

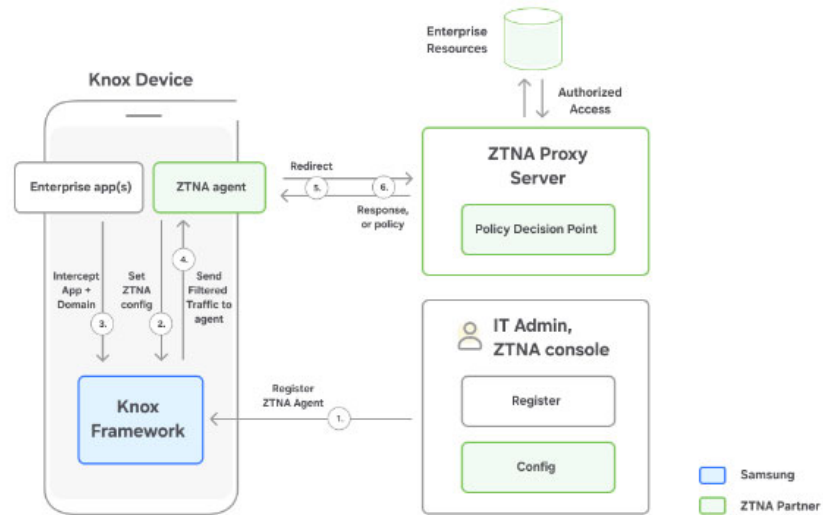
Exhibit 13

EXHIBIT 13 – U.S. Patent No. 8,224,794

Plaintiff asserts that the following products (“Accused Instrumentalities”) infringe the Asserted Claims of U.S. patent No. 8,224,794:

Any enterprise computer system that runs, executes, or uses Samsung’s Knox Suite, including the Knox Admin Portal (including the Knox Manage Portal and/or the Knox Guard Portal), the Knox Cloud Services (including Knox Mobile Enrollment (KME), Knox Manage, Knox Enterprise Firmware Over the Air (E-FOTA), Knox Asset Intelligence (KAI), Knox Configure, Knox Guard, Samsung Care+ for Business, Knox Managed Service Provider (MSP), and/or the Knox Deployment Program), and Knox Agent, and optionally including Knox Platform for Enterprise (KPE), Knox Remote Support, Knox Capture, Knox Authentication Manager, and/or the Knox Deployment Program (collectively, the “Accused Knox Products”).

Claim 20	Accused Knox Products
[20PRE] A clearinghouse system for communications networks, comprising:	<p>The Accused Knox Products constitute the claimed clearinghouse system for communications networks, because they provide a network management platform through a network communication interface for managing mobile devices that interact with an enterprise network.</p> <p>As evidenced herein, the Accused Knox Products enable intermediaries, such as information technology (IT) administrators for an enterprise using the Knox Suite, to deploy new or existing telecommunications assets (e.g., wireless devices of enterprise personnel) and determine where service and which service is best or more preferred to the end user, and to control the operation of such telecommunications assets for enhanced operation. According to the ’794 Patent, these features characterize a “clearinghouse system.” <i>See e.g.</i>, Col. 10, ll. 22-36. For example, the Accused Knox Products provide a central, computerized intermediary by which IT administrators can deploy, monitor, and manage end-user wireless devices connected to one or more communications network.</p>



Samsung Knox Documentation, Secure Remote Access,
<https://docs.samsungknox.com/admin/fundamentals/whitepaper/samsung-knox-mobile-security/network-security/secure-remote-access/> (last accessed September 2, 2025).

Advanced security requires, for example, that a phone support dual layers of encryption when data is at rest or in transit. Agencies and enterprises can satisfy this requirement with the KPE feature [Samsung DualDAR \(or Dual Data-at-Rest\)](#), which double-encrypts data inside a Galaxy device's work profile, using two independent crypto modules. Knox DualDAR also allows third-party crypto modules for inner-layer encryption. **For dual-layered encryption of data in transit, Knox enables Secure Wi-Fi access even on public networks.** These details make Samsung one of the most secure mobile phone providers and the only one to address requirements like CSfC and EUD to the letter.

Good management is part of strong security, so KPE includes deep customization options. These allow businesses to streamline their device deployments, with the added flexibility of granular device management and enforceable app management capabilities. By integrating with Managed Google Play, for example, IT admins can [allowlist and blocklist](#) specific apps for specific users.

Samsung Knox 101: Understanding Samsung's mobile security platform,
<https://insights.samsung.com/2024/08/28/samsung-knox-101-understanding-samsungs-mobile-security-platform-2/>

The Knox Service Guide v3.05 describes Knox Manage (formerly, Knox Enterprise Mobility Management (EMM)), as a platform that includes an EMM console that allows IT administrators to manage mobile devices enrolled with Knox Manage. Knox Service Guide v3.05, p. 7. The Knox Manage Client (e.g., application) is deployed to managed mobile devices when they are enrolled with Knox Manage. Knox Service Guide v3.05, p. 5. In one example, the managed mobile device can be configured, through the EMM application, to report device location information to the EMM console. *See* <https://image-us.samsung.com/SamsungUS/samsungbusiness/pdfs/Samsung-KNOX-QuickStarts-3v05.pdf> ("Knox Service Guide v3.05")

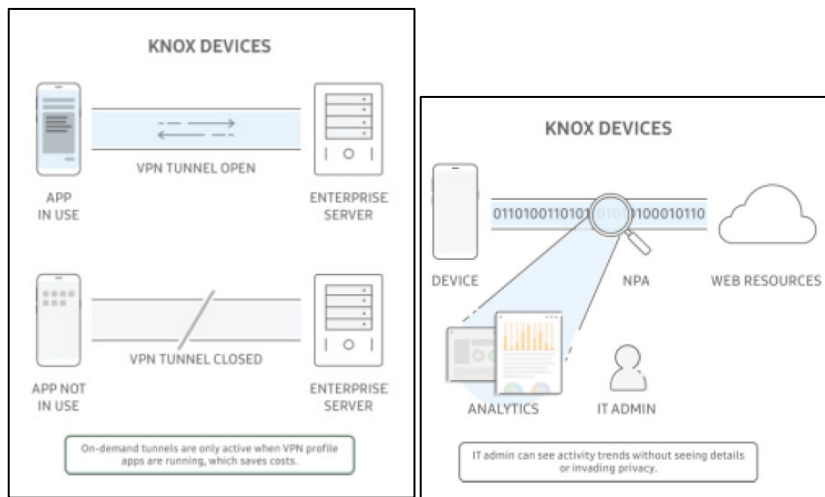
2.7. Device Policy Creation

Device policies are deployed when a device is enrolled in Knox Manage or can be pushed automatically to devices. Knox Manage implements a hierarchy policy set that allows policies to be deployed to all users, while other policies can then be deployed to a subset of users based on your business need. Some of the policies that can be configured include allowing users to use the camera, **configure the device to report the devices location within the EMM console**, and allowing users to wipe devices.

Knox Service Guide v3.05, p. 7 (annotated).

Samsung published several documents outlining the functionality of Knox Suite, including user guides, promotional documents, and white papers. The figures below, from Samsung Knox White Paper v1.5, show the network communication interface that allows for the secure transfer of information between the managed mobile devices and enterprise servers on the enterprise network.

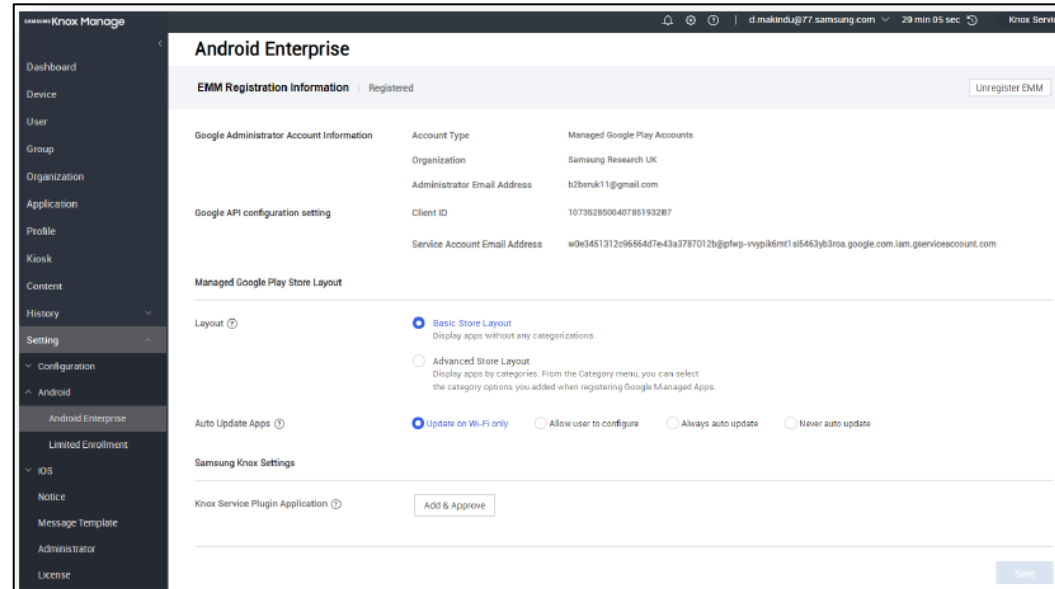
See <https://image-us.samsung.com/SamsungUS/samsungbusiness/solutions/topics/iot/071421/Knox-Whitepaper-v1.5-20210709.pdf> (“Knox White Paper v1.5”)



Knox White Paper v1.5, pp. 35 (left), 37 (Right).

The image below shows the EMM console of Knox Manage that allows the IT administrators to enroll, configure, manage, or review information associated with the managed mobile devices.

See <https://docs.samsungknox.com/admin/knox-platform-for-enterprise/assets/knox-manage-knox-platform-for-enterprise-guide-v3.0.pdf> (“Samsung Knox Manage 22.5”)



Samsung Knox Manage 22.5, p. 8

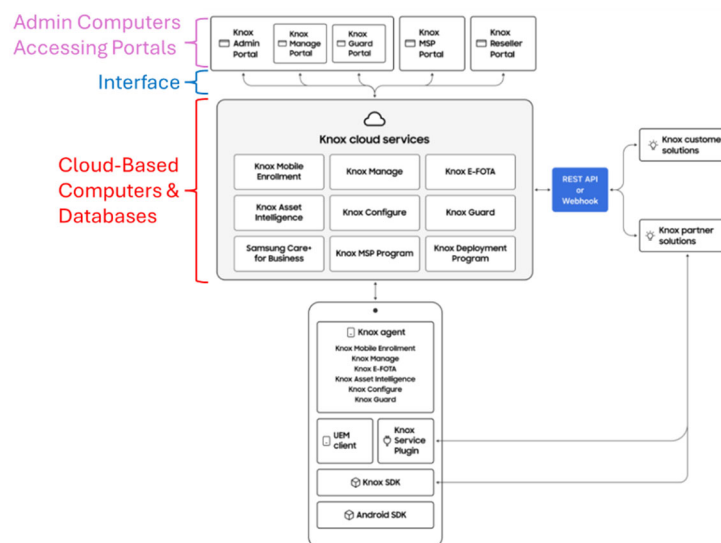
[20A] one or more computers which interface with a database, the database including performance or quality of service

The Accused Knox Products include and/or utilize one or more computers which interface with a database, the database including performance or quality of service information for one or more specific locations and one or more of records for one or more telecommunications carriers which identify infrastructure and location information for one or more specific locations, records for one or more end users which identify telecommunications assets or property assets owned or controlled by said one or more end users, and public records which include, for a plurality of geographic locations, one or more of mapping information for said geographic locations, zoning information for said geographic locations, local ordinances for said geographic

information for one or more specific locations, and one or more of records for one or more telecommunications carriers which identify infrastructure and location information for one or more specific locations, records for one or more end users which identify telecommunications assets or property assets owned or controlled by said one or more end users, and public records which include, for a plurality of geographic locations, one or more of mapping information for said geographic locations, zoning

locations, contact information for government officials for said geographic locations, and information about carriers serving said geographic locations.

For example, the Accused Knox Products include and/or utilize IT administrator's computers that access the Knox Admin Portal, which includes one or more web-based portals that interface with one or more cloud-based computers and databases of the Knox Cloud Services. According to Samsung, "[w]ith Knox Cloud Services, enterprise IT administrators can access a range of device management, monitoring, security, and customization solutions for their fleet of devices." Samsung Knox Documentation, Fundamentals, Introduction, the Big Picture, <https://docs.samsungknox.com/dev/fundamentals/> (last accessed September 2, 2025).



Samsung Knox Documentation, Fundamentals, Introduction, the Big Picture, <https://docs.samsungknox.com/dev/fundamentals/> (last accessed September 2, 2025) (annotated).

