Welcome to Centrify Agent, Centrify Identity Service, Mac Edition

Release Notes for the Centrify Agent, Centrify Identity Service, Mac OS Edition, Suite 2017

Centrify Agent, Centrify Identity Service, Mac Edition *Active Directory-based authentication, single sign-on and group policy support for the Macintosh platform.*

Centrify Agent, Centrify Identity Service, Mac Edition is a part of *Centrify software and is protected by U.S. Patent No. 7,591,005, 8,024,360, 8,321,523, 9,015,103 B2, 9,112,846, 9,197,670 and 9,378,391.*

Notice of Discontinuation of Support for Mac OS 10.9.x: Centrify is discontinuing support for Mac OS *10.9.x* in this release of Centrify for Mac.

What's included in this release (in alphabetical order)

- CentrifyDC-5.4.0.dmg– A Mac disk image for Mac OS 10.10.x, 10.11 and 10.12 containing the following:
    - AD Check.app – Graphical application to perform environment checks before installing Centrify on Mac OS 10.10.x, 10.11 and 10.12
    - CentrifyDC-5.4.0-x86_64.pkg – Graphical installer for Intel Macs for Mac OS X Mac OS 10.10.x, 10.11 and 10.12

Supported platforms and system requirements

The Centrify agent in the applicable package can be installed on the following versions of the Mac OS X operating system:

Mac OS X 10.10.x on Intel Macs
Mac OS X Server version 10.10x on Intel Macs
Mac OS X 10.11.x on Intel Macs
Mac OS X Server version 10.11x on Intel Macs
Mac OS X 10.12.x on Intel Macs
Mac OS X Server version 10.12x on Intel Macs

Installing on Macintosh OS 10.12 "Sierra"

If you are running the current release of Centrify, you MUST UPGRADE Centrify BEFORE upgrading your Mac to OS 10.12 Sierra.

If you upgrade to OS X 10.12 Sierra from a 10.8.x or a 10.9.x version, there is a known Apple bug (22735194) that prevents the Centrify daemon from running upon first boot after the update. To resolve this you will need to login as a local administrator and execute the following command:

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

Alternatively, you can upgrade from 10.8.x or 10.9.x to 10.10 and then safely proceed with the update to Sierra.

Follow these steps:

1) Download the Centrify package for Mac OS

2) Upgrade Centrify using this package.

3) Upgrade to Mac OS 10.12.

If you have already upgraded to 10.12 with a previous version of Centrify and can't log in as an Active Directory User, follow these steps:

1) Log into the Mac with your Mac's local administrator account

2) Download the Centrify package for Mac OS

3) Upgrade Centrify to this package.

You should now be able to log in with Active Directory credentials

Note:

When upgrading this version of the Centrify Mac agent from a previous version, for example, upgrading from version 5.2.3-429 to 5.2.4-464, using Deployment Manager, and at the same time change the license mode, e.g. from Express Edition to Standard Edition, you may get an error result in the Action "Add Software / Join Zone" in Deployment Manager console during the upgrade. The workaround is to provide an Active Directory domain account credential, which is capable to run adleave, in the Manage Software step. (CS-38453).

Installing on Macintosh OS 10.11 "El Capitan"

If you are running the current release of Centrify, you MUST UPGRADE Centrify BEFORE upgrading your Mac to OS 10.11 El Capitan.

If you upgrade to OS X 10.11 El Capitan from a 10.8.x or a 10.9.x version, there is a known Apple bug (22735194) that prevents the Centrify daemon from running upon first boot after the update. To resolve this you will need to login as a local administrator and execute the following command:

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

Alternatively, you can upgrade from 10.8.x or 10.9.x to 10.10 and then safely proceed with the update to El Capitan.

Follow these steps:

1) Download the Centrify package for Mac OS

2) Upgrade Centrify using this package.

3) Upgrade to Mac OS 10.11.

If you have already upgraded to 10.11 with a previous version of Centrify and can't log in as an Active Directory User, follow these steps:

1) Log into the Mac with your Mac's local administrator account

2) Download the Centrify package for Mac OS

3) Upgrade Centrify to this package.

You should now be able to log in with Active Directory credentials

Note:

When upgrading this version of the Centrify Mac agent from a previous version, for example, upgrading from version 5.2.3-429 to 5.2.4-464, using Deployment Manager, and at the same time change the license mode, e.g. from Express Edition to Standard Edition, you may get an error result in the Action "Add Software / Join Zone" in Deployment Manager console during the upgrade. The workaround is to provide an Active Directory domain account credential, which is capable to run adleave, in the Manage Software step. (CS-38453).

Installing on Macintosh OS 10.10 "Yosemite"

If you are running the current release of Centrify, you MUST UPGRADE Centrify BEFORE upgrading your Mac to OS 10.10 Yosemite.

Follow these steps:

1) Download the Centrify package for Mac OS

2) Upgrade Centrify using this package.

3) Upgrade to Mac OS 10.10.

If you have already upgraded to 10.10 with a previous version of Centrify and can't log in as an Active Directory User, follow these steps:

1) Log into the Mac with your Mac's local administrator account

2) Download the Centrify package for Mac OS

3) Upgrade Centrify to this package.

