Release Note: Knox Manage v19.11

November 14th 2019

Please refer to the below list of new features and improvements to be released with Knox Manage version 19.11 scheduled for the 14th of November 2019.

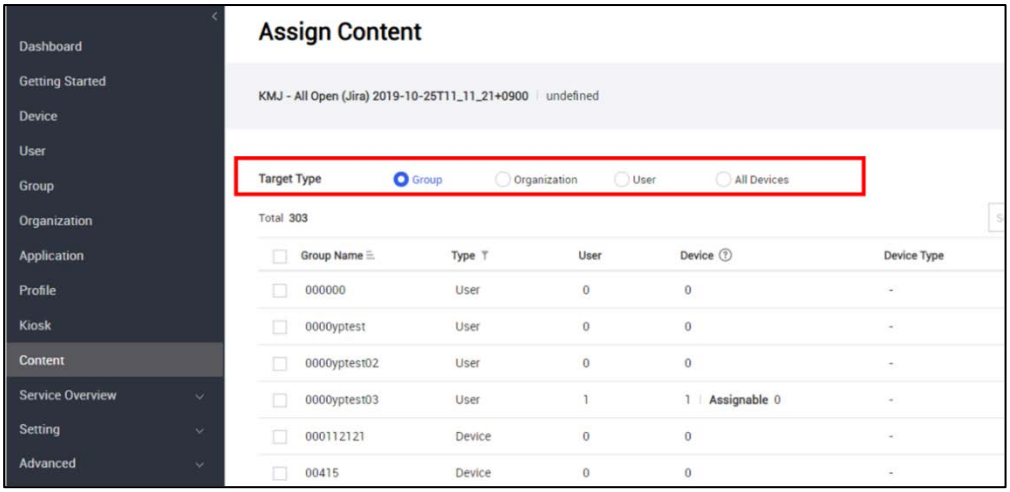
Highlights

1. [Content] Assign to Group, Push to Multi-kiosk Widget
2. [Application] Automatic Uninstallation Options
3. [Admins] OTP (One time password) to Admin Portal, MSP Sub-admin Management
4. [Profile] Profile Update for Group Users
5. [Android Enterprise] SafetyNet, FRP, Advanced Wi-Fi/Certificate Management
6. [Console] Device Filter Customization, Google Map Option, Location Search Period
7. [UI/UX] Refreshment (II)

Details

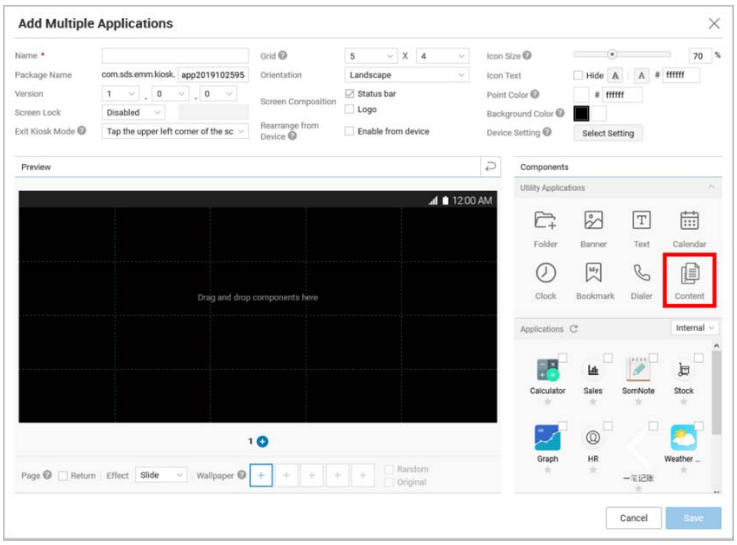
1. [Content] (1/4) Assign Content to Group

- IT Admin can select target types when assigning content file.
- 'Group' has been added to Target Type from v19.11, so assignable target types are now User, Organization, Group and All devices.



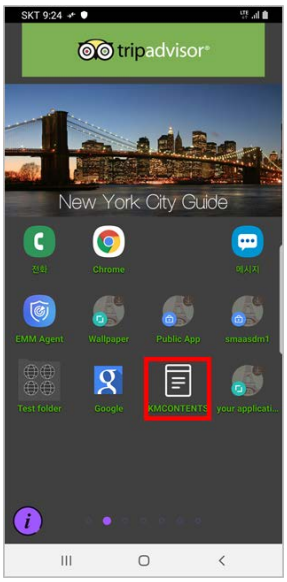
(2/4) Content Push to Multi-kiosk Widget

- IT admin can add content files at multi kiosk wizard through ‘Content Widget’
- Users can access and download files through KM Agent Content widget on the device
- ① Add Content widget to multi-kiosk

