

Exhibit A

U.S. Patent No. 10,028,144 (“144 Patent”)

Accused Devices: Samsung’s mobile electronic devices, and all versions and variations thereof since the issuance of the asserted patent. As a specific example, Headwater identifies and provides a claim-by-claim chart below identifying citations to evidence demonstrating that the Samsung Galaxy S24 infringes Headwater’s Asserted Patent. The Samsung Galaxy S24 is representative of other Samsung devices (e.g., phones and tablets) comprising Android software (e.g., Android OS, Android Enterprise, etc.) or Knox software because there are insubstantial differences between how the accused Samsung devices infringe the claims of the Asserted Patent, including because the accused Samsung devices include the same features, e.g., Android’s Work Profiles and per-app VPN and/or Knox’s “Separated Apps,” “App Isolation,” and VPN policies.

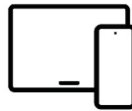
Claim 1

Issued Claim(s)	Public Documentation
1[pre]. A wireless end-user device, comprising:	Samsung’s devices comprise a “wireless end-user device.” <i>See, e.g.,</i> As another example, Samsung’s devices run the Android Operating System, including Android Enterprise, which are each “a wireless end-user device.” <i>See, e.g.,</i> https://www.samsung.com/uk/support/mobile-devices/how-can-i-check-what-version-of-android-i-have-on-my-device/; https://www.android.com/enterprise/; https://androidenterprisepartners.withgoogle.com/devices/#. As a further example, Samsung’s devices operating in the Samsung Knox ecosystem are each “a wireless end-user device.” <i>See, e.g.,</i> https://www.samsung.com/us/business/solutions/services/mobility-software/knox-manage/:



Event-based policies

Manage devices based on pre-defined events—for instance, blocking access to cameras on employee phones during work hours.



Kiosk mode

Built-in tools help you set up devices in kiosk mode with no additional development work.



Works with Android Enterprise

Knox Manage lets you leverage Android Enterprise fully managed and work profile modes.

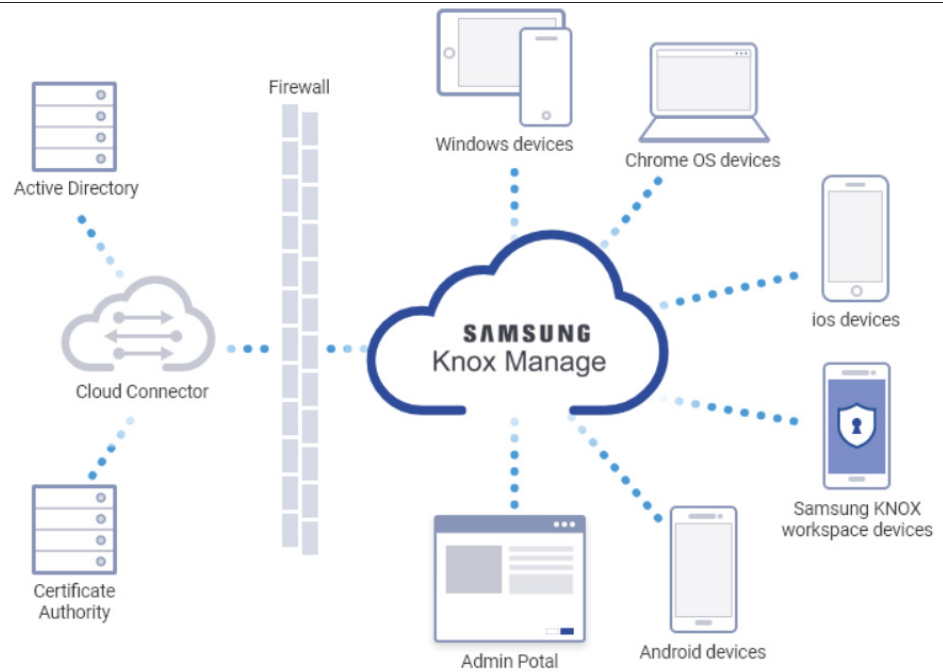
Optimized for Samsung

Knox Manage is a cross-platform EMM that works with other Android, iOS, Windows 10 and Google Chrome devices, but offers the most comprehensive controls for Samsung Galaxy devices, including full support of [Knox Platform for Enterprise](#), [Knox Mobile Enrollment](#) and [Knox E-FOTA](#).



SAMSUNG





<https://docs.samsungknox.com/admin/knox-manage/welcome.htm>;
<https://www.samsungknox.com/en/knox-platform/supported-devices>;

SAMSUNG KnoxAbout KnoxSolutionsProductsSupportBlogFor PartnersContact SalesSign InGET STARTED

Home / Secured by Knox / Devices secured by Knox

Devices Secured by Knox

Find which devices are Secured by Knox and which Knox solutions and features are supported.*

*Available features and device compatibility may vary depending on your region and/or OS platform. Contact your local Samsung sales team for details.

FILTER454 Result(s)RESET FILTERS

Last updated: July 11, 2024

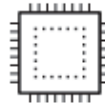
KNOX SOLUTIONS	DEVICE	MODEL CODE	PLATFORM/OS	KNOX VERSION	ANDROID ENTERPRISE RECOMMENDED
Knox Suite ☐ Knox Platform for Enterprise ☐ Knox Mobile Enrollment ☐ Knox Manage ☐ Knox E-FOTA ☐ Knox Asset Intelligence ☐ Knox Capture ☐ Knox Authentication Manager ☐ Knox Configure ☐ Knox Guard	Galaxy A04s	SM-A047M, SM-A047F	Android - Secured by Knox	3.10	
	Galaxy A13	SM-A137F, SM-A135N, SM-A135M, SM-A135F, SM-A135U1, SM-A135U	Android - Secured by Knox	3.10	
	Galaxy A13 5G	SM-A136M, SM-A136B, SM-A136S	Android - Secured by Knox	3.10	
	Galaxy A14	SM-A145MB, SM-A145FB	Android - Secured by Knox	3.10	
	Galaxy A15	SM-A155F, SM-A155M, SM-A155N	Android - Secured by Knox	3.10	Learn more
	Galaxy A15 5G	SM-A1560, SM-A156E, SM-A156M, SM-S156V, SM-A156U, SM-A156W, SM-A156U1, SM-A156B, SM-A156L	Android - Secured by Knox	3.10	Learn more
OTHERS ☐ Knox Deployment App ☐ Knox DualDAR	Galaxy A23	SM-A235F, SM-A235M, SM-A235N	Android - Secured by Knox	3.10	
	Galaxy A23 5G	SM-A2360, SM-A236B, SM-A236M, SM-A236E, SM-A236V, SM-A236U1, SM-A236U2, SM-A236U3, SM-A236U4	Android - Secured by Knox	3.10	Learn more

https://kp4-cdn.samsungknox.com/resource/Leaflet_Knox%20Configure_web_mRxH.pdf;
<https://www.samsungknox.com/en/solutions/it-solutions/knox-configure>;

	SAMSUNG Knox About Knox Solutions ▾ Products ▾ Support ▾ Blog For Partners Contact Sales ▾ Sign In ▾ GET STARTED Which platforms, operating systems, and devices does Knox Configure support? Which specific versions does it support? Knox Configure is supported on Samsung devices running Knox versions 3.0 and higher, and running Android 8 and higher. Each Knox solution, including Knox Configure, supports the five most recent major Android versions. That is, the most recent version plus the four previous versions.
[1a] a wireless wide area network (WWAN) modem to receive and transmit Internet data between the device and at least one WWAN when configured for and connected to the at least one WWAN; and	The Accused Devices comprise “a wireless wide area network (WWAN) modem to receive and transmit Internet data between the device and at least one WWAN when configured for and connected to the at least one WWAN.” <i>See, e.g.,</i> https://www.samsung.com/us/smartphones/galaxy-s24/compare/?device-1=samsung-galaxy-s24-ultra&device-2=samsung-galaxy-s24%2B&device-3=samsung-galaxy-s24:

	Cellular & Wireless  5G^{3 8} (sub6, mmW).
[1b] one or more processors configured to execute one or more processes in a kernel execution partition, one or more processes in an application execution partition, and one or more processes in a protected execution partition,	The Accused Devices comprise “one or more processors configured to execute one or more processes in a kernel execution partition, one or more processes in an application execution partition, and one or more processes in a protected execution partition.” For example, each Accused Device comprises one or more processors. <i>See, e.g.,</i> https://www.samsung.com/us/smartphones/galaxy-s24/compare/?device-1=samsung-galaxy-s24-ultra&device-2=samsung-galaxy-s24%2B&device-3=samsung-galaxy-s24:

Processor



Snapdragon 8 Gen 3 Mobile Platform for Galaxy

As another example, Samsung's devices run the Android Operating System, Android Enterprise, and/or Knox, which execute processes in a kernel execution partition, an application execution partition, and/or a protected execution partition. *See, e.g.,*

<https://www.samsung.com/uk/support/mobile-devices/how-can-i-check-what-version-of-android-i-have-on-my-device/>; <https://www.android.com/enterprise/>;

<https://developer.android.com/work/managed-profiles>;

<https://support.google.com/work/android/answer/9213914?hl=en&sjid=8659651805175691014-NC#zippy=%2Callowed-apps%2Cdisallowed-apps%2Cgoogle-play-traffic>;

<https://www.samsung.com/us/business/solutions/samsung-knox/>;

Advanced mobile security for Android

The Knox mobile security solution protects applications and data by strictly defining what each process is allowed to do and which data it can access. This allows Knox security to separate, encrypt and protect enterprise data within a managed container.