You should now be able to log in with Active Directory credentials

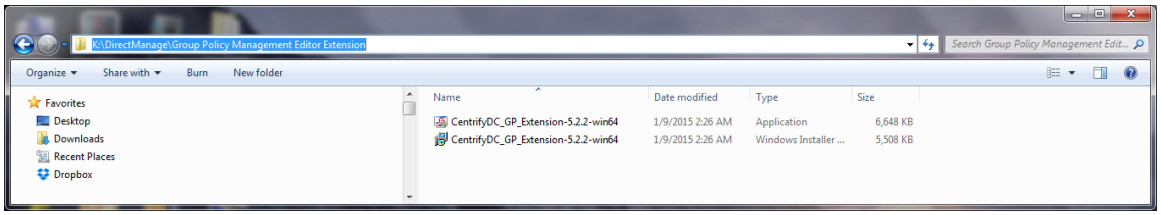
Note: If you are using Centrify Group Policies for Mac OS 10.10 you will need to update the Centrify Windows Administration Console to receive the newest Group Policy Templates.

Installing Mac Group Policies Using The New Streamlined Centrify Windows Administrator Group Policy Extension Package

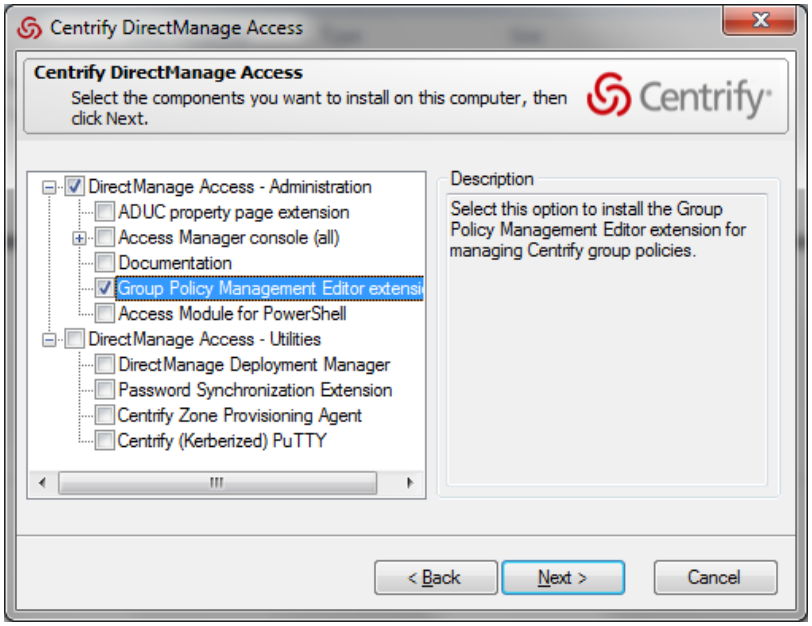
For Mac Admins using Auto-Zones a new streamlined GPOE installation package is now available

1) Mac admin downloads our client CDC package for Mac.
2) Mac admin installs the CDC software and joins to his domain via auto-zone (for traditional zone management the Admin will need to install the full Centrify Access Manager on Windows)
3) Mac admin uses this new, streamlined installer to install only the GPOE extensions to manage these machines via Windows Group Policy System
4) Once installed, Mac admins can now control their Macs via the Windows Group Policy System

Example: The installer is under the below path. The screen below shows ISO is mounted as the K drive. Administrators can run the installer directly



Administrators can also run the Centrify suite installer and select the individual components to be installed. For example, only the GPOE extension is selected in the screen below



Restoring the FileVault user list after adflush:

After you upgrade to release Suite 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. In your Server Suite 2015.1 or later environment, 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

   Bug ID: (78566)

Feature Changes and Notable Fixes in this release:

- Fixed an issue where an end user, after changing their password, might see an error message such as "the system was unable to unlock your login keychain" by relocating the Centrify Group Policy "Centrify Settings -> Mac OS X Settings -> Security and Privacy -> Keychain Policies -> Auto Generate New Login Keychain Properties." (CC-37022).
- Fixed a bug in the Group Policy "Custom Settings->Install MobileConfig Profiles" to support special characters with the exception of Single Quote (') and Ampersand (&) in the PayloadIdentifier for a mobileconfig profile. (CC-42376)
- Added an option (-K --check-kdc-eku) to the command-line utility sctool to allow sctool to check the KDC certificate for the Extended Key Usage (EKU) attribute "Kerberos Authentication". This option was added because EKU checking is disabled by default. (CC-38917).
- RC4 and DES encryption for SmartCard Kerberos authentication is no longer supported. Please configure your Active Directory domain and forest to use AES-128 or AES-256 encryption for Kerberos in order to ensure future compatibility. (CC-39271).
- CDC includes a Kerberos library upgrade allowing support for newly-provisioned smart cards with SHA-256 encryption and Centrify has tested the following SHA-256 smart cards: (CC-42494)
    - - Oberthur ID One 128 v5.5 Dual SHA256 Cards
    - - G&D FIPS 201 SCE 3.2 SHA256 Cards)
- Added the Centrify group policy "Centrify Settings" -> "Mac OS X Settings" -> "Security & Privacy" -> "Enable smart card support for sudo" to support "sudo" operation authentication using name mapping smart cards on OS X 10.11.2 or above. (CC-36493)
- Fixed and issue where a domain user login would fail in FIPS mode after upgrading to macOS 10.12. (CC-42148).
- Fixed an issue where, when the Centrify Group Policy "Computer Configuration -> Policies ->Centrify Settings ->Mac OS X Settings ->802.1X Settings ->Enable Machine Wi-Fi Profile" and/or "Enable Machine Ethernet Profile" were enabled, the signed temporary Wi-Fi / Ethernet profile was not removed from the temporary location after profile installation. (CC-39762).
- Fixed an issue with a cdcsmb printing failing and displaying the error message: "The printer name is invalid". (CC-40746).
- The Centrify Kerberos library has been upgraded based on MIT Kerberos 5-1.14.1. (CS-31783, CC-42493).
- OpenSSL upgraded to 1.0.2h and the CVE-2016-2178 patch applied to OpenSSL and OpenSSL-fips-2.0.11 (CS-40275, CC-42493).
- Fixed an issue where log messages from the group policy mapper scripts were not being redirected from system.log to centrifydc.log on Mac OS Sierra 10.12. (CC-40249).
- Fixed an issue where a previously existing password-protected keychain was not removed when a user logged in with a Smartcard PIN, and a previously existing token-protected keychain was not removed when a user logged in with a password. (CC-41187).
- Added the Centrify Licensing Service to the Mac Installer. (CC-42359).
- Apple resolved the known Apple Bug (25743325) which could cause a Smart Card to be undetected when upgrading from Mac OS 10.11.3 to 10.11.4 GA with the Mac OS update combo "osxupdcombo10.11.4.dmg" (CC-37749).