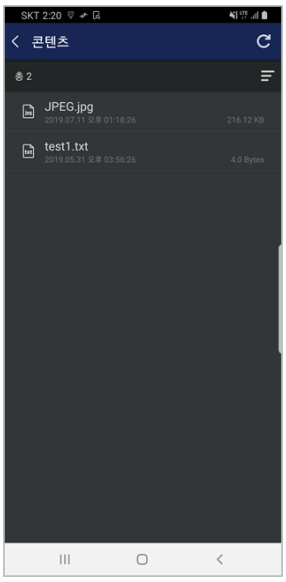


- ② User clicks Content widget from the device

③ User see content files available to be downloaded from Content menu

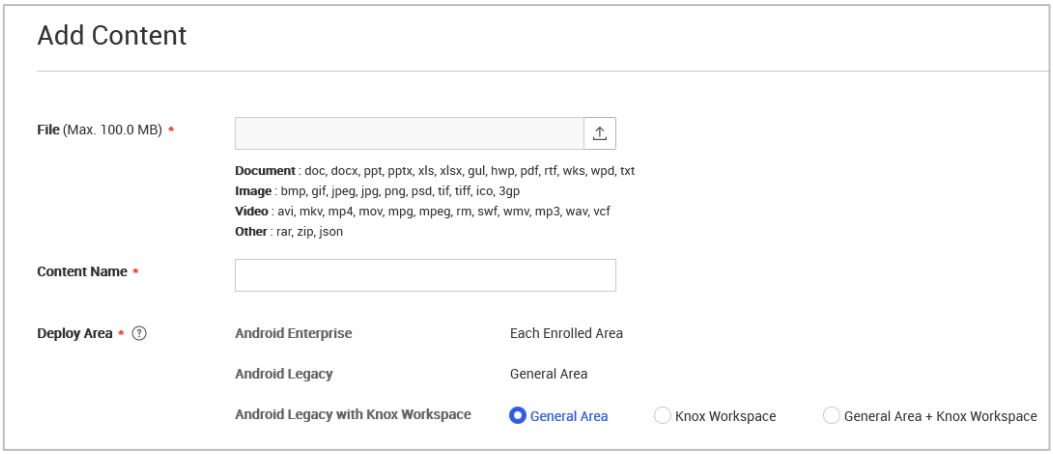


→



(3/4) Automatic Selection of Deploy Area in AE mode

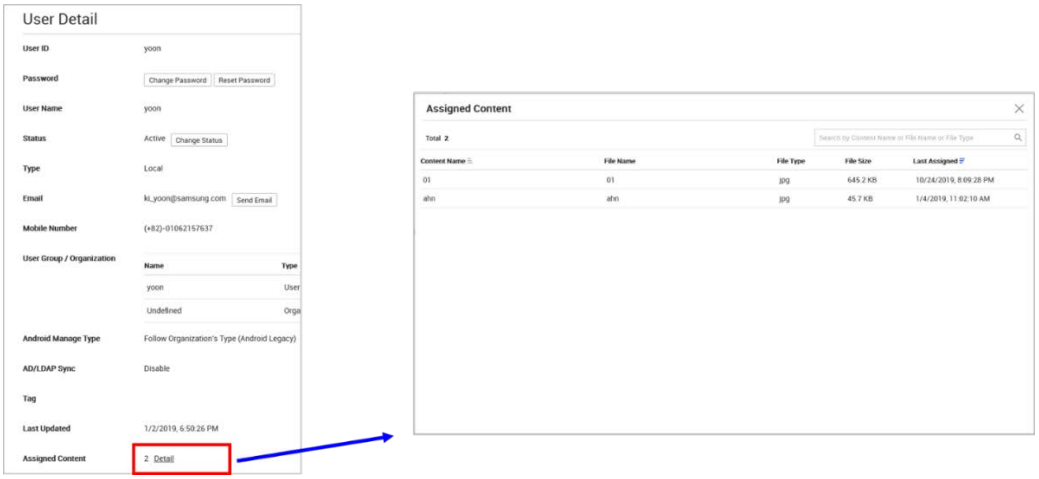
- Previously, IT admin had to manually select deploy area, and all areas were open regardless of enrollment types.
- Now, download area is automatically assigned according to enrollment types.
  - If enrolled device in Android Enterprise, destination is device side (DO) or work profile only (PO). For COMP mode, content will be downloaded in Work Profile only.
  - In device enrolled in Android Legacy, file will be downloaded in general area.
  - Selecting 'Deploy Area' is available for devices with Knox Workspace only, where IT admin can select general area, Knox Workspace or general area + Knox Workspace.



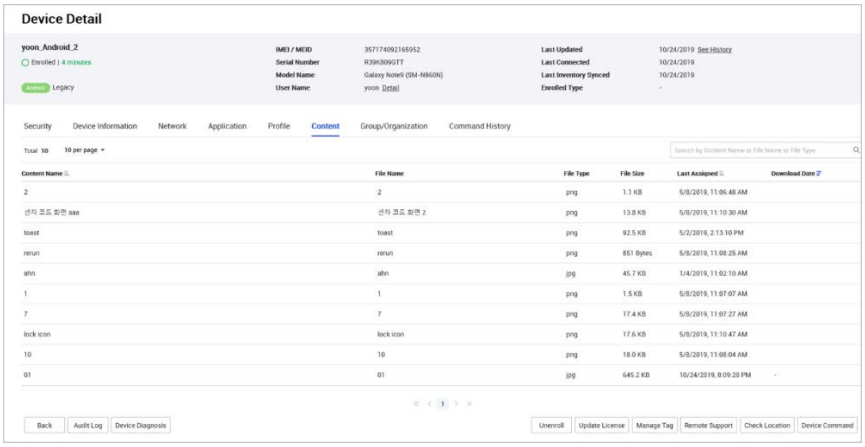
(4/4) View Details of Assigned Content

- IT admin can now view details of assigned content in each menu of User, Device, Organization and Group. This will help to check what files are downloadable from User, Device, Org and Group.

