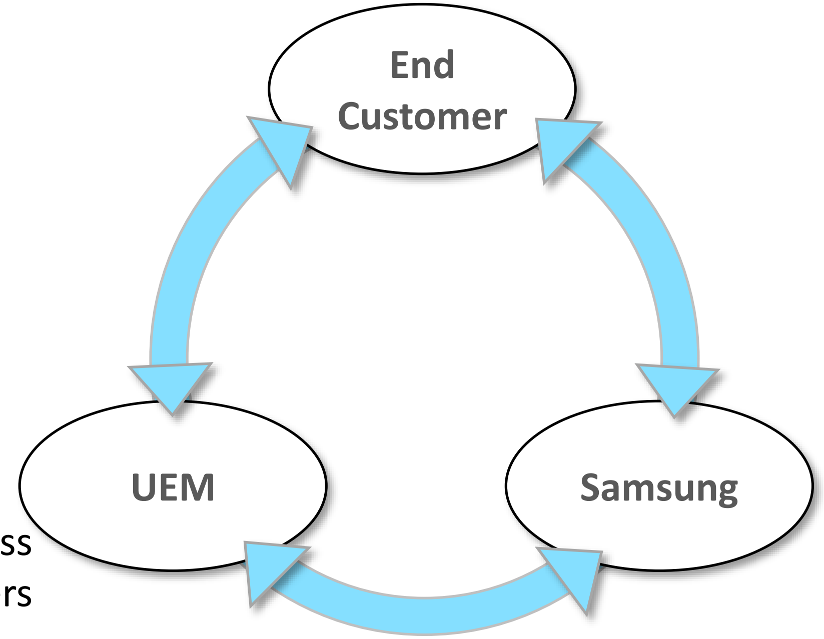
Knox Service Plugin (KSP)

Introduction To Product

New Knox features are not readily available to End Customers today

Need KPE features that may not be supported by my UEM solution vendor

Examples :
- Dex Management
- RCS Messaging Controls
- USB restrictions
- Wi-Fi and Bluetooth scan control



ROI to support a new Knox feature, unless it is widely used by my End Customers

New Knox features not readily available in the hands of End Customers!

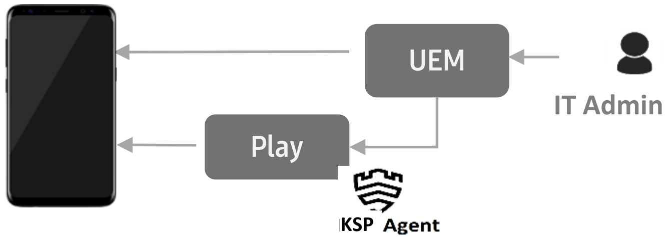
KSP intends to solve that problem

Delivers Knox features faster to end customers while eliminating integration costs for UEM partners

Overview

Support OEMConfig based configuration of Knox policies

KSP Agent published on Play store and supports Knox policies as managed app configuration



Value to UEM

- Invest in supporting OEMConfig once and enable zero day support for Knox policies on Android devices without repeat development

Value to End Customer

- End customer can use KSP Agent to set any Knox policy even if it is not supported by UEM on native console

Note: KSP is envisioned as a two stage solution. Focus of today’s discussion is on Stage 1 of the solution only.

What is KSP?

- Knox Platform for Enterprise (KPE) is our **core product** offering
  - Brings defense-grade security on the most popular consumer devices to all enterprises
  - Provides best-in-class hardware-based security, policy management, and compliance capabilities beyond the standard features in Android
- Knox Service Plugin (KSP) is **a channel** to access KPE features
  - KSP is an application that enables Enterprise Customers – through the use of their chosen UEM Partners – to deploy existing and new Knox features as soon as they are commercially available

KSP supports Android Enterprise deployments

- KSP supports Android Enterprise based deployments (does not support legacy Knox CL/COM modes)
- Customers should use managed Google Play store, for installing KSP and pushing the configuration

* Deploying KSP without managed Google Play is possible, but requires additional development from UEM

COBO

Fully Managed Device
(Device Owner)

Starting from

Android O (8.x) & Knox 3.0

COPE

Fully Managed with Knox Workspace

Starting from

Android P (9.x) & Knox 3.2.1[#1]

