SAMSUNG

Knox Platform for Enterprise White Paper

About this White Paper

This White Paper provides an overview of the Samsung Knox Platform for Enterprise, also known as KPE or Knox Platform, focusing on the unique advantages that differentiate KPE from other options in the mobile device market.

This document is designed for C level executives, security professionals, IT managers, IT admins, and others evaluating KPE as a solution. For additional information about KPE, go to Samsung Knox Product site.

Revision history

Version	Knox Version	Date	Revisions
1.0	3.2 and higher	September 12, 2018	First release.
1.0.1	3.2 and higher	November 1, 2018	Minor revisions.
1.1	3.3 and higher	February 20, 2019	New info about DualDAR Encryption and Knox Verified Boot. Updates to Feature Comparison and Sensitive Data Protection.

Copyright

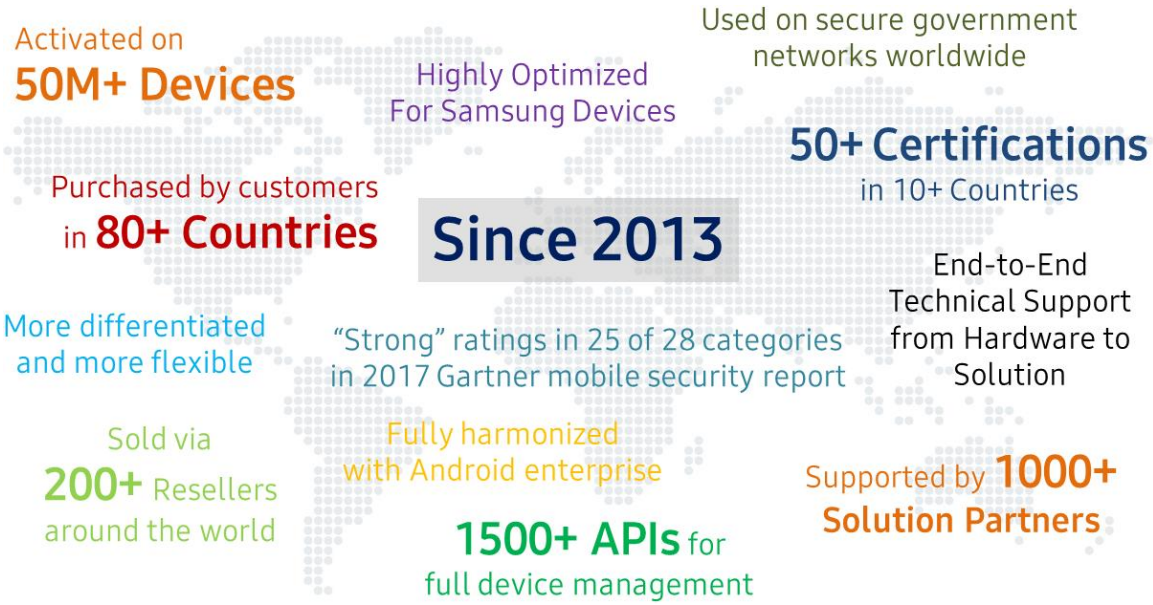
Contents

Introduction

The Samsung Knox Platform

Samsung's Knox platform brings defense-grade security on the most popular consumer devices to all enterprises. The Knox Platform provides best-in-class hardware-based security, policy management, and compliance capabilities beyond the standard features commonplace in today's mobile device market. The Knox platform is the cornerstone of a strong mobile security strategy supporting a wide variety of Samsung devices.

Why use the Knox Platform?



The Knox platform helps you and your enterprise avoid the security gaps common on many mobile platforms. Knox received strong ratings in 25 of 28 categories in Gartner's December 2017 Mobile OSs and Device Security: A Comparison of Platforms and has received strong ratings for the last three years in a row.

The Knox Platform's security hardening supports every aspect of mobile device operation. The Knox Platform enables trust in your mobile endpoints with advanced features like Samsung's patented Real-Time Kernel Protection (RKP) that stands as one of the best kernel protection technologies available from any mobile device vendor. The Knox Platform ensures IT admins can securely bulk deploy the best mobile device hardware, and quickly integrate with existing business infrastructure and apps.

Key benefits for enterprises

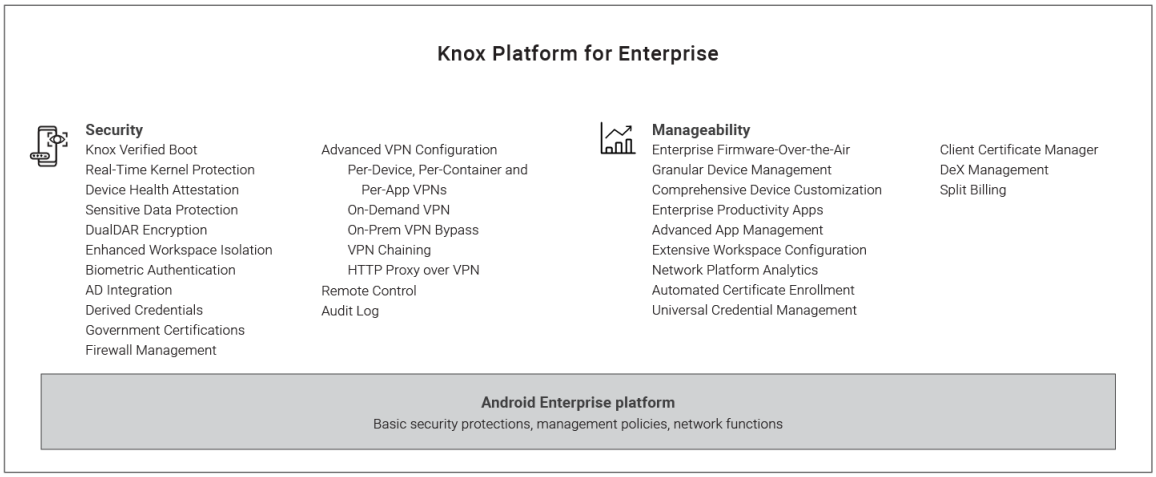
- Easily meet your organization's security and compliance requirements, by providing solid platform integrity, strong data protection, and fine-grained policy enforcement.
- Seamlessly activate and manage Knox Platform features through an Enterprise Mobility Management (EMM) system.

- Flexibly support infrastructure, deployment, and management requirements, through centralized remote device control, advanced VPN management, app whitelisting and blacklisting, and granular policies that control all aspects of Samsung devices.
- Effortlessly upgrade from Android Enterprise, leveraging a comprehensive set of Knox Platform benefits without affecting existing deployments.
- Securely deploy the innovative Samsung Desktop Experience (DeX) in new work environments, unifying mobile and desktop computing on one device.

The Knox Platform's cutting-edge security technology continues to be widely adopted and proven by numerous government, security, and financial agencies throughout the world. Samsung continually works with global government organizations and international regulatory bodies to meet a wide range of certification requirements designed to protect public safety and consumer privacy.

Knox Platform differentiators

The Knox Platform provides a robust set of features that are a superset of features on top of the basic Android platform, to fill security and management gaps, resolve pain points identified by enterprises, and meet the strict requirements of highly regulated industries. The following summarizes the key differentiating features:



For a quick overview of how these features compare across different platforms, see **"Feature Comparison"** on page **8.**

Security highlights

The following sections describe how the Knox Platform provides an industry-leading ecosystem of products and services to secure and ease mobile device management.

Hardware-backed security

The Knox Platform defends against security threats and protects enterprise data through layers of security built on top of a hardware-backed trusted environment.

- **Trusted environment** — A trusted environment separates security-critical code from the rest of the operating system. This strategic separation ensures only trusted processes that are isolated and

protected from attacks and exploits can perform sensitive operations, such as data encryption and decryption. Trusted environments perform integrity checks prior to executing any software. These checks detect malicious attempts to modify the trusted environment and the software running on the device.

- **Hardware-backed** — A trusted environment is hardware-backed if hardware protections isolate the environment from the rest of the running system. This isolation ensures that vulnerabilities in the main operating system don't directly affect the security of the trusted environment. The environment also ties integrity checks of the software running in the trusted environment to cryptographic signatures stored in the device hardware. Hardware-backed integrity checks prevent an attacker from exploiting software vulnerabilities to bypass protections and load unapproved software into the trusted environment.

The Knox Platform uses a hardware-backed trusted environment and the specific components depend on the device hardware. For example, ARM processors provide a Trusted Execution Environment (TEE) that leverages components such as the ARM TrustZone, ARM Hypervisor Mode, and Embedded Secure Elements. Knox features that use the trusted environment include Real-time Kernel Protection (RKP), Trusted Boot, Device Health Attestation, Certificate Management, Sensitive Data Protection (SDP), and Network Platform Analytics (NPA).

App isolation

The Knox Platform uses app isolation to prevent rogue apps from intentionally or inadvertently accessing unauthorized data. The Knox Platform provides several forms of app isolation to create a protected app container space on Samsung devices. Each option is based on the same core isolation technology called Security Enhancements for Android (SE for Android.) SE for Android is an integration of SELinux and Android, expanded to cover Android components and design paradigms. The Knox Platform offers these options:

- **Android Enterprise on Samsung devices** — Android Enterprise provides app isolation through Work Profiles, which provide basic isolation of enterprise apps from personal apps. When using Android Enterprise on Samsung devices, Knox provides features like Real-time Kernel Protection (RKP), secure enterprise apps, and hardware-backed storage of certificates and keys, making Android Enterprise even better on Samsung devices.
- **Knox Workspace** — The Knox Workspace builds on Android Enterprise by providing additional security and management enhancements. Specifically, the Knox Workspace benefits from hardware-backed integrity checks. These checks detect any tampering of the device or its security protections and lock down the Knox Workspace to protect confidential data. The Knox Workspace also supports Sensitive Data Protection (SDP), encrypting data during device runtime and decrypting only after the device user authenticates to unlock the Knox Workspace. Furthermore, the Knox Workspace provides more granular device management, for example, forced two-factor authentication for the Knox Workspace, the use of enterprise Active Directory credentials for authentication, and managed import and export of enterprise data in the Knox Workspace.
- **SE for Android Management Service** (SEAMS) — With SEAMS, you can isolate a single app or small set of trusted apps, to lock down the apps in the same container. App containers created with SEAMS provide the same benefits of the Knox Workspace. Unlike the first two options, however, SEAMS containers have no special GUI. Apps in a SEAMS container appear with the rest of the apps on the device, but are differentiated with a shield badge to show that they're isolated and

protected from apps not sharing their same container. You can create as many of these SEAMS containers as you want on-the-fly.

With the Knox Workspace, enterprises can deploy additional security and management policies to enforce requirements, such as those needed to work within highly regulated industries such as finance, healthcare, and government.

Data protection

Enterprises can protect personal and enterprise data on mobile devices using a rich set of Knox features:

- **User authentication** — Samsung Knox devices support not just password, PIN, and pattern authentication but also the latest biometric authentication: fingerprints, iris, face, and Intelligent Scan. Options are available for both device lockscreen authentication and separate Knox Workspace authentication. Through the Knox Platform, you can provide enforce two-factor authentication for the Knox Workspace or enterprise AD credentials to ensure stronger data protection.
- **Encryption of device data** — Samsung Knox devices provide data encryption through Sensitive Data Protection that binds to the hardware-backed Root of Trust and user authentication. This encryption ensures data is decrypted only on the device where the data is stored, and only by the device owner. DualDAR Encryption offers two instances of encryption to achieve an even higher level of reliability.
- **Encryption of network data** — Samsung Knox devices offer the widest selection of advanced VPN features, providing the ability to configure a separate VPN for the Knox Workspace as well as for individual apps, to reinforce data isolation even further. Knox also offers always-on VPN, on-demand VPN, on-premise VPN bypass, HTTP proxy over VPN, multiple active tunnels, strict data leakage controls, and VPN chaining or cascading.
- **Device tracking, locking, and erasing** — Samsung Knox devices offer the ability to track, geofence, and automatically lock devices based on events and security policies. For example, a device that leaves a specified geographic perimeter is locked, wiped of data, or reset to factory defaults.

Manageability highlights

Device management and deployment

Enterprises with tens, hundreds, or thousands of employee mobile devices need to manage them easily, securely, and efficiently. Through EMM systems, enterprise IT admins can use a web console to centrally and remotely manage devices over-the-air. IT admins can control Samsung Knox devices comprehensively, managing device features with ease.

This management is possible through the Samsung Knox SDK, which offers over 1500 APIs for granular and flexible control over Samsung devices. This functionality is on top of the basic APIs offered through the Android SDK, providing a more powerful superset of capabilities. An EMM app on an employee device receives IT admin commands from the EMM web console, and calls Knox APIs to deploy commands on Knox devices. This integration enables enterprise IT admins to deploy IT policies to manage and secure every aspect of Knox devices.

Device management services

To address a variety of business needs beyond security, the Samsung Knox portfolio is complemented by robust cloud services that ease mobile device deployment, customization, and management. These services include:

- **Knox Mobile Enrollment** — With this free service, enterprises can use a web console or REST API calls to automate device enrollment, either individually or in bulk. After an IT admin registers a device with this service, the device user simply turns it on and connects it to a Wi-Fi or 3G/4G network to enroll it with an EMM system. There is no manual enrollment of individual devices, and no need for IMEI management and verification – all onerous, time-consuming, and error-prone tasks.
- **Knox Configure** — Samsung phones, tablets, and wearables are fully customizable to work in numerous vertical markets such as hospitality, retail, and entertainment. Through a web console, Systems Integrators can create purpose-built devices that present a customized user interface, for example, an information kiosk, point-of-sales terminal, or in-flight entertainment system. The Systems Integrators can customize or restrict almost all aspects of device configuration and the user experience, including boot animations incorporating custom enterprise logos, display settings, wallpapers, network configurations, notifications, and software updates.

Learn more

This White Paper provides an overview of Knox Platform's security features and how they can help resolve common enterprise mobile deployment issues. For information about other Knox features, see the Samsung Knox website.

Feature Comparison

The following table summarizes the advantages provided out-of-box by Samsung Knox devices over non-Samsung devices, and how **Knox Platform for Enterprise** (KPE) extends **Android Enterprise** (AE). For more information, go to the Knox Platform for Enterprise home page.