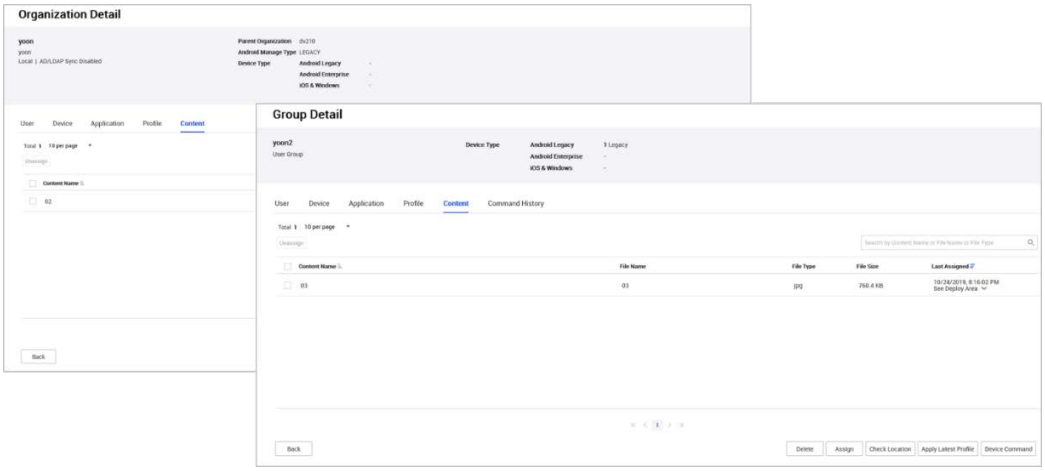
User Details:



Device Details:



- Organization and Group Details:

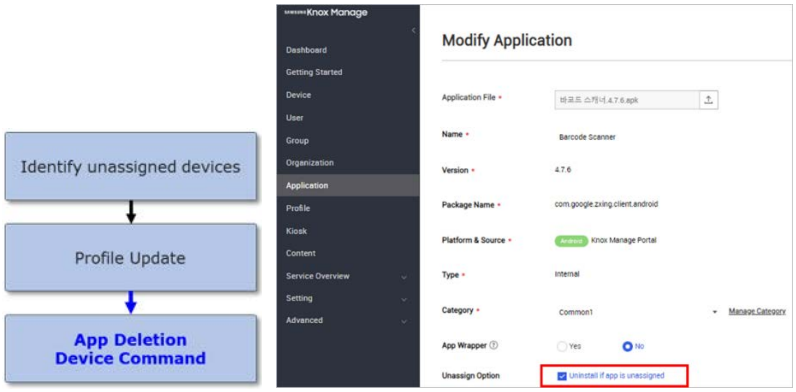


2. [Application] Automatic Uninstallation Option

- Previously, installed applications stayed on the device side (not uninstalled) even if IT admin removed the application from a profile.

- With ‘Unassign Option’, IT admin can choose whether to delete applications upon unassignment automatically or not.

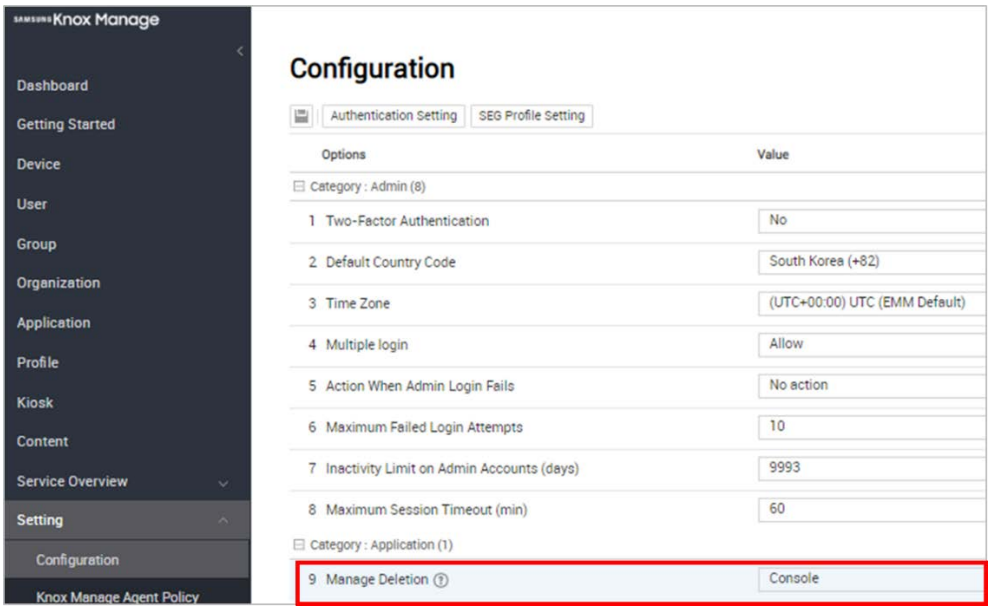
- (1/2) IT Admin can set this option for each application by modifying application policy



- (2/2) IT Admin can also configure the policy for tenant-wise console's default behavior

