

Release Note: Knox Manage v19.12

December 19th, 2019

Please refer to the below list of new features and improvements to be released with Knox Manage version 19.12 scheduled for the 19th of December 2019.

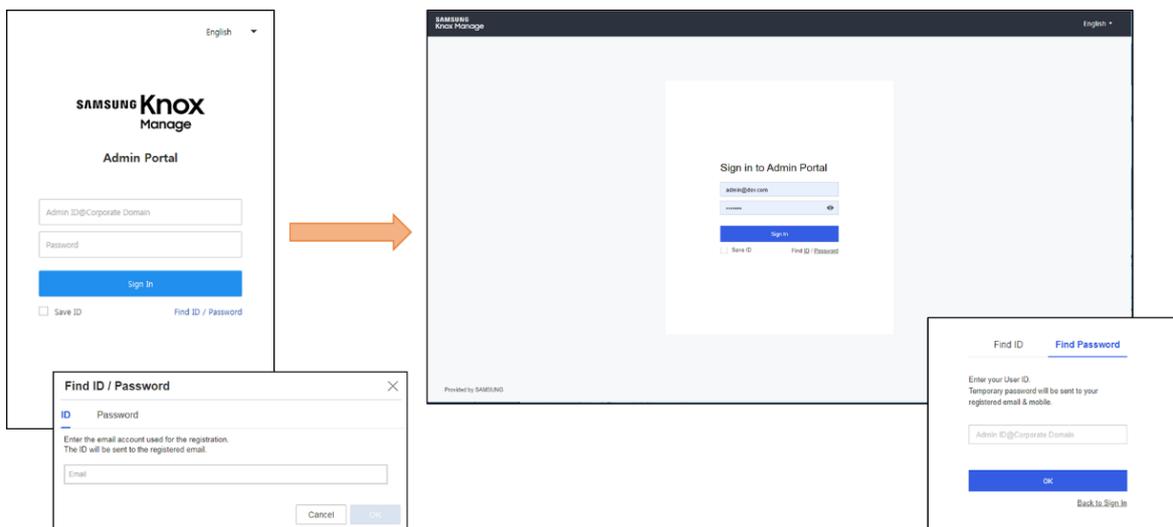
Highlights

1. [UI/UX] 'Getting Started' Improvements
2. [Profile] Knox Service Plug-in Redesign
3. [Android Enterprise] VPN, APN Support
4. [Android Enterprise] Kiosk Utilities Support

