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

| | | |
|---|---|---|
| AGIS SOFTWARE DEVELOPMENT LLC, | § | Case No. 2:22-cv-00263-JRG |
| Plaintiff, | § | **JURY TRIAL DEMANDED** |
| v. | § | |
| SAMSUNG ELECTRONICS CO., LTD. and SAMSUNG ELECTRONICS AMERICA, INC., | § | |
| Defendants. | § | |

**PLAINTIFF'S SECOND AMENDED COMPLAINT FOR PATENT INFRINGEMENT**

Pursuant to the Court's First Amended Docket Control Order (Dkt. 66), Plaintiff, AGIS Software Development LLC ("AGIS Software" or "Plaintiff") files this Second Amended Complaint against Defendants Samsung Electronics Co., Ltd. ("Samsung Electronics") and Samsung Electronics America, Inc. ("Samsung Electronics America") (collectively, "Samsung" or "Defendants") for patent infringement under 35 U.S.C. § 271 and alleges as follows:

**THE PARTIES**

1. Plaintiff AGIS Software is a limited liability company organized and existing under the laws of the State of Texas and maintains its principal place of business at 100 W. Houston Street, Marshall, Texas 75670. AGIS Software is the owner of all right, title, and interest in and to U.S. Patent Nos. 8,213,970, 9,467,838, 9,749,829, and 9,820,123 (the "Patents-in-Suit").

2. Defendant Samsung Electronics is a corporation organized and existing under the laws of the Republic of Korea, with its principal place of business at 129 Samsung-Ro, Yeongtong-Gu, Suwon-Si, Gyeonggi-Do, 443-742, Republic of Korea. Upon information and belief, Samsung Electronics does business in Texas, directly or through intermediaries, and offers its products

and/or services, including those accused herein of infringement, to customers and potential customers located in Texas, including in this Judicial District.

3. Defendant Samsung Electronics America is a corporation organized under the laws of New York, with its principal place of business at 85 Challenger Road, Ridgefield Park, New Jersey 07660. Upon information and belief, Samsung Electronics America has corporate offices in the Eastern District of Texas at 6625 Excellence Way, Plano, Texas 75023,[1] 2601 Preston Road, #1214, Frisco, Texas 75023,[2] 6625 Excellence Way, Plano, Texas 75023, 1303 East Lookout Drive, Richardson, Texas 75082, and 2800 Technology Drive, Suite 200, Plano, Texas 75074.

4. Defendants have authorized sellers and sales representatives that offer and sell products pertinent to this Complaint through the State of Texas, including in this Judicial District, and to consumers throughout this Judicial District, such as: Best Buy, 422 West TX-281 Loop, Suite 100, Longview, Texas 75605; AT&T Store, 1712 East Grand Avenue, Marshall, Texas 75670; Sprint Store, 1806 East End Boulevard North, Suite 100, Marshall, Texas 75670; T-Mobile, 900 East End Boulevard North, Suite 100, Marshall, Texas 75670; Verizon authorized retailers, including Russell Cellular, 1111 East Grand Avenue, Marshall, Texas 75670; Victra, 1006 East End Boulevard, Marshall, Texas 75670; and Cricket Wireless authorized retailer, 120 East End Boulevard South, Marshall, Texas 75670.

## JURISDICTION AND VENUE

5. This is an action for patent infringement arising under the patent laws of the United States, 35 U.S.C. §§ 1, *et seq*. This Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. §§ 1331, 1338(a), and 1367.

[1] https://news.samsung.com/us/samsung-electronics-america-open-flagship-north-texas-campus/
[2] https://news.samsung.com/us/new-frisco-tx-samsung-experience-store-open-galaxy/

6. This Court has specific and personal jurisdiction over each of the Defendants consistent with the requirements of the Due Process Clause of the United States Constitution and the Texas Long Arm Statute. Upon information and belief, each Defendant has sufficient minimum contacts with the forum because each Defendant transacts substantial business in the State of Texas and in this Judicial District. Further, each Defendant has, directly or through subsidiaries or intermediaries, committed and continues to commit acts of patent infringement in the State of Texas and in this Judicial District as alleged in this Complaint, as alleged more particularly below.

7. Venue is proper in this Judicial District pursuant to 28 U.S.C. §§ 1391 and 1400(b) because Defendants are subject to personal jurisdiction in this Judicial District, have committed acts of patent infringement in this Judicial District, and have regular and established places of business in this Judicial District. Defendants, through their own acts and/or through the acts of others, make, use, sell, and/or offer to sell infringing products within this Judicial District, regularly do and solicit business in this Judicial District, and have the requisite minimum contacts with this Judicial District, such that this venue is a fair and reasonable one. Further, on information and belief, Defendants have admitted or not contested proper venue in this Judicial District in other patent infringement actions.

## PATENTS-IN-SUIT

8. On July 3, 2012, the United States Patent and Trademark Office duly and legally issued U.S. Patent No. 8,213,970 (the "'970 Patent") entitled "Method of Utilizing Forced Alerts for Interactive Remote Communications." On September 1, 2021, the United States Patent and Trademark Office issued an *Inter Partes* Review Certificate for the '970 Patent cancelling claims 1 and 3-9. On December 9, 2021, the United States Patent and Trademark Office issued an *Ex Parte* Reexamination Certificate for the '970 Patent determining claims 2 and 10 (as amended)

and claims 11-13 to be valid and patentable. A true and correct copy of the '970 Patent, which includes the September 1, 2021 *Inter Partes* Review Certificate and the December 9, 2021 *Ex Parte* Reexamination Certificate, is attached hereto as **Exhibit A**.

9. On October 11, 2016, the United States Patent and Trademark Office duly and legally issued U.S. Patent No. 9,467,838 (the "'838 Patent") entitled "Method to Provide Ad Hoc and Password Protected Digital and Voice Networks." On May 27, 2021, the United States Patent and Trademark Office issued an *Ex Parte* Reexamination Certificate for the '838 Patent confirming the validity and patentability of claims 1-84. A true and correct copy of the '838 Patent, which includes the May 27, 2021 *Ex Parte* Reexamination Certificate, is attached hereto as **Exhibit B**.

10. On August 29, 2017, the United States Patent and Trademark Office duly and legally issued U.S. Patent No. 9,749,829 (the "'829 Patent") entitled "Method to Provide Ad Hoc and Password Protected Digital and Voice Networks." On August 16, 2021, the United States Patent and Trademark Office issued an *Ex Parte* Reexamination Certificate for the '829 Patent confirming the validity and patentability of claims 1-68. A true and correct copy of the '829 Patent, which includes the August 16, 2021 *Ex Parte* Reexamination Certificate, is attached hereto as **Exhibit C**.

11. On November 14, 2017, the United States Patent and Trademark Office duly and legally issued U.S. Patent No. 9,820,123 (the "'123 Patent") entitled "Method to Provide Ad Hoc and Password Protected Digital and Voice Networks." On September 24, 2021, the United States Patent and Trademark Office issued an *Ex Parte* Reexamination Certificate for the '123 Patent confirming the validity and patentability of claims 1-48. A true and correct copy of the '123 Patent, which includes the September 24, 2021 *Ex Parte* Reexamination Certificate, is attached hereto as **Exhibit D**.

12. AGIS is the sole and exclusive owner of all right, title, and interest in the Patents-in-Suit, and holds the exclusive right to take all actions necessary to enforce its rights to the Patents-in-Suit, including the filing of this patent infringement lawsuit. AGIS also has the right to recover all damages for past, present, and future infringement of the Patents-in-Suit and to seek injunctive relief as appropriate under the law.

## FACTUAL ALLEGATIONS

13. Malcolm K. "Cap" Beyer, Jr., a graduate of the United States Naval Academy and a former U.S. Marine, is the CEO of AGIS Software and a named inventor of the AGIS patent portfolio. Mr. Beyer founded Advanced Ground Information Systems, Inc. ("AGIS, Inc.") shortly after the September 11, 2001 terrorist attacks because he believed that many first responder and civilian lives could have been saved through the implementation of a better communication system. He envisioned and developed a new communication system that would use integrated software and hardware components on mobile devices to give users situational awareness superior to systems provided by conventional military and first responder radio systems.

14. AGIS, Inc. developed prototypes that matured into its LifeRing system. LifeRing provides first responders, law enforcement, and military personnel with what is essentially a tactical operations center built into hand-held mobile devices. Using GPS-based location technology and existing or special-purpose cellular communication networks, LifeRing users can exchange location, heading, speed, and other information with other members of a group, view each other's locations on maps and satellite images, and rapidly communicate and coordinate their efforts.

15. AGIS Software licenses its patent portfolio, including the '970, '838, '829, and '123 Patents, to AGIS, Inc. AGIS, Inc. has marked its products accordingly. AGIS Software and

all previous assignees of the Patents-in-Suit have complied with the requirements of 35 U.S.C. § 287(a).

16. Samsung licenses the Android operating system and related applications and services for use on or in conjunction with Samsung's Android-based devices, including but not limited to the devices listed herein. The Android operating system is the most widely used in smartphones and other mobile devices in the United States.[3]

17. Defendants manufacture, use, sell, offer for sale, and/or import into the United States the Samsung Tactical, TAK, ATAK, and CivTAK, applications, products, and solutions, which also include related servers and services for supporting Samsung Tactical, TAK, ATAK, and CivTAK and Samsung Knox (collectively, the "Accused Products"). Further, Defendants manufacture, use, sell, offer for sale, and/or import into the United States electronic devices, all of which are configured and/or adapted with certain map-based communication applications, products, and solutions such as Samsung Tactical, TAK, ATAK, and CivTAK and Samsung Knox, such as the Galaxy S20 Tactical Edition, Galaxy XCover FieldPro, Galaxy XCover Pro, GT-I7500 Galaxy, i5700 Galaxy Spica, Galaxy S, Galaxy SL, Galaxy S II, Galaxy S Advance, Galaxy S III, Galaxy S Duos, Galaxy S III Mini, Galaxy S II Plus, Galaxy S4, Galaxy S4 Active, Galaxy S4 Mini, Galaxy S4 Zoom, Galaxy S Duos 2, Galaxy S III Slim, Galaxy S5, Galaxy S III Neo, Galaxy S5 Active, Galaxy S5 Mini, Galaxy S Duos 3, Galaxy S5 Plus, Galaxy S6, Galaxy S6 Edge, Galaxy S5 Neo, Galaxy S6 Active, Galaxy S6 Edge+, Galaxy S7, Galaxy S7 Edge, Galaxy S7 Active, Galaxy S8, Galaxy S8+, Galaxy S8 Active, Galaxy S9, Galaxy S9+, Galaxy S10e, Galaxy S10, Galaxy S10+, Galaxy S10 5G, Galaxy S21, Galaxy S20 FE, Galaxy S20 Ultra 5G, Galaxy S20+

[3] https://www.statista.com/statistics/266572/market-share-held-by-smartphone-platforms-in-the-united-states/.

5G, Galaxy S21 5G, Galaxy S21+ 5G, Galaxy S21 Ultra 5G, Galaxy S21 FE 5G, Galaxy S22, Galaxy S22+, Galaxy S22 Ultra, Galaxy S23, Galaxy S23+, Galaxy S23 Ultra, Galaxy Alpha, Galaxy A3, Galaxy A5, Galaxy A7, Galaxy A8, Galaxy A3, Galaxy A5, Galaxy A7, Galaxy A8, Galaxy A8+, Galaxy A6, Galaxy A6+, Galaxy A8 Star, Galaxy A7, Galaxy A9, Galaxy A6s, Galaxy A8s, Galaxy A30, Galaxy A50, Galaxy A10, Galaxy A20, Galaxy A40, Galaxy A70, Galaxy A20e, Galaxy A80, Galaxy A40s, Galaxy A60, Galaxy A10s, Galaxy A20s, Galaxy A10e, Galaxy C5, Galaxy C7, Galaxy C9, Galaxy C9 Pro, Galaxy C7 Pro, Galaxy C5, Pro, Galaxy C8, Galaxy J, Galaxy J1, Galaxy J5, Galaxy J7, Galaxy J2, Galaxy J1 Ace, Galaxy J1 Nxt, Galaxy J1 Mini, Galaxy J5 (2016), Galaxy J3 Pro, Galaxy J7, Galaxy J Max, Galaxy J1 Ace Neo, Galaxy J1 (2016), Galaxy J5 Prime, Galaxy J7, Prime, Galaxy J1 Mini Prime, Galaxy J2 Prime, Galaxy J3 Emerge, Galaxy J7 V, Galaxy J3 Prime, Galaxy J7 Pro, Galaxy J7 Max, Galaxy J7 Nxt, Galaxy J3 Luna Pro, Galaxy J7 Sky Pro, Galaxy J7+, Galaxy J2 Pro, Galaxy J7 Prime 2, Galaxy J7 Duo, Galaxy J4, Galaxy J6, Galaxy J3 (2018), Galaxy J7 (2018), Galaxy J2 Core, Galaxy J4+, Galaxy J6+, Galaxy J4 Core, Galaxy M, Galaxy M10, Galaxy M20, Galaxy M30, Galaxy M40, Galaxy E5, Galaxy E7, Galaxy Grand, Galaxy Core, Galaxy Core Plus, Galaxy Grand 2, Galaxy Grand Neo, Galaxy Core Prime, Galaxy Grand Prime Plus, Galaxy Grand Prime Pro, Galaxy Mega 5.8, Galaxy Mega 6.3, Galaxy Mega 2, Galaxy Mini, Galaxy Mini 2, Galaxy Trend, Galaxy Trend Lite, Galaxy Trend Plus, Galaxy Ace, Galaxy Ace Plus, Galaxy Ace 2, Galaxy Ace 3, Galaxy Ace Style, Galaxy Ace 4, Galaxy On7, Galaxy On5, Galaxy On5 Pro, Galaxy On7 Pro, Galaxy On8, Galaxy On Nxt, Galaxy On Max, Galaxy On7 Prime, Galaxy On6, Galaxy On8 (2018), Galaxy R, Galaxy R Style, Galaxy Y, Galaxy Y Duos, Galaxy Young, Galaxy Young 2, Galaxy Pocket, Galaxy Pocket Plus, Galaxy Pocket Neo, Galaxy Pocket Duos, Galaxy Pocket 2, Galaxy U, Galaxy Neo, Galaxy Pro, Galaxy Precedent, Galaxy Z, Galaxy Rush, Galaxy 5, Galaxy W, Galaxy Fit, Galaxy

Gio, Galaxy Prevail, Galaxy Nexus, Galaxy Discover, Galaxy Reverb, Galaxy Stellar, Galaxy Appeal, Galaxy Express, Galaxy Express 2, Galaxy Fame, Galaxy Star, Galaxy Win, Galaxy Win Pro, Galaxy Star Pro, Galaxy Fame Lite, Galaxy Round, Galaxy Light, Galaxy V, Galaxy V Plus, Galaxy V2, Galaxy K Zoom, Galaxy Folder, Galaxy Active Neo, Galaxy Folder 2, Galaxy Fold, Galaxy Note, Galaxy Note II, Galaxy Note 3, Galaxy Note 4, Galaxy Note Edge, Galaxy Note 5, Galaxy Note 7, Galaxy Note Fan Edition, Galaxy Note 8, Galaxy Note 9, Galaxy Note 10, Galaxy Note 10+, Galaxy Note 10+ 5G, Galaxy Tab, Galaxy Tab 7.0, Galaxy Tab 10.1, Galaxy Tab 10.1N, Galaxy Tab 10.1v, Galaxy Tab 8.9, Galaxy Tab 7.0 Plus, Galaxy Tab 7.7, Galaxy Tab 2 7.0, Galaxy Tab 2 10.1, Galaxy Tab 3 7.0, Galaxy Tab 3 Lite 7.0, Galaxy Tab 3 8.0, Galaxy Tab 3 10.1, Galaxy Tab 4 7.0, Galaxy Tab 4 8.0, Galaxy Tab 4 10.1, Galaxy Tab Pro 8.4, Galaxy Tab Pro 10.1, Galaxy Tab Pro 12.2, Galaxy Tab S 8.4, Galaxy Tab S 10.5, Galaxy Tab S2 8.0, Galaxy Tab S2 9.7, Galaxy Tab S3 9.7, Galaxy Tab S4 10.5, Galaxy Tab E 8, Galaxy Tab E 9.6, Galaxy Tab A 8.0, Galaxy Tab A 9.7, Galaxy Tab A 6.0, Galaxy Tab A 7.0, Galaxy Tab A 10.1, Galaxy Tab A 10.5, Galaxy Tab Pro S 12.0, Galaxy Book 10.6, Galaxy Book 12.0, Galaxy Tab Active, Galaxy Tab Active 2, Galaxy View, Galaxy Note 8.0, Galaxy Note 10, Galaxy Note 10.1, Galaxy Note Pro 12.2, Galaxy Gear, Gear Sport, Gear S3 Frontier, Galaxy Watch, Galaxy Watch Active, and Galaxy Watch Active 2. These Galaxy devices are also Accused Products. The Accused Products comprise any and all versions of the Tactical, TAK, ATAK, and CivTAK solutions, applications, and services including but not limited to, the ATAK-CIV, ATAK-MIL, and ATAK-MIL versions, and Samsung Knox, including Samsung Knox Guard. The Accused Products, which include software components such as, but not limited to, Samsung Tactical, TAK, and ATAK solutions and Samsung Knox, are configured to interact with Defendants' servers which provide corresponding services related to at least Samsung Tactical, TAK, and ATAK and

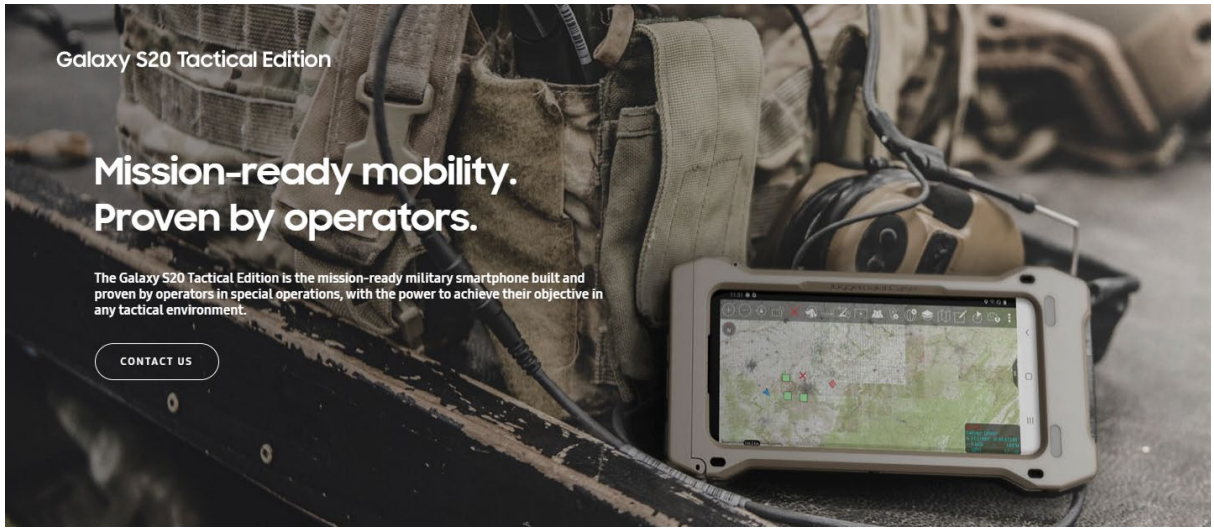
Samsung Knox utilized by Samsung's customers when operating the Accused Products, such as the Galaxy devices identified herein. Such servers, which are made, sold, used, offered for sale, and/or imported into the United States by Defendants, are also Accused Products.

18. The Accused Products include Find My Device,[4] an application provided on all Samsung devices with Android operating systems, including but not limited to the above-listed Accused Products.[5] To date, Find My Device can be located on each Samsung Android-based device by navigating, for example, to Settings > Google > Security > Find My Device. Find My Device is configured to interact with Defendants' servers (which, on information and belief, include third party servers through license or other agreement) which provide corresponding services related to at least Find My Device, utilized by Samsung's customers when operating the Accused Products, such as the above-listed Accused Products identified herein.

19. The Accused Products include functionalities that allow users to form and/or join networks or groups, share and view locations with other users, display symbols corresponding to locations (including locations of other users) on a map, and communicate with other users via text, voice, and multimedia-based communication. Additionally, the Accused Products include functionalities to allow users to form and/or join networks or groups. The Accused Products include the functionalities to display map information, including symbols corresponding with users, entities, and locations. Additionally, the Accused Products include functionalities to form groups that include their own devices in order to track, remotely monitor and control, and/or communicate with other users' devices. The Accused Products include functionalities to enable

[4] AGIS's allegations against Find My Device are limited to the '970 and '838 Patents.
[5] *See* https://www.android.com/certified/partners/

communications, such as voice calls between users. The Accused Products practice the claims of the Asserted Patents to improve user experiences and to improve Samsung's position in the market.



**Interoperable**

Easily connect to tactical radios and mission systems, out of the box, for persistent communications in multi-domain environments.

LEARN MORE ›

**Versatile**

Run mission applications in the field and enterprise applications everywhere else with a single device to meet all your mission requirements.

LEARN MORE ›

**Command and Control**

Deliver complete and accurate real-time intelligence where it's needed most with a powerful, compact End User Device (EUD) that enhances precision and effectiveness.

LEARN MORE ›

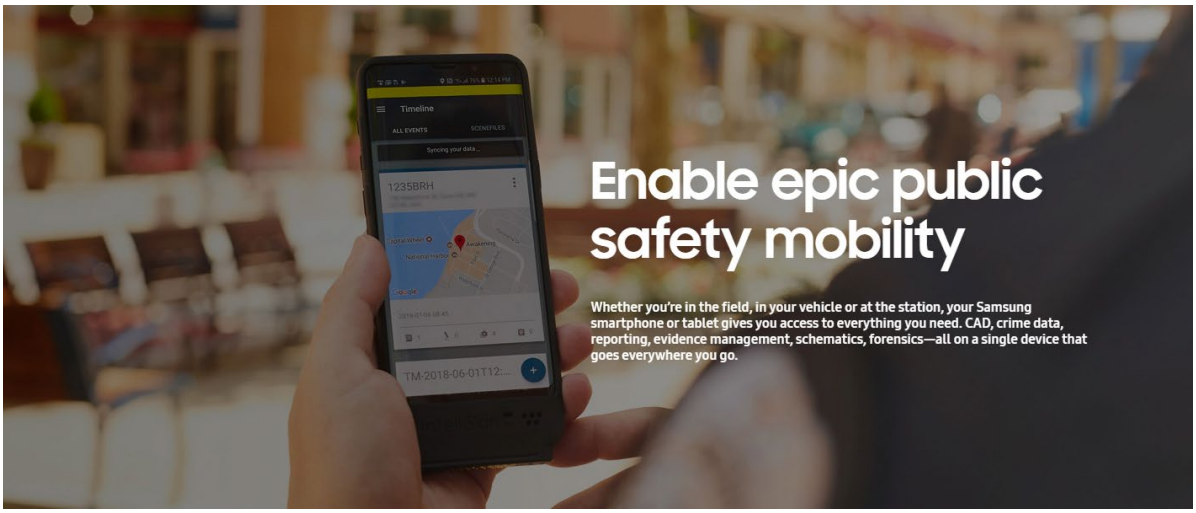
**Tested & proven**

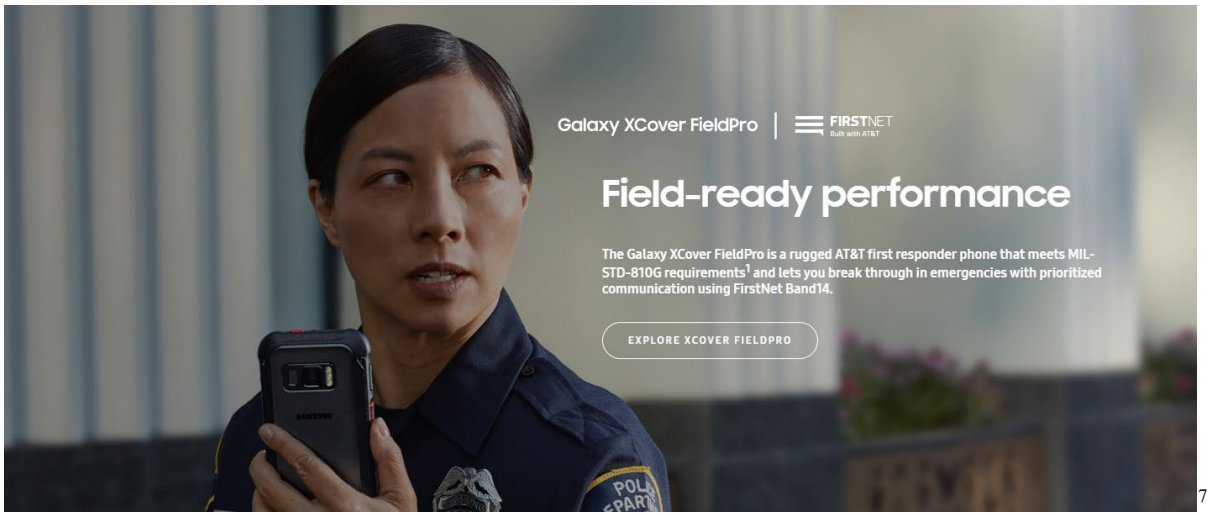
Trust the only COTS military smartphone that's protected by Knox, certified for use in classified communications and proven operationally ready by special forces.

LEARN MORE ›

6

[6] https://www.samsung.com/us/business/solutions/industries/government/tactical-edition/



[7]

[7] https://www.samsung.com/us/business/solutions/industries/public-safety/smartphones-tablets/?cid=com-btb-sky-blg-us-other-na-100219-112001-na-na-na&attributioncampaignid=7011Q000001VMa2QAG

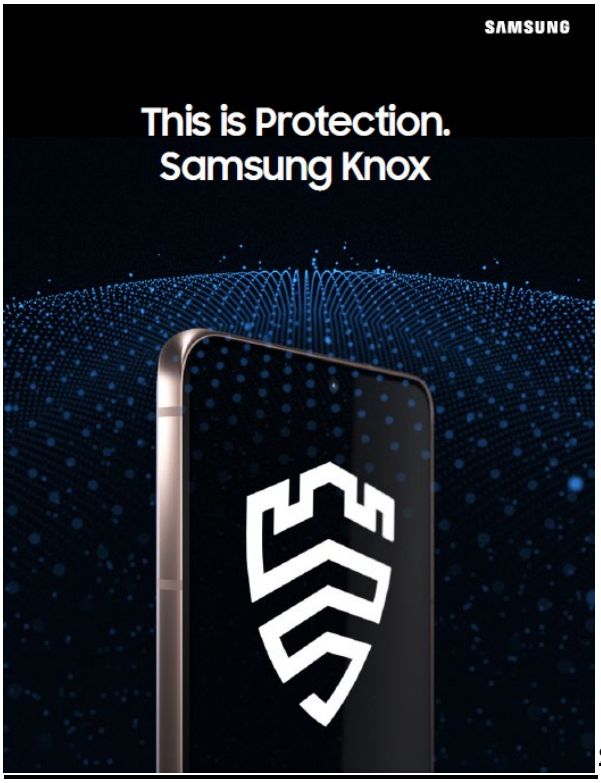
TAK
Distribution Statement A: Approved for public release; distribution is unlimited.

## WHAT IS TAK?

The Android Team Awareness Kit (ATAK), for civilian use, or Android Tactical Assault Kit (also ATAK) for military use - is a suite of software that provides geospatial information and allows user collaboration over geography.

ATAK was originally developed by the Air Force Research Laboratory (AFRL) and is now maintained by the TAK Product Center (TPC).

[8]




[9]

[8] https://www.civtak.org/atak-about/
[9] https://kp4-cdn.samsungknox.com/resource/Samsung%20Knox%20Security%20Handbook_bx4Z.pdf.

# Find, lock, or erase a lost Android device

If you lose an Android phone or tablet, or Wear OS watch, you can find, lock, or erase it. If you've added a Google Account to your device, Find My Device is automatically turned on. If you allow Find My Device to encrypt your phone's most recent location and store it with Google, your device's most recent location is available to the first account activated on the device.

**Tip:** To find, lock, or erase your Wear OS device, connect it to WiFi or mobile data.

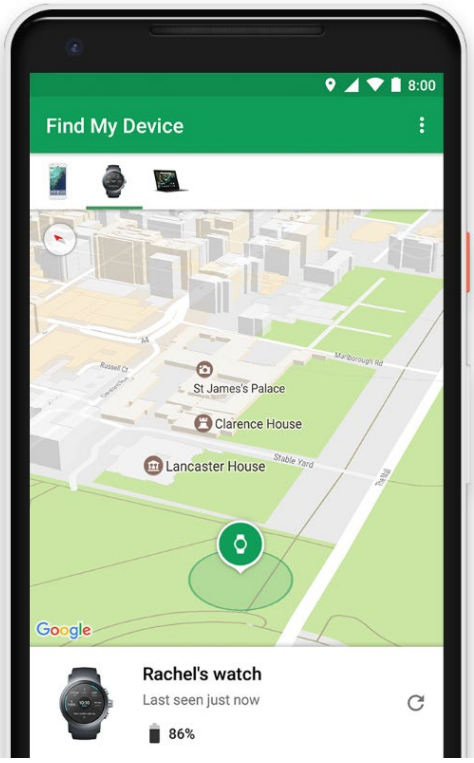
Learn about how to find an Android device.

To find an Android device, make sure that device:

- Is signed in to a Google Account
- Has Location turned on
- Has Find My Device turned on
- Has power and is connected to mobile data or WiFi.
  - If your device is off or isn't connected to mobile data or WiFi, you may still find its most recent location if you've enabled "Store recent location." Learn more about 2-step verification backups.
- Is visible on Google Play

10

Locate your phone, tablet or watch




1112

**COUNT I**
**(Infringement of the '970 Patent)**

20. Paragraphs 1 through 19 are incorporated herein by reference as if fully set forth in their entireties.

21. AGIS Software has not licensed or otherwise authorized Defendants to make, use, offer for sale, sell, or import any Accused Products and/or products that embody the inventions of the '970 Patent.

22. Defendants infringe, contribute to the infringement of, and/or induce infringement of the '970 Patent by making, using, selling, offering for sale, distributing, exporting from, and/or importing into the United States products and/or methods covered by one or more claims of the '970 Patent including, but not limited to, the Accused Products.

23. Defendants have and continue to directly infringe at least claim 10 of the '970 Patent, either literally or under the doctrine of equivalents, by making, using, selling, offering for sale, distributing, exporting from, and/or importing into the United States the Accused Products without authority and in violation of 35 U.S.C. § 271(a).

24. Defendants have and continue to indirectly infringe at least claim 10 of the '970 Patent by actively, knowingly, and intentionally inducing others to directly infringe, either literally or under the doctrine of equivalents, by making, using, selling, offering for sale, distributing, exporting from, and/or importing into the United States the Accused Products and by instructing users of the Accused Products to perform methods claimed in the '970 Patent. For example, Defendants, with knowledge that the Accused Products infringe the '970 Patent at least as of the

[10] https://support.google.com/android/answer/6160491
[11] https://play.google.com/store/apps/details?id=com.google.android.apps.adm&hl=en_US&gl=US
[12] https://www.att.com/device-support/article/wireless/KM1474177/Samsung/SamsungSMA536U

date of this Complaint, actively, knowingly, and intentionally induced, and continue to knowingly and intentionally induce direct infringement of the '970 Patent in violation of 35 U.S.C. § 271(b).

25. For example, Defendants have indirectly infringed and continue to indirectly infringe at least claim 10 of the '970 Patent in the United States because Defendants' customers use the Accused Products, including at least the Samsung Tactical, TAK, ATAK applications and services and Find My Device, alone or in conjunction with additional Accused Products, in accordance with Defendants' instructions and thereby directly infringe at least claim 10 of the '970 Patent in violation of 35 U.S.C. § 271. Defendants directly and/or indirectly intentionally instruct their customers to infringe through training videos, demonstrations, brochures, installations and/or user guides, such as those located at one or more of the following: https://www.samsung.com/us/business/solutions/industries/government/tactical-edition/#COMMAND_AND_CONTROL; https://www.samsung.com/us/business/solutions/services/mobility-software/e-fota/; https://image-us.samsung.com/SamsungUS/samsungbusiness/pdfs/brochures/S20_TE-tactical-brochure-FINAL_July_2021.pdf; https://insights.samsung.com/2021/09/01/atak-enhances-collaboration-and-awareness-for-public-safety-2/; https://www.civtak.org/atak-about/; https://www.civtak.org/documentation/; https://wiki.civtak.org/index.php?title=ATAK_Manual; https://www.pargovernment.com/tactical-sa/docs/S20_brochure.pdf; https://insights.samsung.com/2021/09/22/7-ways-samsungs-galaxy-xcover-pro-supports-first-responders/; https://kp4-cdn.samsungknox.com/resource/Samsung%20Knox%20Security%20Handbook_bx4Z.pdf; https://docs.samsungknox.com/admin/knox-manage/faqs/faq-115013698467.htm; https://docs.samsungknox.com/admin/knox-manage/locate-devices.htm;

https://downloadcenter.samsung.com/content/UM/202303/20230320235240461/SAM_S901_S906_S908_EN_UM_OS13_012323_FINAL_AC.pdf; https://www.att.com/device-support/article/wireless/KM1474177/Samsung/SamsungSMA536U; https://ss7.vzw.com/is/content/VerizonWireless/Devices/Samsung/note/samsung-galaxy-note9-ug.pdf; https://ss7.vzw.com/is/content/VerizonWireless/Devices/Samsung/note/samsung-galaxy-note9-ug.pdf; and Samsung agents and representatives located within this Judicial District. Defendants are thereby liable for infringement of the '970 Patent under 35 U.S.C. § 271(b).

26. For example, Defendants directly infringe and/or indirectly infringe by instructing their customers to infringe by performing claim 10 of the '970 Patent, including: a method of receiving, acknowledging and responding to a forced message alert from a sender PDA/cell phone to a recipient PDA/cell phone, wherein the receipt, acknowledgment, and response to said forced message alert is forced by a forced message alert software application program, said method comprising the steps of: receiving an electronically transmitted electronic message; identifying said electronic message as a forced message alert, wherein said forced message alert comprises a voice or text message and a forced message alert application software packet, which triggers the activation of the forced message alert software application program within the recipient PDA/cell phone; transmitting an automatic acknowledgment of receipt to the sender PDA/cell phone, which triggers the forced message alert software application program to take control of the recipient PDA/cell phone and show the content of the text message and a required response list on the display recipient PDA/cell phone or to repeat audibly the content of the voice message on the speakers of the recipient PDA/cell phone and show the required response list on the display recipient PDA/cell phone; and transmitting a selected required response from the response list in order to allow the message required response list to be cleared from the recipient's cell phone

display, whether said selected response is a chosen option from the response list, causing the forced message alert software to release control of the recipient PDA/cell phone and stop showing the content of the text message and a response list on the display recipient PDA/cell phone and/or stop repeating the content of the voice message on the speakers of the recipient PDA/cell phone; displaying the response received from the PDA/cell phone that transmitted the response on the sender of the forced alert PDA/cell phone; and providing a list of the recipient PDA/cell phones that have automatically acknowledged receipt of a forced alert message and their response to the forced alert message; and displaying a geographical map with georeferenced entities on the display of the sender PDA/cell phone; obtaining location and status data associated with the recipient PDA/cellphone; and presenting a recipient symbol on the geographical map corresponding to a correct geographical location of the recipient PDA/cellphone based on at least the location data. For example, the Accused Products include features as shown below.

## Stay connected to what matters.

**Persistent communications**
The Galaxy S20 Tactical Edition is a COTS military smartphone with tailored software that easily connects to tactical radios and mission-critical devices, out of the box.

**Multi-ethernet capabilities**
Dedicated connections with multiple mission systems including laser range finders, external GPS devices, drones and more keep you connected in degraded and highly contested network environments.

**Next-generation networks**
As technologies evolve, you need a powerful, mission-ready device that can take full advantage of next-generation military networks. The Galaxy S20 Tactical Edition supports Private SIM, 5G, CBRS and is ready for Wi-Fi 6.

# Command and control

**Situational awareness**
The Galaxy S20 Tactical Edition integrates voice, video, and tactical data to provide a common operational picture of the battlespace. This complete and accurate real-time intelligence enhances the precision and effectiveness of your tactical teams.

**Tactical user experience**
Unique features found only on the Galaxy S20 Tactical Edition deliver fast and simple access to the information and applications operators need on-mission.

**Better intelligence**
The pro-grade 64 MP camera on the Galaxy S20 Tactical Edition allows you to discretely capture and share crisp high-resolution photo or 8K video intelligence, even in low light without the use of a flash. View and analyze intelligence in greater detail than ever before with the Galaxy S20 Tactical Edition's Dynamic AMOLED 2.0, a 120Hz[1] display.

**Extend your mission**
The Galaxy S20 Tactical Edition battery is 30% larger than the previous tactical solution and it's intelligent.[2] It optimizes your app usage in the field giving you extended power to complete the mission. When you need a recharge, Super Fast Charging[3] and fast Wireless Charging 2.0 give you power in a flash. And Wireless PowerShare allows you to easily charge a team member's phone in the field just by touching the devices.[4]

**Connect to tactical radios** - Protocols to support tactical radios and mission systems, out of the box.

**Tactical app quick launch** - Instantly expand or hide ATAK, APASS and other mission-critical applications at the push of a button.

**Night vision mode** – Turn on and off LED backlight when wearing night vision devices.

**Stealth mode** – Disable LTE and e-911 and mute all RF broadcasting for complete off-grid communications.

**Lock screen auto-rotate** - Unlock the device in landscape mode for easy access when mounted to the operator's chest.

**Auto-touch sensitivity** – Automatically adjust device operations to work with gloved hands.

# One device to meet all your mission requirements.

**Simple device management**
From device configuration, enrollment, customization and management to advanced mobile security controls and updates, Samsung has the mobility cloud services you need for every stage of the Galaxy S20 Tactical Edition lifecycle.[6] With Knox Services, you can keep pace and maintain control over devices and how they're used. You can manage devices in near real-time, configure settings, and remotely lock or wipe devices if lost or stolen, on the battlefield and anywhere else.

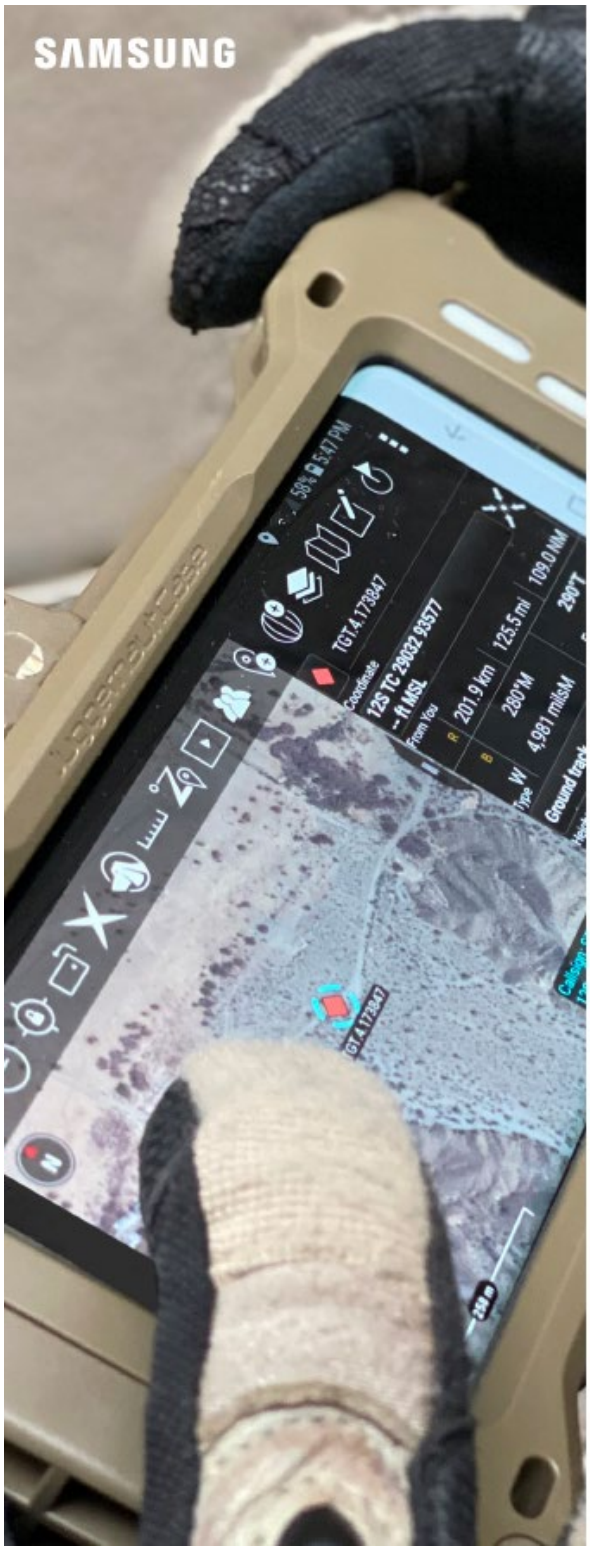
**Run mission apps and enterprise apps**
The Galaxy S20 Tactical Edition has a 64-bit Octa-Core processor with the speed and versatility to run multiple tactical applications in the field and enterprise applications everywhere else.

With Samsung DeX, connect your Galaxy S20 Tactical Edition to a monitor, keyboard and mouse for a desktop-like experience[5] ideally suited for mission planning, training, and everyday use. DeX gives you the power to work seamlessly across Microsoft Office Suite applications,[6] productivity apps, and virtual desktops with secure CAC-authenticated Virtual Desktop Infrastructure (VDI) sessions, all without a laptop.[7] And DeX-in-Vehicle transforms the Galaxy S20 Tactical Edition into a powerful in-vehicle computer.

**Open and secure**
The Galaxy S20 Tactical Edition is built on an open and secure Android operating system enabling seamless integration with a diverse ecosystem of tactical solution partners. Eliminate vulnerabilities with three software updates throughout the life of the device.

[13]

[13] https://www.pargovernment.com/tactical-sa/docs/S20_brochure.pdf




## Galaxy S20 Tactical Edition

# Mission-ready mobility. Proven by operators.

The Samsung Galaxy S20 Tactical Edition is the mission-ready military smartphone built and proven by operators in special operations. Based on the proven success of the S9 Tactical Edition for operators in the field, the S20 Tactical Edition is the only end user device you'll need for mission planning, training, operations and daily use.

### Persistent communications in any domain

**Purpose-built to connect to tactical radios** and mission systems out of the box, the Galaxy S20 Tactical Edition delivers a complete and accurate common operational picture. Run mission applications in the field and enterprise applications everywhere else with a single end user device for mission training, planning, operations and everyday use.

### Interoperable across devices and networks

**Pre-configured software, pre-loaded during the manufacturing process,** includes drivers to support tactical radios and mission-critical devices. Multi-ethernet capabilities provide dedicated connections to multiple mission systems including drone feeds, laser range finders, and external GPS. Support for current and next-generation networks includes Private SIM, 5G, WiFi 6 and CBRS. Allow or disallow USB peripherals based on product or vendor identifiers.

### Command and control

**Integrate voice, video and tactical data** for a complete view of the battlespace to enhance precision and effectiveness. Unique tactical features on the Galaxy S20 Tactical Edition include night-vision mode, stealth mode, lock screen autorotate, hostage negotiation mode, LTE band lock for consistent 4G connection, tactical application quick launch, to keep the operator focused on the objective, Standalone(5G)/Non-standalone (4G) modes to stay on preferred network. Preloaded tactical settings app. Ability to configure hotspot 2.0.

### Capture Intelligence

**A Pro-grade 64 MP camera** on the Galaxy S20 Tactical Edition enhances intel gathering, even in low-light environments without a flash. Capture high-resolution photos or sharp 8K video reconnaissance without giving away your position.

### Power to extend the mission

**Keep going wherever the mission takes you** with the Galaxy S20 Tactical Edition's intelligent2 4000mAh battery is 30% larger than the previous tactical solution and optimizes energy based on your device usage. Easily share power with a team member's smartphone in the field simply by touching devices using Wireless PowerShare.[4]

### One device to meet your requirements

**Run mission applications in the field** and enterprise applications everywhere else with the powerful and efficient Galaxy S20 Tactical Edition 64-bit Octa-Core processor. Connect your device to a monitor keyboard and mouse and use the power of Samsung DeX[5] for a desktop-like experience that is ideal for mission planning, training and everyday use. DeX-in-Vehicle transforms your Galaxy S20 Tactical Edition into an in-vehicle computer.

### Open and secure

**Enable a diverse ecosystem of tactical partners** with the open and secure Android operating system on the Galaxy S20 Tactical Edition. The all-new Tactical Settings feature simplifies device management, while Samsung Knox provides defense-grade security[6] from the hardware layer up and mission-specific device customization capabilities. The DualDAR architecture of the Galaxy S20 Tactical Edition provides two layers of encryption, even when the device is powered off, for securing up-to top secret level data on the device.

### Tested and proven

Samsung Galaxy Tactical Edition smartphones are tested and proven by special operators in the field. The Galaxy S20 Tactical Edition is certified to meet the most stringent requirements including NSA's CSFC Components List, NIAP Common Criteria/MDFPP, DODIN APL, FIPS 140-2, DISA Android 10 STIG, IP68 rating.

**Contact Us:** www.samsung.com/TacticalEdition

14

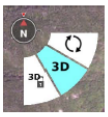
[14] https://image-us.samsung.com/SamsungUS/samsungbusiness/pdfs/flyer/S20_TE-salesflyer_FINAL_July_2021.pdf

## ATAK Civilian Overview

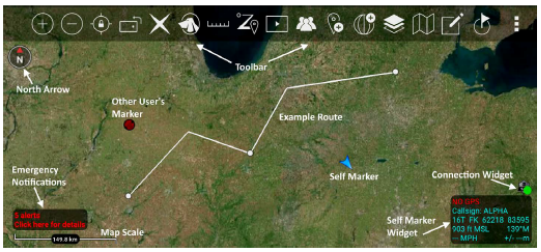
The Civilian Team Awareness Kit for Android (ATAK Civilian) is a Government-off-the-Shelf (GOTS) software application and mapping framework for mobile devices. ATAK Civilian has been designed and developed to run on Android smart devices used in a first responder environment. The ATAK Civilian software application is an extensible moving map display that integrates imagery, map and overlay information to provide enhanced collaboration and Situational Awareness (SA) over a tactical meshed network. ATAK Civilian promotes information flow and communications from the field environment to command enterprise locations.

The first time ATAK Civilian is opened, or after a Clear Content, a passphrase is auto-generated to activate data encryption. The user can supply their own passphrase by using Settings > Show All Preferences > Device Preferences > Change Encryption Passphrase. Following this step, ATAK Civilian's End User License Agreement (EULA) must be accepted. Next, the user will be prompted to change their callsign and/or import preferences or data from a Mission Package. All changes/imports can always be updated later. Finally, the user can place their self-marker by following the instructions located in the lower right corner.

The toolbar runs along the top of the map display. The features whose icons form the center portion of the toolbar are discussed in individual sections of this guide. The three dots at the right of the toolbar provide additional menu items that appear in a drop-down menu. A Long Press on the map will toggle the toolbar between hidden and visible.




The North Arrow appears in the upper left and is used to control map orientation. It has two primary modes: North Up/Track Up (default) and Manual Map Rotation/Lock. While in North Up/Track Up Mode, single press on the [**North Arrow**] icon to cycle between the North Up and Track Up map orientation. Long press the [**North Arrow**] to call out the additional controls menu where the Manual Rotation/Lock and 3D features are available. Select the [**Rotation**] button to enter Manual Map Rotation/Lock Mode. When in Manual Map Rotation/Lock Mode, rotate the map orientation by pressing on the map with two fingers and pivoting them in the desired direction. Single press on the [**North Arrow**] to lock the screen orientation, signified by the appearance of the lock icon, and again to unlock the orientation for further adjustment. 3D controls are discussed in a separate section.



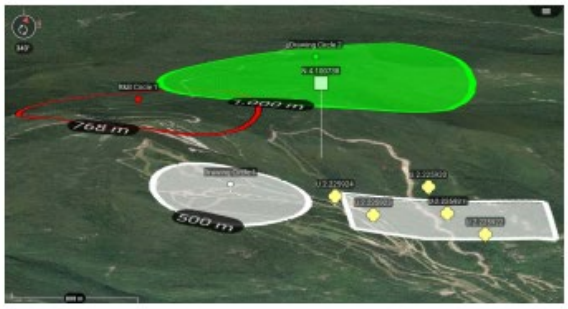

Select the [**Magnifier**] buttons to zoom in or out on the map. The map can also be zoomed by using two fingers on the screen to pinch and spread the map. Select the [**Back**] button to center the screen on the Self Marker or the [**Padlock**] icon to lock the center of the screen to the Self Marker. Select the [**Orientation**] icon to toggle the screen position between portrait and landscape.

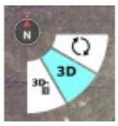
The optional connection widget indicates whether or not the user is connected to a TAK Server. This has a corresponding Android notification that provides the same information. Toggle this display on at Settings > Network Connections > Network Connections > Display Connection Widget.

Alerts and notifications are displayed in the lower left of the map interface.

The Map Scale displays a 1 inch to X mi/km reference on the map. The scale adjusts with the map when zoomed in and out. Hint windows are available to alert users to changes or make suggestions about the use of tools the first time they are opened.

## 3D View




ATAK Civilian features 3D viewing of terrain and map items (DTED required). To enable 3D view, long press on the **[North Arrow]** to call out the additional controls menu and select [**3D**]. A tilt angle indicator will appear around the edge of the [**North Arrow**] when 3D view is active. Touch the screen with two fingers and simultaneously swipe up or down on the screen to tilt the view angle. Once the appropriate viewing angle is set, select the [**3D Lock**] button to retain this view while panning the map. While viewing the map from an angle, some map items will appear raised above the map surface if they have defined elevations.

## 3D Models

ATAK Civilian supports the use of 3D models. OBJ models and other types from products such as Pix4D can be imported via the Import Manager or can be manually placed in the atak/overlays folder prior to startup. If using Import Manager browse to the .OBJ file and import only that file, or browse to a .ZIP file that contains the .OBJ file (and others) and import only that file. If using manual placement to the atak/overlays folder, place a .ZIP file containing the .OBJ file (and others) into the directory and they will be imported on startup.

Once imported, a 3D Model icon will appear on the map. Zoom into the area of the icon until a loading ring appears. After the loading process has finished, the 3D model will be projected onto the map. Enable the map 3D View and tilt the view angle to see the 3D modeling. Loaded 3D models will appear as their own category in Overlay Manager and can be toggled on/off or removed from there.

# Placement

The user can enter locations of interest using the Point Dropper tool. Select the [**Point Dropper**] icon to place internationally standardized markers and other icons on the map, edit the data and share the markers with other network members.

## Self-Marker

The Self-Marker is displayed as a blue arrowhead at the user's current location. The options available on the Self-Marker radial are: Compass Rose, Polar Coordinate Entry, Fine Adjust/Enter Coordinate/MGRS Location, GPS Error, Range & Bearing Line, GPS Lock to Self, Tracking Breadcrumbs, Place a Marker at the user's current location and Details. Other TAK users appear on the display as a colored circle. The color of the circle represents the user's Team affiliation, with additional lettering inside the circle to identify the role the user on the team. Team Member markers that include a diagonal line indicate that the GPS location is not available. A solid icon indicated that the team member has GPS reception.

Available roles include: Team Member, Team Lead (designated by a TL in the center of the marker), Headquarters (HQ in center), Sniper (S), Medic (+), Forward Observer (FO), RTO (R) or K9 (K9). The options available when another user's Self-Marker is selected are: Inner Ring – Delete, Polar Coordinate Entry, Fine Adjust/Enter Coordinate/MGRS Location, Range & Bearing Line, GPS Lock on Friendly, Video Player (if available), Communication Options (if configured by that user), Custom Threat Rings, Tracking Breadcrumbs and Details.

Outer Ring (Communication Options) – Data Package, Email, SMS Messaging, GeoChat, VOIP and Cellular Phone, when available.

## Point Dropper

Selecting the [**Point Dropper**] icon will open the Point Dropper menu, containing marker symbology with one or more icon sets, a Recently Added button and an Iconset Manager button.

The Markers symbology affiliations are: Unknown, Neutral, Red and Friendly. Select the affiliation, then a location on the map interface to drop the marker. To add a marker by manually entering coordinates, long press on the map interface and enter the MGRS location. Change the standard naming convention by entering values into the custom prefix and index fields or leave blank to use the defaults. If values are entered, the next marker will be dropped with the prefix name and starting number(s) or letter(s) and every subsequent marker will be assigned the next consecutive number(s) or letter(s).

The user can select the mission specific pallet to open point options including Waypoint (WP), Sensor or Observation Point (OP).

The user can move between icon sets by either swiping in the icon set area or selecting on the [**Iconset Name**] field to bring up the Icon Pallet drop-down.

The last point placed is shown at the bottom of the Point Dropper window. The information for all recently placed points can be accessed by selecting the [**Clock**] icon. This displays the marker icon, name, coordinates, elevation and range & bearing information. The user can send, rename or remove any recently added markers by selecting the [**Arrows**] next to the marker to reveal [**SEND**], [**RENAME**] or [**DEL**] buttons.

Select the [**Iconset Manager**] (gear) button to add or delete icon sets or to set the default Marker Mapping.

## Radial Menus

**Unknown Object**

**Neutral Object**

**Red Object**

**Friendly Object**

**Spot Object**

The options available for Unknown Object Markers are: Delete, Polar Coordinate Entry, Fine Adjust/Enter Coordinate/MGRS Location, Range & Bearing Line, Lock On, Tasking, Custom Threat Rings, Tracking Breadcrumbs and Details.

The options available for Neutral Object Markers are: Delete, Polar Coordinate Entry, Fine Adjust/Enter Coordinate/MGRS Location, Range & Bearing Line, Lock On, Tasking, Custom Threat Rings, Tracking Breadcrumbs and Details.

The options available for Red Object Markers are: Delete, Polar Coordinate Entry, Compass Rose/Bullseye, Fine Adjust/Enter Coordinate/MGRS Location, Range & Bearing Line, Tasking, Custom Threat Rings, Tracking Breadcrumbs and Details.

The options available for Friendly Object Markers are: Delete, Polar Coordinate Entry, Fine Adjust/Enter Coordinate/MGRS Location, Range & Bearing Line, Lock On, Video, Contact Card, Custom Threat Rings, Tracking Breadcrumbs and Details. The Video radial will activate if a properly formatted packet that includes the link to the video feed is included. Select the video radial to open the associated video. The Contact Card can be selected to display additional communication options, including GeoChat, Email, VoIP, SMS Messaging and Cellular Phone, when available.

The options available for Spot Map are: Delete, Fine Adjust/Enter Coordinate/MGRS Location, Range & Bearing Line, Nav-To, Custom Threat Rings, Labels and Details.

The options for User Defined Iconsets are: Delete, Polar Coordinate Entry, Fine Adjust/Enter Coordinate/MGRS Location, Range & Bearing Line, Lock On, Tasking, Custom Threat Rings. Tracking Breadcrumbs and Details.

Select [**Details**] on the marker radial to make desired modifications, including: Coordinate, Elevation, Name, Type and Remarks. Selecting Marker Type opens a dialog box with extra categories. File attachments, including images, can be associated with the object by selecting the [**Paperclip**] icon. Once all the desired modifications have been made, the Marker can be sent to other network members using [**Send**]. The information can be broadcast to all members or sent to specific recipients. Select the [**Auto Send**] option to broadcast the marker to other TAK users on the network, with updates automatically sent about once every 60 seconds.

## Bloodhound Tool

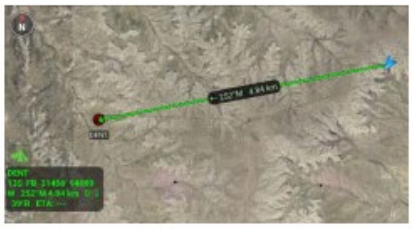
The Bloodhound Tool provides support for tracking and intercepting a map item. It allows the user to select two points on the map and/or map objects and display range & bearing information between the chosen tracker and the target.

Select the [**Bloodhound**] icon to open the Bloodhound Tool. A window will open, prompting the user to choose where to start by tapping the [**From Reticle**] (default = user's self marker) and where to bloodhound (track) to by tapping the [**To Reticle**].

Targets include map objects like other User's Self Markers, DPs, Markers, Shape center points, Range & Bearing endpoints and any other map objects. If the user selects a map location instead of an object as the target, Bloodhound will place a waypoint marker there. The self marker will then track towards the waypoint.

Select [**OK**] and Bloodhound will be activated.

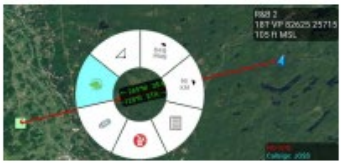
If either point moves, the green widget in the lower left will show the updated information. As the tracking object begins to navigate toward the target, the Estimated Time of Arrival (ETA) will update accordingly.



The green line showing the direct path from the tracker to the target will flash when the user-defined ETA outer threshold is reached (default = 6 minutes from target). The line will flash as the tracker continues toward the target until the next ETA threshold is reached (default = 3 minutes). The line will turn a flashing yellow until the final ETA threshold (default = 1 minute) is reached. The line then flashes red until the target is reached. Colors and thresholds can be modified in Settings > Tool Preferences > Bloodhound Preferences.

Selecting the green Bloodhound icon on the map will pan the map to the Bloodhound Range & Bearing Line. Disengage the Bloodhound Tool by selecting the [**Bloodhound**] icon on the toolbar.

## Multiple Bloodhound

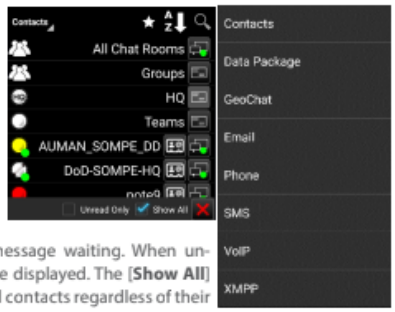


To create multiple bloodhounds, selecting the Range and Bearing Tool and select the [**R&B Line**] icon. Select two markers on the map and once the R&B line is created, select the line to bring up the radial. Select the [**Bloodhound**] radial, and the bloodhound information will be displayed on the R&B Line itself.

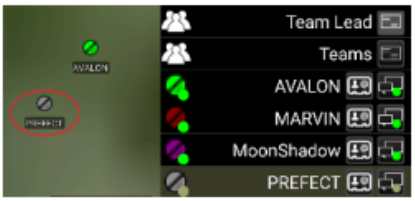
If either point moves, the Bloodhound information shown on the R&B Line will be updated. As the tracking object begins to navigate toward the target, the Estimated Time of Arrival (ETA) will update accordingly.

## Contacts

The Contacts list includes a variety of ways in which a user may communicate with other users, such as GeoChat (ATAK Civilian's built in Chat capability), Data Packages, Email, Phone, SMS, VoIP and XMPP.



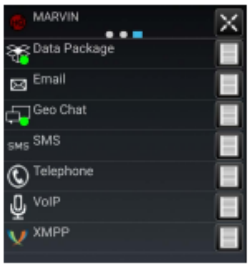

A default communication type (shown in the last column) may be selected and used until another type of communication is selected.




The Contacts list has two filters available at the bottom of the screen. The Unread Only box, when checked, will display only contacts with whom there are unread message waiting. When unchecked (default), all available contacts are displayed. The [**Show All**] box, when checked (default), will display all contacts regardless of their location. When unchecked, only contacts that are visible on current map screen will be displayed.

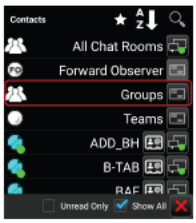
If a contact is no longer online, it will be indicated by changing the contact listing to a yellow color and the marker changes to gray both in the list and on the map.

Profile cards are accessed by selecting the second to last column in the Contacts list and are available for each contact. These contain additional information about that contact including: 1) role, software type and version installed, node type, default connector, last reported time, battery life; 2) location information, and 3) available types of communication.

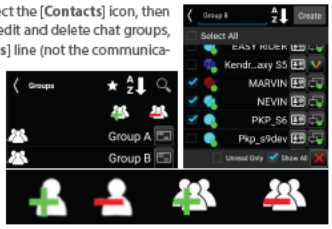


## GeoChat Group Management

Text-based Chat messages may be sent to active network members by using the GeoChat function. To enter GeoChat Group Management, select the [**Contacts**] icon and select [**GeoChat**] from the drop-down menu.

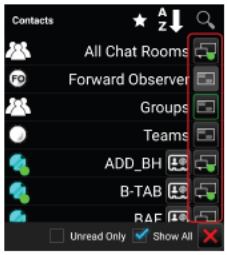



GeoChat Group Management is initiated through Contacts. Select the [**Contacts**] icon, then select GeoChat from the drop-down. The user can now create, edit and delete chat groups, as well as sub-groups. To create a chat group, select the [**Groups**] line (not the communications button). Select the [**Add Group**] icon to create the name of the group and add contacts to the group and then select [**Create**]. If a parent group is being created, no contacts need to be added at this level. To add a nested group, tap the parent group, select the [**Add Group**] icon to create the name of the sub-group and add contacts. Groups may be managed using the options to add/delete contacts or to add/delete GeoChat group.




To add users to a group, select the [**Groups**] line (not the communications button), then select the name of the group to add users. Select the [**Add Users**] icon. A window will open allowing the group creater to add users to the selected group. Select the [**Add**] button when all the users to be added are checked.

## GeoChat Messaging




Group and person-to-person messaging is available. To view messages from or send messages to an individual, tap on the desired contact's [**Communication**] icon. Selecting the [**Pan To**] icon, located at the top right of the call sign in an individual chat, will pan the map interface to that user's location. Select [**All Chat Rooms**] to view all messages from or send messages to those present on the network or TAK Server. Other groupings available for viewing or sending messages are: Forward Observer, Groups, HQ, K9, Medic, RTO, Sniper, Team Lead and Teams. If the user's current role is Forward Observer, HQ, K9, Medic, RTO, Sniper or Team Lead, that user can view or send messages to all other contacts with the same role. If a GeoChat message is sent from the top level of Teams, it will be sent to all contacts, similar to [**All Chat Rooms**].

When a sub-Team is chosen, messages can only be sent to that user's active (My Team) team color. When a parent group is chosen, messages are sent to all members of the parent group, as well as all of the sub-groups. When a sub-group is chosen, messages are sent only to members of the sub-group. Individuals within GeoChat may be removed from the Contacts menu by toggling the visibility of individuals or groups within Overlay Manager.





## GeoChat Messaging (continued)

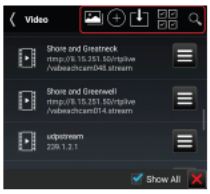
Selecting in the Free Text Entry area will open an onscreen keyboard. At the bottom of the Chat area are pre-defined messages that may be used to quickly create a message to send. Tap the current menu button to scroll through the different menus of canned messages, including: DFLT1, DFLT2, ASLT1, ASLT2, RECON1 and RECON2. These pre-defined messages present an easy way to transmit a brief message to other network members concerning position or other important communication. The pre-defined messages may be changed by long pressing on the button and changing its label and corresponding value.

A numbered red dot will appear on the [**Contacts**] icon when a message has been received successfully. The number denotes the number of unread messages that have been received. Select this icon to view the contact list. The user name who sent the message will appear with a numbered red dot next to their name. Alternatively, the text of the message can be read by dragging down from the top to see the Android notifications window. This notification will only stay available for a short time.

## Video Player

Select the **[Video Player]** icon to bring up the Video player. The Video Player supports playing video streams from IP cameras and H.264 encoders. The menu allows adding, editing, deleting, playing or sending videos to other network members.

Options for the video player include: viewing video snapshots, adding a new video alias, downloading an alias from the TAK Server, selecting the Multi-Select Action option to either Export or Delete aliases or searching for a specific alias.




Select the desired listed video alias or file name to begin playing the stored or streaming video. The video will display half the width of the screen.

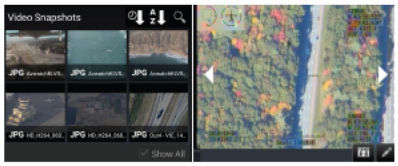
To view a video at full screen, slide the pull bar. To return to half screen, slide the pull bar back to the right.

Select the **[Back]** button to return to the list of available videos.

To add stored video file, select the **[Import Manager]** icon, select **[Local SD]**, and navigate to the video file and select **[OK]** to add the video to the list of available videos. The user can also manually place video files in "atak\tools\videos" to have them listed after ATAK is restarted. When a video is playing at half width, slide the pull bar to the right to hide the video but maintain the connection. Slide the pull bar to the left to unhide the video. The status of the video player is reflected in the main Android toolbar located at the top of the screen.

Select the **[Snapshot]** icon to save the current frame of the video as a JPEG image file, the icon will flash green to indicate that the snapshot has occurred. The file will be saved in the "\atak\tools\videosnaps" folder.

The user can view the saved snap shots by selecting the **[Video Snapshots]** icon. The user has the option of sorting the images by time taken or by the name of the snapshot. The user can also search within the snapshots taken by their name. By selecting an image, the image will be displayed within the window.




The user will have the options of cycling though the images, **[Send]** to a TAK user, or edit in **[Image Markup]**. (Image Markup would need to be installed.)

If a live UDP stream is being viewed, it can be recorded by tapping the **[Record]** icon. The icon will change to a green square while recording. Select the **[Green Square]** to end the recording. The recordings are saved in a folder in "\atak\tools\videos\".

**Note:** This is only available for UDP streams.

To close the video player, select the **[X]** located at the bottom right corner of the video player or select the **[Back]** button.





## Go To

Select the **[Go To]** icon to enter details and navigate to a specific location on the map.

Select from the **[MGRS]** (military grid reference system), **[DD]** (decimal degrees), **[DM]** (degrees- minutes), **[DMS]** (degrees-minutes-seconds), **[UTM]** (Universal Transverse Mercator) or **[ADDR]** tabs on the Go To interface and enter the location data of interest. The address provider name appears beneath the Elevation Data when the user selects the **[ADDR]** tab.

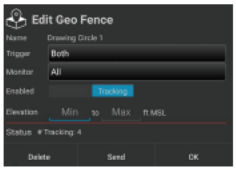
The user can enter the Latitude, Longitude and Elevation in the space provided for **[MGRS]** , **[DD]**, **[D-M]** or **[D-M-S]** searches. If DTED is installed, the elevation value can be automatically populated by tapping the **[Pull From DTED]** button.The user can select a desired marker type (Spot, Unknown, Neutral, Red, or Friendly) to be placed at the entered coordinates. If **[No Point]** is selected, the map will pan to the location but will not add a point.

**Note:** The address provider name appears beneath the Elevation Data when the user selects the **[ADDR]** tab.

The Address Lookup provider used for the ADDR tab can be configured in the Settings > Tool Preferences > Address Lookup Preferences.

## Geofencing

The Geo Fence tool allows users to create a virtual fence that triggers entry/exit notifications if map items of interest cross the virtual boundary lines. The Geo Fence options are added to the existing drawing tools. After a shape has been added, the Geo Fence Tool can be accessed either by selecting the [**Geo Fence**] icon from the menu items or selecting it from the radial.




The Enabled Field slider will move to Tracking by default when a new Geo Fence window is created. Toggle the slider between Tracking and Off to enable/disable the Geo Fence. Use the Trigger field to define which types of Geo Fence breach to monitor. Choose between Entry, Exit or Both. Use the Monitor field to define which entities the Geo Fence will track.

Choose between TAK Users, Friendly, Hostile, Custom or All. Check the [**Specify Elevation**] box to enable the Elevation field, where elevation boundaries for the entities being tracked can be defined. Select the [**OK**] button to finish creating the fence. Select the [**Send**] button to create the fence and send it to another user. Select [**Delete**] to close the Create Geo Fence window and discard changes.

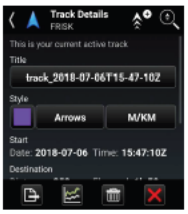
Alerts appear on the map interface. Selecting the [**Alert Notification**] will open the alerts menu, detailing the activity monitored in the user defined region. The default radius for monitoring users (filtered within the "Monitor" field) outside the Geo Fence is set at 75 km. This means the total area monitored begins at the farthest point from the center of the shape plus 75 km. If the user wishes to keep the Geo Fence, but disable tracking, the user can set the tracking [**Enabled**] to off in the Edit Window.

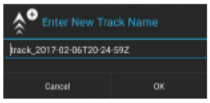
35

Unclassified

## Track History

The device's GPS can be used to track movements with the Track History tool. These tracked paths can be exported to a TAK server, to a route or to a KML, KMZ, GPX or CSV file. A GPS position must be established before tracking can begin.



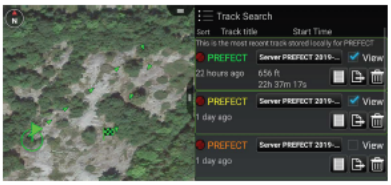




Selecting the [**Track History**] icon will open Track Details for the current active track. The track title, color and style can be modified. Initiate a new track by selecting the [**Add Track**] icon. Accept or edit the default track name and select the [**OK**] button to begin the new track. User location data is recorded as breadcrumbs in a new track file.

## Track Search

Use the Track Search function to view track information that has been previously saved locally or on a TAK Server. The tool searches the track database for matches against the specified time range and by user callsign. Matching tracks are displayed as a list, and can be selected to view on the map interface.

