Centrify® Cloud 16.4 Security and Known Issues

Security

- An internal database function is now disabled that could have allowed remote code execution in the cloud service back end (CC-37861).

- Resolved a potential external entity attack vector in the federation feature by disabling DTD processing (CC-37144).

- Two other minor security issues were resolved in this release.

Known Issues

The following sections describe common known issues or limitations associated with this release of Centrify Cloud.

Centrify Identity Service

Cloud Manager and User Portals

- Downloading certificate fails on Windows Server
  Certificates are encrypted files and Windows Server defaults to disallowing IE from downloading encrypted packages to disk. To download the certificate for a SAML Web application or the APNS certificate on Windows server go Internet Options in IE and uncheck:

  Advanced → Security section → Do not save encrypted packages to disk

- Portal dialogs do not close on Firefox
  Firefox browser security settings can prevent portal dialogs from closing when the close button is clicked. To change the setting to allow dialogs to close:

  - Type "about:config" in the Firefox address bar
  - Search for the "close" keyword
  - Change the "dom.allow_scripts_to_close_windows" setting to "true"

  (CC-17079, 73662)

- Uploading image in Account Customization page has Save button grayed
  The Save button is not enabled after loading a login or portal image in the Account Customization settings page in the Cloud Manager unless another field on the page is also changed. If you wish to change only the image, modify a text field and then remove the modification and the button will be enabled (CC-18892).

- Previews for TIFF and DIB image file logos may not show in Cloud Manager
  Uploaded image files on the Account Customization page in Cloud Manager may not preview if they are TIFF or DIB format. This appears to be a limitation of the image file

formats supported by each browser. JPEG, PNG and GIF files should preview on all supported browsers (CC-17462).

- Bulk user import using CSV file with IE fails
  Internet Explorer tries to open files in the browser if there is no program associated with a given file extension. To work around this, assign a default program, such as Excel or other csv editor, to the csv extension as follows:

  Go to Control Panel
  → Default Programs
  → Associate a file type or protocol with a specific program

  Find the csv extension and associate your preferred program with it (CC-20070).

- Feedback email does not function in User Portal help in Chrome
  The email icon on the top right of the online help screen allows feedback about the documentation to be provided to Centrify support. This does not function using Chrome. To give feedback in this manner, use an alternative browser (CC-20155).

- Multiple user accounts with the same email address
  Although it is possible to create multiple user accounts that have the same email address, logging in using that email address is not supported as it is not possible to definitively map the email address to a single user (CC-21536).

- Missing icons with Internet Explorer
  Depending on IE's security settings, some icons may not be shown in the user portal. Some icons are distributed to browser sessions as fonts, and if these are restricted then the icons will not show on the screen (CC-2893).

- Reports using Cloud.Core.DirectoryUserChange event
  If you have a custom report that uses the Cloud.Core.DirectoryUserChange event, this event has been replaced by the Cloud.Core.DSEntityChange event and you should update your custom reports. The new event has a property "Classification" that can be used to filter for object type, for example

  Where Classification = 'User|Group|Contact|Resource|Other'

  (CC-3179).

- Smart Card login with IE browser
  On Internet Explorer browsers, the "Insert Smart Card" prompt is hidden behind the certificate loading page. Minimize the browser to see the prompt (CC-34118).

- Two certs displayed when logging in with Smart Card on IE and Chrome
  On IE/Windows and Chrome/Mac, two identical certificates will be displayed, but only one is valid. The browsers randomly display the certificates so unfortunately we cannot help you identify the valid one (CC-34117).

App Capture

- Login form only shows after clicking button or link on Web site
  If the login form only shows after clicking a button or link on the Web site being captured, app capture will not correctly capture the app at this time (CC-22790).

Apps

- The Chrome browser extension requires a permission in "Your privacy-related settings" and users will be prompted to allow it (CC-34169).