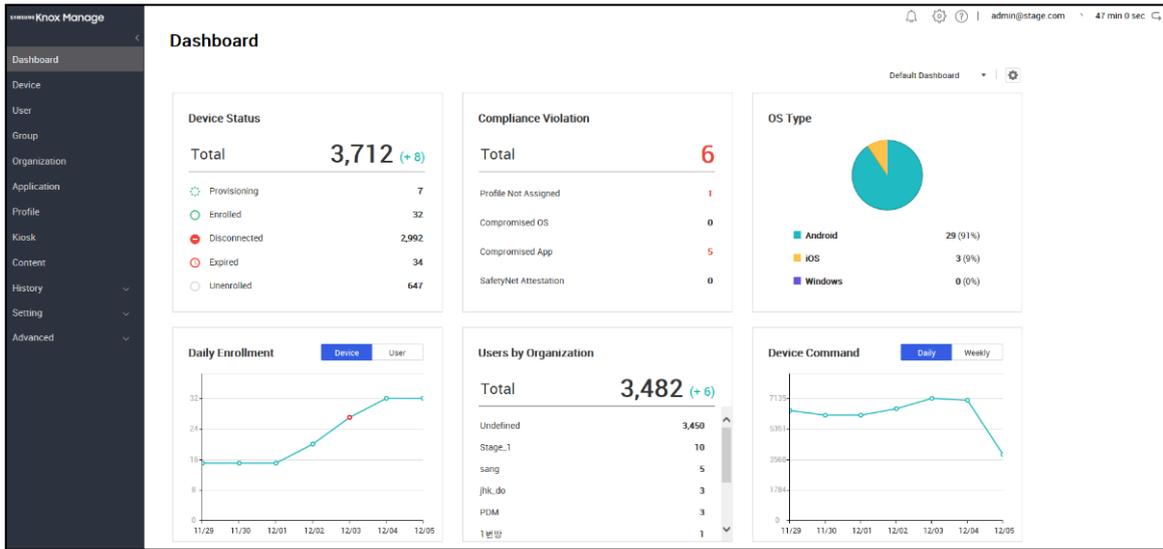
Details

1. [UI/UX] Improved Page Designs: Log-in, Dashboard, Header

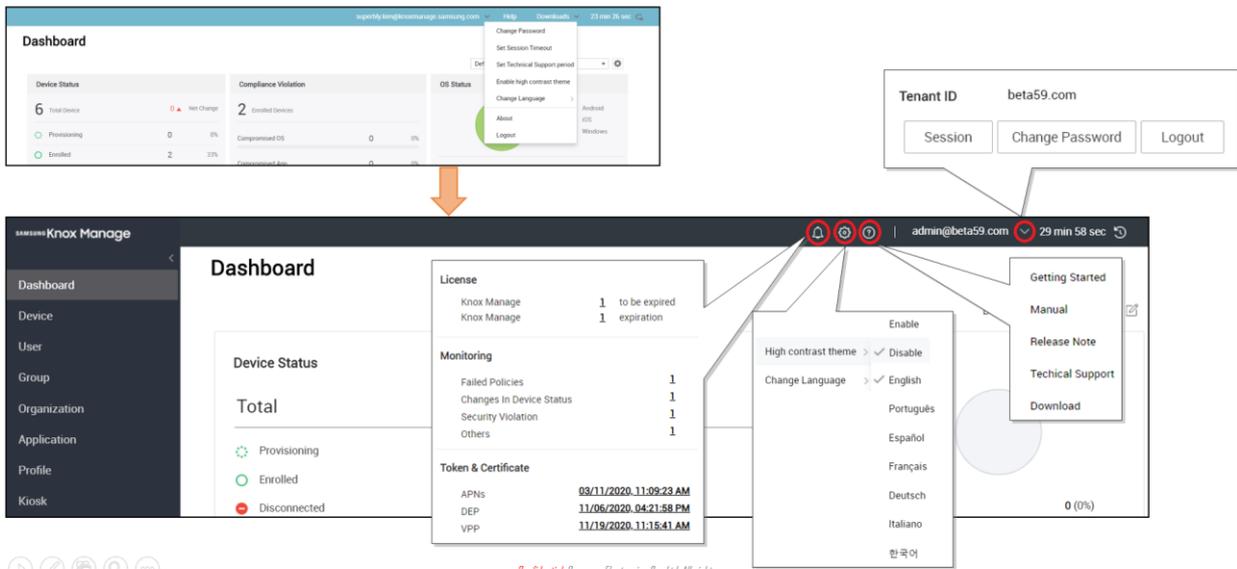
- Log in welcome screen has been changed as below



- Dashboard has been re-designed



- The header menu has been re-designed with icons.

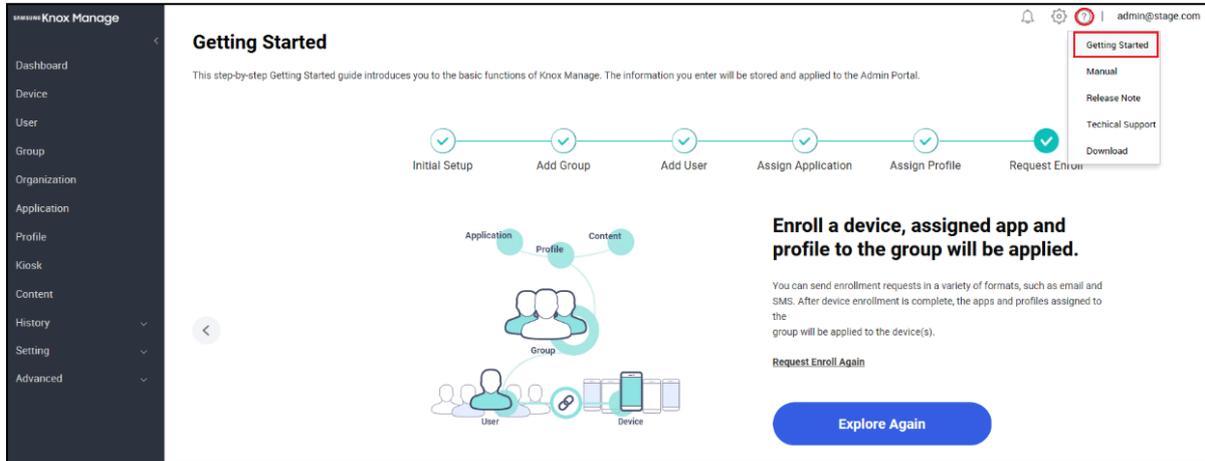


- Some other pages are redesigned to provide similar look & feel with the latest version; there's no functional change, but only UI update

