

**UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TEXAS
MARSHALL DIVISION**

Headwater Research LLC,

Plaintiff,

vs.

Samsung Electronics Co., Ltd. and Samsung
Electronics America, Inc.,

Defendants.

CASE NO. 2:24-cv-00627

JURY DEMANDED

COMPLAINT FOR PATENT INFRINGEMENT

Plaintiff Headwater Research LLC (“Headwater”) files this complaint against Defendants Samsung Electronics Co., Ltd. and Samsung Electronics America, Inc. (collectively, “Defendants” or “Samsung”), alleging infringement of U.S. Patent Nos. 10,028,144 and 10,080,250. The Accused Instrumentalities are mobile electronic devices, including mobile phones and tablets used, made, offered for sale, sold, and/or imported by Defendants in the United States and supplied by Defendants to customers in the United States.

BACKGROUND

1. This complaint arises from Defendants’ infringement of the following United States patents owned by Headwater, each of which relate to wireless communications technology: United States Patent Nos. 10,028,144 (“the ’144 patent”), and 10,080,250 (“the ’250 patent”) (collectively, the “Asserted Patents”).

2. Dr. Gregory Raleigh—the primary inventor of the Asserted Patents—is a world-renowned scientist, inventor, and entrepreneur, with over 25 years of executive experience in several

technology sectors including networking, cloud software, consumer services, wireless and military systems. Dr. Raleigh holds Ph.D. and Masters degrees in Electrical Engineering from Stanford University, and a BS in Electrical Engineering from Cal Poly San Luis Obispo. He is the inventor of over 350 issued U.S. and international patents in several fields including radio systems and components, radar, mobile operating systems, cloud services, IoT, networking, consumer electronics, radiation beam cancer therapy and medical imaging.

3. Dr. Raleigh has a long and distinguished record of significant contributions and advancements in wireless communications technology. His inventions, companies, and products have profoundly and positively impacted virtually every aspect of the mobile device and communications market. In 2005, Dr. Raleigh was named one of the “50 most powerful people in networking” because of his discoveries in wireless communications technology, and his work in multiplying the capacity of a radio link using multiple transmission and receiving antennas to exploit multipath propagation was described as the “most important wireless technology in the works.” *See* <https://www.networkworld.com/article/2316916/the-50-most-powerful-people-in-networking.html?page=2>.

4. In 1996, while at Stanford University, Dr. Raleigh presented the first mathematical proof demonstrating that multiple antennas may be used with special signal processing techniques to transmit multiple data streams at the same time and on the same frequency while in the presence of naturally occurring multipath propagation. Dr. Raleigh’s work at Stanford has been widely adopted in modern multiple-input and multiple-output (“MIMO”) radio communication and implemented in major wireless communication standards including 4G and 5G. *See, e.g.,* https://en.wikipedia.org/wiki/Gregory_Raleigh.

5. Dr. Raleigh's groundbreaking work solved problems that had existed in wireless communication since the late 1800s and overturned a century of research and practice in the fields of radio science and wireless communication theory. His work revealed that a new class of MIMO signal processing architectures would allow wireless devices to transmit multiple data streams at the same time on the same frequency thereby multiplying the information-carrying capacity of wireless networks.

6. Based on his discoveries, Dr. Raleigh co-founded Clarity Wireless to develop smart antenna products incorporating the advances of his MIMO signal processing architecture, and obtained patents now used in 4G and 5G cellular and Wi-Fi standards. Field trials of the smart antennas developed by Clarity Wireless demonstrated performance significantly above anything else contemplated at the time and continue to set standards for multipath broadband wireless access links. Shortly after those field trials, Cisco acquired Clarity in 1998 and hired Dr. Raleigh to continue to commercialize these technologies.

7. After leaving Cisco, Dr. Raleigh founded Airgo Networks to develop the world's first MIMO wireless chipsets, networking software, reference design systems and commercial OEM products. Airgo Networks's chipset products significantly improved the speed and reliability of Wi-Fi, leading to the adoption of its technology as the core of Wi-Fi radio standards since 2006, and adoption of the chipsets into products sold across the globe. In 2006, Qualcomm acquired Airgo Networks and hired Dr. Raleigh to continue to commercialize these technologies. The Airgo team at Qualcomm spearheaded the creation of Wi-Fi standards and developed the first Qualcomm Wi-Fi chips for cell phones.

8. Dr. Raleigh's innovations at Clarity Wireless, Cisco, Airgo Networks, and Qualcomm, resulted in the widespread adoption of his technologies in a multitude of cellular and

Wi-Fi standards, such as LTE, WiMAX, 802.11n, 802.11ac (Wi-Fi 5), as well as 802.11ax (Wi-Fi 6).

9. After successfully founding and selling Clarity Wireless and Airgo Networks to Cisco and Qualcomm, respectively, Dr. Raleigh shifted his focus from solving radio-centric problems to solving problems in how wireless services are provided to consumers. Dr. Raleigh foresaw significant data demand problems presented by the advent and adoption of smartphones. He sought to solve these data demand problems by improving end-user wireless devices and the services that support them.

10. In 2008, Dr. Raleigh formed Headwater to develop mobile operating systems and cloud technology, which today, underpin the mobile phone and app industries. The patents in this action describe and claim some of the extraordinary inventions developed by Dr. Raleigh and the Headwater team.

11. Smartphones and other mobile devices have become ubiquitous and inseparable components of our daily lives, allowing us to make and receive phone calls, get notifications, download music, upload photos, stream entertainment, transact business, exchange ideas, and keep us connected to our family and friends whether they are down the hall or around the globe. Users can get email, install apps, and browse the internet from these tiny devices by making use of data connectivity services. These devices accomplish these amazing feats by exchanging staggering amounts of data over the internet using wireless and cellular networks, relying on ubiquitous data connectivity to keep users up-to-date and connected.

12. Since 2011, mobile device data demand has exploded—increasing by almost 400%—with each user consuming approximately 11.5 gigabytes of data per month. In the aggregate, this equates to approximately 90 exabytes of data consumption per month. *See, e.g.,*

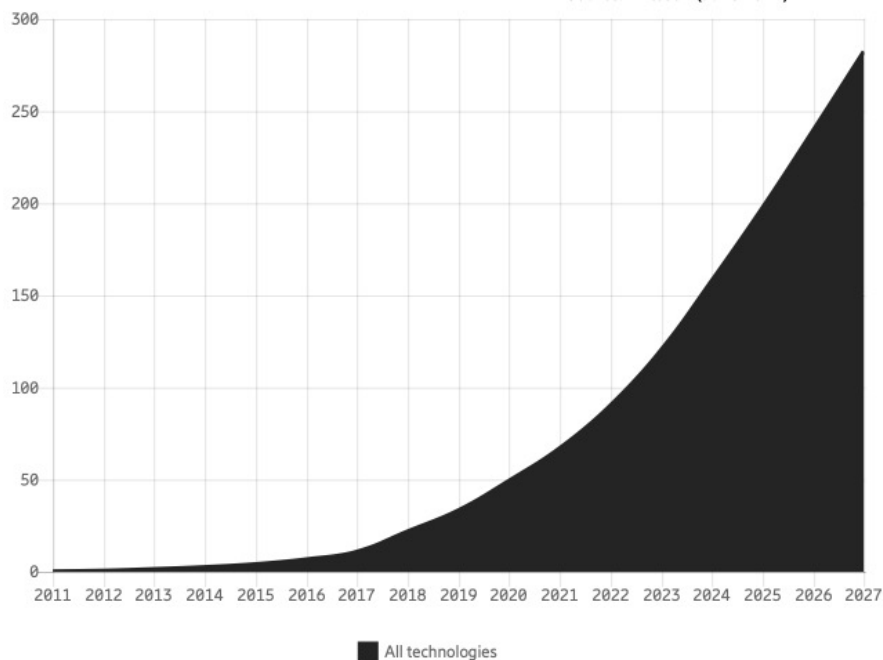
<https://www.ericsson.com/en/reports-and-papers/mobility-report/mobility-visualizer?f=9&ft=2&r=1&t=11,12,13,14,15,16,17&s=4&u=3&y=2011,2027&c=3>. For context: a single exabyte of data is equivalent to one billion gigabytes of data. Said another way, if one gigabyte is the size of the Earth, then an exabyte is the size of the sun. See, e.g., <https://www.backblaze.com/blog/what-is-an-exabyte/>.

13. And mobile device data demand shows no sign of slowing down. Between now and 2027, mobile data demand is projected to increase more than three-fold, from 90 exabytes per month to a staggering 282 exabytes per month, with each user consuming an average of 41 gigabytes of data each and every month. See, e.g., <https://www.ericsson.com/en/reports-and-papers/mobility-report/mobility-calculator?up=2&bp=1&v=0&c=2>; <https://www.ericsson.com/en/reports-and-papers/mobility-report/mobility-visualizer?f=9&ft=2&r=1&t=11,12,13,14,15,16,17&s=4&u=3&y=2011,2027&c=3>.