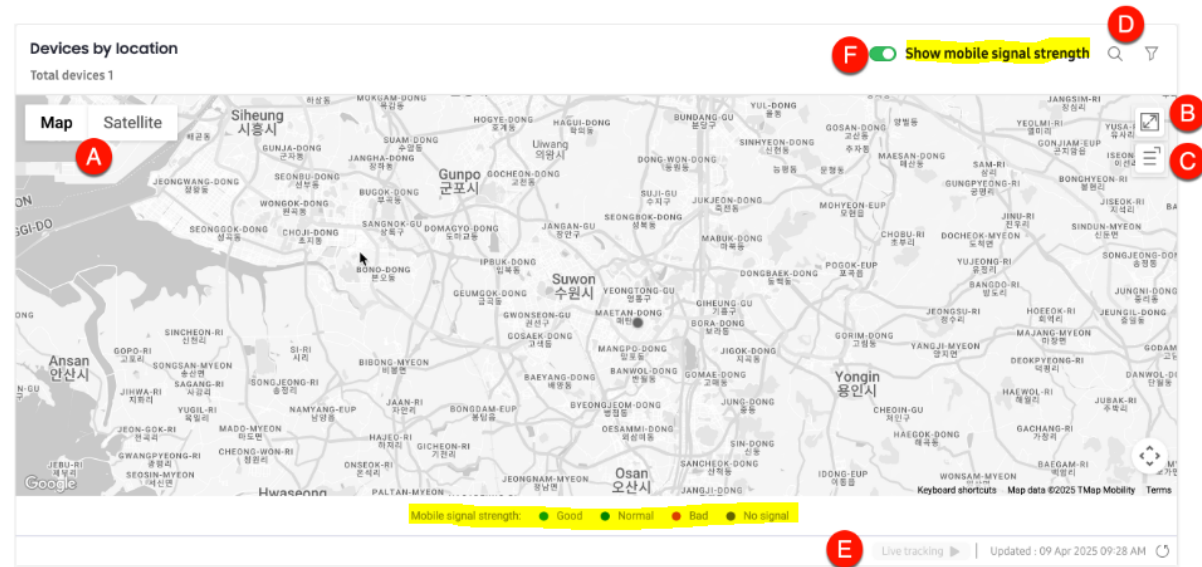
The Accused Knox Products provide "[s]torage of device analysis data," to facilitate "[r]eal-time monitoring of devices," "[s]upport for audits that verify system events, applied policies, tampering and compliance violations," and "[s]upport for appropriate actions after audit." Samsung Knox Documentation, Knox Manage, Introduction, Features and key strengths, <https://docs.samsungknox.com/admin/knox-manage/introduction/features-and-key->

<p>information for said geographic locations, local ordinances for said geographic locations, contact information for government officials for said geographic locations, and information about carriers serving said geographic locations;</p>	<p>strengths/#:~:text=Effortless%20content%20management,Storage%20of%20device%20analysis%20data (last accessed September 2, 2025).</p> <p>Storage of device analysis data</p> <p>In addition to real-time monitoring of devices, Knox Manage also provides audits. You can verify the events that occur in the system, the policies that were applied, any tampering and compliance violations, and so on, and take appropriate actions against them.</p> <ul style="list-style-type: none"> • Real-time monitoring of devices. • Support for audits that verify system events, applied policies, tampering and compliance violations and so on. • Support for appropriate actions after audit. <p>Samsung Knox Documentation, Knox Manage, Introduction, Features and key strengths, https://docs.samsungknox.com/admin/knox-manage/introduction/features-and-key-strengths/#:~:text=Effortless%20content%20management,Storage%20of%20device%20analysis%20data (last accessed September 2, 2025).</p> <p>The Accused Knox Products, for example, capture “mobile signal strength” data (a type of performance or quality of service information for one or more specific locations), which enables the identification of “devices situated in areas with weak cellular coverage or potential dead zones.” Samsung Knox Documentation, Knox Asset Intelligence, Dashboard, Location dashboard, Use location dashboard, https://docs.samsungknox.com/admin/knox-asset-intelligence/dashboard/location-dashboard/use-the-location-dashboard/#:~:text=To%20use%20this%20feature%2C%20you,next%20to%20the%20Search%20icon (last accessed September 2, 2025).</p>
---	--

	<p>F Mobile signal strength Let's you identify when devices are situated in areas with weak cellular coverage or potential dead zones. To use this feature, you must first enable Mobile signal strength with location.</p> <p>On the map, you'll see the mobile signal strength status of every device in your fleet represented by colored dots. These dots are updated at the same rate as your location data collection frequency.</p> <ul style="list-style-type: none"> • Good (green): -70 dBm or higher • Normal (blue): -71 dBm to -80 dBm • Bad (red): -81 dBm to -139 dBm • No signal (grey): -140 dBm or lower, no collection <p>These dots also appear in the map's Device list, letting you quickly correlate the device IDs with each mobile signal strength status. If you want to only show devices with a specific status—for example, only show Bad devices—you can select the status using the map's Filter options next to the Search icon.</p> <p>Samsung Knox Documentation, Knox Asset Intelligence, Dashboard, Location dashboard, Use location dashboard, https://docs.samsungknox.com/admin/knox-asset-intelligence/dashboard/location-dashboard/use-the-location-dashboard/#:~:text=To%20use%20this%20feature%2C%20you,next%20to%20the%20Search%20icon (last accessed September 2, 2025).</p> <p>The Accused Knox Products further provide admin interfaces, via dashboards (e.g., location dashboards) that include maps of device distributions for enterprise end user devices across a given area. Mobile signal strength data can be displayed via such maps, which enables IT administrators to quickly correlate device IDs with each mobile signal strength statuses. This further illustrates how the Accused Knox Products utilize performance or quality of service information associated with specific locations. See Samsung Knox Documentation, Knox Asset Intelligence, Dashboard, Location dashboard, Use location dashboard, https://docs.samsungknox.com/admin/knox-asset-intelligence/dashboard/location-dashboard/use-the-location-dashboard/#:~:text=To%20use%20this%20feature%2C%20you,next%20to%20the%20Search%20icon (last accessed September 2, 2025).</p>
--	---

Location map

The map displays your device groupings (represented by gray circles on the map) as soon as you open the **Location** dashboard. When you zoom in, the circles updates to show the device distribution across a given area.



Samsung Knox Documentation, Knox Asset Intelligence, Dashboard, Location dashboard, Use location dashboard, <https://docs.samsungknox.com/admin/knox-manage/introduction/features-and-key-strengths/#:~:text=Effortless%20content%20management,Storage%20of%20device%20analysis%20data> (last accessed September 2, 2025).

The Accused Knox Products further capture records for one or more end users which identify telecommunications assets or property assets owned or controlled by said one or more end users. For example, the Accused Knox Products enable enterprises and, specifically, IT administrators, to “efficiently manage [a] fleet of mobile devices” owned or controlled by end users, or workforce personnel employed by the enterprise. Samsung, Home, Mobile Security, “How can Knox Manage secure your growing mobile fleet,” Jo Harder, Dec. 13, 2021, <https://insights.samsung.com/2021/12/13/how-can-knox-manage-secure-your-growing-mobile-fleet-2/> (last accessed September 2, 2025). These devices can either be enterprise or employee owned under a Bring Your Own Device program but are nonetheless controlled by the employees during their course of business. *See*

Samsung, Home, Mobile Security, “How can Knox Manage secure your growing mobile fleet,” Jo Harder, Dec. 13, 2021, <https://insights.samsung.com/2021/12/13/how-can-knox-manage-secure-your-growing-mobile-fleet-2/> (last accessed September 2, 2025).

Simplifying mobile management for small businesses

EMM solutions like Samsung's Knox Manage provide a cloud-based command center to efficiently manage your fleet of mobile devices. Once enrolled, devices are configured to a profile that you determine based on your security and workforce productivity needs. The status of all devices can be monitored and issues flagged within the console. If a device is lost or stolen, it can be remotely locked or wiped of data to ensure confidential information does not fall into the wrong hands.

EMM takes MDM to a higher level by enabling IT admins to apply a wide variety of management controls and protections, from disallowing corporate app access over Wi-Fi connections to enforcing biometric or multifactor authentication, providing GPS tracking and more.

Knox Manage can control the device and user interactions at a granular level based on predetermined profiles, such as disallowing screen capture from healthcare applications that would violate company and regulatory requirements. The platform generates alerts such as failed upgrades of containerized applications, while monitoring and reporting capabilities enable administrators to track numerous data points for forensic evaluation and compliance based on devices, users or groups.

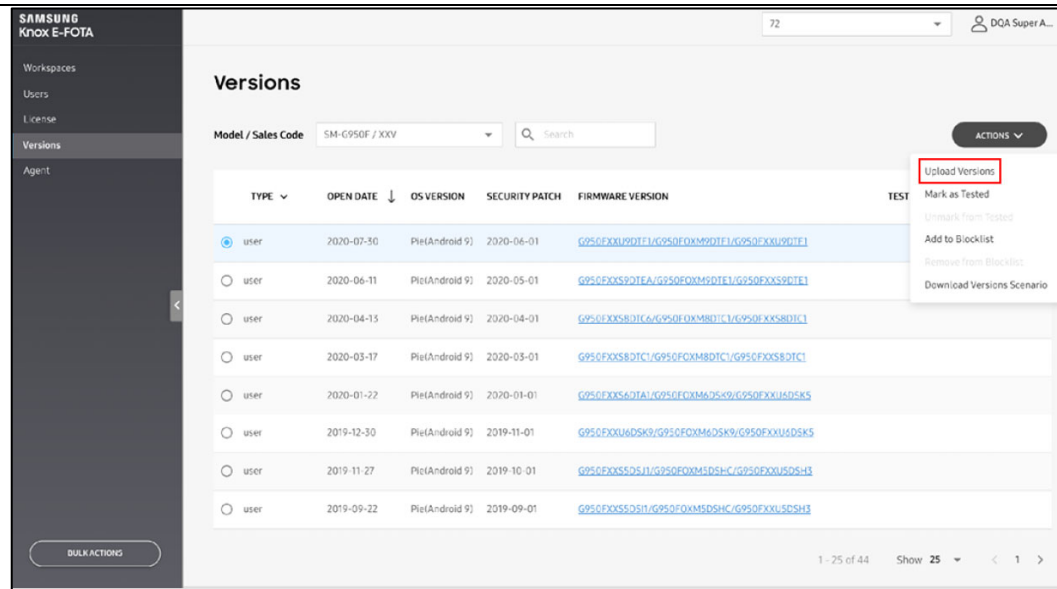
Samsung, Home, Mobile Security, “How can Knox Manage secure your growing mobile fleet,” Jo Harder, Dec. 13, 2021, <https://insights.samsung.com/2021/12/13/how-can-knox-manage-secure-your-growing-mobile-fleet-2/> (last accessed September 2, 2025).

The asset-identifying records used by the Accused Knox Products can include asset-specific information, such as device identifiers, device groups, models, status, permissions, battery status, battery health, device health, firmware versioning information, data usage, total connected time, etc. *See e.g.*, Samsung, Home, Knox Asset

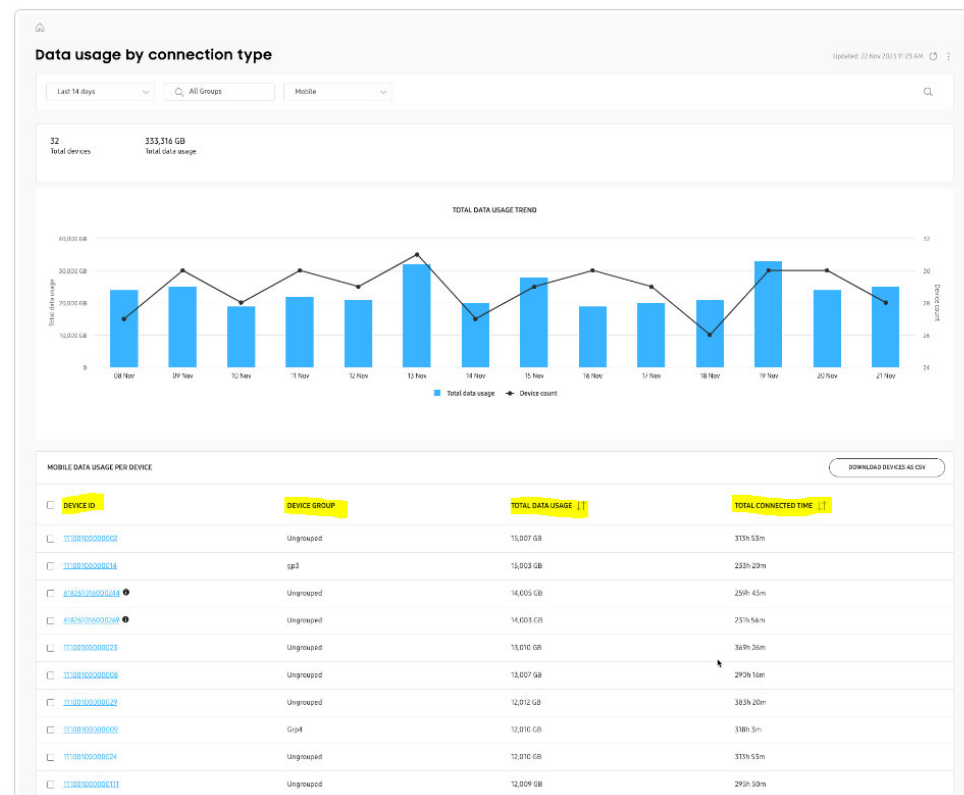
Intelligence, How-to guides, Manage devices, <https://docs.samsungknox.com/admin/knox-asset-intelligence/how-to-guides/manage-devices/> (last accessed September 2, 2025).

Column	Description
DEVICE ID	The device's unique International Mobile Equipment Identity (IMEI) number. If the device supports two SIMs, only the primary IMEI is shown. This column is always displayed.
DEVICE GROUP	The name of the group the device belongs to. Displays Ungrouped if no group configured.
MODEL	The device's model number.
STATUS	The device's current enrollment status: <ul style="list-style-type: none"> • Not enrolled: The device hasn't been enrolled in Knox Asset Intelligence. • Active: The device is enrolled and currently communicating with the Knox Asset Intelligence server. • Inactive: The device is enrolled but not currently communicating with the Knox Asset Intelligence server.
PERMISSIONS	Indicates whether the device has granted location permissions. If location permissions aren't granted, you can send a permission request by clicking ACTIONS > Send permission notification. <p>If your devices are running Android 12 or higher, permissions are granted differently based on your device management mode.</p> <ul style="list-style-type: none"> • On fully managed devices, EMMs can pre-grant location permissions during enrollment. • On company-owned devices with a work profile, the device users must manually grant location permissions before Knox Asset Intelligence can collect location data from the device. If the user denies this permission, then location data cannot be collected.
BATTERY STATUS	Indicates the device's current battery charge status. Available values: <ul style="list-style-type: none"> • Low battery: The device's battery level is below the allowable threshold. • Charging: The device is connected to a battery charger. • Consuming: The device is discharging its battery. • Fully charged: The device's battery is fully charged.
BATTERY HEALTH	Provides a summary of your device fleet's overall battery condition and how much of its original charge the battery can hold, as well as the raw battery state of health value (in brackets). Available values: <ul style="list-style-type: none"> • Good: The device battery is holding its original charge. • Normal: The device battery is holding most of its original charge. • Weak: The device battery has deteriorated from repeated charging. You should consider replacing the battery when possible. • Bad: The device battery has deteriorated, but the device was not used or charged frequently. Battery replacement is strongly recommended.
DEVICE HEALTH	Provides a health score for your device, letting you know if it is operating optimally, or if it requires attention. See Device health for additional information. Available values: <ul style="list-style-type: none"> • Good: Your device health is 90.00 or higher. • Normal: Your device health is between 80.00 and 90.00. • Bad: Your device health is lower than 80.00.

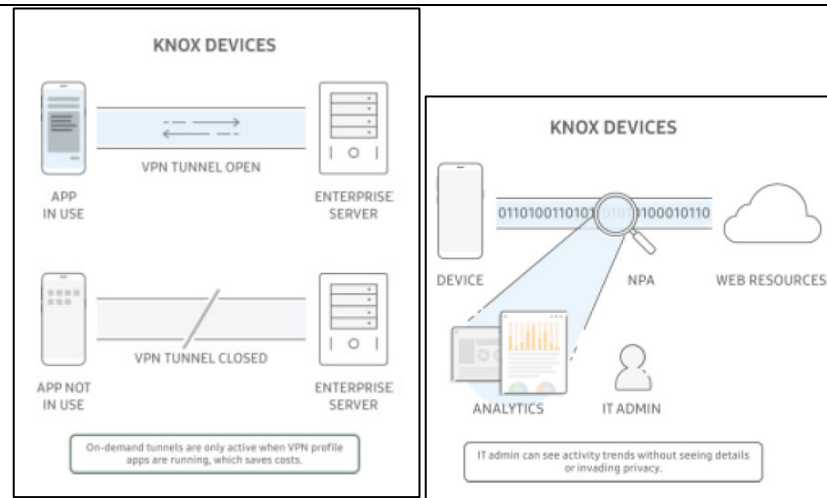
Samsung, Home, Knox Asset Intelligence, How-to guides, Manage devices, <https://docs.samsungknox.com/admin/knox-asset-intelligence/how-to-guides/manage-devices/> (last accessed September 2, 2025).