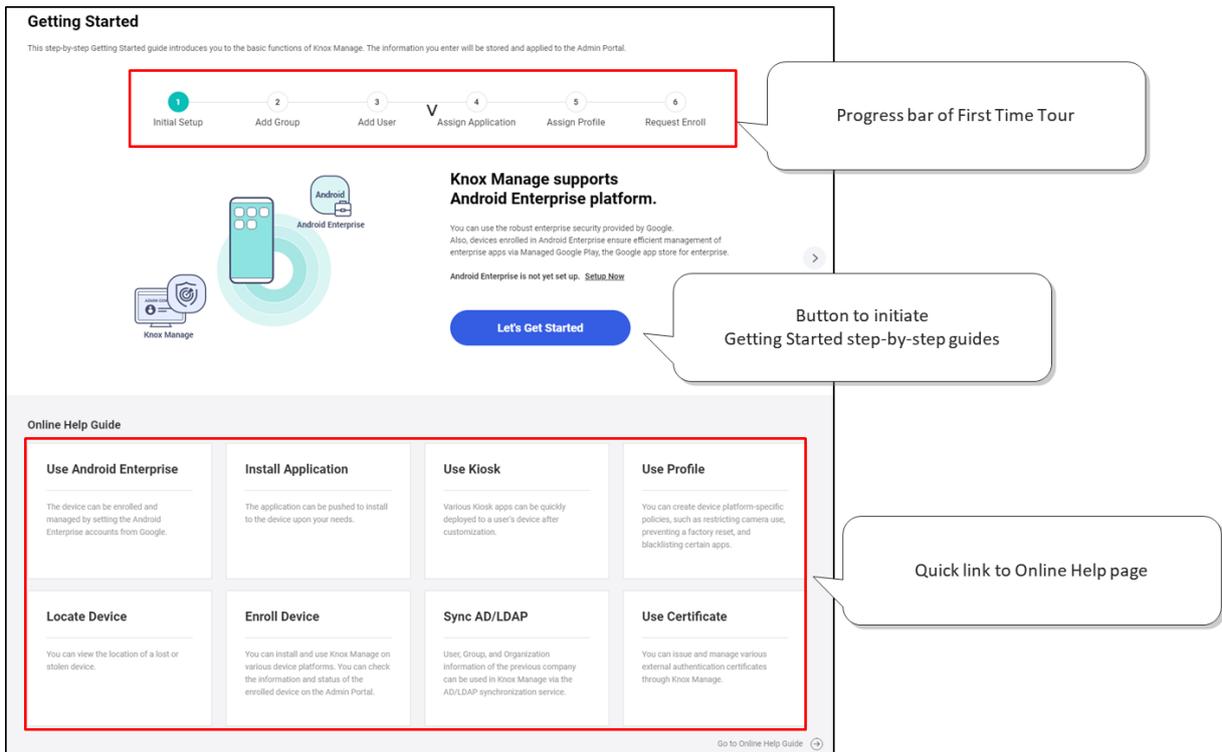
Updated Pages: Directory Service, Directory Pool, Report, Notice, Email & SMS History and Message Template

2. [UI/UX] 'Getting Started' Improvements

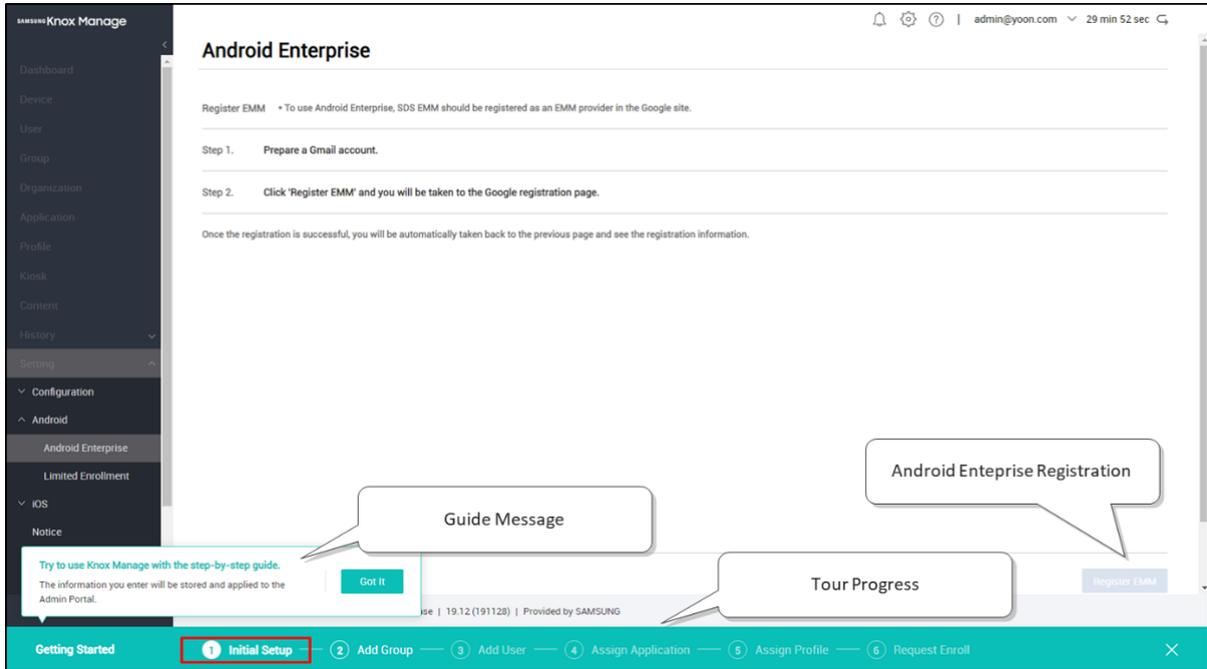
- Shortcut to "Getting Started" is moved to help icon at Header. Clicking the option will deliver IT Admin to the welcome page of Getting Started.
- "Getting Started" page shows up upon IT Admin's first access to the admin console



- Getting Started menu now includes navigating overview of steps and help guide.

