Realize your vision

Samsung SDS

IAM & EMM

Release Note

Version: 19.2
Published: April 2019

SAMSUNG SDS SAMSUNG

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

Contents

About This Release

Samsung SDS IAM & EMM delivers Identity as a Service (IDaaS) for robust, Active Directory- and cloud-based single sign-on, access management, app management and mobile management across any cloud, mobile or on-premise application from a catalog of thousands of tested and pre-integrated apps.

With Samsung SDS MDM/MCM you can use Active Directory and Windows Group Policy to automate security policy enforcement, locate devices, wipe/lock devices as well as auto-issuance/renewal of certificates for strong authentication to Wi-Fi and VPN networks for end-users' Samsung KNOX, Android, Apple iOS and other mobile devices. Mobile application management (MAM) provides a customizable mobile enterprise app store for pushing and maintaining rich mobile client apps.

Samsung SDS IAM & EMM SSO delivers federation, password management and single sign on as a service. It has built-in multifactor authentication with Samsung Mobile Authenticator soft token, one-time passcode (OTP) via text/email and interactive phone calls. Samsung also delivers scriptable per app authentication policies to restrict access or require additional authentication factors.

Installation

Please refer to the Samsung SDS IAM & EMM support site for comprehensive instructions.

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 Samsung mobile app from a previous release, however newer features introduced after the mobile app was introduced will be unavailable.

New Features

With release 19.2, Samsung SDS IAM & EMM supports the following features:

Samsung Knox 3.3 readiness: Idaptive now works with Samsung Knox 3.3, released. We have completed full regression testing of our software with the latest version of Knox.

Account Linking: You can now use account linking to connect your users' various enterprise and social accounts with user accounts in your primary identity store. This allows you to build more seamless experiences and more complete, integrated profiles for your users; for example, you can now associate user's social login with an enterprise login, allowing users to use either to sign in to your applications and thereby mitigating the friction of forgetfulness during future sign-in attempts.

Custom ActiveDirectory (AD) attributes mapping for inbound provisioning: You can now map your custom AD attributes to the attributes in your Human Resource Systems such as Workday, SAP SuccessFactors, BambooHR for seamless provisioning from these source systems into AD. For example, you can define a new custom attribute called "additional_contact" in AD to store employees' additional phone numbers. You can then populate this field in AD during the provisioning process with employees' phone numbers stored in your HRIS system.

Palo Alto Networks integration for adaptive MFA: You can now feed insights collected by Palo Alto Networks' Cortex security platform into Idaptive Intelligent MFA solution. This allows you to improve the accuracy of your users' risk profiles and make smarter decisions about access in your organization. For example, you can now require users deemed as a threat by the Cortex security platform to pass additional Multifactor Authentication challenge. For more details, please visit this here.

Zero Sign-On (ZSO) for native mobile applications: You can now enable users to seamlessly and securely access native enterprise mobile applications, such as Workday, Salesforce, Zendesk, Concur, Workfront, and Slack via certificate-based authentication once their mobile devices are enrolled into the Idaptive Next-Gen Access Cloud. This allows you to simplify user access to enterprise apps, create more seamless experiences for your users, and prevent unauthorized access to corporate data. For example, you can now access the ServiceNow mobile app from an enrolled mobile device without manually entering your credentials. You can also prevent users from accessing your MS Office apps from any device that is not enrolled with the Idaptive Next-Gen Access Cloud.

MFA challenge for Zero Sign-On (ZSO) access: You can now require users to pass additional authentication challenge when accessing native mobile applications using ZSO, Idaptive's certificate-based authentication method. For example, you can enable users to seamlessly access non-sensitive mobile applications, such as Slack or Workfront without entering credentials. You can also require users to pass an MFA challenge to access applications that contain customer data, such as Salesforce and Concur. This allows you to tailor user experience when accessing enterprise apps and take additional steps to protect corporate data.

Continued Focus on Delivering Blazing Fast Performance: 19.2 also delivers optimizations to deliver speed and performance at scale to meet the requirements of large enterprises and for the CIAM market.