Knox E-FOTA On-Premises Admin Guide, p. 15, <https://docs.samsungknox.com/admin/efota-one/assets/knox-efota-on-premises-admin-guide.pdf> (last accessed September 2, 2025).

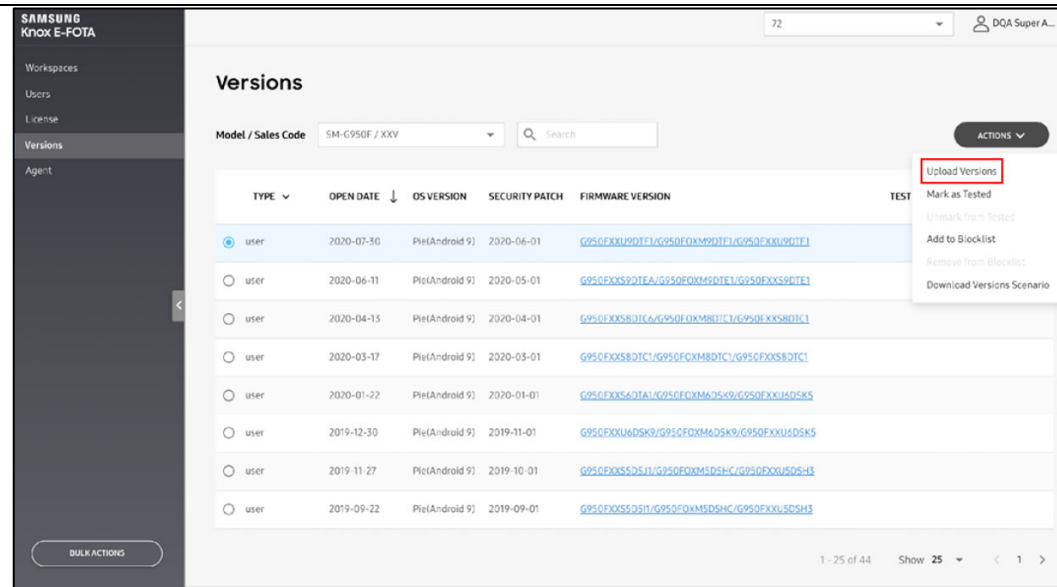


Samsung, Home, Knox Asset Intelligence, Dashboard, Network insights, Data usage by connection type, Expanded view, <https://docs.samsungknox.com/admin/knox-asset-intelligence/dashboard/network-insights/data-usage-by-connection-type/> (last accessed September 2, 2025).



Knox White Paper v1.5, <https://image-us.samsung.com/SamsungUS/samsungbusiness/solutions/topics/iot/071421/Knox-Whitepaper-v1.5-20210709.pdf>, pgs. 35 and 37 (last accessed September 2, 2025).

The Accused Knox Products provide a network communication interface between an IT administrator through the EMM console and the EMM client on the managed mobile devices. The EMM console network communication interface provides a front-end interface for an IT administrator to manage, configure, and review information associated with managed mobile devices. The figure below shows the EMM console which provides a front-end interface for the IT administrator on a first computer device to review a database of mobile device profiles. The figure below, from Samsung's Knox E-FOTA On-Premises Admin Guide, shows a database of information corresponding to each mobile device managed by an employer. In this example, the EMM console accesses device information from a Knox database for user type, operating system version, security patch version, and firmware version for the managed mobile devices.



Knox E-FOTA On-Premises Admin Guide, p. 15, <https://docs.samsungknox.com/admin/efota-one/assets/knox-efota-on-premises-admin-guide.pdf> (last accessed September 2, 2025).

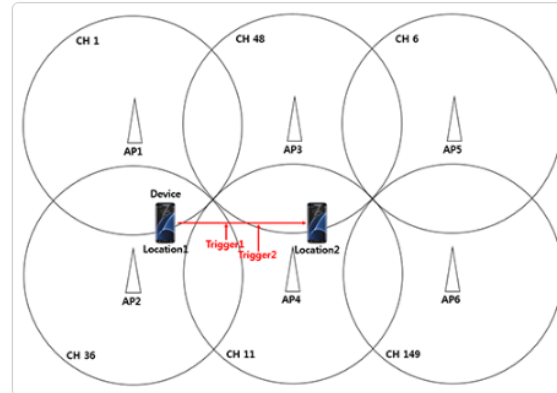
For example, the Accused Knox Products include one or more monitoring applications, such as Knox Asset Intelligence, Knox Agent, and associated dashboards that monitor radio operating conditions for one or more wireless devices. The applications constitute the claimed “monitoring application.” These radio operating conditions are not limited to signal strength, but further include channel utilization assessments to determine whether multiple clients are connected to the same access point such that connectivity is hindered despite having a strong radio signal due to limited resources. *See* Samsung Knox Documentation, Knox Platform for Enterprise, Knox Platform for Enterprise knowledge base articles, <https://docs.samsungknox.com/admin/knox-platform-for-enterprise/kbas/kba-115013403768/> (last accessed September 2, 2025). The access point can notify the clients of its current traffic through a “CU factor” in its beacon and the mobile devices will then trigger a roaming scan if the received CU value is greater than 70 percent and the current RSSI value is between -65dBm and -75dBm. *See id.*

	<p>Additionally, when the mobile device moves from Location1 to Location2, roaming will be triggered at point, Trigger1 due to a weak RSSI value. <i>See id.</i> While the mobile device tries to find a roaming candidate in CH 1 and CH 36 via a partial scan, it is not able to find any other access point from the list other than AP2. Only after a full-scan will the mobile device discover AP3 and AP4 where it will add CH 11 and CH 46 to its roaming channel list after it connects to AP4. <i>See id.</i> Having neighbor reports avoids full-scans from such instance from happening. <i>See id.</i> Initially, mobile device will save CH 1 and CH 36 in the channel list as it connects to AP2, which is equal to previous case. <i>See id.</i> Then, in addition, it will also send a neighbor report request to AP2. AP2 will return a list of nearby AP's, which is AP1, AP2 and AP4. From this response, mobile devices will add CH 11 in its roaming channel list. <i>See id.</i></p>
--	--

1. Neighbor Report

As explained in partial scanning section, the mobile device maintains a roaming channel list to reduce scan time. But, there are cases where the device may trigger a full-scan in order to find a roaming AP. In the following diagram, the mobile device initially finds AP1 and AP2 and saves CH 1 and CH 36 in the roaming channel list after connecting to AP2.

When the mobile device moves from Location1 to Location2, roaming will be triggered at point, Trigger1 due to a weak RSSI value. While the mobile device tries to find a roaming candidate in CH 1 and CH 36 via a partial scan, it is not able to find any other AP from the list other than AP2. Only after a full-scan will the mobile device discover AP3 and AP4 where it will add CH 11 and CH 46 to its roaming channel list after it connects to AP4.



Having neighbor reports avoids full-scans from such instance from happening. Initially, mobile device will save CH 1 and CH 36 in the channel list as it connects to AP2, which is equal to previous case. Then, in addition, it will also send a neighbor report request to AP2. AP2 will return a list of nearby AP's, which is AP1, AP2 and AP4. From this response, mobile devices will add CH 11 in its roaming channel list.

As the mobile device moves away from Location1 to Location2, the device will run a partial roaming scan at Trigger1 for CH 1, CH 11 and CH 36. This time, the device finds AP4 from its partial scan and successfully connects to AP4. After roaming success, mobile device will repeat the steps by sending a neighbor request to AP4.

Samsung Knox Documentation, Knox Platform for Enterprise, Knox Platform for Enterprise knowledge base articles, <https://docs.samsungknox.com/admin/knox-platform-for-enterprise/kbas/kba-115013403768/> (last accessed September 2, 2025).

Knox is involved in the enhanced roaming algorithms for Wi-Fi and mobile data. For example, it can monitor signal strength (RSSI) to trigger a device to scan for a stronger Wi-Fi signal when the current one is weak. *See id.* Knox can monitor and provide reports on network events. This includes when devices connect to or disconnect from Wi-Fi networks. *See id.*

Finally, the applications of the Knox Accused Products monitor signal strength by displaying a real-time graph of a device's mobile or Wi-Fi signal strength within the agent app and on the Location dashboard. Samsung Knox Documentation, Knox Asset Intelligence, Dashboard, Location dashboard, Use location dashboard, <https://docs.samsungknox.com/admin/knox-asset-intelligence/dashboard/location-dashboard/use-the-location-dashboard/#:~:text=To%20use%20this%20feature%2C%20you,next%20to%20the%20Search%20icon> (last accessed September 2, 2025). Users can see this data as a graphical representation over the last 10 seconds, helping them identify areas of weak cellular coverage, potential dead zones, or issues with Wi-Fi connections. *See id.* Signal strength is also displayed as a percentage of good, very good, okay, not good, or unusable based on dBm values in the agent app's Network screen. *See id.* The Accused Knox Products, for example, include "mobile signal strength" data (a type of performance or quality of service information for one or more specific locations), which enables the identification of "devices situated in areas with weak cellular coverage or potential dead zones." *See id.*

F **Mobile signal strength** Let's you identify when devices are situated in areas with weak cellular coverage or potential dead zones. To use this feature, you must first enable **Mobile signal strength with location**.

On the map, you'll see the mobile signal strength status of every device in your fleet represented by colored dots. These dots are updated at the same rate as your location data collection frequency.

- **Good (green):** -70 dBm or higher
- **Normal (blue):** -71 dBm to -80 dBm
- **Bad (red):** -81 dBm to -139 dBm
- **No signal (grey):** -140 dBm or lower, no collection

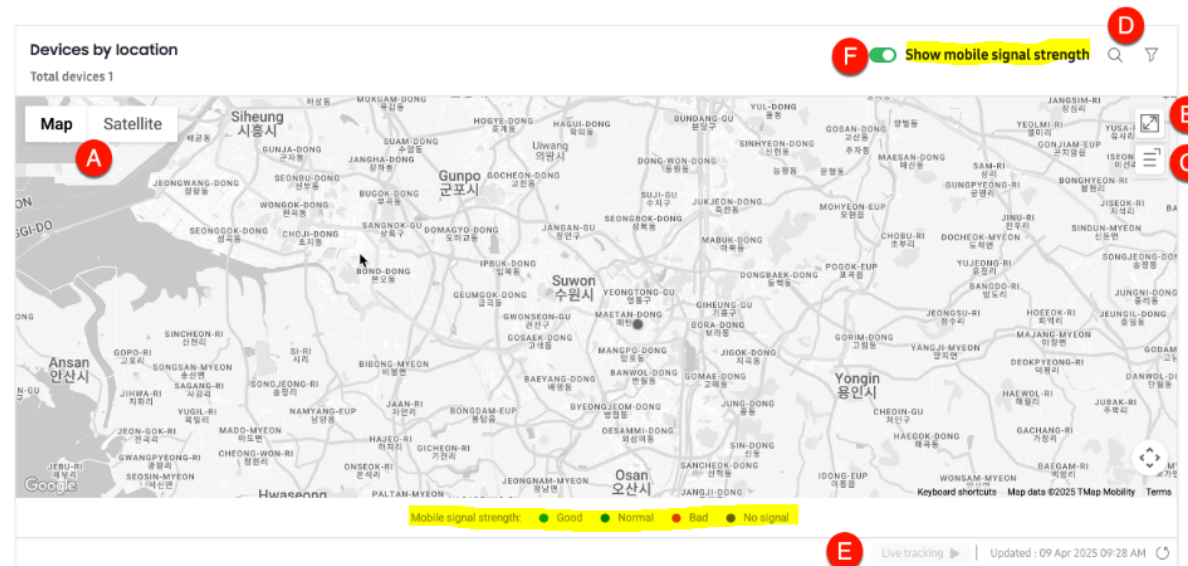
These dots also appear in the map's **Device list**, letting you quickly correlate the device IDs with each mobile signal strength status. If you want to only show devices with a specific status—for example, only show **Bad** devices—you can select the status using the map's **Filter** options next to the Search icon.

Samsung Knox Documentation, Knox Asset Intelligence, Dashboard, Location dashboard, Use location dashboard, <https://docs.samsungknox.com/admin/knox-asset-intelligence/dashboard/location-dashboard/use-the-location-dashboard/#:~:text=To%20use%20this%20feature%2C%20you,next%20to%20the%20Search%20icon> (last accessed September 2, 2025).

The Accused Knox Products further provide admin interfaces, via dashboards (e.g., location dashboards) that include maps of device distributions across a given area. Mobile signal strength data can be displayed via such maps, which enables customers to quickly correlate device IDs with each mobile signal strength statuses. This further illustrates how the Accused Knox Products utilize performance or quality of service information associated with specific locations. *See* Samsung Knox Documentation, Knox Asset Intelligence, Dashboard, Location dashboard, Use location dashboard, <https://docs.samsungknox.com/admin/knox-asset-intelligence/dashboard/location-dashboard/use-the-location-dashboard/#:~:text=To%20use%20this%20feature%2C%20you,next%20to%20the%20Search%20icon> (last accessed September 2, 2025).

Location map

The map displays your device groupings (represented by gray circles on the map) as soon as you open the **Location** dashboard. When you zoom in, the circles updates to show the device distribution across a given area.



Samsung Knox Documentation, Knox Asset Intelligence, Dashboard, Location dashboard, Use location dashboard, <https://docs.samsungknox.com/admin/knox-manage/introduction/features-and-key-strengths/#:~:text=Effortless%20content%20management,Storage%20of%20device%20analysis%20data> (last accessed September 2, 2025).

The KAI service, within the Knox Suite, allows the EMM console to monitor network information associated with each of the managed mobile device, as described below.

Get started with Knox Asset Intelligence

Last updated September 6th, 2023

Knox Asset Intelligence is a data analytics solution that turns device usage information into actionable business insights. With Knox Asset Intelligence, IT admins can monitor the health and status of their device fleet's apps, batteries, and network connectivity through a powerful and highly-customizable dashboard.