- For the Office 365 v2 app, the application ID (the name the mobile app uses to find this application) must be all-lower case, or the mobile app will fail to find the app. You can view / set the application ID in:

  Application Settings → Addtional Options → Application ID

  (CC-28072).

- Configuring Zoho for SP-initiated authentication
  When copying the login URL from the Cloud Manager and pasting into the Zoho Web site, add "amp;" after the ampersand (&) sign in the URL you are pasting (CC-12261).

- No certificate found error when SSO to Webex using SAML
  When you import SAML metadata into Webex and replace an existing certificate, it is possible that the certificate may not actually be changed even though the Site Certificate Manager shows that it is. If you have previously uploaded a certificate you should first remove it using the Site Certificate Manager before importing the Cloud Service SAML metadata (CC-12370).

- Problems launching Arrow Electronics Europe app
  Arrow are using an incorrect certificate on their Web site at the moment, so all browsers will fail to load this app correctly. On IE 10, click Show all content, then after about 10 seconds the app will open correctly. On some versions of Chrome you need to confirm that the script should be run, then again after about 10 seconds the app will run. Firefox will abort the connection, so you should use a different browser to run this app (CC-14828).

- Using Aribaexchange app with IE10
  Aribaexchange does not appear to support IE10 currently, although the site does work with earlier IE versions as well as Firefox and Chrome (CC-14762).

- Using AIM with mobile devices
  The AIM app is designed to work in the browser version of the User Portal. To use AIM on a mobile device you should use the AIM app available in your mobile device's app store (CC-14680).

- Using Windows Azure app with mobile devices
  The Windows Azure app requires Silverlight to launch but this is not currently supported by iOS or Android, so this app should not be used on mobile devices (CC-14226).

- Using My Memova with Internet Explorer 10
  With default settings, launching My Memova will launch to a blank page on IE10. Changing the document mode setting to IE7 will allow the app to launch correctly (CC-14760).

- Asana does not support Internet Explorer
  The Asana app does not support Internet Explorer. Please use another browser in order to use the Asana app (CC-15287).

- Gliffy app does not support mobile devices
  The Gliffy app does not appear to support mobile devices at this time so it should only be used on Windows and Mac (CC-15137).

- ClickTime app does not support mobile Chrome browser
  The ClickTime app does not appear to support the mobile Chrome browser at this time (CC-16537).

- Using the Webex SAML app with users defined in the Centrify User Service
  If you have users created using Centrify User Service, in order to use the WebEx SAML application go to the Application Settings page of WebEx, under "Map to User Accounts" and instead of selecting "Use the following Active Directory field to supply the user name" with "samaccountname" for the "Attribute Name, select the "Use this Script" option instead with the following script:

  ```
  var username = LoginUser.Get('userprincipalname');
  var shortname = username.replace("@YOUR-DOMAIN.com", "");
  LoginUser.Username = shortname;
  ```

  (CC-17315).

- In this release only one configured Office 365 app is supported
  The ability to configure multiple Office 365 apps may be supported in a future release (CC-13690).

- Error encountered with SSO on Android Dropbox app
  On the Samsung Galaxy S4 and Galaxy Note 3 running Android 4.3 an error occurs with the native Android Dropbox app when using single sign-on and the built-in Internet browser. This issue has been reported to Dropbox and may be resolved in a later update of the Dropbox app. To work around this issue, install Chrome for Android in place of the built-in Internet browser (CC-19165).

- Repeat login failures on Box app
  Three consecutive login failures triggers Box to force users to input CAPTCHA for the account. After a successful login this requirement is removed (APPS-6327).

- Updating settings for Egnyte app is rate limited
  You may only change the settings for the Egnyte app a maximum of ten times per hour as the API is rate limited. This is a limitation with Egnyte's API (CC-28780).

- Certificate error when changing App Gateway external URL
  When you save a changed App Gateway external URL you may receive an error that no certificate is found. To resolve this issue simply re-upload the certificate (CC-31343).