Mobile data traffic

Unit: EB/month
All technologies
All devices
Year: 2011 - 2027

Source: Ericsson (June 2022)



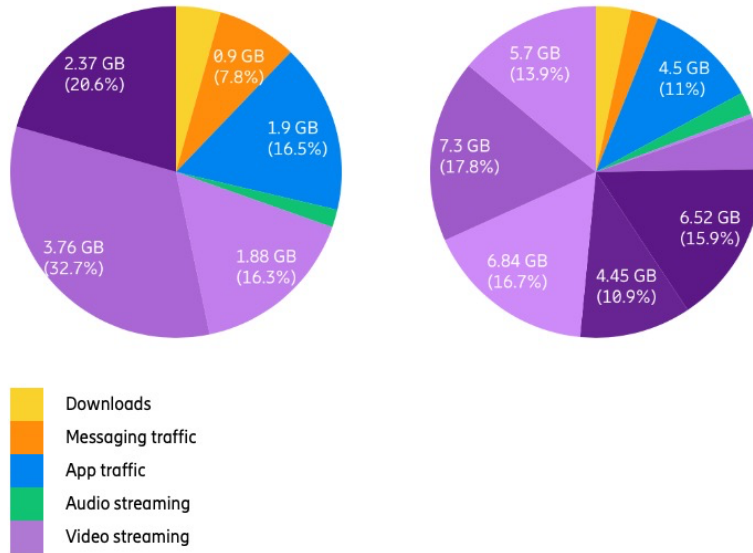
Ericsson Mobility Calculator

Your example of calculated
monthly consumption.

11.45 GB

World average 2027 average
monthly consumption.

40.99 GB



14. Also in 2008, Dr. Raleigh founded ItsOn Inc., which licensed Headwater's intellectual property and implemented Headwater's technology into software and services that expanded cellular service plan offerings and improved device and data management capabilities. The tools and technologies delivered by ItsOn allowed carriers to implement Headwater's technologies in end-user devices—such as mobile phones and tablets—opening up new business models while also providing greater flexibility to carriers and device manufacturers, allowing them to reduce costs while simultaneously improving their devices and services.

15. The Headwater technologies disclosed in the Asserted Patents laid the groundwork for many of the infringing features and functionalities that help device manufacturers, wireless carriers, and customers reduce data usage and network congestion, extend battery life by decreasing power consumption, and enable users to stay connected.

PLAINTIFF HEADWATER AND THE PATENTS-IN-SUIT

16. Plaintiff Headwater was formed in 2011 and has been in continued existence and operation since that time. Headwater is a Texas limited liability company organized under the laws of Texas, with its headquarters at 110 North College Avenue, Suite 1116, Tyler, Texas 75702.

17. Headwater is the owner of U.S. Patent No. 10,080,250, entitled “Enterprise access control and accounting allocation for access networks,” which issued on September 18, 2018. A copy of the ’250 patent is attached to this complaint as Exhibit 1.

18. Headwater is the owner of U.S. Patent No. 10,028,144, entitled “Security techniques for device assisted services,” which issued on July 17, 2018. A copy of the ’144 patent is attached to this complaint as Exhibit 2.

DEFENDANTS AND THE ACCUSED INSTRUMENTALITIES

19. On information and belief, Defendant Samsung Electronics Co., Ltd. (“SEC”) is a corporation organized under the laws of South Korea, with its principal place of business at 129, Samsung-Ro, YeongTong-Gu, Suwon-Si, Gyonggi-Do, 443-742, South Korea.

20. On information and belief, Defendant Samsung Electronics America, Inc. (“SEA”) is a United States corporation organized under the laws of the State of New York, with its principal place of business at 85 Challenger Road, Ridgefield Park, New Jersey 07660. SEA is a wholly-owned subsidiary of SEC. SEA distributes certain Samsung consumer electronics products, including the Accused Instrumentalities, in the United States.

21. On information and belief, SEA has corporate offices in the Eastern District of Texas at 1303 East Lookout Drive, Richardson, Texas 75082, 2800 Technology Drive, Suite 200,

Plano, Texas 75074, and at 6625 Excellence Way, Plano, Texas 75023.¹ On information and belief, SEA may be served with process through its registered agent CT Corporation System, 1999 Bryan Street, Suite 900, Dallas, Texas 75201-3136.

22. The Accused Instrumentalities are mobile electronic devices, including mobile phones and tablets used, offered for sale, sold, and/or imported by Defendants in the United States.

JURISDICTION AND VENUE

23. This action arises under the patent laws of the United States, Title 35 of the United States Code.

24. This Court has original subject matter jurisdiction pursuant to 28 U.S.C. §§ 1331 and 1338(a).

25. This Court has personal jurisdiction over Samsung in this action because Samsung has committed acts of infringement within this District giving rise to this action, has a regular and established place of business in this District, and has established minimum contacts with this forum such that the exercise of jurisdiction over Samsung would not offend traditional notions of fair play and substantial justice. Samsung, directly and/or through subsidiaries or intermediaries, conducts its business extensively throughout Texas, by shipping, distributing, offering for sale, selling, and advertising its products and/or services in Texas and the Eastern District of Texas, regularly do business or solicit business, engage in other persistent courses of conduct, and/or derive substantial revenue from products and/or services provided to individuals in Texas, and commit acts of infringement of Headwater's patents in this District by, among other things, making, using, importing, offering to sell, and selling products that infringe the asserted patents,

¹ <https://news.samsung.com/us/samsung-electronics-america-open-flagship-north-texas-campus/>;
<https://www.themuse.com/profiles/samsungelectronicsamerica/location/plano>.

including without limitation the Samsung tablets and phones accused of infringement in this case.

26. Samsung, directly and/or through subsidiaries or intermediaries, have purposefully and voluntarily placed one or more products and/or services in the stream of commerce that practice the Asserted Patents with the intention and expectation that they will be purchased and used by consumers in the Eastern District of Texas. These products and/or services have been and continue to be purchased and used in the Eastern District of Texas.

27. Venue as to Samsung is proper in this District under 28 U.S.C. §§ 1391 and 1400(b). On information and belief, Samsung has transacted business in this District and has committed acts of direct and indirect infringement in this District by, among other things, making, using, importing, offering to sell, and selling products that infringe the Asserted Patents.

28. Defendant SEA maintains a regular and established place of business at 1303 East Lookout Drive, Richardson, Texas 75082, 2800 Technology Drive, Suite 200, Plano, Texas 75074, and 6625 Excellence Way, Plano, Texas 75023.

29. Defendant SEC is a foreign corporation. Venue is proper as to a foreign defendant in any district. 28 U.S.C. § 1391(c)(3).

30. Further, upon information and belief, Samsung has admitted or not contested proper venue in this Judicial District in other patent infringement actions.

COUNT 1 – CLAIM FOR INFRINGEMENT OF THE '250 PATENT

31. Headwater incorporates by reference each of the allegations in the above paragraphs and further alleges as follows:

32. On September 18, 2018, the United States Patent and Trademark Office issued U.S. Patent No. 10,080,250, entitled “Enterprise access control and accounting allocation for access networks.” Ex. 1.

33. Headwater is the owner of the '250 patent with full rights to pursue recovery of royalties for damages for infringement, including full rights to recover past and future damages.

34. The written description of the '250 patent describes in technical detail each limitation of the claims, allowing a skilled artisan to understand the scope of the claims and how the nonconventional and non-generic combination of claim limitations is patently distinct from and improved upon what may have been considered conventional or generic in the art at the time of the invention.

35. Headwater and its predecessors in interest have satisfied the requirements of 35 U.S.C. § 287(a) with respect to the '250 patent because there are no unmarked articles subject to a duty to mark, and Headwater is entitled to damages for Defendants' past infringement.

36. Defendants have directly infringed (literally and equivalently) and induced others to infringe the '250 patent by making, using, selling, offering for sale, or importing products that infringe the claims of the '250 patent and by inducing others to infringe the claims of the '250 patent without a license or permission from Headwater.

37. On information and belief, Defendants use, import, offer for sale, and sell certain infringing products in the United States. The Accused Instrumentalities are, for example, mobile electronic devices, including mobile phones and tablets.

38. For example, attached as Exhibit 3 is a chart setting forth a description of Defendants' infringement of claim 1 of the '250 patent.

39. Defendants also knowingly and intentionally induce and contribute to infringement of the '250 patent in violation of 35 U.S.C. §§ 271(b) and 271(c).

40. Despite this knowledge of the '250 patent, Defendants continue to actively encourage and instruct its customers to use and integrate the Accused Instrumentalities in ways

that directly infringe the '250 patent. Defendants do so knowing and intending that their customers will commit these infringing acts. Defendants also continue to make, use, offer for sale, sell, and/or import the Accused Instrumentalities, despite their knowledge of the '250 patent, thereby specifically intending for and inducing its customers to infringe the '250 patent through the customers' normal and customary use of the Accused Instrumentalities.

41. Defendants have infringed multiple claims of the '250 patent, including independent claim 1. By way of example only, the normal and customary use of the mobiles phones and tablets made, used, sold, offered for sale and/or imported by Defendants infringes an exemplary claim of the '250 patent, as in the description set forth in Exhibit 3, which Headwater provides without the benefit of information about the Accused Instrumentalities obtained through discovery.

42. Defendants have known how the Accused Instrumentalities are made and have known, or have been willfully blind to the fact, that making, using, offering to sell, and selling the Accused Instrumentalities to their customers, would constitute willful infringement of the '250 patent. Those products imported into and sold within the United States include, without limitation, Samsung Knox-enabled devices.

43. Defendants have induced, and continue to induce, infringement of the '250 patent by actively encouraging others (including its customers) to use, offer to sell, sell, and import the Accused Instrumentalities. On information and belief, these acts include providing information and instructions on the use of the Accused Instrumentalities; providing information, education and instructions to its customers; providing the Accused Instrumentalities to customers; and indemnifying patent infringement within the United States.