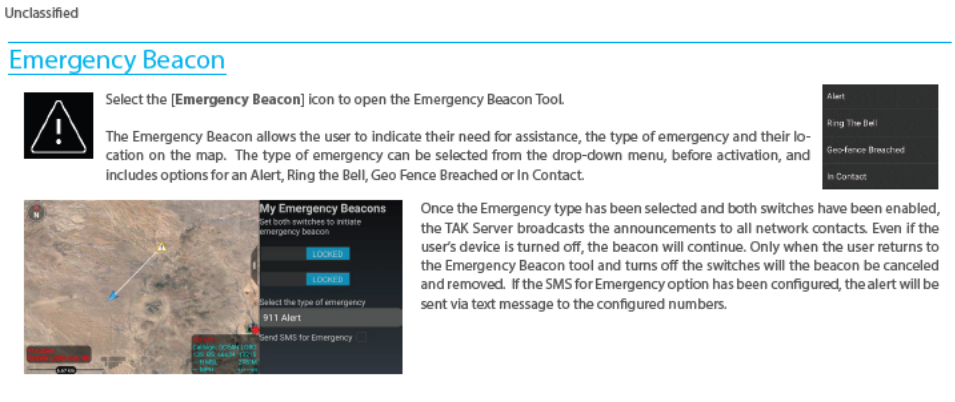
Select the [**Track Search**] icon to access the function. Specify callsign and time frame, check the box for Server Search (if desired), then select [**Search**]. The track list will appear. The query results can be sorted by Track Name or Start Time. Select any of the query results to move to that track. Once selected, the name, color, and style of a selected track can be modified or the track can be cleared. Convert a track to a TAK route or export it as a KML, KMZ, GPX or CSV file by selecting the desired track and then [**Export**]. Enter a file name then select [**Next**] and choose the export format. Select [**Done**] or [**Send**] when the export completes.



When viewing the track list, the Track History Toolbar will appear at the top of the screen. The options include [**Add a Track**], [**Multi-select**], [**Track Search**], [**Clear Tracks**] and [**Exit**]. The Track History List allows the user to select tracks of other users that have been saved on their device. The Track Search – Local Device allows the user to perform a tailored search for tracks meeting their criteria. The searching option allows the user to retrieve all the tracks on the device.

The Track History Breadcrumb and Settings can be configured in the Settings > Tools Preferences > Track History Preferences.

37



Unclassified

Emergency Beacon

Select the [**Emergency Beacon**] icon to open the Emergency Beacon Tool.

The Emergency Beacon allows the user to indicate their need for assistance, the type of emergency and their location on the map. The type of emergency can be selected from the drop-down menu, before activation, and includes options for an Alert, Ring the Bell, Geo Fence Breached or In Contact.

Alert
Ring The Bell
Geo-fence Breached
In Contact

My Emergency Beacons
Set both switches to initiate emergency beacon
LOCKED
LOCKED
Select the type of emergency
911 Alert
Send SMS for Emergency

Once the Emergency type has been selected and both switches have been enabled, the TAK Server broadcasts the announcements to all network contacts. Even if the user's device is turned off, the beacon will continue. Only when the user returns to the Emergency Beacon tool and turns off the switches will the beacon be canceled and removed. If the SMS for Emergency option has been configured, the alert will be sent via text message to the configured numbers.

15

The Team Awareness Kit (TAK), for civilian uses, or Tactical Assault Kit (also TAK) for military uses is a suite of software that provides geospatial information and allows user collaboration over geography. There are numerous TAK Products in the TAK family, all developed at government expense

The Team Awareness Kit for Android (ATAK, also known as CivTAK) was originally developed by the Air Force Research Laboratory (AFRL) and is now maintained by a Joint Product Center.

ATAK (including CivTAK) is an Android smartphone geospatial infrastructure and situational awareness app. It allows for precision targeting, surrounding land formation intelligence, situational awareness, navigation, and data sharing.

All the Android variants of TAK are virtually identical and all are interoperable with each other and with other TAK products. There are small, military-specific additions in military versions of ATAK.

[15] https://drive.google.com/file/d/1bo9WHadg3J3o55OLlx1mn3McqEJzvgrK/view

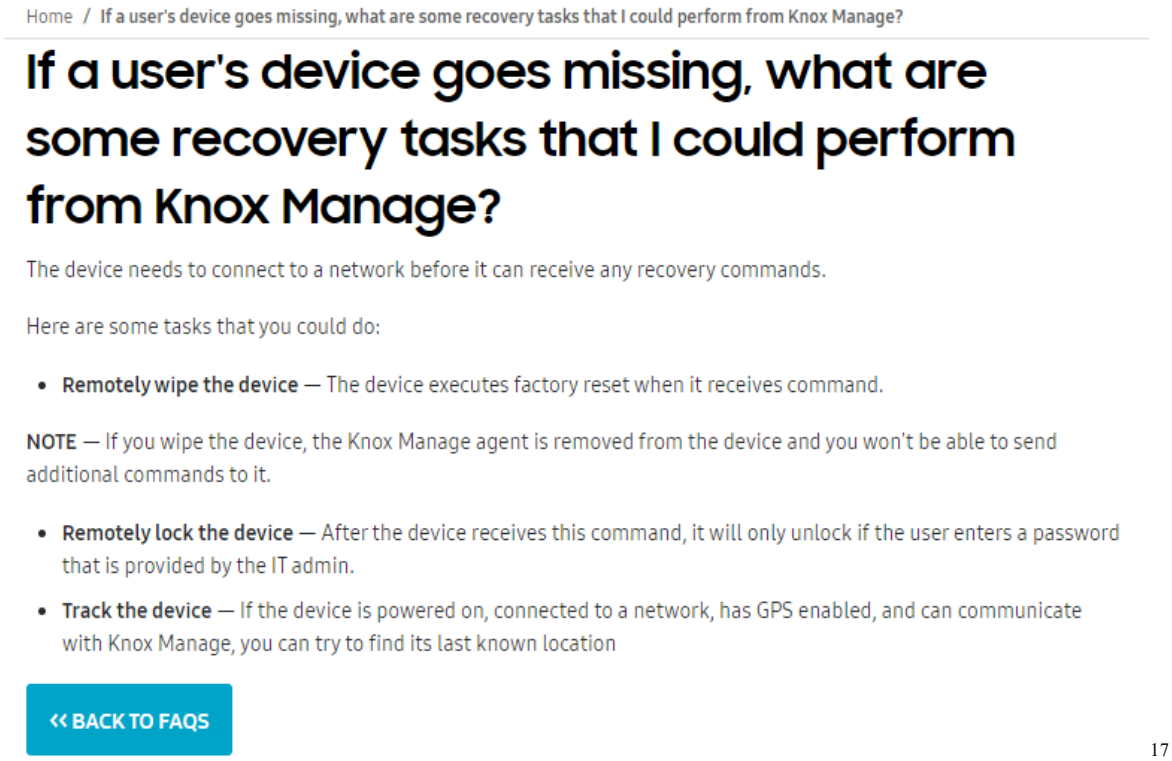
# Features

Industry/civilian capabilities of ATAK/CivTAK include:

- Online and offline mapping (most standard formats), with a blazing fast rendering engine
- Support for very high-resolution imagery (sub 1 cm resolution)
- Collaborative mapping, including points, drawings, locations of interest
- Extensive and customizable set of Icons
- Overlay Manager which allows the Import and display of KML, KMZ, GPX overlays and maps, including online sources
- Location marking, sharing, history
- Chat, file sharing, photo sharing, video sharing, streaming
- Navigation-walking/hiking, driving, also useful flying and air-ground coordination
- Elevation Tools, heat maps, computed contour maps, viewsheds, routes w/DTED, SRTM, including dynamic profiling
- Hashtags and Sticky tags
- Center on Self, Center on other objects (e.g. another person in the network)
- Range, bearing, and other measurement tools
- Network-aware geofences with triggers
- "Bloodhound" destination tracking, including on moving objects
- Team Emergency Beacons
- Customizable Toolbar
- Radio controls and Integration
- Photo to map capability (aka Rubber Sheeting)
- Casualty evacuation tool
- Icon support for a wide variety of First Responder missions with further extensible Icons
- 3D perspective and ability to display 3D geospatial models
- Useful for First Responders, Hunting, fishing, ornithology, wildlife site survey
- An API with an SDK

[16]

[16] https://www.civtak.org/documentation/



Home / If a user's device goes missing, what are some recovery tasks that I could perform from Knox Manage?

# If a user's device goes missing, what are some recovery tasks that I could perform from Knox Manage?

The device needs to connect to a network before it can receive any recovery commands.

Here are some tasks that you could do:

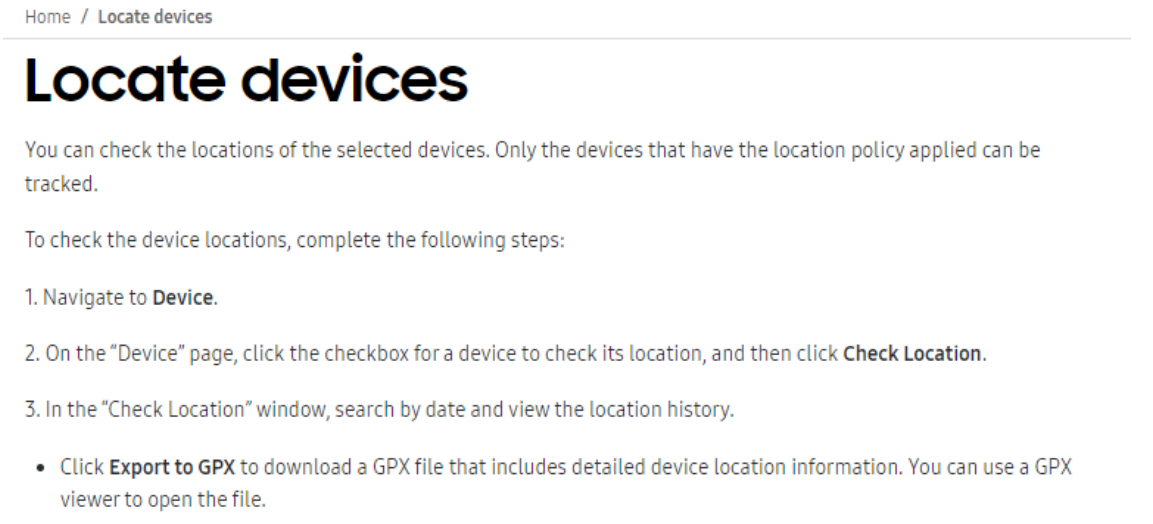
- **Remotely wipe the device** — The device executes factory reset when it receives command.

**NOTE** — If you wipe the device, the Knox Manage agent is removed from the device and you won't be able to send additional commands to it.

- **Remotely lock the device** — After the device receives this command, it will only unlock if the user enters a password that is provided by the IT admin.
- **Track the device** — If the device is powered on, connected to a network, has GPS enabled, and can communicate with Knox Manage, you can try to find its last known location

<< BACK TO FAQS

[17]



Home / Locate devices

# Locate devices

You can check the locations of the selected devices. Only the devices that have the location policy applied can be tracked.

To check the device locations, complete the following steps:

1. Navigate to **Device**.

2. On the "Device" page, click the checkbox for a device to check its location, and then click **Check Location**.

3. In the "Check Location" window, search by date and view the location history.

- Click **Export to GPX** to download a GPX file that includes detailed device location information. You can use a GPX viewer to open the file.

[18]

[17] https://docs.samsungknox.com/admin/knox-manage/faqs/faq-115013698467.htm.
[18] https://docs.samsungknox.com/admin/knox-manage/locate-devices.htm.

Home / Send device commands to users

# Send device commands to users

You can send device commands to the user's enrolled devices. For more information on each device command, see Sending device commands to devices.

To send device commands, complete the following steps:

1. Navigate to **User**.

2. On the "User" page, click the check box next to the user ID to send a device command to.

3. Click **Device Command** and select the supported OS platform (enrolled device).

4. In the "Device Command" window, select a desired device command.

5. In the "Request Command" window, click **OK**.

19

## Knox Guard protects enterprise mobile devices and data against theft and loss

Published May 25, 2022 By: Marcelo Carvalho

Information security experts tend to focus on what's on a smartphone, such as corporate data or access credentials. Meanwhile, the device itself is often seen as disposable, not worth worrying about. But IT managers know that smartphones and tablets represent a significant investment when multiplied by thousands of employees, and deserve to be protected. Samsung Knox Guard offers an inexpensive option to protect and control access to corporate mobile devices — and the data they hold — when a device is lost, stolen or just misplaced.

For less than a penny a day, IT managers can use Knox Guard to remotely lock and even wipe devices whenever they're connected to the network, either through cellular data or Wi-Fi. It's all controlled from a Knox cloud-based portal. Knox Guard capabilities are built into all Samsung smartphones and tablets, and operate using layers of security from the chip level on up — meaning a factory reset or malicious attempt to modify Samsung software can't bypass Knox Guard's fraud and theft protections.

Knox Guard complements mobile device management (MDM) and enterprise mobility management (EMM) solutions, providing another layer of security with protections that extend outside the coverage area of MDM solutions and can't be bypassed. IT managers can use MDM and Knox Guard together to prevent malicious attempts to disable theft and loss protection. Knox Guard operates immediately, like an MDM, when the device is connected to a network. But it also delivers protections even if someone disables the network or removes the SIM. IT managers can define a Knox Guard policy that locks a mobile device that has been disconnected for a set number of days.

If a device is reported as lost or stolen, an IT admin can immediately issue the lock command from the Knox Guard portal. Knox Guard protects against malicious users disabling the lock by leveraging Samsung Knox hardware-backed security that prevents tampering and installation of unauthorized firmware. Knox Guard can even help recover lost or stolen devices by displaying customizable messages and options to contact the company via email or phone call, direct from the lock screen. And if a legitimate user needs to unlock their mobile device but doesn't have a data network connection, Knox Guard's two-step verification provides a secure way to confirm authorization by the IT administrator.

[19] https://docs.samsungknox.com/admin/knox-manage/send-commands-to-users-devices.htm.

### Enhanced lock and wipe capabilities

Knox Guard delivers enterprise-level protection in many different use cases. If people are being assigned smartphones for both business and personal use — also known as Corporate Owned, Personally Enabled (COPE) — Knox Guard mitigates risk from theft and loss of both the devices and their data by allowing IT managers to permanently lock the devices, restricting app use, calls, texts and more.

As part of shipping and transportation operations, for example, companies may need to provide their drivers with dedicated mobile devices that they can use as navigation aids, maintenance/mileage trackers and push-to-talk (PTT) communications devices to stay in touch with dispatchers. If one of those devices goes missing, Knox Guard can permanently lock the device, protect the data contained on it and — because the device is inaccessible and has no use — it immediately reduces theft motivation.[20]

Home / **Lock and unlock devices**

# Lock and unlock devices

Knox Guard managed devices that are overdue, and delinquent, in their subscription payments, can be locked until the subscriber receives payment from the delinquent device user. When subscription payments bring the device back to good standing, the device can be unlocked and its full functionality restored to the user.

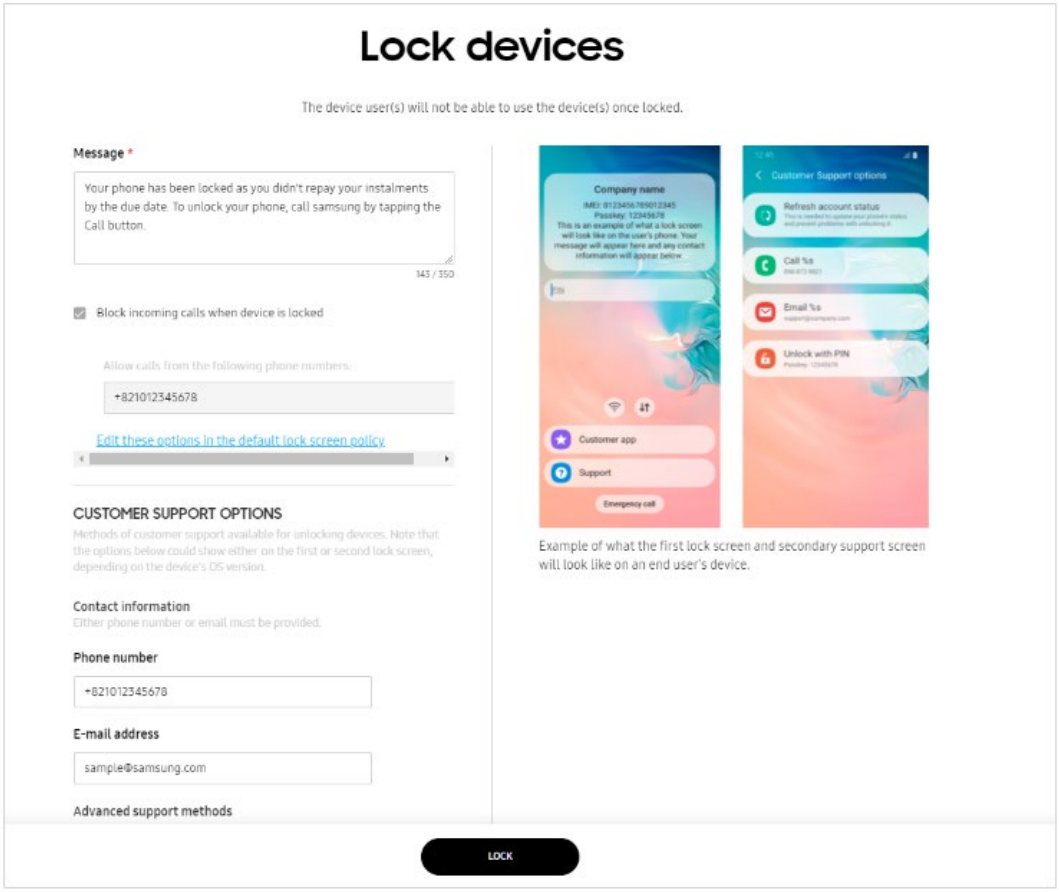
## Lock devices

To lock a device:

**NOTE** - An offline device lock that automatically locks a device when offline for a configurable period of time can also be set. This can occur when the user does not purposely connect to the network, and the device cannot be controlled since its no longer receiving updates from the Knox Guard server. For more information, go to: Manage defaults.

1. Select specific overdue device checkboxes from the left-hand side of the Devices screen.
2. Invoke the **ACTIONS** drop-down menu from the top, right-hand side, of the Devices screen and select **Manage device** > **Lock device**.

[20] https://insights.samsung.com/2022/05/25/knox-guard-protects-enterprise-mobile-devices-and-data-against-theft-and-loss/.




3. Define the 350 character maximum **Message** devices receive informing them how to remedy their delinquent subscription and unlock their device.
4. Enter the **Phone number** of the subscriber contact managing the selected devices delinquent subscription. Either a phone number or E-mail address is required as a contact resource. Special characters can be used if necessary.
5. Enter the **E-mail address** of the subscriber contact managing the selected devices delinquent subscription. Either a phone number or E-mail address is required as a contact resource.
6. Refer to the **Block incoming calls when device is locked** checkbox to block incoming calls when the device is in any lock state (SIM Lock, Offline lock, etc.). Leave this option unselected to permit the receipt of incoming calls when the device is locked. Select **Edit these options in the default lockscreen policy** to configure this option and make available for default device assignment. For more information, go to: manage defaults.
7. Select **LOCK** to proceed with locking the selected devices. A notification message displays on the top portion of the Devices screen stating the selected devices will be locked.

21

27. For example, Defendants directly infringe and/or indirectly infringe by instructing its customers to infringe using the Accused Products as shown below:

[21] https://docs.samsungknox.com/admin/knox-guard/lock-and-unlock-devices.htm.

## Find, lock, or erase a lost Android device

If you lose an Android phone or tablet, or Wear OS watch, you can find, lock, or erase it. If you've added a Google Account to your device, Find My Device is automatically turned on. If you allow Find My Device to encrypt your phone's most recent location and store it with Google, your device's most recent location is available to the first account activated on the device.

**Tip:** To find, lock, or erase your Wear OS device, connect it to WiFi or mobile data.

Learn about how to find an Android device.

To find an Android device, make sure that device:

- Is signed in to a Google Account
- Has Location turned on
- Has Find My Device turned on
- Has power and is connected to mobile data or WiFi.
  - If your device is off or isn't connected to mobile data or WiFi, you may still find its most recent location if you've enabled "Store recent location." Learn more about 2-step verification backups.
- Is visible on Google Play

To lock or erase an Android device, make sure that device:

- Has power
- Is connected to mobile data or WiFi
- Is signed in to a Google Account
- Has Find My Device turned on
- Is visible on Google Play

If you use 2-step Verification, go to 2-step Verification backups.

[22]

## Find, lock, or erase a device remotely

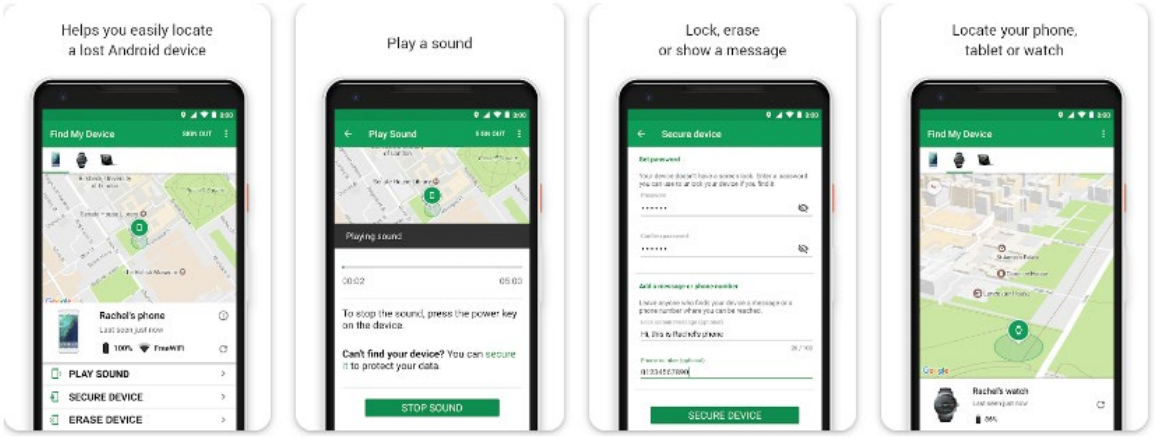
**Important:** If you find your device after you erase it, to use your device again, you need your Google Account password. Learn about device protection.

1. On a browser, go to android.com/find.
2. Sign in to your Google Account.
   - **If you have more than one device:** At the top of the sidebar, select the lost device.
   - **If your lost device has more than one user profile:** Sign in with a Google Account that's on the main or personal profile. Learn about user profiles.
3. The lost device gets a notification.
4. On the map, you'll get info about where the device is.
   - The location is approximate and may not be accurate.
   - If your device can't be found, you may find its last known location, if available.
5. If you get a prompt, tap **Enable lock & erase**.
6. Select what you want to do:
   - **Play sound:** Rings your device at full volume for 5 minutes, even if it's set to silent or vibrate.
   - **Secure device:** Locks your device with your PIN or password. If you don't have a lock, you can set one. To help someone return your device to you, you can add a message or device number to the lock screen.
   - **Erase device:** Permanently deletes all data on your device, but may not delete SD cards. After you erase, Find My Device won't work on the device.

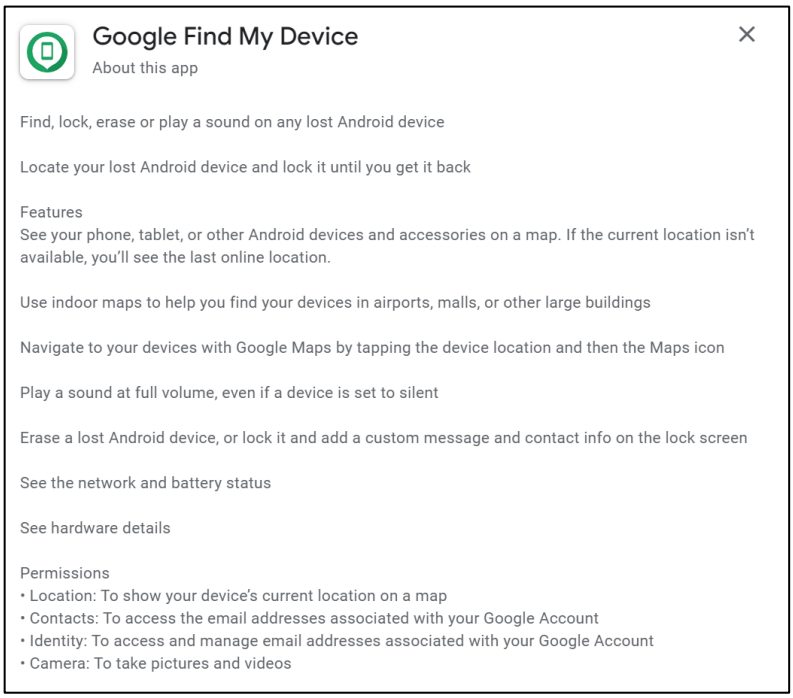
[23]

[22] https://support.google.com/android/answer/6160491; see also https://www.att.com/device-support/article/wireless/KM1474177/Samsung/SamsungSMA536U

[23] *Id.*




[24]




[25]

28. AGIS Software has suffered damages as a result of Defendants' direct and indirect infringement of the '970 Patent in an amount to be proved at trial.

---

[24] https://play.google.com/store/apps/details?id=com.google.android.apps.adm&hl=en_US&gl=US ; see also https://www.att.com/device-support/article/wireless/KM1474177/Samsung/SamsungSMA536U

[25] *Id.*

29. AGIS Software has suffered, and will continue to suffer, irreparable harm as a result of Defendants' infringement of the '970 Patent for which there is no adequate remedy at law unless Defendants' infringement is enjoined by this Court.

30. Defendants have committed and continue to commit acts of infringement that Defendants actually knew or should have known constituted an unjustifiably high risk of infringement of at least one valid and enforceable claim of the '970 Patent. Defendants' infringement of the '970 Patent has been and continues to be willful, entitling AGIS Software to an award of treble damages, reasonable attorney fees, and costs in bringing this action.

## COUNT II
**(Infringement of the '838 Patent)**

31. Paragraphs 1 through 19 are incorporated herein by reference as if fully set forth in their entireties.

32. AGIS Software has not licensed or otherwise authorized Defendants to make, use, offer for sale, sell, or import any Accused Products and/or products that embody the inventions of the '838 Patent.

33. Defendants infringe, contribute to the infringement of, and/or induce infringement of the '838 Patent by making, using, selling, offering for sale, distributing, exporting from, and/or importing into the United States products and/or methods covered by one or more claims of the '838 Patent including, but not limited to, the Accused Products.

34. Defendants have and continue to directly infringe at least claim 54 of the '838 Patent, either literally or under the doctrine of equivalents, by making, using, selling, offering for sale, distributing, exporting from, and/or importing into the United States the Accused Products without authority and in violation of 35 U.S.C. § 271(a).

35. Defendants have and continue to indirectly infringe at least claim 54 of the ’838 Patent by actively, knowingly, and intentionally inducing others to directly infringe, either literally or under the doctrine of equivalents, by making, using, selling, offering for sale, distributing, exporting from, and/or importing into the United States the Accused Products and by instructing users of the Accused Products to perform methods claimed in the ’838 Patent. For example, Defendants, with knowledge that the Accused Products infringe the ’838 Patent at least as of the date of this Complaint, actively, knowingly, and intentionally induced, and continue to actively, knowingly, and intentionally induce direct infringement of the ’838 Patent.

36. For example, Defendants have indirectly infringed and continue to indirectly infringe at least claim 54 of the ’838 Patent in the United States because Defendants’ customers use the Accused Products, including at least the Samsung Tactical, TAK, and ATAK applications and services, Samsung Knox applications and services, and Find My Device, alone or in conjunction with additional Accused Products, in accordance with Defendants’ instructions and thereby directly infringe at least one claim of the ’838 Patent in violation of 35 U.S.C. § 271. Defendants directly and/or indirectly intentionally instruct their customers to infringe through training videos, demonstrations, brochures, installations and/or user guides, such as those located at one or more of the following: https://www.samsung.com/us/business/solutions/industries/government/tactical-edition/#COMMAND_AND_CONTROL; https://www.samsung.com/us/business/solutions/services/mobility-software/e-fota/; https://image-us.samsung.com/SamsungUS/samsungbusiness/pdfs/brochures/S20_TE-tactical-brochure-FINAL_July_2021.pdf; https://insights.samsung.com/2021/09/01/atak-enhances-collaboration-and-awareness-for-public-safety-2/; https://www.civtak.org/atak-about/;

https://www.civtak.org/documentation/; https://wiki.civtak.org/index.php?title=ATAK_Manual; https://www.pargovernment.com/tactical-sa/docs/S20_brochure.pdf; https://insights.samsung.com/2021/09/22/7-ways-samsungs-galaxy-xcover-pro-supports-first-responders/; https://kp4-cdn.samsungknox.com/resource/Samsung%20Knox%20Security%20Handbook_bx4Z.pdf; https://docs.samsungknox.com/admin/knox-manage/faqs/faq-115013698467.htm; https://docs.samsungknox.com/admin/knox-manage/locate-devices.htm; https://downloadcenter.samsung.com/content/UM/202303/20230320235240461/SAM_S901_S906_S908_EN_UM_OS13_012323_FINAL_AC.pdf; https://www.att.com/device-support/article/wireless/KM1474177/Samsung/SamsungSMA536U; https://ss7.vzw.com/is/content/VerizonWireless/Devices/Samsung/note/samsung-galaxy-note9-ug.pdf; https://ss7.vzw.com/is/content/VerizonWireless/Devices/Samsung/note/samsung-galaxy-note9-ug.pdf; and Samsung agents and representatives located within this Judicial District. Defendants are thereby liable for infringement of the '838 Patent under 35 U.S.C. § 271(b).

37. For example, Defendants directly infringe and/or indirectly infringe by instructing their customers to infringe by a system comprising: a first device programmed to perform operations comprising: joining a communication network corresponding to a group, wherein joining the communication network comprises transmitting a message including an identifier corresponding to the group; participating in the group, wherein participating in the group includes sending first location information to a first server and receiving second location information from the first server, the first location information comprising a location of the first device, the second location information comprising one or more locations of one or more respective second devices included in the group; presenting, via an interactive display of the first device, a first interactive,

georeferenced map and a first set of one or more user-selectable symbols corresponding to a first set of one or more of the second devices, wherein the first set of symbols are positioned on the first georeferenced map at respective positions corresponding to the locations of the first set of second devices, and wherein first georeferenced map data relate positions on the first georeferenced map to spatial coordinates; sending, to a second server, a request for second georeferenced map data different from the first georeferenced map data; receiving, from the second server, the second georeferenced map data; presenting, via the interactive display of the first device, a second georeferenced map and a second set of one or more user-selectable symbols corresponding to a second set of one or more of the second devices, wherein the second set of symbols are positioned on the second georeferenced map at respective positions corresponding to the locations of the second set of second devices, and wherein the second georeferenced map data relate positions on the second georeferenced map to spatial coordinates; and identifying user interaction with the interactive display selecting one or more of the second set of user-selectable symbols corresponding to one or more of the second devices and positioned on the second georeferenced map and user interaction with the display specifying an action and, based thereon, sending third data to the selected one or more second devices via the first server. For example, the Accused Products include features as shown below.

## Stay connected to what matters.

**Persistent communications**
The Galaxy S20 Tactical Edition is a COTS military smartphone with tailored software that easily connects to tactical radios and mission-critical devices, out of the box.

**Multi-ethernet capabilities**
Dedicated connections with multiple mission systems including laser range finders, external GPS devices, drones and more keep you connected in degraded and highly contested network environments.

**Next-generation networks**
As technologies evolve, you need a powerful, mission-ready device that can take full advantage of next-generation military networks. The Galaxy S20 Tactical Edition supports Private SIM, 5G, CBRS and is ready for Wi-Fi 6.

# Command and control

**Situational awareness**
The Galaxy S20 Tactical Edition integrates voice, video, and tactical data to provide a common operational picture of the battlespace. This complete and accurate real-time intelligence enhances the precision and effectiveness of your tactical teams.

**Tactical user experience**
Unique features found only on the Galaxy S20 Tactical Edition deliver fast and simple access to the information and applications operators need on-mission.

**Better intelligence**
The pro-grade 64 MP camera on the Galaxy S20 Tactical Edition allows you to discretely capture and share crisp high-resolution photo or 8K video intelligence, even in low light without the use of a flash. View and analyze intelligence in greater detail than ever before with the Galaxy S20 Tactical Edition's Dynamic AMOLED 2.0, a 120Hz[1] display.

**Extend your mission**
The Galaxy S20 Tactical Edition battery is 30% larger than the previous tactical solution and it's intelligent.[2] It optimizes your app usage in the field giving you extended power to complete the mission. When you need a recharge, Super Fast Charging[3] and fast Wireless Charging 2.0 give you power in a flash. And Wireless PowerShare allows you to easily charge a team member's phone in the field just by touching the devices.[4]

**Connect to tactical radios** - Protocols to support tactical radios and mission systems, out of the box.

**Tactical app quick launch** - Instantly expand or hide ATAK, APASS and other mission-critical applications at the push of a button.

**Night vision mode** – Turn on and off LED backlight when wearing night vision devices.

**Stealth mode** – Disable LTE and e-911 and mute all RF broadcasting for complete off-grid communications.

**Lock screen auto-rotate** - Unlock the device in landscape mode for easy access when mounted to the operator's chest.

**Auto-touch sensitivity** – Automatically adjust device operations to work with gloved hands.

# One device to meet all your mission requirements.

**Run mission apps and enterprise apps**
The Galaxy S20 Tactical Edition has a 64-bit Octa-Core processor with the speed and versatility to run multiple tactical applications in the field and enterprise applications everywhere else.

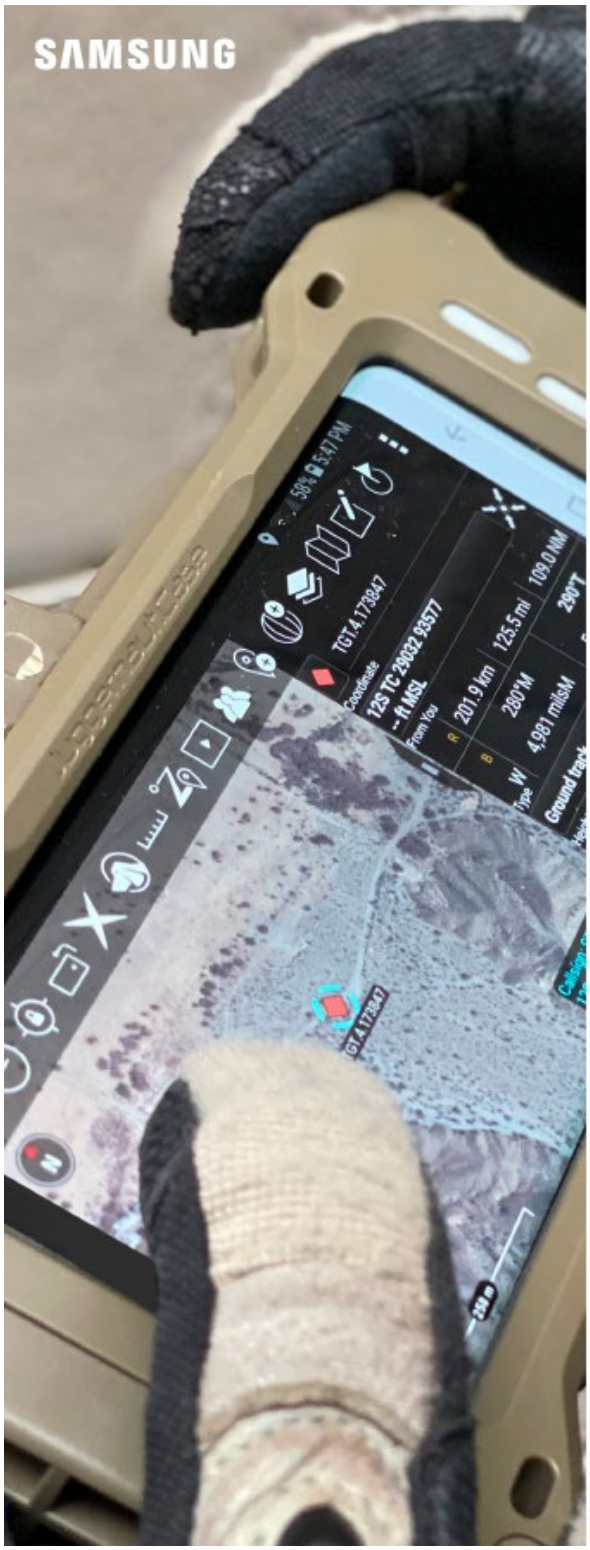
With Samsung DeX, connect your Galaxy S20 Tactical Edition to a monitor, keyboard and mouse for a desktop-like experience[5] ideally suited for mission planning, training, and everyday use. DeX gives you the power to work seamlessly across Microsoft Office Suite applications,[6] productivity apps, and virtual desktops with secure CAC-authenticated Virtual Desktop Infrastructure (VDI) sessions, all without a laptop.[7] And DeX-in-Vehicle transforms the Galaxy S20 Tactical Edition into a powerful in-vehicle computer.

**Simple device management**
From device configuration, enrollment, customization and management to advanced mobile security controls and updates, Samsung has the mobility cloud services you need for every stage of the Galaxy S20 Tactical Edition lifecycle.[8] With Knox Services, you can keep pace and maintain control over devices and how they're used. You can manage devices in near real-time, configure settings, and remotely lock or wipe devices if lost or stolen, on the battlefield and anywhere else.

**Open and secure**
The Galaxy S20 Tactical Edition is built on an open and secure Android operating system enabling seamless integration with a diverse ecosystem of tactical solution partners. Eliminate vulnerabilities with three software updates throughout the life of the device.

[26]

[26] https://www.pargovernment.com/tactical-sa/docs/S20_brochure.pdf




## Galaxy S20 Tactical Edition

# Mission-ready mobility. Proven by operators.

The Samsung Galaxy S20 Tactical Edition is the mission-ready military smartphone built and proven by operators in special operations. Based on the proven success of the S9 Tactical Edition for operators in the field, the S20 Tactical Edition is the only end user device you'll need for mission planning, training, operations and daily use.

### Persistent communications in any domain

**Purpose-built to connect to tactical radios** and mission systems out of the box, the Galaxy S20 Tactical Edition delivers a complete and accurate common operational picture. Run mission applications in the field and enterprise applications everywhere else with a single end user device for mission training, planning, operations and everyday use.

### Interoperable across devices and networks

**Pre-configured software, pre-loaded during the manufacturing process,** includes drivers to support tactical radios and mission-critical devices. Multi-ethernet capabilities provide dedicated connections to multiple mission systems including drone feeds, laser range finders, and external GPS. Support for current and next-generation networks includes Private SIM, 5G, WiFi 6 and CBRS. Allow or disallow USB peripherals based on product or vendor identifiers.

### Command and control

**Integrate voice, video and tactical data** for a complete view of the battlespace to enhance precision and effectiveness. Unique tactical features on the Galaxy S20 Tactical Edition include night-vision mode, stealth mode, lock screen autorotate, hostage negotiation mode, LTE band lock for consistent 4G connection, tactical application quick launch, to keep the operator focused on the objective, Standalone(5G)/Non-standalone (4G) modes to stay on preferred network. Preloaded tactical settings app. Ability to configure hotspot 2.0.

### Capture Intelligence

**A Pro-grade 64 MP camera** on the Galaxy S20 Tactical Edition enhances intel gathering, even in low-light environments without a flash. Capture high-resolution photos or sharp 8K video reconnaissance without giving away your position.

### Power to extend the mission

**Keep going wherever the mission takes you** with the Galaxy S20 Tactical Edition's intelligent2 4000mAh battery is 30% larger than the previous tactical solution and optimizes energy based on your device usage. Easily share power with a team member's smartphone in the field simply by touching devices using Wireless PowerShare.[4]

### One device to meet your requirements

**Run mission applications in the field** and enterprise applications everywhere else with the powerful and efficient Galaxy S20 Tactical Edition 64-bit Octa-Core processor. Connect your device to a monitor keyboard and mouse and use the power of Samsung DeX[5] for a desktop-like experience that is ideal for mission planning, training and everyday use. DeX-in-Vehicle transforms your Galaxy S20 Tactical Edition into an in-vehicle computer.

### Open and secure

**Enable a diverse ecosystem of tactical partners** with the open and secure Android operating system on the Galaxy S20 Tactical Edition. The all-new Tactical Settings feature simplifies device management, while Samsung Knox provides defense-grade security[6] from the hardware layer up and mission-specific device customization capabilities. The DualDAR architecture of the Galaxy S20 Tactical Edition provides two layers of encryption, even when the device is powered off, for securing up-to top secret level data on the device.

### Tested and proven

Samsung Galaxy Tactical Edition smartphones are tested and proven by special operators in the field. The Galaxy S20 Tactical Edition is certified to meet the most stringent requirements including NSA's CSFC Components List, NIAP Common Criteria/MDFPP, DODIN APL, FIPS 140-2, DISA Android 10 STIG, IP68 rating.

**Contact Us:** www.samsung.com/TacticalEdition

27

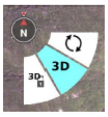
[27] https://image-us.samsung.com/SamsungUS/samsungbusiness/pdfs/flyer/S20_TE-salesflyer_FINAL_July_2021.pdf

## ATAK Civilian Overview

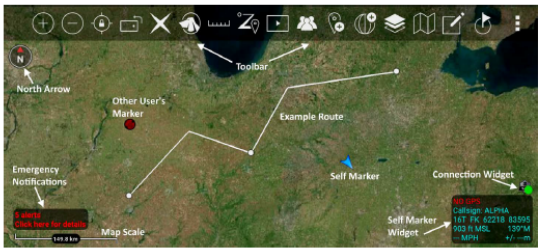
The Civilian Team Awareness Kit for Android (ATAK Civilian) is a Government-off-the-Shelf (GOTS) software application and mapping framework for mobile devices. ATAK Civilian has been designed and developed to run on Android smart devices used in a first responder environment. The ATAK Civilian software application is an extensible moving map display that integrates imagery, map and overlay information to provide enhanced collaboration and Situational Awareness (SA) over a tactical meshed network. ATAK Civilian promotes information flow and communications from the field environment to command enterprise locations.

The first time ATAK Civilian is opened, or after a Clear Content, a passphrase is auto-generated to activate data encryption. The user can supply their own passphrase by using Settings > Show All Preferences > Device Preferences > Change Encryption Passphrase. Following this step, ATAK Civilian's End User License Agreement (EULA) must be accepted. Next, the user will be prompted to change their callsign and/or import preferences or data from a Mission Package. All changes/imports can always be updated later. Finally, the user can place their self-marker by following the instructions located in the lower right corner.

The toolbar runs along the top of the map display. The features whose icons form the center portion of the toolbar are discussed in individual sections of this guide. The three dots at the right of the toolbar provide additional menu items that appear in a drop-down menu. A Long Press on the map will toggle the toolbar between hidden and visible.




The North Arrow appears in the upper left and is used to control map orientation. It has two primary modes: North Up/Track Up (default) and Manual Map Rotation/Lock. While in North Up/Track Up Mode, single press on the [**North Arrow**] icon to cycle between the North Up and Track Up map orientation. Long press the [**North Arrow**] to call out the additional controls menu where the Manual Rotation/Lock and 3D features are available. Select the [**Rotation**] button to enter Manual Map Rotation/Lock Mode. When in Manual Map Rotation/Lock Mode, rotate the map orientation by pressing on the map with two fingers and pivoting them in the desired direction. Single press on the [**North Arrow**] to lock the screen orientation, signified by the appearance of the lock icon, and again to unlock the orientation for further adjustment. 3D controls are discussed in a separate section.



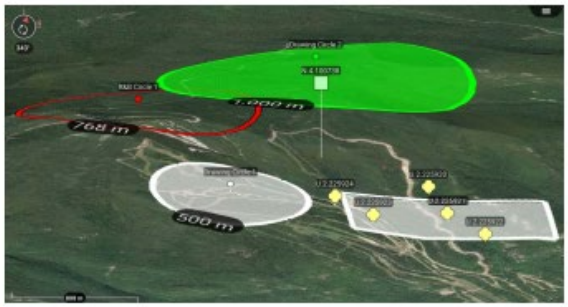

Select the [**Magnifier**] buttons to zoom in or out on the map. The map can also be zoomed by using two fingers on the screen to pinch and spread the map. Select the [**Back**] button to center the screen on the Self Marker or the [**Padlock**] icon to lock the center of the screen to the Self Marker. Select the [**Orientation**] icon to toggle the screen position between portrait and landscape.

The optional connection widget indicates whether or not the user is connected to a TAK Server. This has a corresponding Android notification that provides the same information. Toggle this display on at Settings > Network Connections > Network Connections > Display Connection Widget.

Alerts and notifications are displayed in the lower left of the map interface.

The Map Scale displays a 1 inch to X mi/km reference on the map. The scale adjusts with the map when zoomed in and out. Hint windows are available to alert users to changes or make suggestions about the use of tools the first time they are opened.

## 3D View



ATAK Civilian features 3D viewing of terrain and map items (DTED required). To enable 3D view, long press on the **[North Arrow]** to call out the additional controls menu and select [**3D**]. A tilt angle indicator will appear around the edge of the [**North Arrow**] when 3D view is active. Touch the screen with two fingers and simultaneously swipe up or down on the screen to tilt the view angle. Once the appropriate viewing angle is set, select the [**3D Lock**] button to retain this view while panning the map. While viewing the map from an angle, some map items will appear raised above the map surface if they have defined elevations.

## 3D Models

ATAK Civilian supports the use of 3D models. OBJ models and other types from products such as Pix4D can be imported via the Import Manager or can be manually placed in the atak/overlays folder prior to startup. If using Import Manager browse to the .OBJ file and import only that file, or browse to a .ZIP file that contains the .OBJ file (and others) and import only that file. If using manual placement to the atak/overlays folder, place a .ZIP file containing the .OBJ file (and others) into the directory and they will be imported on startup.

Once imported, a 3D Model icon will appear on the map. Zoom into the area of the icon until a loading ring appears. After the loading process has finished, the 3D model will be projected onto the map. Enable the map 3D View and tilt the view angle to see the 3D modeling. Loaded 3D models will appear as their own category in Overlay Manager and can be toggled on/off or removed from there.

# Placement

The user can enter locations of interest using the Point Dropper tool. Select the [**Point Dropper**] icon to place internationally standardized markers and other icons on the map, edit the data and share the markers with other network members.

## Self-Marker

The Self-Marker is displayed as a blue arrowhead at the user's current location. The options available on the Self-Marker radial are: Compass Rose, Polar Coordinate Entry, Fine Adjust/Enter Coordinate/MGRS Location, GPS Error, Range & Bearing Line, GPS Lock to Self, Tracking Breadcrumbs, Place a Marker at the user's current location and Details. Other TAK users appear on the display as a colored circle. The color of the circle represents the user's Team affiliation, with additional lettering inside the circle to identify the role the user on the team. Team Member markers that include a diagonal line indicate that the GPS location is not available. A solid icon indicated that the team member has GPS reception.

Available roles include: Team Member, Team Lead (designated by a TL in the center of the marker), Headquarters (HQ in center), Sniper (S), Medic (+), Forward Observer (FO), RTO (R) or K9 (K9). The options available when another user's Self-Marker is selected are: Inner Ring – Delete, Polar Coordinate Entry, Fine Adjust/Enter Coordinate/MGRS Location, Range & Bearing Line, GPS Lock on Friendly, Video Player (if available), Communication Options (if configured by that user), Custom Threat Rings, Tracking Breadcrumbs and Details.

Outer Ring (Communication Options) – Data Package, Email, SMS Messaging, GeoChat, VOIP and Cellular Phone, when available.

## Point Dropper

Selecting the [**Point Dropper**] icon will open the Point Dropper menu, containing marker symbology with one or more icon sets, a Recently Added button and an Iconset Manager button.

The Markers symbology affiliations are: Unknown, Neutral, Red and Friendly. Select the affiliation, then a location on the map interface to drop the marker. To add a marker by manually entering coordinates, long press on the map interface and enter the MGRS location. Change the standard naming convention by entering values into the custom prefix and index fields or leave blank to use the defaults. If values are entered, the next marker will be dropped with the prefix name and starting number(s) or letter(s) and every subsequent marker will be assigned the next consecutive number(s) or letter(s).

The user can select the mission specific pallet to open point options including Waypoint (WP), Sensor or Observation Point (OP).

The user can move between icon sets by either swiping in the icon set area or selecting on the [**Iconset Name**] field to bring up the Icon Pallet drop-down.

The last point placed is shown at the bottom of the Point Dropper window. The information for all recently placed points can be accessed by selecting the [**Clock**] icon. This displays the marker icon, name, coordinates, elevation and range & bearing information. The user can send, rename or remove any recently added markers by selecting the [**Arrows**] next to the marker to reveal [**SEND**], [**RENAME**] or [**DEL**] buttons.

Select the [**Iconset Manager**] (gear) button to add or delete icon sets or to set the default Marker Mapping.

## Radial Menus

**Unknown Object**

**Neutral Object**

**Red Object**

**Friendly Object**

**Spot Object**

The options available for Unknown Object Markers are: Delete, Polar Coordinate Entry, Fine Adjust/Enter Coordinate/MGRS Location, Range & Bearing Line, Lock On, Tasking, Custom Threat Rings, Tracking Breadcrumbs and Details.

The options available for Neutral Object Markers are: Delete, Polar Coordinate Entry, Fine Adjust/Enter Coordinate/MGRS Location, Range & Bearing Line, Lock On, Tasking, Custom Threat Rings, Tracking Breadcrumbs and Details.

The options available for Red Object Markers are: Delete, Polar Coordinate Entry, Compass Rose/Bullseye, Fine Adjust/Enter Coordinate/MGRS Location, Range & Bearing Line, Tasking, Custom Threat Rings, Tracking Breadcrumbs and Details.

The options available for Friendly Object Markers are: Delete, Polar Coordinate Entry, Fine Adjust/Enter Coordinate/MGRS Location, Range & Bearing Line, Lock On, Video, Contact Card, Custom Threat Rings, Tracking Breadcrumbs and Details. The Video radial will activate if a properly formatted packet that includes the link to the video feed is included. Select the video radial to open the associated video. The Contact Card can be selected to display additional communication options, including GeoChat, Email, VoIP, SMS Messaging and Cellular Phone, when available.

The options available for Spot Map are: Delete, Fine Adjust/Enter Coordinate/MGRS Location, Range & Bearing Line, Nav-To, Custom Threat Rings, Labels and Details.

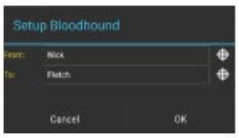
The options for User Defined Iconsets are: Delete, Polar Coordinate Entry, Fine Adjust/Enter Coordinate/MGRS Location, Range & Bearing Line, Lock On, Tasking, Custom Threat Rings. Tracking Breadcrumbs and Details.

Select [**Details**] on the marker radial to make desired modifications, including: Coordinate, Elevation, Name, Type and Remarks. Selecting Marker Type opens a dialog box with extra categories. File attachments, including images, can be associated with the object by selecting the [**Paperclip**] icon. Once all the desired modifications have been made, the Marker can be sent to other network members using [**Send**]. The information can be broadcast to all members or sent to specific recipients. Select the [**Auto Send**] option to broadcast the marker to other TAK users on the network, with updates automatically sent about once every 60 seconds.

## Bloodhound Tool

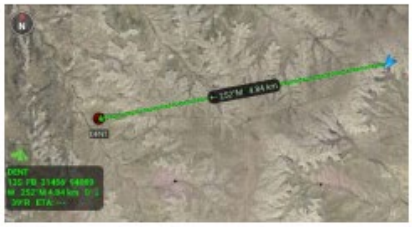
The Bloodhound Tool provides support for tracking and intercepting a map item. It allows the user to select two points on the map and/or map objects and display range & bearing information between the chosen tracker and the target.

Select the [**Bloodhound**] icon to open the Bloodhound Tool. A window will open, prompting the user to choose where to start by tapping the [**From Reticle**] (default = user's self marker) and where to bloodhound (track) to by tapping the [**To Reticle**].




Targets include map objects like other User's Self Markers, DPs, Markers, Shape center points, Range & Bearing end-points and any other map objects. If the user selects a map location instead of an object as the target, Bloodhound will place a waypoint marker there. The self marker will then track towards the waypoint.

Select [**OK**] and Bloodhound will be activated.

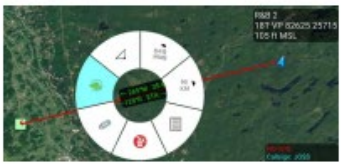


If either point moves, the green widget in the lower left will show the updated information. As the tracking object begins to navigate toward the target, the Estimated Time of Arrival (ETA) will update accordingly.

The green line showing the direct path from the tracker to the target will flash when the user-defined ETA outer threshold is reached (default = 6 minutes from target). The line will flash as the tracker continues toward the target until the next ETA threshold is reached (default = 3 minutes). The line will turn a flashing yellow until the final ETA threshold (default = 1 minute) is reached. The line then flashes red until the target is reached. Colors and thresholds can be modified in Settings > Tool Preferences > Bloodhound Preferences.

Selecting the green Bloodhound icon on the map will pan the map to the Bloodhound Range & Bearing Line. Disengage the Bloodhound Tool by selecting the [**Bloodhound**] icon on the toolbar.

## Multiple Bloodhound

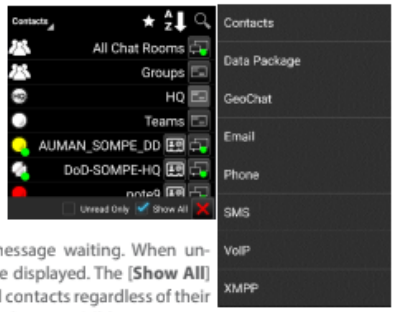


To create multiple bloodhounds, selecting the Range and Bearing Tool and select the [**R&B Line**] icon. Select two markers on the map and once the R&B line is created, select the line to bring up the radial. Select the [**Bloodhound**] radial, and the bloodhound information will be displayed on the R&B Line itself.

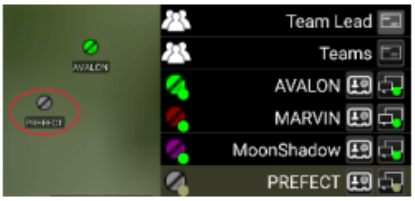
If either point moves, the Bloodhound information shown on the R&B Line will be updated. As the tracking object begins to navigate toward the target, the Estimated Time of Arrival (ETA) will update accordingly.

## Contacts

The Contacts list includes a variety of ways in which a user may communicate with other users, such as GeoChat (ATAK Civilian's built in Chat capability), Data Packages, Email, Phone, SMS, VoIP and XMPP.



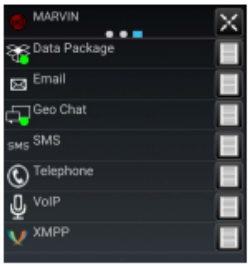

A default communication type (shown in the last column) may be selected and used until another type of communication is selected.




The Contacts list has two filters available at the bottom of the screen. The Unread Only box, when checked, will display only contacts with whom there are unread message waiting. When unchecked (default), all available contacts are displayed. The [**Show All**] box, when checked (default), will display all contacts regardless of their location. When unchecked, only contacts that are visible on current map screen will be displayed.

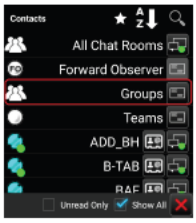
If a contact is no longer online, it will be indicated by changing the contact listing to a yellow color and the marker changes to gray both in the list and on the map.

Profile cards are accessed by selecting the second to last column in the Contacts list and are available for each contact. These contain additional information about that contact including: 1) role, software type and version installed, node type, default connector, last reported time, battery life; 2) location information, and 3) available types of communication.

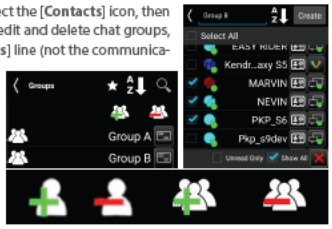


## GeoChat Group Management

Text-based Chat messages may be sent to active network members by using the GeoChat function. To enter GeoChat Group Management, select the [**Contacts**] icon and select [**GeoChat**] from the drop-down menu.

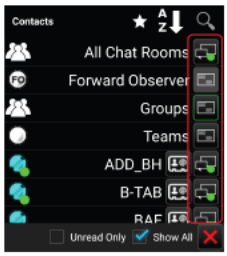



GeoChat Group Management is initiated through Contacts. Select the [**Contacts**] icon, then select GeoChat from the drop-down. The user can now create, edit and delete chat groups, as well as sub-groups. To create a chat group, select the [**Groups**] line (not the communications button). Select the [**Add Group**] icon to create the name of the group and add contacts to the group and then select [**Create**]. If a parent group is being created, no contacts need to be added at this level. To add a nested group, tap the parent group, select the [**Add Group**] icon to create the name of the sub-group and add contacts. Groups may be managed using the options to add/delete contacts or to add/delete GeoChat group.




To add users to a group, select the [**Groups**] line (not the communications button), then select the name of the group to add users. Select the [**Add Users**] icon. A window will open allowing the group creater to add users to the selected group. Select the [**Add**] button when all the users to be added are checked.

## GeoChat Messaging




Group and person-to-person messaging is available. To view messages from or send messages to an individual, tap on the desired contact's [**Communication**] icon. Selecting the [**Pan To**] icon, located at the top right of the call sign in an individual chat, will pan the map interface to that user's location. Select [**All Chat Rooms**] to view all messages from or send messages to those present on the network or TAK Server. Other groupings available for viewing or sending messages are: Forward Observer, Groups, HQ, K9, Medic, RTO, Sniper, Team Lead and Teams. If the user's current role is Forward Observer, HQ, K9, Medic, RTO, Sniper or Team Lead, that user can view or send messages to all other contacts with the same role. If a GeoChat message is sent from the top level of Teams, it will be sent to all contacts, similar to [**All Chat Rooms**].

When a sub-Team is chosen, messages can only be sent to that user's active (My Team) team color. When a parent group is chosen, messages are sent to all members of the parent group, as well as all of the sub-groups. When a sub-group is chosen, messages are sent only to members of the sub-group. Individuals within GeoChat may be removed from the Contacts menu by toggling the visibility of individuals or groups within Overlay Manager.





## GeoChat Messaging (continued)

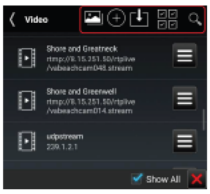
Selecting in the Free Text Entry area will open an onscreen keyboard. At the bottom of the Chat area are pre-defined messages that may be used to quickly create a message to send. Tap the current menu button to scroll through the different menus of canned messages, including: DFLT1, DFLT2, ASLT1, ASLT2, RECON1 and RECON2. These pre-defined messages present an easy way to transmit a brief message to other network members concerning position or other important communication. The pre-defined messages may be changed by long pressing on the button and changing its label and corresponding value.

A numbered red dot will appear on the [**Contacts**] icon when a message has been received successfully. The number denotes the number of unread messages that have been received. Select this icon to view the contact list. The user name who sent the message will appear with a numbered red dot next to their name. Alternatively, the text of the message can be read by dragging down from the top to see the Android notifications window. This notification will only stay available for a short time.

## Video Player

Select the **[Video Player]** icon to bring up the Video player. The Video Player supports playing video streams from IP cameras and H.264 encoders. The menu allows adding, editing, deleting, playing or sending videos to other network members.

Options for the video player include: viewing video snapshots, adding a new video alias, downloading an alias from the TAK Server, selecting the Multi-Select Action option to either Export or Delete aliases or searching for a specific alias.




Select the desired listed video alias or file name to begin playing the stored or streaming video. The video will display half the width of the screen.

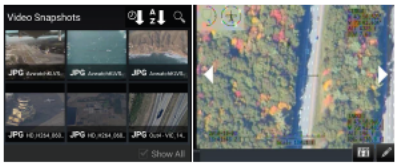
To view a video at full screen, slide the pull bar. To return to half screen, slide the pull bar back to the right.

Select the **[Back]** button to return to the list of available videos.

To add stored video file, select the **[Import Manager]** icon, select **[Local SD]**, and navigate to the video file and select **[OK]** to add the video to the list of available videos. The user can also manually place video files in "atak\tools\videos" to have them listed after ATAK is restarted. When a video is playing at half width, slide the pull bar to the right to hide the video but maintain the connection. Slide the pull bar to the left to unhide the video. The status of the video player is reflected in the main Android toolbar located at the top of the screen.

Select the **[Snapshot]** icon to save the current frame of the video as a JPEG image file, the icon will flash green to indicate that the snapshot has occurred. The file will be saved in the "\atak\tools\videosnaps" folder.

The user can view the saved snap shots by selecting the **[Video Snapshots]** icon. The user has the option of sorting the images by time taken or by the name of the snapshot. The user can also search within the snapshots taken by their name. By selecting an image, the image will be displayed within the window.




The user will have the options of cycling though the images, **[Send]** to a TAK user, or edit in **[Image Markup]**. (Image Markup would need to be installed.)

If a live UDP stream is being viewed, it can be recorded by tapping the **[Record]** icon. The icon will change to a green square while recording. Select the **[Green Square]** to end the recording. The recordings are saved in a folder in "\atak\tools\videos\".

**Note:** This is only available for UDP streams.

To close the video player, select the **[X]** located at the bottom right corner of the video player or select the **[Back]** button.





## Go To

Select the **[Go To]** icon to enter details and navigate to a specific location on the map.

Select from the **[MGRS]** (military grid reference system), **[DD]** (decimal degrees), **[DM]** (degrees- minutes), **[DMS]** (degrees-minutes-seconds), **[UTM]** (Universal Transverse Mercator) or **[ADDR]** tabs on the Go To interface and enter the location data of interest. The address provider name appears beneath the Elevation Data when the user selects the **[ADDR]** tab.

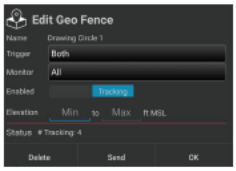
The user can enter the Latitude, Longitude and Elevation in the space provided for **[MGRS]** , **[DD]**, **[D-M]** or **[D-M-S]** searches. If DTED is installed, the elevation value can be automatically populated by tapping the **[Pull From DTED]** button.The user can select a desired marker type (Spot, Unknown, Neutral, Red, or Friendly) to be placed at the entered coordinates. If **[No Point]** is selected, the map will pan to the location but will not add a point.

**Note:** The address provider name appears beneath the Elevation Data when the user selects the **[ADDR]** tab.

The Address Lookup provider used for the ADDR tab can be configured in the Settings > Tool Preferences > Address Lookup Preferences.

## Geofencing

The Geo Fence tool allows users to create a virtual fence that triggers entry/exit notifications if map items of interest cross the virtual boundary lines. The Geo Fence options are added to the existing drawing tools. After a shape has been added, the Geo Fence Tool can be accessed either by selecting the [**Geo Fence**] icon from the menu items or selecting it from the radial.




The Enabled Field slider will move to Tracking by default when a new Geo Fence window is created. Toggle the slider between Tracking and Off to enable/disable the Geo Fence. Use the Trigger field to define which types of Geo Fence breach to monitor. Choose between Entry, Exit or Both. Use the Monitor field to define which entities the Geo Fence will track.

Choose between TAK Users, Friendly, Hostile, Custom or All. Check the [**Specify Elevation**] box to enable the Elevation field, where elevation boundaries for the entities being tracked can be defined. Select the [**OK**] button to finish creating the fence. Select the [**Send**] button to create the fence and send it to another user. Select [**Delete**] to close the Create Geo Fence window and discard changes.

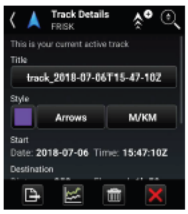
Alerts appear on the map interface. Selecting the [**Alert Notification**] will open the alerts menu, detailing the activity monitored in the user defined region. The default radius for monitoring users (filtered within the "Monitor" field) outside the Geo Fence is set at 75 km. This means the total area monitored begins at the farthest point from the center of the shape plus 75 km. If the user wishes to keep the Geo Fence, but disable tracking, the user can set the tracking [**Enabled**] to off in the Edit Window.

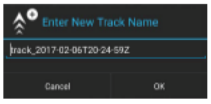




## Track History

The device's GPS can be used to track movements with the Track History tool. These tracked paths can be exported to a TAK server, to a route or to a KML, KMZ, GPX or CSV file. A GPS position must be established before tracking can begin.



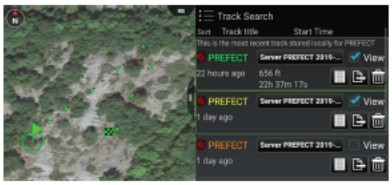




Selecting the [**Track History**] icon will open Track Details for the current active track. The track title, color and style can be modified. Initiate a new track by selecting the [**Add Track**] icon. Accept or edit the default track name and select the [**OK**] button to begin the new track. User location data is recorded as breadcrumbs in a new track file.

## Track Search

Use the Track Search function to view track information that has been previously saved locally or on a TAK Server. The tool searches the track database for matches against the specified time range and by user callsign. Matching tracks are displayed as a list, and can be selected to view on the map interface.

Select the [**Track Search**] icon to access the function. Specify callsign and time frame, check the box for Server Search (if desired), then select [**Search**]. The track list will appear. The query results can be sorted by Track Name or Start Time. Select any of the query results to move to that track. Once selected, the name, color, and style of a selected track can be modified or the track can be cleared. Convert a track to a TAK route or export it as a KML, KMZ, GPX or CSV file by selecting the desired track and then [**Export**]. Enter a file name then select [**Next**] and choose the export format. Select [**Done**] or [**Send**] when the export completes.



When viewing the track list, the Track History Toolbar will appear at the top of the screen. The options include [**Add a Track**], [**Multi-select**], [**Track Search**], [**Clear Tracks**] and [**Exit**]. The Track History List allows the user to select tracks of other users that have been saved on their device. The Track Search – Local Device allows the user to perform a tailored search for tracks meeting their criteria. The searching option allows the user to retrieve all the tracks on the device.

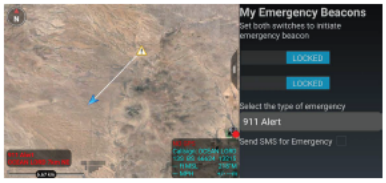
The Track History Breadcrumb and Settings can be configured in the Settings > Tools Preferences > Track History Preferences.

Unclassified

## Emergency Beacon

Select the [**Emergency Beacon**] icon to open the Emergency Beacon Tool.

The Emergency Beacon allows the user to indicate their need for assistance, the type of emergency and their location on the map. The type of emergency can be selected from the drop-down menu, before activation, and includes options for an Alert, Ring the Bell, Geo Fence Breached or In Contact.




Once the Emergency type has been selected and both switches have been enabled, the TAK Server broadcasts the announcements to all network contacts. Even if the user's device is turned off, the beacon will continue. Only when the user returns to the Emergency Beacon tool and turns off the switches will the beacon be canceled and removed. If the SMS for Emergency option has been configured, the alert will be sent via text message to the configured numbers.

28

[28] https://drive.google.com/file/d/1bo9WHadg3J3o55OLlx1mn3McqEJzvgrK/view

The Team Awareness Kit (TAK), for civilian uses, or Tactical Assault Kit (also TAK) for military uses is a suite of software that provides geospatial information and allows user collaboration over geography. There are numerous TAK Products in the TAK family, all developed at government expense

The Team Awareness Kit for Android (ATAK, also known as CivTAK) was originally developed by the Air Force Research Laboratory (AFRL) and is now maintained by a Joint Product Center.

ATAK (including CivTAK) is an Android smartphone geospatial infrastructure and situational awareness app. It allows for precision targeting, surrounding land formation intelligence, situational awareness, navigation, and data sharing.

All the Android variants of TAK are virtually identical and all are interoperable with each other and with other TAK products. There are small, military-specific additions in military versions of ATAK.

# Features

Industry/civilian capabilities of ATAK/CivTAK include:

- Online and offline mapping (most standard formats), with a blazing fast rendering engine
- Support for very high-resolution imagery (sub 1 cm resolution)
- Collaborative mapping, including points, drawings, locations of interest
- Extensive and customizable set of Icons
- Overlay Manager which allows the Import and display of KML, KMZ, GPX overlays and maps, including online sources
- Location marking, sharing, history
- Chat, file sharing, photo sharing, video sharing, streaming
- Navigation-walking/hiking, driving, also useful flying and air-ground coordination
- Elevation Tools, heat maps, computed contour maps, viewsheds, routes w/DTED, SRTM, including dynamic profiling
- Hashtags and Sticky tags
- Center on Self, Center on other objects (e.g. another person in the network)
- Range, bearing, and other measurement tools
- Network-aware geofences with triggers
- “Bloodhound” destination tracking, including on moving objects
- Team Emergency Beacons
- Customizable Toolbar
- Radio controls and Integration
- Photo to map capability (aka Rubber Sheeting)
- Casualty evacuation tool
- Icon support for a wide variety of First Responder missions with further extensible Icons
- 3D perspective and ability to display 3D geospatial models
- Useful for First Responders, Hunting, fishing, ornithology, wildlife site survey
- An API with an SDK

29

SAMSUNG
This is Protection.
Samsung Knox

# INTRO

## A new way of working demands a new level of security. Are you sure your devices are protected?

**This is protection.**

Remember the good old days? The morning commute and the 9 to 5? Well those days are history.

Forget being tied to a desk and a schedule. Today's workplace has nothing to do with time or place and everything to do with productivity and mobility. Without compromise. Today's employees want the same access, speed and resources of the office, even if they're three time zones and two continents away.

While mobile, employees spend a significant amount of time outside of their protected corporate networks as they access the web from locations other than their offices. This can expose businesses to more attacks, errors, leaks and new dangers we haven't even encountered.

For IT leaders, supporting a mobile workforce while maintaining the same level of productivity they would have had in the office is extremely difficult. Doing it while maintaining top level security is nearly impossible. Nearly.

This entirely new way of working demands protection that works in real time, not sometimes. Protection that secures on every layer, not just one. Protection that understands that we're safer when we work together, instead of trying to go it alone. Most importantly, protection is security without compromise and protects without getting in the way of creativity, productivity or freedom.

Protection is what Samsung is all about and it's why we built Samsung Knox, a cutting-edge security platform for mobile experience embedded in your Samsung Galaxy device. We are talking real-time, end-to-end protection, with the best intelligence from leading partners and experts across the industry, including Google, Cisco and more. So if you want to stay a step ahead, you can trust Samsung Galaxy and Samsung Knox to fully protect your way of working.

**This is protection. Samsung Knox.**

30

[30] https://kp4-cdn.samsungknox.com/resource/Samsung%20Knox%20Security%20Handbook_bx4Z.pdf.

