

Zero Trust Privileged Access Service 19.5 – hot fix 4

Security and Known Issues

Security

- Fixed a minor vulnerability in using Google Directory Service - Google Directory users are now blocked from login if the client is disconnected or MFA is disabled. (CC-68769, CC-68750).

The following were resolved in 19.5 hot fix 4:

- Resolved vulnerabilities to cross site scripting (XSS) attacks in the Reports tab (CC-71622, CC-71764).
- Resolved vulnerability to XSS attacks in the Web Applications tab (CC-71848).
- Resolved vulnerabilities to XSS attacks in the Policies tab (CC-71852, CC-71862).

Known Issues

The following sections describe common known issues or limitations associated with this release of Zero Trust Privileged Access Service (PAS).

Privileged Access 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 Identity 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 Infrastructure Services 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 Infrastructure Services 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 Connector 15.10 or above is required (CC-5656).
- 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 Infrastructure Services 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 Admin Portal 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 Infrastructure Services, 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).

- 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).
- Domain Local Groups may no longer be used in the resource permission and account permission pages. Domain Local Groups configured in a previous release will still function correctly. Please change to use Global Groups or Universal Groups (CC-39918).
- Microsoft's Edge browser is not supported by CPS in this release. Please use Internet Explorer, Chrome or Firefox instead (CC-4402).
- A user with Edit permission on an application cannot change the name or description in the application unless the user also has Edit permission on the associated resource and Check out permission on the associated multiplex account, if it is set. Similarly, a user with Grant permission on an application cannot change permissions on the application unless the user also has Edit permission on the associated resource and

Check out permission on the associated multiplex account, if it is set (CC-40897).

- The cflush command does not flush the cache in the name service cache daemon (nscd). If nscd is running, please run the following command instead to ensure the newly updated login shell in Agent Settings is applied:

```
nscd -i passwd
```

(CC-42713).

- Offline login mode (login with cached credentials) will be available to users who have previously logged in, but not for 80 seconds after a network outage event (CC-43018).
- The local client for the SSH feature does not support Active Directory users configured for MFA using Centrify DirectControl. You can challenge users for MFA using Infrastructure Services prior to providing the credentials (KB-8028).
- When using the cunenroll command with the -d (delete) option, any other credentials added manually to the same resource will also be removed without confirmation (CC-42815).
- A Permission Denied error will be displayed when launching a resource session from the User Portal if the Portal Login permission is set with csetaccount with the -p option (CC-44394).
- After locking your screen, and after a period of time, you will be challenged twice for your password. This applies to some versions of Ubuntu using LightDM display manager (CC-44637).
- The SSH gateway file transfer feature has some compatibility issues with Microsoft's SSH service:
 - Files larger than 1MB will fail when using the SSH gateway's file transfer feature with a Windows 10 system enabled with Microsoft's SSH service (CC-50120).
 - Users of the Windows 10 SSH client service may experience Connection Refused errors when using connection strings (CC-52034)
- The Privilege Service User (PSU) entitlement allows for the visibility control of systems, accounts, secrets and other objects. Note that if this entitlement is combined with the Privilege Service Portal User (PSPU), users with these entitlement combinations can view all resource types (CC-50688).
- Accounts in systems created by the default administrator (sysadmin) can be populated by users that belong to roles with the Privilege Service Administrator entitlement (CC-50285).
- In this release it is not possible to individually disable the AD, Web or LDAP proxies from Admin Portal > Settings > Network > Idaptive Connectors. These services are all enabled during connector registration. Any existing configurations (i.e. where one or all of the services is disabled) will be unaffected, however they cannot currently be

changed (CC-66599).

