Realize your vision

Samsung SDS

IAM & EMM

Release Note

Version: 19.4
Published: July 2019

SAMSUNG SDS SAMSUNG

Publisher	Samsung SDS Co., Ltd
Address	125, 35-Gil, Olympic-Ro, Songpa-Gu, Seoul, South Korea

About This Release

- **The following apps have been updated and updated**:
  - 19.4 Android App
  - 19.4 iOS App

- **The following apps have been updated and renamed**:
  None in this release

End of life notification

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

- In release 19.4, the minimum supported Android version will be raised from 4.2 to 4.4.2. Devices running an Android release before 4.4.2 will still be able to access the cloud service using a Samsung mobile app from a previous version, however newer features introduced after the mobile app was introduced will be unavailable.

New Features

- **UltiPro integration:** Admins can now seamlessly import identities from Ultimate Software's UltiPro and provision them to their Active Directory which enables organizations to have an HR-driven primary system of record for user data, in addition to other identity sources across all the applications.

- **MFA for switching to the Admin Portal:** Admins can now enable MFA for switching from the User Portal to the Admin Portal. The new policy set up can be accessed by navigating to Core Services → Policies → Authentication Policies → Samsung Admin Portal.

- **Event-based LDAP Sync:** The sync of user information to the source LDAP directory can now be triggered based on pre-determined events, such as user login or token refresh.
- **Support for Multiple Local Directories in Account Linking:** For customers who have multiple local directories, Samsung now allows customers to select a preferred target directory for account mapping.

- **Usage-based Default MFA Method:** Users will now see the last-used MFA authentication method automatically selected in the MFA dropdown list for each of their devices.

- **Client-specific RADIUS Authentication Policies:** Admins can now create custom authentication profiles specific to individual RADIUS clients. This allows users to have multiple RADIUS authentication profiles that work with specific connections within a single organization. RADIUS settings are available in the RADIUS section of “User Security Policies”. .

- **Prevent Access from Specific IP Ranges:** Admins can now have greater control over the traffic accessing applications by blocking access requests from specific IP addresses or range of addresses.

- **MFA Bypass Report:** With this feature, admins can now run a report to identify instances where MFA requirement was temporarily bypassed to allow users access to the Samsung Portal.

Improvements and behavior changes

- **Android for Work Profile Security Challenge:** Admins can prompt Android Devices to ask security questions if a user attempts to access any work apps, provided a device policy controller is running in work profile mode. Users can be prompted for security questions by configuring “Require Passcode on Device” policy (Endpoint Policies > Common Settings > Mobile Settings > Security Settings) and by Enabling Work profiles (Enable Work Profiles > Android Management Settings). Changes were made to ensure compatibility with new Android operating systems.

- **Users can choose which mobile device receives notifications:** Admins can enable policy to allow user notifications on multiple devices. This feature allows users to define which of their enrolled devices receive notifications in the Samsung User Portal.

- **Improved support for SuccessFactors as an inbound provisioning source:** With this fix, customers can customize the list of custom attributes available in the source SAP Success Factors instance. To customize the list of attributes some tenant-specific settings are required. Customers would need to contact support to set the right configuration flag and the corresponding config data.

- **"PreferredDataLocation" Attribute in Office 365 gets overridden to "null" if not set:** When no value is set in Provisioning Script for PreferredDataLocation, then the value gets overridden with "null" in Office365 portal, which might affect the users who have this value set previously. As a workaround, we recommend that a valid value is always set for this attribute in the provisioning script.

- **Authentication method based on IP Range:** Admins can now define which type of authentication method is used based on IP range. For example, ZSO within the corporate network and MFA outside of the corporate IP range.

Known Issues

- **Unable to launch existing customized SAML applications**: User may run into an issue while trying to launch SAML applications, the user might get “you do not have access to this application, or the application has been removed.” error message. It is not a continually occurring issue. If the user runs into the error mentioned above, the workaround would be to re-configure the app setup and relaunch the app.

- **Modification of RADIUS attribute value is not allowed at the table level**: Admins should delete the attribute instead and re-add it with the desired changes.

- **“Next” icon on the connector wizard is disabled**: To change, repair, or remove Samsung connector, the admin needs to right-click on the connector executable and select “run as administrator” to see these options. Besides, admin can also perform the change, repair, or remove operations by uninstalling the connector from the Control Panel and installing it again.

Security Related Issues

- OAuth events have been added for client credential failures, both for unknown client IDs and bad secrets.
- In addition, one minor security bug was fixed in this release.
- The connector machine account can no longer be managed with a non-admin user.

Realize your vision SAMSUNG SDS

www.samsungsds.com