BYOD

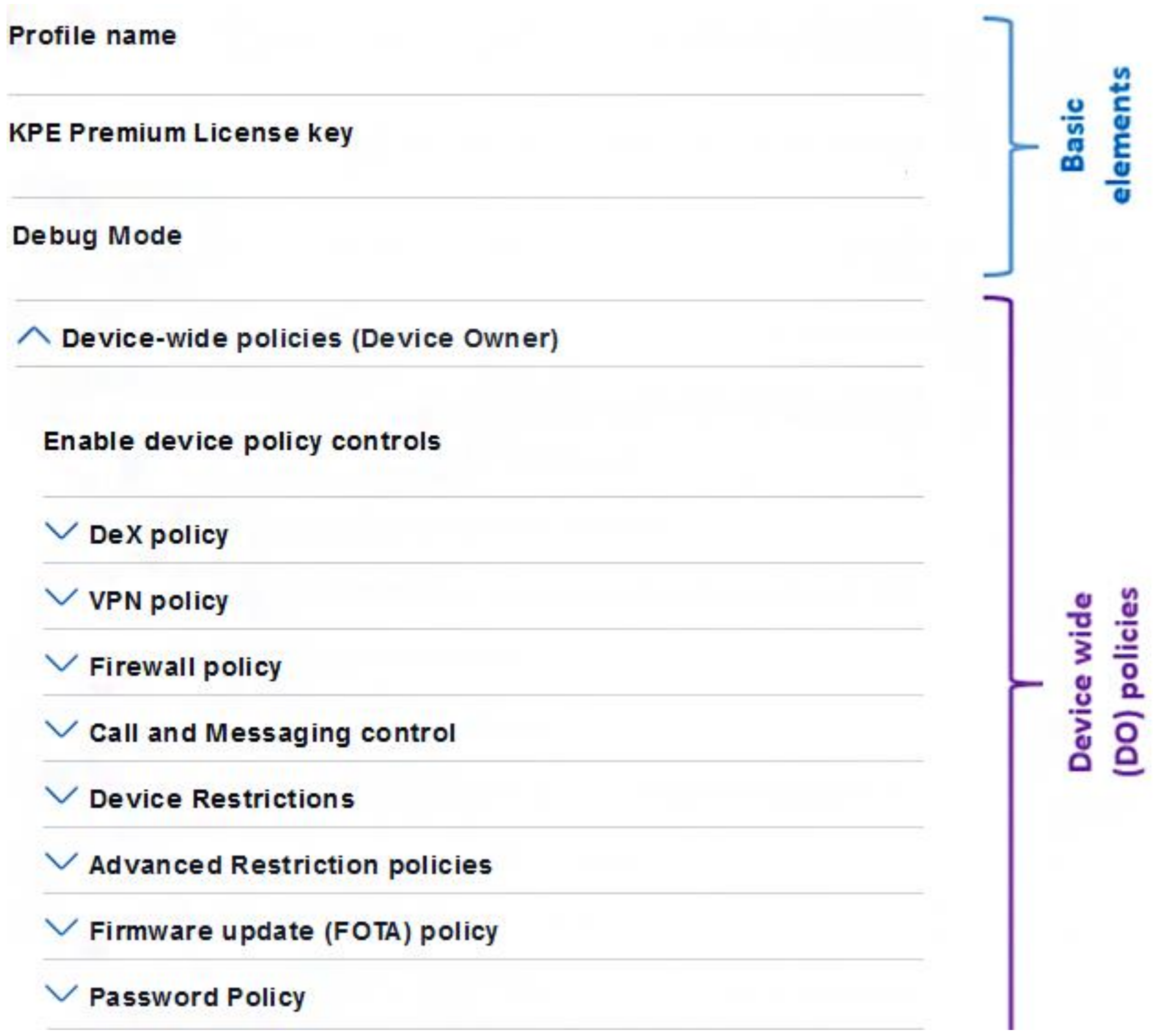
Knox Workspace
(Profile Owner)

Starting from

Android P (9.x) & Knox 3.2.1

#1 Even though KSP supports COPE mode, end customers cannot use it until UEMs complete additional development, for their console to support managed Play in both User 0 (personal space) and within work profile