Feature	AE on non-Samsung devices	KPE Standard on Samsung devices	KPE Premium on Samsung devices	How KPE extends AE
All Android Enterprise Features	●	●	●	KPE extends AE by providing advanced security and manageability controls.
Security				
Secure Lockdown on Tampering	◐	●	●	Upon detecting critical security compromises, the system locks down sensitive areas, preventing enterprise data from being accessed and leaked. In such circumstances, AE restricts access to previously installed keys. KPE extends AE by preventing whole components from running when tampered.
Remote Device Health	◐	●	●	Obtain visibility into which particular devices are experiencing security issues, such as unauthorized firmware, allowing you to

Feature	AE on non-Samsung devices	KPE Standard on Samsung devices	KPE Premium on Samsung devices	How KPE extends AE
				troubleshoot the issue immediately. AE provides software-based SafetyNet APIs, and KPE extends AE by providing reliable hardware-based device attestation.
Knox Verified Boot	◕	◕	●	Knox Verified Boot extends Android Verified Boot by verifying integrity before the device is booted and running, validating the bootloader, TrustZone, and Hypervisor, as well as the kernel.
Audit Log	◕	◕	●	KPE audit log provides comprehensive device logs for troubleshooting potential issues and captures events needed to satisfy government compliance requirements.
Real-Time Kernel Protection (RKP)		●	●	KPE extends AE by providing best-in-class kernel attack prevention features, including kernel code, kernel data, and kernel control flow protections. RKP drastically limits the number of possible attack types against Samsung devices.
Sensitive Data Protection (SDP)		●	●	With basic AE, device data is decrypted once the device boots. With KPE's SDP, selected files remain encrypted at runtime and are decrypted only after a device user authenticates their identity at the device lockscreen, or Knox Workspace login. KPE evicts decryption keys when the device or Knox Workspace locks, and complies with MDFPP requirements for US government and military.
DualDAR Encryption			●	With a single instance of encryption, potential flaws in the implementation can result in a single point of failure. KPE DualDAR provides two independent layers of encryption to achieve an even higher level of reliability by enabling redundancies in protecting Data-At-Rest. This dual encryption is required for classified deployments.
Enforced Two-Factor Authentication			●	KPE extends AE by enabling IT admins to force end-user two-factor authentication for logging into a Knox Workspace, or Managed Device. Authentication can accomplished either using biometrics (fingerprint, iris, face), or with traditional methods (password, PIN, pattern).
Government-Grade Common Criteria Mode			●	KPE extends AE's device controls by exposing a Common Criteria mode to simplify the process of configuring devices into a compliant state for defense deployments.
App Isolation Groups (SEAMS)			●	Unlike classic app containers utilizing a GUI, KPE extends AE by allowing you to manage "invisible" app isolation groups to protect a set of apps from any other set. Up to 300 groupings are possible.
Secure Certificate Enrollment Agents			●	KPE extends AE's certificate management APIs by providing a certificate enrollment service API that closely follow the latest security protocols. There is no reason to enroll certificates insecurely, or implement your own protocols.

Feature	AE on non-Samsung devices	KPE Standard on Samsung devices	KPE Premium on Samsung devices	How KPE extends AE
Manageability				
Manage Device Software Updates	◐	◐	●	A Samsung E-FOTA license enables the controlled rollout of firmware updates upon completion of internal testing, helps avoid compatibility problems with proprietary systems or apps, and minimizes user interaction requirements for updates. KPE provides granular firmware controls that AE does not have. For example, the ability to set highest accepted firmware version, apply specific firmware version to a set of devices at a specific date/time, and the option to block automatic firmware updates.
Remote Control	◐	●	●	KPE extends base remote control capability to allow IT to remotely control employee devices to troubleshoot and fix mobile devices in the field.
Customization	◐	◕	●	With KPE, IT admins can customize various aspects of the device software and UI beyond what is available in AE. Enable/disable task manager, hardware keys, multi-window mode, etc. Custom boot banner/animation, block specific system notifications, customize items appearing on the power off dialog screen, map volume keys to app task switching, and more.
Granular Roaming Controls	◐	◕	●	With KPE, IT admins can allow/disallow the use of "roaming" mobile connections that often incur high call/text/data rates. AE supports disabling mobile data. KPE extends AE by providing additional controls, such as the blocking of calls, or the blocking of app update downloads while allowing other data use. KPE Premium also enables separate roaming controls for each APN to support split billing.
Admin Device Lock	◐	◐	●	An admin device lock enables IT to lock out a device, preventing even valid credentials from being used. This is extremely valuable for managing end-user policy violations, including the travel to hostile countries. While AE supports locking the device screen, it does not lock out the user. KPE extends AE by allowing an IT admin to enforce an admin lock.
Firewall Management		●	●	KPE extends AE by providing an industry-exclusive ability to set device firewall rules. Using KPE, admins can also be notified when employees attempt to visit blocked domains.
Granular Device Policies		◐	●	With KPE's granular device policies, an enterprise can meet compliance or other deployment requirements using unique policies, that are not supported on AE, for SMS/MMS disclaimers, call restrictions, read and write restrictions on SD cards, granular Bluetooth profile restrictions. KPE's refined device policies can even manage DeX deployment settings.

Feature	AE on non-Samsung devices	KPE Standard on Samsung devices	KPE Premium on Samsung devices	How KPE extends AE
Advanced Workspace Configuration			●	KPE extends AE by providing container-specific policy settings. KPE enables strict policy enforcement for Bluetooth, SD Card, USB, and other technologies inside the container, while allowing the full use of these technologies outside the container.
Unlock using Active Directory Credentials			●	With KPE, there is no requirement for employees to remember separate credentials for Windows laptops and mobile devices. Additionally, with KPE device users can utilize their existing Active Directory credentials to unlock their devices.
Split Billing (Dual APNs)			●	KPE extends AE through the support of dual APN management. KPE enables enterprises to pay only for the data usage of approved business apps. Employees are then responsible for fees incurred for personal data usage.
Network Analytics			●	KPE allows an IT admin to deploy network threat detection solutions without granting tools complete access to all network traffic.
VPN				
VPN Granularity: Per-App, Per-Container, or Whole Device	◐	◐	●	KPE extends AE to provide very granular VPN controls. KPE can be configured with a VPN tunnel not just for a container or individual apps, but for the whole device.
Always On VPN	◐	◐	●	KPE utilizes strict controls to block traffic from bypassing a configured VPN, even in cases where the VPN client crashes or when the device is rebooting. AE does not block traffic when a VPN is down.
On-Demand VPN			●	A KPE VPN can be set to only activate when certain target apps are launched/running, and does not require additional VPN client support.
HTTP Proxy over VPN			●	A KPE VPN enables the use of web proxies on tunneled VPN traffic.
VPN Chaining			●	A KPE VPN allows the use of two VPN tunnels to double-encrypt traffic, enhance anonymity, and prevent a single security bug in a VPN layer from compromising network encryption.
Near-instant VPN connection times		●	●	The Knox VPN framework allows a near-instant VPN connection, clocking in at one second. This time is measured from when the VPN handshake and authentication completes, to when the tunnel is established and traffic from any tunneled apps can pass through the VPN. This time threshold applies to all apps, assuming 100 apps enrolled in the VPN profile, whether they are part of the Knox Workspace or not.

Core Platform Security

Root of Trust

Imagine every device in your network simultaneously infected with malware and combing through your confidential data. Attacks and exploits continue to mature in sophistication in an attempt to stay ahead of advancing mobile device safeguards. So what's the single solution that works on all devices at the same time? To build a robust Root of Trust stack that minimizes exposure, detects intrusions, and locks down sensitive information.

A Root of Trust is the cornerstone of any modern security protocol. It is a series of stringent checks and balances, beginning at the hardware level rather than the software level. This feature adds a level of security to devices, making them difficult to subvert as hardware is more immutable than software.

A Root of Trust answers many complicated security questions, such as:

- How do you **know** if a compromised OS was booted at runtime?
- Can you **trust** that your certificates are stored securely?
- Has an exploit **modified** the kernel or other system software?

Samsung's approach to addressing this issue is to bottleneck all security-critical functionality through trustworthy components. These trustworthy components are thoroughly designed, reviewed, and maintained with the following considerations:

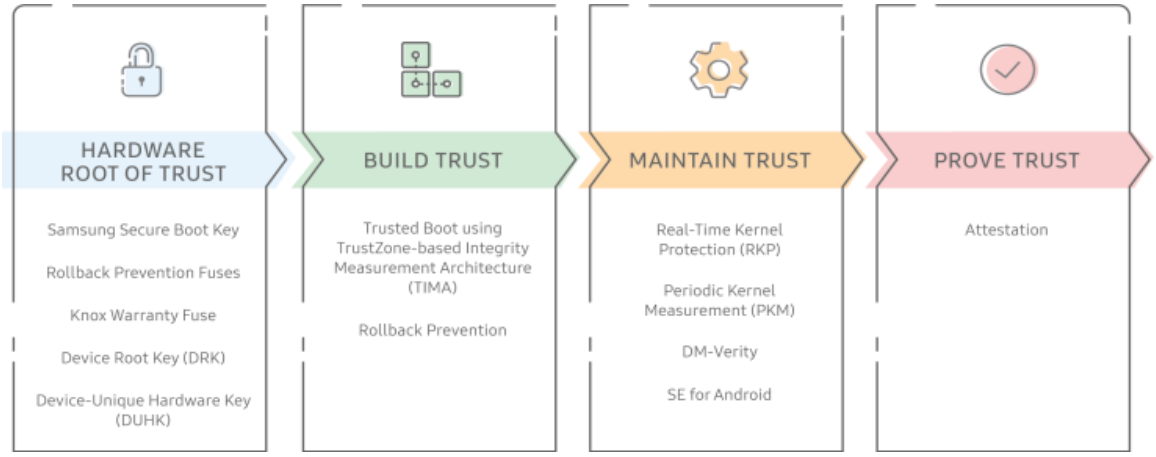
- **What are the assurances required?** High-security enterprise partners require a near-total ability to control and audit the software that interfaces with their systems. End users must have the authority to deny permission to use their device features and data. Each user, partner, and integrated system has its own requirements, many of which are assured in large part through the Roots of Trust.
- **How can components contribute to more complex assurances?** A Trusted Boot process enables the trustworthy transfer of control from the bootloader to the Android framework. This trustworthy transfer of control plays a key role in the admin's ability to audit apps running on the device. Secure boot is a complex process built on top of many smaller components that validate software, configuration files, deployment processes, and update processes. Each of these smaller components contributes to the secure boot process, and a secure boot process itself contributes to the security of other processes.
- **How can we make these components, their assurances, and their usage more robust?** Each Trusted Application on a Samsung Knox device ultimately represents a Root of Trust. These Trusted Applications encompass functionality such as device identity, key management, and remote attestation of device health. Samsung Knox uses these same Trusted Applications to provide its own assurances.

Knox Platform trusted environment

The Knox Platform builds a unique, industry-leading trusted environment in four ways:

- **Establishes** a hardware-backed Root of Trust, on which other components rely.
- **Builds** trust during boot, through features like Trusted Boot.
- **Maintains** trust while the device is in use, through features like Real-Time Kernel Protection.
- **Proves** its trustworthiness on demand, through Device Health Attestation.

This process and its components are as follows:



How the Root of Trust works

1. Knox Platform security starts in the factory—before users even power on their mobile device—when a Device-Unique Hardware Key (DUHK) is generated on the device using its hardware random number generator.
2. Next, the DUHK generates and encrypts the Device Root Key (DRK) and Samsung Attestation Key (SAK). The DRK and SAK contain an authentication code that enables recipients to verify the IMEI and serial number of provisioned devices. Since existing purchasing systems use a device's IMEI and serial number to track devices and not the DRK identifier, this enables users to obtain proof they are interacting with devices they have purchased. The use of the DUHK is only available to the TrustZone operating system. The TrustZone OS uses the DUHK to create subsequent keys unique to each trusted application. Trusted applications uses these keys to securely store data. The DRK and SAK are private keys that enable trusted applications to prove their own identity, as well as the identity of the device they are executing on. These trusted applications integrate deeply with hardware to provide hardware-backed security.
3. Upon device start up, Samsung uses the Samsung Secure Boot Key (SSBK) to check all software components. One of the components is the TrustZone Secure World, a chip partition reserved for secure code and data. Only specially privileged software modules running within the TrustZone Secure World can access these keys.
4. The software performs a check on each Knox Platform feature before allowing it to run. Since this chain of security checks begins with the very first hardware check, each feature is protected by hardware Root of Trust. No matter which link in the chain an attacker targets, one of the security checks detects it.

Hardware-backed security

The Knox Platform trusted environment leverages the following hardware components:

Secure hardware

- **ARM TrustZone Secure World** — The Secure World is the environment where highly sensitive software runs. The ARM TrustZone hardware ensures memory and components marked secure (for example, a fingerprint reader) can only be accessed in the Secure World. Most of the system, including the kernel, middleware, and apps, run in the Normal World. The Secure World software, on the other hand, is more privileged, and can access both Secure and Normal World resources.
- **Bootloader ROM** — The Primary Bootloader (PBL) is the first piece of code to run during the boot process. The PBL is trusted to measure and verify the boot chain. To prevent tampering, the PBL is kept in the ROM of the secure hardware. The device hardware loads and runs the PBL from ROM at boot, and the PBL starts the Secure and Trusted Boot processes.

Hardware keys

- **Device-Unique Hardware Key (DUHK)** — Samsung incorporates the DUHK, a device-unique symmetric key, in device hardware during the initial manufacture of the device. The DUHK binds data—for example, device health attestation data— to a particular device and is accessible only to a hardware cryptography module and not directly exposed to any device software. However, software can request that the DUHK encrypt and decrypt data. This DUHK encrypted data is bound to the device, and cannot be decrypted on any other device.
- **Device Root Key (DRK)** — The DRK is a device-unique, asymmetric RSA key pair that is signed by Samsung's root key through an X.509 certificate. This certificate proves that Samsung produced the DRK. The DRK is generated at manufacture in the Samsung factory and is stored on the device encrypted by the DUHK, thus binding it to the device. The DRK is only accessible from within the TrustZone Secure World and is protected by the DUHK. The DRK is an important part of the Root of Trust, as it derives other signing keys. Because the DRK is device-unique, it can tie data to a device through cryptographic signatures. Signing keys are derived from the DRK and used to sign data.
- **Samsung Secure Boot Key (SSBK)** — The SSBK is an asymmetric key pair used to sign Samsung-approved boot executables.
    - The private part of the SSBK is used by Samsung to sign secondary and app bootloaders.
    - The public part of the SSBK is stored in the hardware's one-time programmable fuse at manufacture in the Samsung factory. The Secure Boot process uses this public key to verify whether each boot component it loads is approved.
- **Samsung Attestation Key (SAK)** — The SAK is also a device-unique, asymmetric key pair that is signed by Samsung's root key. This signed key pair proves that the SAK was produced by Samsung. The SAK is used to sign the Attestation blob that indicates if the device is in a trusted state. The signature proves that Attestation data originated from the TrustZone Secure World on a Samsung device. Unlike the DRK, the SAK is a set of ECDSA keys. ECDSA is a newer asymmetric algorithm, similar to RSA but smaller and faster for the same strength.

Hardware fuses

- **Rollback Prevention (RP) fuses** — RP fuses encode the minimum acceptable version of Samsung-approved bootloaders. Old software may contain known vulnerabilities that may be exploited. Rollback prevention excludes approved, but out-of-date bootloaders from being loaded. The RP fuse version number is set when system software is initially installed and when specific updates

occur. Once the RP fuse version number is set, it is impossible to revert back to legacy software versions.

- **Warranty fuse** — The Knox Platform uses a one-time programmable fuse that signifies whether or not the device has ever booted into an unapproved state. If the Trusted Boot process detects non-approved components are used, or if certain critical security features such as SELinux are disabled, it sets the fuse. When the fuse is set, the following security measures take place:
    - Device Health Attestation checks fail.
    - The Knox Keystore removes the keys used by Sensitive Data Protection for data encryption and decryption, preventing access to sensitive data.
    - The Knox Workspace no longer operates, preventing access to secured enterprise apps and the data within.

Trusted Boot

Trusted Boot is a Knox Platform feature representative of Samsung's industry leading mobile device boot protection. Trusted Boot identifies and distinguishes unauthorized and out-of-date boot loaders before they compromise your mobile device.

If unauthorized boot components happen to load, an enterprise can trust that only validated and current components are loaded after Trusted Boot segregates authorized from unauthorized boot loaders.

Enterprises can check device integrity on demand through Knox Attestation, which reads Trusted Boot collected measurement data, along with an SE for Android enforcement setting, to form the basis of a device health verdict.