- Fixed an issue where the Mac system preferences could not be opened by a user after getting the password expiration notice. (Ref: CC-43441)
- Added support for Smart Card login with select Secmaker branded Smart Cards. (Ref: CC-36347)
- Fixed an issue where the adclient logging mechanism could fail to write to the log after an extended period of time. (Ref: CC-42498)
- Mac OS 10.12.1 resolved a known Apple Bug #28234259 in 10.12.0 where if the Centrify Group Policy "User Configuration -> Centrify Settings -> Mac OS X Settings -> Security & Privacy -> Keychain Policies -> Enable protected keychain" and the Group Policy "Computer Configuration -> Policies -> Centrify Settings -> Mac OS X Settings -> 802.1X Settings -> Enable User Wi-Fi Profile" were both enabled, when the AD user tried to manually connect to the 802.1X network, the user would be incorrectly prompted with multiple user certificates on every login. (CC-41181, CC-41181).
- Fixed an issue that could cause Smart Card name mapping to malfunction due to Serial Numbers and CN values being merged in the certificate subject name. (Ref CC-42564)
- Added support for Proxy PAC URLs in 802.1X Wi-Fi Profiles. (Ref: CC-42825)

The Following Issues were resolved in Centrify CDC Unix and are in those release notes but may also apply to Mac users:

- Fixed a bug that caused a failure in cross-domain group query using both configuration parameters adclient.preferred.login.domains and adclient.cache.upn.index:true. (Ref: CS-39834)
- Support Kerberos Armoring (FAST - Flexible Authentication Secure Tunneling) in Windows Server 2012 and 2012 R2
    - Kerberos armoring options (1) Not supported, (2) Supported, (3) Always provide claims, in Windows Server 2012 or above are also supported with this upgrade. However, we do not support option (4) Fail unarmored auth request (AS-REQ) for now. (Ref: CS-28823, CS-40613)
- The command adjoin has a new option “-F/--forceDeleteObj” to clean up the existing computer object and extension object in AD before joining. (Ref: CS-40845)
- Support of ALTUPN (alternative UPN suffixes) from two-way trust forests.
    - The support of Alternate UPN suffixes (ALTUPN) is now extended to cover two-way trusted forests. (Ref: CS-40190, CS-41755, CS-41794)
    - We will now support authenticating cross-forest users using alternative UPN suffix. (Ref: CS-32538)
- adclient.krb5.principal.name: The default of this parameter is changed from "upn" to "sam". This is because by default, AD user's Kerberos name is generated as samAccountName@<AD REALM>. Also, given a name format as <name>@<REALM>, adclient used to do UPN search first, and then try SamAccountName (SamDom) format match but by the same token, the order is now reversed to look for SamDom first then UPN to be consistent with the default setting. Note: if you really want to set adclient.krb5.principal.name to "upn", be aware of a potential issue when there exists a user A whose UPN matches another user B’s SAM account name and the UPN domain suffix matches the domain realm, user A would be

unable to login using his own password, or user B who logged in using its SAM account name could SSO to user A's account because of the confusion induced from matching UPN with SAM@DOM. For an AD user mapped to MIT user, the Kerberos name generation will ignore this setting as before. (Ref: CS-25166, CS-40920, CS-41125)

- ldapproxy now supports more complex searches, like search by member with posixGroup, search by sAMAccountName with posixAccount/posixGroup, etc. (Ref: CS-34621, CS-39880, CS-40242)

  Examples like:
  - "(&(objectClass=posixAccount)(samAccountName=<user's samAccoutName>))"
  - "(&(objectClass=posixGroup)(samAccountName=<group's samAccountName))"
  - "(&(objectClass=posixGroup)(|(memberuid=<user's unix name>)(member=<user's DN>)))"
  - "(&(objectClass=posixGroup)(|(memberuid=<user's unix name>)(uniqueMember=<user's DN>)))"

  Please note

  - These searches look for UNIX-enabled users and groups only.
  - 'posixGroup.member' and 'posixGroup.uniqueMember' both map to _MemberDN attribute in rfc2307.map

Note: For configuration details of new features, please refer to the Mac admin guide.

Known Mac OS Problems

General Installation Issues

- When upgrading this version of the Centrify Mac agent from a previous version, for example, upgrading from version 5.2.3-429 to 5.2.4-464, using Deployment Manager, and at the same time change the license mode, e.g. from Express Edition to Standard Edition, you may get an error result in the Action “Add Software / Join Zone” in Deployment Manager console during the upgrade. The workaround is to provide an Active Directory domain account credential, which is capable to run adleave, in the Manage Software step. (CS-38453).