Real-time kernel protection integrity measurement architecture

Periodic Kernel Measurement and Real-time Kernel Protection work to constantly inspect the core software of the OS, the kernel. These checks ensure that requests to bypass device security are blocked and sensitive data is protected.

TrustZone

The Knox enterprise security solution leverages a processor architecture known as TrustZone, in which highly sensitive computations are isolated from the rest of the device's operations, protecting enterprise data.

Secure / trusted boot and hardware root of trust

To prevent security measures from being bypassed or compromised, Knox uses Boot-time Protections backed by Hardware Root of Trust to verify integrity of the device during the boot process.



Knox security philosophy

Build Trust Maintain trust Prove trust Make ready

Chipset

The Knox platform ensures only approved versions of system-critical software are loaded. The platform is built-in and the trust starts in the hardware, with unique certificates burnt into the chipset of each device.

Knox warranty fuse

With these unique certificates, the Knox mobile security platform can verify each piece of software that loads. If verification fails, Knox either records the tampering by flipping a one-time fuse called the Knox Warranty Bit, or prevents further booting. Devices with compromised Knox Warranty Bits cannot use certain Knox features or services, such as Knox Workspace or Samsung Pay.

Rollback prevention

Rollback prevention ensures that a Samsung device is not downgraded to an earlier, vulnerable software version.

; <https://docs.samsungknox.com/admin/fundamentals/whitepaper/samsung-knox-for-android/core-platform-security/root-of-trust/>;

Secure hardware

The Knox Platform trusted environment leverages the following hardware components.

- **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.
- **ARM TrustZone Secure world** — The Secure world is the environment in which 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.
- **Knox Vault** — The Knox Vault is an independent, tamper-proof, secure subsystem with its own processor, memory, and an interface to dedicated non-volatile storage. The Knox Vault stores sensitive data such as cryptographic keys and authentication data. Even if the main application processor that runs Android is compromised, the Knox Vault protects secrets and guards against hardware attacks such as probing and fault injection.

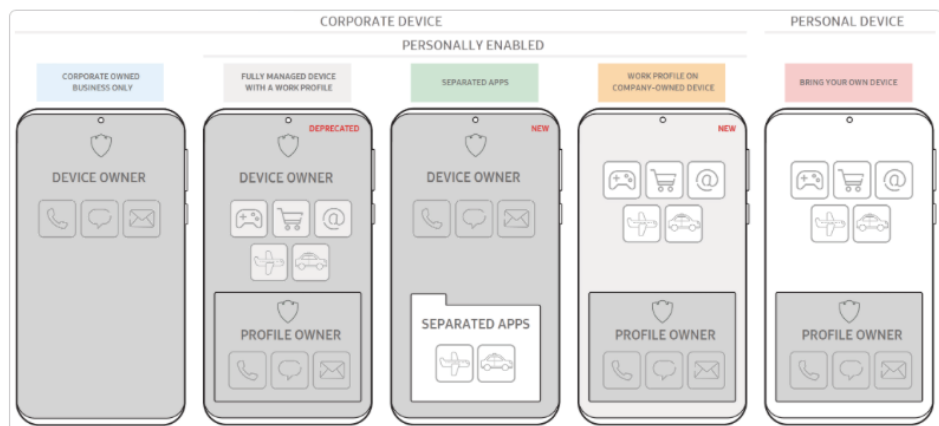
; <https://docs.samsungknox.com/admin/fundamentals/whitepaper/samsung-knox-for-android/core-platform-security/app-security/>:

App Security

Last updated February 20th, 2024

Device users typically want their personal and work apps on the same device. This requirement presents a challenge for enterprises, which need to ensure that they fully protect their confidential corporate assets and don't run into any liability issues by accidentally interfering with a user's personal privacy.

With Android 11, Google continues to protect user privacy, extending these protections to company-owned devices. Specifically, Google has replaced the device management mode called [fully managed device](#) with a [work profile](#) ➤ **work profile on company-owned device**.



<https://docs.samsungknox.com/admin/fundamentals/whitepaper/samsung-knox-for-android/the-samsung-knox-platform/>:

	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. • Separated Apps — For enterprises that need full control over a corporate-owned device, while still enabling authorized third-party business apps, Samsung exclusively offers Separated Apps to isolate third-party apps in a sandboxed folder. • 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. 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. https://docs.samsungknox.com/admin/fundamentals/whitepaper/samsung-knox-for-android/app-and-data-protection/enterprise-productivity-apps/:
--	---

	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 Work profile and users can update these apps independent of firmware updates through Google Play. • App isolation — Apps are sandboxed within the Work profile, which uses SE for Android to prevent personal apps from interfering with the business apps that are in the Work profile. • App permissions — Knox provides App Permission Monitoring to help users prevent malware from using powerful permissions to gain unauthorized access to the device and Work profile. • 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 Work profile 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. ; https://docs.samsungknox.com/admin/knox-platform-for-enterprise/knox-service-plugin/configure-advanced-policies/separated-apps/:
--	--

	Separated Apps Last updated December 22nd, 2023 Separated Apps provides an alternative to keeping apps in the same user space, and provides an option to position specific listed apps in a separate user space. Separated Apps is supported in DO deployments only. For information on how Separated Apps works, go to: Separated Apps. For more information on how Separated Apps works on devices running Android 14 or higher, see Separated Apps for Android 14 Separated Apps policies — Refer to the following group of Separated Apps policies and restrictions: • Enable Separated Apps — Set this control to True before using any using any Separated Apps policies. If disabled (set to False), KSP will apply a policy to remove Separated Apps from the device, and all apps installed inside Separated Apps will be uninstalled. • White Listing Policy — A group of policies <bundle> for specifying a list of apps to be separated, and whether the apps are installed outside or inside of the separate space. This control is available on Knox 3.7 or higher supported devices only. ◦ Location for Separate Apps installation — If set to Outside, the specified apps are installed outside (in user0), apps not in the list are installed inside. If set to Inside, the specified apps are installed inside a separate space, and apps not in the list are installed outside. ◦ List of Apps to Separate — Define a comma separated list of applications <string> that will be separated from the other apps not in this list. If Outside is selected for the Location of Separate Apps installation, then existing apps installed outside in User0 that are not part of this list are uninstalled.
[1c] the one or more processes executed in the kernel execution partition including an operating system packet network stack to pass Internet data packet traffic between the WWAN modem and one or more applications executing in the application execution partition, an	The Accused Devices comprise “the one or more processes executed in the kernel execution partition including an operating system packet network stack to pass Internet data packet traffic between the WWAN modem and one or more applications executing in the application execution partition, an application identification agent to classify individual flows of the Internet data packet traffic passing through the stack according to which of the one or more applications is associated with a particular individual flow, a service measurement agent to measure, for classified individual flows, an amount of the Internet data packet traffic associated with each of

application identification agent to classify individual flows of the Internet data packet traffic passing through the stack according to which of the one or more applications is associated with a particular individual flow, a service measurement agent to measure, for classified individual flows, an amount of the Internet data packet traffic associated with each of the one or more applications, and a policy control agent to apply application-specific traffic policy controls to classified individual flows,	the one or more applications, and a policy control agent to apply application-specific traffic policy controls to classified individual flows.” For example, the Accused Devices include a network stack for passing data between modems and applications that classifies and measures flows of internet traffic associated with applications. <i>See, e.g.,</i> https://source.android.com/docs/core/ota/modular-system/networking: Network Stack  Network Stack is an updatable Mainline module that ensures that Android can adapt to evolving network standards and allows for interoperability with new implementations. For example, updates to captive portal detection and login code allow Android to stay up to date with changing captive portal models, and updates to APF allow Android to save power on Wi-Fi as new types of packets become common. ; https://developers.google.com/android/work/requirements; https://developers.google.com/android/work/requirements/work-profile; https://developers.google.com/android/work/requirements/work-profile-corporate; https://developers.google.com/android/work/requirements/fully-managed-device; https://developers.google.com/android/work/requirements/dedicated-device; https://docs.samsungknox.com/admin/fundamentals/whitepaper/samsung-knox-for-android/device-management/firewall-management/;
--	---

Firewall Management

Last updated February 20th, 2024

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 blocked domains that users accessed

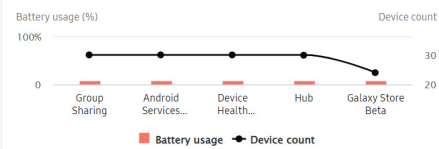
Granular control of Internet access

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.