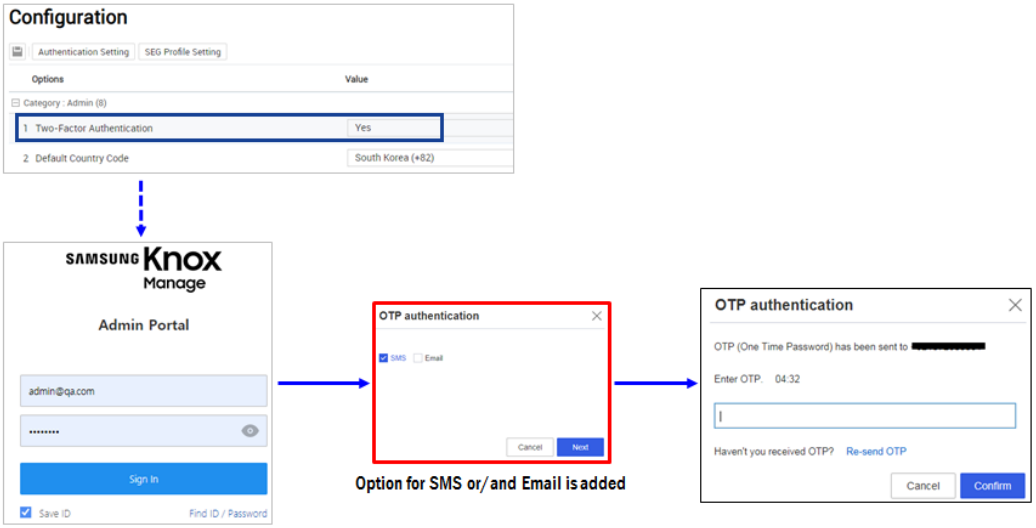
  · If set as "Console," when IT admin deletes the app from the Admin console, application will be removed from the console only; application at the device-side will be still available for user's own decision.

  · If set as "Console + Device," application will be automatically deleted from device when IT admin removes the app from the console, regardless of unassignment option in the application policy.



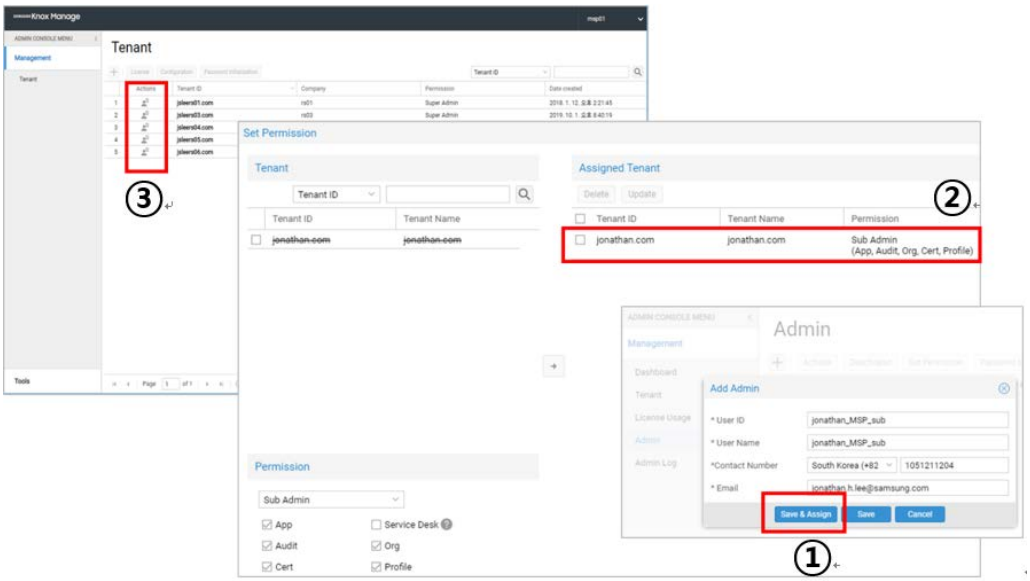
3. [Admin] (1/2) OTP (One Time Password) Option to Admin Portal

- IT admin can configure Two-Factor Authentication by sending OTP through SMS and/or Email of IT Admin.



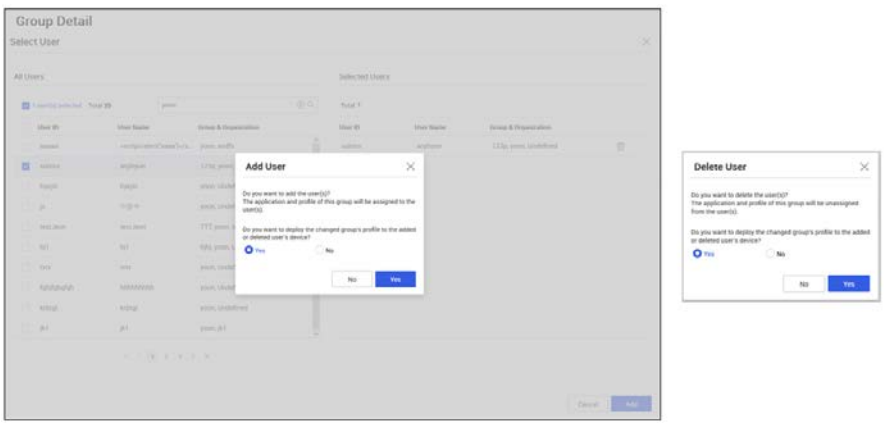
(2/2) Sub-admin for Managed Service Provider's Super-tenant

- Previously, only 1 super -admin was available in MSP super tenant.
- From this release, at the TMS console, MSP super admin can create sub admin accounts in charge of each dedicated sub-tenant and grant limited permission.
  - ① Create MSP sub admin as a MSP admin
  - ② Assign MSP sub admin tenant & permission
  - ③ MSP sub admin log in TMS console and move into the dedicated tenant KM console under Management > Tenant menu.