# Knox Platform for Enterprise

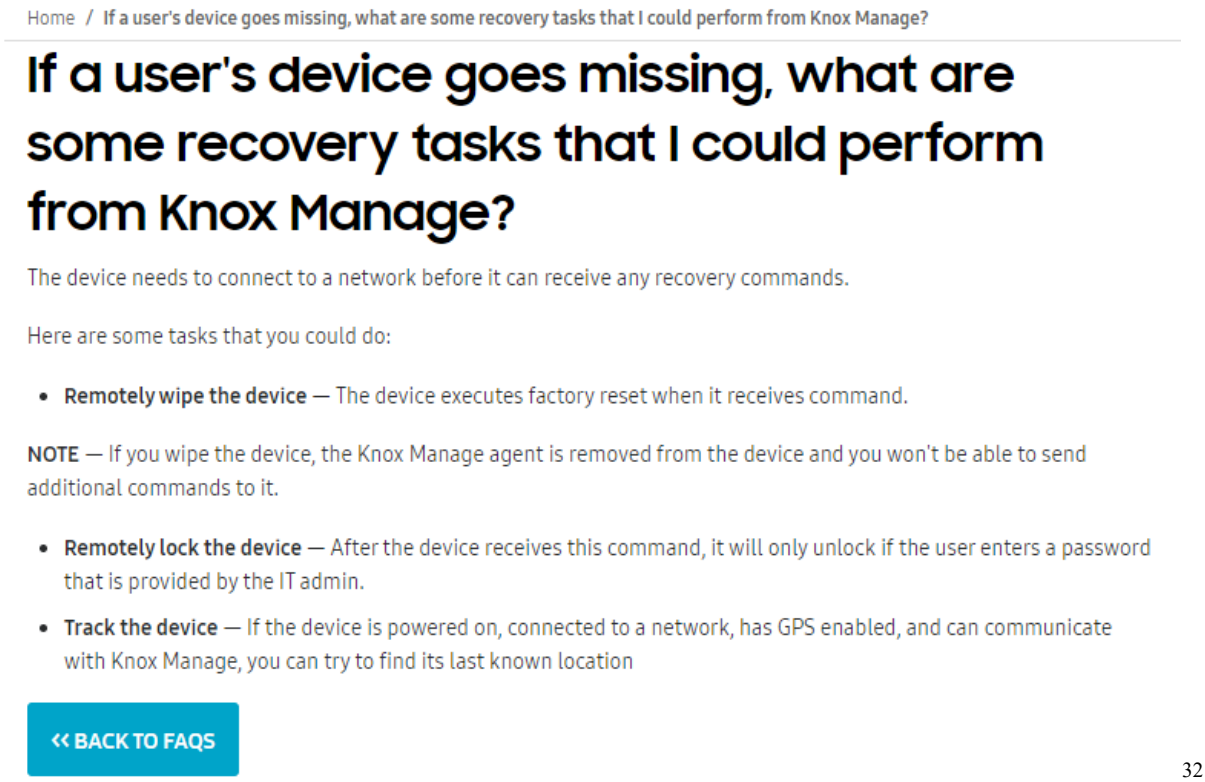
TRY FOR FREE

Samsung's Knox Platform for Enterprise (KPE) brings defense-grade security on the most popular consumer devices to all enterprises.

The Knox Platform provides best-in-class hardware-based security, policy management, and compliance capabilities beyond the standard features commonplace in the mobile device market. The Knox Platform is the cornerstone of a strong mobile security strategy supporting a wide variety of Samsung devices.

[31]

[31] https://docs.samsungknox.com/admin/knox-platform-for-enterprise/welcome.htm.



Home / If a user's device goes missing, what are some recovery tasks that I could perform from Knox Manage?

# If a user's device goes missing, what are some recovery tasks that I could perform from Knox Manage?

The device needs to connect to a network before it can receive any recovery commands.

Here are some tasks that you could do:

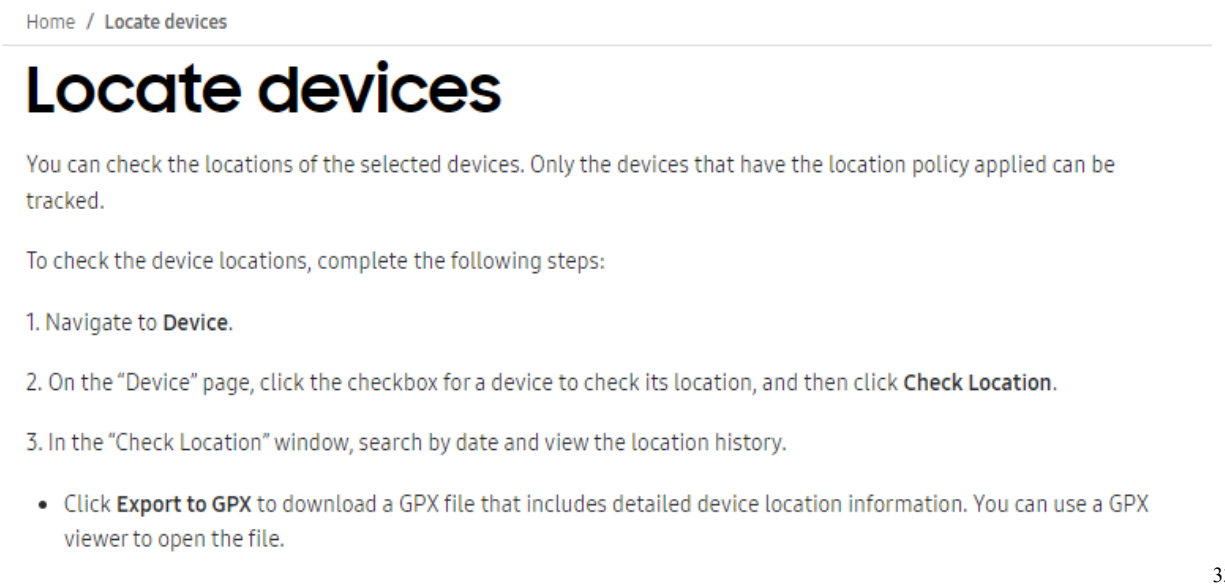
- **Remotely wipe the device** — The device executes factory reset when it receives command.

**NOTE** — If you wipe the device, the Knox Manage agent is removed from the device and you won't be able to send additional commands to it.

- **Remotely lock the device** — After the device receives this command, it will only unlock if the user enters a password that is provided by the IT admin.
- **Track the device** — If the device is powered on, connected to a network, has GPS enabled, and can communicate with Knox Manage, you can try to find its last known location

<< BACK TO FAQS

32



Home / Locate devices

# Locate devices

You can check the locations of the selected devices. Only the devices that have the location policy applied can be tracked.

To check the device locations, complete the following steps:

1. Navigate to **Device**.

2. On the "Device" page, click the checkbox for a device to check its location, and then click **Check Location**.

3. In the "Check Location" window, search by date and view the location history.

- Click **Export to GPX** to download a GPX file that includes detailed device location information. You can use a GPX viewer to open the file.

33

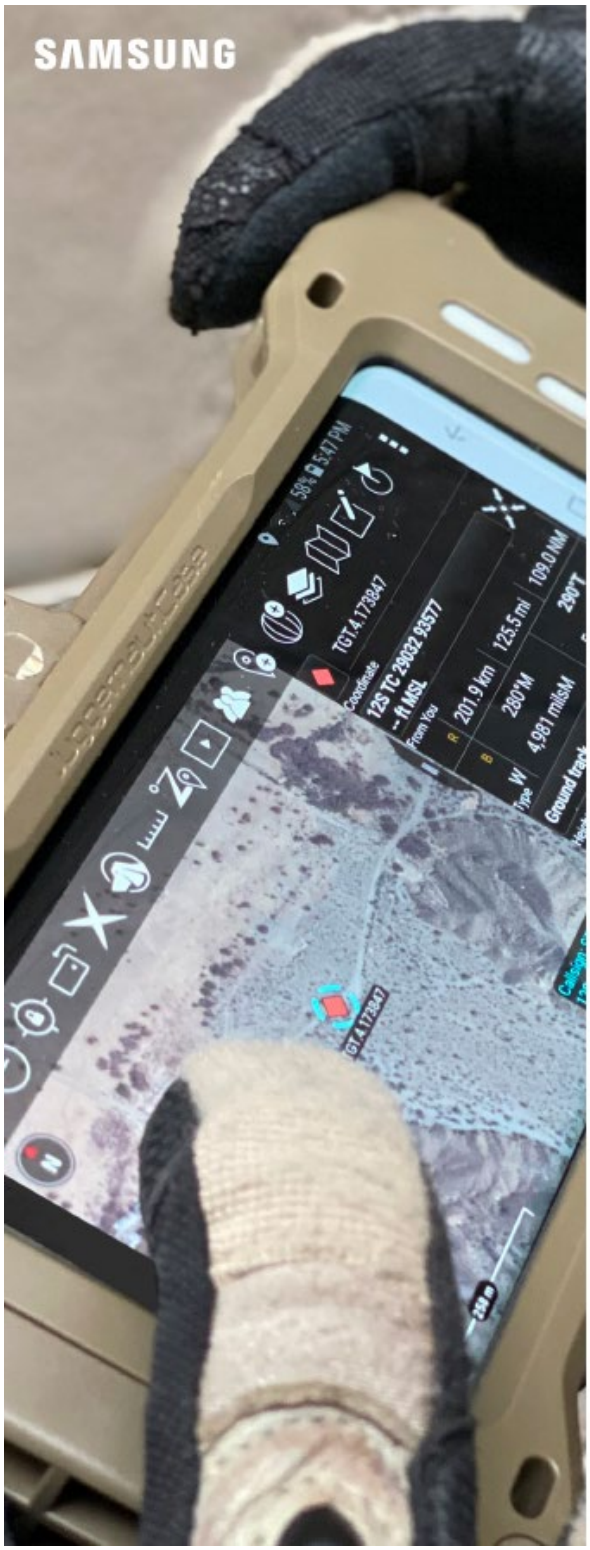
38. For example, Defendants' Accused Products allow users to share their locations and view other users' location on a map and to communicate with those users via the Samsung

[32] https://docs.samsungknox.com/admin/knox-manage/faqs/faq-115013698467.htm.
[33] https://docs.samsungknox.com/admin/knox-manage/locate-devices.htm.

Tactical, TAK, and ATAK applications and services and Samsung Knox applications and services (as shown below).

34

[34] https://www.pargovernment.com/tactical-sa/docs/S20_brochure.pdf




## Galaxy S20 Tactical Edition

# Mission-ready mobility. Proven by operators.

The Samsung Galaxy S20 Tactical Edition is the mission-ready military smartphone built and proven by operators in special operations. Based on the proven success of the S9 Tactical Edition for operators in the field, the S20 Tactical Edition is the only end user device you'll need for mission planning, training, operations and daily use.

### Persistent communications in any domain

**Purpose-built to connect to tactical radios** and mission systems out of the box, the Galaxy S20 Tactical Edition delivers a complete and accurate common operational picture. Run mission applications in the field and enterprise applications everywhere else with a single end user device for mission training, planning, operations and everyday use.

### Interoperable across devices and networks

**Pre-configured software, pre-loaded during the manufacturing process,** includes drivers to support tactical radios and mission-critical devices. Multi-ethernet capabilities provide dedicated connections to multiple mission systems including drone feeds, laser range finders, and external GPS. Support for current and next-generation networks includes Private SIM, 5G, WiFi 6 and CBRS. Allow or disallow USB peripherals based on product or vendor identifiers.

### Command and control

**Integrate voice, video and tactical data** for a complete view of the battlespace to enhance precision and effectiveness. Unique tactical features on the Galaxy S20 Tactical Edition include night-vision mode, stealth mode, lock screen autorotate, hostage negotiation mode, LTE band lock for consistent 4G connection, tactical application quick launch, to keep the operator focused on the objective, Standalone(5G)/Non-standalone (4G) modes to stay on preferred network. Preloaded tactical settings app. Ability to configure hotspot 2.0.

### Capture Intelligence

**A Pro-grade 64 MP camera** on the Galaxy S20 Tactical Edition enhances intel gathering, even in low-light environments without a flash. Capture high-resolution photos or sharp 8K video reconnaissance without giving away your position.

### Power to extend the mission

**Keep going wherever the mission takes you** with the Galaxy S20 Tactical Edition's intelligent2 4000mAh battery is 30% larger than the previous tactical solution and optimizes energy based on your device usage. Easily share power with a team member's smartphone in the field simply by touching devices using Wireless PowerShare.[4]

### One device to meet your requirements

**Run mission applications in the field** and enterprise applications everywhere else with the powerful and efficient Galaxy S20 Tactical Edition 64-bit Octa-Core processor. Connect your device to a monitor keyboard and mouse and use the power of Samsung DeX[5] for a desktop-like experience that is ideal for mission planning, training and everyday use. DeX-in-Vehicle transforms your Galaxy S20 Tactical Edition into an in-vehicle computer.

### Open and secure

**Enable a diverse ecosystem of tactical partners** with the open and secure Android operating system on the Galaxy S20 Tactical Edition. The all-new Tactical Settings feature simplifies device management, while Samsung Knox provides defense-grade security[6] from the hardware layer up and mission-specific device customization capabilities. The DualDAR architecture of the Galaxy S20 Tactical Edition provides two layers of encryption, even when the device is powered off, for securing up-to top secret level data on the device.

### Tested and proven

Samsung Galaxy Tactical Edition smartphones are tested and proven by special operators in the field. The Galaxy S20 Tactical Edition is certified to meet the most stringent requirements including NSA's CSFC Components List, NIAP Common Criteria/MDFPP, DODIN APL, FIPS 140-2, DISA Android 10 STIG, IP68 rating.

**Contact Us:** www.samsung.com/TacticalEdition

35

[35] https://image-us.samsung.com/SamsungUS/samsungbusiness/pdfs/flyer/S20_TE-salesflyer_FINAL_July_2021.pdf

The Team Awareness Kit (TAK), for civilian uses, or Tactical Assault Kit (also TAK) for military uses is a suite of software that provides geospatial information and allows user collaboration over geography. There are numerous TAK Products in the TAK family, all developed at government expense

The Team Awareness Kit for Android (ATAK, also known as CivTAK) was originally developed by the Air Force Research Laboratory (AFRL) and is now maintained by a Joint Product Center.

ATAK (including CivTAK) is an Android smartphone geospatial infrastructure and situational awareness app. It allows for precision targeting, surrounding land formation intelligence, situational awareness, navigation, and data sharing.

All the Android variants of TAK are virtually identical and all are interoperable with each other and with other TAK products. There are small, military-specific additions in military versions of ATAK.

# Features

Industry/civilian capabilities of ATAK/CivTAK include:

- Online and offline mapping (most standard formats), with a blazing fast rendering engine
- Support for very high-resolution imagery (sub 1 cm resolution)
- Collaborative mapping, including points, drawings, locations of interest
- Extensive and customizable set of Icons
- Overlay Manager which allows the Import and display of KML, KMZ, GPX overlays and maps, including online sources
- Location marking, sharing, history
- Chat, file sharing, photo sharing, video sharing, streaming
- Navigation-walking/hiking, driving, also useful flying and air-ground coordination
- Elevation Tools, heat maps, computed contour maps, viewsheds, routes w/DTED, SRTM, including dynamic profiling
- Hashtags and Sticky tags
- Center on Self, Center on other objects (e.g. another person in the network)
- Range, bearing, and other measurement tools
- Network-aware geofences with triggers
- “Bloodhound” destination tracking, including on moving objects
- Team Emergency Beacons
- Customizable Toolbar
- Radio controls and Integration
- Photo to map capability (aka Rubber Sheeting)
- Casualty evacuation tool
- Icon support for a wide variety of First Responder missions with further extensible Icons
- 3D perspective and ability to display 3D geospatial models
- Useful for First Responders, Hunting, fishing, ornithology, wildlife site survey
- An API with an SDK

Unclassified

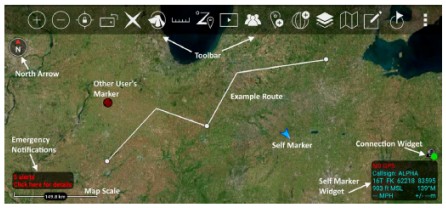
## ATAK Civilian Overview

The Civilian Team Awareness Kit for Android (ATAK Civilian) is a Government-off-the-Shelf (GOTS) software application and mapping framework for mobile devices. ATAK Civilian has been designed and developed to run on Android smart devices used in a first responder environment. The ATAK Civilian software application is an extensible moving map display that integrates imagery, map and overlay information to provide enhanced collaboration and Situational Awareness (SA) over a tactical meshed network. ATAK Civilian promotes information flow and communications from the field environment to command enterprise locations.

The first time ATAK Civilian is opened, or after a Clear Content, a passphrase is auto-generated to activate data encryption. The user can supply their own passphrase by using Settings > Show All Preferences > Device Preferences > Change Encryption Passphrase. Following this step, ATAK Civilian's End User License Agreement (EULA) must be accepted. Next, the user will be prompted to change their callsign and/or import preferences or data from a Mission Package. All changes/imports can always be updated later. Finally, the user can place their self-marker by following the instructions located in the lower right corner.

The toolbar runs along the top of the map display. The features whose icons form the center portion of the toolbar are discussed in individual sections of this guide. The three dots at the right of the toolbar provide additional menu items that appear in a drop-down menu. A Long Press on the map will toggle the toolbar between hidden and visible.

The North Arrow appears in the upper left and is used to control map orientation. It has two primary modes: North Up/Track Up (default) and Manual Map Rotation/Lock. While in North Up/Track Up Mode, single press on the [**North Arrow**] icon to cycle between the North Up and Track Up map orientation. Long press the [**North Arrow**] to call out the additional controls menu where the Manual Rotation/Lock and 3D features are available. Select the [**Rotation**] button to enter Manual Map Rotation/Lock Mode. When in Manual Map Rotation/Lock Mode, rotate the map orientation by pressing on the map with two fingers and pivoting them in the desired direction. Single press on the [**North Arrow**] to lock the screen orientation, signified by the appearance of the lock icon, and again to unlock the orientation for further adjustment. 3D controls are discussed in a separate section.




Select the [**Magnifier**] buttons to zoom in or out on the map. The map can also be zoomed by using two fingers on the screen to pinch and spread the map. Select the [**Back**] button to center the screen on the Self Marker or the [**Padlock**] icon to lock the center of the screen to the Self Marker. Select the [**Orientation**] icon to toggle the screen position between portrait and landscape.

The optional connection widget indicates whether or not the user is connected to a TAK Server. This has a corresponding Android notification that provides the same information. Toggle this display on at Settings > Network Connections > Network Connections > Display Connection Widget.

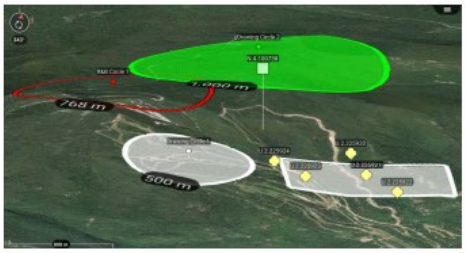
Alerts and notifications are displayed in the lower left of the map interface.

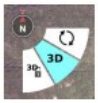
The Map Scale displays a 1 inch to X mi/km reference on the map. The scale adjusts with the map when zoomed in and out. Hint windows are available to alert users to changes or make suggestions about the use of tools the first time they are opened.

5

Unclassified

## 3D View




ATAK Civilian features 3D viewing of terrain and map items (DTED required). To enable 3D view, long press on the [**North Arrow**] to call out the additional controls menu and select [**3D**]. A tilt angle indicator will appear around the edge of the [**North Arrow**] when 3D view is active. Touch the screen with two fingers and simultaneously swipe up or down on the screen to tilt the view angle. Once the appropriate viewing angle is set, select the [**3D Lock**] button to retain this view while panning the map. While viewing the map from an angle, some map items will appear raised above the map surface if they have defined elevations.

## 3D Models

ATAK Civilian supports the use of 3D models. OBJ models and other types from products such as Pix4D can be imported via the Import Manager or can be manually placed in the atak/overlays folder prior to startup. If using Import Manager browse to the .OBJ file and import only that file, or browse to a .ZIP file that contains the .OBJ file (and others) and import only that file. If using manual placement to the atak/overlays folder, place a .ZIP file containing the .OBJ file (and others) into the directory and they will be imported on startup.

Once imported, a 3D Model icon will appear on the map. Zoom into the area of the icon until a loading ring appears. After the loading process has finished, the 3D model will be projected onto the map. Enable the map 3D View and tilt the view angle to see the 3D modeling. Loaded 3D models will appear as their own category in Overlay Manager and can be toggled on/off or removed from there.

6

[36] https://www.civtak.org/documentation/

Unclassified

## Placement

The user can enter locations of interest using the Point Dropper tool. Select the [**Point Dropper**] icon to place internationally standardized markers and other icons on the map, edit the data and share the markers with other network members.

### Self-Marker

The Self-Marker is displayed as a blue arrowhead at the user's current location. The options available on the Self-Marker radial are: Compass Rose, Polar Coordinate Entry, Fine Adjust/Enter Coordinate/MGRS Location, GPS Error, Range & Bearing Line, GPS Lock to Self, Tracking Breadcrumbs, Place a Marker at the user's current location and Details. Other TAK users appear on the display as a colored circle. The color of the circle represents the user's Team affiliation, with additional lettering inside the circle to identify the role the user on the team. Team Member markers that include a diagonal line indicate that the GPS location is not available. A solid icon indicated that the team member has GPS reception.

Available roles include: Team Member, Team Lead (designated by a TL in the center of the marker), Headquarters (HQ in center), Sniper (S), Medic (+), Forward Observer (FO), RTO (R) or K9 (K9). The options available when another user's Self-Marker is selected are: Inner Ring – Delete, Polar Coordinate Entry, Fine Adjust/Enter Coordinate/MGRS Location, Range & Bearing Line, GPS Lock on Friendly, Video Player (if available), Communication Options (if configured by that user), Custom Threat Rings, Tracking Breadcrumbs and Details.

Outer Ring (Communication Options) – Data Package, Email, SMS Messaging, GeoChat, VOIP and Cellular Phone, when available.

Unclassified

## Point Dropper

Selecting the [**Point Dropper**] icon will open the Point Dropper menu, containing marker symbology with one or more icon sets, a Recently Added button and an Iconset Manager button.

The Markers symbology affiliations are: Unknown, Neutral, Red and Friendly. Select the affiliation, then a location on the map interface to drop the marker. To add a marker by manually entering coordinates, long press on the map interface and enter the MGRS location. Change the standard naming convention by entering values into the custom prefix and index fields or leave blank to use the defaults. If values are entered, the next marker will be dropped with the prefix name and starting number(s) or letter(s) and every subsequent marker will be assigned the next consecutive number(s) or letter(s).

The user can select the mission specific pallet to open point options including Waypoint (WP), Sensor or Observation Point (OP).

The user can move between icon sets by either swiping in the icon set area or selecting on the [**Iconset Name**] field to bring up the Icon Pallet drop-down.

The last point placed is shown at the bottom of the Point Dropper window. The information for all recently placed points can be accessed by selecting the [**Clock**] icon. This displays the marker icon, name, coordinates, elevation and range & bearing information. The user can send, rename or remove any recently added markers by selecting the [**Arrows**] next to the marker to reveal [**SEND**], [**RENAME**] or [**DEL**] buttons.

Select the [**Iconset Manager**] (gear) button to add or delete icon sets or to set the default Marker Mapping.

## Radial Menus

**Unknown Object** | **Neutral Object** | **Red Object** | **Friendly Object** | **Spot Object**

The options available for Unknown Object Markers are: Delete, Polar Coordinate Entry, Fine Adjust/Enter Coordinate/MGRS Location, Range & Bearing Line, Lock On, Tasking, Custom Threat Rings, Tracking Breadcrumbs and Details.

The options available for Neutral Object Markers are: Delete, Polar Coordinate Entry, Fine Adjust/Enter Coordinate/MGRS Location, Range & Bearing Line, Lock On, Tasking, Custom Threat Rings, Tracking Breadcrumbs and Details.

The options available for Red Object Markers are: Delete, Polar Coordinate Entry, Compass Rose/Bullseye, Fine Adjust/Enter Coordinate/MGRS Location, Range & Bearing Line, Tasking, Custom Threat Rings, Tracking Breadcrumbs and Details.

The options available for Friendly Object Markers are: Delete, Polar Coordinate Entry, Fine Adjust/Enter Coordinate/MGRS Location, Range & Bearing Line, Lock On, Video, Contact Card, Custom Threat Rings, Tracking Breadcrumbs and Details. The Video radial will activate if a properly formatted packet that includes the link to the video feed is included. Select the video radial to open the associated video. The Contact Card can be selected to display additional communication options, including GeoChat, Email, VoIP, SMS Messaging and Cellular Phone, when available.

The options available for Spot Map are: Delete, Fine Adjust/Enter Coordinate/MGRS Location, Range & Bearing Line, Nav-To, Custom Threat Rings, Labels and Details.

The options for User Defined Iconsets are: Delete, Polar Coordinate Entry, Fine Adjust/Enter Coordinate/MGRS Location, Range & Bearing Line, Lock On, Tasking, Custom Threat Rings. Tracking Breadcrumbs and Details.

Select [**Details**] on the marker radial to make desired modifications, including: Coordinate, Elevation, Name, Type and Remarks. Selecting Marker Type opens a dialog box with extra categories. File attachments, including images, can be associated with the object by selecting the [**Paperclip**] icon. Once all the desired modifications have been made, the Marker can be sent to other network members using [**Send**]. The information can be broadcast to all members or sent to specific recipients. Select the [**Auto Send**] option to broadcast the marker to other TAK users on the network, with updates automatically sent about once every 60 seconds.



## Bloodhound Tool

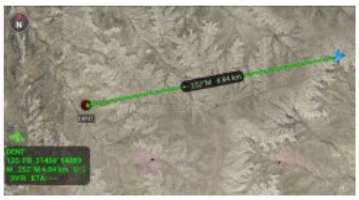
The Bloodhound Tool provides support for tracking and intercepting a map item. It allows the user to select two points on the map and/or map objects and display range & bearing information between the chosen tracker and the target.

Select the [**Bloodhound**] icon to open the Bloodhound Tool. A window will open, prompting the user to choose where to start by tapping the [**From Reticle**] (default = user's self marker) and where to bloodhound (track) to by tapping the [**To Reticle**].

Targets include map objects like other User's Self Markers, DPs, Markers, Shape center points, Range & Bearing endpoints and any other map objects. If the user selects a map location instead of an object as the target, Bloodhound will place a waypoint marker there. The self marker will then track towards the waypoint.

Select [**OK**] and Bloodhound will be activated.

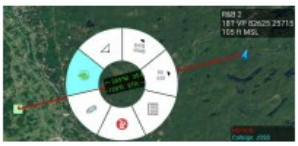
If either point moves, the green widget in the lower left will show the updated information. As the tracking object begins to navigate toward the target, the Estimated Time of Arrival (ETA) will update accordingly.



The green line showing the direct path from the tracker to the target will flash when the user-defined ETA outer threshold is reached (default = 6 minutes from target). The line will flash as the tracker continues toward the target until the next ETA threshold is reached (default = 3 minutes). The line will turn a flashing yellow until the final ETA threshold (default = 1 minute) is reached. The line then flashes red until the target is reached. Colors and thresholds can be modified in Settings > Tool Preferences > Bloodhound Preferences.

Selecting the green Bloodhound icon on the map will pan the map to the Bloodhound Range & Bearing Line. Disengage the Bloodhound Tool by selecting the [**Bloodhound**] icon on the toolbar.

## Multiple Bloodhound



To create multiple bloodhounds, selecting the Range and Bearing Tool and select the [**R&B Line**] icon. Select two markers on the map and once the R&B line is created, select the line to bring up the radial. Select the [**Bloodhound**] radial, and the bloodhound information will be displayed on the R&B Line itself.

If either point moves, the Bloodhound information shown on the R&B Line will be updated. As the tracking object begins to navigate toward the target, the Estimated Time of Arrival (ETA) will update accordingly.

## Go To

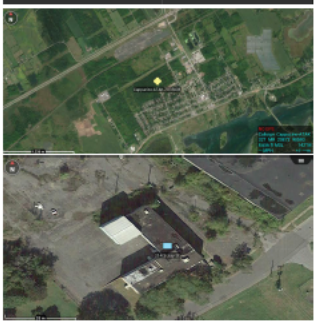
Select the [**Go To**] icon to enter details and navigate to a specific location on the map.

Select from the [**MGRS**] (military grid reference system), [**DD**] (decimal degrees), [**DM**] (degrees- minutes), [**DMS**] (degrees-minutes-seconds), [**UTM**] (Universal Transverse Mercator) or [**ADDR**] tabs on the Go To interface and enter the location data of interest. The address provider name appears beneath the Elevation Data when the user selects the [**ADDR**] tab.

The user can enter the Latitude, Longitude and Elevation in the space provided for [**MGRS**] , [**DD**], [**D-M**] or [**D-M-S**] searches. If DTED is installed, the elevation value can be automatically populated by tapping the [**Pull From DTED**] button.The user can select a desired marker type (Spot, Unknown, Neutral, Red, or Friendly) to be placed at the entered coordinates. If [**No Point**] is selected, the map will pan to the location but will not add a point.

**Note:** The address provider name appears beneath the Elevation Data when the user selects the [**ADDR**] tab.

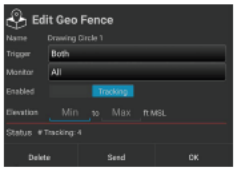
The Address Lookup provider used for the ADDR tab can be configured in the Settings > Tool Preferences > Address Lookup Preferences.



32

## Geofencing

The Geo Fence tool allows users to create a virtual fence that triggers entry/exit notifications if map items of interest cross the virtual boundary lines. The Geo Fence options are added to the existing drawing tools. After a shape has been added, the Geo Fence Tool can be accessed either by selecting the [**Geo Fence**] icon from the menu items or selecting it from the radial.




The Enabled Field slider will move to Tracking by default when a new Geo Fence window is created. Toggle the slider between Tracking and Off to enable/disable the Geo Fence. Use the Trigger field to define which types of Geo Fence breach to monitor. Choose between Entry, Exit or Both. Use the Monitor field to define which entities the Geo Fence will track.

Choose between TAK Users, Friendly, Hostile, Custom or All. Check the [**Specify Elevation**] box to enable the Elevation field, where elevation boundaries for the entities being tracked can be defined. Select the [**OK**] button to finish creating the fence. Select the [**Send**] button to create the fence and send it to another user. Select [**Delete**] to close the Create Geo Fence window and discard changes.

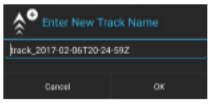
Alerts appear on the map interface. Selecting the [**Alert Notification**] will open the alerts menu, detailing the activity monitored in the user defined region. The default radius for monitoring users (filtered within the "Monitor" field) outside the Geo Fence is set at 75 km. This means the total area monitored begins at the farthest point from the center of the shape plus 75 km. If the user wishes to keep the Geo Fence, but disable tracking, the user can set the tracking [**Enabled**] to off in the Edit Window.

35

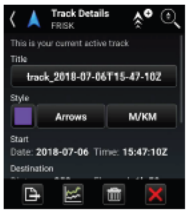
Unclassified

## Track History

The device's GPS can be used to track movements with the Track History tool. These tracked paths can be exported to a TAK server, to a route or to a KML, KMZ, GPX or CSV file. A GPS position must be established before tracking can begin.

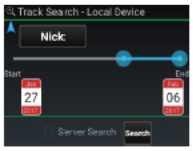



Selecting the [**Track History**] icon will open Track Details for the current active track. The track title, color and style can be modified. Initiate a new track by selecting the [**Add Track**] icon. Accept or edit the default track name and select the [**OK**] button to begin the new track. User location data is recorded as breadcrumbs in a new track file.

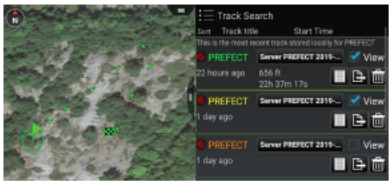



## Track Search

Use the Track Search function to view track information that has been previously saved locally or on a TAK Server. The tool searches the track database for matches against the specified time range and by user callsign. Matching tracks are displayed as a list, and can be selected to view on the map interface.




Select the [**Track Search**] icon to access the function. Specify callsign and time frame, check the box for Server Search (if desired), then select [**Search**]. The track list will appear. The query results can be sorted by Track Name or Start Time. Select any of the query results to move to that track. Once selected, the name, color, and style of a selected track can be modified or the track can be cleared. Convert a track to a TAK route or export it as a KML, KMZ, GPX or CSV file by selecting the desired track and then [**Export**]. Enter a file name then select [**Next**] and choose the export format. Select [**Done**] or [**Send**] when the export completes.



When viewing the track list, the Track History Toolbar will appear at the top of the screen. The options include [**Add a Track**], [**Multi-select**], [**Track Search**], [**Clear Tracks**] and [**Exit**]. The Track History List allows the user to select tracks of other users that have been saved on their device. The Track Search – Local Device allows the user to perform a tailored search for tracks meeting their criteria. The searching option allows the user to retrieve all the tracks on the device.

The Track History Breadcrumb and Settings can be configured in the Settings > Tools Preferences > Track History Preferences.

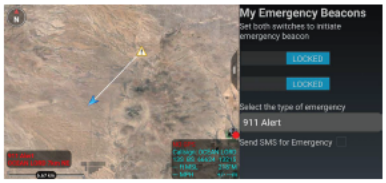
37

Unclassified

## Emergency Beacon

Select the [**Emergency Beacon**] icon to open the Emergency Beacon Tool.

The Emergency Beacon allows the user to indicate their need for assistance, the type of emergency and their location on the map. The type of emergency can be selected from the drop-down menu, before activation, and includes options for an Alert, Ring the Bell, Geo Fence Breached or In Contact.




Once the Emergency type has been selected and both switches have been enabled, the TAK Server broadcasts the announcements to all network contacts. Even if the user's device is turned off, the beacon will continue. Only when the user returns to the Emergency Beacon tool and turns off the switches will the beacon be canceled and removed. If the SMS for Emergency option has been configured, the alert will be sent via text message to the configured numbers.

37

[37] https://drive.google.com/file/d/1bo9WHadg3J3o55OLlx1mn3McqEJzvgrK/view

Home / Locate devices

# Locate devices

You can check the locations of the selected devices. Only the devices that have the location policy applied can be tracked.

To check the device locations, complete the following steps:

1. Navigate to **Device**.

2. On the "Device" page, click the checkbox for a device to check its location, and then click **Check Location**.

3. In the "Check Location" window, search by date and view the location history.

- Click **Export to GPX** to download a GPX file that includes detailed device location information. You can use a GPX viewer to open the file.

[38]

Home / Send device commands to users

# Send device commands to users

You can send device commands to the user's enrolled devices. For more information on each device command, see Sending device commands to devices.

To send device commands, complete the following steps:

1. Navigate to **User**.

2. On the "User" page, click the check box next to the user ID to send a device command to.

3. Click **Device Command** and select the supported OS platform (enrolled device).

4. In the "Device Command" window, select a desired device command.

5. In the "Request Command" window, click **OK**.

[39]

[38] https://docs.samsungknox.com/admin/knox-manage/locate-devices.htm
[39] https://docs.samsungknox.com/admin/knox-manage/send-commands-to-users-devices.htm

# Check the locations of devices

You can check the locations of the selected devices. Only the devices that have the location policy applied can be tracked.

> **NOTE** — You can only check a device's location if location data was collected at least once.

**IMPORTANT** — In order to track the location of Android 11 and 12 devices, the device user must grant the KM agent location access. This affects devices with the following deployment types:

- Employee-owned devices with a Work Profile
- Shared devices with a secondary account

You should inform users with these devices to allow the following access settings:

- Android 11:
  1. When the KM agent requests location access, the user must select **While using this app**.
  2. Then, they must go to **Work profile settings** >**Apps** >**Knox Manage** >**App permissions**, and set **Location** to **Allow all the time**.
- Android 12 and higher:
  - When the KM agent requests location access, the user must select **Precise** and **While using this app**.

1. Navigate to **Device**.
2. On the **Device** page, select one or more devices, and then click **Check Location**.
3. On the **Check Location** page, search by date. The view shows an interactive map of the devices and their location history.

On this page, you can inspect individual device information, as well as export their location history as as a GPX file.

# Device map

On the **Check Location** screen, a map displays the latest locations of all tracked devices. The map uses the following legend:

| Element | Meaning |
|---|---|
| | Active device |
| | Device with expired keepalive |
| | Cluster of 1–9 devices |
| | Cluster of 10–99 devices |
| | Cluster of 100–999 devices |
| | Cluster of 1000–9999 devices |

You can view an individual device's status by hovering over its pin . On hover, a tooltip lists the following information:

- Device name
- IMEI/MEID
- Serial Number
- Mobile Number
- User Name
- Last Location Scanned
- Organization Name
- Group Name
- Tag
- Platform & Management Type
- Model Name
- MAC Address
- Manufacturer

[40]

[40] https://docs.samsungknox.com/admin/knox-manage/check-the-locations-of-devices.htm.

39. Additionally, the exemplary Accused Products allow users to establish groups and to exchange messages via interaction with Samsung's servers which provide the Samsung Tactical, TAK, and ATAK services and Samsung Knox services, among other relevant services. The exemplary Accused Products further allow users to retrieve map information from multiple sources including street-view maps, as well as satellite renderings.

Unclassified

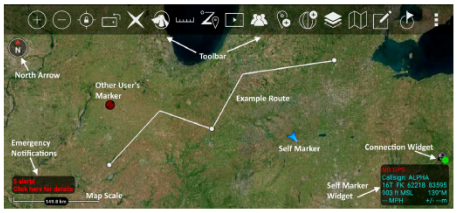
## ATAK Civilian Overview

The Civilian Team Awareness Kit for Android (ATAK Civilian) is a Government-off-the-Shelf (GOTS) software application and mapping framework for mobile devices. ATAK Civilian has been designed and developed to run on Android smart devices used in a first responder environment. The ATAK Civilian software application is an extensible moving map display that integrates imagery, map and overlay information to provide enhanced collaboration and Situational Awareness (SA) over a tactical meshed network. ATAK Civilian promotes information flow and communications from the field environment to command enterprise locations.

The first time ATAK Civilian is opened, or after a Clear Content, a passphrase is auto-generated to activate data encryption. The user can supply their own passphrase by using Settings > Show All Preferences > Device Preferences > Change Encryption Passphrase. Following this step, ATAK Civilian's End User License Agreement (EULA) must be accepted. Next, the user will be prompted to change their callsign and/or import preferences or data from a Mission Package. All changes/imports can always be updated later. Finally, the user can place their self-marker by following the instructions located in the lower right corner.

The toolbar runs along the top of the map display. The features whose icons form the center portion of the toolbar are discussed in individual sections of this guide. The three dots at the right of the toolbar provide additional menu items that appear in a drop-down menu. A Long Press on the map will toggle the toolbar between hidden and visible.

The North Arrow appears in the upper left and is used to control map orientation. It has two primary modes: North Up/Track Up (default) and Manual Map Rotation/Lock. While in North Up/Track Up Mode, single press on the [**North Arrow**] icon to cycle between the North Up and Track Up map orientation. Long press the [**North Arrow**] to call out the additional controls menu where the Manual Rotation/Lock and 3D features are available. Select the [**Rotation**] button to enter Manual Map Rotation/Lock Mode. When in Manual Map Rotation/Lock Mode, rotate the map orientation by pressing on the map with two fingers and pivoting them in the desired direction. Single press on the [**North Arrow**] to lock the screen orientation, signified by the appearance of the lock icon, and again to unlock the orientation for further adjustment. 3D controls are discussed in a separate section.




Select the [**Magnifier**] buttons to zoom in or out on the map. The map can also be zoomed by using two fingers on the screen to pinch and spread the map. Select the [**Back**] button to center the screen on the Self Marker or the [**Padlock**] icon to lock the center of the screen to the Self Marker. Select the [**Orientation**] icon to toggle the screen position between portrait and landscape.

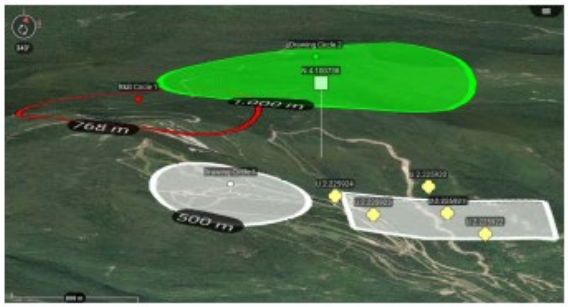
The optional connection widget indicates whether or not the user is connected to a TAK Server. This has a corresponding Android notification that provides the same information. Toggle this display on at Settings > Network Connections > Network Connections > Display Connection Widget.

Alerts and notifications are displayed in the lower left of the map interface.

The Map Scale displays a 1 inch to X mi/km reference on the map. The scale adjusts with the map when zoomed in and out. Hint windows are available to alert users to changes or make suggestions about the use of tools the first time they are opened.

5

## 3D View



ATAK Civilian features 3D viewing of terrain and map items (DTED required). To enable 3D view, long press on the **[North Arrow]** to call out the additional controls menu and select [**3D**]. A tilt angle indicator will appear around the edge of the [**North Arrow**] when 3D view is active. Touch the screen with two fingers and simultaneously swipe up or down on the screen to tilt the view angle. Once the appropriate viewing angle is set, select the [**3D Lock**] button to retain this view while panning the map. While viewing the map from an angle, some map items will appear raised above the map surface if they have defined elevations.

## 3D Models

ATAK Civilian supports the use of 3D models. OBJ models and other types from products such as Pix4D can be imported via the Import Manager or can be manually placed in the atak/overlays folder prior to startup. If using Import Manager browse to the .OBJ file and import only that file, or browse to a .ZIP file that contains the .OBJ file (and others) and import only that file. If using manual placement to the atak/overlays folder, place a .ZIP file containing the .OBJ file (and others) into the directory and they will be imported on startup.

Once imported, a 3D Model icon will appear on the map. Zoom into the area of the icon until a loading ring appears. After the loading process has finished, the 3D model will be projected onto the map. Enable the map 3D View and tilt the view angle to see the 3D modeling. Loaded 3D models will appear as their own category in Overlay Manager and can be toggled on/off or removed from there.

Unclassified

## Placement

The user can enter locations of interest using the Point Dropper tool. Select the [**Point Dropper**] icon to place internationally standardized markers and other icons on the map, edit the data and share the markers with other network members.

### Self-Marker

The Self-Marker is displayed as a blue arrowhead at the user's current location. The options available on the Self-Marker radial are: Compass Rose, Polar Coordinate Entry, Fine Adjust/Enter Coordinate/MGRS Location, GPS Error, Range & Bearing Line, GPS Lock to Self, Tracking Breadcrumbs, Place a Marker at the user's current location and Details. Other TAK users appear on the display as a colored circle. The color of the circle represents the user's Team affiliation, with additional lettering inside the circle to identify the role the user on the team. Team Member markers that include a diagonal line indicate that the GPS location is not available. A solid icon indicated that the team member has GPS reception.

Available roles include: Team Member, Team Lead (designated by a TL in the center of the marker), Headquarters (HQ in center), Sniper (S), Medic (+), Forward Observer (FO), RTO (R) or K9 (K9). The options available when another user's Self-Marker is selected are: Inner Ring – Delete, Polar Coordinate Entry, Fine Adjust/Enter Coordinate/MGRS Location, Range & Bearing Line, GPS Lock on Friendly, Video Player (if available), Communication Options (if configured by that user), Custom Threat Rings, Tracking Breadcrumbs and Details.

Outer Ring (Communication Options) – Data Package, Email, SMS Messaging, GeoChat, VOIP and Cellular Phone, when available.

Unclassified

## Radial Menus

**Unknown Object** **Neutral Object** **Red Object** **Friendly Object** **Spot Object**

The options available for Unknown Object Markers are: Delete, Polar Coordinate Entry, Fine Adjust/Enter Coordinate/MGRS Location, Range & Bearing Line, Lock On, Tasking, Custom Threat Rings, Tracking Breadcrumbs and Details.

The options available for Neutral Object Markers are: Delete, Polar Coordinate Entry, Fine Adjust/Enter Coordinate/MGRS Location, Range & Bearing Line, Lock On, Tasking, Custom Threat Rings, Tracking Breadcrumbs and Details.

The options available for Red Object Markers are: Delete, Polar Coordinate Entry, Compass Rose/Bullseye, Fine Adjust/Enter Coordinate/MGRS Location, Range & Bearing Line, Tasking, Custom Threat Rings, Tracking Breadcrumbs and Details.

The options available for Friendly Object Markers are: Delete, Polar Coordinate Entry, Fine Adjust/Enter Coordinate/MGRS Location, Range & Bearing Line, Lock On, Video, Contact Card, Custom Threat Rings, Tracking Breadcrumbs and Details. The Video radial will activate if a properly formatted packet that includes the link to the video feed is included. Select the video radial to open the associated video. The Contact Card can be selected to display additional communication options, including GeoChat, Email, VoIP, SMS Messaging and Cellular Phone, when available.

The options available for Spot Map are: Delete, Fine Adjust/Enter Coordinate/MGRS Location, Range & Bearing Line, Nav-To, Custom Threat Rings, Labels and Details.

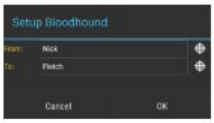
The options for User Defined Iconsets are: Delete, Polar Coordinate Entry, Fine Adjust/Enter Coordinate/MGRS Location, Range & Bearing Line, Lock On, Tasking, Custom Threat Rings. Tracking Breadcrumbs and Details.

Select [**Details**] on the marker radial to make desired modifications, including: Coordinate, Elevation, Name, Type and Remarks. Selecting Marker Type opens a dialog box with extra categories. File attachments, including images, can be associated with the object by selecting the [**Paperclip**] icon. Once all the desired modifications have been made, the Marker can be sent to other network members using [**Send**]. The information can be broadcast to all members or sent to specific recipients. Select the [**Auto Send**] option to broadcast the marker to other TAK users on the network, with updates automatically sent about once every 60 seconds.

## Bloodhound Tool

The Bloodhound Tool provides support for tracking and intercepting a map item. It allows the user to select two points on the map and/or map objects and display range & bearing information between the chosen tracker and the target.

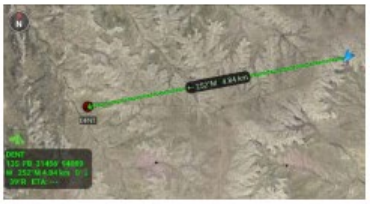
Select the [**Bloodhound**] icon to open the Bloodhound Tool. A window will open, prompting the user to choose where to start by tapping the [**From Reticle**] (default = user's self marker) and where to bloodhound (track) to by tapping the [**To Reticle**].




Targets include map objects like other User's Self Markers, DPs, Markers, Shape center points, Range & Bearing end-points and any other map objects. If the user selects a map location instead of an object as the target, Bloodhound will place a waypoint marker there. The self marker will then track towards the waypoint.

Select [**OK**] and Bloodhound will be activated.

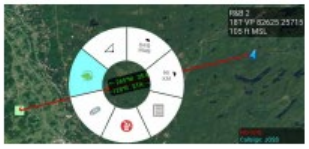
If either point moves, the green widget in the lower left will show the updated information. As the tracking object begins to navigate toward the target, the Estimated Time of Arrival (ETA) will update accordingly.



The green line showing the direct path from the tracker to the target will flash when the user-defined ETA outer threshold is reached (default = 6 minutes from target). The line will flash as the tracker continues toward the target until the next ETA threshold is reached (default = 3 minutes). The line will turn a flashing yellow until the final ETA threshold (default = 1 minute) is reached. The line then flashes red until the target is reached. Colors and thresholds can be modified in Settings > Tool Preferences > Bloodhound Preferences.

Selecting the green Bloodhound icon on the map will pan the map to the Bloodhound Range & Bearing Line. Disengage the Bloodhound Tool by selecting the [**Bloodhound**] icon on the toolbar.

## Multiple Bloodhound



To create multiple bloodhounds, selecting the Range and Bearing Tool and select the [**R&B Line**] icon. Select two markers on the map and once the R&B line is created, select the line to bring up the radial. Select the [**Bloodhound**] radial, and the bloodhound information will be displayed on the R&B Line itself.

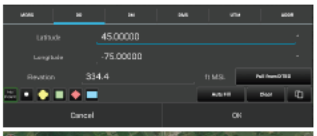
If either point moves, the Bloodhound information shown on the R&B Line will be updated. As the tracking object begins to navigate toward the target, the Estimated Time of Arrival (ETA) will update accordingly.



## Go To

Select the [**Go To**] icon to enter details and navigate to a specific location on the map.

Select from the [**MGRS**] (military grid reference system), [**DD**] (decimal degrees), [**DM**] (degrees - minutes), [**DMS**] (degrees-minutes-seconds), [**UTM**] (Universal Transverse Mercator) or [**ADDR**] tabs on the Go To interface and enter the location data of interest. The address provider name appears beneath the Elevation Data when the user selects the [**ADDR**] tab.



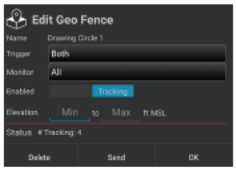

The user can enter the Latitude, Longitude and Elevation in the space provided for [**MGRS**] , [**DD**], [**D-M**] or [**D-M-S**] searches. If DTED is installed, the elevation value can be automatically populated by tapping the [**Pull From DTED**] button.The user can select a desired marker type (Spot, Unknown, Neutral, Red, or Friendly) to be placed at the entered coordinates. If [**No Point**] is selected, the map will pan to the location but will not add a point.

**Note:** The address provider name appears beneath the Elevation Data when the user selects the [**ADDR**] tab.

The Address Lookup provider used for the ADDR tab can be configured in the Settings > Tool Preferences > Address Lookup Preferences.

## Geofencing

The Geo Fence tool allows users to create a virtual fence that triggers entry/exit notifications if map items of interest cross the virtual boundary lines. The Geo Fence options are added to the existing drawing tools. After a shape has been added, the Geo Fence Tool can be accessed either by selecting the [**Geo Fence**] icon from the menu items or selecting it from the radial.




The Enabled Field slider will move to Tracking by default when a new Geo Fence window is created. Toggle the slider between Tracking and Off to enable/disable the Geo Fence. Use the Trigger field to define which types of Geo Fence breach to monitor. Choose between Entry, Exit or Both. Use the Monitor field to define which entities the Geo Fence will track.

Choose between TAK Users, Friendly, Hostile, Custom or All. Check the [**Specify Elevation**] box to enable the Elevation field, where elevation boundaries for the entities being tracked can be defined. Select the [**OK**] button to finish creating the fence. Select the [**Send**] button to create the fence and send it to another user. Select [**Delete**] to close the Create Geo Fence window and discard changes.

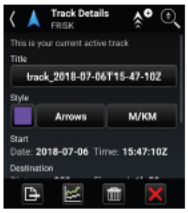
Alerts appear on the map interface. Selecting the [**Alert Notification**] will open the alerts menu, detailing the activity monitored in the user defined region. The default radius for monitoring users (filtered within the "Monitor" field) outside the Geo Fence is set at 75 km. This means the total area monitored begins at the farthest point from the center of the shape plus 75 km. If the user wishes to keep the Geo Fence, but disable tracking, the user can set the tracking [**Enabled**] to off in the Edit Window.

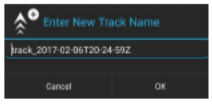
35

Unclassified

## Track History

The device's GPS can be used to track movements with the Track History tool. These tracked paths can be exported to a TAK server, to a route or to a KML, KMZ, GPX or CSV file. A GPS position must be established before tracking can begin.

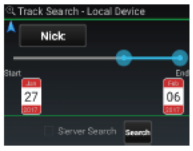


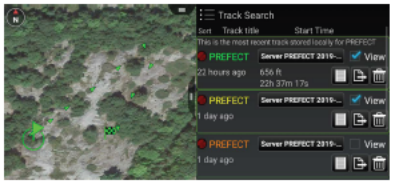

Selecting the [**Track History**] icon will open Track Details for the current active track. The track title, color and style can be modified. Initiate a new track by selecting the [**Add Track**] icon. Accept or edit the default track name and select the [**OK**] button to begin the new track. User location data is recorded as breadcrumbs in a new track file.

## Track Search

Use the Track Search function to view track information that has been previously saved locally or on a TAK Server. The tool searches the track database for matches against the specified time range and by user callsign. Matching tracks are displayed as a list, and can be selected to view on the map interface.




Select the [**Track Search**] icon to access the function. Specify callsign and time frame, check the box for Server Search (if desired), then select [**Search**]. The track list will appear. The query results can be sorted by Track Name or Start Time. Select any of the query results to move to that track. Once selected, the name, color, and style of a selected track can be modified or the track can be cleared. Convert a track to a TAK route or export it as a KML, KMZ, GPX or CSV file by selecting the desired track and then [**Export**]. Enter a file name then select [**Next**] and choose the export format. Select [**Done**] or [**Send**] when the export completes.

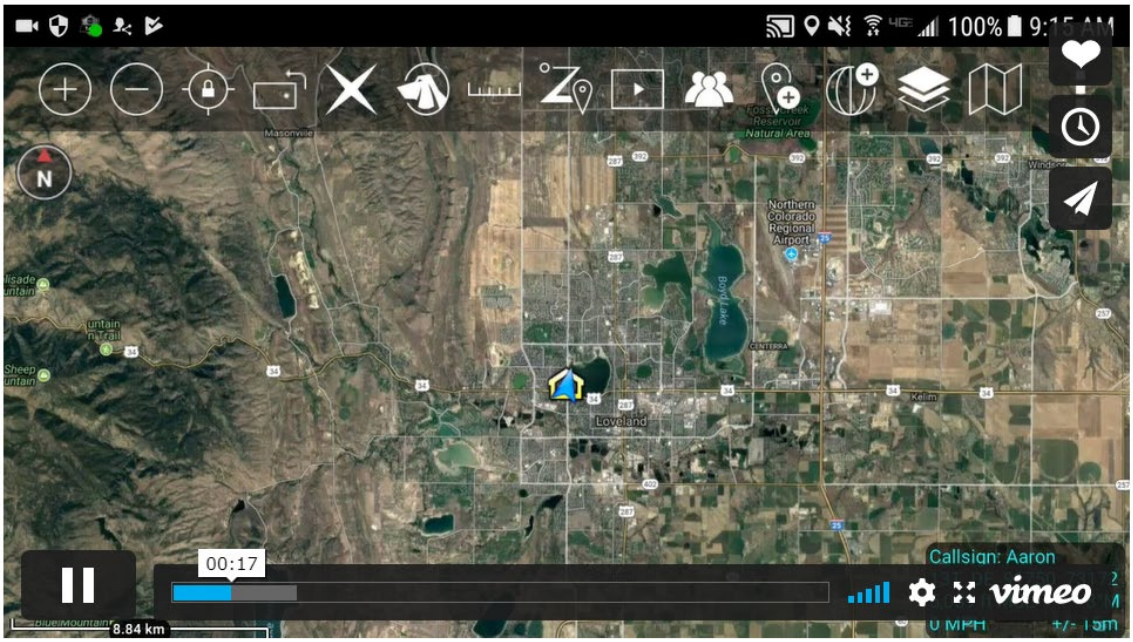


When viewing the track list, the Track History Toolbar will appear at the top of the screen. The options include [**Add a Track**], [**Multi-select**], [**Track Search**], [**Clear Tracks**] and [**Exit**]. The Track History List allows the user to select tracks of other users that have been saved on their device. The Track Search – Local Device allows the user to perform a tailored search for tracks meeting their criteria. The searching option allows the user to retrieve all the tracks on the device.

The Track History Breadcrumb and Settings can be configured in the Settings > Tools Preferences > Track History Preferences.

37 41

[41] https://drive.google.com/file/d/1bo9WHadg3J3o55OLlx1mn3McqEJzvgrK/view




[42]

[42] https://wiki.civtak.org/index.php?title=ATAK_Manual

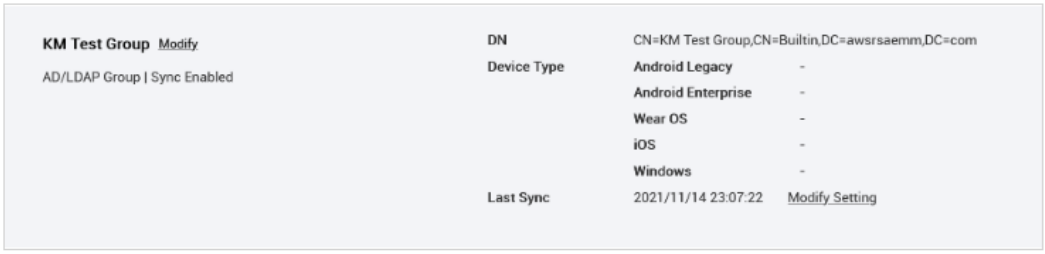
Home / View group details

# View group details

View each group's details by clicking a group name on the group list.

## Summary area

The summary area contains the information about the selected group such as group and user's device types.




- **Modify** — Change the group name.
- **Modify Setting** — Modify the sync settings of the current AD/LDAP group. In the **Modify Sync Setting** window, enter the following information:
  - **AD/LDAP Sync** — Enable or disable sync services.
  - **Sync Group Member** — Select whether sync all users or only the selected users of the group. (**Do Not Sync**, **Sync All**, **Sync Selected Only**)
  - **Profile/App Auto Apply** — Select when to apply a profile or application to a group member automatically. (**When Adding a User**, **When Deleting a User**, **When Deleting a Group**)

## Tab: User (for device groups)

The **User** tab for device groups shows the information of the user's devices and user accounts in the group.

- **Detail** — Move to the **User Details** page for the selected user. For more information on the **User Details** page, see Viewing the user details.

The following function buttons are available:

| Function button | Description |
|---|---|
| Send Email | Send templates or user notifications registered in Knox Manage to users via email. For more information, see Sending templates or user notifications to users via email. |
| Request Enrollment | Send installation guides to the selected users via email and SMS. For more information, see Sending enrollment guides to users via email and SMS.<br>**NOTE** — To send enrollment guides to users via SMS, the mobile numbers of the users must be registered to their accounts. |

# Tab: Device (for device groups)

The **Device** tab for user groups shows the device status and information of the user's devices in the group.

- **Detail** — Move to the **Device Details** page for the selected user's device. For more information on the **Device Details** page, see View details of a device.

The following function buttons are available:

| Function button | Description |
|---|---|
| Refresh | Update the list of devices. |
| Revert Column Settings | Restore the default visibility of all columns. |
| Add | Add a device from the device list to the group. For more information, see Adding devices to device groups. |
| Delete | Delete the selected device from the group. |
| ⚙ | Enable or disable a column in the device list by clicking this button > **Column**, and then selecting a column. |

[43]

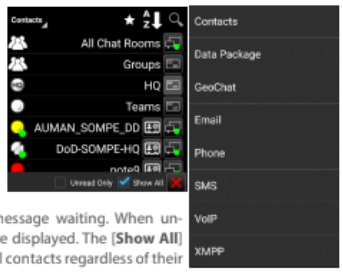
40. The exemplary Accused Products are programmed to form and join groups by transmitting messages.

[43] https://docs.samsungknox.com/admin/knox-manage/view-details-of-group.htm.

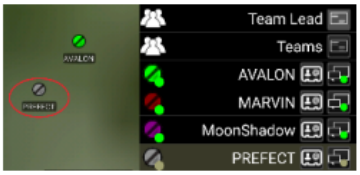
Unclassified

## Contacts

The Contacts list includes a variety of ways in which a user may communicate with other users, such as GeoChat (ATAK Civilian's built in Chat capability), Data Packages, Email, Phone, SMS, VoIP and XMPP.



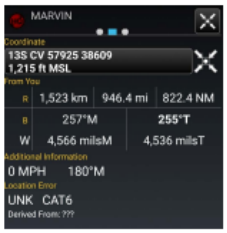

A default communication type (shown in the last column) may be selected and used until another type of communication is selected.




The Contacts list has two filters available at the bottom of the screen. The Unread Only box, when checked, will display only contacts with whom there are unread message waiting. When unchecked (default), all available contacts are displayed. The [**Show All**] box, when checked (default), will display all contacts regardless of their location. When unchecked, only contacts that are visible on current map screen will be displayed.

If a contact is no longer online, it will be indicated by changing the contact listing to a yellow color and the marker changes to gray both in the list and on the map.

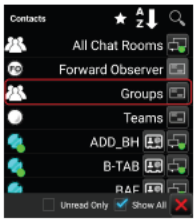
Profile cards are accessed by selecting the second to last column in the Contacts list and are available for each contact. These contain additional information about that contact including: 1) role, software type and version installed, node type, default connector, last reported time, battery life; 2) location information, and 3) available types of communication.



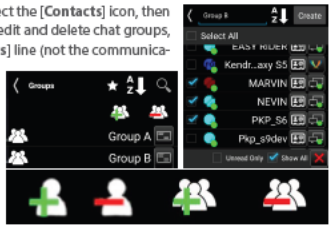
Unclassified

## GeoChat Group Management

Text-based Chat messages may be sent to active network members by using the GeoChat function. To enter GeoChat Group Management, select the [**Contacts**] icon and select [**GeoChat**] from the drop-down menu.

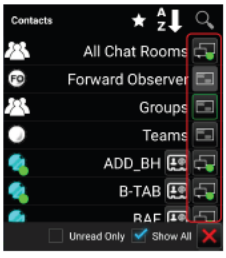



GeoChat Group Management is initiated through Contacts. Select the [**Contacts**] icon, then select GeoChat from the drop-down. The user can now create, edit and delete chat groups, as well as sub-groups. To create a chat group, select the [**Groups**] line (not the communications button). Select the [**Add Group**] icon to create the name of the group and add contacts to the group and then select [**Create**]. If a parent group is being created, no contacts need to be added at this level. To add a nested group, tap the parent group, select the [**Add Group**] icon to create the name of the sub-group and add contacts. Groups may be managed using the options to add/delete contacts or to add/delete GeoChat group.




To add users to a group, select the [**Groups**] line (not the communications button), then select the name of the group to add users. Select the [**Add Users**] icon. A window will open allowing the group creater to add users to the selected group. Select the [**Add**] button when all the users to be added are checked.

## GeoChat Messaging




Group and person-to-person messaging is available. To view messages from or send messages to an individual, tap on the desired contact's [**Communication**] icon. Selecting the [**Pan To**] icon, located at the top right of the call sign in an individual chat, will pan the map interface to that user's location. Select [**All Chat Rooms**] to view all messages from or send messages to those present on the network or TAK Server. Other groupings available for viewing or sending messages are: Forward Observer, Groups, HQ, K9, Medic, RTO, Sniper, Team Lead and Teams. If the user's current role is Forward Observer, HQ, K9, Medic, RTO, Sniper or Team Lead, that user can view or send messages to all other contacts with the same role. If a GeoChat message is sent from the top level of Teams, it will be sent to all contacts, similar to [**All Chat Rooms**].

When a sub-Team is chosen, messages can only be sent to that user's active (My Team) team color. When a parent group is chosen, messages are sent to all members of the parent group, as well as all of the sub-groups. When a sub-group is chosen, messages are sent only to members of the sub-group. Individuals within GeoChat may be removed from the Contacts menu by toggling the visibility of individuals or groups within Overlay Manager.

26

Unclassified

GeoChat Messaging (continued)

Selecting in the Free Text Entry area will open an onscreen keyboard. At the bottom of the Chat area are pre-defined messages that may be used to quickly create a message to send. Tap the current menu button to scroll through the different menus of canned messages, including: DFLT1, DFLT2, ASLT1, ASLT2, RECON1 and RECON2. These pre-defined messages present an easy way to transmit a brief message to other network members concerning position or other important communication. The pre-defined messages may be changed by long pressing on the button and changing its label and corresponding value.

A numbered red dot will appear on the [**Contacts**] icon when a message has been received successfully. The number denotes the number of unread messages that have been received. Select this icon to view the contact list. The user name who sent the message will appear with a numbered red dot next to their name. Alternatively, the text of the message can be read by dragging down from the top to see the Android notifications window. This notification will only stay available for a short time.

44

Home / View group details

# View group details

View each group's details by clicking a group name on the group list.

## Summary area

The summary area contains the information about the selected group such as group and user's device types.

**KM Test Group** Modify

AD/LDAP Group | Sync Enabled

| | | |
|---|---|---|
| DN | CN=KM Test Group,CN=Builtin,DC=awsrsaemm,DC=com | |
| Device Type | Android Legacy | - |
| | Android Enterprise | - |
| | Wear OS | - |
| | iOS | - |
| | Windows | - |
| Last Sync | 2021/11/14 23:07:22 | Modify Setting |

- **Modify** — Change the group name.
- **Modify Setting** — Modify the sync settings of the current AD/LDAP group. In the **Modify Sync Setting** window, enter the following information:
  - **AD/LDAP Sync** — Enable or disable sync services.
  - **Sync Group Member** — Select whether sync all users or only the selected users of the group. (**Do Not Sync**, **Sync All**, **Sync Selected Only**)
  - **Profile/App Auto Apply** — Select when to apply a profile or application to a group member automatically. (**When Adding a User**, **When Deleting a User**, **When Deleting a Group**)

[44] https://drive.google.com/file/d/1bo9WHadg3J3o55OLlx1mn3McqEJzvgrK/view

# Tab: User (for device groups)

The **User** tab for device groups shows the information of the user's devices and user accounts in the group.

- **Detail** — Move to the **User Details** page for the selected user. For more information on the **User Details** page, see Viewing the user details.

The following function buttons are available:

| Function button | Description |
|---|---|
| Send Email | Send templates or user notifications registered in Knox Manage to users via email. For more information, see Sending templates or user notifications to users via email. |
| Request Enrollment | Send installation guides to the selected users via email and SMS. For more information, see Sending enrollment guides to users via email and SMS.<br>**NOTE** — To send enrollment guides to users via SMS, the mobile numbers of the users must be registered to their accounts. |

# Tab: Device (for device groups)

The **Device** tab for user groups shows the device status and information of the user's devices in the group.

- **Detail** — Move to the **Device Details** page for the selected user's device. For more information on the **Device Details** page, see View details of a device.

The following function buttons are available:

| Function button | Description |
|---|---|
| Refresh | Update the list of devices. |
| Revert Column Settings | Restore the default visibility of all columns. |
| Add | Add a device from the device list to the group. For more information, see Adding devices to device groups. |
| Delete | Delete the selected device from the group. |
| ⚙ | Enable or disable a column in the device list by clicking this button > **Column**, and then selecting a column. |

45

[45] https://docs.samsungknox.com/admin/knox-manage/view-details-of-group.htm.

41. The exemplary Accused Products are further programmed to facilitate participation in the groups by communicating with one or more servers and sending to and receiving location information as depicted below.



## Command and control

**Situational awareness**
The Galaxy S20 Tactical Edition integrates voice, video, and tactical data to provide a common operational picture of the battlespace. This complete and accurate real-time intelligence enhances the precision and effectiveness of your tactical teams.

**Tactical user experience**
Unique features found only on the Galaxy S20 Tactical Edition deliver fast and simple access to the information and applications operators need on-mission.

**Better intelligence**
The pro-grade 64 MP camera on the Galaxy S20 Tactical Edition allows you to discretely capture and share crisp high-resolution photo or 8K video intelligence, even in low light without the use of a flash. View and analyze intelligence in greater detail than ever before with the Galaxy S20 Tactical Edition's Dynamic AMOLED 2.0, a 120Hz[1] display.

**Extend your mission**
The Galaxy S20 Tactical Edition battery is 30% larger than the previous tactical solution and it's intelligent.[2] It optimizes your app usage in the field giving you extended power to complete the mission. When you need a recharge, Super Fast Charging[3] and fast Wireless Charging 2.0 give you power in a flash. And Wireless PowerShare allows you to easily charge a team member's phone in the field just by touching the devices.[4]

**Connect to tactical radios** - Protocols to support tactical radios and mission systems, out of the box.

**Tactical app quick launch** - Instantly expand or hide ATAK, APASS and other mission-critical applications at the push of a button.

**Night vision mode** – Turn on and off LED backlight when wearing night vision devices.

**Stealth mode** – Disable LTE and e-911 and mute all RF broadcasting for complete off-grid communications.

**Lock screen auto-rotate** - Unlock the device in landscape mode for easy access when mounted to the operator's chest.

**Auto-touch sensitivity** – Automatically adjust device operations to work with gloved hands.

# One device to meet all your mission requirements.

**Simple device management**
From device configuration, enrollment, customization and management to advanced mobile security controls and updates, Samsung has the mobility cloud services you need for every stage of the Galaxy S20 Tactical Edition lifecycle.[6] With Knox Services, you can keep pace and maintain control over devices and how they're used. You can manage devices in near real-time, configure settings, and remotely lock or wipe devices if lost or stolen, on the battlefield and anywhere else.

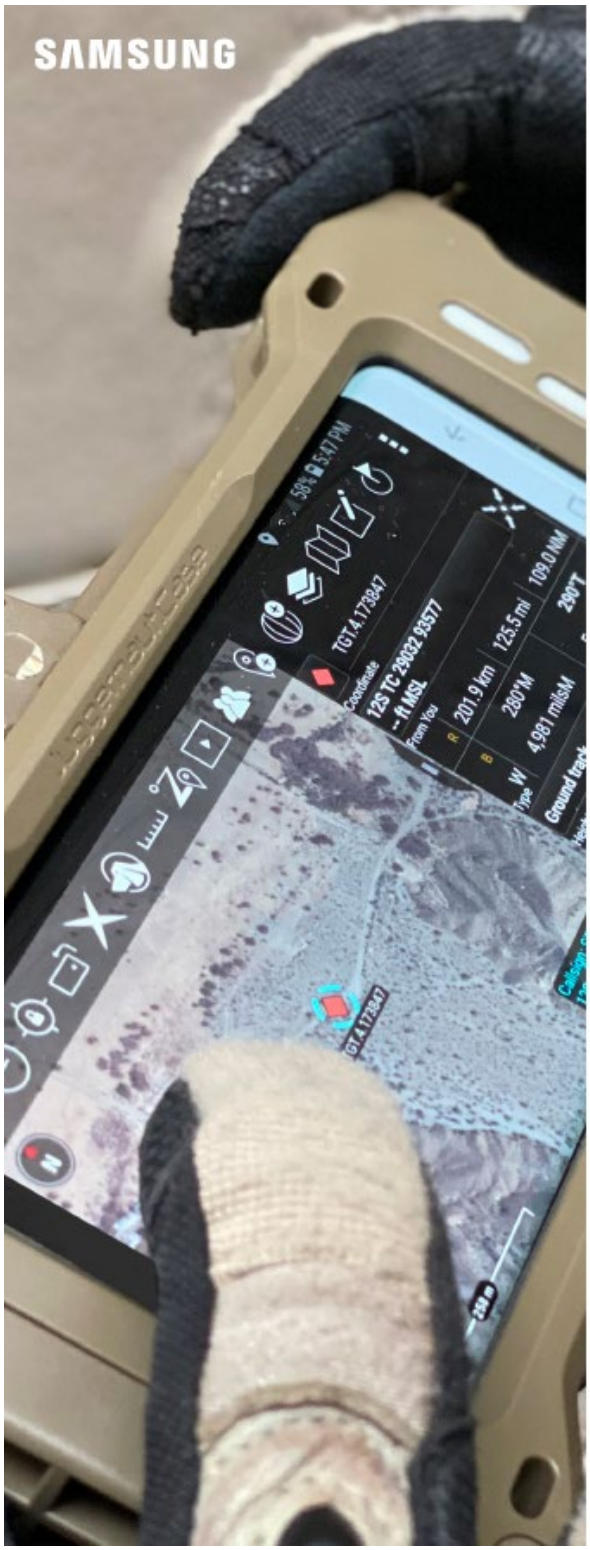
**Run mission apps and enterprise apps**
The Galaxy S20 Tactical Edition has a 64-bit Octa-Core processor with the speed and versatility to run multiple tactical applications in the field and enterprise applications everywhere else.