; <https://docs.samsungknox.com/admin/knox-asset-intelligence/dashboard/app-insights/app-usage/>;

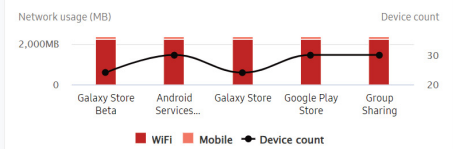
Apps with highest battery consumption ⓘ



Group Sharing	9.5%
Android Services Library Beta	9.4%
Device Health Services	9.4%
Hub	9.4%
Galaxy Store Beta	9.4%

Excluding 6 apps... Updated: 09 Jun 2023 06:30 PM

Apps with highest network usage ⓘ



Galaxy Store Beta	2,364.31MB
Android Services Library	2,358.03MB
Galaxy Store	2,356.76MB
Google Play Store	2,352.09MB
Group Sharing	2,347.49MB

⚠ 21 apps consumed 20MB or more network (mobile+WiFi) data per device in a day [View](#)

⚠ 21 apps consumed 50MB or more mobile data per device in a day [View](#)

Excluding 6 apps... Updated: 09 Jun 2023 06:30 PM

Below the line graph is a detailed list of app usage metrics, broken down into the following categories:

- **APP** — The name of the app. Click to open the drill-down view for metrics on running time and the number of devices using an app version.
- **PACKAGE NAME** — The package name. Use this to uniquely identify an app on your devices.
- **DEVICE COUNT** — The number of devices that use the app
- **TOTAL RUN TIME** — The total amount of time, in hours, that the app has been running on your devices. Sum of total foreground and background run times.
- **TOTAL FOREGROUND RUN TIME** — The total amount of time, in hours, that the app was running in the foreground on your devices.
- **TOTAL BACKGROUND RUN TIME** — The total amount of time, in hours, that the app was running in the background on your devices.
- **AVG RUN TIME** — The average amount of time, in hours and minutes, per device that the app ran.
- **AVG MOBILE DATA USAGE** — The average amount of mobile data the app used on a device.
- **AVG WIFI DATA USAGE** — The average amount of Wi-Fi data the app used on a device.
- **AVG NETWORK DATA USAGE** — The average amount of data, in MB, per device that the app consumed.
- **AVG BATTERY CONSUMPTION** — The average battery percentage consumed by an app on the device.
- **NORMALIZED BATTERY CONSUMPTION** — The percentage of battery power consumed per hour of app run time

As a further example, the Accused Devices include one or more applications. *See, e.g.,* <https://support.google.com/work/android/answer/9563584?hl=en&sjid=6738515987769519593-NC> (describing “apps and data,” including “work apps” and “personal apps.”):

Work Profile and its features

A Work Profile is a self contained profile on an Android device for storing work apps and data. Work Profile allows separation of work apps and data, giving organizations full control of the data, apps, and security policies within a Work Profile. Simultaneously, users retain privacy over their personal apps, data, and usage. On devices designated as company-owned during setup, [organizations can enforce some policies](#) that apply to a device's personal profile and overall device behavior.

Apps installed in the Work Profile are marked with the briefcase icon, so as to be easily distinguishable from personal apps. For more information on how to use a Work Profile device, see [What is a Work Profile](#).

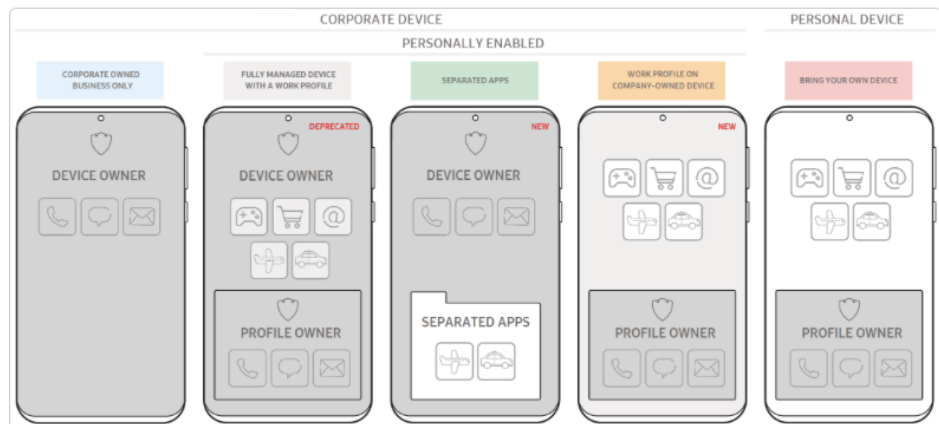
<https://docs.samsungknox.com/admin/fundamentals/whitepaper/samsung-knox-for-android/core-platform-security/app-security/> (describing “personal and work apps”):

App Security

Last updated February 20th, 2024

Device users typically want their personal and work apps on the same device. This requirement presents a challenge for enterprises, which need to ensure that they fully protect their confidential corporate assets and don't run into any liability issues by accidentally interfering with a user's personal privacy.

With Android 11, Google continues to protect user privacy, extending these protections to company-owned devices. Specifically, Google has replaced the device management mode called [fully managed device](#) with a [work profile](#) ➤ [work profile on company-owned device](#).



As a further example, the Accused Devices apply application-specific traffic policy controls through “Work profiles,” “Per-app VPN” policies, firewalls, and/or Knox VPN policies. *See, e.g.,* <https://support.google.com/work/android/answer/7502354?sjid=13758559053961042295-NC#zippy=%2Cmy-organization-owns-my-device%2Ci-own-my-device>:

What policies is my organization enforcing on my device?

If your device has a [Work Profile](#), your organization can view and manage your work apps and data. Your personal apps, data, and usage details aren't visible or accessible to your organization. Your organization may be able to manage certain settings on your device (e.g. time and date, language, Wi-Fi configurations) and enforce app defaults such as messaging and browser if your device is company-owned.

<https://www.android.com/enterprise/>; <https://developer.android.com/work/managed-profiles:>

Work profiles

The Android platform allows devices to have [work profiles](#) (sometimes referred to as managed profiles). A work profile is controlled by an IT admin, and the functionality available to it is set separately from the functionality of the user's primary profile. This approach lets organizations control the environment where company-specific apps and data are running on a user's device, while still letting users use their personal apps and profiles.

This lesson shows you how to modify your application so it functions reliably on a device with a work profile. You don't need to do anything besides the ordinary app-development best practices. However, some of these best practices become especially important on devices with work profiles. This document highlights the issues you need to be aware of.

:

<https://support.google.com/work/android/answer/9213914?hl=en&sjid=8659651805175691014-NC#zippy=%2Callowed-apps%2Cdisallowed-apps%2Cgoogle-play-traffic:>

Per-app VPN

Many VPN apps can filter which installed apps are allowed to send traffic through the VPN connection. You can create either an allowed list, or, a disallowed list, but not both. If you don't create a list, the system sends all network traffic through the VPN.

You normally configure per-app VPN in your EMM console or directly in the VPN app.

Allowed apps

You can choose which apps are allowed to use the VPN using an allowed list. If you allow one or more apps, then only the apps in the list use the VPN. All other apps (that aren't in the list) use the system networks as if the VPN isn't running.

When you also turn on *Block connections without VPN*, then only apps in the allowed list have network access.

Disallowed apps

You can select which apps you don't want to use the VPN by creating a disallowed list. Network traffic of disallowed apps uses system networking as if the VPN wasn't running—all other apps use the VPN.

When you also turn on *Block connections without VPN*, then these disallowed apps lose network access.

