XStealth PRO

TACTICAL DPC

DEVICE POLICY CONTROL

- Mission-Ready Stealth Phone
- Device Policy Management
- Device Owner & Profile Owner
- Security Controls
- Application Management
- User Restrictions
- Network Configuration
- And More

FOR DEFENSE, INTELLIGENCE, OR HARSH OPERATIONAL ENVIRONMENTS AND RELIABLE MISSION-CRITICAL COMMUNICATIONS

This User Manual covers only the use of the Tactical DPC application, which is installed by default on XStealth PRO Tactical. For the XStealth PRO Tactical User Manual, please read the manual here.

IF SOMETHING GOES WRONG OR YOU ARE BLOCKED INTO A SETTING YOU CAN'T UNDERSTAND OR DISABLE, DO NOT FACTORY RESET THE DEVICE! THIS WILL PERMANENTLY DELETE ALL YOUR DATA AND UNINSTALL ALL SPECIAL APPS! ONLY TRY TO RESTART THE DEVICE.

DO NOT CHANGE DEFAULT SETTINGS UNLESS YOU KNOW WHAT YOU ARE DOING!

Contents

XStealth PRO VERSIONS: SIMILARITIES AND DIFFERENCES

SIMILARITIES

SIMILARITIES	
Tactical	Dominator
Same hardware platform (same custom-built cell phone)	
Same OS (X-OS, our proprietary Android fork), same UI	
Same special apps & functions: IMEI change, IMSI change, Encrypted SMS and calls, XTerminator, native anti-virus, SATcom, etc.	
100% degoogled (no Google Play Store, no Google apps, no Google dependencies)	
ZERO IMEI feature	
Cell Tower Lock	

No Bluetooth (permanently removed)
GPS toggle
Camera and mics removal by request
No wireless ADB (permanently removed)

DIFFERENCES

	XStealth PRO Tactical	XStealth PRO Dominator
SOFTWARE APPS		
Tactical DPC app	Yes	No
FOSS app stores (non-Google)	No	Yes
Persistent folder	No	Yes
HARDWARE		
Disable Camera	Yes, ON/OFF toggle switch	By request
Disable Mic	Yes, ON/OFF toggle switch	By request
Block USB-C port (USB data transfer)	Yes, ON/OFF toggle switch	By request
Files folder	Removal by request	Removal by request
Mute Audio	Yes, ON/OFF toggle switch	No
Block/Unblock Cell Broadcast Service	Yes	No
WI-FI management	Yes	No
Block WIFI settings	Yes, ON/OFF toggle switch	No
Block mobile network configuration	Yes, ON/OFF toggle switch	No
Block mounting physical media (Micro-SD card)	Yes, ON/OFF toggle switch	No
Keyboard lock, disable other input methods than the AOSP keyboard	Yes, ON/OFF toggle switch	No
Block outgoing calls	Yes, ON/OFF toggle switch	No
Block safe boot	Yes, ON/OFF toggle switch	No
Block printing services	Yes, ON/OFF toggle switch	No
Monitoring & Alerts		
Apps monitoring: install/uninstall/modify/update	Yes	No
Alert on package changes: new app installation, existing app update and/or uninstallation	Yes	No
SOFTWARE SECURITY FEATURES		
Block App installation	Yes, ON/OFF toggle switch	No
Block existing App uninstallation/removal	Yes, ON/OFF toggle switch	No
Hide/Unhide installed apps	Yes, ON/OFF toggle switch	No

App suspension	Yes, ON/OFF toggle switch	No
Enable/Disable apps	Yes, ON/OFF toggle switch	No
Block developer mode	Yes, ON/OFF toggle switch	No
Disable screen capture	Yes, ON/OFF toggle switch	No
Tactical mode	Yes, ON/OFF toggle switch	No
Common Criteria mode	Yes, ON/OFF toggle switch	No
Private DNS mode	Automatic + user settings (ON/OFF)	Automatic
App permissions management	Automatic	Manual
Password management policy	Yes	No

WHAT IS Xstealth PRO Tactical?