- Cannot have two system volumes joined to the same domain: for the purpose of migrating from an earlier release of Mac OS to Mac OS 10.7, it can be helpful to have both versions installed on different volumes of one machine. If Centrify is installed on the same machine on two different system volumes, the following restriction applies. It is not possible to have both system volumes joined to the same domain at the same time. If Centrify on volume A is joined to the domain, booting into volume B will hang the machine, and vice-versa. Therefore, you should leave the domain prior to switching the boot volume. Once the machine is booted into volume B, you can re-join the domain.

- In order to meet the requirements of the Apple OS X Software Installation Gatekeeper, Centrify DirectControl Mac package is now code-signed. A User will no longer able to extract, alter, repack the package and expect the installation to work. (77255).

- The GUI installer "Install/Upgrade" button may unexpectedly read "Install" rather than "Upgrade" even though a previous version of Centrify is already installed on the system. In this case, clicking the "Install" button will start an upgrade with no undesired effects (27884).

- When using a Mac whose IP address is determined dynamically via DHCP, if after joining to a domain, the Mac's host name is changed; Centrify will not function properly until performing an adleave and adjoin.

- A .local entry is automatically added into the DNS search domain after adjoin by Centrify for Mac to deal with issues related to Bonjour, which can cause issues in some environments. A workaround to this is to manually set the DNS search order and to limit the .local search timeout. (Ref: CS-36229

Known Mac OS X 10.12 "Sierra" Problems

- The Centrify group policy setting, "Computer Configuration -> Centrify Settings -> "Mac OS X Settings -> Security & Privacy -> Log out after number of minutes of inactivity" behaves inconsistently. For example, if set to log out after 5 minutes, log out may not occur until 10 minutes later. However, setting the timeout to 6 minutes behaves as expected. Status: Under investigation. (CC-39736).
- Due to Apple dropping support for portable home directories in Mac OS 10.12, the Centrify Group Policy "User Configuration > Centrify Settings > Mac OS X Settings > Mobility Settings" will not include synchronization options for Mac OS 10.12 and above. Release Note from Apple: "Mobile home directories, which have networks accounts that are cached locally, can still be created. However, their home folder will no longer sync with their network home directory." (CC-39802).
- When upgrading to OS X 10.12 El Capitan from a 10.8.x or a 10.9.x version, there is a known Apple bug (22735194) that prevents the Centrify daemon from running upon first boot after the update. See "Installing on Macintosh OS 10.12 "Sierra" for more information about this issue. (CC-41684).
- TouchID, available on some Mac computers, is only compatible with an AD user who is also a Mac mobile user. Non-Mac mobile users will not be able to set up TouchID. Privilege Elevation, for example, Unlock Padlock, will only work if the user is directly assigned to administer the computer via System Preference > Users & Groups > "Allow user to administer this computer". Other ways of mapping the user as an admin, such as mapping user group to local admin group via GP will not work. (Ref: CC-43848).
- If Touch ID fingerprint authentication setup is skipped at the time of the creation of a mobile user with smart card support, Touch ID authentication cannot successfully be added later. (CC-44297).
- Even if a user account is locked, disabled or expired, that user will still be able to unlock their Mac using Touch ID fingerprint authentication. (CC-44402).
- Uninstalling the Centrify application from within the Mac System Preferences may result in an unexpected quit of the Mac System Preferences, though the uninstall does complete successfully. (CC-44772).

Known Mac OS X 10.11 "El Capitan" Problems

- When upgrading this version of the Centrify Mac agent from a previous version, for example, upgrading from version 5.2.3-429 to 5.2.4-464, using Deployment Manager, and at the same time change the license mode, e.g. from Express Edition to Standard Edition, you may get an error result in the Action "Add Software / Join Zone" in Deployment Manager console during the upgrade. The workaround is to provide an Active Directory domain account credential, which is capable to run adleave, in the Manage Software step. (CS-38453).

- If you upgrade to OS X 10.11 El Capitan from a 10.8.x or a 10.9.x version, there is a known Apple bug (22735194) that prevents the Centrify daemon from running upon first boot after the update. See "***Installing on Macintosh OS 10.11 "El Capitan",*** page 3, for more information about this issue.

Known Mac OS X 10.10 "Yosemite" Problems

- A "Home sync error" dialog shows up at Mobile user login and logout during home synchronization, which can cause logout time to be abnormally long. However, there is no problem with home content synchronization itself once completed, and files can be synchronized successfully. This issue was determined to be an Apple problem, has been reported to Apple and logged as Apple Bug #17999579. (69707.)
- When trying to unlock the screen from screensaver or sleep, if an incorrect password is initially entered, the Mac's password entry dialog will not allow the user to input their password again. The workaround is to reboot the Mac and enter the password correctly the first time. This issue was determined to be an Apple problem, has been reported to Apple and logged as Apple Bug #18239041. (70120.)
- A user will not automatically be directed to the System Preferences change password pane after being warned that their password is about to expire. The workaround is for the user to manually open the Mac System Preferences and change their password. This issue has been reported to Apple and logged into their bug tracking system as bug #18333542. (70124.)
- If "Enable smart card support" Group Policy is enabled, a user is at the login window and the screensaver is active, after a user fast-switches, the screensaver will not dismiss and the user will be locked out. The workaround is for the user to avoid fast-switching in this scenario. This issue was determined to be an Apple problem, has been reported to Apple and logged as Apple Bug # 18334799. (70543.)
- On OS X 10.10, mobile user accounts may fail to login if they were created after the Mac was already joined to the Active Directory domain using Centrify DirectControl. This issue was determined to be Apple problem, has been reported to Apple and logged as Apple Bug #18392074. (71181.)
- When logging in without a network connection (disconnected mode), network shares will not be automatically mounted even when a network connection is established. (CC-36349).