Example of KSP policies on an UEM Console



Profile name

KPE Premium License key

Debug Mode

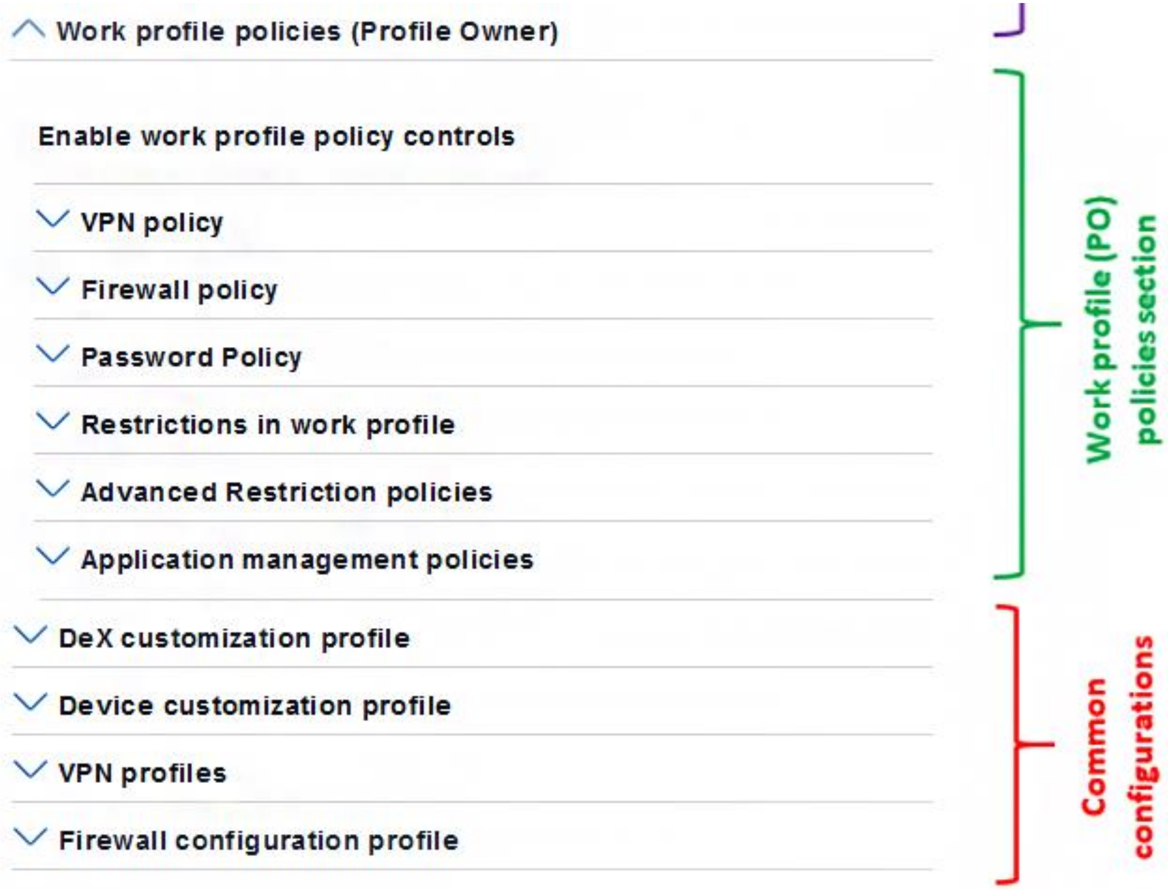
Device-wide policies (Device Owner)

Enable device policy controls

- DeX policy
- VPN policy
- Firewall policy
- Call and Messaging control
- Device Restrictions
- Advanced Restriction policies
- Firmware update (FOTA) policy
- Password Policy

Continued…

Continued…



Work profile policies (Profile Owner)

Enable work profile policy controls

- VPN policy
- Firewall policy
- Password Policy
- Restrictions in work profile
- Advanced Restriction policies
- Application management policies

- DeX customization profile
- Device customization profile
- VPN profiles
- Firewall configuration profile

KPE features already supported with KSP (1/2)

Completed & available on Play store

As of July 2019

Currently Supported

DeX

- Enable or disable DeX
- Enforce Ethernet, virtual MAC
- Disable packages in DeX mode
- Configure Home screen alignment
- Add app and URL shortcuts
- Setup screen timeout
- Disable over scan of monitor when connected in DeX
- Hide app icons in app drawer when in DeX mode
- Set Loading Logo
- Skip welcome screen
- Enable mouse cursor in Dual monitor mode
- Auto-start DeX mode on HDMI connect
- Disable DeX control from Quick Panel
- Customize DeX button options
- Set DeX wallpaper
- Configure app launch behavior (Knox 3.3+)

Standard restrictions

- Allow/block controls for Mic, Developer mode, power saving mode, Setting change, Share via list.
- Wi-Fi, Wi-Fi direct, BT, Tethering, Cellular data, VPN
- USB exception list, USB host storage, USB media player, USB debugging

Advanced restrictions

- Disable Wi-Fi and BT scanning for location accuracy
- Firmware controls
- Allow remote control
- Dual SIM control

RCS control

- Enable / Disable RCS messaging

Knox VPN

- Cisco AnyConnect, Pulse Secure, Built-in (Strong Swan) are supported
- Device wide, user wide & per-app VPN
- Proxy with VPN
- Blacklist apps
- Chaining

Device customization

- Keyboard controls (turn off predictive text & settings)
- Quick Panel configuration
- Enable battery protection settings (Knox 3.4+)
- Disable app suggestions (Knox 3.4+)

https://docs.samsungknox.com/knox-service-plugin/admin-guide/ksp-features.htm

KPE features already supported with KSP (2/2)

Completed & available on Play store

As of July 2019

Currently Supported

Device controls

- NFC control
- Wi-Fi controls for hotspot configuration and open network connection