While XStealth PRO Dominator is a commercial, everyday-use Stealth Phone developed as a privacy-oriented, secure smartphone, XStealth PRO Tactical is different: it has no app stores, no new apps can be installed, no web browser, and the Files folder, camera, and microphone are removed (by request). All these, while the phone user or their organization has total control over the phone, to cater to the unique requirements of tactical teams operating in the field.
XStealth PRO Tactical is a mission-ready Stealth Phone, a specialized, hardened mobile device built for defense, tactical, and high-security environments. It features full hardware-level security, true "off-grid" capabilities, and a Stealth Mode designed to operate in hostile, silent, or surveillance-heavy operational theaters (IMEI & IMSI change, Cell tower lock, encrypted voice and text comms, cross-platform encrypted comms, interception and location tracking alerts, over-the-air IMSI catcher attack capabilities via XTerminator, etc.).

Being a top-tier tactical secure phone is defined by several core military-grade features.

Tactical Features & Hardware

Tactical Application Support:

Pre-loaded with Tactical DPC, a mission-ready software for real-time situational awareness and enhanced security policies.

Mission-ready security:

Secure from the inside out with a hardened OS, encrypted storage, and protected communications. Maintain complete control of devices, app management, and compliance. No bloatware and regular updates to ensure your mission stays protected.

True Stealth Mode:

A hardened Airplane mode (Shield mode) that mutes all RF broadcasts (Wi-Fi, Cellular), allowing for completely off-grid passive mobile network monitoring.

Software Kill Switches:

Software switches that cut the camera and microphone to prevent snooping. The phone has neither Bluetooth nor wireless ADB.

Security & Software

Encrypted Operating Systems:

Runs on a forked Android OS architecture (X-ROM) to eliminate backdoors and facilitate secure inter-device communications.

Ideal for mission-critical demands:

No app stores, no web browser, no Bluetooth, and the user cannot install new apps or update/remove existing ones.

Serverless operating environment:

Eliminates the need for a data connection, streamlining setup for tactical teams working in remote locations without immediate data connectivity. Needs no internet.

Free to use:

No fees, no contract, no special SIM card required. No other strings attached.

Designed from the ground up for security and resilience, this Stealth Phone delivers encrypted baseband communications in contested environments. It supports data and multimedia-heavy military applications, all at the cost of a commercial smartphone. With it, forces gain enhanced situational awareness and the

tools they need to succeed in their mission. XStealth PRO Tactical features advanced situational-awareness tools that help tactical teams stay alert in the field and enhance their decision-making capabilities. It is always ready for tactical environments and mission requirements. Ready when you are.

WHAT IS Tactical DPC?

The new solutions take security a step further with a Device Policy Control App (DPC), one of the strongest layers of defense-in-depth to prevent hacking of all types, communications interception, and awareness alerts. By utilizing DPC, the solutions enforce restrictions on app installation/uninstallation, connectivity, device owner and user accounts, thereby enhancing control and safeguarding. Tactical DPC is a reference implementation of Android Enterprise Device Policy Controller. It enables administrators and/or users to configure Android device management policies in Device Owner and Profile Owner modes.

KEY POINTS:

- Device Policy Management – Applies Android Enterprise device management policies.
- Device Owner Mode – Manages the entire device, including security settings, restrictions, and system policies.
- Profile Owner Mode – Creates and manages a separate work profile while leaving the personal profile independent.
- Security Controls – Configures password requirements, screen lock policies, encryption settings, and other security options.
- Application Management – Enables, disables, hides, suspends, or permits applications according to configured policies.
- User Restrictions – Controls access to selected device features, such as cameras, screen capture, USB file transfer, and app installation.
- Network Configuration – Supports configuration of managed Wi-Fi networks, VPN settings, certificates, and other enterprise networking features.
- Certificate Management – Installs and manages CA certificates and client certificates for enterprise authentication.
- Logging and Diagnostics – Provides access to various Android Enterprise policy information, security logs (where available), and device management status.

REQUIREMENTS

There are different requirements depending on whether you are a Single User, a Managed User of a Private Enterprise/Private Sector Organization, or a state-owned enterprise (SOE).

Single User (private person)

There are no special requirements for a Single User (private person).

The Tactical DPC app comes preinstalled on your XStealth PRO Tactical phone. It acts as a device owner app, giving you full control over app management, user restrictions, and network configuration, among other security features. No need to run Android Enterprise via a Mobile Device Management (MDM). Also, no need for security certificates or any other Android Enterprise requirements. Just launch the Tactical DPC app and take advantage of being a Device Owner (DO).