With Samsung DeX, connect your Galaxy S20 Tactical Edition to a monitor, keyboard and mouse for a desktop-like experience[5] ideally suited for mission planning, training, and everyday use. DeX gives you the power to work seamlessly across Microsoft Office Suite applications,[6] productivity apps, and virtual desktops with secure CAC-authenticated Virtual Desktop Infrastructure (VDI) sessions, all without a laptop.[7] And DeX-in-Vehicle transforms the Galaxy S20 Tactical Edition into a powerful in-vehicle computer.

**Open and secure**
The Galaxy S20 Tactical Edition is built on an open and secure Android operating system enabling seamless integration with a diverse ecosystem of tactical solution partners. Eliminate vulnerabilities with three software updates throughout the life of the device.

46

[46] https://www.pargovernment.com/tactical-sa/docs/S20_brochure.pdf




## Galaxy S20 Tactical Edition

# Mission-ready mobility. Proven by operators.

The Samsung Galaxy S20 Tactical Edition is the mission-ready military smartphone built and proven by operators in special operations. Based on the proven success of the S9 Tactical Edition for operators in the field, the S20 Tactical Edition is the only end user device you'll need for mission planning, training, operations and daily use.

### Persistent communications in any domain

**Purpose-built to connect to tactical radios** and mission systems out of the box, the Galaxy S20 Tactical Edition delivers a complete and accurate common operational picture. Run mission applications in the field and enterprise applications everywhere else with a single end user device for mission training, planning, operations and everyday use.

### Interoperable across devices and networks

**Pre-configured software, pre-loaded during the manufacturing process,** includes drivers to support tactical radios and mission-critical devices. Multi-ethernet capabilities provide dedicated connections to multiple mission systems including drone feeds, laser range finders, and external GPS. Support for current and next-generation networks includes Private SIM, 5G, WiFi 6 and CBRS. Allow or disallow USB peripherals based on product or vendor identifiers.

### Command and control

**Integrate voice, video and tactical data** for a complete view of the battlespace to enhance precision and effectiveness. Unique tactical features on the Galaxy S20 Tactical Edition include night-vision mode, stealth mode, lock screen autorotate, hostage negotiation mode, LTE band lock for consistent 4G connection, tactical application quick launch, to keep the operator focused on the objective, Standalone(5G)/Non-standalone (4G) modes to stay on preferred network. Preloaded tactical settings app. Ability to configure hotspot 2.0.

### Capture Intelligence

**A Pro-grade 64 MP camera** on the Galaxy S20 Tactical Edition enhances intel gathering, even in low-light environments without a flash. Capture high-resolution photos or sharp 8K video reconnaissance without giving away your position.

### Power to extend the mission

**Keep going wherever the mission takes you** with the Galaxy S20 Tactical Edition's intelligent2 4000mAh battery is 30% larger than the previous tactical solution and optimizes energy based on your device usage. Easily share power with a team member's smartphone in the field simply by touching devices using Wireless PowerShare.[4]

### One device to meet your requirements

**Run mission applications in the field** and enterprise applications everywhere else with the powerful and efficient Galaxy S20 Tactical Edition 64-bit Octa-Core processor. Connect your device to a monitor keyboard and mouse and use the power of Samsung DeX[5] for a desktop-like experience that is ideal for mission planning, training and everyday use. DeX-in-Vehicle transforms your Galaxy S20 Tactical Edition into an in-vehicle computer.

### Open and secure

**Enable a diverse ecosystem of tactical partners** with the open and secure Android operating system on the Galaxy S20 Tactical Edition. The all-new Tactical Settings feature simplifies device management, while Samsung Knox provides defense-grade security[6] from the hardware layer up and mission-specific device customization capabilities. The DualDAR architecture of the Galaxy S20 Tactical Edition provides two layers of encryption, even when the device is powered off, for securing up-to top secret level data on the device.

### Tested and proven

Samsung Galaxy Tactical Edition smartphones are tested and proven by special operators in the field. The Galaxy S20 Tactical Edition is certified to meet the most stringent requirements including NSA's CSFC Components List, NIAP Common Criteria/MDFPP, DODIN APL, FIPS 140-2, DISA Android 10 STIG, IP68 rating.

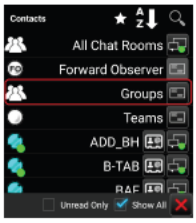
**Contact Us:** www.samsung.com/TacticalEdition

47

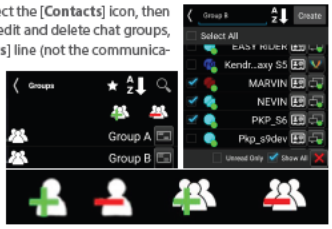
[47] https://image-us.samsung.com/SamsungUS/samsungbusiness/pdfs/flyer/S20_TE-salesflyer_FINAL_July_2021.pdf

## GeoChat Group Management

Text-based Chat messages may be sent to active network members by using the GeoChat function. To enter GeoChat Group Management, select the [**Contacts**] icon and select [**GeoChat**] from the drop-down menu.

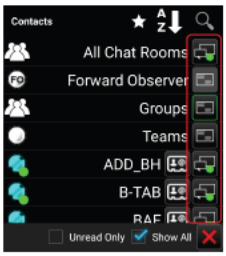



GeoChat Group Management is initiated through Contacts. Select the [**Contacts**] icon, then select GeoChat from the drop-down. The user can now create, edit and delete chat groups, as well as sub-groups. To create a chat group, select the [**Groups**] line (not the communications button). Select the [**Add Group**] icon to create the name of the group and add contacts to the group and then select [**Create**]. If a parent group is being created, no contacts need to be added at this level. To add a nested group, tap the parent group, select the [**Add Group**] icon to create the name of the sub-group and add contacts. Groups may be managed using the options to add/delete contacts or to add/delete GeoChat group.




To add users to a group, select the [**Groups**] line (not the communications button), then select the name of the group to add users. Select the [**Add Users**] icon. A window will open allowing the group creater to add users to the selected group. Select the [**Add**] button when all the users to be added are checked.

## GeoChat Messaging




Group and person-to-person messaging is available. To view messages from or send messages to an individual, tap on the desired contact's [**Communication**] icon. Selecting the [**Pan To**] icon, located at the top right of the call sign in an individual chat, will pan the map interface to that user's location. Select [**All Chat Rooms**] to view all messages from or send messages to those present on the network or TAK Server. Other groupings available for viewing or sending messages are: Forward Observer, Groups, HQ, K9, Medic, RTO, Sniper, Team Lead and Teams. If the user's current role is Forward Observer, HQ, K9, Medic, RTO, Sniper or Team Lead, that user can view or send messages to all other contacts with the same role. If a GeoChat message is sent from the top level of Teams, it will be sent to all contacts, similar to [**All Chat Rooms**].

When a sub-Team is chosen, messages can only be sent to that user's active (My Team) team color. When a parent group is chosen, messages are sent to all members of the parent group, as well as all of the sub-groups. When a sub-group is chosen, messages are sent only to members of the sub-group. Individuals within GeoChat may be removed from the Contacts menu by toggling the visibility of individuals or groups within Overlay Manager.





## GeoChat Messaging (continued)

Selecting in the Free Text Entry area will open an onscreen keyboard. At the bottom of the Chat area are pre-defined messages that may be used to quickly create a message to send. Tap the current menu button to scroll through the different menus of canned messages, including: DFLT1, DFLT2, ASLT1, ASLT2, RECON1 and RECON2. These pre-defined messages present an easy way to transmit a brief message to other network members concerning position or other important communication. The pre-defined messages may be changed by long pressing on the button and changing its label and corresponding value.

A numbered red dot will appear on the [**Contacts**] icon when a message has been received successfully. The number denotes the number of unread messages that have been received. Select this icon to view the contact list. The user name who sent the message will appear with a numbered red dot next to their name. Alternatively, the text of the message can be read by dragging down from the top to see the Android notifications window. This notification will only stay available for a short time.

## Go To

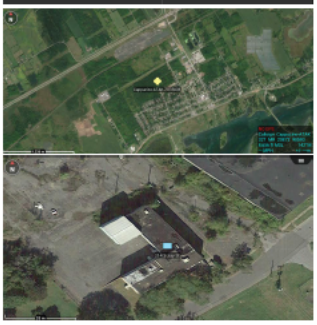
Select the [**Go To**] icon to enter details and navigate to a specific location on the map.

Select from the [**MGRS**] (military grid reference system), [**DD**] (decimal degrees), [**DM**] (degrees- minutes), [**DMS**] (degrees-minutes-seconds), [**UTM**] (Universal Transverse Mercator) or [**ADDR**] tabs on the Go To interface and enter the location data of interest. The address provider name appears beneath the Elevation Data when the user selects the [**ADDR**] tab.

The user can enter the Latitude, Longitude and Elevation in the space provided for [**MGRS**] , [**DD**], [**D-M**] or [**D-M-S**] searches. If DTED is installed, the elevation value can be automatically populated by tapping the [**Pull From DTED**] button.The user can select a desired marker type (Spot, Unknown, Neutral, Red, or Friendly) to be placed at the entered coordinates. If [**No Point**] is selected, the map will pan to the location but will not add a point.

**Note:** The address provider name appears beneath the Elevation Data when the user selects the [**ADDR**] tab.

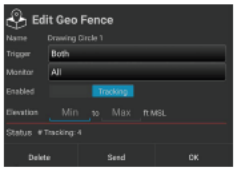
The Address Lookup provider used for the ADDR tab can be configured in the Settings > Tool Preferences > Address Lookup Preferences.



32

## Geofencing

The Geo Fence tool allows users to create a virtual fence that triggers entry/exit notifications if map items of interest cross the virtual boundary lines. The Geo Fence options are added to the existing drawing tools. After a shape has been added, the Geo Fence Tool can be accessed either by selecting the [**Geo Fence**] icon from the menu items or selecting it from the radial.




The Enabled Field slider will move to Tracking by default when a new Geo Fence window is created. Toggle the slider between Tracking and Off to enable/disable the Geo Fence. Use the Trigger field to define which types of Geo Fence breach to monitor. Choose between Entry, Exit or Both. Use the Monitor field to define which entities the Geo Fence will track.

Choose between TAK Users, Friendly, Hostile, Custom or All. Check the [**Specify Elevation**] box to enable the Elevation field, where elevation boundaries for the entities being tracked can be defined. Select the [**OK**] button to finish creating the fence. Select the [**Send**] button to create the fence and send it to another user. Select [**Delete**] to close the Create Geo Fence window and discard changes.

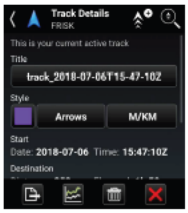
Alerts appear on the map interface. Selecting the [**Alert Notification**] will open the alerts menu, detailing the activity monitored in the user defined region. The default radius for monitoring users (filtered within the "Monitor" field) outside the Geo Fence is set at 75 km. This means the total area monitored begins at the farthest point from the center of the shape plus 75 km. If the user wishes to keep the Geo Fence, but disable tracking, the user can set the tracking [**Enabled**] to off in the Edit Window.

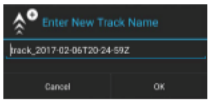
35

Unclassified

## Track History

The device's GPS can be used to track movements with the Track History tool. These tracked paths can be exported to a TAK server, to a route or to a KML, KMZ, GPX or CSV file. A GPS position must be established before tracking can begin.

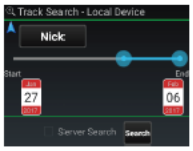


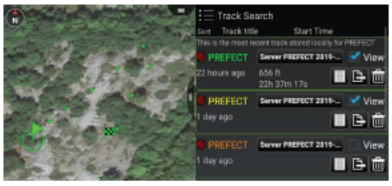

Selecting the [**Track History**] icon will open Track Details for the current active track. The track title, color and style can be modified. Initiate a new track by selecting the [**Add Track**] icon. Accept or edit the default track name and select the [**OK**] button to begin the new track. User location data is recorded as breadcrumbs in a new track file.

## Track Search

Use the Track Search function to view track information that has been previously saved locally or on a TAK Server. The tool searches the track database for matches against the specified time range and by user callsign. Matching tracks are displayed as a list, and can be selected to view on the map interface.




Select the [**Track Search**] icon to access the function. Specify callsign and time frame, check the box for Server Search (if desired), then select [**Search**]. The track list will appear. The query results can be sorted by Track Name or Start Time. Select any of the query results to move to that track. Once selected, the name, color, and style of a selected track can be modified or the track can be cleared. Convert a track to a TAK route or export it as a KML, KMZ, GPX or CSV file by selecting the desired track and then [**Export**]. Enter a file name then select [**Next**] and choose the export format. Select [**Done**] or [**Send**] when the export completes.



When viewing the track list, the Track History Toolbar will appear at the top of the screen. The options include [**Add a Track**], [**Multi-select**], [**Track Search**], [**Clear Tracks**] and [**Exit**]. The Track History List allows the user to select tracks of other users that have been saved on their device. The Track Search – Local Device allows the user to perform a tailored search for tracks meeting their criteria. The searching option allows the user to retrieve all the tracks on the device.

The Track History Breadcrumb and Settings can be configured in the Settings > Tools Preferences > Track History Preferences.

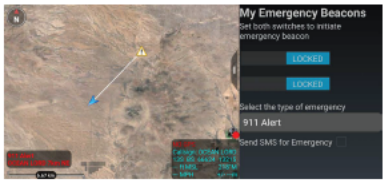
37

Unclassified

## Emergency Beacon

Select the [**Emergency Beacon**] icon to open the Emergency Beacon Tool.

The Emergency Beacon allows the user to indicate their need for assistance, the type of emergency and their location on the map. The type of emergency can be selected from the drop-down menu, before activation, and includes options for an Alert, Ring the Bell, Geo Fence Breached or In Contact.




Once the Emergency type has been selected and both switches have been enabled, the TAK Server broadcasts the announcements to all network contacts. Even if the user's device is turned off, the beacon will continue. Only when the user returns to the Emergency Beacon tool and turns off the switches will the beacon be canceled and removed. If the SMS for Emergency option has been configured, the alert will be sent via text message to the configured numbers.

48

[48] https://drive.google.com/file/d/1bo9WHadg3J3o55OLlx1mn3McqEJzvgrK/view

# Check the locations of devices

You can check the locations of the selected devices. Only the devices that have the location policy applied can be tracked.

> **NOTE** — You can only check a device's location if location data was collected at least once.

**IMPORTANT** — In order to track the location of Android 11 and 12 devices, the device user must grant the KM agent location access. This affects devices with the following deployment types:

- Employee-owned devices with a Work Profile
- Shared devices with a secondary account

You should inform users with these devices to allow the following access settings:

- Android 11:
  1. When the KM agent requests location access, the user must select **While using this app**.
  2. Then, they must go to **Work profile settings** >**Apps** >**Knox Manage** >**App permissions**, and set **Location** to **Allow all the time**.
- Android 12 and higher:
  - When the KM agent requests location access, the user must select **Precise** and **While using this app**.

1. Navigate to **Device**.
2. On the **Device** page, select one or more devices, and then click **Check Location**.
3. On the **Check Location** page, search by date. The view shows an interactive map of the devices and their location history.

On this page, you can inspect individual device information, as well as export their location history as as a GPX file.

# Device map

On the **Check Location** screen, a map displays the latest locations of all tracked devices. The map uses the following legend:

| Element | Meaning |
|---|---|
| | Active device |
| | Device with expired keepalive |
| | Cluster of 1–9 devices |
| | Cluster of 10–99 devices |
| | Cluster of 100–999 devices |
| | Cluster of 1000–9999 devices |

You can view an individual device's status by hovering over its pin . On hover, a tooltip lists the following information:

- Device name
- IMEI/MEID
- Serial Number
- Mobile Number
- User Name
- Last Location Scanned
- Organization Name
- Group Name
- Tag
- Platform & Management Type
- Model Name
- MAC Address
- Manufacturer

[49]

[49] https://docs.samsungknox.com/admin/knox-manage/check-the-locations-of-devices.htm.

42. This location information is presented on interactive displays on the exemplary Accused Products which include interactive maps and a plurality of user selectable symbols corresponding to other devices. These symbols are positioned on the map at positions corresponding to the locations of the other devices, as depicted below.

# One device to meet all your mission requirements.

**Run mission apps and enterprise apps**
The Galaxy S20 Tactical Edition has a 64-bit Octa-Core processor with the speed and versatility to run multiple tactical applications in the field and enterprise applications everywhere else.

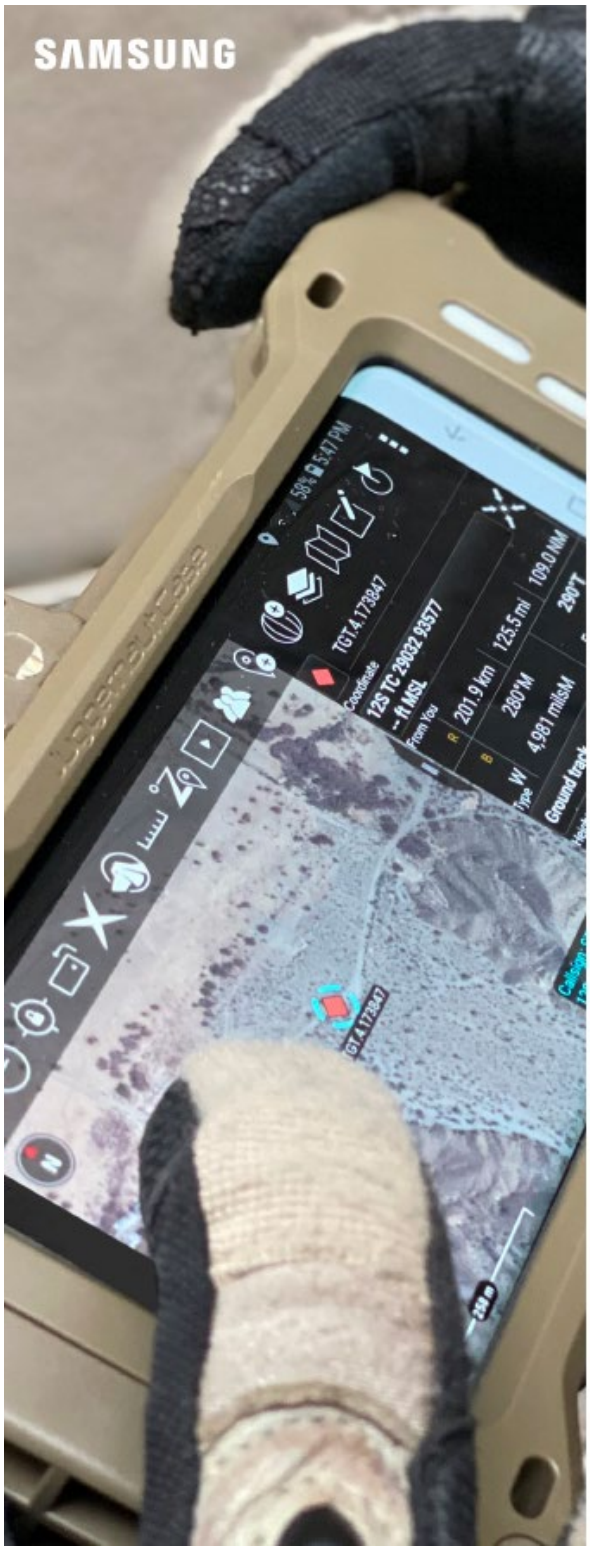
With Samsung DeX, connect your Galaxy S20 Tactical Edition to a monitor, keyboard and mouse for a desktop-like experience[5] ideally suited for mission planning, training, and everyday use. DeX gives you the power to work seamlessly across Microsoft Office Suite applications,[6] productivity apps, and virtual desktops with secure CAC-authenticated Virtual Desktop Infrastructure (VDI) sessions, all without a laptop.[7] And DeX-in-Vehicle transforms the Galaxy S20 Tactical Edition into a powerful in-vehicle computer.

**Simple device management**
From device configuration, enrollment, customization and management to advanced mobile security controls and updates, Samsung has the mobility cloud services you need for every stage of the Galaxy S20 Tactical Edition lifecycle.[8] With Knox Services, you can keep pace and maintain control over devices and how they're used. You can manage devices in near real-time, configure settings, and remotely lock or wipe devices if lost or stolen, on the battlefield and anywhere else.

**Open and secure**
The Galaxy S20 Tactical Edition is built on an open and secure Android operating system enabling seamless integration with a diverse ecosystem of tactical solution partners. Eliminate vulnerabilities with three software updates throughout the life of the device.

50

[50] https://www.pargovernment.com/tactical-sa/docs/S20_brochure.pdf




## Galaxy S20 Tactical Edition

# Mission-ready mobility. Proven by operators.

The Samsung Galaxy S20 Tactical Edition is the mission-ready military smartphone built and proven by operators in special operations. Based on the proven success of the S9 Tactical Edition for operators in the field, the S20 Tactical Edition is the only end user device you'll need for mission planning, training, operations and daily use.

### Persistent communications in any domain

**Purpose-built to connect to tactical radios** and mission systems out of the box, the Galaxy S20 Tactical Edition delivers a complete and accurate common operational picture. Run mission applications in the field and enterprise applications everywhere else with a single end user device for mission training, planning, operations and everyday use.

### Interoperable across devices and networks

**Pre-configured software, pre-loaded during the manufacturing process,** includes drivers to support tactical radios and mission-critical devices. Multi-ethernet capabilities provide dedicated connections to multiple mission systems including drone feeds, laser range finders, and external GPS. Support for current and next-generation networks includes Private SIM, 5G, WiFi 6 and CBRS. Allow or disallow USB peripherals based on product or vendor identifiers.

### Command and control

**Integrate voice, video and tactical data** for a complete view of the battlespace to enhance precision and effectiveness. Unique tactical features on the Galaxy S20 Tactical Edition include night-vision mode, stealth mode, lock screen autorotate, hostage negotiation mode, LTE band lock for consistent 4G connection, tactical application quick launch, to keep the operator focused on the objective, Standalone(5G)/Non-standalone (4G) modes to stay on preferred network. Preloaded tactical settings app. Ability to configure hotspot 2.0.

### Capture Intelligence

**A Pro-grade 64 MP camera** on the Galaxy S20 Tactical Edition enhances intel gathering, even in low-light environments without a flash. Capture high-resolution photos or sharp 8K video reconnaissance without giving away your position.

### Power to extend the mission

**Keep going wherever the mission takes you** with the Galaxy S20 Tactical Edition's intelligent2 4000mAh battery is 30% larger than the previous tactical solution and optimizes energy based on your device usage. Easily share power with a team member's smartphone in the field simply by touching devices using Wireless PowerShare.[4]

### One device to meet your requirements

**Run mission applications in the field** and enterprise applications everywhere else with the powerful and efficient Galaxy S20 Tactical Edition 64-bit Octa-Core processor. Connect your device to a monitor keyboard and mouse and use the power of Samsung DeX[5] for a desktop-like experience that is ideal for mission planning, training and everyday use. DeX-in-Vehicle transforms your Galaxy S20 Tactical Edition into an in-vehicle computer.

### Open and secure

**Enable a diverse ecosystem of tactical partners** with the open and secure Android operating system on the Galaxy S20 Tactical Edition. The all-new Tactical Settings feature simplifies device management, while Samsung Knox provides defense-grade security[6] from the hardware layer up and mission-specific device customization capabilities. The DualDAR architecture of the Galaxy S20 Tactical Edition provides two layers of encryption, even when the device is powered off, for securing up-to top secret level data on the device.

### Tested and proven

Samsung Galaxy Tactical Edition smartphones are tested and proven by special operators in the field. The Galaxy S20 Tactical Edition is certified to meet the most stringent requirements including NSA's CSFC Components List, NIAP Common Criteria/MDFPP, DODIN APL, FIPS 140-2, DISA Android 10 STIG, IP68 rating.

**Contact Us:** www.samsung.com/TacticalEdition

51

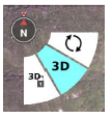
[51] https://image-us.samsung.com/SamsungUS/samsungbusiness/pdfs/flyer/S20_TE-salesflyer_FINAL_July_2021.pdf

## ATAK Civilian Overview

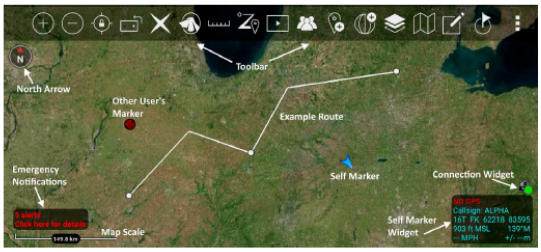
The Civilian Team Awareness Kit for Android (ATAK Civilian) is a Government-off-the-Shelf (GOTS) software application and mapping framework for mobile devices. ATAK Civilian has been designed and developed to run on Android smart devices used in a first responder environment. The ATAK Civilian software application is an extensible moving map display that integrates imagery, map and overlay information to provide enhanced collaboration and Situational Awareness (SA) over a tactical meshed network. ATAK Civilian promotes information flow and communications from the field environment to command enterprise locations.

The first time ATAK Civilian is opened, or after a Clear Content, a passphrase is auto-generated to activate data encryption. The user can supply their own passphrase by using Settings > Show All Preferences > Device Preferences > Change Encryption Passphrase. Following this step, ATAK Civilian's End User License Agreement (EULA) must be accepted. Next, the user will be prompted to change their callsign and/or import preferences or data from a Mission Package. All changes/imports can always be updated later. Finally, the user can place their self-marker by following the instructions located in the lower right corner.

The toolbar runs along the top of the map display. The features whose icons form the center portion of the toolbar are discussed in individual sections of this guide. The three dots at the right of the toolbar provide additional menu items that appear in a drop-down menu. A Long Press on the map will toggle the toolbar between hidden and visible.




The North Arrow appears in the upper left and is used to control map orientation. It has two primary modes: North Up/Track Up (default) and Manual Map Rotation/Lock. While in North Up/Track Up Mode, single press on the [**North Arrow**] icon to cycle between the North Up and Track Up map orientation. Long press the [**North Arrow**] to call out the additional controls menu where the Manual Rotation/Lock and 3D features are available. Select the [**Rotation**] button to enter Manual Map Rotation/Lock Mode. When in Manual Map Rotation/Lock Mode, rotate the map orientation by pressing on the map with two fingers and pivoting them in the desired direction. Single press on the [**North Arrow**] to lock the screen orientation, signified by the appearance of the lock icon, and again to unlock the orientation for further adjustment. 3D controls are discussed in a separate section.




Select the [**Magnifier**] buttons to zoom in or out on the map. The map can also be zoomed by using two fingers on the screen to pinch and spread the map. Select the [**Back**] button to center the screen on the Self Marker or the [**Padlock**] icon to lock the center of the screen to the Self Marker. Select the [**Orientation**] icon to toggle the screen position between portrait and landscape.

The optional connection widget indicates whether or not the user is connected to a TAK Server. This has a corresponding Android notification that provides the same information. Toggle this display on at Settings > Network Connections > Network Connections > Display Connection Widget.

Alerts and notifications are displayed in the lower left of the map interface.

The Map Scale displays a 1 inch to X mi/km reference on the map. The scale adjusts with the map when zoomed in and out. Hint windows are available to alert users to changes or make suggestions about the use of tools the first time they are opened.

## Go To

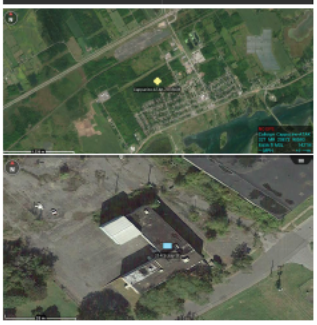
Select the [**Go To**] icon to enter details and navigate to a specific location on the map.

Select from the [**MGRS**] (military grid reference system), [**DD**] (decimal degrees), [**DM**] (degrees- minutes), [**DMS**] (degrees-minutes-seconds), [**UTM**] (Universal Transverse Mercator) or [**ADDR**] tabs on the Go To interface and enter the location data of interest. The address provider name appears beneath the Elevation Data when the user selects the [**ADDR**] tab.

The user can enter the Latitude, Longitude and Elevation in the space provided for [**MGRS**] , [**DD**], [**D-M**] or [**D-M-S**] searches. If DTED is installed, the elevation value can be automatically populated by tapping the [**Pull From DTED**] button.The user can select a desired marker type (Spot, Unknown, Neutral, Red, or Friendly) to be placed at the entered coordinates. If [**No Point**] is selected, the map will pan to the location but will not add a point.

**Note:** The address provider name appears beneath the Elevation Data when the user selects the [**ADDR**] tab.

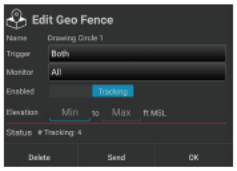
The Address Lookup provider used for the ADDR tab can be configured in the Settings > Tool Preferences > Address Lookup Preferences.





## Geofencing

The Geo Fence tool allows users to create a virtual fence that triggers entry/exit notifications if map items of interest cross the virtual boundary lines. The Geo Fence options are added to the existing drawing tools. After a shape has been added, the Geo Fence Tool can be accessed either by selecting the [**Geo Fence**] icon from the menu items or selecting it from the radial.




The Enabled Field slider will move to Tracking by default when a new Geo Fence window is created. Toggle the slider between Tracking and Off to enable/disable the Geo Fence. Use the Trigger field to define which types of Geo Fence breach to monitor. Choose between Entry, Exit or Both. Use the Monitor field to define which entities the Geo Fence will track.

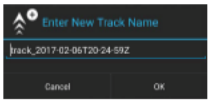
Choose between TAK Users, Friendly, Hostile, Custom or All. Check the [**Specify Elevation**] box to enable the Elevation field, where elevation boundaries for the entities being tracked can be defined. Select the [**OK**] button to finish creating the fence. Select the [**Send**] button to create the fence and send it to another user. Select [**Delete**] to close the Create Geo Fence window and discard changes.

Alerts appear on the map interface. Selecting the [**Alert Notification**] will open the alerts menu, detailing the activity monitored in the user defined region. The default radius for monitoring users (filtered within the "Monitor" field) outside the Geo Fence is set at 75 km. This means the total area monitored begins at the farthest point from the center of the shape plus 75 km. If the user wishes to keep the Geo Fence, but disable tracking, the user can set the tracking [**Enabled**] to off in the Edit Window.

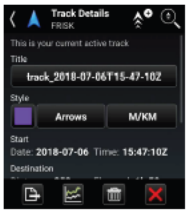
Unclassified

## Track History

The device's GPS can be used to track movements with the Track History tool. These tracked paths can be exported to a TAK server, to a route or to a KML, KMZ, GPX or CSV file. A GPS position must be established before tracking can begin.

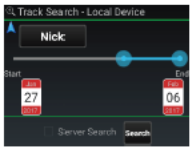



Selecting the [**Track History**] icon will open Track Details for the current active track. The track title, color and style can be modified. Initiate a new track by selecting the [**Add Track**] icon. Accept or edit the default track name and select the [**OK**] button to begin the new track. User location data is recorded as breadcrumbs in a new track file.

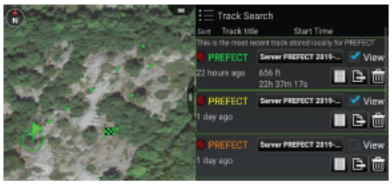



## Track Search

Use the Track Search function to view track information that has been previously saved locally or on a TAK Server. The tool searches the track database for matches against the specified time range and by user callsign. Matching tracks are displayed as a list, and can be selected to view on the map interface.




Select the [**Track Search**] icon to access the function. Specify callsign and time frame, check the box for Server Search (if desired), then select [**Search**]. The track list will appear. The query results can be sorted by Track Name or Start Time. Select any of the query results to move to that track. Once selected, the name, color, and style of a selected track can be modified or the track can be cleared. Convert a track to a TAK route or export it as a KML, KMZ, GPX or CSV file by selecting the desired track and then [**Export**]. Enter a file name then select [**Next**] and choose the export format. Select [**Done**] or [**Send**] when the export completes.



When viewing the track list, the Track History Toolbar will appear at the top of the screen. The options include [**Add a Track**], [**Multi-select**], [**Track Search**], [**Clear Tracks**] and [**Exit**]. The Track History List allows the user to select tracks of other users that have been saved on their device. The Track Search – Local Device allows the user to perform a tailored search for tracks meeting their criteria. The searching option allows the user to retrieve all the tracks on the device.

The Track History Breadcrumb and Settings can be configured in the Settings > Tools Preferences > Track History Preferences.

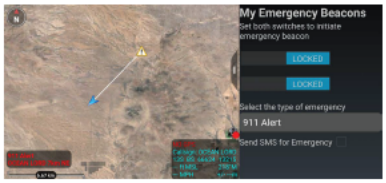
37

Unclassified

## Emergency Beacon

Select the [**Emergency Beacon**] icon to open the Emergency Beacon Tool.

The Emergency Beacon allows the user to indicate their need for assistance, the type of emergency and their location on the map. The type of emergency can be selected from the drop-down menu, before activation, and includes options for an Alert, Ring the Bell, Geo Fence Breached or In Contact.




Once the Emergency type has been selected and both switches have been enabled, the TAK Server broadcasts the announcements to all network contacts. Even if the user's device is turned off, the beacon will continue. Only when the user returns to the Emergency Beacon tool and turns off the switches will the beacon be canceled and removed. If the SMS for Emergency option has been configured, the alert will be sent via text message to the configured numbers.

52

[52] https://drive.google.com/file/d/1bo9WHadg3J3o55OLlx1mn3McqEJzvgrK/view

# Check the locations of devices

You can check the locations of the selected devices. Only the devices that have the location policy applied can be tracked.

> **NOTE** — You can only check a device's location if location data was collected at least once.

**IMPORTANT** — In order to track the location of Android 11 and 12 devices, the device user must grant the KM agent location access. This affects devices with the following deployment types:

- Employee-owned devices with a Work Profile
- Shared devices with a secondary account

You should inform users with these devices to allow the following access settings:

- Android 11:
  1. When the KM agent requests location access, the user must select **While using this app**.
  2. Then, they must go to **Work profile settings** >**Apps** >**Knox Manage** >**App permissions**, and set **Location** to **Allow all the time**.
- Android 12 and higher:
  - When the KM agent requests location access, the user must select **Precise** and **While using this app**.

1. Navigate to **Device**.
2. On the **Device** page, select one or more devices, and then click **Check Location**.
3. On the **Check Location** page, search by date. The view shows an interactive map of the devices and their location history.

On this page, you can inspect individual device information, as well as export their location history as as a GPX file.

# Device map

On the **Check Location** screen, a map displays the latest locations of all tracked devices. The map uses the following legend:

| Element | Meaning |
|---|---|
| | Active device |
| | Device with expired keepalive |
| | Cluster of 1–9 devices |
| | Cluster of 10–99 devices |
| | Cluster of 100–999 devices |
| | Cluster of 1000–9999 devices |

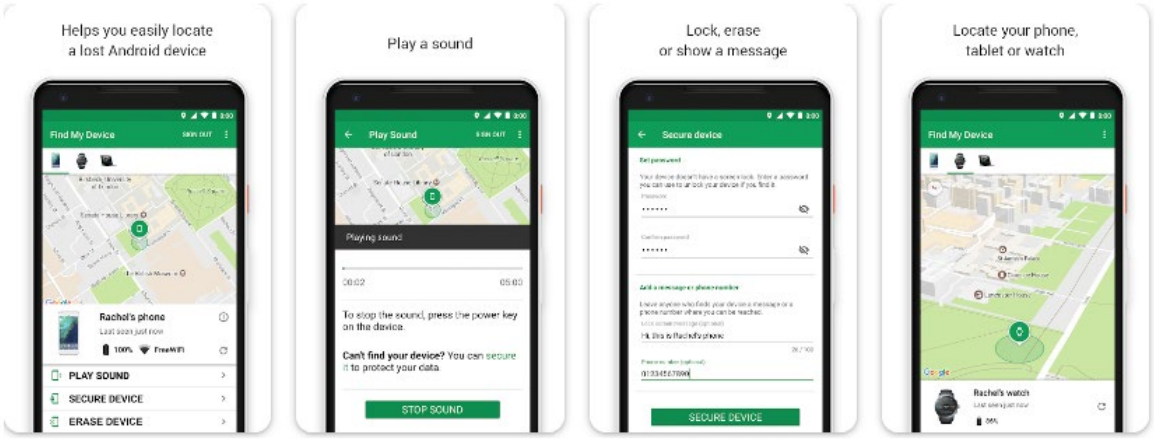
You can view an individual device's status by hovering over its pin . On hover, a tooltip lists the following information:

- Device name
- IMEI/MEID
- Serial Number
- Mobile Number
- User Name
- Last Location Scanned
- Organization Name
- Group Name
- Tag
- Platform & Management Type
- Model Name
- MAC Address
- Manufacturer

[53]

[53] https://docs.samsungknox.com/admin/knox-manage/check-the-locations-of-devices.htm.

43. For example, Defendants' Accused Products include Find My Device which allows devices to share their locations and view other devices' locations on a map and to communicate with those devices via Find My Device (as shown below):

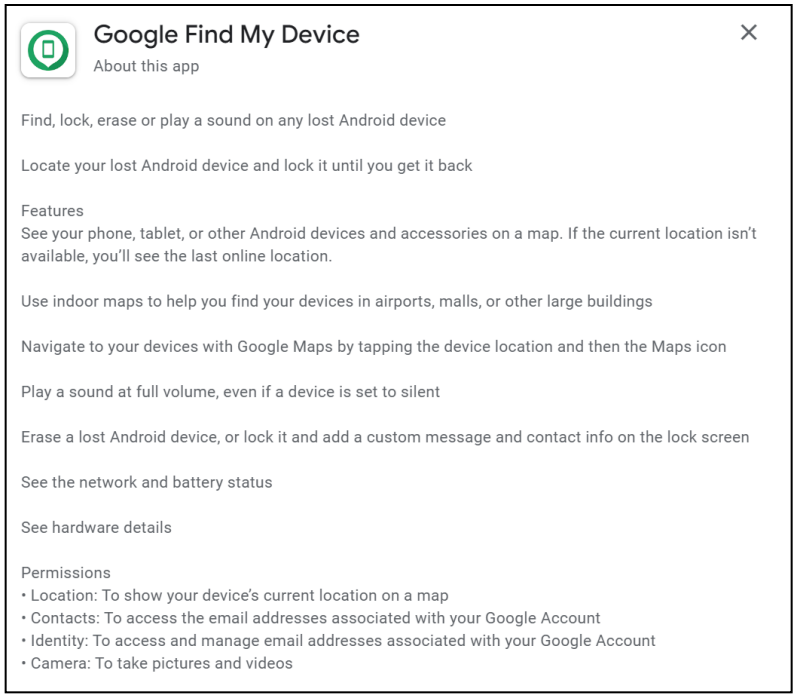



54

44. Additionally, the exemplary Accused Products allow devices and users to establish groups and to exchange messages via interaction with Samsung's servers which provide services related to the operation of Find My Device, among other relevant services. The exemplary Accused Products further allow users to retrieve map information from multiple sources.

45. The exemplary Accused Products are programmed to form and join groups by transmitting messages:

54 https://play.google.com/store/apps/details?id=com.google.android.apps.adm&hl=en_US&gl=US ; see also https://www.att.com/device-support/article/wireless/KM1474177/Samsung/SamsungSMA536U



Google Find My Device

About this app

Find, lock, erase or play a sound on any lost Android device

Locate your lost Android device and lock it until you get it back

Features
See your phone, tablet, or other Android devices and accessories on a map. If the current location isn't available, you'll see the last online location.

Use indoor maps to help you find your devices in airports, malls, or other large buildings

Navigate to your devices with Google Maps by tapping the device location and then the Maps icon

Play a sound at full volume, even if a device is set to silent

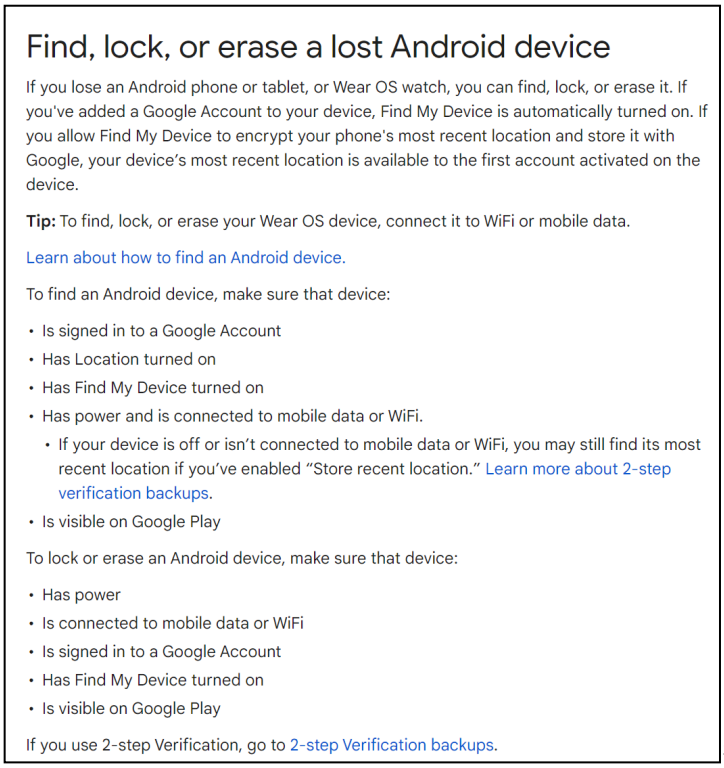
Erase a lost Android device, or lock it and add a custom message and contact info on the lock screen

See the network and battery status

See hardware details

Permissions
• Location: To show your device's current location on a map
• Contacts: To access the email addresses associated with your Google Account
• Identity: To access and manage email addresses associated with your Google Account
• Camera: To take pictures and videos

[55]



## Find, lock, or erase a lost Android device

If you lose an Android phone or tablet, or Wear OS watch, you can find, lock, or erase it. If you've added a Google Account to your device, Find My Device is automatically turned on. If you allow Find My Device to encrypt your phone's most recent location and store it with Google, your device's most recent location is available to the first account activated on the device.

**Tip:** To find, lock, or erase your Wear OS device, connect it to WiFi or mobile data.

Learn about how to find an Android device.

To find an Android device, make sure that device:

- Is signed in to a Google Account
- Has Location turned on
- Has Find My Device turned on
- Has power and is connected to mobile data or WiFi.
  - If your device is off or isn't connected to mobile data or WiFi, you may still find its most recent location if you've enabled "Store recent location." Learn more about 2-step verification backups.
- Is visible on Google Play

To lock or erase an Android device, make sure that device:

- Has power
- Is connected to mobile data or WiFi
- Is signed in to a Google Account
- Has Find My Device turned on
- Is visible on Google Play

If you use 2-step Verification, go to 2-step Verification backups.

[56]

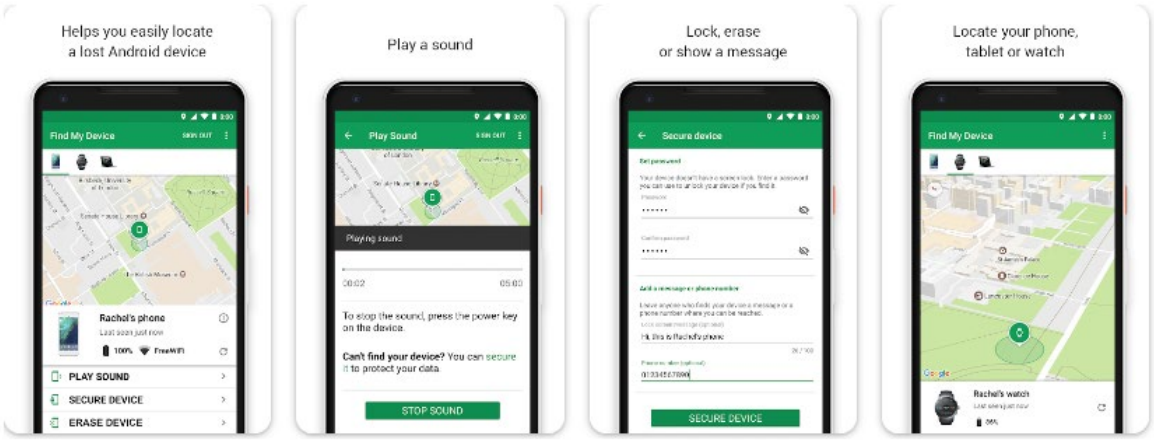
[55] *Id.*

[56] https://support.google.com/android/answer/6160491; see also https://www.att.com/device-support/article/wireless/KM1474177/Samsung/SamsungSMA536U

> **Find, lock, or erase a device remotely**
>
> **Important:** If you find your device after you erase it, to use your device again, you need your Google Account password. Learn about device protection.
>
> 1. On a browser, go to android.com/find.
> 2. Sign in to your Google Account.
>    - **If you have more than one device:** At the top of the sidebar, select the lost device.
>    - **If your lost device has more than one user profile:** Sign in with a Google Account that's on the main or personal profile. Learn about user profiles.
> 3. The lost device gets a notification.
> 4. On the map, you'll get info about where the device is.
>    - The location is approximate and may not be accurate.
>    - If your device can't be found, you may find its last known location, if available.
> 5. If you get a prompt, tap **Enable lock & erase**.
> 6. Select what you want to do:
>    - **Play sound:** Rings your device at full volume for 5 minutes, even if it's set to silent or vibrate.
>    - **Secure device:** Locks your device with your PIN or password. If you don't have a lock, you can set one. To help someone return your device to you, you can add a message or device number to the lock screen.
>    - **Erase device:** Permanently deletes all data on your device, but may not delete SD cards. After you erase, Find My Device won't work on the device.

[57]

46. The exemplary Accused Products are further programmed to facilitate participation in the groups by communicating with one or more servers and sending to and receiving location information as depicted below:

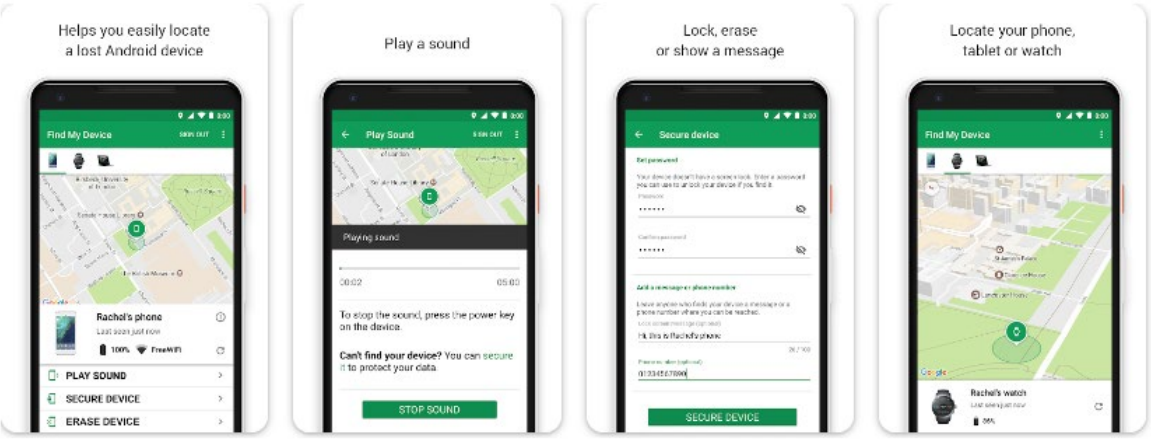



[58]

[57] *Id.*

[58] https://play.google.com/store/apps/details?id=com.google.android.apps.adm&hl=en_US&gl=US

47. This location information is presented on interactive displays on the exemplary Accused Products which include interactive maps and a plurality of user-selectable symbols corresponding to other devices. These symbols are positioned on the map at positions corresponding to the locations of the other devices as depicted below:




59

48. The exemplary Accused Products are further programmed to permit users to request and display additional maps from additional servers by, for example, moving the map screen and/or by selecting satellite images or other types of maps. The exemplary Accused Products are further programmed to permit interaction with the display where a user may select one or more symbols and where the exemplary Accused Products further permit data to be sent to other devices based on that interaction.

49. AGIS Software has suffered damages as a result of Defendants' direct and indirect infringement of the '838 Patent in an amount to be proved at trial.

59 https://play.google.com/store/apps/details?id=com.google.android.apps.adm&hl=en_US&gl=US ; see also https://www.att.com/device-support/article/wireless/KM1474177/Samsung/SamsungSMA536U

50. AGIS Software has suffered, and will continue to suffer, irreparable harm as a result of Defendants' infringement of the '838 Patent for which there is no adequate remedy at law unless Defendants' infringement is enjoined by this Court.

51. Defendants have committed and continue to commit acts of infringement that Defendants actually knew or should have known constituted an unjustifiably high risk of infringement of at least one valid and enforceable claim of the '838 Patent. Defendants' infringement of the '838 Patent has been and continues to be willful, entitling AGIS Software to an award of treble damages, reasonable attorney fees, and costs in bringing this action.

## COUNT III
**(Infringement of the '829 Patent)**

52. Paragraphs 1 through 19 are incorporated herein by reference as if fully set forth in their entireties.

53. AGIS Software has not licensed or otherwise authorized Defendants to make, use, offer for sale, sell, or import any products that embody the inventions of the '829 Patent.

54. Defendants have and continue to directly infringe at least claim 34 of the '829 Patent, either literally or under the doctrine of equivalents, by making, using, selling, offering for sale, distributing, exporting from, and/or importing into the United States the Accused Products without authority and in violation of 35 U.S.C. § 271(a).

55. Defendants have and continue to indirectly infringe at least claim 34 of the '829 Patent by actively, knowingly, and intentionally inducing others to directly infringe, either literally or under the doctrine of equivalents, by making, using, selling, offering for sale, distributing, exporting from, and/or importing into the United States the infringing Accused Products and by instructing users of the Accused Products to perform at least the method of claim 34 in the '829 Patent. For example, Defendants, with knowledge that the Accused Products infringe the '829

Patent at least as of the date of this Complaint, actively, knowingly, and intentionally induced, and continue to actively, knowingly, and intentionally induce, direct infringement of at least claim 34 of the '839 Patent in violation of 35 U.S.C. § 271(b).

56. For example, Defendants have indirectly infringed and continue to indirectly infringe at least claim 34 of the '829 Patent in the United States because Defendants' customers use such Accused Products, including at least the Samsung Tactical, TAK, and ATAK applications and/or services and Samsung Knox applications and/or services installed on the Accused Products, in accordance with Defendants' instructions and thereby directly infringe at least claim 34 of the '829 Patent in violation of 35 U.S.C. § 271. Defendants directly and/or indirectly intentionally instruct their customers to infringe through training videos, demonstrations, brochures, installations and/or user guides, such as those located at one or more of the following: https://www.samsung.com/us/business/solutions/industries/government/tactical-edition/#COMMAND_AND_CONTROL; https://www.samsung.com/us/business/solutions/services/mobility-software/e-fota/; https://image-us.samsung.com/SamsungUS/samsungbusiness/pdfs/brochures/S20_TE-tactical-brochure-FINAL_July_2021.pdf; https://insights.samsung.com/2021/09/01/atak-enhances-collaboration-and-awareness-for-public-safety-2/; https://www.civtak.org/atak-about/; https://www.civtak.org/documentation/; https://wiki.civtak.org/index.php?title=ATAK_Manual; https://www.pargovernment.com/tactical-sa/docs/S20_brochure.pdf; https://insights.samsung.com/2021/09/22/7-ways-samsungs-galaxy-xcover-pro-supports-first-responders/; https://kp4-cdn.samsungknox.com/resource/Samsung%20Knox%20Security%20Handbook_bx4Z.pdf; https://docs.samsungknox.com/admin/knox-manage/faqs/faq-115013698467.htm;

https://docs.samsungknox.com/admin/knox-manage/locate-devices.htm; and Samsung's agents and representatives located within this Judicial District. Defendants are thereby liable for infringement of the '829 Patent under 35 U.S.C. § 271(b).

57. For example, Defendants directly infringe and/or indirectly infringe by instructing their customers to infringe by a system comprising: one or more server devices programmed to perform operations comprising: forwarding, to a first device, a request to join a group, wherein the request is received from a second device and the group includes the second device; based on acceptance of the request by the first device, joining the first device to the group, wherein joining the first device to the group comprises authorizing the first device to repeatedly share device location information and repeatedly engage in remote control operations with each device included in the group; receiving a first message comprising a request for a first updated location of the first device, wherein the first message is sent by the second device and includes data identifying the first device; in response to receiving the first message, sending, to the first device, a second message comprising a request for the first updated location of the first device; after sending the second message, receiving a response to the second message, the response including first location information comprising the first updated location of the first device; sending, to the second device, the first location information and georeferenced map data, wherein the second device is configured to present, via a display of the second device, a georeferenced map based on the georeferenced map data and a symbol corresponding to the first device, wherein the symbol is positioned on the georeferenced map at a first position corresponding to the first updated location of the first device, and wherein the georeferenced map data relate positions on the georeferenced map to spatial coordinates; after sending the first location information and the georeferenced map data to the second device, receiving second location information comprising a second updated location of the

first device and sending the second location information to the second device, wherein the second device is configured to use the server-provided georeferenced map data and the second location information to reposition the symbol on the georeferenced map at a second position corresponding to the second updated location of the first device; receiving a third message related to remotely controlling the first device to perform an action, wherein the third message is sent by the second device; and after receiving the third message, sending, to the first device, a fourth message related to remotely controlling the first device to perform the action, wherein the first device is configured to perform the action based on receiving the fourth message. For example, the Accused Products include features as shown below.

## Stay connected to what matters.

**Persistent communications**
The Galaxy S20 Tactical Edition is a COTS military smartphone with tailored software that easily connects to tactical radios and mission-critical devices, out of the box.

**Multi-ethernet capabilities**
Dedicated connections with multiple mission systems including laser range finders, external GPS devices, drones and more keep you connected in degraded and highly contested network environments.

**Next-generation networks**
As technologies evolve, you need a powerful, mission-ready device that can take full advantage of next-generation military networks. The Galaxy S20 Tactical Edition supports Private SIM, 5G, CBRS and is ready for Wi-Fi 6.

# Command and control

**Situational awareness**
The Galaxy S20 Tactical Edition integrates voice, video, and tactical data to provide a common operational picture of the battlespace. This complete and accurate real-time intelligence enhances the precision and effectiveness of your tactical teams.

**Tactical user experience**
Unique features found only on the Galaxy S20 Tactical Edition deliver fast and simple access to the information and applications operators need on-mission.

**Better intelligence**
The pro-grade 64 MP camera on the Galaxy S20 Tactical Edition allows you to discretely capture and share crisp high-resolution photo or 8K video intelligence, even in low light without the use of a flash. View and analyze intelligence in greater detail than ever before with the Galaxy S20 Tactical Edition's Dynamic AMOLED 2.0, a 120Hz[1] display.

**Extend your mission**
The Galaxy S20 Tactical Edition battery is 30% larger than the previous tactical solution and it's intelligent.[2] It optimizes your app usage in the field giving you extended power to complete the mission. When you need a recharge, Super Fast Charging[3] and fast Wireless Charging 2.0 give you power in a flash. And Wireless PowerShare allows you to easily charge a team member's phone in the field just by touching the devices.[4]

**Connect to tactical radios** - Protocols to support tactical radios and mission systems, out of the box.

**Tactical app quick launch** - Instantly expand or hide ATAK, APASS and other mission-critical applications at the push of a button.

**Night vision mode** – Turn on and off LED backlight when wearing night vision devices.

**Stealth mode** – Disable LTE and e-911 and mute all RF broadcasting for complete off-grid communications.

**Lock screen auto-rotate** - Unlock the device in landscape mode for easy access when mounted to the operator's chest.

**Auto-touch sensitivity** – Automatically adjust device operations to work with gloved hands.

# One device to meet all your mission requirements.

**Simple device management**
From device configuration, enrollment, customization and management to advanced mobile security controls and updates, Samsung has the mobility cloud services you need for every stage of the Galaxy S20 Tactical Edition lifecycle.[6] With Knox Services, you can keep pace and maintain control over devices and how they're used. You can manage devices in near real-time, configure settings, and remotely lock or wipe devices if lost or stolen, on the battlefield and anywhere else.

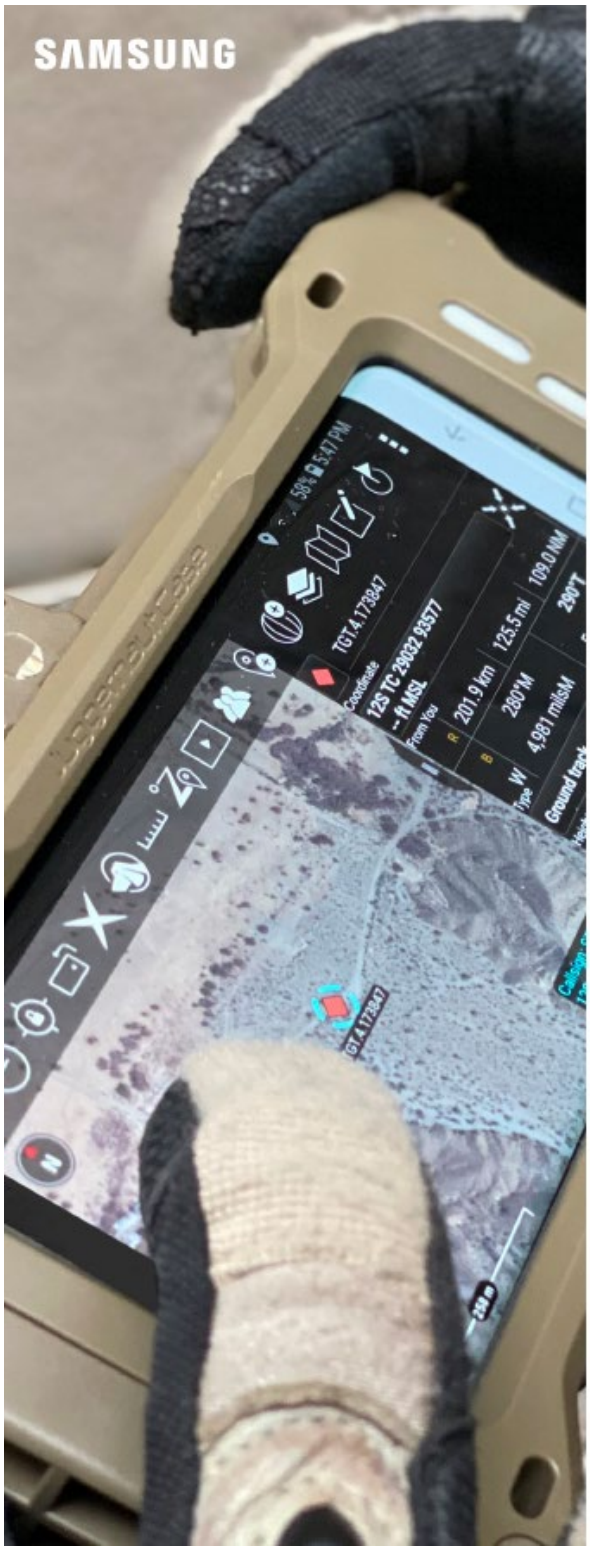
**Run mission apps and enterprise apps**
The Galaxy S20 Tactical Edition has a 64-bit Octa-Core processor with the speed and versatility to run multiple tactical applications in the field and enterprise applications everywhere else.

With Samsung DeX, connect your Galaxy S20 Tactical Edition to a monitor, keyboard and mouse for a desktop-like experience[5] ideally suited for mission planning, training, and everyday use. DeX gives you the power to work seamlessly across Microsoft Office Suite applications,[6] productivity apps, and virtual desktops with secure CAC-authenticated Virtual Desktop Infrastructure (VDI) sessions, all without a laptop.[7] And DeX-in-Vehicle transforms the Galaxy S20 Tactical Edition into a powerful in-vehicle computer.

**Open and secure**
The Galaxy S20 Tactical Edition is built on an open and secure Android operating system enabling seamless integration with a diverse ecosystem of tactical solution partners. Eliminate vulnerabilities with three software updates throughout the life of the device.

60

[60] https://www.pargovernment.com/tactical-sa/docs/S20_brochure.pdf




## Galaxy S20 Tactical Edition

# Mission-ready mobility. Proven by operators.

The Samsung Galaxy S20 Tactical Edition is the mission-ready military smartphone built and proven by operators in special operations. Based on the proven success of the S9 Tactical Edition for operators in the field, the S20 Tactical Edition is the only end user device you'll need for mission planning, training, operations and daily use.

### Persistent communications in any domain

**Purpose-built to connect to tactical radios** and mission systems out of the box, the Galaxy S20 Tactical Edition delivers a complete and accurate common operational picture. Run mission applications in the field and enterprise applications everywhere else with a single end user device for mission training, planning, operations and everyday use.

### Interoperable across devices and networks

**Pre-configured software, pre-loaded during the manufacturing process,** includes drivers to support tactical radios and mission-critical devices. Multi-ethernet capabilities provide dedicated connections to multiple mission systems including drone feeds, laser range finders, and external GPS. Support for current and next-generation networks includes Private SIM, 5G, WiFi 6 and CBRS. Allow or disallow USB peripherals based on product or vendor identifiers.

### Command and control

**Integrate voice, video and tactical data** for a complete view of the battlespace to enhance precision and effectiveness. Unique tactical features on the Galaxy S20 Tactical Edition include night-vision mode, stealth mode, lock screen autorotate, hostage negotiation mode, LTE band lock for consistent 4G connection, tactical application quick launch, to keep the operator focused on the objective, Standalone(5G)/Non-standalone (4G) modes to stay on preferred network. Preloaded tactical settings app. Ability to configure hotspot 2.0.

### Capture Intelligence

**A Pro-grade 64 MP camera** on the Galaxy S20 Tactical Edition enhances intel gathering, even in low-light environments without a flash. Capture high-resolution photos or sharp 8K video reconnaissance without giving away your position.

### Power to extend the mission

**Keep going wherever the mission takes you** with the Galaxy S20 Tactical Edition's intelligent2 4000mAh battery is 30% larger than the previous tactical solution and optimizes energy based on your device usage. Easily share power with a team member's smartphone in the field simply by touching devices using Wireless PowerShare.[4]

### One device to meet your requirements

**Run mission applications in the field** and enterprise applications everywhere else with the powerful and efficient Galaxy S20 Tactical Edition 64-bit Octa-Core processor. Connect your device to a monitor keyboard and mouse and use the power of Samsung DeX[5] for a desktop-like experience that is ideal for mission planning, training and everyday use. DeX-in-Vehicle transforms your Galaxy S20 Tactical Edition into an in-vehicle computer.

### Open and secure

**Enable a diverse ecosystem of tactical partners** with the open and secure Android operating system on the Galaxy S20 Tactical Edition. The all-new Tactical Settings feature simplifies device management, while Samsung Knox provides defense-grade security[6] from the hardware layer up and mission-specific device customization capabilities. The DualDAR architecture of the Galaxy S20 Tactical Edition provides two layers of encryption, even when the device is powered off, for securing up-to top secret level data on the device.

### Tested and proven

Samsung Galaxy Tactical Edition smartphones are tested and proven by special operators in the field. The Galaxy S20 Tactical Edition is certified to meet the most stringent requirements including NSA's CSFC Components List, NIAP Common Criteria/MDFPP, DODIN APL, FIPS 140-2, DISA Android 10 STIG, IP68 rating.

**Contact Us:** www.samsung.com/TacticalEdition

61

[61] https://image-us.samsung.com/SamsungUS/samsungbusiness/pdfs/flyer/S20_TE-salesflyer_FINAL_July_2021.pdf

The Team Awareness Kit (TAK), for civilian uses, or Tactical Assault Kit (also TAK) for military uses is a suite of software that provides geospatial information and allows user collaboration over geography. There are numerous TAK Products in the TAK family, all developed at government expense

The Team Awareness Kit for Android (ATAK, also known as CivTAK) was originally developed by the Air Force Research Laboratory (AFRL) and is now maintained by a Joint Product Center.

ATAK (including CivTAK) is an Android smartphone geospatial infrastructure and situational awareness app. It allows for precision targeting, surrounding land formation intelligence, situational awareness, navigation, and data sharing.

All the Android variants of TAK are virtually identical and all are interoperable with each other and with other TAK products. There are small, military-specific additions in military versions of ATAK.

# Features

Industry/civilian capabilities of ATAK/CivTAK include:

- Online and offline mapping (most standard formats), with a blazing fast rendering engine
- Support for very high-resolution imagery (sub 1 cm resolution)
- Collaborative mapping, including points, drawings, locations of interest
- Extensive and customizable set of Icons
- Overlay Manager which allows the Import and display of KML, KMZ, GPX overlays and maps, including online sources
- Location marking, sharing, history
- Chat, file sharing, photo sharing, video sharing, streaming
- Navigation-walking/hiking, driving, also useful flying and air-ground coordination
- Elevation Tools, heat maps, computed contour maps, viewsheds, routes w/DTED, SRTM, including dynamic profiling
- Hashtags and Sticky tags
- Center on Self, Center on other objects (e.g. another person in the network)
- Range, bearing, and other measurement tools
- Network-aware geofences with triggers
- "Bloodhound" destination tracking, including on moving objects
- Team Emergency Beacons
- Customizable Toolbar
- Radio controls and Integration
- Photo to map capability (aka Rubber Sheeting)
- Casualty evacuation tool
- Icon support for a wide variety of First Responder missions with further extensible Icons
- 3D perspective and ability to display 3D geospatial models
- Useful for First Responders, Hunting, fishing, ornithology, wildlife site survey
- An API with an SDK

62

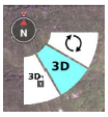
[62] https://www.civtak.org/documentation/

## ATAK Civilian Overview

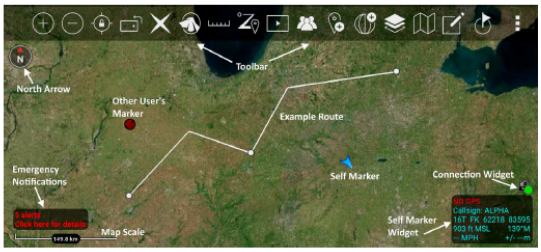
The Civilian Team Awareness Kit for Android (ATAK Civilian) is a Government-off-the-Shelf (GOTS) software application and mapping framework for mobile devices. ATAK Civilian has been designed and developed to run on Android smart devices used in a first responder environment. The ATAK Civilian software application is an extensible moving map display that integrates imagery, map and overlay information to provide enhanced collaboration and Situational Awareness (SA) over a tactical meshed network. ATAK Civilian promotes information flow and communications from the field environment to command enterprise locations.

The first time ATAK Civilian is opened, or after a Clear Content, a passphrase is auto-generated to activate data encryption. The user can supply their own passphrase by using Settings > Show All Preferences > Device Preferences > Change Encryption Passphrase. Following this step, ATAK Civilian's End User License Agreement (EULA) must be accepted. Next, the user will be prompted to change their callsign and/or import preferences or data from a Mission Package. All changes/imports can always be updated later. Finally, the user can place their self-marker by following the instructions located in the lower right corner.

The toolbar runs along the top of the map display. The features whose icons form the center portion of the toolbar are discussed in individual sections of this guide. The three dots at the right of the toolbar provide additional menu items that appear in a drop-down menu. A Long Press on the map will toggle the toolbar between hidden and visible.




The North Arrow appears in the upper left and is used to control map orientation. It has two primary modes: North Up/Track Up (default) and Manual Map Rotation/Lock. While in North Up/Track Up Mode, single press on the [**North Arrow**] icon to cycle between the North Up and Track Up map orientation. Long press the [**North Arrow**] to call out the additional controls menu where the Manual Rotation/Lock and 3D features are available. Select the [**Rotation**] button to enter Manual Map Rotation/Lock Mode. When in Manual Map Rotation/Lock Mode, rotate the map orientation by pressing on the map with two fingers and pivoting them in the desired direction. Single press on the [**North Arrow**] to lock the screen orientation, signified by the appearance of the lock icon, and again to unlock the orientation for further adjustment. 3D controls are discussed in a separate section.



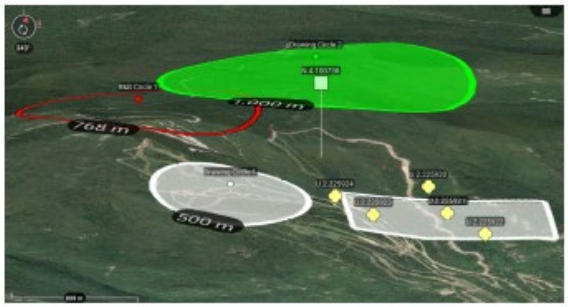

Select the [**Magnifier**] buttons to zoom in or out on the map. The map can also be zoomed by using two fingers on the screen to pinch and spread the map. Select the [**Back**] button to center the screen on the Self Marker or the [**Padlock**] icon to lock the center of the screen to the Self Marker. Select the [**Orientation**] icon to toggle the screen position between portrait and landscape.

