New features – 19.2 Hot Fix 2

The following apps have been updated:

- Lynda (User / Password)
- SEMRush (User / Password)

The following apps have been renamed:

- 1 and 1 → 1&1 IONOS

End of life notification

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

- In release 19.3 the minimum supported Android version will be raised from 4.2 to 4.4.2. Devices running an Android release prior to 4.4.2 will still be able to access the cloud service using a Centrify mobile app from a previous release, however newer features introduced after the mobile app was introduced will be unavailable.

Changes for hot fix 2

- Existing inbound provisioning rules (i.e. rules created in release 19.1 or earlier) can now be synced successfully using both incremental and full sync (CC-67078).
- Updates to the Idaptive Android and iOS mobile apps to allow a browser extension Web app to be launched from the mobile client built-in browser (CC-66904).
- The Computer Login and Privilege Elevation administrative right is now available for Idaptive-branded tenants (CC-66760).
- Single Sign-On is once again possible with the Symphony mobile app on both iOS and Android (CC-66310).
- Workday incremental and full inbound provisioning is once again possible (CC-67206).
- An Active Directory Federation Services (ADFS) plug in is now provided for Multi-Factor Authentication (MFA). The plug-in can be downloaded via the Admin portal,

Downloads section (CC-63658).

- The user interface responsiveness has been improved for the role members display when there are a large number of role members to display (CC-63772).

Changes for hot fix 1

- Security issue: events are now recorded for Oauth tokens, access can no longer be granted to the system without an audit trail (CC-66881).

Changes

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

- New installs of the self-hosted Centrify Privilege Access Service will default to the new Centrify user interface. If you upgrade an existing instance of self-hosted Privilege Access Service it will continue to use the legacy user interface until you explicitly switch to the new UI. See Centrify KB article 11539 for more information (CC-66924).

- The PAS report error output has been improved to provide more information about the error condition (CC-62183).

- The capacity of the service discovery feature can be increased in conjunction with Centrify Support to allow more complex environments to be completely discovered (CC-66427).

- Discovery no longer stops when an unwanted account type (for example system) is encountered, instead it now ignores the unwanted type and continues iterating through accounts (CC-66665).

- Only one login session event is now generated for a native SSH login session. Previously two events had been generated for each login (CC-65323).

- Systems no longer display with warning icons in the Top Systems Checkouts list on the Infrastructure dashboard (CC-64303).

- Inbound provisioning has been enhanced to support user specified / custom attributes (CC-65342).

- The IWA service now starts automatically after a connector auto-upgrade (CC-66213).

- Android OS 9 devices no longer show as “unknown” in the Endpoints dashboard Total Devices by OS Version list (CC-64887).”

- On Samsung devices with KNOX version 3 and above, it is now possible to configure a POP email account that uses SSL / TLS (CC-64974).