Agents

- Users can login to a Linux machine with Centrify Agent for Linux installed via their Centrify Directory user account as long as the account is granted AgentAuth permission on the Linux resource. However, the user is required to specify the full name of their Centrify Directory user account, including the domain suffix (e.g. username@yourdomain.com), if this is the first time the account is used to login to the machine. The short name can be used (i.e. the user name without the domain suffix) in subsequent logins (CC-42982).
- Starting from release 19.3, you need to set the MFA policy for Centrify Client for Linux under "Authentication Policies" → "Zero Trust Agents" → "Agent Login". In addition, if you specify to use the pre-created " - Always Allowed -" authentication profile, the user will still be challenged for MFA (CC-65176).
- Timestamps in the cloud agent logs are based on UTC (CC-63703).

Centrify Identity Service Platform

Admin Portal

- 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 Admin Portal 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 Admin Portal
Uploaded image files on the Account Customization page in Admin Portal 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).

- 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).
- 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).
- If a set is configured with users / roles and later a new application is added to the set, the existing permissions are not propagated to the new application. Permissions will be propagated if they are edited after the application is added (CC-60689).

User Enrollment

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

Centrify Connector and Administration

- Connector prompts for reboot in post manual update
When updating Centrify Connector to a newer version, the installer may intermittently prompt for unnecessary reboot to continue the update. This only happens in a manual update but not with auto-update. (CC-70383)
- Behavior of shadowExpire attribute with LDAP users
The behavior of the shadowExpire attribute with LDAP has been corrected but creates a breaking change between behavior in 18.11 and earlier, and 19.1 and later. To continue using the previous behavior, you should call Centrify support with the name of the LDAP DS name you have set in the cloud (CC-55975).
- UserType attribute for a user shows as NULL in a report
This is expected for users that have not yet logged in, it is not an error. The field will be updated once the user has logged in or an event occurs which causes the user to be refreshed (CC-54160).
- In some circumstances connector upgrades may fail because the connector cannot be stopped as part of the upgrade process. If this happens, please stop the connector process and manually upgrade the connector. If your connectors auto-update, you can download the latest connector package from the Admin Portal by going to

Settings > Network > Centrify Connectors

clicking Add Centrify Connector and then downloading from the 64-bit link in the first step (CC-43527).

- Integrated Windows Authentication (IWA) fails through Web proxies
Integrated Windows Authentication (IWA) uses negotiation between a user's Web browser and an online Connector instance to validate the user's identity. If connectivity between the user's Web browser and an online 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 Connector machine running a firewall
To support IWA, you should check and ensure that https traffic is allowed to the Centrify.Cloud.Core.ProxyHost.exe executable for any/all networks on the Connector machine (CC-15625).
- Close ADUC before upgrading Centrify Connector
If the Active Directory Users and Computers (ADUC) extension for the Centrify Identity Service is installed, you should close ADUC before upgrading the Connector or the upgrade will fail as ADUC will have the extension open, preventing the binaries from being updated (CC-12447).
- 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 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 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 Admin Portal (CC-4928).

Derived Credentials

- Minimum key length and signature algorithms supported
The minimum key length supported for derived credentials is 2048, a key size of 1024 will cause an error. SHA-256, 384 and 512 signature algorithms are supported, however SHA-224 causes an error and cannot be used (CC-39249).
- SSL handshake error with derived credentials
In order to use derived credential authentication against a Web server, you should configure your Web server host SSL certificate (both root and intermediate certs) to be signed with SHA256 only. SHA512 signed SSL certificates do not function on iOS devices (CC-39069)

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 Identity 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
- Occasional login failures when using third party RADIUS authentication
RADIUS should not be used for authentication unless all of your Connectors can reach the RADIUS server. Authentication is shared between the configured Connectors, so unless all Connectors can reach the RADIUS server the auth will appear to fail at random intervals. This issue will be resolved in an upcoming release (CC-40963).

iOS Devices

- 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).

Android Devices

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

Mac OS X

- For Macs that are both joined to a domain using DirectControl and enrolled in the Identity 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 Identity 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).
- Zero Sign On (ZSO) does not function with OS/X 10.12 due to an Apple issue. The issue has been resolved in OS/X 10.13 and later, so ZSO now functions for the latest releases of OS/X (CC-60782).