as you want to make available for authenticated printing.

You can now use the Copy Files group policy to copy the new *printerName*.ppd file and updated CUPS configuration file (`printers.conf`) to the appropriate locations on each of your Mac computers in the domain.

To copy printer files to other computers:

1. In the Finder on the Mac template computer, navigate to the `/etc/cups` directory by clicking **Go > Go to Folder**, then type `/etc/cups` and click **Go**.
2. Select `printers.conf` and copy it to the desktop. When prompted, enter your administrator password to copy the file.
3. Open the ppd folder (`/etc/cups/ppd`). Select the files for all the authenticated printers you defined in the previous procedure and copy them to the desktop.
4. On the desktop, change the file permissions for the `printers.conf` and `*.ppd` files so you can copy them to sysvol:
   a. Select the files and click **File > Get Info**.
   b. For each open dialog box, expand **Sharing & Permissions**, then click the lock icon and provide administrator credentials for making changes. Set the permissions for **everyone** to **Read only**.
   c. Reset the lock and close all the open dialogs.
5. On the Windows domain controller create a sub-directory for the printer file in SYSVOL.

SYSVOL is a well-known shared directory on the domain controller that stores server copies of public files that must be shared throughout the domain. You can use it to copy the printer definition and configuration files to all Mac computers that join the domain.

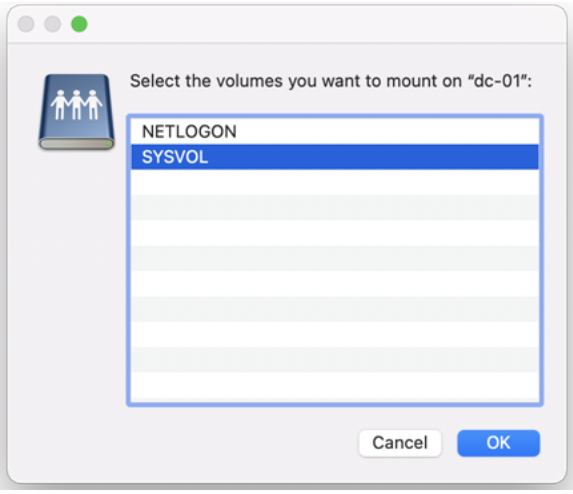
SYSVOL is located at:

`C:WindowsSYSVOLsysvoldomainName`

For example, assuming the domain is acme.com, and using the name MacPrinters for the directory, create the following directory:

`C:WindowsSYSVOLsysvolacme.comMacPrinters`

6. On the Mac computer, copy the files from the desktop to SYSVOL on the Windows domain controller. If you are connected to the domain, you should see the domain controller in the Finder. If the domain controller is not visible in the Finder, connect to it:
   a. Click **Go > Connect to Server** and select the domain controller.
   b. When prompted select SYSVOL; for example:



   c. Navigate to the MacPrinters directory you created, for example by clicking **acme.com** then **MacPrinters**.
   d. Drag the printer files to MacPrinters.
7. Configure the Copy Files group policy.
   a. On the Windows domain controller, open the Group Policy Management Editor and select the GPO that is used to manage Mac computers.
   b. Navigate to **Computer Configuration > Policies > Common UNIX Settings** and double-click **Copy Files**.
   c. In **Copy file policy setting**, select **Enabled**.
   d. Click **Add**, then **Browse**. Double-click to open the directory you created for the printer files in Step 5 (for example, MacPrinters).
   e. Select the printers.conf file. Filename now shows `MacPrinters/printers.conf`.

f. In **Destination**, type `/etc/cups`. This group policy will copy `printers.conf` to the `/etc/cups` directory of each computer that joins the domain.

g. Select **Use destination file ownership and permissions**. The file will be assigned the default ownership and permissions:

   owner: `root (0)`

   group: `lp (26)`

   permission `0600 (rw- --- ---)`

h. Select **OK** to add the printers.conf file.

8. Click **Add** again and browse to MacPrinters to add the PPD files.

   a. Select one of the PPD files you copied to the MacPrinters directory.

   b. In **Destination**, type `/etc/cups/ppd`.

   c. Select **Use destination file ownership and permissions**. The file will be assigned the default ownership and permissions:
   owner: `root (0)`

   group: `lp (26)`

   permission `0644 (rw- r-- r--)`

   d. Click **OK** to add the file.

9. Repeat the sub-steps in Step 8 for each of the PPD files that you have defined, then click **OK** to enable the policy.

   This group policy will copy each *printerName*.ppd file to the `/etc/cups/ppd` directory of every computer to which the policy applies and that is joined to the domain.

10. Run the adgpupdate command on each target Mac computer to trigger an update of group policies and execute the new Copy Files policy.

    By default, group policies are updated automatically every 90 minutes, so you can skip this step and wait for the automatic update if you wish. You should also log out and back in again on each computer to update the printer configuration dialogs.

Removing a Printer Definition from Client Computers

This section explains how to remove printer definitions that you created for Mac computers in the domain. It assumes that you set up the Copy Files group policy to add printer definitions to each of your joined Mac computers, as explained in Setting up Authenticated Printing.

To remove a printer definition from computers in a domain:

1. Identify the name of the PPD file to delete in `/etc/cups/ppd`; for example, `laserjet4300.ppd`.
2. On the Mac template computer (the computer on which you originally defined the authenticated printer), open **System Preferences > Print & Scan**. Select the printer to delete, click the minus (-) button, then click **Delete Printer**.

Deleting the printer removes the printer from the list, updates the `/etc/cups/printers.conf` file by removing the definition of the deleted printer, and removes the *printerName*.ppd file from the `/etc/cups/ppd` directory.

3. Copy the updated `printers.conf` file to the desktop and change the permissions to **everyone: Read only**.
4. Copy the updated `printers.conf` file to the SYSVOL and replace the existing file; also remove the PPD file for the deleted printer.

   SYSVOL is a well-known shared directory on the domain controller that stores server copies of public files that must be shared throughout the domain. When authenticated printing was set up, the CUPS configuration file, printers.conf was placed in the `SYSVOL/acme.com/MacPrinters` folder.

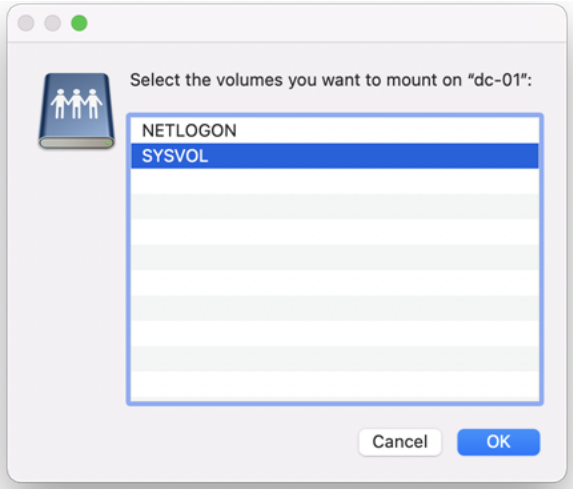
   SYSVOL is located at:

   `C:WindowsSYSVOLsysvoldomainName`

   If you are connected to the domain, you should see the domain controller in the Finder. If the domain controller is not visible in the Finder, connect to it:

   a. Click **Go > Connect to Server** and select the domain controller.

   b. When prompted, select **SYSVOL**; for example:



   c. Navigate to the directory you created (*domainName*/*subdirectory*), for example by clicking **acme.com** then **MacPrinters**.

   d. Drag the printer configuration file to this directory.

   e. Remove the PPD file for the deleted printer.

5. Remove the deleted `printerName.ppd` file from the Copy Files policy.

   a. On the Windows domain controller, open the group policy editor and select the policy to edit, such as **Default Domain Policy**.

   b. Navigate to **Computer Configuration > Policies > Common UNIX Settings** and double-click **Copy Files**.

   c. Select the file to delete and click **Remove**.

   d. Click **OK** to save the updated policy.

6. Configure the **Specify commands to run** group policy to remove the deleted *printerName*.ppd file from all the Mac computers in the domain.
   a. In the same folder of the group policy editor (Common UNIX Settings), open the Specify commands to run policy and select **Enabled**.
   b. Click **Add**.
   c. In **Run command**, enter a command similar to the following to remove the *printerName*.ppd file from the /etc/cups/ppd directory on each computer:

      ```
      rm /etc/cups/ppd/*printerName*.ppd; for example:
      rm /etc/cups/ppd/laserjet4300.ppd
      ```

   d. Click **OK** to save the policy.

The next time group policy is updated on computers in the domain (every 90 minutes by default), the following occurs:

- The Copy Files group policy copies the updated printers.conf file to each computer.
- The Specify commands to run group policy removes the specified PPD file on each computer.

Setting Up Local and Remote Administrative Privileges

Delinea provides two group policies to set administrative privileges on the local computer

- Map zone groups to local admin groups allows you to specify one or more zone groups to map to the local admin group. Members of the specified group are given administrative privileges on Mac computers managed by Access Manager.
- Enable administrator access groups allows users in the zone group *ard_admin* to access a computer via Apple Remote Desktop with full privileges.

This section shows you how to use these policies together to enable local and remote administrative access to Mac computers.

To enable remote and local access for a group:

1. Create an Active Directory group, for example, *My_Mac_Admins*, and add users who you want to have administrative privileges.
2. Create an Active Directory group that is a Domain Local Security group. For convenience, name it *ard_admin*.
3. Add *My_Mac_Admins* as a member of *ard_admin*.
4. Create a Delinea zone group, *My_Mac_Admins* and map it to the Active Directory group *My_Mac_Admins*.

   Note: If the local computer is connected to the domain through Auto Zone, you cannot create a zone group because there are no zones. However, all Active Directory groups are valid for the joined computer, so you can map any group, such as *My_Mac_Admins*, to the local admin group, but you need to know the group's UNIX name, which you can retrieve on the local computer, by using the `adquery` command, as follows

   ```
   [root]#adquery group -n
   ```

   For example, the following shows an adquery command and the name it returns:

```
[root]#adquery group -n |grep -i Mac_Admins my_mac_admins
```

5. Create a zone group, *ard_admin*, and map it to the Active Directory group *ard_admin*.

   Note: This zone group must be named *ard_admin*.

6. In the Group Policy Editor, edit the group policy for the domain, then click **Computer Configuration > Policies > Centrify Settings > Mac OS X Settings > Accounts > Map zone groups to local admin group**.
7. Open the policy, select **Enable**, then click **Add**. Enter *My_Mac_Admins* (or the name retrieved from the `adquery -n` command in Step 4), then click **OK**.

   This step maps *My_Mac_Admins* to the admin group on the local computer and gives members of *My_Mac_Admins* all privileges.

8. Click **Computer Configuration > Policies > Centrify Settings > Mac OS X Settings > Remote Management > Enable administrator access groups**.
9. Open the policy and select **Enable**.

   This step allows members of *ard_admin* to access a computer via Apple Remote Desktop with full privileges. In Step 7, you effectively gave members of *My_Mac_Admins* administrative privileges. Since *My_Mac_Admins* includes members of *ard_admin*, members of *ard_admin* now have full local and remote administrative access.

Querying User Information for Active Directory Users

When you run commands or use applications that look up user information in the directory, the local Mac directory service is always consulted first before the look-up request is made to Active Directory. If a local user exists with the same name as a UNIX profile name that has been defined for the zone, a lookup request such as id *username* will return the UID and GID associated with the local user account from the local directory service rather than the information associated with the UNIX profile defined in Active Directory.

For example, if you have a UNIX profile in Active Directory for the user `mia` with the UID of `10024` and the user's primary group is `mia` with the GID of `10024` and the user is also a member of the Active Directory group `users` and GID of `10001`, running the `id mia` command returns the following information from Active Directory:

```
uid=10024(mia) gid=10024(mia) groups=10024(mia), 10001(users)
```

However, if there is also a local user account with the same user name of `mia`, but with a UID of 502 and a primary group named *mia* with a GID of 502, running `id mia` returns the information for the local user retrieved from the Mac directory service, then any additional group membership information retrieved from Active Directory. For example:

```
id mia
uid=502(mia) gid=502(mia) groups=502(mai), 10001(users)
```

Because the Mac directory service is queried first, the information for the local user mia takes precedence over the information defined in Active Directory. To avoid retrieving the information for a local user instead of the UNIX profile defined in Active Directory, you should make sure that the UNIX profile user names in Active Directory are different from the local user or disable local user accounts.

Migrating from Open Directory to Active Directory

If you install the Delinea DirectControl Agent for Mac in an environment where existing Mac users and computers are managed with Open Directory, you may need to migrate the account information and home directories for those users from the Open Directory environment to Delinea Active Directory. Open Directory and Active Directory support three types of users:

- Local users
- Network home users
- Portable home, or mobile home, users

For example, you may need to migrate existing mobile user accounts from Open Directory to Active Directory or migrate local home directories to a network share.

To migrate users with existing mobile accounts from Open Directory to Active Directory:

1. Create a copy of the user's local home directory in a temporary location if you have enough disk space to do so. This copy can serve as a backup to restore the user's home directory if you run into any synchronization problems.
2. Log on to the Mac client as an administrator.
3. Disable the LDAP service.

   Open the Directory Utility and select the **Services** tab; then deselect **LDAPv3** and click **Apply**.
4. Open a Terminal window and run the following Directory Service command to delete the user's record:

   ```
   dscl /Local/Default -delete /Users/userName
   ```

   where *userName* is a local user; for example, to delete the record for cain:

   ```
   dscl /Local/Default -delete /Users/cain
   ```
5. Navigate to the `/Users/user_name/Library/Mirrors` directory and delete this folder.
6. Join the Mac computer to an Active Directory domain and restart the computer to shut down and restart services.
7. Create an Active Directory user account for the Open Directory user account, if one does not already exist.

   If you are creating a new Active Directory user, use Active Directory Users and Computers to add the user account.
8. Add the Active Directory user to the Mac computer's zone and define the Delinea Profile for the user:
   - Use the same user name, UID, and GID as the Open Directory user account. You can change this information later with the `adfixid` program, but for migration you must use the same values.
   - Set the home directory for the user to the appropriate network share using the `/SMB/share/path` or `/AFP/share/path` syntax. For example, `/SMB/cain/server2003.myDomain.com/Users/cain`.

     Note: For synchronizing new mobile user accounts, the empty home directory must exist on the network share. If the user home directories are on the same network share as you previously used with Open Directory, logging on with the new Active Directory account should not affect the files available on the share.

Because GID values of 0 to 99 are usually reserved for system accounts, you may see a warning message when you save the user's profile if the user's primary GID value is less than 99.

If you have Open Directory users that do not have mobile accounts or portable home directories and you want to synchronize their local home directories with their network home, you should first use the Workgroup Manager to create mobile accounts for those users to establish a portable home directory. You can then follow the steps above to synchronize the portable home directories with their network home directory. If you don't want to synchronize the local home directory with the home directory on the network share, you can simply create Active Directory accounts for the Open Directory users and remove the local user records.

Changing the Delinea UIDs and GIDs

To change the UID and GID values in Delinea Active Directory to match the existing values:

1. Log in to the Mac computer as a local administrator.
2. Open a terminal session.
3. Open the user's home folder and type:

   ```
   ls -ln total 32
   -rw-r--r--@ 1 505 505 3 Mar 26 2007 .CFUserTextEncoding
   -rw-r--r--@ 1 505 505 6148 Mar 26 2007 .DS_Store
   -rw------- 1 505 505 74 Mar 26 2007 .bash_history
   drwx------@ 3 505 505 102 Mar 26 2007 Desktop
   drwx------@ 3 505 505 102 Mar 26 2007 Documents
   drwx------@ 19 505 505 646 Mar 26 2007 Library
   drwx------@ 3 505 505 102 Mar 26 2007 Movies
   drwx------@ 3 505 505 102 Mar 26 2007 Music
   drwx------@ 4 505 505 136 Mar 26 2007 Pictures
   drwxr-xr-x@ 4 505 505 136 Mar 26 2007 Public
   drwxr-xr-x@ 5 505 505 170 Mar 26 2007 Sites
   ```

   The third column shows the UID (505 in this example) and the fourth column shows the GID (also 505).
4. On the Windows workstation, open the Access Manager console. Expand the zone, expand users, and double-click the user to open the property page.
5. Type 505 for the UID.
6. To change the GID, you need to either change the GID of the group to which the user belongs (which will change for all users who belong to that group) or create a new group. To create a new group:
   - Open ADUC. Then right-click **Users > New > Group**. Enter a name for the group and click **OK**.
   - In the Access Manager console, right click **Groups > Create UNIX Group**. Search for the group you created. Change the GID to the desired value (for example, 505) and click **OK**.

7. To change the GID of the existing group to which the user belongs, expand **Groups** and double-click the group name. Change the GID to the desired value (for example, 505). Click **Yes** on the warning message.

Modifying the Mac UID and GID to Match AD

To change the existing UID and GID to match the values in Active Directory depends on whether you have a local home directory, a network home directory, or a mobile home directory.

To change the existing UID and GID if you have a local home or network home directory:

1. Log in to the Mac computer as a local administrator.
2. Open **Applications > Directory Utility > Services**. Double-click **Active Directory**, then click **Unbind**. Enter your administrator name and password if necessary.
3. Use the `ADJoin` tool (either the GUI or the command-line version) to connect to an Active Directory domain.
4. Open a terminal session and type the following:

   ```
   id userName
   ```

   Note the primary group. For example:

   ```
   id cain
   ...
   gid=10000(support)
   ```

5. Type:

   ```
   chown -R userName:primaryGroupName /Users/userName
   ```

   For example, for a local home directory:

   ```
   chown -R cain:support /Users/cain
   ```

   For example, for a network home directory:

   ```
   chown -R cain:support /SMB/Users/cain
   ```

To change the existing UID and GID if you have a mobile home directory:

1. Be certain the local home directory is synchronized with the network home directory.
2. Log in to the Mac computer as a local administrator.
3. Open **Applications > Directory Utility > Services**. Double-click **Active Directory**, then click **Unbind**. Enter your administrator name and password if necessary.
4. Use the ADJoin tool (either the GUI or the command-line version) to connect to an Active Directory domain.
5. Open a terminal session and type the following Directory Service command to delete the cached local user:

   ```
   dscl . -delete /Users/userName
   ```

   For example:

   ```
   dscl . -delete /Users/cain
   ```

6. Then type the following commands to remove the home directory so that it syncs again from the network and remove the local copy of mcx so you are prompted to create a mobile account:

   ```
   rm -rf /Users/userName
   ```

```
rm -rf /Library/Managed Preferences/userName
```

7. On the Windows Active Directory computer, set the **User Configuration > Policies > Centrify Settings > Macintosh Settings > Mobility Synchronization Settings** group policies.

   Note: Mobile home directory synchronization is no longer supported since macOS 10.12.

Converting a Local User to an Active Directory User

Although local user accounts can co-exist with Active Directory user accounts, in some cases, you may want to convert some or all of your local accounts to Active Directory user accounts. Converting local users to Active Directory users simplifies account management, but requires you to take some steps manually.

On Mac computers, the local account database is always checked for authentication before Active Directory. If a local user has the same username as an Active Directory user, the local user account is used for authentication. If the local user's password is different from the Active Directory user's password whether logging on using the Mac login window, or remotely (for example, using `telnet` or `ssh`), the local user password is required for authentication to succeed. Although authentication succeeds, Access Manager will generate a username conflict warning.

In most cases, you should remove or convert local user accounts to avoid conflicts between Active Directory and local user accounts and to ensure Active Directory password and configuration policies are enforced. If you need to keep local user accounts, you should ensure the logins are distinguishable from Active Directory accounts. For more information, see the Planning and Deployment Guide.

To convert a local Mac user to an Active Directory user:

1. Open a Terminal window and run the following Directory Service command to delete the user's record:

   ```
   dscl /Local/Default -delete /Users/userName
   ```

   where *userName* is a local user; for example, to delete the record for cain:

   ```
   dscl /Local/Default -delete /Users/cain
   ```

   Although the user record is deleted, the home directory for the user (/Users/cain), including all sub-directories and files, still exists. When you create an Active Directory user with the same name, this user will have access to everything in the existing local home directory.

2. On a Windows computer, use Active Directory Users and Computers to create an Active Directory user account for the local user account (for example, `cain`), if one does not already exist.

3. In the Access Manager console add the Active Directory user to the appropriate zone and define the Delinea Profile for the user. Set the home directory for the user:

   Note: The default home directory for Mac users is the `/Users` directory, unlike most UNIX systems where `/home` is the default by convention.

   - To a local home directory: /Users/*userName*; for example, `/Users/cain`.
   - To an appropriate network share using the `/SMB/share/path` or `/AFP/share/path` syntax. For example, `/SMB/cain/server2003.myDomain.com/Users/cain`. See Configuring a network home directory.
   - To a network home directory. If you wish, you can create a mobile account for the user and synchronize the user's folders the next time the user logs on.

4. Reboot the Mac computer, then log in as the new Active Directory user.

Migrating a User from Apple's Active Directory Plugin to Delinea Active Directory

When you create an Active Directory user by using the Mac Directory Utility Active Directory plug-in it creates numeric user (UID) and group (GID) identifiers. When you migrate a current Active Directory user to Delinea Management Services for Mac, the Access Manager console creates a UID and GID that are different than the current UID and GID. When an Active Directory user attempts to log in after the agent is installed, the changed UID and GID cause ownership and permission problems with the user's home directory.

There are two basic approaches to solving this problem:

- Changing the Delinea UIDs and GIDs
- Modifying the Mac UID and GID to Match AD

Using Apple's Scheme to Generate UIDs And GIDs For Mac Users

By default, Delinea uses a different scheme than the Apple Active Directory plugin to generate numeric user (UID) and group (GID) identifiers for Mac users added to Active Directory. If you use the default Delinea scheme to generate identifiers, you must resolve UID and GID conflicts after migrating users. For example, after migrating you can change ownership on the existing files (see Modifying the Mac UID and GID to Match AD otherwise users have Delinea-generated UIDs whereas their files belong to Apple-generated UIDs so users will be unable to access files and folders in their home directories.

On the other hand, Delinea allows you to use the Apple scheme, rather than the default Delinea scheme, to create UIDs and GIDs for migrated users. This method ensures compatibility with Mac tools, such as ExtremeZ-IP, that require UIDs and GIDs generated with the Apple scheme, not the Delinea scheme.

This section explains how to create Apple-generated UIDs and GIDs for Mac users who you are adding to Active Directory with Delinea Management Services for Mac when a computer is connected to Delinea Active Directory through Auto Zone.

> **Note:** If your computer is joined to a zone, however you are adding users to the zone, you can choose to use the Apple scheme to generate UID and GID values. For example, you can specify the Apple scheme with `adedit`, with the Zone Provisioning Agent, and in the Access Manager Console.

Delinea provides the `auto.schema.apple_scheme` parameter to enable use of the Apple schema for generating UIDs for new users. The recommended way to set this parameter is by way of group policy so that you can set it for a group of computers. You may also set the parameter on individual computers by editing the Delinea configuration file

To use group policy to enable the Apple scheme for generating UIDs and GIDs:

1. If you are generating new UIDs and GIDs for files that reside remotely in AFP or NFS mounted shares, back up the UIDs and GIDs on the computer where the share resides by executing a command similar to the following:

   ```
   adquery user > olduid
   ```

   > **Note:** You do not need to perform this step for Samba shares.

2. On a Windows computer, open the Group Policy Management Editor and edit a group policy object that applies to Mac computers.
3. Expand **Computer Configuration > Policies > User Configuration > Policies > Centrify Settings > Direct Control Settings > Adclient Settings**, and double-click **Generate New UID/GID using Apple scheme in Auto Zone**.
4. Select **Enabled** and click **OK** to set the policy.

To edit the configuration file and enable the Apple scheme for generating UIDs and GIDs on a single computer:

1. If you are generating new UIDs and GIDs for files that reside remotely in AFP or NFS mounted shares, back up the UIDs and GIDs on the server where the computer resides by executing a command similar to the following:

   ```
   adquery user > olduid
   ```

   Note: You do not need to perform this step for Samba shares.

2. Log in to a Mac computer.
3. Edit the Delinea configuration file: `/etc/centrifydc/centrifydc.conf`.
4. Find the following parameter, remove the comment and set its value to true:

   ```
   auto.schema.apple_scheme: true
   ```

You may also enable the Apple scheme to set the primary GID for users if you wish.

Note: You may set the primary GID in this way only if the parameter `auto.schema.private.group` is set to false. Otherwise, the primary GID is set to the value of the user's UID.

To enable the Apple scheme for generating the primary GID:

1. If you are generating new UIDs and GIDs for files that reside remotely in AFP or NFS mounted shares, back up the UIDs and GIDs on the computer where the share resides by executing a command similar to the following:

   ```
   adquery user > olduid
   ```

   Note: You do not need to perform this step for Samba shares.

2. In the Group Policy Management Editor, edit a group policy object that applies to Mac computers, expand **Computer Configuration > Policies > User Configuration > Policies > Centrify Settings > Direct Control Settings > Adclient Settings**, and double-click **Set user's primary gid in Auto Zone**.
3. Select **Enabled**.
4. In **Set user's primary gid in Auto Zone**, type `-1`.

   The primary GID for each user will be generated by the Apple scheme, as specified with the "Generate New uid/gid using Apple scheme in Auto Zone" group policy, which you enabled in the previous procedure.

5. Click **OK** to save the setting.

After setting these policies, run `adgpupdate` to update the group policies you just set, and flush the cache on each joined computer to update the UID and GID values for any existing users.

To flush the cache on each Mac computer:

1. Log in to a Mac computer and open the Terminal application.
2. Execute the following command as root:

   ```
   adflush
   ```

New users who you migrate to Active Directory from the Apple Active Directory plug-in will automatically keep the same UID, GID, and primary GID values that they had before migration, and their home ownership will work properly.

After you flush the cache, any existing users and groups will have their UID, GID, and primary GID values changed from the Delinea scheme to the Apple scheme. However, ownership of files and folders in home directories will still belong to the Delinea UID and GID. To change ownership to the new UID and GID generated by the Apple scheme, run the `fixhome.pl` script as explained in the following procedure.

To correct file ownership by running fixhome.pl

Note: If you generated new UIDs and GIDs for files that reside remotely in AFP or NFS mounted shares, the `fixhome.pl` script does not have permission to change UIDs and GIDs in the share, and you must manually update the UIDs and GIDs on the server where the share folders reside. In this scenario, skip to *Workaround for AFP and NFS Mounted Shares* below and continue from there.

For Samba shares and local UIDs and GIDs:

1. Log in on a Mac computer for which you have changed UID and GID values to the Apple scheme.
2. Execute the following command as root:

   ```
   /usr/local/share/centrifydc/sbin/fixhome.pl
   ```

The script changes ownership of files and folders in the home directory of all Active Directory users from the Delinea-generated UID or GID to the Apple-generated UID or GID.

The script uses /Users as the root for all home directories. You may specify a different home root if necessary by using the `--dir` option. Use the `--help` option to see a list of options that you can specify with this command:

```
/usr/local/share/centrifydc/sbin/fixhome.pl --help
```

For example, you can run the command in test mode to see the changes that will be made, but without committing the changes:

```
[root]#/usr/local/share/centrifydc/sbin/fixhome.pl --test
User Home UID Map GID Map
user1 /Users/user1 796918879=>558948313 20=>5287576209
```

Or you could update specific users rather than all users:

```
[root]#/usr/local/share/centrifydc/sbin/fixhome.pl --include user2
```

Workaround for AFP and NFS Mounted Shares

For AFP and NFS mounted share folders (or remote file systems), fixhome.pl does not have permission to change the UID/GID of files in the folder. Perform the following steps to work around this issue:

1. On the server where the share folders reside, open the UID/GID backup file to have access to the old UID/GID strings.
2. On the server where the share folders reside, change the old UIDs and GIDs to the new UIDs and GIDs one at a time by executing commands similar to the following:

   ```
   find ShareFolder -user previous_uid -group previous_gid -exec chown new_uid:new_gid {} ;
   ```

To enable the Apple scheme for mobile users:

Additional steps are required to enable the Apple scheme for mobile users. After enabling the Apple scheme as described in the preceding sections, you must ensure that the UID and PGID for the mobile user's local user record match the UID and PGID used by the DirectControl agent.

1. Change the UID and PGID in the local user record so that they match the IDs used by the agent:
   a. Open **Users and Groups**.
   b. Right-click the mobile user account.
   c. Choose **Advanced Options**, and change the UID and PGID so that they match the IDs used by the agent.
2. After changing the UIDs and PGIDs of mobile users, run the `fixhome.pl` script as described above in *To correct file ownership by running fixhome.pl*.

To use the Zone Provisioning Agent to enable the Apple scheme for generating UIDs and GIDs:

1. Ensure that the Zone Provisioning Agent is configured as described in the section "Configure the Zone Provisioning Agent" in the *Planning and Deployment Guide*.
2. Ensure that zone provisioning groups are created and configured as described in Chapter 8, "Preparing the Environment for Migration of Existing Users and Groups" in the *Planning and Deployment Guide*.
3. Start Access Manager.
4. In the console tree, expand the **Zones** node.
5. Select the top-level parent zone, right-click, then click **Properties**.
6. Click the **Provisioning** tab.
7. Click **Enable auto-provisioning for group profiles**.
8. Click the Find icon to search for and select the primary group (typically the Domain Users group) as the Source Group.
9. Select **Generate using Apple scheme** as the method for assigning a new GID to new UNIX group profiles.

   This method generates group GIDs based on the Apple algorithm for generating numeric identifiers from the Active Directory group's `objectGuid`. This option is only supported for hierarchical zones.
10. Select a method for assigning a new group name to new UNIX group profiles:
    - **SamAccountName attribute** generates the group name for the new UNIX group profile based on the `samAccountName` value.
    - **CN attribute** can be used if you verify the common name does not contain spaces or special characters. Otherwise, you should not use this option.

- **RFC 2307 attribute** can be used if you have added the RFC 2307 groupName attribute to Active Directory group principals. Otherwise, you should not use this option.
- **Zone default value** to use the setting from the Group Defaults tab for the zone. In most cases, the default is a variable that uses the `sAMAccountName` attribute.
- By default, all UNIX group names are lowercase and invalid characters are replaced with underscores.

11. Click **OK** to save your changes.

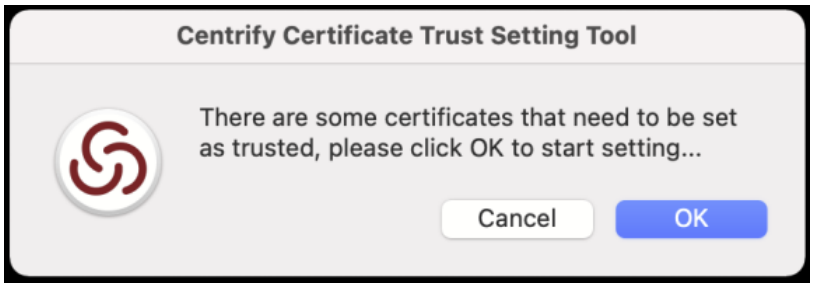
Configuring Auto-Enrollment

Delinea uses the Microsoft Windows certificate auto-enrollment feature to make certificates available to UNIX and Mac computers. If auto-enrollment is enabled, when a UNIX or Mac computer joins a domain, certificates are requested from the Certification Authority based on particular templates, and the certificates are installed on the joined computer

To enable auto-enrollment:

- Enable auto-enrollment for the group policy.
- Create a certificate template with auto-enrollment enabled.

> **Note:** As of MacOS Big Sur (11.0), Apple no longer allows silently adding root certificates to Keychain with a trusted setting. If there are some root certificates installed from your domain by the Delinea Agent, the Delinea Certificate Trust Setting Tool will open automatically. Please follow the instructions to set certificates as trusted.



Configuring 802.1X Wireless Authentication

This section explains how to configure Active Directory and Mac to authenticate Active Directory users by using a Microsoft RADIUS server with the 802.1X PEAP (MSCHAPv2) protocol over a wireless network from a Mac computer.

On Mac OS X, 802.1X wireless authentication does not rely on Delinea Access Manager or Apple's Active Directory plugin but is configured primarily through group policies that apply to the Windows server and the Mac computers.

System Configuration for 802.1X Wireless Authentication

The following table summarizes the environment that is needed for 802.1X wireless authentication:

Environment	Components / Configuration
Windows side	Windows Server 2003 R2 Enterprise Edition Domain Controller (supports PEAP) with Internet Authentication Service (IAS) installed; on Windows server 2003, RADIUS server is part of IAS. or Windows Server 2008 R2 Enterprise Edition Domain Controller (supports PEAP/TLS) with Network Policy Server (NPS) installed; on Windows Server 2008, Radius server is part of NPS.
	Active Directory on the Windows Server
	Group Policy Management Console (GPMC), which is required to configure 802.1x group policies and deploy certificates.
	Certificate Services, which is required to obtain the required certificates.
	Access Manager console 5.1.*x* or later, which is required to set group policies that apply to Mac computer.
Mac side	DirectControl agent 5.0.1-171 or later to enforce group policies on the Mac computer.
Wireless access point device	Supports 802.1x wireless authentication through one of these protocols: * WPA Enterprise WPA2 Enterprise 802.1X WEP (the name can be different, for example, RADIUS)

Note: Although it is possible to configure other RADIUS servers for 802.1X wireless authentication, or use other protocols, this document focuses on the Microsoft RADIUS server and the PEAP and TLS protocols.

These instructions assume that you have a RADIUS server properly configured for 802.1X wireless authentication, so that you can now proceed to configure your Mac environment. For a description of how the RADIUS server must be configured to support 802.1X wireless authentication on Mac OS X, see the section below named *Confirming that Windows Server Supports Certificate Auto-enrollment*. Click a link if you have questions about whether your RADIUS server is configured properly with regard to any particular item:

Of course, there are other configuration steps that are required to set up a RADIUS server, such as configuring the RADIUS client and configuring a remote access policy, however, the important consideration for Mac 802.1X authentication is that the specified certificate and private key have been created and deployed to the domain. When a Mac computer joins a Windows domain, Access Manager automatically finds certificates on the Domain Controller and adds them as trusted certificates to Keychain Access on the Mac computer.

Once you are certain that the RADIUS server is properly configured, you can configure your Mac environment; see the following section for instructions on configuring OS X 10.7 or later.

Configuring Mac OS X 10.7 or Later for 802.1X Wireless Authentication

Mac OS X 10.7 changed the way to create and manage profiles such that configuring 802.1X wireless authentication varies significantly between 10.7 and earlier versions of OS X. This section explains how to configure a Mac OS X 10.7 or later computer for 802.1X wireless authentication.

Before configuring your Mac environment, be certain that the RADIUS server is configured as described above in the section, *System Configuration for 802.1X Wireless Authentication*. This configuration includes a domain root CA

certificate or RAS/IAS server certificate, as well as a private key that are required to be trusted on the Mac computer.

However, there are no manual steps that you must perform to trust these certificates on your Mac computers. As mentioned previously, when a computer is joined to a domain, Access Manager automatically looks for certificates on the domain controller, and adds these certificates and the private key to the system Keychain on the Mac computer.

Through group policy settings you can use these certificates to create two different types of system profiles

- To create a system profile that allows users to authenticate to an 802.1X-protected ethernet network, see the next procedure, *To configure Mac OS X 10.7 or Later to Create an 802.1X Ethernet Profile*.
- To create a system profile that allows users to authenticate to an 802.1X wireless network, see the procedure further down, *To configure Mac OS X 10.7 or Later to Create an 802.1X WiFi Profile*.

The certificate template – as well as a certificate chain file and private key – are pushed to `/var/Centrify/net/certs` on the Mac computer when it joins the domain. Before you configure the group policy for the Mac computer, if you want to verify that auto-enrollment is operating correctly, you can open a Terminal window on the Mac computer and run a command similar to the following to check that the certificate has been downloaded to the computer:

```
admin$ls /var/Centrify/net/certs |grep -i auto_

...

auto_TemplateName.cert

auto_TemplateName.chain

auto_TemplateName.key
```

You should see three `auto_` files as shown in the example.

To configure Mac OS X 10.7 or later to create an 802.1X Ethernet profile

1. On a Windows computer, open the Group Policy Management Editor and edit a group policy object that applies to Mac computers.
2. Expand **Computer Configuration > Policies > User Configuration > Policies > Centrify Settings > Mac OS X Settings > 802.1X Settings**, and double-click **Enable Ethernet Profile**.
3. Select **Enable**, then click **Add**.
4. Type the name of the auto-enrollment machine certificate that has been pushed down from the Windows domain server.

   When pushed to a Mac computer, certificate names are prepended with `auto_`; for example:

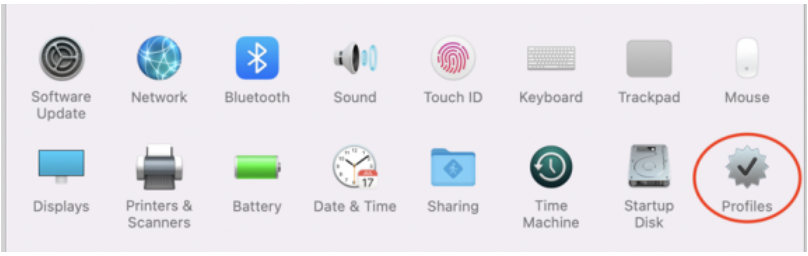
   `auth_Centrify-1X`

   This group policy runs a script that looks for the specified certificate template in the /var/Centrify/net/certs directory (which contains the certificate templates pushed down to Mac when they join the domain) and creates a WiFi profile from this certificate.
5. Click **OK** to save the profile information and **OK** again to save the policy setting.

> **Note:** This group policy will take effect at the next group policy update interval, or you can run `adgpupdate` in a terminal window on the Mac computer to have the policy take effect immediately.

When the group policy takes effect, it runs a script to create an ethernet profile for the computer from the certificate template and private key downloaded from the domain controller. This policy supports the TLS protocol for certificate-based authentication. The Mac computer is now configured for access to the radius access point.

On the Mac computer you can view the profile in System Preferences.



To configure Mac OS X 10.7 or later to create an 802.1X WiFi profile

1. On a Windows computer, open the Group Policy Management Editor and edit a group policy object that applies to Mac computers.
2. Expand **Computer Configuration > Policies > User Configuration > Policies > Centrify Settings > Mac OS X Settings > 802.1X Settings**, and double-click **Enable Wi-Fi Profile**.
3. Select **Enable**, then click **Add**.
4. Enter the following information for the Wi-Fi profile:

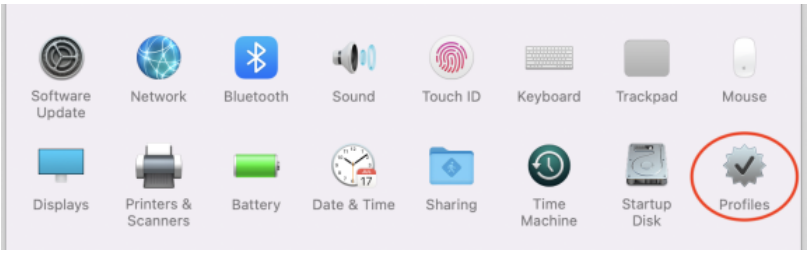
Select this	To do this
SSID	Type the SSID for the wireless network.
Template name	Type the name of the auto-enrollment machine certificate that has been pushed down from the Windows domain server. When pushed to a Mac computer, certificate names are prepended with auto_; for example: auth_Centrify-1X This group policy runs a script that looks for the specified certificate template in the /var/Centrify/net/certs directory (which contains the certificate templates pushed down from the domain controller) and creates an ethernet profile from this certificate.
Security type	Select the Security type from the drop-down list.
Other options	Select one or more of the following options: **Auto join**: Select this option to specify that the computer automatically join a Wi-Fi network that it recognizes. Do not select this option to specify that the logged in user must manually join a Wi-Fi network. **Hidden network**: Select this option if the Wi-Fi network does not broadcast its SSID.

5. Click **OK** to save the profile information and **OK** again to save the policy setting.

> **Note:** This group policy will take effect at the next group policy update interval, or you can run `adgpupdate` in a Terminal window on the Mac computer to have the policy take effect immediately.

When the group policy takes effect, it runs a script to create a WiFi profile for the computer from the certificate template and private key downloaded from the domain controller. This policy supports WEP or WPA/WPA2 security with the TLS protocol for certificate-based authentication. The Mac computer is now configured for access to the radius access point.

On the Mac computer you can view the profile in System Preferences.



Confirming that Windows Server Supports Certificate Auto-enrollment

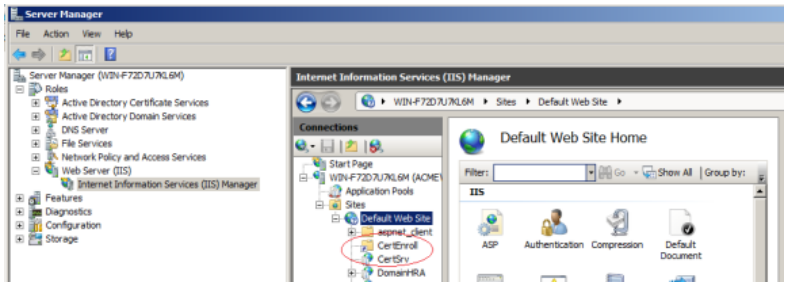
This section describes how the RADIUS server must be configured to support 802.1X wireless configuration for Mac computers.

Internet Information Services (IIS) Supports CertEnroll and CertSrv URLs

IIS must support the CertEnroll and CertSrv URLs to enable web-based access to certificate tasks.

To verify that IIs supports the CertEnroll and CertSrv URLs

1. On the Windows Certificate Authority server, click **Start > Administrative Tools > Server Manager** to open Server Manager.
2. Expand **Roles > Web Server (IIS)** and click **Internet Information Services (IIS) Manager**.
3. In the right, **Connections** pane, expand **Sites > Default Web Site** and you should see CertEnroll and CertSrv:



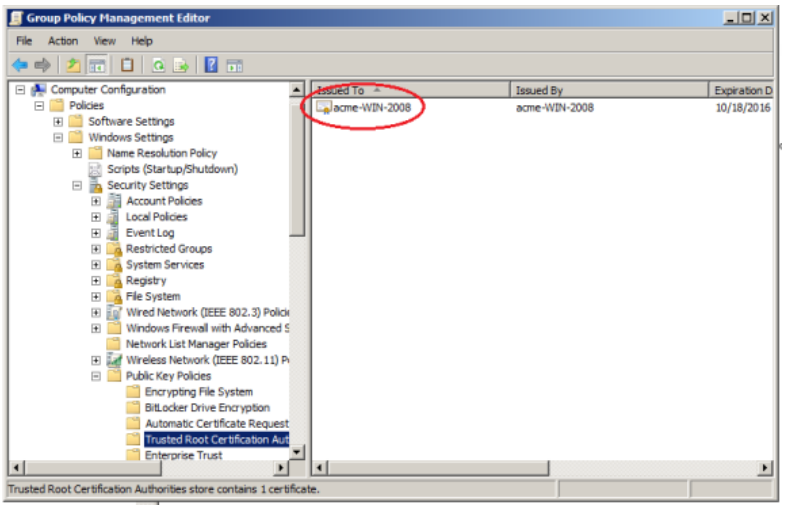
Windows Public Key Group Policies are Set to Trust the Root Certificate Authority and Enroll Certificates Automatically

Through group policy settings, the root certificate must be imported into the Trusted Root Certification Authorities group policy and set to enroll certificates automatically.

To verify that Windows public key group policies are set to trust the root certificate authority and enroll certificates automatically

1. On the Windows Certificate Authority server, click **Start > Administrative Tools > Server Manager** to open the Group Policy Management Editor.
2. Expand **Computer Configuration > Policies > Windows Settings > Security Settings > Public Key Policies** and select **Trusted Root Certification Authorities**.

   You should see your root certificate:



3. Expand **Computer Configuration > Policies > Windows Settings > Security Settings > Public Key Policies** and double-click **Certificate Services Client - Auto-Enrollment**.
4. In **Configuration Model** select **Enabled**.
5. Select both boxes, **Renew expired certificates** and **Update certificates that use certificate templates**.
6. Click **OK** to save the policy.

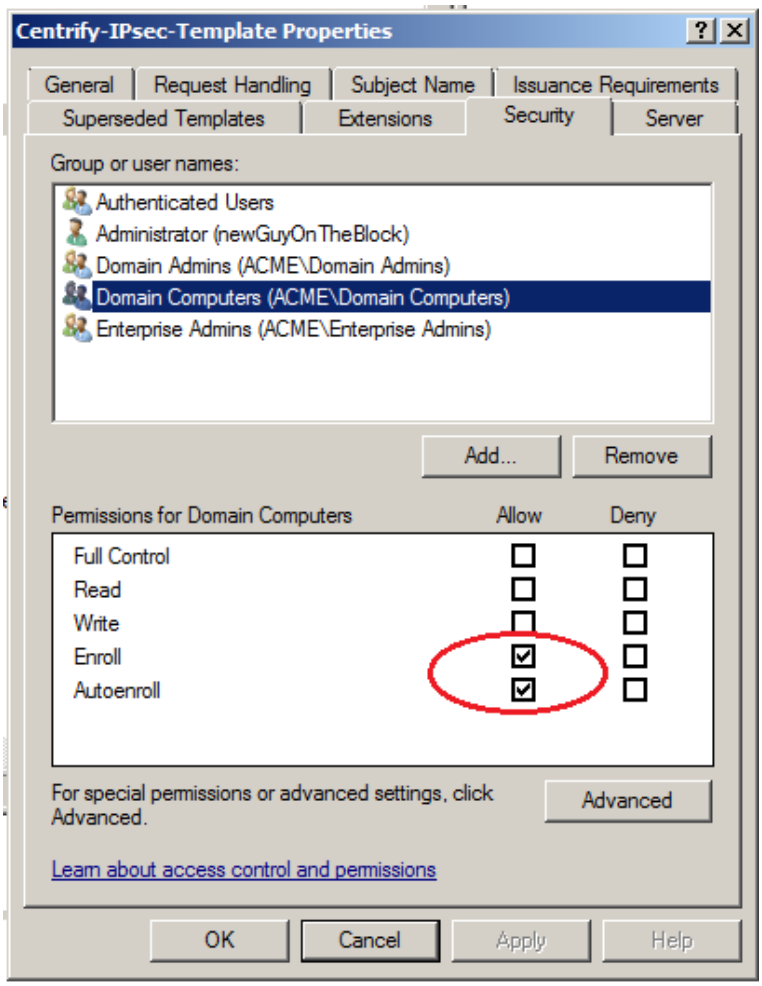
A Certificate Template is Configured to Automatically Enroll Domain Computers

To automatically enroll domain computers, you must have a certificate template that supports auto-enrollment for domain computers.

To configure a certificate template to automatically enroll domain computers

1. On the Windows Certificate Authority server, open an mmc console that contains the Certification Authority and Certificates snap-ins (**Start > Run >**`mmc.exe`).
2. If snap-ins for Certificate Templates, Certificates, and Certifications Authority are not displayed under Console Root in the navigation pane, add them now. To do so, click **File > Add/Remove Snap-in**.
   a. Select **Certificate Templates** and click **Add**.
   b. Click **Certificates** and click **Add**.
   c. Select **Computer Account** and click **Next**.