- The DoD-supplied tool, "Encryption Wizard," versions "Public-3.4.4" or below, does not properly decrypt the encrypted file on OS X 10.10 because it uses Java Runtime Environment version 7, while Mac OS X 10.10 uses Java Runtime Environment version 8. (70647.)

Known Mac OS Problems (sorted by OS, then Category):

This section describes the unique characteristics or known limitations that are specific to using Centrify on a computer with the Apple Macintosh OS X operating environment. Where available, suggested workarounds are provided.

Applicable Mac OS Version	Category	Description
All Mac	CLI	The command '-passwd' does not work to change a user's password. Other methods to change a user's password, such as the passwd command and the Mac GUI password methods do work. (12574).
All Mac	CLI	The command line command dscl /CentrifyDC -list /Users will not function properly in disconnected mode (14922).
All Mac	CLI	Prior to using the Wish shell, preload Centrify Kerberos libraries to load the Centrify libadedit library, for example: $DYLD_INSERT_LIBRARIES=/usr/share/centrifydc/kerberos/lib/libk5crypto.dylib:/usr/share/centrifydc/kerberos/lib/libkrb5.dylib wish (26993).
All Mac	CLI	Adinfo will incorrectly report that a Mac is not joined to a domain after a successful remote install and join. (31988).
All Mac	Configuration	The centrifydc.conf configuration parameter, "adclient.cache.expires" does not have any effect on the actual cache expiration time (28793).

All Mac	Configuration	Currently, when using the Centrify Mac OS X System Preference Pane, manually adding 2 domain controllers with the same name to the preferred domain controllers field and adding 2 or more records of the same domain to the Centrify group policy "Centrify Settings"->"DirectControl Settings"->"Network and Cache Settings"->"Specify DNS DC hostnames" will be prevented with the warning prompt: "This value already exists, please enter another value." The workaround is to adding dns.dc records in the correct format with unique domain controller names. (36700).
All Mac	Configuration	Using the Centrify Account Migration tool to map a mobile or network user to a local home directory will disable the network home directory mounting for those users. (36096).
All Mac	General	At the Windows Active Directory Users and Computers console, when specifying the user's home directory for a use whose home directory resides on the local system, if the /User/ parent directory does not already exist, AD user home directory will not be auto-created during login. (11000).
All Mac	General	Due to Apple bug 6638310, it is possible to hang the DirectoryService by repeatedly changing a search for users in Apple Workgroup Manager before the previous search has completed. It is recommended that you allow each search to complete, or minimize the number of search interruptions you make. (14603).
All Mac	General	A local user with admin rights cannot lock the screen saver (23225).
All Mac	General	An AD user can unlock another AD user’s screen lock when the other AD user’s display name is identical (23366).
All Mac	GP	In Mac OS System Preferences -> Users & Groups, if "Show fast user switching menu as" has been manually unchecked by the AD user, then the group policy setting for fast user switching will not applied for the next user log in. (CC-39626).

All Mac	GP	The group policy Disable automatic login requires manually running adgpupdate once and then rebooting the machine or rebooting twice to take effect (12872).
All Mac	GP	The Group Policy 'User Configuration -> Centrify Settings -> Mac OS X Settings -> Dock Settings -> Place Documents and Folders in Dock'' will not function properly if the entry starts with SPACE (21700).
All Mac	GP	Group Policy setting 'Computer Configuration' > 'Centrify Settings' > 'Mac OS X Settings' > 'Firewall' > 'Enable stealth mode'' to 'disabled' does not disable stealth mode if the user has enabled stealth mode in Mac System Preferences (23581).
All Mac	GP	The Group Policy 'User Configuration' > 'Centrify Settings' > 'Mac OS X Settings' > 'Dock Settings' > 'Adjust the Dock's magnified icon size' does not match the explanatory text when disabled. (24030).
All Mac	GP	The Group Policy "User configuration -> Centrify Settings -> Mac OS X Settings-> Automount Settings ->Automount user's Windows home"' doesn't work properly when user fast switching is enabled (24395).
All Mac	GP	The Mac's preferred network and keychain password created by the 802.1x group policy settings are not automatically removed when leaving the domain (25835).
All Mac	GP	When an AFP share has been mounted using the Group Policy "User configuration -> Centrify Settings -> Mac OS X Settings-> Automount Settings -> Automount network shares" and the network cable is then disconnected, a logout may take up to 10 minutes to complete (26537).
All Mac	GP	The Group Policy "Mac OS Settings-> Printing Settings->Specify printer list" with "Only show managed printers" doesn't function. (27403).
All Mac	GP	The Group Policy ""User Configuration"->"Mobility Setting"->"Mac OS X 10.7 Settings"->"Synchronization Rules"->"Home Sync"->"Skip items that end with" does not function as expected (28505).

