

Welcome to Centrify for Mac

Release Notes for Centrify for Mac, macOS Release 11.1 “Big Sur” Edition

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

Centrify for Mac is a part of Centrify software and is protected by U.S. Patents 7,591,005; 8,024,360; 8,321,523; 9,015,103; 9,112,846; 9,197,670; 9,378,391 and 9,442,962. (Ref: CS-44575)

Notice of Discontinuation of Support for Mac OS 10.13.x, 10.12.x, and 10.11.x: Centrify has discontinued support for Mac OS 10.13.x, 10.12.x, and 10.11.x from this release on of Centrify for Mac.

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

- CentrifyDC-5.7.0.dmg– A Mac disk image for macOS 11.1, 11.0, 10.15, and 10.14 containing the following:
 - AD Check.app – Graphical application to perform environment checks before installing Centrify on macOS 11.1, 11.0, 10.15, and 10.14
 - CentrifyDC-5.7.0-x86_64.pkg – Graphical installer for Intel Macs for macOS X macOS 11.1, 11.0, 10.15, and 10.14

Supported platforms and system requirements

The Centrifly for Mac in the applicable package can be installed on the following versions of the macOS operating system:

- macOS 11.1.x on Intel Macs
- macOS 11.0.x on Intel Macs
- macOS 10.15.x on Intel Macs
- macOS 10.14.x on Intel Macs

Note: Apple M1 chips are not supported.

Installing on macOS 11.1 “Big Sur”

If you are running the current release of Centrifly, you **MUST UPGRADE** Centrifly **BEFORE** upgrading your Mac to OS 11.1 Big Sur.

Follow these steps:

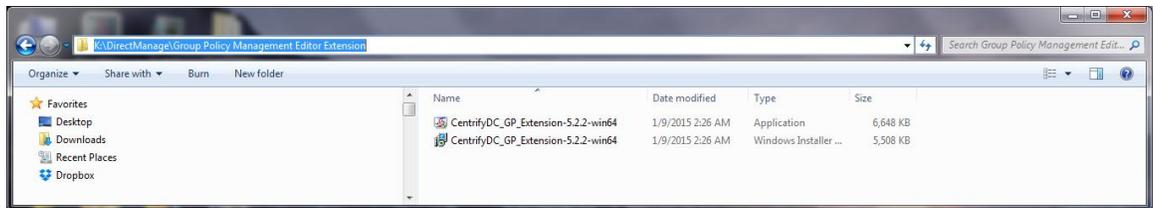
- 1) Download the Centrifly package for macOS
- 2) Upgrade Centrifly using this package.
- 3) Upgrade to macOS 11.1.

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

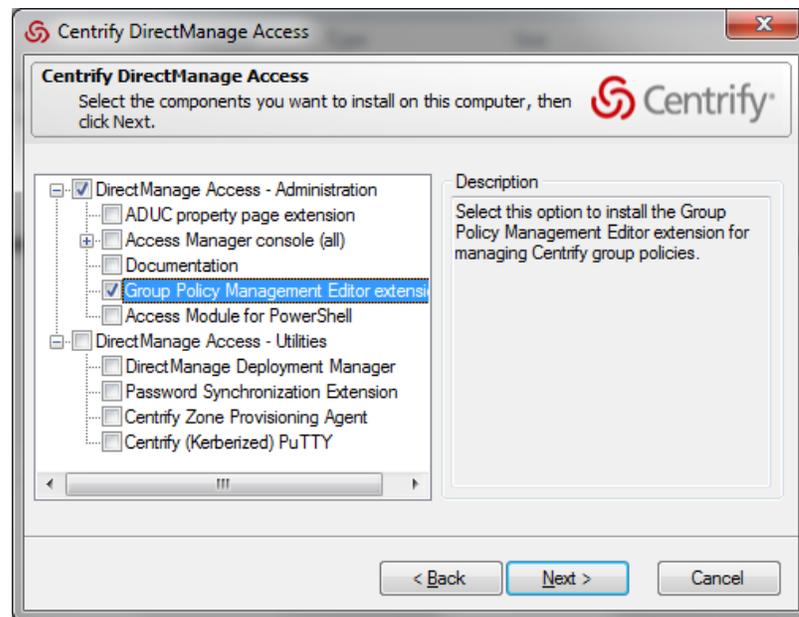
For Mac Admins using Auto-Zones a new streamlined GPOE installation package is now available