What can you do as a Single User?
You can:

- Block new app installations.
- Block existing app uninstallation/removal.
- Hide/Unhide installed apps.
- Suspend apps.
- Enable/Disable apps.
- Block developer mode launching.
- Disable screen capture.
- Disable Camera.
- Disable Mic.
- Block USB-C port (USB data transfer).
- Mute Audio.
- Block/Unblock Cell Broadcast Service.
- Manage WI-FI connection.
- Block WIFI settings.
- Block mobile network configuration.
- Block mounting physical media (Micro-SD card).
- Lock the Keyboard, disable other input methods than the AOSP keyboard.
- Block outgoing calls.
- Block safe boot.
- Block printing services.
- Monitor app install/uninstall/modify/update.
- Get alerts on package changes: new app installation, existing app update, and/or uninstallation.
- Launch Tactical mode.
- Launch Common Criteria mode.
- Launch Private DNS mode.
- Manage apps permissions.
- Manage password policy.

Supplementary security measures you can take:

- Set up a password/PIN to restrict Tactical DPC access via System Manager > App Lock, so only you can use the app and have 100% control over the device.
- Enable a password /PIN to open the phone's Settings app (lock the Settings via System Manager > App Lock > Settings).

- Enable Secure Wipe, Self-Destruct, and XDuress apps, which protect against brute-force attacks, password guessing, and other hacking attempts to open the phone.

Managed User / Tactical team

It requires Android Enterprise to connect your device to an enterprise mobility or Mobile Device Management (MDM) solution, typically provided by your organization's IT admin. Contact your IT department to find out which MDM provider they use (common ones include Microsoft Intune Company Portal or Google Endpoint Management).

If XStealth PRO Tactical is an organization-owned device and needs to be fully managed by your organization (with no personal space), you will likely need to perform a factory reset. Your IT admin will give you a specific QR code or token (e.g., by typing afw#setup on the Google sign-in screen) to scan or enter on the welcome screen to finalize the enterprise setup. In this situation, you are not the Device Owner but only a Managed User with restricted rights to use the device, per mission requirements.

If your organization does not have access to any of the above, please contact us or your reseller for further arrangements.

What you can do as a Tactical team / Corporate user

Use of XStealth PRO Tactical can be restricted by your organization (PSO) or SOE. It usually involves a password-protected / PIN-access to the Tactical DPC app, so only the organization can decide how you use the device during the assigned mission.

Besides the actions you can take as a Private User, your organization can:

- Manage the entire device, including security settings, restrictions, and system policies.
- Apply Android Enterprise device management policies.
- Create and manage a separate work profile while leaving the personal profile independent.
- Configure password requirements, screen lock policies, encryption settings, and other security options.
- Apply Managed User Restrictions, controlling access to selected device features, such as cameras, screen capture, USB file transfer, and app installation.
- Manage app use – Enable, disable, hide, suspend, or permit applications according to configured policies.
- Control access to selected device features, such as cameras, screen capture, USB file transfer, and app installation.
- Install and manage CA certificates and client certificates for enterprise authentication.

Supplementary security measures DO (Device Owner - Private Enterprise/Private Sector Organization, or SOE) can take:

- Set up a password/PIN to restrict Tactical DPC access via System Manager > App Lock, so no one can use the app and have no control over the device.
- Enable a password /PIN to open the phone's Settings app (lock the Settings via System Manager > App Lock > Settings).
- Enable Secure Wipe, Self-Destruct, and XDuress apps, which protect against brute-force attacks, password guessing, and other hacking attempts to open the phone.