Security

One minor security issue was resolved in this release. Events are now recorded for Oauth tokens, access can no longer be granted to the system without an audit trail (CC-66881)

Resolved Issues and Behavior Changes

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

- It is now possible for users who either logged into the portal before their password expired, or who use IWA or certificates to login, to change their password once it has expired (CC-64966, CC-65063).
- Devices marked as personal can now successfully be imported to be corporate-owned (CC-64777).
- Android for Work mobile app deployment and auto-install once again work as documented (CC-60982, CC-63610, CC-63684).
- Reapply policy no longer removes bookmarks from the home screen on Android devices using Android 7 or earlier (CC-64498).
- Options to unenroll a device are now not shown if the selected device was enrolled via device-owner mode (CC-63779, CC-63372).
- In device-owner mode the delete command now wipes the selected device rather than unenrolling it (CC-63994).
- Where Partner Management has been configured between an external IdP (i.e. one that is not Samsung) and the cloud service, and a user has IdP single-signed on to the cloud service via Partner Management, it is now possible to launch SAML apps without the User Portal being visible during the launch / sign-on (CC-64706).
- Administrators now have the ability to assign a Windows machine to a user on the Endpoints page. A “Set User” command will be displayed if the Windows machine is not currently assigned to any user (CC-64748).
- Administrators can now create a custom login banner for the User Portal. Banners can be created in plain text in multiple languages, and once configured

will be shown to users on login until the button is clicked on the dialog. An event is logged when the user clicks the button (CC-64330, CC-64850).

- Administrators and users can now choose a default view for apps, choosing between grid or grouped, large or small icons, with/without titles (CC-64471).
- 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).
- 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).
- 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).
- 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).

Known Issues

The following sections describe common known issues or limitations associated with this release of Samsung SDS EMM&EMM Identity Platform.

Admin and User Portals

- Portal dialogs do not close on Firefox
    - 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)

- 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

- 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).

- Feedback email does not function in User Portal help in Chrome

  The email icon on the top right of the online help screen allows feedback about the documentation to be provided to Samsung support. This does not function using Chrome. To give feedback in this manner, use an alternative browser (CC-20155).

- 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).

- Missing icons with Internet Explorer

Depending on IE's security settings, some icons may not be shown in the user portal. Some icons are distributed to browser sessions as fonts, and if these are restricted then the icons will not show on the screen (CC-2893).

- Reports using Cloud.Core.DirectoryUserChange event

  If you have a custom report that uses the Cloud.Core.DirectoryUserChange event, this event has been replaced by the Cloud.Core.DSEntityChange event and you should update your custom reports. The new event has a property "Classification" that can be used to filter for object type, for example

  Where Classification = 'User|Group|Contact|Resource|Other'

  (CC-3179).

- 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).

App Capture

- Login form only shows after clicking button or link on Web site

  If the login form only shows after clicking a button or link on the Web site being captured, app capture will not correctly capture the app at this time (CC-22790).

Apps

- To give a user permission to edit the Application Permissions tab they must be assigned to a role with the Application Management right (CC-60762).

- Users with Application Management permission cannot add a linked app or enable application provisioning. In order to perform these tasks, you need system administrator permission (CC-60764).

- The Chrome browser extension requires a permission in "Your privacy-related settings" and users will be prompted to allow it (CC-34169).
- The form filling browser extension does not support apps that require high authentication. To launch a high auth, launch the app from the User Portal (CC-43978).
- For the Office 365 v2 app, the application ID (the name the mobile app uses to find this application) must be all-lower case, or the mobile app will fail to find the app. You can view / set the application ID in:

  Application Settings > Additional Options > Application ID

  (CC-28072)
- Configuring Zoho for SP-initiated authentication

  When copying the login URL from the Admin Portal and pasting into the Zoho Web site, add "amp;" after the ampersand (&) sign in the URL you are pasting (CC-12261).
- No certificate found error when SSO to Webex using SAML

  When you import SAML metadata into Webex and replace an existing certificate, it is possible that the certificate may not actually be changed even though the Site Certificate Manager shows that it is. If you have previously uploaded a certificate you should first remove it using the Site Certificate Manager before importing the Identity Service SAML metadata (CC-12370).
- Problems launching Arrow Electronics Europe app

  Arrow are using an incorrect certificate on their Web site at the moment, so all browsers will fail to load this app correctly. On some versions of Chrome you need to confirm that the script should be run, then again after about 10 seconds the app will run. Firefox will abort the connection, so you should use a different browser to run this app (CC-14828).
- Using AIM with mobile devices

  The AIM app is designed to work in the browser version of the User Portal. To use AIM on a mobile device you should use the AIM app available in your mobile device's app store (CC-14680).
- Using Windows Azure app with mobile devices

  The Windows Azure app requires Silverlight to launch but this is not currently supported by iOS or Android, so this app should not be used on mobile devices (CC-14226).
- Asana does not support Internet Explorer

The Asana app does not support Internet Explorer. Please use another browser in order to use the Asana app (CC-15287).