4. [Profile] Profile Update Option for Group Users

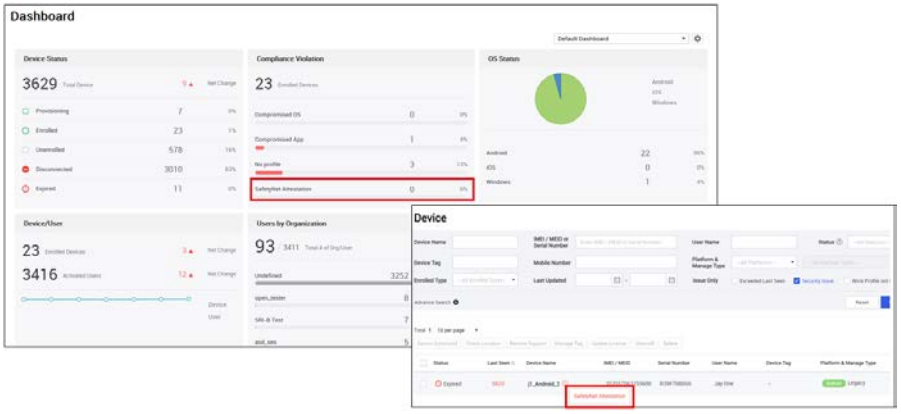
- Previously, IT admin had to send profile update command whenever a user is added or deleted from a group.
- Now, IT admin can select whether to update profile when a user is added or deleted.



5. [Android Enterprise] (1/4) Google SafetyNet Support

- Device attestation check provided by Google is now supported. You can check SafetyNet attestation devices at dashboard or device detail information.

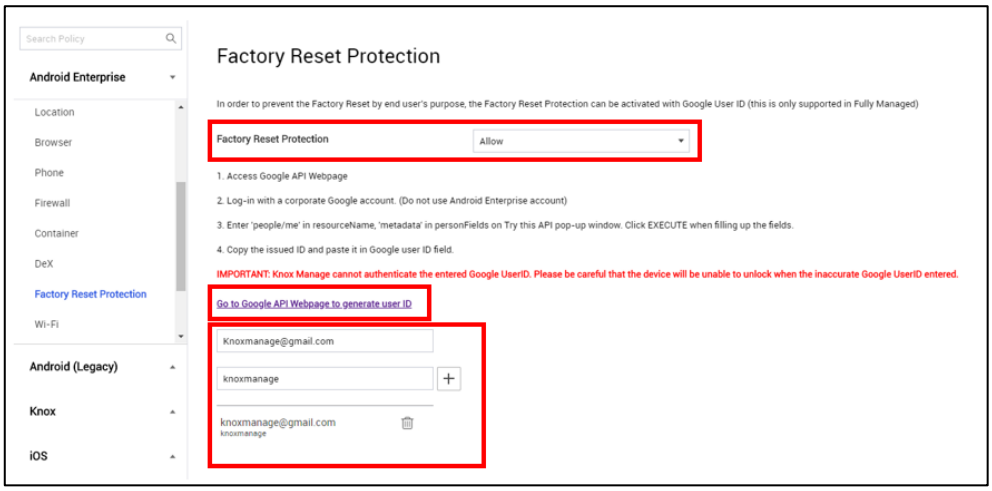
- IT Admin can also set timing of verification and which action to apply to device when verification fails through Profile > Android Enterprise > Security



(2/4) Google Factory Reset Protection

- Google provides Factory Reset Protection policy at fully managed device profile to prohibit abnormal usage after doing kinds of factory reset.

- IT admin needs to define for-purpose google ID in advance and End user must input the same google ID to continue to use that device after factory reset

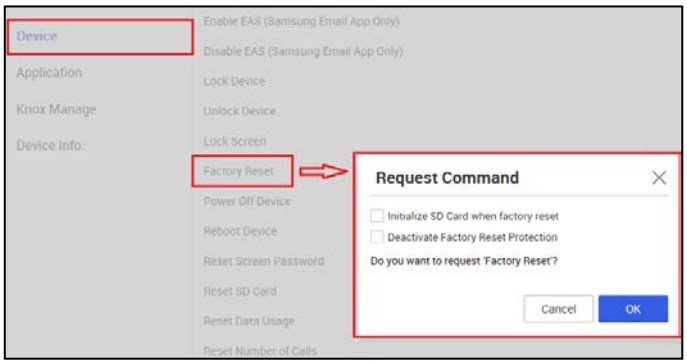


- KM with Knox devices prevents Factory Reset via Setting and Recovery Mode altogether without FRP. But it needs FRP to prohibit Recovery Mode in case of KM with non-Knox devices because previous Google API only responds to Factory Reset via Setting.

- IT admin can choose whether to release FRP option after factory reset device.