44. Headwater has been damaged by Defendant's infringement of the '250 patent and is entitled to damages as provided for in 35 U.S.C. § 284, including reasonable royalty damages.

COUNT 2 – CLAIM FOR INFRINGEMENT OF THE '144 PATENT

45. Headwater incorporates by reference each of the allegations in the above paragraphs and further alleges as follows:

46. On July 17, 2018, the United States Patent and Trademark Office issued U.S. Patent No. 10,028,144, entitled "Security techniques for device assisted services." Ex. 2.

47. Headwater is the owner of the '144 patent with full rights to pursue recovery of royalties for damages for infringement, including full rights to recover past and future damages.

48. The written description of the '144 patent describes in technical detail each limitation of the claims, allowing a skilled artisan to understand the scope of the claims and how the nonconventional and non-generic combination of claim limitations is patently distinct from and improved upon what may have been considered conventional or generic in the art at the time of the invention.

49. Headwater and its predecessors in interest have satisfied the requirements of 35 U.S.C. § 287(a) with respect to the '144 patent because there are no unmarked articles subject to a duty to mark and Headwater is entitled to damages for Defendants' past infringement.

50. Defendants have directly infringed (literally and equivalently) and induced others to infringe the '144 patent by making, using, selling, offering for sale, or importing products that infringe the claims of the '144 patent and by inducing others to infringe the claims of the '144 patent without a license or permission from Headwater.

51. On information and belief, Defendants use, import, offer for sale, and sell certain infringing products in the United States. The Accused Instrumentalities are, for example, mobile electronic devices, including mobile phones and tablets.

52. For example, attached as Exhibit 4 is a chart setting forth a description of Defendants' infringement of claim 1 of the '144 patent.

53. Defendants also knowingly and intentionally induce and contribute to infringement of the '144 patent in violation of 35 U.S.C. §§ 271(b) and 271(c).

54. Despite this knowledge of the '144 patent, Defendants continue to actively encourage and instruct its customers to use and integrate the Accused Instrumentalities in ways that directly infringe the '144 patent. Defendants do so knowing and intending that their customers will commit these infringing acts. Defendants also continue to make, use, offer for sale, sell, and/or import the Accused Instrumentalities, despite their knowledge of the '144 patent, thereby specifically intending for and inducing its customers to infringe the '144 patent through the customers' normal and customary use of the Accused Instrumentalities.

55. Defendants have infringed multiple claims of the '144 patent, including independent claim 1. By way of example only, the normal and customary use of the mobile phones and tablets made, used, sold, offered for sale and/or imported by Defendants infringes an exemplary claim of the '144 patent, as in the description set forth in Exhibit 4, which Headwater provides without the benefit of information about the Accused Instrumentalities obtained through discovery.

56. Defendants have known how the Accused Instrumentalities are made and have known, or have been willfully blind to the fact, that making, using, offering to sell, and selling the Accused Instrumentalities to their customers, would constitute willful infringement of the '144

patent. Those products imported into and sold within the United States include, without limitation, Samsung Knox-enabled devices.

57. Defendants have induced, and continue to induce, infringement of the '144 patent by actively encouraging others (including its customers) to use, offer to sell, sell, and import the Accused Instrumentalities. On information and belief, these acts include providing information and instructions on the use of the Accused Instrumentalities; providing information, education and instructions to its customers; providing the Accused Instrumentalities to customers; and indemnifying patent infringement within the United States.

58. Headwater has been damaged by Defendant's infringement of the '144 patent and is entitled to damages as provided for in 35 U.S.C. § 284, including reasonable royalty damages.

JURY DEMAND

59. Headwater demands a jury trial pursuant to Federal Rule of Civil Procedure 38.

RELIEF REQUESTED

Headwater prays for the following relief:

A. A judgment in favor of Headwater that Defendants have infringed the Asserted Patents, and that the Asserted Patents are valid and enforceable;

B. A judgment and order requiring Defendants to pay Headwater past and future damages arising out of Defendants' infringement of the Asserted Patents in an amount no less than a reasonable royalty, costs, expenses, and pre- and post-judgment interest for its infringement of the asserted patents, as provided under 35 U.S.C. § 284;

C. A permanent injunction prohibiting Defendants from further acts of infringement of the Asserted Patents;

D. A judgment and order requiring Defendants to provide an accounting and to pay supplemental damages to Headwater, including, without limitation, pre-judgment and post-judgment interest;

E. A judgement that Defendants' infringement is willful and enhanced damages and fees as a result of that willfulness under 35 U.S.C. § 284;

F. A finding that this case is exceptional under 35 U.S.C. § 285, and an award of Headwater' reasonable attorney's fees and costs; and

G. Any and all other relief to which Headwater may be entitled.

Dated: August 2, 2024

Respectfully submitted,

/s/ Marc Fenster

Marc Fenster

CA State Bar No. 181067

Email: mfenster@raklaw.com

Reza Mirzaie

CA State Bar No. 246953

Email: rmirzaie@raklaw.com

Brian Ledahl

CA State Bar No. 186579

Email: bledahl@raklaw.com

Ben Wang

CA State Bar No. 228712

Email: bwang@raklaw.com

Paul Kroeger

CA State Bar No. 229074

Email: pkroeger@raklaw.com

Neil A. Rubin

CA State Bar No. 250761

Email: nrubin@raklaw.com

Kristopher Davis

CA State Bar No. 329627

Email: kdavis@raklaw.com

James S. Tsuei

CA State Bar No. 285530

Email: jtsuei@raklaw.com

Philip Wang

CA State Bar No. 262239

Email: pwang@raklaw.com

Amy Hayden

CA State Bar No. 287026

Email: ahayden@raklaw.com

Peter Tong

TX State Bar No. 24119042

Email: ptong@raklaw.com

James Pickens

CA State Bar No. 307474

Email: jpickens@raklaw.com

Jason M. Wietholter

CA State Bar No. 337139

Email: jwietholter@raklaw.com

RUSS AUGUST & KABAT

12424 Wilshire Blvd. 12th Floor

Los Angeles, CA 90025

Telephone: 310-826-7474

**ATTORNEYS FOR PLAINTIFF,
Headwater Research LLC**

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.

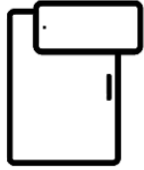
Claim 1

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.