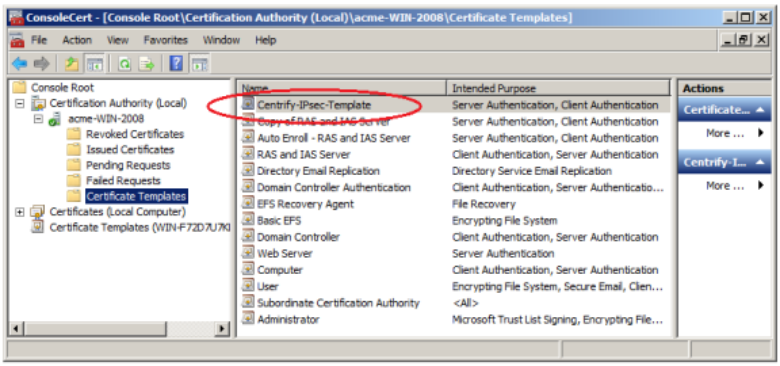
   d. Select **Local computer** and click **Finish**.
   e. Select **Certification Authority** and click **Add**.
   f. Select **Local computer** and click **Finish**.
   g. Click **OK**.
3. Select **Certificate Templates (domainController)** in the navigation pane.
4. In **Certificate Templates**, duplicate the Workstation Authentication certificate. Right-click **Workstation Authentication** and select **All Tasks > Duplicate Template**.
5. Perform the following steps in the **Properties of New Template** dialog:
   a. In the **General** tab, type a template name of your choice (for example, **Mac Auto-Enroll Certificates**) in the **Template name** field (do not use special characters such as brackets and asterisks). Type the same name in the **Template display name** field so that the template displays by that name in the Certificate Templates list.
   b. In the **Extensions** tab, select **Application Policies > Edit**. In the resulting dialog, select **Add > Server Authentication** and click **OK**.
   c. In the **Extensions** tab, verify the **Client Authentication** is already in the application policy list. If it is not, add it in the same way that you added the **Server Authentication** policy.
   d. In the **Subject Name** tab, select **Build from this Active Directory information**. In the **Subject name format** field, select **Fully distinguished name**. In the **Include this information in alternate subject name** list, select **User Principle Name (UPN)**.
   e. In the **Security** tab, select **Domain Computers (domainController)** and ensure that the template is enabled for Enroll and Autoenroll.



f. Click **Apply** and **OK** to save your settings.

6. Verify that the new template has been added to the certification authority.

   Expand **Console Root > Certification Authority > domainController** and select **Certificate Templates**. You should see that the certificate template that you have configured for auto-enrollment is contained in the certification authority for the domain:



If the new certificate template is not contained in the certification authority, add it now:

a. In the navigation pane, right-click **Certification Templates** under **Console Root > Certification Authority >** domainController.

b. Select **New > Certificate Template to Issue**.

c. Scroll to the newly created template, select it, and click **OK**.

7. Enable the following group policy:

   - On Windows 2008: **Computer configuration > Policies > Windows Settings > Security Settings > Public Key Policies > Certificate Services Client - Auto-Enrollment Settings**.
   - On Windows 2012: **Computer configuration > Policies > Windows Settings > Security Settings > Public Key Policies > Certificate Services Client - Auto-Enrollment**

   Note: To enable a group policy, open the Group Policy Management console by selecting **Start > Administrative Tools > Group Policy Management**. In the Group Policy Management console navigation pane, expand **Group Policy Management >***ForestName***> Domains >** DomainName **> Group Policy Objects**. Right-click **Default Domain Policy** and select **Edit**. In the resulting Group Policy Management Editor, navigate to the group policy described above and double-click the group policy. In the resulting dialog, select **Enabled** in the **Configuration Model** field.

8. On the Mac computer, download the certificates by executing the following commands in a terminal window:

```
sudo adflush
adgpupdate
```

9. Verify that the certificates were downloaded:

   a. On the Mac computer, open Keychain Access and verify that the certificates are there.

   b. On the Mac computer, verify that the certificates are in `/var/Centrify/net/certs`.

   c. On the Windows Certificate Authority server, open the Certification Authority console (**Start > Run >** certsrv.msc) and verify that the certificates are in the **Issued Certificates** folder.

A Certificate Template is Configured to Automatically Enroll Domain Users

To automatically enroll domain users, you must have a certificate template that supports auto-enrollment for domain users.

To configure a certificate template to automatically enroll domain users

1. On the Windows Certificate Authority server, open an mmc console that contains the Certification Authority and Certificates snap-ins (**Start > Run >**`mmc.exe`).
2. Verify that the snap-ins described in Step 2 are present under Console Root in the navigation pane. If they are not, add them now as described in Step 2.
3. Select **Certificate Templates (domainController)** in the navigation pane.
4. In **Certificate Templates**, duplicate the User certificate. Right-click **User** and select **All Tasks > Duplicate Template**.
5. Perform the following steps in the **Properties of New Template** dialog:

a. In the **General** tab, type a template name in the **Template name** field. Type the same name in the **Template display name** field so that the template displays by that name in the Certificate Templates list. For Mac, you can specify a name of your choice (do not use special characters such as brackets and asterisks). For mobile devices, the template name *must* be **User-ClientAuth**.

b. In the **Security** tab, select **Domain Users (domainController)** and ensure that the template is enabled for Enroll and Autoenroll.

c. Optionally, in the **Subject Name** tab, select **Build from this Active Directory information**. De-select the **Include email in subject name** and **E-mail name** check boxes. If you perform this step, Active Directory users do not need an email address.

6. Verify that the new template has been added to the certification authority as described in Step 6. If the new certificate template is not contained in the certification authority, add it now as described in Step 6.
7. Enable the following group policy:
   - On Windows 2008: **Computer configuration > Windows Settings > Security Settings > Public Key Policies > Certificate Services Client - Auto-Enrollment Settings**.
   - On Windows 2012: **Computer configuration > Windows Settings > Security Settings > Public Key Policies > Certificate Services Client - Auto-Enrollment**.

     Note: See Step 7 for details about how to enable the group policy.
8. On the Mac computer, download the certificates by executing the following commands in a terminal window.

   As the local Administrator:

   ```
   sudo adflush
   ```

   As an Active Directory user:

   ```
   adgpupdate
   ```
9. Verify that the certificates were downloaded:

   a. On the Mac computer, open Keychain Access and verify that the certificates are in the Login keychain.

   b. On the Mac computer, verify that the certificates are in `~/.centrify/`:

```
ls -l ~./centrify/
```

Configuring Single Sign-On for SSH and Screen Sharing

On OS X 10.10 and later, you can change configuration settings to allow single sign-on for SSH and Screen Sharing using Kerberos. Kerberos authorization for SSH and Screen Sharing allows you to establish an SSH or Screen Sharing connection to configured target machines joined to the same domain within the same single sign-on (SSO) session. In addition to authorizing SSH or Screen Sharing for the currently logged in user, you can authorize SSH or Screen Sharing for a different smart card user (for example, an admin user) by obtaining that user's Kerberos credentials.

To configure SSH SSO

Note: Smart card authentication for SSH sessions across different forests or domains is not supported.

1. Verify that all client and target machines are joined to the same AD domain.

   See **Joining an Active Directory Domain** for more information.

2. Enable `GSSAPIAuthentication` and `GSSAPIDelegateCredentials` in the `/etc/ssh/ssh_config` (`/etc/ssh_config` on OS X 10.10) file on both the client and target machine.

   ```
   GSSAPIAuthentication yes
   GSSAPIDelegateCredentials yes
   ```

3. Enable GSSAPIAuthentication and GSSAPIKeyExchange in the `/etc/ssh/sshd_config` (`/etc/sshd_config` on OS X 10.10) file on both the client and target machine.

   ```
   GSSAPIAuthentication yes
   GSSAPIKeyExchange yes
   ```

   Note: As of macOS 10.12, Apple's built-in ssh server no longer supports as the target machine. You can still use SSH SSO to login to other server machines, such as Linux/UNIX machines.

4. Enable `adclient.krb5.autoedit` on the target machine.

   The easiest way to do this is enabling the **DirectControl Settings > Kerberos Settings > Manage Kerberos configuration** group policy.

5. Restart Delinea Management Services on the target machine.

   ```
   $ sudo /usr/local/share/centrifydc/bin/centrifydc restart
   ```

   The logged in user can now open SSH connections to the target machine using a FQDN.

   ```
   $ ssh hostname.domainname
   ```

To configure Screen Sharing SSO

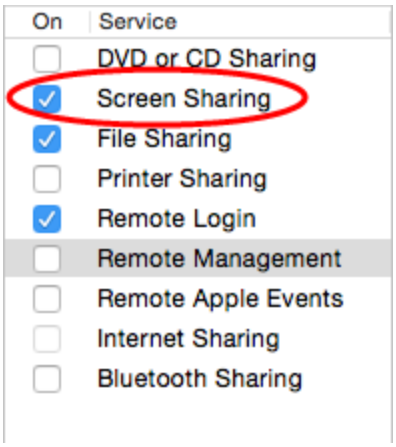
Note: Single sign-on for Screen Sharing requires Mac OS X 10.11 or higher.

1. Verify that both the client and target machines are updated to at least Delinea Management Services 5.3.1.

   ```
   $ adinfo -v
   adinfo (CentrifyDC 5.3.1-xxx)
   ```

   If an update is necessary, refer to Upgrading the Delinea DirectControl Agent for Mac for instructions and best practices.

2. Open **System Preferences > Sharing**, then select **Screen Sharing** and specify which users can initiate Screen Sharing sessions in the **Allow access for:** list.



Note: Only Screen Sharing supports SSO, as Remote Management can not allow access for network users.

The logged in user can now open Screen Sharing connections to the target machine using a FQDN.

```
$ open vnc://hostname.domainname
```

To obtain Kerberos credentials for a smart card user for SSH or Screen Sharing SSO

1. Complete all the steps in **To Configure SSH SSO** and **To Configure Screen Sharing SSO** above.
2. Insert the user's smart card into the reader.
3. Obtain Kerberos credentials from the smart card currently in the reader and use those credentials to authorize SSH.

   For multi-user PIV cards or multi-user smart cards:

   ```
   $ /usr/local/bin/sctool -a unixName
   ```

   For all other smart cards:

   ```
   $ /usr/local/bin/sctool -k userPrincipalName
   ```

   Refer to **Understanding sctool** for more information about the sctool `-a` and `-k` options.

   After unlocking the smart card, you can now open SSH or Screen Sharing connections to the target machine using the obtained Kerberos credentials.

Configuring FileVault 2

FileVault 2, available in OS X 10.8 and later, allows encryption of an entire drive to keep data secure. Although you can enable FileVault 2 through System Preferences on your Mac computers, using Delinea Management Services for Mac to configure FileVault 2 through group policy provides the advantage of creating an institutional recovery key for each of your Mac computers. Two different recovery key approaches–institutional and personal–guarantee that you will always have access to all of your encrypted computers, even if users forget their passwords.

For more information about FileVault 2, see the following Apple Knowledge Base article: "OS X: About FileVault 2".

How Filevault2 Protection Is Enabled by Delinea

Delinea relies on two features to enable FileVault 2 protection

- The "Managed By" user setting, which specifies an Active Directory user who can manage and unlock an encrypted disk.

  You specify the “Managed By” user in Active Directory Users and Computers on the domain controller. The "Managed By" user is associated with the Mac computer object, so it is possible for each computer to have its own "Managed By" user.

- The FileVault recovery key, which can be either one “institutional” key that is applied to multiple Mac computers, or computer-specific keys which are generated individually for each Mac computer.

  - If you choose to use one institutional key, you first create a FileVaultMaster certificate, which is applied to Mac computers through the Enable FileVault 2 group policy.

    When you enable the Enable FileVault 2 group policy, the FileVaultMaster certificate is applied to Mac computers automatically at the next scheduled group policy update interval. Or, you can apply the FileVaultMaster certificate immediately by executing the adgpupdate command.

  - If you choose to use computer-specific keys that are unique to each Mac computer, you do not create a FileVaultMaster certificate.

    Instead, the key is generated automatically when the “Managed By” user logs into the Mac computer for the first time and then logs out. The key, which is the “Managed By” user’s personal key, is then stored in the computer’s computer object in Active Directory.

    >**Note**: Enabling the Enable FileVault 2 group policy does not enable FileVault 2 protection on the Mac computers to which the group policy is applied. Instead, FileVault 2 protection is enabled on Mac computers as described in the remainder of this section.

The following list describes the overall process that results in FileVault 2 protection being enabled on a Mac computer.

1. The “Managed By” user is set in ADUC for one or more Mac computers.
2. The Enable FileVault 2 group policy is enabled.
   - If you select the **Use Institutional Recovery Key** option in the group policy, the FileVaultMaster certificate is applied to Mac computers. In this situation, all of the Mac computers to which the group policy was applied use the same key.
   - If you did not select the **Use Institutional Recovery Key** option in the group policy, a recovery key is not generated until the “Managed By” user logs into a Mac computer.
3. A user logs into a Mac computer. If FileVault 2 protection is not already enabled on the computer, the user’s Active Directory credentials are checked to verify that the user is the “Managed By” user. For this step to complete successfully, one of the following conditions must exist:
   - The Mac computer must be able to communicate with the domain controller (that is, it must be in connected mode), or
   - If the Mac computer is disconnected from the domain controller, locally cached AD user credentials must be available in the Delinea cache.
4. When the user is verified to be the “Managed By” user, one of the following actions takes place:

- If you selected the **Use Institutional Recovery Key** option in the Enable FileVault 2 group policy, the FileVaultMaster certificate data is used to enable FileVault 2 protection on the computer.
- If you did not select the **Use Institutional Recovery Key** option in the Enable FileVault 2 group policy, a personal recovery key is created for the computer and stored in the computer object in Active Directory. The personal recovery key is used to enable FileVault2 protection on the computer.

FileVault 2 Configuration Overview

Configuring a Mac computer for FileVault 2 protection requires configuration steps on both the Mac computer and the domain controller (or any Windows computer on which you can configure Group Policy on the domain controller). The following is a list of the major steps in the process, with links to each procedure that you must complete.

1. Create FileVault master keychain. The master keychain contains a private key that can be used to unlock the encrypted disk.

   Note: This step is required only if you are using one institutional key for multiple Mac computers. If you are using computer-specific ("personal") keys, go to Step 4.

2. Export certificate from FileVault master keychain and upload it to a domain server. Uploading the certificate to a domain server allows you to select it when you enable the "FileVault 2" group policy.

   Note: This step is required only if you are using one institutional key for multiple Mac computers. If you are using computer-specific ("personal") keys, go to Step 4.

3. Enable BitLocker Recovery Password Viewer in Active Directory.

   This step is required only if you are using computer-specific ("personal") keys. If you are using one institutional key for multiple Mac computers, go to Step 4.

4. Assign an Active Directory user who is authorized to manage an encrypted disk. FileVault 2 requires that you specify one or more "Managed By" users who can manage the encrypted disk, including the ability to lock and unlock it.
5. Enable the Enable FileVault 2 group policy. Enabling the "FileVault 2" group policy applies the FileVaultMaster certificate to Mac computers.
6. Set up and verify FileVault 2 protection. After FileVault 2 protection is enabled, the disk encryption process begins after the FileVault-authorized user logs off the computer.

Before You Begin Configuring Filevault 2

Be aware of the following requirements and limitations when configuring FileVault 2 through Delinea group policy:

- The Mac computer must be running OS X 10.9 or above.
- The Mac computer must have a recovery partition – generally, this partition is created by default during Mac OS X or macOS installation.
- FileVault 2 must *not* be enabled on the Mac computer (through the Security & Privacy System Preference).

  If it is already configured, configuring FileVault 2 through Delinea Management Services for Mac will have no effect.

- Enabling FileVault 2 protection disables auto log on for the Mac computer.
- FileVault 2 protection does not support smart card authentication at start up of the computer.

  The Apple technical white paper, "Best Practices for Deploying FileVault2" provides more information about using FileVault 2; specifically, the section “Two Factor Authentication” discusses the limitations of using FileVault 2 with alternate authentication methods such as smart cards.

Create Filevault Master Keychain

The procedure described in this section is required only if you are using one institutional key for multiple Mac computers. If you are using computer-specific (“personal”) keys, go to the section below, **Assign an Active Directory User Who is Authorized to Manage an Encrypted Disk**.

On the Mac computer, you create a FileVault master keychain, which contains a private key that can be used to unlock the encrypted drive on the computer.

You can create the master keychain through the Mac user interface, or by executing commands in the Terminal application. Instructions are provided for each procedure.

Note: If the computer already has a FileVault master keychain, you can skip this procedure and go to Export certificate from FileVault master keychain and upload it to a domain server.

To create a master keychain through the user interface

1. On a computer running OS X 10.9 or above, log on with an administrator’s account and open **System Preferences**, then double-click **Users & Groups**.
2. If necessary, click the lock icon and enter credentials to authenticate.
3. Select an administrator’s account, then click the service icon (⚙) and select **Set Master Password** from the pop-up menu.

4. Create a master password by typing it in **Master password** and re-typing in **Verify**.
5. Click **OK** to save the master password.

Setting a master password creates a keychain file in the following location:

/Library/Keychains/FileVaultMaster.keychain

This file contains the private key required to unlock the encrypted disc and is the only recovery method you will have for encrypted disc recovery. Store FileVaultMaster.keychain in a safe location, such as an external drive or an encrypted disk image on another physical disk.

To create a master keychain by executing commands in the Terminal application

1. On a Mac computer, open the Terminal application.
2. Run the following command:

   `sudo security create-filevaultmaster-keychain`
3. Enter the password for the root account when prompted as follows:

   To proceed, enter your password or type `Ctrl-C` to abort
4. Enter the master password to create when prompted to do so:

   password for new keychain
5. Retype the new master password when prompted to do so:

   retype password for new keychain

   You will see a message that the new password is being created:

   Generating a 2048 bit key pair; ...

Setting a master password creates a keychain file in the following location:

`/Library/Keychains/FileVaultMaster.keychain`

This file contains the private key required to unlock the encrypted disc and is the only recovery method you will have for encrypted disc recovery. Store FileVaultMaster.keychain in a safe location, such as an external drive or an encrypted disk image on another physical disk.

Export Certificate from Filevault Master Keychain and Upload it to a Domain Server

The procedure described in this section is required only if you are using one institutional key for multiple Mac computers. If you are using computer-specific ("personal") keys, go to the section below **Assign an Active Directory User Who is Authorized to Manage an Encrypted Disk**.

After you create a master password, as explained in the previous section, you must export the certificate associated with the master keychain to make it available for upload to the domain controller.

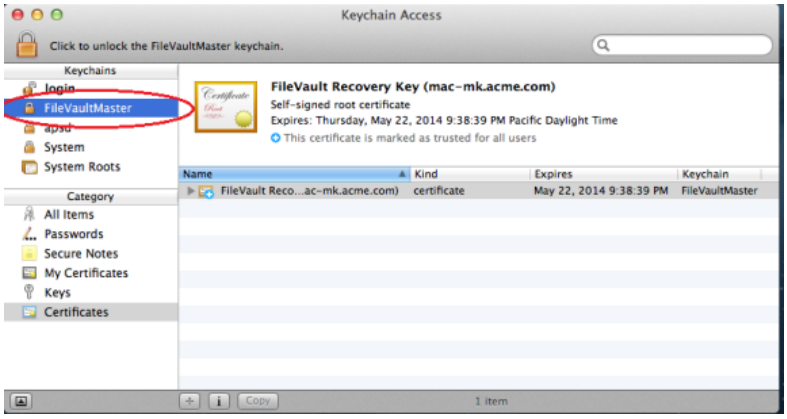
You can export the certificate by using the Mac user interface, or by executing commands in the Terminal application. Instructions are provided for each procedure.

To export the certificate by using the Keychain Access utility

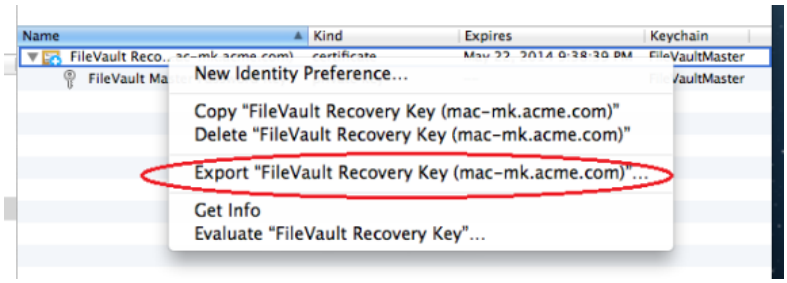
1. On the Mac computer, open the Keychain Access utility, or double-click the FileVaultMaster.keychain file, which is at the following location:

   `/Library/Keychains/FileVaultMaster.keychain`

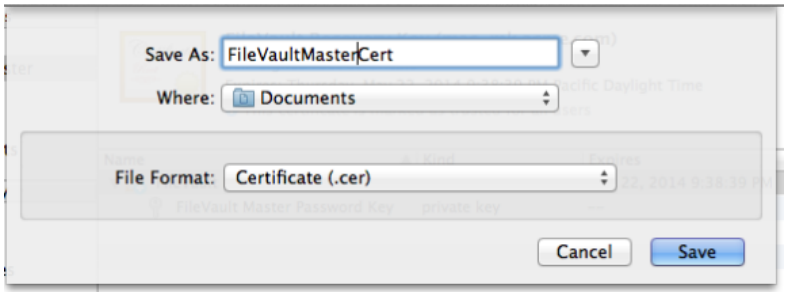
2. Enter you password if prompted to do so.
3. In **Keychains**, select **FileVaultMaster**.



4. Select the certificate, **FileVault Recovery Key** in the right pane and expand it; then right-click and select **Export "FileVault Recovery Key"**.



5. Enter the following information for saving the certificate:



- **Save As**: Type a name for the certificate, such as "FileVaultMasterCert".
- **Where**: Navigate to a folder in which to save the certificate.

- **File Format**: Select **Certificate (.cer)** from the scroll-down list.

  The certificate is now available for upload to a domain controller.

6. Copy the certificate to a location on a server that is accessible from the computer that you use to configure Group Policy for the domain.

   Later, when you enable the group policy to turn on FileVault 2 protection (see **Enable the Enable FileVault 2 Group Policy** below), you must be able to access this certificate from the domain controller on which you are running the Group Policy Editor.

To export the certificate by using Terminal commands

1. On the Mac computer, open the Terminal utility application.
2. Run the following command:

   ```
   sudo security export -k /PathToKeychain -t certs -f x509 -o /PathToCert
   ```

   Note: The sudo command is required only if FileVaultMaster.keychain is owned by root.

   where:

   - *PathToKeychain* is the path to FileVaultMaster.keychain; for example:

     `/Library/Keychains/FileVaultMaster.keychain`
   - *PathToCert* is the path to the location in which to export the certificate; for example:

     `/Documents/FileVaultMaster.cer`
   - The certificate is now available for upload to a domain controller.
3. Copy the certificate to a location on a server that is accessible from the computer that you are using to configure Group Policy for the domain.

   Later, when you enable the group policy to turn on FileVault 2 protection (see **Enable the Enable FileVault 2 Group Policy** below), you must be able to access this certificate from the domain controller on which you are running the Group Policy Editor.

Enable Bitlocker Recovery Password Viewer in Active Directory

The procedure described in this section is required only if you are using computer-specific (“personal”) keys. If you are using one institutional key for multiple Mac computers, go to **Assign an Active Directory User Who is Authorized to Manage an Encrypted Disk**, below.

To enable the BitLocker Recovery Password Viewer feature in Active Directory

1. On the domain controller, open **Administrative Tools > Server Manager**.
2. In the navigation pane, right-click **Features** and select **Add Features**.
3. In the Add Features wizard, expand **Remote Server Administration Tools > Feature Administration Tools**, select **BitLocker Drive Encryption Administration Utilities**, click **Next**, and click **Install**.
4. After the BitLocker Drive Encryption Administration Utilities are installed, click **Close**.
5. To verify that the BitLocker Drive Encryption Administration Utilities are installed:

a. Open Active Directory Users and Computers.

b. Navigate to **domaincontroller > Domain Controllers**.

c. In the right-hand ADUC pane, right-click the domain controller and select **Properties**.

d. If the BitLocker Drive Encryption Administration Utilities installed correctly, the Properties dialog contains a **Bitlocker Recovery** tab. On that tab, a “No items in this view” message displays. That message is normal, and does not indicate a problem with the BitLocker Drive Encryption Administration Utilities installation.

Assign an Active Directory User Who is Authorized to Manage an Encrypted Disk

Before enabling FileVault 2, you must assign a user account that is able to open the disk for the Mac computer after it is encrypted by FileVault 2. This setting specifies the “Managed By” user for a computer.

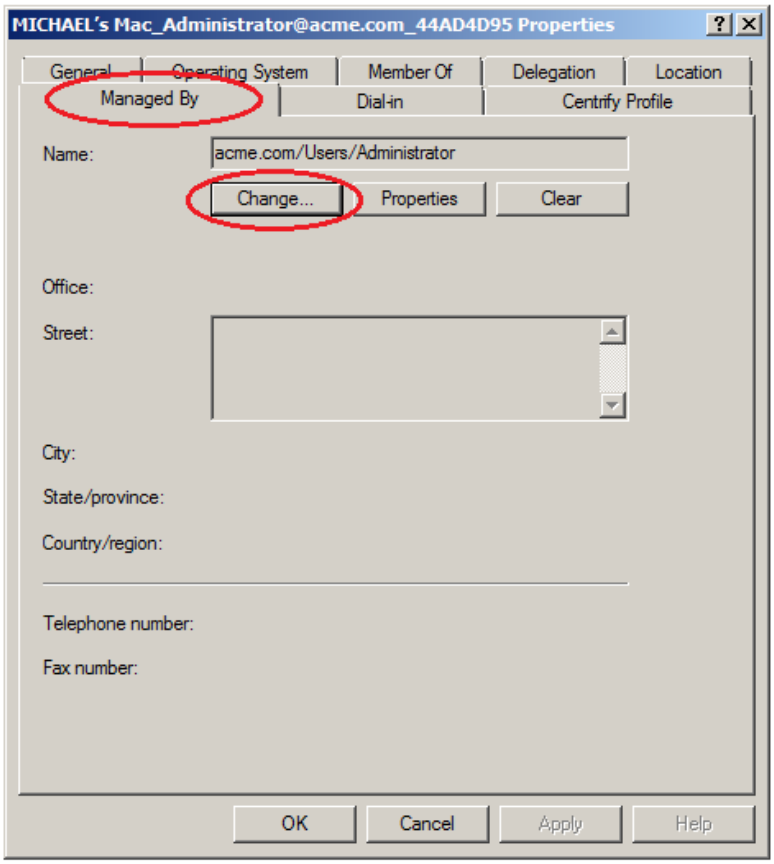
Note: Enabling the “FileVault2” group policy, as explained in the next section, encrypts the entire disk for the computer. The user account that you assign in the current procedure will be authorized to access the disk during boot up so that this account will be able to log on. You can later add other accounts, but for now, this is the only account that will be able to log on to this computer.

The “Managed By” user account must be an Active Directory mobile user account.

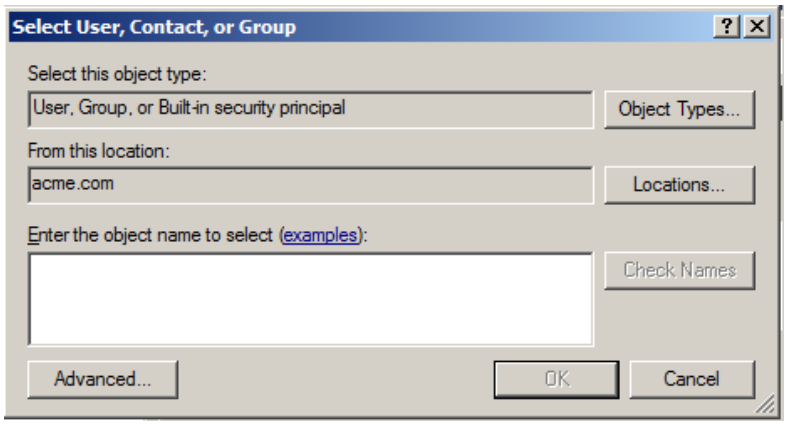
Note: After you enable a user account to open an encrypted disk at start up, you cannot remove that account from the list. If you no longer want this user account to be able to unlock the disk, you can delete the account from Active Directory. Before doing so, be certain that you have at least one other account that can unlock the hard disk on this computer, otherwise you will no longer be able to access this computer.

To assign an account that can unlock the encrypted disk

1. On a domain controller, open Active Directory Users and Computers
2. Expand the domain object and navigate to the container that contains the Mac computer, for example, **Computers**.
3. Select the Mac computer that you plan to encrypt, right-click and select **Properties**.
4. Click the **Managed By** tab.



5. Click **Change**.
6. Enter the all or part of the name to search for (make certain that **User** is selected in **Object Type**) and click Check Names.



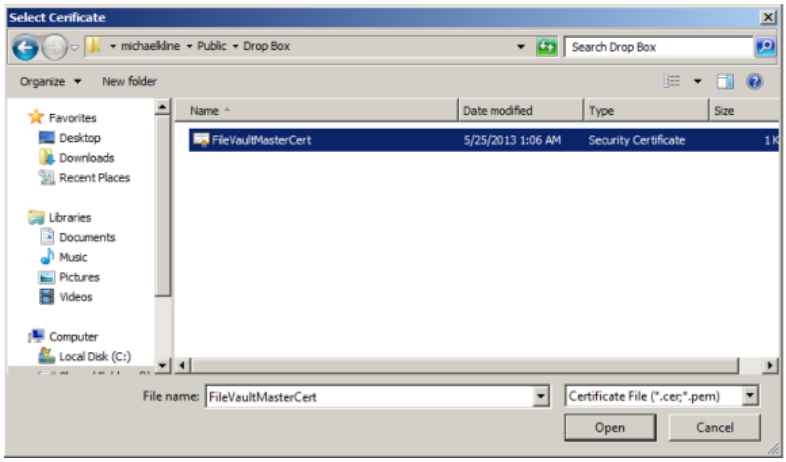
7. If the name is correct, click **OK** then **OK** again to save your changes.

Enable the Enable Filevault 2 Group Policy

Next, enable the “Enable FileVault 2” group policy to encrypt the disk. When you enable this group policy, you select whether to use one institutional key for multiple Mac computers, or computer-specific (“personal”) keys.

To enable the Enable FileVault 2 group policy

1. On a Windows computer, open the Group Policy Management Editor.
2. Select a Group Policy Object that applies to the Mac computer you are planning to encrypt, then right-click and select **Edit**.
3. Open **Computer Configuration > User Configuration > Policies > Centrify Settings > Mac OS X Settings > Security & Privacy**, then double-click **Enable FileVault 2**.
4. Click **Enable**.
5. Specify whether to use one institutional key for multiple Mac computers, or computer-specific (“personal”) keys:
   - To use one institutional key for multiple Mac computers, select **Use Institutional Recovery Key**. Then click **Select** to select the FileVault keychain certificate that you created earlier as described above in **Create FileVault Master Keychain**. If you select this option, the FileVaultMaster certificate is distributed to all of the Mac computers to which the group policy applies. Go to Step 6 and continue from there.
   - To use computer-specific (“personal”) keys, leave **Use Institutional Recovery Key** unchecked. In this situation, a personal recovery key is created for the Mac computer and stored in the computer object in Active Directory. The key is created and sent to the computer object in Active Directory after the “Managed By” user reboots the Mac computer (or restarts the agent), logs in, logs out, and provides the user password as described below in **Set Up and Verify FileVault 2 Protection**. The personal recovery key is used to enable FileVault2 protection on the Mac computer. Go to Step 8 and continue from there.
6. In the Explorer dialogue, navigate to the folder in which you uploaded the certificate.
7. Select the certificate and click **Open**.

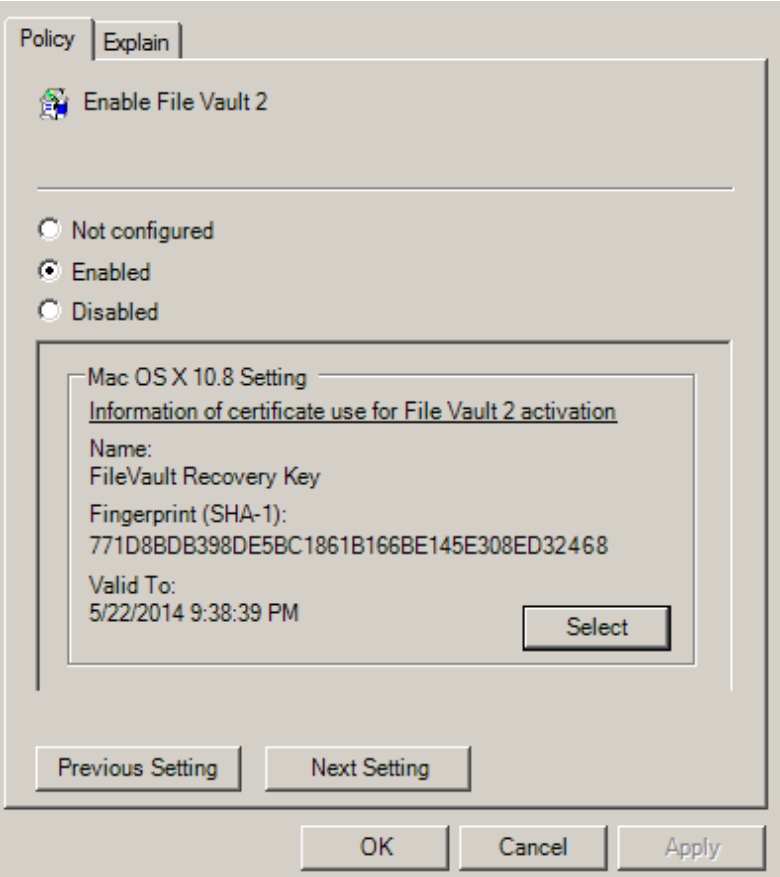


8. Click **OK** to enable the group policy.

   This group policy will automatically take effect at the next group policy update interval. To have it take effect immediately, run the following command in the Terminal application on the Mac computer:

```
adgpudate
```

If you selected **Use Institutional Recovery Key** in Step 5, the FileVaultMaster certificate name, a thumbnail, and the expiration date are displayed in the Group Policy.



Note: The expiration date is not important because OS X does no revocation checking on this certificate.

The selected certificate should have the following usages: “Digital Signature”, “Key Encipherment”, “Data Encipherment” and “Key Certificate Sign”. If the certificate does not have these usages, an error message will appear:

Set Up and Verify Filevault 2 Protection

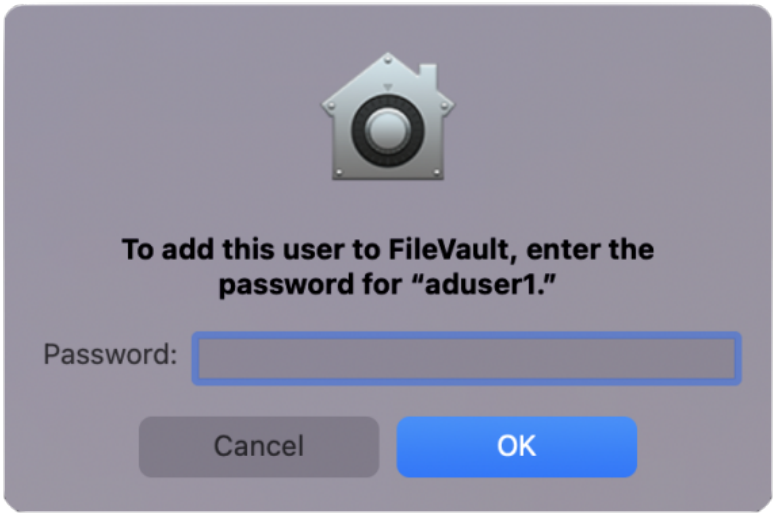
FileVault 2 protects a Mac computer by encrypting the entire hard drive when a FileVault-authorized user (the “Managed By” user) logs out. To set up FileVault 2 for the first time, you must log on to the Mac computer as the

“Managed By” user, then log out, as explained in the following procedure. After FileVault 2 is set up, only a FileVault 2-authorized user may start up the Mac computer. You may add more authorized users if you wish, or maintain a single account.

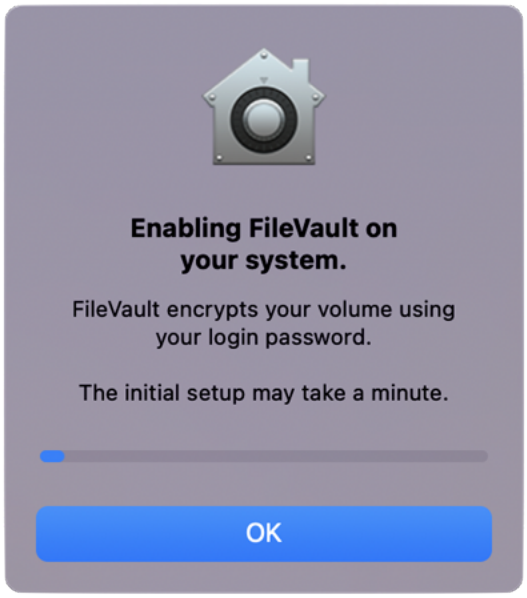
Note: Although starting up the Mac computer requires a user account that is authorized to decrypt the start up disk, after the computer has started, this user account may log out to allow other user accounts to log in.

To set up FileVault 2 protection

1. Log on to the Mac computer with the “Managed By” account that you specified above in **Assign an Active Directory User Who is Authorized to Manage an Encrypted Disk**.
2. Log the “Managed By” user out of the Mac computer, and when prompted, enter the user’s password to set up FileVault 2 protection.



The system displays a message that it is enabling FileVault protection, and when finished, restarts the computer.



3. Log back on to the Mac computer with the “Managed By” account.

   The log on screen will show the FileVault 2-authorized user alone, because this is the only user authorized to open the start up disk.

4. Open **System Preferences**, click **Security & Privacy** and click the **FileVault** tab to verify details about FileVault protection.
5. Log out the FileVault-authorized user.

   The log on screen now shows all users who are authorized for the computer.

A FileVault-authorized user is always required to start up the computer because the start up disk is encrypted. However, after the computer is running, any authorized user can log on to the computer. At this point, you have specified a single authorized account. To add more FileVault-authorized users, see the next section, **Adding FileVault-Authorized Users**.

Adding Filevault-Authorized Users

You can assign only one user as the “Managed By” user for the computer in Active Directory. If you want to authorize additional users to manage FileVault 2 protection, you must do so on the Mac computer by performing either one of the following procedures.

To authorize FileVault 2 users by using System Preferences

1. On the Mac computer, open **System Preferences > Security & Privacy**.
2. Click the **FileVault** tab, and if necessary, unlock the padlock.
3. Click the **Enable Users** button and an account list pops up.
4. Click **Enable Users** to add and enter password of that user.

To authorize FileVault 2 users by using Terminal commands

1. On the Mac computer, open the Terminal application.
2. Run the following command:

   ```
   sudo fdesetup add -usertoadd user1
   ```

   If prompted, enter the sudo password.
3. When prompted, enter the primary FileVault-authorized user name – this is the user who you specified to manage FileVault 2 (in the section above, **Assign an Active Directory User Who is Authorized to Manage an Encrypted Disk**).
4. When prompted, enter the password for the primary FileVault-authorized user.
5. When prompted, enter the password for the new user who you specified on the command line (`user1` in this example).

Changing FileVault 2 Settings

After you enable FileVault 2, the settings that you are most likely to change at a later time are the “Managed By” user and the FileVaultMaster certificate.

To change the “Managed By” user on a Mac computer

1. Disable FileVault 2 manually on the Mac computer as described below in **Disabling FileVault 2 Protection**.
2. On the domain controller, change the “Managed By” user as described in the section above, **Assign an Active Directory User Who is Authorized to Manage an Encrypted Disk**.
3. Ensure that the Mac computer can communicate with the domain controller (that is, it is in connected mode) so that it can fetch the new “Managed By” user information from Active Directory.

After you complete these steps, FileVault 2 protection is enabled on the Mac computer the next time the new “Managed By” user logs into the Mac computer.

To change the FileVaultMaster certificate

> **Note:** The procedure described in this section is supported only if you are using one institutional key for multiple Mac computers (that is, if you selected **Use Institutional Recovery Key** in **Enable the Enable FileVault 2 Group Policy**, above).

1. Disable FileVault 2 manually on each Mac computer that will use the new FileVaultMaster certificate. In most situations, this includes all computers to which the Enable FileVault 2 group policy is applied.
2. Specify a new FileVaultMaster certificate in the Enable FileVault 2 group policy as described in **Enable the Enable FileVault 2 Group Policy**, above.
3. Execute the `adgpupdate` command to have the Enable FileVault 2 group policy implement the new FileVaultMaster certificate on the Mac computers.

   If you do not execute `adgpupdate`, the old FileVaultMaster certificate is used until the next scheduled group policy update interval.

After you complete these steps:

- All Mac computers on which you disabled FileVault 2 (in Step 1) will use the new FileVaultMaster certificate the next time the “Managed By” user logs in.

- FileVault 2 protection is enabled on a Mac computer the next time the “Managed By” user logs into that Mac computer.

Disabling FileVault 2 Protection

The only way to disable FileVault 2 protection is manually on the Mac computer. You cannot disable it by disabling the Enable FileVault 2 group policy.

You can disable FileVault 2 protection through the Security & Privacy System Preference, or by issuing commands in the Terminal application – view one or the other of the two sets of instructions that follow.

To disable FileVault 2 protection by using Security & Privacy preferences

1. On the Mac computer, open **System Preferences > Security & Privacy** and click the FileVault tab.
2. Click the padlock and enter authentication information to unlock System Preferences.
3. Click **Turn Off FileVault**.
4. Click the padlock to secure the changes.
5. Restart the Mac computer.

The disk is no longer encrypted and all authorized users, not just FileVault-authorized users, should be visible on the log on screen.

To disable FileVault 2 protection by issuing Terminal commands

1. On the Mac computer, open the Terminal application.
2. Enter the following command:

   ```
   sudo fdesetup disable
   ```
3. Enter the root password when prompted.
4. Enter the password for the user account that is authorized to lock or unlock the disk.

   This is the password for the user who you assigned in Active Directory to manage the Mac OS X computer.
5. Restart the Mac computer.

The disk is no longer encrypted and all authorized users, not just FileVault-authorized users, should be visible on the log on screen.

What Happens if the Filevault-Authorized User’s Password is Reset?

If the password is reset while the computer is off or not connected to the domain, the password will not be immediately updated so the user must first log in with the old password, then back in with the new password.

For example, follow these steps for a sample set up such as the following:

- The Mac computer is turned off.
- FileVault 2 is enabled.
- `user1` is the primary FileVault 2 authorized user.

1. An administrator changes the `user1` password in Active Directory Users and Computers (through Reset Password), and informs user1 of the change.
2. You start up the computer, log on as `user1`, and enter the new password, which fails.
3. Enter the old password, which works.
4. Restart the computer, log on and enter the new password, which should be successful.

Restoring the Filevault User List After Adflush

In Server Suite, if your FileVault 2 user list contains mobile users from another forest with one-way trust (that is, cross-forest mobile users), it is possible that those users will be removed from the FileVault 2 user list after you execute `adflush` or `adflush -f`.

After you upgrade to release 2015.1 or later, perform the following steps to ensure that cross-forest mobile users are added to the FileVault 2 user list permanently:

1. Execute the following command:

   ```
   adflush -f
   ```

   Executing this command removes the 2015-format, temporary GUID from cross-forest mobile users.
2. Execute the following command for each cross-forest mobile user that you want to add permanently to the FileVault 2 user list:

   ```
   adquery user -guid cross-forest-mobile-user-name
   ```

   Executing this command assigns a new, permanent GUID to each user that you specify.
3. Execute the following command for each cross-forest mobile user that you want to add to the FileVault 2 user list:

   ```
   fdesetup add -usertoadd cross-forest-mobile-user-name
   ```

   Executing this command adds the specified user to the FileVault 2 user list.
4. Execute the following command to verify that the users are added to the FileVault 2 user list:

   ```
   fdesetup list
   ```

How to Recover an Encrypted Disk

If a user forgets the password for their encrypted disk, you can unlock the disk for them using the institutional recovery key that you created. See the following two Web articles for information:

- Apple Support: "OS X: How to create and deploy a recovery key for FileVault 2".

  Note that you have already created the recovery key – you only need to read the information in the "Recovery" section.
- "Unlock or decrypt your FileVault 2-encrypted boot drive from the command line"

Deploy Configuration Profiles to Multiple Computers

This section explains how to deploy mobile configuration profiles to multiple computers by using a group policy setting (Install mobileconfig Profiles).

Note: You can create mobile configuration profiles in a number of ways, for example by using the iPhone Config utility or OS X Server Profile Manager. This document assumes that you have already created a profile that you want to deploy, but does not show you how to do so.

You can deploy either computer or user profiles. For computer profiles, this feature requires OS X 10.7 or higher. For user profiles, this feature requires OS X 10.9 and higher.

The process for deploying a mobile configuration profile is as follows:

1. Create the mobile configuration profile.
2. Create a subdirectory in `SYSVOL` on the domain controller and copy the mobile configuration profile file to this directory. `SYSVOL` is a well-known shared directory on the domain controller that stores server copies of public files that must be shared throughout the domain.
3. Enable the “Install mobileconfig Profiles” group policy and specify the name of the file that you copied to `SYSVOL`.
4. The mapper script for the group policy runs on each Mac computer controlled by the GPO (when a user logs in or runs `adupdate`), downloads the profiles from the Active Directory server, and installs them in the Profiles system preference.

To create a subdirectory in SYSVOL:

1. Log in to the domain controller.
2. Change to the `SYSVOL` directory.

   For example, go to this directory:

   `C:WindowsSYSVOLdomain`
3. Create a new folder named `mobileconfig`.

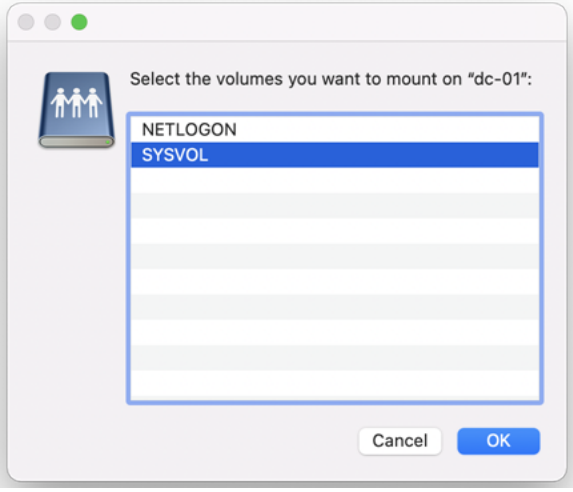
   Note: Be certain that the name of the folder is exactly as shown in the step above. The group policy setting allows you to specify the name of the file but it always looks in `SYSVOL\mobileconfig`. Likewise, do not create sub-folders – the group policy does not look in sub-folders.

To copy configuration files to SYSVOL on the domain controller:

1. In the Finder on the Mac computer navigate to the folder that contains the profile to copy.
2. Select the file, for example, `settings_for_all.mobileconfig` and copy it to the desktop. When prompted, enter your administrator password to copy the file.
3. On the desktop, change the file permissions for `settings_for_all.mobileconfig` as follows, so you can copy it to `SYSVOL`:
   a. Select the file and click **File > Get Info**.
   b. In the dialog box, expand **Sharing & Permissions**, then click the lock icon and provide administrator credentials for making changes. Set the permissions for **everyone** to **Read only**.
   c. Reset the lock and close the open dialog.
4. On the Mac computer, copy the file from the desktop to SYSVOL on the Windows domain controller. If you are connected to the domain, you should see the domain controller in the Finder. If the domain controller is not visible in the Finder, connect to it:

a. Click **Go > Connect to Server** and select the domain controller.

b. When prompted select **SYSVOL**; for example:



c. Navigate to the mobileconfig directory you created, for example by clicking **acme.com** then **mobileconfig**.

d. Drag the settings_for_all.mobileconfig file to mobileconfig.

To configure the "Install MobileConfig Profiles" group policy:

1. On the Windows domain controller, open the Group Policy Management Editor and select the GPO that is used to manage Mac computers.
2. Navigate to **Computer Configuration > Policies > Mac OS X Settings > Custom Settings** and double-click **Install MobileConfig Profiles** to install a machine profile.

   To install a user profile, navigate to **User Configuration > Policies > Mac OS X Settings > Custom Settings** and double-click **Install MobileConfig Profiles**.
3. Select **Enabled**.
4. Click **Add**, then enter the name of the file that you copied to SYSVOL, for example, `settings_for_all.mobileconfig`.