- Updating guests in the Yammer app
  Yammer APIs only allow creating and deleting users, they do not allow updating Yammer guests (CC-4228)

- SSO with Chromebook
  When the Centrify for Chromebook app is installed and started the user portal opens and the user is logged in using single sign-on. If the user clocks "Logout" from the Chrome browser, the cookie is lost and SSO will fail if the Centrify for Chromebook app is restarted (CC-5370).

- OpenID Connect and app gateway
  For this release of OpenID connect support there is no App Gateway support. App gateway support will be added in a future release (CC-32645).

- Cannot block access for rich clients in Office 2016
  Office 2013 / 2016 thick clients will not work using ADAL as Microsoft does not support this (CC-36869).

- Policy restricting IP address range slow to take effect on Office 365
  The policy "Restrict app to clients within corporate IP range" is slow to take effect on Office 365. If a device is disconnected from the corporate network while logged in, it can connect to Office 365 on an external network if attempted immediately. After a period of time (which may be up to 72 hours) the policy will take effect (CC-31492).

Centrify Privilege Service

- Recorded Windows sessions are always shown as In progress in Centrify DirectAudit Audit Analyzer console if the RDP session is initiated from the Centrify Privilege Manager portal via IE9 (CC-4281).

- Centrify Privilege Service has a compatibility issue with the HP-UX 11.23 PA SSH server, version 3.7, and SSH to HP-UX 11.23 PA Trusted Mode will not work. We suggest you upgrade to a later SSH server upgrade or use Centrify OpenSSH in the Centrify Server Suite (CC-2670).

- Audit events for secure shell sessions are recorded as Windows logon audit events if you use Centrify Privilege Service to log on to a UNIX or Linux computer (CC-30466).

- UNIX machines may have different types of accounts. For example, NIS user account, Active Directory user account and local user account. Centrify Privilege Service supports password management for local user account only. If other types of account are specified, the account health status might display "Failed" (CC-2616).

- Copy and paste feature is not working properly if SSH console is launched from Firefox and Safari in Mac OSX (CC-3973).

- To store the password in a SafeNet KeySecure appliance, Centrify Cloud Connector 15.10 or above is required (CC-5656).

- Centrify Privilege Service records all the password related activities, including password checkout, password update and viewing the retired passwords; they can be found in the activity tab of the resources. For activity records for viewing the retired passwords, the activity description mentions the date and time when the password was retired. This date is displayed in the GMT time zone rather than the local time zone (CC-34644).

- RDP session may get disconnected after 5 minutes if there is no user input. This problem happens only on Windows 2008 R2 running on Azure. It does not happen if Windows 2008 R2 is not running on Azure. It also does not happen when RDP into Windows 2012 R2 or later version of Windows OS on Azure (CC-4283).

- Centrify Privilege Service fails to manage the account password on a Juniper switch if there is another account sharing the same UID (CC-33459).

- Emailing the Administration Activity report from Cloud Manager cannot be completed successfully in this release (CC-34920).

- Some of the CLI commands provided in CLI toolkit requires user to type provide password. For example, cjoin and csetaccount. If user terminates the CLI commands by CTRL+C at this time, terminal state will be corrupted. The newly entered commands will not be able to show on the new line. Please run command "reset" to fix this (CC-35194).

- If a SafeNet appliance is used to store the password for Privilege Service, the SafeNet appliance firmware must be version 8.2 or above (CC-35809).

- For the UNIX machines with Centrify Server Suite installed and it is configured to use Centrify MFA in the login, CPS login session pauses at the prompt if Centrify Server Suite is configured to use a custom password prompt and the custom password prompt does not start with the word "Password". Hitting enter will continue the logon. This is a known issue.

- To avoid this behavior, please make sure the custom password prompt starts with the word "Password". For example, "Password for AD account" (CC-35567, CC-35397).