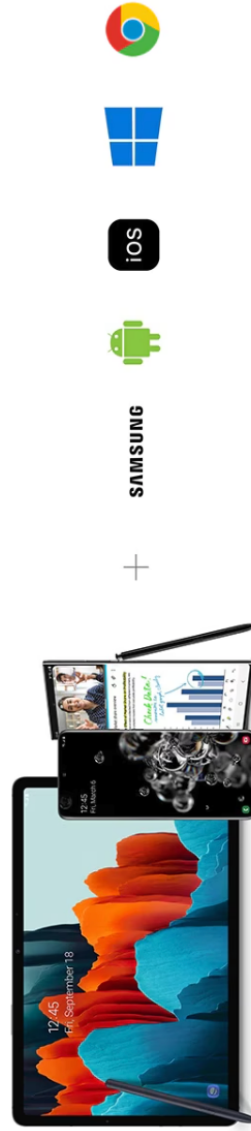


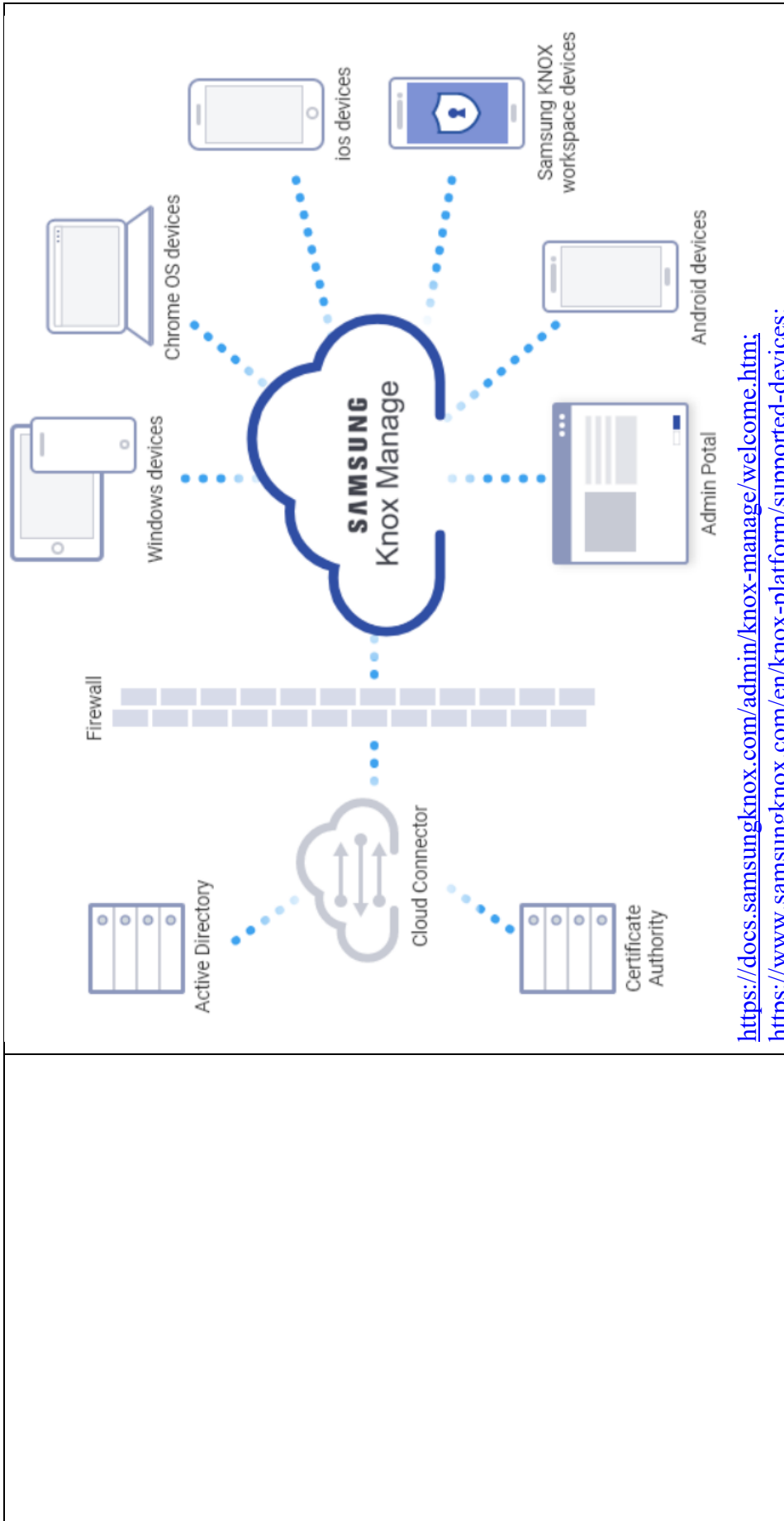
Works with Android Enterprise

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](#).





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.

FILTER 454 Result(s)

RESET FILTERS

Last updated: July 11, 2024

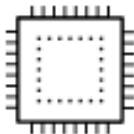
Feedback			
KNOX SOLUTIONS	DEVICE	MODEL CODE	PLATFORM/OS
Knox Suite ☐ Knox Platform for Enterprise ☐ Knox Mobile Enrollment ☐ Knox Manage ☐ Knox E-FOTA ☐ Knox Asset Intelligence ☐ Knox Capture ☐ Knox Authentication Manager ☐ Knox Configure ☐ Knox Guard	Galaxy A04s	SM-A047M, SM-A047F	Android - Secured by Knox
	Galaxy A13	SM-A137F, SM-A135N, SM-A135M, SM-A135F, SM-A135U1, SM-A135U	Android - Secured by Knox
	Galaxy A13 5G	SM-A136M, SM-A136B, SM-A136S	Android - Secured by Knox
	Galaxy A14	SM-A145MB, SM-A145FB	Android - Secured by Knox
	Galaxy A15	SM-A155F, SM-A155M, SM-A155N	Android - Secured by Knox
	Galaxy A15 5G	SM-A1560, SM-A156E, SM-A156M, SM-A156V, SM-A156U, SM-A156W, SM-A156U1, SM-A156B, SM-A156L	Android - Secured by Knox
	Galaxy A23	SM-A235F, SM-A235M, SM-A235N	Android - Secured by Knox
	Galaxy A23 5G	SM-A2360, SM-A236B, SM-A236M, SM-A236E, SM-A236V, SM-A236U1, SM-A236W, SM-A236U1, SM-A236B, SM-A236L	Android - Secured by Knox
	Galaxy A23 5G	SM-A2360, SM-A236B, SM-A236M, SM-A236E, SM-A236V, SM-A236U1, SM-A236W, SM-A236U1, SM-A236B, SM-A236L	Android - Secured by Knox
	Galaxy A23 5G	SM-A2360, SM-A236B, SM-A236M, SM-A236E, SM-A236V, SM-A236U1, SM-A236W, SM-A236U1, SM-A236B, SM-A236L	Android - Secured by Knox
OTHERS ☐ Knox Deployment App ☐ Knox DualDAR	Galaxy A23 5G	SM-A2360, SM-A236B, SM-A236M, SM-A236E, SM-A236V, SM-A236U1, SM-A236W, SM-A236U1, SM-A236B, SM-A236L	Android - Secured by Knox
	Galaxy A23 5G	SM-A2360, SM-A236B, SM-A236M, SM-A236E, SM-A236V, SM-A236U1, SM-A236W, SM-A236U1, SM-A236B, SM-A236L	Android - Secured by Knox
ANDROID ENTERPRISE RECOMMENDED			
Learn more			
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 Knox Configure Remotely configure Samsung devices in bulk and tailor them to specific needs, right out of the box WATCH VIDEO GET STARTED 
[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 WWAN; and	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. 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.” See, e.g., 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

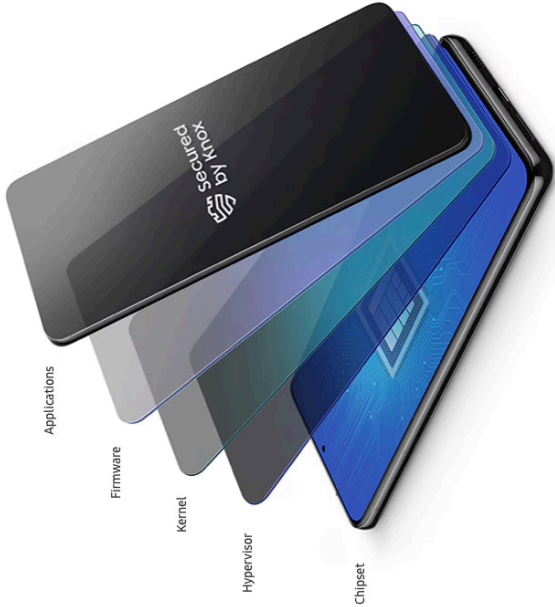
Periodic Kernel Measurement and Real-time Kernel Protection work to constantly inspect the core software of the OS, the kernel. These checks ensure that requests to bypass device security are blocked and sensitive data is protected.

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

<u>Build Trust</u>		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.

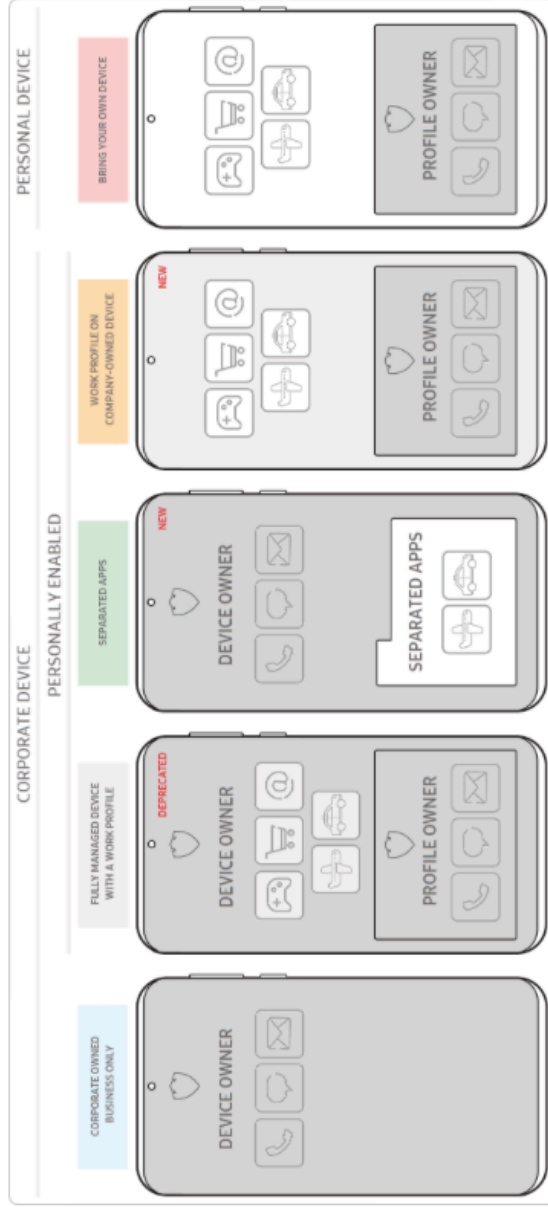
; <https://docs.samsungknox.com/admin/fundamentals/whitepaper/samsung-knox-for-android/core-platform-security/app-security/>;

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 T1, 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 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 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. *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://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 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](#).

