Realize your vision

Samsung SDS

IAM & EMM

Release Note

SAMSUNG SDS · SAMSUNG

Contents

1. 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 EMM 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.

2. Installation

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

3.   New Features

- Certificate auto-renewal for Android and iOS
    - Certificates are now automatically renewed
    - Effective for all mobile policies leveraging sets, including email, WiFi, VPN and the ZSO certificate.
    - Renewal request starts when 20% of the certificate lifetime remains.

- Delegated administration for end points via Sets
    - Endpoint administrators can now create and manage custom Sets of end points, beyond the built-in sets.
    - Assign policies to admin-defined sets of end points.
    - Ability to specify permissions for a user, group or role to Grant, View, Edit and Delete Sets of end points.

- Delegated administration for apps via Sets
    - Ability to create or delete a set of apps through the Admin Portal by either selecting apps manually or via a dynamic script
    - Ability to specify permissions for a user, group or role to Grant, View, Edit and Delete Sets of apps.
    - Ability to review recent activity on a Set.

- SAP SuccessFactors is now supported for inbound provisioning, provides seamless provisioning of user information from SAP SuccessFactors into Active Directory
    - Configurable provisioning rules enable:
        - Explicit mapping of attributes between SAP SuccessFactors and AD
        - Specifying AD group in which user can be created
        - Selective provisioning of all users or a subset (i.e. a business unit)
        - Periodic full sync or incremental syncs
        - Customizable attribute mapping via scripts
    - Deeper insight into provisioning status via job reports.

- The following apps have been updated:
    - Sydney Morning Herald (User name / Password)
    - JIRA Server (SAML)
    - Webex (User name / Password)
    - DocuSign (User name / Password)

4. End of Life Notification

This section contains notifications for upcoming termination of apps, features or programmatic access (APIs):

- From this 18.6 release, Connectors earlier than 17.7-108 will lose service if not upgraded. As a reminder, support is provided for Connectors running the current release and two prior releases, and running a connector from a prior release may limit the use of newer functionality.

5. Resolved Issues and Behavior Changes

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

- Unassigned users in a provisioning group from Workday are no longer synched to an Active Directory "test" group (CC-57998).

- Tagging a SAML app in the User Portal no longer generates an error (CC-54368).

- The Dynamic CRM plug-in now works using WS-Trust (CC-60305).

- New default load sample scripts are supplied in the Source to Target tab for Workday inbound provisioning (CC-57792).

- Report names can now include the pound ("#") symbol (CC-54880).

- The Export Reports and Email Reports commands have been restored to the option drop down in My Reports (CC-59978).

- The Samanage app configuration documentation has been updated (CC-59414).

- Users with the User Management right now have the right to update the policy needed to invite users (CC-60184).

- Users now need the Application Management or Read Only System Administration right in order to see the job history list (CC-60191).

- Users are no longer prompted for a certificate to use when attempting to Zero Sign On when using an external Certificate Authority but with no Certificate Authorities available (CC-59389).

- It is now possible to select more than one department in the Source Selection Rule for inbound provisioning (CC-60062).

- The Trace function now functions correctly in an Office 365 advanced script (CC-58773).

- Iterating in a SAML script through users who are members of a large number of groups no longer produces an exception (CC-59099).

- CNAME is now removed from DNS when the tenant URL is deleted in the Admin Portal (CC-60821).

- Exception no longer generated with SCIM provisioning when target app (for example TalentLMS) does not accept URL-encoded schema (CC-60618).

- Enterprise Grid Provisioning is now supported for Slack (RFE-1967)

- Clock drift tracking has been updated for OATH tokens to prevent mobile authenticator failures (CC-60952).

- A new policy has been added for default message language. By default, the language used is the message sender's language setting (i.e. the language setting for the administrator that caused the message to be sent), but that can be overridden to a specific language by setting the policy (CC-51721).

- Advanced script capabilities have been added to all SAML applications, previously this was only available on some SAML applications (CC-55466).

- When enrolling devices, if PKI certificates are defined by Active Directory group policy to be downloaded, three certificates are now sent: root CA, user CA and issuing CA. This matches the behavior when PKI certificates are defined in a cloud policy (CC-57705).

- An error is no longer shown when a user with read-only management right enters the Partner Management page (CC-58426).

- Emailed reports no longer show an error if a relative date type is set (CC-57562).

- Network unavailable is no longer shown on an iOS device using Safari when launching a bookmark app that has a mobile authenticator profile, with the MFA approval step on the same device (CC-58453).