- 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 Centrifry 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 Centrifry installer and select the individual components to be installed. For example, only the GPOE extension is selected in the screen below



Feature Changes and Notable Fixes in this release (Centrify for Mac - Release 2020 Component Update):

- This release supports macOS 11.1 “Big Sur”.

Feature Changes and Notable Fixes in this release (Centrify for Mac - Release 2020):

- This release supports macOS 11.0 “Big Sur”.
- We are not supporting MDM anymore. All MDM group policies will not work.
- We are not supporting Keychain Sync on macOS Big Sur anymore.
- Printer, Smart Card, Keychain Sync and Auto-enrollment are not covered for now.
- GP "Application Access Settings" is deprecated. (CS-49229)

Known macOS Problems

General Installation Issues

- The "Store AD password in the login Keychain" Group Policy should not be enabled in conjunction with the "Enable protected keychain" Group Policy since one is meant for AD users and the other is meant for Smartcard users. (CC-56153)
- User profiles deployed using the User Group Policy "Install MobileConfig Profiles" are successfully installed at user login but are first in effect at the next group policy update. (CC-55484)
- Upgrading from a CDC version prior to Release 2017.2 to a CDC version > Release 2017.3 will still require a user to logout and log back in before the notification appears on the GUI. (CC-53530)
- 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 be able to extract, alter, repack the package and expect the installation to work. (77255).
- 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)
- If a Mac device has already been encrypted by FileVault, when enabling the Manage Local Admin Account policy, the local account created by Centrify Privilege Service may not immediately have admin rights. The workaround is to restart the mac, sometimes multiple times, until the correct admin rights are present. (Ref: CC-46221)
- If you upgrade to OS X 11.1, or 11.0 Big Sur 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 11.1, or 11.0

Known macOS 11.1, 11.0 “Big Sur” Problems

- As of macOS Big Sur, Apple no longer permits to silently install configuration profiles. It affects the following GPs and they will not work on macOS Big Sur: (CS-49308)
 1. GP "Install MobileConfig Profiles" (CS-49198)
 2. GP "Enable Profile Custom Settings" (CS-49200)
 3. GP "Require password to wake this computer from sleep or screen saver" (CS-49233)
 4. GP "Enable Machine Ethernet Profile"
 5. GP "Enable Machine Wi-Fi Profile"
 6. GP "Enable User Ethernet Profile"
 7. GP "Enable User Wi-Fi Profile"
 - When installing CentrifyDC on macOS 10.15 and later, you may be prompted "CentrifyDC can't be opened because Apple cannot check it for malicious software". Please open System Preferences> Security & Privacy, CentrifyDC will appear under the "General" tab, click "Open Anyway" to continue to open and install CentrifyDC. (CS-49242)
 - When upgrading Mac from macOS 10.14 or lower to macOS 10.15 or higher, the CentrifyDC must be reinstalled, no need to leave the domain or uninstall the old CentrifyDC. (CS-49416)
 - Network user cannot work on macOS 10.15 and higher. We suggest using mobile user or general AD user instead. (CS-49185)
 - When mobile user first-ever login on macOS Big Sur, maybe cannot set up Touch ID for adding fingerprints. Just need to re-login to work. (CS-49349)
- Apple Support has provided the following resolutions:
- Reset the SMC of Mac: <https://support.apple.com/en-us/HT201295>
 - Reset NVRAM or PRAM on Mac: <https://support.apple.com/en-us/HT204063>