See <https://docs.samsungknox.com/admin/knox-asset-intelligence/get-started/tutorials/get-started-with-knox-asset-intelligence/>

In a KAI promotional document, Samsung describes the KAI service as “a web portal designed to give enterprise IT a much deeper understanding of mobile device and app performance.”

See https://kp4-cdn.samsungknox.com/resource/Knox%20Asset%20Intelligence%20-%20Design%20feature_3k-O.pdf (“KAI Design Features”)

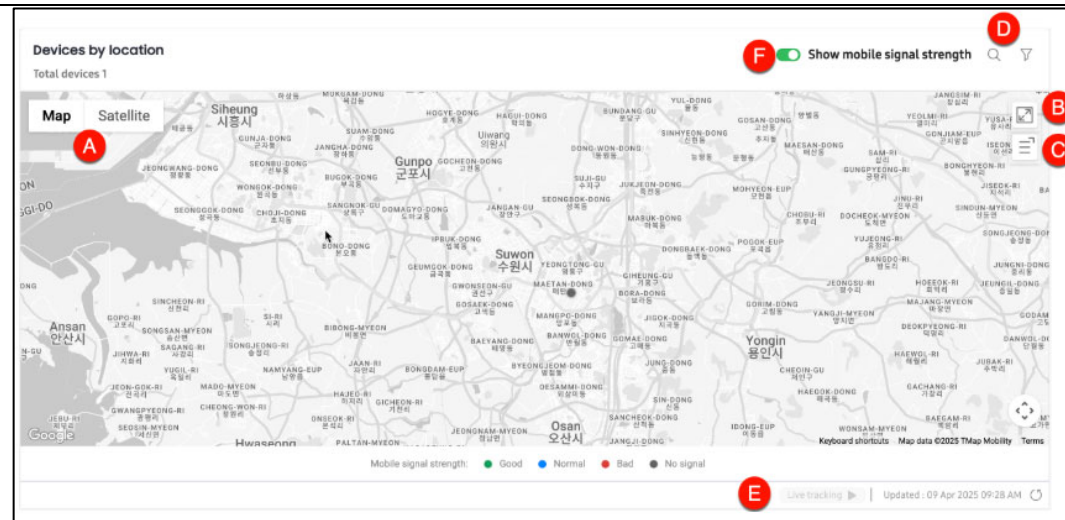
Knox Asset Intelligence brings visibility to mobile device performance

IT departments traditionally haven't had the necessary visibility across their device fleet to identify performance issues and have struggled to assess how well devices and apps are being utilized and what factors are reducing the life cycle of their mobile assets.

Through research and multiple iterations, Knox Asset Intelligence was created—a web portal designed to give enterprise IT a much deeper understanding of mobile device and app performance, helping to ensure that any problems that could impact productivity are quickly resolved.

KAI Design Features, p. 2

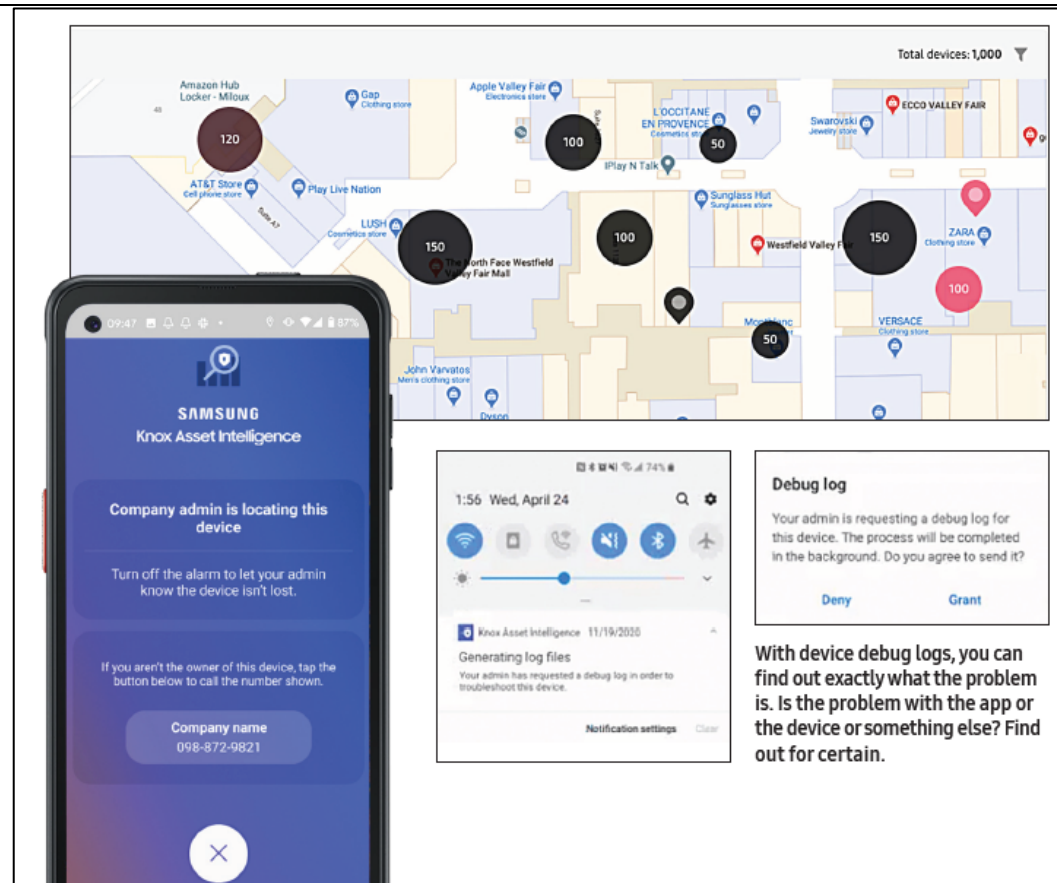
The KAI service allows IT administrator to track the location of managed mobile devices through a locations dashboard and interactive map (see below). The interactive map includes a toggle button (see F in the figure below) that allows the IT administrator to view the mobile signal strength of a managed mobile device in real-time, at a specific location.



See <https://docs.samsungknox.com/admin/knox-asset-intelligence/dashboard/location-dashboard/use-the-location-dashboard/>

The Accused Knox Products retrieve real-time data from the managed mobile devices, associated with the network performance and location of the managed mobile devices. The IT administrator can view, through the EMM console, live tracking for up to 30 seconds at a time. The table below states that the mobile signal strength information, associated with managed mobile devices is “updated at the same rate as your location data collection frequency.” Mobile signal strength information is quality or service information associated with at least one mobile device or end user associated with one or more wireless communications networks, mobile devices, or end users.

The figure below shows another example of the interactive maps provided by the KAI service that allows the IT administrator to track the location of the managed mobile devices.



Knox Asset Intelligence Flyer, p. 9

See https://image-us.samsung.com/SamsungUS/samsungbusiness/solutions/services/mobility-software/Knox_Asset_Intelligence_Flyer.pdf (“Knox Asset Intelligence Flyer”)

The data storage servers for the KAI service store data associated with the managed mobile devices in a queryable database as well as continuing to monitor, collect, and process, in automated fashion, data associated

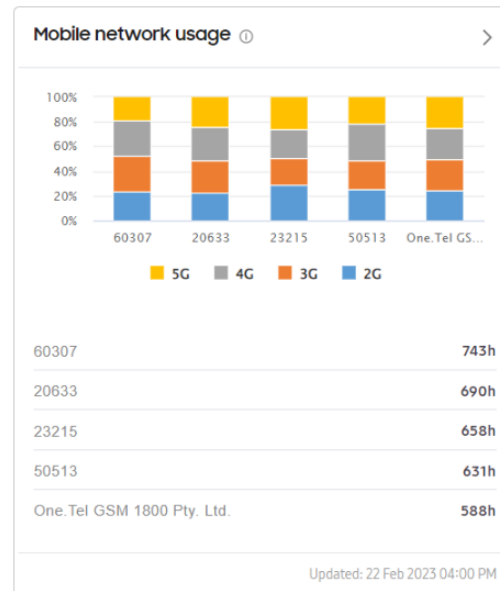
with the managed devices. The figure below shows the queryable available date ranges for specific data stored in the database.

Data type	Data insight	Dashboard update rate	Available date ranges
Common	Device status	Real-time	Can only view data for Today
Battery	Battery status and state of health	Real-time	Can only view data for Today
	Low battery, Battery drain, and Charge events	Previous day	Can view data for Yesterday, or Last 7, 14, 30, or 60 days.
	Battery level at shift start	Real-time when viewing Today's issues , otherwise Previous day.	Can view data for Yesterday, or Last 7, 14, 30, or 60 days.
	Battery level at shift end	Previous day	Can view data for Yesterday, or Last 7, 14, 30, or 60 days.
App	App usage	Previous day	Can view data for Yesterday, or Last 7, 14, 30, or 60 days.
	App issues	Real-time sent hourly by default. Can be changed in Dashboard Settings.	Can view data for Today, Yesterday, or Last 7, 14, 30, or 60 days.
Network	Wi-Fi disconnections	Real-time	Can view data for Today, Yesterday, Last 7, or 14 days.
	Mobile network usage	Previous day	Can view data for Yesterday, or Last 7, 14, 30, or 60 days.
	Network latency response time	Previous day	Can view data for Last 7, 14, or 30, days.
System	Storage usage status	Real-time every every 3 hours.	Can only view data for Today.
Scan	Scanning performance	Real-time when viewing data for Today , otherwise Previous day.	Can view data for Today, Yesterday, or Last 7, 14, 30, or 60 days.
KSP	Knox Service Plugin	Real-time	Can only view data for Today.
Location	Location status	Real-time	Can only view data for Today.
Security	Warranty bit	Real-time	Can only view data for Today.

See <https://docs.samsungknox.com/admin/knox-asset-intelligence/dashboard/overview/>

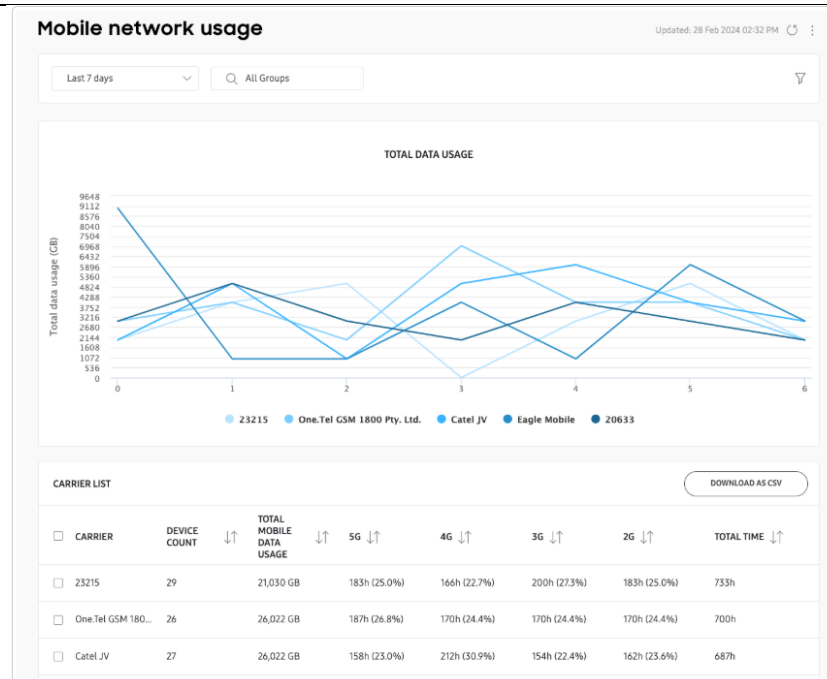
The figure below shows data analytics provided by the KAI service which are from the database associated with the manage mobile devices. The EMM console provides data analytics to the IT administrator, which is

automatically tracked and tabulated using a computer, that summarizes the cumulative mobile network usage by all managed mobile devices, based on the network generation and telecommunication carrier (shown as Mobile Country Codes, Mobile Network Codes, or carrier name).



See <https://docs.samsungknox.com/admin/knox-asset-intelligence/dashboard/network-insights/mobile-network-usage/>

The figure below shows more granular data analytics for mobile network usage provided by the KAI service. This infographic parses telecommunication carrier usage by the number of managed mobile device enrolled for an example employer, over a 7-day period.



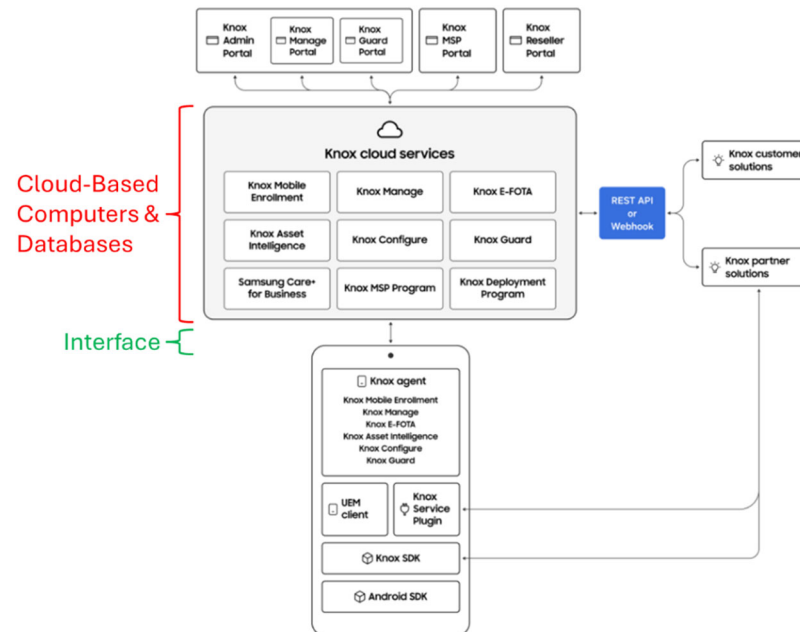
See <https://docs.samsungknox.com/admin/knox-asset-intelligence/dashboard/network-insights/mobile-network-usage/>

[20B] one or more electronic interfaces to said one or more computers which permit performance or quality of service information obtained from one or more mobile or

The Accused Knox Products include one or more electronic interfaces to said one or more computers which permit performance or quality of service information obtained from one or more mobile or fixed devices that are located in one of said one or more specific locations to be automatically or manually updated into said database, and which permits at least one of said one or more telecommunications carriers or said one or more end users or one or more parties which are not telecommunications carriers or end users to review, catalog or sort information in said database.

fixed devices that are located in one of said one or more specific locations to be automatically or manually updated into said database, and which permits at least one of said one or more telecommunications carriers or said one or more end users or one or more parties which are not telecommunications carriers or end users to review, catalog or sort information in said database; and

For example, the Accused Knox Products include an application, the Knox Agent, that can be downloaded and executed on a mobile device and can interface with one or more of the cloud-based computers of the Knox Cloud Services via an application programming interface.