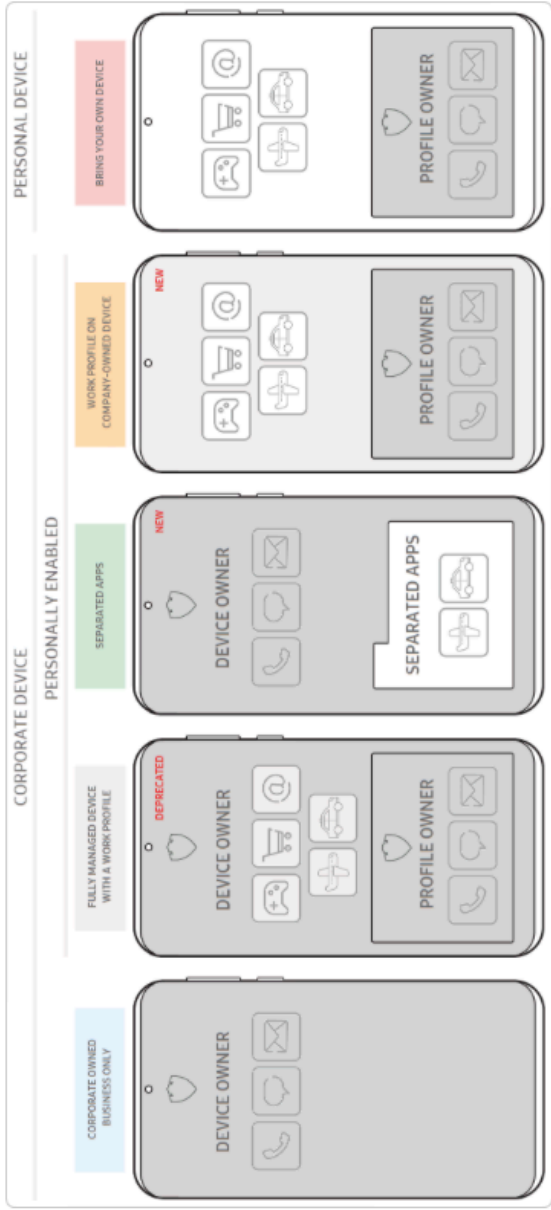
<https://docs.samsungknox.com/admin/fundamentals/whitepaper/samsung-knox-for-android/core-platform-security/app-security/> (describing “personal and work apps”):

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 T1, 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 though “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)

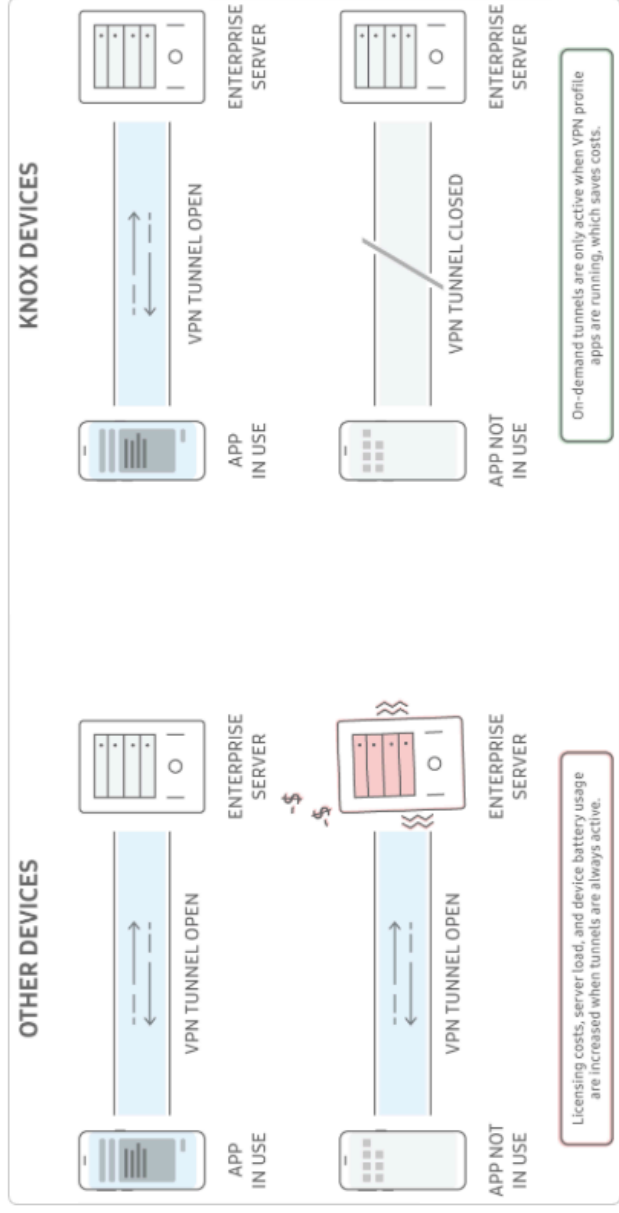
Last updated February 20th, 2024

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://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,. 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)

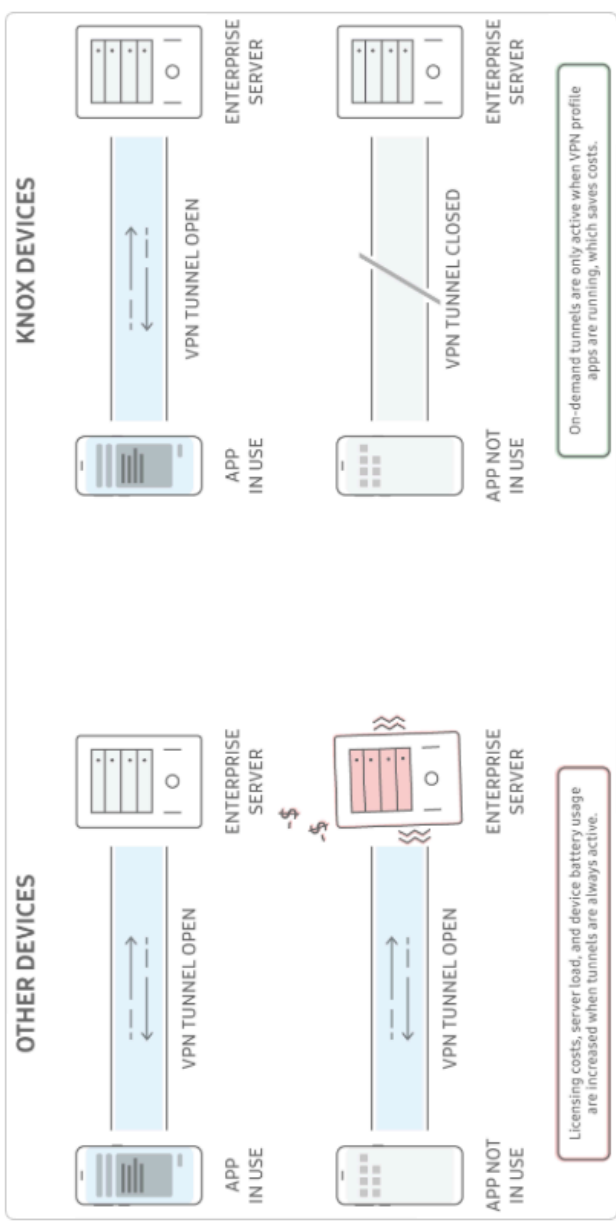
Last updated February 20th, 2024

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. ; 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

<u>Build Trust</u>	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.

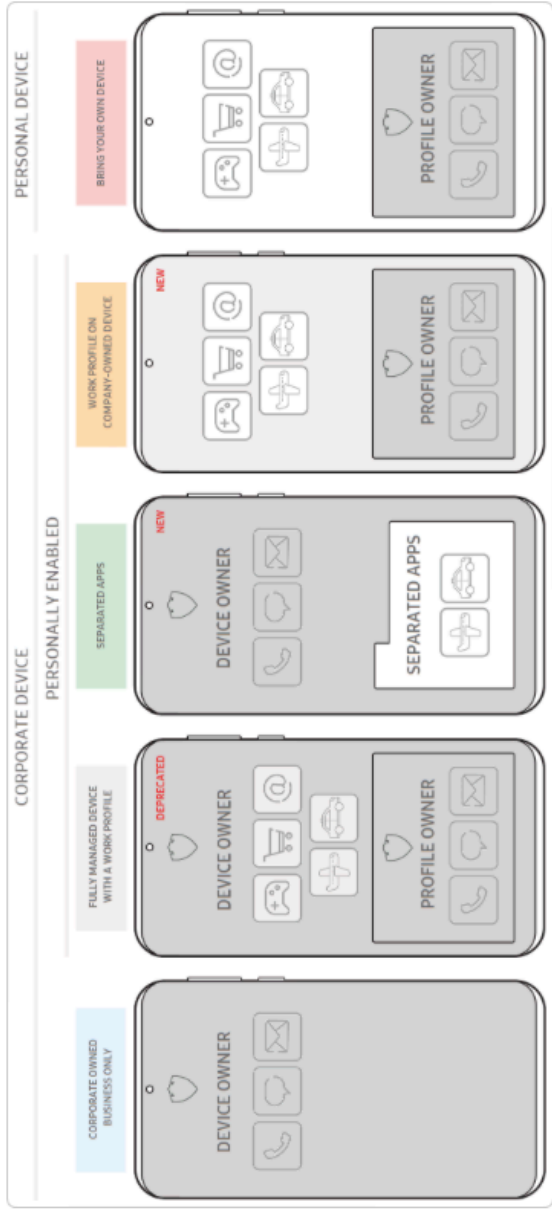
; <https://docs.samsungknox.com/admin/fundamentals/whitepaper/samsung-knox-for-android/core-platform-security/app-security/>;

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 T1, 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 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)