   Be certain to include the `.mobileconfig` suffix.
5. Click **OK** to add the `settings_for_all.mobileconfig` file.
6. Click **OK** to enable the policy.

   This group policy will copy the `settings_for_all.mobileconfg` file, and install the profile, on every computer to which the GPO applies and that is joined to the domain. Note that after the profile is installed, it is deleted from the Mac computer.
7. Run the `adgpupdate` command on each target Mac computer to trigger an update of group policies and execute the new Install MobileConfig Profiles policy settings.

   By default, group policies are updated automatically every 90 minutes, so you can skip this step and wait for the automatic update if you wish.

Note the following about this process:

- If you add a profile file to `SYSVOL`, but do not specify it in the group policy setting, the profile will not be installed. Likewise, if you specify a file in the group policy that does not exist in `SYSVOL`, the profile will not be installed.
- If you add new files to the existing list in the group policy, those profiles will be installed – existing profiles will not be touched.
- If you remove a file from the group policy list (after the profile for the file was installed), the profile for that file will be uninstalled from the managed Mac computers.
- If you modify a file, the corresponding profile will be reinstalled.
- If two or more profile files have the same `payloadIdentifier` attribute, only one of them will be installed.
- If you change the group policy to “Disabled” or “Not Configured”, all existing profiles that were installed previously by the group policy will now be uninstalled from the managed Mac computers.

Note: The "Install MobileConfig Profiles" group policy only supports macOS 10.15 and lower.

Understanding Group Policies for Mac Users and Computers

Centrify group policies allow administrators to extend the configuration management capabilities of Windows Group Policy Objects to managed Mac computers and to users who log on to Mac computers. This chapter provides an overview to using the Delinea Mac group policies that can be applied to Mac computers and users

For reference information about the Mac OS X-specific computer and user policies that you can set, see the following topics.

- Setting Computer-based Group Policies
- Setting User-based Group Policies

For additional information about creating and using group policies and Group Policy Objects, see your Windows or Active Directory documentation, such as https://technet.microsoft.com/en-us/windowsserver/bb310732.aspx.

For information about other Centrify group policies that are not specific to Mac computers and users, see the *Group Policy Guide*.

The following topics are covered:

Understanding Group Policies and System Preferences

In many organizations, administrators who have both Windows and Mac computers in their organization want to manage settings for their Windows and Macintosh computers and users using a standard set of tools. In a Windows

environment, the standard method for managing computer and user configuration settings is through Group Policy Objects applied to the appropriate site, domain, or organizational unit (OU) for different sets of computer and user accounts.

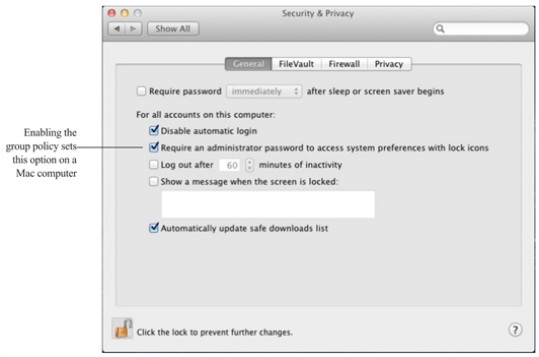
Delinea provides this capability for Mac computers and users through a group policy extension. The Delinea administrative template for Mac OS X (`centrify_mac_settings.xml or centrify_mac_settings.adm`) provides group policies that can be applied from a Windows server to control Mac OS X settings and behavior. These group policies can be applied to Mac OS X computers and to users who log on to those computers

Through the Delinea administrative template for Mac OS X, Windows administrators using the Group Policy Management Editor can centrally access and control native Mac system preferences.

In the current Delinea administrative template for Mac OS X, Centrify group policies control settings for Personal, Hardware, Internet & Network, and System preferences, including:

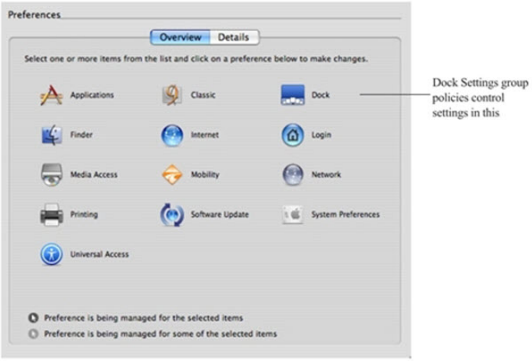
- Accounts, (General) Appearance, Desktop & Screen Saver, Dock, Energy Saver, Network, Security & Privacy, Sharing, Software Update, and so on.

When you enable a group policy in a Windows Group Policy Object, you effectively set a corresponding system preference on the local Mac computer where the group policy is applied. For example, if you enable the group policy **Computer Configuration > Delinea Settings > Mac OS X Settings > Security > Require password to unlock each secure system preference**, it is the same as selecting the General tab of the Security & Privacy system preference, then clicking the **Require an administrator password to access system preferences with lock icons** option on a local Mac OS X computer. Once the group policy is enabled in the Windows Group Policy Object and updated on the local Mac computer, the corresponding option is checked:



In addition to the system preferences that are typically set on individual computers, there are many Mac configuration settings that are typically set from a Mac OS X server using the Workgroup Manager. These

workgroup policies control application or media access, synchronization rules for mobile user accounts, the look and operation of the Dock, and other settings. The Delinea administrative template for Mac provides centralized access to many of these Workgroup Manager settings, including Applications, Dock, Media Access, Mobility, Software Update, and System Preferences.



Note: Not all group policies apply to all versions of the Mac operating environment or all computer models. If a particular system preference does not exist, is not applicable to the installed operating system, or is implemented differently on some computers, the group policy setting may be ignored or overridden by a local setting.

Group policies are available after you install the Delinea administrative template for Mac as described in **Installing the Administrative Template**, below. After you install the administrative template, the Windows administrator can use Active Directory MMC snap-ins or the Group Policy Management Console to create and link Group Policy Objects to sites, domains, or organizational units that include Mac computers that are joined to an Active Directory domain. Administrators can then use the Group Policy Management Editor to enable and configure the specific policies they want to enforce on Mac computers that are joined to the Active Directory domain.

See the *Group Policy Guide* for more information about using Active Directory Users and Computers or using the Group Policy Management Console or adding other Delinea administrative templates to a Group Policy Object.

Linking Group Policy Objects

To apply group policies to Mac computers, you can link an existing group policy object (GPO) that you are using for a Windows or UNIX computer, or create a new GPO to link to a domain or OU that contains your Mac computers and users. In general, it is recommended that you create an OU specifically for your Mac computers and link a new GPO to that OU. However, there is no problem adding the Mac group policies to an existing GPO and configuring policies for Mac computers; Mac OS X-specific policies that are applied to Windows or UNIX computers are simply ignored.

You apply GPOs to Mac users the same way; link the GPO to an OU containing the users. Group policies are only applied to users and computers in the organizational unit (OU) linked to the Group Policy object (GPO) and any of the child OUs. If your users and computers are in different OUs (which is common), Delinea recommends using user Group Policy loopback processing to make sure user policies are applied to everyone who logs on to a Mac. This is a standard Microsoft Group Policy that applies to every user to the computer. See Setting User-based Group Policies for more information about applying user policies.

Installing Mac Group Policies

Centrify group policies for Mac consist of two components

- The DirectControl agent for Mac and its associated configuration and system plug-in files that reside on the Mac computer. The DirectControl agent and related files determine the policies that have been applied to the local computer, or to the user who is logging on, and implement the policy through system preferences or other local configuration settings. This guide assumes that you have installed the DirectControl agent on your Mac computers.
- An administrative template (`.xml` or `.admx` file) that describes the policy settings available to the Group Policy Management Editor. The administrative template must be installed on a Windows computer that has the Group Policy Management Editor and the Delinea Group Policy Management Editor Extension. The Group Policy Management Editor and the Delinea Group Policy Management Editor Extension must be available for you to enable and configure policies. See the *Mac Quick Start Guide* for more information.

Installing the Administrative Template

Delinea provides templates in both XML and ADMX format. In most cases it is best to use the XML templates, which provide greater flexibility, such as the ability to edit settings after setting them initially, and in many cases contain validation scripts for the policies implemented in the template

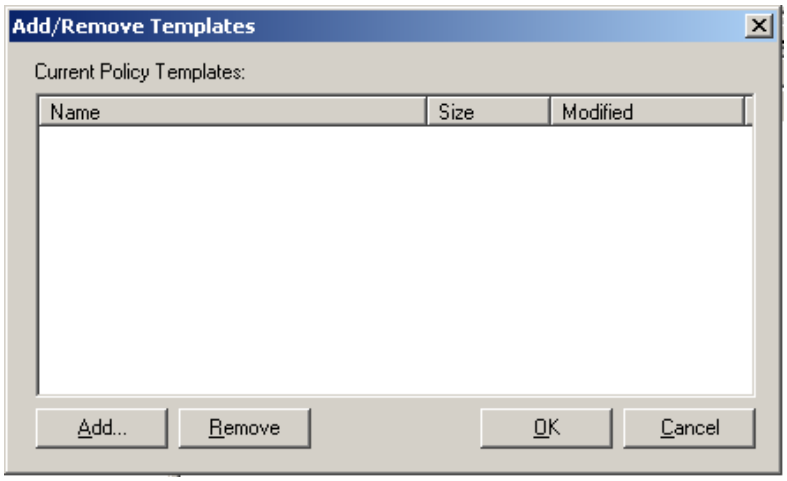
However, in certain cases, you may want to add templates by using the ADMX files. For example, if you have implemented a set of custom tools for the Windows ADMX-based policies, and want to extend those tools to work with the Delinea policies, you can implement the policies with ADMX template files. The Group Policy Management Editor will automatically read all ADMX files stored in the `%systemroot%PolicyDefinitions` folder.

The ADMX templates do not support extended ASCII code for locales that require double-byte characters. For these locales, you should use the XML templates.

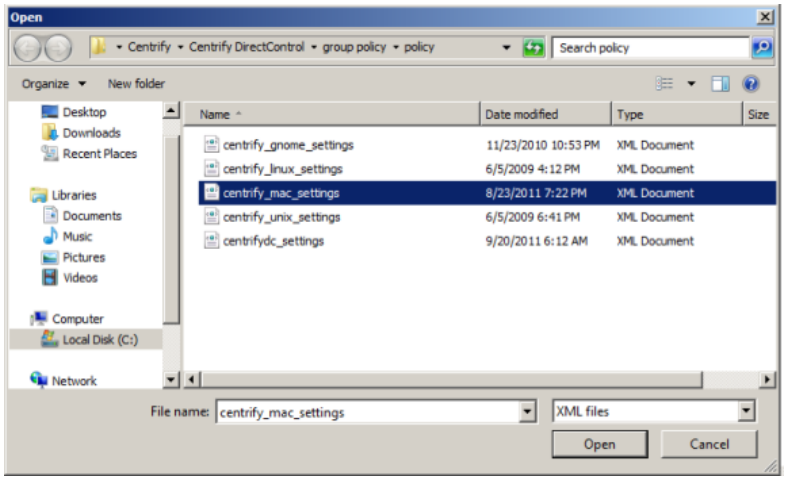
To install the Delinea XML administrative template for Mac group policies

This procedure assumes that you are using the Group Policy Management Console and have created a Mac OS X-specific GPO. For information about using a different console, such as ADUC, see the *Group Policy Guide*.

1. Open the Group Policy Management Console and select the Group Policy Object that you are using for Mac computers, right-click, then click **Edit** to open the Group Policy Management Editor.
2. Expand **Computer Configuration > Policies** and select **Delinea Settings**. Right click and click **Add/Remove Templates**.
3. Click **Add**, then navigate to the directory that contains the Delinea`centrify_mac_settings.xml` administrative template. By default, Delinea administrative templates are located in the `C:Program Files\Common Files\Centrify Shared\Group Policy Management Editor Extension\policy` folder.

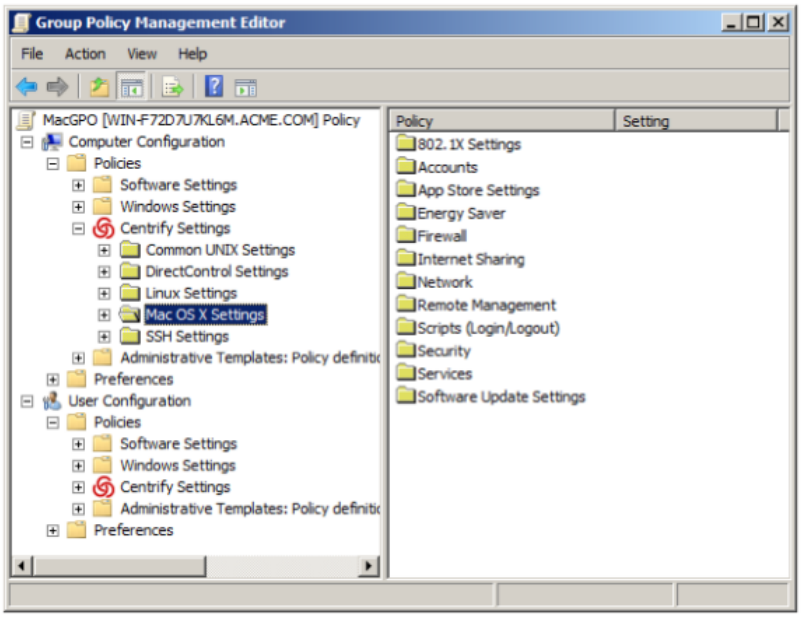


4. Select the `centrify_mac_settings.xml` file, then click **Open** to add this template to the list of Policy Templates.



5. Click **OK**.

You should now see the categories of Mac group policies listed as **Mac OS X Settings** under Delinea Settings in the Group Policy Management Editor. For example:



Note: If you update Delinea to a new version, new templates may be included with the installation. To make any new policies included in the templates available for use, you must reapply each template by following the steps in one of these procedures. If you see the message, `The selected XML file already exists. Do you want to overwrite it?`, click **Yes**. This action overwrites the template with any new or modified group policies. It does not affect any configuration in the template that has been applied; that is, any policies that you have enabled remain enabled.

Setting Mac Group Policies

Like other group policies, policies for Mac users and computers are organized into categories within the Group Policy Management Editor under **Computer Configuration > Policies > Centrify Settings > Mac OS X Settings** (Setting Computer-based Group Policies) or **Delinea Settings > Mac OS X Settings** (Setting User-based Group Policies). In general, these categories map directly to different types of Mac system preferences and individual policy settings within the categories map to specific settings within the system preference.

Normally, once enabled, policies get applied at the next group policy refresh interval, after the user logs out and logs back in, or after the computer has been rebooted. Some Mac group policies, however, require the user to log out and log back in or the computer to be rebooted. The description of each group policy indicates whether the policy can be applied “dynamically” at the next refresh interval or requires a re-login or a reboot.

You may also update group policies manually by running the adgpupdate command on an individual computer. See the next section, **Updating Configuration Policies Manually**.

Note: The system preference updated on an individual computer must be closed, then reopened for the group policy setting to be visible.

In most cases, group policies can be Enabled to activate the policy or Disabled to deactivate a previously enabled policy. Changing a policy to Not Configured has no effect for any Mac group policies. Once a group policy is set on a local computer, it remains in effect even if the computer leaves the Active Directory domain. The administrator or

users with an administrative account can change settings manually at the local computer, but any manual changes are overwritten when the group policy is applied.

Updating Configuration Policies Manually

Although there are Windows group policy settings that control whether group policies should be refreshed in the background at a set interval, Delinea also provides a command line program to manually refresh group policy settings at any time. This command line program, `adgpupdate`, forces the `adclient` daemon to contact Active Directory and collect group policy settings. With the `adgpupdate` command, you can specify whether you want to refresh computer configuration policies, user configuration policies, or both.

When you run the `adgpupdate` command, the `adclient` daemon does the following:

- Contacts Active Directory for computer configuration policies, user configuration policies, or both. By default, `adclient` collects both computer and user configuration policies.
- Determines all of the configuration settings that apply to the computer, the current user, or both, and retrieves those settings from the System Volume (`SYSVOL`).
- Writes all of the configuration settings to a virtual registry on the local computer.
- Starts the `runmappers` program to initiate the mapping of configuration settings using individual mapping programs for user and computer policies.
- Resets the clock for the next refresh interval.

For more information about using the `adgpupdate` command, see the `adgpupdate` page or *Using adgpupdate* in the *Administrator's Guide for Linux and UNIX*.

Applying Standard Windows Policies to Mac OS X

Every Group Policy Object includes several default Windows-based group policy categories and default Windows-based administrative templates for user and computer configuration. Most of the settings in the default Windows policies and administrative templates only apply to Windows computers and Windows user accounts. However, some of the common Windows configuration settings for password enforcement, such as the policies for minimum password length and complexity, do apply to Mac computers. If these settings are enabled for a Group Policy Object applied to a site, domain, or OU that includes Mac OS X computers, the settings are enforced for Mac users and computers.

The following sections describe the standard Windows group policies that you can apply to Mac computers and users and where you can find these policies when viewing a Group Policy Object in the Group Policy Management Editor.

Group Policy Refresh and Loopback Processing

The **Computer Configuration > Administrative Templates > System > Group Policy** object contains the following policies that you can use to control how group policies are refreshed and applied.

- Turn off background refresh of Group Policy
- Group Policy refresh interval for computers
- User Group Policy loopback processing mode

Synchronizing Time

By default, the local Network Time Protocol (NTP) Client is enabled and synchronizes your computer's clock to the Domain Controller. If you do not want your local NTP service to synchronize to the NTP service on the Domain Controller, explicitly disable the (Windows) Enable Windows NTP Client group policy. You can also synchronize to a different NTP server by specifying one in the Configure Windows NTP Client group policy.

To set these policies, in the Group Policy Editor, click **Computer Configuration > Administrative Templates > System > Windows Time Service > Time Providers**. The following policies are available to control time synchronization settings.

- Enable Windows NTP Client
- Configure Windows NTP Client

Specifying Time Sync Polling Interval

The **Computer Configuration > Administrative Templates > System > Windows Time Service > Global Configuration Settings** policy allows you to control the max polling interval with the MaxPollInterval option.

Configure Interactive Log On

Select the **Computer Configuration > Windows Settings > Security Settings > Local Policies > Security Options** object to configure the following policies related to interactive log on.

Note: These policies apply to SSH login only, not to login through the graphical user interface.

- Interactive logon: Message text for users attempting to log on
- Interactive logon: Prompt user to change password before expiration

Set Password Requirements

Select the **Computer Configuration > Windows Settings > Security Settings > Account Policies > Password Policy** object to set password requirements.

- Enforce password history
- Maximum password age
- Minimum password age
- Minimum password length
- Password must meet complexity requirements
- Store passwords using reversible encryption

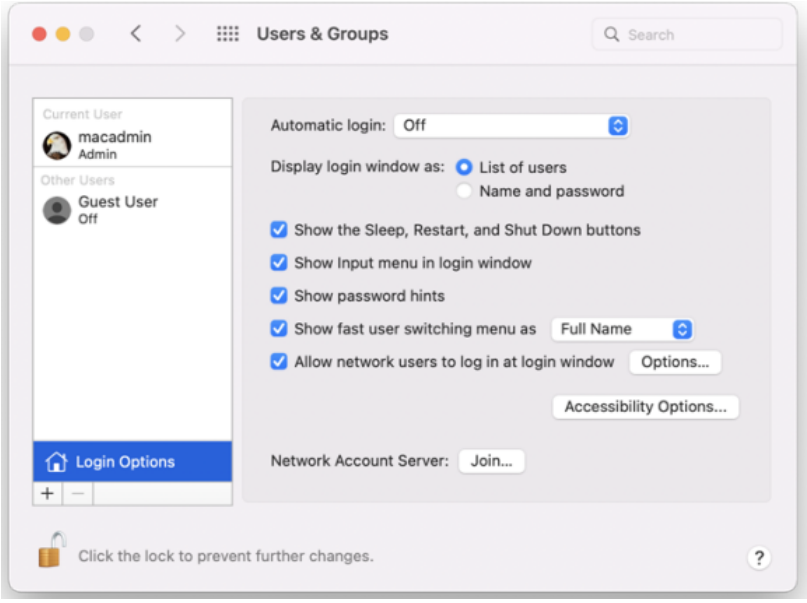
Configuring Mac-specific Parameters

Most configuration parameters apply to both Mac or only to actual UNIX or Linux systems. All these parameters are described in the *Configuration and Tuning Reference Guide*. However, the following parameters apply only to Mac OS X and are described in this section.

- adclient.autoedit.mac.netlogin
- adclient.mac.map.home.to.users
- adclient.network.wait.max
- mac.auto.generate.new.login.keychain
- mac.protected.keychain.enable
- mac.protected.keychain.user.default
- mac.protected.keychain.delete
- mac.protected.keychain.lock.inactivity
- mac.protected.keychain.lock.when.sleeping
- mac.keychain.sync.enabled
- mac.keychain.sync.polling.interval
- logger.login.log

adclient.autoedit.mac.netlogin

System Preferences > Users & Groups (Accounts) has a login option: **Allow network users to log in at login window**:



If this option is deselected, Active Directory users will not be able to log into the computer. The configuration parameter `adclient.autoedit.mac.netlogin` controls whether this option can be deselected by users. By default, the parameter is `true` in the `/etc/centrifydc/centrifydc.conf` file:

```
adclient.autoedit.mac.netlogin: true
```

In this case, even if a user deselects the box, the box is selected again when `adclient` is restarted, effectively preventing a user from deactivating network login.

If you want to allow a user to deactivate network login, set the parameter to `false`. If a user deselects network login in **System Preferences > Accounts**, the next time `adclient` starts, network users will be unable to log in to the computer.

adclient.mac.map.home.to.users

On some versions of Mac OS X, `/home` is an automount point. If a zone user's home directory is set to `/home/username`, the operating system cannot create the home directory and the user cannot log in. Therefore, you should not specify `/home/username` as the home directory for any Mac OS X users, but since this is a typical UNIX home directory, there may be Active Directory users who have a `/home/username` home directory.

To avoid potential problems, you can configure Delinea to change `/home/username` to `/Users/username` (the default Mac OS X home directory), in one of two ways:

- Enable the group policy, Map /home to /Users.
- Set the parameter, `adclient.mac.map.home.to.users` to `true` to enable the change for the local computer only; for example:

  ```
  adclient.mac.map.home.to.users:true
  ```

adclient.network.wait.max

The Delinea agent for Mac OS X performs network checks during startup to determine whether the device is connected to the domain. The `adclient.network.wait.max` parameter sets the maximum time the agent waits for the network before deciding to boot in either connected or disconnected mode. The default value is five seconds.

If DNS latency is high in your environment, the agent might determine that the device is in a Disconnected state too soon.

You can increase the value for the `adclient.network.wait.max` parameter if it's appropriate for your network environment; however, this might result in increased boot times.

logger.login.log

Login events are captured in `/var/log/centrifydc-login.log` by default. You can turn off this feature by setting the `logger.login.log` parameter to off. Refer to Collecting Information Specific to Login Events for more information about `/var/log/centrifydc-login`.

mac.auto.generate.new.login.keychain

Use this parameter to automatically generate a new login keychain if a user's keychain password does not match the password they used to successfully login.

The default value is `false`.

Refer to Auto Generate New Login Keychain for more information about the group policy that controls this parameter.

mac.protected.keychain.enable

Setting this parameter to `true` creates a new keychain protected by either an asymmetric token stored on a smart card or by a password, depending on the log in type.

The default value is `false`.

Refer to Enable Protected Keychain for more information about the group policy that controls this parameter.

Note: Changing the group policy setting for this parameter does not change the parameter's value in this file. The two are set independently, with the group policy setting taking priority.

mac.protected.keychain.user.default

Setting this parameter to true sets the protected keychain as the default keychain for that user.

The default value is `true`.

Refer to Enable Protected Keychain for more information about the group policy setting that controls this parameter.

Note: Changing the group policy setting for this parameter does not change the parameter's value in this file. The two are set independently, with the group policy setting taking priority.

mac.protected.keychain.delete

Setting this parameter to `true` deletes the existing password-protected Login Keychain after logging in.

The default value is `false`.

Note: This parameter only works if `mac.protected.keychain.enable` is set to `true`.

Refer to Enable Protected Keychain for more information about the group policy setting that controls this parameter.

Note: Changing the group policy setting for this parameter does not change the parameter's value in this file. The two are set independently, with the group policy setting taking priority.

mac.protected.keychain.lock.inactivity

Use this parameter to set the period of inactivity in minutes to automatically lock the protected keychain.

The default value is `0`, which means the protected keychain is never automatically locked.

Refer to Lock Protected Keychain after Number of Minutes of Inactivity for more information about the group policy that controls this parameter.

Note: Changing the group policy setting for this parameter does not change the parameter's value in this file. The two are set independently, with the group policy setting taking priority.

mac.protected.keychain.lock.when.sleeping

Setting this parameter to true locks the protected keychain when the Mac sleeps.

The default value is `false`.

Refer to Lock Protected Keychain When Sleeping for more information about the group policy that controls this parameter.

Note: Changing the group policy setting for this parameter does not change the parameter's value in this file. The two are set independently, with the group policy setting taking priority.

mac.keychain.sync.enabled

This configuration parameter enables Keychain synchronization for the users on a mac.

If this parameter is enabled, the current login user will receive a password change notification when his/her password is changed remotely. When the user clicks on the notification, the Delinea Keychain Sync utility appears and allows the user to synchronize the Keychain password.

Note: Password changes can only be detected when the machine is in connected mode.

The default value is `false`.

Refer to Enable Keychain Synchronization for more information about the related group policy.

mac.keychain.sync.polling.interval

This configuration parameter sets the password change detection interval when `mac.keychain.sync.enabled` is enabled.

This parameter determines the time (in minutes) between checking for changed passwords. There is a random zero to five minute variance in the actual interval each device is checked for a changed password to maintain performance. As a result, the minimum interval is five minutes.

Note: Valid intervals are between 5 minutes and 1440 minutes (1 day).

The default value is `30`.

Refer to Enable Keychain Synchronization for more information about the related group policy.

Setting Computer-Based Group Policies

Centrify group policies allow administrators to extend the configuration management capabilities of Windows Group Policy Objects to managed Mac computers and to users who log on to Mac computers. This chapter provides reference information for the Centrify Mac group policies that can be applied specifically to Mac computers

The computer-based group policies are defined in the Centrify Mac administrative template (`centrify_mac_settings.xml`) and accessed from **Computer Configuration > Policies > Centrify Settings > Mac OS X Settings**. See Understanding Group Policies for Mac Users and Computers for general information about how Delinea uses group policies to manage Mac settings and for information on how to install the group policy administrative templates.

For reference information about user-based policies, see Setting User-based Group Policies.

For information, see Applying Standard Windows Policies to Mac OS X and Configuring Mac-specific Parameters.

Note: For more complete information about creating and using group policies and Group Policy Objects, see your Windows or Active Directory documentation. For more information about adding and using other Centrify group policies that are not specific to Mac computers and users, see the *Group Policy Guide*

Setting Computer-Based Policies for Mac

The following table provides a summary of the group policies you can set for Mac computers. These group policies are in the Centrify Mac administrative template (`centrify_mac_settings.xml`) and accessed from **Computer Configuration > Policies > Centrify Settings > Mac OS X Settings**.

Use this policy	To do this
Allow Certificates with No Extended Key Usage Certificate Attribute	For smart card log in, allow the use of certificates that do not contain the extended key usage (EKU) attribute. This is a Windows policy that is defined in the **Administrative Templates > Windows Components > Smart Card** folder using an adm template.
Map /home to /Users	Map the /home/*username* directory to /Users/*username*. This is a Mac OS X-specific policy but defined in the **Direct Control Settings > Adclient Settings** folder using the centrifydc_settings.xml template.
802.1x Settings	Create login and system profiles for wireless authentication. These group policies correspond to 802.1X Options in the **Networks** system preference.
Accounts	Control the look and operation of the login window on Mac computers and map zone groups to the local administrator group. These group policies correspond to Login Options in the **Accounts** system preference.
App Store Settings Deprecated	Control the users and groups who can access the App Store. These group policies correspond to settings in the Sleep and Options panes in the **Energy Saver** system preference.
Custom Settings	Customize and install configuration profiles.
Energy Saver	Control sleep and wake-up option on Mac computers. These group policies correspond to settings in the Sleep and Options panes in the **Energy Saver** system preference.
Firewall	Control the firewall configuration on Mac computers. These group policies correspond to settings in the Firewall pane of the **Sharing** system preference.
Internet Sharing	Manage Internet connections on Mac computers. These group policies correspond to settings in the Internet pane of the **Sharing** system preference.
Network	Control DNS searching and proxy settings. These group policies correspond to settings in the TCP/IP and Proxies panes of the **Network** system preference.
Remote Management	Control Apple Remote Desktop access for zone users. These group policies correspond to the **Manage > Change Client Settings** options in Apple Remote Desktop.
Security & Privacy	Control security settings on Mac computers. These group policies correspond to settings in the **Security** system preferences.
Services	Control access to various services on Mac computers. These group policies correspond to settings in the Services pane of the **Sharing** system preference.
Software Update Settings	Control the options for automatic software updates on Mac computers. These group policies correspond to settings in the **Software Update** system preference.

For information about specific policies and how to set them, see the policy description (Explain text) or the corresponding discussion of the specific system preference or individual setting in the Mac Help.

Allow Certificates with no Extended Key Usage Certificate Attribute

Path

Computer Configuration > Policies > Administrative Templates: Policy Definitions> Windows Components> Smart Card.

Description

The group policy, “Allow certificates with no extended key usage certificate attribute” is defined in a Windows administrative template file (`.adm`), not in `centrify_mac_settings.xml`, and is in Administrative Templates, not in Mac Settings.

To enable or disable this policy, click **Computer Configuration > Policies > Administrative Templates: Policy Definitions > Windows Components > Smart Card**.

Enabling this policy setting allows the use of certificates for smart card login that do not have the Extended Key Usage (EKU) attribute set. Normally, certificates that are used for smart card login require this attribute with a smart card logon object identifier.

When you enable this policy, it sets the `smartcard.allow.noeku` parameter to true in the Centrify configuration file. Certificates with the following attributes can also be used to log on with a smart card:

- Certificates with no EKU
- Certificates with an All Purpose EKU
- Certificates with a Client Authentication EKU

If you disable or do not configure this policy setting (and do not set the `smartcard.allow.noeku` parameter to true in the Centrify configuration file) only certificates that contain the smart card logon object identifier can be used with smart card log in.

After changing the value of this parameter, you must re-enable smart card support by running the following sctool command as root:

```
[root]$ sctool -E
```

Note: You must also specify the `--altpkinit` or `--pkinit` parameter when you run `sctool` with the `-E` option.

Map /home to /Users

Path

Computer Configuration > Policies > Centrify Settings > DirectControl Settings > Adclient Settings.

Description

The Mac group policy, Map /home to /Users is defined in the `centrifydc_settings.xml` file, not in `centrify_mac_settings.xml`, and is in Delinea Settings, not in Mac Settings.

To enable or disable this policy, click **Computer Configuration > Policies > Centrify Settings > DirectControl Settings > Adclient Settings**.

On some versions of Mac OS X, /home is an automount point. If a zone user's home directory is set to /home/*username*, the operating system cannot create the home directory and the user cannot log in. Therefore, you should not specify /home/*username* as the home directory for any Mac users, but since this is a typical UNIX home directory, there may be Active Directory users who have a /home/*username* home directory. To avoid potential problems, enable this group policy, Map /home to /Users, to configure Delinea to change /home/*username* to /Users/*username* (the default Mac home directory). If you do not enable this policy, the change does not take effect.

This policy modifies the `adclient.mac.map.home.to.users` parameter in the Centrify configuration file.

802.1X Settings

Path

Computer Configuration > Policies > Centrify Settings > Mac OS X Settings > 802.1X Wireless Settings

Description

Use the **Computer Configuration > Policies > Centrify Settings > Mac OS X Settings > 802.1X Settings** to create profiles for wireless network authentication. The profiles you specify with these group policies are created in the Network system preferences pane.

Enable Machine Ethernet Profile

Path

Computer Configuration > Policies > Centrify Settings > Mac OS X Settings > 802.1X Wireless Settings > Enable Machine Ethernet Profile

Description

Enable this policy to create an 802.1X ethernet profile so users can authenticate to an 802.1X-protected network by using the specified machine certificate.

Note: This group policy only supports macOS 10.15 and lower.

This policy supports the TLS protocol for certificate-based authentication for computers.

Before you can enable this policy, you must have a Windows server configured for 802.1X wireless authentication. The configuration includes certificate templates that are configured for auto-enrollment of domain computers and automatically downloaded to Mac computers when they join the domain. See Configuring 802.1X Wireless Authentication for details about what you must configure before enabling the current policy.

After enabling this policy, set the following:

- **Template Name**: Type the name of the auto-enrollment machine certificate that has been pushed down from the Windows domain server.

  When pushed to a Mac computer, certificate names are prepended with `auto_`; for example:

  `auth_Centrify-1X`

This group policy runs a script that looks for the specified certificate template in the `/var/centrify/net/certs` directory (which contains the certificate templates pushed down from the domain controller) and creates an Ethernet profile from this certificate.

Once enabled, this policy takes effect dynamically at the next group policy refresh interval.

Enable Machine Wi-Fi Profile

Path

Computer Configuration > Policies > Centrify Settings > Mac OS X Settings > 802.1X Wireless Settings Enable Machine Wi-Fi Profile

Description

Enable this policy to create an 802.1X Wi-Fi profile for wireless network authentication for a computer.

Note: This group policy only supports macOS 10.15 and lower.

This policy supports WEP or WPA/WPA2 security with the TLS protocol for certificate-based authentication for computers.

Before you can enable this policy, you must have a Windows server configured for 802.1X wireless authentication. The configuration includes certificate templates that are configured for auto-enrollment of domain computers and automatically downloaded to Mac computers when they join the domain. See Configuring 802.1X Wireless Authentication for details about what you must configure before enabling the current policy.

After enabling this policy, set the following:

- **SSID**: Type the SSID for the wireless network.
- **Template Name**: Type the name of the auto-enrollment machine certificate that has been pushed down from the Windows domain server.

  When pushed to a Mac computer, certificate names are prepended with auto_; for example: `auth_Centrify-1x`

  This group policy runs a script that looks for the specified certificate template in the `/var/centrify/net/certs` directory (which contains the certificate templates downloaded from the domain controller) and creates a WiFi profile from this certificate.
- **Security Type**: Select the security type from the drop-down list.
- **Other options**: Select one or more of the following options:
  - **Auto join**: Select this option to specify that the computer automatically join a Wi-Fi network that it recognizes. Do not select this option to specify that the logged in user must manually join a Wi-Fi network.
  - **Hidden network**: Select this option if the Wi-Fi network does not broadcast its SSID.
  - **Proxy PAC URL**: The URL of the PAC file that defines the proxy configuration. You can enter any string without spaces.
  - **Proxy PAC Fallback**: Allows the device to connect directly to the destination if the PAC file is unreachable. This option is disabled by default.

Once enabled, this policy takes effect dynamically at the next group policy refresh interval.

Enable User Ethernet Profile

Path

Computer Configuration > Policies > Centrify Settings > Mac OS X Settings > 802.1X Wireless Settings > Enable User Ethernet Profile

Description

Enable this policy to create an 802.1X ethernet profile so users can authenticate to an 802.1X-protected network by using the specified user certificate.

Note: This group policy only supports macOS 10.15 and lower.

This policy supports the TLS protocol for certificate-based authentication for users.

By default, the auto-enrolled user certificates are pushed down to `~/.centrify/autouser_(name).{cert.key.chain}`. Certificates are also imported into each user's login keychain.

Before you can enable this policy, you must have a Windows server configured for 802.1X wireless authentication. The configuration includes certificate templates that are configured for auto-enrollment of domain computers and automatically downloaded to Mac computers when they join the domain. See Configuring 802.1X Wireless Authentication for details about what you must configure before enabling the current policy.

Users must perform these steps after login to authenticate to the network as the user:

1. Select **System Preferences > Network > Ethernet**.
2. If there are any pre-existing 802.1X connections, click **Disconnect** to disconnect the pre-existing connections. For example, if a machine 802.1X Ethernet policy has been set, the computer will already be authenticated using the machine credential.
3. Click Connect. This action prompts the user with a list of available user identities in *certificate-key* pair format.
4. Choose the appropriate auto-enrolled user identity.

Enable User Wi-Fi Profile

Path

Computer Configuration > Policies > Centrify Settings > Mac OS X Settings > 802.1X Wireless Settings > Enable User Wi-Fi Profile

Description

Enable this policy to create an 802.1X Wi-Fi profile for wireless network authentication for a user.

Note: This group policy only supports macOS 10.15 and lower.

This policy supports the TLS protocol for certificate-based authentication for users.

By default, the auto-enrolled user certificates are pushed down to `~/.centrify/autouser_(name).{cert.key.chain}`. Certificates are also imported into each user's login keychain.

The resulting profile is signed using the first available auto-enrolled machine certificates, which are under `/var/centrify/net/certs/auto_(name).{cert.key.chain}`. If an auto-enrolled machine certificate is not available, the profile will be unsigned.

Before you can enable this policy, you must have a Windows server configured for 802.1X wireless authentication. The configuration includes certificate templates that are configured for auto-enrollment of domain computers and automatically downloaded to Mac computers when they join the domain. See Configuring 802.1X Wireless Authentication for details about what you must configure before enabling the current policy.

After enabling this policy, set the following:

- **SSID**: Type the SSID for the wireless network.
- **Security Type**: Select the security type from the drop-down list.
- **Other options**: Select one or more of the following options:
  - **Auto join**: Select this option to specify that the computer automatically join a Wi-Fi network that it recognizes. Do not select this option to specify that the logged in user must manually join a Wi-Fi network.
  - **Hidden network**: Select this option if the Wi-Fi network does not broadcast its SSID.
  - **Proxy PAC URL**: The URL of the PAC file that defines the proxy configuration. You can enter any string without spaces.
  - **Proxy PAC Fallback**: Allows the device to connect directly to the destination if the PAC file is unreachable. This option is disabled by default.

Users must perform these steps after login to authenticate to the network as the user:

1. Select **System Preferences > Network > Wi-Fi**.
2. If there are any pre-existing 802.1X connections, click **Disconnect** to disconnect the pre-existing connections. For example, if a machine 802.1X Ethernet policy has been set, the computer will already be authenticated using the machine credential.
3. Click **Connect**. This action prompts the user with a list of available user identities in *certificate-key* pair format.
4. Choose the appropriate auto-enrolled user identity (a *certificate-key* pair).

Specify System Profile (Deprecated)

Path

Computer Configuration > Policies > Centrify Settings > Mac OS X Settings > 802.1X Wireless Settings > Specify System Profile (Deprecated)

Description

This group policy is provided for backward compatibility with Mac OS X 10.6. If your environment does not contain any 10.6 computers, do not use this group policy.

Enable this policy to specify 802.1X system profile for wireless network authentication.

System profile can establish a wireless connection without a user login.

To add a system profile, enable the policy and click **Add** to enter the profile name and setting, then type a name for the profile.

The setting must follow this format:

- `Network;Security Type;Authentication` Method, where each field is separated by a semi-colon (;)
- Network is the wireless network name
- Security type is one of `802.1X WEP`, `WPA Enterprise`, `WPA2 Enterprise`
- Authentication method is one or more of the following, separated by commas: `TTLS, PEAP, LEAP, MD5`

For example:

```
OFFICE1;WPA Enterprise;PEAP
```

```
OFFICE2;802.1X WEP;TTLS,PEAP
```

Automatically turn on Airport; to automatically turn on AirPort device if this type of profile is specified. Otherwise, the status of the AirPort device will not change.

Once enabled, this policy takes effect dynamically at the next group policy refresh interval.

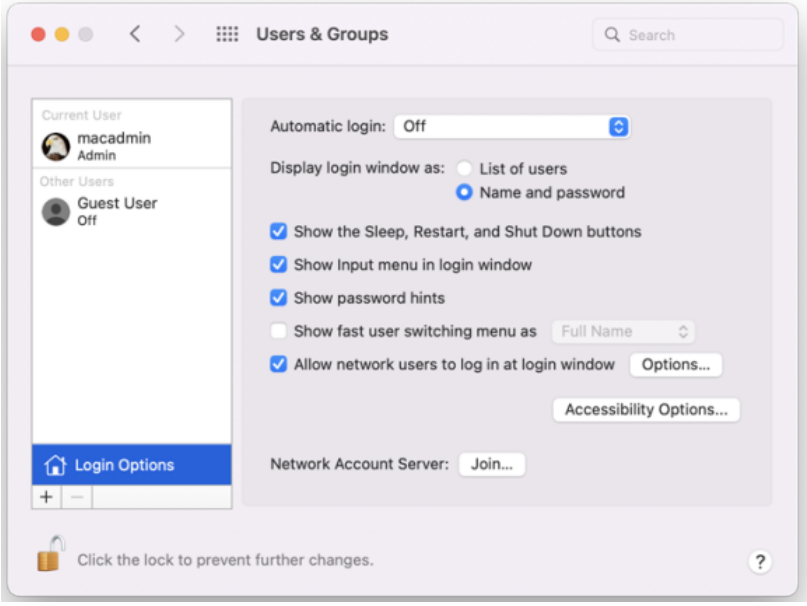
Accounts

Path

Computer Configuration > Policies > Centrify Settings > Mac OS X Settings > Accounts

Description

Use the **Computer Configuration > Policies > Centrify Settings > Mac OS X Settings > Accounts** settings to manage the options from the Accounts ( ) system preference on Mac computers. These group policies correspond to the options displayed when you select the **Accounts** system preference, then click **Login Options**. For example:



Set Login Window Settings

Path

Computer Configuration > Policies > Centrify Settings > Mac OS X Settings > Accounts > Set login window settings

Description

Configure the Login Options on a computer. If you enable this policy, you can configure the Login Window to:

- Display a text string as a login banner. The Banner you specify is displayed when the user is prompted to log on.
- Display a List of Users or a Name and Password field. Displaying the Name and Password requires users to provide their account name and password, and is more secure than displaying a list of user names.
- Show the Restart, Sleep, and Shut Down buttons.
- Show the Input menu in the login window to allow users to change the current Keyboard Layout.
- Show password hints in the login window.
- Use VoiceOver at the login window.
- Enable fast user switching.
- Display the HostName, IP Address, and OS X or macOS Version. Users need to click the clock in the top right corner to view each field.
- Disable reopening applications when logging back in. Check this to always uncheck the **Reopen Windows when logging back in** checkbox at logout, restart, or shutdown.
- Hide all Local Users with a UID less than 500.
- Enabling the options in this group policy is the same as clicking **Login Options** in the Accounts system preference and setting the corresponding login window options.

  Note: This policy does not impact lock screens. It only impacts the login window.

  Note: If you click **Enable Fast User Switching**, this setting does not take effect until the Login Options in the Accounts system preference is opened manually by a user on the local host. This step is required to display the list of users in the upper-right corner of the menu bar. After users log on, the user's full name, short name, or icon identifier is displayed in the menu bar. If you want to change how users are displayed in the menu, you also must do so manually from the Login Options in the Accounts system preference.

Once enabled, this group policy takes effect when users log out and log back in or when the computer is rebooted.

Map Zone Groups to Local Admin Group

Path

Computer Configuration > Policies > Centrify Settings > Mac OS X Settings > Accounts > Map zone group to local admin group

Description

Specify one or more zone groups to map to the admin group on the local computer. Members of the groups you specify here have administrative privileges on the local computer, including:

- The use of `sudo` command in a shell
- The ability to unlock and make changes to System Preferences.

Be certain to create a zone group in Access Manager (or adedit) and add users who you want to have administrative privileges on managed Mac computers.

Note: If the local computer is connected to the domain through Auto Zone, you cannot create a zone group because there are no zones. However, all Active Directory groups are valid for the joined computer, so you can map any group to the local admin group, but you need to know the group's UNIX name, which you can retrieve on the local computer by using the `adquery` command, as shown in the following example.

```
[root]#adquery group -n
```

To set this policy

1. Open the policy and select **Enabled**.
2. Click **Add**.
3. Enter the name of a zone group in the box (or the UNIX group name if connected through Auto Zone). Then click **OK**.

Map Zone Groups to Local Group

Path

Computer Configuration > Policies > Centrify Settings > Mac OS X Settings > Accounts > Map zone group to local group

Description

Specify one or more zone groups to map to a Mac local group on the local computer. Members of the zone groups you specify here will be given the privileges of the local group on the local computer; for example:

- If you map to the `_lpadmin` and `_lpoperator` local groups, members of the zone group can manage printer settings on the local computer.
- If you map to the admin local group, members of the zone group obtain administrator privileges on the local computer.

  Note: To obtain administrator privileges for a zone group, you can either map to the local admin group with this policy, or use the Map zone groups to local admin group policy. However, do not do both as the results are unpredictable.

Be certain to create a zone group in Access Manager (or adedit) and add users who you want to have administrative privileges on managed Mac computers.

Note: If the local computers is connected to the domain through Auto Zone, you cannot create a zone group because there are no zones. However, all Active Directory groups are valid for the joined computer, so you can map any group to the local admin group, but you need to know the group's UNIX name, which you can retrieve on the local computer, by using the `adquery` command, as follows

```
[root]#adquery group -n
```

To set this policy

1. Open the policy and select **Enabled**.
2. Click **Add**.
3. Enter the name of a local group and of a zone group in the respective boxes (or the UNIX group name if

connected through Auto Zone), then click **OK**.

You can repeat this step multiple times to map the zone group to more than one local group.

App Store Settings Deprecated

Path

Computer Configuration > Policies > Centrify Settings > Mac OS X Settings > App Store Settings (Deprecated)

Description

Note: This policy has been deprecated and is no longer supported. Enabling it will have no effect. It is provided simply to allow you to disable the policy if it was set in an earlier version of the product. You can use the **Application Access Settings (deprecated)** group policies to control access to the App Store if you wish.

Prohibit Access to the App Store (Deprecated)

Path

Computer Configuration > Policies > Centrify Settings > Mac OS X Settings > App Store Settings (Deprecated) > Prohibit Access to the App Store (Deprecated)

Description

Use the **Computer Configuration > Policies > Centrify Settings > Mac OS X Settings > App Store > Prohibit Access to App Store** group policy to control access to the App Store.

By default, all users can access the App Store. Enable this group policy to prohibit access to App Store to all users except the root user and those you specifically authorize with the options, **Allow these users to access App store**, and **Allow these groups to access App Store**.

You can set the following options with this policy:

Use this option	To do this
Allow these users to access App Store	The names of local or AD users who are allowed to access the App Store. When this policy is enabled, only users on this list and the root user are allowed to access the App Store.
Allow these groups to access App Store	The names of local or AD groups that are allowed to access the App Store. When this policy is enabled, only users in the specified groups, and the root user, are allowed to access the App Store.

This policy can take effect dynamically at the next group policy refresh interval without rebooting the computer.

Custom Settings

Path

Computer Configuration > Policies > Centrify Settings > Mac OS X Settings > Custom Settings

Description

Use the **Computer Configuration > Policies > Centrify Settings > Mac OS X Settings > Custom Settings** group policy settings to customize and install configuration profiles. The “Install MobileConfig Profiles” policy installs a device profile. To install a user profile, use the same policy in **User Configuration > Policies > Centrify Settings > Mac OS X Settings > Custom Settings.**

Enable Profile Custom Settings

Path

Computer Configuration > Policies > Centrify Settings > Mac OS X Settings > Custom Settings > Enable profile custom settings

Description

Enable this group policy to use the Custom payload to specify preference settings for applications that use the standard plist format for their preference files.

Note: This group policy only supports macOS 10.15 and lower.

You can use this GP to add specific keys and values to an existing preferences plist file. However, not all applications work with managed preferences, and in some cases only specific settings can be managed.

By default, you should place the plist files with preference settings in the folder `\\domain\SYSVOL\<domain>\customsettings`.