Universal Credential Management

- Smart card based Email encryption & signing

Dual Data-at-Rest encryption

- Works with KME 1.23 and above

Biometrics Authentication controls

- Fingerprint, Iris and Face unlock control
- Multi-factor authentication

Application management

- Battery optimization whitelist
- Device Admin whitelisting
- Notification whitelist

Common Criteria

- Set CC mode
- SDCard Encryption
- Certificate revocation

Firewall and Proxy

- Allow, Deny rules
- Domain filters
- Static and PAC based proxy configuration

Enterprise Billing

https://docs.samsungknox.com/knox-service-plugin/admin-guide/ksp-features.htm

Appendix

FAQ

- **Is KSP application preloaded on Samsung devices?**
  - No. KSP is installed via managed Play.
- **Is it mandatory to have managed Play support to use KSP?**
  - UEM has to support managed Play in DO or PO to push KSP app and managed config to device.
  - Using KSP for deployments without managed Play is technically possible but it depends on UEM solution vendor’s support.
- **Can I use KSP with an on-prem UEM deployment?**
  - It is highly recommended to enable managed Play store.
  - To use KSP on-prem (without managed Play) depends on UEM solution vendor’s support. Please talk to your solution vendor to get them to prioritize support.
- **Does KSP work with Knox CL & COM deployments?**
  - KSP will not support Knox CL and COM deployments. It supports only Android Enterprise deployments.
  - As of April 2019, KSP is fully tested with COBO (fully managed) and BYOD (Knox Workspace / work profile) deployments.
  - Support for COMP mode (fully managed with Knox Workspace) will depend on UEM support and *may be* enabled later this year.
    - Please note that with COMP deployments UEMs support managed Play within PO (Workspace), so you can still use KSP for applying policies within the Workspace.
  - KSP works with Android 8.0 and above for fully managed device deployments, and works with Android 9.0 and above for all deployment modes.
- **Which devices support KSP?**
  - KSP has no device model restrictions per se, it depends on the Android version used.
  - KSP works on any Samsung mobile and tablet models with Android Pie (9.0) / Knox 3.2.1 and above
    - *For COBO (DO / fully managed device) deployments, KSP can also support Android 8.0 (Knox 3.x) based devices*

FAQ

- **Do customers need a license to use KSP?**
  - KSP is a free application on Play store
  - However Customers may need a valid KPE Premium license if they wish to apply any *premium* Knox policy using KSP.
    - Please note Customers need a valid KPE Premium License to use any policies inside Knox Workspace (PO) deployment, *regardless of KSP*.
- **How are new Knox policies released to customers?**
  - As a KSP app update in Play store and IT Admins can readily use it. *UEMs do not have do any additional development for each release.*
  - Each Knox policy supported by KSP is published as a "managed configuration" i.e., as an XML file within that app. So when new version of KSP is released to Play store (with new policies), IT Admin can use same UEM console to immediately pull the new version and see the new policies.
  - As a general guideline, use any feature provided by your UEM console natively first and use only KSP for bridging the gap i.e., apply only additional policies desired using KSP
- **Where can I find user guide for KSP and documentation on policies supported?**
  - We are working on publishing the information on Samsung Knox website, please watch this space for details and the URL.
- **How can IT admin know if policies are applied properly on the device?**
  - KSP will return results to UEM console via "Feedback channel". However this functionality will not be available until UEMs integrate Google API
- **What if my UEM console natively supports some Knox policies (like say, device restrictions) which are also part of KSP – should I duplicate my policy rules in both places?**
  - As a general guideline, Customers should use any feature provided by your UEM console natively first and use KSP only for bridging the gap i.e., apply only additional policies desired using KSP

Terminology

- Feedback channel: Return path to route status from the OEMConfig application to the UEM backend
- COMP: Corporate Owned with Managed Profile (same as COPE)
- COPE: Corporate Owned, Personally Enabled (also known as “fully managed device with work profile”)
- DPC: Device Policy Controller
- DO: Device Owner; a DPC app that controls the device in case of “fully managed device” deployments
- KPE: Knox Platform for Enterprise
- KPU: Knox Plugin for UEM, the working name used *in the past* for this project before the official name Knox Service Plugin (KSP)
- KSP: Knox Service Plugin
- KSP Agent: OEMConfig application in Play store for Samsung Knox mobile devices
- OEM: Original Equipment Manufacturer (such as Samsung)
- OEMConfig: Specification by Google and App Config community for Android
- Personal profile: On devices with a work profile, the area of the device outside the work profile
- PO: Profile Owner; a DPC app that controls the policies specific to work profile in case of BYOD or “fully managed device with work profile” deployment
- UEM: Unified Endpoint Management
- User 0: Main or default user for Android mobile platform; in case of deployments with a Work Profile this designates the Personal profile.
- User 10: User designed for Work Profile in an Android platform