Secure lockdown on tampering

Bootloader measurements are recorded in secure TrustZone memory during device boot. At runtime, apps operating in the secure TrustZone can use these measurements to make security-critical decisions, such as whether or not to:

- Release cryptographic keys from the Knox Keystore.
- Launch the Knox Workspace app container.

If an unauthorized or out-of-date component version is detected, a tamper fuse is set. Once the fuse is set, sensitive work apps and data within the Knox Workspace are permanently encrypted and inaccessible since the integrity of the device is no longer guaranteed or validated.

The device user can still boot the device and launch personal apps. This flexibility promotes a nice balance between consumer functions, such as smartphone calls and personal apps, and the requirement to protect enterprise data.

Building on Secure Boot

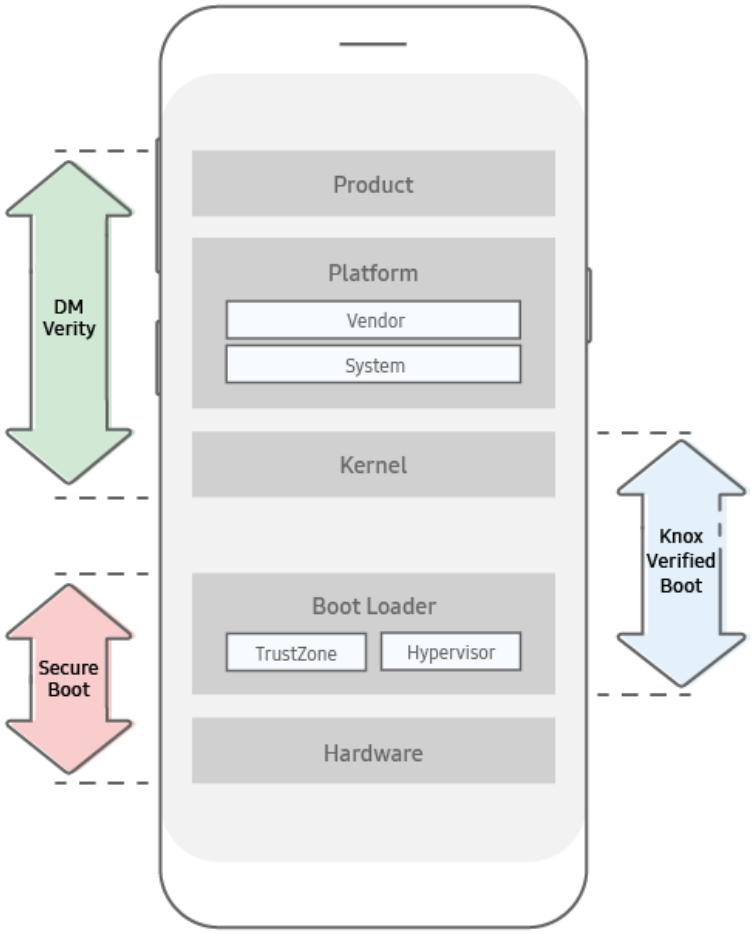
Before adopting Trusted Boot to work along with Secure Boot, Samsung devices were using Secure Boot to prevent unauthorized bootloaders and operating systems from loading during start-up. Secure Boot is implemented by each bootloader cryptographically verifying the signature of the next bootloader in

sequence, using a certificate chain with its root-of-trust resident in hardware. If verification fails at any step, the boot process terminates.

While Secure Boot is effective at preventing unauthorized bootloaders, it is unable to distinguish between different authorized binary versions. For example, Secure Boot can't distinguish between a bootloader with a known vulnerability as opposed to a later patched version, since both versions have valid signatures. Trusted Boot however was introduced to verify the same bootloader, kernel and platform build.

Knox Verified Boot (KVB)

Knox Verified Boot (KVB) is a new solution that both extends and enhances Android Verified Boot (AVB). While AVB only checks the integrity of the kernel and platform components, KVB extends those checks to also cover the earlier bootloaders. This provides a more comprehensive guarantee the device is booting using properly signed components that are all from the same build. KVB performs the same type of validations as the existing Trusted Boot mechanism, but it is able to do so before the device kernel is booted, and thus provides the same data protection guarantees earlier.



With KVB, component checks are conducted in the bootloader, and validations are made before system services are even started.

KVB is supported on Samsung S10 and above devices running the Android P operating system or later.

Real-time Kernel Protection (RKP)

The Knox Platform's patented Real-time Kernel Protection (RKP) is the industry's strongest protection against kernel threats and exploits. RKP works seamlessly out-of-the-box, with no setup required. Simply powering on a Samsung Knox device provides world-class threat protection and attack mitigation. RKP supports the rest of the Knox security offerings to provide full security coverage without the typical gaps anticipated with mobile devices.

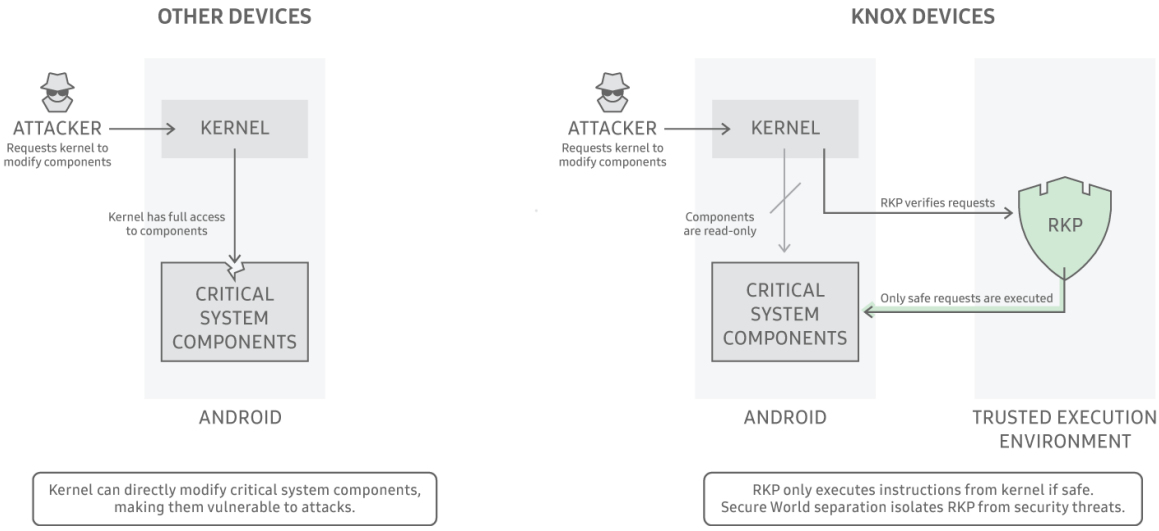
Why does kernel protection matter?

Kernel protection is central to device security and enterprise data protection. When attackers find software vulnerabilities, they often escalate privileges and compromise the core of the OS: the kernel.

A compromised kernel can leak sensitive data and even allow remote monitoring and control of the affected device. Other more commonplace protections like Secure Boot or hardware-backed keystores are of little value if the kernel itself is controlled at runtime. After a device boots and decrypts sensitive content, a kernel compromise can result in data leaks that directly impact an enterprise's data integrity.

RKP design and structure

As part of the Knox Platform's security offerings, RKP employs a security monitor within an isolated execution environment. Depending on the device model, either a dedicated hypervisor or the hardware-backed secure world provided by ARM TrustZone technology provides the isolated execution environment.



RKP's isolation from the kernel shrinks the Trusted Computing Base (TCB) and helps secure it from attacks designed to compromise the kernel. This unique ability enables RKP to detect and prevent the most common kernel attacks. RKP protections are grouped into three areas:

- **Kernel code** — RKP prevents modification of kernel code and logic.
- **Kernel data** — RKP prevents modification of critical kernel data structures.

- **Kernel control flow** — RKP prevents Return-Oriented Programming (ROP) and Jump-Oriented Programming (JOP) attacks that reuse existing kernel logic to piece together exploits from the kernel's own code.

How is kernel protection possible?

A kernel protection mechanism can't exist completely in the kernel only, since an attacker could circumvent it if the kernel itself has a flaw. The kernel is the lowest granular control level over the OS and, as such, usually can't be effectively monitored from any lower level in the system.

RKP uniquely employs a security monitor within an isolated execution environment. Running within an isolated execution environment would normally compromise a security mechanism's ability to see into the kernel and monitor activities at runtime. However, RKP succeeds by utilizing patented techniques to control device memory management and by intercepting and inspecting critical kernel actions before allowing them to execute. RKP is thus able to prevent a compromised kernel from bypassing other security protections. This prevention significantly reduces the severity of kernel attacks and limits the effectiveness of exploits that would typically cripple a mobile device.

Since RKP is always active and requires no management control, kernel protection is only possible if it meets strict usability and performance requirements. RKP's protections are activated out-of-the-box, with no performance impact to customers.

Periodic Kernel Measurement (PKM)

The TrustZone-based Integrity Measurement Architecture (TIMA) architecture provides a number of core features to protect against mobile device compromise. One of these central TIMA features is Periodic Kernel Measurement (PKM).

PKM periodically monitors the kernel to detect if legitimate kernel code and data were modified maliciously. PKM also monitors the key SE for Android data structures in OS kernel memory to prevent malicious attacks from corrupting and potentially disabling SE for Android. PKM protects the Linux kernel code and data pages from malicious exploits and helps prevent attacks attempting to disable SE for Android.

During a device firmware build, the SHA1 hash of every kernel code, and read-only data page, is calculated and gathered into a measurement file. These measurements are signed by Samsung to ensure data integrity and authenticity before its included in the firmware. When TIMA is initialized, PKM receives the kernel page measurements and verifies the signature to prove integrity and authenticity before storing the measurements in the secure world. During device operation, TIMA periodically recalculates the measurements of the running kernel and compares them to the signed measurements stored on the device. If any discrepancy is detected, a violation is reported to both system logs and the user.

When PKM runs, it reads the physical memory addresses used by SE for Android to determine whether:

• SE for Android is enabled

• SE for Android is in enforcing mode.

If malicious code manages to disable SE for Android, or switch it to permissive mode, PKM detects the state change and reports a violation to quickly assist an administrator in problem diagnoses.

Full security coverage

Each year, Samsung's research and development teams add the latest runtime protections to a growing list of unique capabilities found only within RKP.

Although RKP is only one piece of Samsung's holistic security solution, it successfully demonstrates the unique security guarantees possible when combining hardware, software, and advanced security research. Ensuring security claims are low maintenance, highly effective, and industry-leading is what provides enterprise customers the trust they need to deploy mobile devices in high-security environments.

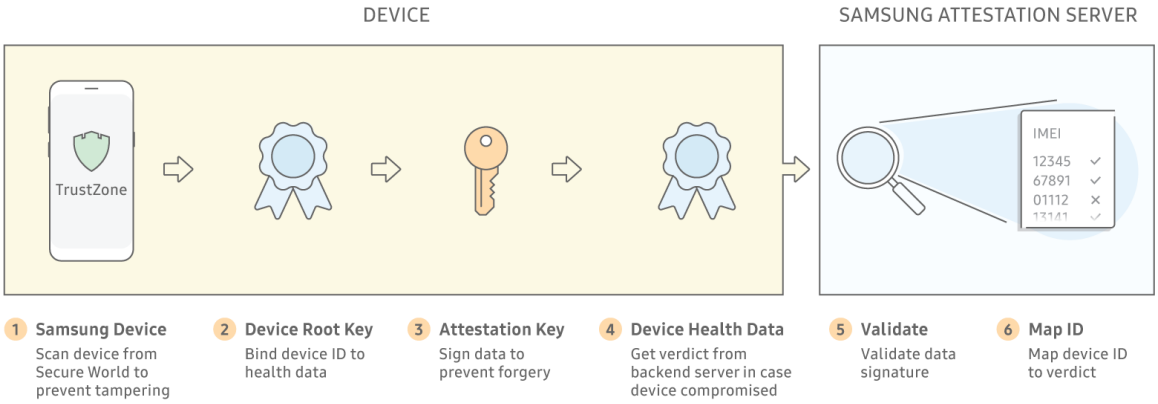
Device Health Attestation

A mobile device can be compromised if unauthorized agents gain super-user access permissions to the powerful system files that control device operation and data access. This loss of control is possible if a device user roots their device to get full control over the device firmware, files, UI, and apps. Unfortunately, malware can exploit this vulnerability to steal passwords, hijack identities, access secret info, install apps, and modify firmware.

Enterprises with Bring Your Own Device programs are especially at risk, as employees may potentially use rooted Android devices in the workplace. Risks range from the undetected exposure of confidential enterprise assets to wider more insidious attacks on other enterprise resources and infrastructure. Enterprises must have a fail-safe way to detect if a device is compromised, before allowing device users to deploy it in the workplace.

Reliable detection of compromised devices

Malware can potentially intercept and forge the results of a device health check, making a compromised device seem secure. The Knox platform leverages its hardware-backed trusted environment to reliably detect and report compromised devices.



Because a Device Root Key (DRK) is unique to each device, it can tie data to a device through cryptographic signatures. The Samsung Attestation Key (SAK) signs the Attestation data to prove that it originated from the TrustZone Secure World on a Samsung Knox device.

Knox Attestation works in tandem with Trusted Boot and Periodic Kernel Measurements to ensure the integrity of devices during deployment, bootup, and operation.

How Knox Attestation works

1. A device check is initiated by either:
    - An enterprise IT admin using an EMM console
    - A web script executing a regularly scheduled check
2. The web server that initiated the check requests a nonce from Samsung's Attestation server. A nonce is just an arbitrary number used in cryptographic communication to uniquely identify each attestation result.
3. The web server instructs the device to begin a check, passing the nonce as a check identifier.
4. A Knox Attestation agent on the device operates within the Secure World partition within the ARM TrustZone to create a blob, that is, a binary large object. This blob is a snapshot of the device's current state. It contains data about whether the device was ever rooted, or if the device has a bootloader or firmware file that was not factory installed or part of an official upgrade.
5. Samsung's Attestation server validates the data signature on the blob to ensure that it was from a trusted Samsung source, analyzes the blob data, and derives a verdict indicating whether or not the device is compromised.
6. The original requestor of the device check can quickly take action, for example,
    - Report the verdict to the device user.
    - Immediately prevent the device from accessing enterprise systems.
    - Uninstall any enterprise apps or assets already on the device.

Unique advantages of Knox Attestation

Knox Attestation provides these key differentiators:

- Health measurements guaranteed per device, through a Device Root Key.
- Health results that easily map to device identifiers like an IMEI.

Unlike other solutions on the market, Knox Attestation enables IT admins to determine which attestation result correlates with which device, without having to painstakingly map IDs manually. With competitor solutions, results are returned for separate devices, but IT admins can't differentiate between devices, and consequently the results are not actionable. Knox Attestation returns a single device ID and enables IT admins to prevent or contain issues promptly.

Sensitive Data Protection (SDP)

Protecting Data-At-Rest (DAR) on mobile devices is a major concern. While the industry standard is to encrypt all the data on a device, that data is decrypted and accessible after the device boots successfully. This access process means that once a device is lost or stolen, a sophisticated attack can extract data as long as the device is still running, even if the device is locked. Samsung created Sensitive Data Protection (SDP) to address this specific issue.

SDP meets the Mobile Device Fundamentals Protection Profile (MDFPP) requirements defined by the National Information Assurance Partnership (NIAP) for DAR, meaning that SDP is approved for use by the US government and military.