To add a file, click **Add** and enter name of a file that you placed in the SYSVOL location. The file you specify is relative to this path:

`\\domain\SYSVOL\domain\customsettings`

For example, if you enter:

`com.apple.plist`

the file that is imported is:

`\\domain\SYSVOL\domain\customsettings\com.apple.plist`

Install MobileConfig Profiles

Path

Computer Configuration > Policies > Centrify Settings > Mac OS X Settings > Custom Settings > Install MobileConfig Profiles

Description

Enable this group policy to install mobile configuration profiles on managed Mac computers.

Note: There is a Computer Configuration version of this policy (which installs device profiles) and a User Configuration version (which installs user profiles).

Note: This group policy only supports macOS 10.15 and lower.

Before enabling this policy, you must create a directory and copy mobile configuration files to `SYSVOL` on the domain controller. `SYSVOL` is a well-known shared directory on the domain computer that stores server copies of public files that must be shared throughout the domain.

Specifically, create the following directory on the domain controller:

`\\domainName\SYSVOL\domainName\mobileconfig`

and copy one or more mobile configuration profile files to this directory. See Deploy Configuration Profiles to Multiple Computers for details on how to do this.

To specify mobile configuration files to install, enable the policy, then click **Add**. Enter the name of a mobile configuration file that you placed in SYSVOL on the domain controller. Include the .mobileconfig suffix with the name.

If you specify a file that is not in the SYSVOL mobileconfig directory, the profile will not be installed.

If you add new files to the existing list in the group policy, those profiles will be installed – existing profiles will not be touched. If you remove previously specified files, the profiles defined by these files will be uninstalled.

If you add two or more profile files that have the same payloadIdentifier, only one of them will be installed.

If you change the group policy to “Disabled” or “Not Configured”, all existing profiles that were installed previously by the group policy will now be uninstalled from the managed Mac computers.

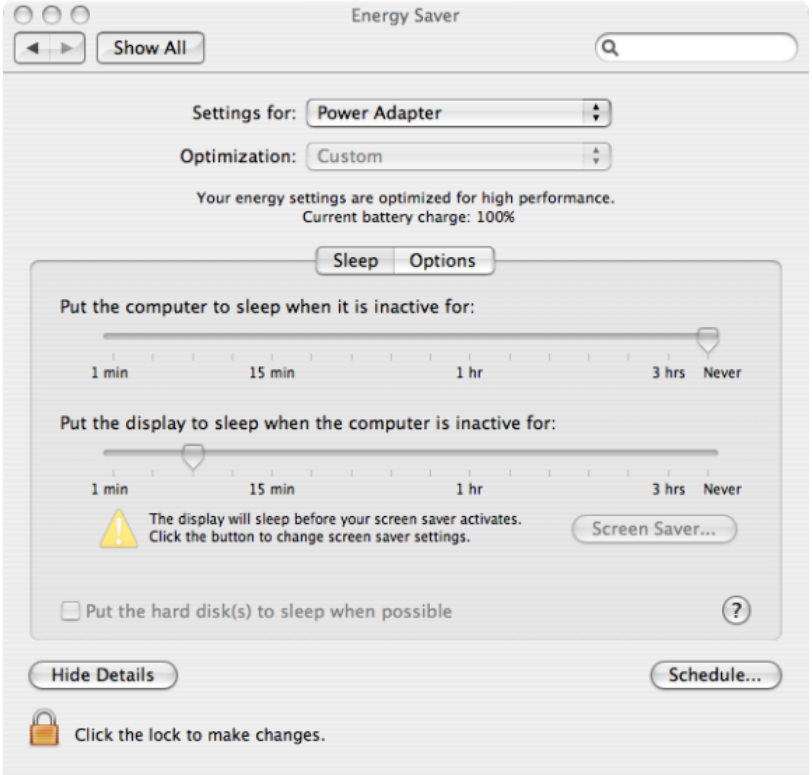
Energy Saver

Path

Computer Configuration > Policies > Centrify Settings > Mac OS X Settings > Energy Saver

Description

Use the **Computer Configuration > Policies > Centrify Settings > Mac OS X Settings > Energy Saver** settings to manage sleep and wake-up options from the Energy Saver ( ) system preference on Mac computers. For example:



You can configure power options or schedule startup and shutdown times.

Open the appropriate folder to set power options when running on AC power or battery power. Each folder has the identical set of group policies:

- On AC power
- On battery power

Allow Power Button to Sleep the Computer

Path

Computer Configuration > Policies > Centrify Settings > Mac OS X Settings > Energy Saver > Allow power button to sleep the computer

Description

Allow the power button to sleep the computer.

Enabling this group policy is the same as selecting the **Allow power button to sleep the computer** option in the Options pane of Energy Saver system preference.

This policy can take effect dynamically at the next group policy refresh interval.

Put The Hard Disk(s) to Sleep When Possible

Path

Computer Configuration > Policies > Centrify Settings > Mac OS X Settings > Energy Saver > Put the hard disk(s) to sleep when possible

Description

Put computer hard disks to sleep when they are inactive.

Enabling this group policy is the same as selecting the **Put the hard disk(s) to sleep when possible** option in the Sleep pane of Energy Saver system preference.

This policy can take effect dynamically at the next group policy refresh interval.

Restart Automatically After a Power Failure

Path

Computer Configuration > Policies > Centrify Settings > Mac OS X Settings > Energy Saver > Restart automatically after a power failure

Description

Enable to set the computer to automatically restart after a power failure.

Enabling this group policy is the same as selecting the **Restart automatically after a power failure** option in the Options pane of Energy Saver system preference.

This policy can take effect dynamically at the next group policy refresh interval.

Set Computer Sleep Time

Path

Computer Configuration > Policies > Centrify Settings > Mac OS X Settings > Energy Saver > Set computer sleep time

Description

Specify the number of minutes of inactivity to allow before automatically putting a computer into the sleep mode.

If you enable this group policy, the period of inactivity you specify applies only when the computer is using its power adapter. If the computer is inactive for the number of minutes you specify, it is put in sleep mode.

Enabling this group policy is the same as selecting a time using the **Put the computer to sleep when it is inactive for** slider in the Sleep pane of Energy Saver system preference.

To prevent the computer from ever going into sleep mode, enter 0 for the number of minutes, or disable the policy.

This policy can take effect dynamically at the next group policy refresh interval.

Set Display Sleep Time

Path

Computer Configuration > Policies > Centrify Settings > Mac OS X Settings > Energy Saver > Set display sleep time

Description

Specify the number of minutes of inactivity to allow before automatically putting the display into the sleep mode.

If you enable this group policy, the period of inactivity you specify applies when the computer is using its power adapter. If the computer is inactive for the number of minutes you specify, the display is put in sleep mode.

Enabling this group policy is the same as selecting a time using the **Put the display to sleep when it is inactive for** slider in the Sleep pane of Energy Saver system preference.

To prevent the display from ever going into sleep mode, enter 0 for the number of minutes, or disable the policy.

This policy can take effect dynamically at the next group policy refresh interval.

Wake When the Modem Detects a Ring

Path

Computer Configuration > Policies > Centrify Settings > Mac OS X Settings > Energy Saver > Wake when the modem detects a ring

Description

Automatically take a computer out of sleep mode when the modem detects a ring. This group policy allows a computer that has been put to sleep to remain available to answer the modem.

This policy can take effect dynamically at the next group policy refresh interval.

Wake for Ethernet network administrator access

Automatically take a computer out of sleep mode when the computer receives a Wake-on-LAN packet from an administrator. This group policy allows a computer that has been put to sleep to remain available to network administrator access.

Enabling this group policy is the same as selecting the **Wake for Ethernet network administrator access** option in the Options pane of Energy Saver system preference.

This policy can take effect dynamically at the next group policy refresh interval.

Scheduled Events

Path

Computer Configuration > Policies > Centrify Settings > Mac OS X Settings > Energy Saver > Scheduled events

Description

To configure sleep/shutdown times and startup times, open the Scheduled events folder (**Computer Configuration Policies > Centrify Settings > Mac OS X Settings > EnergySaver > Scheduled events**).

Set Machine Sleep/Shutdown Time

Path

Computer Configuration > Policies > Centrify Settings > Mac OS X Settings > Energy Saver > Scheduled events > Set machine sleep/shutdown time

Description

Specify a time to shut down or put the computer to sleep.

Enabling this group policy is the same as selecting the **Schedule** button in the Energy Saver system preference, then specifying times and days to shut down or put the computer to sleep.

After enabling this policy, specify values for the following:

- **Action**: Select **sleep** or **shutdown**
- **Set machine sleep/shutdown time**: Enter a time in the format HH:mm using a 24 hour clock; for example, to shut down or put the computer to sleep at 10:05 P.M:

22:05

- **Sleep/shutdown machine on every:** Select the days of the week on which to shut down or sleep the computer at the specified time. All days are selected by default.

This policy can take effect dynamically at the next group policy refresh interval.

Set Machine Startup Time

Path

Computer Configuration > Policies > Centrify Settings > Mac OS X Settings > Energy Saver > Scheduled events > Set machine startup time

Description

Specify a time to start up the computer.

Enabling this group policy is the same as selecting the **Schedule** button in the Energy Saver system preference, then specifying times and days to start up the computer.

After enabling this policy, specify values for the following:

- **Set machine startup time**: Enter a time in the format HH:mm using a 24 hour clock; for example, to start up the computer at 7:55 A.M.:

07:55

- **Start machine on every**: Select the days of the week on which to start the computer at the specified time. All days are selected by default.

This policy can take effect dynamically at the next group policy refresh interval.

Firewall

Path

Computer Configuration > Policies > Centrify Settings > Mac OS X Settings > Firewall

Description

Use the **Computer Configuration > Policies > Centrify Settings > Mac OS X Settings > Firewall** settings to manage the firewall options on Mac computers.

Enabling the Centrify firewall group policies is the same as setting options from **System Preferences > Security > Firewall**.

> **Note:** With the Centrify Firewall Group Policies, you can allow all incoming connections, or limit connections to the specified services and applications. You cannot block all connections:

In addition, group policies are available for the Advanced firewall settings, Enable Firewall Logging, and Enable Stealth Mode.

Enable Firewall

Path

Computer Configuration > Policies > Centrify Settings > Mac OS X Settings > Firewall > Enable firewall

Description

Prevent incoming network communication to all services and ports other than those explicitly enabled for the services specified in the Services pane of the Sharing system preferences.

This group policy turns on default firewall protection.

- Block all incoming connections:

  Block all incoming connections except those required for basic Internet services, such as DHCP, Bonjour, and IPSec.

- Automatically allow signed software to receive incoming connections:

  Allows software signed by a valid certificate authority to provide services accessed from the network. This setting will not take effect if **Block all incoming connections** is selected.

This policy takes effect dynamically at the next group policy refresh interval without rebooting the computer.

Enable iChat

Path

Computer Configuration > Policies > Centrify Settings > Mac OS X Settings > Firewall > Enable iChat

Description

On Mac OS X Servers, enabling this policy has no effect. If the firewall is enabled, the iChat service is not allowed through the firewall.

If the firewall is enabled, enabling this group policy is the same as clicking the **On** checkbox to allow communication through the firewall for iChat Bonjour. If you do not enable this group policy, traffic for iChat Bonjour will be blocked from the local computer.

This policy can take effect dynamically at the next group policy refresh interval without rebooting the computer.

Enable iPhoto Sharing

Path

Computer Configuration > Policies > Centrify Settings > Mac OS X Settings > Firewall > Enable iPhoto Sharing

Description

On Mac OS X Servers, enabling this policy has no effect. If the firewall is enabled, the iPhoto Sharing service is not allowed through the firewall.

If the firewall is enabled, enabling this group policy is the same as clicking the **On** checkbox to allow communication through the firewall for iPhoto Bonjour Sharing. If you do not enable this group policy, traffic for iPhoto Bonjour Sharing will be blocked from the local computer. Users will be able to access iPhoto collections on other computers, but the local computer cannot be used to serve any iPhoto collections.

This policy can take effect dynamically at the next group policy refresh interval without rebooting the computer.

Enable iTunes Music Sharing

Path

Computer Configuration > Policies > Centrify Settings > Mac OS X Settings > Firewall > Enable iTunes Music Sharing

Description

Enabling this group policy is the same as clicking the **On** checkbox to allow communication through the firewall for iTunes Music Sharing.

On Mac OS X Servers, enabling this policy has no effect. If the firewall is enabled, the iTunes Music Sharing service is not allowed through the firewall.

If you do not enable this group policy, traffic for iTunes Music Sharing will be blocked from the local computer. Users will be able to access iTunes collections on other computers, but the local computer cannot be used to serve any iTunes collections.

This policy can take effect dynamically at the next group policy refresh interval without rebooting the computer.

Enable Network Time

Path

Computer Configuration > Policies > Centrify Settings > Mac OS X Settings > Firewall > Enable network time

Description

On Mac OS X Servers, enabling this policy has no effect. If the firewall is enabled, the Network Time service is not allowed through the firewall.

If the firewall is enabled, enabling this group policy is the same as clicking the **On** checkbox to allow communication through the firewall for Network Time. If you do not enable this group policy, traffic from the Network Time service will be blocked.

This policy can take effect dynamically at the next group policy refresh interval without rebooting the computer.

Block UDP Traffic

Path

Computer Configuration > Policies > Centrify Settings > Mac OS X Settings > Firewall > Block UDP traffic

Description

Enabling this group policy is the same as clicking the **Block UDP Traffic** checkbox in the Advanced firewall settings.

This group policy does not block UDP communications that are related to requests initiated on the local computer.

This policy can take effect dynamically at the next group policy refresh interval without rebooting the computer.

Enable Firewall Logging

Path

Computer Configuration > Policies > Centrify Settings > Mac OS X Settings > Firewall > Enable firewall logging

Description

Log information about firewall activity, including all of the sources, destinations, and access attempts that are blocked by the firewall. The activity is recorded in the secure.log file on the local computer.

Enabling this group policy is the same as clicking the **System Preferences > Security > Firewall** then clicking **Enable Firewall Logging** in the Advanced firewall settings.

On Mac OS X Servers, enabling this policy has no effect.

This policy takes effect dynamically at the next group policy refresh interval without rebooting the computer.

Enable Stealth Mode

Prevent uninvited traffic from receiving a response from the local computer.

Enabling this group policy is the same as clicking the **System Preferences > Security > Firewall** then clicking **Enable Stealth Mode** in the Advanced firewall settings.

If you enable this group policy, the local computer will not respond to any network requests, including ping requests. Because the computer will not reply to ping requests, using this policy may prevent you from using network diagnostic tools that require a response from the local computer.

On Mac OS X Servers, enabling this policy has no effect.

This policy takes effect dynamically at the next group policy refresh interval without rebooting the computer.

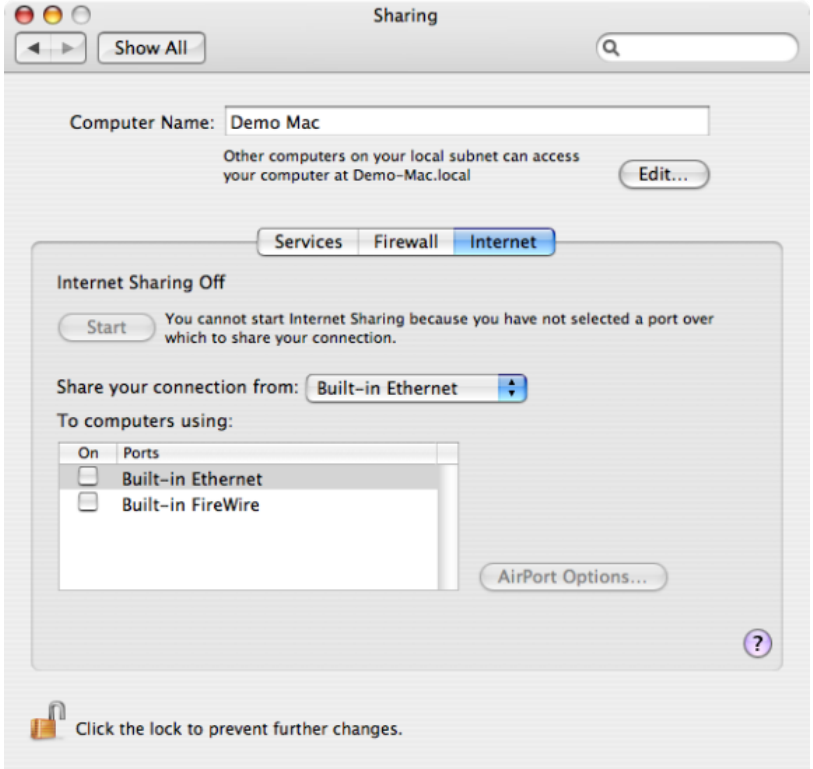
Internet Sharing

Path

Computer Configuration > Policies > Centrify Settings > Mac OS X Settings > Internet Sharing

Description

Use the **Computer Configuration > Policies > Centrify Settings > Mac OS X Settings >Internet Sharing** group policy to prevent any kind of Internet sharing on the local computer. This group policy can only be used to prevent Internet sharing. Although this group policy corresponds to a setting on the Internet pane of the Sharing ( ) system preference, you can not use it to start Internet sharing, configure the shared connection, or set any other options. For example:



Disallow All Internet Sharing

Path

Computer Configuration > Policies > Centrify Settings > Mac OS X Settings > Internet Sharing > Disallow all Internet Sharing

Description

Prevent any kind of Internet sharing on the local computer. Enabling this group policy is the same as clicking **Stop** to prevent other computers from sharing an Internet connection on a local computer in the Internet pane of the Sharing system preference.

For this group policy, clicking Disabled or Not Configured has no effect. If you have previously Enabled the group policy, Internet sharing will remain off until you manually start it on the local computer.

Once enabled, this group policy takes effect when users log out and log back in, or dynamically at the next group policy refresh interval without rebooting the computer.

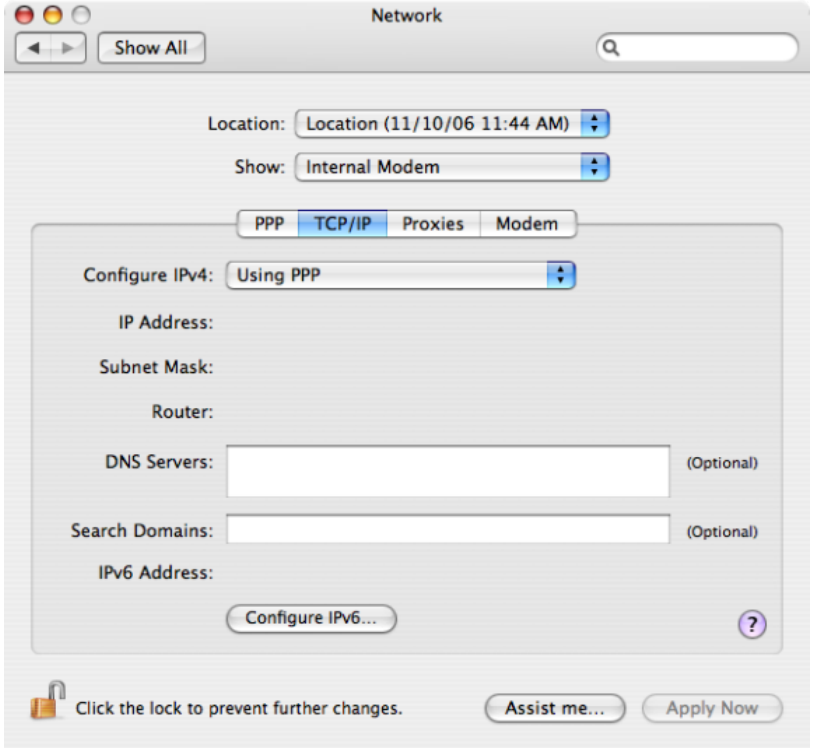
Network

Path

Computer Configuration > Policies > Centrify Settings > Mac OS X Settings > Network

Description

Use the **Computer Configuration > Policies > Centrify Settings > Mac OS X Settings > Network** settings to manage DNS search requests and proxy settings. These group policies correspond to settings in the TCP/IP and Proxies panes of the Network ( ) system preference on Mac computers. For example:



Legacy Location Settings

Path

Computer Configuration > Policies > Centrify Settings > Mac OS X Settings > Network > Legacy location settings

Description

Use **Computer Configuration > Policies > Centrify Settings > Mac OS X Settings > Network > Legacy location settings** to configure network settings for the Automatic network location.

Adjust List of DNS servers

Path

Computer Configuration > Policies > Centrify Settings > Mac OS X Settings > Network > Legacy location settings > Adjust list of DNS servers

Description

Control the list of DNS servers when performing DNS lookups.

To use this policy, click **Enabled**, then click **Add**, type the IP address for a DNS server, then click **OK** to add the server to the list of DNS servers. Add as many servers as you want in this manner. When you are finished adding the servers, click **OK** to close the dialog box.

At any time while the policy is enabled, you can select an address in the list and click **Edit** to change the address, or **Remove** to remove it as a DNS server.

This policy can take effect dynamically at the next group policy refresh interval without rebooting the computer.

Adjust List of Searched Domains

Path

Computer Configuration > Policies > Centrify Settings > Mac OS X Settings > Network > Legacy location settings > Adjust list of searched domains

Description

Control the list of domains to search when performing DNS lookups.

To use this policy, click **Enabled**, then click **Add**, type a domain name, then click **OK** to add the domain to the list of domains to search. Add as many domains as you want in this manner. When you are finished adding the domains to search, click **OK** to close the dialog box.

At any time while the policy is enabled, you can select a domain in the list and click **Edit** to change the name, or **Remove** to remove it as a domain to be searched.

This policy can take effect dynamically at the next group policy refresh interval without rebooting the computer.

Configure Proxies

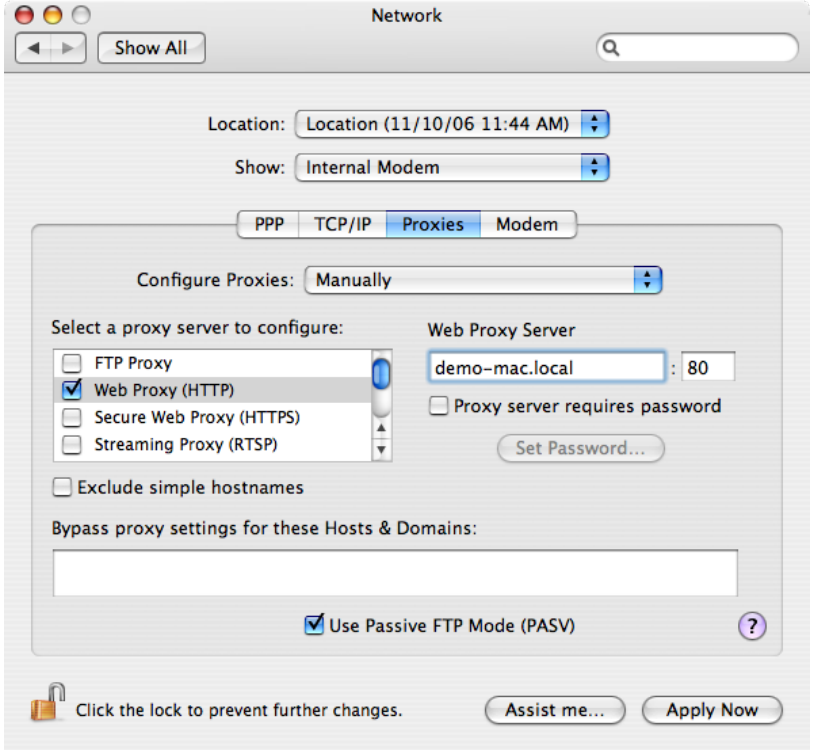
Path

Computer Configuration > Policies > Centrify Settings > Mac OS X Settings > Network > Legacy location settings > Configure Proxies

Description

Configure proxy servers to provide access to services through a firewall.

Use the **Computer Configuration > Policies > Centrify Settings > Mac OS X Settings > Network > Configure Proxies** settings to manage settings on the Proxies panes of the Network system preference. For example:



These group policies enable you to configure the host names (or IP addresses) and port numbers for the computers providing specific services, such as File Transfer Protocol (ftp), Hypertext Transfer Protocol (http), and HTTP over Secure Sockets Layer (https), through a firewall. A proxy server is a computer on a local network that acts as an intermediary between computer users and the Internet to ensure the security and administrative control of the network.

Enable Proxies

Path

Computer Configuration > Policies > Centrify Settings > Mac OS X Settings > Network > Legacy location settings > Configure Proxies > Enable Proxies

Description

Configure the host name (or IP address) and port number for the computers providing specific services. Within this category, you can enable the following proxy servers:

- Use the **Enable FTP Proxy** policy to configure the host name and port number for the FTP proxy server (FTP protocol).
- Use the **Enable Web Proxy** policy to configure the host name and port number for the Web proxy server (HTTP protocol).
- Use the **Enable Secure Web Proxy** policy to configure the host name and port number for the Secure Web proxy server (HTTPS protocol).
- Use the **Enable Streaming Proxy** policy to configure the host name and port number for the Streaming proxy server (RTSP protocol).

- Use the **Enable SOCKS Proxy** policy to configure the host name and port number for the Streaming proxy server (SOCKS protocol).
- Use the **Enable Gopher Proxy** policy to configure the host name and port number for the Gopher proxy server.
- Use the **Enable Streaming Proxy** policy to configure the host name and port number for the Streaming proxy server (RTSP protocol).
- Use the **Enable Proxies using a PAC file** policy to configure proxy servers from a proxy configuration file.

These policies can take effect dynamically at the next group policy refresh interval without rebooting the computer.

Exclude Simple Hostnames

Path

Computer Configuration > Policies > Centrify Settings > Mac OS X Settings > Network > Legacy location settings > Configure Proxies > Exclude simple hostnames

Description

Prevent requests to unqualified host names from using proxy servers. If you enable this policy, users can enter unqualified host names to contact servers directly rather than through a proxy.

This policy can take effect dynamically at the next group policy refresh interval without rebooting the computer.

Use Passive FTP Mode (PASV)

Path

Computer Configuration > Policies > Centrify Settings > Mac OS X Settings > Network > Legacy location settings > Configure Proxies > Use Passive FTP Mode (PASV)

Description

Use the FTP passive mode (PASV) to access Internet sites when computers are protected by a firewall.

This policy can take effect dynamically at the next group policy refresh interval without rebooting the computer.

Bypass Proxy Settings for these Hosts & Domains

Path

Computer Configuration > Policies > Centrify Settings > Mac OS X Settings > Network > Legacy location settings > Configure Proxies > Bypass Proxy settings for these Hosts & Domains

Description

Specify fully-qualified host names and domains for which you want to bypass proxy settings.

You should use this policy to define the hosts or domains that should never be contacted by proxy.

To use this policy, click **Enabled**, then click **Add**, type a host or domain name, and click **OK** to add the entry to the Show Contents list.

Each host or domain should be listed as a separate line in the Hosts and Domains list. For each host or domain, click **Add**, type the host or domain name, and click **OK** to add the host or domain as a new entry in the list. When you are finished adding items to the list, click **OK** to close the policy dialog box.

This policy can take effect dynamically at the next group policy refresh interval without rebooting the computer.

Location 1 and Location 2

Path

Computer Configuration > Policies > Centrify Settings > Mac OS X Settings > Network > Location 1

Computer Configuration > Policies > Centrify Settings > Mac OS X Settings > Network > Location 2

Description

Use **Computer Configuration > Policies > Centrify Settings > Mac OS X Settings > Network > Location 1** to configure network settings for an additional network location. The group policies in Location 2 are identical, and allow you to configure network settings for another network location.

Adjust List of DNS Servers

Path

Computer Configuration > Policies > Centrify Settings > Mac OS X Settings > Network > Location 1/Location 2 > Adjust list of DNS servers

Description

Control the list of DNS servers when performing DNS lookups.

To use this policy, click **Enabled**, then click **Add**, type the IP address for a DNS server, then click **OK** to add the server to the list of DNS servers. Add as many servers as you want in this manner. When you are finished adding the servers, click **OK** to close the dialog box.

At any time while the policy is enabled, you can select an address in the list and click **Edit** to change the address, or **Remove** to remove it as a DNS server.

This policy can take effect dynamically at the next group policy refresh interval without rebooting the computer.

Adjust List of Searched Domains

Path

Computer Configuration > Policies > Centrify Settings > Mac OS X Settings > Network > Location 1/Location 2 > Adjust list of searched domains

Description

Control the list of domains to search when performing DNS lookups.

To use this policy, click **Enabled**, then click **Add**, type a domain name, then click **OK** to add the domain to the list of domains to search. Add as many domains as you want in this manner. When you are finished adding the domains to search, click **OK** to close the dialog box.

At any time while the policy is enabled, you can select a domain in the list and click **Edit** to change the name, or **Remove** to remove it as a domain to be searched.

This policy can take effect dynamically at the next group policy refresh interval without rebooting the computer.

Enable Network Location

Path

Computer Configuration > Policies > Centrify Settings > Mac OS X Settings > Network > Location 1/Location 2 > Enable network location

Description

Enable all network location settings under the current location category and set its location name. This policy must be enabled to apply settings in this location category (for example, Location1).

This policy can take effect dynamically at the next group policy refresh interval without rebooting the computer.

Configure Proxies

Path

Computer Configuration > Policies > Centrify Settings > Mac OS X Settings > Network > Location 1/Location 2 > Configure Proxies

Description

Configure proxy servers to provide access to services through a firewall. The group policies in this folder are the same as the ones in Computer Configuration > Policies > Centrify Settings > Mac OS X Settings > Network > Legacy Location settings> Configure Proxies. Refer to Configure Proxies for more information.

Remote Management

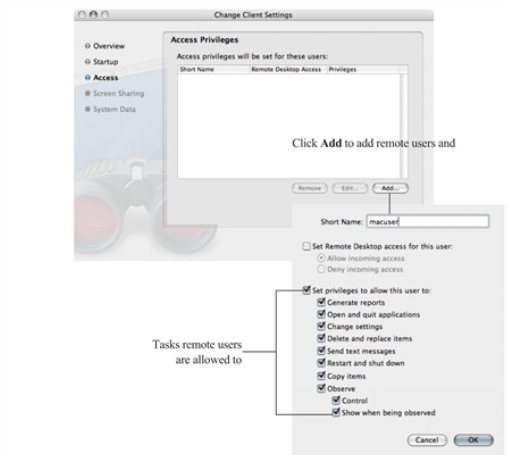
Path

Computer Configuration > Policies > Centrify Settings > Mac OS X Settings > Remote Management

Description

Use the **Computer Configuration > Policies > Centrify Settings > Mac OS X Settings > Remote Management** settings to control Apple Remote Desktop access for zone users. You can use these group policies to give Active Directory group members permission to remotely control Mac computers without physically having to activate the Apple Remote Desktop on the remote Mac computer.

The Remote Management group policies correspond to the **Manage > Change Client Settings** options in Apple Remote Desktop and are similar to access privileges defined on a client computer using the Sharing system preference. For example:



Note: Because the group policies correspond to the **Manage > Change Client Settings** options in Apple Remote Desktop, the group policy settings are not displayed in the local system preference on the Mac client. Although the tasks you can assign to different groups by group policy correspond to tasks you can assign using the local Sharing system preference on a Mac client computer, the group policy settings do not update the local system preference to display check marks for the tasks that the remote users have been given permission to perform.

Enable Administrator Access Groups

Path

Computer Configuration > Policies > Centrify Settings > Mac OS X Settings > Remote Management > Enable administrator access groups

Description

Allow all users who are members of the following Apple Remote Desktop administrator groups to access this computer using Apple Remote Desktop.

Before enabling this group policy, you should create each Active Directory security group you intend to use and add a UNIX profile for each group to the zone, using the exact UNIX group names (`ard_admin, ard_reports, ard_manage, ard_interact`).

Note: Creating UNIX profiles with these group names displays a warning message because the names are longer than eight characters. You can safely ignore this warning message.

Enabling this policy allows users in the following groups to manage Mac computers through Apple Remote Desktop:

- `ard_admin` gives all members of the group the ability to remotely control the computer desktop.
- `ard_reports` gives all members of the group the ability to remotely generate reports on the computer.
- `ard_manage` gives all members of the group the ability to manage the computer using Apple Remote Desktop. Users in this group can perform the following tasks by using Apple Remote Desktop:
  - Generate reports
  - Open and quit applications
  - Change settings
  - Copy Items
  - Delete and replace items
  - Send text messages
  - Restart and shut down
- `ard_interact` gives all members of the group the ability to interactively observe or control the computer using Apple Remote Desktop.

  Users in this group can perform the following tasks by using Apple Remote Desktop:
  - Send text messages

- Observe
- Control

This policy can take effect dynamically at the next group policy refresh interval without rebooting the computer.

See Setting Up Local and Remote Administrative Privileges for information on how to use this group policy with the Map Zone Groups to Local Admin Group policy to enable both local and remote administrative access for the same group of users.

Scripts (Login/Logout)

Path

Computer Configuration > Policies > Centrify Settings > Mac OS X Settings > Scripts (Login/Logout)

Description

Use the **Computer Configuration > Policies > Centrify Settings > Mac OS X Settings > Scripts (Login/Logout) > Specify multiple login scripts** group policy to deploy login scripts that run when an Active Directory or local user logs on. When you use this group policy, the login scripts are stored in the Active Directory domain's system volume (sysvol) and transferred to the Mac computer when the group policies are applied. Login scripts are useful for performing common tasks such as mounting and un-mounting shares

This policy is also available as a user policy. If you specify scripts using both the computer and user policies, the computer scripts are executed first.

Specify Multiple Login Scripts

Path

Computer Configuration > Policies > Centrify Settings > Mac OS X Settings > Scripts (Login/Logout) > Specify multiple login scripts

Description

Specify the names of one or more login scripts to execute when an AD or local user logs on. The scripts you specify run simultaneously in no particular order.

Before enabling this policy, you should create the scripts and copy them to the system volume (sysvol) on the domain controller. By default, the login scripts are stored in the system volume (SYSVOL) on the domain controller in the directory:

```
\\domain\SYSVOL\domain\Scripts
\scriptname1
\scriptname2
...
```

After enabling this policy, click **Add** and enter the following information:

- **Script**: The name of the script and an optional path, which are relative to `\\domain\SYSVOL\domain\scripts\`

  For example, if the domain name is `ajax.org` and you enter a script name of `start.sh`, the script that gets executed on the domain controller is:

  `\\ajax.org\SYSVOL\ajax.org\Scripts\mlogin.sh`

You can specify additional relative directories in the path, if needed; for example, if you type `submlogin.sh`, the file that gets executed is: `\\ajax.org\SYSVOL\ajax.org\Scripts\sub\mlogin.sh`

- **Parameters**: An optional set of arguments to pass to the script. These arguments are interpreted the same way as in a UNIX shell; that is, space is a delimiter, and backslash is an escape character. You can also use `$USER` to represent the current user's name. For example:

```
arg1 arg2 arg3
arg1 'a r g 2' arg3
```

> **Note:** Be certain authenticated users have permission to read these files so the scripts can run when they log in.

Once this group policy is enabled, it takes effect when users log out and log back in.

Scripts (LaunchDaemons)

Path

Computer Configuration > Policies > Centrify Settings > Mac OS X Settings > Scripts (launchDaemons)

Description

Use the **Computer Configuration > Policies > Centrify Settings > Mac OS X Settings > Scripts (LaunchDaemons) > Specify multiple LaunchDaemon scripts** group policy to deploy scripts that run when launchd starts (system boot up). When you use this group policy, the LaunchDaemon scripts are stored in the Active Directory domain's system volume (sysvol) and transferred to the Mac computer when the group policies are applied. Using LaunchDaemons to run scripts allows you to run the scripts as root, where the **Specify multiple login scripts** group policy can only be run as the logged in user.

Refer to the following Apple resources to learn more about Launch Daemons and Agents.

- https://developer.apple.com/library/content/documentation/MacOSX/Conceptual/BPSystemStartup/Chapters/CreatingLaunchdJobs.html
- https://developer.apple.com/library/content/technotes/tn2083/_index.html#//apple_ref/doc/uid/DTS10003794

Specify Multiple LaunchDaemon Scripts

Path

Computer Configuration > Policies > Centrify Settings > Mac OS X Settings > Scripts (launchDaemons) > Specify multiple LaunchDaemon scripts

Description

Enable this group policy to specify multiple scripts to run automatically when `launchd` starts (system boot up).

The scripts you specify run simultaneously in no particular order.

Before enabling this policy, you should create the scripts and copy them to the system volume (`sysvol`) on the domain controller. By default, the LaunchDaemon scripts are stored in the system volume (`SYSVOL`) on the domain controller in the directory:

```
\\domain\SYSVOL\domain\Scripts
\scriptname1
```

```
\scriptname2
...
```

After enabling this policy, click **Add** and enter the following information:

- **Script**: The name of the script and an optional path, which are relative to `\\domain\SYSVOL\domain\scripts\`.

  For example, if the domain name is `ajax.org` and you enter a script name of `startup.sh`, the script that gets executed on the domain controller is:

  `\\ajax.org\SYSVOL\ajax.org\Scripts\startup.sh`

You can specify additional relative directories in the path, if needed; for example, if you type `submlogin.sh`, the file that gets executed is: `\\ajax.org\SYSVOL\ajax.org\Scripts\sub\startup.sh`

- **Parameters**: An optional set of arguments to pass to the script. These arguments are interpreted the same way as in a UNIX shell; that is, space is a delimiter, and backslash is an escape character. For example:

```
arg1 arg2 arg3
arg1 'a r g 2' arg3
```

Security & Privacy

Path

Computer Configuration > Policies > Centrify Settings > Mac OS X Settings > Security & Privacy

Description

Use the Centrify group policies found in **Computer Configuration > Policies > Centrify Settings > Mac OS X Settings > Security & Privacy** to manage the Keychain, public and private keys, and the options from the Security & Privacy ( ) system preference on Mac OS X computers.

Auto Generate New Login Keychain

Path

Computer Configuration > Policies > Centrify Settings > Mac OS X Settings > Security & Privacy Settings > Auto Generate New Login Keychain

Description

Use this policy to automatically generate a new login keychain if a user's keychain password does not match the password they used to successfully login, resulting in the message "the system was unable to unlock your login keychain".

This commonly occurs if someone has changed their account password on another system.

If this policy is enabled, a new keychain will be generated when a password sync issue is discovered. This new keychain will be set as the default login keychain and the previous keychain will be moved to a backup.

Delinea recommends disabling this policy if you plan to use Enable Keychain Synchronization.

This policy is disabled by default.

Certificate Validation Method

Path

Computer Configuration > Policies > Centrify Settings > Mac OS X Settings > Security & Privacy > Certificate validation method

Description

Specify the certificate validation method to use for the Mac computer.

> **Note:** This group policy has no effect on the "Keychain Access > Preferences > Certificates" settings. Keychain Access > Preferences are per-user settings, which are not used by a Mac computer during login. This group policy changes Centrify SmartCardTool > Revocation settings, which represent the system settings used by a Mac computer during login.

This policy allows you to choose either one, or both of the two common methods for verifying the validity of a certificate:

- **Certificate Revocation List**: Use a certificate revocation list (CRL) from a revocation server.
- **Online Certificate Status Protocol**: Use an online certificate status protocol (OCSP) responder to validate certificates.

  If you select this option, you can specify a local responder to override the one provided in the certificates.

For each validation option, you can select one of the following settings:

- **Off**: No revocation checking is performed.
- **Best attempt**: The certificate passes unless the server returns an indication of a bad certificate.

  This setting is recommended for most environments.
- **Require if cert indicates**: If the URL to the revocation server is provided in the certificate, this setting requires a successful connection to a revocation server as well as no indication of a bad certificate.

  Specify this option only in a tightly controlled environment that guarantees the presence of a CRL server or OCSP responder. If a CRL server or OCSP responder is not available, SSL and S/MIME evaluations could hang or fail.
- **Require for all certs**: This setting requires successful validation of all certificates.

  Use only in a tightly controlled environment that guarantees the presence of a CRL server or OCSP responder. If a CRL server or OCSP responder is not available, SSL and S/MIME evaluations could hang or fail.
- **Local Responder**: If you choose to validate the certificate via OCSP, you can specify a local responder to override that provided in the certificates.
- **Priority**: The priority determines which method (OCSP or CRL) is attempted first.

  If the first method chosen returns a successful validation, the second method is not attempted, unless you choose to require both.

Disable Automatic Login

Path

Computer Configuration > Policies > Centrify Settings > Mac OS X Settings > Security & Privacy > Disable automatic login

Description

Disable the automatic login setting. If you enable this group policy, it overrides the Login Options set in the General tab of the Security & Privacy system preference.

For this group policy, clicking Disabled or Not Configured has no effect.

Once enabled, this group policy takes effect when the computer is rebooted.

Disable Location Services

Path

Computer Configuration > Policies > Centrify Settings > Mac OS X Settings > Security & Privacy > Disable Location Services

Description

Disable the “Enable Location Services” setting. If you enable this group policy, it overrides the Enable Location Services setting in the Privacy tab of the Security & Privacy system preference.

Note: As of MacOS Catalina, it is not enough to wait for the next group policy refresh or execute adgpupdate. You also need to restart the Mac for this GP to take effect.

For this group policy, clicking Disabled or Not Configured has no effect.

Once enabled, this group policy takes effect at the next group policy refresh interval.

Enable Smart Card Support

Path

Computer Configuration > Policies > Centrify Settings > Mac OS X Settings > Security & Privacy > Enable smart card support

Description

Enable users to logon with smart cards. If you enable this group policy, it adds smart card support to the authorization database on Mac computers that are linked to the group policy object.

Delinea smart card support for macOS is based on the macOS modern native framework, CryptoTokenKit

See Configuring a Mac Computer for Smart Card Login for details.

Select **Enable smart card support for the SUDO command**, then when executing the SUDO command, smart card user can authenticate identity by smart card PIN.

Select **Enable smart card support for the SU command**, then when executing the SU command, smart card user can authenticate identity by smart card PIN.

Select **Enable smart card support for the LOGIN command**, then when executing the LOGIN command, smart card user can authenticate identity by smart card PIN.

Select **Enforce smart card login**, then only smart card users with a smart card can log in to the Mac machine.

Edit **Exception group** to add a exception group for the "Enforce smart card login", then any users belong to this group always can log in to the Mac machine by a username and password. In general, we recommend set a exception group, for example, admin, when **Enforce smart card login** is selected.

Select one of options in **Certificate trust behavior** to set smart card certificate trust behavior, the meaning of number:

0: Smart card certificate trust isn't required.

1: Smart card certificate and chain must be trusted.

2: Certificate and chain must be trusted and not receive a revoked status.

3: Certificate and chain must be trusted and revocation status is returned valid.

Once enabled, this policy takes effect dynamically at the next group policy refresh interval.

Enable FileVault 2

Path

Computer Configuration > Policies > Centrify Settings > Mac OS X Settings > Security & Privacy > Enable FileVault 2

Description

This group policy allows you to select whether to use one institutional key for multiple Mac computers, or computer-specific ("personal") keys.

To use one institutional key for multiple Mac computers, select **Use Institutional Recovery Key**. Then click **Select** to select the certificate that contains the FileVault master keychain that can unlock the encrypted disk. You must already have created a FileVault master keychain and exported the certificate for the master keychain to a Windows domain server before you perform this step.

To use computer-specific ("personal") keys instead of one institutional key, leave **Use Institutional Recovery Key** unchecked. In this situation, a personal recovery key is created for the Mac computer and stored in the computer object in Active Directory. The key is created and sent to the computer object in Active Directory after the "Managed By" user logs in, logs out, and provides the user password.

This policy is available only for OS X 10.9 and later.

For complete instructions, see Configuring Filevault 2.

> **Note:** Enabling this group policy does not immediately enable FileVault 2 protection on a Mac computer. FileVault 2 protection is enabled when the FileVault-enabled user (that is, the "Managed By" user) logs on to the computer. Disabling this group policy does not disable FileVault 2 protection – disabling FileVault 2 can only be done manually.

Once enabled, this group policy takes effect at the next group policy update interval or when you execute the `adgpupdate` command.

Enable Gatekeeper

Path

Computer Configuration > Policies > Centrify Settings > Mac OS X Settings > Security & Privacy > Enable Gatekeeper

Description

Enable the Gatekeeper feature, which controls access to the Mac App store. This policy overrides the “Allow applications downloaded from” setting on the General tab of the Security & Privacy system preference pane.

After enabling the policy, select one of the following options:

- **Mac App Store** Only allow installation of applications that have been downloaded from the Mac App store.
- **Mac App Store** and identified developers. Only allow installation of applications that have been downloaded from the Mac App Store or were created by Apple-sanctioned developers.
- **Anywhere** Allow installation of any applications.

Enable Keychain Synchronization

Path

Computer Configuration > Policies > Centrify Settings > Mac OS X Settings > Security & Privacy > Enable Keychain synchronization

Description

This group policy controls whether to enable keychain synchronization, which synchronizes the login keychain to the login user’s AD password when a password change is detected.

Note: Keychain synchronization is password-focused and should not be used in smart card environments.

Set the **Password change detection interval (minutes)** option to determine the time (in minutes) between checking for changed passwords. There is a random zero to five minute variance in the actual interval each device is checked for a changed password to maintain performance. As a result, the minimum interval is five minutes.

The default value is 30 minutes.

The **Store AD password in the login Keychain** option is used to streamline updates of the user's login Keychain password. If this option is enabled the Keychain Sync utility stores the user's AD password in the login keychain the next time the user logs in. If the password is changed after the policy is enabled but before the previous password is stored in the login keychain, the keychain sync application requests the previous password.

When this option is selected, the user's AD password is encrypted using a static AES256 key that is unique to that user and stored in the login Keychain as an application password. The key and password are added to the keychain using the SecItemAdd API. In addition, an Access Control List ensures that only the Keychain Sync utility can access the key used to encrypt and decrypt the password.

Delinea recommends disabling Auto Generate New Login Keychain before enabling this policy

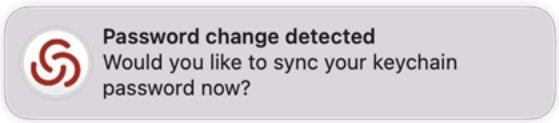
Please note the following limitations with the **Store AD Password in the login Keychain** option:

- This option only works on macOS 10.12 or later.
- The user’s AD password is inaccessible when the login keychain is locked.

  The most common scenario that causes this is if a user’s AD password is changed and the user logs out before synchronizing the keychain, then logs back in. When the user logs back in, the password check fails due to the new password, locking the login Keychain and preventing the Keychain Sync utility from accessing it.
- Password changes can only be detected when the machine is in connected mode.

User experience when the AD password is already stored in the login Keychain

1. The login user receives a password change notification when his/her password is changed remotely.

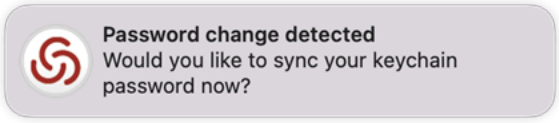


2. When the user clicks **Yes** on the notification, the Delinea Keychain Sync utility appears and asks for the current password to synchronize the keychain.

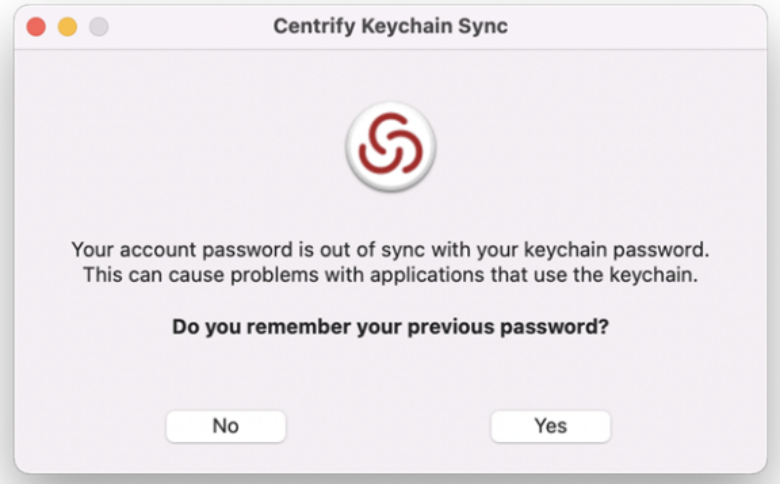
After entering the current password and clicking **OK**, the Keychain Sync utility synchronizes the login keychain with the new password.