Known macOS 10.15 “Catalina” Problems

- When installing CentrifyDC on macOS 10.15 and later, you may be prompted "CentrifyDC can't be opened because Apple cannot check it for malicious software". Please open System Preferences> Security & Privacy, CentrifyDC will appear under the "General" tab, click "Open Anyway" to continue to open and install CentrifyDC. (CS-49242)
- When upgrading Mac from macOS 10.14 or lower to macOS 10.15 or higher, the CentrifyDC must be reinstalled, no need to leave the domain or uninstall the old CentrifyDC. (CS-49416)
- Network user cannot work on macOS 10.15 and higher. We suggest using mobile user or general AD user instead. (CS-49185)

Known macOS 10.14 “Mojave” Problems

- On macOS 10.14 the Group Policy to control "Allow user to modify the printer list" (under User Configuration > Policies > Centrify Settings > Mac OS X Settings > Printing Settings > Specify printer list(with model)) may not work properly. Users may be able to modify the printer list on 10.14.(CC-61753)
- The Centrify Join Assistant cannot be used by the root account on 10.14. Workaround is to use an admin account that is not root. (CC-60683)
- Unlock screen window still exists after unlock screen with fingerprint when smart card is enabled. [Apple bug#42177021] (CC-60410)
- On macOS 10.14, if you have smartcard support enabled there may be some padlocks that you can't unlock in System Preferences with a local admin account. A workaround is to use an AD account that has local admin rights to unlock the padlock. (CC-61903)

Known macOS 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 macOS Version	Category	Description
All Mac	GP	When we set GP 'Permit/prohibit access: Internal Disks' with 'allow, require authentication' or 'allow, require authentication, read-only', the authentication can be bypassed. See https://developer.apple.com/forums/thread/665970 (Apple bug# FB8888815, CS-49239)
All Mac	CLI	The command '/usr/bin/passwd' does not work to change a user's password. Other methods to change a user's password, such as the /usr/bin/dscl command with -passwd option and the Mac GUI password methods do work. (12574).
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	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 macOS 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	DC	Release 18.8 includes an update to Coolkey to support Giesecke & Devrient 144k, Gemalto DLGX4-A 144, and HID Crescendo 144K FIPS cards. However, this has caused known issues that may cause CAC cards to only work sporadically. A workaround for CAC cards is to wait for it to prompt for PIN and Welcome, without removing the card, and then try again.
All Mac	General	At the Windows Active Directory Users and Computers console, when specifying the user's home directory for a user 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	GP	In macOS 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 'User Configuration -> Centrify Settings -> macOS 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' > 'macOS 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 "macOS 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"->"macOS 10.7 Settings"->"Synchronization Rules"->"Home Sync"->"Skip items that end with" does not function as expected (28505).
All Mac	GP	<p>Some group policies will not be enforced on any version of macOS, however in each case the behavior is consistent with Mac Workgroup Manager. The policies affected are:</p> <ul style="list-style-type: none"> • User Configuration>Centrify Settings>macOS 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 <p>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 macOS installed. In each case the behavior is consistent with Mac Workgroup Manager (7904).</p>

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->macOS 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" -> "macOS 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" -> "macOS 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 macOS "Print & Fax" System Preference Pane after the the Centrify group policy 'User Configuration' > 'Centrify Settings'> macOS 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->macOS 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" -> "macOS 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" -> "macOS settings" ->"802.1x settings" -> "Enable Machine Wi-Fi Profile," a user must manually select an identity cert-key pair for use in authentication. macOS 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	The Centrify Group policy: User Configurarion->Policies->Centrify Settings->macOS Settings->Security&Privacy", enable "Require password to wake this computer from sleep or screen saver" may not work in some scenarios

		when changing the time value. (CC-50135).
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 / 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	Login / Authentication	<p>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).</p> <p>Changed:</p> <pre>adclient.user.lookup.cn: true adclient.user.lookup.display: true</pre> <p>to:</p> <pre>adclient.user.lookup.cn: false adclient.user.lookup.display: false</pre>
All Mac	Login / Authentication	<p>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 username will fail. Using the form domain/username with a single forward slash "/" does work.</p> <p>Example:</p> <pre>swim/stest1 PASS swim//stest1 FAIL swim\stest1 FAIL swim\\stest1 FAIL</pre>