Two levels of protection

KPE protects user data on the device through Data-at-Rest encryption. Data remains encrypted on disk, and can only be decrypted when the device is powered on. Recovery of data decryption keys is tied to:

- device hardware, meaning data is recoverable only on the same device
- device boot-time integrity measurements
- a user credential dependent on configuration

Additionally, a mechanism is provided to optionally mark data as sensitive, which subsequently cannot be decrypted while the device is in the locked state. Here are the two protection modes that KPE provides for Data-at-Rest:

- **Protected**: All files stored on the device are treated as Protected by default. Protected data is stored on the device file system as encrypted data, and is only decrypted when an application accesses the data. This mechanism provides the data-at-rest protection while the device is powered off. Even if the device is in the lock state, applications can access protected data.
- **Sensitive**: Files can also be optionally marked as sensitive, using the Sensitive Data Protection (SDP) mechanism. SDP uses a key management scheme which ensures sensitive files can only be decrypted in the unlocked state, by purging keys from RAM when the device is locked. However, SDP also provides the ability for new files to be written and encrypted in the locked state using public key cryptography.

How SDP works

Samsung Galaxy devices supporting Knox 3.3 and above are enabled to support Android's File Based Encryption (FBE) for Data-at-Rest. Data encryption is enforced across the device using:

- EXT4 encryption FBE mechanism
- FIPS compliant hardware crypto module (AES256-XTS)

Optionally, the external SD Card can be used with:

- eCryptfs stacked file system
- FIPS compliant Kernel crypto module (AES256-CBC).

FBE keys are derived using a password entry, which is either the default hard-coded password or the device user's password used to unlock the device.

While in the unlocked state, SDP works as follows:

- Encrypts sensitive data using a per-file File Encryption Key (FEK). These keys are encrypted with the SDPK.sym (Sensitive Data Protection Key, symmetric), which is encrypted by the SdpMasterKey.
- Keeps the SdpMasterKey in memory only while the device is unlocked, to allow decryption of the SDPK.sym and SDPK.pri (private).
- Encrypts the SdpMasterKey using the key that is protected by both ephemeral keys derived from the device user's password and a key chaining to the Root Encryption Key (REK) using the Keystore.
- Clears the SdpMasterKey when it transitions to the locked state, and re-derives it when the user unlocks the device or workspace.

While in the locked state, SDP handles apps writes of sensitive data differently:

- Rejects app attempts to open sensitive data files, as KPE no longer has the keys needed to retrieve sensitive data in memory and cannot re-derive them until the user unlocks the device or workspace.
- Encrypts any new sensitive app data by using both a:
  - per-user sensitive data ECDH asymmetric key pair (SDPK.pri/pub)
  - per-file ECDH key pair [DataK.pri/pub] generated on behalf of the app
- Protects the private portion of the ECDH key pair (SPDK.pri) with the SdpMasterKey, the same Key Encryption Key (KEK) used to encrypt the sensitive data per-file FEKs.
- Clears the SdpMasterKey when it transitions to the locked state.

SDP protection of apps

The native **Samsung Email** app automatically uses SDP to protect email bodies and attachments. For performance reasons, the email header (including the subject and sender) is not protected with SDP.

The **Knox Chamber** is a dedicated directory in the Knox container file system. All stored files within the Knox Chamber directory are automatically marked as sensitive and are handled by the SDP mechanism.

Unique advantages of Knox SDP

- **MDFPP-Compliant** — Knox SDP is certified as MDFPP-compliant. Without Knox SDP, the base Android system is not certified as satisfying MDFPP requirements, which mandates a form of SDP.

MDFPP compliance is a requirement for many government agencies and the companies they work with. Samsung has more MDFPP-certified products than any other mobility solution provider.

- **Granular Control** — You can use Knox SDP to protect not just the whole device, a container, or individual files but also selected database columns.
- **Per-App Password** — You can further customize Knox SDP to decrypt a particular app's Sensitive Data only after an app user enters an app-specific password. In this case, the device or container unlock authentication alone does not decrypt app data. An app password is also needed for a higher layer of security.
- **App Protection** — Knox SDP is enabled by default to secure both Samsung Email as well as Knox Chamber.

App Container

Device users typically want their personal data and work data on one device. This requirement presents a challenge for enterprises, which need to ensure that:

- Work data is fully protected; and
- They don't run into any liability issues by accidentally interfering with a user's personal data.

Knox Workspace is an app container that provides enterprises with a solution to securely isolate personal and work data on one device. Protected by best-in-class hardware security, Knox Workspace provides IT admins with granular management policies. The Knox Workspace goes far beyond the standard data isolation provided by competitor container solutions.

Hardware-Backed Security

The Knox Workspace benefits from many of the Knox platform security features. For example:

- Device users can't create or use the Knox Workspace if the device is compromised due to unauthorized boot loaders or unauthorized modifications.
- The device's Knox Workspace data is protected against these types of kernel exploits, which can compromise other mobile platforms, in one or more of the following ways:
  - A malicious process in the personal space exploiting the mapping of kernel data.
  - Privileges of processes running in the personal space escalating to allow access to data in the Workspace.

Granular Management Policies

The Knox Workspace provides an IT admin with granular management policies to address the challenges of maintaining personal and work data on the same device.

Data Transfer

With the isolation of work and personal data, a device user has access to two separate spaces. To increase productivity in certain situations, it is often required to share data from one space to another. For example, while using a phone app in the personal space, it may be necessary to call a work contact saved in the secure work space. With the Knox Workspace, an IT admin has the granular management policies to manage the import and export of data to and from the Knox Workspace. This data can include apps, files, clipboard data, call logs, contacts, calendar events, bookmarks, notifications, shortcuts, and SMS.

Container-Only Control

For liability and productivity purposes, an IT admin can't apply effective policies on a mobile device with both personal and work data. The Knox Workspace provides the IT admin the ability to configure and control critical functionality for the container only. An IT admin can enable or disable the following exclusively for the container:

- Bluetooth
- NFC
- USB access
- External storage

Container Configuration

With the isolation of work and personal data, the device user has access to two separate spaces. This dual access presents some challenges to quickly identify and access work data.

To enhance usability, the Knox Workspace provides an IT admin the ability to add work shortcuts to their personal space so they can quickly access work data. The Knox Workspace also provides an IT admin with the ability to set custom resources, such as work badges on app icons so a user can quickly identify their company's work apps.

Password Policy

An enterprise IT admin must ensure only authorized people have access to work data inside container. The Knox Workspace supports advanced authentication mechanisms to meet all enterprise needs.

An IT admin can enforce and configure:

- Complex password or code scheme
- Two-factor authentication
- Active Directory authentication

Additionally, an IT admin can lock the container to restrict access. This restriction is necessary when a device is out of compliance, lost, or stolen.

Network Security

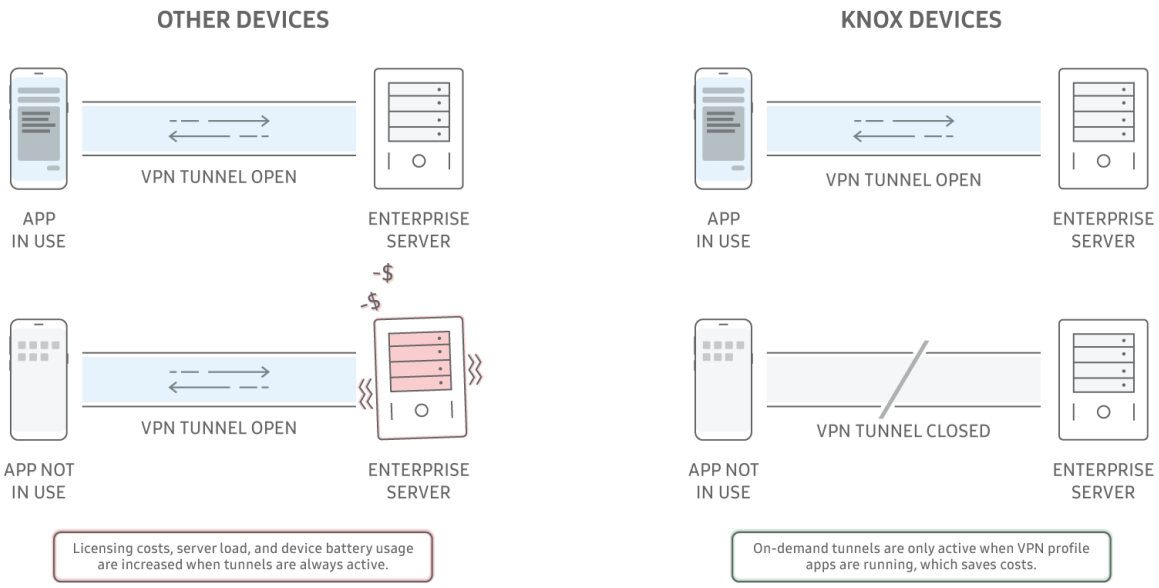
Virtual Private Networks (VPN)

Standard Android comes with basic VPN abilities that are adequate for most consumers. But many enterprises need better security and more flexible VPN controls for larger deployments. The Knox VPN framework includes the most advanced enterprise-focused feature set, which ensures that VPN connections are efficient, reliable, secure, and compliant with industry regulations and best practices. The Knox Platform VPN framework allows the integration of third-party VPN clients in addition to the built-in VPN client.

Unique advantages of Knox VPN framework

The Knox Platform VPN framework supports all common VPN types, protocols, and configuration options. When deploying VPN solutions, enterprise IT admins must ensure VPN deployments work smoothly, don't waste server resources, limit the VPN solution licensing costs, and enforce strict security policies that prevent data leakage.

The following is an example showing how Knox on-demand VPNs save cost:



The Knox Platform provides the following differentiating VPN features and advantages:

- The flexibility to use a VPN tunnel for the entire device, the Knox Workspace only, or a single app only.
- The unique ability to use a single VPN tunnel for traffic both inside and outside the Knox Workspace, without requiring separate VPN clients and licenses.
- The cost saving benefit of using VPN tunnels on-demand, only when apps in a VPN profile are running.
- The convenience to bypass VPN tunnels when a device is on-premise in a local corporate network.

- The strict coverage of corner cases to prevent data leakage outside of VPN tunnels, even during a device boot.
- The ability to connect multiple tunnels simultaneously.
- The extra security of chaining VPNs (also known as cascading or nesting VPNs) for greater anonymity, for example, in classified deployments.
- The power of configuring web proxies over VPN:
    - Web proxy configurations are tunnel-specific.
    - Web proxy support for NTLM authentication, basic authentication, PAC, and PAC with authentication.

The following Knox VPN features are also available, but are dependent on the VPN client:

- **QoS or traffic tracking and shaping.** The Knox VPN framework can inform the VPN client when any installed apps generate any traffic.
- **Automatic reconnection of VPN tunnels when the server side disconnects.** Server-side disconnections are more difficult to detect and handle than device-side disconnections, which are usually related to detectable conditions like loss of connectivity or the presence of new network connections, such as a new Wi-Fi connection.

Robust handling of enterprise requirements

Regardless of the features you choose, the VPN should act predictably even when the unexpected occurs. The following are some common scenarios where Knox Platform enhancements ensure proper VPN behavior:

- During a download, VPN tunnels direct download manager traffic to the VPN tunnel tied to the app that requested the download.
- VPN tunnels handle system events such as power saving mode entry or exit, package addition or removal, connectivity changes, and admin app changes.
- VPN profiles can specify which non-present apps must also use a VPN tunnel if they are ever installed.
- Even the free, built-in VPN client supports all the advanced VPN features listed in the previous list items.
- Robust blocking rules prevent data from leaking to the outside of the tunnel. Common gaps in coverage that Knox Platform VPNs correctly handle include:
    - A VPN client crash or other client app issues
    - A tunnel that has not yet been established, for example, during boot
    - A VPN client that is unable to connect to a VPN server
    - A proxy port that is blocking
- Handle captive portal prior to VPN tunnel establishment.

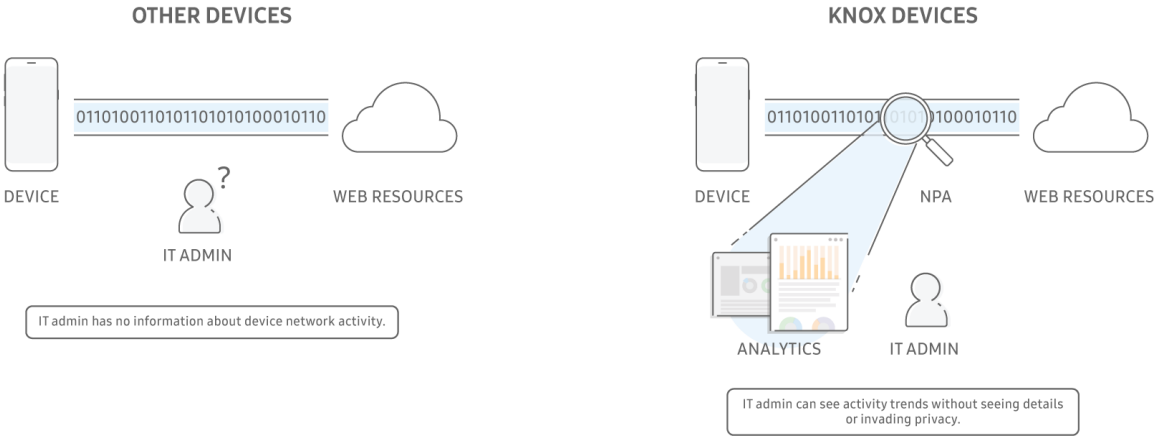
High-security built-in VPN client

The built-in Android VPN client (also called StrongSwan) is available on all Samsung devices, and is also integrated within the Knox Platform VPN framework, enabling the extra properties available within the Knox platform. The built-in VPN client, even without the Knox VPN framework, is differentiated from what Android offers, providing these advanced VPN features:

- FIPS 140-2 certified device cryptography components
- CPA certification at the Foundation grade, based on its successful Common Criteria evaluation against the Protection Profile for IPsec VPN Clients v1.4
- Security characteristics of IPSec VPN client version 2.5, as set by the NCSC
- Internet Key Exchange (IKE and IKEv2) and Suite-B algorithms:
    - IPsec IETF RFCs – IKEv1
    - IKEv1 – Main and aggressive IKE exchange modes with pre-shared key, certificates, Hybrid RSA, and EAP-MD5 authentications
    - IKEv2 with PSK and certificate-based authentication
    - IKEv2 – Pre-shared key, certificates, EAP-MD5 EAP-MSCHAPv2 authentication methods, and mobile extensions
    - Triple DES (56/168-bit), AES (128/256-bit) with MD5 or SHA
    - IKEv1 Suite B Cryptography supported with PSK and ECDS signature-based authentications
    - IKEv2 Suite B Cryptography supported with ECDSA signatures

Network Platform Analytics (NPA)

Endpoint devices, such as mobile devices, are hard to monitor for security issues. Third-party apps can't inspect OS behaviors and networking patterns, something that is possible on desktop platforms. These limitations, combined with the prevalent use of endpoint encryption create an information "black hole". This information black hole makes it more difficult to detect misconfigurations, troubling network usage patterns, the misuse of enterprise resources, or other signs of issues that impact an enterprise's bottom line.



The NPA framework enables insights into mobile software and network use, misconfiguration, and network-based threats. Powerful analytics solutions use the NPA framework to increase endpoint visibility without violating the confidentiality of data moving across enterprise devices and networks.