The optional connection widget indicates whether or not the user is connected to a TAK Server. This has a corresponding Android notification that provides the same information. Toggle this display on at Settings > Network Connections > Network Connections > Display Connection Widget.

Alerts and notifications are displayed in the lower left of the map interface.

The Map Scale displays a 1 inch to X mi/km reference on the map. The scale adjusts with the map when zoomed in and out. Hint windows are available to alert users to changes or make suggestions about the use of tools the first time they are opened.

## 3D View



ATAK Civilian features 3D viewing of terrain and map items (DTED required). To enable 3D view, long press on the **[North Arrow]** to call out the additional controls menu and select [**3D**]. A tilt angle indicator will appear around the edge of the [**North Arrow**] when 3D view is active. Touch the screen with two fingers and simultaneously swipe up or down on the screen to tilt the view angle. Once the appropriate viewing angle is set, select the [**3D Lock**] button to retain this view while panning the map. While viewing the map from an angle, some map items will appear raised above the map surface if they have defined elevations.

## 3D Models

ATAK Civilian supports the use of 3D models. OBJ models and other types from products such as Pix4D can be imported via the Import Manager or can be manually placed in the atak/overlays folder prior to startup. If using Import Manager browse to the .OBJ file and import only that file, or browse to a .ZIP file that contains the .OBJ file (and others) and import only that file. If using manual placement to the atak/overlays folder, place a .ZIP file containing the .OBJ file (and others) into the directory and they will be imported on startup.

Once imported, a 3D Model icon will appear on the map. Zoom into the area of the icon until a loading ring appears. After the loading process has finished, the 3D model will be projected onto the map. Enable the map 3D View and tilt the view angle to see the 3D modeling. Loaded 3D models will appear as their own category in Overlay Manager and can be toggled on/off or removed from there.

# Placement

The user can enter locations of interest using the Point Dropper tool. Select the [**Point Dropper**] icon to place internationally standardized markers and other icons on the map, edit the data and share the markers with other network members.

## Self-Marker

The Self-Marker is displayed as a blue arrowhead at the user's current location. The options available on the Self-Marker radial are: Compass Rose, Polar Coordinate Entry, Fine Adjust/Enter Coordinate/MGRS Location, GPS Error, Range & Bearing Line, GPS Lock to Self, Tracking Breadcrumbs, Place a Marker at the user's current location and Details. Other TAK users appear on the display as a colored circle. The color of the circle represents the user's Team affiliation, with additional lettering inside the circle to identify the role the user on the team. Team Member markers that include a diagonal line indicate that the GPS location is not available. A solid icon indicated that the team member has GPS reception.

Available roles include: Team Member, Team Lead (designated by a TL in the center of the marker), Headquarters (HQ in center), Sniper (S), Medic (+), Forward Observer (FO), RTO (R) or K9 (K9). The options available when another user's Self-Marker is selected are: Inner Ring – Delete, Polar Coordinate Entry, Fine Adjust/Enter Coordinate/MGRS Location, Range & Bearing Line, GPS Lock on Friendly, Video Player (if available), Communication Options (if configured by that user), Custom Threat Rings, Tracking Breadcrumbs and Details.

Outer Ring (Communication Options) – Data Package, Email, SMS Messaging, GeoChat, VOIP and Cellular Phone, when available.

## Point Dropper

Selecting the [**Point Dropper**] icon will open the Point Dropper menu, containing marker symbology with one or more icon sets, a Recently Added button and an Iconset Manager button.

The Markers symbology affiliations are: Unknown, Neutral, Red and Friendly. Select the affiliation, then a location on the map interface to drop the marker. To add a marker by manually entering coordinates, long press on the map interface and enter the MGRS location. Change the standard naming convention by entering values into the custom prefix and index fields or leave blank to use the defaults. If values are entered, the next marker will be dropped with the prefix name and starting number(s) or letter(s) and every subsequent marker will be assigned the next consecutive number(s) or letter(s).

The user can select the mission specific pallet to open point options including Waypoint (WP), Sensor or Observation Point (OP).

The user can move between icon sets by either swiping in the icon set area or selecting on the [**Iconset Name**] field to bring up the Icon Pallet drop-down.

The last point placed is shown at the bottom of the Point Dropper window. The information for all recently placed points can be accessed by selecting the [**Clock**] icon. This displays the marker icon, name, coordinates, elevation and range & bearing information. The user can send, rename or remove any recently added markers by selecting the [**Arrows**] next to the marker to reveal [**SEND**], [**RENAME**] or [**DEL**] buttons.

Select the [**Iconset Manager**] (gear) button to add or delete icon sets or to set the default Marker Mapping.

## Radial Menus

**Unknown Object**

**Neutral Object**

**Red Object**

**Friendly Object**

**Spot Object**

The options available for Unknown Object Markers are: Delete, Polar Coordinate Entry, Fine Adjust/Enter Coordinate/MGRS Location, Range & Bearing Line, Lock On, Tasking, Custom Threat Rings, Tracking Breadcrumbs and Details.

The options available for Neutral Object Markers are: Delete, Polar Coordinate Entry, Fine Adjust/Enter Coordinate/MGRS Location, Range & Bearing Line, Lock On, Tasking, Custom Threat Rings, Tracking Breadcrumbs and Details.

The options available for Red Object Markers are: Delete, Polar Coordinate Entry, Compass Rose/Bullseye, Fine Adjust/Enter Coordinate/MGRS Location, Range & Bearing Line, Tasking, Custom Threat Rings, Tracking Breadcrumbs and Details.

The options available for Friendly Object Markers are: Delete, Polar Coordinate Entry, Fine Adjust/Enter Coordinate/MGRS Location, Range & Bearing Line, Lock On, Video, Contact Card, Custom Threat Rings, Tracking Breadcrumbs and Details. The Video radial will activate if a properly formatted packet that includes the link to the video feed is included. Select the video radial to open the associated video. The Contact Card can be selected to display additional communication options, including GeoChat, Email, VoIP, SMS Messaging and Cellular Phone, when available.

The options available for Spot Map are: Delete, Fine Adjust/Enter Coordinate/MGRS Location, Range & Bearing Line, Nav-To, Custom Threat Rings, Labels and Details.

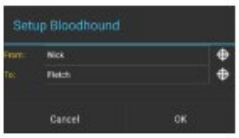
The options for User Defined Iconsets are: Delete, Polar Coordinate Entry, Fine Adjust/Enter Coordinate/MGRS Location, Range & Bearing Line, Lock On, Tasking, Custom Threat Rings. Tracking Breadcrumbs and Details.

Select [**Details**] on the marker radial to make desired modifications, including: Coordinate, Elevation, Name, Type and Remarks. Selecting Marker Type opens a dialog box with extra categories. File attachments, including images, can be associated with the object by selecting the [**Paperclip**] icon. Once all the desired modifications have been made, the Marker can be sent to other network members using [**Send**]. The information can be broadcast to all members or sent to specific recipients. Select the [**Auto Send**] option to broadcast the marker to other TAK users on the network, with updates automatically sent about once every 60 seconds.

# Bloodhound Tool

The Bloodhound Tool provides support for tracking and intercepting a map item. It allows the user to select two points on the map and/or map objects and display range & bearing information between the chosen tracker and the target.

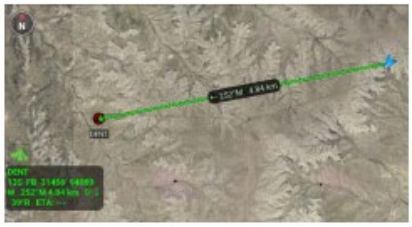
Select the [**Bloodhound**] icon to open the Bloodhound Tool. A window will open, prompting the user to choose where to start by tapping the [**From Reticle**] (default = user's self marker) and where to bloodhound (track) to by tapping the [**To Reticle**].




Targets include map objects like other User's Self Markers, DPs, Markers, Shape center points, Range & Bearing end-points and any other map objects. If the user selects a map location instead of an object as the target, Bloodhound will place a waypoint marker there. The self marker will then track towards the waypoint.

Select [**OK**] and Bloodhound will be activated.

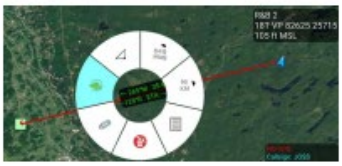
If either point moves, the green widget in the lower left will show the updated information. As the tracking object begins to navigate toward the target, the Estimated Time of Arrival (ETA) will update accordingly.



The green line showing the direct path from the tracker to the target will flash when the user-defined ETA outer threshold is reached (default = 6 minutes from target). The line will flash as the tracker continues toward the target until the next ETA threshold is reached (default = 3 minutes). The line will turn a flashing yellow until the final ETA threshold (default = 1 minute) is reached. The line then flashes red until the target is reached. Colors and thresholds can be modified in Settings > Tool Preferences > Bloodhound Preferences.

Selecting the green Bloodhound icon on the map will pan the map to the Bloodhound Range & Bearing Line. Disengage the Bloodhound Tool by selecting the [**Bloodhound**] icon on the toolbar.

## Multiple Bloodhound

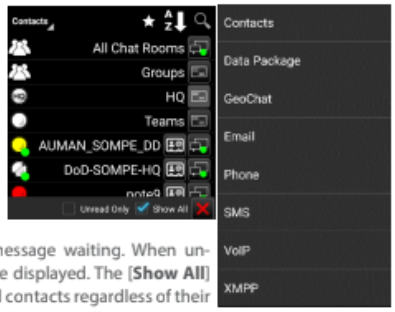


To create multiple bloodhounds, selecting the Range and Bearing Tool and select the [**R&B Line**] icon. Select two markers on the map and once the R&B line is created, select the line to bring up the radial. Select the [**Bloodhound**] radial, and the bloodhound information will be displayed on the R&B Line itself.

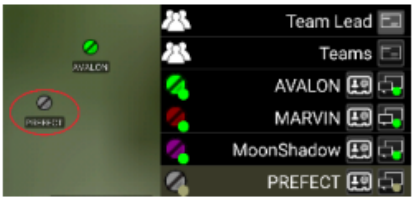
If either point moves, the Bloodhound information shown on the R&B Line will be updated. As the tracking object begins to navigate toward the target, the Estimated Time of Arrival (ETA) will update accordingly.

## Contacts

The Contacts list includes a variety of ways in which a user may communicate with other users, such as GeoChat (ATAK Civilian's built in Chat capability), Data Packages, Email, Phone, SMS, VoIP and XMPP.



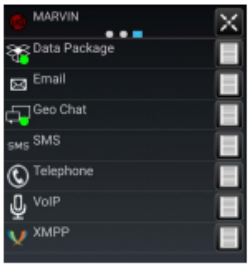

A default communication type (shown in the last column) may be selected and used until another type of communication is selected.




The Contacts list has two filters available at the bottom of the screen. The Unread Only box, when checked, will display only contacts with whom there are unread message waiting. When unchecked (default), all available contacts are displayed. The [**Show All**] box, when checked (default), will display all contacts regardless of their location. When unchecked, only contacts that are visible on current map screen will be displayed.

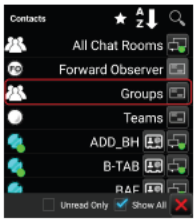
If a contact is no longer online, it will be indicated by changing the contact listing to a yellow color and the marker changes to gray both in the list and on the map.

Profile cards are accessed by selecting the second to last column in the Contacts list and are available for each contact. These contain additional information about that contact including: 1) role, software type and version installed, node type, default connector, last reported time, battery life; 2) location information, and 3) available types of communication.

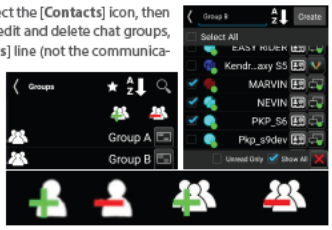


## GeoChat Group Management

Text-based Chat messages may be sent to active network members by using the GeoChat function. To enter GeoChat Group Management, select the [**Contacts**] icon and select [**GeoChat**] from the drop-down menu.

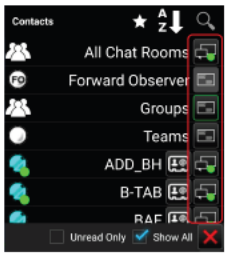



GeoChat Group Management is initiated through Contacts. Select the [**Contacts**] icon, then select GeoChat from the drop-down. The user can now create, edit and delete chat groups, as well as sub-groups. To create a chat group, select the [**Groups**] line (not the communications button). Select the [**Add Group**] icon to create the name of the group and add contacts to the group and then select [**Create**]. If a parent group is being created, no contacts need to be added at this level. To add a nested group, tap the parent group, select the [**Add Group**] icon to create the name of the sub-group and add contacts. Groups may be managed using the options to add/delete contacts or to add/delete GeoChat group.




To add users to a group, select the [**Groups**] line (not the communications button), then select the name of the group to add users. Select the [**Add Users**] icon. A window will open allowing the group creater to add users to the selected group. Select the [**Add**] button when all the users to be added are checked.

## GeoChat Messaging




Group and person-to-person messaging is available. To view messages from or send messages to an individual, tap on the desired contact's [**Communication**] icon. Selecting the [**Pan To**] icon, located at the top right of the call sign in an individual chat, will pan the map interface to that user's location. Select [**All Chat Rooms**] to view all messages from or send messages to those present on the network or TAK Server. Other groupings available for viewing or sending messages are: Forward Observer, Groups, HQ, K9, Medic, RTO, Sniper, Team Lead and Teams. If the user's current role is Forward Observer, HQ, K9, Medic, RTO, Sniper or Team Lead, that user can view or send messages to all other contacts with the same role. If a GeoChat message is sent from the top level of Teams, it will be sent to all contacts, similar to [**All Chat Rooms**].

When a sub-Team is chosen, messages can only be sent to that user's active (My Team) team color. When a parent group is chosen, messages are sent to all members of the parent group, as well as all of the sub-groups. When a sub-group is chosen, messages are sent only to members of the sub-group. Individuals within GeoChat may be removed from the Contacts menu by toggling the visibility of individuals or groups within Overlay Manager.

26



## GeoChat Messaging (continued)

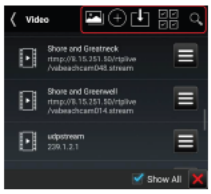
Selecting in the Free Text Entry area will open an onscreen keyboard. At the bottom of the Chat area are pre-defined messages that may be used to quickly create a message to send. Tap the current menu button to scroll through the different menus of canned messages, including: DFLT1, DFLT2, ASLT1, ASLT2, RECON1 and RECON2. These pre-defined messages present an easy way to transmit a brief message to other network members concerning position or other important communication. The pre-defined messages may be changed by long pressing on the button and changing its label and corresponding value.

A numbered red dot will appear on the [**Contacts**] icon when a message has been received successfully. The number denotes the number of unread messages that have been received. Select this icon to view the contact list. The user name who sent the message will appear with a numbered red dot next to their name. Alternatively, the text of the message can be read by dragging down from the top to see the Android notifications window. This notification will only stay available for a short time.

## Video Player

Select the **[Video Player]** icon to bring up the Video player. The Video Player supports playing video streams from IP cameras and H.264 encoders. The menu allows adding, editing, deleting, playing or sending videos to other network members.

Options for the video player include: viewing video snapshots, adding a new video alias, downloading an alias from the TAK Server, selecting the Multi-Select Action option to either Export or Delete aliases or searching for a specific alias.




Select the desired listed video alias or file name to begin playing the stored or streaming video. The video will display half the width of the screen.

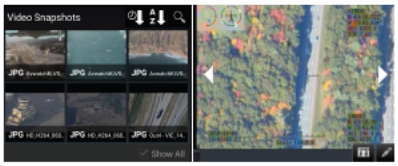
To view a video at full screen, slide the pull bar. To return to half screen, slide the pull bar back to the right.

Select the **[Back]** button to return to the list of available videos.

To add stored video file, select the **[Import Manager]** icon, select **[Local SD]**, and navigate to the video file and select **[OK]** to add the video to the list of available videos. The user can also manually place video files in "atak\tools\videos" to have them listed after ATAK is restarted. When a video is playing at half width, slide the pull bar to the right to hide the video but maintain the connection. Slide the pull bar to the left to unhide the video. The status of the video player is reflected in the main Android toolbar located at the top of the screen.

Select the **[Snapshot]** icon to save the current frame of the video as a JPEG image file, the icon will flash green to indicate that the snapshot has occurred. The file will be saved in the "\atak\tools\videosnaps" folder.

The user can view the saved snap shots by selecting the **[Video Snapshots]** icon. The user has the option of sorting the images by time taken or by the name of the snapshot. The user can also search within the snapshots taken by their name. By selecting an image, the image will be displayed within the window.




The user will have the options of cycling though the images, **[Send]** to a TAK user, or edit in **[Image Markup]**. (Image Markup would need to be installed.)

If a live UDP stream is being viewed, it can be recorded by tapping the **[Record]** icon. The icon will change to a green square while recording. Select the **[Green Square]** to end the recording. The recordings are saved in a folder in "\atak\tools\videos\".

**Note:** This is only available for UDP streams.

To close the video player, select the **[X]** located at the bottom right corner of the video player or select the **[Back]** button.





## Go To

Select the **[Go To]** icon to enter details and navigate to a specific location on the map.

Select from the **[MGRS]** (military grid reference system), **[DD]** (decimal degrees), **[DM]** (degrees- minutes), **[DMS]** (degrees-minutes-seconds), **[UTM]** (Universal Transverse Mercator) or **[ADDR]** tabs on the Go To interface and enter the location data of interest. The address provider name appears beneath the Elevation Data when the user selects the **[ADDR]** tab.

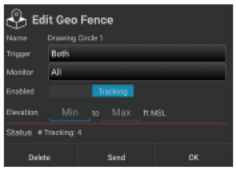
The user can enter the Latitude, Longitude and Elevation in the space provided for **[MGRS]** , **[DD]**, **[D-M]** or **[D-M-S]** searches. If DTED is installed, the elevation value can be automatically populated by tapping the **[Pull From DTED]** button.The user can select a desired marker type (Spot, Unknown, Neutral, Red, or Friendly) to be placed at the entered coordinates. If **[No Point]** is selected, the map will pan to the location but will not add a point.

**Note:** The address provider name appears beneath the Elevation Data when the user selects the **[ADDR]** tab.

The Address Lookup provider used for the ADDR tab can be configured in the Settings > Tool Preferences > Address Lookup Preferences.

## Geofencing

The Geo Fence tool allows users to create a virtual fence that triggers entry/exit notifications if map items of interest cross the virtual boundary lines. The Geo Fence options are added to the existing drawing tools. After a shape has been added, the Geo Fence Tool can be accessed either by selecting the [**Geo Fence**] icon from the menu items or selecting it from the radial.




The Enabled Field slider will move to Tracking by default when a new Geo Fence window is created. Toggle the slider between Tracking and Off to enable/disable the Geo Fence. Use the Trigger field to define which types of Geo Fence breach to monitor. Choose between Entry, Exit or Both. Use the Monitor field to define which entities the Geo Fence will track.

Choose between TAK Users, Friendly, Hostile, Custom or All. Check the [**Specify Elevation**] box to enable the Elevation field, where elevation boundaries for the entities being tracked can be defined. Select the [**OK**] button to finish creating the fence. Select the [**Send**] button to create the fence and send it to another user. Select [**Delete**] to close the Create Geo Fence window and discard changes.

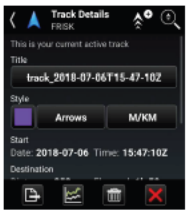
Alerts appear on the map interface. Selecting the [**Alert Notification**] will open the alerts menu, detailing the activity monitored in the user defined region. The default radius for monitoring users (filtered within the "Monitor" field) outside the Geo Fence is set at 75 km. This means the total area monitored begins at the farthest point from the center of the shape plus 75 km. If the user wishes to keep the Geo Fence, but disable tracking, the user can set the tracking [**Enabled**] to off in the Edit Window.

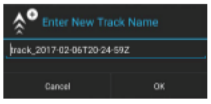




## Track History

The device's GPS can be used to track movements with the Track History tool. These tracked paths can be exported to a TAK server, to a route or to a KML, KMZ, GPX or CSV file. A GPS position must be established before tracking can begin.



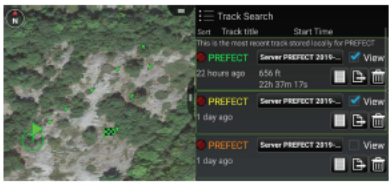




Selecting the [**Track History**] icon will open Track Details for the current active track. The track title, color and style can be modified. Initiate a new track by selecting the [**Add Track**] icon. Accept or edit the default track name and select the [**OK**] button to begin the new track. User location data is recorded as breadcrumbs in a new track file.

## Track Search

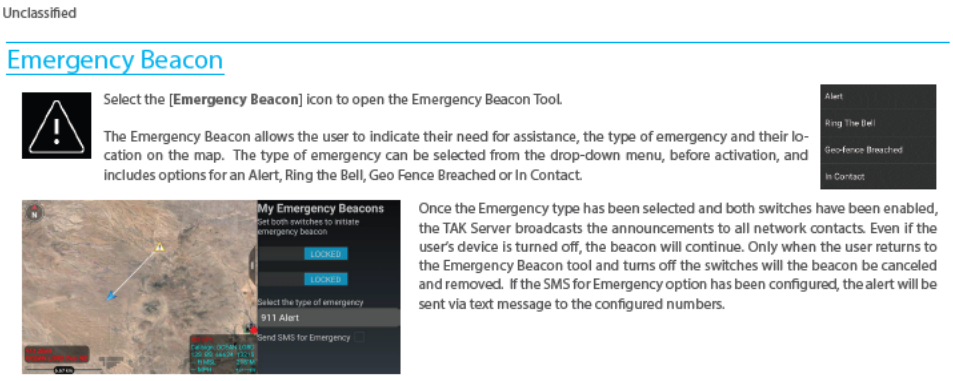
Use the Track Search function to view track information that has been previously saved locally or on a TAK Server. The tool searches the track database for matches against the specified time range and by user callsign. Matching tracks are displayed as a list, and can be selected to view on the map interface.

Select the [**Track Search**] icon to access the function. Specify callsign and time frame, check the box for Server Search (if desired), then select [**Search**]. The track list will appear. The query results can be sorted by Track Name or Start Time. Select any of the query results to move to that track. Once selected, the name, color, and style of a selected track can be modified or the track can be cleared. Convert a track to a TAK route or export it as a KML, KMZ, GPX or CSV file by selecting the desired track and then [**Export**]. Enter a file name then select [**Next**] and choose the export format. Select [**Done**] or [**Send**] when the export completes.



When viewing the track list, the Track History Toolbar will appear at the top of the screen. The options include [**Add a Track**], [**Multi-select**], [**Track Search**], [**Clear Tracks**] and [**Exit**]. The Track History List allows the user to select tracks of other users that have been saved on their device. The Track Search – Local Device allows the user to perform a tailored search for tracks meeting their criteria. The searching option allows the user to retrieve all the tracks on the device.

The Track History Breadcrumb and Settings can be configured in the Settings > Tools Preferences > Track History Preferences.


Unclassified

Emergency Beacon

Select the [**Emergency Beacon**] icon to open the Emergency Beacon Tool.

The Emergency Beacon allows the user to indicate their need for assistance, the type of emergency and their location on the map. The type of emergency can be selected from the drop-down menu, before activation, and includes options for an Alert, Ring the Bell, Geo Fence Breached or In Contact.





Once the Emergency type has been selected and both switches have been enabled, the TAK Server broadcasts the announcements to all network contacts. Even if the user's device is turned off, the beacon will continue. Only when the user returns to the Emergency Beacon tool and turns off the switches will the beacon be canceled and removed. If the SMS for Emergency option has been configured, the alert will be sent via text message to the configured numbers.

63

[63] https://drive.google.com/file/d/1bo9WHadg3J3o55OLlx1mn3McqEJzvgrK/view

# INTRO

## A new way of working demands a new level of security. Are you sure your devices are protected?

**This is protection.**

Remember the good old days? The morning commute and the 9 to 5? Well those days are history.

Forget being tied to a desk and a schedule. Today's workplace has nothing to do with time or place and everything to do with productivity and mobility. Without compromise. Today's employees want the same access, speed and resources of the office, even if they're three time zones and two continents away.

While mobile, employees spend a significant amount of time outside of their protected corporate networks as they access the web from locations other than their offices. This can expose businesses to more attacks, errors, leaks and new dangers we haven't even encountered.

For IT leaders, supporting a mobile workforce while maintaining the same level of productivity they would have had in the office is extremely difficult. Doing it while maintaining top level security is nearly impossible. Nearly.

This entirely new way of working demands protection that works in real time, not sometimes. Protection that secures on every layer, not just one. Protection that understands that we're safer when we work together, instead of trying to go it alone. Most importantly, protection is security without compromise and protects without getting in the way of creativity, productivity or freedom.

Protection is what Samsung is all about and it's why we built Samsung Knox, a cutting-edge security platform for mobile experience embedded in your Samsung Galaxy device. We are talking real-time, end-to-end protection, with the best intelligence from leading partners and experts across the industry, including Google, Cisco and more. So if you want to stay a step ahead, you can trust Samsung Galaxy and Samsung Knox to fully protect your way of working.

**This is protection. Samsung Knox.**

64

[64] https://kp4-cdn.samsungknox.com/resource/Samsung%20Knox%20Security%20Handbook_bx4Z.pdf.

# Knox Platform for Enterprise

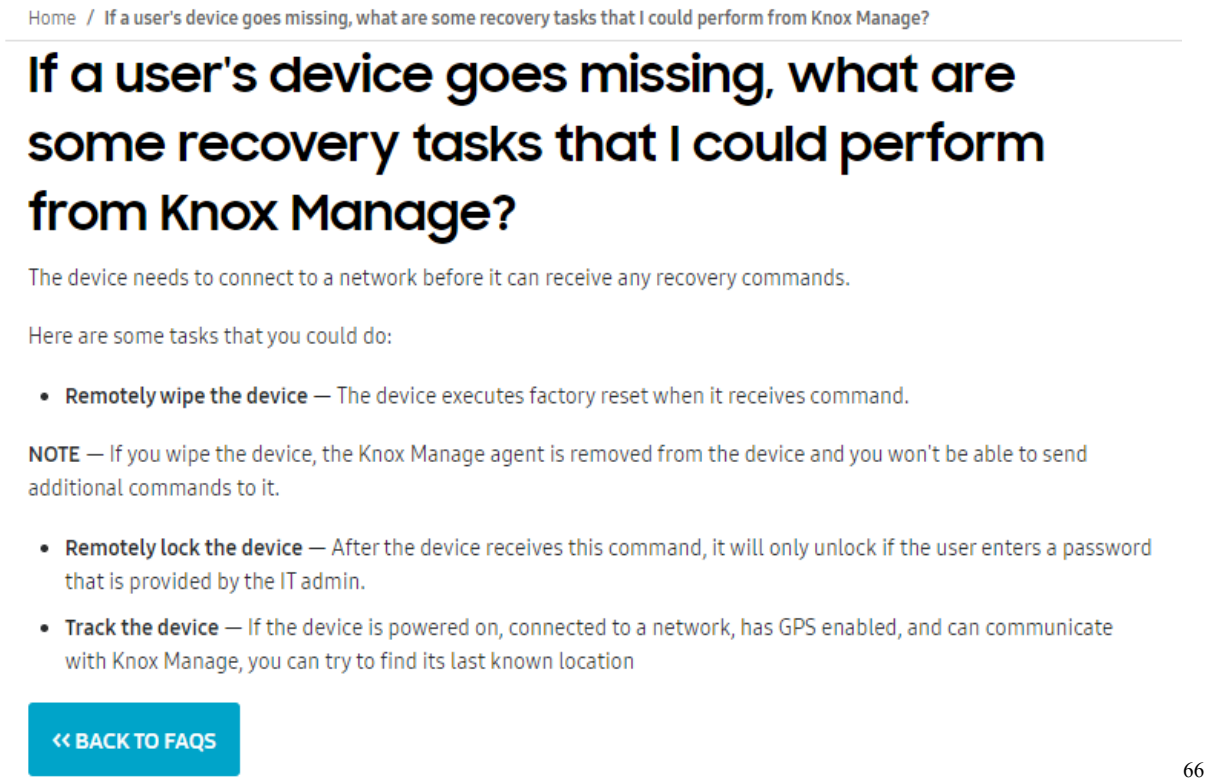
TRY FOR FREE

Samsung's Knox Platform for Enterprise (KPE) brings defense-grade security on the most popular consumer devices to all enterprises.

The Knox Platform provides best-in-class hardware-based security, policy management, and compliance capabilities beyond the standard features commonplace in the mobile device market. The Knox Platform is the cornerstone of a strong mobile security strategy supporting a wide variety of Samsung devices.

65

[65] https://docs.samsungknox.com/admin/knox-platform-for-enterprise/welcome.htm.



Home / If a user's device goes missing, what are some recovery tasks that I could perform from Knox Manage?

# If a user's device goes missing, what are some recovery tasks that I could perform from Knox Manage?

The device needs to connect to a network before it can receive any recovery commands.

Here are some tasks that you could do:

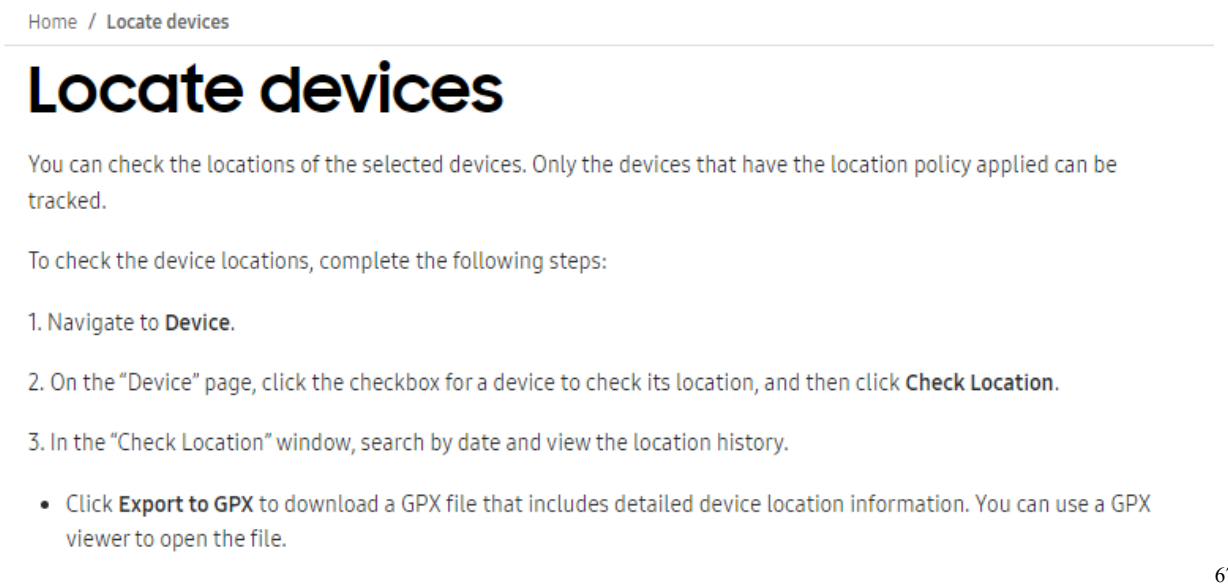
- **Remotely wipe the device** — The device executes factory reset when it receives command.

**NOTE** — If you wipe the device, the Knox Manage agent is removed from the device and you won't be able to send additional commands to it.

- **Remotely lock the device** — After the device receives this command, it will only unlock if the user enters a password that is provided by the IT admin.
- **Track the device** — If the device is powered on, connected to a network, has GPS enabled, and can communicate with Knox Manage, you can try to find its last known location

<< BACK TO FAQS

66



Home / Locate devices

# Locate devices

You can check the locations of the selected devices. Only the devices that have the location policy applied can be tracked.

To check the device locations, complete the following steps:

1. Navigate to **Device**.

2. On the "Device" page, click the checkbox for a device to check its location, and then click **Check Location**.

3. In the "Check Location" window, search by date and view the location history.

- Click **Export to GPX** to download a GPX file that includes detailed device location information. You can use a GPX viewer to open the file.

67

[66] https://docs.samsungknox.com/admin/knox-manage/faqs/faq-115013698467.htm.
[67] https://docs.samsungknox.com/admin/knox-manage/locate-devices.htm.

58. For example, Defendants' Accused Products allow users to share their locations and view other users' locations on a map and to communicate with those users via the Samsung Tactical, TAK, and ATAK applications and services and Samsung Knox applications and services (as shown below).

# One device to meet all your mission requirements.

**Simple device management**
From device configuration, enrollment, customization and management to advanced mobile security controls and updates, Samsung has the mobility cloud services you need for every stage of the Galaxy S20 Tactical Edition lifecycle.[8] With Knox Services, you can keep pace and maintain control over devices and how they're used. You can manage devices in near real-time, configure settings, and remotely lock or wipe devices if lost or stolen, on the battlefield and anywhere else.

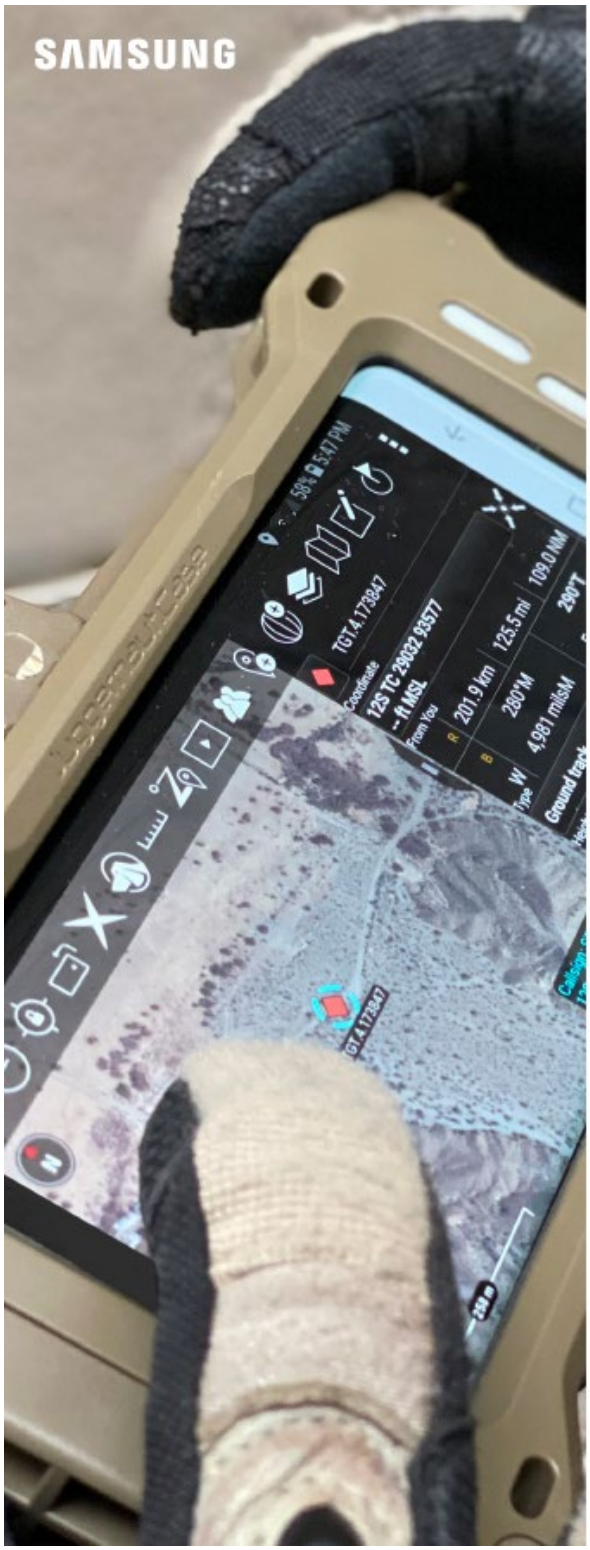
**Run mission apps and enterprise apps**
The Galaxy S20 Tactical Edition has a 64-bit Octa-Core processor with the speed and versatility to run multiple tactical applications in the field and enterprise applications everywhere else.

With Samsung DeX, connect your Galaxy S20 Tactical Edition to a monitor, keyboard and mouse for a desktop-like experience[5] ideally suited for mission planning, training, and everyday use. DeX gives you the power to work seamlessly across Microsoft Office Suite applications,[6] productivity apps, and virtual desktops with secure CAC-authenticated Virtual Desktop Infrastructure (VDI) sessions, all without a laptop.[7] And DeX-in-Vehicle transforms the Galaxy S20 Tactical Edition into a powerful in-vehicle computer.

**Open and secure**
The Galaxy S20 Tactical Edition is built on an open and secure Android operating system enabling seamless integration with a diverse ecosystem of tactical solution partners. Eliminate vulnerabilities with three software updates throughout the life of the device.

68

[68] https://www.pargovernment.com/tactical-sa/docs/S20_brochure.pdf




## Galaxy S20 Tactical Edition

# Mission-ready mobility. Proven by operators.

The Samsung Galaxy S20 Tactical Edition is the mission-ready military smartphone built and proven by operators in special operations. Based on the proven success of the S9 Tactical Edition for operators in the field, the S20 Tactical Edition is the only end user device you'll need for mission planning, training, operations and daily use.

### Persistent communications in any domain

**Purpose-built to connect to tactical radios** and mission systems out of the box, the Galaxy S20 Tactical Edition delivers a complete and accurate common operational picture. Run mission applications in the field and enterprise applications everywhere else with a single end user device for mission training, planning, operations and everyday use.

### Interoperable across devices and networks

**Pre-configured software, pre-loaded during the manufacturing process,** includes drivers to support tactical radios and mission-critical devices. Multi-ethernet capabilities provide dedicated connections to multiple mission systems including drone feeds, laser range finders, and external GPS. Support for current and next-generation networks includes Private SIM, 5G, WiFi 6 and CBRS. Allow or disallow USB peripherals based on product or vendor identifiers.

### Command and control

**Integrate voice, video and tactical data** for a complete view of the battlespace to enhance precision and effectiveness. Unique tactical features on the Galaxy S20 Tactical Edition include night-vision mode, stealth mode, lock screen autorotate, hostage negotiation mode, LTE band lock for consistent 4G connection, tactical application quick launch, to keep the operator focused on the objective, Standalone(5G)/Non-standalone (4G) modes to stay on preferred network. Preloaded tactical settings app. Ability to configure hotspot 2.0.

### Capture Intelligence

**A Pro-grade 64 MP camera** on the Galaxy S20 Tactical Edition enhances intel gathering, even in low-light environments without a flash. Capture high-resolution photos or sharp 8K video reconnaissance without giving away your position.

### Power to extend the mission

**Keep going wherever the mission takes you** with the Galaxy S20 Tactical Edition's intelligent2 4000mAh battery is 30% larger than the previous tactical solution and optimizes energy based on your device usage. Easily share power with a team member's smartphone in the field simply by touching devices using Wireless PowerShare.[4]

### One device to meet your requirements

**Run mission applications in the field** and enterprise applications everywhere else with the powerful and efficient Galaxy S20 Tactical Edition 64-bit Octa-Core processor. Connect your device to a monitor keyboard and mouse and use the power of Samsung DeX[5] for a desktop-like experience that is ideal for mission planning, training and everyday use. DeX-in-Vehicle transforms your Galaxy S20 Tactical Edition into an in-vehicle computer.

### Open and secure

**Enable a diverse ecosystem of tactical partners** with the open and secure Android operating system on the Galaxy S20 Tactical Edition. The all-new Tactical Settings feature simplifies device management, while Samsung Knox provides defense-grade security[6] from the hardware layer up and mission-specific device customization capabilities. The DualDAR architecture of the Galaxy S20 Tactical Edition provides two layers of encryption, even when the device is powered off, for securing up-to top secret level data on the device.

### Tested and proven

Samsung Galaxy Tactical Edition smartphones are tested and proven by special operators in the field. The Galaxy S20 Tactical Edition is certified to meet the most stringent requirements including NSA's CSFC Components List, NIAP Common Criteria/MDFPP, DODIN APL, FIPS 140-2, DISA Android 10 STIG, IP68 rating.

**Contact Us:** www.samsung.com/TacticalEdition

69

[69] https://image-us.samsung.com/SamsungUS/samsungbusiness/pdfs/flyer/S20_TE-salesflyer_FINAL_July_2021.pdf

The Team Awareness Kit (TAK), for civilian uses, or Tactical Assault Kit (also TAK) for military uses is a suite of software that provides geospatial information and allows user collaboration over geography. There are numerous TAK Products in the TAK family, all developed at government expense

The Team Awareness Kit for Android (ATAK, also known as CivTAK) was originally developed by the Air Force Research Laboratory (AFRL) and is now maintained by a Joint Product Center.

ATAK (including CivTAK) is an Android smartphone geospatial infrastructure and situational awareness app. It allows for precision targeting, surrounding land formation intelligence, situational awareness, navigation, and data sharing.

All the Android variants of TAK are virtually identical and all are interoperable with each other and with other TAK products. There are small, military-specific additions in military versions of ATAK.

# Features

Industry/civilian capabilities of ATAK/CivTAK include:

- Online and offline mapping (most standard formats), with a blazing fast rendering engine
- Support for very high-resolution imagery (sub 1 cm resolution)
- Collaborative mapping, including points, drawings, locations of interest
- Extensive and customizable set of Icons
- Overlay Manager which allows the Import and display of KML, KMZ, GPX overlays and maps, including online sources
- Location marking, sharing, history
- Chat, file sharing, photo sharing, video sharing, streaming
- Navigation-walking/hiking, driving, also useful flying and air-ground coordination
- Elevation Tools, heat maps, computed contour maps, viewsheds, routes w/DTED, SRTM, including dynamic profiling
- Hashtags and Sticky tags
- Center on Self, Center on other objects (e.g. another person in the network)
- Range, bearing, and other measurement tools
- Network-aware geofences with triggers
- "Bloodhound" destination tracking, including on moving objects
- Team Emergency Beacons
- Customizable Toolbar
- Radio controls and Integration
- Photo to map capability (aka Rubber Sheeting)
- Casualty evacuation tool
- Icon support for a wide variety of First Responder missions with further extensible Icons
- 3D perspective and ability to display 3D geospatial models
- Useful for First Responders, Hunting, fishing, ornithology, wildlife site survey
- An API with an SDK

[70]

[70] https://www.civtak.org/documentation/

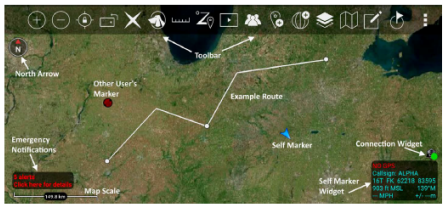
## ATAK Civilian Overview

The Civilian Team Awareness Kit for Android (ATAK Civilian) is a Government-off-the-Shelf (GOTS) software application and mapping framework for mobile devices. ATAK Civilian has been designed and developed to run on Android smart devices used in a first responder environment. The ATAK Civilian software application is an extensible moving map display that integrates imagery, map and overlay information to provide enhanced collaboration and Situational Awareness (SA) over a tactical meshed network. ATAK Civilian promotes information flow and communications from the field environment to command enterprise locations.

The first time ATAK Civilian is opened, or after a Clear Content, a passphrase is auto-generated to activate data encryption. The user can supply their own passphrase by using Settings > Show All Preferences > Device Preferences > Change Encryption Passphrase. Following this step, ATAK Civilian's End User License Agreement (EULA) must be accepted. Next, the user will be prompted to change their callsign and/or import preferences or data from a Mission Package. All changes/imports can always be updated later. Finally, the user can place their self-marker by following the instructions located in the lower right corner.

The toolbar runs along the top of the map display. The features whose icons form the center portion of the toolbar are discussed in individual sections of this guide. The three dots at the right of the toolbar provide additional menu items that appear in a drop-down menu. A Long Press on the map will toggle the toolbar between hidden and visible.

The North Arrow appears in the upper left and is used to control map orientation. It has two primary modes: North Up/Track Up (default) and Manual Map Rotation/Lock. While in North Up/Track Up Mode, single press on the [**North Arrow**] icon to cycle between the North Up and Track Up map orientation. Long press the [**North Arrow**] to call out the additional controls menu where the Manual Rotation/Lock and 3D features are available. Select the [**Rotation**] button to enter Manual Map Rotation/Lock Mode. When in Manual Map Rotation/Lock Mode, rotate the map orientation by pressing on the map with two fingers and pivoting them in the desired direction. Single press on the [**North Arrow**] to lock the screen orientation, signified by the appearance of the lock icon, and again to unlock the orientation for further adjustment. 3D controls are discussed in a separate section.




Select the [**Magnifier**] buttons to zoom in or out on the map. The map can also be zoomed by using two fingers on the screen to pinch and spread the map. Select the [**Back**] button to center the screen on the Self Marker or the [**Padlock**] icon to lock the center of the screen to the Self Marker. Select the [**Orientation**] icon to toggle the screen position between portrait and landscape.

The optional connection widget indicates whether or not the user is connected to a TAK Server. This has a corresponding Android notification that provides the same information. Toggle this display on at Settings > Network Connections > Network Connections > Display Connection Widget.

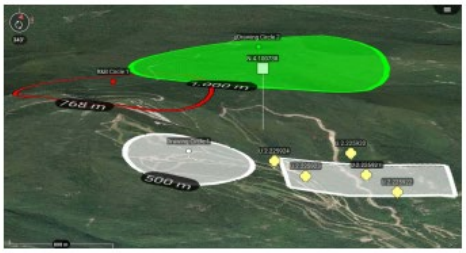
Alerts and notifications are displayed in the lower left of the map interface.

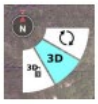
The Map Scale displays a 1 inch to X mi/km reference on the map. The scale adjusts with the map when zoomed in and out. Hint windows are available to alert users to changes or make suggestions about the use of tools the first time they are opened.





## 3D View




ATAK Civilian features 3D viewing of terrain and map items (DTED required). To enable 3D view, long press on the **[North Arrow]** to call out the additional controls menu and select [**3D**]. A tilt angle indicator will appear around the edge of the [**North Arrow**] when 3D view is active. Touch the screen with two fingers and simultaneously swipe up or down on the screen to tilt the view angle. Once the appropriate viewing angle is set, select the [**3D Lock**] button to retain this view while panning the map. While viewing the map from an angle, some map items will appear raised above the map surface if they have defined elevations.

## 3D Models

ATAK Civilian supports the use of 3D models. OBJ models and other types from products such as Pix4D can be imported via the Import Manager or can be manually placed in the atak/overlays folder prior to startup. If using Import Manager browse to the .OBJ file and import only that file, or browse to a .ZIP file that contains the .OBJ file (and others) and import only that file. If using manual placement to the atak/overlays folder, place a .ZIP file containing the .OBJ file (and others) into the directory and they will be imported on startup.

Once imported, a 3D Model icon will appear on the map. Zoom into the area of the icon until a loading ring appears. After the loading process has finished, the 3D model will be projected onto the map. Enable the map 3D View and tilt the view angle to see the 3D modeling. Loaded 3D models will appear as their own category in Overlay Manager and can be toggled on/off or removed from there.

Unclassified

## Placement

The user can enter locations of interest using the Point Dropper tool. Select the [**Point Dropper**] icon to place internationally standardized markers and other icons on the map, edit the data and share the markers with other network members.

### Self-Marker

The Self-Marker is displayed as a blue arrowhead at the user's current location. The options available on the Self-Marker radial are: Compass Rose, Polar Coordinate Entry, Fine Adjust/Enter Coordinate/MGRS Location, GPS Error, Range & Bearing Line, GPS Lock to Self, Tracking Breadcrumbs, Place a Marker at the user's current location and Details. Other TAK users appear on the display as a colored circle. The color of the circle represents the user's Team affiliation, with additional lettering inside the circle to identify the role the user on the team. Team Member markers that include a diagonal line indicate that the GPS location is not available. A solid icon indicated that the team member has GPS reception.

Available roles include: Team Member, Team Lead (designated by a TL in the center of the marker), Headquarters (HQ in center), Sniper (S), Medic (+), Forward Observer (FO), RTO (R) or K9 (K9). The options available when another user's Self-Marker is selected are: Inner Ring – Delete, Polar Coordinate Entry, Fine Adjust/Enter Coordinate/MGRS Location, Range & Bearing Line, GPS Lock on Friendly, Video Player (if available), Communication Options (if configured by that user), Custom Threat Rings, Tracking Breadcrumbs and Details.

Outer Ring (Communication Options) – Data Package, Email, SMS Messaging, GeoChat, VOIP and Cellular Phone, when available.

Unclassified

## Point Dropper

Selecting the [**Point Dropper**] icon will open the Point Dropper menu, containing marker symbology with one or more icon sets, a Recently Added button and an Iconset Manager button.

The Markers symbology affiliations are: Unknown, Neutral, Red and Friendly. Select the affiliation, then a location on the map interface to drop the marker. To add a marker by manually entering coordinates, long press on the map interface and enter the MGRS location. Change the standard naming convention by entering values into the custom prefix and index fields or leave blank to use the defaults. If values are entered, the next marker will be dropped with the prefix name and starting number(s) or letter(s) and every subsequent marker will be assigned the next consecutive number(s) or letter(s).

The user can select the mission specific pallet to open point options including Waypoint (WP), Sensor or Observation Point (OP).

The user can move between icon sets by either swiping in the icon set area or selecting on the [**Iconset Name**] field to bring up the Icon Pallet drop-down.

The last point placed is shown at the bottom of the Point Dropper window. The information for all recently placed points can be accessed by selecting the [**Clock**] icon. This displays the marker icon, name, coordinates, elevation and range & bearing information. The user can send, rename or remove any recently added markers by selecting the [**Arrows**] next to the marker to reveal [**SEND**], [**RENAME**] or [**DEL**] buttons.

Select the [**Iconset Manager**] (gear) button to add or delete icon sets or to set the default Marker Mapping.

## Radial Menus

**Unknown Object** | **Neutral Object** | **Red Object** | **Friendly Object** | **Spot Object**

The options available for Unknown Object Markers are: Delete, Polar Coordinate Entry, Fine Adjust/Enter Coordinate/MGRS Location, Range & Bearing Line, Lock On, Tasking, Custom Threat Rings, Tracking Breadcrumbs and Details.

The options available for Neutral Object Markers are: Delete, Polar Coordinate Entry, Fine Adjust/Enter Coordinate/MGRS Location, Range & Bearing Line, Lock On, Tasking, Custom Threat Rings, Tracking Breadcrumbs and Details.

The options available for Red Object Markers are: Delete, Polar Coordinate Entry, Compass Rose/Bullseye, Fine Adjust/Enter Coordinate/MGRS Location, Range & Bearing Line, Tasking, Custom Threat Rings, Tracking Breadcrumbs and Details.

The options available for Friendly Object Markers are: Delete, Polar Coordinate Entry, Fine Adjust/Enter Coordinate/MGRS Location, Range & Bearing Line, Lock On, Video, Contact Card, Custom Threat Rings, Tracking Breadcrumbs and Details. The Video radial will activate if a properly formatted packet that includes the link to the video feed is included. Select the video radial to open the associated video. The Contact Card can be selected to display additional communication options, including GeoChat, Email, VoIP, SMS Messaging and Cellular Phone, when available.

The options available for Spot Map are: Delete, Fine Adjust/Enter Coordinate/MGRS Location, Range & Bearing Line, Nav-To, Custom Threat Rings, Labels and Details.

The options for User Defined Iconsets are: Delete, Polar Coordinate Entry, Fine Adjust/Enter Coordinate/MGRS Location, Range & Bearing Line, Lock On, Tasking, Custom Threat Rings. Tracking Breadcrumbs and Details.

Select [**Details**] on the marker radial to make desired modifications, including: Coordinate, Elevation, Name, Type and Remarks. Selecting Marker Type opens a dialog box with extra categories. File attachments, including images, can be associated with the object by selecting the [**Paperclip**] icon. Once all the desired modifications have been made, the Marker can be sent to other network members using [**Send**]. The information can be broadcast to all members or sent to specific recipients. Select the [**Auto Send**] option to broadcast the marker to other TAK users on the network, with updates automatically sent about once every 60 seconds.



## Bloodhound Tool

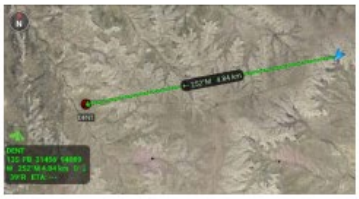
The Bloodhound Tool provides support for tracking and intercepting a map item. It allows the user to select two points on the map and/or map objects and display range & bearing information between the chosen tracker and the target.

Select the [**Bloodhound**] icon to open the Bloodhound Tool. A window will open, prompting the user to choose where to start by tapping the [**From Reticle**] (default = user's self marker) and where to bloodhound (track) to by tapping the [**To Reticle**].

Targets include map objects like other User's Self Markers, DPs, Markers, Shape center points, Range & Bearing endpoints and any other map objects. If the user selects a map location instead of an object as the target, Bloodhound will place a waypoint marker there. The self marker will then track towards the waypoint.

Select [**OK**] and Bloodhound will be activated.

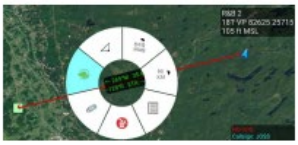
If either point moves, the green widget in the lower left will show the updated information. As the tracking object begins to navigate toward the target, the Estimated Time of Arrival (ETA) will update accordingly.



The green line showing the direct path from the tracker to the target will flash when the user-defined ETA outer threshold is reached (default = 6 minutes from target). The line will flash as the tracker continues toward the target until the next ETA threshold is reached (default = 3 minutes). The line will turn a flashing yellow until the final ETA threshold (default = 1 minute) is reached. The line then flashes red until the target is reached. Colors and thresholds can be modified in Settings > Tool Preferences > Bloodhound Preferences.

Selecting the green Bloodhound icon on the map will pan the map to the Bloodhound Range & Bearing Line. Disengage the Bloodhound Tool by selecting the [**Bloodhound**] icon on the toolbar.

## Multiple Bloodhound



To create multiple bloodhounds, selecting the Range and Bearing Tool and select the [**R&B Line**] icon. Select two markers on the map and once the R&B line is created, select the line to bring up the radial. Select the [**Bloodhound**] radial, and the bloodhound information will be displayed on the R&B Line itself.

If either point moves, the Bloodhound information shown on the R&B Line will be updated. As the tracking object begins to navigate toward the target, the Estimated Time of Arrival (ETA) will update accordingly.

## Go To

Select the [**Go To**] icon to enter details and navigate to a specific location on the map.

Select from the [**MGRS**] (military grid reference system), [**DD**] (decimal degrees), [**DM**] (degrees- minutes), [**DMS**] (degrees-minutes-seconds), [**UTM**] (Universal Transverse Mercator) or [**ADDR**] tabs on the Go To interface and enter the location data of interest. The address provider name appears beneath the Elevation Data when the user selects the [**ADDR**] tab.

The user can enter the Latitude, Longitude and Elevation in the space provided for [**MGRS**] , [**DD**], [**D-M**] or [**D-M-S**] searches. If DTED is installed, the elevation value can be automatically populated by tapping the [**Pull From DTED**] button.The user can select a desired marker type (Spot, Unknown, Neutral, Red, or Friendly) to be placed at the entered coordinates. If [**No Point**] is selected, the map will pan to the location but will not add a point.

**Note:** The address provider name appears beneath the Elevation Data when the user selects the [**ADDR**] tab.

The Address Lookup provider used for the ADDR tab can be configured in the Settings > Tool Preferences > Address Lookup Preferences.

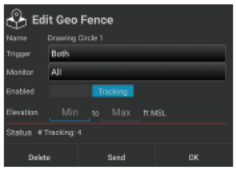




32

## Geofencing

The Geo Fence tool allows users to create a virtual fence that triggers entry/exit notifications if map items of interest cross the virtual boundary lines. The Geo Fence options are added to the existing drawing tools. After a shape has been added, the Geo Fence Tool can be accessed either by selecting the [**Geo Fence**] icon from the menu items or selecting it from the radial.




The Enabled Field slider will move to Tracking by default when a new Geo Fence window is created. Toggle the slider between Tracking and Off to enable/disable the Geo Fence. Use the Trigger field to define which types of Geo Fence breach to monitor. Choose between Entry, Exit or Both. Use the Monitor field to define which entities the Geo Fence will track.

Choose between TAK Users, Friendly, Hostile, Custom or All. Check the [**Specify Elevation**] box to enable the Elevation field, where elevation boundaries for the entities being tracked can be defined. Select the [**OK**] button to finish creating the fence. Select the [**Send**] button to create the fence and send it to another user. Select [**Delete**] to close the Create Geo Fence window and discard changes.

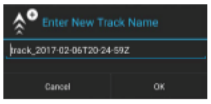
Alerts appear on the map interface. Selecting the [**Alert Notification**] will open the alerts menu, detailing the activity monitored in the user defined region. The default radius for monitoring users (filtered within the "Monitor" field) outside the Geo Fence is set at 75 km. This means the total area monitored begins at the farthest point from the center of the shape plus 75 km. If the user wishes to keep the Geo Fence, but disable tracking, the user can set the tracking [**Enabled**] to off in the Edit Window.

35

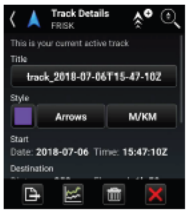
Unclassified

## Track History

The device's GPS can be used to track movements with the Track History tool. These tracked paths can be exported to a TAK server, to a route or to a KML, KMZ, GPX or CSV file. A GPS position must be established before tracking can begin.

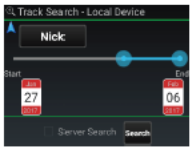



Selecting the [**Track History**] icon will open Track Details for the current active track. The track title, color and style can be modified. Initiate a new track by selecting the [**Add Track**] icon. Accept or edit the default track name and select the [**OK**] button to begin the new track. User location data is recorded as breadcrumbs in a new track file.

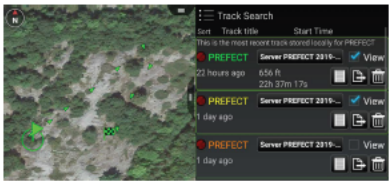



## Track Search

Use the Track Search function to view track information that has been previously saved locally or on a TAK Server. The tool searches the track database for matches against the specified time range and by user callsign. Matching tracks are displayed as a list, and can be selected to view on the map interface.




Select the [**Track Search**] icon to access the function. Specify callsign and time frame, check the box for Server Search (if desired), then select [**Search**]. The track list will appear. The query results can be sorted by Track Name or Start Time. Select any of the query results to move to that track. Once selected, the name, color, and style of a selected track can be modified or the track can be cleared. Convert a track to a TAK route or export it as a KML, KMZ, GPX or CSV file by selecting the desired track and then [**Export**]. Enter a file name then select [**Next**] and choose the export format. Select [**Done**] or [**Send**] when the export completes.



When viewing the track list, the Track History Toolbar will appear at the top of the screen. The options include [**Add a Track**], [**Multi-select**], [**Track Search**], [**Clear Tracks**] and [**Exit**]. The Track History List allows the user to select tracks of other users that have been saved on their device. The Track Search – Local Device allows the user to perform a tailored search for tracks meeting their criteria. The searching option allows the user to retrieve all the tracks on the device.

The Track History Breadcrumb and Settings can be configured in the Settings > Tools Preferences > Track History Preferences.

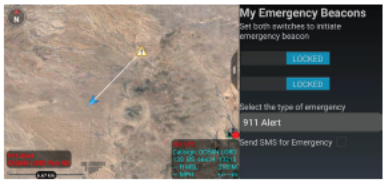
37

Unclassified

## Emergency Beacon

Select the [**Emergency Beacon**] icon to open the Emergency Beacon Tool.

The Emergency Beacon allows the user to indicate their need for assistance, the type of emergency and their location on the map. The type of emergency can be selected from the drop-down menu, before activation, and includes options for an Alert, Ring the Bell, Geo Fence Breached or In Contact.




Once the Emergency type has been selected and both switches have been enabled, the TAK Server broadcasts the announcements to all network contacts. Even if the user's device is turned off, the beacon will continue. Only when the user returns to the Emergency Beacon tool and turns off the switches will the beacon be canceled and removed. If the SMS for Emergency option has been configured, the alert will be sent via text message to the configured numbers.

71

[71] https://drive.google.com/file/d/1bo9WHadg3J3o55OLlx1mn3McqEJzvgrK/view

Home / Locate devices

# Locate devices

You can check the locations of the selected devices. Only the devices that have the location policy applied can be tracked.

To check the device locations, complete the following steps:

1. Navigate to **Device**.

2. On the "Device" page, click the checkbox for a device to check its location, and then click **Check Location**.

3. In the "Check Location" window, search by date and view the location history.

- Click **Export to GPX** to download a GPX file that includes detailed device location information. You can use a GPX viewer to open the file.

72

Home / Send device commands to users

# Send device commands to users

You can send device commands to the user's enrolled devices. For more information on each device command, see Sending device commands to devices.

To send device commands, complete the following steps:

1. Navigate to **User**.

2. On the "User" page, click the check box next to the user ID to send a device command to.

3. Click **Device Command** and select the supported OS platform (enrolled device).

4. In the "Device Command" window, select a desired device command.

5. In the "Request Command" window, click **OK**.

73

[72] https://docs.samsungknox.com/admin/knox-manage/locate-devices.htm
[73] https://docs.samsungknox.com/admin/knox-manage/send-commands-to-users-devices.htm

# Check the locations of devices

You can check the locations of the selected devices. Only the devices that have the location policy applied can be tracked.

> **NOTE** — You can only check a device's location if location data was collected at least once.

**IMPORTANT** — In order to track the location of Android 11 and 12 devices, the device user must grant the KM agent location access. This affects devices with the following deployment types:

- Employee-owned devices with a Work Profile
- Shared devices with a secondary account

You should inform users with these devices to allow the following access settings:

- Android 11:
  1. When the KM agent requests location access, the user must select **While using this app**.
  2. Then, they must go to **Work profile settings** >**Apps** >**Knox Manage** >**App permissions**, and set **Location** to **Allow all the time**.
- Android 12 and higher:
  - When the KM agent requests location access, the user must select **Precise** and **While using this app**.

1. Navigate to **Device**.
2. On the **Device** page, select one or more devices, and then click **Check Location**.
3. On the **Check Location** page, search by date. The view shows an interactive map of the devices and their location history.

On this page, you can inspect individual device information, as well as export their location history as as a GPX file.

# Device map

On the **Check Location** screen, a map displays the latest locations of all tracked devices. The map uses the following legend:

| Element | Meaning |
|---|---|
| | Active device |
| | Device with expired keepalive |
| | Cluster of 1–9 devices |
| | Cluster of 10–99 devices |
| | Cluster of 100–999 devices |
| | Cluster of 1000–9999 devices |

You can view an individual device's status by hovering over its pin . On hover, a tooltip lists the following information:

- Device name
- IMEI/MEID
- Serial Number
- Mobile Number
- User Name
- Last Location Scanned
- Organization Name
- Group Name
- Tag
- Platform & Management Type
- Model Name
- MAC Address
- Manufacturer

[74]

[74] https://docs.samsungknox.com/admin/knox-manage/check-the-locations-of-devices.htm.

59. For example, the exemplary Accused Products allow users to establish groups and to exchange messages via interaction with Samsung's servers which provide the Samsung Tactical, TAK, and ATAK applications and services and Samsung Knox applications and services, among other relevant applications and services. The exemplary Accused Products further allow users to retrieve map information from multiple sources including street-view maps, as well as satellite renderings.

Unclassified

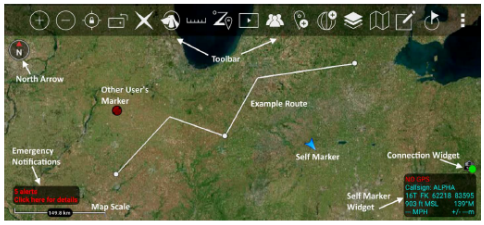
## ATAK Civilian Overview

The Civilian Team Awareness Kit for Android (ATAK Civilian) is a Government-off-the-Shelf (GOTS) software application and mapping framework for mobile devices. ATAK Civilian has been designed and developed to run on Android smart devices used in a first responder environment. The ATAK Civilian software application is an extensible moving map display that integrates imagery, map and overlay information to provide enhanced collaboration and Situational Awareness (SA) over a tactical meshed network. ATAK Civilian promotes information flow and communications from the field environment to command enterprise locations.

The first time ATAK Civilian is opened, or after a Clear Content, a passphrase is auto-generated to activate data encryption. The user can supply their own passphrase by using Settings > Show All Preferences > Device Preferences > Change Encryption Passphrase. Following this step, ATAK Civilian's End User License Agreement (EULA) must be accepted. Next, the user will be prompted to change their callsign and/or import preferences or data from a Mission Package. All changes/imports can always be updated later. Finally, the user can place their self-marker by following the instructions located in the lower right corner.

The toolbar runs along the top of the map display. The features whose icons form the center portion of the toolbar are discussed in individual sections of this guide. The three dots at the right of the toolbar provide additional menu items that appear in a drop-down menu. A Long Press on the map will toggle the toolbar between hidden and visible.

The North Arrow appears in the upper left and is used to control map orientation. It has two primary modes: North Up/Track Up (default) and Manual Map Rotation/Lock. While in North Up/Track Up Mode, single press on the [**North Arrow**] icon to cycle between the North Up and Track Up map orientation. Long press the [**North Arrow**] to call out the additional controls menu where the Manual Rotation/Lock and 3D features are available. Select the [**Rotation**] button to enter Manual Map Rotation/Lock Mode. When in Manual Map Rotation/Lock Mode, rotate the map orientation by pressing on the map with two fingers and pivoting them in the desired direction. Single press on the [**North Arrow**] to lock the screen orientation, signified by the appearance of the lock icon, and again to unlock the orientation for further adjustment. 3D controls are discussed in a separate section.




Select the [**Magnifier**] buttons to zoom in or out on the map. The map can also be zoomed by using two fingers on the screen to pinch and spread the map. Select the [**Back**] button to center the screen on the Self Marker or the [**Padlock**] icon to lock the center of the screen to the Self Marker. Select the [**Orientation**] icon to toggle the screen position between portrait and landscape.

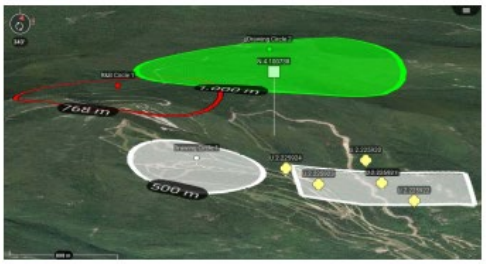
The optional connection widget indicates whether or not the user is connected to a TAK Server. This has a corresponding Android notification that provides the same information. Toggle this display on at Settings > Network Connections > Network Connections > Display Connection Widget.

Alerts and notifications are displayed in the lower left of the map interface.

The Map Scale displays a 1 inch to X mi/km reference on the map. The scale adjusts with the map when zoomed in and out. Hint windows are available to alert users to changes or make suggestions about the use of tools the first time they are opened.

5

## 3D View



ATAK Civilian features 3D viewing of terrain and map items (DTED required). To enable 3D view, long press on the **[North Arrow]** to call out the additional controls menu and select [**3D**]. A tilt angle indicator will appear around the edge of the [**North Arrow**] when 3D view is active. Touch the screen with two fingers and simultaneously swipe up or down on the screen to tilt the view angle. Once the appropriate viewing angle is set, select the [**3D Lock**] button to retain this view while panning the map. While viewing the map from an angle, some map items will appear raised above the map surface if they have defined elevations.

## 3D Models

ATAK Civilian supports the use of 3D models. OBJ models and other types from products such as Pix4D can be imported via the Import Manager or can be manually placed in the atak/overlays folder prior to startup. If using Import Manager browse to the .OBJ file and import only that file, or browse to a .ZIP file that contains the .OBJ file (and others) and import only that file. If using manual placement to the atak/overlays folder, place a .ZIP file containing the .OBJ file (and others) into the directory and they will be imported on startup.

Once imported, a 3D Model icon will appear on the map. Zoom into the area of the icon until a loading ring appears. After the loading process has finished, the 3D model will be projected onto the map. Enable the map 3D View and tilt the view angle to see the 3D modeling. Loaded 3D models will appear as their own category in Overlay Manager and can be toggled on/off or removed from there.

Unclassified

## Placement

The user can enter locations of interest using the Point Dropper tool. Select the [**Point Dropper**] icon to place internationally standardized markers and other icons on the map, edit the data and share the markers with other network members.

### Self-Marker

The Self-Marker is displayed as a blue arrowhead at the user's current location. The options available on the Self-Marker radial are: Compass Rose, Polar Coordinate Entry, Fine Adjust/Enter Coordinate/MGRS Location, GPS Error, Range & Bearing Line, GPS Lock to Self, Tracking Breadcrumbs, Place a Marker at the user's current location and Details. Other TAK users appear on the display as a colored circle. The color of the circle represents the user's Team affiliation, with additional lettering inside the circle to identify the role the user on the team. Team Member markers that include a diagonal line indicate that the GPS location is not available. A solid icon indicated that the team member has GPS reception.

Available roles include: Team Member, Team Lead (designated by a TL in the center of the marker), Headquarters (HQ in center), Sniper (S), Medic (+), Forward Observer (FO), RTO (R) or K9 (K9). The options available when another user's Self-Marker is selected are: Inner Ring – Delete, Polar Coordinate Entry, Fine Adjust/Enter Coordinate/MGRS Location, Range & Bearing Line, GPS Lock on Friendly, Video Player (if available), Communication Options (if configured by that user), Custom Threat Rings, Tracking Breadcrumbs and Details.

Outer Ring (Communication Options) – Data Package, Email, SMS Messaging, GeoChat, VOIP and Cellular Phone, when available.

Unclassified

## Radial Menus

**Unknown Object**

**Neutral Object**

**Red Object**

**Friendly Object**

**Spot Object**

The options available for Unknown Object Markers are: Delete, Polar Coordinate Entry, Fine Adjust/Enter Coordinate/MGRS Location, Range & Bearing Line, Lock On, Tasking, Custom Threat Rings, Tracking Breadcrumbs and Details.