Samsung Knox Documentation, Fundamentals, Introduction, the Big Picture,
<https://docs.samsungknox.com/dev/fundamentals/> (last accessed September 2, 2025).

The Knox Asset Intelligence agent is responsible for collecting device health and usage information, and sending this information back to the server to be converted into meaningful dashboard insights. *See* Samsung Knox Documentation, Home, Knox Asset Intelligence, How-to guides, Use the agent app, <https://docs.samsungknox.com/admin/knox-asset-intelligence/how-to-guides/use-the-agent-app/> (last accessed September 2, 2025). Once the agent app is downloaded and installed, device users simply launch the app to let the agent begin collecting data. *See id.* For example, performance or quality of service information for the mobile device, such as mobile network signal strength, can be updated in real time, for example, every 10 seconds. *See*

id. Furthermore, users can view their device's Wi-Fi network signal strength over the last ten seconds, updated in real time. *See id.*

Use the agent app

Last updated September 25th, 2024

The Knox Asset Intelligence agent is responsible for enrolling devices into the service, collecting device health and usage information, and sending this information back to the server to be converted into meaningful dashboard insights. Once the agent app is downloaded and installed, device users simply launch the app to let the agent begin collecting data.

Samsung Knox Documentation, Home, Knox Asset Intelligence, How-to guides, Use the agent app, <https://docs.samsungknox.com/admin/knox-asset-intelligence/how-to-guides/use-the-agent-app/> (last accessed September 2, 2025).

Network

The **Network** screen displays the mobile network signal strength of the device, along with information about the carrier network and mobile data usage.

On the chart, users can view their device's mobile network signal strength over the last 10 seconds, updated in real time. Users can tap the **Mobile data usage** field to view additional usage details, or tap **Error report** to send a debug log to their IT admins to help troubleshoot mobile network related issues.

Samsung Knox Documentation, Home, Knox Asset Intelligence, How-to guides, Use the agent app, <https://docs.samsungknox.com/admin/knox-asset-intelligence/how-to-guides/use-the-agent-app/> (last accessed September 2, 2025)

Wi-Fi**Status**

The **Wi-Fi** screen shows the **Status** tab default. Here, device users can view the signal strength of a Wi-Fi connection, along with information about the Wi-Fi network's IP address, SSID, and MAC information. On the chart, users can view their device's Wi-Fi network signal strength over the last ten seconds, updated in real time.

If Wi-Fi roaming is detected, additional roaming information is displayed. The signal strength is shown in real-time as a graph, with three statuses indicating the network latency. The status ranges are as follows:

Status	Strength
Excellent	-67 dBm or higher
Very good	-68 dBm to -70 dBm
Okay	-71 dBm to -80 dBm
Not good	-81 dBm to -90 dBm
Unusable	-91 dBm or lower

Samsung Knox Documentation, Home, Knox Asset Intelligence, How-to guides, Use the agent app, <https://docs.samsungknox.com/admin/knox-asset-intelligence/how-to-guides/use-the-agent-app/> (last accessed September 2, 2025)

The Accused Knox Products further enable the Knox Cloud Services, such as Knox Asset Intelligence, to be updated with the most recent signal strength information (e.g., performance or quality of service information) from the mobile device via the first interface. For example, the “data upload” section of the Knox Asset Intelligence settings has several data upload settings. See Samsung Knox Documentation, Home, Knox Asset Intelligence, Dashboard, Settings, Data conditions tab, <https://docs.samsungknox.com/admin/knox-asset-intelligence/dashboard/settings/data-conditions/> (last accessed September 2, 2025).

Data upload

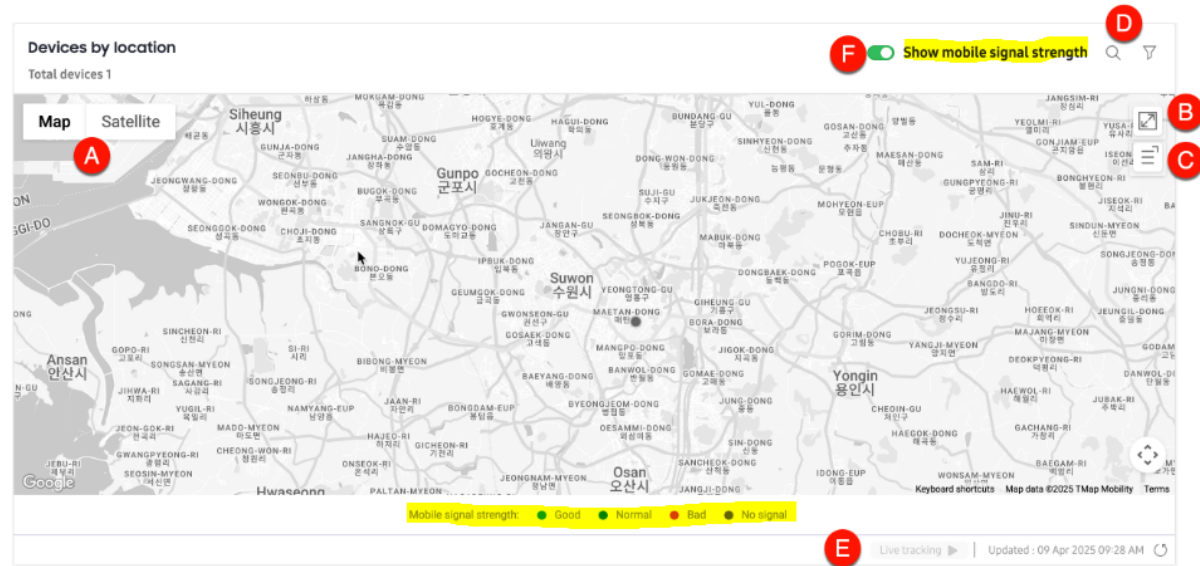
The **Data upload** section lets you specify what type of data gets collected, and — for some insights — how often data gets collected. The following table describes the data upload options available. Select a data upload option checkbox in each category to let Knox Asset Intelligence collect that specific type of data from your devices. To disable data collection for an entire category altogether, toggle the category option off.

Samsung Knox Documentation, Home, Knox Asset Intelligence, Dashboard, Settings, Data conditions tab, <https://docs.samsungknox.com/admin/knox-asset-intelligence/dashboard/settings/data-conditions/> (last accessed September 2, 2025)

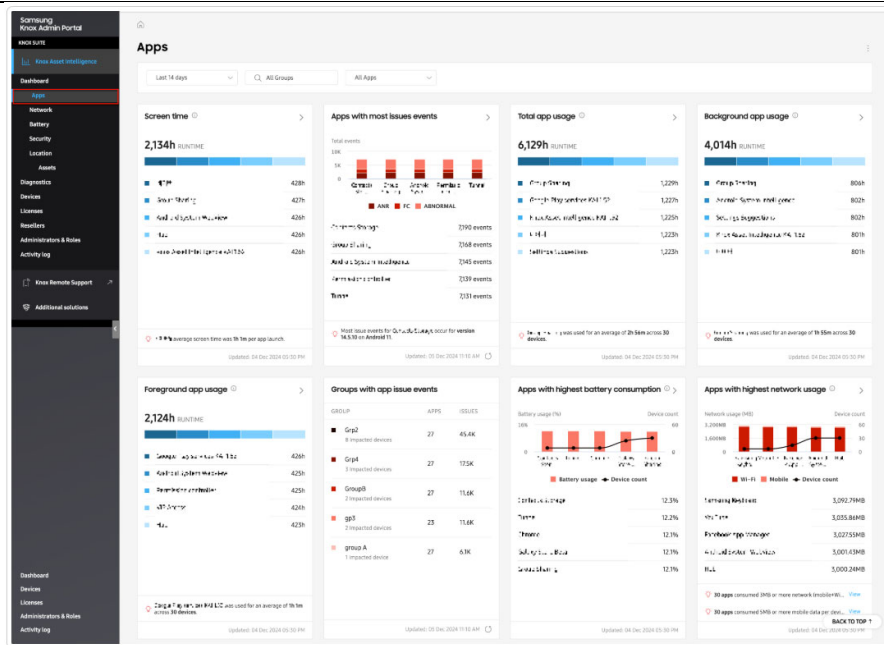
The Accused Knox Products further allow end users, such as enterprise IT administrators, to review, catalog or sort information, such as the mobile signal strength data. Specifically, the mobile signal strength data can be displayed via maps, which enable customers to quickly correlate device IDs with each mobile signal strength statuses. On the map, users can see the mobile signal strength status of every device in a fleet represented by colored dots, which are updated at the same rate as the location data collection frequency. See Samsung Knox Documentation, Knox Asset Intelligence, Dashboard, Location dashboard, Use location dashboard, <https://docs.samsungknox.com/admin/knox-asset-intelligence/dashboard/location-dashboard/use-the-location-dashboard/#:~:text=To%20use%20this%20feature%2C%20you,next%20to%20the%20Search%20icon> (last accessed September 2, 2025).

Location map

The map displays your device groupings (represented by gray circles on the map) as soon as you open the **Location** dashboard. When you zoom in, the circles updates to show the device distribution across a given area.



Samsung Knox Documentation, Knox Asset Intelligence, Dashboard, Location dashboard, Use location dashboard, <https://docs.samsungknox.com/admin/knox-manage/introduction/features-and-key-strengths/#:~:text=Effortless%20content%20management,Storage%20of%20device%20analysis%20data> (last accessed September 2, 2025).



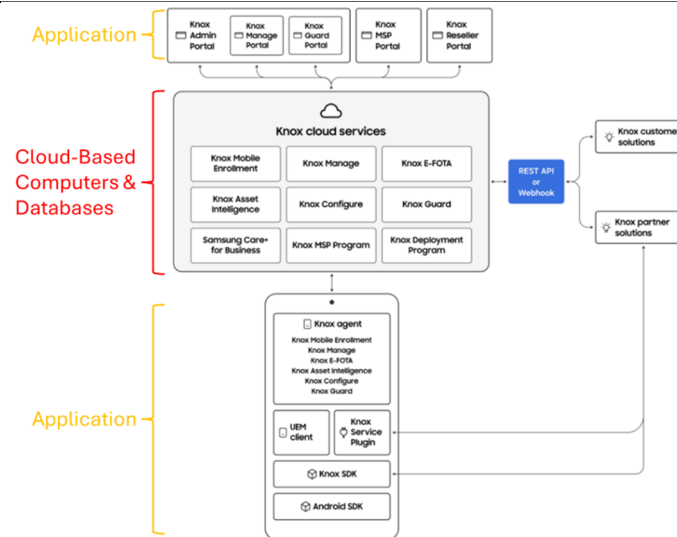
See <https://docs.samsungknox.com/admin/knox-asset-intelligence/dashboard/app-insights/app-usage/overview/>

[20C] one or more applications operable with said one or more mobile or fixed devices or said one or more computers for obtaining and providing said performance or quality of service information to said one or more

The Accused Knox Products include one or more applications operable with said one or more mobile or fixed devices (e.g., end user devices) or said one or more computers (e.g., IT administrator computers) for obtaining and providing said performance or quality of service information to said one or more electronic interfaces.

For example, the Accused Knox Products include applications, such as the Knox Agent, which are downloaded and executed by mobile devices and communicate with the cloud-based computers and databases of the Knox Cloud Services. The Accused Knox Products also include applications, such as the web-based applications of the Knox Admin Portal, that enable IT administrator computers to interface with the cloud-based computers and databases of the Knox Cloud Services.

electronic
interfaces.

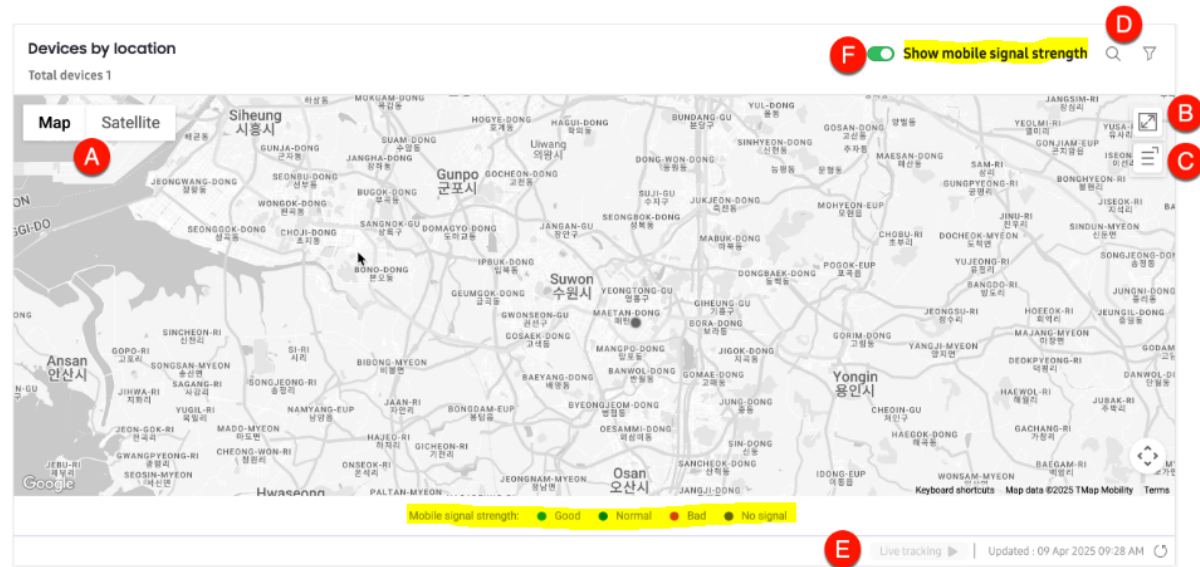


Samsung Knox Documentation, Fundamentals, Introduction, the Big Picture,
<https://docs.samsungknox.com/dev/fundamentals/> (last accessed September 2, 2025) (annotated).

The web-based applications of the Knox Admin Portal enable the IT administrator computers to obtain performance or quality of service information from the electronic interface described in reference to claim element [20A]. For example, mobile signal strength data (performance or quality of service information) can be displayed on maps via the Knox the Admin Portal. See Samsung Knox Documentation, Knox Asset Intelligence, Dashboard, Location dashboard, Use location dashboard, <https://docs.samsungknox.com/admin/knox-asset-intelligence/dashboard/location-dashboard/use-the-location-dashboard/#:~:text=To%20use%20this%20feature%2C%20you,next%20to%20the%20Search%20icon> (last accessed September 2, 2025).

Location map

The map displays your device groupings (represented by gray circles on the map) as soon as you open the **Location** dashboard. When you zoom in, the circles updates to show the device distribution across a given area.