- SSH and RDP remote sessions do not accept any input after the Cloud Connector is upgraded to a newer version. Rebooting the Cloud Connector fixes this issue (CC-33242, CC-37845).

- For Windows machines configured to use only 15-bit color depth for remote sessions, remote access to the machine via CPS does not show the color and screen correctly. Setting the machine to use 16-bit color depth will fix the issue (CC-37770).

Centrify Cloud Service Platform

User Enrollment

- The Android app requires a minimum password length of 4 (CC-7884).

- Need to tap login button twice on Samsung Galaxy Tab
  When enrolling on a Samsung Galaxy Tab running Android 3.1 you will need to tap login twice. Tapping login the first time will show the device admin warning screen; after accepting this, the login screen is displayed again and you should tap the login button again to start the login process (CC-8082).

- Enrolling a Mac that is also joined using Centrify Server Suite
  Macs that are joined to the domain using Server Suite should enroll to the same OU as they are currently joined or the enrollment will fail. If users attempt to enroll joined Macs and the OUs are not the same they will receive 404 – Enrollment errors (CC-14177, CC-14901).

- Existing SAML apps and federation
  Existing SAML apps may need to be updated to use a tenant-specific URL for login in order to work with federated users (CC-33372).

- Manual configuration of federation
  Support for IDP Logout is not supported in this release when a federation is manually configured. IDP Logout is supported when using IDP metadata (CC-33333).

Cloud Connector and Administration

- High memory / CPU usage by Cloud Connector
  A caching facility has been added to the cloud service and cloud connector which can cause high CPU / RAM usage while the cache is building and may last several hours, depending on the number of Active Directory users and the number and type of Active Directory groups used. However, after the cache has built the CPU / memory usage should reduce significantly. Please contact Centrify Support for options to reduce the peak CPU / memory usage if this cannot be supported by the hardware used (-).

- Disabling a user does not remove profiles
  If a user is disabled in Active Directory their profiles are not removed from the device (-).

- Only one Exchange profile installed if two profiles specified
  If you create two Exchange profiles with different profile names but pointing to the same Exchange host, only one profile will be installed (CC-7626).

- Ratings region cannot be set to region other than the US
  The GP setting "Restrictions Settings" has the ability to set the region to locations other than the United States, but this setting never reflects on an iOS device due to an Apple bug. This issue will be resolved once Apple provides a fix (CC-7619).

- WiFi will auto-connect even if the GP is set to not auto join
  This is due to the different way Android and Apple devices behave with WiFi settings (CC-8106).

- Deleting the ManagedBy property prevents device from being managed
  Centrify Identity Service uses the ManagedBy property in the device's property pages to provide a link to the user using the device. Therefore, if you delete the ManagedBy property value the device can no longer be managed (CC-7095).

- Changing APNS certificate causes previous devices to be unreachable
  If you change the APNS certificate after enrolling some iOS devices in the Cloud Service, those devices enrolled with the previous APNS certificate will be unreachable. If you have to change your APNS cert for some reason, ensure all currently enrolled devices are unenrolled first (CC-9819).

- Integrated Windows Authentication (IWA) fails through Web proxies
  Integrated Windows Authentication (IWA) uses negotiation between a user's Web browser and an online Cloud Connector instance to validate the user's identity. If connectivity between the user's Web browser and an online Cloud Connector is not possible (e.g. the user is not on premise) or if that connectivity flows through a Web proxy, then IWA will silently fail and the user will be presented with the standard login process (CC-12126).

- Using IWA with a Cloud Connector machine running a firewall
  To support IWA, you should check and ensure that http traffic is allowed to the Centrify.Cloud.Core.ProxyHost.exe executable for any/all networks on the Cloud Connector machine (CC-15625).

- Close ADUC before upgrading Cloud Connector
  If the Active Directory Users and Computers (ADUC) extension for the Centrify Cloud Service is installed, you should close ADUC before upgrading the Cloud Connector or the upgrade will fail as ADUC will have the extension open, preventing the binaries from being updated (CC-12447).