		(9413).
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	When using a computer configured with the Group Policy "Computer Configuration" -> "Centrify Settings" -> "macOS 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	Centrify Infrastructure Service release will align with Cloud release train number: i.e. there will be no 2018.x, instead it will be 18.8 (for 2018.1), and 18.12 (if we release in Dec). Note that we don't have a cloud release in Dec. This is yet to be discussed with PM Note: component version number stays the same: e.g. CDC is still 5.x.x. (CC-58646)
All Mac	Misc	Add a parameter in centrifydc.conf to control the feature that the adclient merges SPN automatically. (CC-56106)
All Mac	Misc	Add Mac to Windows Workstations login Policies. Currently, Admin Portal has a section under Policies -> Login Policies called Windows Workstations, where you can create rules for the authentication profiles to use for Mac or Windows workstations (add rule, filter by OS).(CC-53586)

All Mac	Misc	Take out enrollment prompt when logging into User Portal on Safari, if not all browsers. (CC-52319)
All Mac	Misc	Support certificate pinning for Mac Cloud Agent. Malicious hackers can do a Man in the Middle Attack on our Cloud Agent if they install a root certificate that allows them to receive and modify https requests from the client. (CC-49484)
All Mac	Misc	kcopycreds seems to be overwriting the host ticket with a ldap ticket (CC-48216)
All Mac	Misc	Using one cert-key pair for both 802.1x wifi and ethernet connection. Customer observed that there are different private for different 802.1x profile in keychain. Customer would like to use only one certificate for both wifi and ethernet 802.1x connection. (CC42824)
All Mac	Misc	[RFE] Register NTLM domain value in opendirectory attribute to enable compatibility with Websense Endpoint agent (Bug 79681) (CC-2734)
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. To login with CAC identity, the PIV identity would need to be deleted from AD. (27870).
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

		<p>Keychain instead of the valid one. The workaround is to manually copy the valid certificate into the Mac's keychain.</p> <p>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).</p>
All Mac	Smart Card	<p>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).</p>
All Mac	Smart Card	<p>If a Smart Card is inserted and left in the Smart Card reader during a restart, when the macOS 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).</p>
All Mac	Smart Card	<p>Screen saver shows password not PIN prompt: Most smart card users can log on with a smart card and PIN only and cannot authenticate with a username and password. However, it is possible to configure users for both smart card/PIN and username/password authentication. Generally, this set up works seamlessly: the user either enters a username and password at the log on prompt, or inserts a smart card and enters a PIN at the prompt.</p> <p>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).</p>
All Mac	Smart Card	<p>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).</p>
All Mac	Smart Card	<p>When using a Name Mapping User, Microsoft Outlook will prompt for a PIN when sending encrypted mail. (45658).</p>
All Mac	Smart Card	<p>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</p>

		workaround is to use FileVault2 if possible. (39711).
All Mac	Smart Card	Made an update to PIV.tokenend to support PIV-5 and PIV-C cards. This update may only work for Macs on 10.13 or higher depending on the certificate provisioned on the card. (CC-60497)
All Mac	Smart Card	Smart Card login required to exempt SSH, but not console (CC-59519)
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)

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

The Centrify Resources web site provides access to a wide range of information including analyst report, best practice brief, case study, datasheet, ebook, white papers, etc., that may help you optimize your use of Centrify products. For more information, see the Centrify Resources web site:

www.centrify.com/resources

Copyright (C) 2004-2020 Centrify Corporation. All rights reserved.