The options available for Neutral Object Markers are: Delete, Polar Coordinate Entry, Fine Adjust/Enter Coordinate/MGRS Location, Range & Bearing Line, Lock On, Tasking, Custom Threat Rings, Tracking Breadcrumbs and Details.

The options available for Red Object Markers are: Delete, Polar Coordinate Entry, Compass Rose/Bullseye, Fine Adjust/Enter Coordinate/MGRS Location, Range & Bearing Line, Tasking, Custom Threat Rings, Tracking Breadcrumbs and Details.

The options available for Friendly Object Markers are: Delete, Polar Coordinate Entry, Fine Adjust/Enter Coordinate/MGRS Location, Range & Bearing Line, Lock On, Video, Contact Card, Custom Threat Rings, Tracking Breadcrumbs and Details. The Video radial will activate if a properly formatted packet that includes the link to the video feed is included. Select the video radial to open the associated video. The Contact Card can be selected to display additional communication options, including GeoChat, Email, VoIP, SMS Messaging and Cellular Phone, when available.

The options available for Spot Map are: Delete, Fine Adjust/Enter Coordinate/MGRS Location, Range & Bearing Line, Nav-To, Custom Threat Rings, Labels and Details.

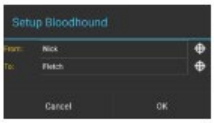
The options for User Defined Iconsets are: Delete, Polar Coordinate Entry, Fine Adjust/Enter Coordinate/MGRS Location, Range & Bearing Line, Lock On, Tasking, Custom Threat Rings. Tracking Breadcrumbs and Details.

Select [**Details**] on the marker radial to make desired modifications, including: Coordinate, Elevation, Name, Type and Remarks. Selecting Marker Type opens a dialog box with extra categories. File attachments, including images, can be associated with the object by selecting the [**Paperclip**] icon. Once all the desired modifications have been made, the Marker can be sent to other network members using [**Send**]. The information can be broadcast to all members or sent to specific recipients. Select the [**Auto Send**] option to broadcast the marker to other TAK users on the network, with updates automatically sent about once every 60 seconds.

## Bloodhound Tool

The Bloodhound Tool provides support for tracking and intercepting a map item. It allows the user to select two points on the map and/or map objects and display range & bearing information between the chosen tracker and the target.

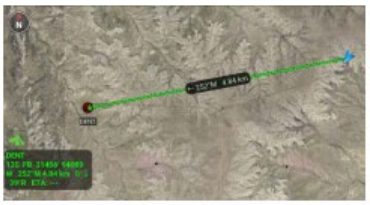
Select the [**Bloodhound**] icon to open the Bloodhound Tool. A window will open, prompting the user to choose where to start by tapping the [**From Reticle**] (default = user's self marker) and where to bloodhound (track) to by tapping the [**To Reticle**].




Targets include map objects like other User's Self Markers, DPs, Markers, Shape center points, Range & Bearing end-points and any other map objects. If the user selects a map location instead of an object as the target, Bloodhound will place a waypoint marker there. The self marker will then track towards the waypoint.

Select [**OK**] and Bloodhound will be activated.

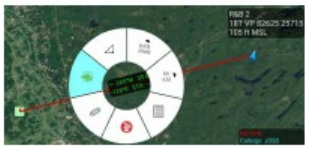
If either point moves, the green widget in the lower left will show the updated information. As the tracking object begins to navigate toward the target, the Estimated Time of Arrival (ETA) will update accordingly.



The green line showing the direct path from the tracker to the target will flash when the user-defined ETA outer threshold is reached (default = 6 minutes from target). The line will flash as the tracker continues toward the target until the next ETA threshold is reached (default = 3 minutes). The line will turn a flashing yellow until the final ETA threshold (default = 1 minute) is reached. The line then flashes red until the target is reached. Colors and thresholds can be modified in Settings > Tool Preferences > Bloodhound Preferences.

Selecting the green Bloodhound icon on the map will pan the map to the Bloodhound Range & Bearing Line. Disengage the Bloodhound Tool by selecting the [**Bloodhound**] icon on the toolbar.

## Multiple Bloodhound



To create multiple bloodhounds, selecting the Range and Bearing Tool and select the [**R&B Line**] icon. Select two markers on the map and once the R&B line is created, select the line to bring up the radial. Select the [**Bloodhound**] radial, and the bloodhound information will be displayed on the R&B Line itself.

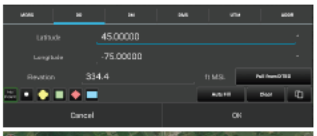
If either point moves, the Bloodhound information shown on the R&B Line will be updated. As the tracking object begins to navigate toward the target, the Estimated Time of Arrival (ETA) will update accordingly.



## Go To

Select the [**Go To**] icon to enter details and navigate to a specific location on the map.

Select from the [**MGRS**] (military grid reference system), [**DD**] (decimal degrees), [**DM**] (degrees - minutes), [**DMS**] (degrees-minutes-seconds), [**UTM**] (Universal Transverse Mercator) or [**ADDR**] tabs on the Go To interface and enter the location data of interest. The address provider name appears beneath the Elevation Data when the user selects the [**ADDR**] tab.



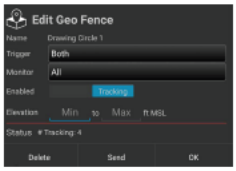

The user can enter the Latitude, Longitude and Elevation in the space provided for [**MGRS**] , [**DD**], [**D-M**] or [**D-M-S**] searches. If DTED is installed, the elevation value can be automatically populated by tapping the [**Pull From DTED**] button.The user can select a desired marker type (Spot, Unknown, Neutral, Red, or Friendly) to be placed at the entered coordinates. If [**No Point**] is selected, the map will pan to the location but will not add a point.

**Note:** The address provider name appears beneath the Elevation Data when the user selects the [**ADDR**] tab.

The Address Lookup provider used for the ADDR tab can be configured in the Settings > Tool Preferences > Address Lookup Preferences.

## Geofencing

The Geo Fence tool allows users to create a virtual fence that triggers entry/exit notifications if map items of interest cross the virtual boundary lines. The Geo Fence options are added to the existing drawing tools. After a shape has been added, the Geo Fence Tool can be accessed either by selecting the [**Geo Fence**] icon from the menu items or selecting it from the radial.




The Enabled Field slider will move to Tracking by default when a new Geo Fence window is created. Toggle the slider between Tracking and Off to enable/disable the Geo Fence. Use the Trigger field to define which types of Geo Fence breach to monitor. Choose between Entry, Exit or Both. Use the Monitor field to define which entities the Geo Fence will track.

Choose between TAK Users, Friendly, Hostile, Custom or All. Check the [**Specify Elevation**] box to enable the Elevation field, where elevation boundaries for the entities being tracked can be defined. Select the [**OK**] button to finish creating the fence. Select the [**Send**] button to create the fence and send it to another user. Select [**Delete**] to close the Create Geo Fence window and discard changes.

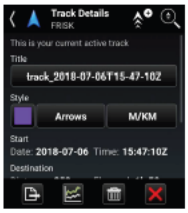
Alerts appear on the map interface. Selecting the [**Alert Notification**] will open the alerts menu, detailing the activity monitored in the user defined region. The default radius for monitoring users (filtered within the "Monitor" field) outside the Geo Fence is set at 75 km. This means the total area monitored begins at the farthest point from the center of the shape plus 75 km. If the user wishes to keep the Geo Fence, but disable tracking, the user can set the tracking [**Enabled**] to off in the Edit Window.

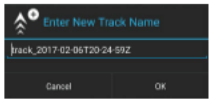
35

Unclassified

## Track History

The device's GPS can be used to track movements with the Track History tool. These tracked paths can be exported to a TAK server, to a route or to a KML, KMZ, GPX or CSV file. A GPS position must be established before tracking can begin.

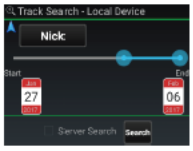


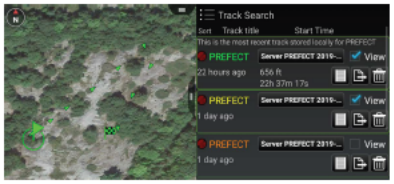

Selecting the [**Track History**] icon will open Track Details for the current active track. The track title, color and style can be modified. Initiate a new track by selecting the [**Add Track**] icon. Accept or edit the default track name and select the [**OK**] button to begin the new track. User location data is recorded as breadcrumbs in a new track file.

## Track Search

Use the Track Search function to view track information that has been previously saved locally or on a TAK Server. The tool searches the track database for matches against the specified time range and by user callsign. Matching tracks are displayed as a list, and can be selected to view on the map interface.




Select the [**Track Search**] icon to access the function. Specify callsign and time frame, check the box for Server Search (if desired), then select [**Search**]. The track list will appear. The query results can be sorted by Track Name or Start Time. Select any of the query results to move to that track. Once selected, the name, color, and style of a selected track can be modified or the track can be cleared. Convert a track to a TAK route or export it as a KML, KMZ, GPX or CSV file by selecting the desired track and then [**Export**]. Enter a file name then select [**Next**] and choose the export format. Select [**Done**] or [**Send**] when the export completes.

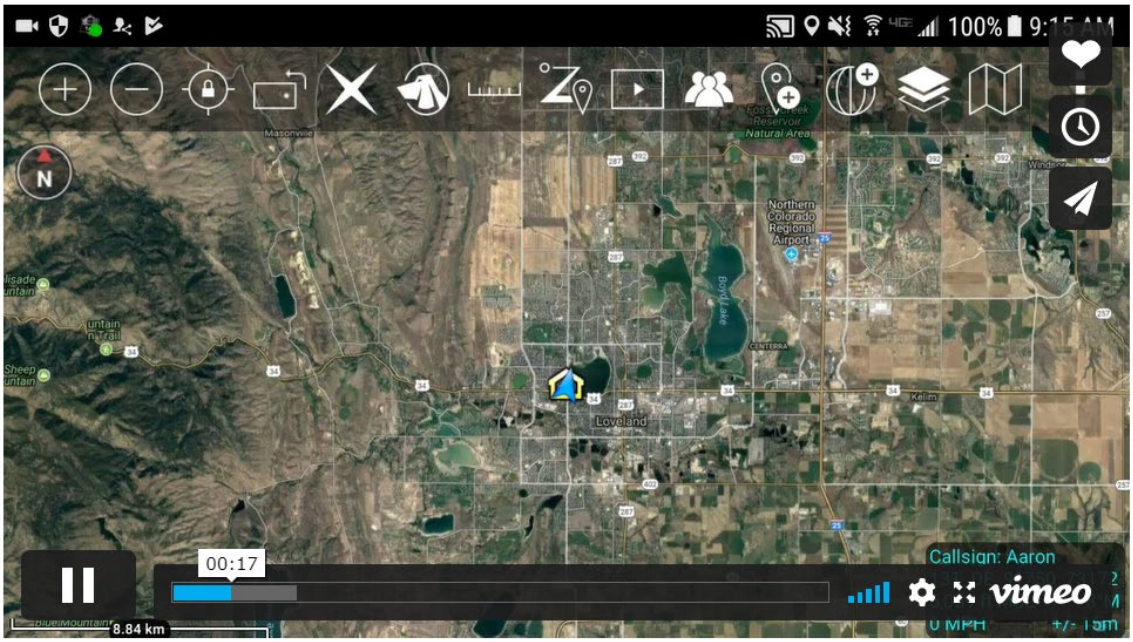


When viewing the track list, the Track History Toolbar will appear at the top of the screen. The options include [**Add a Track**], [**Multi-select**], [**Track Search**], [**Clear Tracks**] and [**Exit**]. The Track History List allows the user to select tracks of other users that have been saved on their device. The Track Search – Local Device allows the user to perform a tailored search for tracks meeting their criteria. The searching option allows the user to retrieve all the tracks on the device.

The Track History Breadcrumb and Settings can be configured in the Settings > Tools Preferences > Track History Preferences.

37 75

[75] https://drive.google.com/file/d/1bo9WHadg3J3o55OLlx1mn3McqEJzvgrK/view




[76]

[76] https://wiki.civtak.org/index.php?title=ATAK_Manual

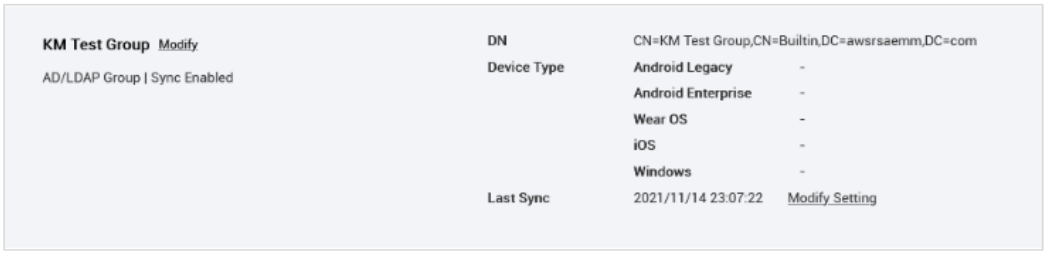
Home / View group details

# View group details

View each group's details by clicking a group name on the group list.

## Summary area

The summary area contains the information about the selected group such as group and user's device types.




- **Modify** — Change the group name.
- **Modify Setting** — Modify the sync settings of the current AD/LDAP group. In the **Modify Sync Setting** window, enter the following information:
  - **AD/LDAP Sync** — Enable or disable sync services.
  - **Sync Group Member** — Select whether sync all users or only the selected users of the group. (**Do Not Sync**, **Sync All**, **Sync Selected Only**)
  - **Profile/App Auto Apply** — Select when to apply a profile or application to a group member automatically. (**When Adding a User**, **When Deleting a User**, **When Deleting a Group**)

## Tab: User (for device groups)

The **User** tab for device groups shows the information of the user's devices and user accounts in the group.

- **Detail** — Move to the **User Details** page for the selected user. For more information on the **User Details** page, see Viewing the user details.

The following function buttons are available:

| Function button | Description |
|---|---|
| Send Email | Send templates or user notifications registered in Knox Manage to users via email. For more information, see Sending templates or user notifications to users via email. |
| Request Enrollment | Send installation guides to the selected users via email and SMS. For more information, see Sending enrollment guides to users via email and SMS.<br>**NOTE** — To send enrollment guides to users via SMS, the mobile numbers of the users must be registered to their accounts. |

# Tab: Device (for device groups)

The **Device** tab for user groups shows the device status and information of the user's devices in the group.

- **Detail** — Move to the **Device Details** page for the selected user's device. For more information on the **Device Details** page, see View details of a device.

The following function buttons are available:

| Function button | Description |
|---|---|
| Refresh | Update the list of devices. |
| Revert Column Settings | Restore the default visibility of all columns. |
| Add | Add a device from the device list to the group. For more information, see Adding devices to device groups. |
| Delete | Delete the selected device from the group. |
| ⚙ | Enable or disable a column in the device list by clicking this button > **Column**, and then selecting a column. |

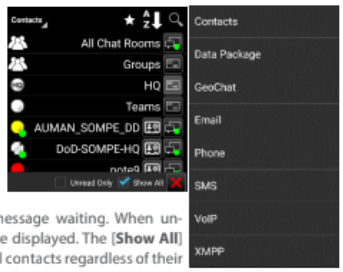
[77]

60. The exemplary Accused Products are programmed to form and join groups by transmitting messages.

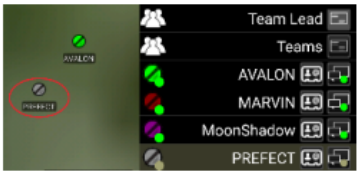
[77] https://docs.samsungknox.com/admin/knox-manage/view-details-of-group.htm.

## Contacts

The Contacts list includes a variety of ways in which a user may communicate with other users, such as GeoChat (ATAK Civilian's built in Chat capability), Data Packages, Email, Phone, SMS, VoIP and XMPP.



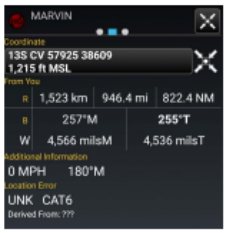

A default communication type (shown in the last column) may be selected and used until another type of communication is selected.




The Contacts list has two filters available at the bottom of the screen. The Unread Only box, when checked, will display only contacts with whom there are unread message waiting. When unchecked (default), all available contacts are displayed. The [**Show All**] box, when checked (default), will display all contacts regardless of their location. When unchecked, only contacts that are visible on current map screen will be displayed.

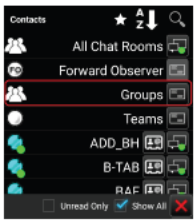
If a contact is no longer online, it will be indicated by changing the contact listing to a yellow color and the marker changes to gray both in the list and on the map.

Profile cards are accessed by selecting the second to last column in the Contacts list and are available for each contact. These contain additional information about that contact including: 1) role, software type and version installed, node type, default connector, last reported time, battery life; 2) location information, and 3) available types of communication.

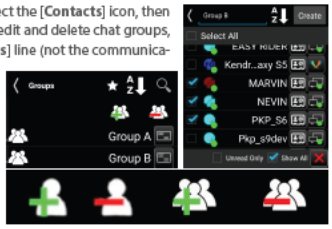


## GeoChat Group Management

Text-based Chat messages may be sent to active network members by using the GeoChat function. To enter GeoChat Group Management, select the [**Contacts**] icon and select [**GeoChat**] from the drop-down menu.

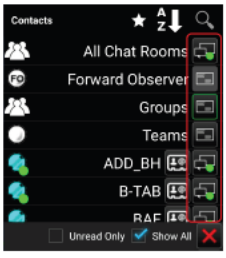



GeoChat Group Management is initiated through Contacts. Select the [**Contacts**] icon, then select GeoChat from the drop-down. The user can now create, edit and delete chat groups, as well as sub-groups. To create a chat group, select the [**Groups**] line (not the communications button). Select the [**Add Group**] icon to create the name of the group and add contacts to the group and then select [**Create**]. If a parent group is being created, no contacts need to be added at this level. To add a nested group, tap the parent group, select the [**Add Group**] icon to create the name of the sub-group and add contacts. Groups may be managed using the options to add/delete contacts or to add/delete GeoChat group.




To add users to a group, select the [**Groups**] line (not the communications button), then select the name of the group to add users. Select the [**Add Users**] icon. A window will open allowing the group creater to add users to the selected group. Select the [**Add**] button when all the users to be added are checked.

## GeoChat Messaging




Group and person-to-person messaging is available. To view messages from or send messages to an individual, tap on the desired contact's [**Communication**] icon. Selecting the [**Pan To**] icon, located at the top right of the call sign in an individual chat, will pan the map interface to that user's location. Select [**All Chat Rooms**] to view all messages from or send messages to those present on the network or TAK Server. Other groupings available for viewing or sending messages are: Forward Observer, Groups, HQ, K9, Medic, RTO, Sniper, Team Lead and Teams. If the user's current role is Forward Observer, HQ, K9, Medic, RTO, Sniper or Team Lead, that user can view or send messages to all other contacts with the same role. If a GeoChat message is sent from the top level of Teams, it will be sent to all contacts, similar to [**All Chat Rooms**].

When a sub-Team is chosen, messages can only be sent to that user's active (My Team) team color. When a parent group is chosen, messages are sent to all members of the parent group, as well as all of the sub-groups. When a sub-group is chosen, messages are sent only to members of the sub-group. Individuals within GeoChat may be removed from the Contacts menu by toggling the visibility of individuals or groups within Overlay Manager.

Unclassified

GeoChat Messaging (continued)

Selecting in the Free Text Entry area will open an onscreen keyboard. At the bottom of the Chat area are pre-defined messages that may be used to quickly create a message to send. Tap the current menu button to scroll through the different menus of canned messages, including: DFLT1, DFLT2, ASLT1, ASLT2, RECON1 and RECON2. These pre-defined messages present an easy way to transmit a brief message to other network members concerning position or other important communication. The pre-defined messages may be changed by long pressing on the button and changing its label and corresponding value.

A numbered red dot will appear on the [**Contacts**] icon when a message has been received successfully. The number denotes the number of unread messages that have been received. Select this icon to view the contact list. The user name who sent the message will appear with a numbered red dot next to their name. Alternatively, the text of the message can be read by dragging down from the top to see the Android notifications window. This notification will only stay available for a short time.

78

Home / **View group details**

# View group details

View each group's details by clicking a group name on the group list.

## Summary area

The summary area contains the information about the selected group such as group and user's device types.

**KM Test Group** Modify

AD/LDAP Group | Sync Enabled

| | | |
|---|---|---|
| DN | CN=KM Test Group,CN=Builtin,DC=awsrsaemm,DC=com | |
| Device Type | Android Legacy | - |
| | Android Enterprise | - |
| | Wear OS | - |
| | iOS | - |
| | Windows | - |
| Last Sync | 2021/11/14 23:07:22 | Modify Setting |

- **Modify** — Change the group name.
- **Modify Setting** — Modify the sync settings of the current AD/LDAP group. In the **Modify Sync Setting** window, enter the following information:
  - **AD/LDAP Sync** — Enable or disable sync services.
  - **Sync Group Member** — Select whether sync all users or only the selected users of the group. (**Do Not Sync**, **Sync All**, **Sync Selected Only**)
  - **Profile/App Auto Apply** — Select when to apply a profile or application to a group member automatically. (**When Adding a User**, **When Deleting a User**, **When Deleting a Group**)

[78] https://drive.google.com/file/d/1bo9WHadg3J3o55OLlx1mn3McqEJzvgrK/view

# Tab: User (for device groups)

The **User** tab for device groups shows the information of the user's devices and user accounts in the group.

- **Detail** — Move to the **User Details** page for the selected user. For more information on the **User Details** page, see Viewing the user details.

The following function buttons are available:

| Function button | Description |
|---|---|
| Send Email | Send templates or user notifications registered in Knox Manage to users via email. For more information, see Sending templates or user notifications to users via email. |
| Request Enrollment | Send installation guides to the selected users via email and SMS. For more information, see Sending enrollment guides to users via email and SMS.<br>**NOTE** — To send enrollment guides to users via SMS, the mobile numbers of the users must be registered to their accounts. |

# Tab: Device (for device groups)

The **Device** tab for user groups shows the device status and information of the user's devices in the group.

- **Detail** — Move to the **Device Details** page for the selected user's device. For more information on the **Device Details** page, see View details of a device.

The following function buttons are available:

| Function button | Description |
|---|---|
| Refresh | Update the list of devices. |
| Revert Column Settings | Restore the default visibility of all columns. |
| Add | Add a device from the device list to the group. For more information, see Adding devices to device groups. |
| Delete | Delete the selected device from the group. |
| ⚙ | Enable or disable a column in the device list by clicking this button > **Column**, and then selecting a column. |

[79]

[79] https://docs.samsungknox.com/admin/knox-manage/view-details-of-group.htm.

61. The exemplary Accused Products are further programmed to facilitate participation in the groups by communicating with one or more servers and sending to and receiving location information, as depicted below.

5

## Command and control

**Situational awareness**
The Galaxy S20 Tactical Edition integrates voice, video, and tactical data to provide a common operational picture of the battlespace. This complete and accurate real-time intelligence enhances the precision and effectiveness of your tactical teams.

**Tactical user experience**
Unique features found only on the Galaxy S20 Tactical Edition deliver fast and simple access to the information and applications operators need on-mission.

**Better intelligence**
The pro-grade 64 MP camera on the Galaxy S20 Tactical Edition allows you to discretely capture and share crisp high-resolution photo or 8K video intelligence, even in low light without the use of a flash. View and analyze intelligence in greater detail than ever before with the Galaxy S20 Tactical Edition's Dynamic AMOLED 2.0, a 120Hz[1] display.

**Extend your mission**
The Galaxy S20 Tactical Edition battery is 30% larger than the previous tactical solution and it's intelligent.[2] It optimizes your app usage in the field giving you extended power to complete the mission. When you need a recharge, Super Fast Charging[3] and fast Wireless Charging 2.0 give you power in a flash. And Wireless PowerShare allows you to easily charge a team member's phone in the field just by touching the devices.[4]

**Connect to tactical radios** - Protocols to support tactical radios and mission systems, out of the box.

**Tactical app quick launch** - Instantly expand or hide ATAK, APASS and other mission-critical applications at the push of a button.

**Night vision mode** – Turn on and off LED backlight when wearing night vision devices.

**Stealth mode** – Disable LTE and e-911 and mute all RF broadcasting for complete off-grid communications.

**Lock screen auto-rotate** - Unlock the device in landscape mode for easy access when mounted to the operator's chest.

**Auto-touch sensitivity** – Automatically adjust device operations to work with gloved hands.

# One device to meet all your mission requirements.

**Simple device management**
From device configuration, enrollment, customization and management to advanced mobile security controls and updates, Samsung has the mobility cloud services you need for every stage of the Galaxy S20 Tactical Edition lifecycle.[6] With Knox Services, you can keep pace and maintain control over devices and how they're used. You can manage devices in near real-time, configure settings, and remotely lock or wipe devices if lost or stolen, on the battlefield and anywhere else.

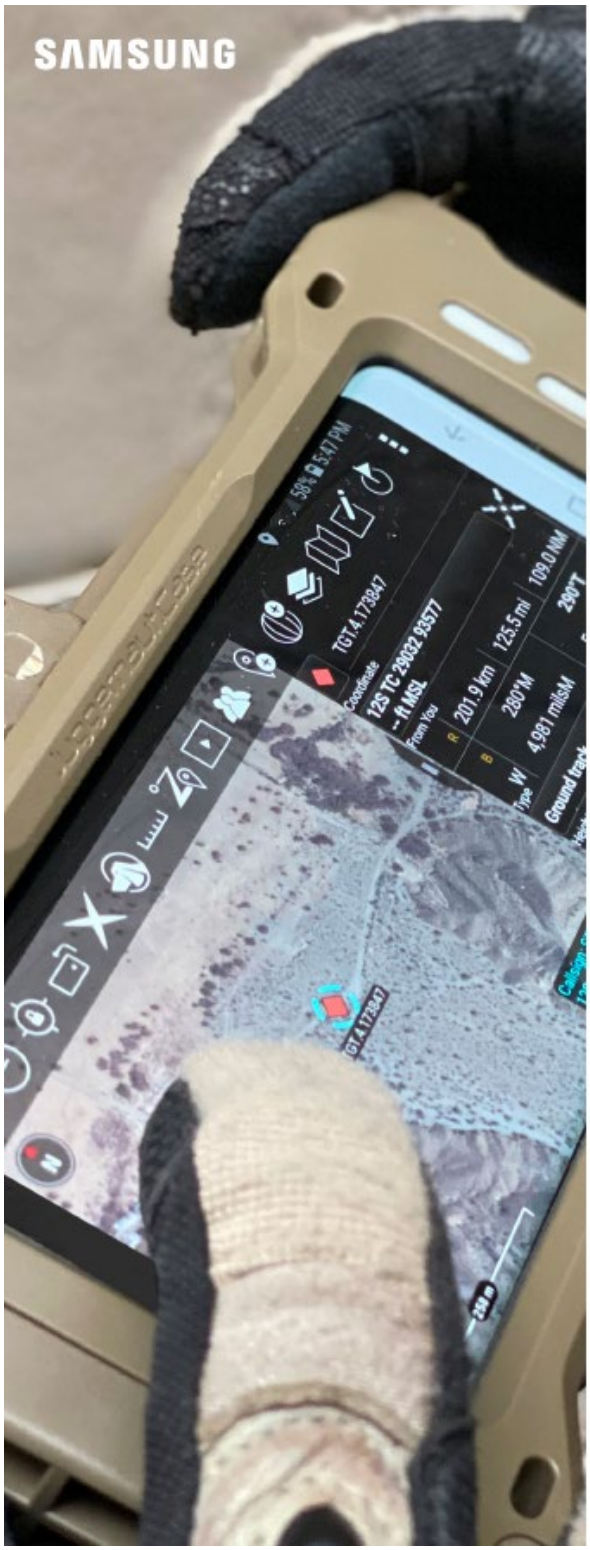
**Run mission apps and enterprise apps**
The Galaxy S20 Tactical Edition has a 64-bit Octa-Core processor with the speed and versatility to run multiple tactical applications in the field and enterprise applications everywhere else.

With Samsung DeX, connect your Galaxy S20 Tactical Edition to a monitor, keyboard and mouse for a desktop-like experience[5] ideally suited for mission planning, training, and everyday use. DeX gives you the power to work seamlessly across Microsoft Office Suite applications,[6] productivity apps, and virtual desktops with secure CAC-authenticated Virtual Desktop Infrastructure (VDI) sessions, all without a laptop.[7] And DeX-in-Vehicle transforms the Galaxy S20 Tactical Edition into a powerful in-vehicle computer.

**Open and secure**
The Galaxy S20 Tactical Edition is built on an open and secure Android operating system enabling seamless integration with a diverse ecosystem of tactical solution partners. Eliminate vulnerabilities with three software updates throughout the life of the device.

[80]

[80] https://www.pargovernment.com/tactical-sa/docs/S20_brochure.pdf




## Galaxy S20 Tactical Edition

# Mission-ready mobility. Proven by operators.

The Samsung Galaxy S20 Tactical Edition is the mission-ready military smartphone built and proven by operators in special operations. Based on the proven success of the S9 Tactical Edition for operators in the field, the S20 Tactical Edition is the only end user device you'll need for mission planning, training, operations and daily use.

### Persistent communications in any domain

**Purpose-built to connect to tactical radios** and mission systems out of the box, the Galaxy S20 Tactical Edition delivers a complete and accurate common operational picture. Run mission applications in the field and enterprise applications everywhere else with a single end user device for mission training, planning, operations and everyday use.

### Interoperable across devices and networks

**Pre-configured software, pre-loaded during the manufacturing process,** includes drivers to support tactical radios and mission-critical devices. Multi-ethernet capabilities provide dedicated connections to multiple mission systems including drone feeds, laser range finders, and external GPS. Support for current and next-generation networks includes Private SIM, 5G, WiFi 6 and CBRS. Allow or disallow USB peripherals based on product or vendor identifiers.

### Command and control

**Integrate voice, video and tactical data** for a complete view of the battlespace to enhance precision and effectiveness. Unique tactical features on the Galaxy S20 Tactical Edition include night-vision mode, stealth mode, lock screen autorotate, hostage negotiation mode, LTE band lock for consistent 4G connection, tactical application quick launch, to keep the operator focused on the objective, Standalone(5G)/Non-standalone (4G) modes to stay on preferred network. Preloaded tactical settings app. Ability to configure hotspot 2.0.

### Capture Intelligence

**A Pro-grade 64 MP camera** on the Galaxy S20 Tactical Edition enhances intel gathering, even in low-light environments without a flash. Capture high-resolution photos or sharp 8K video reconnaissance without giving away your position.

### Power to extend the mission

**Keep going wherever the mission takes you** with the Galaxy S20 Tactical Edition's intelligent2 4000mAh battery is 30% larger than the previous tactical solution and optimizes energy based on your device usage. Easily share power with a team member's smartphone in the field simply by touching devices using Wireless PowerShare.[4]

### One device to meet your requirements

**Run mission applications in the field** and enterprise applications everywhere else with the powerful and efficient Galaxy S20 Tactical Edition 64-bit Octa-Core processor. Connect your device to a monitor keyboard and mouse and use the power of Samsung DeX[5] for a desktop-like experience that is ideal for mission planning, training and everyday use. DeX-in-Vehicle transforms your Galaxy S20 Tactical Edition into an in-vehicle computer.

### Open and secure

**Enable a diverse ecosystem of tactical partners** with the open and secure Android operating system on the Galaxy S20 Tactical Edition. The all-new Tactical Settings feature simplifies device management, while Samsung Knox provides defense-grade security[6] from the hardware layer up and mission-specific device customization capabilities. The DualDAR architecture of the Galaxy S20 Tactical Edition provides two layers of encryption, even when the device is powered off, for securing up-to top secret level data on the device.

### Tested and proven

Samsung Galaxy Tactical Edition smartphones are tested and proven by special operators in the field. The Galaxy S20 Tactical Edition is certified to meet the most stringent requirements including NSA's CSFC Components List, NIAP Common Criteria/MDFPP, DODIN APL, FIPS 140-2, DISA Android 10 STIG, IP68 rating.

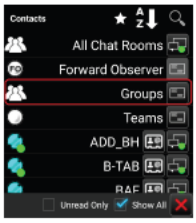
**Contact Us:** www.samsung.com/TacticalEdition

[81]

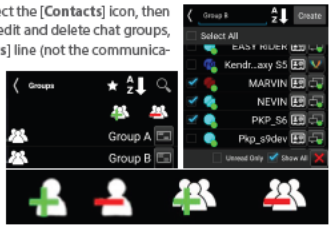
[81] https://image-us.samsung.com/SamsungUS/samsungbusiness/pdfs/flyer/S20_TE-salesflyer_FINAL_July_2021.pdf

## GeoChat Group Management

Text-based Chat messages may be sent to active network members by using the GeoChat function. To enter GeoChat Group Management, select the [**Contacts**] icon and select [**GeoChat**] from the drop-down menu.

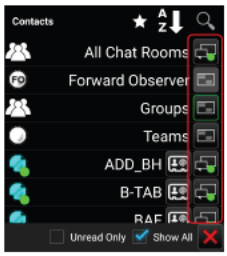



GeoChat Group Management is initiated through Contacts. Select the [**Contacts**] icon, then select GeoChat from the drop-down. The user can now create, edit and delete chat groups, as well as sub-groups. To create a chat group, select the [**Groups**] line (not the communications button). Select the [**Add Group**] icon to create the name of the group and add contacts to the group and then select [**Create**]. If a parent group is being created, no contacts need to be added at this level. To add a nested group, tap the parent group, select the [**Add Group**] icon to create the name of the sub-group and add contacts. Groups may be managed using the options to add/delete contacts or to add/delete GeoChat group.




To add users to a group, select the [**Groups**] line (not the communications button), then select the name of the group to add users. Select the [**Add Users**] icon. A window will open allowing the group creater to add users to the selected group. Select the [**Add**] button when all the users to be added are checked.

## GeoChat Messaging




Group and person-to-person messaging is available. To view messages from or send messages to an individual, tap on the desired contact's [**Communication**] icon. Selecting the [**Pan To**] icon, located at the top right of the call sign in an individual chat, will pan the map interface to that user's location. Select [**All Chat Rooms**] to view all messages from or send messages to those present on the network or TAK Server. Other groupings available for viewing or sending messages are: Forward Observer, Groups, HQ, K9, Medic, RTO, Sniper, Team Lead and Teams. If the user's current role is Forward Observer, HQ, K9, Medic, RTO, Sniper or Team Lead, that user can view or send messages to all other contacts with the same role. If a GeoChat message is sent from the top level of Teams, it will be sent to all contacts, similar to [**All Chat Rooms**].

When a sub-Team is chosen, messages can only be sent to that user's active (My Team) team color. When a parent group is chosen, messages are sent to all members of the parent group, as well as all of the sub-groups. When a sub-group is chosen, messages are sent only to members of the sub-group. Individuals within GeoChat may be removed from the Contacts menu by toggling the visibility of individuals or groups within Overlay Manager.





## GeoChat Messaging (continued)

Selecting in the Free Text Entry area will open an onscreen keyboard. At the bottom of the Chat area are pre-defined messages that may be used to quickly create a message to send. Tap the current menu button to scroll through the different menus of canned messages, including: DFLT1, DFLT2, ASLT1, ASLT2, RECON1 and RECON2. These pre-defined messages present an easy way to transmit a brief message to other network members concerning position or other important communication. The pre-defined messages may be changed by long pressing on the button and changing its label and corresponding value.

A numbered red dot will appear on the [**Contacts**] icon when a message has been received successfully. The number denotes the number of unread messages that have been received. Select this icon to view the contact list. The user name who sent the message will appear with a numbered red dot next to their name. Alternatively, the text of the message can be read by dragging down from the top to see the Android notifications window. This notification will only stay available for a short time.

## Go To

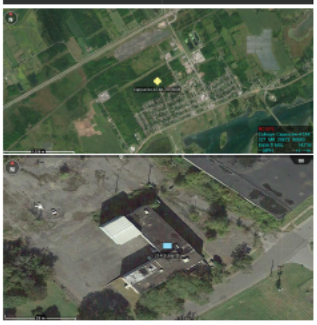
Select the [**Go To**] icon to enter details and navigate to a specific location on the map.

Select from the [**MGRS**] (military grid reference system), [**DD**] (decimal degrees), [**DM**] (degrees- minutes), [**DMS**] (degrees-minutes-seconds), [**UTM**] (Universal Transverse Mercator) or [**ADDR**] tabs on the Go To interface and enter the location data of interest. The address provider name appears beneath the Elevation Data when the user selects the [**ADDR**] tab.

The user can enter the Latitude, Longitude and Elevation in the space provided for [**MGRS**] , [**DD**], [**D-M**] or [**D-M-S**] searches. If DTED is installed, the elevation value can be automatically populated by tapping the [**Pull From DTED**] button.The user can select a desired marker type (Spot, Unknown, Neutral, Red, or Friendly) to be placed at the entered coordinates. If [**No Point**] is selected, the map will pan to the location but will not add a point.

**Note:** The address provider name appears beneath the Elevation Data when the user selects the [**ADDR**] tab.

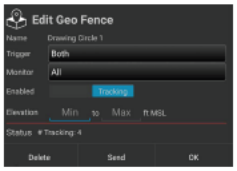
The Address Lookup provider used for the ADDR tab can be configured in the Settings > Tool Preferences > Address Lookup Preferences.



32

## Geofencing

The Geo Fence tool allows users to create a virtual fence that triggers entry/exit notifications if map items of interest cross the virtual boundary lines. The Geo Fence options are added to the existing drawing tools. After a shape has been added, the Geo Fence Tool can be accessed either by selecting the [**Geo Fence**] icon from the menu items or selecting it from the radial.




The Enabled Field slider will move to Tracking by default when a new Geo Fence window is created. Toggle the slider between Tracking and Off to enable/disable the Geo Fence. Use the Trigger field to define which types of Geo Fence breach to monitor. Choose between Entry, Exit or Both. Use the Monitor field to define which entities the Geo Fence will track.

Choose between TAK Users, Friendly, Hostile, Custom or All. Check the [**Specify Elevation**] box to enable the Elevation field, where elevation boundaries for the entities being tracked can be defined. Select the [**OK**] button to finish creating the fence. Select the [**Send**] button to create the fence and send it to another user. Select [**Delete**] to close the Create Geo Fence window and discard changes.

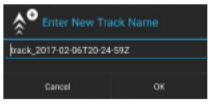
Alerts appear on the map interface. Selecting the [**Alert Notification**] will open the alerts menu, detailing the activity monitored in the user defined region. The default radius for monitoring users (filtered within the "Monitor" field) outside the Geo Fence is set at 75 km. This means the total area monitored begins at the farthest point from the center of the shape plus 75 km. If the user wishes to keep the Geo Fence, but disable tracking, the user can set the tracking [**Enabled**] to off in the Edit Window.

35

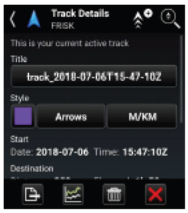
Unclassified

## Track History

The device's GPS can be used to track movements with the Track History tool. These tracked paths can be exported to a TAK server, to a route or to a KML, KMZ, GPX or CSV file. A GPS position must be established before tracking can begin.

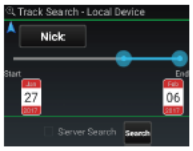



Selecting the [**Track History**] icon will open Track Details for the current active track. The track title, color and style can be modified. Initiate a new track by selecting the [**Add Track**] icon. Accept or edit the default track name and select the [**OK**] button to begin the new track. User location data is recorded as breadcrumbs in a new track file.

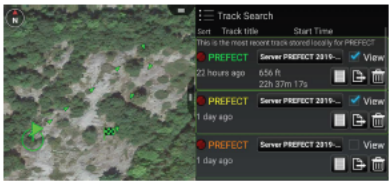



## Track Search

Use the Track Search function to view track information that has been previously saved locally or on a TAK Server. The tool searches the track database for matches against the specified time range and by user callsign. Matching tracks are displayed as a list, and can be selected to view on the map interface.




Select the [**Track Search**] icon to access the function. Specify callsign and time frame, check the box for Server Search (if desired), then select [**Search**]. The track list will appear. The query results can be sorted by Track Name or Start Time. Select any of the query results to move to that track. Once selected, the name, color, and style of a selected track can be modified or the track can be cleared. Convert a track to a TAK route or export it as a KML, KMZ, GPX or CSV file by selecting the desired track and then [**Export**]. Enter a file name then select [**Next**] and choose the export format. Select [**Done**] or [**Send**] when the export completes.



When viewing the track list, the Track History Toolbar will appear at the top of the screen. The options include [**Add a Track**], [**Multi-select**], [**Track Search**], [**Clear Tracks**] and [**Exit**]. The Track History List allows the user to select tracks of other users that have been saved on their device. The Track Search – Local Device allows the user to perform a tailored search for tracks meeting their criteria. The searching option allows the user to retrieve all the tracks on the device.

The Track History Breadcrumb and Settings can be configured in the Settings > Tools Preferences > Track History Preferences.

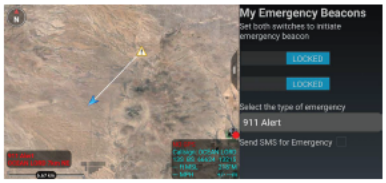
37

Unclassified

## Emergency Beacon

Select the [**Emergency Beacon**] icon to open the Emergency Beacon Tool.

The Emergency Beacon allows the user to indicate their need for assistance, the type of emergency and their location on the map. The type of emergency can be selected from the drop-down menu, before activation, and includes options for an Alert, Ring the Bell, Geo Fence Breached or In Contact.




Once the Emergency type has been selected and both switches have been enabled, the TAK Server broadcasts the announcements to all network contacts. Even if the user's device is turned off, the beacon will continue. Only when the user returns to the Emergency Beacon tool and turns off the switches will the beacon be canceled and removed. If the SMS for Emergency option has been configured, the alert will be sent via text message to the configured numbers.

82

[82] https://drive.google.com/file/d/1bo9WHadg3J3o55OLlx1mn3McqEJzvgrK/view

# Check the locations of devices

You can check the locations of the selected devices. Only the devices that have the location policy applied can be tracked.

> **NOTE** — You can only check a device's location if location data was collected at least once.

**IMPORTANT** — In order to track the location of Android 11 and 12 devices, the device user must grant the KM agent location access. This affects devices with the following deployment types:

- Employee-owned devices with a Work Profile
- Shared devices with a secondary account

You should inform users with these devices to allow the following access settings:

- Android 11:
  1. When the KM agent requests location access, the user must select **While using this app**.
  2. Then, they must go to **Work profile settings** >**Apps** >**Knox Manage** >**App permissions**, and set **Location** to **Allow all the time**.
- Android 12 and higher:
  - When the KM agent requests location access, the user must select **Precise** and **While using this app**.

1. Navigate to **Device**.
2. On the **Device** page, select one or more devices, and then click **Check Location**.
3. On the **Check Location** page, search by date. The view shows an interactive map of the devices and their location history.

On this page, you can inspect individual device information, as well as export their location history as as a GPX file.

# Device map

On the **Check Location** screen, a map displays the latest locations of all tracked devices. The map uses the following legend:

| Element | Meaning |
|---|---|
| | Active device |
| | Device with expired keepalive |
| | Cluster of 1–9 devices |
| | Cluster of 10–99 devices |
| | Cluster of 100–999 devices |
| | Cluster of 1000–9999 devices |

You can view an individual device's status by hovering over its pin . On hover, a tooltip lists the following information:

- Device name
- IMEI/MEID
- Serial Number
- Mobile Number
- User Name
- Last Location Scanned
- Organization Name
- Group Name
- Tag
- Platform & Management Type
- Model Name
- MAC Address
- Manufacturer

[83]

[83] https://docs.samsungknox.com/admin/knox-manage/check-the-locations-of-devices.htm.

62. This location information is presented on interactive displays on the exemplary Accused Products which include interactive maps and a plurality of user selectable symbols corresponding to other devices. These symbols are positioned on the map at positions corresponding to the locations of the other devices as depicted below.

# One device to meet all your mission requirements.

**Simple device management**
From device configuration, enrollment, customization and management to advanced mobile security controls and updates, Samsung has the mobility cloud services you need for every stage of the Galaxy S20 Tactical Edition lifecycle.[8] With Knox Services, you can keep pace and maintain control over devices and how they're used. You can manage devices in near real-time, configure settings, and remotely lock or wipe devices if lost or stolen, on the battlefield and anywhere else.

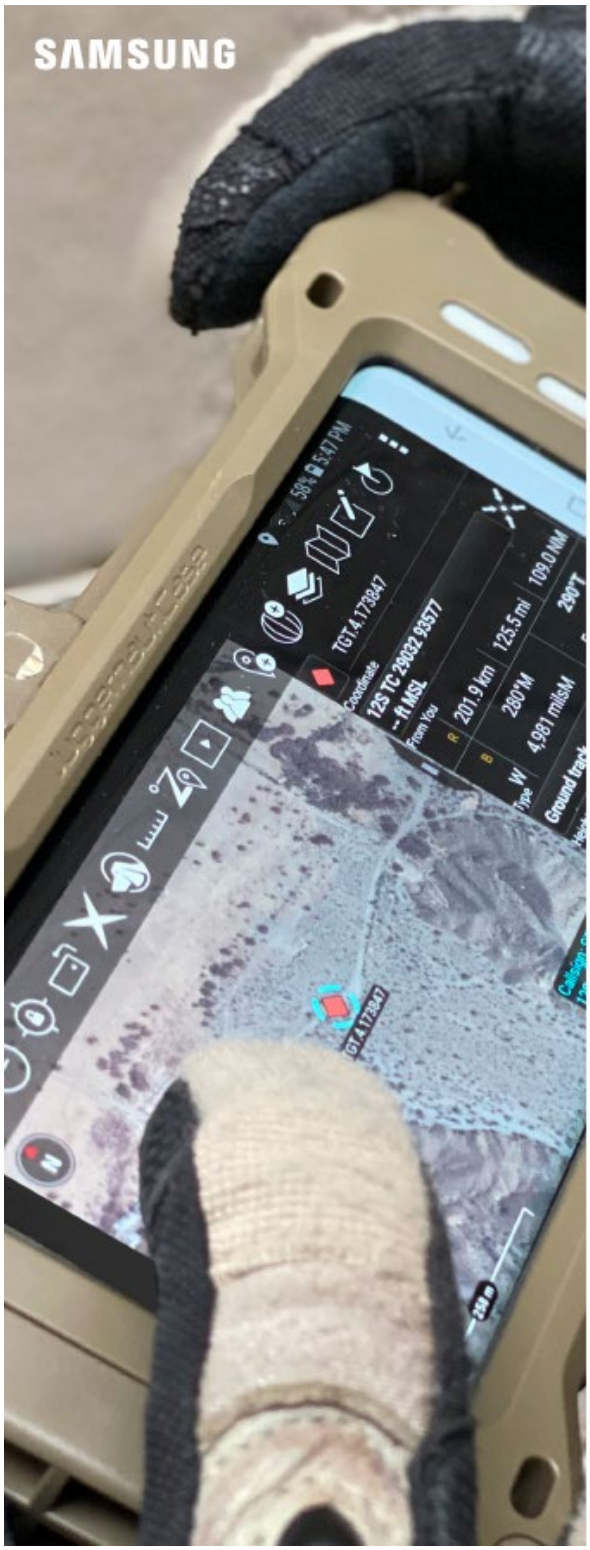
**Run mission apps and enterprise apps**
The Galaxy S20 Tactical Edition has a 64-bit Octa-Core processor with the speed and versatility to run multiple tactical applications in the field and enterprise applications everywhere else.

With Samsung DeX, connect your Galaxy S20 Tactical Edition to a monitor, keyboard and mouse for a desktop-like experience[5] ideally suited for mission planning, training, and everyday use. DeX gives you the power to work seamlessly across Microsoft Office Suite applications,[6] productivity apps, and virtual desktops with secure CAC-authenticated Virtual Desktop Infrastructure (VDI) sessions, all without a laptop.[7] And DeX-in-Vehicle transforms the Galaxy S20 Tactical Edition into a powerful in-vehicle computer.

**Open and secure**
The Galaxy S20 Tactical Edition is built on an open and secure Android operating system enabling seamless integration with a diverse ecosystem of tactical solution partners. Eliminate vulnerabilities with three software updates throughout the life of the device.

84

[84] https://www.pargovernment.com/tactical-sa/docs/S20_brochure.pdf




## Galaxy S20 Tactical Edition

# Mission-ready mobility. Proven by operators.

The Samsung Galaxy S20 Tactical Edition is the mission-ready military smartphone built and proven by operators in special operations. Based on the proven success of the S9 Tactical Edition for operators in the field, the S20 Tactical Edition is the only end user device you'll need for mission planning, training, operations and daily use.

### Persistent communications in any domain

**Purpose-built to connect to tactical radios** and mission systems out of the box, the Galaxy S20 Tactical Edition delivers a complete and accurate common operational picture. Run mission applications in the field and enterprise applications everywhere else with a single end user device for mission training, planning, operations and everyday use.

### Interoperable across devices and networks

**Pre-configured software, pre-loaded during the manufacturing process,** includes drivers to support tactical radios and mission-critical devices. Multi-ethernet capabilities provide dedicated connections to multiple mission systems including drone feeds, laser range finders, and external GPS. Support for current and next-generation networks includes Private SIM, 5G, WiFi 6 and CBRS. Allow or disallow USB peripherals based on product or vendor identifiers.

### Command and control

**Integrate voice, video and tactical data** for a complete view of the battlespace to enhance precision and effectiveness. Unique tactical features on the Galaxy S20 Tactical Edition include night-vision mode, stealth mode, lock screen autorotate, hostage negotiation mode, LTE band lock for consistent 4G connection, tactical application quick launch, to keep the operator focused on the objective, Standalone(5G)/Non-standalone (4G) modes to stay on preferred network. Preloaded tactical settings app. Ability to configure hotspot 2.0.

### Capture Intelligence

**A Pro-grade 64 MP camera** on the Galaxy S20 Tactical Edition enhances intel gathering, even in low-light environments without a flash. Capture high-resolution photos or sharp 8K video reconnaissance without giving away your position.

### Power to extend the mission

**Keep going wherever the mission takes you** with the Galaxy S20 Tactical Edition's intelligent2 4000mAh battery is 30% larger than the previous tactical solution and optimizes energy based on your device usage. Easily share power with a team member's smartphone in the field simply by touching devices using Wireless PowerShare.[4]

### One device to meet your requirements

**Run mission applications in the field** and enterprise applications everywhere else with the powerful and efficient Galaxy S20 Tactical Edition 64-bit Octa-Core processor. Connect your device to a monitor keyboard and mouse and use the power of Samsung DeX[5] for a desktop-like experience that is ideal for mission planning, training and everyday use. DeX-in-Vehicle transforms your Galaxy S20 Tactical Edition into an in-vehicle computer.

### Open and secure

**Enable a diverse ecosystem of tactical partners** with the open and secure Android operating system on the Galaxy S20 Tactical Edition. The all-new Tactical Settings feature simplifies device management, while Samsung Knox provides defense-grade security[6] from the hardware layer up and mission-specific device customization capabilities. The DualDAR architecture of the Galaxy S20 Tactical Edition provides two layers of encryption, even when the device is powered off, for securing up-to top secret level data on the device.

### Tested and proven

Samsung Galaxy Tactical Edition smartphones are tested and proven by special operators in the field. The Galaxy S20 Tactical Edition is certified to meet the most stringent requirements including NSA's CSFC Components List, NIAP Common Criteria/MDFPP, DODIN APL, FIPS 140-2, DISA Android 10 STIG, IP68 rating.

**Contact Us:** www.samsung.com/TacticalEdition

85

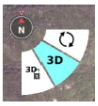
[85] https://image-us.samsung.com/SamsungUS/samsungbusiness/pdfs/flyer/S20_TE-salesflyer_FINAL_July_2021.pdf

## ATAK Civilian Overview

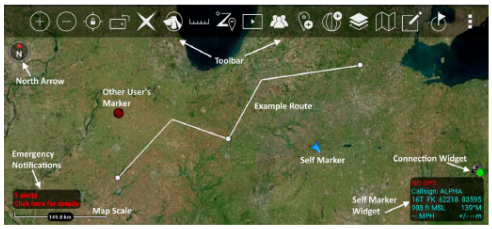
The Civilian Team Awareness Kit for Android (ATAK Civilian) is a Government-off-the-Shelf (GOTS) software application and mapping framework for mobile devices. ATAK Civilian has been designed and developed to run on Android smart devices used in a first responder environment. The ATAK Civilian software application is an extensible moving map display that integrates imagery, map and overlay information to provide enhanced collaboration and Situational Awareness (SA) over a tactical meshed network. ATAK Civilian promotes information flow and communications from the field environment to command enterprise locations.

The first time ATAK Civilian is opened, or after a Clear Content, a passphrase is auto-generated to activate data encryption. The user can supply their own passphrase by using Settings > Show All Preferences > Device Preferences > Change Encryption Passphrase. Following this step, ATAK Civilian's End User License Agreement (EULA) must be accepted. Next, the user will be prompted to change their callsign and/or import preferences or data from a Mission Package. All changes/imports can always be updated later. Finally, the user can place their self-marker by following the instructions located in the lower right corner.

The toolbar runs along the top of the map display. The features whose icons form the center portion of the toolbar are discussed in individual sections of this guide. The three dots at the right of the toolbar provide additional menu items that appear in a drop-down menu. A Long Press on the map will toggle the toolbar between hidden and visible.




The North Arrow appears in the upper left and is used to control map orientation. It has two primary modes: North Up/Track Up (default) and Manual Map Rotation/Lock. While in North Up/Track Up Mode, single press on the [**North Arrow**] icon to cycle between the North Up and Track Up map orientation. Long press the [**North Arrow**] to call out the additional controls menu where the Manual Rotation/Lock and 3D features are available. Select the [**Rotation**] button to enter Manual Map Rotation/Lock Mode. When in Manual Map Rotation/Lock Mode, rotate the map orientation by pressing on the map with two fingers and pivoting them in the desired direction. Single press on the [**North Arrow**] to lock the screen orientation, signified by the appearance of the lock icon, and again to unlock the orientation for further adjustment. 3D controls are discussed in a separate section.




Select the [**Magnifier**] buttons to zoom in or out on the map. The map can also be zoomed by using two fingers on the screen to pinch and spread the map. Select the [**Back**] button to center the screen on the Self Marker or the [**Padlock**] icon to lock the center of the screen to the Self Marker. Select the [**Orientation**] icon to toggle the screen position between portrait and landscape.

The optional connection widget indicates whether or not the user is connected to a TAK Server. This has a corresponding Android notification that provides the same information. Toggle this display on at Settings > Network Connections > Network Connections > Display Connection Widget.

Alerts and notifications are displayed in the lower left of the map interface.

The Map Scale displays a 1 inch to X mi/km reference on the map. The scale adjusts with the map when zoomed in and out. Hint windows are available to alert users to changes or make suggestions about the use of tools the first time they are opened.

## Go To

Select the [**Go To**] icon to enter details and navigate to a specific location on the map.

Select from the [**MGRS**] (military grid reference system), [**DD**] (decimal degrees), [**DM**] (degrees- minutes), [**DMS**] (degrees-minutes-seconds), [**UTM**] (Universal Transverse Mercator) or [**ADDR**] tabs on the Go To interface and enter the location data of interest. The address provider name appears beneath the Elevation Data when the user selects the [**ADDR**] tab.

The user can enter the Latitude, Longitude and Elevation in the space provided for [**MGRS**] , [**DD**], [**D-M**] or [**D-M-S**] searches. If DTED is installed, the elevation value can be automatically populated by tapping the [**Pull From DTED**] button.The user can select a desired marker type (Spot, Unknown, Neutral, Red, or Friendly) to be placed at the entered coordinates. If [**No Point**] is selected, the map will pan to the location but will not add a point.

**Note:** The address provider name appears beneath the Elevation Data when the user selects the [**ADDR**] tab.

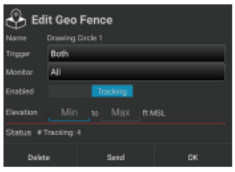
The Address Lookup provider used for the ADDR tab can be configured in the Settings > Tool Preferences > Address Lookup Preferences.



32

## Geofencing

The Geo Fence tool allows users to create a virtual fence that triggers entry/exit notifications if map items of interest cross the virtual boundary lines. The Geo Fence options are added to the existing drawing tools. After a shape has been added, the Geo Fence Tool can be accessed either by selecting the [**Geo Fence**] icon from the menu items or selecting it from the radial.




The Enabled Field slider will move to Tracking by default when a new Geo Fence window is created. Toggle the slider between Tracking and Off to enable/disable the Geo Fence. Use the Trigger field to define which types of Geo Fence breach to monitor. Choose between Entry, Exit or Both. Use the Monitor field to define which entities the Geo Fence will track.

Choose between TAK Users, Friendly, Hostile, Custom or All. Check the [**Specify Elevation**] box to enable the Elevation field, where elevation boundaries for the entities being tracked can be defined. Select the [**OK**] button to finish creating the fence. Select the [**Send**] button to create the fence and send it to another user. Select [**Delete**] to close the Create Geo Fence window and discard changes.

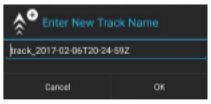
Alerts appear on the map interface. Selecting the [**Alert Notification**] will open the alerts menu, detailing the activity monitored in the user defined region. The default radius for monitoring users (filtered within the "Monitor" field) outside the Geo Fence is set at 75 km. This means the total area monitored begins at the farthest point from the center of the shape plus 75 km. If the user wishes to keep the Geo Fence, but disable tracking, the user can set the tracking [**Enabled**] to off in the Edit Window.

35

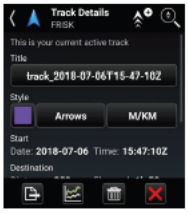
Unclassified

## Track History

The device's GPS can be used to track movements with the Track History tool. These tracked paths can be exported to a TAK server, to a route or to a KML, KMZ, GPX or CSV file. A GPS position must be established before tracking can begin.

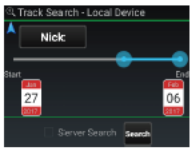



Selecting the [**Track History**] icon will open Track Details for the current active track. The track title, color and style can be modified. Initiate a new track by selecting the [**Add Track**] icon. Accept or edit the default track name and select the [**OK**] button to begin the new track. User location data is recorded as breadcrumbs in a new track file.

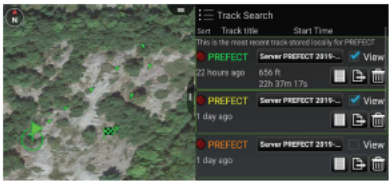



## Track Search

Use the Track Search function to view track information that has been previously saved locally or on a TAK Server. The tool searches the track database for matches against the specified time range and by user callsign. Matching tracks are displayed as a list, and can be selected to view on the map interface.




Select the [**Track Search**] icon to access the function. Specify callsign and time frame, check the box for Server Search (if desired), then select [**Search**]. The track list will appear. The query results can be sorted by Track Name or Start Time. Select any of the query results to move to that track. Once selected, the name, color, and style of a selected track can be modified or the track can be cleared. Convert a track to a TAK route or export it as a KML, KMZ, GPX or CSV file by selecting the desired track and then [**Export**]. Enter a file name then select [**Next**] and choose the export format. Select [**Done**] or [**Send**] when the export completes.



When viewing the track list, the Track History Toolbar will appear at the top of the screen. The options include [**Add a Track**], [**Multi-select**], [**Track Search**], [**Clear Tracks**] and [**Exit**]. The Track History List allows the user to select tracks of other users that have been saved on their device. The Track Search – Local Device allows the user to perform a tailored search for tracks meeting their criteria. The searching option allows the user to retrieve all the tracks on the device.

The Track History Breadcrumb and Settings can be configured in the Settings > Tools Preferences > Track History Preferences.

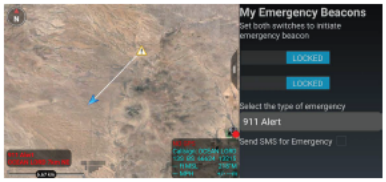
37

Unclassified

## Emergency Beacon

Select the [**Emergency Beacon**] icon to open the Emergency Beacon Tool.

The Emergency Beacon allows the user to indicate their need for assistance, the type of emergency and their location on the map. The type of emergency can be selected from the drop-down menu, before activation, and includes options for an Alert, Ring the Bell, Geo Fence Breached or In Contact.




Once the Emergency type has been selected and both switches have been enabled, the TAK Server broadcasts the announcements to all network contacts. Even if the user's device is turned off, the beacon will continue. Only when the user returns to the Emergency Beacon tool and turns off the switches will the beacon be canceled and removed. If the SMS for Emergency option has been configured, the alert will be sent via text message to the configured numbers.

86

[86] https://drive.google.com/file/d/1bo9WHadg3J3o55OLlx1mn3McqEJzvgrK/view

# Device map

On the **Check Location** screen, a map displays the latest locations of all tracked devices. The map uses the following legend:

| Element | Meaning |
|---|---|
| | Active device |
| | Device with expired keepalive |
| | Cluster of 1–9 devices |
| | Cluster of 10–99 devices |
| | Cluster of 100–999 devices |
| | Cluster of 1000–9999 devices |

You can view an individual device's status by hovering over its pin . On hover, a tooltip lists the following information:

- Device name
- IMEI/MEID
- Serial Number
- Mobile Number
- User Name
- Last Location Scanned
- Organization Name
- Group Name
- Tag
- Platform & Management Type
- Model Name
- MAC Address
- Manufacturer

[87]

[87] https://docs.samsungknox.com/admin/knox-manage/check-the-locations-of-devices.htm.

63. The exemplary Accused Products are further programmed to permit users to request and display additional maps by, for example, moving the map screen and/or by selecting satellite image maps. The exemplary Accused Products are further programmed to permit interaction with the display where a user may select one or more symbols and where the exemplary Accused Products further permit data to be sent to other devices based on that interaction.

64. AGIS Software has suffered damages as a result of Defendants' direct and indirect infringement of the '829 Patent in an amount to be proved at trial.

65. AGIS Software has suffered, and will continue to suffer, irreparable harm as a result of Defendants' infringement of the '829 Patent for which there is no adequate remedy at law unless Defendants' infringement is enjoined by this Court.

66. Defendants have committed and continue to commit acts of infringement that Defendants actually knew or should have known constituted an unjustifiably high risk of infringement of at least one valid and enforceable claim of the '829 Patent. Defendants' infringement of the '829 Patent has been and continues to be willful, entitling AGIS Software to an award of treble damages, reasonable attorney fees, and costs in bringing this action.

## COUNT IV
**(Infringement of the '123 Patent)**

67. Paragraphs 1 through 19 are incorporated herein by reference as if fully set forth in their entireties.

68. AGIS Software has not licensed or otherwise authorized Defendants to make, use, offer for sale, sell, or import any products that embody the inventions of the '123 Patent.

69. Defendants have and continue to directly infringe at least claim 23 of the '123 Patent, either literally or under the doctrine of equivalents, by making, using, selling, offering for

sale, distributing, exporting from, and/or importing into the United States the Accused Products without authority and in violation of 35 U.S.C. § 271(a).

70. Defendants have and continue to indirectly infringe at least claim 23 of the '123 Patent by actively, knowingly, and intentionally inducing others to directly infringe, either literally or under the doctrine of equivalents, by making, using, selling, offering for sale, distributing, exporting from, and/or importing into the United States the infringing Accused Products and by instructing users of the Accused Products to perform at least the method of claim 23 in the '123 Patent. For example, Defendants, with knowledge that the Accused Products infringe the '123 Patent at least as of the date of this Complaint, actively, knowingly, and intentionally induced, and continue to actively, knowingly, and intentionally induce, direct infringement of at least claim 23 of the '123 Patent in violation of 35 U.S.C. § 271(b).

71. For example, Defendants have indirectly infringed and continue to indirectly infringe at least claim 23 of the '123 Patent in the United States because Defendants' customers use such Accused Products, including at least the Samsung Tactical, TAK, and ATAK applications and services and Samsung Knox applications and services installed on the Accused Products, in accordance with Defendants' instructions and thereby directly infringe at least claim 23 of the '123 Patent in violation of 35 U.S.C. § 271. Defendants directly and/or indirectly intentionally instruct their customers to infringe through training videos, demonstrations, brochures, installations and/or user guides, such as those located at one or more of the following: https://www.samsung.com/us/business/solutions/industries/government/tactical-edition/#COMMAND_AND_CONTROL;

https://www.samsung.com/us/business/solutions/services/mobility-software/e-fota/;

https://image-us.samsung.com/SamsungUS/samsungbusiness/pdfs/brochures/S20_TE-tactical-

brochure-FINAL_July_2021.pdf; https://insights.samsung.com/2021/09/01/atak-enhances-collaboration-and-awareness-for-public-safety-2/; https://www.civtak.org/atak-about/; https://www.civtak.org/documentation/; https://wiki.civtak.org/index.php?title=ATAK_Manual; https://www.pargovernment.com/tactical-sa/docs/S20_brochure.pdf; https://insights.samsung.com/2021/09/22/7-ways-samsungs-galaxy-xcover-pro-supports-first-responders/; https://kp4-cdn.samsungknox.com/resource/Samsung%20Knox%20Security%20Handbook_bx4Z.pdf; https://docs.samsungknox.com/admin/knox-manage/faqs/faq-115013698467.htm; https://docs.samsungknox.com/admin/knox-manage/locate-devices.htm; and Samsung's agents and representatives located within this Judicial District. Defendants are thereby liable for infringement of the '123 Patent under 35 U.S.C. § 271(b).

72. For example, Defendants directly infringe and/or indirectly infringe by instructing their customers to infringe by a system comprising: a first device programmed to perform operations comprising: receiving a message sent by a second device, wherein the message relates to joining a group; based on receipt of the message sent by the second device, sending first location information to a first server and receiving second location information from the first server, the first location information comprising a location of the first device, the second location information comprising one or more locations of one or more respective second devices included in the group; sending, from the first device to a second server, a request for georeferenced map data; receiving, from the second server, the georeferenced map data; presenting, via an interactive display of the first device, a georeferenced map and one or more user-selectable symbols corresponding to one or more of the second devices, wherein the symbols are positioned on the georeferenced map at respective positions corresponding to the locations of the second devices represented by the

symbols, and wherein the georeferenced map data relate positions on the georeferenced map to spatial coordinates; and identifying user interaction with the interactive display selecting a particular user-selectable symbol corresponding to a particular second device and user interaction with the display specifying an action and, based thereon, using an Internet Protocol to send data to the particular second device, wherein identifying the user interaction selecting the particular user-selectable symbol comprises: detecting user selection of a portion of the interactive display corresponding to a position on the georeferenced map, and identifying the particular user-selectable symbol based, at least in part, on coordinates of the selected position, comprising: searching a set of symbols for a symbol located nearest to the coordinates of the selected position, wherein the set of symbols includes the user-selectable symbols corresponding to the second devices in the group, and wherein data associated with the set of symbols include coordinates of portions of the display corresponding to the symbols in the set, and based on a result of searching the set of symbols, identifying the particular user-selectable symbol as the symbol located nearest to the coordinates of the selected position, wherein the particular user-selectable symbol corresponds to the particular second device. For example, the Accused Products include features as shown below.

## Stay connected to what matters.

**Persistent communications**
The Galaxy S20 Tactical Edition is a COTS military smartphone with tailored software that easily connects to tactical radios and mission-critical devices, out of the box.

**Multi-ethernet capabilities**
Dedicated connections with multiple mission systems including laser range finders, external GPS devices, drones and more keep you connected in degraded and highly contested network environments.

**Next-generation networks**
As technologies evolve, you need a powerful, mission-ready device that can take full advantage of next-generation military networks. The Galaxy S20 Tactical Edition supports Private SIM, 5G, CBRS and is ready for Wi-Fi 6.

# Command and control

**Situational awareness**
The Galaxy S20 Tactical Edition integrates voice, video, and tactical data to provide a common operational picture of the battlespace. This complete and accurate real-time intelligence enhances the precision and effectiveness of your tactical teams.

**Tactical user experience**
Unique features found only on the Galaxy S20 Tactical Edition deliver fast and simple access to the information and applications operators need on-mission.

**Better intelligence**
The pro-grade 64 MP camera on the Galaxy S20 Tactical Edition allows you to discretely capture and share crisp high-resolution photo or 8K video intelligence, even in low light without the use of a flash. View and analyze intelligence in greater detail than ever before with the Galaxy S20 Tactical Edition's Dynamic AMOLED 2.0, a 120Hz[1] display.

**Extend your mission**
The Galaxy S20 Tactical Edition battery is 30% larger than the previous tactical solution and it's intelligent.[2] It optimizes your app usage in the field giving you extended power to complete the mission. When you need a recharge, Super Fast Charging[3] and fast Wireless Charging 2.0 give you power in a flash. And Wireless PowerShare allows you to easily charge a team member's phone in the field just by touching the devices.[4]

**Connect to tactical radios** - Protocols to support tactical radios and mission systems, out of the box.

**Tactical app quick launch** - Instantly expand or hide ATAK, APASS and other mission-critical applications at the push of a button.

**Night vision mode** – Turn on and off LED backlight when wearing night vision devices.

**Stealth mode** – Disable LTE and e-911 and mute all RF broadcasting for complete off-grid communications.

**Lock screen auto-rotate** - Unlock the device in landscape mode for easy access when mounted to the operator's chest.

**Auto-touch sensitivity** – Automatically adjust device operations to work with gloved hands.

# One device to meet all your mission requirements.

**Simple device management**
From device configuration, enrollment, customization and management to advanced mobile security controls and updates, Samsung has the mobility cloud services you need for every stage of the Galaxy S20 Tactical Edition lifecycle.[6] With Knox Services, you can keep pace and maintain control over devices and how they're used. You can manage devices in near real-time, configure settings, and remotely lock or wipe devices if lost or stolen, on the battlefield and anywhere else.