User experience when the AD password is not yet stored in the login Keychain

1. The login user receives a password change notification when his/her password is changed remotely.



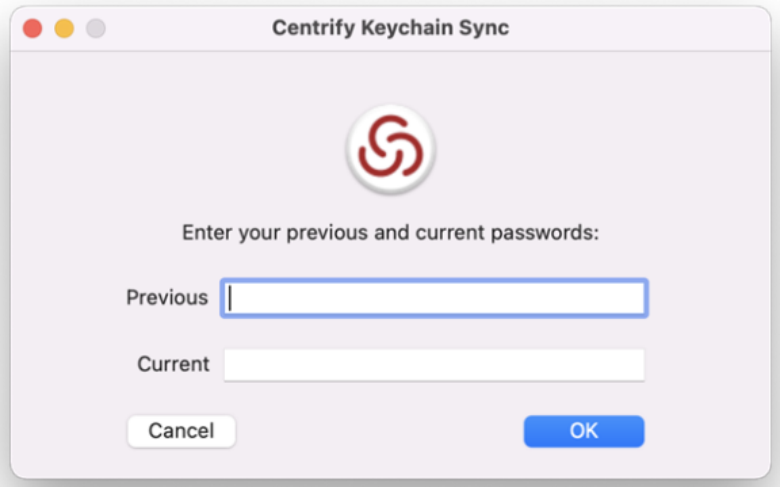
2. When the user clicks **Yes** on the notification, the Delinea Keychain Sync utility appears and asks if the user remembers the previous password.



3. The user clicks **Yes** or **No**.

- If the user clicks **No**, the Keychain Sync utility creates a new login keychain.

- If the user clicks **Yes**, the Keychain Sync utility asks for the previous and current passwords.



After entering the previous and current passwords and clicking **OK**, the Keychain Sync utility synchronizes the login keychain with the new password.

Log Out After Number of Minutes of Inactivity

Path

Computer Configuration > Policies > Centrify Settings > Mac OS X Settings > Security & Privacy > Log out after number of minutes of inactivity

Description

Specify the number of minutes of inactivity to allow on a computer before automatically logging out the current user. The default value is 5 minutes.

Setting the value to less than 5 minutes disables automatic logout. If you plan to disable automatic logout, it is recommended that you set the value to 0 to preserve backward compatibility.

Note: Disabling this policy does not disable automatic logout.

This policy takes effect when users log out and log back in after the next group policy refresh.

Require a Password to Wake this Computer from Sleep or Screen Saver

Path

Computer Configuration > Policies > Centrify Settings > Mac OS X Settings > Security & Privacy Settings > Require a password to wake this computer from sleep or screen saver

Note: This group policy only supports macOS 10.15 and lower.

Description

Lock the computer screen when the computer goes into sleep or screen saver mode and requires users to enter a user name and password to unlock the screen.

Enabling this group policy is the same as clicking the Require a password to wake this computer from sleep or screen saver option in the Security system preference.

After this group policy is enabled, it takes effect dynamically at the next group policy refresh interval.

Require Password to Unlock Each Secure System Preference

Path

Computer Configuration > Policies > Centrify Settings > Mac OS X Settings > Security & Privacy > Require password to unlock each secure system preference

Description

Lock sensitive system preferences to prevent users who aren't administrators from changing them. This group policy requires users to provide an administrator's password to unlock each secure system preference before they can make changes.

If you enable this policy, users must provide an administrator password to access any secure system preference. If the current user is logged on as an administrator and this policy is not configured or disabled, the user can access and change secure system preferences without providing the administrator password.

This policy can take effect dynamically at the next group policy refresh interval.

Use Secure Virtual Memory

Path

Computer Configuration > Policies > Centrify Settings > Mac OS X Settings > Security & Privacy > Use secure virtual memory

Description

Prevent passwords from being recoverable from virtual memory.

Any time a password is entered, it is possible for system to write that password in a block of memory that it dumps to a file in `/var/vm`, making the password recoverable.

Enabling this group policy ensures that the virtual memory `/var/vm` files are encrypted, preventing any passwords written there from being recovered.

This policy can take effect dynamically at the next group policy refresh interval.

Allow All Applications to Access the Auto-Enrollment Private Key(S)

Path

Computer Configuration > Policies > Centrify Settings > Mac OS X Settings > Security & Privacy > Public Key Policies > Allow all applications to access the auto-enrollment private key(s)

Description

Enabling this policy allows all applications to access the auto-enrollment private key(s) in the System keychain.

See Configuring Auto-Enrollment for more information about auto-enrollment keys.

Note: This setting only applies to a new auto-enrollment private key(s); it will not update already imported auto-enrollment private key(s) that are in the System keychain.

Allow Specific Applications to Access the Auto-Enrollment Private Key(S)

Path

Computer Configuration > Policies > Centrify Settings > Mac OS X Settings > Security & Privacy > Public Key Policies > Allow specific applications to use the auto-enrollment private key(s)

Description

Enabling this policy allows specified applications to access the auto-enrollment private key(s) in System keychain.

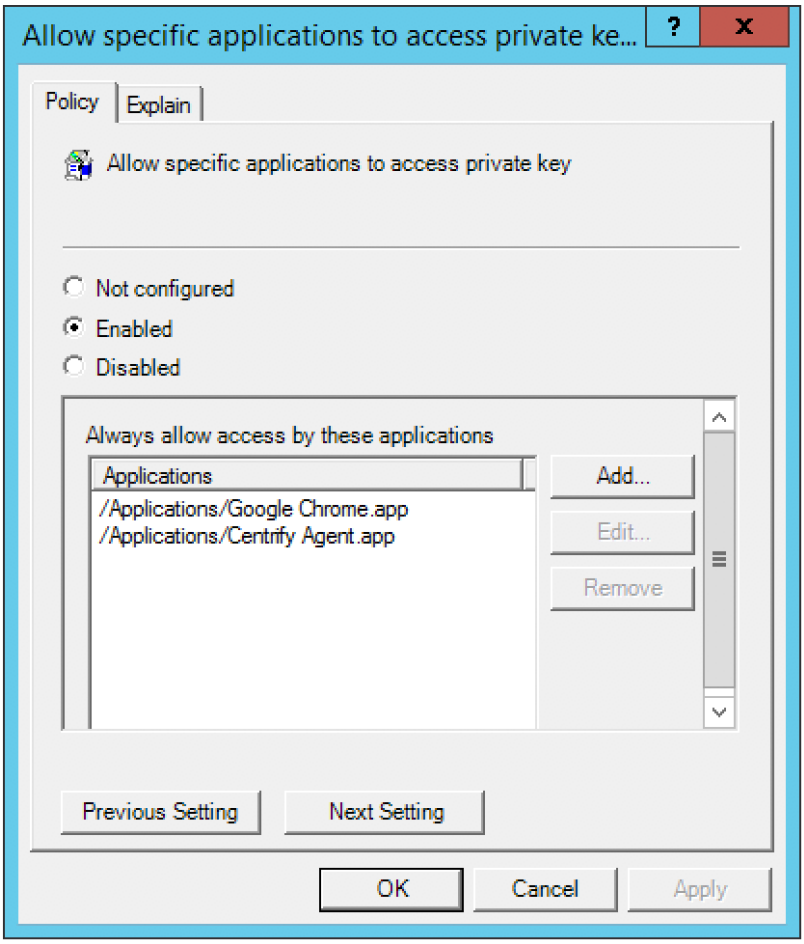
After you enable this policy, click **Add** to enter the path to the application you want to allow access to the auto-enrollment private key, then click **OK**. You can click **Add** again to add additional applications.

For example, to give Google Chrome and Delinea Agent access to the auto-enrollment private key, enter the application path for Google Chrome:

```
/Applications/Google Chrome.app
```

Click **OK**. Then click **Add** and enter the application path for Delinea Agent:

`/Applications/Centrify Agent.app`



After this group policy is enabled, the list of applications specified in the group policy are added to the access control list of the auto-enrollment private key in System keychain.

See Configuring Auto-Enrollment for more information about auto-enrollment keys.

> **Note:** This setting only applies to a new auto-enrollment private key. It does not change auto-enrolled private keys that are already in the keychain.

If the group policy **Allow all applications to access the auto-enrollment private key(s)** (above) is enabled, this group policy will be ignored.

Do Not Allow the Private Key(S) to be Extractable

Path

Computer Configuration > Policies > Centrify Settings > Mac OS X Settings > Security & Privacy > Public Key Policies > Do not allow private key(s) to be extractable

Description

Enabling this policy prevents exporting the auto-enrollment private key(s).

Note: This setting only applies to a new auto-enrollment private key. It does not change the auto-enrolled private key(s) that are already in the keychain.

Store The Private and Public Key(S) Only in the Keychain

Path

Computer Configuration > Policies > Centrify Settings > Mac OS X Settings > Security & Privacy > Public Key Policies > Store the private and public key(s) only in the keychain

Description

Enable this group policy to store the auto-enrollment key(s) only in the keychain.

User certificate auto-enrollment always uses the Keychain and is not controlled by any Group Policy.

Note: 802.1X profiles installed through the "Mac OSX Settings -> 802.1X Settings" Group Policies will no longer be signed if this GP is enabled before profiles are installed.

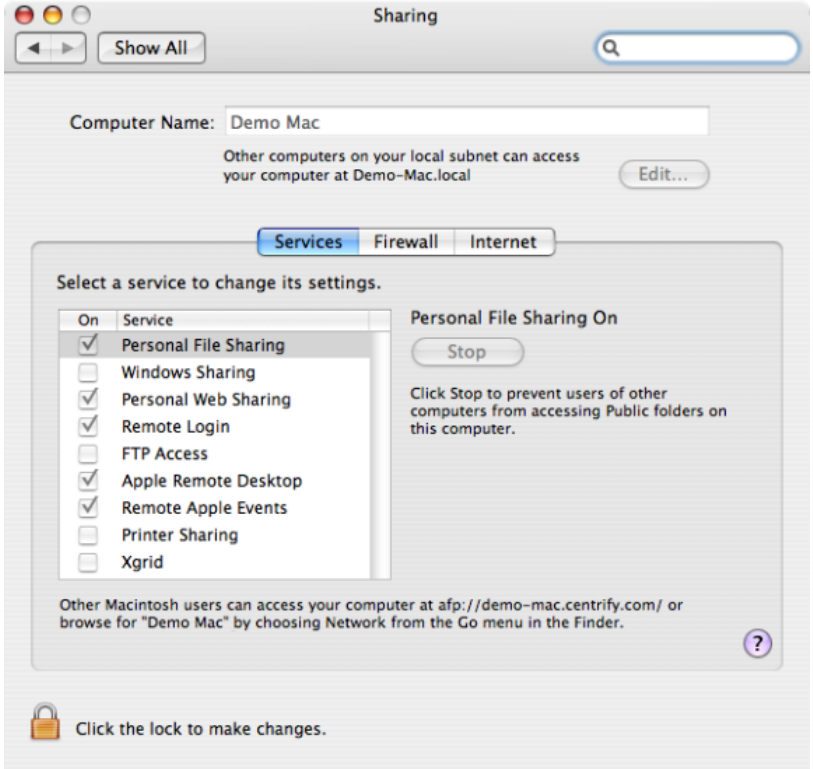
Services

Path

Computer Configuration > Policies > Centrify Settings > Mac OS X Settings > Services

Description

Use the **Computer Configuration > Policies > Centrify Settings > Mac OS X Settings > Services** settings to manage access to the service options from the Sharing ( ) system preference on Mac computers. These group policies correspond to the options displayed on the Services pane. For example:



Enable Personal File Sharing

Path

Computer Configuration > Policies > Centrify Settings > Mac OS X Settings > Services > Enable Personal File Sharing

Description

Allow users on other Mac computers access to `Public` folders on the local computer. If you enable this group policy, all users can access files in the `Public` folder through the Apple File Sharing protocol. Users with appropriate permission can also access other folders on the local computer if properly authenticated.

Enabling this group policy is the same as opening the Sharing system preference, selecting **File Sharing**, then clicking the **Options** button and selecting the **Share Files and Folders using AFP** option.

On Mac OS X Servers, enabling this policy has no effect.

This policy can take effect dynamically at the next group policy refresh interval without rebooting the computer.

Enable Windows Sharing

Path

Computer Configuration > Policies > Centrify Settings > Mac OS X Settings > Services > Enable Windows Sharing

Description

Allow users on Windows computers access to shared folders on the local computer through SMB/CIFS file shares.

Enabling this group policy is the same as opening the Sharing system preference, selecting **File Sharing**, then clicking the **Options** button and selecting the **Share Files and Folders using SMB** option.

On Mac OS X Servers, this policy has no effect.

This policy can take effect dynamically at the next group policy refresh interval without rebooting the computer.

Enable Personal Web Sharing

Path

Computer Configuration > Policies > Centrify Settings > Mac OS X Settings > Services > Enable Personal Web Sharing

Description

Allow users on other computers to view Web pages in each user's sites folder on the local computer.

Enabling this group policy is the same as opening the Sharing system preference and selecting the Web Sharing option.

On Mac OS X Servers, enabling this policy has no effect.

This policy can take effect dynamically at the next group policy refresh interval without rebooting the computer.

Enable Remote Login

Path

Computer Configuration > Policies > Centrify Settings > Mac OS X Settings > Services > Enable Remote Login

Description

Allow users on other computers to access this computer using SSH.

Enabling this group policy is the same as opening the Sharing system preference and selecting the Remote Login option.

This policy can take effect dynamically at the next group policy refresh interval without rebooting the computer.

Enable FTP Access (deprecated)

Path

Computer Configuration > Policies > Centrify Settings > Mac OS X Settings > Services > Enable FTP Access

Description

Allow users on other computers to exchange files with this computer using FTP applications.

Enabling this group policy is the same as opening the Sharing system preference, selecting **File Sharing**, then clicking the **Options** button and selecting the **Share Files and Folders using FTP** option.

On Mac OS X Servers enabling this policy has no effect.

This policy can take effect dynamically at the next group policy refresh interval without rebooting the computer.

Enable Apple Remote Desktop

Path

Computer Configuration > Policies > Centrify Settings > Mac OS X Settings > Services > Enable Apple Remote Desktop

Description

Allow others to access this computer using the Apple Remote Desktop program.

Enabling this group policy is the same as opening the Sharing system preference and selecting the Remote Management option.

If you enable this group policy, you can set the following access privileges:

- Allow guest users to request permission to control the screen
- Prevent VNC viewers from controlling the screen.

Because allowing VNC viewers to control the screen requires setting a password to take control of the screen and this behavior presents a potential security issue, this group policy can only be used to disallow VNC access.

This policy can take effect dynamically at the next group policy refresh interval without rebooting the computer.

Enable Remote Apple Events

Path

Computer Configuration > Policies > Centrify Settings > Mac OS X Settings > Services > Enable Remote Apple Events

Description

Allow applications on other Mac computers to send Apple Events to the local computer.

Enabling this group policy is the same as opening the Sharing system preference and selecting the Remote Apple Events option.

This policy can take effect dynamically at the next group policy refresh interval without rebooting the computer.

Enable Printer Sharing

Path

Computer Configuration > Policies > Centrify Settings > Mac OS X Settings > Services > Enable Printer Sharing

Description

Allow other people to use printers connected to the local computer.

Enabling this group policy is the same as opening the Sharing system preference and selecting the Printer Sharing option.

On Mac OS X Servers, enabling this policy has no effect.

This policy can take effect dynamically at the next group policy refresh interval without rebooting the computer.

Enable Xgrid

Path

Computer Configuration > Policies > Centrify Settings > Mac OS X Settings > Services > Enable Xgrid

Description

Allow clustered Mac OS Xgrid controllers to distribute tasks to the local computer for completion.

Enabling this group policy is the same as opening the Sharing system preference and selecting the Xgrid Sharing option.

On Mac OS X Servers enabling this policy has no effect.

This policy can take effect dynamically at the next group policy refresh interval without rebooting the computer.

Software Update Settings

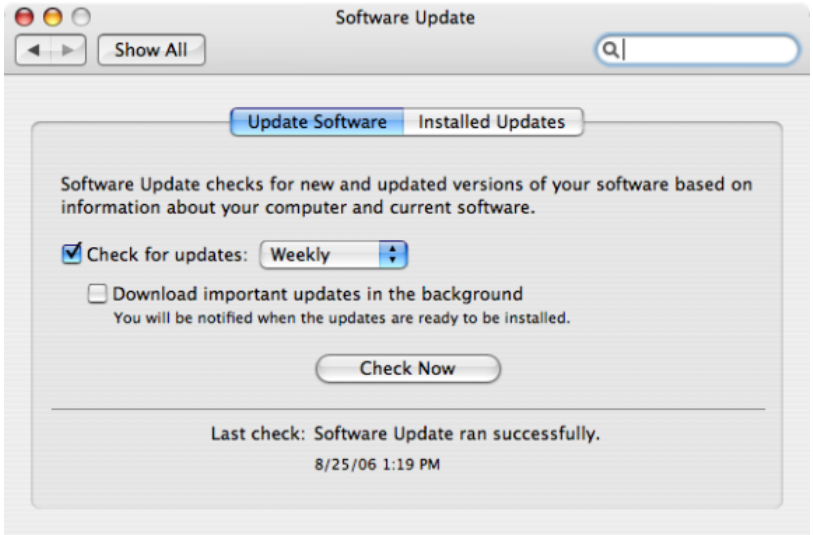
Path

Computer Configuration > Policies > Centrify Settings > Mac OS X Settings > Software Update Settings

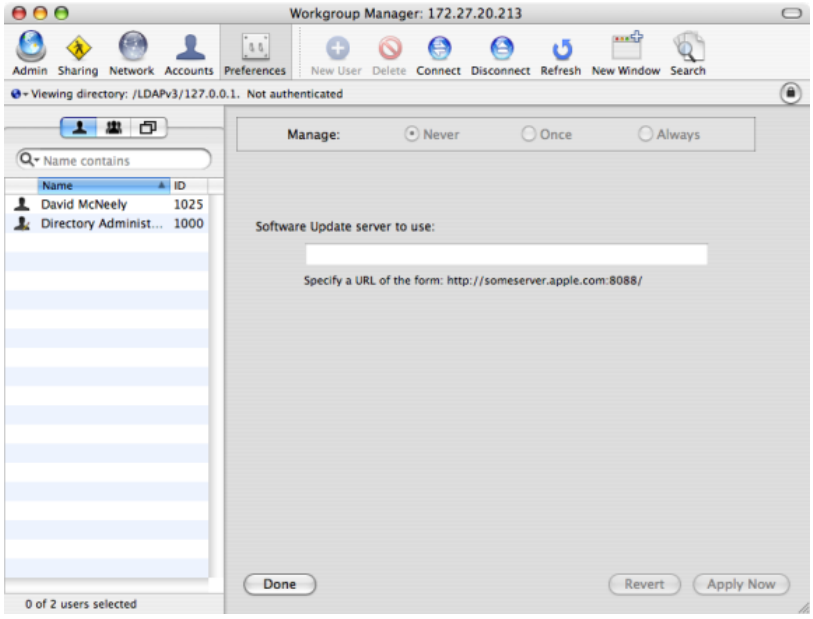
Description

Use the **Computer Configuration > Policies > Centrify Settings > Mac OS X Settings > Software Update Settings** group policies to manage software updates. The group policies in this category enable you to set the interval for checking for software updates and to identify a specific server from which updates should be received.

These group policies correspond to settings you make using the Software Update ( ) system preference on client Mac OS X computers and the Software Update preference in the Workgroup Manager on Mac OS X servers. For example, the interval for checking for software updates is typically configured Software Update system preference on client Mac computers:



Note: Identifying a software update server to use for downloading updates is configured on a Mac OS X server using the Software Update preference in the Workgroup Manager. For example:



The software update group policies are computer policies, applied as the root user, and apply to all users of the computer. Setting these group policies updates the plist files for individual users with the group policy parameters, such as update server URL, update interval, and so on. However, to prevent local users from using Software Update in System Preferences to manually set software update server parameters, an administrator should also limit access to the Software Update Preferences Pane by setting the group policy, **Limit Items Shown in System Preferences**, and then enabling the group policy, **Enable System Preferences Pane: System** > **Enable Software Update**.

Otherwise, you may see anomalous behavior. For example, a user can open Software Update and change parameters, such as disabling software updates (by deselecting Check for updates). If the user then re-enables software updates, the update server resets to the Apple software update server, not the server specified in the software update server group policy. However, at the next login, or at the next adgpupdate period, the Server URL and other group parameters will be re-applied.

The Software Update Settings contain separate folders that allow you to specify a different update server for each operating system version that you are running. For example, if you have computers with different versions of OS X in your environment, you can specify a different update server for each one by enabling the Specify software update server policy in each of the version-specific folders. In order to do this you must enable Use version specific settings.

If you do not enable Use version specific settings, Legacy Settings are used instead. If you applied Software Update Settings to computers running previous versions of the product, those settings are in Legacy Settings, though you may update them if you wish.

Note: The Automatically download and install software updates policy applies to all computers, regardless of version.

Automatically Check For Software Updates (Legacy, Currently Supported)

Path

Computer Configuration > Policies > Centrify Settings > Mac OS X Settings > Software Update Settings > Automatically check for software updates (Legacy, Currently supported)

Description

Note: There are actually separate versions of this policy in version-specific folders.

Periodically check for updated versions of the software installed on the local computer and automatically download and install newer versions. You can configure the version-specific versions of this policy the same way you can configure the Software Update system preference for the corresponding operating system version.

This policy takes effect when users log out and log back in.

Use Version Specific Settings

Path

Computer Configuration > Policies > Centrify Settings > Mac OS X Settings > Software Update Settings > Use version specific settings

Description

Enable the use of version-specific settings.

You can then set platform-specific preferences settings for each platform in your environment, which enables you to specify a different update server depending on the version of Mac OS X running on a computer. For example, if you have only 10.10 computers, you can enable this policy and then use Mac OS X 10.10 settings. If you have 10.10 and 10.9 computers, enable this policy, and then configure the version-specific policies as appropriate:

- Mac OS X 10.10 Settings
- Mac OS X 10.9 Settings

If this policy is disabled or not configured, Legacy Settings are used instead of version-specific settings. Likewise, Delinea versions prior to 4.4.2 always use Legacy Settings and ignore this policy setting.

If you configured Software Update Settings with a version of the product prior to 4.4.2, these settings are saved to Legacy Settings when you upgrade to the current Delinea version. You can keep or edit these settings as you wish.

Specify Software Update Server (Legacy, Currently Supported)

Path

Computer Configuration > Policies > Centrify Settings > Mac OS X Settings > Software Update Settings > Specify software update server (Legacy, Currently supported)

Description

Note: There are actually separate versions of this policy in version-specific folders.

This enables you to specify a separate update server based on the version of the Mac OS X computer.

Type the URL that identifies the computer you are using as the software update server. It is recommended that you specify the hostname of the server rather than the IP address; for example:

```
http://myHost.local:8088
```

In addition, to ensure that DNS associates the hostname of the update server with the IP address, add a line such as the following to the `/etc/hosts` file:

```
192.168.2.79 myHost.local
```

where: `192.168.2.79` is the IP address of the update server and `myHost.local` is the hostname.

This policy can take effect dynamically at the next group policy refresh interval.

Setting User-Based Group Policies

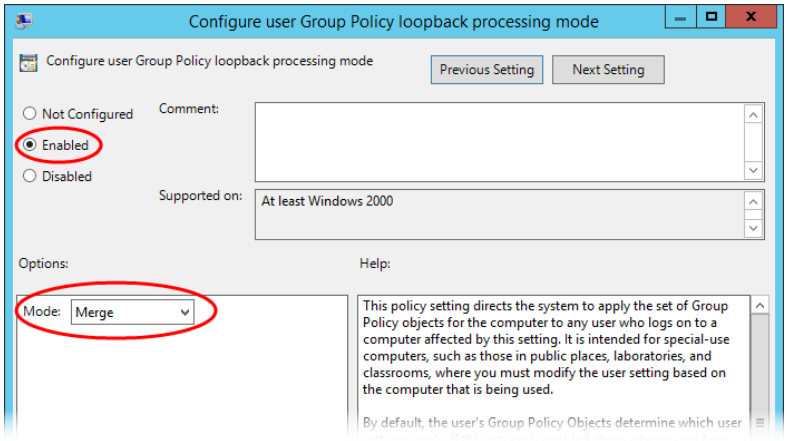
Centrify group policies allow administrators to extend the configuration management capabilities of Windows Group Policy Objects to managed Mac computers and to users who log on to Mac computers. This chapter describes the Mac group policies that can be applied to Mac users

The user-based group policies are defined in the Centrify Mac administrative template (`centrify_mac_settings.xml`) and accessed from **User Configuration > Policies > Centrify Settings > Mac OS X Settings**.

Group policies are only applied to users and computers in the GPO's linked OU and any child OUs. If your users and computers are in different OUs (which is common), Delinea recommends using user Group Policy loopback processing to make sure user policies are applied to everyone who logs on to a Mac. This is a standard Microsoft Group Policy that applies to every user to the computer.

To implement user Group Policy loopback processing mode

1. In the Group Policy Management Editor, navigate to **Computer Configuration > Administrative Templates > System > Group Policy > Configure user Group Policy loopback processing mode**.
2. Enable the policy, set **Mode:** to **Merge**, then click **OK**.



See https://technet.microsoft.com/en-us/library/cc978513.aspx for more information about loopback processing.

See Understanding Group Policies for Mac Users and Computers for general information about how to use group policies to manage Mac settings and for information on how to install the group policy administrative templates.

Note: For additional information about creating and using group policies and Group Policy Objects, see your Windows or Active Directory documentation. For more information about adding and using other Centrify group policies that are not specific to Mac computers and users, see the *Group Policy Guide*.

Setting User-Based Policies

This section describes user-based policies for Mac that you can set. The following table provides a summary of the group policies you can set for Mac users. These group policies are in the Centrify Mac administrative template (`centrify_mac_settings.xml`) and accessed from **User Configuration > Policies > Centrify Settings > Mac OS X Settings**.

Note: Group policies are only applied to users and computers in the GPO's linked OU and any child OUs. Enable **Computer Configuration > Administrative Templates > System > Group Policy > Configure user Group Policy loopback processing mode** in Merge mode to make sure user policies are applied to everyone who logs on to a Mac.

Use this policy	To do this
802.1X Wireless Settings	Create user profiles for wireless authentication. This group policy corresponds to 802.1X Options in the **Networks** system preference.
Application Access Settings (deprecated)	Control the specific applications users are either permitted to use or prohibited from using. These group policies correspond to **Applications** preferences set in the Workgroup Manager.
Desktop Settings	Control the desktop and screen saver options for users on Mac computers. These group policies correspond to settings in the **Desktop & Screen Saver** system preference.
Dock Settings	Control the look and operation of the Dock displayed on the user's desktop. These group policies correspond to **Dock** preferences set in the Workgroup Manager.
Finder Settings	Specify whether to use the standard Finder, or the Simple Finder, which restricts users to applications and folders in the Dock.
Folder Redirection	Redirect specified network home folders to the local computer to improve performance.
Import Settings	Specify plist files to import preferences from another computer. This group policy corresponds to the import plist functionality in Workgroup Manager.
Login Settings	Specify frequently used applications, folders, and server connections to open when a user logs in. This group policy corresponds to the login functionality in Workgroup Manager.
Media Access Settings	Control the specific media types users are either permitted to use or prohibited from using. These group policies correspond to **Media Access** preferences set in the Workgroup Manager.
Mobility Settings	Control the synchronization rules applied for users access services from mobile devices. These group policies correspond to **Mobility** preferences set in the Workgroup Manager.
Scripts (Login/Logout)	Specify login and logout scripts that run when Active Directory users log on or log out.

Security & Privacy Settings	Control the secure login options for users on Mac computers. These group policies correspond to settings in the **Security** system preference.
System Preference Settings	Control the specific system preferences displayed for users. These group policies correspond to **System Preferences** set in the Workgroup Manager.

802.1X Wireless Settings

Path

User Configuration > Policies > Centrify Settings > Mac OS X Settings > 802.1X Wireless Settings

Description

Use the **User Configuration > Policies > Centrify Settings > Mac OS X Settings > 802.1X** settings to create profiles for wireless network authentication. The profiles you specify with these group policies are created in the Network system preferences pane.

Specify User Profiles (Deprecated)

Path

User Configuration > Policies > Centrify Settings > Mac OS X Settings > 802.1X Wireless Settings > Specify User Profiles (Deprecated)

Description

Enable this policy to specify 802.1X User Profiles for wireless network authentication.

When using a user profile, a user will be prompted for username and password to authenticate to a wireless network after login.

To add a user profile

1. Enable the policy and click **Add** to enter the profile name and setting.
2. Type a name for the profile.
3. Type the setting using the following format:
   - `Network;Security Type;Authentication Method`, where each field is separated by a semi-colon `;`.
   - Network is the wireless network name
   - Security type is one of `802.1X WEP, WPAEnterprise, WPA2 Enterprise`
   - Authentication method is one or more of the following, separated by commas: `TTLS, PEAP, TLS, EAP-FAST, LEAP, MD5`

For example:

```
OFFICE1;WPA Enterprise;PEAP
OFFICE2;802.1X WEP;TTLS,PEAP
```

Set the **Automatically turn on Airport** option to automatically turn on AirPort device if this type of profile is specified. Otherwise, the status of the AirPort device will not change.

Once enabled, this policy takes effect dynamically at the next group policy refresh interval.

Application Access Settings (deprecated)

Path

User Configuration > Policies > Centrify Settings > Mac OS X Settings > Application Access Settings

Description

Use the **User Configuration > Policies > Centrify Settings > Mac OS X Settings > Application Access Settings** group policies to manage the applications Mac users are allowed to open or prevented from opening.

These group policies correspond to settings you can make using the Applications preference in the Workgroup Manager.

Permit/Prohibit Access to Application List: Applescript (Deprecated)

Path

User Configuration > Policies > Centrify Settings > Mac OS X Settings > Application Access Settings > Permit/prohibit access to application list: AppleScript

Description

Select the specific applications in the Finder's Applications/AppleScript folder that users are permitted to use if you selected **Users can only open these applications**, or not allowed to use if you selected **Users can open all applications except these**.

This policy is only effective if the **Permit/prohibit access to applications** group policy is enabled. If the **Permit/prohibit access to applications** group policy is not configured or disabled, this group policy is ignored.

Once enabled, this group policy takes effect dynamically at the next group policy refresh interval.

Permit/Prohibit Access to Application List: Applications (Deprecated)

Path

User Configuration > Policies > Centrify Settings > Mac OS X Settings > Application Access Settings > Permit/prohibit access to application list: Applications

Description

Select the specific applications in the Finder's Applications folder that users are permitted to use if you selected **Users can only open these applications**, or not allowed to use if you selected **Users can open all applications except these**.

This policy is only effective if the **Permit/prohibit access to applications** group policy is enabled. If the **Permit/prohibit access to applications** group policy is not configured or disabled, this group policy is ignored.

Once enabled, this group policy takes effect dynamically at the next group policy refresh interval.

Permit/Prohibit Access to Application List: Server (Deprecated)

Path

User Configuration > Policies > Centrify Settings > Mac OS X Settings > Application Access Settings > Permit/prohibit access to application list: Server

Description

Select the specific applications in the Finder's Applications/Server folder that users are permitted to use if you selected **Users can only open these applications**, or not allowed to use if you selected **Users can open all applications except these**.

This policy is only effective if the **Permit/prohibit access to applications** group policy is enabled. If the **Permit/prohibit access to applications** group policy is not configured or disabled, this group policy is ignored. In addition, this policy is only applicable for Mac OS X Server computers.

Once enabled, this group policy takes effect dynamically at the next group policy refresh interval.

Permit/Prohibit Access to Application List: Utilities (Deprecated)

Path

User Configuration > Policies > Centrify Settings > Mac OS X Settings > Application Access Settings > Permit/prohibit access to application list: Utilities

Description

Select the specific applications in the Finder's Applications/Utilities folder that users are permitted to use if you selected **Users can only open these applications**, or not allowed to use if you selected **Users can open all applications except these**.

This policy is only effective if the **Permit/prohibit access to applications** group policy is enabled. If the **Permit/prohibit access to applications** group policy is not configured or disabled, this group policy is ignored.

Once enabled, this group policy takes effect dynamically at the next group policy refresh interval.

Permit/Prohibit Access to Applications (Deprecated)

Path

User Configuration > Policies > Centrify Settings > Mac OS X Settings > Application Access Settings > Permit/prohibit access to applications

Description

Allow other policies to specify the applications that users are permitted to access or prohibited from accessing. You must enable this policy for any other application access group policies to take effect. Once enabled, only the applications explicitly specified in Application List policies are permitted or prohibited.

If you enable this policy, in **Access mode**, select one of the following:

- **Users can only open these applications** to grant access only to the applications you select with the other application access policies.

  Note: If you select the option, **User can also open all applications on local volumes**, users can access any local applications. Restrictions only apply to applications on CDs, DVDs, or external disks.

- **Users can open all applications except these** to prevent access only to the applications you select with the other application access policies.

You can also set the following options in this group policy:

- Select **User can also open all applications on local volumes** to allow access to applications on a computer's local hard drive.

  If selected, users can access any local applications in addition to the applications explicitly approved using the other application access policies. If you uncheck this option, users can only access applications on CDs, DVDs, or external disks that have been explicitly approved.
- Select **Allow approved applications to launch non-approved applications** to allow approved applications to open applications that aren't explicitly approved.

  For example, if users click a link in an email message, this option allows the email application to open a browser to display the Web page even if the browser is not listed as an approved application. To prevent approved applications from opening applications that aren't explicitly approved, uncheck this option.
- Select **Allow UNIX tools to run** to allow applications or the operating system to run tools, such as the QuickTime Image Converter, without explicitly listing them as approved applications.

  These tools usually operate in the background, but can be run from the command line. If you want to prevent access to these tools, do not check this option.

Once enabled, this group policy takes effect dynamically at the next group policy refresh interval.

Permit/Prohibit Access to the User-Specific Applications (Deprecated)

Path

User Configuration > Policies > Centrify Settings > Mac OS X Settings > Application Access Settings > Permit/prohibit access to the user-specific applications

Description

Define a list of additional applications that users are permitted to run if you selected **Users can only open these applications**, or not allowed to use if you selected **Users can open all applications except these**. If enabled, you must specify the CFBundleIdentifier to identify the application; for example, for the Firefox browser, the `CFBundleIdentifier` is: `org.mozilla.firefox`. To find the `CFBundleIdentifier` complete the following steps:

1. In the Finder, locate the application to control.
2. Control-click or right-click the application, then select **Show Package Contents**.
3. If necessary, expand the **Contents** folder, then open `info.plist` with a text editor.
4. Find the string: CFBundleIdentifier.

   On the next line is the application's `CFBundleIdentifier`; for example:

   `org.mozilla.firefox`
5. Use `org.mozilla.firefox` to identify the Firefox browser.

To add an application to the list, select **Enabled**, then click **Add** and enter the `CFBundleIdentifier` and click **OK**.

You may also control access to system preference panes by using the `CFBundleIdentifier`. You can find the `CFBundleIdentifier` for system preference panes in `/System/Library/PreferencePanes`. You can specify any application object that has a `CFBundleIdentifier` in its info.plist file.

> **Note:** Some applications may not have a `CFBundleIdentifier` (when you right-click the application name, there is no **Show Package Contents** menu item). In this case, you cannot add the application to the list of permitted or prohibited applications.

This policy is only effective if the **Permit/prohibit access to applications** group policy is enabled. If the **Permit/prohibit access to applications** group policy is not configured or disabled, this group policy is ignored.

Once enabled, this group policy takes effect when users log out and log back in.

Automount Settings

Path

User Configuration > Policies > Centrify Settings > Mac OS X Settings > Automount Settings

Description

Use the Automount Settings to automatically mount network shares and the user's Windows home directory when a user logs in.

Automount Network Shares

Path

User Configuration > Policies > Centrify Settings > Mac OS X Settings > Automount Settings > Automount network shares

Description

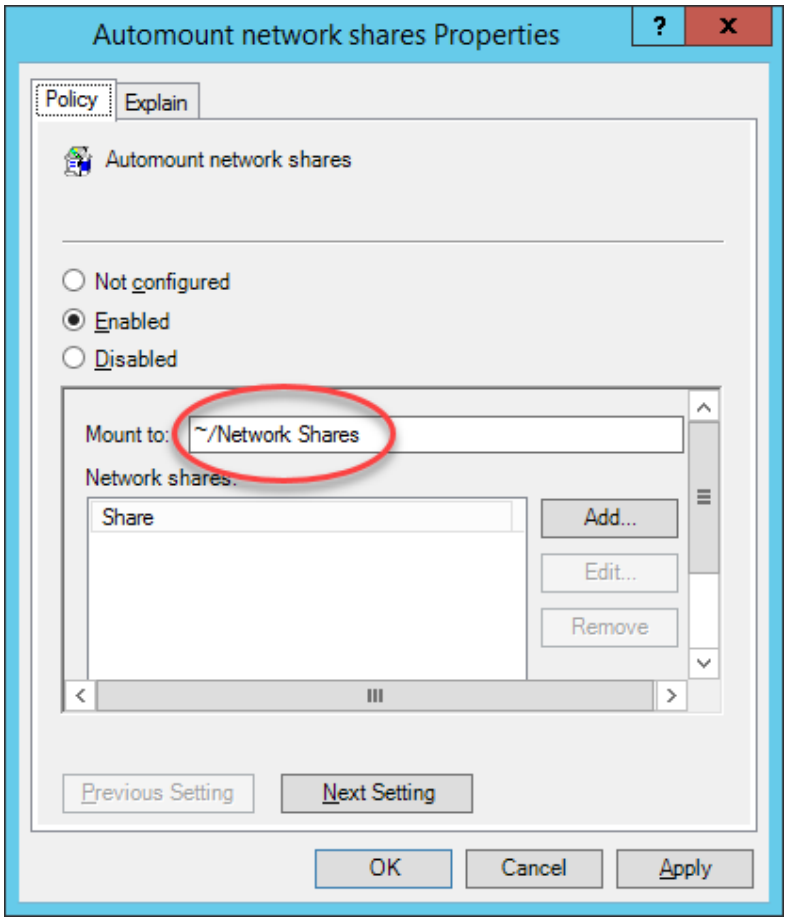
Specify the network shares to automatically mount when a user logs in. The default network share mount location is *User_Home*/Network Share.

This policy supports SMB, AFP, and NFS shares.

To add a share

1. Enter a path to mount the share in the **Mount to:** field.

   The path should start with `/` or `~`. The default value is `~/Network Shares`. In this case, network share folders would be mounted under the directory `Network Shares` of user's home directory.



2. Click **Enabled**, then click **Add** and enter the share in one of the following formats:
3. `keyword://server/share`

   where:

   - `keyword` is one of `smb`, `nfs`, `afp`
   - `server` is the name or IP address of the server and can include a user or user and password in the form: `user:@server` or `user:password@server`.
   - `share` can include spaces and be followed by a subdirectory.

   For example, the following are all valid share specifications:

   `smb://acme.com/MacUsers`

   `smb://acme.com/Mac Users`

   `smb://acme.com/MacUsers/Shared_resources`

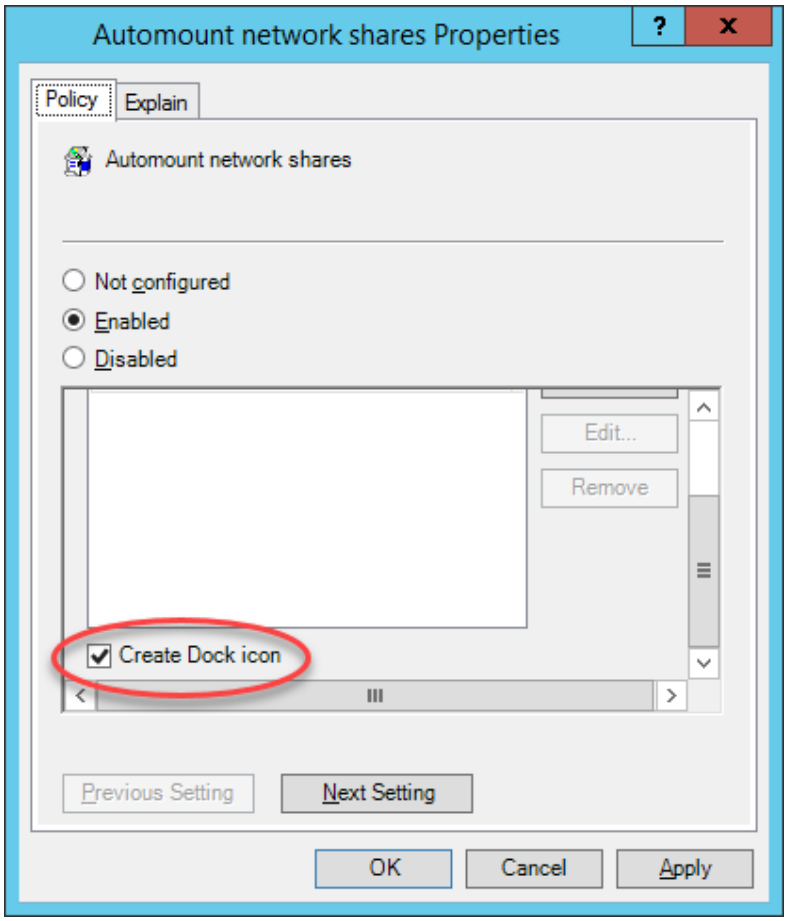
   `smb://jsmith:pass1234@acme.com/MacUsers`

   `afp://acme.com/Users_server`

   `nfs://acme.com/MacUsers`

```
nfs://192.168.0.1/MacUsers
```

4. (Optional) Select **Create Dock icon** to create a link to the network share in the user's Dock.



Once enabled, this policy takes effect when a user logs out and back in to a computer.

Automount User's Windows Home

Path

User Configuration > Policies > Centrify Settings > Mac OS X Settings > Automount Settings > Automount user's Windows home

Description

Automatically mount the user's Windows home directory when the user logs in.

Specify the Windows home directory by using the Profile tab for a user in Active Directory Users and Computers (ADUC).

Once enabled, this policy takes effect when a user logs out and back in to a computer.

Create Alias Instead of Symbolic Link

Path

User Configuration > Policies > Centrify Settings > Mac OS X Settings > Automount Settings > Create alias instead of symbolic link

Description

This group policy is provided for compatibility with Delinea releases earlier than 2015. If you are using release 2015 or later, do not use this group policy.

In releases prior to 2015, the default mount point for network shares was `/var/centrify/mnt/user`. Starting with release 2015, the default mount point for network shares is `User_Home/Network Share`.

In Delinea releases prior to 2015, the "Automount network shares" group policy creates symbolic links to the specified shared network directories. However, certain versions of Microsoft Office are unable to save files to a shared folder by using the symbolic link (the link is greyed-out). The "Create alias instead of symbolic link" group policy corrects the problem by creating an alias instead of a symbolic link. In release 2015 or later, because of the new mount location, symbolic links are not required, and this group policy has no effect.

If you enable this group policy, the alias points to network shares that are automatically mounted when a user logs in.

> **Note:** The operating system treats an alias as a file, which means that you cannot use the Terminal program to access files or folders that are pointed to by the alias.

Once enabled, this policy takes effect when a user logs out and back in to a computer.

Custom Settings

Path

User Configuration > Policies > Centrify Settings > Mac OS X Settings > Custom Settings

Description

Use the **User Configuration > Policies > Centrify Settings > Mac OS X Settings > Custom Settings > Install MobileConfig Profiles** group policy to install mobile configuration profiles. This policy installs a user profile. To install a device profile, use the same policy in **Computer Configuration > Centrify Settings > Mac OS X Settings > Custom Settings.**

Install MobileConfig Profiles

Path

User Configuration > Policies > Centrify Settings > Mac OS X Settings > Custom Settings > Install MobileConfig profiles

Description

Enable this group policy to install mobile configuration profiles on managed Mac computers.

> **Note:** There is a Computer Configuration version of this policy (which installs device profiles) and a User Configuration version (which installs user profiles).

> **Note:** This group policy only supports macOS 10.15 and lower.

Before enabling this policy, you must create a directory and copy mobile configuration files to `SYSVOL` on the domain controller. `SYSVOL` is a well-known shared directory on the domain computer that stores server copies of public files that must be shared throughout the domain.

Specifically, create the following directory on the domain controller:
`\\domainName\SYSVOL\domainName\mobileconfig`

and copy one or more mobile configuration profile files to this directory. See Deploy Configuration Profiles to Multiple Computers for details on how to do this.

To specify mobile configuration files to install, enable the policy, then click **Add**. Enter the name of a mobile configuration file that you placed in `SYSVOL` on the domain controller. Include the `.mobileconfig` suffix with the name.

If you specify a file that is not in the SYSVOL mobileconfig directory, the profile will not be installed.

If you add new files to the existing list in the group policy, those profiles will be installed – existing profiles will not be touched. If you remove previously specified files, the profiles defined by these files will be uninstalled.

If you add two or more profile files that have the same `payloadIdentifier`, only one of them will be installed.

If you change the group policy to “Disabled” or “Not Configured”, all existing profiles that were installed previously by the group policy will now be uninstalled from the managed Mac computers.

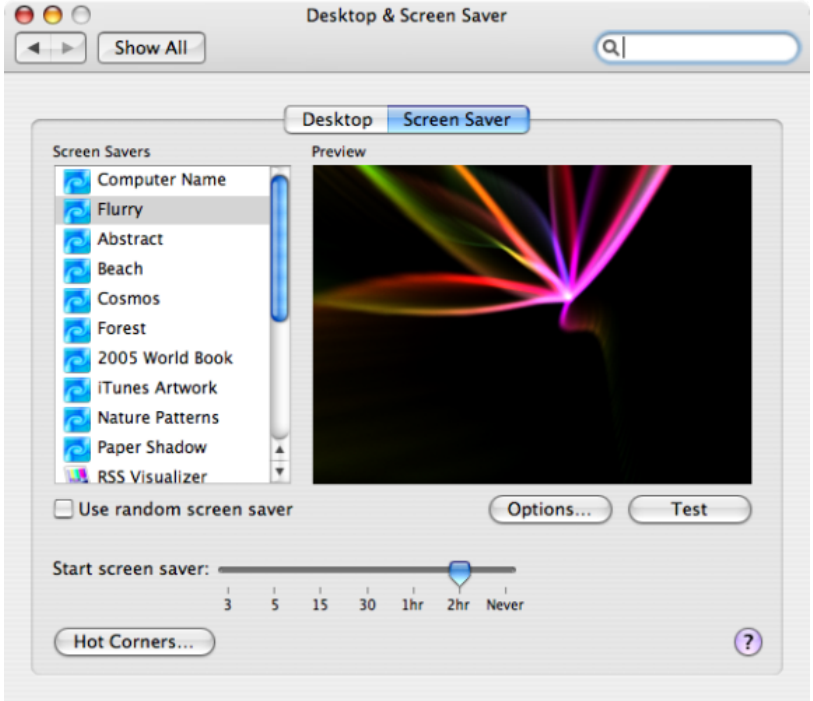
Desktop Settings

Path

User Configuration > Policies > Centrify Settings > Mac OS X Settings > Desktop Settings

Description

Use the **User Configuration > Policies > Centrify Settings > Mac OS X Settings > Desktop Settings** group policy to manage the start time for the screen saver from the Desktop & Screen Saver () system preference on Mac computers. This group policy corresponds to the **Start screen saver** option displayed on the Screen Saver pane. For example:



Set Computer Idle Time for Starting Screen Saver

Path

User Configuration > Policies > Centrify Settings > Mac OS X Settings > Desktop Settings > Set computer idle time for starting screen saver

Description

Select the length of time to wait before starting the screen saver. If you enable this group policy, you can specify the number of minutes to wait while a computer is not in use before starting the screen saver. For example, if you want the screen saver to start after a computer has been idle for 10 minutes, you can set Start screen saver to 10 minutes.