Google Play traffic

You might want to explicitly include or exclude Google Play traffic from your VPN if traffic is metered. Here are the Google Play app packages that you'd need to allow or disallow:

- com.android.packageinstaller
- com.android.vending
- com.google.android.gms
- com.google.android.packageinstaller

; <https://developers.google.com/android/work/requirements>;
<https://developers.google.com/android/work/requirements/work-profile>;
<https://developers.google.com/android/work/requirements/work-profile-corporate>;
<https://developers.google.com/android/work/requirements/fully-managed-device>;
<https://developers.google.com/android/work/requirements/dedicated-device>;
<https://docs.samsungknox.com/admin/fundamentals/whitepaper/samsung-knox-for-android/device-management/firewall-management/>;

Firewall Management

Last updated February 20th, 2024

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:

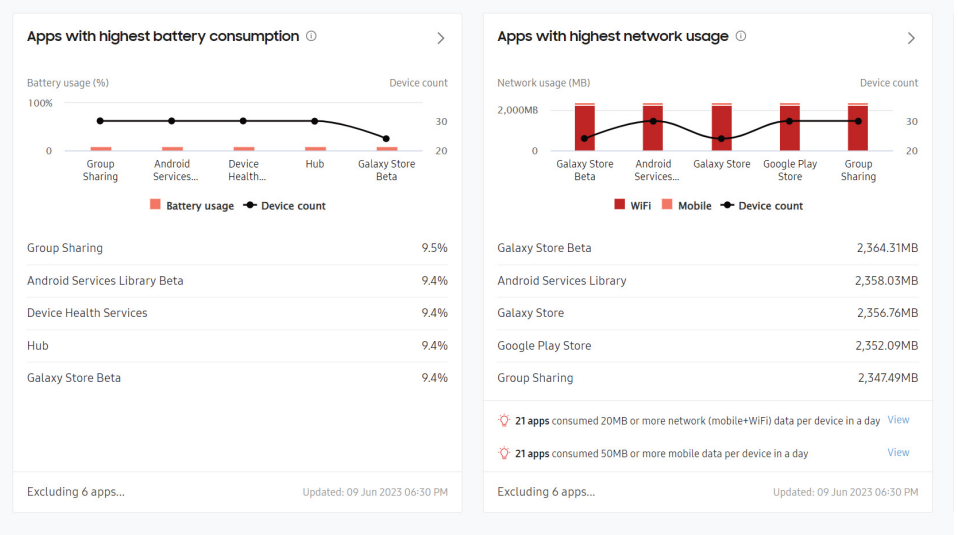
- Restrict and redirect Internet access to specific IP addresses and domains
- Set firewall policies on a per-app or device basis
- Produce logs reporting the blocked domains that users accessed

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.

; <https://docs.samsungknox.com/admin/knox-asset-intelligence/dashboard/app-insights/app-usage/>;



	Below the line graph is a detailed list of app usage metrics, broken down into the following categories: • APP — The name of the app. Click to open the drill-down view for metrics on running time and the number of devices using an app version. • PACKAGE NAME — The package name. Use this to uniquely identify an app on your devices. • DEVICE COUNT — The number of devices that use the app • TOTAL RUN TIME — The total amount of time, in hours, that the app has been running on your devices. Sum of total foreground and background run times. • TOTAL FOREGROUND RUN TIME — The total amount of time, in hours, that the app was running in the foreground on your devices. • TOTAL BACKGROUND RUN TIME — The total amount of time, in hours, that the app was running in the background on your devices. • AVG RUN TIME — The average amount of time, in hours and minutes, per device that the app ran. • AVG MOBILE DATA USAGE — The average amount of mobile data the app used on a device. • AVG WIFI DATA USAGE — The average amount of Wi-Fi data the app used on a device. • AVG NETWORK DATA USAGE — The average amount of data, in MB, per device that the app consumed. • AVG BATTERY CONSUMPTION — The average battery percentage consumed by an app on the device. • NORMALIZED BATTERY CONSUMPTION — The percentage of battery power consumed per hour of app run time ; https://docs.samsungknox.com/admin/knox-platform-for-enterprise/knox-service-plugin/configure-advanced-policies/vpn-policies/:
--	--

VPN policies

Last updated July 26th, 2023

Configuring and applying VPN policies with KSP is a two step process:

Note

To use VPN features on Samsung One UI Core devices, you are required to add the KSP package name `com.samsung.android.knox.kpu` to the certificate allow list using the **allow applications to read private keys without alerting user** feature in the [Certificate Management Policies](#) section.

Note

VPN policies require a free Knox Platform for Enterprise Premium license.

1. **Set up the VPN configuration profile** — Choose the VPN settings and policies to suit your organization. These settings are saved as a profile you can reuse in later configurations, such as setting up a DO or PO profile.
2. **Create the VPN policy** — The VPN Policy uses settings from the VPN configuration profile created in the previous step. This VPN policy allows you to specify other rules, such as which apps should use this VPN.

<https://docs.samsungknox.com/admin/fundamentals/whitepaper/samsung-knox-for-android/network-security/virtual-private-networks/>:

Virtual Private Networks (VPN)

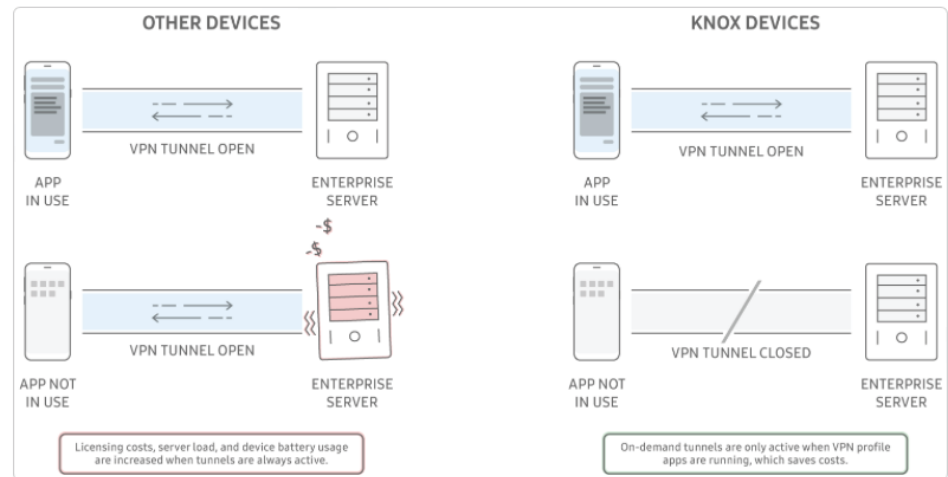
Last updated February 20th, 2024

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 (work profile as well as fully managed device) or a single app only. • 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 ability to configure SSL/IPSEC VPN profiles on multiple devices. • The advantage of extending VPN tunnels from a mobile device to a tethered laptop, in situations where a laptop does not have network connectivity. ; https://docs.samsungknox.com/admin/knox-asset-intelligence/dashboard/network-insights/mobile-network-usage/.
--	---

[1d] the one or more processes executed in the protected execution partition including one or more device agents with limited privileges to access processes executing in the kernel execution partition, including a privilege to configure the application-specific traffic policy controls of the policy control agent, and a privilege to receive at least one of Internet data packet traffic passing between the operating system packet network stack and the WWAN modem, and	The Accused Devices comprise “the one or more processes executed in the protected execution partition including one or more device agents with limited privileges to access processes executing in the kernel execution partition, including a privilege to configure the application-specific traffic policy controls of the policy control agent, and a privilege to receive at least one of Internet data packet traffic passing between the operating system packet network stack and the WWAN modem.” For example, Samsung devices include agents with privileges to access processes and configure application-specific policies as well as receive at least one of Internet data packet traffic passing between the operating system packet network stack and the WWAN modem. See e.g., https://source.android.com/docs/core/ota/modular-system/networking: Network Stack  Network Stack is an updatable Mainline module that ensures that Android can adapt to evolving network standards and allows for interoperability with new implementations. For example, updates to captive portal detection and login code allow Android to stay up to date with changing captive portal models, and updates to APF allow Android to save power on Wi-Fi as new types of packets become common. ; https://support.google.com/work/android/answer/9562029?hl=en&sjid=8659651805175691014-NC; https://support.google.com/work/android/answer/9563584?hl=en&sjid=6738515987769519593-NC;
---	--

Work Profile and its features

A Work Profile is a self contained profile on an Android device for storing work apps and data. Work Profile allows separation of work apps and data, giving organizations full control of the data, apps, and security policies within a Work Profile. Simultaneously, users retain privacy over their personal apps, data, and usage. On devices designated as company-owned during setup, [organizations can enforce some policies](#) that apply to a device's personal profile and overall device behavior.

