

New features

- Upgraded Centrify Privileged Access Request application in ServiceNow marketplace to support the New York release
- Documented support for SAML and MFA with Azure AD as an Identity Provider
- Documented support for SAML and MFA with Okta as an Identity Provider

End of life notification

This section contains notifications for upcoming termination of apps, features, programmatic access or device support.

- In this release 19.5, the minimum supported iOS version has been raised from 10.0 to 11.0. Devices running an iOS release prior to 11.0 are still able to access Privileged Access Service using the Centrify mobile app from a previous release; however newer features introduced after the mobile app was introduced will be unavailable (CC-69019).

Changes in 19.5 hot fix 4

The following security issues 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).

Changes

The following list records issues resolved in this release and behavior changes.

- Starting with release 19.5, newly provisioned Centrify tenants will be using new tenant URLs in this format, <tenant>.my.centrify.net.
- Here are a few UI changes: (1) Reports are now under Builtin Reports -> Resources, (2) Import tab is available on Web Apps page, (3) Export tab is also available (CC-67432).
- The time format on the workflow approval screen is changed to 24-hour format from 12-hour format (CC-67605).
- Web apps launched in admin portal are now launched in their own new tab (CC-69861).
- The following features are available: (1) an end user can set which device should receive notification via the Profile UI, (2) an admin user can see a default report

showing all registered devices, (3) an admin user can perform actions (Unregister Device) on the registered devices via the report, (4) an end user can perform actions on one's registered devices via the Profile UI (CC-67502, CC-67503).

- Local client support for RDP and SSH is now available on Mac (CC-65810).
- 'Use My Account' feature is now available to federated users (CC-67069).
- Partner Federation now also works with AD domain that is already registered as a login suffix (CC-68358).
- Fixed a bug that fingerprint is not working on Samsung 9.0 device (CC-67605).
- Fixed a bug that OATH OTP verification fails if MFA is enabled (CC-67930).
- Fixed a bug that 'Use My Account' feature does not work with sshd for OpenSSH version 7.8p1 or above (CC-68056).
- Fixed a bug in UK keyboard mapping on RDP web client (CC-68112).
- Fixed a bug that allows Domain Local Group being added to Role in PAS (CC-68272).
- Fixed an intermittent bug that the first MFA prompt does not work on iOS client (CC-68490).
- Fixed an intermittent bug that "Sync all apps" fails with an unhandled exception (CC-68884).
- Fixed a bug that vaulted account password is not expiring in a rare race condition (CC-69335).
- Fixed a bug that the command csetaccount returns with non-zero error code even in a successful execution (CC-69394).
- Fixed a bug that fails to add Sybase Database in PAS (CC-70175).
- Fixed a bug that adding a Centrify Directory User to a tenant fails with error saying, "The request failed with unhandled error." (CC-70204).