Disabling this policy does *not* disable the screen saver. To disable the screen saver, enable this policy and set the value to 0.

Although you may specify values greater than 60 minutes, and the screen saver works appropriately, the Macintosh Screen Saver dialog box shows values that are greater than 60 as **Never**.

Enabling this group policy is the same as selecting when to start the screen saver using the **Start screen saver** slider in the Desktop & Screen Saver system preference.

Once enabled, this group policy takes effect when users log out and log back in.

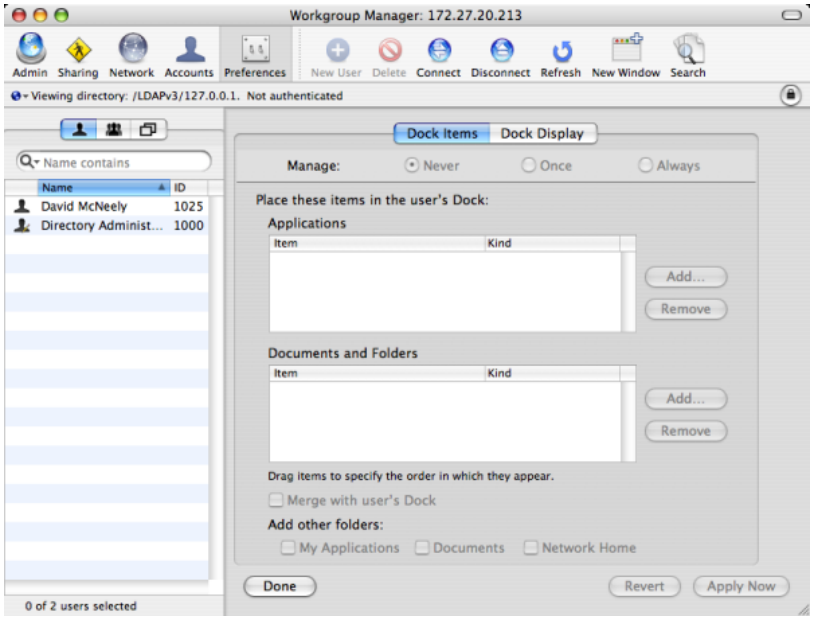
Dock Settings

Path

User Configuration > Policies > Centrify Settings > Mac OS X Settings > Dock Settings

Description

Use the **User Configuration > Policies > Centrify Settings > Mac OS X Settings > Dock Settings** group policies to manage the characteristics of the Dock for Mac users. These settings correspond to the Dock preferences you can manage using the Workgroup Manager. In the Workgroup Manager, the Dock Items pane controls the items placed in the Dock and whether the workgroup Dock is merged with the user's Dock, and the Dock Display pane controls attributes such as the Dock size, magnification, position, and animation. For example:



Add Other Folders to the Dock

Path

User Configuration > Policies > Centrify Settings > Mac OS X Settings > Dock Settings > Add other folders to the Dock

Description

Add icons for the other commonly-used folders to the Dock. You can choose to add the following folder icons to the Dock:

- My Applications
- Documents

The **My Applications** folder contains aliases to all approved applications you have defined in the Application list. If you do not manage access to applications, all available applications are included in the My Applications folder. If you enable Simple Finder, you should display the My Applications folder.

The **Documents** folder is the Documents folder found in the user's home folder. For example, the `/Users/username/Documents` folder for local user accounts.

Once enabled, this group policy takes effect when users log out and log back in.

Adjust the Dock's Icon Size

Path

User Configuration > Policies > Centrify Settings > Mac OS X Settings > Dock Settings > Adjust the Dock's icon size

Description

Set the approximate size of Dock icons in pixels. The valid settings for the Dock size range from 16 pixels (small) to 128 pixels (large). The default size is 80 pixels.

> **Note:** This setting is approximate because the actual size of Dock icons depends on screen resolution and the number of icons in the Dock.

Once enabled, this group policy takes effect when users log out and log back in.

Adjust the Dock's Magnified Icon Size

Path

User Configuration > Policies > Centrify Settings > Mac OS X Settings > Dock Settings > Adjust the Dock's magnified icon size

Description

Set the level of magnification to use for items in the Dock. If you enable this group policy, icons in the Dock are magnified to display in a larger size as the pointer moves over them. The valid settings for Dock magnification range from 16 pixels for minimum magnification to 128 pixels for maximum magnification. The default size is 80 pixels.

If you do not configure or disable this group policy, icons in the Dock are not magnified when the pointer moves over them.

Once enabled, this group policy takes effect when users log out and log back in.

Adjust the Dock's Position on Screen

Path

User Configuration > Policies > Centrify Settings > Mac OS X Settings > Dock Settings > Adjust the Dock's position on screen

Description

Specify the location for displaying the Dock on the screen. If you enable this group policy, you can position the Dock on the left, bottom, or right of the screen. The default location for displaying the Dock is at the bottom of the screen.

Once enabled, this group policy takes effect when users log out and log back in.

Adjust The Effect Shown When Minimizing the Dock

Path

User Configuration > Policies > Centrify Settings > Mac OS X Settings > Dock Settings > Adjust the effect shown when minimizing the Dock

Description

Specify the effect to use when a window or application is minimized and placed in the Dock. The valid effects are:

- Genie
- Scale

- Suck

Once enabled, this group policy takes effect when users log out and log back in.

Animate Opening Applications

Path

User Configuration > Policies > Centrify Settings > Mac OS X Settings > Dock Settings > Animate opening applications

Description

Animate application icons so that the icon displayed in the Dock bounces when the user opens the application.

Once enabled, this group policy takes effect when users log out and log back in.

Automatically Hide and Show the Dock

Path

User Configuration > Policies > Centrify Settings > Mac OS X Settings > Dock Settings > Automatically hide and show the Dock

Description

Hide the Dock from view automatically. If you enable this policy, the Dock is hidden during normal operation. The Dock is then automatically displayed again if the pointer moves over the position on the screen where the Dock is located.

Once enabled, this group policy takes effect when users log out and log back in.

Lock the Dock

Path

User Configuration > Policies > Centrify Settings > Mac OS X Settings > Dock Settings > Lock the Dock

Description

Lock the applications displayed in the Dock. If you enable this policy, icons cannot be moved into or out of the Dock.

Once enabled, this group policy takes effect when users log out and log back in.

Place Applications in Dock

Path

User Configuration > Policies > Centrify Settings > Mac OS X Settings > Dock Settings > Place applications in Dock

Description

List the applications to include in the Dock. After you enable this policy, click **Add** to enter the path to the application you want included in the Dock. Then click **OK**. You can click **Add** again to add additional applications. For example, to add Firefox and Chess icons to the Dock, type the application paths:

```
/Applications/Firefox.app
```

Click **OK**. Then click **Add** and enter:

```
/Applications/Chess.app
```

The icons for the applications you specify are placed to the left or above the separator line in the Dock in the order you enter them, up to 10 items. if you add more than 10 the order may be random. If the path to an application is incorrect, a question mark (?) is displayed in the Dock in place of the application's icon.

This group policy does not sort icons from the initial system list. To sort these items, such as the Mail application icon, you can add the item to the list.

Once enabled, this group policy takes effect when users log out and log back in.

Place Documents and Folders in Dock

Path

User Configuration > Policies > Centrify Settings > Mac OS X Settings > Dock Settings > Place documents and folders in Dock

Description

List the documents or folders to include in the Dock. After you enable this policy, click **Add** to enter the path to the folder or document you want to include in the Dock. Then click **OK**. You can specify additional folders or documents by clicking **Add** again. For example, to add the `Users` folder and the `Copyright.txt` document to the Dock, type the paths to each:

```
/Users
```

Click **OK**, then click Add and type:

```
/Documents/Copyright.txt
```

The icons for the items you specify are placed to the left or above the separator line in the Dock. Items are sorted in the order you enter them up to 10 items. If you specify more than 10 items the order may be random. If the path to an item is incorrect, a question mark (?) is displayed in the Dock.

> **Note:** You may not specify the path to a network share; for example, `smb://serverName`. Network share paths are implemented as aliases, which work differently than folder and document paths. If you specify a network share, a question mark (?) is displayed in the Dock.

Once enabled, this group policy takes effect when users log out and log back in.

Merge with User's Dock

Path

User Configuration > Policies > Centrify Settings > Mac OS X Settings > Dock Settings > Merge with user's Dock

Description

Merge the Workgroup Dock settings with the user's Dock.

Once enabled, this group policy takes effect when users log out and log back in.

Finder Settings

Path

User Configuration > Policies > Centrify Settings > Mac OS X Settings > Finder Settings

Description

Use the **User Configuration> Policies > Centrify Settings > Mac OS X Settings > Finder Settings** group policies to configure Finder commands, preferences and views.

The **Configure Finder Commands (Deprecated)** policy, below, allows you to control which commands are available in the Apple menu and Finder menus for users.

The **Configure Finder Preferences (Deprecated)** policy, below, enables you to specify the type of Finder for the user environment. After enabling the policy, you can choose one of two types from the drop-down list:

- **Normal Finder** applies the standard Mac desktop. This is the default value, and is the environment that all users will have if the policy is not enabled.
- **Simple Finder** restricts users to applications that are in the Dock.

When Simple Finder is enabled, users cannot open applications, open, modify, or delete documents, or create folders in the Finder. They also cannot mount network drives. They can only use items that are in the Dock. Use the **Dock Settings** policies above to configure the Dock; for example, enable **Place Applications in Dock** and **Place Documents and Folders in Dock** to control the applications and folders that users can access.

The **Configure Finder Preferences (Deprecated)** policy, below, enables you to control the arrangement and appearance of items on the user's desktop, in Finder windows, and in the top-level folder of the computer.

Configure Finder Commands (Deprecated)

Path

User Configuration > Policies > Centrify Settings > Mac OS X Settings > Finder Settings > Configure Finder commands (Deprecated)

Description

Specify the commands in Finder menus and the Apple menu that are available to users. Select commands from the following list:

- **Connect to Server**

  Select to allow users to connect to a remote server by choosing 'Connect to Server' in the Finder Go menu. Deselect to prevent users from accessing this command.

- **Go to iDisk**

  Select to allow users to connect to an iDisk by choosing 'Go to iDisk' in the Finder Go menu. Deselect to prevent users from accessing this command.

- **Eject**

  Select to allow users to eject discs (for example, CDs, DVDs, floppy disks, or FireWire drives). Deselect to prevent users from ejecting disks.

- **Burn Disc**

  Select to allow user on computers with relevant hardware to burn discs. Deselect to prevent users from burning disks.

- **Go to Folder**

Select to allow users to open a specific folder by choosing the 'Go to Folder' command in the Finder Go menu. Deselect to prevent users from using the 'Go to Folder' command.

- **Restart**

  Select to allow users to restart the computer they're using, or deselect to prevent them from restarting the computer.

- **Shut Down**

  Select to allow users to shut down the computer they're using, or deselect to prevent them from shutting down the computer.

Once enabled, this group policy takes effect when users log out and back in.

Configure Finder Preferences (Deprecated)

Path

User Configuration > Policies > Centrify Settings > Mac OS X Settings > Finder Settings > Configure Finder preferences (Deprecated)

Description

Configure Finder preferences, including whether to use normal or Simple Finder, which items to show on the desktop, how a new window behaves, and whether to show filename extensions and the Empty Trash warning.

Select from the following options:

- **Finder type**

  Select the normal Finder or Simple Finder as the user environment. The normal Finder looks and acts like the standard Mac desktop. Simple Finder removes the ability to use a Finder window to access applications or modify files, limiting users' access to only what is in the Dock. In addition, users can't mount network volumes, create folders, or delete files.

- **Show these items on the Desktop**

  Choose whether users see icons for local hard disks, external disks, CDs (DVDs and iPods), and connected servers on the desktop.

  If you hide them, icons for disks and servers still appear in the top-level folder when a user clicks the Computer icon in a Finder window's toolbar.

- **New Finder window shows**

  Select **Home** to show items in the user's home folder, or select **Computer** to show the top-level folder, which includes local disks and mounted volumes.

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

  Select this option to display folder contents in a separate window when a user opens a folder.

- **Always open windows in column view**

  Select this option to display folders in column view, which maintains a consistent view across windows.

- **Show warning before emptying the Trash**

Select this option to display the normal warning when a user empties the Trash, or deselect it if you don't want users to see this message.

- **Always show file extensions**

  Select this option to show filename extensions (such as `.txt` or `.jpg`) that identify the file type; or deselect it to hide filename extensions.

  Once enabled, this group policy takes effect when users log out and back in.

- **Configure Finder views**

  Enable this group policy to control Finder views, for example the arrangement and appearance of items on a user's desktop, in Finder windows, and in the top-level folder of the computer.

The options in **Desktop View** allow you to adjust the size and arrangement of icons on the desktop.

Use **Icon Size** to adjust the icon size.

Use **Icon Arrangement** to specify how to arrange icons:

- To keep items aligned in rows and columns, select **Snap to grid**.
- To arrange items by criteria such as name or type (for example, all folders grouped together), select **Keep arranged by**.

Items in Finder windows are viewed in a list or as icons and you can control aspects of how these items look.

Default View settings control the overall appearance of all Finder windows. **Computer View** settings control the view for the top-level computer folder, showing hard disks and disk partitions, external hard drives, mounted volumes, and removable media (such as CDs or DVDs).

In **Icon View**, use **Icon Size** to adjust the size of icons.

Use **Icon Arrangement** to specify how to arrange icons:

- To keep items aligned in rows and columns, select **Snap to grid**.
- To arrange items by criteria such as name or type (for example, all folders grouped together), select **Keep arranged by**.

In **List View**, set the following:

- Select **relative dates** to show an item's creation or modification date relative to today, rather than as a fixed date; for example, `Today` or `Yesterday`, instead of `3/24/10`.
- Select **Calculate folder sizes** to calculate the total size of each folder shown in a Finder window, which can take a lot of time depending on the size of the folder.

In **Icon Size**, select **small** or **big** for the size of icons in list view.

Once enabled, this group policy takes effect when users log out and back in.

Folder Redirection

Path

User Configuration > Policies > Centrify Settings > Mac OS X Settings > Folder Redirection

Description

Use the **User Configuration > Policies > Centrify Settings > Mac OS X Settings > Folder Redirection** group policies to redirect specified folders from a network home directory to the local computer.

When you set up a network home directory, all home directory files are written to the network share. Some folders, such as `/Library/Caches`, get heavy I/O from Apple and third-party applications, which may cause performance issues. The folder redirection policies enable you to redirect specific folders, such as `/Library/Caches`, to the local computers, which can result in dramatic performance improvements.

Folder Redirection contains two folders with identical sets of four policies:

- **Folder redirection actions at login time** applies the specified policy when the user logs in. For example, at login delete a folder in the network home directory and create a symbolic link to it on the local computer.
- **Folder redirection actions at logout time** applies the specified policy when the user logs out. For example, at logout, delete the symbolic link on the local computer (created at login) and restore the original folder to the network home directory.

After enabling the policy, click **Add**, then enter the following:

- **Path** The path to the folder on the network share. You do not need to specify the actual network share location – you can simply use the tilde (~) for the user's home directory; for example, `~/Library/Caches` specifies the `/Library/Caches` directory in the user's network home directory.
- **Link** The location to create or delete on the local computer. For example:

  `/tmp/Library/Caches`
- If you wish, you can use the syntax %@ to specify the logged in user's name. For example:

  `/tmp/%@/Library/Caches`

If cain is the logged in user, the folder that is created is:

`/tmp/cain/Library/Caches`

The Folder Redirection policies are listed here and explained below:

- Delete path
- Delete symbolic link and restore
- Delete and create symbolic link
- Rename and create symbolic link

Delete path

Path

User Configuration > Policies > Centrify Settings > Mac OS X Settings > Folder Redirection > Folder Redirect Actions at Login/Logout Time > Delete path

Description

Deletes the specified directory from the network home directory. For example, to delete the `/Library/Caches` file from each user's home directory, enter the following in the **Path** box:

`~/Library/Caches`

Typically, you enable this policy for the **login time** folder.

Note: You are not required to enter anything in the **Link** box for this group policy, and in fact, anything you enter in this box will be ignored. All the policies in this folder are implemented with the same UI and the other policies require the Link box so it appears for this policy as well.

Once this group policy is enabled, it takes effect when users log in (enabled for **login time** folder) or log out (enabled for **logout time** folder).

Delete Symbolic Link and Restore

Path

User Configuration > Policies > Centrify Settings > Mac OS X Settings > Folder Redirection > Folder Redirect Actions at Login/Logout Time > Delete symbolic link and restore

Description

Deletes a previously defined symbolic link on the local computer and restores the specified directory to the network home directory. Typically, you use this policy with the Rename and create symbolic link policy. For example:

At login (using Rename and create symbolic link) you save `~/Library/Caches` in the network home directory to a temporary folder and redirect it to a folder on the local computer, for example `/tmp/user/Library/Caches`. At logout, you can enable Delete symbolic link and restore to delete the symbolic link and restore the folder on the network home directory, by specifying the following:

- **Path**: `~/Library/Caches`
- **Link**: `/tmp/%@/Library/Caches`

where: `%@` specifies the logged in user's name on the local computer.

Once this group policy is enabled, it takes effect when users log in (enabled for **login time** folder) or log out (enabled for **logout time** folder).

Delete and Create Symbolic Link

Path

User Configuration > Policies > Centrify Settings > Mac OS X Settings > Folder Redirection > Folder Redirect Actions at Login/Logout Time > Delete and create symbolic link

Description

Deletes the specified directory from the network home directory and creates a symbolic link to it on the local computer.

For example, to delete the user's `/Library/Caches` policy from the network home directory and create a link to it on the local computer, specify the following after enabling the policy:

- **Path**: `~/Library/Caches`
- **Link**: `/tmp/%@/Library/Caches`

where `%@` specifies the logged in user's name on the local computer. For example, if cain is the logged in user, the cache files are written to:

`/tmp/cain/Library/Caches`

Once this group policy is enabled, it takes effect when users log in (enabled for **login time** folder) or log out (enabled for **logout time** folder).

Rename And Create Symbolic Link

Path

User Configuration > Policies > Centrify Settings > Mac OS X Settings > Folder Redirection > Folder Redirect Actions at Login/Logout Time > Rename and create symbolic link

Description

Renames the specified directory in the network home directory to a temporary folder and creates a symbolic link to it on the local computer.

For example, to rename the user's `/Library/Caches` policy on the network home directory and create a link to it on the local computer, specify the following after enabling the policy for the **login time** folder:

- **Path:**`~/Library/Caches`
- **Link:**`/tmp/%@/Library/Caches`

where `%@` specifies the logged in user's name on the local computer. For example, if cain is the logged in user, the cache files are written to:

`/tmp/cain/Library/Caches`

To restore the original `/Library/Caches` directory, use the Delete symbolic link and restore policy (enabled for the **logout time** folder).

Once this group policy is enabled, it takes effect when users log in (enabled for **login time** folder) or log out (enabled for **logout time** folder).

Import Settings

Path

User Configuration > Policies > Centrify Settings > Mac OS X Settings > Import Settings

Description

Mac OS X uses plist files to store application and other preferences. Use the **User Configuration > Policies > Centrify Settings > Mac OS X Settings > Import Settings** group policies to import plist files to customize your preferences:

- **Import plist files.** This group policy allows you to import preferences from another computer to computers in your Delinea-managed domain. To do so you:
  - Copy the plist files you want to use to the system volume on the domain controller.
  - Use the Import plist files group policy to import the plist files to computers in the domain.

This group policy automatically processes plist files to extract MCX settings when the files are imported.

- **Import MCX setting plist files.** This group policy is similar to the **Import plist file** group policy, except that it does not process any data from the inputted plist files. This group policy copies the exact content (that is, the "raw" content) from the plist file and imports it to the Active Directory user record.

When you import the plist files, Delinea copies them to the appropriate directories on the local computers to implement the preferences that they control.

You can gather and copy plist files from multiple computers and paste them to the `sysvol` directory on the domain controller, but a more structured approach is to set up a preferences 'template' computer, that is, a computer that is set up with your desired preferences. Then you can copy the appropriate plist files to `sysvol` on the domain controller. Finally, you can use either of the group policies described here to import the plist files to Delinea-managed computers in the domain.

Mac OS X stores plist files in the `/Library/Preferences` directory and in the `/Users/userName/Library/Preferences` directory.

The following section shows specifics of using these group policies.

Import plist Files

Path

User Configuration > Policies > Centrify Settings > Mac OS X Settings > Import Settings > Import plist files

Description

Specify the names of plist files to import from the system volume (`SYSVOL`) — similar to importing plist files in Mac Workgroup Manager. By default, the system volume folder is at: `\\domain\SYSVOL\domain\plist`.

Before enabling this policy, you should copy all the plist files to import to the system volume (`sysvol`) on the domain controller.

To add a file, select **Enabled**, click **Add**, then type a filename.

The path you type in **plist file** is relative to `\\domain\SYSVOL\domain\plist`. For example, if the domain name is `ajax.org` and you enter a plist file named `com.apple.MCX.plist`, the file that gets imported is:

`\\ajax.org\sysvol\ajax.org\com.apple.MCX.plist`

You can specify additional relative directories in the path, if needed.

Once this group policy is enabled, it takes effect when users log out and log back in.

Import MCX Setting plist Files

Path

User Configuration > Policies > Centrify Settings > Mac OS X Settings > Import Settings > Import MCX setting plist files

Description

Enable this group policy to import raw MCX settings plist files from SYSVOL. By default the folder is `\\<domain>\SYSVOL\<domain>\mcxplist`, similar to importing plist files in Mac Workgroup Manager.

The plist file path that you specify is relative to this path:

`\\<domain>\SYSVOL\<domain>\mcxplist`

For example, if you specify this path:

`com.apple.MCX.plist`

the following plist file is imported:

```
\\<domain>\SYSVOL\<domain>\mcxplist\com.apple.MCX.plist
```

This group policy is similar to "Import plist files". However, instead of extracting MCX settings from the plist file like "Import plist files" does, this policy imports the entire plist file without processing it.

An example plist file format is as follows:

```
<?xml version="1.0" encoding="UTF-8"?>

<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">

<plist version="1.0">

<dict>

    <key>mcx_application_data</key>

    <dict>

        <key>TARGET</key>

        <dict>

            <key>Forced</key>

            <array>

              <dict>

                Settings

              </dict>

            </array>

        </dict>

    </dict>

</dict>

</plist>
```

In this example, TARGET is the targeted MCX settings (such as com.apple.dock or com.apple.finder)

The recommended way to obtain the plist file with the correct format is by using the dscl command, and reading the MCX settings attribute of the user object that has the same MCX settings configured. Then copy the exact MCX settings and paste them into a plist file.

For example:

```
dscl /CentrifyDC read /Users/XXXX MCXSettings
```

where *XXXX* is an Active Directory user with the desired MCX settings.

Login Settings

Path

User Configuration > Policies > Centrify Settings > Mac OS X Settings > Login Settings

Description

Use the **User Configuration > Policies > Centrify Settings > Mac OS X Settings > Login Settings** group policy to specify frequently used items, such as applications, folders, or server connections to automatically open when a user logs in.

After enabling this policy, you can do the following:

- Use the **Add** button to specify the path to applications to open.
- In the **Network Home** area, use the **Add** button to specify URLs for servers to connect to; use the check box to specify whether to automatically connect the logged in user to the specified servers.
- Use the other check boxes to control whether users have the ability to add or remove login items.

The following table shows specifics of using this group policy.

> **Note:** Only the **Login items** area is visible when you first open the properties page for the group policy. Use the scroll bar to see the **Network share** area and other items that you can configure with this policy.

Enable Login Items

Path

User Configuration > Policies > Centrify Settings > Mac OS X Settings > Login Settings > Enable login items

Description

Specify the names of applications, folders, and server locations to open automatically when a user logs in. Select **Enable**, then do any or all of the following:

- **Login items**. To add an application to open automatically, click **Add**, then type the path to the application; for example:

```
/Applications/TextEdit.app
```

To initially hide the application, select **Hide**. The application will open, but its window and menu bar remain hidden until the user activates the application (for example, by clicking the application icon in the doc).

Click **OK** to save the item you entered. You can click **Add** as often as necessary to add multiple applications. You can also select an item in the window and click **Edit** to change it, or **Remove** to delete it.

- **Network share**. To add access to a network share, click **Add**, then type the URL in one of the following formats:

```
smb://server/share

smb://server/hidden$

smb://server/share/subdir

smb://user:password@server/share

smb://user:@server/share

afp://server/share

nfs://server/share
```

`nfs://192.168.0.1/share`

To automatically connect the user to the share with the user's login name and password, select **Authenticate selected share point with user's login name and password**.

> **Note:** If you uncheck this option, the share name must comply with RFC 1738 - Uniform Resource Locators (URL), which specifies that special characters need to be encoded, for example, by using `%20` instead of a space.

If the network share can be authenticated using Kerberos, this option can be ignored. If the network share cannot be authenticated using Kerberos, and this option is unchecked, then the user will be prompted for a username and password.

If a username is specified in the URL for the network share, then checking this option will still mount the share as the login user, while deselecting this option will mount the share as the user specified in the URL. For example, if network share is `smb://mount_user:password@server/share`, checking the option will mount the share as `login_user`, while deselecting the option will mount the share as `mount_user`.

Click **OK** to save the item you entered. You can click **Add** as often as necessary to add multiple shares. You can also select an item in the window and click **Edit** to change it, or **Remove** to delete it.

- Select **User may add and remove additional items** to allow users to add items to the list and remove items from the list.

  Deselect this box to prevent users from adding items or removing the items that you have specified. Note that they can remove login items that they specified on their own.
- Select **User may press Shift to keep items from opening** to allow user's to stop items from opening by holding down the Shift key during login until the Finder appears on the desktop.

  Deselect this option to prevent users from stopping applications from opening automatically.

Once enabled, this group policy takes effect when users log out and log back in.

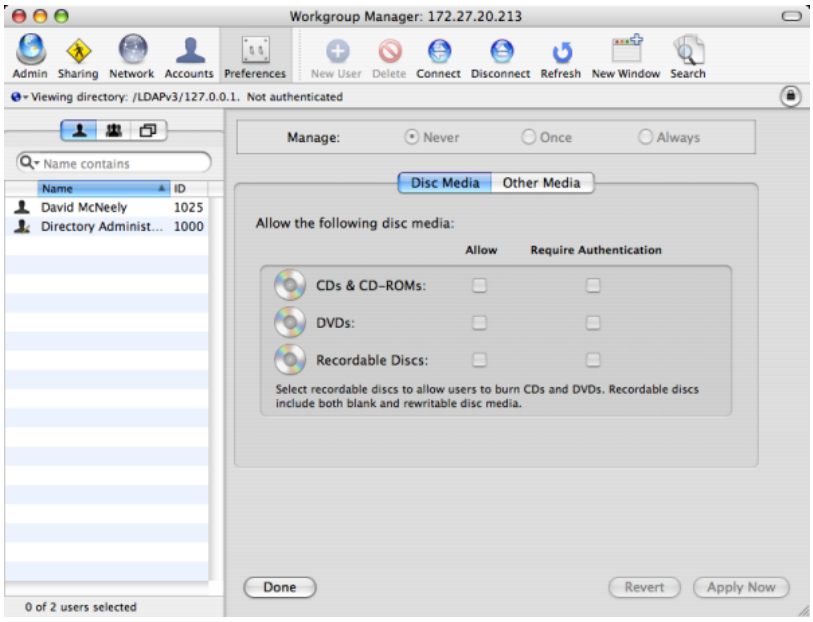
Media Access Settings

Path

User Configuration > Policies > Centrify Settings > Mac OS X Settings > Media Access Settings

Description

Use the **User Configuration > Policies > Centrify Settings > Mac OS X Settings > Media Access Settings** group policies to manage the access to discs and other media for Mac users. These group policies enable you to control access to specific types of media, such as CDs or DVDs, but you cannot restrict access to specific discs or to specific items, such as music or movies, on a disc type users are permitted to access. These settings correspond to the Media Access preferences you can manage using the Workgroup Manager. For example:



Permit/Prohibit Access: CDs and CD-ROMs

Path

User Configuration > Policies > Centrify Settings > Mac OS X Settings > Media Access Settings > Permit/prohibit access: CDs and CD-ROMs

Description

Control whether users can access data and applications on CDs and CD-ROMs. The valid options are:

- **allow** to allow access to CDs and CD-ROMs without authentication.
- **allow, require authentication** to require users to provide credentials for authentication before allowing them access to CDs and CD-ROMs.
- **deny** to prevent users from accessing any data or applications on CDs and CD-ROMs.

Once this group policy is enabled, it takes effect when users log out and log back in.

Permit/Prohibit Access: DVDs

Path

User Configuration > Policies > Centrify Settings > Mac OS X Settings > Media Access Settings > Permit/prohibit access: DVDs

Description

Control whether users can access data and applications on DVDs. The valid options are:

- **allow** to allow access to DVDs without authentication.
- **allow, require authentication** to require users to provide credentials for authentication before allowing them

access to DVDs.

- **deny** to prevent users from accessing any data or applications on DVDs.

Once this group policy is enabled, it takes effect when users log out and log back in.

Permit/Prohibit Access: Recordable Discs

Path

User Configuration > Policies > Centrify Settings > Mac OS X Settings > Media Access Settings > Permit/prohibit access: Recordable Discs

Description

Control whether users can record or access data and applications on recordable discs. The valid options are:

- **allow** to allow access to recordable discs without authentication.
- **allow, require authentication** to require users to provide credentials for authentication before allowing them access to recordable discs.
- **deny** to prevent users from accessing any data or applications on recordable discs.

Allowing users access to recordable discs enables users to burn CDs and DVDs. Recordable discs can be blank or rewritable disc media.

Once this group policy is enabled, it takes effect when users log out and log back in.

Permit/Prohibit Access: Internal Discs

Path

User Configuration > Policies > Centrify Settings > Mac OS X Settings > Media Access Settings > Permit/prohibit access: Internal Discs

Description

Control whether users can access data and applications on internal discs. The valid options are:

- **allow** to allow read and write access to internal discs without authentication.
- **allow, read-only** to allow read-only access to the media.
- **allow, require authentication** to require users to provide credentials for authentication before allowing them access to the media.
- **allow, require authentication, read-only** to require users to provide credentials for authentication before allowing them access to internal discs, and grant **read-only access to the media** if authentication is successful.
- **deny** to prevent users from accessing any data or applications on internal discs.

Once this group policy is enabled, it takes effect when users log out and log back in.

Permit/Prohibit Access: External Discs

Path

User Configuration > Policies > Centrify Settings > Mac OS X Settings > Media Access Settings > Permit/prohibit access: External Discs

Description

Control whether users can access data and applications on external discs. External disks include floppy disks, FireWire drives, and all other external storage devices except CDs and DVDs. The valid options are:

- **allow** to allow read and write access to external discs without authentication.
- **allow, read-only to allow read-only access to** external discs.
- **allow, require authentication** to require users to provide credentials for authentication before allowing them access to external discs.
- **allow, require authentication, read-only** to require users to provide credentials for authentication before allowing them access to external discs, and grant **read-only access to the media** if authentication is successful.
- **deny** to prevent users from accessing any data or applications on external discs.

Once this group policy is enabled, it takes effect when users log out and log back in.

Eject All Removable Media at Logout

Path

User Configuration > Policies > Centrify Settings > Mac OS X Settings > Media Access Settings > Eject all removable media at logout

Description

Control whether removable media, such as CDs, DVDs, Zip disks, or FireWire drives, are automatically ejected when users log out. If you enable this group policy, CDs, DVDs, and other disk media are automatically ejected when users log out to ensure removable media is properly disconnected and put away when users end their sessions.

Once this group policy is enabled, it takes effect when users log out and log back in.

Mobility Settings

Use the **Computer Configuration > Policies > Centrify Settings > Mac OS X Settings > Mobility Settings** group policies to control if macOS creates a Mobile Account for the Active Directory user when logging in.

Configure Mobile Account Creation

Path

Computer Configuration > Policies > Centrify Settings > Mac OS X Settings > Mobility Settings > Configure mobile account creation

Description

Configure whether mobile accounts are created when users log in.

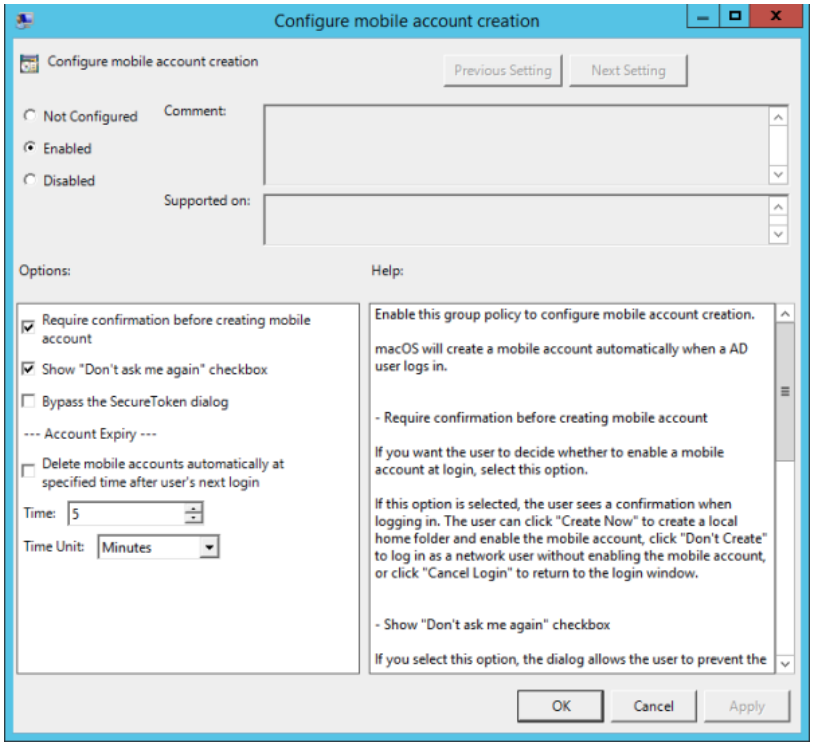
Check **Require confirmation before creating mobile account** to allow users to decide whether to enable a mobile account at login. Users see a confirmation dialog when logging in and can click one of the following:

- “Create Now” to create a local home folder and enable the mobile account.
- “Don't Create” to log in as a network user without enabling the mobile account.
- “Cancel Login” to return to the login window.

Select **Show “Don't ask me again” checkbox** to provide a check box that allows users to prevent display of the mobile account creation dialog on that computer in the future. Users who select “Don't ask me again” and click “Don't Create”, are not asked to create a mobile account on that computer (unless they hold down the Option key during login to redisplay the dialog).

Select **Bypass the SecureToken dialog** so that the system will bypass the secure token authorization dialog. The Active Directory user can continue to create a mobile account. However, if this volume is encrypted, the Active Directory mobile user may not be able to log in with this account when the computer starts. This dialog only affects APFS volumes.

Select **Delete mobile accounts automatically at specified time after user's next login** so that MacOS will delete the mobile account and its local home folder automatically after a period of inactivity.



Printing settings

Path

User Configuration > Policies > Centrify Settings > Mac OS X Settings > Printing Settings > Specify printer list (with model)

Description

Use the **User Configuration > Policies > Centrify Settings > Mac OS X Settings > Printing Settings > Specify printer list (with model)** group policy to specify a list of printers for a user.

The printers that are available to a user are a combination of those specified in this policy and those added through System Preferences on the local computer. Note that this policy allows an administrator to control whether the user can add or see printers on the local computer, or is only allowed to use the managed printers specified by this policy.

Specify a managed list of network printers that are available to a user on this computer. Printers specified by this policy use a generic PostScript driver.

To add a printer, click **Add** and enter the following information:

- **Name**: A name of your choosing for the printer.
- **DeviceURI**: The device Uniform Resource Identifier, which specifies the device that is assigned to the printer (see **Specifying the Device URI**, below); for example:
  - `socket://192.168.0.20:9100` (which identifies the protocol, IP address, and port number)
  - `cdcsmb://dc1.acme.com/HPLaserJet2` (which identifies a Windows printer added using the Delinea protocol and identified by hostname.)
- (Optional) **Model**: The printer driver for the printer model (see **Specifying the Model (printer driver)**, below); for example: `HP Photosmart C6100 series. Fax`

You can use the following options to control access to the printers on the local computer:

- **Allow user to modify the printer list**: Check this option to allow local users to make changes in System Preferences to the printers that have been added by this policy, including deleting them.

  Deselect this option to prevent local users from modifying the printers added by this policy.
- **Allow printers that connect directly to user's computer**: Check this option to allow users to add their own local printers.

  Deselect this option to prevent users from adding local printers.
- **Require an administrator password**: Check this option to require an administrator's password when adding local printers.
- **Only show managed printers**: Check this option to allow local users to use only the managed printers specified by this option.

  Printers added locally, for example, through System Preferences, will not be visible.

  Deselect this option to allow local users to use printers added locally, as well as the managed printers added by this policy.

Printers added through this group policy appear after the next group policy refresh interval.

Specifying the Device URI

When you add a printer through the **Specify printer list** group policy, or locally by using the **Print & Scan, Add Printer** advanced options, the printer is implemented through the Common UNIX Printing System (CUPS), which was developed by Apple for Mac OS X and other UNIX-like operating systems.

The CUPS system supports the following device Uniform Resource Identifier (URI) protocols that you can use to specify the printers to add.

AppSocket or Jetdirect Protocol

The AppSocket, or JetDirect, protocol normally prints over port 9100 and uses the socket URI scheme:

```
socket://ip-address-or-hostname
socket://ip-address-or-hostname:port-number
```

Internet Printing Protocol (IPP)

CUPS supports IPP natively. IPP printing normally happens over port 631 and uses the http and ipp URI schemes:

```
ipp://ip-address-or-hostname/resource
ipp://ip-address-or-hostname:port-number/resource
http://ip-address-or-hostname:port-number/resource
```

Line Printer Daemon Protocol (LPD)

LPD is the original network printing protocol and is supported by many network printers. LPD printing normally happens over port 515 and uses the `lpd` URI scheme:

```
lpd://ip-address-or-hostname/queue
lpd://username@ip-address-or-hostname/queue
```

Windows Printer via Delinea

When Mac users print on a Windows network printer, they must authenticate separately. Specifying a Windows printer via Delinea allows users to access the printer without providing credentials as they have already been authenticated through Active Directory.

Delinea printing normally happens over port 445 and uses the `cdcsmb` URI scheme

```
cdcsmb://server_fqdn/printersharename
```

Windows

Windows printing normally happens over port 445 and uses the smb URI scheme:

> **Note:** You can use the Delinea protocol (`cdcsmb`), if you want to use Windows network printers without providing credentials each time.

```
smb://workgroup/server/printersharename
smb://ip-address-or-hostname/printersharename
smb://username:password@workgroup/ip-address-or-hostname/printersharename
smb://username:password@ip-address-or-hostname/printersharename
```

Specifying the Model (printer driver)

Model specifies the model name of the added printer and is used to determine which device driver to associate with the printer. Be certain to specify model correctly, otherwise, if model is not specified, or does not match a driver installed on the client Mac OX X computer, Generic PostScript driver will be selected for the printer, which may result in fewer printing options.

To find the correct model name, take one of these two approaches:

Use Printers & Scanners to identify the model:

1. On a Mac OX X computer, open **System Preferences > Printers & Scanners**.
2. Click **Add (+)** to add a printer.
3. When you select a printer, the correct model name appears on the "Use" drop down menu.

Use `lpinfo` to identify the model

1. On a Mac OX X computer, open the Terminal application.
2. Run the following command to obtain the list of all the models available:

   `"lpinfo -m" command`

   In the output from `lpinfo`, the correct model string appears right after `*.ppd.gz`. For example:

   `Library/Printers/PPDs/Contents/Resources/HP Photosmart C6100 Series Fax.ppd.gz HP Photosmart C6100 series. Fax`

   The model string is:

   `HP Photosmart C6100 series. Fax`
3. Type this in the group policy's **Model** field.

Scripts (Login/Logout)

Path

User Configuration > Policies > Centrify Settings > Mac OS X Settings > Scripts (Login/Logout)

Description

Use the **User Configuration > Policies > Centrify Settings > Mac OS X Settings > Scripts (Login/Logout)** group policies to deploy login and logout scripts that run when an Active Directory user logs on or logs out. When you use these group policies, the login and logout scripts are stored in the Active Directory domain's system volume (`sysvol`) and transferred to the Mac computer when the group policies are applied. Login and logout scripts are useful for performing common tasks such as mounting and un-mounting shares.

> **Note:** When these group policies are enabled, the first login by an AD user will restart the login script and return the user to the login window. Subsequent logins by this user or a different user occur normally and the changes generated by the script happen immediately.

Specify Login Script (Deprecated)

Path

User Configuration > Policies > Centrify Settings > Mac OS X Settings > Scripts (Login/Logout) > Specify login script

Description

Specify the name of a login script to execute when users log on. You can specify only one file as the login script.

Before enabling this policy, you should create the login script and copy it to the system volume (`sysvol`) on the domain controller. By default, the login script is stored in the system volume (`SYSVOL`) on the domain controller in the directory:

`\\domain\SYSVOL\domain\Scripts\scriptname`

The script path you type in **Login script** is relative to `\\domain\SYSVOL\domain\scripts\`. For example, if the domain name is `ajax.org` and you enter a script name of `mlogin.sh`, the script that gets executed on the domain controller is:

`\\ajax.org\SYSVOL\ajax.org\Scripts\mlogin.sh`

You can specify additional relative directories in the path, if needed.

Note: Be certain authenticated users have permission to read this file so the script can run when they log in.

By default, the script runs with the Active Directory user's permissions. If the script contains commands that require root permission to run, select **Run with root user privileges**.

Once this group policy is enabled, it takes effect when users log out and log back in.

Note: The first AD user to log in is taken back to the login screen. Subsequent logins by this user or a different user occur normally and changes generated by the script happen immediately.

Specify Logout Script

Path

User Configuration > Policies > Centrify Settings > Mac OS X Settings > Scripts (Login/Logout) > Specify logout script

Description

Specify the name of a logout script to execute when users log out. You can specify only one file as the logout script.

Before enabling this policy, you should create the logout script and copy it to the system volume (`SYSVOL`) on the domain controller. By default, the logout script is stored in the system volume (`SYSVOL`) on the domain controller in the following directory:

`\\domain\SYSVOL\domain\Scripts\scriptname`

The script path you type in **Logout script** is relative to: `\domain\SYSVOL\domain\scripts\`.

For example, if the domain name is `ajax.org` and you enter a script name of `mlogout.sh`, the script that gets executed on the domain controller is:

`\\ajax.org\SYSVOL\ajax.org\Scripts\mlogout.sh`

Note: Be certain authenticated users have permission to read this file so the script can run when they log out.

By default, the script runs with the Active Directory user's permissions. If the script contains commands that require root permission to run, select **Run with root user privileges**.

Once this group policy is enabled, it takes effect when users log out and log back in.

Specify Multiple Login Scripts

Path

User Configuration > Policies > Centrify Settings > Mac OS X Settings > Scripts (Login/Logout) > Specify multiple login scripts

Description

Specify the names of one or more login scripts to execute when a user logs on. The scripts you specify run simultaneously in no particular order.

This policy is also available as a computer policy. If you specify scripts using both the computer and user policies, the computer scripts are executed first.

Before enabling this policy, you should create the scripts and copy them to the system volume (sysvol) on the domain controller. By default, the login scripts are stored in the system volume (SYSVOL) on the domain controller in the directory:

```
\\domain\SYSVOL\domain\Scripts
\scriptname1
\scriptname
...
```

After enabling this policy, click **Add** and enter the following information:

- __Script:__The name of the script and an optional path, which are relative to `\\domain\SYSVOL\domain\scripts\`.

For example, if the domain name is `ajax.org` and you enter a script name of `mlogin.sh`, the script that gets executed on the domain controller is:

```
\ajax.org\SYSVOL\ajax.org\Scripts\mlogin.sh`
```

You can specify additional relative directories in the path, if needed; for example, if you type `submlogin.sh`, the file that gets executed is:

```
\\ajax.org\SYSVOL\ajax.org\Scripts\sub\mlogin.sh
```

- **Parameters**: An optional set of arguments to pass to the script.

These arguments are interpreted the same way as in a UNIX shell; that is, space is a delimiter, and backslash is an escape character. You can also use `$USER` to represent the current user's name. For example:

```
arg1 arg2 arg3
arg1 'a r g 2' arg3
arg' $USER.
```

Note: Be certain authenticated users have permission to read these files so the scripts can run when they log in.

Once this group policy is enabled, it takes effect when users log out and log back in.

Security & Privacy Settings

Path

User Configuration > Policies > Centrify Settings > Mac OS X Settings > Security & Privacy

Description

Use the Security & Privacy group policies to control user security and privacy settings.

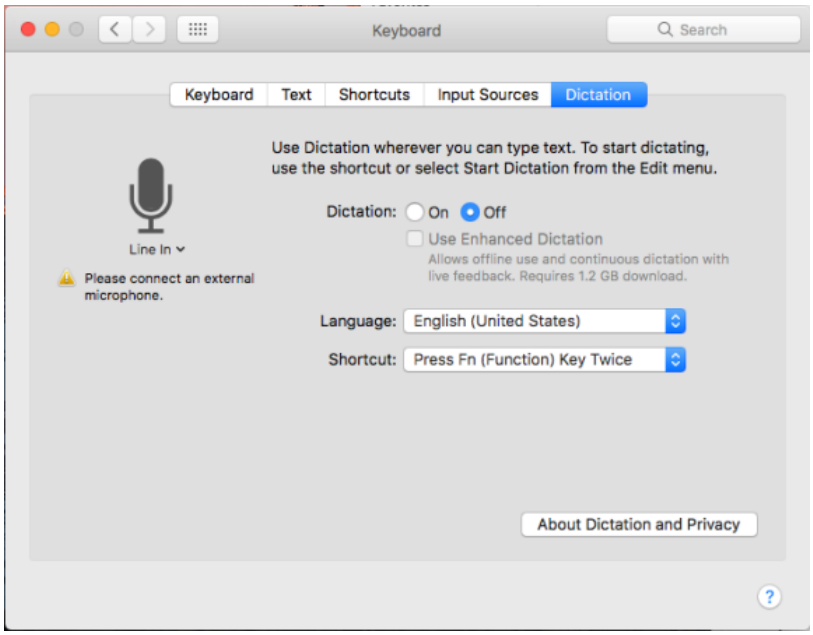
Disable Dictation

Path

User Configuration > Policies > Centrify Settings > Mac OS X Settings > Security & Privacy Settings > Disable Dictation

Description

Enable this policy to turn off Dictation in the System Preferences > Keyboard pane.



Once enabled, this group policy takes effect dynamically at the next group policy refresh interval.

Require a Password to Wake this Computer from Sleep or Screen Saver (Deprecated)

Note: This group policy is deprecated, and will not work anymore. Please use the new same name group policy under "Computer Configuration > Policies > Centrify Settings > Mac OS X Settings > Security & Privacy Settings > Require a password to wake this computer from sleep or screen saver" instead.

Path

User Configuration > Policies > Centrify Settings > Mac OS X Settings > Security & Privacy Settings > Require a password to wake this computer from sleep or screen saver

Description

Lock the computer screen when the computer goes into sleep or screen saver mode and requires users to enter a user name and password to unlock the screen.

Enabling this group policy is the same as clicking the **Require a password to wake this computer from sleep or screen saver** option in the Security system preference.

After this group policy is enabled, it takes effect when the computer is rebooted.

Prohibit Authentication with Expired Password

Path

User Configuration > Policies > Centrify Settings > Mac OS X Settings > Security & Privacy Settings > Prohibit authentication with expired password

Description

Prohibit a user from unlocking the screen if a password change is required while the screen is locked. If a user logs in with a password that must be changed, and the computer goes into sleep or screen saver mode before the user updates the password, the user is locked out. Disabling this policy allows a user to specify the old password to remove the screen lock.