Combined with a compatible analytics solution, NPA simplifies many device administration tasks:

- Detect **more** IT problems — "I don't know what I can't see!"
- Detect problems **faster** — "Notify me automatically of suspicious patterns."
- Investigate more **easily** — "Walk me through the chain of events."
- See root cause **attribution** — "Am I being attacked? Is this a bug? Is something misconfigured?"

- Provide **visibility** required to **trust** mobile devices — "Show me how my network is being used."
- Enable quicker **remediation** — "Lock down the device, user, or app causing this issue!"

NPA design

The NPA framework provides real-time information about the network packets leaving a device and the context surrounding the flow of data. An NPA-compatible Network Analyzer then analyzes the available data to provide valuable insights. Is your new beta app sending sensitive data to an unexpected server in a foreign country? Analyzing endpoint flow data gives us insights into network traffic, such as:

- The destination of every network flow, using either IPv4 or IPv6 addresses
- The domain name originator associated with the destination IP address
- The start and stop time for the network flow
- The number of bytes transferred in and out during the network session
- The name of the process or app initiating the data flow
- The cryptographic signature of the app initiating the data flow, and of its parent process
- Whether or not traffic originated from a tethered device (for example, a mobile hotspot) or from within the device

NPA maintains enterprise data confidentiality as it only inspects the header data and the context surrounding network traffic patterns. NPA and NPA-compatible network analyzers don't have access to actual data packets. This feature is a strong differentiator compared to solutions that unnecessarily collect and redirect all endpoint network traffic, usually by means of a web proxy or VPN.

Unique advantages of Knox NPA

The Knox platform NPA provides the only mobile platform for granular endpoint networking insights. Some unique advantages are:

- NPA is unaffected by endpoint network encryption.
- NPA can uniquely attribute network patterns to the specific software responsible.
- NPA can differentiate between traffic originating from a well-known Android app and a fake app impersonating the app.
- NPA does not expose your entire network traffic to the analytics solution.

NPA-compatible solutions

Samsung's release partner for NPA is Cisco. Cisco's network security products can now interface with Knox NPA to provide endpoint visibility of Knox devices. Admins can get this visibility even when a VPN is encrypting endpoint traffic. These insights are exposed to admins using the Cisco StealthWatch console and remediation steps performed using Cisco ICE.

Other Knox partners are preparing NPA-based solutions to help solve other common problems associated with mobile device deployments.

Certificate Management

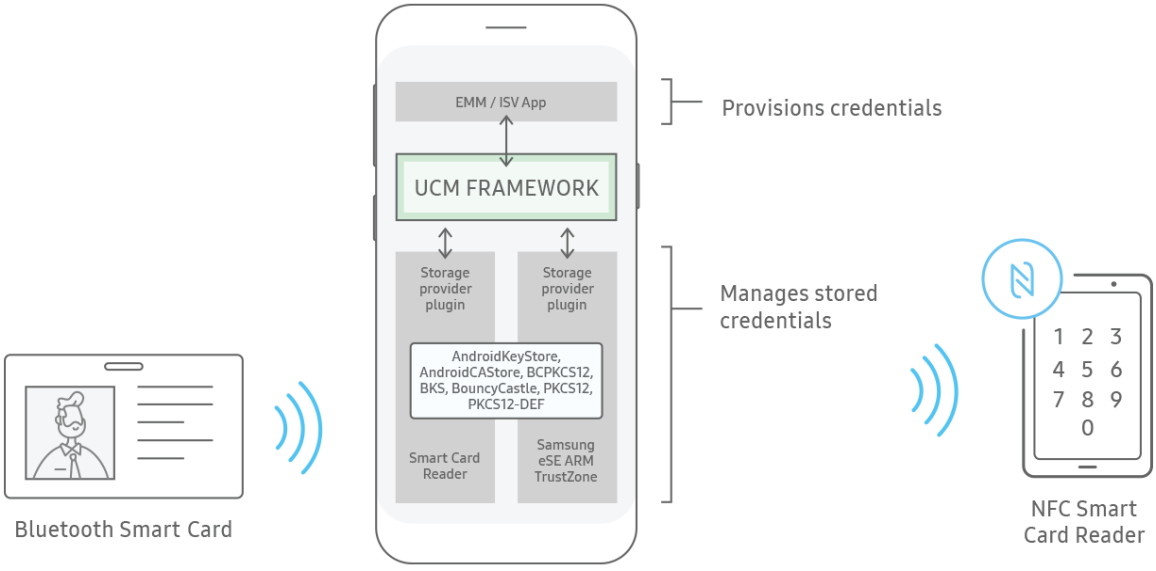
Universal Credential Management (UCM)

Digital credentials are critical mobile security building blocks, leveraging trusted authorities to validate identity and secure private channels across public deployments. Your mobile device credentials provide seamless access to secured Wi-Fi, VPN, email, and websites. Credentials include certificates providing identity and private keys to decrypt sensitive data. These credentials must be securely stored to prevent malicious parties from exploiting your identity and accessing confidential data.

The storage available to you can evolve with the introduction of new technology, and emerging security standards. For example, a mobile device used in a regulated industry may need to obtain personal credentials from a physical Smart Card. In the future, it may need to switch from physical smart cards to virtual ones on an NFC chip. This change process presents a fragmentation problem for credential consuming app developers, since each storage provider has its own proprietary APIs, so adding or switching to new storage hardware introduces new coding cycles, testing, and app re-distribution.

UCM framework

The Knox Platform's Universal Credential Management (UCM) provides a plug-and-play framework for credential management across a variety of different storage media. A significant benefit of the UCM framework is that it uniquely enables storage vendors to develop a plugin, distributed as a standard Android app, that provides access to their storage space and cryptographic operations without forcing app developers to change their code or forcing IT admins or end users to update their apps. The plugin essentially acts as the link between the UCM framework and a specific storage device.



The UCM framework consolidates and standardizes credential services to provide a streamlined interface for:

- **EMM or ISV apps** — These apps configure, provision, and consume credentials, managing credential storage access permissions, and activating advanced UCM permissions. The apps can enforce the installation, removal, or per-app access control of a credential.
- **Storage provider plugin** — These apps are provided by storage vendors to link the UCM framework to their storage solution, to manage stored credentials.
- **Secure storage** — This feature currently includes the Samsung eSE and Smart Card readers described in **"Secure storage options"** on page **30. You can easily support other storage options through additional vendor plugins.**

The Knox SDK provides credential storage vendors a set of UCM APIs to make current and future storage options available on Samsung devices, hiding the implementation details of their solution so that mobile app developers can transparently access stored credentials through standard APIs, such as the Android Keychain. Similarly, developers can use the Java Cryptography Extension APIs to offload cryptographic operations to a capable Smart Card. This abstraction, made possible by the UCM framework, eliminates the need for complex vendor-specific code within mobile apps, meaning enterprise customers have a wide range of existing apps available to them and can easily develop in-house apps without worrying about the underlying storage implementation.

Secure storage options

The UCM framework supports the following secure storage options:

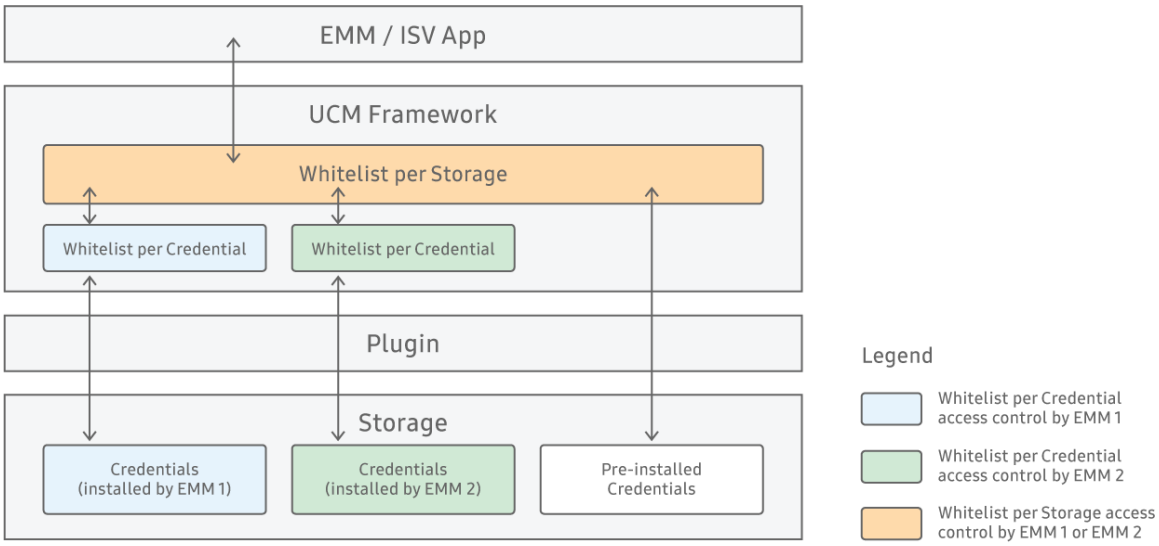
- **Samsung Embedded Secure Element** (eSE) — eSE supports the storing and accessing of credentials, allowing secure storage on the device without additional hardware.
  Note — eSE is not available with the following countries and carriers: USA-Verizon, Korea-All, Japan-All, Canada-Telus.

- **Smart cards** — Smart cards' resiliency makes them ideal for storing credentials if the threat model calls for trust to be shifted outside the device. You can use Smart Cards for unlock actions such as:
  - **Knox Platform's On Device Encryption (ODE)** — You can configure ODE to depend cryptographically on the PIN unlock of a Smart Card inserted in the device, which manages the decryption key for the internal data partition.
  - **Device lockscreen** — You can store the device unlock passcode in a Smart Card.

UCM whitelists

The UCM framework uses two types of whitelists, which uniquely manage access controls for credential storage and offer fully customizable access permissions:

- **App whitelist** — Enforces which apps can access each secure storage type. Every secure storage device maps to its respective UCM plugin, that a secure storage solution provider creates and maintains.
- **Credential whitelist** — Enforces each app's access to credentials, providing app-specific access permissions. By enforcing access control, admins can prevent credential usage by malicious or untrusted apps.



Client Certificate Manager (CCM)

Samsung builds upon the Android Keystore by providing a tamper-proof, detection-based lock-down of cryptographic keys and certificates. This solution supports a variety of high-security use cases important to enterprises, as described in the following sections.

Granular certificate and key access control

The Knox Platform supports an app whitelist for certificates, allowing the certificate installer to define which apps are allowed to perform cryptographic operations based on their certificates. This certificate whitelist process offers better control and flexibility than simply allowing app-only or device-wide access rights to certificates.

Signing with device-specific certificates

A special certificate called the **Device Default Certificate** (DDC) resides within each device. What makes this certificate special is that it is tied to that device's hardware, is signed by the Device Root Key (DRK), and can never leave the device.

Any objects signed by the same DDC are guaranteed to have come from the same Samsung device. There is no way to spoof the identity of a device by reusing a DDC and its key pair on a different device.

Device integrity assurance

Objects signed with this certificate were signed while the device was in good health, meaning when the device was uncompromised. If a device fails its integrity checks—by failing the signature check of the kernel or OS or disabling SE for Android—the following happens:

- A tamper fuse is set; and
- The DDC is rendered permanently unusable.

This lockdown helps attest to the health of the device where the data was signed. After all, you can't trust a signature if the device doing the signing is compromised. The Knox Platform provides a CSR agent that

benefits from this device health attestation claim. A CSR produced and signed by the CSR agent carries implicit device health security claims.

Keystore integration with other features

A keystore is only as useful as the use cases it supports. In addition to manual cryptographic actions—such as sign, verify, encrypt, and decrypt—the Knox Platform provides built-in logic to support sensitive certificate-based actions enterprises often need to secure their solutions such as the following:

- **Certificate Signing Requests** (CSRs) — The ability to complete CSRs with a trusted agent, tied to the Knox Platform's hardware-based Root of Trust, simplifies the secure handling of mobile endpoint requests for digital identity certificates. Instead of sending key pairs and certificates from servers, keys can instead be securely generated on-device and bound to hardware. The public certificate is then included in an appropriate CSR request. Using the CSR agent to validate CSR contents and sign the request avoids trusting sensitive actions to third-party code running in less trusted areas of the device.
- **Certificate Enrollment Protocols** (CEPs) — Similar to CSR, CEP provides built-in agents for logic that enterprises rely on, saving time and enhancing security claims. For more information, see Certificate Enrollment Protocols.

In addition to the DDC, you can generate or install your own certificate and key pairs and specify they are accessible only if the device is in good health. This additional process locks down the keystore in the event of a device integrity failure.

Certificate Enrollment Protocols (CEP)

The Certificate Enrollment Protocols (CEP) provision and support digital certificates for apps within Samsung devices. This feature is of great assistance to EMMs and third-party vendors. Why? Because the CEP helps complete certificate enrollment without device user intervention, further solidifying the claim that Samsung Knox devices provide both world-class security as well as industry-leading manageability.

Enterprises can use CEP to:

- Enroll, renew, or delete certificates
- Check your deployment's certificate enrollment or renewal status

The CEP service is very robust, and supports the following enrollment protocols and standards:

- Simple Certificate Enrollment Protocol (SCEP)
- Certificate Management Protocol (CMP)
- Certificate Management over Cryptographic Message Syntax, Enrollment Over Secure Transport (CMC-EST)

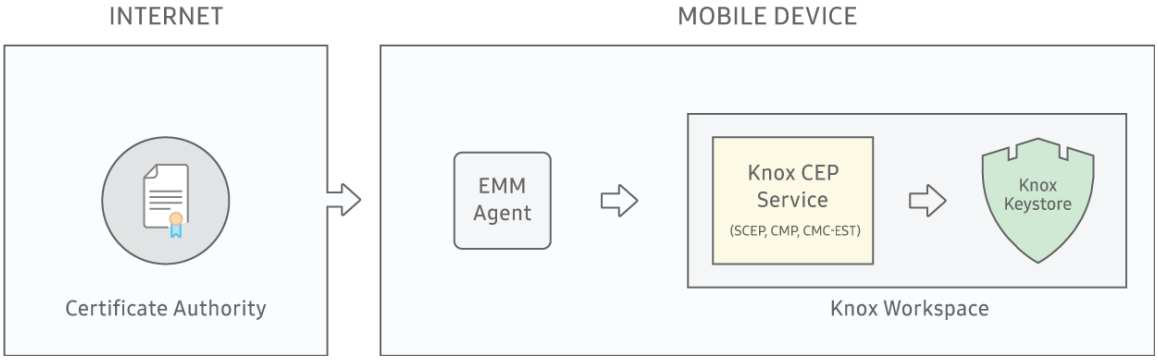
SCEP, CMP, and CMC are frequently used certificate enrollment protocols for provisioning digital certificates. For more information on these protocols, see Internet Engineering Task Force (IETF).

CEP asymmetric key acquisition

Apps use CEP to acquire the public part of an asymmetric key. Asymmetric keys have a public part and a private part. The private part never leaves the Keystore, but the public part is freely distributed. The key owner can use the Keystore to apply the private part of the asymmetric key to an encrypted message to decrypt it.

CEP operational environment

CEP functions within the scope of either the Knox Workspace or personal space, depending on where it is installed. If the deployment objective is to provision and manage certificates for apps inside the Knox Workspace only, then you must install the CEP services within the Knox Workspace as follows:



If the objective is to provision and manage certificates for apps in the personal space, then you can install the CEP services in the personal space to provision and manage certificates.