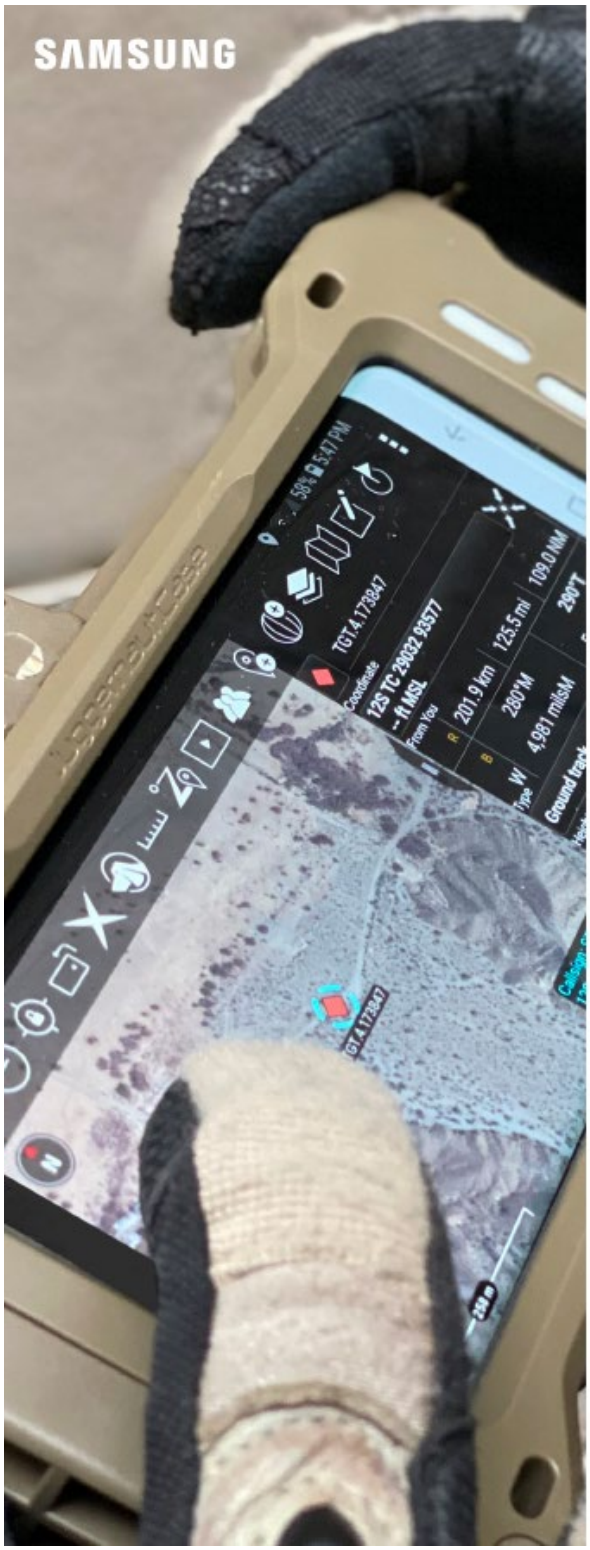
**Run mission apps and enterprise apps**
The Galaxy S20 Tactical Edition has a 64-bit Octa-Core processor with the speed and versatility to run multiple tactical applications in the field and enterprise applications everywhere else.

With Samsung DeX, connect your Galaxy S20 Tactical Edition to a monitor, keyboard and mouse for a desktop-like experience[5] ideally suited for mission planning, training, and everyday use. DeX gives you the power to work seamlessly across Microsoft Office Suite applications,[6] productivity apps, and virtual desktops with secure CAC-authenticated Virtual Desktop Infrastructure (VDI) sessions, all without a laptop.[7] And DeX-in-Vehicle transforms the Galaxy S20 Tactical Edition into a powerful in-vehicle computer.

**Open and secure**
The Galaxy S20 Tactical Edition is built on an open and secure Android operating system enabling seamless integration with a diverse ecosystem of tactical solution partners. Eliminate vulnerabilities with three software updates throughout the life of the device.

88

[88] https://www.pargovernment.com/tactical-sa/docs/S20_brochure.pdf




## Galaxy S20 Tactical Edition

# Mission-ready mobility. Proven by operators.

The Samsung Galaxy S20 Tactical Edition is the mission-ready military smartphone built and proven by operators in special operations. Based on the proven success of the S9 Tactical Edition for operators in the field, the S20 Tactical Edition is the only end user device you'll need for mission planning, training, operations and daily use.

### Persistent communications in any domain

**Purpose-built to connect to tactical radios** and mission systems out of the box, the Galaxy S20 Tactical Edition delivers a complete and accurate common operational picture. Run mission applications in the field and enterprise applications everywhere else with a single end user device for mission training, planning, operations and everyday use.

### Interoperable across devices and networks

**Pre-configured software, pre-loaded during the manufacturing process,** includes drivers to support tactical radios and mission-critical devices. Multi-ethernet capabilities provide dedicated connections to multiple mission systems including drone feeds, laser range finders, and external GPS. Support for current and next-generation networks includes Private SIM, 5G, WiFi 6 and CBRS. Allow or disallow USB peripherals based on product or vendor identifiers.

### Command and control

**Integrate voice, video and tactical data** for a complete view of the battlespace to enhance precision and effectiveness. Unique tactical features on the Galaxy S20 Tactical Edition include night-vision mode, stealth mode, lock screen autorotate, hostage negotiation mode, LTE band lock for consistent 4G connection, tactical application quick launch, to keep the operator focused on the objective, Standalone(5G)/Non-standalone (4G) modes to stay on preferred network. Preloaded tactical settings app. Ability to configure hotspot 2.0.

### Capture Intelligence

**A Pro-grade 64 MP camera** on the Galaxy S20 Tactical Edition enhances intel gathering, even in low-light environments without a flash. Capture high-resolution photos or sharp 8K video reconnaissance without giving away your position.

### Power to extend the mission

**Keep going wherever the mission takes you** with the Galaxy S20 Tactical Edition's intelligent2 4000mAh battery is 30% larger than the previous tactical solution and optimizes energy based on your device usage. Easily share power with a team member's smartphone in the field simply by touching devices using Wireless PowerShare.[4]

### One device to meet your requirements

**Run mission applications in the field** and enterprise applications everywhere else with the powerful and efficient Galaxy S20 Tactical Edition 64-bit Octa-Core processor. Connect your device to a monitor keyboard and mouse and use the power of Samsung DeX[5] for a desktop-like experience that is ideal for mission planning, training and everyday use. DeX-in-Vehicle transforms your Galaxy S20 Tactical Edition into an in-vehicle computer.

### Open and secure

**Enable a diverse ecosystem of tactical partners** with the open and secure Android operating system on the Galaxy S20 Tactical Edition. The all-new Tactical Settings feature simplifies device management, while Samsung Knox provides defense-grade security[6] from the hardware layer up and mission-specific device customization capabilities. The DualDAR architecture of the Galaxy S20 Tactical Edition provides two layers of encryption, even when the device is powered off, for securing up-to top secret level data on the device.

### Tested and proven

Samsung Galaxy Tactical Edition smartphones are tested and proven by special operators in the field. The Galaxy S20 Tactical Edition is certified to meet the most stringent requirements including NSA's CSFC Components List, NIAP Common Criteria/MDFPP, DODIN APL, FIPS 140-2, DISA Android 10 STIG, IP68 rating.

**Contact Us:** www.samsung.com/TacticalEdition

89

[89] https://image-us.samsung.com/SamsungUS/samsungbusiness/pdfs/flyer/S20_TE-salesflyer_FINAL_July_2021.pdf

The Team Awareness Kit (TAK), for civilian uses, or Tactical Assault Kit (also TAK) for military uses is a suite of software that provides geospatial information and allows user collaboration over geography. There are numerous TAK Products in the TAK family, all developed at government expense

The Team Awareness Kit for Android (ATAK, also known as CivTAK) was originally developed by the Air Force Research Laboratory (AFRL) and is now maintained by a Joint Product Center.

ATAK (including CivTAK) is an Android smartphone geospatial infrastructure and situational awareness app. It allows for precision targeting, surrounding land formation intelligence, situational awareness, navigation, and data sharing.

All the Android variants of TAK are virtually identical and all are interoperable with each other and with other TAK products. There are small, military-specific additions in military versions of ATAK.

# Features

Industry/civilian capabilities of ATAK/CivTAK include:

- Online and offline mapping (most standard formats), with a blazing fast rendering engine
- Support for very high-resolution imagery (sub 1 cm resolution)
- Collaborative mapping, including points, drawings, locations of interest
- Extensive and customizable set of Icons
- Overlay Manager which allows the Import and display of KML, KMZ, GPX overlays and maps, including online sources
- Location marking, sharing, history
- Chat, file sharing, photo sharing, video sharing, streaming
- Navigation-walking/hiking, driving, also useful flying and air-ground coordination
- Elevation Tools, heat maps, computed contour maps, viewsheds, routes w/DTED, SRTM, including dynamic profiling
- Hashtags and Sticky tags
- Center on Self, Center on other objects (e.g. another person in the network)
- Range, bearing, and other measurement tools
- Network-aware geofences with triggers
- "Bloodhound" destination tracking, including on moving objects
- Team Emergency Beacons
- Customizable Toolbar
- Radio controls and Integration
- Photo to map capability (aka Rubber Sheeting)
- Casualty evacuation tool
- Icon support for a wide variety of First Responder missions with further extensible Icons
- 3D perspective and ability to display 3D geospatial models
- Useful for First Responders, Hunting, fishing, ornithology, wildlife site survey
- An API with an SDK

[90]

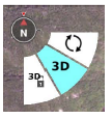
[90] https://www.civtak.org/documentation/

## ATAK Civilian Overview

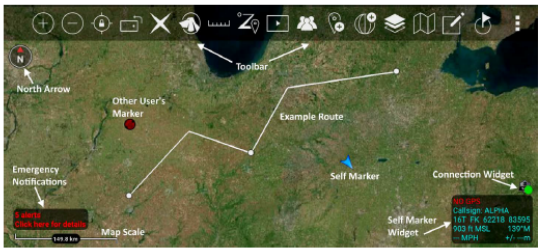
The Civilian Team Awareness Kit for Android (ATAK Civilian) is a Government-off-the-Shelf (GOTS) software application and mapping framework for mobile devices. ATAK Civilian has been designed and developed to run on Android smart devices used in a first responder environment. The ATAK Civilian software application is an extensible moving map display that integrates imagery, map and overlay information to provide enhanced collaboration and Situational Awareness (SA) over a tactical meshed network. ATAK Civilian promotes information flow and communications from the field environment to command enterprise locations.

The first time ATAK Civilian is opened, or after a Clear Content, a passphrase is auto-generated to activate data encryption. The user can supply their own passphrase by using Settings > Show All Preferences > Device Preferences > Change Encryption Passphrase. Following this step, ATAK Civilian's End User License Agreement (EULA) must be accepted. Next, the user will be prompted to change their callsign and/or import preferences or data from a Mission Package. All changes/imports can always be updated later. Finally, the user can place their self-marker by following the instructions located in the lower right corner.

The toolbar runs along the top of the map display. The features whose icons form the center portion of the toolbar are discussed in individual sections of this guide. The three dots at the right of the toolbar provide additional menu items that appear in a drop-down menu. A Long Press on the map will toggle the toolbar between hidden and visible.




The North Arrow appears in the upper left and is used to control map orientation. It has two primary modes: North Up/Track Up (default) and Manual Map Rotation/Lock. While in North Up/Track Up Mode, single press on the [**North Arrow**] icon to cycle between the North Up and Track Up map orientation. Long press the [**North Arrow**] to call out the additional controls menu where the Manual Rotation/Lock and 3D features are available. Select the [**Rotation**] button to enter Manual Map Rotation/Lock Mode. When in Manual Map Rotation/Lock Mode, rotate the map orientation by pressing on the map with two fingers and pivoting them in the desired direction. Single press on the [**North Arrow**] to lock the screen orientation, signified by the appearance of the lock icon, and again to unlock the orientation for further adjustment. 3D controls are discussed in a separate section.



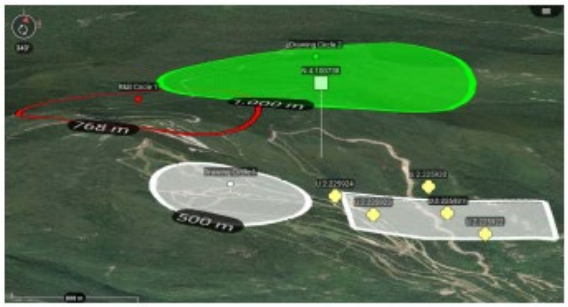

Select the [**Magnifier**] buttons to zoom in or out on the map. The map can also be zoomed by using two fingers on the screen to pinch and spread the map. Select the [**Back**] button to center the screen on the Self Marker or the [**Padlock**] icon to lock the center of the screen to the Self Marker. Select the [**Orientation**] icon to toggle the screen position between portrait and landscape.

The optional connection widget indicates whether or not the user is connected to a TAK Server. This has a corresponding Android notification that provides the same information. Toggle this display on at Settings > Network Connections > Network Connections > Display Connection Widget.

Alerts and notifications are displayed in the lower left of the map interface.

The Map Scale displays a 1 inch to X mi/km reference on the map. The scale adjusts with the map when zoomed in and out. Hint windows are available to alert users to changes or make suggestions about the use of tools the first time they are opened.

## 3D View



ATAK Civilian features 3D viewing of terrain and map items (DTED required). To enable 3D view, long press on the **[North Arrow]** to call out the additional controls menu and select [**3D**]. A tilt angle indicator will appear around the edge of the [**North Arrow**] when 3D view is active. Touch the screen with two fingers and simultaneously swipe up or down on the screen to tilt the view angle. Once the appropriate viewing angle is set, select the [**3D Lock**] button to retain this view while panning the map. While viewing the map from an angle, some map items will appear raised above the map surface if they have defined elevations.

## 3D Models

ATAK Civilian supports the use of 3D models. OBJ models and other types from products such as Pix4D can be imported via the Import Manager or can be manually placed in the atak/overlays folder prior to startup. If using Import Manager browse to the .OBJ file and import only that file, or browse to a .ZIP file that contains the .OBJ file (and others) and import only that file. If using manual placement to the atak/overlays folder, place a .ZIP file containing the .OBJ file (and others) into the directory and they will be imported on startup.

Once imported, a 3D Model icon will appear on the map. Zoom into the area of the icon until a loading ring appears. After the loading process has finished, the 3D model will be projected onto the map. Enable the map 3D View and tilt the view angle to see the 3D modeling. Loaded 3D models will appear as their own category in Overlay Manager and can be toggled on/off or removed from there.

# Placement

The user can enter locations of interest using the Point Dropper tool. Select the [**Point Dropper**] icon to place internationally standardized markers and other icons on the map, edit the data and share the markers with other network members.

## Self-Marker

The Self-Marker is displayed as a blue arrowhead at the user's current location. The options available on the Self-Marker radial are: Compass Rose, Polar Coordinate Entry, Fine Adjust/Enter Coordinate/MGRS Location, GPS Error, Range & Bearing Line, GPS Lock to Self, Tracking Breadcrumbs, Place a Marker at the user's current location and Details. Other TAK users appear on the display as a colored circle. The color of the circle represents the user's Team affiliation, with additional lettering inside the circle to identify the role the user on the team. Team Member markers that include a diagonal line indicate that the GPS location is not available. A solid icon indicated that the team member has GPS reception.

Available roles include: Team Member, Team Lead (designated by a TL in the center of the marker), Headquarters (HQ in center), Sniper (S), Medic (+), Forward Observer (FO), RTO (R) or K9 (K9). The options available when another user's Self-Marker is selected are: Inner Ring – Delete, Polar Coordinate Entry, Fine Adjust/Enter Coordinate/MGRS Location, Range & Bearing Line, GPS Lock on Friendly, Video Player (if available), Communication Options (if configured by that user), Custom Threat Rings, Tracking Breadcrumbs and Details.

Outer Ring (Communication Options) – Data Package, Email, SMS Messaging, GeoChat, VOIP and Cellular Phone, when available.

## Point Dropper

Selecting the [**Point Dropper**] icon will open the Point Dropper menu, containing marker symbology with one or more icon sets, a Recently Added button and an Iconset Manager button.

The Markers symbology affiliations are: Unknown, Neutral, Red and Friendly. Select the affiliation, then a location on the map interface to drop the marker. To add a marker by manually entering coordinates, long press on the map interface and enter the MGRS location. Change the standard naming convention by entering values into the custom prefix and index fields or leave blank to use the defaults. If values are entered, the next marker will be dropped with the prefix name and starting number(s) or letter(s) and every subsequent marker will be assigned the next consecutive number(s) or letter(s).

The user can select the mission specific pallet to open point options including Waypoint (WP), Sensor or Observation Point (OP).

The user can move between icon sets by either swiping in the icon set area or selecting on the [**Iconset Name**] field to bring up the Icon Pallet drop-down.

The last point placed is shown at the bottom of the Point Dropper window. The information for all recently placed points can be accessed by selecting the [**Clock**] icon. This displays the marker icon, name, coordinates, elevation and range & bearing information. The user can send, rename or remove any recently added markers by selecting the [**Arrows**] next to the marker to reveal [**SEND**], [**RENAME**] or [**DEL**] buttons.

Select the [**Iconset Manager**] (gear) button to add or delete icon sets or to set the default Marker Mapping.

## Radial Menus

**Unknown Object**

**Neutral Object**

**Red Object**

**Friendly Object**

**Spot Object**

The options available for Unknown Object Markers are: Delete, Polar Coordinate Entry, Fine Adjust/Enter Coordinate/MGRS Location, Range & Bearing Line, Lock On, Tasking, Custom Threat Rings, Tracking Breadcrumbs and Details.

The options available for Neutral Object Markers are: Delete, Polar Coordinate Entry, Fine Adjust/Enter Coordinate/MGRS Location, Range & Bearing Line, Lock On, Tasking, Custom Threat Rings, Tracking Breadcrumbs and Details.

The options available for Red Object Markers are: Delete, Polar Coordinate Entry, Compass Rose/Bullseye, Fine Adjust/Enter Coordinate/MGRS Location, Range & Bearing Line, Tasking, Custom Threat Rings, Tracking Breadcrumbs and Details.

The options available for Friendly Object Markers are: Delete, Polar Coordinate Entry, Fine Adjust/Enter Coordinate/MGRS Location, Range & Bearing Line, Lock On, Video, Contact Card, Custom Threat Rings, Tracking Breadcrumbs and Details. The Video radial will activate if a properly formatted packet that includes the link to the video feed is included. Select the video radial to open the associated video. The Contact Card can be selected to display additional communication options, including GeoChat, Email, VoIP, SMS Messaging and Cellular Phone, when available.

The options available for Spot Map are: Delete, Fine Adjust/Enter Coordinate/MGRS Location, Range & Bearing Line, Nav-To, Custom Threat Rings, Labels and Details.

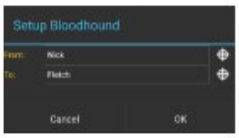
The options for User Defined Iconsets are: Delete, Polar Coordinate Entry, Fine Adjust/Enter Coordinate/MGRS Location, Range & Bearing Line, Lock On, Tasking, Custom Threat Rings. Tracking Breadcrumbs and Details.

Select [**Details**] on the marker radial to make desired modifications, including: Coordinate, Elevation, Name, Type and Remarks. Selecting Marker Type opens a dialog box with extra categories. File attachments, including images, can be associated with the object by selecting the [**Paperclip**] icon. Once all the desired modifications have been made, the Marker can be sent to other network members using [**Send**]. The information can be broadcast to all members or sent to specific recipients. Select the [**Auto Send**] option to broadcast the marker to other TAK users on the network, with updates automatically sent about once every 60 seconds.

# Bloodhound Tool

The Bloodhound Tool provides support for tracking and intercepting a map item. It allows the user to select two points on the map and/or map objects and display range & bearing information between the chosen tracker and the target.

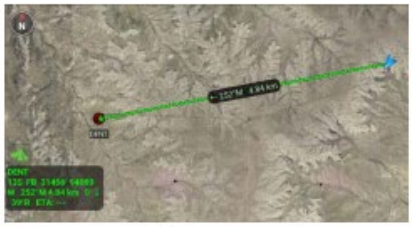
Select the [**Bloodhound**] icon to open the Bloodhound Tool. A window will open, prompting the user to choose where to start by tapping the [**From Reticle**] (default = user's self marker) and where to bloodhound (track) to by tapping the [**To Reticle**].




Targets include map objects like other User's Self Markers, DPs, Markers, Shape center points, Range & Bearing end-points and any other map objects. If the user selects a map location instead of an object as the target, Bloodhound will place a waypoint marker there. The self marker will then track towards the waypoint.

Select [**OK**] and Bloodhound will be activated.

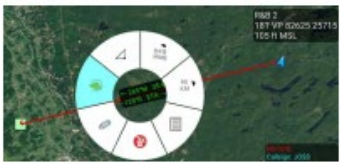
If either point moves, the green widget in the lower left will show the updated information. As the tracking object begins to navigate toward the target, the Estimated Time of Arrival (ETA) will update accordingly.



The green line showing the direct path from the tracker to the target will flash when the user-defined ETA outer threshold is reached (default = 6 minutes from target). The line will flash as the tracker continues toward the target until the next ETA threshold is reached (default = 3 minutes). The line will turn a flashing yellow until the final ETA threshold (default = 1 minute) is reached. The line then flashes red until the target is reached. Colors and thresholds can be modified in Settings > Tool Preferences > Bloodhound Preferences.

Selecting the green Bloodhound icon on the map will pan the map to the Bloodhound Range & Bearing Line. Disengage the Bloodhound Tool by selecting the [**Bloodhound**] icon on the toolbar.

## Multiple Bloodhound

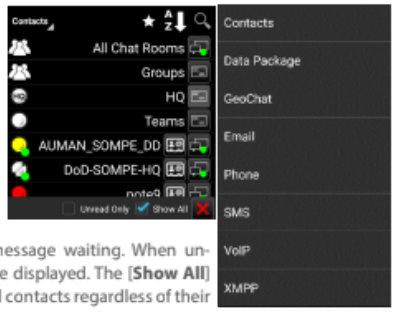


To create multiple bloodhounds, selecting the Range and Bearing Tool and select the [**R&B Line**] icon. Select two markers on the map and once the R&B line is created, select the line to bring up the radial. Select the [**Bloodhound**] radial, and the bloodhound information will be displayed on the R&B Line itself.

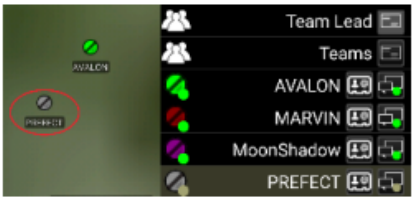
If either point moves, the Bloodhound information shown on the R&B Line will be updated. As the tracking object begins to navigate toward the target, the Estimated Time of Arrival (ETA) will update accordingly.

## Contacts

The Contacts list includes a variety of ways in which a user may communicate with other users, such as GeoChat (ATAK Civilian's built in Chat capability), Data Packages, Email, Phone, SMS, VoIP and XMPP.



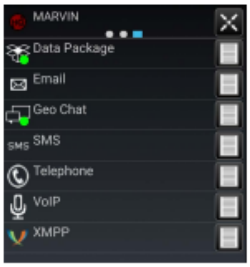

A default communication type (shown in the last column) may be selected and used until another type of communication is selected.




The Contacts list has two filters available at the bottom of the screen. The Unread Only box, when checked, will display only contacts with whom there are unread message waiting. When unchecked (default), all available contacts are displayed. The [**Show All**] box, when checked (default), will display all contacts regardless of their location. When unchecked, only contacts that are visible on current map screen will be displayed.

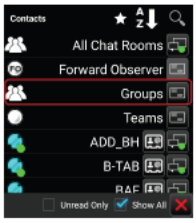
If a contact is no longer online, it will be indicated by changing the contact listing to a yellow color and the marker changes to gray both in the list and on the map.

Profile cards are accessed by selecting the second to last column in the Contacts list and are available for each contact. These contain additional information about that contact including: 1) role, software type and version installed, node type, default connector, last reported time, battery life; 2) location information, and 3) available types of communication.

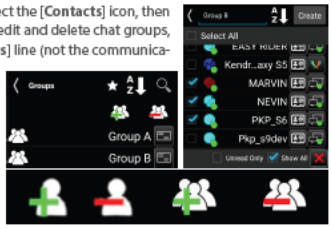


## GeoChat Group Management

Text-based Chat messages may be sent to active network members by using the GeoChat function. To enter GeoChat Group Management, select the [**Contacts**] icon and select [**GeoChat**] from the drop-down menu.

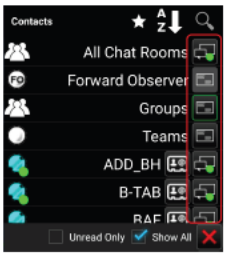



GeoChat Group Management is initiated through Contacts. Select the [**Contacts**] icon, then select GeoChat from the drop-down. The user can now create, edit and delete chat groups, as well as sub-groups. To create a chat group, select the [**Groups**] line (not the communications button). Select the [**Add Group**] icon to create the name of the group and add contacts to the group and then select [**Create**]. If a parent group is being created, no contacts need to be added at this level. To add a nested group, tap the parent group, select the [**Add Group**] icon to create the name of the sub-group and add contacts. Groups may be managed using the options to add/delete contacts or to add/delete GeoChat group.




To add users to a group, select the [**Groups**] line (not the communications button), then select the name of the group to add users. Select the [**Add Users**] icon. A window will open allowing the group creater to add users to the selected group. Select the [**Add**] button when all the users to be added are checked.

## GeoChat Messaging




Group and person-to-person messaging is available. To view messages from or send messages to an individual, tap on the desired contact's [**Communication**] icon. Selecting the [**Pan To**] icon, located at the top right of the call sign in an individual chat, will pan the map interface to that user's location. Select [**All Chat Rooms**] to view all messages from or send messages to those present on the network or TAK Server. Other groupings available for viewing or sending messages are: Forward Observer, Groups, HQ, K9, Medic, RTO, Sniper, Team Lead and Teams. If the user's current role is Forward Observer, HQ, K9, Medic, RTO, Sniper or Team Lead, that user can view or send messages to all other contacts with the same role. If a GeoChat message is sent from the top level of Teams, it will be sent to all contacts, similar to [**All Chat Rooms**].

When a sub-Team is chosen, messages can only be sent to that user's active (My Team) team color. When a parent group is chosen, messages are sent to all members of the parent group, as well as all of the sub-groups. When a sub-group is chosen, messages are sent only to members of the sub-group. Individuals within GeoChat may be removed from the Contacts menu by toggling the visibility of individuals or groups within Overlay Manager.





## GeoChat Messaging (continued)

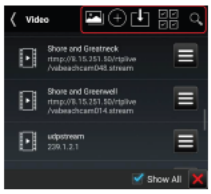
Selecting in the Free Text Entry area will open an onscreen keyboard. At the bottom of the Chat area are pre-defined messages that may be used to quickly create a message to send. Tap the current menu button to scroll through the different menus of canned messages, including: DFLT1, DFLT2, ASLT1, ASLT2, RECON1 and RECON2. These pre-defined messages present an easy way to transmit a brief message to other network members concerning position or other important communication. The pre-defined messages may be changed by long pressing on the button and changing its label and corresponding value.

A numbered red dot will appear on the [**Contacts**] icon when a message has been received successfully. The number denotes the number of unread messages that have been received. Select this icon to view the contact list. The user name who sent the message will appear with a numbered red dot next to their name. Alternatively, the text of the message can be read by dragging down from the top to see the Android notifications window. This notification will only stay available for a short time.

## Video Player

Select the **[Video Player]** icon to bring up the Video player. The Video Player supports playing video streams from IP cameras and H.264 encoders. The menu allows adding, editing, deleting, playing or sending videos to other network members.

Options for the video player include: viewing video snapshots, adding a new video alias, downloading an alias from the TAK Server, selecting the Multi-Select Action option to either Export or Delete aliases or searching for a specific alias.




Select the desired listed video alias or file name to begin playing the stored or streaming video. The video will display half the width of the screen.

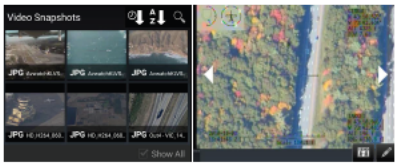
To view a video at full screen, slide the pull bar. To return to half screen, slide the pull bar back to the right.

Select the **[Back]** button to return to the list of available videos.

To add stored video file, select the **[Import Manager]** icon, select **[Local SD]**, and navigate to the video file and select **[OK]** to add the video to the list of available videos. The user can also manually place video files in "atak\tools\videos" to have them listed after ATAK is restarted. When a video is playing at half width, slide the pull bar to the right to hide the video but maintain the connection. Slide the pull bar to the left to unhide the video. The status of the video player is reflected in the main Android toolbar located at the top of the screen.

Select the **[Snapshot]** icon to save the current frame of the video as a JPEG image file, the icon will flash green to indicate that the snapshot has occurred. The file will be saved in the "\atak\tools\videosnaps" folder.

The user can view the saved snap shots by selecting the **[Video Snapshots]** icon. The user has the option of sorting the images by time taken or by the name of the snapshot. The user can also search within the snapshots taken by their name. By selecting an image, the image will be displayed within the window.




The user will have the options of cycling though the images, **[Send]** to a TAK user, or edit in **[Image Markup]**. (Image Markup would need to be installed.)

If a live UDP stream is being viewed, it can be recorded by tapping the **[Record]** icon. The icon will change to a green square while recording. Select the **[Green Square]** to end the recording. The recordings are saved in a folder in "\atak\tools\videos\".

**Note:** This is only available for UDP streams.

To close the video player, select the **[X]** located at the bottom right corner of the video player or select the **[Back]** button.





## Go To

Select the **[Go To]** icon to enter details and navigate to a specific location on the map.

Select from the **[MGRS]** (military grid reference system), **[DD]** (decimal degrees), **[DM]** (degrees- minutes), **[DMS]** (degrees-minutes-seconds), **[UTM]** (Universal Transverse Mercator) or **[ADDR]** tabs on the Go To interface and enter the location data of interest. The address provider name appears beneath the Elevation Data when the user selects the **[ADDR]** tab.

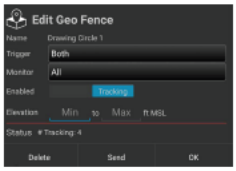
The user can enter the Latitude, Longitude and Elevation in the space provided for **[MGRS]** , **[DD]**, **[D-M]** or **[D-M-S]** searches. If DTED is installed, the elevation value can be automatically populated by tapping the **[Pull From DTED]** button.The user can select a desired marker type (Spot, Unknown, Neutral, Red, or Friendly) to be placed at the entered coordinates. If **[No Point]** is selected, the map will pan to the location but will not add a point.

**Note:** The address provider name appears beneath the Elevation Data when the user selects the **[ADDR]** tab.

The Address Lookup provider used for the ADDR tab can be configured in the Settings > Tool Preferences > Address Lookup Preferences.

## Geofencing

The Geo Fence tool allows users to create a virtual fence that triggers entry/exit notifications if map items of interest cross the virtual boundary lines. The Geo Fence options are added to the existing drawing tools. After a shape has been added, the Geo Fence Tool can be accessed either by selecting the [**Geo Fence**] icon from the menu items or selecting it from the radial.




The Enabled Field slider will move to Tracking by default when a new Geo Fence window is created. Toggle the slider between Tracking and Off to enable/disable the Geo Fence. Use the Trigger field to define which types of Geo Fence breach to monitor. Choose between Entry, Exit or Both. Use the Monitor field to define which entities the Geo Fence will track.

Choose between TAK Users, Friendly, Hostile, Custom or All. Check the [**Specify Elevation**] box to enable the Elevation field, where elevation boundaries for the entities being tracked can be defined. Select the [**OK**] button to finish creating the fence. Select the [**Send**] button to create the fence and send it to another user. Select [**Delete**] to close the Create Geo Fence window and discard changes.

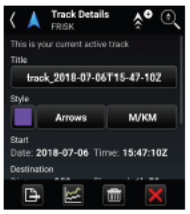
Alerts appear on the map interface. Selecting the [**Alert Notification**] will open the alerts menu, detailing the activity monitored in the user defined region. The default radius for monitoring users (filtered within the "Monitor" field) outside the Geo Fence is set at 75 km. This means the total area monitored begins at the farthest point from the center of the shape plus 75 km. If the user wishes to keep the Geo Fence, but disable tracking, the user can set the tracking [**Enabled**] to off in the Edit Window.

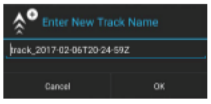




## Track History

The device's GPS can be used to track movements with the Track History tool. These tracked paths can be exported to a TAK server, to a route or to a KML, KMZ, GPX or CSV file. A GPS position must be established before tracking can begin.



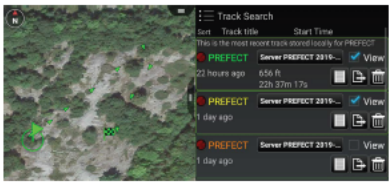




Selecting the [**Track History**] icon will open Track Details for the current active track. The track title, color and style can be modified. Initiate a new track by selecting the [**Add Track**] icon. Accept or edit the default track name and select the [**OK**] button to begin the new track. User location data is recorded as breadcrumbs in a new track file.

## Track Search

Use the Track Search function to view track information that has been previously saved locally or on a TAK Server. The tool searches the track database for matches against the specified time range and by user callsign. Matching tracks are displayed as a list, and can be selected to view on the map interface.

Select the [**Track Search**] icon to access the function. Specify callsign and time frame, check the box for Server Search (if desired), then select [**Search**]. The track list will appear. The query results can be sorted by Track Name or Start Time. Select any of the query results to move to that track. Once selected, the name, color, and style of a selected track can be modified or the track can be cleared. Convert a track to a TAK route or export it as a KML, KMZ, GPX or CSV file by selecting the desired track and then [**Export**]. Enter a file name then select [**Next**] and choose the export format. Select [**Done**] or [**Send**] when the export completes.



When viewing the track list, the Track History Toolbar will appear at the top of the screen. The options include [**Add a Track**], [**Multi-select**], [**Track Search**], [**Clear Tracks**] and [**Exit**]. The Track History List allows the user to select tracks of other users that have been saved on their device. The Track Search – Local Device allows the user to perform a tailored search for tracks meeting their criteria. The searching option allows the user to retrieve all the tracks on the device.

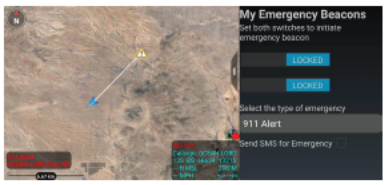
The Track History Breadcrumb and Settings can be configured in the Settings > Tools Preferences > Track History Preferences.

Unclassified

## Emergency Beacon

Select the [**Emergency Beacon**] icon to open the Emergency Beacon Tool.

The Emergency Beacon allows the user to indicate their need for assistance, the type of emergency and their location on the map. The type of emergency can be selected from the drop-down menu, before activation, and includes options for an Alert, Ring the Bell, Geo Fence Breached or In Contact.




Once the Emergency type has been selected and both switches have been enabled, the TAK Server broadcasts the announcements to all network contacts. Even if the user's device is turned off, the beacon will continue. Only when the user returns to the Emergency Beacon tool and turns off the switches will the beacon be canceled and removed. If the SMS for Emergency option has been configured, the alert will be sent via text message to the configured numbers.

91

[91] https://drive.google.com/file/d/1bo9WHadg3J3o55OLlx1mn3McqEJzvgrK/view

# INTRO

## A new way of working demands a new level of security. Are you sure your devices are protected?

**This is protection.**

Remember the good old days? The morning commute and the 9 to 5? Well those days are history.

Forget being tied to a desk and a schedule. Today's workplace has nothing to do with time or place and everything to do with productivity and mobility. Without compromise. Today's employees want the same access, speed and resources of the office, even if they're three time zones and two continents away.

While mobile, employees spend a significant amount of time outside of their protected corporate networks as they access the web from locations other than their offices. This can expose businesses to more attacks, errors, leaks and new dangers we haven't even encountered.

For IT leaders, supporting a mobile workforce while maintaining the same level of productivity they would have had in the office is extremely difficult. Doing it while maintaining top level security is nearly impossible. Nearly.

This entirely new way of working demands protection that works in real time, not sometimes. Protection that secures on every layer, not just one. Protection that understands that we're safer when we work together, instead of trying to go it alone. Most importantly, protection is security without compromise and protects without getting in the way of creativity, productivity or freedom.

Protection is what Samsung is all about and it's why we built Samsung Knox, a cutting-edge security platform for mobile experience embedded in your Samsung Galaxy device. We are talking real-time, end-to-end protection, with the best intelligence from leading partners and experts across the industry, including Google, Cisco and more. So if you want to stay a step ahead, you can trust Samsung Galaxy and Samsung Knox to fully protect your way of working.

**This is protection. Samsung Knox.**

92

[92] https://kp4-cdn.samsungknox.com/resource/Samsung%20Knox%20Security%20Handbook_bx4Z.pdf.

# Knox Platform for Enterprise

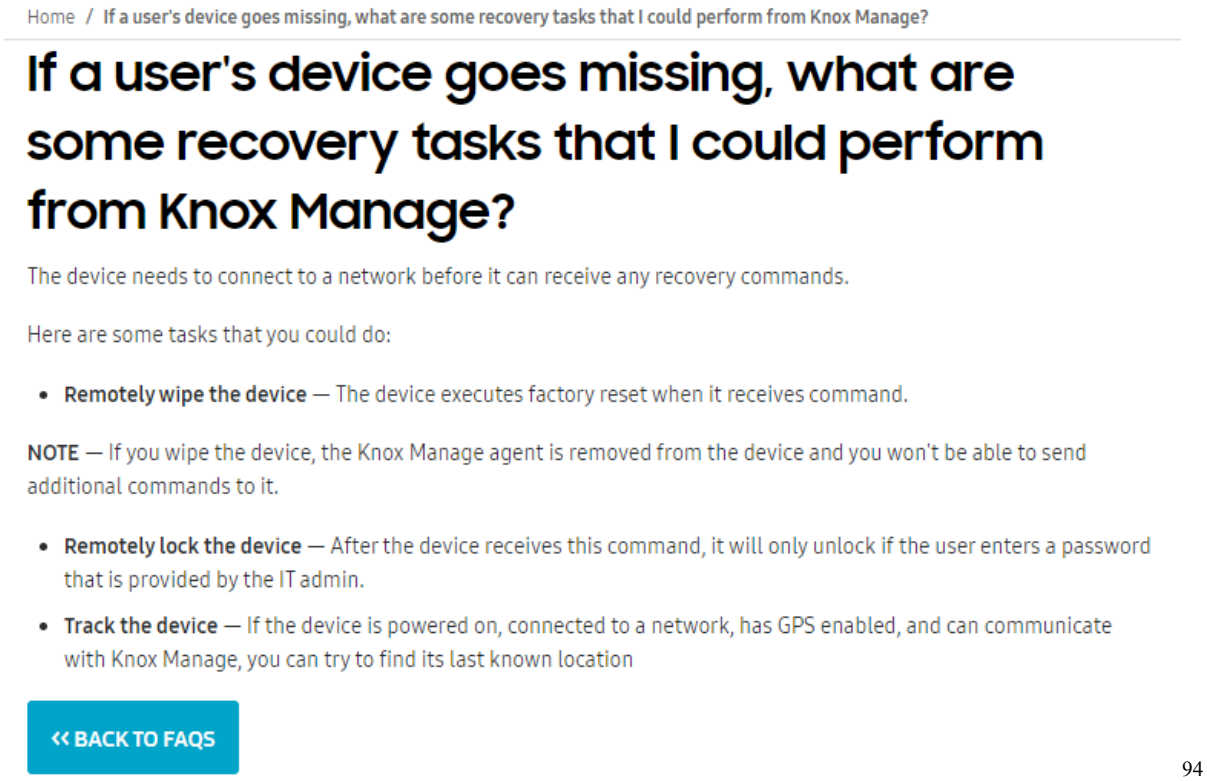
TRY FOR FREE

Samsung's Knox Platform for Enterprise (KPE) brings defense-grade security on the most popular consumer devices to all enterprises.

The Knox Platform provides best-in-class hardware-based security, policy management, and compliance capabilities beyond the standard features commonplace in the mobile device market. The Knox Platform is the cornerstone of a strong mobile security strategy supporting a wide variety of Samsung devices.

93

[93] https://docs.samsungknox.com/admin/knox-platform-for-enterprise/welcome.htm.



Home / If a user's device goes missing, what are some recovery tasks that I could perform from Knox Manage?

# If a user's device goes missing, what are some recovery tasks that I could perform from Knox Manage?

The device needs to connect to a network before it can receive any recovery commands.

Here are some tasks that you could do:

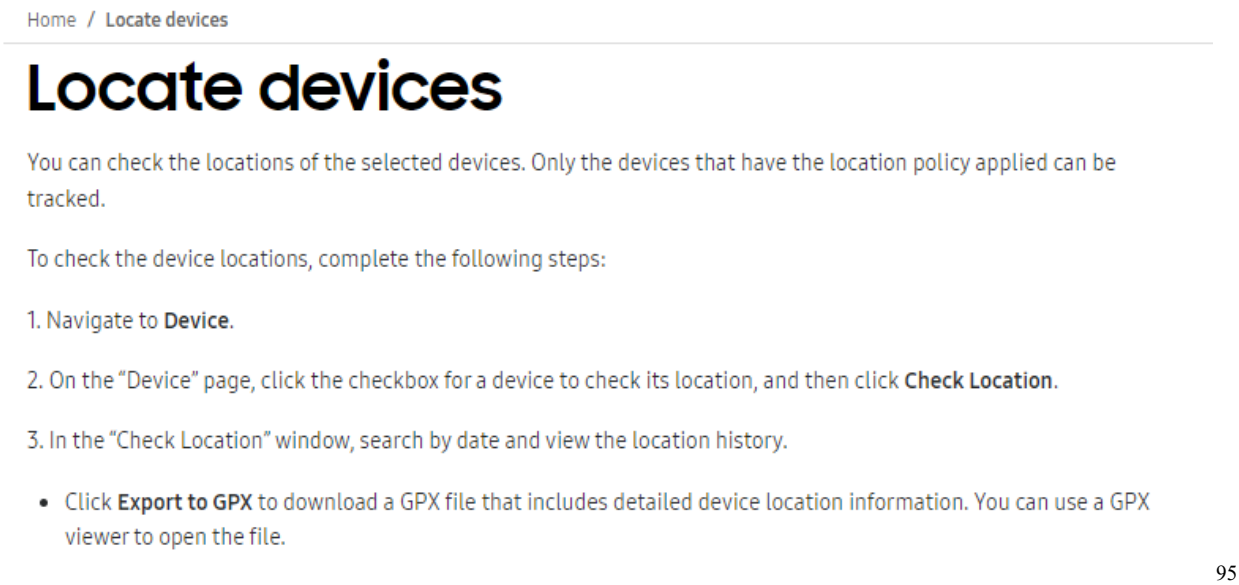
- **Remotely wipe the device** — The device executes factory reset when it receives command.

**NOTE** — If you wipe the device, the Knox Manage agent is removed from the device and you won't be able to send additional commands to it.

- **Remotely lock the device** — After the device receives this command, it will only unlock if the user enters a password that is provided by the IT admin.
- **Track the device** — If the device is powered on, connected to a network, has GPS enabled, and can communicate with Knox Manage, you can try to find its last known location

<< BACK TO FAQS

94



Home / Locate devices

# Locate devices

You can check the locations of the selected devices. Only the devices that have the location policy applied can be tracked.

To check the device locations, complete the following steps:

1. Navigate to **Device**.

2. On the "Device" page, click the checkbox for a device to check its location, and then click **Check Location**.

3. In the "Check Location" window, search by date and view the location history.

- Click **Export to GPX** to download a GPX file that includes detailed device location information. You can use a GPX viewer to open the file.

95

[94] https://docs.samsungknox.com/admin/knox-manage/faqs/faq-115013698467.htm.
[95] https://docs.samsungknox.com/admin/knox-manage/locate-devices.htm.

73. For example, Defendants' Accused Products allow users to share their locations and view other users' locations on a map and to communicate with those users via the Samsung Tactical, TAK, and ATAK applications and services and Samsung Knox applications and services (as shown below).

# One device to meet all your mission requirements.

**Simple device management**
From device configuration, enrollment, customization and management to advanced mobile security controls and updates, Samsung has the mobility cloud services you need for every stage of the Galaxy S20 Tactical Edition lifecycle.[5] With Knox Services, you can keep pace and maintain control over devices and how they're used. You can manage devices in near real-time, configure settings, and remotely lock or wipe devices if lost or stolen, on the battlefield and anywhere else.

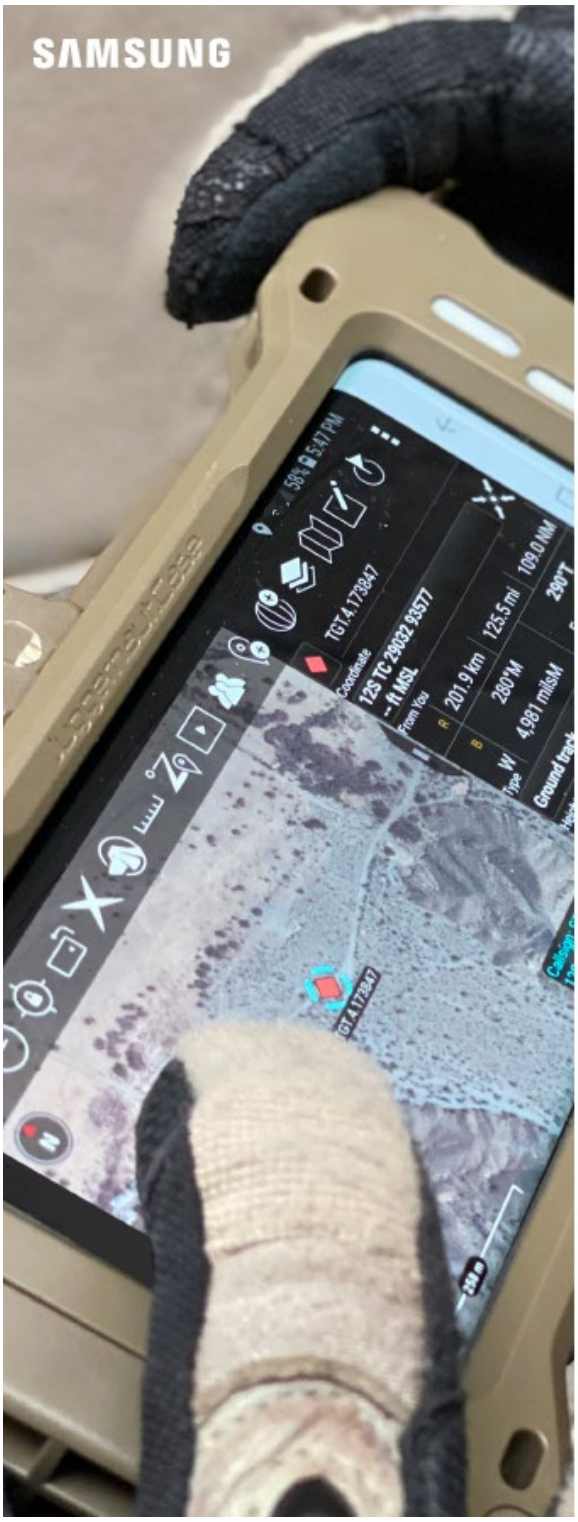
**Run mission apps and enterprise apps**
The Galaxy S20 Tactical Edition has a 64-bit Octa-Core processor with the speed and versatility to run multiple tactical applications in the field and enterprise applications everywhere else.

With Samsung DeX, connect your Galaxy S20 Tactical Edition to a monitor, keyboard and mouse for a desktop-like experience[5] ideally suited for mission planning, training, and everyday use. DeX gives you the power to work seamlessly across Microsoft Office Suite applications,[6] productivity apps, and virtual desktops with secure CAC-authenticated Virtual Desktop Infrastructure (VDI) sessions, all without a laptop.[7] And DeX-in-Vehicle transforms the Galaxy S20 Tactical Edition into a powerful in-vehicle computer.

**Open and secure**
The Galaxy S20 Tactical Edition is built on an open and secure Android operating system enabling seamless integration with a diverse ecosystem of tactical solution partners. Eliminate vulnerabilities with three software updates throughout the life of the device.

96

[96] https://www.pargovernment.com/tactical-sa/docs/S20_brochure.pdf




## Galaxy S20 Tactical Edition

# Mission-ready mobility. Proven by operators.

The Samsung Galaxy S20 Tactical Edition is the mission-ready military smartphone built and proven by operators in special operations. Based on the proven success of the S9 Tactical Edition for operators in the field, the S20 Tactical Edition is the only end user device you'll need for mission planning, training, operations and daily use.

### Persistent communications in any domain

**Purpose-built to connect to tactical radios** and mission systems out of the box, the Galaxy S20 Tactical Edition delivers a complete and accurate common operational picture. Run mission applications in the field and enterprise applications everywhere else with a single end user device for mission training, planning, operations and everyday use.

### Interoperable across devices and networks

**Pre-configured software, pre-loaded during the manufacturing process,** includes drivers to support tactical radios and mission-critical devices. Multi-ethernet capabilities provide dedicated connections to multiple mission systems including drone feeds, laser range finders, and external GPS. Support for current and next-generation networks includes Private SIM, 5G, WiFi 6 and CBRS. Allow or disallow USB peripherals based on product or vendor identifiers.

### Command and control

**Integrate voice, video and tactical data** for a complete view of the battlespace to enhance precision and effectiveness. Unique tactical features on the Galaxy S20 Tactical Edition include night-vision mode, stealth mode, lock screen autorotate, hostage negotiation mode, LTE band lock for consistent 4G connection, tactical application quick launch, to keep the operator focused on the objective, Standalone(5G)/Non-standalone (4G) modes to stay on preferred network. Preloaded tactical settings app. Ability to configure hotspot 2.0.

### Capture Intelligence

**A Pro-grade 64 MP camera** on the Galaxy S20 Tactical Edition enhances intel gathering, even in low-light environments without a flash. Capture high-resolution photos or sharp 8K video reconnaissance without giving away your position.

### Power to extend the mission

**Keep going wherever the mission takes you** with the Galaxy S20 Tactical Edition's intelligent2 4000mAh battery is 30% larger than the previous tactical solution and optimizes energy based on your device usage. Easily share power with a team member's smartphone in the field simply by touching devices using Wireless PowerShare.[4]

### One device to meet your requirements

**Run mission applications in the field** and enterprise applications everywhere else with the powerful and efficient Galaxy S20 Tactical Edition 64-bit Octa-Core processor. Connect your device to a monitor keyboard and mouse and use the power of Samsung DeX[5] for a desktop-like experience that is ideal for mission planning, training and everyday use. DeX-in-Vehicle transforms your Galaxy S20 Tactical Edition into an in-vehicle computer.

### Open and secure

**Enable a diverse ecosystem of tactical partners** with the open and secure Android operating system on the Galaxy S20 Tactical Edition. The all-new Tactical Settings feature simplifies device management, while Samsung Knox provides defense-grade security[6] from the hardware layer up and mission-specific device customization capabilities. The DualDAR architecture of the Galaxy S20 Tactical Edition provides two layers of encryption, even when the device is powered off, for securing up-to top secret level data on the device.

### Tested and proven

Samsung Galaxy Tactical Edition smartphones are tested and proven by special operators in the field. The Galaxy S20 Tactical Edition is certified to meet the most stringent requirements including NSA's CSFC Components List, NIAP Common Criteria/MDFPP, DODIN APL, FIPS140-2, DISA Android 10 STIG, IP68 rating.

**Contact Us:** www.samsung.com/TacticalEdition

97

[97] https://image-us.samsung.com/SamsungUS/samsungbusiness/pdfs/flyer/S20_TE-salesflyer_FINAL_July_2021.pdf

The Team Awareness Kit (TAK), for civilian uses, or Tactical Assault Kit (also TAK) for military uses is a suite of software that provides geospatial information and allows user collaboration over geography. There are numerous TAK Products in the TAK family, all developed at government expense

The Team Awareness Kit for Android (ATAK, also known as CivTAK) was originally developed by the Air Force Research Laboratory (AFRL) and is now maintained by a Joint Product Center.

ATAK (including CivTAK) is an Android smartphone geospatial infrastructure and situational awareness app. It allows for precision targeting, surrounding land formation intelligence, situational awareness, navigation, and data sharing.

All the Android variants of TAK are virtually identical and all are interoperable with each other and with other TAK products. There are small, military-specific additions in military versions of ATAK.

# Features

Industry/civilian capabilities of ATAK/CivTAK include:

- Online and offline mapping (most standard formats), with a blazing fast rendering engine
- Support for very high-resolution imagery (sub 1 cm resolution)
- Collaborative mapping, including points, drawings, locations of interest
- Extensive and customizable set of Icons
- Overlay Manager which allows the Import and display of KML, KMZ, GPX overlays and maps, including online sources
- Location marking, sharing, history
- Chat, file sharing, photo sharing, video sharing, streaming
- Navigation-walking/hiking, driving, also useful flying and air-ground coordination
- Elevation Tools, heat maps, computed contour maps, viewsheds, routes w/DTED, SRTM, including dynamic profiling
- Hashtags and Sticky tags
- Center on Self, Center on other objects (e.g. another person in the network)
- Range, bearing, and other measurement tools
- Network-aware geofences with triggers
- "Bloodhound" destination tracking, including on moving objects
- Team Emergency Beacons
- Customizable Toolbar
- Radio controls and Integration
- Photo to map capability (aka Rubber Sheeting)
- Casualty evacuation tool
- Icon support for a wide variety of First Responder missions with further extensible Icons
- 3D perspective and ability to display 3D geospatial models
- Useful for First Responders, Hunting, fishing, ornithology, wildlife site survey
- An API with an SDK

[98]

[98] https://www.civtak.org/documentation/

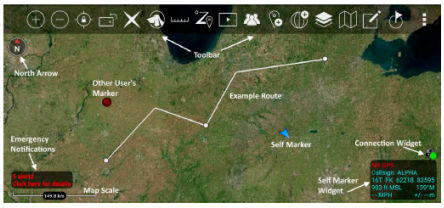
## ATAK Civilian Overview

The Civilian Team Awareness Kit for Android (ATAK Civilian) is a Government-off-the-Shelf (GOTS) software application and mapping framework for mobile devices. ATAK Civilian has been designed and developed to run on Android smart devices used in a first responder environment. The ATAK Civilian software application is an extensible moving map display that integrates imagery, map and overlay information to provide enhanced collaboration and Situational Awareness (SA) over a tactical meshed network. ATAK Civilian promotes information flow and communications from the field environment to command enterprise locations.

The first time ATAK Civilian is opened, or after a Clear Content, a passphrase is auto-generated to activate data encryption. The user can supply their own passphrase by using Settings > Show All Preferences > Device Preferences > Change Encryption Passphrase. Following this step, ATAK Civilian's End User License Agreement (EULA) must be accepted. Next, the user will be prompted to change their callsign and/or import preferences or data from a Mission Package. All changes/imports can always be updated later. Finally, the user can place their self-marker by following the instructions located in the lower right corner.

The toolbar runs along the top of the map display. The features whose icons form the center portion of the toolbar are discussed in individual sections of this guide. The three dots at the right of the toolbar provide additional menu items that appear in a drop-down menu. A Long Press on the map will toggle the toolbar between hidden and visible.

The North Arrow appears in the upper left and is used to control map orientation. It has two primary modes: North Up/Track Up (default) and Manual Map Rotation/Lock. While in North Up/Track Up Mode, single press on the [**North Arrow**] icon to cycle between the North Up and Track Up map orientation. Long press the [**North Arrow**] to call out the additional controls menu where the Manual Rotation/Lock and 3D features are available. Select the [**Rotation**] button to enter Manual Map Rotation/Lock Mode. When in Manual Map Rotation/Lock Mode, rotate the map orientation by pressing on the map with two fingers and pivoting them in the desired direction. Single press on the [**North Arrow**] to lock the screen orientation, signified by the appearance of the lock icon, and again to unlock the orientation for further adjustment. 3D controls are discussed in a separate section.




Select the [**Magnifier**] buttons to zoom in or out on the map. The map can also be zoomed by using two fingers on the screen to pinch and spread the map. Select the [**Back**] button to center the screen on the Self Marker or the [**Padlock**] icon to lock the center of the screen to the Self Marker. Select the [**Orientation**] icon to toggle the screen position between portrait and landscape.

The optional connection widget indicates whether or not the user is connected to a TAK Server. This has a corresponding Android notification that provides the same information. Toggle this display on at Settings > Network Connections > Network Connections > Display Connection Widget.

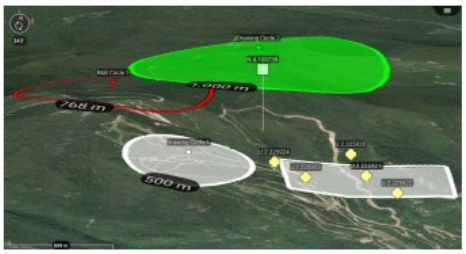
Alerts and notifications are displayed in the lower left of the map interface.

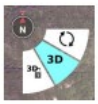
The Map Scale displays a 1 inch to X mi/km reference on the map. The scale adjusts with the map when zoomed in and out. Hint windows are available to alert users to changes or make suggestions about the use of tools the first time they are opened.





## 3D View




ATAK Civilian features 3D viewing of terrain and map items (DTED required). To enable 3D view, long press on the [**North Arrow**] to call out the additional controls menu and select [**3D**]. A tilt angle indicator will appear around the edge of the [**North Arrow**] when 3D view is active. Touch the screen with two fingers and simultaneously swipe up or down on the screen to tilt the view angle. Once the appropriate viewing angle is set, select the [**3D Lock**] button to retain this view while panning the map. While viewing the map from an angle, some map items will appear raised above the map surface if they have defined elevations.

## 3D Models

ATAK Civilian supports the use of 3D models. OBJ models and other types from products such as Pix4D can be imported via the Import Manager or can be manually placed in the atak/overlays folder prior to startup. If using Import Manager browse to the .OBJ file and import only that file, or browse to a .ZIP file that contains the .OBJ file (and others) and import only that file. If using manual placement to the atak/overlays folder, place a .ZIP file containing the .OBJ file (and others) into the directory and they will be imported on startup.

Once imported, a 3D Model icon will appear on the map. Zoom into the area of the icon until a loading ring appears. After the loading process has finished, the 3D model will be projected onto the map. Enable the map 3D View and tilt the view angle to see the 3D modeling. Loaded 3D models will appear as their own category in Overlay Manager and can be toggled on/off or removed from there.

## Placement

The user can enter locations of interest using the Point Dropper tool. Select the [**Point Dropper**] icon to place internationally standardized markers and other icons on the map, edit the data and share the markers with other network members.

### Self-Marker

The Self-Marker is displayed as a blue arrowhead at the user's current location. The options available on the Self-Marker radial are: Compass Rose, Polar Coordinate Entry, Fine Adjust/Enter Coordinate/MGRS Location, GPS Error, Range & Bearing Line, GPS Lock to Self, Tracking Breadcrumbs, Place a Marker at the user's current location and Details. Other TAK users appear on the display as a colored circle. The color of the circle represents the user's Team affiliation, with additional lettering inside the circle to identify the role the user on the team. Team Member markers that include a diagonal line indicate that the GPS location is not available. A solid icon indicated that the team member has GPS reception.

Available roles include: Team Member, Team Lead (designated by a TL in the center of the marker), Headquarters (HQ in center), Sniper (S), Medic (+), Forward Observer (FO), RTO (R) or K9 (K9). The options available when another user's Self-Marker is selected are: Inner Ring – Delete, Polar Coordinate Entry, Fine Adjust/Enter Coordinate/MGRS Location, Range & Bearing Line, GPS Lock on Friendly, Video Player (if available), Communication Options (if configured by that user), Custom Threat Rings, Tracking Breadcrumbs and Details.

Outer Ring (Communication Options) – Data Package, Email, SMS Messaging, GeoChat, VOIP and Cellular Phone, when available.



## Point Dropper

Selecting the [**Point Dropper**] icon will open the Point Dropper menu, containing marker symbology with one or more icon sets, a Recently Added button and an Iconset Manager button.

The Markers symbology affiliations are: Unknown, Neutral, Red and Friendly. Select the affiliation, then a location on the map interface to drop the marker. To add a marker by manually entering coordinates, long press on the map interface and enter the MGRS location. Change the standard naming convention by entering values into the custom prefix and index fields or leave blank to use the defaults. If values are entered, the next marker will be dropped with the prefix name and starting number(s) or letter(s) and every subsequent marker will be assigned the next consecutive number(s) or letter(s).

The user can select the mission specific pallet to open point options including Waypoint (WP), Sensor or Observation Point (OP).

The user can move between icon sets by either swiping in the icon set area or selecting on the [**Iconset Name**] field to bring up the Icon Pallet drop-down.

The last point placed is shown at the bottom of the Point Dropper window. The information for all recently placed points can be accessed by selecting the [**Clock**] icon. This displays the marker icon, name, coordinates, elevation and range & bearing information. The user can send, rename or remove any recently added markers by selecting the [**Arrows**] next to the marker to reveal [**SEND**], [**RENAME**] or [**DEL**] buttons.

Select the [**Iconset Manager**] (gear) button to add or delete icon sets or to set the default Marker Mapping.

## Radial Menus

**Unknown Object** | **Neutral Object** | **Red Object** | **Friendly Object** | **Spot Object**

The options available for Unknown Object Markers are: Delete, Polar Coordinate Entry, Fine Adjust/Enter Coordinate/MGRS Location, Range & Bearing Line, Lock On, Tasking, Custom Threat Rings, Tracking Breadcrumbs and Details.

The options available for Neutral Object Markers are: Delete, Polar Coordinate Entry, Fine Adjust/Enter Coordinate/MGRS Location, Range & Bearing Line, Lock On, Tasking, Custom Threat Rings, Tracking Breadcrumbs and Details.

The options available for Red Object Markers are: Delete, Polar Coordinate Entry, Compass Rose/Bullseye, Fine Adjust/Enter Coordinate/MGRS Location, Range & Bearing Line, Tasking, Custom Threat Rings, Tracking Breadcrumbs and Details.

The options available for Friendly Object Markers are: Delete, Polar Coordinate Entry, Fine Adjust/Enter Coordinate/MGRS Location, Range & Bearing Line, Lock On, Video, Contact Card, Custom Threat Rings, Tracking Breadcrumbs and Details. The Video radial will activate if a properly formatted packet that includes the link to the video feed is included. Select the video radial to open the associated video. The Contact Card can be selected to display additional communication options, including GeoChat, Email, VoIP, SMS Messaging and Cellular Phone, when available.

The options available for Spot Map are: Delete, Fine Adjust/Enter Coordinate/MGRS Location, Range & Bearing Line, Nav-To, Custom Threat Rings, Labels and Details.

The options for User Defined Iconsets are: Delete, Polar Coordinate Entry, Fine Adjust/Enter Coordinate/MGRS Location, Range & Bearing Line, Lock On, Tasking, Custom Threat Rings. Tracking Breadcrumbs and Details.

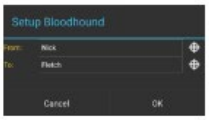
Select [**Details**] on the marker radial to make desired modifications, including: Coordinate, Elevation, Name, Type and Remarks. Selecting Marker Type opens a dialog box with extra categories. File attachments, including images, can be associated with the object by selecting the [**Paperclip**] icon. Once all the desired modifications have been made, the Marker can be sent to other network members using [**Send**]. The information can be broadcast to all members or sent to specific recipients. Select the [**Auto Send**] option to broadcast the marker to other TAK users on the network, with updates automatically sent about once every 60 seconds.



## Bloodhound Tool

The Bloodhound Tool provides support for tracking and intercepting a map item. It allows the user to select two points on the map and/or map objects and display range & bearing information between the chosen tracker and the target.

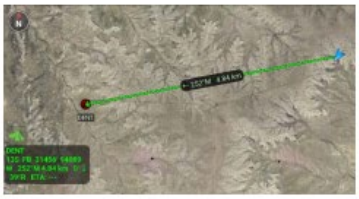
Select the [**Bloodhound**] icon to open the Bloodhound Tool. A window will open, prompting the user to choose where to start by tapping the [**From Reticle**] (default = user's self marker) and where to bloodhound (track) to by tapping the [**To Reticle**].




Targets include map objects like other User's Self Markers, DPs, Markers, Shape center points, Range & Bearing endpoints and any other map objects. If the user selects a map location instead of an object as the target, Bloodhound will place a waypoint marker there. The self marker will then track towards the waypoint.

Select [**OK**] and Bloodhound will be activated.

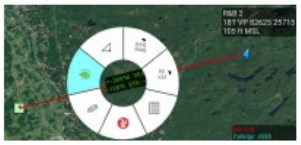
If either point moves, the green widget in the lower left will show the updated information. As the tracking object begins to navigate toward the target, the Estimated Time of Arrival (ETA) will update accordingly.



The green line showing the direct path from the tracker to the target will flash when the user-defined ETA outer threshold is reached (default = 6 minutes from target). The line will flash as the tracker continues toward the target until the next ETA threshold is reached (default = 3 minutes). The line will turn a flashing yellow until the final ETA threshold (default = 1 minute) is reached. The line then flashes red until the target is reached. Colors and thresholds can be modified in Settings > Tool Preferences > Bloodhound Preferences.

Selecting the green Bloodhound icon on the map will pan the map to the Bloodhound Range & Bearing Line. Disengage the Bloodhound Tool by selecting the [**Bloodhound**] icon on the toolbar.

## Multiple Bloodhound



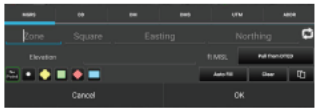
To create multiple bloodhounds, selecting the Range and Bearing Tool and select the [**R&B Line**] icon. Select two markers on the map and once the R&B line is created, select the line to bring up the radial. Select the [**Bloodhound**] radial, and the bloodhound information will be displayed on the R&B Line itself.

If either point moves, the Bloodhound information shown on the R&B Line will be updated. As the tracking object begins to navigate toward the target, the Estimated Time of Arrival (ETA) will update accordingly.

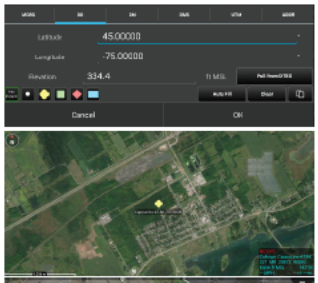
## Go To

Select the [**Go To**] icon to enter details and navigate to a specific location on the map.

Select from the [**MGRS**] (military grid reference system), [**DD**] (decimal degrees), [**DM**] (degrees- minutes), [**DMS**] (degrees-minutes-seconds), [**UTM**] (Universal Transverse Mercator) or [**ADDR**] tabs on the Go To interface and enter the location data of interest. The address provider name appears beneath the Elevation Data when the user selects the [**ADDR**] tab.




The user can enter the Latitude, Longitude and Elevation in the space provided for [**MGRS**] , [**DD**], [**D-M**] or [**D-M-S**] searches. If DTED is installed, the elevation value can be automatically populated by tapping the [**Pull From DTED**] button.The user can select a desired marker type (Spot, Unknown, Neutral, Red, or Friendly) to be placed at the entered coordinates. If [**No Point**] is selected, the map will pan to the location but will not add a point.



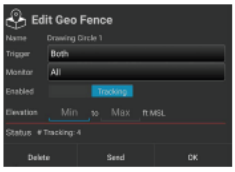
**Note:** The address provider name appears beneath the Elevation Data when the user selects the [**ADDR**] tab.

The Address Lookup provider used for the ADDR tab can be configured in the Settings > Tool Preferences > Address Lookup Preferences.

32

## Geofencing

The Geo Fence tool allows users to create a virtual fence that triggers entry/exit notifications if map items of interest cross the virtual boundary lines. The Geo Fence options are added to the existing drawing tools. After a shape has been added, the Geo Fence Tool can be accessed either by selecting the [**Geo Fence**] icon from the menu items or selecting it from the radial.




The Enabled Field slider will move to Tracking by default when a new Geo Fence window is created. Toggle the slider between Tracking and Off to enable/disable the Geo Fence. Use the Trigger field to define which types of Geo Fence breach to monitor. Choose between Entry, Exit or Both. Use the Monitor field to define which entities the Geo Fence will track.

Choose between TAK Users, Friendly, Hostile, Custom or All. Check the [**Specify Elevation**] box to enable the Elevation field, where elevation boundaries for the entities being tracked can be defined. Select the [**OK**] button to finish creating the fence. Select the [**Send**] button to create the fence and send it to another user. Select [**Delete**] to close the Create Geo Fence window and discard changes.

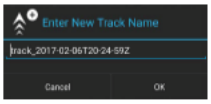
Alerts appear on the map interface. Selecting the [**Alert Notification**] will open the alerts menu, detailing the activity monitored in the user defined region. The default radius for monitoring users (filtered within the "Monitor" field) outside the Geo Fence is set at 75 km. This means the total area monitored begins at the farthest point from the center of the shape plus 75 km. If the user wishes to keep the Geo Fence, but disable tracking, the user can set the tracking [**Enabled**] to off in the Edit Window.

35

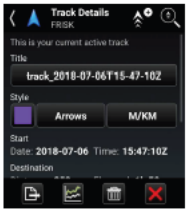
Unclassified

## Track History

The device's GPS can be used to track movements with the Track History tool. These tracked paths can be exported to a TAK server, to a route or to a KML, KMZ, GPX or CSV file. A GPS position must be established before tracking can begin.

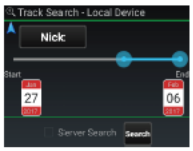



Selecting the [**Track History**] icon will open Track Details for the current active track. The track title, color and style can be modified. Initiate a new track by selecting the [**Add Track**] icon. Accept or edit the default track name and select the [**OK**] button to begin the new track. User location data is recorded as breadcrumbs in a new track file.

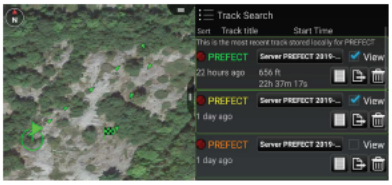



## Track Search

Use the Track Search function to view track information that has been previously saved locally or on a TAK Server. The tool searches the track database for matches against the specified time range and by user callsign. Matching tracks are displayed as a list, and can be selected to view on the map interface.