All Mac	GP	Some group policies will not be enforced on any version of Mac OS X, however in each case the behavior is consistent with Mac Workgroup Manager. The policies affected are: • User Configuration>Centrify Settings>Mac OS X Settings>Media Access Settings>Permit/prohibit access: Internal Disks • "Applications to be Allowed or Disabled" This will not work with user-entered applications that do not have a valid CFBundleidentifier ID. See the Explain tab of the Mac Settings XML template for more information. • Cannot remove permission to access the printer setup utility or print center • Cannot remove permission to access the help viewer • Cannot remove permission for approved applications to launch non-approved applications In some cases group policies will not be enforced, are enforced only after a logout and re-login, or will exhibit different behavior for machines with Mac OS X installed. In each case the behavior is consistent with Mac Workgroup Manager (7904).
All Mac	GP	Group Policy User Configuration>Permit/Prohibit access: Internal Disks from "Deny" to "Allow" requires reboot to function properly. The same problem exists using the Apple Native Workgroup Manager configuration. (7939).
All Mac	GP	The Centrify Group Policy "Enable Stealth Mode" requires a reboot of the machine to take effect. (30251).
All Mac	GP	If the Centrify Group Policy, "Enable Auto Zone user home directory" is not enabled and the machine is joined to Auto Zone, all users will be treated as local home directory users regardless if they have network home directory. (38879).
All Mac	GP	The Group Policy "Setting user mapping" will fail to successfully map a local user to an AD user whose password has expired. The workaround is for the AD admin to unblock the AD user. (32061).

All Mac	GP	When using multiple profiles with the same SSID in the Group Policy "Computer Configuration-> Centrify Settings->Mac OS X settings->802.1x settings->Enable Wifi Profile" more than 1 profile may not be downloaded to the Mac. The workaround is to use a unique SSID for each profile. (46563).
All Mac	GP	When using two domains with the same Template Name in the Group Policy "Computer Configuration" -> "Centrify Settings" -> "Mac OS X settings" -> "802.1x settings" -> "Enable Wifi Profile", new certificates will not be automatically downloaded. The workaround is to ensure each domain has a unique Template Name. (46710).
All Mac	GP	If user manually deletes the 802.1x network profiles, once deleted, the Centrify software will not automatically restore those profiles. Administrators should instruct users to refrain from deleting profiles without understanding the consequences. An Administrator can force Centrify to re-install all the profiles by deleting the files: "/var/centrifydc/profiles/com.centrify.cdc.ethernet" for 802.1x Ethernet profiles and "/var/centrifydc/profiles/com.centrify.cdc.wifi" for 802.1x wifi profiles. (54101).
All Mac	GP	User Certificates will not be imported to the Mac's keychain at the first login of user with group policies that should result in importing user certificates to the Mac Keychain, such as the Group Policy "User Configuration" -> "Centrify Settings" -> "Mac OS X settings" ->"802.1x settings" -> "Enable Wi-Fi Profile". The workaround is for the user to logout and login again. (56471.)
All Mac	GP	If user modifies his Mac's printer brand and model manually using the Mac OS X "Print & Fax" System Preference Pane after the the Centrify group policy 'User Configuration' > 'Centrify Settings'> Mac OS X Settings ' > 'Printing Settings'> 'Specify printer list' has been configured and the group policy enabled, the group policy will not reflect the new manually configured printer choice even after the group policy updates. The workaround is to disable the group policy and then manually delete the printer previously used in the group policy, and then select the new printer in the Centrify group policy. (57048).

All Mac	GP	The Group Policy "User configuration->Centrify Settings-> Mac OS X Settings->Automount Settings->Automount network shares" does not function when the user password contains the "@" symbol. (48893).
All Mac	GP	Due to a current Apple bug in User-Based Wifi profiles, the Centrify Group Policy ""Computer Configure" -> "Centrify Settings" -> "Mac OS X Settings" -> "802.1X Settings" -> "Enable User Wi-Fi Settings" does not function properly. Centrify is working closely with Apple to correct this problem. (58632).
All Mac	GP	The Centrify Auto-enrollment Group Policy will not support home directory names or certificate template names containing spaces. (47983).
All Mac	GP	With the Centrify Group Policy "Computer Configuration" -> "Centrify Settings" -> "Mac OS X settings" ->"802.1x settings" -> "Enable Machine Wi-Fi Profile," a user must manually select an identity cert-key pair for use in authentication. Mac OS X presents the user with an identity selection dialog, which lists each identity's common name. A consequence of this behavior is that: (1) If 802.1X (Ethernet/WiFi) User GPs have been enabled, and (2) If there are multiple user certificate templates configured for auto-enrollment, then all of the auto-enrolled certificates will show up in the identity selection dialog with the same common name.