Apps installed in the Work Profile are marked with the briefcase icon, so as to be easily distinguishable from personal apps. For more information on how to use a Work Profile device, see [What is a Work Profile](#).

;
<https://support.google.com/work/android/answer/7502354?hl=en&sjid=8659651805175691014-NC#zippy=>; <https://www.android.com/enterprise/>;
<https://developer.android.com/work/managed-profiles>:

Work profiles

The Android platform allows devices to have [work profiles](#) (sometimes referred to as managed profiles). A work profile is controlled by an IT admin, and the functionality available to it is set separately from the functionality of the user's primary profile. This approach lets organizations control the environment where company-specific apps and data are running on a user's device, while still letting users use their personal apps and profiles.

This lesson shows you how to modify your application so it functions reliably on a device with a work profile. You don't need to do anything besides the ordinary app-development best practices. However, some of these best practices become especially important on devices with work profiles. This document highlights the issues you need to be aware of.

;
<https://support.google.com/work/android/answer/9213914?hl=en&sjid=8659651805175691014-NC#zippy=%2Callowed-apps%2Cdisallowed-apps%2Cgoogle-play-traffic>:

Per-app VPN

Many VPN apps can filter which installed apps are allowed to send traffic through the VPN connection. You can create either an allowed list, or, a disallowed list, but not both. If you don't create a list, the system sends all network traffic through the VPN.

You normally configure per-app VPN in your EMM console or directly in the VPN app.

Allowed apps

You can choose which apps are allowed to use the VPN using an allowed list. If you allow one or more apps, then only the apps in the list use the VPN. All other apps (that aren't in the list) use the system networks as if the VPN isn't running.

When you also turn on *Block connections without VPN*, then only apps in the allowed list have network access.

Disallowed apps

You can select which apps you don't want to use the VPN by creating a disallowed list. Network traffic of disallowed apps uses system networking as if the VPN wasn't running—all other apps use the VPN.

When you also turn on *Block connections without VPN*, then these disallowed apps lose network access.

Google Play traffic

You might want to explicitly include or exclude Google Play traffic from your VPN if traffic is metered. Here are the Google Play app packages that you'd need to allow or disallow:

- com.android.packageinstaller
- com.android.vending
- com.google.android.gms
- com.google.android.packageinstaller

; <https://developers.google.com/android/work/requirements>;
<https://developers.google.com/android/work/requirements/work-profile>;
<https://developers.google.com/android/work/requirements/work-profile-corporate>;
<https://developers.google.com/android/work/requirements/fully-managed-device>;
<https://developers.google.com/android/work/requirements/dedicated-device>;
<https://docs.samsungknox.com/admin/fundamentals/whitepaper/samsung-knox-for-android/device-management/firewall-management/>;

Firewall Management

Last updated February 20th, 2024

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:

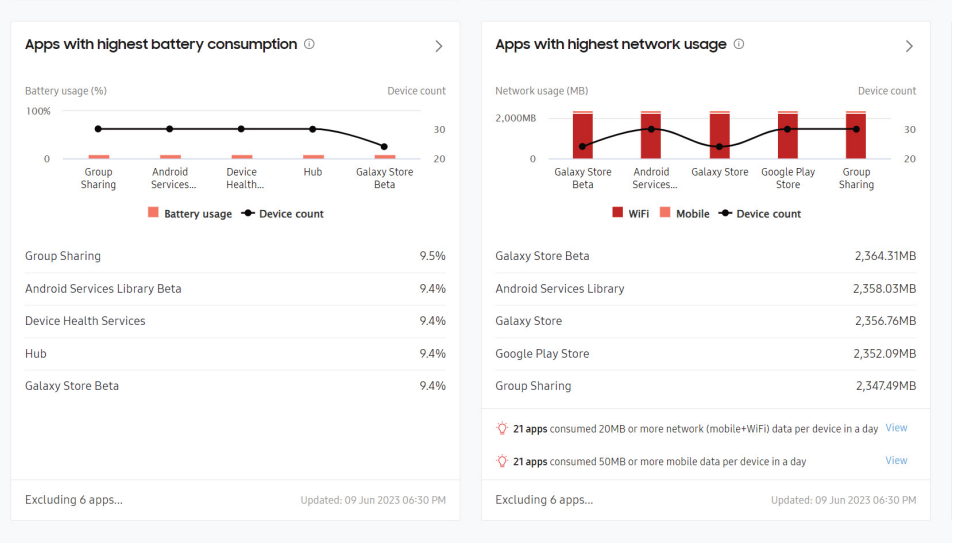
- Restrict and redirect Internet access to specific IP addresses and domains
- Set firewall policies on a per-app or device basis
- Produce logs reporting the blocked domains that users accessed

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.

; <https://docs.samsungknox.com/admin/knox-asset-intelligence/dashboard/app-insights/app-usage/>;



	Below the line graph is a detailed list of app usage metrics, broken down into the following categories: • APP — The name of the app. Click to open the drill-down view for metrics on running time and the number of devices using an app version. • PACKAGE NAME — The package name. Use this to uniquely identify an app on your devices. • DEVICE COUNT — The number of devices that use the app • TOTAL RUN TIME — The total amount of time, in hours, that the app has been running on your devices. Sum of total foreground and background run times. • TOTAL FOREGROUND RUN TIME — The total amount of time, in hours, that the app was running in the foreground on your devices. • TOTAL BACKGROUND RUN TIME — The total amount of time, in hours, that the app was running in the background on your devices. • AVG RUN TIME — The average amount of time, in hours and minutes, per device that the app ran. • AVG MOBILE DATA USAGE — The average amount of mobile data the app used on a device. • AVG WIFI DATA USAGE — The average amount of Wi-Fi data the app used on a device. • AVG NETWORK DATA USAGE — The average amount of data, in MB, per device that the app consumed. • AVG BATTERY CONSUMPTION — The average battery percentage consumed by an app on the device. • NORMALIZED BATTERY CONSUMPTION — The percentage of battery power consumed per hour of app run time As a further example, the Accused Devices apply application-specific traffic policy controls traffic,. <i>See, e.g.</i>, https://docs.samsungknox.com/admin/knox-platform-for-enterprise/knox-service-plugin/configure-advanced-policies/vpn-policies/:
--	---

VPN policies

Last updated July 26th, 2023

Configuring and applying VPN policies with KSP is a two step process:

Note

To use VPN features on Samsung One UI Core devices, you are required to add the KSP package name `com.samsung.android.knox.kpu` to the certificate allow list using the **allow applications to read private keys without alerting user** feature in the [Certificate Management Policies](#) section.

Note

VPN policies require a free Knox Platform for Enterprise Premium license.

1. **Set up the VPN configuration profile** — Choose the VPN settings and policies to suit your organization. These settings are saved as a profile you can reuse in later configurations, such as setting up a DO or PO profile.
2. **Create the VPN policy** — The VPN Policy uses settings from the VPN configuration profile created in the previous step. This VPN policy allows you to specify other rules, such as which apps should use this VPN.

<https://docs.samsungknox.com/admin/fundamentals/whitepaper/samsung-knox-for-android/network-security/virtual-private-networks/>:

Virtual Private Networks (VPN)

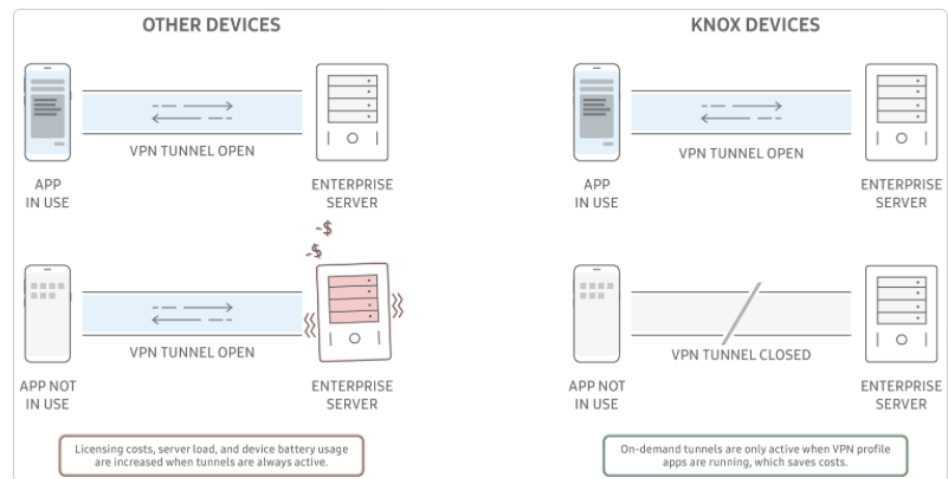
Last updated February 20th, 2024

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 (work profile as well as fully managed device) or a single app only. • 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 ability to configure SSL/IPSEC VPN profiles on multiple devices. • The advantage of extending VPN tunnels from a mobile device to a tethered laptop, in situations where a laptop does not have network connectivity. ; https://docs.samsungknox.com/admin/knox-asset-intelligence/dashboard/network-insights/mobile-network-usage/; https://www.samsung.com/us/business/solutions/samsung-knox/;
--	---

Advanced mobile security for Android

The Knox mobile security solution protects applications and data by strictly defining what each process is allowed to do and which data it can access. This allows Knox security to separate, encrypt and protect enterprise data within a managed container.