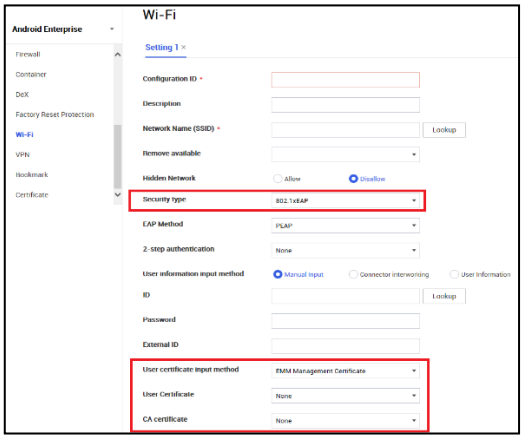
  · If checked the option, FRP mode is released and user can continue to use a device.

  · If unchecked, FRP mode is kept and device requires google ID set by IT admin.



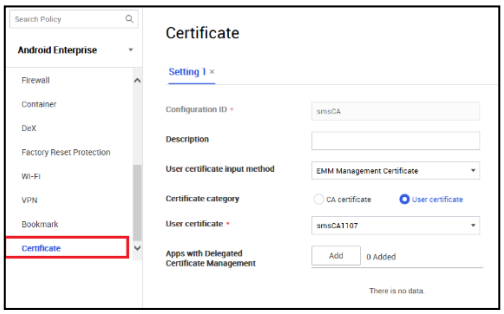
(3/4) Certificate Management for Wi-Fi (802.1xEAP)

- Profile > Android Enterprise > Wi-Fi (802.1xEAP) > Certificate



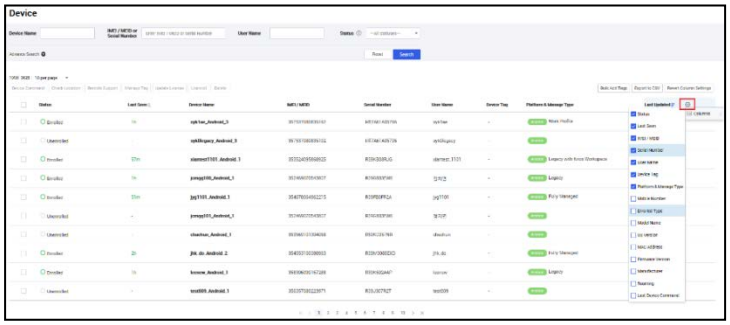
(4/4) Standard/Advanced Certificate Management

- Profile > Android Enterprise > Certificate menu has been added



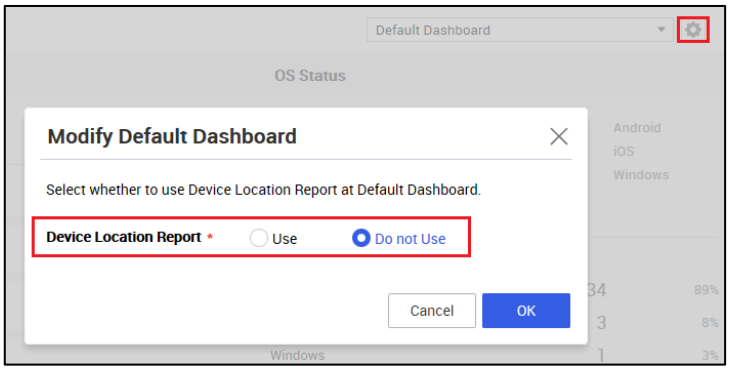
6. [Console] (1/3) Device Column Customization

- IT admin can add/remove columns for device information such as Model number, OS version, Firmware version, Manufacturer, Roaming and Last device command.



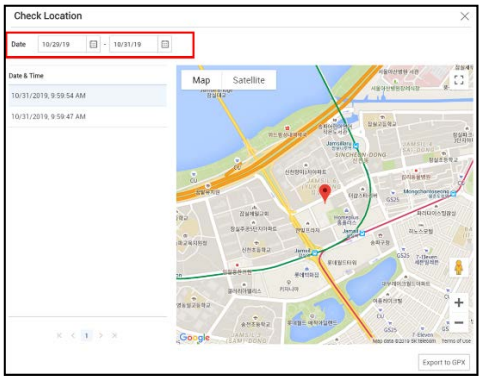
(2/3) Dashboard Option for Google Map

- Customers not using location policy requested option to hide google map at dashboard.
- Now IT Admins can choose whether to show Google Map at the dashboard from the console. The default value is Do not Use.



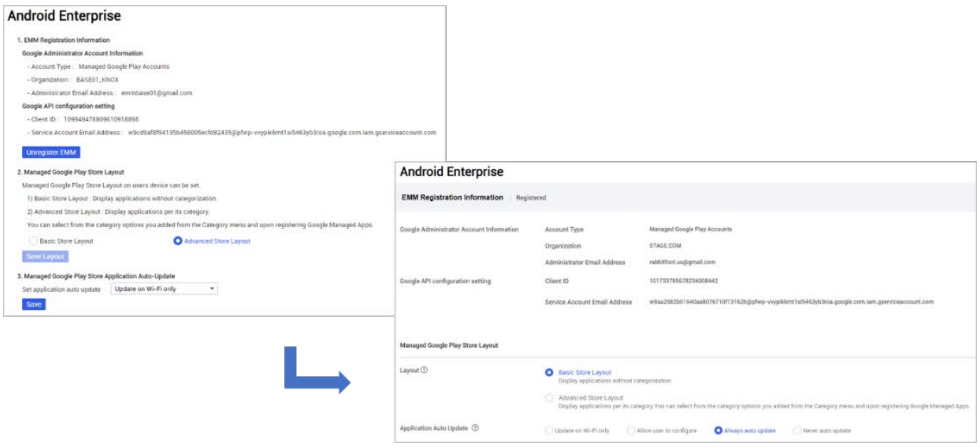
(3/3) Set Search Period for Device Location

- Previously, there were only 2 options - ‘Current location’ and ‘Location history in 30days’.
- From this version, IT admin can set search period for device location.