All Mac	GP	If user upgrades to Centrify Agent, Centrify Identity Service, Mac Edition 5.2.x from a previous version, 802.1x PEAP authentication may not function properly. To workaround the problem, a User can run the CLI command "sudo adkeytab -C -m" to update the password item in the Mac keychain, properly enabling 802.1x PEAP authentication. (67139).
All Mac	GP / Parity with WGM	The Group Policy 'User Configuration>Centrify Settings>Mac OS X Settings>Media Access Settings>Permit/prohibit access: Internal Disks' is not functional. The same problem exists using the Apple Native Workgroup Manager configuration. (11955).
All Mac	Installation	If a network user's home directory is going to reside on a SMB share, his home directory needs to exist before creating a new network home user from a Mac with Centrify installed. (35026).
All Mac	Installation	Unpredictable behavior when a Mac is joined using the Centrify Active Directory Plugin while already joined with Apple's Active Directory Plugin. The workaround is to leave / unjoin the Apple Directory Plugin before attempting to join using Centrify. (36591).
All Mac	Installation	Cloud Enrollment performed post-join requires the local hostname to match the hostname when the machine was first joined. Otherwise, enrollment may fail and report an error warning about incorrect samaccountname. (65684.)
All Mac	Installation / Upgrade	When in Fast user switching mode, and switching from a local user to a Smart Card user, and the smart card then inserted the login prompt may ask for password rather than PIN. It is recommended to avoid using Fast User Switching Mode with Smart Card enabled Macs. (24425).
All Mac	Installation / Upgrade	If the network is disconnected soon after a DirectControl installation and ADjoin, an AD user may fail to login in disconnected mode. The solution is to reconnect the network, wait 10 minutes and try to login again. (24534).
All Mac	Installation / Upgrade	When using the Centrify Join Assistant GUI, if invalid information is entered into the "Computer" field while the "Computer Alias Name" is checked, Join will fail on the current and subsequent attempts (28366).

All Mac	Login / Authentication	Changed the default behavior to disable logging in with the AD account display name and / or common name for security purposes. This change was made in the centrifydc.conf file. (J5585). Changed: adclient.user.lookup.cn: true adclient.user.lookup.display: true to: adclient.user.lookup.cn: false adclient.user.lookup.display: false
All Mac	Login / Authentication	Logging in using the SAM account name: remotely logging into a Mac with DirectControl installed, using the form of domain\username with a backslash '\' character as a separator between the domain and user name will fail. Using the form domain/username with a single forward slash "/" does work. Example: swim/stest1 PASS swim//stest1 FAIL swim\stest1 FAIL swim\\stest1 FAIL (9413).
All Mac	Login / Authentication	FTP login restrictions: setting an AD user's properties in ADUC to disallow login to other machines will not prevent that AD user from logging in, via FTP, into Macintosh computers with DirectControl installed. The login restrictions are enforced properly with telnet, ssh, rlogin and rsh. (10116).
All Mac	Login and Authentication	In Auto Zone mode, if the username contains a space, and is configured to be a network home directory user, the network home directory will not mount, preventing the user from logging in (22788).

All Mac	Login and Authentication	Network Home Directory Users attempting to log in via a non GUI Login Window will be able to log in but their home directory will not be mounted and will get an error message: "Failed to create home directory" The workaround is to log in via GUI Login Window first. (29603).
All Mac	Login and Authentication	Login will not work when the UID value is set to a value larger than 2,147,483,647. (39239).
All Mac	Login and Authentication	A user will not automatically be directed to the System Preferences change password pane after being warned that their password is about to expire. The workaround is for the user to manually open the Mac System Preferences and change their password. (70124.)
All Mac	Login and Authentication	On Mac OS X 10.10, if “Enable smart card support” Group Policy is enabled, a user is at the login window and the screensaver is active, after a user fast-switches, the screensaver will not dismiss and the user will be locked out. The workaround is for the user to avoid fast-switching in this scenario. This issue was determined to be Apple problem, has been reported to Apple and logged as Apple Bug #18334799. (70543.)
All Mac	Login and Authentication	When using a computer configured with the Group Policy "Computer Configuration" -> "Centrify Settings" -> "Mac OS X settings" -> "802.1x settings" -> "Enable WiFi Profile,” a root user attempting to log in may fail with the connect status hung with the message “Authenticating.” The workaround is to use the “Auto Join” setting in WiFi configuration, or to log in as a user other than root. (53787).
All Mac	Misc	The secure.log of a DirectControl-enabled Mac, after mounting an AFP share created by ExtremeZ-IP AFP will indicate that the mounter complains of UIDs not matching. This will not result in any problems. (7959).
All Mac	Misc	When a local user with non-administrative rights has the identical name as an Active Directory administrator user, the local user will be changed to an administrator user. (32290).

All Mac	Smart Card	If a user has 2 AD Identities, each with certificates for both CAC and PIV on a single CACNG Smart Card, the Apple Login Window will always choose the PIV identity to login. In order to login with CAC identity, the PIV identity would need to be deleted from AD. (27870).
All Mac	Smart Card	For proper operation of Smart Card functionality immediately after installation of DirectControl, a reboot is required. (28651).
All Mac	Smart Card	When using Smart Card, and the AD user has been set to "User must change password at next logon" and the GP "Prohibit Expired Password" is not set, the screensaver cannot be unlocked (28794).
All Mac	Smart Card	When using DirectControl with Smart Card authentication, and an expired certificate as well as a valid certificate exists in the AD store, the DirectControl may download the expired certificate to the Mac's Keychain instead of the valid one. The workaround is to manually copy the valid certificate into the Mac's keychain. In addition, in this situation, even when the valid certificate has been copied to the Mac's keychain "sctool -D" will still report the error: "could not get issuer certificate." (29885).
All Mac	Smart Card	When using DirectControl with Smart Card authentication, and an expired certificate as well as a valid certificate exists in the AD store, the DirectControl may download the expired certificate to the Mac's Keychain instead of the valid one. The workaround is to manually copy the valid certificate into the Mac's keychain. In addition, in this situation, even when the valid certificate has been copied to the Mac's keychain "sctool -D" will still report the error: "could not get issuer certificate." (29887).
All Mac	Smart Card	The command, "sctool -e" does not enable the Group Policy "Lock Smart Card screen". The workaround is to use Group Policy to Enable the Smart Card. (32066).
All Mac	Smart Card	If a Smart Card is inserted and left in the Smart Card reader during a restart, when the Mac OS X login screen appears, the Smart Card may not be recognized and the Login Screen may not show the Smart Card Pin prompt as expected. The workaround is to remove and reinsert the Smartcard. (36540).