EMM agents can call the CEP services in either the personal space or Knox Workspace. EMM agents don't have access to a service created outside their scope.

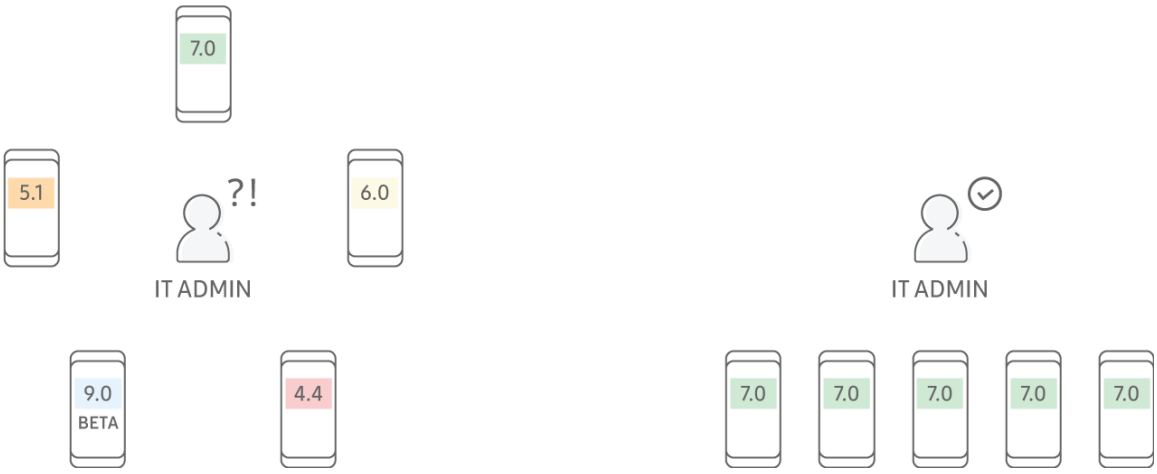
Device Management

Device Software Update Management

Frequent software updates are often necessary to resolve bugs, patch security vulnerabilities, and enhance device capabilities. But IT admins must understand and validate software changes prior to mass deployment. Samsung released the mobile industry's first firmware update management system on Android to enable IT to test and validate software updates and to control roll-out scope and timing.

Why manage device software updates?

In enterprises with fragmented platforms and firmware versions, mobile device deployment and support becomes a time-consuming and tedious task. Proprietary enterprise apps and websites behave inconsistently on different firmware versions, so features require testing and troubleshooting on a widening array of device platforms.



Controlling the rollout of software updates allows IT admins to:

- Homogenize the firmware versions and capabilities of deployed device models.
- Carry out interoperability or compatibility testing with in-house or proprietary servers, apps, and endpoint settings.
- Ensure that known issues are patched before deployment of major firmware version updates.
- Perform field tests of new firmware and software on a subset of devices before mass deployment.
- Force the use of firmware versions that have been validated to meet industry certification or regulation requirements.

Strict control over device firmware updates

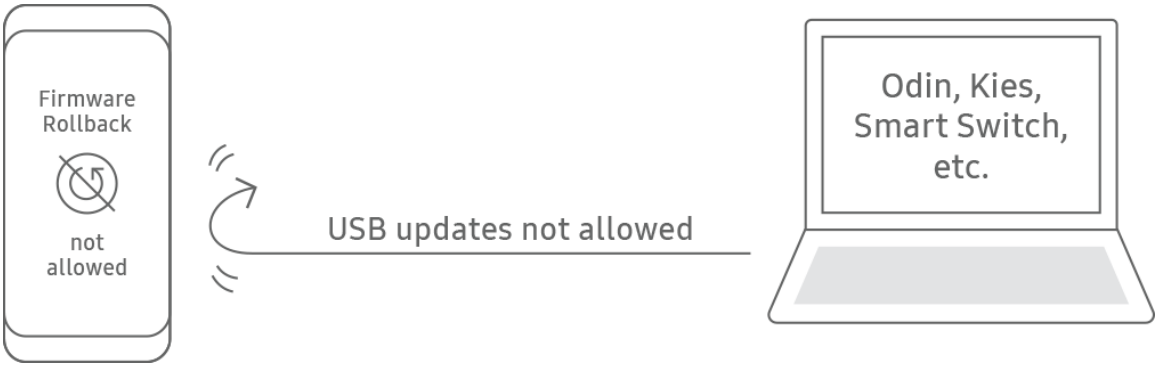
Samsung developed Enterprise Firmware Over-the-Air (E-FOTA) to enable enterprises to save time and support costs, and manage the mobile infrastructure as efficiently as possible.

With E-FOTA, enterprises can control device software updates as follows:

- **Select the highest firmware version allowed on devices** — This option ensures that device users can't independently update to an unsupported firmware version, preventing issues that could negatively impact employee productivity, support costs, and data security.
- **Force the download of a specific firmware version onto select devices** — Enterprises can download new firmware to a few test devices to run interoperability or compatibility tests. This mandatory download is done with proprietary systems and apps to find any corner cases that might result in operational or performance issues.
- **Mass deploy a new firmware version** — Mass deployment prevents software version fragmentation so IT teams don't need to support multiple legacy firmware versions for each deployed device model.
- **Schedule updates during non-peak work times** — This option ensures updates don't interfere with employee productivity.

Knox control over user updates

A wide range of EMM partners support Samsung's firmware management features, integrating firmware management with other asset management activities. IT admins can use these tools to test and deploy software updates in a consistent and low-risk way. Through EMM solutions, enterprises can restrict users from loading unauthorized firmware, through their devices or USB-connected computers.



Through the Knox Platform, enterprises can:

- **Prevent firmware rollback** – This option prevents valid, but out-of-date firmware versions from being maliciously or accidentally installed onto an enterprise's devices. On Samsung Knox devices, a Rollback Prevention fuse encodes the minimum acceptable version of Samsung-approved software. With specific updates, the next set of fuses are burned to indicate the new update is now the minimum version allowed to boot. You can't disable this basic, built-in security feature.
- **Disable automatic firmware updates** – IT admins can prevent users from going to their Android Settings to enable or disable automatic firmware updates.
- **Disable all OTA updates** – IT admins can prevent users from going to their Android Settings to enable or disable software updates in general. This restriction includes updates for firmware, security patches, bug fixes, and apps.
- **Disable USB-connected updates** – IT admins can prevent users from booting into Download Mode and installing a manual software update. This restriction includes updates through the Odin, Kies, and Smart Switch update tools.

Granular Device Management

The Knox Platform's granular device management features are specifically curated, from partner feedback and industry data, to solve some of the most common frustrations enterprises face when mass deploying devices. These unique policies provide device flexibility and customization beyond any other device provider. The policies help organizations manage operations more effectively, secure confidential assets, and reduce administrative overhead. They also solve particular issues regarding industry regulation and compliance. For example, Rich Communication Services (RCS) logging is required by law in the financial industry. Samsung is the only vendor to provide this critical auditing feature.

Custom boot banner

Samsung Knox is the only mobile platform that allows an enterprise to natively change the device boot logo. In many industries, such as government or defense, this change is mandatory for compliance. Through the Knox Platform, enterprise IT admins and developers can customize the following:

- Samsung boot up display
- Splash screen animation, when the device is turned on or off
- Lockscreen image, which can provide an enterprise logo or contact info for lost phones

Enterprises can use these capabilities to mitigate problems such as the following:

- **Phone is lost and found** — Owner information is available by simply powering on the device. There is no need to attempt to unlock the device or call the carrier. The device can be returned to the enterprise quickly.
- **Multiple phones** — Displaying an enterprise logo on bootup lets users know that the device belongs to and is secured by the enterprise. This logo clearly distinguishes it from other devices in the user's possession.

Split billing (Dual APN)

Split billing separates enterprise and personal data usage.

- In Bring Your Own Device (BYOD) deployments, enterprise billing allows employees to be properly compensated for data costs generated from work-related app usage.
- In Corporately Owned, Personally Enabled (COPE) deployments, enterprise billing allows employers to pay for data usage incurred only for work purposes.

Split billing also works with dual SIM devices, by mapping some apps to using the data plan from one SIM, and other apps to the other SIM's data plan.

Remote admin lock of device

This feature allows an IT admin to remotely lock out a device, for example, when the device is out of compliance. Once the device is locked, only an IT admin can unlock it and not a device user. This functionality solves two problems:

- Prevents unauthorized users from accessing the device if it gets lost or stolen.

- Prevents users with valid login credentials from using the device, for example, if the credentials are stolen or the user is no longer allowed to use the device.

With stock Android, an IT admin can lock a device only if it is currently unlocked. If the device is already locked, an admin can't lock it to prevent future unauthorized logins.

Enterprise roaming

Roaming mobile connections can incur unexpected data costs. Multiplied across an enterprise's mobile workforce, these costs can become exorbitant.

Rather than just simply disabling all mobile roaming, the Knox Platform provides more granular controls for enterprises, letting them control which mission-critical apps are allowed to use data during mobile roaming. Enterprises could enable roaming data for:

- All apps in the Knox Workspace
- A single app within the Knox Workspace
- A single app in the personal space

They can also set up Split Billing, with separate roaming policies for the APNs set up for personal and enterprise billing.

Granular policies

Call restrictions

Enterprises can apply granular settings to the caller app, allowing only:

- Emergency calling
- Calling to certain numbers
- A limited number of calls per day

RCS logging

The Knox Platform allows an enterprise to log RCS messages. For many industries, such as financial services, the ability to audit sent and received messages is required by law.

RCS messaging is a new messaging protocol that replaces SMS as the default messaging platform for carriers. It adds much needed features such as group messages and allows users to send more file types. Currently, enterprises that can't capture RCS messages must turn RCS off and lose the benefits of this new protocol. Knox RCS logging capabilities mean deployments can use powerful RCS abilities while staying compliant.

SMS management

Knox provides many advanced SMS policies. Policies frequently used by organizations include:

- Adding an automatic company disclaimer to the bottom of every outgoing text
- Restricting the number of texts per day

- Auditing and recording all incoming and outgoing SMS messages

SD card restrictions

Most vendors don't provide sophisticated options to manage an SD card. Typically, enterprises must choose between one of two options: allow full read and write access to the SD card or completely block it.

The Knox Platform addresses this industry pain point by giving enterprises independent control over read and write access. Knox can:

- Allow read access but block write access
- Allow write access but block read access

This level of control means you can provide one-way data access to sensitive data to effectively meet your security requirements.

Bluetooth restrictions

To mitigate attacks perpetrated through Bluetooth connections, Knox provides these controls:

- **Completely disable Bluetooth** — Turn off Bluetooth and Bluetooth background scanning.
- **Block specific Bluetooth profile types** — Restrict the types of Bluetooth devices that the user can connect to the device, for example:
  - Allow Bluetooth headphones
  - Block Bluetooth file transfers, which could leak private data

USB class restrictions

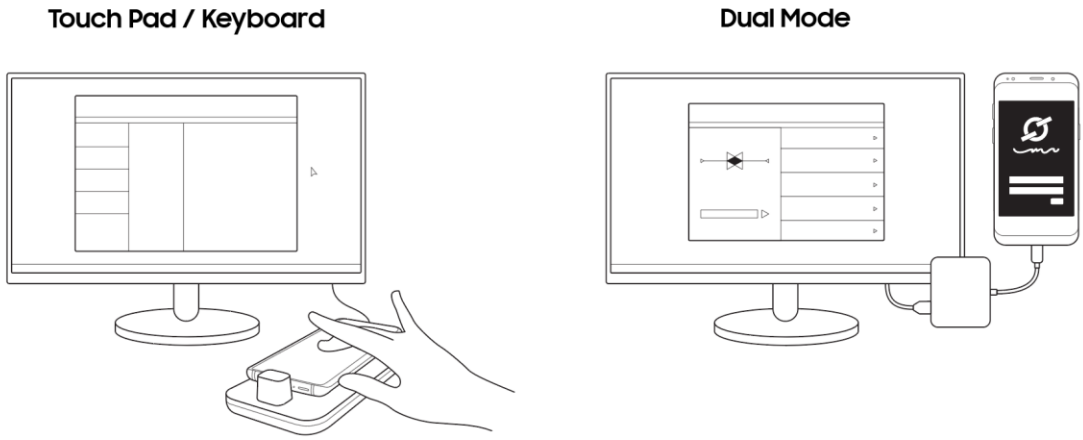
Knox can restrict or allow different types of USB-connected devices, more specifically, the USB device classes defined through usb.org. This feature includes access to the following USB device classes:

- Audio, Video, Audio/Video
- Mass Storage
- Content Security
- Smart Card
- Printer
- Hub, Type-C Bridge, Wireless Controller
- Human Interface Device (HID)
- Communications, CDC Control, CDC Data
- Personal Healthcare
- Billboard
- Diagnostic

For example, you could block all USB devices except Smart Card readers.

Samsung DeX Management

Samsung DeX is a unique product that lets you use your phone as if it were a laptop or desktop computer. You simply connect your phone to a monitor, and optionally use a mouse, keyboard, or S-Pen to launch apps, move objects, type text, write text, or draw images.



DeX supports two different modes:

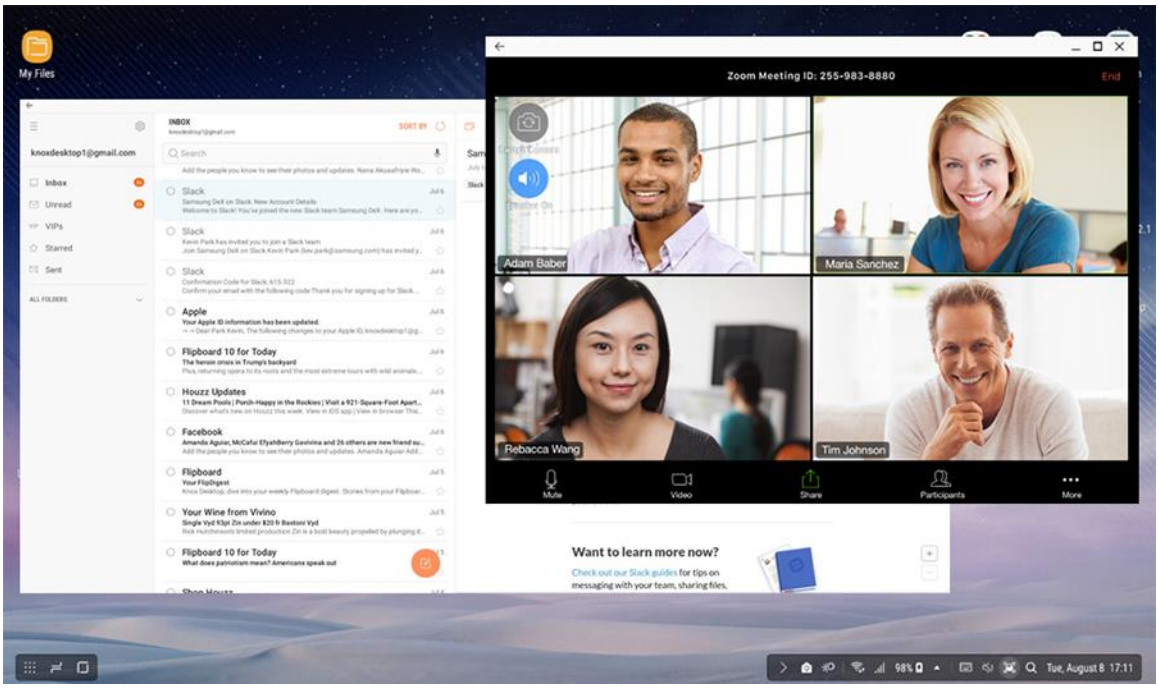
- **Touch Pad/Keyboard** — The phone's screen appears on the connected monitor. You can use the phone's touch pad or a connected keyboard and mouse to enter text and move the cursor on the monitor. Use this mode to read or write documents, participate in video conferences, compose more complex emails, edit images, or develop slide presentations.
- **Dual Mode** — You can use both the phone screen and the monitor at the same time.