Real-time kernel protection integrity measurement architecture

Periodic Kernel Measurement and Real-time Kernel Protection work to constantly inspect the core software of the OS, the kernel. These checks ensure that requests to bypass device security are blocked and sensitive data is protected.

TrustZone

The Knox enterprise security solution leverages a processor architecture known as TrustZone, in which highly sensitive computations are isolated from the rest of the device's operations, protecting enterprise data.

Secure / trusted boot and hardware root of trust

To prevent security measures from being bypassed or compromised, Knox uses Boot-time Protections backed by Hardware Root of Trust to verify integrity of the device during the boot process.



Knox security philosophy

Build Trust

Maintain trust

Prove trust

Make ready

Chipset

The Knox platform ensures only approved versions of system-critical software are loaded. The platform is built-in and the trust starts in the hardware, with unique certificates burnt into the chipset of each device.

Knox warranty fuse

With these unique certificates, the Knox mobile security platform can verify each piece of software that loads. If verification fails, Knox either records the tampering by flipping a one-time fuse called the Knox Warranty Bit, or prevents further booting. Devices with compromised Knox Warranty Bits cannot use certain Knox features or services, such as Knox Workspace or Samsung Pay.

Rollback prevention

Rollback prevention ensures that a Samsung device is not downgraded to an earlier, vulnerable software version.

; <https://docs.samsungknox.com/admin/fundamentals/whitepaper/samsung-knox-for-android/core-platform-security/root-of-trust/>;

Secure hardware

The Knox Platform trusted environment leverages the following hardware components.

- **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.
- **ARM TrustZone Secure world** — The Secure world is the environment in which 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.
- **Knox Vault** — The Knox Vault is an independent, tamper-proof, secure subsystem with its own processor, memory, and an interface to dedicated non-volatile storage. The Knox Vault stores sensitive data such as cryptographic keys and authentication data. Even if the main application processor that runs Android is compromised, the Knox Vault protects secrets and guards against hardware attacks such as probing and fault injection.

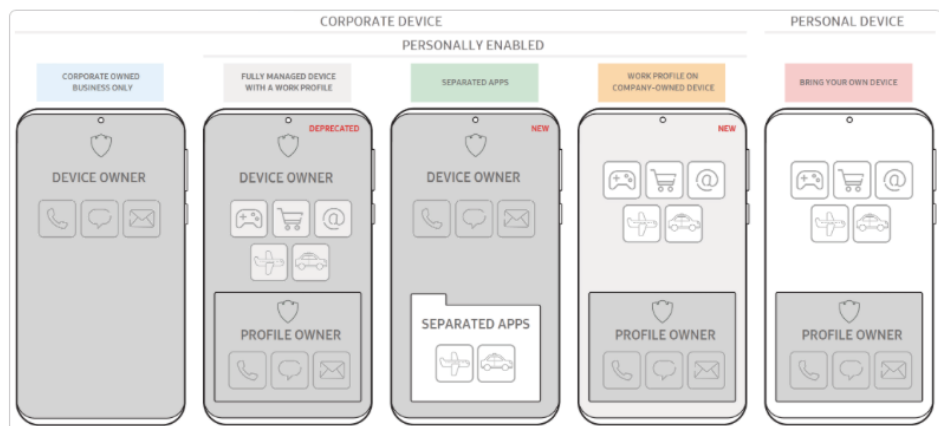
; <https://docs.samsungknox.com/admin/fundamentals/whitepaper/samsung-knox-for-android/core-platform-security/app-security/>:

App Security

Last updated February 20th, 2024

Device users typically want their personal and work apps on the same device. This requirement presents a challenge for enterprises, which need to ensure that they fully protect their confidential corporate assets and don't run into any liability issues by accidentally interfering with a user's personal privacy.

With Android 11, Google continues to protect user privacy, extending these protections to company-owned devices. Specifically, Google has replaced the device management mode called [fully managed device](#) with a [work profile](#) ➤ [work profile on company-owned device](#).



<https://docs.samsungknox.com/admin/fundamentals/whitepaper/samsung-knox-for-android/the-samsung-knox-platform/>:

	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. • Separated Apps — For enterprises that need full control over a corporate-owned device, while still enabling authorized third-party business apps, Samsung exclusively offers Separated Apps to isolate third-party apps in a sandboxed folder. • 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. 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. https://docs.samsungknox.com/admin/fundamentals/whitepaper/samsung-knox-for-android/app-and-data-protection/enterprise-productivity-apps/:
--	---

	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 Work profile and users can update these apps independent of firmware updates through Google Play. • App isolation — Apps are sandboxed within the Work profile, which uses SE for Android to prevent personal apps from interfering with the business apps that are in the Work profile. • App permissions — Knox provides App Permission Monitoring to help users prevent malware from using powerful permissions to gain unauthorized access to the device and Work profile. • 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 Work profile 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. ; https://docs.samsungknox.com/admin/knox-platform-for-enterprise/knox-service-plugin/configure-advanced-policies/separated-apps/:
--	--

Separated Apps

Last updated December 22nd, 2023

Separated Apps provides an alternative to keeping apps in the same user space, and provides an option to position specific listed apps in a separate user space. Separated Apps is supported in DO deployments only.

For information on how Separated Apps works, go to: [Separated Apps](#).

For more information on how Separated Apps works on devices running Android 14 or higher, see [Separated Apps for Android 14](#)

Separated Apps policies — Refer to the following group of Separated Apps policies and restrictions:

- **Enable Separated Apps** — Set this control to **True** before using any using any Separated Apps policies. If disabled (set to **False**), KSP will apply a policy to remove Separated Apps from the device, and all apps installed inside Separated Apps will be uninstalled.
- **White Listing Policy** — A group of policies <bundle> for specifying a list of apps to be separated, and whether the apps are installed outside or inside of the separate space. This control is available on Knox 3.7 or higher supported devices only.
 - **Location for Separate Apps installation** — If set to **Outside**, the specified apps are installed outside (in user0), apps not in the list are installed inside. If set to **Inside**, the specified apps are installed inside a separate space, and apps not in the list are installed outside.
 - **List of Apps to Separate** — Define a comma separated list of applications <string> that will be separated from the other apps not in this list. If Outside is selected for the **Location of Separate Apps installation**, then existing apps installed outside in User0 that are not part of this list are uninstalled.

For further example, Samsung devices store secure policy information indicative of a configurable communication security policy (e.g., a configurable VPN policy). *See e.g.*, <https://docs.samsungknox.com/admin/knox-platform-for-enterprise/knox-service-plugin/configure-advanced-policies/vpn-policies/>:

VPN policies

Last updated July 26th, 2023

Configuring and applying VPN policies with KSP is a two step process:

Note

To use VPN features on Samsung One UI Core devices, you are required to add the KSP package name `com.samsung.android.knox.kpu` to the certificate allow list using the **allow applications to read private keys without alerting user** feature in the [Certificate Management Policies](#) section.

Note

VPN policies require a free Knox Platform for Enterprise Premium license.

1. **Set up the VPN configuration profile** — Choose the VPN settings and policies to suit your organization. These settings are saved as a profile you can reuse in later configurations, such as setting up a DO or PO profile.
2. **Create the VPN policy** — The VPN Policy uses settings from the VPN configuration profile created in the previous step. This VPN policy allows you to specify other rules, such as which apps should use this VPN.