- Users moved to another Active Directory container/OU are unenrolled
  Active Directory users that are moved from one container / OU to another may find that their devices are unenrolled. In a future release users will no longer be unenrolled in such a case, but for the time being users who find themselves unenrolled due to this should re-enroll their devices (CC-20124).

- Use of Active Directory administration tools
  If you wish to use the Active Directory administration tools such as the ADUC plug-in or the Group Policy extension on computers not running the Cloud Connector, you should ensure you log into those computers with a local system account rather than a service account (CC-20059).

- Deleted AD users exist in roles and users list
  If the connector does not have permission to query deleted objects then deleted AD users will remain in the roles and users list after deletion, but these users will no longer be allowed to login. To remove deleted users, either give the Cloud Connector the

necessary permission or manually remove them from the user list and role member list (CC-31317).

Workflow

- The description column on the requests page (accessed via the requests tab) is English-only for the current version. In a future release this will be localized to the same language set as the rest of the Cloud Manager (CC-4928).

Multi-factor Authentication (MFA)

- Ensure required data for each selected authentication factor is present
  When selecting the use of a secondary factor (SMS, phone, email, etc) you should ensure that the data is present in Active Directory for all users otherwise it is possible that users with missing data may be locked out. You can specify a preferred factor and if not present an alternative factor will be used. For example, if a user has no phone number in AD and SMS was the preferred factor, the cloud service will fall back to another selected factor (for example, email). If there is no phone number or email in AD in this case, the user would effectively be locked out.

- Email as an MFA mechanism is subject to spam / junk filters
  Be aware that using email as an MFA mechanism may be affected by users' email providers' spam or junk filters.

- SMS / phone are only attempted once a password is validated
  This prevents spam and billing issues if an attacker attempts to brute force passwords to gain entry.

- Can't close email authentication page on Firefox (CC-17079)
  This is due to Firefox security setting not allowing scripts to close browser windows, a workaround is:

    - Type about:config in the firefox address bar
    - Now search for close keyword
    - Look for dom.allow_scripts_to_close_windows setting and set the value to true

- High auth "lock" icon shows incorrectly
  It is possible for the high auth "lock" icon to show for an application for which it should not, and vice versa. The app should launch / not launch as expected, the issue is only with the display of the icon (CC-20895).

- Controlling high authentication behavior
  Although it is possible to set the authentication level to high or low within an app script, the portal login behavior is controlled only by policy, not app policy (CC-28309).

iOS Devices

- Cannot unenroll iOS device while it is waiting for group policies
  You should wait for an enrollment operation to complete, including receiving group policies, before unenrolling an iOS device (CC-9404).

- Cannot establish VPN connection on iOS device using 56-bit encryption
  In this release MPPE 56-bit encryption cannot be used for VPN connections, you should use MPPE 40- or 128-bit encryption instead (CC-9109).

- Error when proceeding to App Store during mobile app download
  When you tap on the link provided in an enrollment invitation email and you do not currently have the Centrify mobile app installed, you are taken to an enrollment landing screen with a "Proceed" button to take you to the App Store. Tapping on this button will show a "Cannot Open Page" error from Safari. Tapping OK at this point will proceed to the App Store normally (CC-37423).

Android Devices

- Always vibrate on email notification does not function on Samsung KNOX devices
  The Samsung KNOX Device Exchange GP setting "Always vibrate on email notification" does not function in this release of the Centrify app, the vibrate setting remains at the user's current setting (CC-12312).

- Some Samsung KNOX devices do not support PKI auth for VPN or WiFi
  Appears to be a device specific issue with Galaxy III on Android 4.0.4, Galaxy Tablet 2 on Android 4.0.3 and Galaxy Note II on Android 4.1.1 (CC-11847, CC-11806).