Keychain Policies

Path

User Configuration > Policies > Centrify Settings > Mac OS X Settings > Security & Privacy Settings > Keychain Policies

Description

On OS X 10.11, you can create a keychain protected by a smart card token or a password. Once the Enable smart card protected keychain group policy takes effect, the token-protected keychain can only be unlocked with a PIN when the associated smart card is present. This group policy can be configured to allow users who lose or forget their smart card to continue to log in with a password. In this case, a new password-protected keychain is created to ensure users can continue to log in to their account; however, keychain items are not transferred from the token-protected keychain to the password-protected keychain.

This feature is not supported on OS X 10.10 and earlier.

Enable Protected Keychain

Path

User Configuration > Policies > Centrify Settings > Mac OS X Settings > Security & Privacy Settings > Keychain Policies > Enable protected keychain

Description

Create a new keychain protected by either an asymmetric token stored on a smart card or by a password, depending on the log in type. Enabling this policy requires users to have the smart card present to unlock the token-protected keychain.

When the smart card is renewed it will no longer unlock the protected keychain. There is no way to export a token-protected keychain; you will have to recreate the keychain items in the new token-protected keychain. In addition, if a smart card is lost, there is no way to recover items from the token-protected keychain.

The **Set as user default keychain** option is selected by default. This option is required to be able to log in with a password after this group policy takes effect. With this option set, the default keychain will be switched based on the login type (smart card login or password login). Deselect this option to leave the existing login keychain as the default keychain.

The **Delete the Password protected 'Login' Keychain after login** option is deselected by default. Select this option to delete the existing password-protected 'Login' Keychain after logging in with a smart card, leaving no keychains that can be unlocked without a smart card. This option is required to be able to log in with a password after this group policy takes effect without seeing keychain errors.

Note: This feature is not supported on OS X 10.10 and earlier.

Lock Protected Keychain After Number of Minutes of Inactivity

Path

User Configuration > Policies > Centrify Settings > Mac OS X Settings > Security & Privacy Settings > Keychain Policies > Lock protected keychain after number of minutes of inactivity

Description

Lock the protected keychain after a period of inactivity that you specify in minutes.

This policy only works if you have enabled the Enable protected keychain group policy.

This policy takes effect at the next user login using smart card authentication.

Lock Protected Keychain When Sleeping

Path

User Configuration > Policies > Centrify Settings > Mac OS X Settings > Security & Privacy Settings > Keychain Policies > Lock protected keychain when sleeping

Description

Lock the protected keychain when the machine sleeps.

This policy only works if you have enabled the Enable protected keychain group policy.

This policy takes effect at the next user login using smart card authentication.

Allow All Applications to Access The Auto-Enrollment Private Key(S)

Path

User Configuration > Policies > Centrify Settings > Mac OS X Settings > Security & Privacy > Public Key Policies > Allow all applications to access the auto-enrollment private key(s)

Description

Enabling this policy allows all applications to access the auto-enrollment private key(s) in the System keychain.

See Configuring Auto-Enrollment for more information about auto-enrollment keys.

Note: This setting only applies to new auto-enrollment private key(s); it will not update already imported auto-enrollment private key(s) that are in the System keychain.

Allow Specific Applications to Access the Auto-Enrollment Private Key(S)

Path

User Configuration > Policies > Centrify Settings > Mac OS X Settings > Security & Privacy > Public Key Policies > Allow specific applications to access the auto-enrollment private key(s)

Description

Enabling this policy allows specified applications to access the auto-enrollment private key(s) in System keychain.

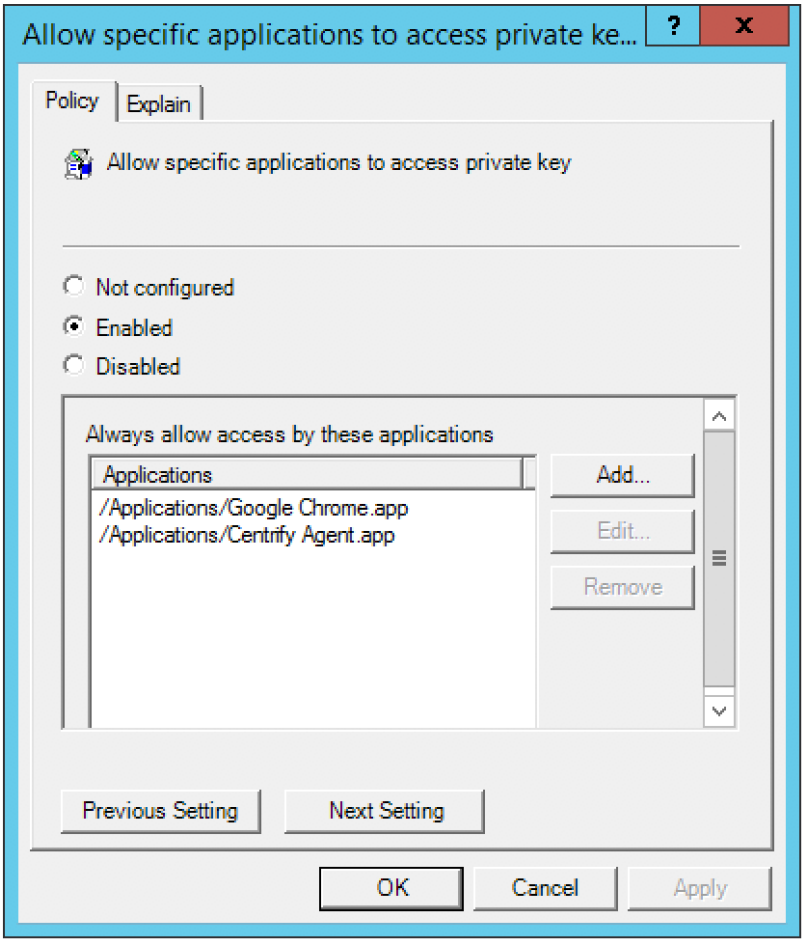
After you enable this policy, click **Add** to enter the path to the application you want to allow access to the auto-enrollment private key, then click **OK**. You can click **Add** again to add additional applications.

For example, to give Google Chrome and Delinea Agent access to the auto-enrollment private key, enter the application path for Google Chrome:

```
/Applications/Google Chrome.app
```

Click **OK**. Then click **Add** and enter the application path for Delinea Agent:

```
/Applications/Centrify Agent.app
```



After this group policy is enabled, the list of applications specified in the group policy are added to the access control list of the auto-enrollment private key in system keychain.

See Configuring Auto-Enrollment for more information about auto-enrollment keys.

> **Note:** This setting only applies to a new auto-enrollment private key. It does not change auto-enrolled private keys that are already in the keychain.

If the group policy above, **Allow All Applications to Access the Auto-enrollment Private Key(s)** is enabled, this group policy will be ignored.

Do Not Allow the Private Key(S) To Be Extractable

Path

User Configuration > Policies > Centrify Settings > Mac OS X Settings > Security & Privacy > Public Key Policies > Do not allow private key(s) to be extractable

Description

Enabling this policy prevents exporting the auto-enrollment private key(s).

> **Note:** This setting only applies to new auto-enrollment private key(s). It does not change auto-enrolled private keys that are already in the keychain.

System Preference Settings

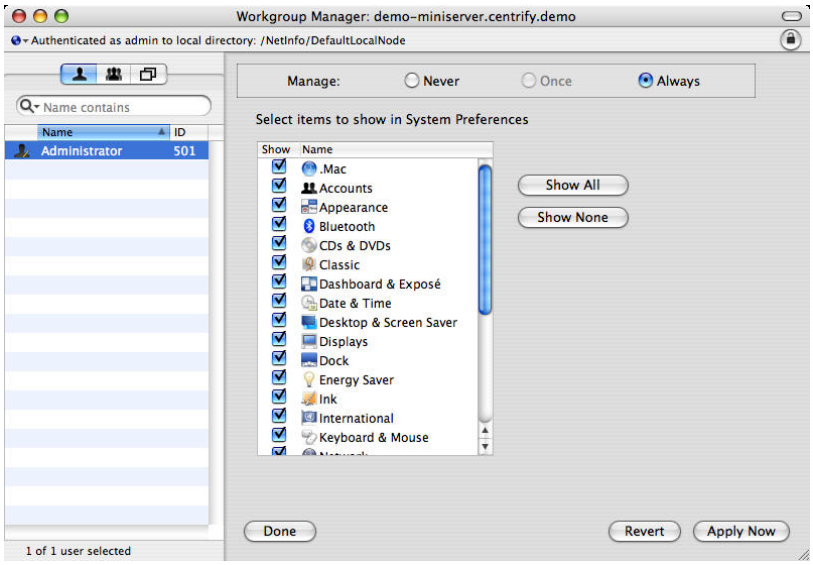
Path

User Configuration > Policies > Centrify Settings > Mac OS X Settings > Security & Privacy Settings > System Preference Settings

Description

Use the **User Configuration > Policies > Centrify Settings > Mac OS X Settings > System Preference Settings** group policies to specify which preferences are enabled for use in System Preferences for Mac OS X users. Enabling a preference for use does not enable non-admin users to modify that preference. For example, some preferences, such as Startup Disk preferences, require an administrator name and password before a user can modify its settings. Displaying a preference does enable a user to view the preference's current settings.

By default, no system preference panes are displayed unless explicitly enabled. The group policies in this category correspond to System Preferences you can select for display in the Workgroup Manager. For example:



The user interface for System Preferences Settings differs significantly between different versions of Mac OS X. Therefore, there are separate System Preferences policies for each supported version of Mac OS X. In addition, to support existing installations that configured group policies by using a previous `centrifydc_mac_settings` template, the Centrify group policies provide a set of legacy preferences settings.

The **Use Version Specific Settings** group policy below determines whether to use legacy settings or platform-specific system preferences settings. By default (if you do not configure or disable this policy) legacy settings are used.

If you enable this policy, you can then enable platform-specific system preferences settings for each platform in your environment; see the following sections for information on each set of policies:

Use Version Specific Settings

Path

User Configuration > Policies > Centrify Settings > Mac OS X Settings > Security & Privacy Settings > System Preference Settings > Use version specific settings

Description

Enable the use of version-specific System Preferences settings.

If you enable this policy, you can then set platform-specific preferences settings for each platform in your environment. For example, if you have only 10.10 computers, you can enable this policy and then use Mac OS X 10.10 settings. If you have 10.9 and 10.10 computers, enable this policy, and then configure the version-specific policies as appropriate:

- Mac OS X 10.9 Settings
- Mac OS X 10.10 Settings

When a computer joins the domain, Delinea Management Services determines the OS version and applies the appropriate Preferences settings.

If this policy is disabled or not configured, Legacy Settings are used instead of version-specific settings. Likewise, Delinea versions prior to 4.4.2 always use Legacy Settings and ignore this policy setting.

If you configured System Preferences settings with a version of the product prior to 4.4.2, these settings are saved to Legacy Settings when you upgrade to the current version. You can keep or edit these settings as you wish.

Note: The Legacy Settings may not match exactly the settings for each OS version; for example, some settings may be missing while others may be redundant for a particular OS version.

Legacy Settings

Path

User Configuration > Policies > Centrify Settings > Mac OS X Settings > Security & Privacy Settings > System Preference Settings > Legacy Settings

Description

When you upgrade from a version of Delinea prior to 4.4.2, your System Preferences settings are saved to Legacy Settings. You can keep or edit the individual legacy system preferences group policy settings as you wish.

Note: The legacy settings may not match exactly the settings for each OS version; for example, some settings may be missing while others may be redundant for a particular OS version.

Use this policy	To do this
Showing items in the Personal pane of System Preferences	Select the items to display in the Personal pane of System Preferences.
Showing items in the Hardware System pane of Preferences	Select the items to display in the Hardware pane of System Preferences.
Showing items in the Internet & Network pane of System Preferences	Select the items to display in the Internet & Network pane of System Preferences.
Showing items in the System pane of System Preferences	Select the items to display in the System pane of System Preferences.
Showing items in the Other pane of System Preferences	Select the items to display in the Other pane of System Preferences.
Limit items usage in System Preferences (deprecated)	Limit the usage of items in System Preferences. You must enable this group policy for any of the other group policy settings to take effect. Once this group policy is enabled, it takes effect when users log out and log back in.

Showing items in the Personal pane of System Preferences

Path

User Configuration > Policies > Centrify Settings > Mac OS X Settings > Security & Privacy Settings > System Preference Settings > Enable System Preferences Pane: Personal

Description

Use the group policies in this category to choose which items to display in the Personal pane of System Preferences.

Enable Appearance

Enable usage of Appearance preferences in the Personal pane of System Preferences.

Once this group policy is enabled, it takes effect when users log out and log back in.

Enable Dashboard & Expose

Enable usage of Dashboard & ExposE preferences in the Personal pane of System Preferences.

Once this group policy is enabled, it takes effect when users log out and log back in.

Enable Desktop & Screen Saver

Enable usage of Desktop & Screen Saver preferences in the Personal pane of System Preferences.

Once this group policy is enabled, it takes effect when users log out and log back in.

Enable Dock

Enable usage of Dock preferences in the Personal pane of System Preferences.

Once this group policy is enabled, it takes effect when users log out and log back in.

Enable International (Language & Text)

Enable usage of International preferences in the Personal pane of System Preferences.

Once this group policy is enabled, it takes effect when users log out and log back in.

Enable Security

Enable usage of Security preferences in the Personal pane of System Preferences.

Once this group policy is enabled, it takes effect when users log out and log back in.

Enable Spotlight

Enable usage of Spotlight preferences in the Personal pane of System Preferences.

Once this group policy is enabled, it takes effect when users log out and log back in.

Showing items in the Hardware System pane of Preferences

Use the group policies in this category to display items in the Hardware pane of System Preferences.

Enable Bluetooth

Enable usage of Bluetooth preferences in the Hardware pane of System Preferences.

Once this group policy is enabled, it takes effect when users log out and log back in.

Enable CDs & DVDs

Enable usage of CDs & DVDs preferences in the Hardware pane of System Preferences.

Once this group policy is enabled, it takes effect when users log out and log back in.

Enable Displays

Enable usage of Displays preferences in the Hardware pane of System Preferences.

Once this group policy is enabled, it takes effect when users log out and log back in.

Enable Energy Saver

Enable usage of Energy Saver preferences in the Hardware pane of System Preferences.

Once this group policy is enabled, it takes effect when users log out and log back in.

Enable Ink

Enable usage of Ink preferences in the Hardware pane of System Preferences.

Note: Ink preferences are only shown if a graphics tablet is connected to the Mac computer.

Once this group policy is enabled, it takes effect when users log out and log back in.

Enable Keyboard & Mouse (Keyboard)

Enable usage of Keyboard & Mouse preferences in the Hardware pane of System Preferences.

Once this group policy is enabled, it takes effect when users log out and log back in.

Enable Mouse

Enable usage of Mouse preferences in the Hardware pane of System Preferences.

Once this group policy is enabled, it takes effect when users log out and log back in.

Enable Print & FAX

Enable usage of Print & FAX preferences in the Hardware pane of System Preferences.

Once this group policy is enabled, it takes effect when users log out and log back in.

Enable Sound

Enable usage of Sound preferences in the Hardware pane of System Preferences.

Once this group policy is enabled, it takes effect when users log out and log back in.

Enable Trackpad

Enable usage of Trackpad preferences in the Hardware pane of System Preferences.

Once this group policy is enabled, it takes effect when users log out and log back in.

Showing Items in the Internet & Network Pane of System Preferences

Path

User Configuration > Policies > Centrify Settings > Mac OS X Settings > Security & Privacy Settings > System Preference Settings > Enable System Preferences Pane: Internet & Network

Description

Use the group policies in this category to display items in the Internet & Network pane of System Preferences.

Enable .Mac (MobileMe)

Enable usage of .Mac preferences in the Internet & Network pane of System Preferences.

Once this group policy is enabled, it takes effect when users log out and log back in.

Enable Fibre Channel

Enable usage of Fibre Channel preferences in the Internet & Network pane of System Preferences.

Once this group policy is enabled, it takes effect when users log out and log back in.

Enable Network

Enable usage of Network preferences in the Internet & Network pane of System Preferences.

Once this group policy is enabled, it takes effect when users log out and log back in.

Enable QuickTime

Enable usage of QuickTime preferences in the Internet & Network pane of System Preferences.

Once this group policy is enabled, it takes effect when users log out and log back in.

Enable Sharing

Enable usage of Sharing preferences in the Internet & Network pane of System Preferences.

Once this group policy is enabled, it takes effect when users log out and log back in.

Showing items in the System pane of System Preferences

Path

User Configuration > Policies > Centrify Settings > Mac OS X Settings > Security & Privacy Settings > System Preference Settings > Enable System Preferences Pane: System

Description

Use the group policies in this category to display items in the System pane of System Preferences.

Enable Accounts

Enable usage of Accounts preferences in the System pane of System Preferences.

Once this group policy is enabled, it takes effect when users log out and log back in.

Enable Classic

Enable usage of Classic preferences in the System pane of System Preferences.

Once this group policy is enabled, it takes effect when users log out and log back in.

Enable Date & Time

Enable usage of Date & Time preferences in the System pane of System Preferences.

Once this group policy is enabled, it takes effect when users log out and log back in.

Enable Parental Controls

Enable usage of Parental Controls preferences in the System pane of System Preferences.

Once this group policy is enabled, it takes effect when users log out and log back in.

Enable Software Update

Enable usage of Software Update preferences in the System pane of System Preferences.

Once this group policy is enabled, it takes effect when users log out and log back in.

Enable Speech

Enable usage of Speech preferences in the System pane of System Preferences.

Once this group policy is enabled, it takes effect when users log out and log back in.

Enable Startup Disk

Enable usage of Startup Disk preferences in the System pane of System Preferences.

Once this group policy is enabled, it takes effect when users log out and log back in.

Enable Time Machine

Enable usage of Time Machine preferences in the System pane of System Preferences.

Once this group policy is enabled, it takes effect when users log out and log back in.

Enable Universal Access

Enable usage of Universal Access preferences in the System pane of System Preferences.

Once this group policy is enabled, it takes effect when users log out and log back in.

Showing Items in the Other Pane of System Preferences

Path

User Configuration > Policies > Centrify Settings > Mac OS X Settings > Security & Privacy Settings > System Preference Settings > Enable System Preferences Pane: Other

Description

Use the group policies in this category to display the items you specify in the Other pane of System Preferences.

Other Preferences Panes

Enable usage of additional preferences panes of System Preferences.

Once this group policy is enabled, it takes effect when users log out and log back in.

System Preferences Mac OS X 10.5 Settings (deprecated)

Path

User Configuration > Policies > Centrify Settings > Mac OS X Settings > Security & Privacy Settings > System Preference Settings > Mac OS X 10.5 Settings

Description

If your environment does not contain Mac OS X 10.5 computers, you can ignore the group policies in this folder.

System Preferences Mac OS X 10.6 Settings (deprecated)

Path

User Configuration > Policies > Centrify Settings > Mac OS X Settings > Security & Privacy Settings > System Preference Settings > Mac OS X 10.6 Settings

Description

If your environment does not contain Mac OS X 10.6 computers, you can ignore the group policies in this folder.

System Preferences Mac OS X 10.7 Settings (deprecated)

Path

User Configuration > Policies > Centrify Settings > Mac OS X Settings > Security & Privacy Settings > System Preference Settings > Mac OS X 10.7 Settings

Description

The Mac OS X 10.7 Settings allow you to configure system preferences policies that apply specifically to Mac OS X 10.7 computers. Because the user interface varies between different versions of Mac OS X, separate policies are provided for each version. See **Legacy Settings**, above, for older versions of Mac OS X.

If your environment does not contain Mac OS X 10.7 computers, you can ignore these settings.

Limit Items Usage in System Preferences (deprecated)

Path

User Configuration > Policies > Centrify Settings > Mac OS X Settings > Security & Privacy Settings > System Preference Settings > Mac OS X 10.7 Settings > Limit items usage in System Preferences

Description

Limit the usage of items in the System Preferences panel.

Once enabled, this group policy takes effect when users log out and log back in.

Enable System Preferences Panes 10.7 (deprecated)

Path

User Configuration > Policies > Centrify Settings > Mac OS X Settings > Security & Privacy Settings > System Preference Settings > Mac OS X 10.7 Settings > Enable System Preferences Panes

Description

Use **Enable built-in System Preferences Panes**, below, to select the items to add to the standard System Preferences panes.

Use **Enable other System Preferences Panes**, below, to add preferences for third-party applications to the Other pane of the System Preferences.

Enable Built-in System Preferences Panes (deprecated)

Path

User Configuration > Policies > Centrify Settings > Mac OS X Settings > Security & Privacy Settings > System Preference Settings > Mac OS X 10.7 Settings > Enable System Preferences Panes > Enable built-in System Preferences Panes

Description

Select items to add to the System Preferences panel.

This policy is only effective if the **Limit items usage in System Preferences** group policy, above, is enabled. Otherwise this group policy is ignored.

Once enabled, this group policy takes effect when users log out and log back in.

Enable Other System Preferences Panes (deprecated)

Path

User Configuration > Policies > Centrify Settings > Mac OS X Settings > Security & Privacy Settings > System Preference Settings > Mac OS X 10.7 Settings > Enable System Preferences Panes > Enable other System Preferences panes

Description

Define a list of additional items to add to the Other pane of the System Preferences panel.

Preference pane applications are actually collections of files inside a directory (called bundles). Inside the `Contents` directory of every preference pane application is the `info.plist` file, and inside that file is the `CFBundleIdentifier` key that identifies the preference pane application. You need to use the value for this key when adding a preference pane application.

Generally, installed third party preference panes can be found in `/System/Library/PreferencePanes`, `/Library/PreferencePanes` or `~/Library/PreferencePanes`.

You can find the `CFBundleIdentifier` key by using the `defaults` command. For example, to find the value for the QuickTime pane, use the following command in a terminal window:

```
defaults read /System/Library/PreferencePanes/QuickTime.prefPane /Contents/info
CFBundleIdentifier
```

which returns:

```
com.apple.preference.quicktime
```

To display the QuickTime icon in the **Other** pane of the System Preferences Panel, enable this policy, then click **Add** and enter `com.apple.preference.quicktime`.

This policy is effective only if the **Limit Items Usage on System Preferences** group policy, below, is enabled. Otherwise, this group policy is ignored.

Once enabled, this group policy takes effect when users log out and log back in.

System Preferences Mac OS X 10.8 Settings (deprecated)

Path

User Configuration > Policies > Centrify Settings > Mac OS X Settings > Security & Privacy Settings > System Preference Settings > Mac OS X 10.8 Settings

Description

The Mac OS X 10.8 Settings allow you to configure system preferences policies that apply specifically to Mac OS X 10.8 computers. Because the user interface varies between different versions of Mac OS X, separate policies are provided for each version. See Legacy Settings for older versions of Mac OS X.

If your environment does not contain Mac OS X 10.8 computers, you can ignore these settings.

Limit Items Usage in System Preferences (deprecated)

Path

User Configuration > Policies > Centrify Settings > Mac OS X Settings > Security & Privacy Settings > System Preference Settings > Mac OS X 10.8 Settings > Limit items usage in System Preferences

Description

Limit the usage of items in the System Preferences panel.

Once enabled, this group policy takes effect when users log out and log back in.

Enable System Preferences Panes 10.8 (deprecated)

Path

User Configuration > Policies > Centrify Settings > Mac OS X Settings > Security & Privacy Settings > System Preference Settings > Mac OS X 10.8 Settings > Enable System Preferences Panes

Description

Use **Enable Built-in System Preferences Panes**, below, to select the items to add to the standard System Preferences panes.

Use **Enable Other System Preferences Panes**, below, to add preferences for third-party applications to the Other pane of the System Preferences.

Enable Built-in System Preferences Panes (deprecated)

Path

User Configuration > Policies > Centrify Settings > Mac OS X Settings > Security & Privacy Settings > System Preference Settings > Mac OS X 10.8 Settings > Enable System Preferences Panes > Enable built-in System Preferences panes

Description

Select items to add to the System Preferences panel.

This policy is effective only if the Limit Items Usage on System Preferences group policy is enabled. Otherwise, this group policy is ignored.

Once enabled, this group policy takes effect when users log out and log back in.

Enable Other System Preferences Panes (deprecated)

Path

User Configuration > Policies > Centrify Settings > Mac OS X Settings > Security & Privacy Settings > System Preference Settings > Mac OS X 10.8 Settings > Enable System Preferences Panes > Enable other System Preferences panes

Description

Define a list of additional items to add to the Other pane of the System Preferences panel.

Preference pane applications are actually collections of files inside a directory (called bundles). Inside the `Contents` directory of every preference pane application is the `info.plist` file, and inside that file is the `CFBundleIdentifier` key that identifies the preference pane application. You need to use the value for this key when adding a preference pane application.

Generally, installed third party preference panes can be found in `/System/Library/PreferencePanes`, `/Library/PreferencePanes`, or `~/Library/PreferencePanes`.

You can find the `CFBundleIdentifier` key by using the `defaults` command. For example, to find the value for the QuickTime pane, use the following command in a terminal window:

```
defaults read /System/Library/PreferencePanes/QuickTime.prefPane /Contents/info
CFBundleIdentifier
```

which returns:

```
com.apple.preference.quicktime
```

To display the QuickTime icon in the **Other** pane of the System Preferences Panel, enable this policy, then click **Add** and enter `com.apple.preference.quicktime`.

This policy is effective only if the **Limit Items Usage on System Preferences** group policy, below, is enabled. Otherwise, this group policy is ignored.

Once enabled, this group policy takes effect when users log out and log back in.

System Preferences Mac OS X 10.9 Settings (deprecated)

Path

User Configuration > Policies > Centrify Settings > Mac OS X Settings > Security & Privacy Settings > System Preference Settings > Mac OS X 10.9 Settings

Description

The Mac OS X 10.9 Settings allow you to configure system preferences policies that apply specifically to Mac OS X 10.9 computers. Because the user interface varies between different versions of Mac OS X, separate policies are provided for each version. See **Legacy Settings**, above, for older versions of Mac OS X.

If your environment does not contain Mac OS X 10.9 computers, you can ignore these settings.

Limit Items Usage in System Preferences (deprecated)

Path

User Configuration > Policies > Centrify Settings > Mac OS X Settings > Security & Privacy Settings > System Preference Settings > Mac OS X 10.9 Settings > Limit items usage in System Preferences

Description

Limit the usage of items in the System Preferences panel.

Once enabled, this group policy takes effect when users log out and log back in.

Enable Built-in System Preferences Panes (deprecated)

Path

User Configuration > Policies > Centrify Settings > Mac OS X Settings > Security & Privacy Settings > System Preference Settings > Mac OS X 10.9 Settings > Enable System Preferences Panes > Enable built-in System Preferences panes

Description

Select items to add to the System Preferences panel.

This policy is effective only if the **Limit Items Usage on System Preferences** group policy, below, is enabled. Otherwise, this group policy is ignored.

Once enabled, this group policy takes effect when users log out and log back in.

Enable Other System Preferences Panes (deprecated)

Path

User Configuration > Policies > Centrify Settings > Mac OS X Settings > Security & Privacy Settings > System Preference Settings > Mac OS X 10.9 Settings > Enable System Preferences Panes > Enable other System Preferences panes

Description

Define a list of additional items to add to the Other pane of the System Preferences panel.

Preference pane applications are actually collections of files inside a directory (called bundles). Inside the `Contents` directory of every preference pane application is the `info.plist` file, and inside that file is the `CFBundleIdentifier` key that identifies the preference pane application. You need to use the value for this key when adding a preference pane application.

Generally, installed third party preference panes can be found in `/System/Library/PreferencePanes`, `/Library/PreferencePanes` or `~/Library/PreferencePanes`.

You can find the `CFBundleIdentifier` key by using the `defaults` command. For example, to find the value for the QuickTime pane, use the following command in a terminal window:

```
defaults read /System/Library/PreferencePanes/QuickTime.prefPane /Contents/info
CFBundleIdentifier
```

which returns:

```
com.apple.preference.quicktime
```

To display the QuickTime icon in the **Other** pane of the System Preferences Panel, enable this policy, then click **Add** and enter com.apple.preference.quicktime.

This policy is effective only if the **Limit Items Usage on System Preferences** group policy, below, is enabled. Otherwise, this group policy is ignored.

Once enabled, this group policy takes effect when users log out and log back in.

System Preferences Mac OS X 10.10 or Above Settings

Path

User Configuration > Policies > Centrify Settings > Mac OS X Settings > Security & Privacy Settings > System Preference Settings > Mac OS X 10.10 Settings

Description

The Mac OS X 10. 10 or above Settings allow you to configure system preferences policies that apply specifically to Mac OS X 10.10 and above computers. Because the user interface varies between different versions of Mac OS X, separate policies are provided for each version. See **Legacy Settings**, above, for other versions of Mac OS X.

If your environment does not contain Mac OS X 10.10 or above computers, you can ignore these settings.

Limit Items Usage on System Preferences

Path

User Configuration > Policies > Centrify Settings > Mac OS X Settings > Security & Privacy Settings > System Preference Settings > Mac OS X 10.10 Settings > Limit items usage on System Preferences

Description

Limit the usage of items in the System Preferences panel.

Once enabled, this group policy takes effect when users log out and log back in.

Enable System Preferences Panes 10.10

Path

User Configuration > Policies > Centrify Settings > Mac OS X Settings > Security & Privacy Settings > System Preference Settings > Mac OS X 10.10 Settings > Enable System Preferences Panes

Description

Use **Enable other System Preferences Panes**, below, to add preferences for third-party applications to the Other pane of the System Preferences.

Enable Built-in System Preferences Panes

Path

User Configuration > Policies > Centrify Settings > Mac OS X Settings > Security & Privacy Settings > System Preference Settings > Mac OS X 10.10 Settings > Enable System Preferences Panes > Enable built-in System Preferences panes

Description

Enable this group policy to enable the built-in System Preferences panes.

Enable or disable usage of items in the built-in System Preferences panes by checking or unchecking boxes corresponding to the items.

This policy is effective only if the **Limit Items Usage on System Preferences** group policy, above, is enabled. Otherwise, this group policy is ignored.

Once enabled, this group policy takes effect when users log out and log back in.

Enable Other System Preferences Panes

Path

User Configuration > Policies > Centrify Settings > Mac OS X Settings > Security & Privacy Settings > System Preference Settings > Mac OS X 10.10 Settings > Enable System Preferences Panes > Enable other System Preferences panes

Description

Define a list of additional items to add to the Other pane of the System Preferences panel.

Preference pane applications are actually collections of files inside a directory (called bundles). Inside the `Contents` directory of every preference pane application is the `info.plist` file, and inside that file is the `CFBundleIdentifier` key that identifies the preference pane application. You need to use the value for this key when adding a preference pane application.

Generally, installed third party preference panes can be found in `/System/Library/PreferencePanes`, `/Library/PreferencePanes` or `~/Library/PreferencePanes`.

You can find the `CFBundleIdentifier` key by using the `defaults` command. For example, to find the value for the QuickTime pane, use the following command in a terminal window:

```
defaults read /System/Library/PreferencePanes/QuickTime.prefPane /Contents/info
CFBundleIdentifier
```

which returns:

```
com.apple.preference.quicktime
```

To display the QuickTime icon in the **Other** pane of the System Preferences Panel, enable this policy, then click **Add** and enter com.apple.preference.quicktime.

This policy is effective only if the **Limit Items Usage on System Preferences** group policy, above, is enabled. Otherwise, this group policy is ignored.

Once enabled, this group policy takes effect when users log out and log back in.

Configuring a Mac Computer for Smart Card Login

This section explains how to set up smart card login for a Mac computer:

Understanding Smart Card Login

Smart cards provide an enhanced level of security authentication for logging into an Active Directory domain. To configure a smart card for use on a Mac computer that is running the DirectControl agent, requires that you have already set up a smart card for use in a Windows domain. You do not need to add any smart card infrastructure to the Mac computer, other than a smart card reader and a provisioned smart card.

If you have set up smart card login for Windows clients in a domain, you can use Access Manager to configure smart card login for Mac clients joined to the same domain. If you have provisioned a smart card for use on a Windows computer once you configure smart card support for a Mac computer, you can use the same smart card to log in to a Mac computer.

Supported Smart Card Types

Delinea Smart Card Support for MacOS is based on the MacOS modern native framework, CryptoTokenKit. TokenD is no longer supported.

For macOS 10.15 and later, Delinea supports personal identity verification (PIV) smart cards, USB CCID class-compliant readers, and hard tokens that support the PIV standard.

Configuring Smart Card Login

Delinea provides group policies, configuration options, and account options to perform the smart card configuration tasks described below.

Note: Before configuring smart card login, refer to the next section, **Verifying Prerequisites for Configuring Smart Card Login** to ensure your environment meets all the prerequisites.

Verifying Prerequisites for Configuring Smart Card Login

- Make sure that your smart card is supported by MacOS.

  MacOS 10.15 and later supports personal identity verification (PIV) smart cards, USB CCID class-compliant readers, and hard tokens that support the PIV standard.

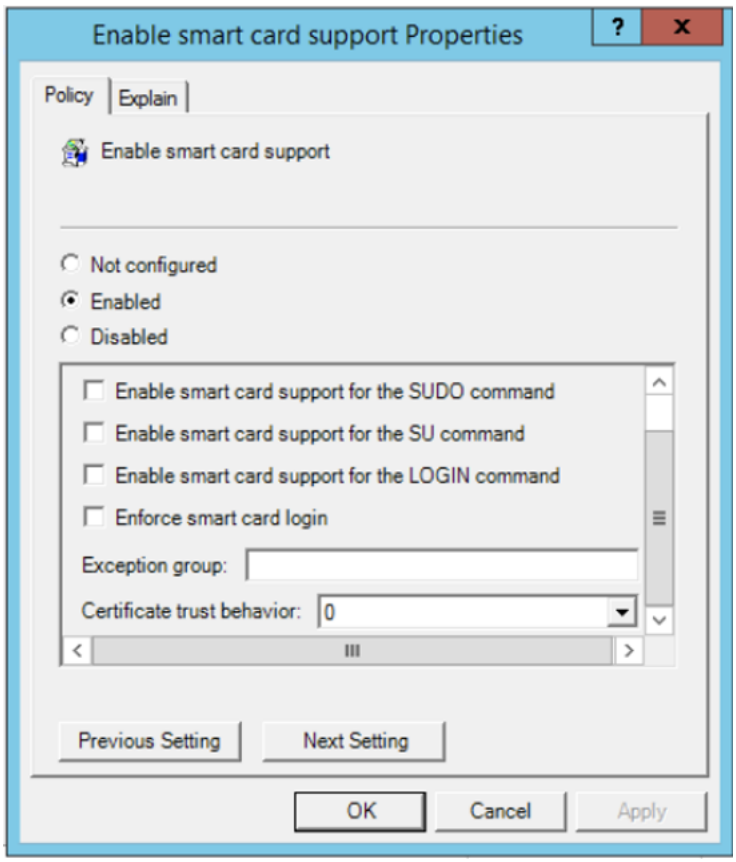
  - Provision a smart card with an NT principal name and PIN.
  - Verify that the Active Directory user's UPN matches the UPN on the smart card.
  - Make sure that there are at least two certificates in your smart card; these two certificates are for two different purposes: "Signature and smartcard logon" and "Encryption." MacOS will use the certificate which purpose is "Signature and smartcard logon" to logon, and use the certificate which purpose is "Encryption" to encrypt and decrypt the user's Keychain automatically. If there is no certificate which is for "Encryption", the user will need to input the Keychain password every time when that they log in.
- Make sure that your smart card is able to log in to a Windows computer.

  If a user is able to log in to a Windows computer with a smart card, and you have a card reader and a fully-provisioned card for the Mac computer, the user should be able to log in to the Mac computer once you configure it for smart card support.

Enabling Smart Card Support

To enable smart card support for logging on

1. Make sure that you have configured the Delinea Agent to have full disk access.
2. Create or edit an existing Group Policy Object linked to a site, domain, or OU that includes Mac computers.
3. In the Group Policy Management Editor, expand **Computer Configuration > Policies > Centrify Settings > Mac OS X Settings > Security & Privacy**, then double-click **Enable smart card support**.



4. Select **Enabled** to enable smart card support.
5. Select any of the following smart card options:
   - **Enable smart card support for the SUDO command**: When executing the SUDO command, the smart card user can authenticate by entering their smart card PIN.
   - **Enable smart card support for the SU command**: When executing the SU command, the smart card user can authenticate by entering their smart card PIN.
   - **Enable smart card support for the LOGIN command**: When executing the LOGIN command, the smart card user can authenticate by entering their smart card PIN.
   - **Enforce smart card login**: Users can only log in to the Mac computer by way of smart card login.
   - **Exception group**: Any users who belong to this group can always log in to the Mac computer with user name and password (no smart card required). In general, we recommend that you set an exception group, such as admins, when you select the option to enforce smart card login.
   - **Certificate trust behavior**: You can select one of these numbers to set smart card certificate behavior. The numbers mean the following:
     - 0: Smart card certificate trust isn't required.
     - 1: Smart card certificate and certificate chain must be trusted.

- 2: Certificate and certificate chain must be trusted and not receive a revoked status.
- 3: Certificate and certificate chain must be trusted and revocation status is returned valid.

6. Because smart card login is not password-based, **do not** enable the "Enable Keychain synchronization" group policy: Computer Configuration > Policies > Centrify Settings > Mac OS X Settings > Security & Privacy > Enable Keychain synchronization
7. If FileVault is enabled on your Mac, please enable the "Disable automatic login" group policy: Computer Configuration > Policies > Centrify Settings > Mac OS X Settings > Security & Privacy > FileVault2 > Disable automatic login.

   The policy takes effect dynamically at the next group policy refresh interval or after you run adgpupdate.

Verifying Smart Card Configuration

After enabling smart card support as described above in Configuring Smart Card Login, do the following to verify that a smart card is working:

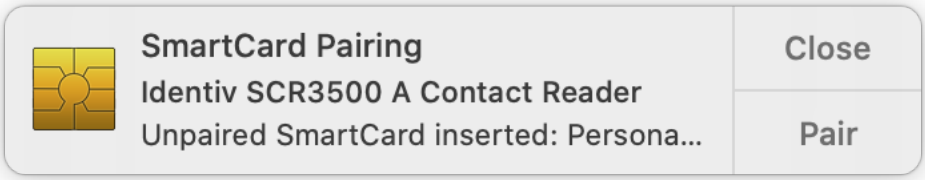
1. Insert the smart card into the reader.
2. Open the Terminal.app and run the following command:

   ```
   % sc_auth identities
   ```

   You should see that the smart card has paired to the Active Directory user. For example:

```
SmartCard: com.apple.pivtoken:00000000000000000000000000000000
Paired identities which are used for authentication:
9800A35AD2A41AEFB03CF431B76BA194E22F48EE    pivau1 - Certificate For PIV Authentication (PIV
AU 1)
```

Note: You never need to pair your smart card manually. If you see the following SmartCard Pairing dialog, that means that the smart card support is not ready. Please re-check the smart card support GP and then execute the command adgpupdate.



Enabling the Screen Saver for Smart Card removal

Currently, we don't have a group policy to enable the screen saver when the smart card is removed. Please use the group policy entitled "Specify multiple login scripts" to deploy the following script:

```
#!/bin/bash
user_name=ls -l /dev/console | cut -d " " -f 4
defaults write /Users/$user_name/Library/Preferences/com.apple.screensaver tokenRemovalAction
-int 1
chown $user_name:staff /Users/$user_name/Library/Preferences/com.apple.screensaver.plist
exit 0
```

The script sets the Mac to start the screen saver automatically when the smart card is removed.

Disabling Smart Card Support

To disable smart card support:

1. Edit the Group Policy Object linked to a site, domain, or OU that includes Mac computers, expand **Computer Configuration > Policies > Centrify Settings > Mac OS X Settings > Security & Privacy**, then double-click **Enable smart card support**.
2. Select **Disabled** and click **OK**.

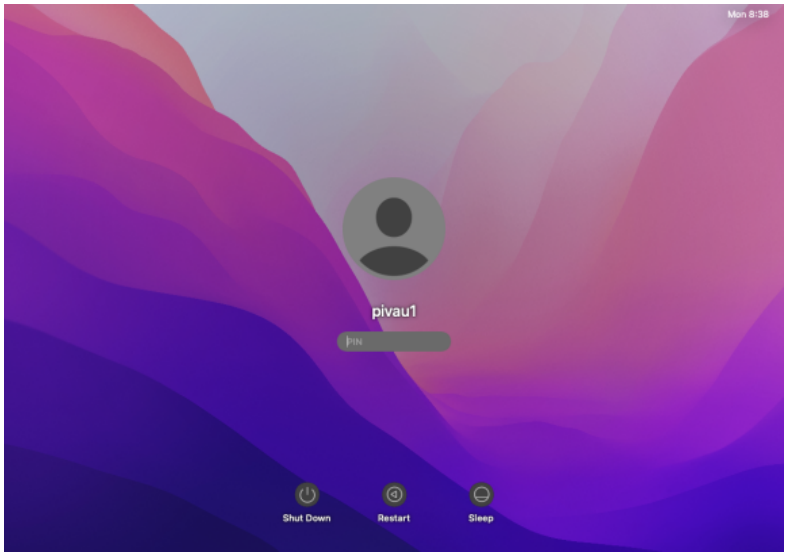
Using Smart Card Login

When a user inserts a smart card into the card reader attached to a Mac computer that is waiting for login, the login screen is replaced by a smart card enabled login screen.

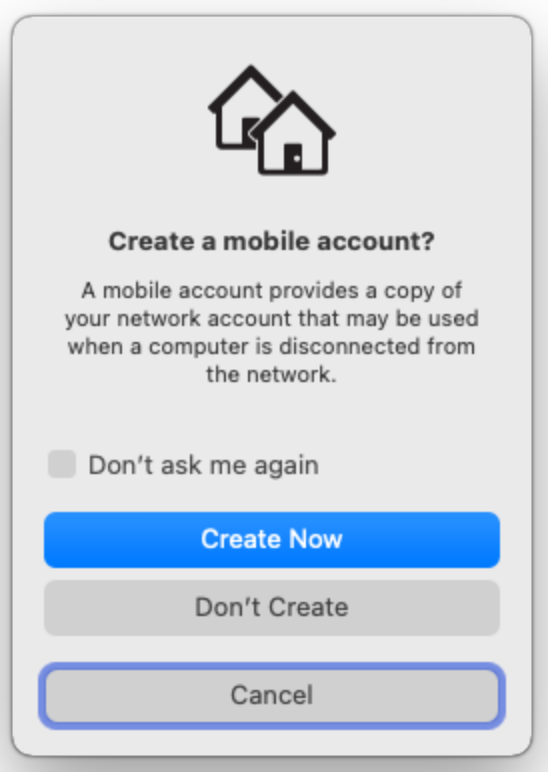
To log in with a smart card:

1. Insert the smart card into the smart card reader.

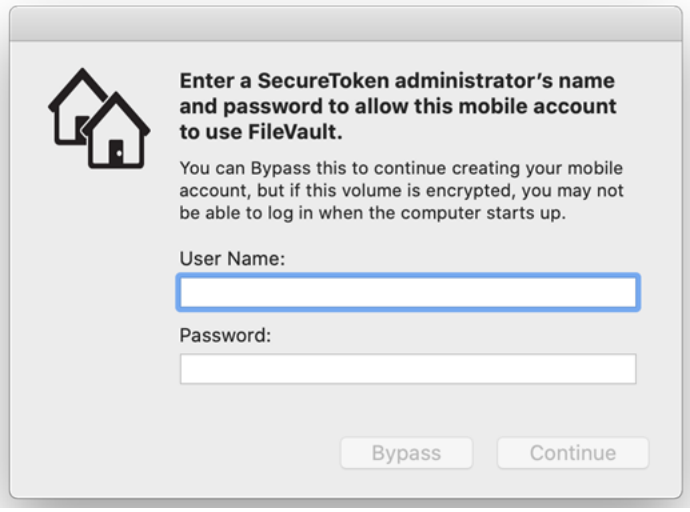
   A login screen displays, prompting you to enter your PIN.



2. If the "Configure mobile account creation" group policy is enabled, you are prompted to create a mobile account.



If the **Bypass the SecureToken dialog** is not enabled, after creating the mobile account, you are prompted to authenticate the SecureToken.



3. The system will then prompt you to set a password for Keychain.

   The password can be the same as or different than your Active Directory password. For security reasons, the password here should not be the same as your smart card PIN.

Troubleshooting Smart Card Login

If you have problems with smart card logon, Access Manager provides a command-line tool, `sctool`, which you can run to configure smart card logon, as well as to provide diagnostic information. See the `sctool` man page.

Additional smart card diagnostic procedures are provided in Diagnosing Smart Card Login Problems.

Other Functions of Smart Card Support on MacOS

MacOS 10.15 includes built-in support for the following capabilities:

- Authentication: LoginWindow, PKINIT, SSH, Screen saver, Safari, authorization dialogs, and in third-party apps supporting CTK
- Signing: Mail and third-party apps supporting CTK
- Encryption: Mail, Keychain Access, and third-party apps supporting CTK

For more information, please see https://support.apple.com/guide/deployment-reference-macos/intro-to-smart-card-integration-apd1fa5245b2/1/web/1.0.

Known Issues of Using Smart Cards with MacOS

Due to a limitation of MacOS, a smart card user cannot get the User Group Policy automatically. The Computer Group Policy works normally. The workaround is to run the following commands after logging in with a smart card:

```
% sctool -k
% adgpupdate
```

After you run the above commands, log out and log back in. Most User Group Policy should work normally.

Troubleshooting Tips

This section provides troubleshooting tips for administrators using the Delinea DirectControl Agent for Mac.

The following topics are covered:

Using Common Account Management Commands

Most UNIX-based platforms store account information in the local /etc/passwd file, and use commands such as getent command to query that information. On Mac computers, however, you would typically use the Directory Service application to manage local accounts and retrieve user information. For troubleshooting purposes, therefore, you should be familiar with the commands to use for retrieving information about Active Directory users and groups.

The following table describes several common Directory Service Command Line (dscl) commands that you may find useful.

Use this command	To do this
`dscl /Search -list /Users`	List all of the users in the Directory Service and in Active Directory for the zone.
`dscl /CentrifyDC -list /Users`	List only the Active Directory users enabled for the zone.

`dscl /CentrifyDC -read /Users/username`	Display detailed information about the specified Active Directory *username*.
`dscl /Search -list /Groups`	List all of the groups in the Directory Service and in Active Directory for the zone.
`dscl /CentrifyDC -list /Groups`	List only the Active Directory groups enabled for the zone.
`dscl /CentrifyDC -read /Groups/groupname`	Display detailed information about the specified Active Directory *groupname*.

To get detailed information for all users or groups recognized on the Mac computer, you can use the following commands:

```
lookupd -q user -a name
lookupd -q group -a name
```

To get detailed information for a specific user or group, you can use the following commands:

```
lookupd -q user -a name username
lookupd -q group -a name groupname
```

To clear the Directory Service cache, you can use the following command:

```
lookupd -flushcache
```

To completely clear the cache of Active Directory login credentials, you should also run the `adflush command:

```
adflush
```

To retrieve Mac OS version and build information that `uname -a` does not provide, you can run the following command:

```
/usr/bin/sw_vers
```

Viewing the Agent Version on the Macs Joined to Active Directory

You can use the Active Directory module for Windows PowerShell to view the version of the Delinea DirectControl Agent for Mac on the Macs joined to your AD domain. This is useful to verify that all Macs joined to your AD have an appropriate version of the Delinea DirectControl Agent for Mac to avoid compatibility issues with OS updates.

Install the Active Directory Module for Windows PowerShell

The Active Directory module for Windows PowerShell is already installed on domain controllers. If you are using a member server, you will have to install it.

