

Realize your vision



Samsung SDS  
**IAM & EMM**

Release Note



Version: 19.3  
Published: June 2019

Copyright © 2019 Samsung SDS Co., Ltd. All rights reserved.

Samsung SDS Co., Ltd. has complete trust in the information contained in this document. However, Samsung SDS is not responsible for any circumstances which arise from inaccurate content or typographical errors.

The content and specifications in this document are subject to change without notice.

Samsung SDS Co., Ltd. holds all intellectual property rights, including the copyrights, to this document. Using, copying, disclosing to a third party or disturbing this document without explicit permission from Samsung SDS is strictly prohibited. These activities constitute an infringement of the intellectual property rights of this company.

---

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 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 prior to 4.4.2 will still be able to access the cloud service using a Samsung SDS IAM&EMM mobile app from a previous release, however newer features introduced after the mobile app was introduced will be unavailable.

## New Features

- **Configurable OTP code length:** Admins can now specify the number of digits in the one-time password (OTP) sent to users in the email or SMS authentication messages allowing organizations to tailor the end-user authentication experience to match their corporate security policy.
- **MFA for Federated Users via account linking:** With this, our customers can deliver a seamless MFA experience in the scenario where they are using Samsung as the MFA provider for another IDP (for e.g. IBM etc). This also allows our customers to make Samsung SDS IAM&EMM as the consolidation point of identities by bringing those from other disparate identity sources and federating and augmenting those with additional attributes in Samsung SDS IAM&EMM as they launch applications federated with Samsung SDS IAM&EMM and made available to the other IDP through B2B federation.
- **Custom RADIUS attributes:** Admins can now define custom values and attributes that Samsung RADIUS server passes to RADIUS clients during the user authentication process. This enables admins to take actions and create policies based on these attributes and support vendor-specific attributes (VSAs) backed by different types of RADIUS clients.



## Improvements and behavior changes

- **Additional duration options for MFA pass-through:** Admins can now define a 10, 12, or 25-hour window for MFA challenge pass-through.
- **Search device table using phone number:** Admins can now use phone number to search for enrolled MDM devices in the device table.
- **Authorization Server Improvements:** The authorization server now supports HTTP POST method in OIDC and OAuth2.
- **SSO for federated user:** Service Provider (SP) Initiated login for B2B federated users for seamless launch of applications after authentication.

## Known Issues

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

.....

Realize your vision **SAMSUNG SDS**