- Gliffy app does not support mobile devices

  The Gliffy app does not appear to support mobile devices at this time so it should only be used on Windows (CC-15137).

- ClickTime app does not support mobile Chrome browser

  The ClickTime app does not appear to support the mobile Chrome browser at this time (CC-16537).

- Using the Webex SAML app with users defined in the Samsung SDS EMM&EMM Directory

  If you have users created using Samsung SDS EMM&EMM Directory, in order to use the WebEx SAML application, go to the Application Settings page of WebEx, under "Map to User Accounts" and instead of selecting "Use the following Active Directory field to supply the user name" with "samaccountname" for the "Attribute Name, select the "Use this Script" option instead with the following script:

  ```
  var username = LoginUser.Get('userprincipalname');

  var shortname = username.replace("@YOUR-DOMAIN.com", "");

  LoginUser.Username = shortname;
  ```

  (CC-17315)

- In this release only one configured Office 365 app is supported

  The ability to configure multiple Office 365 apps may be supported in a future release (CC-13690).

- Error encountered with SSO on Android Dropbox app

  On the Samsung Galaxy S4 and Galaxy Note 3 running Android 4.3 an error occurs with the native Android Dropbox app when using single sign-on and the built-in Internet browser. This issue has been reported to Dropbox and may be resolved in a later update of the Dropbox app. To work around this issue, install Chrome for Android in place of the built-in Internet browser (CC-19165).

- Repeat login failures on Box app

  Three consecutive login failures triggers Box to force users to input CAPTCHA for the account. After a successful login this requirement is removed (APPS-6327).

- Updating settings for Egnyte app is rate limited

You may only change the settings for the Egnyte app a maximum of ten times per hour as the API is rate limited. This is a limitation with Egnyte's API (CC-28780).

- Certificate error when changing App Gateway external URL

  When you save a changed App Gateway external URL you may receive an error that no certificate is found. To resolve this issue simply re-upload the certificate (CC-31343).

- Updating guests in the Yammer app

  Yammer APIs only allow creating and deleting users, they do not allow updating Yammer guests (CC-4228)

- SSO with Chromebook

  When the Samsung for Chromebook app is installed and started the user portal opens and the user is logged in using single sign-on. If the user clocks "Logout" from the Chrome browser, the cookie is lost and SSO will fail if the Samsung for Chromebook app is restarted (CC-5370).

- OpenID Connect and app gateway

  For this release of OpenID connect support there is no App Gateway support. App gateway support will be added in a future release (CC-32645).

- MFA prompted twice launching app through app gateway

  If the challenge pass-through duration in the auth profile for an app is set to “No pass-through”, when the app is launched from outside the corporate through the app gateway, users will be prompted for MFA twice before the app can be launched. If the pass-through duration is set to any other time, then the user is only prompted once (CC-42440).

- Policy restricting IP address range slow to take effect on Office 365

  The policy "Restrict app to clients within corporate IP range" is slow to take effect on Office 365. If a device is disconnected from the corporate network while logged in, it can connect to Office 365 on an external network if attempted immediately. After a period of time (which may be up to 72 hours) the policy will take effect (CC-31492).

- Microsoft Dynamics CRM app usage

  The Microsoft Dynamics CRM (WS-Fed) application is intended to be used for on-premises scenarios, please see this link for more information. This application currently supports WS-Federation but not WS-Trust, and as a result Samsung currently supports only browser-based scenarios with Dynamics CRM on-prem. Samsung is working to add WS-Trust support for non-browser scenarios in a future release (CISSUP-2520).

- Errors when SCIM provisioning cloud users

  SCIM provisioning requires a UPN with a valid domain name suffix (CC-48394).

- Browser extension icon on IE toolbar shows as initializing

  Whenever the IE browser extension is freshly installed or updated, IE will prompt the user to approve the Samsung toolbar. Once approved, the toolbar icon will be displayed and will be shown as initializing. The icon will continue to be shown as initializing until IE is restarted due to a design limitation with IE (CC-45978).