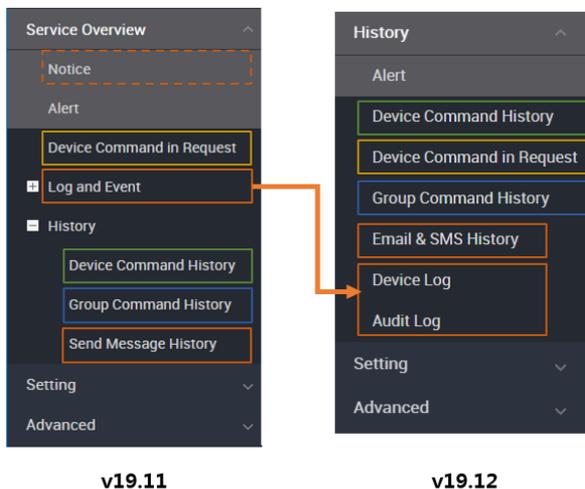


- From this release, the default enrollment method of Getting Started is by using Android Enterprise. Getting Started will firstly guide IT Admin to setup Android Enterprise, and then to the next steps.



3. [UI/UX] Menu Relocation

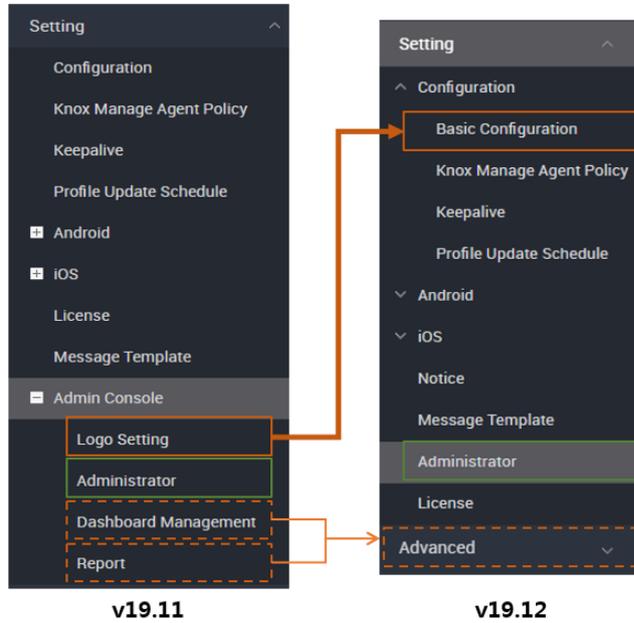
- 'Service Overview' is now changed to 'History'
 - 'Notice' is moved to under 'Setting'
 - 'Device Log' & 'Audit Log' under 'Log and Event' are moved to one upper level
 - 'Device Command History', 'Group Command History' & 'Send Message History' are moved to one upper level
 - 'Send Message History' is changed to 'Email & SMS History'.



v19.11

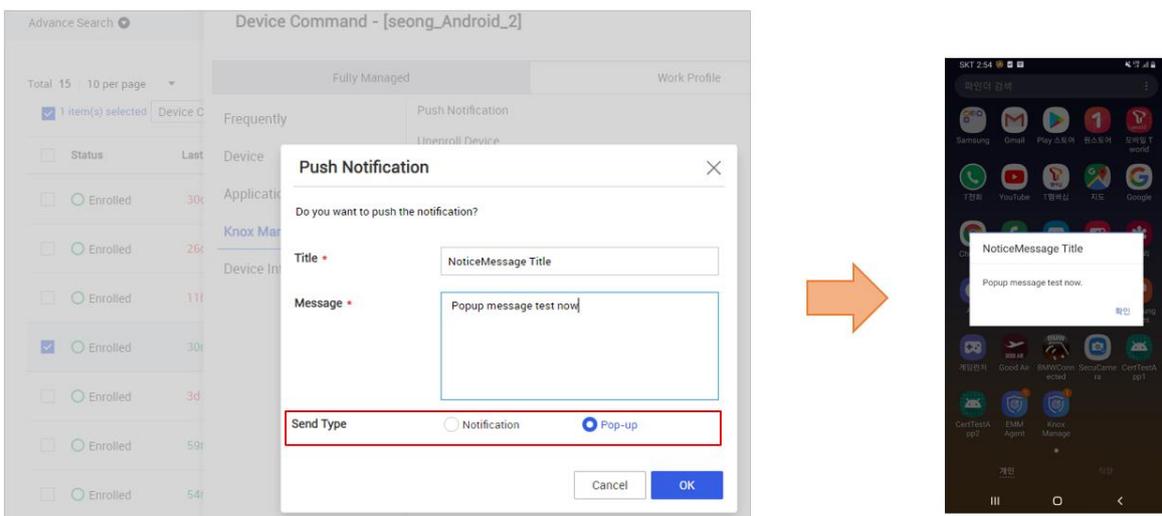
v19.12

- Sub-menus under 'Settings > Admin Console' has been relocated.
 - 'Logo Setting' is changed to 'Basic Configuration'
 - 'Administrator' is moved to under 'Settings'
 - 'Dashboard Management' & 'Report' are moved to under 'Advanced'



4. [Agent] Push Pop-up Notification

- IT admin can select send type when pushing notification to device - in the notification bar or as a pop-up message.
- Pop up is useful for Kiosk modes when the use of notification bar is prohibited.