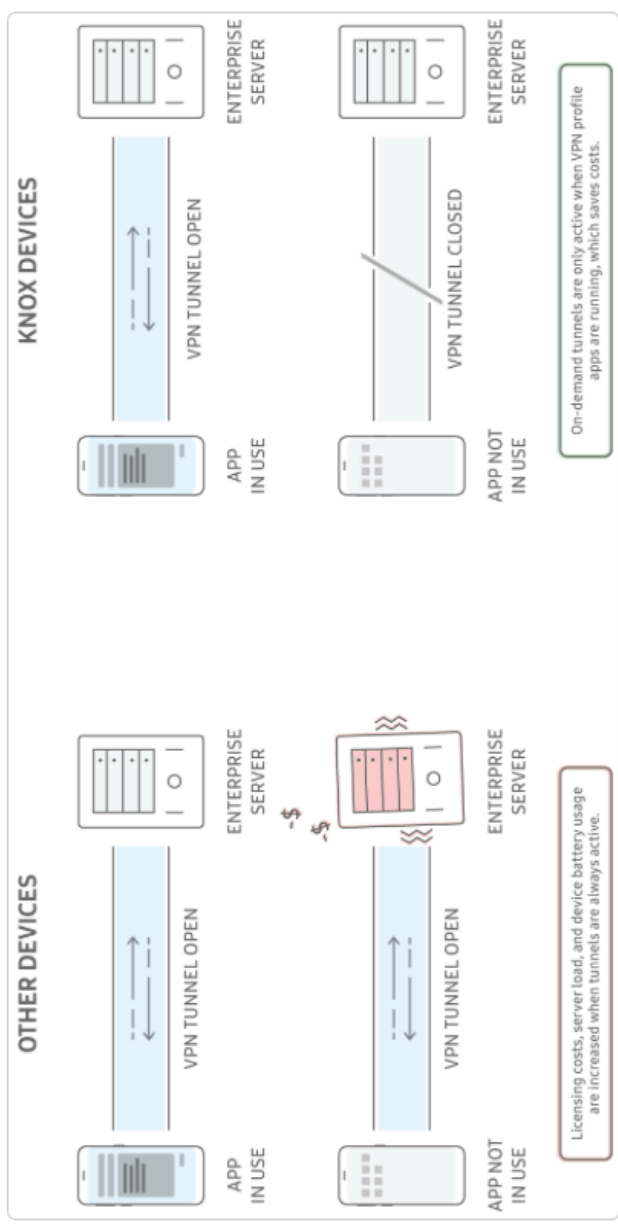
Last updated February 20th, 2024

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., https://source.android.com/docs/core/ota/modular-system/networking:</i> 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,. 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/>; <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/knox-platform-for-enterprise/knox-service-plugin/configure-advanced-policies/separated-apps/](https://docs.samsungknox.com/admin/fundamentals/whitepaper/samsung-knox-for-android/app-and-data-protection/enterprise-productivity-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 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 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 device agents executed in the protected execution partition."	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 Internet data packet 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.

73

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.

Exhibit B

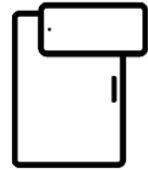
U.S. Patent No. 10,080,250 (“250 Patent”)

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 method of operating a wireless end-user device, the method comprising:	Samsung’s devices comprise “a wireless end-user device.” <i>See, e.g.,</i> Secured by Samsung Knox Rest easy with our unparalleled mobile protection, fortified by the impenetrable Knox Vault, as well as Knox Matrix, Samsung’s vision for multi-device security. https://www.samsung.com/us/smartphones/galaxy-s24/. 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/#.

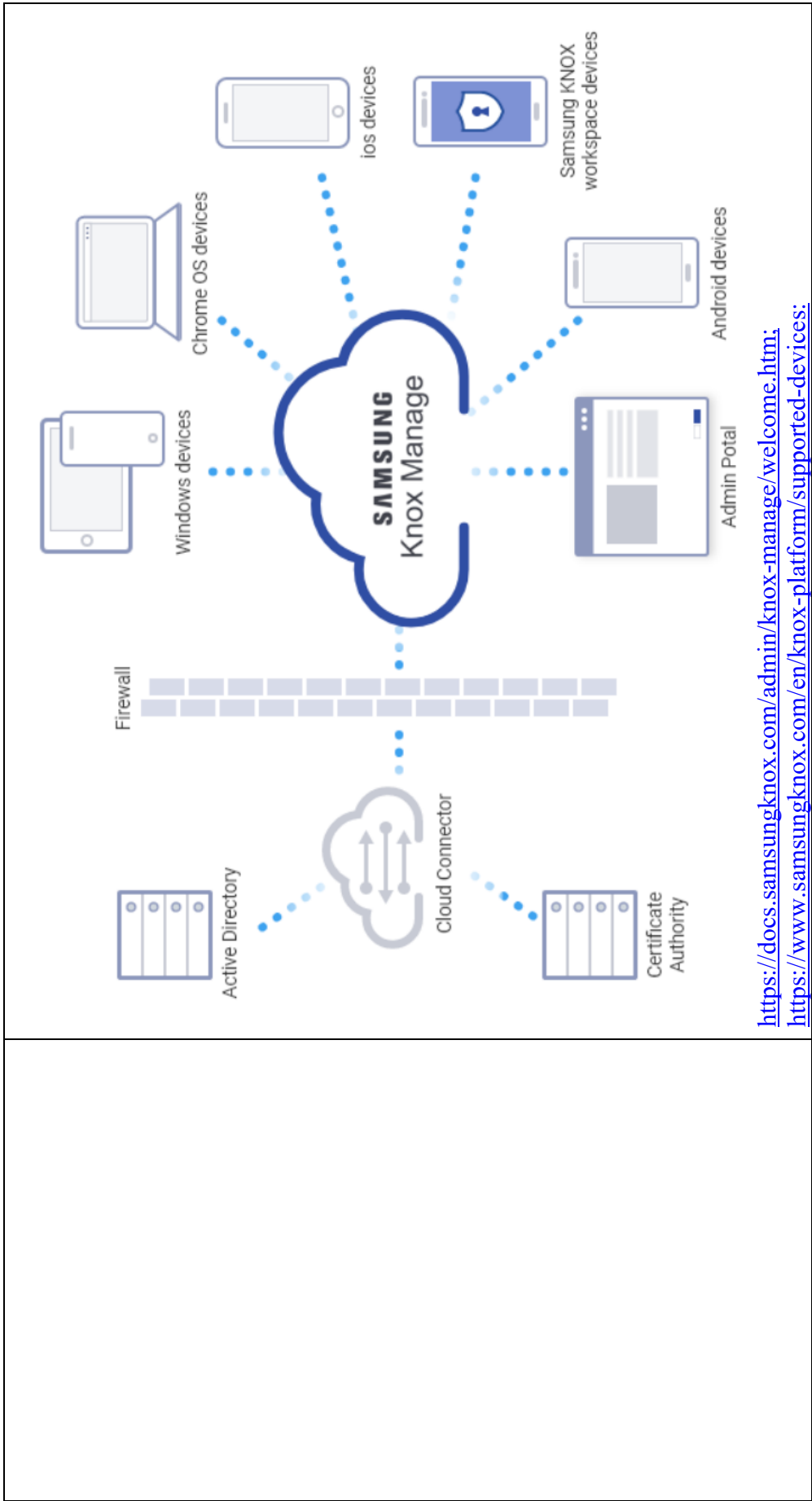
As a further example, Samsung’s devices operating in the Samsung Knox ecosystem are each “a wireless end-user device.” See, e.g., <https://www.samsung.com/us/business/solutions/services/mobility-software/knox-manage/>:

		
Event-based policies	Kiosk mode	Works with Android Enterprise
Manage devices based on pre-defined events—for instance, blocking access to cameras on employee phones during work hours.	Built-in tools help you set up devices in kiosk mode with no additional development work.	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-FOIA](#).





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.

Last updated: July 11, 2024

FILTER 454 Result(s)

RESET FILTERS

Feedback

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-A156Y, 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-A236U	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 Knox Configure Remotely configure Samsung devices in bulk and tailor them to specific needs, right out of the box WATCH VIDEO GET STARTED Feedback 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. Samsung devices perform the step of “storing secure policy information indicative of an application-specific execution environment policy and a configurable communication security policy.” As another example, Samsung’s devices run the Android Operating System, including Android Enterprise, which store secure policy information indicative of a configurable communication security policy (e.g., a configurable VPN policy, such as VPN options, including “Per-app VPN” settings). 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/;
[1a] storing secure policy information indicative of an application-specific execution environment policy and a configurable communication security policy;	

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`

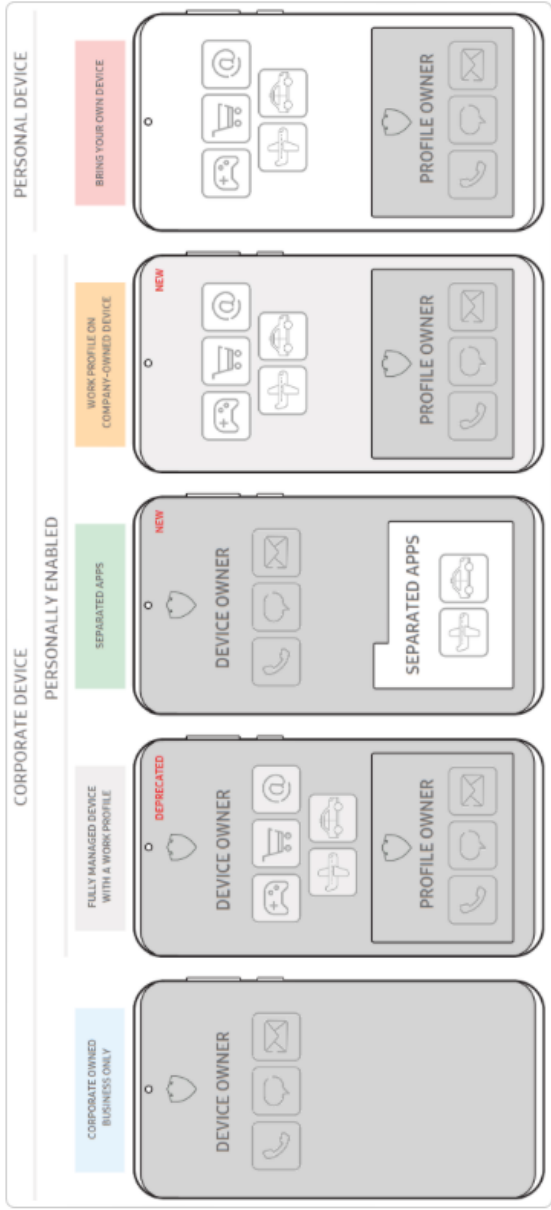
	https://developers.google.com/android/work/requirements; https://developers.google.com/android/work/requirements/work-profile; https://developers.google.com/android/work/requirements/work-profile-corporate; https://developers.google.com/android/work/requirements/fully-managed-device; https://developers.google.com/android/work/requirements/dedicated-device. For example, Samsung devices store secure policy information indicative of an application-specific execution environment policy (e.g., policies which result in “Separated Apps” or provide “App Isolation”). <i>See e.g.</i>, 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 T1, 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 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)