- Browser extension on Firefox requires restart after upgrade

  The browser extension on Firefox does require Firefox to be restarted for the browser to recognize that the upgrade has completed and should no longer prompt for upgrade (CC-48555).

- Second AWS SAML app session logs out the first

  The AWS SAML app appears to handle only one logged in session per user at any one time. If you start a session in a browser tab and then later create another browser tab and repeat, the first session will be logged out (CC-49927).

User Enrollment

- The Android app requires a minimum password length of 4 (CC-7884).
- Need to tap login button twice on Samsung Galaxy Tab

  When enrolling on a Samsung Galaxy Tab running Android 3.1 you will need to tap login twice. Tapping login the first time will show the device admin warning screen; after accepting this, the login screen is displayed again and you should tap the login button again to start the login process (CC-8082).

- 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).

Samsung SDS EMM&EMM Connector and Administration

- 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 19.1 and later. To continue using the previous behavior, you should call Samsung 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 circumstance's 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 > Samsung SDS EMM&EMM Connectors

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

- Disabling a user does not remove profiles

  If a user is disabled in Active Directory their profiles are not removed from the device (-).

- Only one Exchange profile installed if two profiles specified

  If you create two Exchange profiles with different profile names but pointing to the same Exchange host, only one profile will be installed (CC-7626).

- Ratings region cannot be set to region other than the US

  The GP setting "Restrictions Settings" has the ability to set the region to locations other than the United States, but this setting never reflects on an iOS device due to an Apple bug. This issue will be resolved once Apple provides a fix (CC-7619).

- WiFi will auto-connect even if the GP is set to not auto join

  This is due to the different way Android and Apple devices behave with WiFi settings (CC-8106).

- Deleting the ManagedBy property prevents device from being managed

  Samsung SDS EMM&EMM Identity Platform uses the ManagedBy property in the device's property pages to provide a link to the user using the device.

Therefore, if you delete the ManagedBy property value the device can no longer be managed (CC-7095).

- Changing APNS certificate causes previous devices to be unreachable

  If you change the APNS certificate after enrolling some iOS devices in the Identity Service, those devices enrolled with the previous APNS certificate will be unreachable. If you have to change your APNS cert for some reason, ensure all currently enrolled devices are unenrolled first (CC-9819).

- 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 Samsung. Cloud.Core.ProxyHost.exe executable for any/all networks on the Connector machine (CC-15625).

- Close ADUC before upgrading Samsung SDS EMM&EMM Connector

  If the Active Directory Users and Computers (ADUC) extension for the Samsung SDS EMM&EMM Identity Platform 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).

- Users moved to another Active Directory container/OU are unenrolled

  Active Directory users that are moved from one container / OU to another may find that their devices are unenrolled. In a future release users will no longer be unenrolled in such a case, but for the time being users who find themselves unenrolled due to this should re-enroll their devices (CC-20124).

- 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).

- Communication from Identity Platform to Connector with Web proxy

  In order for the Identity Platform to communicate with the Connector when a Web proxy is used, the connector must be run as a domain account. This appears to be an Azure Service Bus limitation where it does not use the user name and password specified in the global Web proxy configuration for Kerberos or NTLM auth, instead it uses the process identity when the Web proxy challenges for authentication. This is not unreasonable in a Windows environment as most users would use a proxy that is in their domain and in such cases NTLM or Kerberos would succeed (CC-42250).

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)

Inbound Provisioning

- Cannot add second domain tree in a forest

  Where an AD forest has more than one domain tree (two or more root domains in the same forest), this release will allow you to add only one of them in the Settings > Administrative Accounts page (CC-44600).

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 is 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

- High auth "lock" icon shows incorrectly

  It is possible for the high auth "lock" icon to show for an application for which it should not, and vice versa. The app should launch / not launch as expected, the issue is only with the display of the icon (CC-20895).

- Controlling high authentication behavior

  Although it is possible to set the authentication level to high or low within an app script, the portal login behavior is controlled only by policy, not app policy (CC-28309).

- 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).

- Users cannot change their password in Samsung mobile apps if challenges are enabled for password change (CC-48275).

iOS Devices

- Prompt for Exchange credentials and mail re-sync on iOS devices

  If Exchange ActiveSync profiles are pushed to iOS devices via the Samsung cloud, when an administrator next manually updates device policies, or the user updates their Samsung iOS app, users will receive a request for their Exchange credentials, followed by a full re-sync of mail. This will be a one-time request and should not reoccur (CC-37402).