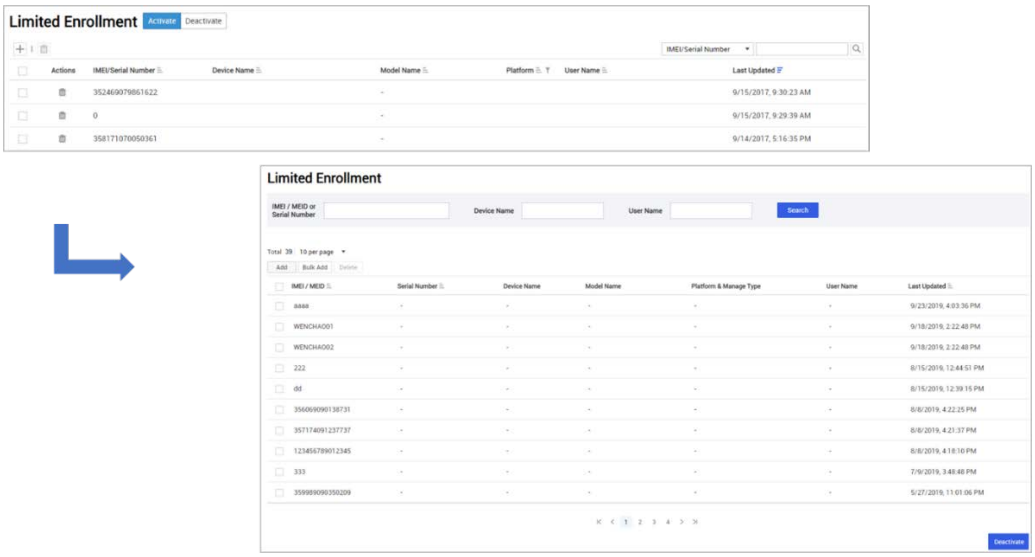


7. [UI/UX] Refreshment (II)

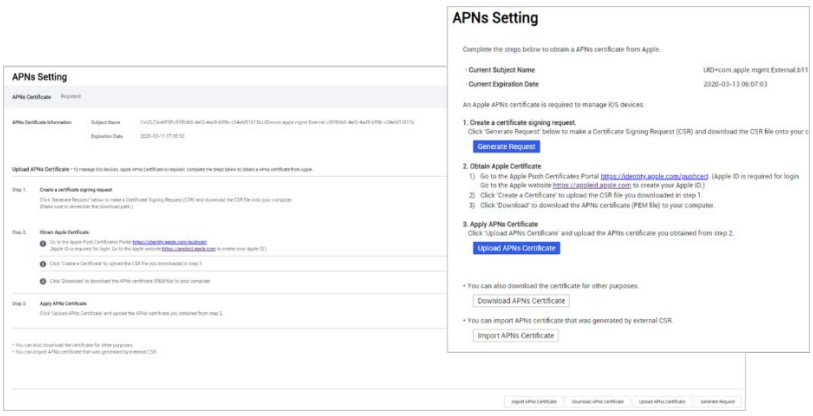
(1/6) Setting > Android > Android Enterprise



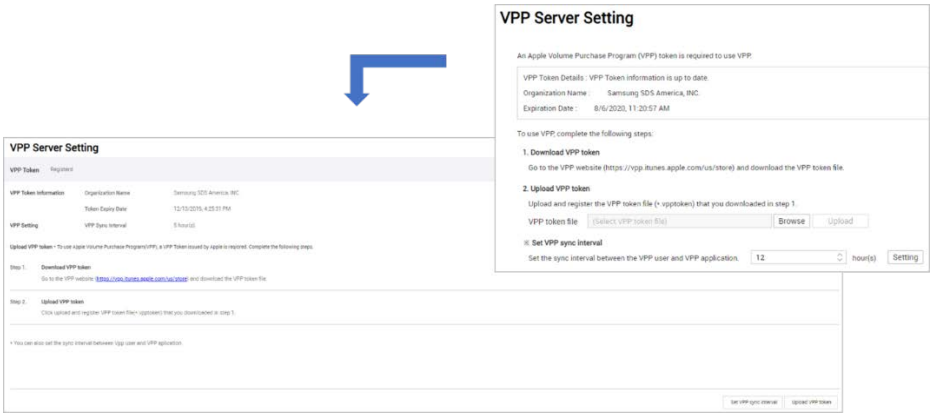
(2/6) Setting > Android > Limited Enrollment