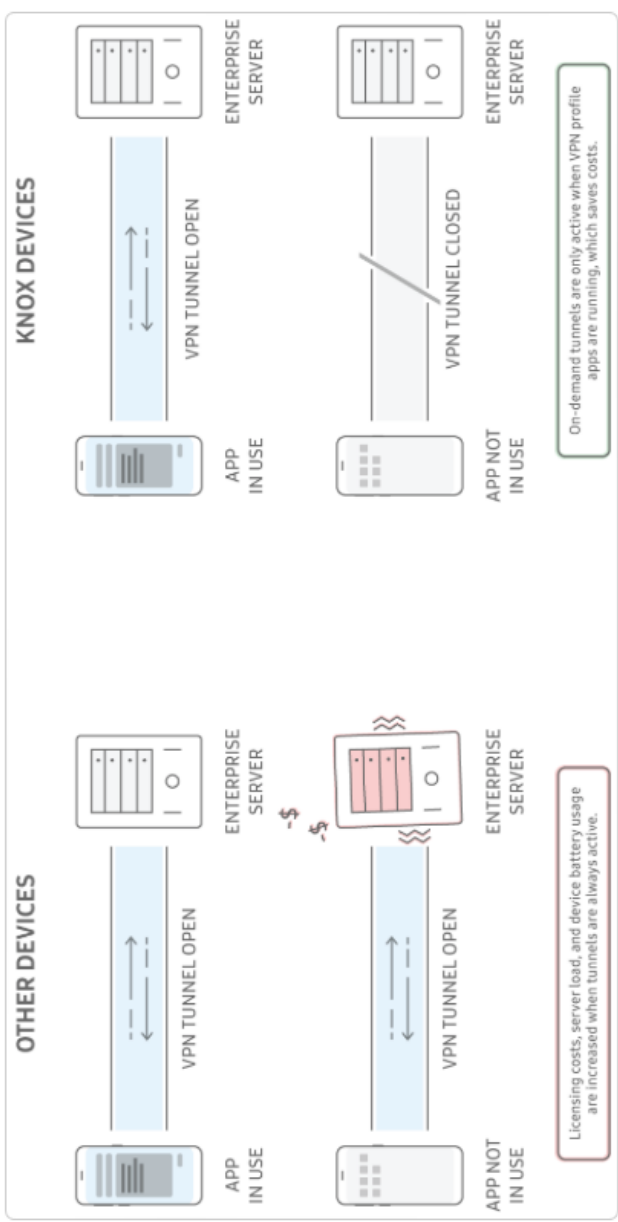
Last updated February 20th, 2024

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.
--	--

[1b] based on the secure stored information indicative of an application-specific execution environment policy, allowing a first set of multiple device application instances to run only in a first secure application environment on the wireless end-user device, and allowing a second set of device application instances to run only outside of the first secure application environment; and

Samsung devices perform the step of “based on the secure stored information indicative of an application-specific execution environment policy, allowing a first set of multiple device application instances to run only in a first secure application environment on the wireless end-user device, and allowing a second set of device application instances to run only outside of the first secure application environment.”

For example, Samsung’s devices run the Android Operating System, including Android Enterprise, allow a first set of multiple device application instances to run only in a first secure application environment on the wireless end-user device, (e.g., with “Work profiles”), and allowing a second set of device application instances to run only outside of the first secure application environment. 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>;

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>;
<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>.

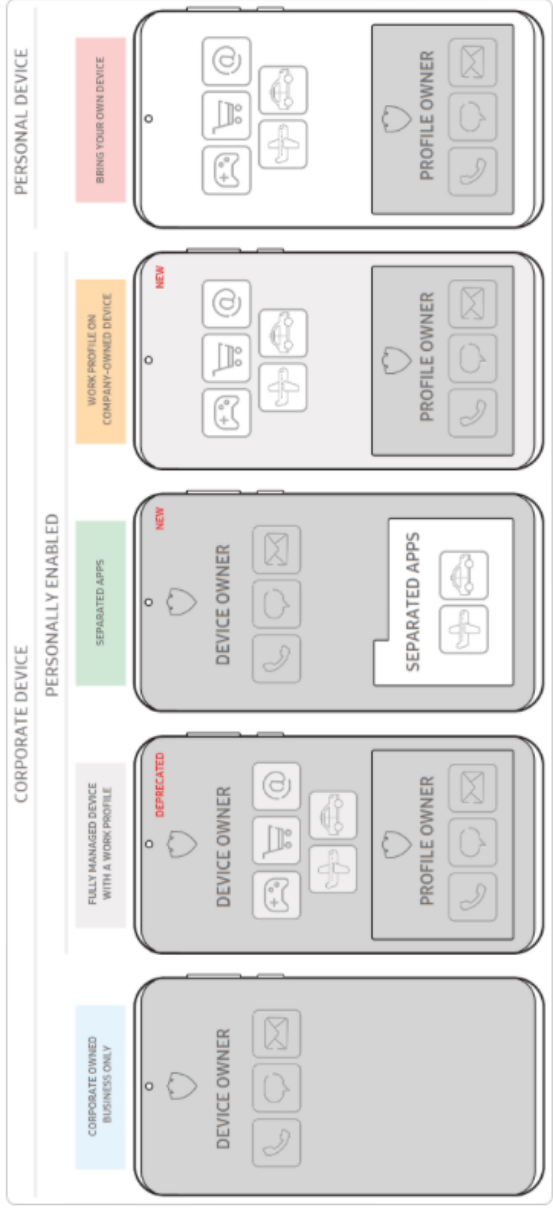
As another example, Samsung devices allowing a first set of multiple device application instances to run only in a first secure application environment on the wireless end-user device, (e.g., “Separated Apps” or “App Isolation”), and allowing a second set of device application instances to run only outside of the first secure application environment. See e.g., <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 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] based on the secure stored information indicative of a configurable communication security policy, initiate a first secure tunnel to a network tunnel endpoint, and direct all network data communications to and from device application instances executing in the	Samsung devices perform the step of “based on the secure stored information indicative of a configurable communication security policy, initiate a first secure tunnel to a network tunnel endpoint, and direct all network data communications to and from device application instances executing in the first secure application environment through the first secure tunnel.” For example, Samsung’s devices run the Android Operating System, including Android Enterprise, initiate a first secure tunnel to a network tunnel endpoint, and direct all network data communications to and from device application instances executing in the first secure

first secure application environment through the first secure tunnel.

application environment through the first secure tunnel (e.g., a configurable VPN policy, such as VPN options, including “Per-app VPN” settings). 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>;

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>.

For example, initiate a first secure tunnel to a network tunnel endpoint, and direct all network data communications to and from device application instances executing in the first secure application environment through the first secure tunnel (e.g., advanced VPN policies in Knox secure app-specific traffic secured through Knox VPNs). *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)