5. [Content] Select Download Path

- IT admin can select download path under internal storage
- A file will be pushed to Internal Storage or a newly created folder under internal storage

The screenshot shows the 'Add Content' interface in Samsung Knox Manage. On the left is a navigation menu with 'Content' selected. The main area has a 'File (Max. 300.0 MB)' upload field, supported file types (Document, Image, Video, Other), and a 'Content Name' field. The 'Download Path' field is highlighted with a red box and contains the path 'Internal storage/ Download/KnoxManage/Content'. Below this, the 'Deploy Area' section shows 'General Area' selected with a radio button, while other options like 'Each Enrolled Area', 'Android Enterprise', 'Android Legacy', and 'General Area' are unselected.

6. [Console] Import/Export Profile

- Profile Import/Export functions are supported again from this release.
- IT Admin can Export policy from each Profile Detail menu, and import it to the Profile List.

The screenshot shows the 'Profile Detail' page for a profile named 'Profile for KSP TEST'. The 'Policy' tab is active, showing a table with columns 'Category', 'Policy', and 'Value'. The table is empty, with the text 'There is no data.' displayed. Below the table are buttons for 'Back', 'Delete', 'Export Policy' (highlighted with a red box), 'Modify Profile Info', 'Modify Policy', 'Assign', and 'Apply'. An 'Import' dialog box is overlaid on the 'Profile' list, showing a 'Profile Name' field and a 'File(.coa)' selection field with a 'Browse' button.

7. [Profile] Call/SMS Blacklist

- IT Admin can add specific numbers to restrict incoming/outgoing of call and SMS.
- Only numbers are allowed in the input field

Prohibit voice call ⓘ Apply

- Voice call • Incoming Outgoing

- Incoming Call blacklist • +
There is no data.

- Outgoing Call blacklist • +
There is no data.

Disallow SMS/MMS ⓘ Apply

- Disallow Incoming/Outgoing SMS/MMS • Incoming SMS Outgoing SMS Incoming MMS Outgoing MMS
You must select at least one item in this group

- Incoming SMS blacklist • +
There is no data.

- Outgoing SMS blacklist • +
There is no data.

8. [Profile] Google Backup and Restore

- IT Admin can set policy whether to allow Google Backup and Restore option or not.

Android Enterprise

System

Interface

Security

Kiosk

Application

Location

Browser

Phone

Samsung Knox

Android Enterprise

Android Legacy

Knox Workspace

Android Legacy

Fully Managed ⓘ Work Profile ⓘ

User Certificate Setting ⓘ - -

Camera ⓘ

Screen capture ⓘ

Account Modification

- Account Blacklist

VPN Setting ⓘ - -

Backup Allow Disallow

Tooltip is being made

IT Admin can set policy whether to allow Google Backup and Restore option or not

[Configuration Value]

- N/A: No Settings.

- Allow: Allow 'data backup' provided by Google.

- Disallow: Disallow 'data backup' provided by Google.

[Note]

In Work Profile, Android 10 or later can adopt this policy.

[Supported device]: Android 8.0+

9. [Profile] Knox Service Plug-in Deployment

- Knox Service Plug-in is an add-on deployment profile for Samsung specific policies. Once 'KSP App' is approved, a new category 'Samsung Knox' appears.
- More policies will be available in 2020 Feb.

※ Customers who registered KSP before KM v19.12 as Managed Google Play or Public App through Console > Application menu, are required to un-assign and delete the previously deployed KSP app and approve it through Setting > Android Enterprise

※ KSP app has been relocated from Application menu to Setting from KM v19.12

The screenshot shows the 'Set Policy' interface for a profile named 'Jonathan'. The 'System' tab is selected, and the 'Fully Managed' section is visible. The 'Android Enterprise' section is expanded, and 'Samsung Knox' is highlighted in a red box. An orange arrow points from this box to the 'Samsung Knox Settings' section at the bottom, which includes 'Knox Service Plug-in Application' and 'Approved' buttons.