- Changes in account name in Cloud Manager does not show on Android devices
  Any changes made to the account name in the Cloud Manager are not reflected on enrolled Android devices. The account name is only set on enrollment (CC-11880).

- HTC One X cannot accept passcodes with minimum number of complex characters restriction greater than zero. This appears to be a limitation of this device as other devices do not have the problem (CC-11700).

- In this release, Samsung KNOX Device app management restrictions only apply to Samsung KNOX Workspace devices. In a future release this will be expanded to other KNOX devices (CC-14149).

- Notify on receiving new mail does not function on KNOX devices
  The Samsung KNOX Device Exchange GP setting "Notify on receiving new mail" does not function, the setting remains at the user's current setting. This appears to be an issue with KNOX devices (CC-12327).

- Must remove the KNOX container in order to re-enroll
  In order to re-enroll a Samsung device with a KNOX container, you should wait for the container to be completely removed before trying to re-enroll. The reason for this is that there can only be one KNOX container on a device and the enrollment may fail if it tries to auto-create a container before the old container is completely removed (CC-15248, CC-14399).

- Samsung Galaxy Note II does not accept WPA/WPA2 setting in GP
  Some versions of the Galaxy Note II firmware do not accept the WPA/WPA2 setting in the WiFi group policy. Settings → WiFi shows that the setting has been made but it is not possible to connect to the network (CC-12464).

- Cannot login to bookmark app whose url is "ftp://***" on Android mobile device
  The stock Android browser doesn't support ftp (CC-15328).

- Provide only numeric passwords when trying to lockout device
  When trying to lockout a device, admin would be prompted a password, please use only numeric passwords (CC-17741).

- Exchange email on Samsung Galaxy S4 running older Android version does not have the "Load more details" button. This is a known Samsung Galaxy S4 device issue and is fixed after build JDQ39.I9505ZHUDMI1 (CC-17874).

- Cannot set password containing complex characters on HTC One X
  If the minimum number of complex characters password policy is set, it is not possible to change a password on the HTC One X. This appears to be an issue with the OS on the HTC One X and may be fixed by a later ROM upgrade (CC-19444).

- Camera app stops on LG Nexus 5 when GP applied
  The camera app stops on the LG Nexus 5 when the Permit/prohibit camera use group policy is applied to it. This effect has been observed with Android 4.4 but appears to be resolved with Android 4.4.2 (CC-19908).

- Cannot configure Exchange account on Samsung Galaxy S4
  It is not possible to successfully configure an exchange account on a Samsung Galaxy S4 running Android 4.2.2 if the UPN is used for the user name. This issue does not exists with later Android versions (CC-23091).

Mac OS X

- For Macs that are both joined to a domain using DirectControl and enrolled in the Cloud Service, unenrolling the Mac will cause it to go into DirectControl disconnected mode as the same Active Directory object is used for both DirectControl and the Cloud Service. If you wish to unenroll a Mac that is also using DirectControl, you should first leave the domain, unenroll and then re-join the domain. Similarly, leaving the domain results in profiles being removed if the Mac is also enrolled (CC-12673).

- Cannot open Profiles after unenrolling device
  Occasionally, after unenrolling a device, opening the Profiles setting in System Preferences will hang at "Loading Profiles". If this happens, restart the Settings app (CC-13832).

- Using Certification validation method GP with OS X 10.7.5
  Setting both options for this GP to Require for all certs causes Macs to fail to load GPs while enrolling. To work around this issue, you should delete the cert revocation plist file as follows:

rm -rf /Library/Preferences/com.apple.security.revocation.plist

and re-run enrollment (CC-13967).

- Mac app management features and root user
  Mac app management features cannot be used when the user is logged in as root on the enrolled Mac (CC-2072).

- Mac may not respond to commands / policies after enrollment
  In some circumstances a Mac may not respond to commands or apply policies for a period after enrollment. This is usually caused by apps being pushed to the Mac as part of enrollment and will resolve itself once the apps are deployed (CC-33790).