To install the Active Directory module for Windows PowerShell

Open an elevated PowerShell session on a Windows server in the domain and run the following command:

```
Add-WindowsFeature RSAT-AD-PowerShell
```

When the installation finishes it returns the following:

```
PS C:\Windows\system32>
PS C:\Windows\system32>
PS C:\Windows\system32> Add-WindowsFeature RSAT-AD-PowerShell

Success Restart Needed Exit Code      Feature Result
------- -------------- ---------      --------------
True    No             Success        {Active Directory module for Windows Power...
```

Once installed, on Windows Server 2012 and 2012 R2 the module automatically loads when you use one of its cmdlets; you do not need to import it.

Show PowerShell Output of Agent Versions for AD-Joined Computers

If you have a small environment, or just want to see a sample of the information that will be in the report, run the following from a Windows server with the AD PowerShell module installed:

```
Get-ADComputer -Filter * -Properties OperatingSystem,OperatingSystemServicePack | Format-Table Name,OperatingSystem,OperatingSystemServicePack -wrap -auto
```

For example:

```
PS C:\> Get-ADComputer -Filter * -Properties OperatingSystem,OperatingSystemServicePack | Format-Table Name,OperatingSystem,OperatingSystemServicePack -wrap -auto

Name            OperatingSystem                OperatingSystemServicePack
----            ---------------                --------------------------
DC1             Windows Server 2012 R2 Standard
WIN-10          Windows 10 Pro
MEMBER2         Windows Server 2012 R2 Standard
MEMBER1         Windows Server 2012 R2 Standard
WIN-7           Windows 7 Professional         Service Pack 1
centos-6        CentOS                         CentrifyDC 5.4.0-183:Z:CDC
mac2            OS X                           CentrifyDC 5.4.0-242:W:CDC
adam-mini       OS X                           CentrifyDC 5.4.2-668:W:CDC
rauns-macbook-pro OS X                         CentrifyDC 5.4.2-830:W:CDC

PS C:\>
```

The report includes all AD-joined computers in the domain. The example above shows a mix of Windows, Linux, and Mac computers. Where `OperatingSystemServicePack` is empty, it means there is no Service Pack installed (Windows computers), or there is no DirectControl agent installed (Mac or Linux/Unix).

In most cases there are too many computers for the PowerShell output to be easily readable. In these cases, refer to the next section, **Export the Report of Agent Versions to a CSV File**.

Export the Report of Agent Versions to a CSV File

You can export a report of Delinea DirectControl Agent for Mac versions on AD-joined computers to a CSV file for easier manipulation by running the following:

```
Get-ADComputer -Filter * -Properties OperatingSystem,OperatingSystemServicePack | Select-Object Name,OperatingSystem,OperatingSystemServicePack | Export-CSV CDCVersion.csv -NoTypeInformation -Encoding UTF8
```

In this example, PowerShell exports the data described above in **Show PowerShell Output of Agent Versions for AD-joined Computers** to a CSV file named `CDCVersion.csv` in the current directory. You can then open that CSV file using a spreadsheet application such as Excel to more easily analyze the data.

Enabling Logging for the Delinea DirectControl Agent for Mac

The Delinea DirectControl Agent for Mac installation includes some basic diagnostic tools and a logging mechanism to help you trace the source of problems if they occur. These diagnostic tools and log files allow you to periodically check your environment and view information about the agent operation, your Active Directory connections, and the configuration settings for individual computers.

In most cases, logging is not enabled by default for performance reasons. Once enabled, however, log files provide a detailed record of Delinea DirectControl Agent for Mac activity and can be used to analyze the behavior of Delinea Management Services and communication with Active Directory to locate points of failure.

For performance and security reasons, you should only enable agent logging when necessary, for example, when requested to do so by Delinea Corporation Technical Support, and for short periods of time to diagnose a problem. Keep in mind that sensitive information may be written to this file and you should evaluate the contents of the file before giving others access to it.

You can enable logging either by using the `cdcdebug` command or the Delinea for Mac Diagnostic Tool application.

To enable logging with the `cdcdebug` command:

1. Log in to the Mac as Local Admin and open the Terminal.
2. Run the following commands to clear and then enable the Delinea DirectControl Agent for Mac log file:

   ```
   % sudo /usr/local/share/centrifydc/bin/cdcdebug clear
   % sudo /usr/local/share/centrifydc/bin/cdcdebug on
   ```
3. Record the start time point:

   ```
   % date +%s
   ```

   For example: the output is 1610614011, please remember this output, it is the start time point.
4. Log out of the local admin user account.
5. Reproduce the issue: try to log in as the affected Active Directory user. Let it fail.
6. Log back in as Local Admin and open the Terminal again.
7. Record the end time point:

   ```
   % date +%s
   ```

   For example: the output is 1610614043, please remember this output, it is the end time point)
8. Enter the following commands to collect the Delinea DirectControl Agent for Mac log file:

   ```
   % sudo /usr/local/share/centrifydc/bin/cdcdebug -f pack [affected_AD_user_name] [start_time_point] [end_time_point]
   % adquery user -A [affected_AD_user_name] > /tmp/adquery.log
   ```
9. Send us the following files for analysis:

   ```
   /var/centrify/tmp/cdcdebug.tar.gz
   /tmp/adquery.log
   ```
10. Disable the Delinea DirectControl Agent for Mac log:

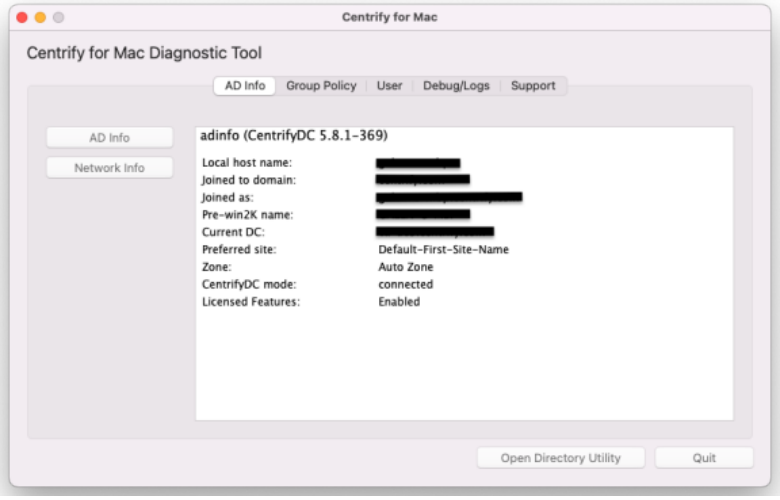
    ```
    % sudo /usr/local/share/centrifydc/bin/cdcdebug off
    ```

To enable logging with the Delinea for Mac Diagnostic Tool:

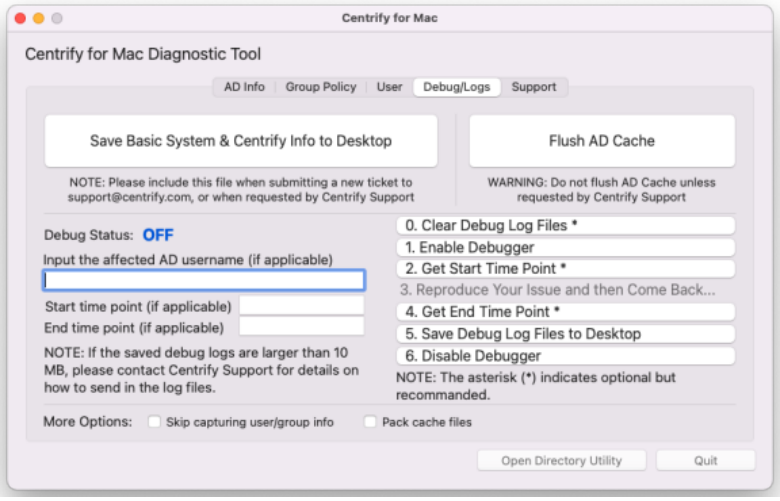
1. Log in to the Mac as Local Admin and open the application MacDiagnosticTool.app.

   The location of this app is “/Library/Application Support/Centrify/MacDiagnosticTool.app.” You can run the following command to open it:

   ```
   % open /Library/Application Support/Centrify/MacDiagnosticTool.app
   ```

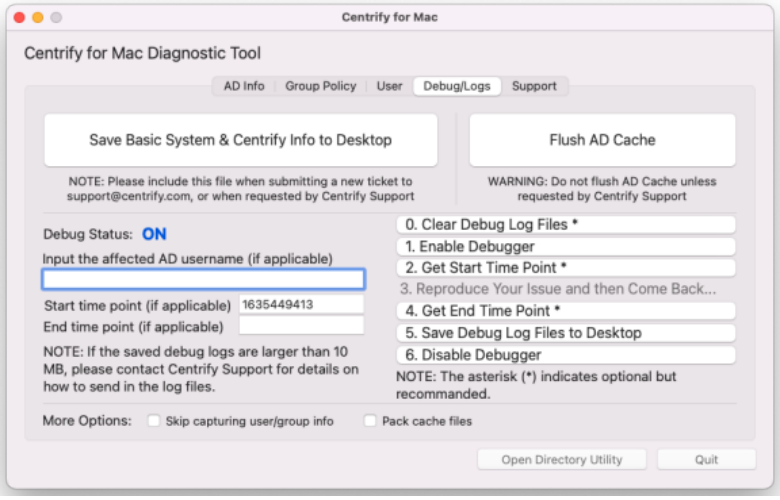


2. Click the **Debug/Logs** tab.

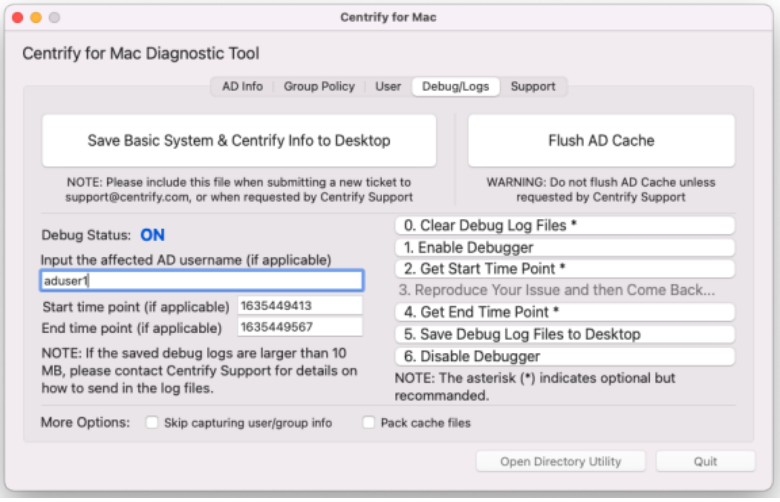


3. Click **0. Clear Debug Log Files**.
4. Click **1. Enable Debugger**.
5. Click **2. Get Start Time Point**.

> **Note:** You do not need to remember the start time point; it will be saved automatically.

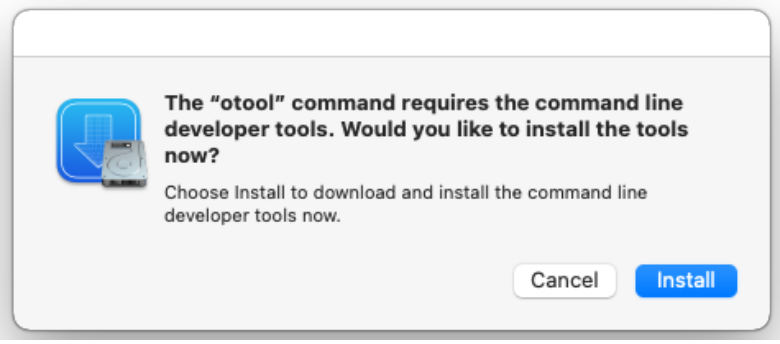


6. Click **Quit** to close the application.
7. Log out of the Local Admin account.
8. Reproduce the issue: try to log in as the affected Active Directory user. Let it fail.
9. Log back in as Local Admin and open the application MacDiagnosticTool.app again.
10. Click **4. Get End Time Point** and enter input the affected Active Directory user name.



11. Click **5. Save Debug Log Files to Desktop**, the tool will start to collect agent log files.

> **Note:** You might see a message display about installing the “otool” command; you can select **Cancel** or **Install**; either choice works.



The log file "CENTRIFY_FULL_LOG_PACK.zip" will be on the Desktop. Send the file to Delinea Technical Support for analysis.

12. Click **6. Disable Debugger**, then click **Quit** to close the application.

Enabling Logging for the Mac Directory Service

In addition to enabling logging for the agent, you may find it necessary to enable logging for the Open Directory Service.

To create a log file for the Open Directory Service:

1. Log in as or switch to the `root` or `admin` user.
2. Run the following command:

```
odutil set log debug
```

After running this command, you can find the resulting log files at: `/var/log/opendirectoryd.log*`. You can then provide both the agent log file and the Directory Service log file to Delinea Support if you need assistance troubleshooting issues.

Using the Agent on a Dual-Boot System

If you are using a dual-boot system, and the computer name is the same for each version of the operating system, the Delinea DirectControl Agent for Mac(`adclient`) will not launch when you reboot and switch operating systems. The problem is that each operating system sets its own password for `adclient` and the password does not work for the other operating system.

The best way to avoid this problem is to provide a different computer name for each operating system. Because the computer names are different, the password for one operating system is not changed by the other operating system.

If you want to use the same computer name for both operating systems, you can work around the problem, as follows:

1. Leave the domain (`adleave`) before rebooting and switching operating systems.

   Note: You may leave and join the domain after rebooting and switching the operating system. However, you will experience some delay while `adclient` attempts to launch and fails.

2. Reboot with the other operating system.
3. Rejoin the domain (`adjoin`).

Using adgpupdate Appropriately

If `adgpupdate` is run multiple times in succession, it is possible that not all group policies will be applied correctly. To avoid this problem, do not run `adgpupdate` more than once per minute.

Understanding Delays when Logging on the First Time with a New User Account

Depending on the configuration of your startup services, you may find that new users are unable to log on to a computer immediately (within the first 15 to 30 seconds) after a computer is rebooted.

By default, the Mac login window only requires the `Disks` and `SecurityService` startup services to start successfully to prompt for the user to log in. Authenticating users to Active Directory, however, requires the additional `DirectoryServices` startup service to be available. Starting the `DirectoryServices` startup service causes a 10 to 15 second delay before the `LoginWindow` can successfully authenticate new Active Directory users.

Configuring Single-sign on to Work with Non-Mac Computers

On a Mac computer, the `ssh` client does not forward (delegate) credentials to the server by default. Therefore, when attempting to use ssh from a Mac computer with DirectControl agent installed to a non-Mac computer with DirectControl agent installed, single sign-on (SSO) does not work. To fix this problem, set the configuration parameter, `GSSAPIDelegateCredentials`, to `yes` in the `/etc/ssh_config` file on the Mac computer.

Restricting Login Using FTP

In Active Directory, you can set properties to prevent a user from logging in to other Macintosh computers. However, this restriction will not prevent a user from logging in via FTP to Macintosh computers with the

DirectControl agent installed. It does restrict logging in with `telnet`, `ssh`, `rlogin`, and `rsh`.

Logging on Using Localhost

For many UNIX platforms, you can log on using `localhost` to refer to the local computer; for example:

```
root@localhost
```

This syntax does not work when logging on to a Macintosh computer, whether using the Macintosh UI, or remotely through `ssh` or `FTP`.

Changing the Password for Active Directory Users

In the Mac OS X, the `passwd` command authenticates the user only after you type the user password. Because of this, the `passwd` command does not recognize the user as an Active Directory user until after the password is entered and the password prompts defined for Active Directory users, which are typically set through group policy or by modifying the Delinea configuration file, are not displayed. You can still use the `passwd` or `chpass` command to change the Active Directory password for a user, but you will not see any visual indication that you are modifying an Active Directory account rather than a local user account.

Disabling the Apple Built-in Active Directory Plug-in

Apple provides a built-in Apple Directory plug-in that may interfere with the Delinea DirectControl Agent for Mac installation and operation. Therefore, before installing the agent, disable Apple's built-in Active Directory plug-in. In addition, remove Active Directory from the Authentication and Contacts search paths. If this plug-in is enabled and the Delinea DirectControl Agent for Mac has been installed, disable the plug-in, then reboot the Macintosh computer for reliable operation.

To disable the Apple Directory plug-in and remove Apple Directory from the Authentication and Contacts search paths:

1. On a Mac computer, open the Directory Utility.

   You can find the Directory Utility in one of these folders depending on the operating system that you are running:

   - `/System/Library/CoreServices`
   - `/Applications/Utilities`

2. Click the lock icon and enter credentials to allow you to make changes.
3. Click the **Search Policy** icon.
4. Click the **Authentication** tab, then select Custom path in the **Search** box.

   If Active Directory was previously enabled, Active Directory appears in the Directory Domains box; for example:

   `/Active Directory/All Domains`

5. Select **/Active Directory/All Domains** and click **Remove** – or select the minus - sign). Then click **Apply**.
6. Click the **Contacts** tab, then select Custom path in the **Search** box. If Active Directory was previously enabled, Active Directory shows (in red font) in the Directory Domains box; for example:

   `/Active Directory/All Domains`

7. Select **/Active Directory/All Domains** and click **Remove**. Then click **Apply**.
8. Close the window.
9. If you have already installed the Delinea DirectControl Agent for Mac, reboot the computer.

Showing the Correct Status of the Delinea Plug-in

The Delinea plug-in is automatically added to the list of Apple Directory Utility plug-ins that are used for lookup and authentication. However, if the Apple Directory Utility tool is running when you install the Delinea DirectControl Agent for Mac, or when you join or leave a domain before updating to a new version of the agent, it will incorrectly display the status of the plug-in. For example, it will show the status as disabled, when in fact, the plug-in is enabled.

To avoid this problem, before launching the installer, be certain that the Apple Directory Utility tool is closed.

If the Directory Utility was open during installation, simply close and re-open Directory Utility, then make certain that the Delinea plug-in is enabled.

You may also restart the Delinea plug-in from the command line, as follows:

1. Close the Directory Utility.
2. Open a terminal.
3. Enter the following command:

   ```
   /usr/local/share/centrifydc/bin/dsconfig restart
   ```
4. Open the Directory Utility. The status of Delinea should be enabled.

Resolving VPN Access Issues with Mac OS X 10.7 and Later

Starting with Mac OS X 10.7, `/etc/resolv.conf` is no longer used for domain controller name resolution. Therefore, some VPN programs no longer update DNS server information in `/etc/resolv.conf` when signing on. On computers running Mac OS X 10.7 and later, this can result in the computer not being able to connect to a domain controller through a VPN.

To resolve this issue, explicitly specify in centrifydc.conf the location of DNS servers that are used to resolve domain controller names:

1. Open `/etc/centrifydc/centrifydc.conf` for editing.
2. Specify the IP addresses of DNS servers in the `dns.servers` parameter (if the parameter does not exist yet, create it now):
   ```
   dns.servers: x.x.x.x y.y.y.y
   ```

   where `x.x.x.x y.y.y.y` are the IP addresses of the DNS servers to use. This example shows two IP addresses; note that each IP address is separated by a space.
3. Save your changes to `centrifydc.conf`.
4. Restart the agent for the changes to take effect:

   ```
   sudo /usr/local/share/centrifydc/bin/centrifydcrestart
   ```

Diagnosing Smart Card Login Problems

Two general methods for diagnosing smart card log in problems are provided:

- By using the `sctool` utility as described in the sctool man page.
- By performing the diagnostic procedures described in this section.

The following procedures are intended to diagnose multiple causes of smart card log in failure. It is recommended that you retest smart card login at regular intervals (such as after each step) as you perform this procedure.

1. Ensure that macOS built-in PIV token is not disabled.

   ```
   % defaults read /Library/Preferences/com.apple.security.smartcard DisabledTokens
   ```

   It should not exist.

2. Ensure that smart card support is enabled.

   ```
   % sctool -s
   ```

   It should show that smart card support is enabled.

3. Ensure that the smart card can be recognized by MacOS.

   ```
   % sc_auth identities
   ```

   It should show your card and the card has been paired to the Active Directory user.

4. Collect support information.

   ```
   % sctool -S
   ```

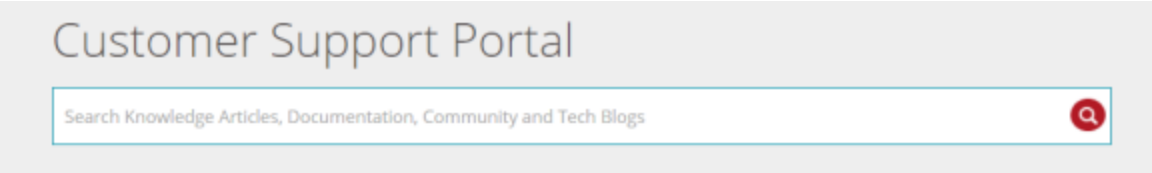
   Send the file `/tmp/sctool.support` to Delinea Support.

Opening a Support Case Online

If you need assistance with troubleshooting an issue, you may need to open a case with Delinea Support. Before opening a new case, Delinea recommends searching the Delinea Support Portal to see if your problem is a known issue or something for which there is a recommended solution.

To search the Delinea Support Portal

1. Open https://www.delinea.com/support/ in a Web browser.
2. Click in the search field and type one or more key words to describe the issue, then click the search icon to view potential answers to your question.

   If your issue is not covered in one of the search results, you should open a case with Delinea Support.

To open a new support case

1. Log in to the Delinea support portal.
2. Click **Manage Cases**, then click **Open a New Support Case**.

   The NEW CASE DETAIL page appears.
3. Enter your case details, then click **Next**.

   Provide as much information as possible about your case, including the operating environment where you encountered the issue, and the version of the Delinea product you are working with.

   A new page appears showing Suggest Knowledge Articles and Technical Resources. You can click **Show More** to see additional resources that might solve your problem.
4. Click **No Thanks, Submit a Case** to open a new case.

Collecting Information for Support Cases

To help ensure your issue gets resolved quickly and efficiently, gather as much information about your working environment as possible. See the information below in these two sections:

- Collecting general information about your environment
- Collecting information specific to login events

Collecting Information Specific to Smart Card Login Failure

Collect the following information prior to opening a support case related to smart card log in failure:

- The smart card type (for example, PIV, CAC, CACNG, and so on), manufacturer, and model.
- A screen image of the smart card and its certificates in Keychain Access.
- The following log files:

  ```
  /tmp/sctool_D.log
  /tmp/adquery.log
  /tmp/tokendfolder.log
  /var/Centrify/tmp/adinfo_support.tar.gz
  ```

To generate these logs, run the following commands while logged in as the local administrator:

```
sctool -D > /tmp/sctool_D.log
adquery user -A username_of_smartcard_user > /tmp/adquery.log
sudo ls -l /System/Library/Security/tokend/ > /tmp/tokendfolder.log
sudo adinfo -t
```

Collecting General Information about Your Environment

Take the following steps to gather information about your working environment before opening a support case.

1. Verify that the DirectControl agent is running on the computer where you have encountered a problem. For example, run the following command:

   ```
   ps aux | grep adclient
   ```

If the adclient process is not running, check whether the watchdog process, cdcwatch, is running:

```
ps aux | grep cdcwatch
```

The cdcwatch process is used to restart adclient if it stops unexpectedly.

Note: The commands in the following three steps must be run as root or with the sudo command.

2. Enable logging for the DirectControl agent; for example:

```
sudo /usr/local/share/centrifydc/bin/cdcdebug on
```

Note: Login events are captured in `/var/log/centrifydc-login.log` by default. Turning on cdcdebug captures login events in `/var/log/centrifydc.log`.

3. Create a log file for the Mac Directory Service. For example:

- To enable logging for `opendirectoryd`:

```
odutil set log debug
```

- To disable logging for `opendirectoryd` when sufficient log information is collected:

```
odutil set log default
```

4. Duplicate the steps that led to the problem you want to report. For example, if an Active Directory user can't log in to a managed system, attempt to log the user in and confirm that the attempt fails. Be sure to make note of key information such as the user name or group name being used, so that Delinea Support can identify problem accounts more quickly.
5. Verify that log file `/var/log/centrifydc.log` or `/var/adm/syslog/centrifydc.log` exists and contains data.
6. Run the `cdcdebug` command to generate logs that describe the domain and current environment; for example:

```
sudo /usr/local/share/centrifydc/bin/cdcdebug -f pack username
```

The following log files are created in `/var/centrify/tmp` when you execute the `cdcdebug` command:

- `adinfo_support.tar.gz`
- `adinfo_support.txt`
- `cdcdebug.tar.gz`
- `dump_cache_error.log`
- `stacktrace.txt`

7. If there is a core dump during or related to the problem, save the core file and inform Delinea Support about it. Delinea Support may ask for the file to be uploaded for review.

If the core dump is caused by a Delinea process or command, such as `adclient` or `adinfo`, open the `/etc/centrifydc/centrifydc.conf` file and change the `adclient.dumpcore` parameter from `never` to `always` and restart the agent:

```
sudo /usr/local/share/centrifydc/bin/centrifydcrestart
```

Note: For more information about starting and stopping the agent, see the *Administrator's Guide for Linux and UNIX*.

8. If there is a cache-related issue, Delinea Support may want the contents of the `/var/centrifydc` directory. You should be able to create an archive of the directory, if needed.
9. If there is a DNS, LDAP, or other network issue, Delinea Support may require a network trace. You can use Ethereal to create the network trace from Windows or UNIX. You can also use Netmon on Windows computers.
10. Create an archive (for example, a `.tar` or `.zip` file) that contains all of the log files and diagnostic reports you have generated, and add the archive to your case or send it directly to Delinea Support.
11. Consult with Delinea Support to determine whether to turn off debug logging. If no more information is needed, run the following commands, which must be run as `root` or with `sudo`:

    ```
    odutil set log default
    sudo /usr/local/share/centrifydc/bin/cdcdebug off
    ```

Collecting Information Specific to Login Events

Login events are captured in `/var/log/centrifydc-login.log` by default. If you enable logging for the DirectControl agent by turning on `cdcdebug`, login events are then captured in `/var/log/centrifydc.log`.

The `/var/log/centrifydc-login.log` grows to a maximum size of 50M before it is compressed. When all compressed `centrifydc-login.log` files combined with the current log file exceed 250M, the oldest compressed log is replaced.

Installing and Removing the Agent and Leaving a Domain

This section shows other methods of installing the agent besides the standard method using the package installer (`DMG` file); see Installing the Delinea DirectControl Agent for Mac. It also shows how to remove the agent and how to join and leave a domain.

The following topics are covered:

Installing Using the install.sh Script

This section explains how to install using the `install.sh` script. This method is recommended for experienced UNIX administrators who are familiar with UNIX command-line installations. Otherwise, you should install by using the graphical user interface, which is described in Installing the Delinea DirectControl Agent for Mac.

To install using the `install.sh` command-line program:

> Before launching the installer, be certain that Apple Directory Utility is closed. If it is open while running the installer, it causes the Delinea Directory Access plug-in to show the incorrect status, that is, it shows that the plug-in is disabled when in fact it is enabled.

1. Log on with a valid user account.

   > You are not required to log on as the `root` user on, but you must know the password for the Administrator account to complete the installation.

2. Mount the CD-ROM device using the appropriate command for the local computer's operating environment, if it is not automatically mounted.
3. Change to the appropriate directory on the CD or on the network where the DirectControl agent package is located. For example, change to the `Agent_Mac` directory.
4. Run the `install.sh` script to start the installation of the Delinea software on the local computer's operating environment. For example:

   ```
   sudo ./install.sh
   ```

   Before beginning the installation, the `install.sh` script runs the `ADCheck` utility, which performs a set of operating system, network, and Active Directory checks to verify that the Mac computer meets the system requirements necessary to install the Delinea DirectControl Agent for Mac and join an Active Directory domain.
5. Review the results of the checks performed. If the target computer, DNS environment, and Active Directory configuration pass all checks with no warnings or errors, you should be able to perform a successful installation and join. If you receive errors or warnings, correct them before proceeding with the installation.
6. Follow the prompts displayed to select the services you want to install and the tasks you want to perform. For example, you can choose whether you want to join a domain or restart the local computer automatically at the conclusion of the installation.

When installation is complete, see **Understanding the Directory Structure** below for a description of the directories and files installed for Centrify.

Installing Silently on a Remote Computer

You can install the agent silently on a remote Mac computer in either of these ways:

- By using sudo commands from the command line. If you use this method, no user interaction on the target Mac computer is required. See the section below, **Installing Remotely on a Mac Computer Using sudo Commands**.
- By using Apple Remote Desktop. This method requires that you have Apple Remote Desktop 3 for remote software distribution. See the section below, **Installing Remotely on a Mac Computer Using Apple Remote Desktop**.

  If you use this method to install version 5.1.0 of the agent, the Delinea Join Assistant launches on the target Mac computer after the installation completes, and a user must interact with the Delinea Join Assistant to complete the join process. This limitation exists only in version 5.1.0 of the agent. Earlier versions of the agent (that is, 5.0.x and lower) and later versions (5.1.1 and above) do not have this limitation, and can be installed using Apple Remote Desktop without any user interaction on the target Mac computer.

Installing Remotely on a Mac Computer Using Sudo Commands

Perform the following steps to use `sudo` commands to install the agent remotely on a target Mac computer without requiring any user interaction on the target Mac computer.

To install the agent remotely using sudo commands:

1. Ensure that you have administrator account credentials on the target Mac computer, and that SSH is installed on the target Mac computer.
2. On the computer where the Delinea packages were downloaded (that is, the source computer), use an appropriate file transfer method to push the `CentrifyDC-x.x.x.pkg` file to the target Mac computer.

   For example, perform these steps to transfer files from a PC source computer to the target Mac computer:

   a. On the source computer, ensure that file sharing is enabled, and that the folder containing the Delinea packages is a shared folder.

   b. On the target Mac computer:

      i. Open a new window in the Finder.

      ii. In the sidebar under **Shared**, click **All**.

      iii. Select the source computer.

      iv. Click **Connect As**, type the user name and password for the source computer, and click **Connect**.

   c. The folder that you shared on the source computer appears in the Finder on the target Mac computer. Locate the `CentrifyDC-x.x.x.pkg` file on the source computer and drag it to the location of your choice on the target Mac computer.
3. On the source computer, use a program such as Putty to connect remotely to the target Mac computer through SSH. Log in to the target Mac computer using an account that has local administration privileges, such as the Local Admin account.
4. On the target Mac computer, navigate to the directory where the `.pkg` file was transferred and execute the following command:

   ```
   sudo /usr/sbin/installer -pkg CentrifyDC-x.x.x.pkg -target /
   ```

   When you execute this command, the agent is installed silently on the target Mac computer.

   - If an agent was already installed on the target Mac computer and this was an update of the existing agent, the target Mac computer was already joined to the domain, and you do not need to perform any additional steps.
   - If this was the first installation of the agent on the target Mac computer, you must enable licensed features and join the target Mac computer to a domain as described in Step 5 and Step 6.
5. Execute the following command on the target Mac computer to enable licensed features:

   ```
   sudo adlicense -l
   ```
6. When you join the target Mac computer to a domain, you can choose to join the auto zone or a specified hierarchical zone.

   - Execute the following command on the target Mac computer to join the target Mac computer to a domain and the Auto Zone:

```
sudo /usr/local/sbin/adjoin --user Domain_Admin --container "domain.com/Path/To/OU" --
name computer_name --workstation domain_name.com
```

- Alternatively, execute the following command on the target Mac computer to join the target Mac computer to a domain and a specified hierarchical zone:

```
sudo /usr/local/sbin/adjoin --user Domain_Admin --container "domain.com/Path/To/OU" --
name computer_name --zone zone_namedomain_name.com
```

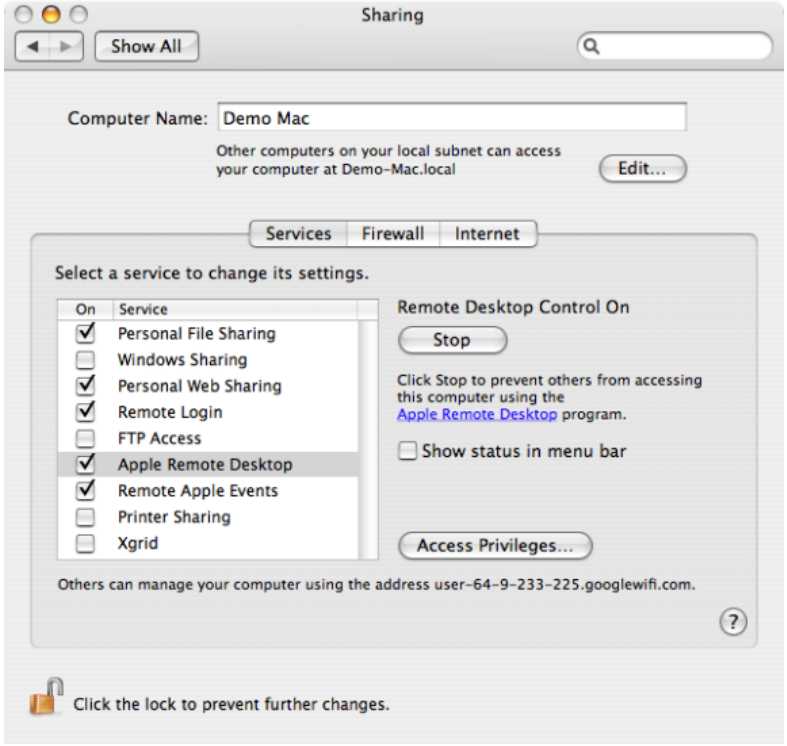
Installing Remotely on a Mac Computer Using Apple Remote Desktop

Perform the following steps to install the agent remotely on a target Mac computer without requiring any user interaction on the target Mac computer.

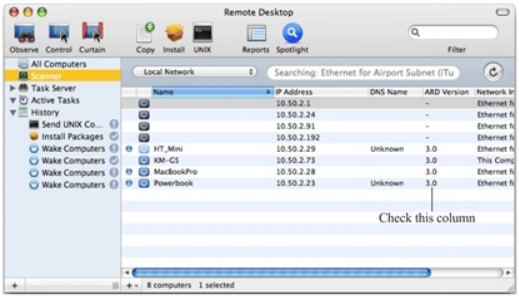
> If you use this method to install version 5.1.0 of the agent, the Delinea Join Assistant launches on the target Mac computer after the installation completes, and a user must interact with the Delinea Join Assistant to complete the join process. For all other versions of the agent, no user interaction on the target Mac computer is required.

To remotely install the DirectControl agent and join a computer to the domain using Apple Remote Desktop 3:

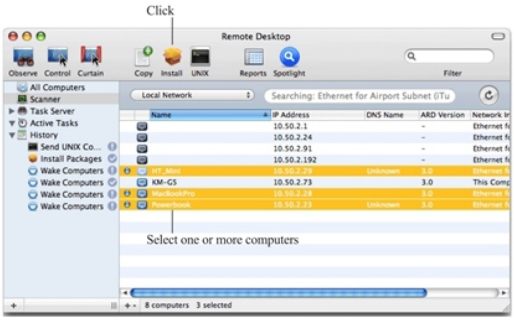
1. Verify that you have an Apple Remote Desktop 3 Admin station and one or more Apple Remote Desktop 3 Clients.
2. Verify that all of the Apple Remote Desktop 3 Client computers where you want to install the DirectControl agent are set to **Allow Remote Desktop** using the Service pane in the Sharing system preference. For example:



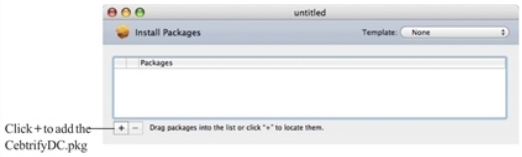
3. Copy the DirectControl agent package, for example `centrifydc-release-macversion-i386.dmg`, to the Apple Remote Desktop 3 Admin computer and verify that you can access the disk image.
4. Open Remote Desktop on the Admin Computer, then click **Scanner** and verify that the Mac computers on which you plan to install Delinea are listed and that ARD Version column displays 3.0 (or later). For example:



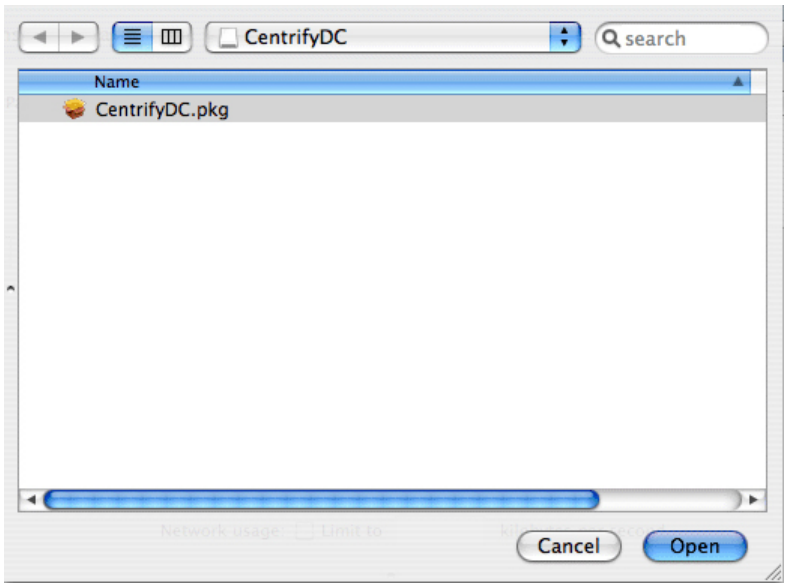
5. Select one or more computers from the list, then click **Install**. For example:



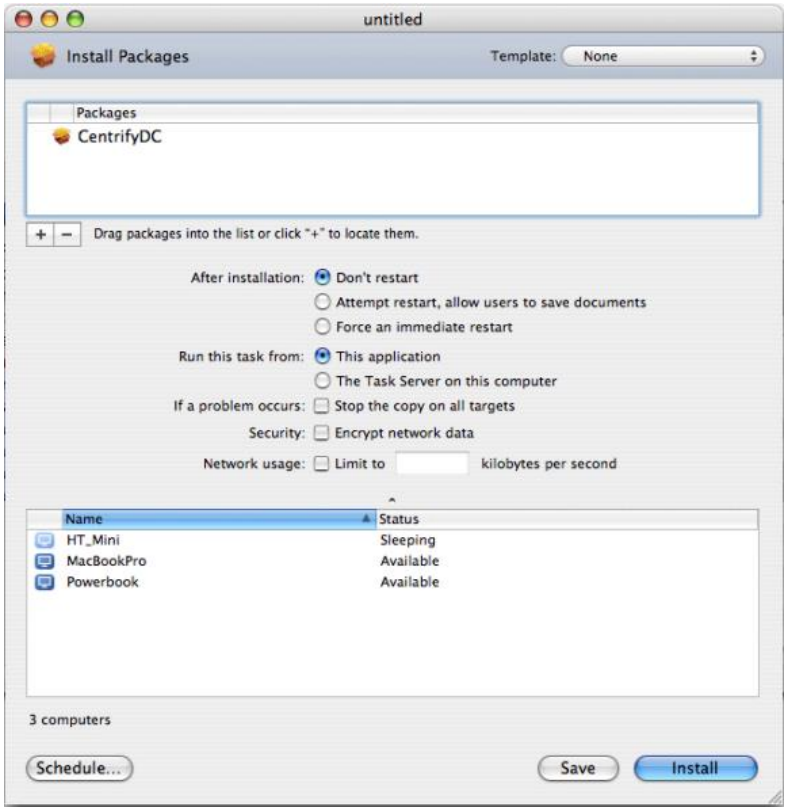
6. In the Install Packages window, click **+** to locate the `CentrifyDC.pkg` in the DirectControl agent disk image. For example:



7. In the DirectControl agent disk image, select the `CentrifyDC.pkg` file and click **Open** to add it to the Install Packages list. For example:



8. In the Install Packages window, click **Install** to install the listed packages, for example:



In most cases, you can use the default settings to install the Delinea DirectControl Agent for Mac. If you want to schedule the installation for another time rather than completing the installation now, click **Schedule**. For more information about the Apple Remote Desktop installation parameters, see Chapter 8 “Administering Client Computers,” in the Apple Remote Desktop Manual.

If you click **Install** the Remote Desktop displays a progress bar and task status for each of the computers selected for the installation.

Understanding the Directory Structure

When you complete the installation, the local computer will be updated with the following directories and files:

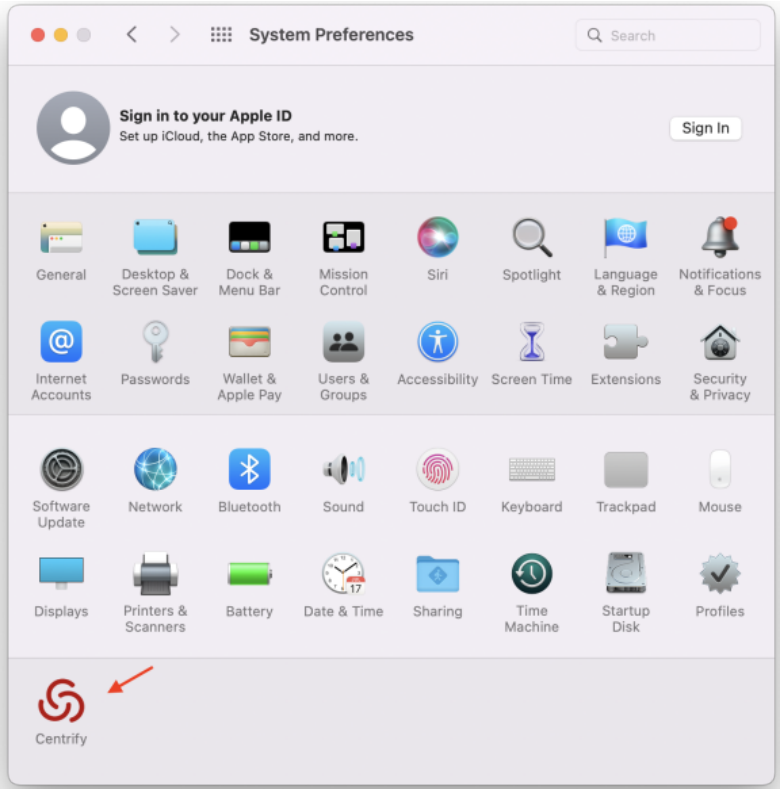
This directory	
/etc/centrifydc	The Delinea DirectControl Agent for Mac configuration file and the Kerberos configuration file.
/usr/local/share/centrifydc	Kerberos-related files and service library files used by the Delinea DirectControl Agent for Mac to enable group policy and authentication and authorization services.
/usr/local/sbin /usr/bin	Command line programs to perform Active Directory tasks, such as join the domain and change a user password.
/var/centrifydc	No files until you join the domain. After you join the domain, several files are created in this directory to record information about the Active Directory domain the computer is joined to, the Active Directory site the computer is part of, and other details.
/System/Library/Frameworks/DirectoryService.framework/Resources/Plugins	The Delinea Directory Service Plugin, `CentrifyDC.dsplug`, that enables you to join or leave the domain using the graphical user interface.

Uninstall from the Delinea System Preferences Pane

The Delinea System Preferences pane is created when you install the Delinea DirectControl Agent for Mac. You can use this pane to uninstall the Delinea DirectControl Agent for Mac. Uninstalling the agent from the Delinea System Preferences pane also leaves the AD domain.

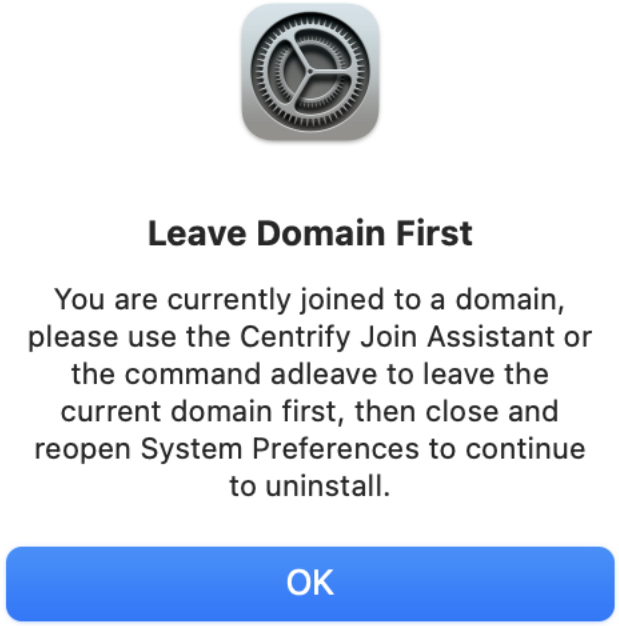
To uninstall the Delinea DirectControl Agent for Mac from the Delinea System Preferences pane

1. Open **System Preferences**, then click **Centrify**.



2. Click **Uninstall**, then click **OK** at the confirmation prompt.

   If you are currently joined to a domain, it will prompt the Leave Domain First dialog. For more information, see **Leaving an Active Directory Domain** below.



3. Enter administrator credentials and click **OK**.

   The uninstall process starts.

4. Click **OK** to quit when you see the window indicating that the Delinea DirectControl Agent for Mac was uninstalled.

Run the uninstall.sh Script

The `uninstall.sh` script is installed by default in the `/usr/local/share/centrifydc/bin` directory on each Centrify-managed system.

To remove the Delinea DirectControl Agent for Mac by running the `uninstall.sh` script

1. Open a Terminal window on the computer where the DirectControl agent is installed. For example, select **Applications > Utilities > Terminal**.
2. Switch to the root user or a user with superuser permissions. For example:

   ```
   su -
   ```

   Password: `root_password`

3. Run the `uninstall.sh` script. For example:

   ```
   /bin/sh /usr/local/share/centrifydc/bin/uninstall.sh
   ```

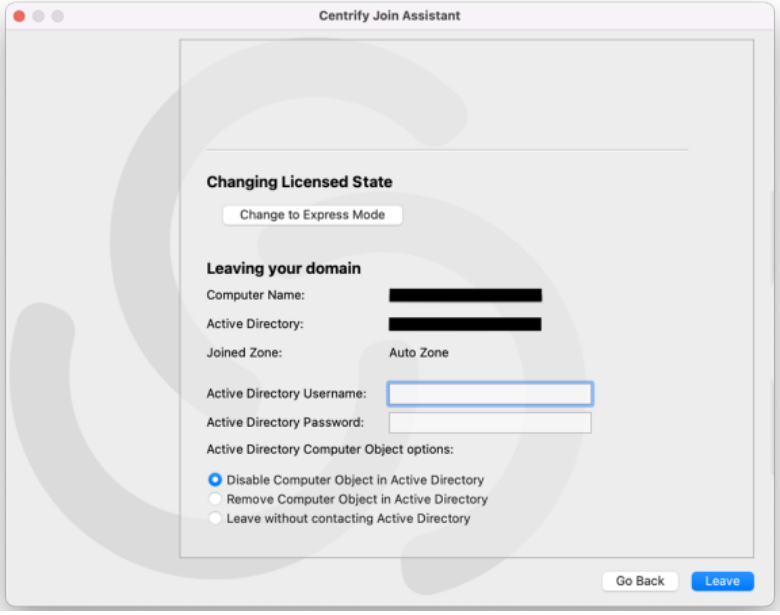
   The `uninstall.sh` script will detect whether the Delinea DirectControl Agent for Mac is currently installed on the local computer and whether the computer is currently joined to a domain. If the computer is not currently joined to a domain, the script will begin removing Delinea files from the local computer.

Leaving an Active Directory Domain

To start the Delinea program for joining or leaving a domain:

1. Click **Applications > Utilities > Delinea**, then double-click **Delinea Join Assistant** to open it.

   Click **Continue** on the Welcome page and the join assistant displays information about the domain to which the computer is connected:



2. Select whether to disable the computer object in Active Directory, remove the computer object from Active Directory, or leave without contacting Active Directory.
   - Disable: Disables the computer object in Active Directory.
   - Remove: Removes the computer object from Active Directory.
   - Leave without contacting Active Directory: This option forces the local computer's settings to their pre-join conditions without contacting Active Directory. The Computer Object will not be removed or disabled in Active Directory.

   Use this option if the Active Directory computer account has been modified or deleted so that the host computer can no longer work with it.
3. Click **Leave** to leave the domain.