10. [Profile] Android Enterprise – VPN support

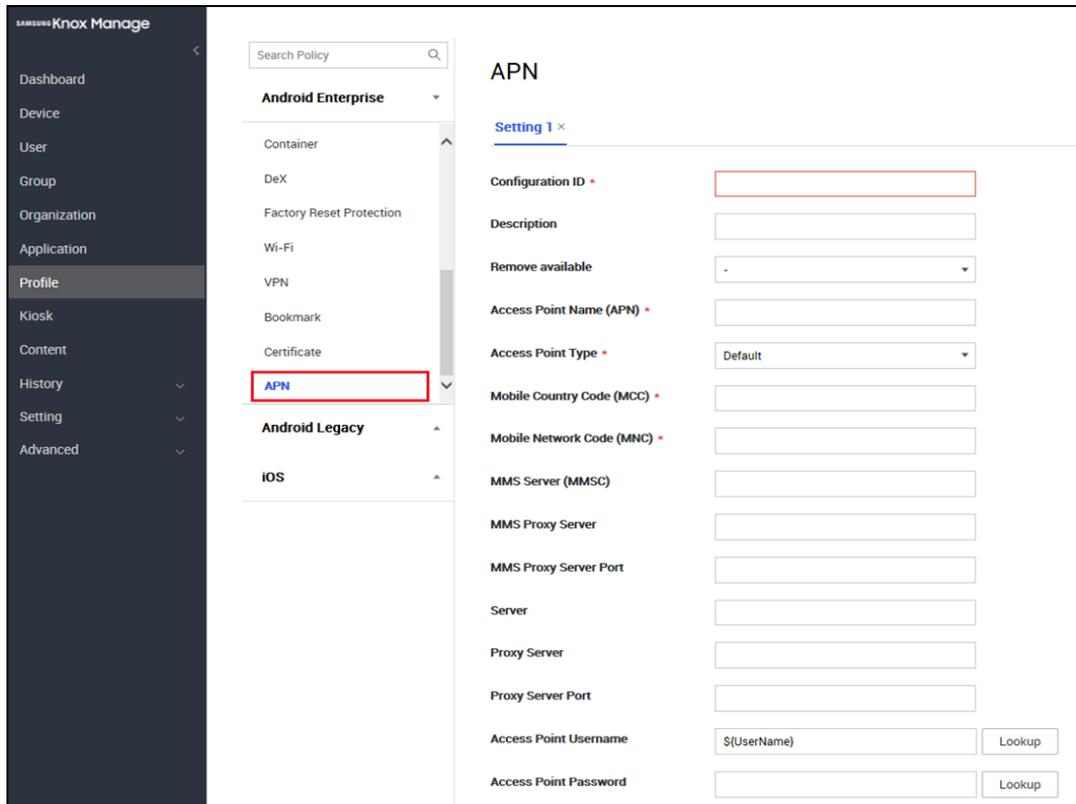
- 'Pulse Secure' VPN has been added.
- Other VPNs (F5 or AnyConnect) are also to be supported in the future.

The screenshot shows the 'VPN' configuration interface. The 'VPN type' is set to 'Pulse Secure', 'Always On VPN' is set to 'Do not use', 'Authentication Type' is set to 'Password', and 'Route Type' is set to 'Device'. Callout boxes provide additional information:

- KM V19.12 supports Pulse Secure only. F5 and Anyconnect will be supported later.**
- Always On VPN**
 - Use: Automatic VPN connection after device reboot
 - Do not use: Manual connection is needed
- Authentication Type**
 - Password: User ID & Password
 - Certificate: Certificate based Authentication
 - Password + Certificate: Both conditions are needed
- Route Type**
 - Device: Every application use VPN (Device wide)
 - Application: Can define App list using VPN configuration through white/black list

11. [Profile] Android Enterprise – APN support

- IT Admin can configure APN settings from Profile > Android Enterprise > APN

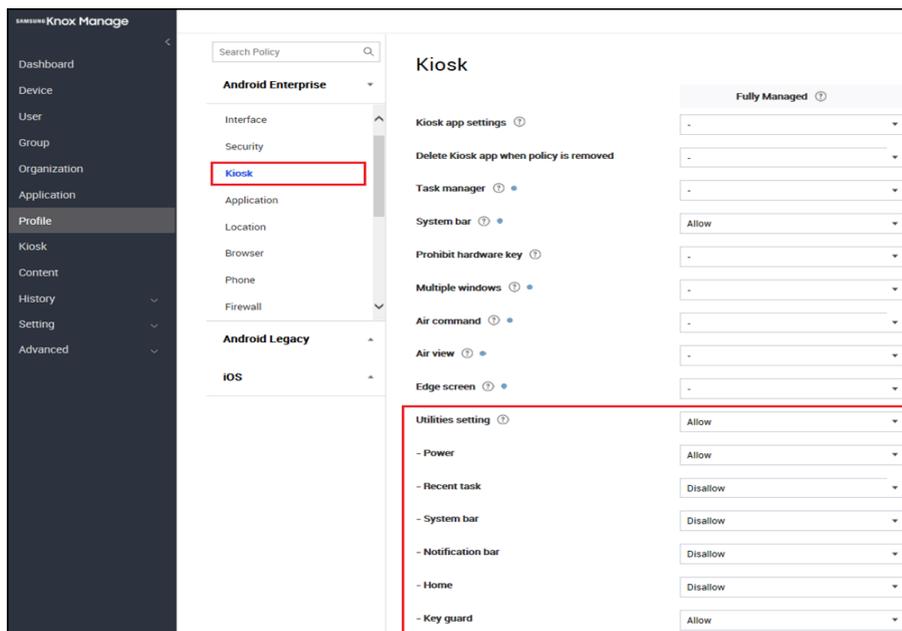


The screenshot shows the Samsung Knox Manage interface for configuring APN settings. The left sidebar contains a navigation menu with 'Profile' selected. The main content area is titled 'APN' and shows 'Setting 1' configuration. The 'APN' menu item in the sidebar is highlighted with a red box. The configuration fields include:

Field	Value
Configuration ID	[Empty]
Description	[Empty]
Remove available	-
Access Point Name (APN)	[Empty]
Access Point Type	Default
Mobile Country Code (MCC)	[Empty]
Mobile Network Code (MNC)	[Empty]
MMS Server (MMSC)	[Empty]
MMS Proxy Server	[Empty]
MMS Proxy Server Port	[Empty]
Server	[Empty]
Proxy Server	[Empty]
Proxy Server Port	[Empty]
Access Point Username	\$(UserName) [Lookup]
Access Point Password	[Empty] [Lookup]

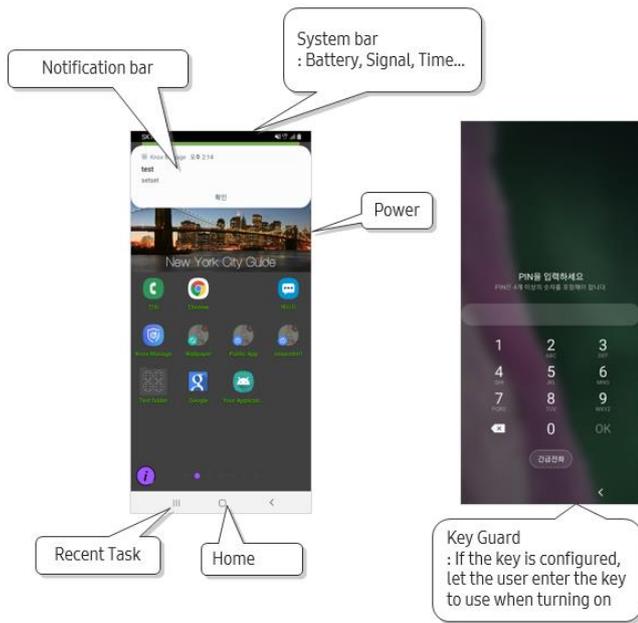
12. [Profile] Android Enterprise – Utilities Setting in Kiosk Mode

- Android Enterprise Kiosk mode has been improved; IT Admin can configure specific components such as controlling system bar, notification bar and more (P OS+)



The screenshot shows the Samsung Knox Manage interface for configuring Kiosk Utilities settings. The left sidebar contains a navigation menu with 'Profile' selected. The main content area is titled 'Kiosk' and shows 'Fully Managed' configuration. The 'Kiosk' menu item in the sidebar is highlighted with a red box. The configuration fields include:

Field	Value
Kiosk app settings	-
Delete Kiosk app when policy is removed	-
Task manager	-
System bar	Allow
Prohibit hardware key	-
Multiple windows	-
Air command	-
Air view	-
Edge screen	-
Utilities setting	Allow
- Power	Allow
- Recent task	Disallow
- System bar	Disallow
- Notification bar	Disallow
- Home	Disallow
- Key guard	Allow



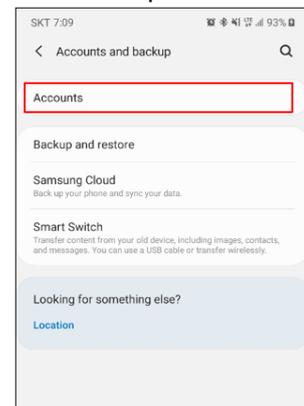
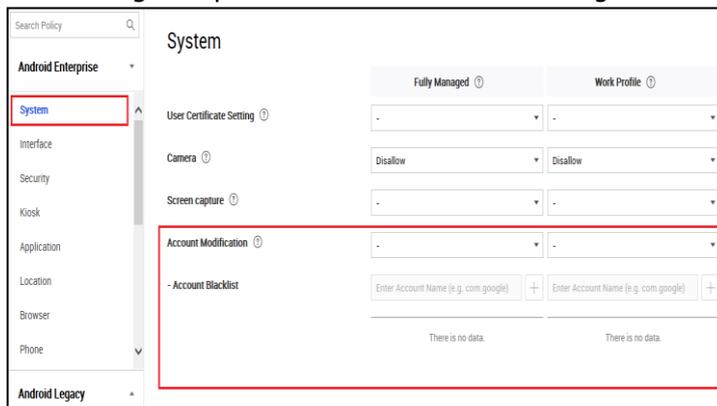
* To enable 'Recent Task', 'System bar' and 'Notification bar', 'Home' setting should be set as 'allow'.

- From KM v19.12, the default Utilities settings have been changed as below.