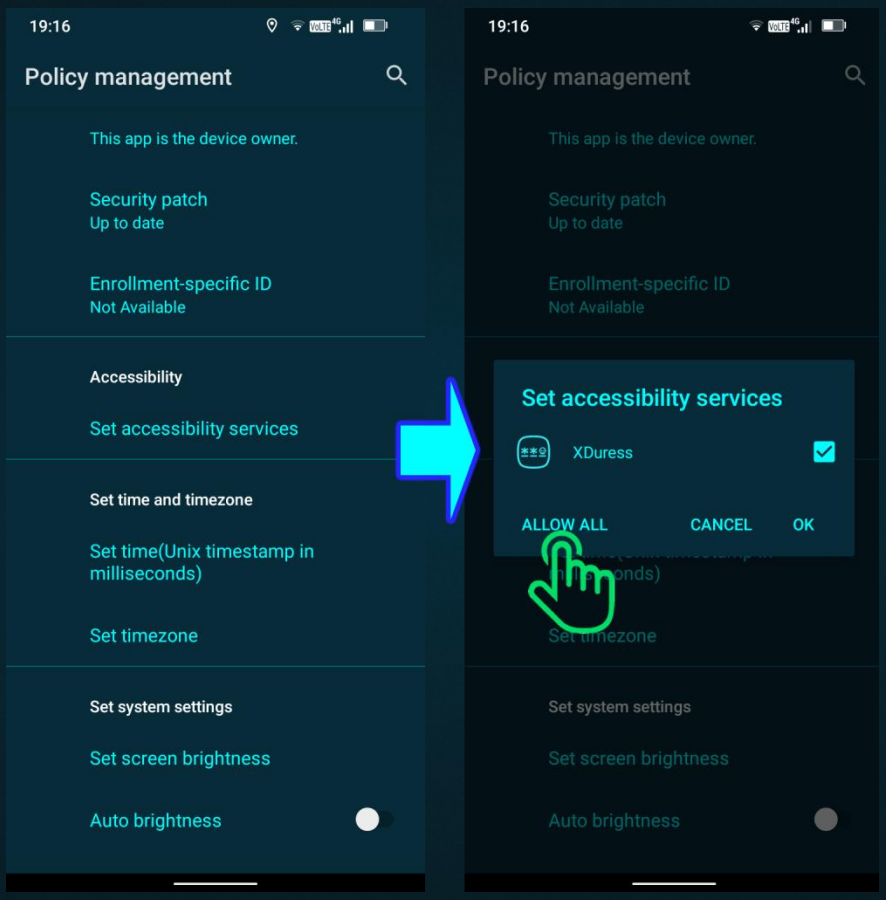
HOW TO USE Tactical DPC? FEATURES AND SETTINGS

The phone is delivered with all the settings you need enabled, so you don't really have to change any unless you need to.

Accessibility

You can set which installed apps have access to accessibility services. Tap on "ALLOW ALL". The XDuress app should be checked on the list. No need to change this setting. "ALLOW ALL" is already set up.

Do not uncheck XDuress.