You can connect your phone to a monitor and peripherals using one of the following options:

- Samsung DeX docking station
- Samsung DeX docking pad
- USB-C to HDMI adapter

Why use Samsung DeX?

Instead of having to carry both a laptop and phone, you now need only a phone. Through a single portable device, you can quickly write documents, edit spreadsheets, and create presentations on a conventional large screen. There is no need to purchase or carry along a separate laptop. The DeX mode untethers employees from their laptops, and offers enterprises many capital cost savings opportunities.



Using Knox to customize DeX

Enterprises can use the Samsung Knox platform to secure the way Samsung DeX works, allowing them to benefit from the Knox Platform's defense-grade security features without sacrificing the innovation and productivity that comes with DeX.

Using a large screen in DeX mode means that sensitive information may be visible to passersby. As such, you can use the Knox platform to improve security in DeX mode. You can deploy security policies such as:

- Setting a screen timeout while in DeX mode
- Allowing only Ethernet connections, no Wi-Fi or cellular data
- Disabling specific apps in DeX mode, for example, apps displaying confidential data
- Disabling DeX mode

You can also use the Knox Platform to customize the DeX interface. Available customizations include:

- Uploading a company logo to the DeX loading screen
- Adding or removing shortcuts from the DeX launcher

Unique advantages of Samsung DeX

- **Mobile desktop experience** — Enables phone use, on the go, in a desktop environment. A separate laptop is unnecessary. You can access the apps and files necessary directly using your phone.
- **Defense-grade security on a desktop** — Protects users and enterprises with industry-leading security while preserving the productivity enhancements of a desktop environment.

- **Universal app compatibility** — Compatible with the native Samsung and Android apps that are pre-installed on devices. Popular apps such as Microsoft Office apps and Adobe Photoshop Express are also optimized for use with DeX to take advantage of larger, multi-app displays.
- **Customizable** — Mobile app developers can enhance and control their apps while in use with DeX, using DeX APIs from the Knox SDK.

Firewall Management

Most mobile device platforms use built-in firewalls, but don't provide granular control over firewall settings and activity. With the Knox Platform, you can deploy firewall configurations specifically catered to your enterprise security needs.

Why manage and customize device firewalls?

Default firewalls may not provide your organization with the security and data protection it needs. In fact, some firewalls may not even let you see the rules they are enforcing. However, when configuring firewalls with the Samsung Knox Platform, you can know exactly what policies are deployed and take additional measures to secure your enterprise systems.

With the Samsung Knox Platform, you can:

- Restrict and redirect Internet access to specific IP addresses and domains
- Set firewall policies on a per-app or device basis
- Produce logs reporting the blacklisted domains that users accessed

Granular control of Internet access

You can limit the permissible network connections to only trusted addresses, by setting the appropriate Internet access restrictions. The Knox Platform offers a variety of restriction methods, all of which can be used together:

- **IP address filters** — Allow, deny, and redirect access to specific IP addresses. Configure a filter to apply to transmitted data, received data, or both. Allow or deny both IPv4 and IPv6 formatted addresses.
- **Domain name filters** — Allow or deny access to an entire domain or sub-domain.
- **Per-app and device-wide modes** — Give specific apps—for example, ones that handle confidential data—stronger firewalls, and all other apps on a device a more lenient firewall configuration.

Log unsafe URL access

The Knox Platform provides visibility into denied attempts to access blocked domains. The improved visibility helps you to remain aware of potential security breaches or insecure browsing practices within your organization.

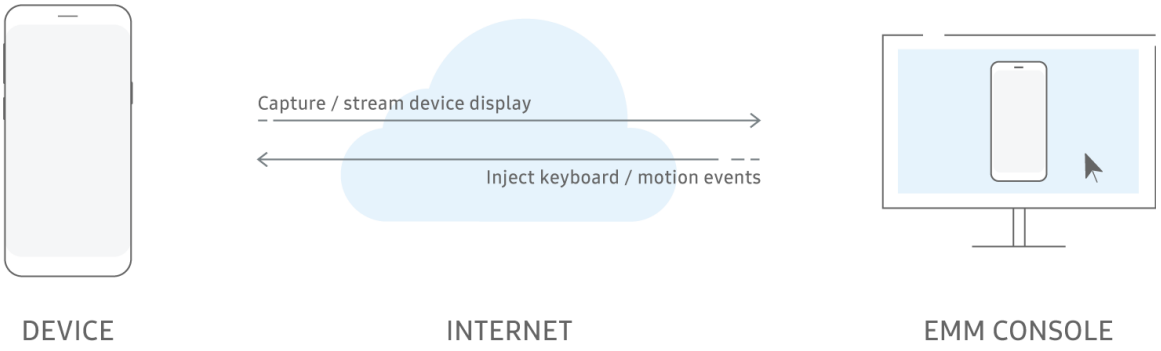
The Knox Platform logs reports with the following information:

- **App name** — The package name of the app attempting to access a blocked domain.

- **Blocked domain URL** — The URL of the domain name blacklisted by your firewall.
- **Timestamp** — The time the incident occurred, to assist with troubleshooting incidents.

Remote Control

With the increasing complexity of problems that IT admins must solve, Knox Remote Control provides IT admins a powerful way to quickly and remotely fix issues. Not only can IT admins have real-time access to what the remote device screen is displaying, but also control it by injecting actions such as finger, keyboard, and mouse events. Although other mobile platforms also offer remote viewing of remote device displays, only Knox provides built-in remote control of devices without requiring third-party solutions.



Here is an example use case: An enterprise employee is on a business trip. On encountering a problem with the company-issued mobile phone, the employee contacts an enterprise IT admin. The IT admin uses an EMM console to remotely view the device screen to observe the issue first hand, then remotely controls the device, through finger, mouse, or keyboard actions. The IT admin directly accesses the environment to remotely debug the issue on the device. The employee is now quickly productive, without the frustrating downtime associated with relaying instructions verbally or through email.

The continuous polling of the device screens doesn't impact device performance as devices send only screen changes.

Unique advantages of Knox Remote Control

The Knox Platform provides built-in remote control without requiring third-party solutions. For enterprises, this control:

- **Saves time** by enabling IT admins to troubleshoot remote mobile device issues in real-time and utilize high performance screen sharing.
- **Reduces employee down-time** and **optimizes employee productivity** through quick problem resolution.
- **Enables monitoring** of devices for corporate policy violations along with corrective actions on the devices, as well as an ability to monitor only for screen changes.

Audit Log

Organizations that need to troubleshoot serious security breaches rely on audit logs for a forensic analysis of the activities leading up to actual and potential breaches. In regulated industries, these audit trails are a mandated requirement to comply with security audits.

With the Knox platform, an enterprise IT admin can use an EMM console to enable audit logging on all corporate devices. IT admins can proactively pull audit logs from time to time, to detect and defend against malware or viruses at the earliest onset. In the event of a possible intrusion, IT admins can parse the logged events for unauthorized activities.

The Knox platform Audit Log provides comprehensive information about device events, including:

- Knox Workspace container activities
- Password policies set for devices and containers
- App installation and removal
- Certificate failure and key generation
- Account creation and removal
- File exchange attempts over Wi-Fi

To help better manage device storage, IT admins can control the Audit Log size.

The benefits to an enterprise include:

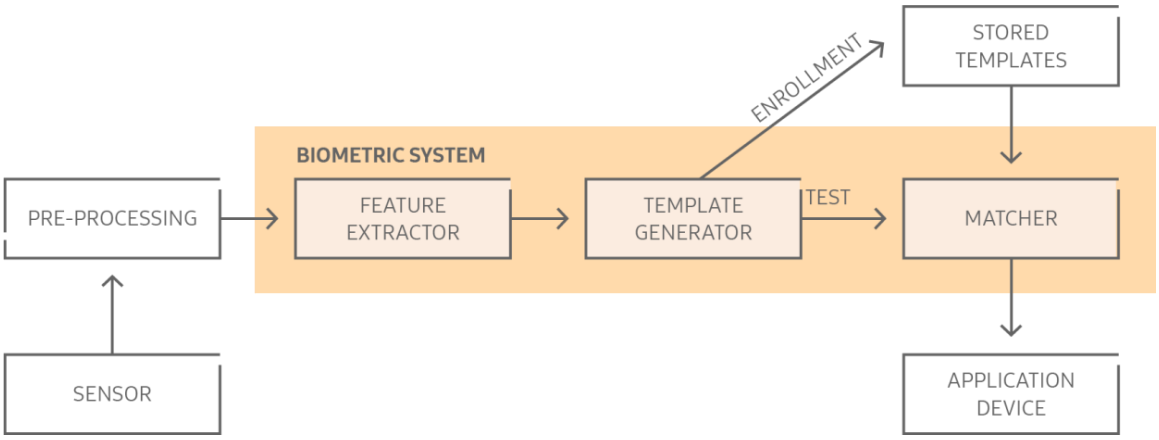
- Early detection and defense against malware and viruses.
- Empowering IT admins with powerful troubleshooting data.
- Adherence to mandated requirements in regulated industries.
- Compliance with the Mobile Device Fundamentals Protection Profile (MDFPP) 2.0 requirements to collect events.

User Authentication

Biometric authentication

Traditional user authentication relies on things you know or have, like a password or ID card. These are susceptible to human mistakes, phishing, and duplication. Biometric authentication validates a personal trait, for example: fingerprints, irises, or facial features. Biometrics can lower the false acceptance rate (FAR). Users can use biometrics to unlock devices and app containers. Through Samsung Pass, users can also use biometrics to log into apps and websites.

Advantages of Knox Biometrics



The Knox Platform provides the following in addition to standard Android capabilities:

- **Secure storage** — On Samsung devices, the authentication software doesn't share or distribute the biometric measurements of any user. The measurements are stored in a format that can't be used to reproduce the original biometric, and can only be accessed and decoded within the specific part of the TrustZone that has access to the biometric hardware. Biometrics are used only on the correct device and by the correct user. This functionality means there is a lower chance of someone spoofing biometrics credentials to access a device.
- **Enforced two-factor authentication** (2FA) — The Knox Platform provides IT admins the option to enforce two-factor authentication with biometrics for the Knox Workspace. For example, a user can be required to authenticate with an iris scan in addition to a standard device unlock method (password, PIN, pattern). While Android provides some combinations of two-factor authentication, the Knox Platform allows you to take your security one step further with biometric integration.
- **Samsung Pass integration** — Apps can use Samsung Pass APIs to enforce biometric authentication in place of a traditional login and password. This authentication method can save an organization a large amount of password management overhead, while further increasing device security. Samsung Pass features the ability to:
    - Support Fast IDentification Online (FIDO) authentication
    - Register and deregister a user's biometrics
    - Respond to remote wipe requests
    - Manage authentication transactions

    - Work in the Secure World of the TrustZone
- **Enterprise credentials override** — As required by enterprise policy, Knox devices allow you to enforce the use of enterprise AD credentials to unlock a device or Knox Workspace container. This setting overrides any biometrics set by the user, and forces them to use their enterprise credentials.

App and Data Protection

Enterprise Productivity Apps

Mobile apps have changed the way we work by providing new channels of communication, innovating customer engagement, and empowering organizations with critical data in real-time. Samsung Knox devices include a set of productivity apps for both personal and business use.

Business-critical apps include Samsung Email, Internet browser, Calendar, and Contacts. Enterprise IT admins can secure these apps within the Knox Workspace, along with other apps used by the enterprise.

The Knox Platform secures enterprise apps and protects confidential app data through these methods:

- **App installations and updates** — Apps are pre-installed within the mobile device's secure Knox Workspace and users can update these apps independent of firmware updates through Google Play.
- **App isolation** — Apps are sandboxed within the Knox Workspace, which uses SE for Android to prevent personal apps from interfering with the business apps that are in the Knox Workspace.
- **App permissions** — Knox provides App Permission Monitoring to help users prevent malware from using powerful permissions to gain unauthorized access to the device and Knox Workspace.
- **Data-At-Rest** — Through Knox's Sensitive Data Protection (SDP), the files and data used by an app can remain encrypted until device users authenticate at device unlock or Knox Workspace login. Individual apps can further deploy an app-specific password as another line of defense.
- **Data-In-Transit** — App data sent through the public Internet can be secured using Knox's advanced VPN features.
- **DeX integration** — Not only are all Samsung native apps optimized to work within DeX, enterprises can secure apps while they're displayed in DeX.

Samsung Email

The Samsung Email app is uniquely designed for customers requiring the secure synchronization of their mobile device's Email calendar, tasks, and memo functions. The Email app can use MS Exchange ActiveSync (EAS) for Single Sign On using company credentials.

In contrast with third-party security solutions, the Samsung Email app uses Sensitive Data Protection (SDP) by default, to automatically:

- Protect email text and attachments
- Secure incoming emails and notifications in real time

The Samsung Email app provides these key benefits:

- Productivity
    - Single Sign On (SSO) with EAS
    - EAS synchronization of contacts, calendar, tasks, and note data
    - Federated LDAP query support
- Security
    - EAS certification for account
    - EAS certification for S/MIME messages
    - EAS certification revocation checks
    - EAS certification history support
    - Card certification support
- Management
    - LDAP account management
    - EAS account management

Samsung Internet Browser

The Samsung Internet Browser provides enterprises with the following security features:

- **Biometric Authentication** — IT admins can enforce biometric authentication for website logins, web payments, and accessing Secret Mode.
- **Secret Mode Password** — IT admins can enforce password access to Secret Mode, which can contain confidential bookmarks and saved pages.
- **Protected Browsing** — IT admins can enable warnings to alert users if they try to view known malicious sites, which might try to steal confidential data such as passwords or credit card information.
- **Content Blockers** — IT admins can allow the use of third-party plugins to filter out content such as:
    - ads, which can come with cookies, malware, or viruses
    - invisible trackers, which can monitor online activity

Enterprises can take advantage of the following additional capabilities to secure mobile browsing:

- Set up an HTTP proxy
- Enable TLS encryption of browser traffic
- Filter URLs or domains
- Block pop-ups through extensions
- Disable or enable JavaScript
- Disable or enable the auto-fill of forms
- Disable or enable cookies, saved sign-in data
- Delete or preserve personal data

Samsung Contacts

Contacts are the lifeline of any collaborative business environment and empower mobile workers to stay connected. Enterprises need to strike a fine balance between providing employees with easy access to contacts and protecting private contact information from exploitation.