<https://docs.samsungknox.com/admin/fundamentals/whitepaper/samsung-knox-for-android/network-security/virtual-private-networks/>:

Virtual Private Networks (VPN)

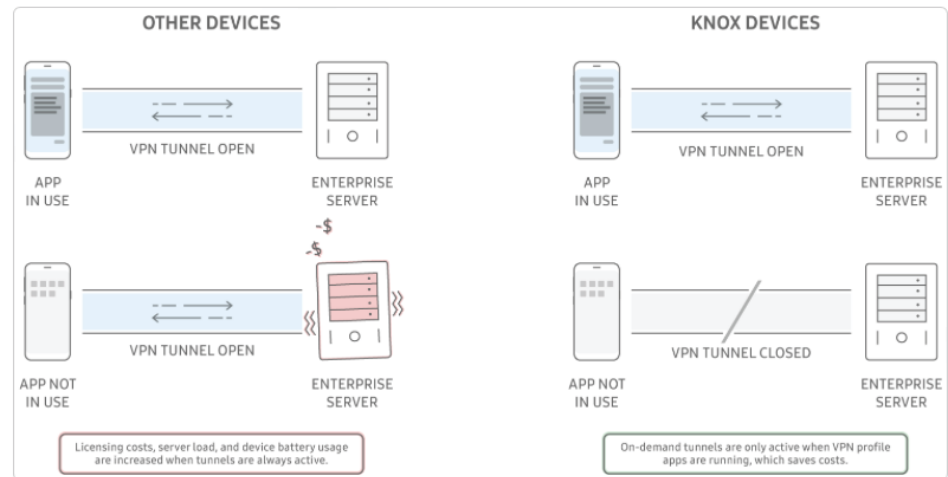
Last updated February 20th, 2024

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 (work profile as well as fully managed device) or a single app only. • 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 ability to configure SSL/IPSEC VPN profiles on multiple devices. • The advantage of extending VPN tunnels from a mobile device to a tethered laptop, in situations where a laptop does not have network connectivity.
[1e] traffic information including the measured amount of the Internet data packet traffic associated with each of the one or more applications.	The Accused Devices comprise “traffic information including the measured amount of the Internet data packet traffic associated with each of the one or more applications.” <i>See e.g.</i>, https://source.android.com/docs/core/ota/modular-system/networking: Network Stack  Network Stack is an updatable Mainline module that ensures that Android can adapt to evolving network standards and allows for interoperability with new implementations. For example, updates to captive portal detection and login code allow Android to stay up to date with changing captive portal models, and updates to APF allow Android to save power on Wi-Fi as new types of packets become common. ; https://developers.google.com/android/work/requirements; https://developers.google.com/android/work/requirements/work-profile: 4.21. Network statistics collection Android 6.0+  IT admins can query network usage statistics from a device's work profile.

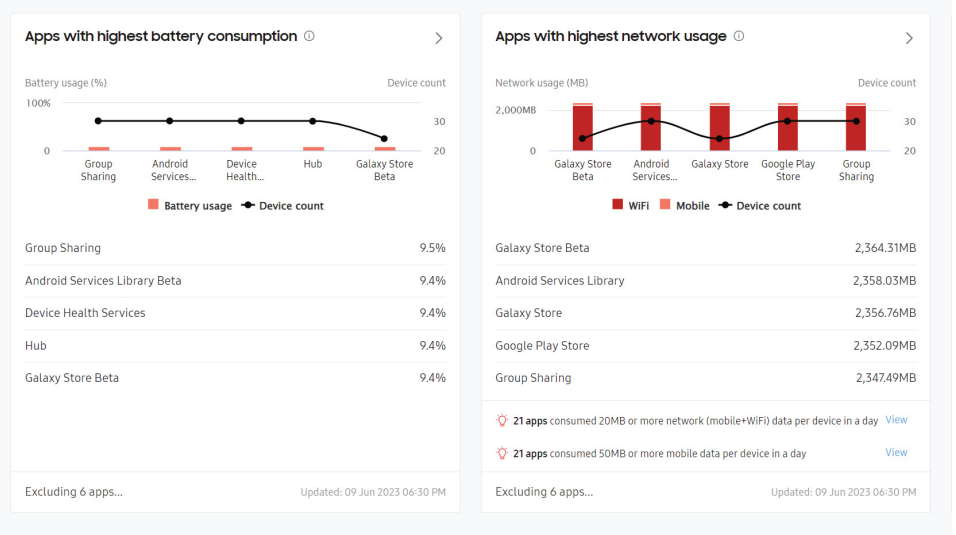
https://developers.google.com/android/work/requirements/work-profile-corporate:		
4.21. Network statistics collection	Android 6.0+	☆ IT admins can query network usage statistics from a device's work profile.
https://developers.google.com/android/work/requirements/fully-managed-device:		
4.22. Advanced network statistics collection	Android 6.0+	☆ IT admins can query network usage statistics for an entire managed device.
https://developers.google.com/android/work/requirements/dedicated-device:		
4.22. Advanced network statistics collection	Android 6.0+	☆ IT admins can query network usage statistics for an entire managed device.
; https://docs.samsungknox.com/admin/fundamentals/whitepaper/samsung-knox-for-android/device-management/firewall-management/ :		
Firewall Management Last updated February 20th, 2024 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 blocked 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.

; <https://docs.samsungknox.com/admin/knox-asset-intelligence/dashboard/app-insights/app-usage/>;



	Below the line graph is a detailed list of app usage metrics, broken down into the following categories: • APP — The name of the app. Click to open the drill-down view for metrics on running time and the number of devices using an app version. • PACKAGE NAME — The package name. Use this to uniquely identify an app on your devices. • DEVICE COUNT — The number of devices that use the app • TOTAL RUN TIME — The total amount of time, in hours, that the app has been running on your devices. Sum of total foreground and background run times. • TOTAL FOREGROUND RUN TIME — The total amount of time, in hours, that the app was running in the foreground on your devices. • TOTAL BACKGROUND RUN TIME — The total amount of time, in hours, that the app was running in the background on your devices. • AVG RUN TIME — The average amount of time, in hours and minutes, per device that the app ran. • AVG MOBILE DATA USAGE — The average amount of mobile data the app used on a device. • AVG WIFI DATA USAGE — The average amount of Wi-Fi data the app used on a device. • AVG NETWORK DATA USAGE — The average amount of data, in MB, per device that the app consumed. • AVG BATTERY CONSUMPTION — The average battery percentage consumed by an app on the device. • NORMALIZED BATTERY CONSUMPTION — The percentage of battery power consumed per hour of app run time As a further example, the Accused Devices apply application-specific traffic policy controls traffic,. <i>See, e.g.</i>, https://docs.samsungknox.com/admin/knox-platform-for-enterprise/knox-service-plugin/configure-advanced-policies/vpn-policies/:
--	---

VPN policies

Last updated July 26th, 2023

Configuring and applying VPN policies with KSP is a two step process:

Note

To use VPN features on Samsung One UI Core devices, you are required to add the KSP package name `com.samsung.android.knox.kpu` to the certificate allow list using the **allow applications to read private keys without alerting user** feature in the [Certificate Management Policies](#) section.

Note

VPN policies require a free Knox Platform for Enterprise Premium license.

1. **Set up the VPN configuration profile** — Choose the VPN settings and policies to suit your organization. These settings are saved as a profile you can reuse in later configurations, such as setting up a DO or PO profile.
2. **Create the VPN policy** — The VPN Policy uses settings from the VPN configuration profile created in the previous step. This VPN policy allows you to specify other rules, such as which apps should use this VPN.

<https://docs.samsungknox.com/admin/fundamentals/whitepaper/samsung-knox-for-android/network-security/virtual-private-networks/>; <https://docs.samsungknox.com/admin/knox-asset-intelligence/dashboard/network-insights/mobile-network-usage/>;
<https://www.samsung.com/us/business/solutions/samsung-knox/>;
<https://docs.samsungknox.com/admin/fundamentals/whitepaper/samsung-knox-for-android/core-platform-security/root-of-trust/>;
<https://docs.samsungknox.com/admin/fundamentals/whitepaper/samsung-knox-for-android/core-platform-security/app-security/>;
<https://docs.samsungknox.com/admin/fundamentals/whitepaper/samsung-knox-for-android/the-samsung-knox-platform/>;
<https://docs.samsungknox.com/admin/fundamentals/whitepaper/samsung-knox-for-android/app-and-data-protection/enterprise-productivity-apps/>; <https://docs.samsungknox.com/admin/knox-platform-for-enterprise/knox-service-plugin/configure-advanced-policies/separated-apps/>.