Accessibility settings

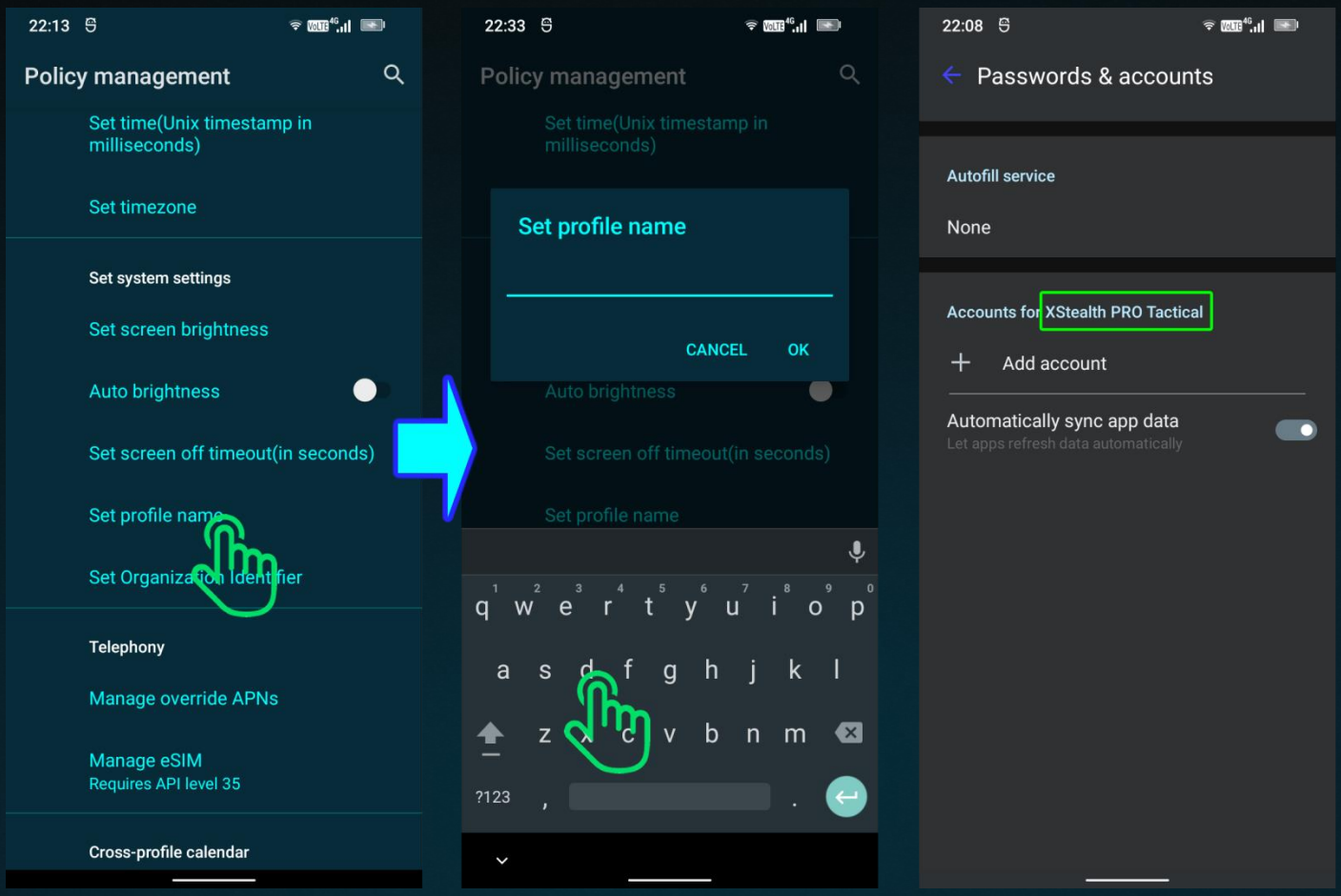
Set time and timezone

You can set the device time zone and Unix timestamp. No actions are needed; the app reads the time from the phone. However, you can modify the time zone from this section.

Set system settings

- **Set screen brightness**. Self explanatory.
- **Auto brightness (on/off)**. Self explanatory.

- **Set screen off timeout (in seconds)**. Self explanatory.
- **Set profile name**. You can manage the profile name from Tactical DPC settings, by going to Set system settings > Set profile name > add whatever name you want > tap OK.
- **Set Organization Identifier**. The organization's IT admin should do this.



Set profile name

Telephony

- **Manage override APNs** > Override APN management. Here, you can enter an APN so the phone uses only that specific APN, even if other APNs are added to the phone's settings. You can insert, remove, and enable APNs for override.

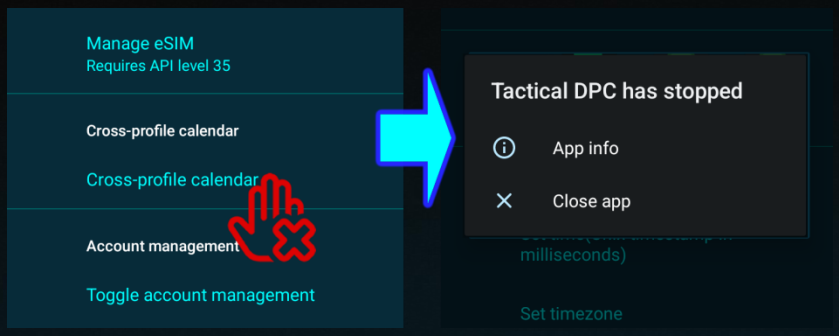
  ⚠ To be used only if you know what you are doing! Otherwise, no internet connection will be available.

  ✅ We recommend using the APN provided by your network carrier.
- **Manage eSIM**. The settings are available only if an eSIM is active on the phone, and require API level 35 (Android 15). Not available on XStealth PRO versions.

  ⚠ Using an e-SIM is not recommended; it disables the alerts the phone displays during RF baseband attacks.

Cross-profile calendar

⚠ If tapped, the app will crash if no profile has been added by the organization's IT admin beforehand.