- Cannot unenroll iOS device while it is waiting for group policies

  You should wait for an enrollment operation to complete, including receiving group policies, before unenrolling an iOS device (CC-9404).

- 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).

- Error when proceeding to App Store during mobile app download

  When you tap on the link provided in an enrollment invitation email and you do not currently have the Samsung mobile app installed, you are taken to an enrollment landing screen with a "Proceed" button to take you to the App Store. Tapping on this button will show a "Cannot Open Page" error from Safari. Tapping OK at this point will proceed to the App Store normally (CC-37423).

- Updating from iOS 11 to iOS 12 with a VPN app installed (for example Cisco Anyconnect) may damage the user certificate, which will affect PKI Exchange / VPN / WiFi. The workaround is to reapply policies to any affected devices (CC-62194).

Android Devices

- Starting with Android Oreo on Samsung devices, Samsung KNOX generic and Samsung SSO have been deprecated. The Samsung for KNOX container application will now require the user to login using their credentials to gain access (CC-54955).

- Android 5.1.1 has a limitation with device lock with passcode, pushing the authenticator notification on the lock screen does not require unlocking the device. To work around this issue, in the Admin Portal, set Enforce App Pin > Fingerprint Policy, and on the device go to Settings > Hide Contents of the Notification. Then, once the user gets the notification they have to go to the Samsung app and that requires them to unlock the device (CC-53641).

- Shortcuts that are added to the home screen cannot be deleted from devices running Android 5.1.1 and later. This is an OS-enforced limitation (CC-50422).
- Always vibrate on email notification does not function on Samsung KNOX devices

  The Samsung KNOX Device Exchange GP setting "Always vibrate on email notification" does not function in this release of the Samsung app, the vibrate setting remains at the user's current setting (CC-12312).
- 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).
- HTC One X cannot accept passcodes with minimum number of complex characters restriction greater than zero. This appears to be a limitation of this device as other devices do not have the problem (CC-11700).
- In this release, Samsung KNOX Device app management restrictions only apply to Samsung KNOX Workspace devices. In a future release this will be expanded to other KNOX devices (CC-14149).
- Notify on receiving new mail does not function on KNOX devices

  The Samsung KNOX Device Exchange GP setting "Notify on receiving new mail" does not function, the setting remains at the user's current setting. This appears to be an issue with KNOX devices (CC-12327).
- Must remove the KNOX container in order to re-enroll

  In order to re-enroll a Samsung device with a KNOX container, you should wait for the container to be completely removed before trying to re-enroll. The reason for this is that there can only be one KNOX container on a device and the enrollment may fail if it tries to auto-create a container before the old container is completely removed (CC-15248, CC-14399).
- Samsung Galaxy Note II does not accept WPA/WPA2 setting in GP

  Some versions of the Galaxy Note II firmware do not accept the WPA/WPA2 setting in the WiFi group policy. Settings > WiFi shows that the setting has been made but it is not possible to connect to the network (CC-12464).
- Cannot login to bookmark app whose url is "ftp://***" on Android mobile device

  The stock Android browser doesn't support ftp (CC-15328).
- Provide only numeric passwords when trying to lockout device

When trying to lockout a device, admin would be prompted a password, please use only numeric passwords (CC-17741).

- Exchange email on Samsung Galaxy S4 running older Android version does not have the "Load more details" button. This is a known Samsung Galaxy S4 device issue and is fixed after build JDQ39.I9505ZHUDMI1 (CC-17874).
- Cannot set password containing complex characters on HTC One X

  If the minimum number of complex characters password policy is set, it is not possible to change a password on the HTC One X. This appears to be an issue with the OS on the HTC One X and may be fixed by a later ROM upgrade (CC-19444).
- Camera app stops on LG Nexus 5 when GP applied

  The camera app stops on the LG Nexus 5 when the Permit/prohibit camera use group policy is applied to it. This effect has been observed with Android 4.4 but appears to be resolved with Android 4.4.2 (CC-19908).
- Cannot configure Exchange account on Samsung Galaxy S4

  It is not possible to successfully configure an exchange account on a Samsung Galaxy S4 running Android 4.2.2 if the UPN is used for the user name. This issue does not exist with later Android versions (CC-2309).

Realize your vision SAMSUNG SDS

www.samsungsds.com