Select the [**Track Search**] icon to access the function. Specify callsign and time frame, check the box for Server Search (if desired), then select [**Search**]. The track list will appear. The query results can be sorted by Track Name or Start Time. Select any of the query results to move to that track. Once selected, the name, color, and style of a selected track can be modified or the track can be cleared. Convert a track to a TAK route or export it as a KML, KMZ, GPX or CSV file by selecting the desired track and then [**Export**]. Enter a file name then select [**Next**] and choose the export format. Select [**Done**] or [**Send**] when the export completes.



When viewing the track list, the Track History Toolbar will appear at the top of the screen. The options include [**Add a Track**], [**Multi-select**], [**Track Search**], [**Clear Tracks**] and [**Exit**]. The Track History List allows the user to select tracks of other users that have been saved on their device. The Track Search – Local Device allows the user to perform a tailored search for tracks meeting their criteria. The searching option allows the user to retrieve all the tracks on the device.

The Track History Breadcrumb and Settings can be configured in the Settings > Tools Preferences > Track History Preferences.

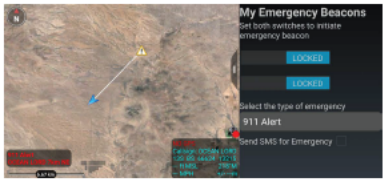
37

Unclassified

## Emergency Beacon

Select the [**Emergency Beacon**] icon to open the Emergency Beacon Tool.

The Emergency Beacon allows the user to indicate their need for assistance, the type of emergency and their location on the map. The type of emergency can be selected from the drop-down menu, before activation, and includes options for an Alert, Ring the Bell, Geo Fence Breached or In Contact.




Once the Emergency type has been selected and both switches have been enabled, the TAK Server broadcasts the announcements to all network contacts. Even if the user's device is turned off, the beacon will continue. Only when the user returns to the Emergency Beacon tool and turns off the switches will the beacon be canceled and removed. If the SMS for Emergency option has been configured, the alert will be sent via text message to the configured numbers.

99

[99] https://drive.google.com/file/d/1bo9WHadg3J3o55OLlx1mn3McqEJzvgrK/view

Home / Locate devices

# Locate devices

You can check the locations of the selected devices. Only the devices that have the location policy applied can be tracked.

To check the device locations, complete the following steps:

1. Navigate to **Device**.

2. On the "Device" page, click the checkbox for a device to check its location, and then click **Check Location**.

3. In the "Check Location" window, search by date and view the location history.

- Click **Export to GPX** to download a GPX file that includes detailed device location information. You can use a GPX viewer to open the file.

100

Home / Send device commands to users

# Send device commands to users

You can send device commands to the user's enrolled devices. For more information on each device command, see Sending device commands to devices.

To send device commands, complete the following steps:

1. Navigate to **User**.

2. On the "User" page, click the check box next to the user ID to send a device command to.

3. Click **Device Command** and select the supported OS platform (enrolled device).

4. In the "Device Command" window, select a desired device command.

5. In the "Request Command" window, click **OK**.

101

[100] https://docs.samsungknox.com/admin/knox-manage/locate-devices.htm
[101] https://docs.samsungknox.com/admin/knox-manage/send-commands-to-users-devices.htm

# Check the locations of devices

You can check the locations of the selected devices. Only the devices that have the location policy applied can be tracked.

> **NOTE** — You can only check a device's location if location data was collected at least once.

**IMPORTANT** — In order to track the location of Android 11 and 12 devices, the device user must grant the KM agent location access. This affects devices with the following deployment types:

- Employee-owned devices with a Work Profile
- Shared devices with a secondary account

You should inform users with these devices to allow the following access settings:

- Android 11:
  1. When the KM agent requests location access, the user must select **While using this app**.
  2. Then, they must go to **Work profile settings** >**Apps** >**Knox Manage** >**App permissions**, and set **Location** to **Allow all the time**.
- Android 12 and higher:
  - When the KM agent requests location access, the user must select **Precise** and **While using this app**.

1. Navigate to **Device**.
2. On the **Device** page, select one or more devices, and then click **Check Location**.
3. On the **Check Location** page, search by date. The view shows an interactive map of the devices and their location history.

On this page, you can inspect individual device information, as well as export their location history as as a GPX file.

# Device map

On the **Check Location** screen, a map displays the latest locations of all tracked devices. The map uses the following legend:

| Element | Meaning |
|---|---|
| | Active device |
| | Device with expired keepalive |
| | Cluster of 1–9 devices |
| | Cluster of 10–99 devices |
| | Cluster of 100–999 devices |
| | Cluster of 1000–9999 devices |

You can view an individual device's status by hovering over its pin . On hover, a tooltip lists the following information:

- Device name
- IMEI/MEID
- Serial Number
- Mobile Number
- User Name
- Last Location Scanned
- Organization Name
- Group Name
- Tag
- Platform & Management Type
- Model Name
- MAC Address
- Manufacturer

[102]

[102] https://docs.samsungknox.com/admin/knox-manage/check-the-locations-of-devices.htm.

74. For example, the exemplary Accused Products allow users to establish groups and to exchange messages via interaction with Samsung's servers which provide the Samsung Tactical, TAK, and ATAK applications and services and Samsung Knox applications and services, among other relevant applications and services. The exemplary Accused Products further allow users to retrieve map information from multiple sources including street-view maps.

Unclassified

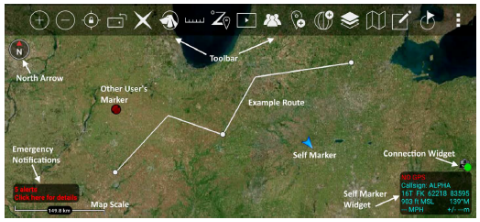
## ATAK Civilian Overview

The Civilian Team Awareness Kit for Android (ATAK Civilian) is a Government-off-the-Shelf (GOTS) software application and mapping framework for mobile devices. ATAK Civilian has been designed and developed to run on Android smart devices used in a first responder environment. The ATAK Civilian software application is an extensible moving map display that integrates imagery, map and overlay information to provide enhanced collaboration and Situational Awareness (SA) over a tactical meshed network. ATAK Civilian promotes information flow and communications from the field environment to command enterprise locations.

The first time ATAK Civilian is opened, or after a Clear Content, a passphrase is auto-generated to activate data encryption. The user can supply their own passphrase by using Settings > Show All Preferences > Device Preferences > Change Encryption Passphrase. Following this step, ATAK Civilian's End User License Agreement (EULA) must be accepted. Next, the user will be prompted to change their callsign and/or import preferences or data from a Mission Package. All changes/imports can always be updated later. Finally, the user can place their self-marker by following the instructions located in the lower right corner.

The toolbar runs along the top of the map display. The features whose icons form the center portion of the toolbar are discussed in individual sections of this guide. The three dots at the right of the toolbar provide additional menu items that appear in a drop-down menu. A Long Press on the map will toggle the toolbar between hidden and visible.

The North Arrow appears in the upper left and is used to control map orientation. It has two primary modes: North Up/Track Up (default) and Manual Map Rotation/Lock. While in North Up/Track Up Mode, single press on the [**North Arrow**] icon to cycle between the North Up and Track Up map orientation. Long press the [**North Arrow**] to call out the additional controls menu where the Manual Rotation/Lock and 3D features are available. Select the [**Rotation**] button to enter Manual Map Rotation/Lock Mode. When in Manual Map Rotation/Lock Mode, rotate the map orientation by pressing on the map with two fingers and pivoting them in the desired direction. Single press on the [**North Arrow**] to lock the screen orientation, signified by the appearance of the lock icon, and again to unlock the orientation for further adjustment. 3D controls are discussed in a separate section.




Select the [**Magnifier**] buttons to zoom in or out on the map. The map can also be zoomed by using two fingers on the screen to pinch and spread the map. Select the [**Back**] button to center the screen on the Self Marker or the [**Padlock**] icon to lock the center of the screen to the Self Marker. Select the [**Orientation**] icon to toggle the screen position between portrait and landscape.

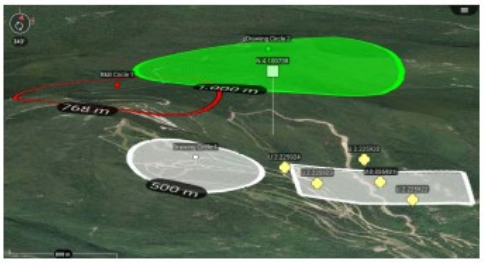
The optional connection widget indicates whether or not the user is connected to a TAK Server. This has a corresponding Android notification that provides the same information. Toggle this display on at Settings > Network Connections > Network Connections > Display Connection Widget.

Alerts and notifications are displayed in the lower left of the map interface.

The Map Scale displays a 1 inch to X mi/km reference on the map. The scale adjusts with the map when zoomed in and out. Hint windows are available to alert users to changes or make suggestions about the use of tools the first time they are opened.

5

## 3D View



ATAK Civilian features 3D viewing of terrain and map items (DTED required). To enable 3D view, long press on the **[North Arrow]** to call out the additional controls menu and select [**3D**]. A tilt angle indicator will appear around the edge of the [**North Arrow**] when 3D view is active. Touch the screen with two fingers and simultaneously swipe up or down on the screen to tilt the view angle. Once the appropriate viewing angle is set, select the [**3D Lock**] button to retain this view while panning the map. While viewing the map from an angle, some map items will appear raised above the map surface if they have defined elevations.

## 3D Models

ATAK Civilian supports the use of 3D models. OBJ models and other types from products such as Pix4D can be imported via the Import Manager or can be manually placed in the atak/overlays folder prior to startup. If using Import Manager browse to the .OBJ file and import only that file, or browse to a .ZIP file that contains the .OBJ file (and others) and import only that file. If using manual placement to the atak/overlays folder, place a .ZIP file containing the .OBJ file (and others) into the directory and they will be imported on startup.

Once imported, a 3D Model icon will appear on the map. Zoom into the area of the icon until a loading ring appears. After the loading process has finished, the 3D model will be projected onto the map. Enable the map 3D View and tilt the view angle to see the 3D modeling. Loaded 3D models will appear as their own category in Overlay Manager and can be toggled on/off or removed from there.

Unclassified

## Placement

The user can enter locations of interest using the Point Dropper tool. Select the [**Point Dropper**] icon to place internationally standardized markers and other icons on the map, edit the data and share the markers with other network members.

### Self-Marker

The Self-Marker is displayed as a blue arrowhead at the user's current location. The options available on the Self-Marker radial are: Compass Rose, Polar Coordinate Entry, Fine Adjust/Enter Coordinate/MGRS Location, GPS Error, Range & Bearing Line, GPS Lock to Self, Tracking Breadcrumbs, Place a Marker at the user's current location and Details. Other TAK users appear on the display as a colored circle. The color of the circle represents the user's Team affiliation, with additional lettering inside the circle to identify the role the user on the team. Team Member markers that include a diagonal line indicate that the GPS location is not available. A solid icon indicated that the team member has GPS reception.

Available roles include: Team Member, Team Lead (designated by a TL in the center of the marker), Headquarters (HQ in center), Sniper (S), Medic (+), Forward Observer (FO), RTO (R) or K9 (K9). The options available when another user's Self-Marker is selected are: Inner Ring – Delete, Polar Coordinate Entry, Fine Adjust/Enter Coordinate/MGRS Location, Range & Bearing Line, GPS Lock on Friendly, Video Player (if available), Communication Options (if configured by that user), Custom Threat Rings, Tracking Breadcrumbs and Details.

Outer Ring (Communication Options) – Data Package, Email, SMS Messaging, GeoChat, VOIP and Cellular Phone, when available.

Unclassified

## Radial Menus

**Unknown Object**

**Neutral Object**

**Red Object**

**Friendly Object**

**Spot Object**

The options available for Unknown Object Markers are: Delete, Polar Coordinate Entry, Fine Adjust/Enter Coordinate/MGRS Location, Range & Bearing Line, Lock On, Tasking, Custom Threat Rings, Tracking Breadcrumbs and Details.

The options available for Neutral Object Markers are: Delete, Polar Coordinate Entry, Fine Adjust/Enter Coordinate/MGRS Location, Range & Bearing Line, Lock On, Tasking, Custom Threat Rings, Tracking Breadcrumbs and Details.

The options available for Red Object Markers are: Delete, Polar Coordinate Entry, Compass Rose/Bullseye, Fine Adjust/Enter Coordinate/MGRS Location, Range & Bearing Line, Tasking, Custom Threat Rings, Tracking Breadcrumbs and Details.

The options available for Friendly Object Markers are: Delete, Polar Coordinate Entry, Fine Adjust/Enter Coordinate/MGRS Location, Range & Bearing Line, Lock On, Video, Contact Card, Custom Threat Rings, Tracking Breadcrumbs and Details. The Video radial will activate if a properly formatted packet that includes the link to the video feed is included. Select the video radial to open the associated video. The Contact Card can be selected to display additional communication options, including GeoChat, Email, VoIP, SMS Messaging and Cellular Phone, when available.

The options available for Spot Map are: Delete, Fine Adjust/Enter Coordinate/MGRS Location, Range & Bearing Line, Nav-To, Custom Threat Rings, Labels and Details.

The options for User Defined Iconsets are: Delete, Polar Coordinate Entry, Fine Adjust/Enter Coordinate/MGRS Location, Range & Bearing Line, Lock On, Tasking, Custom Threat Rings. Tracking Breadcrumbs and Details.

Select [**Details**] on the marker radial to make desired modifications, including: Coordinate, Elevation, Name, Type and Remarks. Selecting Marker Type opens a dialog box with extra categories. File attachments, including images, can be associated with the object by selecting the [**Paperclip**] icon. Once all the desired modifications have been made, the Marker can be sent to other network members using [**Send**]. The information can be broadcast to all members or sent to specific recipients. Select the [**Auto Send**] option to broadcast the marker to other TAK users on the network, with updates automatically sent about once every 60 seconds.

## Bloodhound Tool

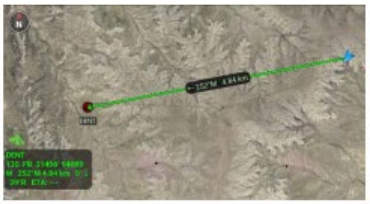
The Bloodhound Tool provides support for tracking and intercepting a map item. It allows the user to select two points on the map and/or map objects and display range & bearing information between the chosen tracker and the target.

Select the [**Bloodhound**] icon to open the Bloodhound Tool. A window will open, prompting the user to choose where to start by tapping the [**From Reticle**] (default = user's self marker) and where to bloodhound (track) to by tapping the [**To Reticle**].

Targets include map objects like other User's Self Markers, DPs, Markers, Shape center points, Range & Bearing end-points and any other map objects. If the user selects a map location instead of an object as the target, Bloodhound will place a waypoint marker there. The self marker will then track towards the waypoint.

Select [**OK**] and Bloodhound will be activated.

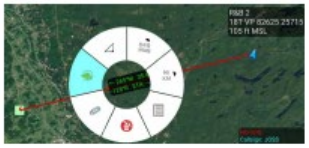
If either point moves, the green widget in the lower left will show the updated information. As the tracking object begins to navigate toward the target, the Estimated Time of Arrival (ETA) will update accordingly.



The green line showing the direct path from the tracker to the target will flash when the user-defined ETA outer threshold is reached (default = 6 minutes from target). The line will flash as the tracker continues toward the target until the next ETA threshold is reached (default = 3 minutes). The line will turn a flashing yellow until the final ETA threshold (default = 1 minute) is reached. The line then flashes red until the target is reached. Colors and thresholds can be modified in Settings > Tool Preferences > Bloodhound Preferences.

Selecting the green Bloodhound icon on the map will pan the map to the Bloodhound Range & Bearing Line. Disengage the Bloodhound Tool by selecting the [**Bloodhound**] icon on the toolbar.

## Multiple Bloodhound



To create multiple bloodhounds, selecting the Range and Bearing Tool and select the [**R&B Line**] icon. Select two markers on the map and once the R&B line is created, select the line to bring up the radial. Select the [**Bloodhound**] radial, and the bloodhound information will be displayed on the R&B Line itself.

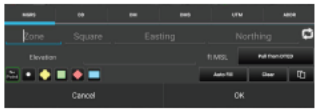
If either point moves, the Bloodhound information shown on the R&B Line will be updated. As the tracking object begins to navigate toward the target, the Estimated Time of Arrival (ETA) will update accordingly.



## Go To

Select the [**Go To**] icon to enter details and navigate to a specific location on the map.

Select from the [**MGRS**] (military grid reference system), [**DD**] (decimal degrees), [**DM**] (degrees - minutes), [**DMS**] (degrees-minutes-seconds), [**UTM**] (Universal Transverse Mercator) or [**ADDR**] tabs on the Go To interface and enter the location data of interest. The address provider name appears beneath the Elevation Data when the user selects the [**ADDR**] tab.



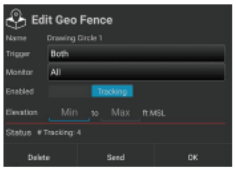

The user can enter the Latitude, Longitude and Elevation in the space provided for [**MGRS**] , [**DD**], [**D-M**] or [**D-M-S**] searches. If DTED is installed, the elevation value can be automatically populated by tapping the [**Pull From DTED**] button.The user can select a desired marker type (Spot, Unknown, Neutral, Red, or Friendly) to be placed at the entered coordinates. If [**No Point**] is selected, the map will pan to the location but will not add a point.

**Note:** The address provider name appears beneath the Elevation Data when the user selects the [**ADDR**] tab.

The Address Lookup provider used for the ADDR tab can be configured in the Settings > Tool Preferences > Address Lookup Preferences.

## Geofencing

The Geo Fence tool allows users to create a virtual fence that triggers entry/exit notifications if map items of interest cross the virtual boundary lines. The Geo Fence options are added to the existing drawing tools. After a shape has been added, the Geo Fence Tool can be accessed either by selecting the [**Geo Fence**] icon from the menu items or selecting it from the radial.




The Enabled Field slider will move to Tracking by default when a new Geo Fence window is created. Toggle the slider between Tracking and Off to enable/disable the Geo Fence. Use the Trigger field to define which types of Geo Fence breach to monitor. Choose between Entry, Exit or Both. Use the Monitor field to define which entities the Geo Fence will track.

Choose between TAK Users, Friendly, Hostile, Custom or All. Check the [**Specify Elevation**] box to enable the Elevation field, where elevation boundaries for the entities being tracked can be defined. Select the [**OK**] button to finish creating the fence. Select the [**Send**] button to create the fence and send it to another user. Select [**Delete**] to close the Create Geo Fence window and discard changes.

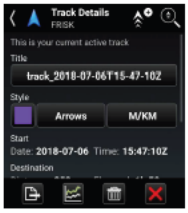
Alerts appear on the map interface. Selecting the [**Alert Notification**] will open the alerts menu, detailing the activity monitored in the user defined region. The default radius for monitoring users (filtered within the "Monitor" field) outside the Geo Fence is set at 75 km. This means the total area monitored begins at the farthest point from the center of the shape plus 75 km. If the user wishes to keep the Geo Fence, but disable tracking, the user can set the tracking [**Enabled**] to off in the Edit Window.

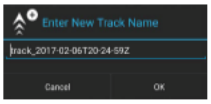
35

Unclassified

## Track History

The device's GPS can be used to track movements with the Track History tool. These tracked paths can be exported to a TAK server, to a route or to a KML, KMZ, GPX or CSV file. A GPS position must be established before tracking can begin.

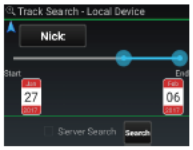


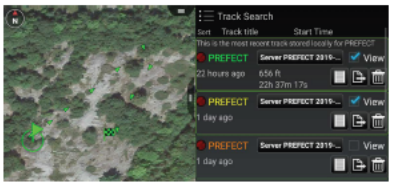

Selecting the [**Track History**] icon will open Track Details for the current active track. The track title, color and style can be modified. Initiate a new track by selecting the [**Add Track**] icon. Accept or edit the default track name and select the [**OK**] button to begin the new track. User location data is recorded as breadcrumbs in a new track file.

## Track Search

Use the Track Search function to view track information that has been previously saved locally or on a TAK Server. The tool searches the track database for matches against the specified time range and by user callsign. Matching tracks are displayed as a list, and can be selected to view on the map interface.




Select the [**Track Search**] icon to access the function. Specify callsign and time frame, check the box for Server Search (if desired), then select [**Search**]. The track list will appear. The query results can be sorted by Track Name or Start Time. Select any of the query results to move to that track. Once selected, the name, color, and style of a selected track can be modified or the track can be cleared. Convert a track to a TAK route or export it as a KML, KMZ, GPX or CSV file by selecting the desired track and then [**Export**]. Enter a file name then select [**Next**] and choose the export format. Select [**Done**] or [**Send**] when the export completes.

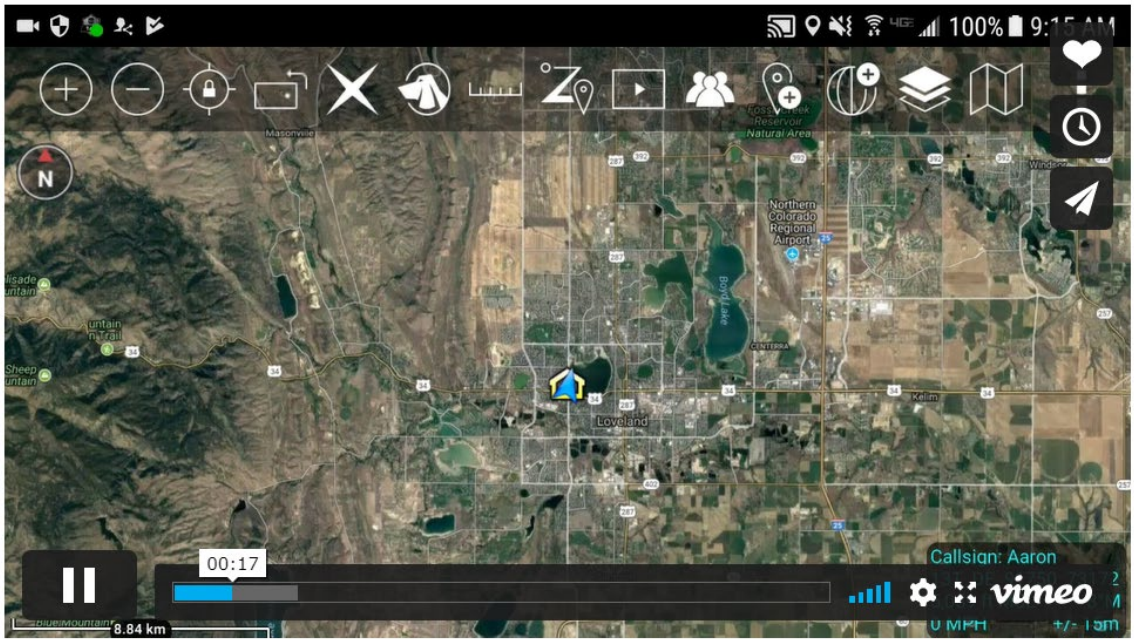


When viewing the track list, the Track History Toolbar will appear at the top of the screen. The options include [**Add a Track**], [**Multi-select**], [**Track Search**], [**Clear Tracks**] and [**Exit**]. The Track History List allows the user to select tracks of other users that have been saved on their device. The Track Search – Local Device allows the user to perform a tailored search for tracks meeting their criteria. The searching option allows the user to retrieve all the tracks on the device.

The Track History Breadcrumb and Settings can be configured in the Settings > Tools Preferences > Track History Preferences.

37 103

[103] https://drive.google.com/file/d/1bo9WHadg3J3o55OLlx1mn3McqEJzvgrK/view




104

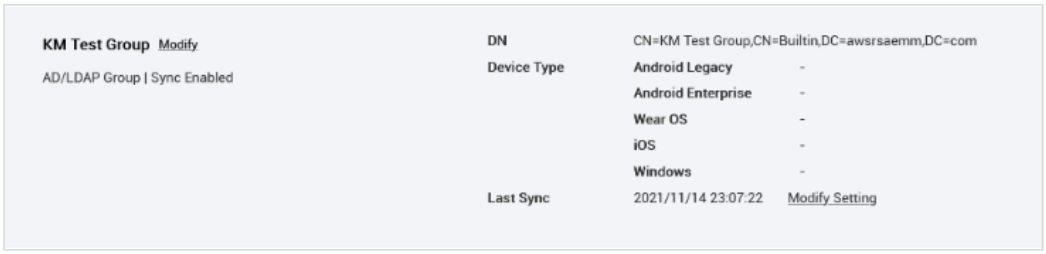
[104] https://wiki.civtak.org/index.php?title=ATAK_Manual

# View group details

View each group's details by clicking a group name on the group list.

## Summary area

The summary area contains the information about the selected group such as group and user's device types.




- **Modify** — Change the group name.
- **Modify Setting** — Modify the sync settings of the current AD/LDAP group. In the **Modify Sync Setting** window, enter the following information:
  - **AD/LDAP Sync** — Enable or disable sync services.
  - **Sync Group Member** — Select whether sync all users or only the selected users of the group. (**Do Not Sync**, **Sync All**, **Sync Selected Only**)
  - **Profile/App Auto Apply** — Select when to apply a profile or application to a group member automatically. (**When Adding a User**, **When Deleting a User**, **When Deleting a Group**)

## Tab: User (for device groups)

The **User** tab for device groups shows the information of the user's devices and user accounts in the group.

- **Detail** — Move to the **User Details** page for the selected user. For more information on the **User Details** page, see Viewing the user details.

The following function buttons are available:

| Function button | Description |
|---|---|
| Send Email | Send templates or user notifications registered in Knox Manage to users via email. For more information, see Sending templates or user notifications to users via email. |
| Request Enrollment | Send installation guides to the selected users via email and SMS. For more information, see Sending enrollment guides to users via email and SMS.<br>**NOTE** — To send enrollment guides to users via SMS, the mobile numbers of the users must be registered to their accounts. |

# Tab: Device (for device groups)

The **Device** tab for user groups shows the device status and information of the user's devices in the group.

- **Detail** — Move to the **Device Details** page for the selected user's device. For more information on the **Device Details** page, see View details of a device.

The following function buttons are available:

| Function button | Description |
|---|---|
| Refresh | Update the list of devices. |
| Revert Column Settings | Restore the default visibility of all columns. |
| Add | Add a device from the device list to the group. For more information, see Adding devices to device groups. |
| Delete | Delete the selected device from the group. |
| ⚙ | Enable or disable a column in the device list by clicking this button > **Column**, and then selecting a column. |

105

75. The exemplary Accused Products are programmed to receive messages from other devices where those messages relate to joining groups, as depicted below.

[105] https://docs.samsungknox.com/admin/knox-manage/view-details-of-group.htm.

# View group details

View each group's details by clicking a group name on the group list.

## Summary area

The summary area contains the information about the selected group such as group and user's device types.

- **Modify** — Change the group name.
- **Modify Setting** — Modify the sync settings of the current AD/LDAP group. In the **Modify Sync Setting** window, enter the following information:
  - **AD/LDAP Sync** — Enable or disable sync services.
  - **Sync Group Member** — Select whether sync all users or only the selected users of the group. (**Do Not Sync**, **Sync All**, **Sync Selected Only**)
  - **Profile/App Auto Apply** — Select when to apply a profile or application to a group member automatically. (**When Adding a User**, **When Deleting a User**, **When Deleting a Group**)

## Tab: User (for device groups)

The **User** tab for device groups shows the information of the user's devices and user accounts in the group.

- **Detail** — Move to the **User Details** page for the selected user. For more information on the **User Details** page, see Viewing the user details.

The following function buttons are available:

| Function button | Description |
|---|---|
| Send Email | Send templates or user notifications registered in Knox Manage to users via email. For more information, see Sending templates or user notifications to users via email. |
| Request Enrollment | Send installation guides to the selected users via email and SMS. For more information, see Sending enrollment guides to users via email and SMS.<br>**NOTE** — To send enrollment guides to users via SMS, the mobile numbers of the users must be registered to their accounts. |

## Tab: Device (for device groups)

The **Device** tab for user groups shows the device status and information of the user's devices in the group.

- **Detail** — Move to the **Device Details** page for the selected user's device. For more information on the **Device Details** page, see View details of a device.

The following function buttons are available:

| Function button | Description |
|---|---|
| Refresh | Update the list of devices. |
| Revert Column Settings | Restore the default visibility of all columns. |
| Add | Add a device from the device list to the group. For more information, see Adding devices to device groups. |
| Delete | Delete the selected device from the group. |
| ⚙ | Enable or disable a column in the device list by clicking this button > **Column**, and then selecting a column. |

106

76. The exemplary Accused Products are further programmed to facilitate participation in the groups by communicating with a server and sending to and receiving location information, as depicted below.

[106] https://docs.samsungknox.com/admin/knox-manage/view-details-of-group.htm.

# Command and control

**Situational awareness**
The Galaxy S20 Tactical Edition integrates voice, video, and tactical data to provide a common operational picture of the battlespace. This complete and accurate real-time intelligence enhances the precision and effectiveness of your tactical teams.

**Tactical user experience**
Unique features found only on the Galaxy S20 Tactical Edition deliver fast and simple access to the information and applications operators need on-mission.

**Better intelligence**
The pro-grade 64 MP camera on the Galaxy S20 Tactical Edition allows you to discretely capture and share crisp high-resolution photo or 8K video intelligence, even in low light without the use of a flash. View and analyze intelligence in greater detail than ever before with the Galaxy S20 Tactical Edition's Dynamic AMOLED 2.0, a 120Hz[1] display.

**Extend your mission**
The Galaxy S20 Tactical Edition battery is 30% larger than the previous tactical solution and it's intelligent.[2] It optimizes your app usage in the field giving you extended power to complete the mission. When you need a recharge, Super Fast Charging[3] and fast Wireless Charging 2.0 give you power in a flash. And Wireless PowerShare allows you to easily charge a team member's phone in the field just by touching the devices.[4]

**Connect to tactical radios** - Protocols to support tactical radios and mission systems, out of the box.

**Tactical app quick launch** - Instantly expand or hide ATAK, APASS and other mission-critical applications at the push of a button.

**Night vision mode** – Turn on and off LED backlight when wearing night vision devices.

**Stealth mode** – Disable LTE and e-911 and mute all RF broadcasting for complete off-grid communications.

**Lock screen auto-rotate** - Unlock the device in landscape mode for easy access when mounted to the operator's chest.

**Auto-touch sensitivity** – Automatically adjust device operations to work with gloved hands.

# One device to meet all your mission requirements.

**Simple device management**
From device configuration, enrollment, customization and management to advanced mobile security controls and updates, Samsung has the mobility cloud services you need for every stage of the Galaxy S20 Tactical Edition lifecycle.[8] With Knox Services, you can keep pace and maintain control over devices and how they're used. You can manage devices in near real-time, configure settings, and remotely lock or wipe devices if lost or stolen, on the battlefield and anywhere else.

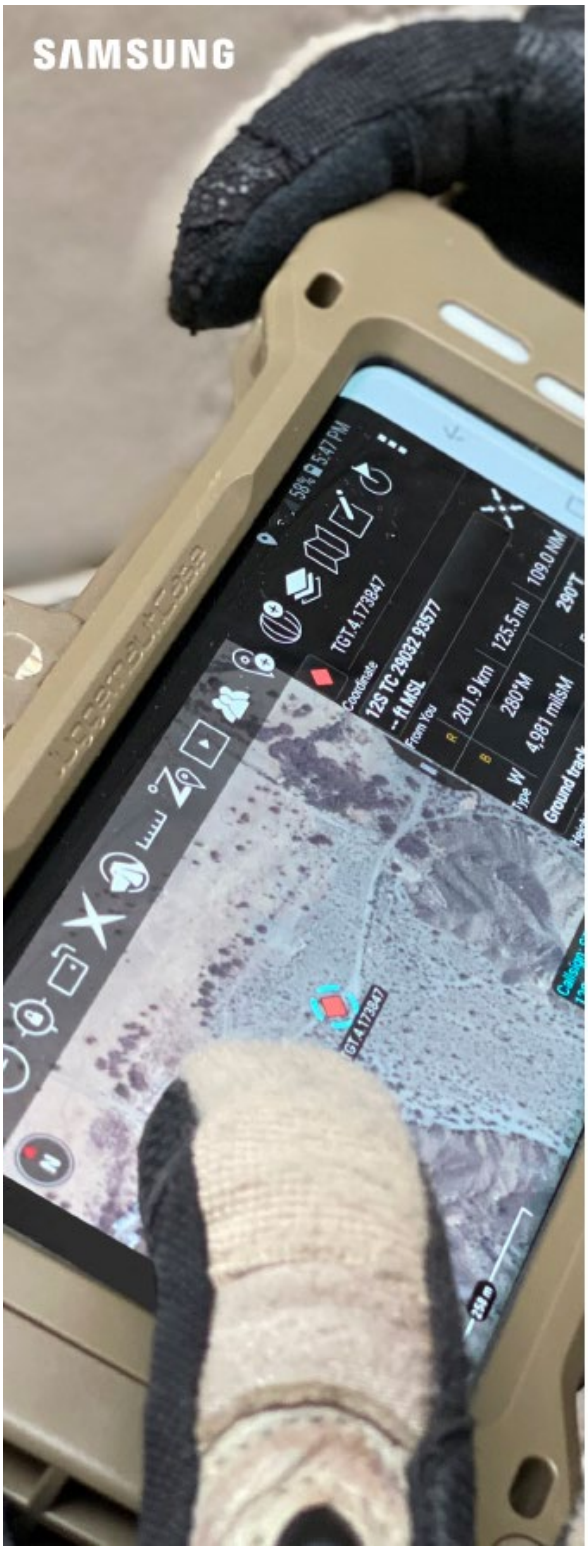
**Run mission apps and enterprise apps**
The Galaxy S20 Tactical Edition has a 64-bit Octa-Core processor with the speed and versatility to run multiple tactical applications in the field and enterprise applications everywhere else.

With Samsung DeX, connect your Galaxy S20 Tactical Edition to a monitor, keyboard and mouse for a desktop-like experience[5] ideally suited for mission planning, training, and everyday use. DeX gives you the power to work seamlessly across Microsoft Office Suite applications,[6] productivity apps, and virtual desktops with secure CAC-authenticated Virtual Desktop Infrastructure (VDI) sessions, all without a laptop.[7] And DeX-in-Vehicle transforms the Galaxy S20 Tactical Edition into a powerful in-vehicle computer.

**Open and secure**
The Galaxy S20 Tactical Edition is built on an open and secure Android operating system enabling seamless integration with a diverse ecosystem of tactical solution partners. Eliminate vulnerabilities with three software updates throughout the life of the device.

107

[107] https://www.pargovernment.com/tactical-sa/docs/S20_brochure.pdf




## Galaxy S20 Tactical Edition

# Mission-ready mobility. Proven by operators.

The Samsung Galaxy S20 Tactical Edition is the mission-ready military smartphone built and proven by operators in special operations. Based on the proven success of the S9 Tactical Edition for operators in the field, the S20 Tactical Edition is the only end user device you'll need for mission planning, training, operations and daily use.

### Persistent communications in any domain

**Purpose-built to connect to tactical radios** and mission systems out of the box, the Galaxy S20 Tactical Edition delivers a complete and accurate common operational picture. Run mission applications in the field and enterprise applications everywhere else with a single end user device for mission training, planning, operations and everyday use.

### Interoperable across devices and networks

**Pre-configured software, pre-loaded during the manufacturing process,** includes drivers to support tactical radios and mission-critical devices. Multi-ethernet capabilities provide dedicated connections to multiple mission systems including drone feeds, laser range finders, and external GPS. Support for current and next-generation networks includes Private SIM, 5G, WiFi 6 and CBRS. Allow or disallow USB peripherals based on product or vendor identifiers.

### Command and control

**Integrate voice, video and tactical data** for a complete view of the battlespace to enhance precision and effectiveness. Unique tactical features on the Galaxy S20 Tactical Edition include night-vision mode, stealth mode, lock screen autorotate, hostage negotiation mode, LTE band lock for consistent 4G connection, tactical application quick launch, to keep the operator focused on the objective, Standalone(5G)/Non-standalone (4G) modes to stay on preferred network. Preloaded tactical settings app. Ability to configure hotspot 2.0.

### Capture Intelligence

**A Pro-grade 64 MP camera** on the Galaxy S20 Tactical Edition enhances intel gathering, even in low-light environments without a flash. Capture high-resolution photos or sharp 8K video reconnaissance without giving away your position.

### Power to extend the mission

**Keep going wherever the mission takes you** with the Galaxy S20 Tactical Edition's intelligent2 4000mAh battery is 30% larger than the previous tactical solution and optimizes energy based on your device usage. Easily share power with a team member's smartphone in the field simply by touching devices using Wireless PowerShare.[1]

### One device to meet your requirements

**Run mission applications in the field** and enterprise applications everywhere else with the powerful and efficient Galaxy S20 Tactical Edition 64-bit Octa-Core processor. Connect your device to a monitor keyboard and mouse and use the power of Samsung DeX[2] for a desktop-like experience that is ideal for mission planning, training and everyday use. DeX-in-Vehicle transforms your Galaxy S20 Tactical Edition into an in-vehicle computer.

### Open and secure

**Enable a diverse ecosystem of tactical partners** with the open and secure Android operating system on the Galaxy S20 Tactical Edition. The all-new Tactical Settings feature simplifies device management, while Samsung Knox provides defense-grade security[4] from the hardware layer up and mission-specific device customization capabilities. The DualDAR architecture of the Galaxy S20 Tactical Edition provides two layers of encryption, even when the device is powered off, for securing up-to top secret level data on the device.

### Tested and proven

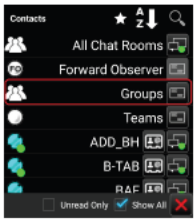
Samsung Galaxy Tactical Edition smartphones are tested and proven by special operators in the field. The Galaxy S20 Tactical Edition is certified to meet the most stringent requirements including NSA's CSFC Components List, NIAP Common Criteria/MDFPP, DODIN APL, FIPS 140-2, DISA Android 10 STIG, IP68 rating.

**Contact Us:** www.samsung.com/TacticalEdition

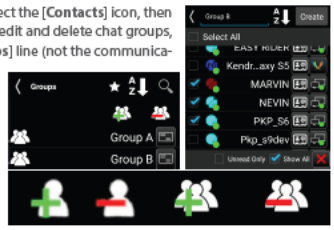
Unclassified

## GeoChat Group Management

Text-based Chat messages may be sent to active network members by using the GeoChat function. To enter GeoChat Group Management, select the [**Contacts**] icon and select [**GeoChat**] from the drop-down menu.

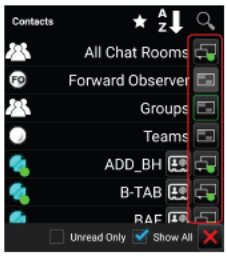



GeoChat Group Management is initiated through Contacts. Select the [**Contacts**] icon, then select GeoChat from the drop-down. The user can now create, edit and delete chat groups, as well as sub-groups. To create a chat group, select the [**Groups**] line (not the communications button). Select the [**Add Group**] icon to create the name of the group and add contacts to the group and then select [**Create**]. If a parent group is being created, no contacts need to be added at this level. To add a nested group, tap the parent group, select the [**Add Group**] icon to create the name of the sub-group and add contacts. Groups may be managed using the options to add/delete contacts or to add/delete GeoChat group.




To add users to a group, select the [**Groups**] line (not the communications button), then select the name of the group to add users. Select the [**Add Users**] icon. A window will open allowing the group creater to add users to the selected group. Select the [**Add**] button when all the users to be added are checked.

## GeoChat Messaging




Group and person-to-person messaging is available. To view messages from or send messages to an individual, tap on the desired contact's [**Communication**] icon. Selecting the [**Pan To**] icon, located at the top right of the call sign in an individual chat, will pan the map interface to that user's location. Select [**All Chat Rooms**] to view all messages from or send messages to those present on the network or TAK Server. Other groupings available for viewing or sending messages are: Forward Observer, Groups, HQ, K9, Medic, RTO, Sniper, Team Lead and Teams. If the user's current role is Forward Observer, HQ, K9, Medic, RTO, Sniper or Team Lead, that user can view or send messages to all other contacts with the same role. If a GeoChat message is sent from the top level of Teams, it will be sent to all contacts, similar to [**All Chat Rooms**].

When a sub-Team is chosen, messages can only be sent to that user's active (My Team) team color. When a parent group is chosen, messages are sent to all members of the parent group, as well as all of the sub-groups. When a sub-group is chosen, messages are sent only to members of the sub-group. Individuals within GeoChat may be removed from the Contacts menu by toggling the visibility of individuals or groups within Overlay Manager.

26

Unclassified

## GeoChat Messaging (continued)

Selecting in the Free Text Entry area will open an onscreen keyboard. At the bottom of the Chat area are pre-defined messages that may be used to quickly create a message to send. Tap the current menu button to scroll through the different menus of canned messages, including: DFLT1, DFLT2, ASLT1, ASLT2, RECON1 and RECON2. These pre-defined messages present an easy way to transmit a brief message to other network members concerning position or other important communication. The pre-defined messages may be changed by long pressing on the button and changing its label and corresponding value.

A numbered red dot will appear on the [**Contacts**] icon when a message has been received successfully. The number denotes the number of unread messages that have been received. Select this icon to view the contact list. The user name who sent the message will appear with a numbered red dot next to their name. Alternatively, the text of the message can be read by dragging down from the top to see the Android notifications window. This notification will only stay available for a short time.

[108] https://image-us.samsung.com/SamsungUS/samsungbusiness/pdfs/flyer/S20_TE-salesflyer_FINAL_July_2021.pdf

## Go To

Select the [**Go To**] icon to enter details and navigate to a specific location on the map.

Select from the [**MGRS**] (military grid reference system), [**DD**] (decimal degrees), [**DM**] (degrees- minutes), [**DMS**] (degrees-minutes-seconds), [**UTM**] (Universal Transverse Mercator) or [**ADDR**] tabs on the Go To interface and enter the location data of interest. The address provider name appears beneath the Elevation Data when the user selects the [**ADDR**] tab.

The user can enter the Latitude, Longitude and Elevation in the space provided for [**MGRS**] , [**DD**], [**D-M**] or [**D-M-S**] searches. If DTED is installed, the elevation value can be automatically populated by tapping the [**Pull From DTED**] button.The user can select a desired marker type (Spot, Unknown, Neutral, Red, or Friendly) to be placed at the entered coordinates. If [**No Point**] is selected, the map will pan to the location but will not add a point.

**Note:** The address provider name appears beneath the Elevation Data when the user selects the [**ADDR**] tab.

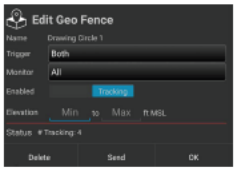
The Address Lookup provider used for the ADDR tab can be configured in the Settings > Tool Preferences > Address Lookup Preferences.



32

## Geofencing

The Geo Fence tool allows users to create a virtual fence that triggers entry/exit notifications if map items of interest cross the virtual boundary lines. The Geo Fence options are added to the existing drawing tools. After a shape has been added, the Geo Fence Tool can be accessed either by selecting the [**Geo Fence**] icon from the menu items or selecting it from the radial.




The Enabled Field slider will move to Tracking by default when a new Geo Fence window is created. Toggle the slider between Tracking and Off to enable/disable the Geo Fence. Use the Trigger field to define which types of Geo Fence breach to monitor. Choose between Entry, Exit or Both. Use the Monitor field to define which entities the Geo Fence will track.

Choose between TAK Users, Friendly, Hostile, Custom or All. Check the [**Specify Elevation**] box to enable the Elevation field, where elevation boundaries for the entities being tracked can be defined. Select the [**OK**] button to finish creating the fence. Select the [**Send**] button to create the fence and send it to another user. Select [**Delete**] to close the Create Geo Fence window and discard changes.

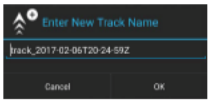
Alerts appear on the map interface. Selecting the [**Alert Notification**] will open the alerts menu, detailing the activity monitored in the user defined region. The default radius for monitoring users (filtered within the "Monitor" field) outside the Geo Fence is set at 75 km. This means the total area monitored begins at the farthest point from the center of the shape plus 75 km. If the user wishes to keep the Geo Fence, but disable tracking, the user can set the tracking [**Enabled**] to off in the Edit Window.

35

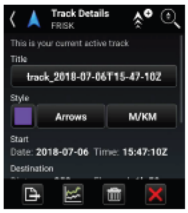
Unclassified

## Track History

The device's GPS can be used to track movements with the Track History tool. These tracked paths can be exported to a TAK server, to a route or to a KML, KMZ, GPX or CSV file. A GPS position must be established before tracking can begin.

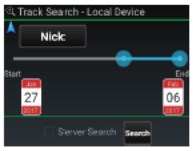



Selecting the [**Track History**] icon will open Track Details for the current active track. The track title, color and style can be modified. Initiate a new track by selecting the [**Add Track**] icon. Accept or edit the default track name and select the [**OK**] button to begin the new track. User location data is recorded as breadcrumbs in a new track file.

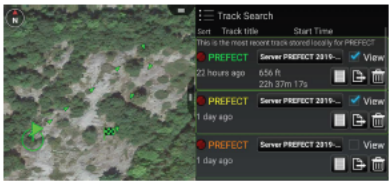



## Track Search

Use the Track Search function to view track information that has been previously saved locally or on a TAK Server. The tool searches the track database for matches against the specified time range and by user callsign. Matching tracks are displayed as a list, and can be selected to view on the map interface.




Select the [**Track Search**] icon to access the function. Specify callsign and time frame, check the box for Server Search (if desired), then select [**Search**]. The track list will appear. The query results can be sorted by Track Name or Start Time. Select any of the query results to move to that track. Once selected, the name, color, and style of a selected track can be modified or the track can be cleared. Convert a track to a TAK route or export it as a KML, KMZ, GPX or CSV file by selecting the desired track and then [**Export**]. Enter a file name then select [**Next**] and choose the export format. Select [**Done**] or [**Send**] when the export completes.



When viewing the track list, the Track History Toolbar will appear at the top of the screen. The options include [**Add a Track**], [**Multi-select**], [**Track Search**], [**Clear Tracks**] and [**Exit**]. The Track History List allows the user to select tracks of other users that have been saved on their device. The Track Search – Local Device allows the user to perform a tailored search for tracks meeting their criteria. The searching option allows the user to retrieve all the tracks on the device.

The Track History Breadcrumb and Settings can be configured in the Settings > Tools Preferences > Track History Preferences.

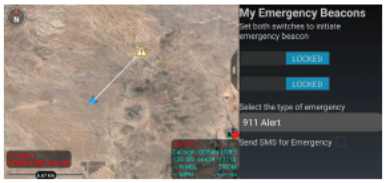
37

Unclassified

## Emergency Beacon

Select the [**Emergency Beacon**] icon to open the Emergency Beacon Tool.

The Emergency Beacon allows the user to indicate their need for assistance, the type of emergency and their location on the map. The type of emergency can be selected from the drop-down menu, before activation, and includes options for an Alert, Ring the Bell, Geo Fence Breached or In Contact.




Once the Emergency type has been selected and both switches have been enabled, the TAK Server broadcasts the announcements to all network contacts. Even if the user's device is turned off, the beacon will continue. Only when the user returns to the Emergency Beacon tool and turns off the switches will the beacon be canceled and removed. If the SMS for Emergency option has been configured, the alert will be sent via text message to the configured numbers.

109

[109] https://drive.google.com/file/d/1bo9WHadg3J3o55OLlx1mn3McqEJzvgrK/view

# Check the locations of devices

You can check the locations of the selected devices. Only the devices that have the location policy applied can be tracked.

> **NOTE** — You can only check a device's location if location data was collected at least once.

**IMPORTANT** — In order to track the location of Android 11 and 12 devices, the device user must grant the KM agent location access. This affects devices with the following deployment types:

- Employee-owned devices with a Work Profile
- Shared devices with a secondary account

You should inform users with these devices to allow the following access settings:

- Android 11:
  1. When the KM agent requests location access, the user must select **While using this app**.
  2. Then, they must go to **Work profile settings** >**Apps** >**Knox Manage** >**App permissions**, and set **Location** to **Allow all the time**.
- Android 12 and higher:
  - When the KM agent requests location access, the user must select **Precise** and **While using this app**.

1. Navigate to **Device**.
2. On the **Device** page, select one or more devices, and then click **Check Location**.
3. On the **Check Location** page, search by date. The view shows an interactive map of the devices and their location history.

On this page, you can inspect individual device information, as well as export their location history as as a GPX file.

# Device map

On the **Check Location** screen, a map displays the latest locations of all tracked devices. The map uses the following legend:

| Element | Meaning |
|---|---|
| | Active device |
| | Device with expired keepalive |
| | Cluster of 1–9 devices |
| | Cluster of 10–99 devices |
| | Cluster of 100–999 devices |
| | Cluster of 1000–9999 devices |

You can view an individual device's status by hovering over its pin . On hover, a tooltip lists the following information:

- Device name
- IMEI/MEID
- Serial Number
- Mobile Number
- User Name
- Last Location Scanned
- Organization Name
- Group Name
- Tag
- Platform & Management Type
- Model Name
- MAC Address
- Manufacturer

[110]

[110] https://docs.samsungknox.com/admin/knox-manage/check-the-locations-of-devices.htm.

77. This location information is presented on interactive displays on the exemplary Accused Products which include interactive maps and a plurality of user selectable symbols corresponding to other devices. These symbols are positioned on the map at positions corresponding to the locations of the other devices, as depicted below.

# One device to meet all your mission requirements.

**Simple device management**
From device configuration, enrollment, customization and management to advanced mobile security controls and updates, Samsung has the mobility cloud services you need for every stage of the Galaxy S20 Tactical Edition lifecycle.[8] With Knox Services, you can keep pace and maintain control over devices and how they're used. You can manage devices in near real-time, configure settings, and remotely lock or wipe devices if lost or stolen, on the battlefield and anywhere else.

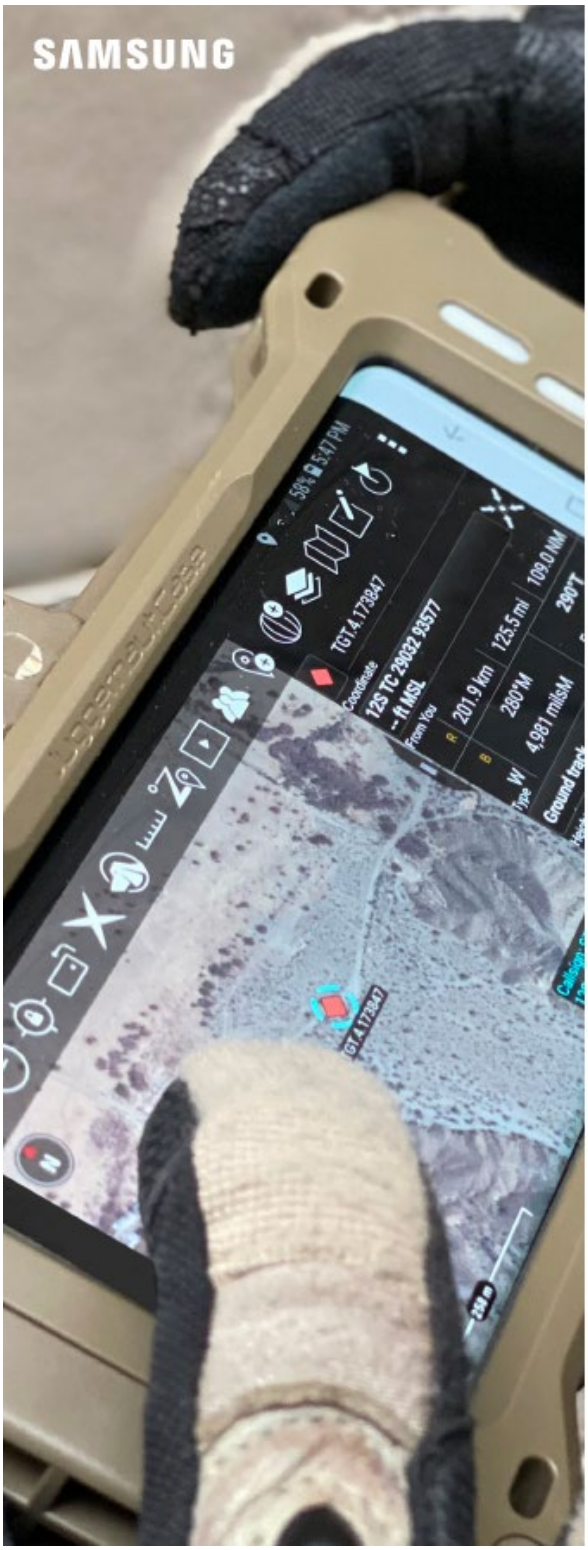
**Run mission apps and enterprise apps**
The Galaxy S20 Tactical Edition has a 64-bit Octa-Core processor with the speed and versatility to run multiple tactical applications in the field and enterprise applications everywhere else.

With Samsung DeX, connect your Galaxy S20 Tactical Edition to a monitor, keyboard and mouse for a desktop-like experience[5] ideally suited for mission planning, training, and everyday use. DeX gives you the power to work seamlessly across Microsoft Office Suite applications,[6] productivity apps, and virtual desktops with secure CAC-authenticated Virtual Desktop Infrastructure (VDI) sessions, all without a laptop.[7] And DeX-in-Vehicle transforms the Galaxy S20 Tactical Edition into a powerful in-vehicle computer.

**Open and secure**
The Galaxy S20 Tactical Edition is built on an open and secure Android operating system enabling seamless integration with a diverse ecosystem of tactical solution partners. Eliminate vulnerabilities with three software updates throughout the life of the device.

111

[111] https://www.pargovernment.com/tactical-sa/docs/S20_brochure.pdf




# Galaxy S20 Tactical Edition

## Mission-ready mobility. Proven by operators.

The Samsung Galaxy S20 Tactical Edition is the mission-ready military smartphone built and proven by operators in special operations. Based on the proven success of the S9 Tactical Edition for operators in the field, the S20 Tactical Edition is the only end user device you'll need for mission planning, training, operations and daily use.

### Persistent communications in any domain

**Purpose-built to connect to tactical radios** and mission systems out of the box, the Galaxy S20 Tactical Edition delivers a complete and accurate common operational picture. Run mission applications in the field and enterprise applications everywhere else with a single end user device for mission training, planning, operations and everyday use.

### Interoperable across devices and networks

**Pre-configured software, pre-loaded during the manufacturing process,** includes drivers to support tactical radios and mission-critical devices. Multi-ethernet capabilities provide dedicated connections to multiple mission systems including drone feeds, laser range finders, and external GPS. Support for current and next-generation networks includes Private SIM, 5G, WiFi 6 and CBRS. Allow or disallow USB peripherals based on product or vendor identifiers.

### Command and control

**Integrate voice, video and tactical data** for a complete view of the battlespace to enhance precision and effectiveness. Unique tactical features on the Galaxy S20 Tactical Edition include night-vision mode, stealth mode, lock screen autorotate, hostage negotiation mode, LTE band lock for consistent 4G connection, tactical application quick launch, to keep the operator focused on the objective, Standalone(5G)/Non-standalone (4G) modes to stay on preferred network. Preloaded tactical settings app. Ability to configure hotspot 2.0.

### Capture Intelligence

**A Pro-grade 64 MP camera** on the Galaxy S20 Tactical Edition enhances intel gathering, even in low-light environments without a flash. Capture high-resolution photos or sharp 8K video reconnaissance without giving away your position.

### Power to extend the mission

**Keep going wherever the mission takes you** with the Galaxy S20 Tactical Edition's intelligent2 4000mAh battery is 30% larger than the previous tactical solution and optimizes energy based on your device usage. Easily share power with a team member's smartphone in the field simply by touching devices using Wireless PowerShare.[1]

### One device to meet your requirements

**Run mission applications in the field** and enterprise applications everywhere else with the powerful and efficient Galaxy S20 Tactical Edition 64-bit Octa-Core processor. Connect your device to a monitor keyboard and mouse and use the power of Samsung DeX[2] for a desktop-like experience that is ideal for mission planning, training and everyday use. DeX-in-Vehicle transforms your Galaxy S20 Tactical Edition into an in-vehicle computer.

### Open and secure

**Enable a diverse ecosystem of tactical partners** with the open and secure Android operating system on the Galaxy S20 Tactical Edition. The all-new Tactical Settings feature simplifies device management, while Samsung Knox provides defense-grade security[4] from the hardware layer up and mission-specific device customization capabilities. The DualDAR architecture of the Galaxy S20 Tactical Edition provides two layers of encryption, even when the device is powered off, for securing up-to top secret level data on the device.

### Tested and proven

Samsung Galaxy Tactical Edition smartphones are tested and proven by special operators in the field. The Galaxy S20 Tactical Edition is certified to meet the most stringent requirements including NSA's CSFC Components List, NIAP Common Criteria/MDFPP, DODIN APL, FIPS 140-2, DISA Android 10 STIG, IP68 rating.

**Contact Us:** www.samsung.com/TacticalEdition

112

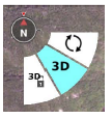
Unclassified

## ATAK Civilian Overview

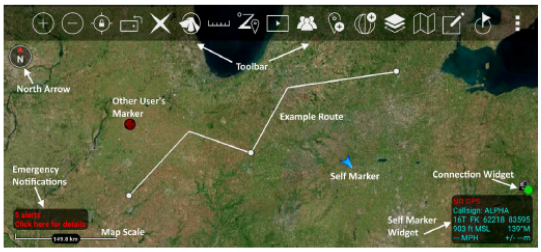
The Civilian Team Awareness Kit for Android (ATAK Civilian) is a Government-off-the-Shelf (GOTS) software application and mapping framework for mobile devices. ATAK Civilian has been designed and developed to run on Android smart devices used in a first responder environment. The ATAK Civilian software application is an extensible moving map display that integrates imagery, map and overlay information to provide enhanced collaboration and Situational Awareness (SA) over a tactical meshed network. ATAK Civilian promotes information flow and communications from the field environment to command enterprise locations.

The first time ATAK Civilian is opened, or after a Clear Content, a passphrase is auto-generated to activate data encryption. The user can supply their own passphrase by using Settings > Show All Preferences > Device Preferences > Change Encryption Passphrase. Following this step, ATAK Civilian's End User License Agreement (EULA) must be accepted. Next, the user will be prompted to change their callsign and/or import preferences or data from a Mission Package. All changes/imports can always be updated later. Finally, the user can place their self-marker by following the instructions located in the lower right corner.

The toolbar runs along the top of the map display. The features whose icons form the center portion of the toolbar are discussed in individual sections of this guide. The three dots at the right of the toolbar provide additional menu items that appear in a drop-down menu. A Long Press on the map will toggle the toolbar between hidden and visible.




The North Arrow appears in the upper left and is used to control map orientation. It has two primary modes: North Up/Track Up (default) and Manual Map Rotation/Lock. While in North Up/Track Up Mode, single press on the [**North Arrow**] icon to cycle between the North Up and Track Up map orientation. Long press the [**North Arrow**] to call out the additional controls menu where the Manual Rotation/Lock and 3D features are available. Select the [**Rotation**] button to enter Manual Map Rotation/Lock Mode. When in Manual Map Rotation/Lock Mode, rotate the map orientation by pressing on the map with two fingers and pivoting them in the desired direction. Single press on the [**North Arrow**] to lock the screen orientation, signified by the appearance of the lock icon, and again to unlock the orientation for further adjustment. 3D controls are discussed in a separate section.




Select the [**Magnifier**] buttons to zoom in or out on the map. The map can also be zoomed by using two fingers on the screen to pinch and spread the map. Select the [**Back**] button to center the screen on the Self Marker or the [**Padlock**] icon to lock the center of the screen to the Self Marker. Select the [**Orientation**] icon to toggle the screen position between portrait and landscape.

The optional connection widget indicates whether or not the user is connected to a TAK Server. This has a corresponding Android notification that provides the same information. Toggle this display on at Settings > Network Connections > Network Connections > Display Connection Widget.

Alerts and notifications are displayed in the lower left of the map interface.

The Map Scale displays a 1 inch to X mi/km reference on the map. The scale adjusts with the map when zoomed in and out. Hint windows are available to alert users to changes or make suggestions about the use of tools the first time they are opened.

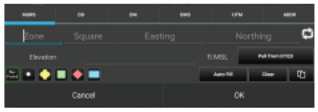
5

[112] https://image-us.samsung.com/SamsungUS/samsungbusiness/pdfs/flyer/S20_TE-salesflyer_FINAL_July_2021.pdf

## Go To

Select the [**Go To**] icon to enter details and navigate to a specific location on the map.

Select from the [**MGRS**] (military grid reference system), [**DD**] (decimal degrees), [**DM**] (degrees- minutes), [**DMS**] (degrees-minutes-seconds), [**UTM**] (Universal Transverse Mercator) or [**ADDR**] tabs on the Go To interface and enter the location data of interest. The address provider name appears beneath the Elevation Data when the user selects the [**ADDR**] tab.



The user can enter the Latitude, Longitude and Elevation in the space provided for [**MGRS**] , [**DD**], [**D-M**] or [**D-M-S**] searches. If DTED is installed, the elevation value can be automatically populated by tapping the [**Pull From DTED**] button.The user can select a desired marker type (Spot, Unknown, Neutral, Red, or Friendly) to be placed at the entered coordinates. If [**No Point**] is selected, the map will pan to the location but will not add a point.

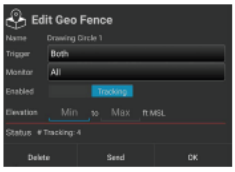
**Note:** The address provider name appears beneath the Elevation Data when the user selects the [**ADDR**] tab.

The Address Lookup provider used for the ADDR tab can be configured in the Settings > Tool Preferences > Address Lookup Preferences.

32

## Geofencing

The Geo Fence tool allows users to create a virtual fence that triggers entry/exit notifications if map items of interest cross the virtual boundary lines. The Geo Fence options are added to the existing drawing tools. After a shape has been added, the Geo Fence Tool can be accessed either by selecting the [**Geo Fence**] icon from the menu items or selecting it from the radial.




The Enabled Field slider will move to Tracking by default when a new Geo Fence window is created. Toggle the slider between Tracking and Off to enable/disable the Geo Fence. Use the Trigger field to define which types of Geo Fence breach to monitor. Choose between Entry, Exit or Both. Use the Monitor field to define which entities the Geo Fence will track.

Choose between TAK Users, Friendly, Hostile, Custom or All. Check the [**Specify Elevation**] box to enable the Elevation field, where elevation boundaries for the entities being tracked can be defined. Select the [**OK**] button to finish creating the fence. Select the [**Send**] button to create the fence and send it to another user. Select [**Delete**] to close the Create Geo Fence window and discard changes.

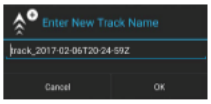
Alerts appear on the map interface. Selecting the [**Alert Notification**] will open the alerts menu, detailing the activity monitored in the user defined region. The default radius for monitoring users (filtered within the "Monitor" field) outside the Geo Fence is set at 75 km. This means the total area monitored begins at the farthest point from the center of the shape plus 75 km. If the user wishes to keep the Geo Fence, but disable tracking, the user can set the tracking [**Enabled**] to off in the Edit Window.

35

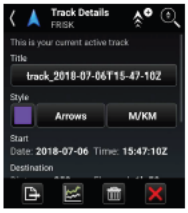
Unclassified

## Track History

The device's GPS can be used to track movements with the Track History tool. These tracked paths can be exported to a TAK server, to a route or to a KML, KMZ, GPX or CSV file. A GPS position must be established before tracking can begin.

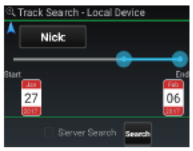



Selecting the [**Track History**] icon will open Track Details for the current active track. The track title, color and style can be modified. Initiate a new track by selecting the [**Add Track**] icon. Accept or edit the default track name and select the [**OK**] button to begin the new track. User location data is recorded as breadcrumbs in a new track file.

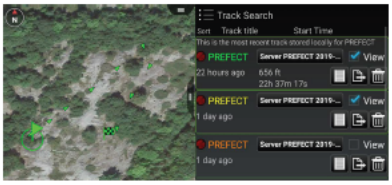



## Track Search

Use the Track Search function to view track information that has been previously saved locally or on a TAK Server. The tool searches the track database for matches against the specified time range and by user callsign. Matching tracks are displayed as a list, and can be selected to view on the map interface.




Select the [**Track Search**] icon to access the function. Specify callsign and time frame, check the box for Server Search (if desired), then select [**Search**]. The track list will appear. The query results can be sorted by Track Name or Start Time. Select any of the query results to move to that track. Once selected, the name, color, and style of a selected track can be modified or the track can be cleared. Convert a track to a TAK route or export it as a KML, KMZ, GPX or CSV file by selecting the desired track and then [**Export**]. Enter a file name then select [**Next**] and choose the export format. Select [**Done**] or [**Send**] when the export completes.



When viewing the track list, the Track History Toolbar will appear at the top of the screen. The options include [**Add a Track**], [**Multi-select**], [**Track Search**], [**Clear Tracks**] and [**Exit**]. The Track History List allows the user to select tracks of other users that have been saved on their device. The Track Search – Local Device allows the user to perform a tailored search for tracks meeting their criteria. The searching option allows the user to retrieve all the tracks on the device.

The Track History Breadcrumb and Settings can be configured in the Settings > Tools Preferences > Track History Preferences.

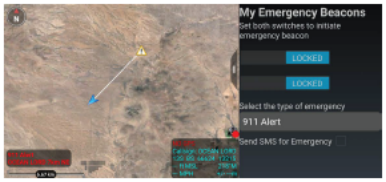
37

Unclassified

## Emergency Beacon

Select the [**Emergency Beacon**] icon to open the Emergency Beacon Tool.

The Emergency Beacon allows the user to indicate their need for assistance, the type of emergency and their location on the map. The type of emergency can be selected from the drop-down menu, before activation, and includes options for an Alert, Ring the Bell, Geo Fence Breached or In Contact.




Once the Emergency type has been selected and both switches have been enabled, the TAK Server broadcasts the announcements to all network contacts. Even if the user's device is turned off, the beacon will continue. Only when the user returns to the Emergency Beacon tool and turns off the switches will the beacon be canceled and removed. If the SMS for Emergency option has been configured, the alert will be sent via text message to the configured numbers.

113

[113] https://drive.google.com/file/d/1bo9WHadg3J3o55OLlx1mn3McqEJzvgrK/view

# Device map

On the **Check Location** screen, a map displays the latest locations of all tracked devices. The map uses the following legend:

| Element | Meaning |
|---|---|
| | Active device |
| | Device with expired keepalive |
| | Cluster of 1–9 devices |
| | Cluster of 10–99 devices |
| | Cluster of 100–999 devices |
| | Cluster of 1000–9999 devices |

You can view an individual device's status by hovering over its pin . On hover, a tooltip lists the following information:

- Device name
- IMEI/MEID
- Serial Number
- Mobile Number
- User Name
- Last Location Scanned
- Organization Name
- Group Name
- Tag
- Platform & Management Type
- Model Name
- MAC Address
- Manufacturer

114

[114] https://docs.samsungknox.com/admin/knox-manage/check-the-locations-of-devices.htm.

78. The exemplary Accused Products are further programmed to permit users to request and display additional maps by, for example, moving the map screen and/or by selecting satellite image maps. The exemplary Accused Products are further programmed to permit interaction with the display where a user may select one or more symbols and where the exemplary Accused Products further permit data to be sent to other devices based on that interaction.

79. AGIS Software has suffered damages as a result of Defendants' direct and indirect infringement of the '123 Patent in an amount to be proved at trial.

80. AGIS Software has suffered, and will continue to suffer, irreparable harm as a result of Defendants' infringement of the '123 Patent for which there is no adequate remedy at law unless Defendants' infringement is enjoined by this Court.

81. Defendants have committed and continue to commit acts of infringement that Defendants actually knew or should have known constituted an unjustifiably high risk of infringement of at least one valid and enforceable claim of the '123 Patent. Defendants' infringement of the '123 Patent has been and continues to be willful, entitling AGIS Software to an award of treble damages, reasonable attorney fees, and costs in bringing this action.

## DEMAND FOR JURY TRIAL

Plaintiff hereby demands a jury for all issues so triable.

## PRAYER FOR RELIEF

WHEREFORE, AGIS Software prays for relief against Defendants as follows:

a. Entry of judgment declaring that Defendants have directly and/or indirectly infringed one or more claims of each of the Patents-in-Suit;

b. Entry of judgment declaring that Defendants' infringement of the Patents-in-Suit has been willful and deliberate;

c. An order pursuant to 35 U.S.C. § 283 permanently enjoining Defendants, their officers, agents, servants, employees, attorneys, and those persons in active concert or participation with them, from further acts of infringement of the Patents-in-Suit;

d. An order awarding damages sufficient to compensate AGIS Software for Defendants' infringement of the Patents-in-Suit including, but not limited to, lost profits or at a minimum reasonable royalties, together with pre- and post-judgment interest and costs;

e. An order awarding AGIS Software all ongoing lost profits, royalties, and/or other damages caused by Defendants' continuing infringement of the Patents-in-Suit;

f. An order awarding AGIS Software treble damages under 35 U.S.C. § 284 as a result of Defendants' willful and deliberate infringement of the Patents-in-Suit;

g. Entry of judgment declaring that this case is exceptional and awarding AGIS Software its costs and reasonable attorney fees under 35 U.S.C. § 285; and

h. Such other and further relief as the Court deems just and proper.

Dated: June 16, 2023

Respectfully submitted,

*/s/Alfred R. Fabricant*

Alfred R. Fabricant
NY Bar No. 2219392
Email: ffabricant@fabricantllp.com
Peter Lambrianakos
NY Bar No. 2894392
Email: plambrianakos@fabricantllp.com
Vincent J. Rubino, III
NY Bar No. 4557435
Email: vrubino@fabricantllp.com
**FABRICANT LLP**
411 Theodore Fremd Avenue,
Suite 206 South
Rye, New York 10580
Telephone: (212) 257-5797
Facsimile: (212) 257-5796

Samuel F. Baxter
Texas State Bar No. 01938000
sbaxter@mckoolsmith.com
Jennifer L. Truelove
Texas State Bar No. 24012906
jtruelove@mckoolsmith.com
**MCKOOL SMITH, P.C.**
104 E. Houston Street, Suite 300
Marshall, Texas 75670
Telephone: (903) 923-9000
Facsimile: (903) 923-9099

**ATTORNEYS FOR PLAINTIFF, AGIS SOFTWARE DEVELOPMENT LLC**