Claim 2

Issued Claim(s)	Public Documentation
2. The wireless end-user device of claim 1, the one or more processors further configured to execute, in the application execution partition, at least one device-assisted-services agent to communicate with at least one device agent executed in the protected execution partition.	Samsung's devices comprise "the one or more processors further configured to execute, in the application execution partition, at least one device-assisted-services agent to communicate with at least one device agent executed in the protected execution partition." <i>See supra</i> claim 1, describing agents which communicate with agents in a protected execution partition.

Claim 3

Issued Claim(s)	Public Documentation
3. The wireless end-user device of claim 1, further comprising one or more memory partitions to store program code for the respective processes of the operating system packet network stack, the application identification agent, the service measurement agent, the policy control agent, and the one or more device agents, the one or more processors configured to retrieve the stored program code from the one or more memory partitions to execute the respective processes.	Samsung's devices further comprise "one or more memory partitions to store program code for the respective processes of the operating system packet network stack, the application identification agent, the service measurement agent, the policy control agent, and the one or more device agents, the one or more processors configured to retrieve the stored program code from the one or more memory partitions to execute the respective processes." <i>See supra</i> claim 1, describing one or more partitions for storing code.

Claim 4

Issued Claim(s)	Public Documentation
-----------------	----------------------

4. The wireless end-user device of claim 3, wherein the one or more memory partitions include a separately protected device-assisted services partition to store the program code for the one or more device agents, the one or more device agents further comprising an access control integrity agent having exclusive permission to update program code stored in the separately protected device-assisted services partition.	Samsung's devices further comprise "[t]he wireless end-user device of claim 3, wherein the one or more memory partitions include a separately protected device-assisted services partition to store the program code for the one or more device agents, the one or more device agents further comprising an access control integrity agent having exclusive permission to update program code stored in the separately protected device-assisted services partition." <i>See supra</i> claims 1 and 3, describing one or more partitions for storing code.
---	--

Claim 5

Issued Claim(s)	Public Documentation
5. The wireless end-user device of claim 4, the access control integrity agent further configured to validate the program code for the one or more device agents.	Samsung's devices further comprise "[t]he wireless end-user device of claim 4, wherein the one or more memory partitions include a separately protected device-assisted services partition to store the program code for the one or more device agents, the one or more device agents further comprising an access control integrity agent having exclusive permission to update program code stored in the separately protected device-assisted services partition." <i>See supra</i> claims 1 and 4.

Claim 6

Issued Claim(s)	Public Documentation
6. The wireless end-user device of claim 3, wherein the one or more memory partitions comprise a device-assisted services partition to store device service state information, the device service state information only modifiable by the one or more device agents.	Samsung's devices further comprise "[t]he wireless end-user device of claim 3, wherein the one or more memory partitions comprise a device-assisted services partition to store device service state information, the device service state information only modifiable by the one or more device agents." <i>See supra</i> claims 1 and 3.

--	--

Claim 7

Issued Claim(s)	Public Documentation
7. The wireless end-user device of claim 6, the one or more device agents further comprising a service control link configured to securely communicate with a network service controller.	Samsung's devices further comprise "[t]he wireless end-user device of claim 6, the one or more device agents further comprising a service control link configured to securely communicate with a network service controller." <i>See supra</i> claims 1 and 6, describing Knox and/or Android Enterprise servers which securely communicate with device agents.

Claim 8

Issued Claim(s)	Public Documentation
8. The wireless end-user device of claim 7, wherein the service control link is further configured to receive at least one of the application-specific traffic policy controls from the network service controller.	Samsung's devices further comprise "[t]he wireless end-user device of claim 7, wherein the service control link is further configured to receive at least one of the application-specific traffic policy controls from the network service controller." <i>See supra</i> claims 1 and 7, describing policy controls received from Knox and/or Android Enterprise servers.

Claim 9

Issued Claim(s)	Public Documentation
9. The wireless end-user device of claim 7, wherein the service control link is further configured to transmit at least some of the device service state information to the network service controller.	Samsung's devices further comprise "[t]he wireless end-user device of claim 7, wherein the service control link is further configured to transmit at least some of the device service state information to the network service controller." <i>See supra</i> claims 1 and 7, describing information regarding device service states transmitted by the device to Knox and/or Android Enterprise servers.

--	--

Claim 10

Issued Claim(s)	Public Documentation
10. The wireless end-user device of claim 9, wherein the one or more device agents are further configured to retain the transmitted device service state information until after an instruction is received from the network service controller acknowledging that the device service state information can be deleted.	Samsung's devices further comprise "[t]he wireless end-user device of claim 9, wherein the one or more device agents are further configured to retain the transmitted device service state information until after an instruction is received from the network service controller acknowledging that the device service state information can be deleted." <i>See supra</i> claims 1 and 9.

Claim 11

Issued Claim(s)	Public Documentation
11. The wireless end-user device of claim 1, the one or more device agents further configured to, based on the application-specific traffic policy controls, configure application settings for the one or more applications.	Samsung's devices further comprise "[t]he wireless end-user device of claim 1, the one or more device agents further configured to, based on the application-specific traffic policy controls, configure application settings for the one or more applications." <i>See supra</i> claims 1, describing settings for the one or more applications.

Claim 12

Issued Claim(s)	Public Documentation
12. The wireless end-user device of claim 1, the one or more device agents further configured to calculate, separate from the traffic information, a service usage measurement for the Internet data packet	Samsung's devices further comprise "[t]he wireless end-user device of claim 1, the one or more device agents further configured to calculate, separate from the traffic information, a service usage measurement for the Internet data packet traffic passing between the operating system packet network stack and the WWAN modem."

traffic passing between the operating system packet network stack and the WWAN modem.	<i>See supra</i> claim 1.
---	---------------------------

Claim 13

Issued Claim(s)	Public Documentation
13. The wireless end-user device of claim 1, the one or more device agents further configured to encrypt Internet data packet traffic passing from the operating system packet network stack to the WWAN modem.	Samsung's devices further comprise "[t]he wireless end-user device of claim 1, the one or more device agents further configured to encrypt Internet data packet traffic passing from the operating system packet network stack to the WWAN modem." <i>See supra</i> claim 1.

Claim 14

Issued Claim(s)	Public Documentation
14. The wireless end-user device of claim 1, wherein the protected execution partition comprises a secure virtual execution environment.	Samsung's devices further comprise "[t]he wireless end-user device of claim 1, wherein the protected execution partition comprises a secure virtual execution environment." <i>See supra</i> claim 1.

Claim 15

Issued Claim(s)	Public Documentation
15. The wireless end-user device of claim 1, wherein the privilege to configure the application-specific traffic policy controls of the policy control agent is an exclusive privilege for one or more of the	Samsung's devices further comprise "[t]he wireless end-user device of claim 1, wherein the privilege to configure the application-specific traffic policy controls of the policy control agent is an exclusive privilege for one or more of the device agents executed in the protected execution partition."

device agents executed in the protected execution partition.	<i>See supra</i> claim 1.
--	---------------------------

Claim 16

Issued Claim(s)	Public Documentation
16. The wireless end-user device of claim 1, the WWAN modem comprising a modem execution partition configured to calculate, separate from the traffic information, a service usage measurement for the Internet data packet traffic passing between the operating system packet network stack and the WWAN modem.	Samsung's devices further comprise "[t]he wireless end-user device of claim 1, the WWAN modem comprising a modem execution partition configured to calculate, separate from the traffic information, a service usage measurement for the Internet data packet traffic passing between the operating system packet network stack and the WWAN modem." <i>See supra</i> claim 1.

Claim 17

Issued Claim(s)	Public Documentation
17. The wireless end-user device of claim 16, the modem execution partition further comprising a modem control link to communicate the calculated service usage measure to at least one of a network service controller and at least one device agent executed in the protected execution partition.	Samsung's devices further comprise "[t]he wireless end-user device of claim 16, the modem execution partition further comprising a modem control link to communicate the calculated service usage measure to at least one of a network service controller and at least one device agent executed in the protected execution partition." <i>See supra</i> claims 1 and 16.

Claim 18

Issued Claim(s)	Public Documentation
18. The wireless end-user device of claim 2, further comprising a user interface, the at least one device-assisted-services agent comprising a user-interface agent to display to a user, and allow modification to, at least one policy setting affecting at least one of the application-specific policy controls.	Samsung's devices further comprise "[t]he wireless end-user device of claim 2, further comprising a user interface, the at least one device-assisted-services agent comprising a user-interface agent to display to a user, and allow modification to, at least one policy setting affecting at least one of the application-specific policy controls." <i>See supra</i> claims 1 and 2, describing policies which users can change through settings on the Accused Devices, such as Data Saver, Power Save Mode, App Standby, etc.