Samsung Knox Documentation, Knox Asset Intelligence, Dashboard, Location dashboard, Use location dashboard, <https://docs.samsungknox.com/admin/knox-manage/introduction/features-and-key-strengths/#:~:text=Effortless%20content%20management,Storage%20of%20device%20analysis%20data> (last accessed September 2, 2025).

The Knox Agent, also, can be used to obtain signal strength data (performance or quality of service information for the mobile device), as such data can be viewed from the mobile device itself. *See* Samsung Knox Documentation, Knox Asset Intelligence, Knox Asset Intelligence release notes, <https://docs.samsungknox.com/admin/knox-asset-intelligence/release-notes/23-09/> (last accessed September 2, 2025).

Mobile network diagnostics in agent app

The Knox Asset Intelligence agent app now lets device users view mobile network diagnostic information like total data consumption for each SIM card in their device, and network signal strength.

Samsung Knox Documentation, Knox Asset Intelligence, Knox Asset Intelligence release notes, <https://docs.samsungknox.com/admin/knox-asset-intelligence/release-notes/23-09/> (last accessed September 2, 2025).

Additionally, applications such as the Knox Agent can be downloaded and executed by mobile devices to provide performance or quality of service information to the cloud-based computers and databases of the Knox Cloud Services via the electronic interface described in reference to claim element [20B]. Samsung Knox Documentation, Home, Knox Asset Intelligence, How-to guides, Use the agent app, <https://docs.samsungknox.com/admin/knox-asset-intelligence/how-to-guides/use-the-agent-app/> (last accessed September 2, 2025). For example, mobile signal strength data and/or Wi-Fi network signal strength (performance or quality of service information) can be captured by the mobile device and uploaded to the cloud-based computers and databases of the Knox Cloud Services in real time or, for example, every 10 seconds. *See id.*

Use the agent app

Last updated September 25th, 2024

The Knox Asset Intelligence agent is responsible for enrolling devices into the service, collecting device health and usage information, and sending this information back to the server to be converted into meaningful dashboard insights. Once the agent app is downloaded and installed, device users simply launch the app to let the agent begin collecting data.

Samsung Knox Documentation, Home, Knox Asset Intelligence, How-to guides, Use the agent app, <https://docs.samsungknox.com/admin/knox-asset-intelligence/how-to-guides/use-the-agent-app/> (last accessed September 2, 2025).

Network

The **Network** screen displays the mobile network signal strength of the device, along with information about the carrier network and mobile data usage.

On the chart, users can view their device's mobile network signal strength over the last 10 seconds, updated in real time. Users can tap the **Mobile data usage** field to view additional usage details, or tap **Error report** to send a debug log to their IT admins to help troubleshoot mobile network related issues.

Samsung Knox Documentation, Home, Knox Asset Intelligence, How-to guides, Use the agent app, <https://docs.samsungknox.com/admin/knox-asset-intelligence/how-to-guides/use-the-agent-app/> (last accessed September 2, 2025)

Wi-Fi

Status

The **Wi-Fi** screen shows the **Status** tab default. Here, device users can view the signal strength of a Wi-Fi connection, along with information about the Wi-Fi network's IP address, SSID, and MAC information. On the chart, users can view their device's Wi-Fi network signal strength over the last ten seconds, updated in real time.

If Wi-Fi roaming is detected, additional roaming information is displayed. The signal strength is shown in real-time as a graph, with three statuses indicating the network latency. The status ranges are as follows:

Status	Strength
Excellent	-67 dBm or higher
Very good	-68 dBm to -70 dBm
Okay	-71 dBm to -80 dBm
Not good	-81 dBm to -90 dBm
Unusable	-91 dBm or lower

Samsung Knox Documentation, Home, Knox Asset Intelligence, How-to guides, Use the agent app, <https://docs.samsungknox.com/admin/knox-asset-intelligence/how-to-guides/use-the-agent-app/> (last accessed September 2, 2025)

Data upload

The **Data upload** section lets you specify what type of data gets collected, and — for some insights — how often data gets collected. The following table describes the data upload options available. Select a data upload option checkbox in each category to let Knox Asset Intelligence collect that specific type of data from your devices. To disable data collection for an entire category altogether, toggle the category option off.

Samsung Knox Documentation, Home, Knox Asset Intelligence, Dashboard, Settings, Data conditions tab, <https://docs.samsungknox.com/admin/knox-asset-intelligence/dashboard/settings/data-conditions/> (last accessed September 2, 2025)

The Accused Knox Products also allow the IT admin to obtain network performance data through the EMM console (e.g., applications).

The EMM console can access the following network performance data from the managed devices:

Network

This section displays Wi-Fi consumption data related to your device. Information displayed is based on the last time the device connected to a Wi-Fi connection. The following information is available:

- **Network name (SSID):** Service Set Identifier, the unique name assigned to the network.
- **AP Vendor:** Name of the Wi-Fi access point manufacturer.
- **AP BSSID:** Access Point Basic Service Set Identifier, the unique MAC (Media Access Control) address that identifies the access point.
- **Wi-Fi strength (RSSI):** Received Signal Strength Indicator, the measure of the Wi-Fi signal's power level typically ranging from -30 dBm (very strong signal) to -90 dBm (very weak signal).
- **Bands:** Frequency range used by the Wi-Fi network to transmit data.
- **Link speed:** Maximum data transfer speed between the AP and the client (this device), measured in megabits per second (Mbps).
- **Last connected time:** Date and time the device last connected to a Wi-Fi network.
- **Wi-Fi calling:** Indicator of whether the device is configured for Wi-Fi calling, or if Wi-Fi calling is unsupported by the device.

See <https://docs.samsungknox.com/admin/knox-asset-intelligence/how-to-guides/manage-devices/>

The document excerpt below further describes management features of the Knox Suite that allows the IT admin to obtain network statistics through the EMM console. See

https://images.samsung.com/is/content/samsung/p5/ch/business/enterprise-edition/Knox_Platform_for_Enterprise_Whitepaper_2019.pdf (“Knox Whitepaper”)

Advanced App Management

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

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

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

Knox Whitepaper, p. 59 (annotated).

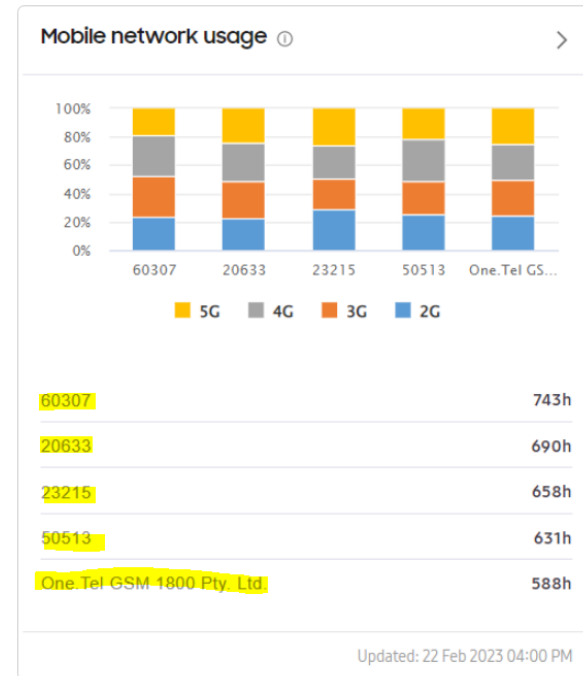
In another example, the managed mobile device can be configured, through the EMM application, to report device location information to the EMM console.

	<p>2.7. Device Policy Creation</p> <p>Device policies are deployed when a device is enrolled in Knox Manage or can be pushed automatically to devices. Knox Manage implements a hierarchy policy set that allows policies to be deployed to all users, while other policies can then be deployed to a subset of users based on your business need. Some of the policies that can be configured include allowing users to use the camera, configure the device to report the devices location within the EMM console, and allowing users to wipe devices.</p> <p>Knox Service Guide v3.05, p. 7 (annotated).</p>	
Claim 22	Accused Knox Products	
[22] The clearinghouse system of claim 20 wherein said performance or quality of service information includes multiple bands and multiple carriers.	<p>The performance or quality of service information in the Accused Knox Products includes multiple bands and multiple carriers.</p> <p>For example, the Accused Knox Products are capable of provide performance information, such as mobile network usage, on a “per carrier” basis. This helps monitor and measure how device users are using mobile data by collecting data about mobile data usage by network generations and carrier. For example, device users might primarily be using 4G networks, meaning a 5G data plan could be unnecessary. <i>See</i> Samsung Knox Documentation, Home, Knox Asset Intelligence, Dashboard, Network insights, https://docs.samsungknox.com/admin/knox-asset-intelligence/dashboard/network-insights/mobile-network-usage/ (last accessed September 2, 2025). According to Samsung, “Knox Asset Intelligence collects the MCC/MNC code and matches it to a carrier name.” <i>See id.</i></p>	

	Network	Wi-Fi disconnection events: Groups	Get in-depth visibility into device groups with the highest amount of disconnection problems, including detailed event logs.
		Wi-Fi disconnection events: BSSIDs and APs	Get in-depth visibility into Wi-Fi networks with the highest amount of disconnection problems, including detailed event logs.
		Mobile network usage	Get in-depth visibility into cellular usability information, including which network generations are used per carrier.
		Network latency	Lets you see which IP addresses or domains have the longest response time or don't respond at all to device requests.

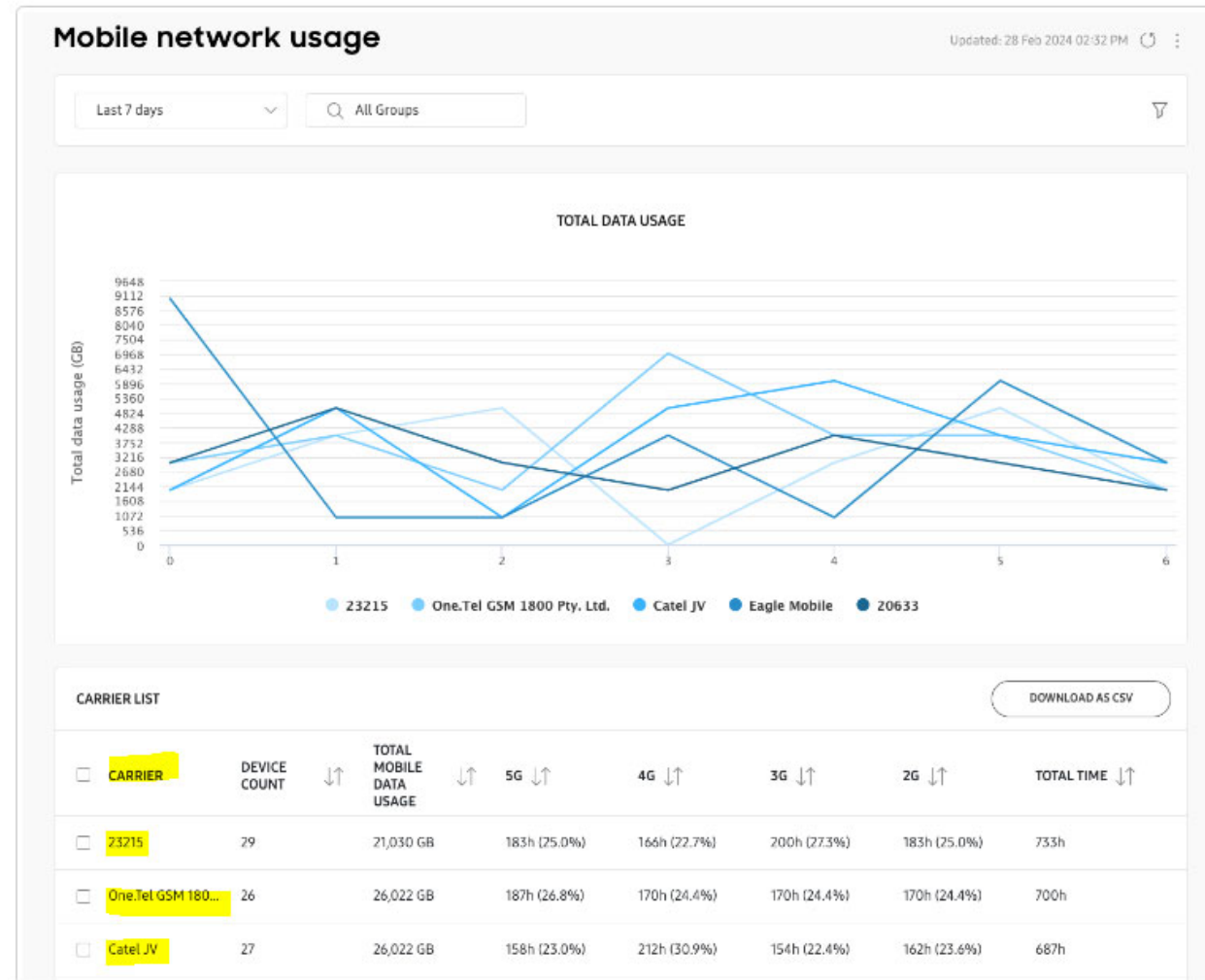
Samsung Knox Documentation, Home, Knox Asset Intelligence, Dashboard, Overview, <https://docs.samsungknox.com/admin/knox-asset-intelligence/dashboard/overview/> (last accessed September 2, 2025)

The **Mobile network usage** dashboard chart displays **cellular signal information arranged by carrier network**, providing insight into which network generations — 2G, 3G, 4G, and 5G — are used per carrier.



The **five carriers with the longest cumulative connection durations are shown**, along with the percentage of **total carrier usage time** associated with each network generation. The information also includes the **type of cellular network**, the **connection duration** for each network generation, and the **cellular usage by carrier**.

Samsung Knox Documentation, Home, Knox Asset Intelligence, Dashboard, Network insights,
<https://docs.samsungknox.com/admin/knox-asset-intelligence/dashboard/network-insights/mobile-network-usage/>
 (last accessed September 2, 2025).