The Samsung Contacts app provides enterprises with the ability to disable or enable the following features:

- Synchronization of contact data with an MS Exchange or ActiveSync server
- Synchronization of contact data inside and outside the Knox Workspace container
- Copying of contact info to a SIM card
- Accessing contact info at the end of a phone call

Advanced App Management

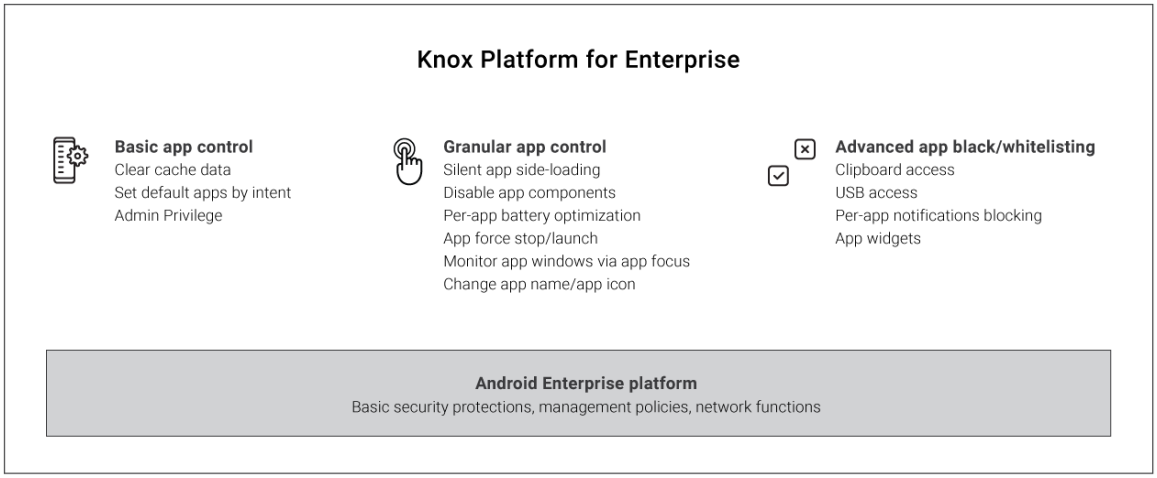
Enterprises need a strong Mobile Application Management (MAM) strategy to deploy apps effectively, manage app licenses, secure apps, optimize app usage, and handle app data safely. The Knox platform provides comprehensive app management capabilities that allow IT admins to control all aspects of apps installed on a device. These capabilities can also be extended inside the secure Knox Workspace to provide a safe haven for sensitive apps and data.

Enterprises use EMM solutions to centrally configure and remotely manage apps. Knox provides a full complement of management functions, providing IT admins with the ability to:

- Install, uninstall, update, enable, disable, start, stop, or wipe data for an app
- Whitelist or blacklist the following:
    - apps that can be installed
    - apps that can auto-update
    - apps that can use the Clipboard
    - apps that can be started and stopped by users
    - apps that can access the USB port
    - app accounts, permissions, and notifications
- Disable or enable other apps like Google Play, Google Chrome, Voice Dialer, and YouTube
- Get info like the app code size, cache size, data size, total size, notification mode, and restrictions
- Get statistics like app launch count, component state, app focus state, CPU usage, data size, memory usage, and network stats

Unique advantages of Knox App Management

What sets the Knox platform apart from other mobile platforms are the advanced app management features not found in other solutions, providing additional advantages that enable enterprises to be fully efficient and productive.



App control

- **Clear cache data** — Remove cache memory for an individual or list of apps to help optimize space and have complete control over your data.
- **Set default apps by intent** — Set an app as the primary app for a given task. For example, ensure your solution only uses a certain Internet browser or force your SMS service to comply with your strict company policies.
- **Admin privilege** — An admin can prevent the activation of another admin's app, unless the app is part of the whitelisted apps.

Advanced app black and whitelisting

- **Clipboard access** — Prevent access to the native Android clipboard within an app. If an app tries to use the clipboard, the content is deleted.
- **USB access** — Prevent user permission for one or more USB devices to be used by an app.
- **Per-app notifications blocking** — Prevent status bar notifications for an app and choose to block either text, sound, or both.
- **App widgets** — Allow only approved widget packages into your Knox Workspace container, and view them in launcher mode on a Samsung device.

Granular app control

- **Silent app side loading** — Silently install any app without user interaction or permission.
- **Disable app components** — Enable or disable a specific package component such as the activity, receiver, service, or provider class.
- **Battery optimization** — Whitelist apps from Google's Doze mode, app standby or power saving mode.
- **App force stop and launch** — Force stop any app including background processes and system apps.
- **App focus** — Monitor any app and receive a notification if a user leaves the window of a whitelisted app.
- **Change app name or app icon** — Change an app's package name and icon.

DualDAR Encryption

Protecting Data-At-Rest (DAR) on mobile devices is a major concern for security conscious enterprises. The Samsung Knox Sensitive Data Protection (SDP) already addresses this issue, by decrypting data only after user authentication, providing per-file and per-data decryption keys, offering per-app password checks, and meeting MDFPP requirements for US government and military use.

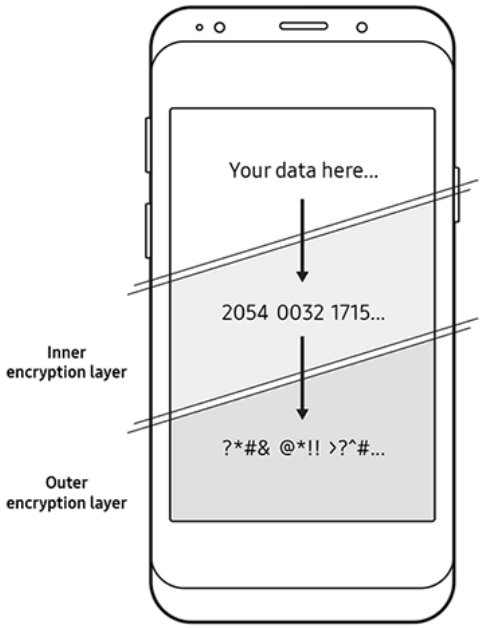
Knox DualDAR adds two separate layers of encryption, further meeting the requirements of classified deployments. Knox DualDAR secures all Workspace data on devices with two distinct levels of encryption. The solution also protects data by restricting apps from writing or saving data to the unencrypted space on the device. As the name implies, Knox DualDAR is based on two layers of data encryption. To fully understand how DualDAR works, we need to examine how the two layers of encryption within DualDAR work.

The DualDAR solution provides the following two separate layers of encryption and key generation. All data placed inside the Workspace is dually encrypted by both layers. Currently, DualDAR only secures data placed inside the Workspace or designated Work profile.

- **Outer layer**: The outer layer of the DualDAR solution is built on top of Android's FBE and enhanced by Samsung to meet MDFPP requirements. This layer is implemented through the SoC dedicated to flash storage encryption. In this context, the SoC could be Qualcomm Integrated Crypto Engine (ICE) or Exynos Flash Memory Protector (FMP). Data encryption at this layer is AES 256 XTS and file encryption keys are encrypted using AES-GCM 256.
- **Inner layer**: The inner layer of encryption is based on a framework that allows an independent third party to install a separate cryptographic module. If no third party module is installed, an separate inner layer of encryption is secured by a FIPS 140-2 certified cryptographic module included with the Samsung Knox framework.

DualDAR is supported on all devices with Knox version 3.3 or later and compatible with Android FBE. For more information on finding your Knox version, see the Prerequisite section on the DualDAR UEM integration page.

How DualDAR encryption works



DualDAR's inner and outer security layers are independent and protect all information stored in the Workspace when the device is in a powered off or unauthenticated state. Samsung Knox DualDAR leverages Android File Based Encryption (FBE) architecture.

On a FBE-enabled device, every device has the following two storage locations available to an app.

- **Credential Encrypted (CE) storage**: Default storage location and only available after a user has unlocked the device.
- **Device Encrypted (DE) storage**: Storage location available both during Direct Boot mode and after the user has unlocked the device.

From an app point of view, the DualDAR Workspace functions as CE storage. The Knox framework prevents apps from writing data to non-DualDAR protected DE storage. In some cases an app is aware of both CE and DE storage, and needs to write unclassified content to DE storage. In such cases, IT admins can whitelist that app to write to DE storage. This strict whitelist process ensures that no app can write sensitive or classified content to DE storage without explicit IT admin approval.

When the Workspace container is configured for DualDAR, the secured data is available as follows.

1. On a device that supports and is configured for DualDAR, access to app data inside the container is only available when the container is unlocked, that is when the user is actively using the container.
2. When the container—or device as a whole—is locked, the container encryption keys are evicted from memory.
3. In a data lock state, the Samsung device remains powered on but the user is locked out of both the Workspace and device. All sensitive data is protected in Credential Encrypted (CE) storage within the Workspace. CE storage is not available until the user provides both their device and Workspace credentials.

Unique advantages of Knox DualDAR

DualDAR encryption has the following significant advantages over traditional single layer encryption methods.

- **Mitigate risks of implementation flaws**: DualDAR reduces the likelihood of unauthorized data access by mitigating the risks that arise from vulnerabilities in a single encryption layer. While one of the many methods available for unauthorized data access may crack through a single layer of encryption, the chances are very low that such vulnerabilities are available on both layers of encryption.
- **Mitigate risks of password configuration flaws**: Both layers of encryption on a DualDAR configured device use separate and distinct authentication methods to allow access. This separation of authentication methods reduces the likelihood that a single misplaced or misconfigured password is exploited on both layers of data encryption at the same time. Two layers of encryption and two methods of authentication ensure that encrypted data remains protected even in the event of breach on one layer.
- **Provide access using strict security evaluation criteria**: DualDAR meets the standards laid out in the FIPS 140 certification requirements. Both the inner and outer layers use FIPS 140 certified cryptographic modules. GCM is used to encrypt the key while data is encrypted using XTS or CBC.
- **Ease of deployment**: DualDAR leverages the in-built Android FBE framework and builds additional layers of security on top of this framework. This solution is available on devices that use a Knox Workspace in PO mode as well as fully managed devices that include a PO mode. For more information on configuring this solution for your supported device, see the DualDAR architecture page.
- **Customize the second layer of encryption**: DualDAR allows IT admins to implement third party encryption solutions at the inner layer of encryption. This freedom of implementation means IT admins can use and configure any third party cryptographic modules, including solutions that meet FIPS 140 certification criteria.
- **Flexible deployment methods**: IT admins can implement and configure DualDAR on all kinds of devices, including BYOD and company-issued devices. Whether the device uses a Knox Workspace in PO mode or is a fully managed device that includes a PO mode, DualDAR is compatible with both models. This flexibility means IT admins can use this superior data security solution on a wide variety of devices within their enterprise.

For more information on DualDAR and its unique design, see DualDAR architecture.

Appendix

Knox Certifications

The Knox Platform has successfully met the rigorous security requirements set by governments and major enterprises around the world, providing organizations with a trusted mobile security solution. The certifications acquired by the Knox Platform allow its mobile devices to be deployed in highly sensitive industries such as the military.

Samsung Knox continuously adds to its growing list of certifications for industries and agencies around the world. For more information on certifications and to review the latest list, see Knox certifications.

Unlike other mobile platforms, the Knox Platform is certified to have met the following countries' security requirements.

	USA	UK		Germany		France	Spain	Finland	Netherlands
	MDFPP	EUD	CPA	Endorsement	VS-NfD	CSPN	CCN	TRAFICOM	NCSA
Samsung	✔	✔	✔	✔	✔ pre-approved	✔	✔	✔	✔

Methodology

Certifications are granted by independent boards that use a specific set of hardware and software, for example, one certificate might be granted for the Galaxy S8 running Knox 3.0. These certifications must be renewed with each device and OS iteration to remain valid. Samsung remains dedicated to maintaining industry compliance and continues to grow and maintain our numerous certifications.

Security principles

Many of these certifications have a set of security principals that a device must uphold. Here are some examples of the security principles validated during certification.

- **Data-in-transit protection** — Does the device sufficiently protect data-in-transit?
  Yes - achieved with Advanced VPNs, Certificate Management, and Common Criteria mode.
- **Data-at-rest protection** — Does the device provide data that is encrypted by default? Is that data encrypted when the device is locked?
  Yes - achieved with the Knox Workspace and Sensitive Data Protection.
- **Authentication** — Does the device provide secure authentication methods?
  Yes - achieved with the Client Certificate Manager and user authentication methods that include biometrics.
- **Secure boot** — Does the device have mechanisms to ensure the boot up process is free from modification?
  Yes - achieved with a hardware-backed Root of Trust and Trusted Boot.
- **Platform integrity** — Does the device ensure the integrity of the platform? Can it query the integrity of the platform?
  Yes - achieved with the Real-Time Kernel Protection, Device Health Attestation, and Secure lockdown on tampering.
- **App sandboxing** — Does the device provide app sandboxing?
  Yes - achieved with through the Knox Workspace and SEAMS.
- **App Whitelisting** — Does the device allow app whitelisting and blacklisting?
  Yes - achieved with Advanced App Management.
- **Security policy enforcement** — Does the device allow the enforcement of security policies? Can they take precedence over user activities?
  Yes - achieved with a full complement of EMM policies built on a Knox SDK offering over 1500 APIs.
- **External interface protection** — Does the device allow control over external peripherals such as Bluetooth, USB, and NFC?
  Yes - achieved with Granular Device Management.
- **Device Update Policy** — Can the device provide deliberate OS updates that match an organizations evolving needs?
  Yes - achieved with Device Software Update Management.
- **Event collection for enterprise analysis** — Does the device allow the collection, and subsequent audit, of business data?
  Yes - achieved with Audit Logs.
- **Incident Response** — Can the device be managed if it is lost, stolen or damaged?
  Yes - achieved with custom lockscreen info, remote data wipe, auto-wipe after a number of unsuccessful log-in attempts, and remote factory reset.

What does this mean to you? You can rest easy knowing that Samsung Knox's holistic security platform is compliant with the highest security requirements and standards. Samsung Knox devices are built from the ground up to secure your organization's apps and data, providing robust integration with existing IT infrastructure and ensuring there are no functional or security gaps in your deployment.

Common Criteria Mode

Knox supports advanced device configurations tailored to the defense industry. A single Knox setting can apply many of the settings needed to put the device into a compliant state. This setting, called Common Criteria Mode or CC Mode, helps simplify the task of correctly configuring a device for deployments that must meet defense-grade security requirements. The Common Criteria for Information Technology Security Evaluation, commonly referred to as Common Criteria, is an internationally-recognized standard for defining security objectives of information technology products and for evaluating vendor compliance with these objectives. A number of Governments use Common Criteria as the basis for their own certification schemes.

Select Samsung Galaxy devices with the Knox Platform embedded received Common Criteria (CC) certification. The current CC certification targets the new Mobile Device Fundamentals Protection Profile (MDFPP) of the National Information Assurance Partnership (NIAP), which addresses the security requirements of mobile devices for use in enterprise. Samsung Knox is approved by the United States Government as the first NIAP-validated consumer mobile devices to handle the full range of classified information.

An IT admin can enable the device to be placed into the Common Criteria configuration. When enabled, the device:

- Blocks bootloader download mode, the manual method for software updates
- Mandates additional key zeroization on key deletion
- Prevents non-authenticated Bluetooth connections
- Requires that FOTA updates have a 2048-bit RSA-PSS signature
- Uses many other security settings

While other optional configuration steps are still recommended on top of Common Criteria Mode, the value is clear: simplifying the correct configuration of endpoints for high-security deployments saves time and prevents mistakes that can lead to misconfigurations and added security risks.

More information

Refer to the following Knowledge Base Articles for details about:

- Common Criteria Mode, supported Samsung devices, and test APKs
- Common Criteria evaluation, by Android version