KM v19.11	KM v19.12
- Power : Allow	- Power : Allow
- Recent task : Allow	- Recent task : Disallow
- System bar : Allow	- System bar : Disallow
- Notification bar : Allow	- Notification bar : Disallow
- Home : Allow	- Home : Disallow
- Key guard : Allow	- Key guard : Allow

13. [Profile] Android Enterprise – Account Blacklist

- IT admin can blacklist the use of certain account. Account Name should match each service name, for example, Gmail: com.google.android.gm.pop3, Naver: com.nhn.android.naveraccount, Facebook: com.facebook.auth.login
- If the policy is set (Profile > System > Account Modification) end users are prohibited from adding the specified account at device setting > Accounts and backup > Accounts



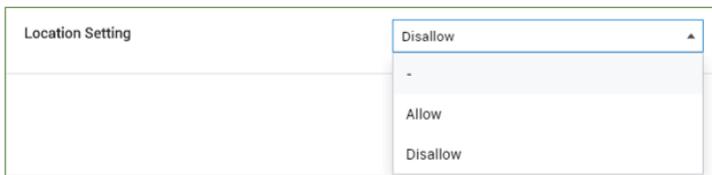
14. [Profile] Android Enterprise – Location Policy

- Location policy has been added as a new menu under system category (now there are two location policies)
 - Android Enterprise > Location > GPS: IT admin can configure GPS feature availability. If GPS disable is "Disable On", location feature is forced off, and user cannot use GPS on the phone.
 - Android Enterprise > System > Location Setting: IT admin can configure whether to allow users to change Location setting on the device.
 - For example, in case of GPS (Disable On) & Location Setting (Allow), users can change the feature on/off by themselves.
- IT admin can force on the GPS feature of Fully Managed devices by configuring Location Setting policy as "Disallow" since the default GPS policy of device is "On".

Profile > Android Enterprise > Location > GPS



Profile > Android Enterprise > System > Location



15. [Profile] Android Enterprise – Password Policy

- Android Enterprise > Security > Device Password, is applied to each enrollment type

Security

Device Password

- Minimum strength
- Minimum length
- Minimum number of letters
- Minimum number of non-letters
- Minimum number of lowercase letters
- Minimum number of capital letters

Work profile password

- Minimum strength
- Minimum length
- Minimum number of letters
- Minimum number of non-letters
- Minimum number of lowercase letters
- Minimum number of capital letters
- Minimum number of numeric characters

Legend:

- ① Fully Managed (DO)
- ② + ③ Work Profile (PO: Device /Work Profile Area)
- ① + ③ Work Profile on Fully Managed (COMP)

- Expiration rule triggered through 'Expiration after (days)' is defined to provide unified usability. The below table is summary for password expiration behaviors.

Initial Setup		Zone	Compliance	Force	Expiration	Force
Android Enterprise	Fully Managed Device	Device	Lock task through Custom UI	O	Lock task through Custom UI	O
	Work Profile	Device	1) Alert on Status bar	X	1) Alert on Status bar	X
			Setting menu through Custom UI	△ (Back key control)	Setting menu through Custom UI	△ (Back key control)
		Work Profile	1) App Hidden 2) Alert on Status bar	X	1) App Hidden 2) Alert on Status bar	X
			Setting menu through Custom UI	△ (Back key control)	Setting menu through Custom UI	△ (Back key control)
	Work Profile on Fully Managed	Device	Same to that of Fully Managed Device		Same to that of Fully Managed Device	
		Work Profile	Same to that of Work Profile		Same to that of Work Profile	
Legacy	Device	Alert on Status bar	X	Until setting it up 1) Alert on Status bar ※ Some other brand's is dependent to OS	X	
		Pop-up when exiting screen lock (System Setting)	X			
	Workspace (BYOD)	Alert on Status bar (Since v19.12)	X	Alert on Status bar	X	

Resolved Issues and Improvements

- [KMVOC-8411 / 00173394] Email app issue on older email client and legacy deployment
- [KMVOC-8420 / 00175087] Can't use the dialer keystring *#06# when under AE Kiosk Multi-app
- [KMVOC-8553 / 00178499] v19.9 - High Contrast Text Color in "Add Control App"
- [KMVOC-8620] Adding Wi-Fi in profile is breaking the Work profile on Fully managed device flow
- [KMVOC-8674,8818 / 00181890] Server,DB data error or..... - only one tenant affected after patch
- [KMVOC-8701 / 00179950]BLAUD-i1910 0180 - Knox manage report won't save but no explanation
- [KMVOC-8733 / 00180449] {ETS} KNOX Manage | S10/S9 | Enrolled KNOX Manage devices are sporadically locking
- [KMVOC-8765 / 00180804] Email Sync Interval is not properly set in Exchange ActiveSync / Knox Container
- [KMVOC-8779,8812 / 00181590] WiFi Event Profile Not applied
- [KMVOC-8813 / 00182372] Runtime error after modifying application options
- [KMVOC-8816 / 00182369] An error occurred. Please try again. (Error Code: 500), DB Error: The query has timed out [Code: -1]
- [KMVOC-8820 / 00181039] Copy of profile not applying on devices
- [KMVOC-8836 / 00182113] Day & Time Profile not applying
- [KMVOC-8844 / 00182824] [TMS problem with tenants]
- [KMVOC-8850 / 00182991] KM kiosk mode adding internal apps issue
- [KMVOC-8859 / 00183224] Profile Rest after modify