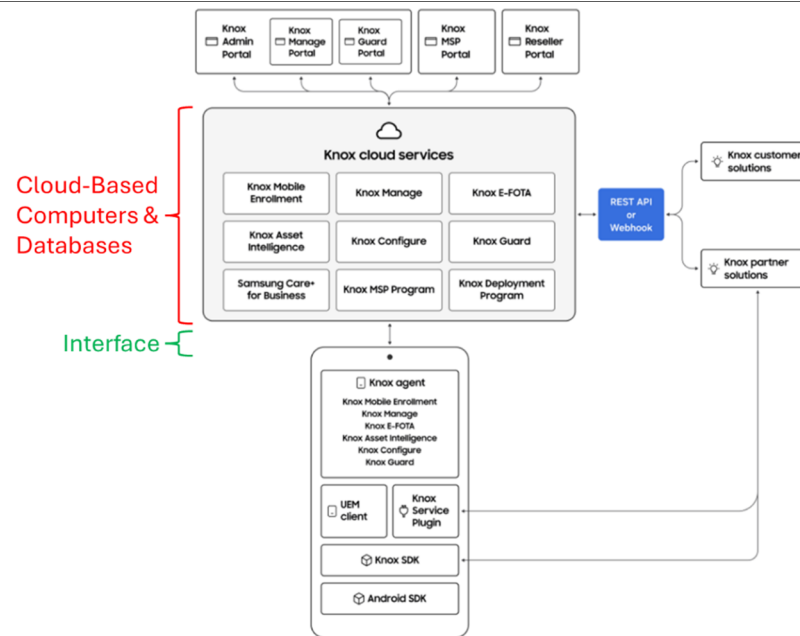


The **Mobile network usage** expanded view page features a chart that lists the top 5 mobile carriers with the highest network usage (in GB) over the selected reporting period. Click any carrier name in the legend to show or hide the data on the chart.

In the **CARRIER LIST** table below, you'll see usage data for every carrier that your devices connected to during the selected reporting period. For each carrier, you can view how many devices connected, view the total usage (in GB), and view the total connection time (in hours) for that carrier (with connection time data broken down by network generation (5G, 4G, and so on)).

	<p>Samsung Knox Documentation, Home, Knox Asset Intelligence, Dashboard, Network insights, https://docs.samsungknox.com/admin/knox-asset-intelligence/dashboard/network-insights/mobile-network-usage/ (last accessed September 2, 2025).</p>
--	---

Claim 23	Accused Knox Products
<p>[23] The clearinghouse system of claim 20 further comprising means for sending instructions from one of said one or more electronic interfaces to one or more wireless devices for configuring or reconfiguring said one or more wireless devices based on a ranking of performance or specific requests of an end user.</p>	<p>The Accused Knox Products further include means for sending instructions from one of said one or more electronic interfaces to one or more wireless devices for configuring or reconfiguring said one or more wireless devices based on a ranking of performance or specific requests of an end user.</p> <p>For example, via the Knox Manage Portal a web-based console of the Knox Admin Portal, IT administrators can cause one or more computers of the Knox Cloud Services to run various actions on targeted mobile, wireless devices. <i>See</i> Samsung Knox Documentation, Knox Manage, New Knox Manage console, How-to guides, Run an action on a device, https://docs.samsungknox.com/admin/knox-manage/new-console/how-to-guides/run-an-action-on-a-device/ (last accessed September 2, 2025).</p>



Samsung Knox Documentation, Fundamentals, Introduction, the Big Picture,
<https://docs.samsungknox.com/dev/fundamentals/> (last accessed September 2, 2025).

Such actions can include pushing new profiles, locking or unlocking the screen, locking or unlocking the device, and viewing device logs, among other actions that configure or reconfigure the mobile, wireless device based on specific requests of the end user (e.g., IT administrators, workforce personnel, etc.). *Id.*

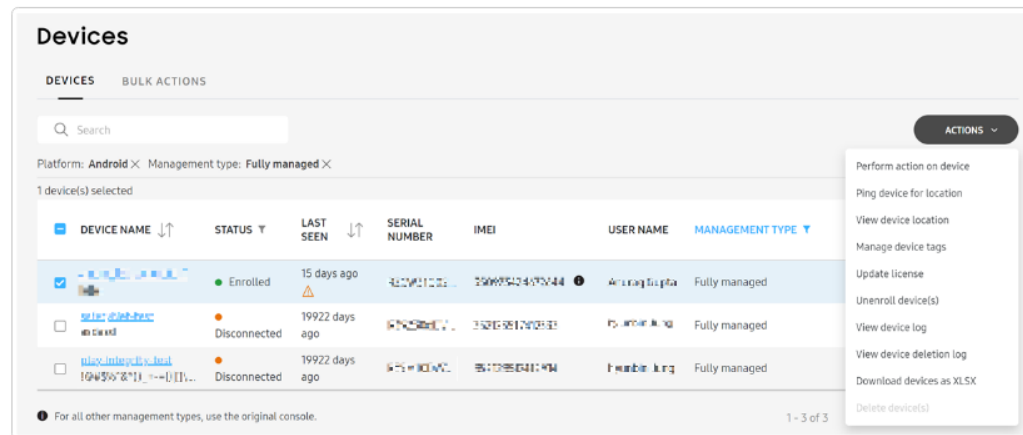
Run an action on a device

Last updated September 25th, 2024

Through **Knox Manage**, you can **run various actions on target devices** — including pushing new profiles, locking or unlocking the screen, locking or unlocking the device, and viewing device logs, among others.

To run an action on a device enrolled in Knox Manage:

1. Go to **Devices**.
2. **Select one or more devices to run an action on.**
3. Click **ACTIONS**. **Select an applicable action to run** on the devices.



Samsung Knox Documentation, Knox Manage, New Knox Manage console, How-to guides, Run an action on a device, <https://docs.samsungknox.com/admin/knox-manage/new-console/how-to-guides/run-an-action-on-a-device/> (last accessed September 2, 2025)

	<div><h2>Push a profile</h2><p>Last updated December 6th, 2023</p><p>When you edit a profile, you don't have to push it to its assigned devices or groups right away. Also, sometimes a device user modifies a setting or an app on the device, and you want to undo those changes through the profile. In these cases, you can push the profile to the devices again, which re-applies the profile settings.</p><p>To re-sync or update a profile, you need to send the Push profile action to the affected devices.</p><h3>Push a profile to a group</h3><p>To push a profile to its assigned group:</p><ol style="list-style-type: none">1. Go to Profiles and policies.2. Select the profile you want to push.3. Click ACTIONS > Push profile. The Push profile(s) dialog opens.4. Confirm the action to send it.<p>Samsung Knox Documentation, Knox Manage, New Knox Manage console, How-to guides, Edit a profile, https://docs.samsungknox.com/admin/knox-manage/new-console/how-to-guides/edit-a-profile/ (last accessed September 2, 2025).</p></div>
--	---

Assign app

Configure Select Review

Search

SELECTED APPS

Knox Remote...

[Bulk configure settings](#)

KNOX REMOTE SUPPORT

App source
Managed Google Play - Public

Installation type
Set whether users can choose to install an app on their device, and if they can remove it.

☒ Installed by the user

☐ Auto-installed (can be removed by the user)

☐ Auto-installed (can't be removed by the user)

Automatic app updates
The default can be modified in the [Android Enterprise settings](#).

☒ Default (Only auto-update over Wi-Fi)

☐ High priority

☐ Postpone for 90 days

Automatically run app

☒ After installation

☐ After installation and every app update

☐ Don't automatically run app

☒ **Managed configuration**
Already have an existing configuration? [Import a config file](#)

Configuration name *

my config

☐ Secret Key

NEXT: SELECT

Samsung Knox Documentation, Knox Manage, New Knox Manage console, How-to guides, Add an app, <https://docs.samsungknox.com/admin/knox-manage/new-console/how-to-guides/add-an-app/> (last accessed September 2, 2025)

Additionally, Knox E-FOTA can enable IT administrators to select the target firmware version, force target firmware version update onto select devices, schedule updates during non-peak work times and granular network resource management, and mass deploy the target firmware version. See Samsung Knox Documentation, Samsung Knox white papers, Samsung Knox Mobile Security, Knox Cloud Services & Integrations, Knox E-FOTA, <https://docs.samsungknox.com/admin/fundamentals/whitepaper/samsung-knox-mobile-security/kcs-integrations/knox-e-fota/> (last accessed September 2, 2025).

Knox E-FOTA

Last updated March 7th, 2025

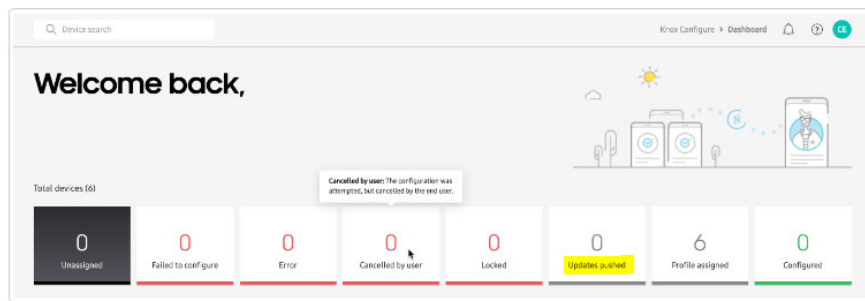
Samsung developed Knox Enterprise Firmware Over-the-Air (E-FOTA) to enable enterprises to efficiently manage mobile infrastructure, reduce support costs, and save time. With Knox E-FOTA, IT admins can ensure that device users can't independently update to unsupported firmware versions, preventing issues that could negatively impact employee productivity, support costs, and data security.

With Knox E-FOTA, enterprises can control device software updates in the following ways:

- **Select the target firmware version:** Knox E-FOTA provides a list of firmware options and their corresponding details based on your device model. You can set the target Android OS version or update to the latest version.
- **Force target firmware version update onto select devices:** Enterprises can push new firmware to specific devices to ensure interoperability and compatibility with proprietary systems and apps. This prevents any operational or performance issues that may arise due to incompatibility.
- **Schedule updates during non-peak work times and granular network resource management:** Knox E-FOTA offers setting granular control over when to download the update, and how. This ensures update scheduling prevents any interruptions to employee productivity. Additionally, Knox E-FOTA enables enterprises to manage network bandwidth restrictions through a set of configuration options, and deploy the updates entirely on-premises.
- **Mass deploy the target firmware version:** Mass deployment eliminates the issue of software version fragmentation, and there's no need to support multiple legacy firmware versions for every deployed device. You can ensure that all devices are updated to the desired firmware version, regardless of their current firmware version.

Samsung Knox Documentation, Samsung Knox white papers, Samsung Knox Mobile Security, Knox Cloud Services & Integrations, Knox E-FOTA,
<https://docs.samsungknox.com/admin/fundamentals/whitepaper/samsung-knox-mobile-security/kcs-integrations/knox-e-fota/> (last accessed September 2, 2025).

Furthermore, via the Knox Configure Dashboard, a web-based console of the Knox Admin Portal, IT administrators can cause one or more computers of the Knox Cloud Services to push an application or command to a wireless device based on a specific request of an end user.



The Knox Configure Dashboard displays the following:

- **Total Devices** — Lists the cumulative number of devices, in any state, currently managed within the Knox Configure console.
- **Unassigned** — Lists the total number of devices that have been added to the console but are yet to receive a profile assignment.
- **Failed to configure** — Lists the total number of devices that were assigned a configuration profile but failed before completion.
- **Error** — Lists the total number of devices whose profile assignment resulted in an error and placed the device in an error state and awaiting troubleshooting assistance.
- **Cancelled by user** — Lists the total number of devices whose profile assignment was cancelled by the admin before completion.
- **Updates pushed** — Lists the **total number of devices successfully receiving a profile push update** since the last trending period.
- **Profile assigned** — Lists the total number of devices that received a profile assignment successfully without cancellation or error.
- **Configured** — Lists the total number of newly configured devices since the last trending period.

Samsung Knox Documentation, Knox Configure, How-to guides, About the Dashboard, <https://docs.samsungknox.com/admin/knox-configure/how-to-guides/use-the-dashboard/> (last accessed September 2, 2025).

End user requests can include requests to: 1) homogenize firmware versions and capabilities of deployed device models; 2) carry out interoperability or compatibility testing with in-house or proprietary servers, apps, and endpoint settings; 3) ensure that known issues are patched before the deployment of major firmware version updates; 4) perform field tests of new firmware and software on a subset of devices before mass deployment; and 5) force the use of firmware versions that have been validated to meet industry certification or regulation requirements. *See* Samsung Knox Documentation, Samsung Knox white papers, Samsung Knox Mobile Security, Knox Cloud Services & Integrations, Managed software updates, <https://docs.samsungknox.com/admin/fundamentals/whitepaper/samsung-knox-mobile-security/kcs-integrations/managed-software-updates> (last accessed September 2, 2025).

In the Accused Knox Products, the “means for sending” is implemented, for example, by one or more processors executing the Knox Suite Applications (including the Knox Manage server/console, Knox Admin Portal, and Knox Agent), in combination with the network communication interface (including APIs and/or wireless/cellular network modules) that transmit data, device management commands, and configuration instructions to managed mobile devices.

The Accused Knox Products allow the user of the managed mobile device to request support in response to network performance issues. The IT admin can configure network setting on the managed mobile device in response to the request.

The excerpt below describes features of the Knox Configure service that allows IT admins to reconfigure device settings on a managed mobile device, including network settings.

Device management services

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

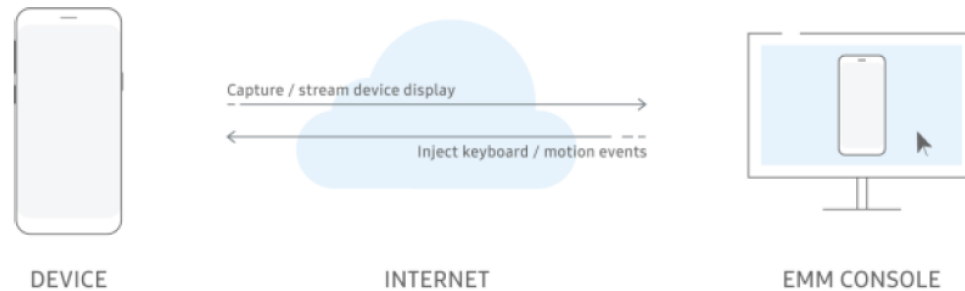
- **Knox Mobile Enrollment** — With this free service, enterprises can use a web console or REST API calls to automate device enrollment, either individually or in bulk. After an IT admin registers a device with this service, the device user simply turns it on and connects it to a Wi-Fi or 3G/4G/5G mobile network to enroll it with an EMM system. There is no manual enrollment of individual devices, and no need for IMEI management and verification – all onerous, time-consuming, and error-prone tasks.
- **Knox Configure** — Samsung phones, tablets, and wearables are fully customizable to work in numerous vertical markets such as hospitality, retail, and entertainment. Through a web console, Systems Integrators can create purpose-built devices that present a customized user interface, for example, an information kiosk, point-of-sales terminal, or in-flight entertainment system. The Systems Integrators can customize or restrict almost all aspects of device configuration and the user experience, including boot animations incorporating custom enterprise logos, display settings, wallpapers, **network configurations**, notifications, and software updates.

Knox Whitepaper v1.5, p. 52 (annotated).