- Phone numbers for newly enrolled Android devices are now correctly shown in the Admin Portal (CC-58622).

- Resolved an issue whereby some iOS native apps would continuously prompt for update due to two different version numbers inside the app (CC-58652).

- Administrators can now block access from the Samsung SDS IAM&IAM mobile app to various domains in the firewall policy for Android devices. Individual domains can be blocked in the domain deny rules – denying all will still allow the mobile app to access the cloud service (CC-58029).

6. Security

Four minor security issues were resolved in this release.

7. Known Issues

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

Admin and User Portals

- 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**

- Portal dialogs do not close on Firefox:

  Firefox browser security settings can prevent portal dialogs from closing when the close button is clicked. To change the setting to allow dialogs to close:
  - 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)

- 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 the 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).

- 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).

- Permissions propagation when a new application is added:
  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, enable application provisioning or enable an app to use the Application Gateway. 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).

- 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 > Addidtional 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 IAM & EMM 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 and Mac (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 IAM & EMM User Service:

  If you have users created using Samsung SDS IAM & EMM User Service, 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).
  ```

- Number of Office 365 supported:

  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).

- 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:

  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. This application currently supports WS-Federation but not WS-Trust, and as a result SDS IAM & EMM 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).

- Adobe EchoSign provisioning tab loading slowly
  All EchoSign apps created before Cloud release 17.5 use EchoSign API version 1 and will only be upgraded to the newer version 5 if you re-auth. All apps using version 1 are expected to load slower because of differences between the version 1 and 5 APIs (CC-46834).

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

- Browser extension on Firefox requires restart after upgrade
  The browser extension on Firefox does require Firefox to be restarted in order for the browser to recognize that the upgrade has completed and 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

- 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 Connector and Administration

- Behavior of shadowExpire attribute with LDAP users

  The current behavior of the shadowExpire attribute with LDAP is incorrect, it will be corrected in a future update. Until that time, the password expiration time (i.e. how far into the future the expiration will be pushed after a password change) is governed not by policy, but by a registry setting (ibmSdsShadowExpireDays). The default value if not otherwise set in the registry is 90 days (CC-56019).

- 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 circumstances 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 Connectors**

  clicking Add Samsung 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 IAM & EMM 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 EMM 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 Centrify.Cloud.Core.ProxyHost.exe executable for any/all networks on the Connector machine (CC-15625).

- Close ADUC before upgrading Connector:
  If the Active Directory Users and Computers (ADUC) extension for the Samsung SDS IAM & EMM 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).

- Report query returns unknown for device type:
  Using the new field internaldevicetype in queries with events prior to the 17.2 release can return a response other than the device type identifier (I for iOS, A for Android, and W for Windows). The correct information is returned for events after the 17.2 release (CC-44777).

Workflow.

- The description column on the requests page (accessed via the requests tab) is English-only for the current version. In a future release this will be localized to the same language set as the rest of the Admin Portal (CC-4928).

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 EMM 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 are 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:

  This is due to Firefox security setting not allowing scripts to close browser windows, a workaround is:

    1) Type about:config in the firefox address bar

    2) Now search for close keyword

    3) Look for dom.allow_scripts_to_close_windows setting and set the value to true (CC-17079).

- 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 SDS IAM & EMM mobile apps if challenges are enabled for password change (CC-48275).

Android Devices

- Existing IAM & EMM Android app users may find that they cannot use pattern for mobile unlock. The issue is that the Android app now properly honors the minimum passcode length. We found that Google has changed the behavior of their API from Android 7.1.1 regarding change in passcode length. To restore pattern as a factor, the "Minimum passcode length" policy must be set to the default value (--) (CC-51805).

- Starting with Android Oreo on Samsung devices, the KNOX container application now requires the user to login using their credentials to gain access (CC-54955).

- 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 EMM app, the vibrate setting remains at the user's current setting (CC-12312).

- Some Samsung Knox devices do not support PKI auth for VPN or WiFi:

  Appears to be a device specific issue with Galaxy III on Android 4.0.4, Galaxy Tablet 2 on Android 4.0.3 and Galaxy Note II on Android 4.1.1 (CC-11847, CC-11806).

- Changes in account name in the 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).

- 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 exists with later Android versions (CC-23091).

iOS Devices

- 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 IAM & EMM iOS 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).

8. Additional Information and Support

In addition to the documentation provided with this package, you can visit the Samsung Knox support site (www.samsungknox.com/support) to get Q&As and knowledge base articles, and also to contact our Samsung Knox support team for assistance.

Realize your vision **SAMSUNG SDS**