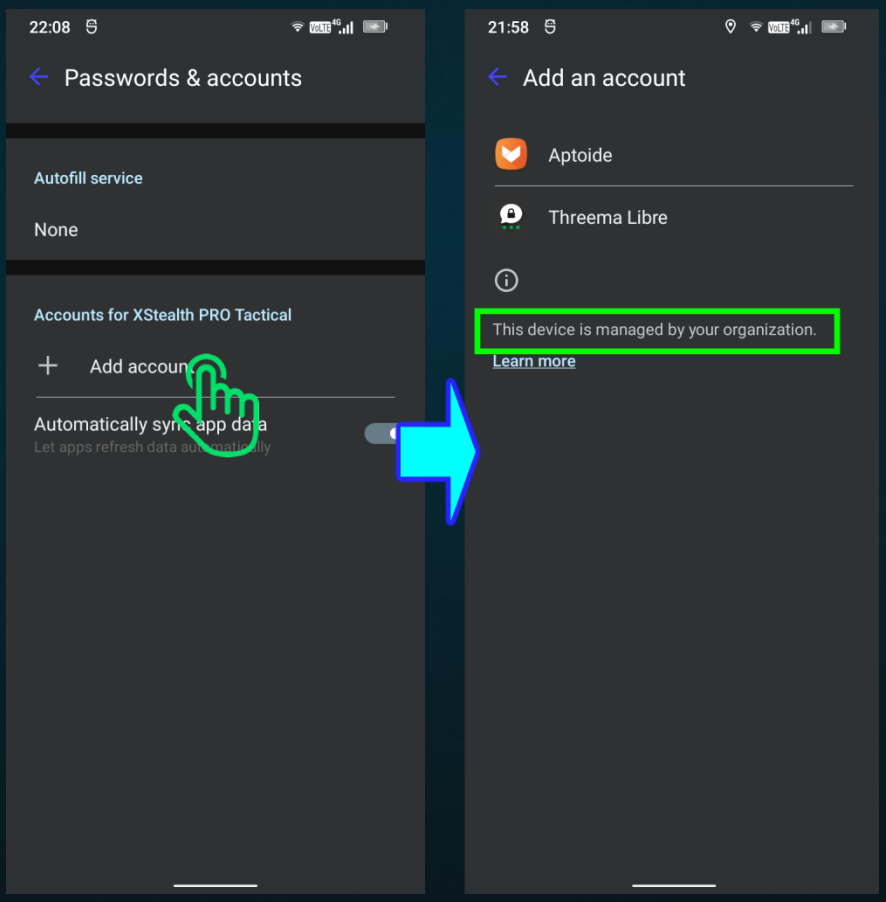
Cross-profile calendar

Account management

Here, only your organization can manage all accounts, including adding a new one.

⚠ You cannot add a new Managed account or remove an existing one already created by the DO. There is nothing you can do in this section; only your organization's IT admin can

⚠ You cannot add a Google / Personal account to your device. When going to device Settings > Passwords & accounts > Add account, this setting is managed by the DO (Tactical DPC). Adding a Personal account on a Tactical device is locked due to mission security requirements.



Profile name

⚠ An account added via Tactical DPC cannot be removed from device Settings > Passwords accounts, but only via Tactical DPC settings, by your organization's IT manager.

⚠ Adding a personal account on a Tactical device is blocked due to mission-oriented use.

Apps management

- **Enable system apps**: you can enable system apps that were disabled previously (if any).
- **Enable a system app by package name**. Self-explanatory.
- **Enable a system app by intent**. A custom action can be added. You need advanced Android programming skills to use this setting.

  To be used only if you know what you are doing!
- **Install an existing package**. You can install an APK file that is already contained in the phone's internal memory.
- **Install package from APK file**. Self-explanatory.
- **Uninstall package**. You can uninstall any app, including system ones.

  The phone can brick! To be used with precautions!
- **Hide apps**. Here, you can hide any installed app, including system and special apps.

  Tactical scenario: In a covert action, you can hide the special apps during a cross-border phone check, so the phone looks unsuspicious even after unlocking the phone screen on demand.

  IMPORTANT: while a special app is in a hidden state, it will not work! Unhide the app before using it!
- **Hide apps on parent**. Requires an organization-owned profile owner added by your organization's IT admin.
- **Unhide apps**. Self-explanatory.
- **Unhide apps on parent**. Requires an organization-owned profile owner added by your organization's IT admin.
- **Suspend apps**. You can select which app activity is suspended, including system and special apps. A suspended app will not work, but will remain visible on the phone.
- **Unsuspend apps**. Self-explanatory.
- **Clear app data**. System and regular/3rd-party app data can be cleared.