	<div data-bbox="722 196 1751 587"> <p>6.4. Review desired capability</p> <p>Before developing a configuration profile or profiles to meet your business need, Samsung will review with you, your desired end state. In addition Samsung will discuss Knox Configures capabilities and how they can meet those needs. Some of the capabilities that can be implemented in device profiles are: -</p> <p>Applications & EMM deployment</p> <ul style="list-style-type: none"> • Configure the automatic deployment of applications on initiation of the device • Automatic Enrollment of your EMM (Knox Manage) when the device first connects. • Dynamically update apps and configurations. (Knox Configure Dynamic only) • Skip unwanted setup wizard steps during installations </div> <p style="text-align: center;">Knox Service Guide v3.05, p. 13 (annotated).</p> <p>In another example, the IT admin can use the EMM console remotely to resolve problems with the managed mobile device, based on a support request from the user of the managed device. (See remote control excerpts below).</p>
--	---

Remote Control

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



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

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

Knox Whitepaper v1.5, p. 52.

2.8. Remote Device control (Knox Manage only)

Knox Manage provides the capability for an administrator to take remote control of a managed device (with the user's agreement) and allow the administrator to view and control the users screen, allowing for remote faultfinding of issues without needing the device to be present. Samsung will show you how to enable this functionality and demonstrate its use.

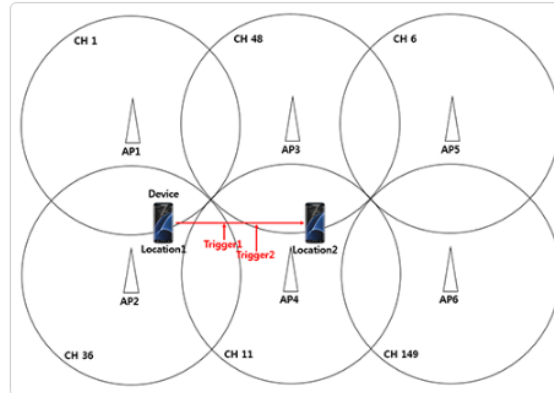
Knox Service Guide v3.05, p. 8.

Claim 25	Accused Knox Products
<p>[25] The clearinghouse system of claim 20 further comprising a monitoring application which permits monitoring of radio operating conditions of one or more wireless devices, wherein monitored radio operating conditions are used to update performance or quality of service information in said database.</p>	<p>The Accused Knox Products include a monitoring application which permits monitoring of radio operating conditions of one or more wireless devices, wherein monitored radio operating conditions are used to update performance or quality of service information in said database.</p> <p>For example, the Accused Knox Products include one or more monitoring applications, such as Knox Asset Intelligence, Knox Agent, and associated dashboards that monitor radio operating conditions for one or more wireless devices. The applications constitute the claimed “monitoring application.” These radio operating conditions are not limited to signal strength, but further include channel utilization assessments to determine whether multiple clients are connected to the same access point such that connectivity is hindered despite having a strong radio signal due to limited resources. <i>See</i> Samsung Knox Documentation, Knox Platform for Enterprise, Knox Platform for Enterprise knowledge base articles, https://docs.samsungknox.com/admin/knox-platform-for-enterprise/kbas/kba-115013403768/ (last accessed September 2, 2025). The access point can notify the clients of its current traffic through a “CU factor” in its beacon and the mobile devices will then trigger a roaming scan if the received CU value is greater than 70 percent and the current RSSI value is between -65dBm and -75dBm. <i>See id.</i></p> <p>Additionally, when the mobile device moves from Location1 to Location2, roaming will be triggered at point, Trigger1 due to a weak RSSI value. <i>See id.</i> While the mobile device tries to find a roaming candidate in CH 1 and CH 36 via a partial scan, it is not able to find any other access point from the list other than AP2. Only after a full-scan will the mobile device discover AP3 and AP4 where it will add CH 11 and CH 46 to its roaming channel list after it connects to AP4. <i>See id.</i> Having neighbor reports avoids full-scans from such instance from happening. <i>See id.</i> Initially, mobile device will save CH 1 and CH 36 in the channel list as it connects to AP2, which is equal to previous case. <i>See id.</i> Then, in addition, it will also send a neighbor report request to AP2. AP2 will return a list of nearby AP’s, which is AP1, AP2 and AP4. From this response, mobile devices will add CH 11 in its roaming channel list. <i>See id.</i></p>

1. Neighbor Report

As explained in partial scanning section, the mobile device maintains a roaming channel list to reduce scan time. But, there are cases where the device may trigger a full-scan in order to find a roaming AP. In the following diagram, the mobile device initially finds AP1 and AP2 and saves CH 1 and CH 36 in the roaming channel list after connecting to AP2.

When the mobile device moves from Location1 to Location2, roaming will be triggered at point, Trigger1 due to a weak RSSI value. While the mobile device tries to find a roaming candidate in CH 1 and CH 36 via a partial scan, it is not able to find any other AP from the list other than AP2. Only after a full-scan will the mobile device discover AP3 and AP4 where it will add CH 11 and CH 46 to its roaming channel list after it connects to AP4.



Having neighbor reports avoids full-scans from such instance from happening. Initially, mobile device will save CH 1 and CH 36 in the channel list as it connects to AP2, which is equal to previous case. Then, in addition, it will also send a neighbor report request to AP2. AP2 will return a list of nearby AP's, which is AP1, AP2 and AP4. From this response, mobile devices will add CH 11 in its roaming channel list.

As the mobile device moves away from Location1 to Location2, the device will run a partial roaming scan at Trigger1 for CH 1, CH 11 and CH 36. This time, the device finds AP4 from its partial scan and successfully connects to AP4. After roaming success, mobile device will repeat the steps by sending a neighbor request to AP4.

Samsung Knox Documentation, Knox Platform for Enterprise, Knox Platform for Enterprise knowledge base articles, <https://docs.samsungknox.com/admin/knox-platform-for-enterprise/kbas/kba-115013403768/> (last accessed September 2, 2025).

Knox is involved in the enhanced roaming algorithms for Wi-Fi and mobile data. For example, it can monitor signal strength (RSSI) to trigger a device to scan for a stronger Wi-Fi signal when the current one is weak. *See id.* Knox can monitor and provide reports on network events. This includes when devices connect to or disconnect from Wi-Fi networks. *See id.*

Finally, the applications of the Knox Accused Products monitor signal strength by displaying a real-time graph of a device's mobile or Wi-Fi signal strength within the agent app and on the Location dashboard. Samsung Knox Documentation, Knox Asset Intelligence, Dashboard, Location dashboard, Use location dashboard, <https://docs.samsungknox.com/admin/knox-asset-intelligence/dashboard/location-dashboard/use-the-location-dashboard/#:~:text=To%20use%20this%20feature%2C%20you,next%20to%20the%20Search%20icon> (last accessed September 2, 2025). Users can see this data as a graphical representation over the last 10 seconds, helping them identify areas of weak cellular coverage, potential dead zones, or issues with Wi-Fi connections. *See id.* Signal strength is also displayed as a percentage of good, very good, okay, not good, or unusable based on dBm values in the agent app's Network screen. *See id.* The Accused Knox Products, for example, include "mobile signal strength" data (a type of performance or quality of service information for one or more specific locations), which enables the identification of "devices situated in areas with weak cellular coverage or potential dead zones." *See id.*

F **Mobile signal strength**

Let's you identify when devices are situated in areas with weak cellular coverage or potential dead zones. To use this feature, you must first enable **Mobile signal strength with location**.

On the map, you'll see the mobile signal strength status of every device in your fleet represented by colored dots. These dots are updated at the same rate as your location data collection frequency.

- **Good (green):** -70 dBm or higher
- **Normal (blue):** -71 dBm to -80 dBm
- **Bad (red):** -81 dBm to -139 dBm
- **No signal (grey):** -140 dBm or lower, no collection

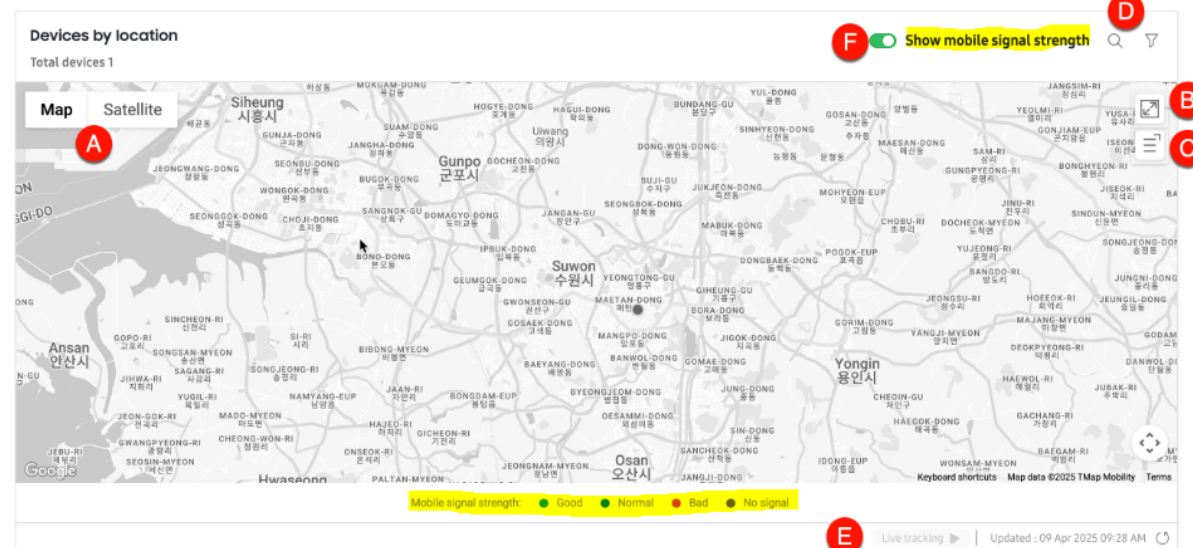
These dots also appear in the map's **Device list**, letting you quickly correlate the device IDs with each mobile signal strength status. If you want to only show devices with a specific status—for example, only show **Bad** devices—you can select the status using the map's **Filter** options next to the Search icon.

Samsung Knox Documentation, Knox Asset Intelligence, Dashboard, Location dashboard, Use location dashboard, <https://docs.samsungknox.com/admin/knox-asset-intelligence/dashboard/location-dashboard/use-the-location-dashboard/#:~:text=To%20use%20this%20feature%2C%20you,next%20to%20the%20Search%20icon> (last accessed September 2, 2025).

The Accused Knox Products further provide admin interfaces, via dashboards (e.g., location dashboards) that include maps of device distributions across a given area. Mobile signal strength data can be displayed via such maps, which enables customers to quickly correlate device IDs with each mobile signal strength statuses. This further illustrates how the Accused Knox Products utilize performance or quality of service information associated with specific locations. See Samsung Knox Documentation, Knox Asset Intelligence, Dashboard, Location dashboard, Use location dashboard, <https://docs.samsungknox.com/admin/knox-asset-intelligence/dashboard/location-dashboard/use-the-location-dashboard/#:~:text=To%20use%20this%20feature%2C%20you,next%20to%20the%20Search%20icon> (last accessed September 2, 2025).

Location map

The map displays your device groupings (represented by gray circles on the map) as soon as you open the **Location** dashboard. When you zoom in, the circles updates to show the device distribution across a given area.

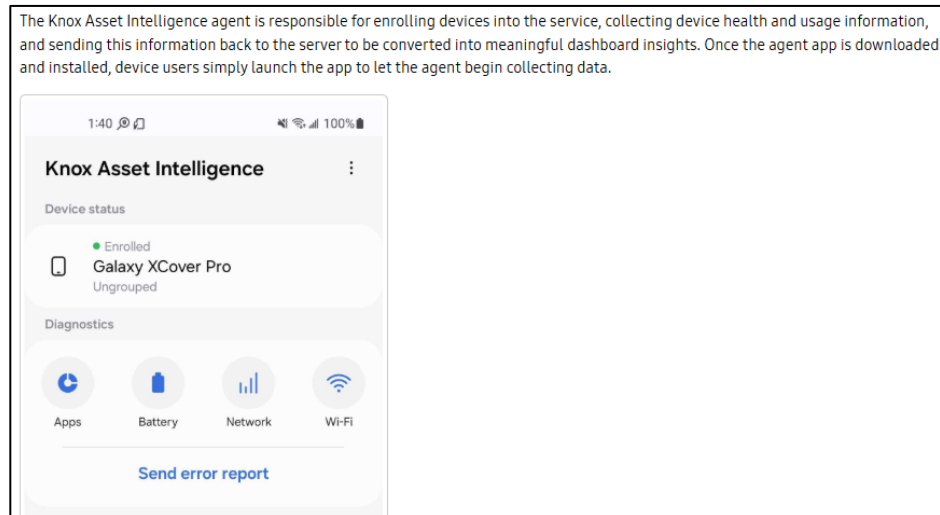


Samsung Knox Documentation, Knox Asset Intelligence, Dashboard, Location dashboard, Use location dashboard, <https://docs.samsungknox.com/admin/knox-manage/introduction/features-and-key->

[strengths/#:~:text=Effortless%20content%20management,Storage%20of%20device%20analysis%20data](#)
(last accessed September 2, 2025).

The Accused Knox Products allow the EMM application on the managed mobile device to provide network performance information to the IT admin through the EMM console, where the IT admin can monitor managed devices through the EMM console, such as signal strength at geographic locations (See claim element [20A] above).

The document below describes that the EMM application on the managed mobile device can collect health and network information associated with the performance of the managed mobile device and send the information to the Knox server. The collected information is provided to the IT Admin through various dashboards in the EMM console, allowing the IT admin to monitor the managed mobile devices through the EMM console.



See <https://docs.samsungknox.com/admin/knox-asset-intelligence/how-to-guides/use-the-agent-app/>

The document excerpt below describes that the managed mobile device can receive commands at the EMM application on the device to provide data through a Knox API to the EMM console.

	<div data-bbox="709 191 1755 548"> <p>Manageability highlights</p> <p>Device management and deployment</p> <p>Enterprises with tens, hundreds, or thousands of employee mobile devices need to manage them easily, securely, and efficiently. Through EMM systems, IT admins can use a web console to centrally manage remote devices over-the-air. IT admins can control Samsung Knox devices comprehensively, managing device features with ease.</p> <p>This management is possible through the <u>Samsung Knox SDK</u>, which offers over 1300 APIs for granular and flexible control over Samsung devices. This functionality is on top of the basic APIs offered through the Android SDK, providing an even more powerful superset of capabilities. An EMM app on an employee device receives IT admin commands from the EMM web console, and calls Knox APIs to deploy commands on Knox devices. This integration enables enterprise IT admins to deploy IT policies to manage and secure every aspect of Knox devices.</p> </div> <p>Knox Whitepaper v1.5, p. 7 (annotated).</p>
--	---