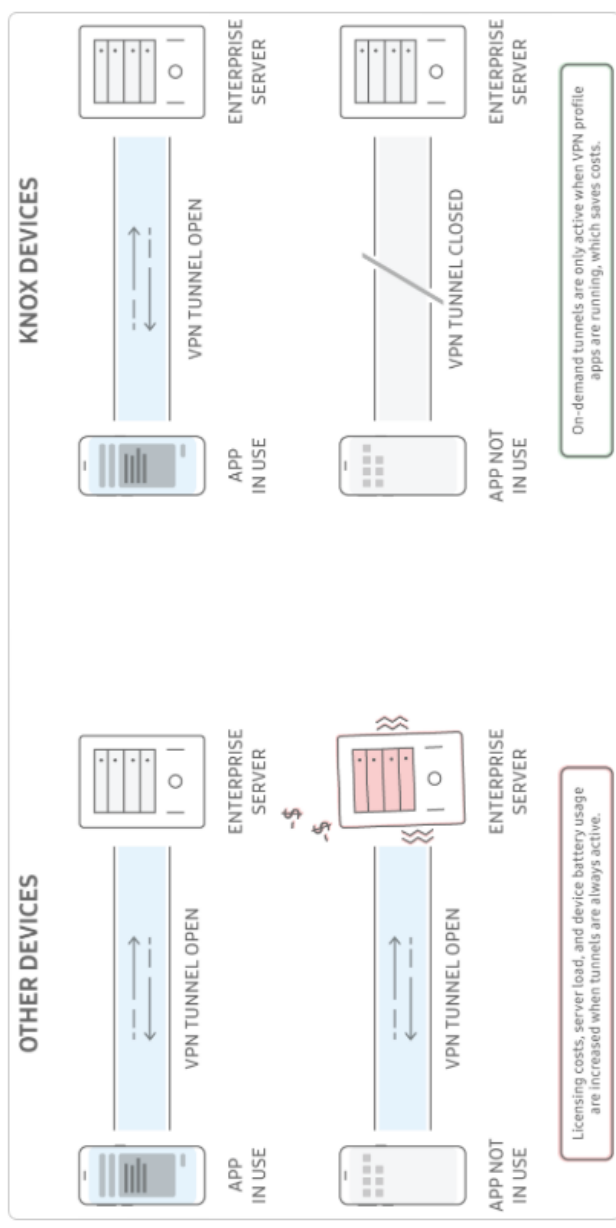
Last updated February 20th, 2024

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

	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 such as ultrasonic fingerprint sensors. Options are available for both device lockscreen authentication as well as work profile authentication. Through the Knox Platform, you can enforce two-factor authentication or enterprise AD credentials for the work profile to ensure stronger data protection. • Encryption of device data — Samsung Knox devices provide data encryption through Sensitive Data Protection, which 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 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. ; 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.
--	---

Claim 2

Issued Claim(s)	Public Documentation
2. The method of claim 1, wherein the configurable communication security policy defines a first configuration, which indicates that application instances in the second set of device application instances are not allowed to use the first secure tunnel, the method further comprising, based on the secure stored information indicative of a configurable communication security policy indicating the first configuration, directing all network data communications to and from device application instances executing outside of the first secure application environment through a network path outside of the first secure tunnel.”	Samsung devices perform steps of the method of claim 1. <i>See supra</i> claim 1. Samsung devices perform the step of “wherein the configurable communication security policy defines a first configuration, which indicates that application instances in the second set of device application instances are not allowed to use the first secure tunnel, the method further comprising, based on the secure stored information indicative of a configurable communications security policy indicating the first configuration, directing all network data communications to and from device application instances executing outside of the first secure application environment through a network path outside of the first secure tunnel.” For example, Samsung’s devices run the Android Operating System, including Android Enterprise, indicate applications in the second set of device application instances are not allowed to use the first secure tunnel (e.g., a configurable VPN policy, such as VPN options, including

executing outside of the first secure application environment through a network path outside of the first secure tunnel.

“Per-app VPN” settings). 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>;

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>.

For example, advanced VPN policies in Knox security indicate applications in the second set of device application instances are not allowed to use the first secure tunnel, such as by creating a VPN policy that specifies “which apps should use this VPN.” *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/ (“The flexibility to use a VPN tunnel for the entire device (work profile as well as fully managed device) or a single app only.”):
--	--

Virtual Private Networks (VPN)

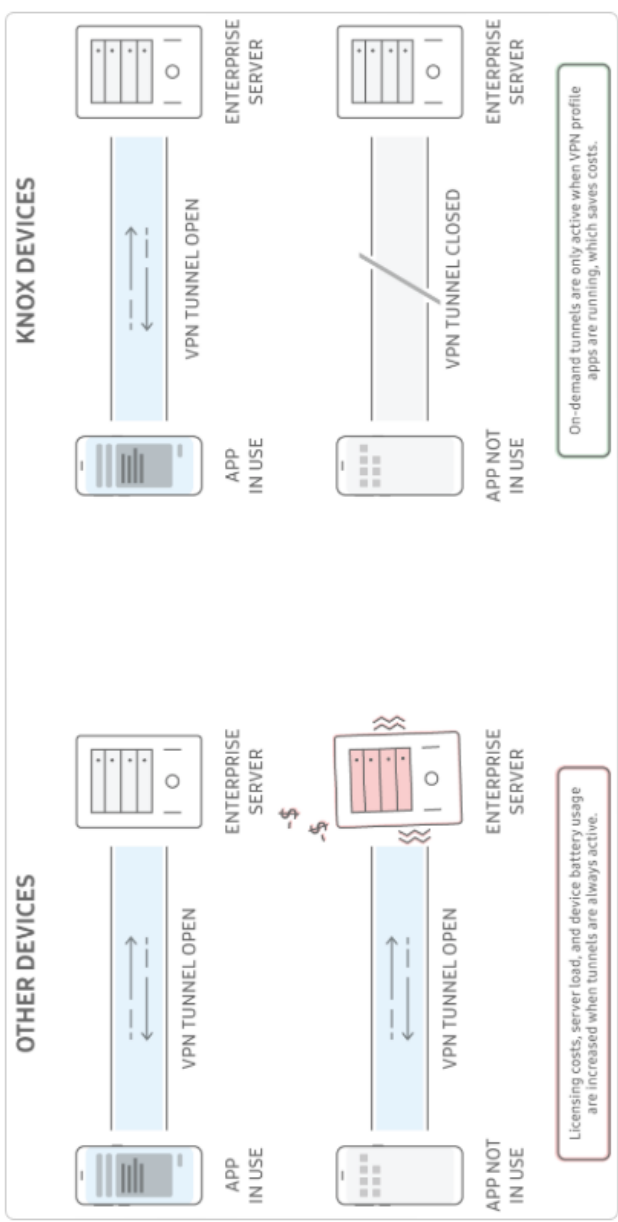
Last updated February 20th, 2024

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/fundamentals/whitepaper/samsung-knox-for-android/the-samsung-knox-platform/;
--	--

	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 such as ultrasonic fingerprint sensors. Options are available for both device lockscreen authentication as well as work profile authentication. Through the Knox Platform, you can enforce two-factor authentication or enterprise AD credentials for the work profile to ensure stronger data protection. • Encryption of device data — Samsung Knox devices provide data encryption through Sensitive Data Protection, which 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 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. ; 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. As a further example, advanced VPN policies in Knox security policies include multiple configurations, e.g., multiple policies, which direct network data communications to and from device application instances executing outside of the first secure application environment through a network path outside of the first secure tunnel, such as by creating a VPN policy that specifies “which apps should use this VPN.” 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/ (“The flexibility to use a VPN tunnel for the entire device (work profile as well as fully managed device) or a single app only.”):
--	---

Virtual Private Networks (VPN)

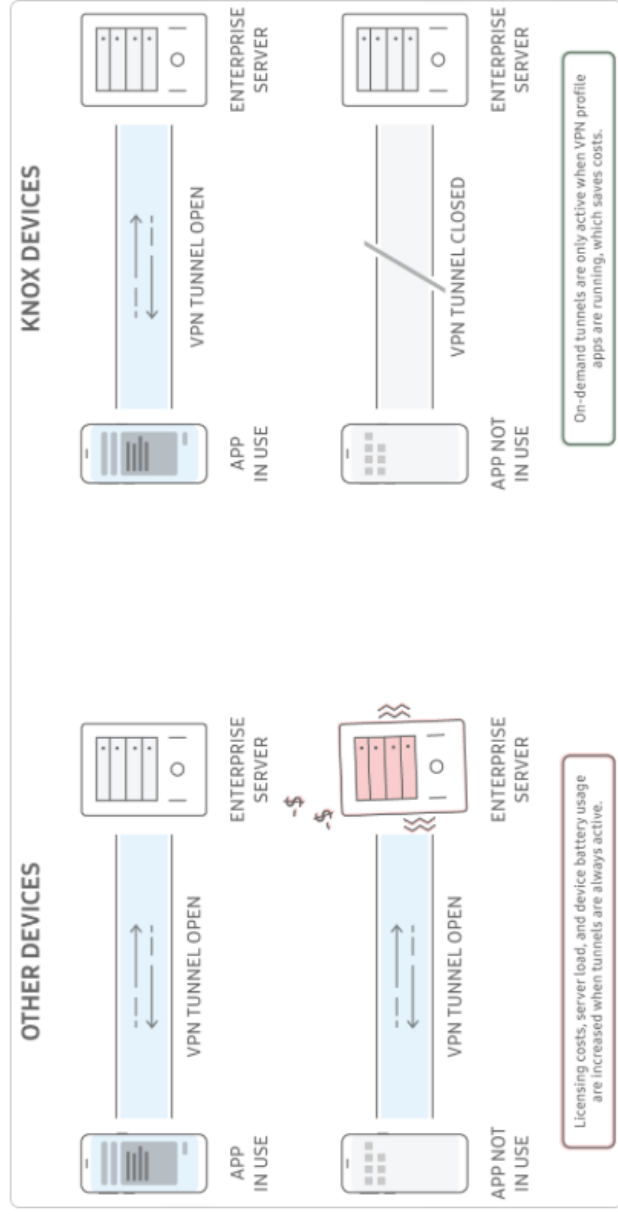
Last updated February 20th, 2024

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/fundamentals/whitepaper/samsung-knox-for-android/the-samsung-knox-platform/;
--	--

	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 such as ultrasonic fingerprint sensors. Options are available for both device lockscreen authentication as well as work profile authentication. Through the Knox Platform, you can enforce two-factor authentication or enterprise AD credentials for the work profile to ensure stronger data protection. • Encryption of device data — Samsung Knox devices provide data encryption through Sensitive Data Protection, which 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 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. ; 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.
--	---