All Mac	Smart Card	When logged in as a Smart Card user and running a CDC upgrade with the Centrify Group Policies "Mac OS X Setting->Security Settings->Lock Smart Card screen" and "Mac OS X Setting->Security Settings->Require password to wake this computer from sleep or screen saver" enabled, if the Mac Screen Saver activates, a normal screen saver unlock password entry field will appear instead of the expected Smart Card Pin entry field. Entering the Smart Card Pin will not unlock the screen saver. The workaround to enable the correct Smart Card pin prompt at the Screen Saver unlock screen is to force-restart the Mac by holding the power key for several seconds. After the Mac restarts the Smart Card Login and screen saver unlock will work normally. (39601).
All Mac	Smart Card	Screen saver shows password not PIN prompt: Most smart card users are allowed to log on with a smart card and PIN only and cannot authenticate with a user name and password. However, it is possible to configure users for both smart card/PIN and user name/password authentication. Generally, this set up works seamlessly: the user either enters a user name and password at the log on prompt, or inserts a smart card and enters a PIN at the prompt. However, for multi-user cards, it can be problematic when the screen locks and the card is in the reader. When a user attempts to unlock the screen, the system prompts for a password, not for a PIN, although the PIN is required because the card is in the reader. If the user is not aware that the card is still in the reader and enters his password multiple times, the card will lock once the limit for incorrect entries is reached. (47966).
All Mac	Smart Card	When using a Smart Card with a PIN is longer than 8 digits, login will not function properly. The workaround is to only use Smart Cards with a PIN of 8 or less digits. (45075).
All Mac	Smart Card	When using a Name Mapping User, Microsoft Outlook will prompt for a PIN when sending encrypted mail. (45658).
All Mac	Smart Card	Creating a Mobile Account Smart card User with Filevault 1 encryption activated via Centrify Group Policies may fail with the prompt: "Unable to create mobile account." The workaround is to use FileVault2 if possible. (39711).

All Mac	SSO	Using SSH to login with single-sign on (SSO) from using a Unix SSH client to a Mac with OS X 10.4 and 10.5 will only function properly within specific scenarios and SSH command syntax. The following 3 scenarios should work: 1. SSH SSO from Unix client to Mac with same Unix and sAM name or 2. SSH SSO from Unix client to Mac with different Unix and sAM name will only work if the zone user has logged in to the Mac previously or 3. If #2 is true, use the principle name in the SSH command i.e.: "sAMName@domainname (13721).
All Mac	SSO	A Mac mobile user at first login, cannot sync or perform any operations requiring Single Sign-On if home directory is created using a local home directory template. The problem is resolved after a logout and login. (21945).
Mac OS/X 10.10	Network and Portable Home Directory	A "Home sync error" dialog shows up at Mobile user login and logout during home synchronization, which can cause logout time to be abnormally long. However, there is no problem with home content synchronization itself once completed, and files can be synchronized successfully. This issue was determined to be an Apple problem, has been reported to Apple and logged as Apple Bug #17999579. (69707.)
Mac OS/X 10.10	Login / Authentication	When trying to unlock the screen from screensaver or sleep, if an incorrect password is initially entered, the Mac's password entry dialog will not allow the user to input their password again. The workaround is to reboot the Mac and enter the password correctly the first time. This issue was determined to be an Apple problem, has been reported to Apple and logged as Apple Bug #18239041. (70120.)
Mac OS/X 10.10	Misc	The DoD-supplied tool, "Encryption Wizard," versions "Public-3.4.4" or below, does not properly decrypt the encrypted file on OS X 10.10 because it uses Java Runtime Environment version 7, while Mac OS X 10.10 uses Java Runtime Environment version 8. (70647.)

Other Notes

Using the Software Update group policy: for reliable operation of the Software Update group policy, Software Update Settings>Software Update server to use, you should enter the hostname of the software update server rather than an IP address. In addition, if DNS has not made the association of the hostname of the server with its IP address, you should associate the IP address and hostname by adding a line to the local Mac's etc/hosts file.

Example: For "Software Update server to use:" enter
http://SERVER.local:8088/
instead of
http://192.168.2.79:8088/

Where SERVER.local is the hostname of the Software Update Server. In the case of DNS failing to associate the hostname of the software update server with an IP address, adding a line like this to /etc/hosts will create the proper association:
192.168.2.79 SERVER.local

Additional information and support

In addition to the documentation provided with this package, you can find the answers to common questions and information about any general or platform-specific known limitations as well as tips and suggestions from the Centrify Knowledge Base.

The Centrify Resource Center provides access to a wide range of packages and tools that you can download and install separately. For more information, see the Centrify Resource Center Web site:

http://www.centrify.com/resources

You can also contact Centrify Support directly with your questions through the Centrify Web site, by email, or by telephone. To contact Centrify Support or to get help with installing or using this version of Centrify Server Suite, send email to support@centrify.com or call 1-669-444-5200, option 2. For information about purchasing or evaluating Centrify products, send email to info@centrify.com.

Getting other packages

The Centrify Resource Center provides access to a wide range of packages and tools that you can download and install separately, such as updated Kerberos and PuTTY programs that have been optimized to work with DirectControl. For more information, see the Centrify Resource Center Web site:

http://www.centrify.com/resources