(3/6) Setting > iOS > APNs Setting

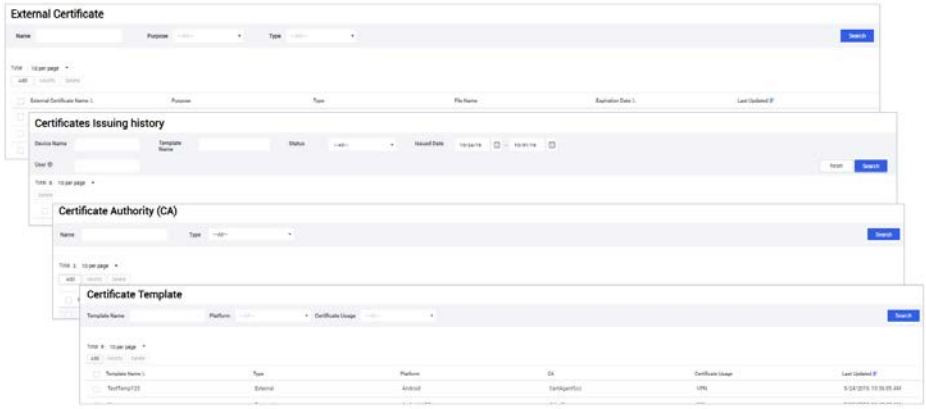


(4/6) Setting > iOS > VPP Server Setting



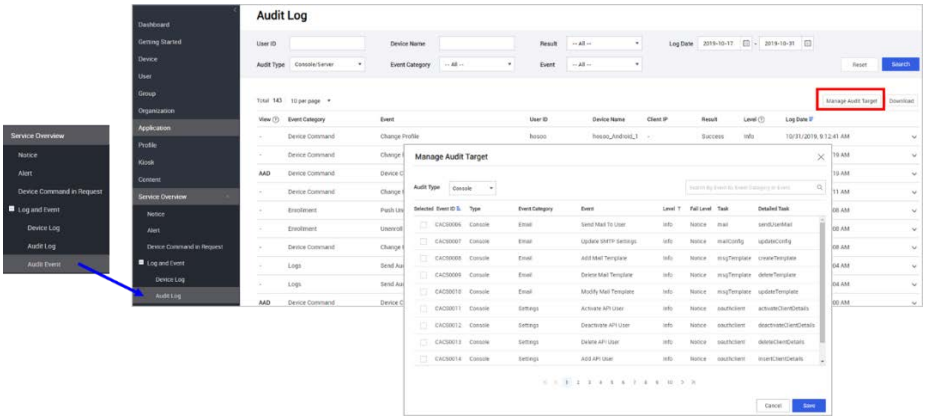
(5/6) Advanced > Certificate

- Enhanced “Search” is available at Advanced > Certificate > External Certificate, Certificate Issuing History, Certificate Authority, Certificate Template or Advanced > EMM API > API Client, API Log, API Client Log



(6/6) Log and Event > Device Log

- Audit Log: Audit Event is now merged into Audit Log



Resolved Issues and Improvements

- [KMVOC-8526 / 00178126] Unable to edit some policies since 19.9
- [KMVOC-8532 / 00178169] 19.9 Release - Enable/disable option in KNOX Manage no longer available
- [KMVOC-8548 / 00178186] 19.9 Release - Kiosk mode exit (no policy applied)
- [KMVOC-8535 / 00178177] Knox Manage problems after updates
- [KMVOC-8540 / 00178129] 19.9 Release - Report View Time has been exceeded
- [KMVOC-8541 / 00178191] You have entered an invalid user ID or password.
- [KMVOC-8544 / 00178082] Web Kiosk broken since 19.9
- [KMVOC-8546 / 00178322] 19.9 release : Unable to modify profile, screesn are blank
- [KMVOC-8556 / 00178302] 19.9 release : AE manual enrollment. > Settings are not restricted> & Kiosk app never downloads/installs.
- [KMVOC-8557 / 00178342] Profile create and edit failure at ap02
- [KMVOC-8559 / 00178485] KM console performance issues
- [KMVOC-8561 / 00178297] 19.9 release : Legacy manual enrollment. > Policy shows on device> Devices Still are not restricted> & Kiosk app never downloads/installs.
- [KMVOC-8567 / 0017536] SM-T385M - Cannot launch apps unless connected to internet
- [KMVOC-8568,8581 / 00178747,00178532]This occurred problem would be from Server, DB
- [KMVOC-8573 / 00178800] AE Bookmark not installing
- [KMVOC-8575 / 00178462] Email app - authentication request after each app installation
- [KMVOC-8586 / 00179062] Google Enterprise applications failing to install
- [KMVOC-8618 / 00179493] Issues with Accessing WiFi Profile Settings
- [KMVOC-8619 / Internal] able to add the same package as public and control application
- [KMVOC-8628 / 00179402] Manage google playstore categories issue
- [KMVOC-8629, 8714/ 00179111] Marking Wi-fi config as removable seems te be impossible in KM
- [KMVOC-8635 / 00178295] KME not showing as enrolled type
- [KMVOC-8644 / 00179439] Profile or some other tenant data corruption

- [KMVOC-8645 / 178932] VPP token not syncing, Supervisory Certificate not listed
- [KMVOC-8658 / 00179341] KNOX VPN profile - not saved correctly
- [KMVOC-8663 / 00180028] Installed App Report fails to generate
- [KMVOC-8670 / 00180033] Bulk import users error
- [KMVOC-8678 / 00178693] AD/LDAP Group not receiving policies
- [KMVOC-8685 / Internal] Error message when deleting multiple profiles together
- [KMVOC-8694 / 00179002] Auto app update mechanism MGP