  DO NOT CLEAR SPECIAL APP DATA! If cleared, special apps stop working. App restoring is not possible.
- **Keep uninstalled packages**.

  To be used only if you know what you are doing!
- **Managed configurations**. You can check the restrictions in every app's manifest. Requires advanced Android programming skills.
- **Disable metered data**. Metered data refers to internet connections with strict data caps, limits, or per-megabyte costs. A metered connection tells your phone to restrict heavy background data and block large automatic downloads, ensuring you do not exceed your data limit or incur extra charge.

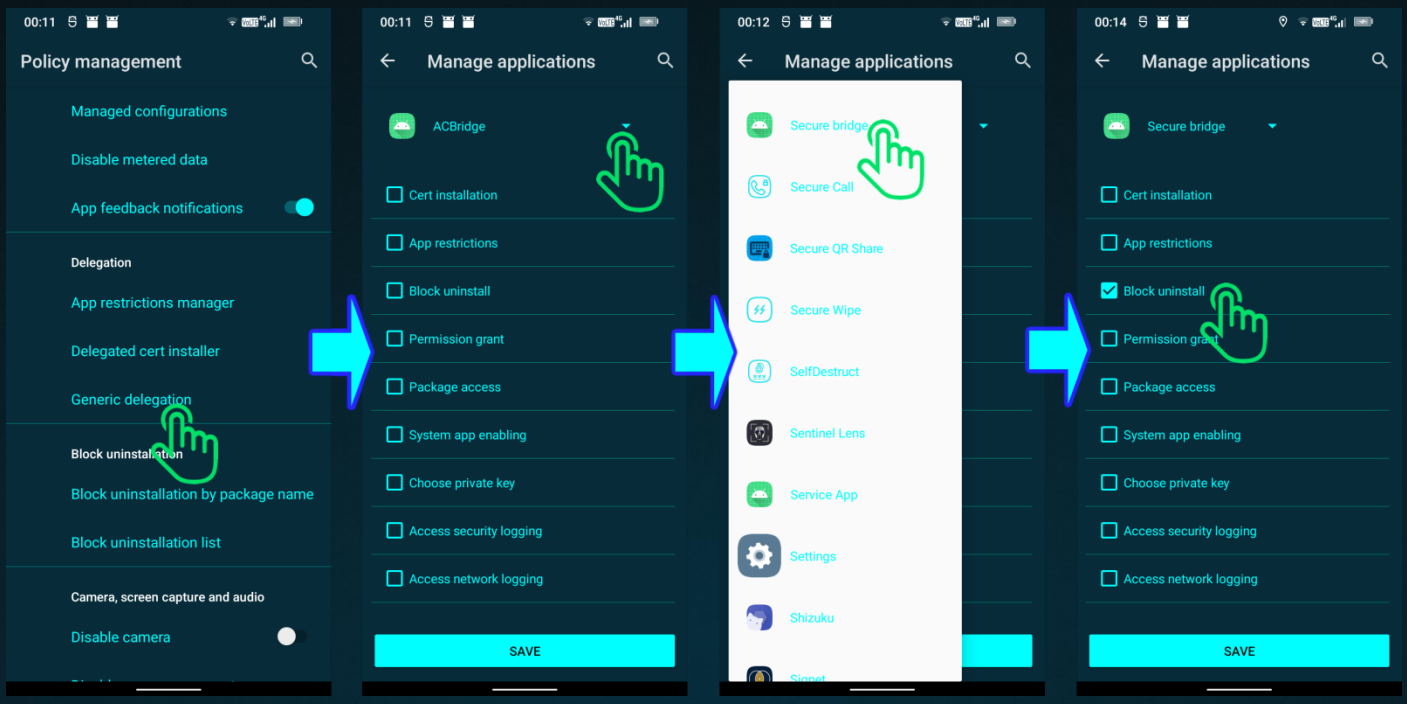
  To be used only if you know what you are doing!
- **App feedback notifications**. Enable/disable Tactical DPC notifications.

Delegation

- **App restrictions manager**. You can set/clear every app restriction.

  ⚠ Requires advanced Android programming skills.

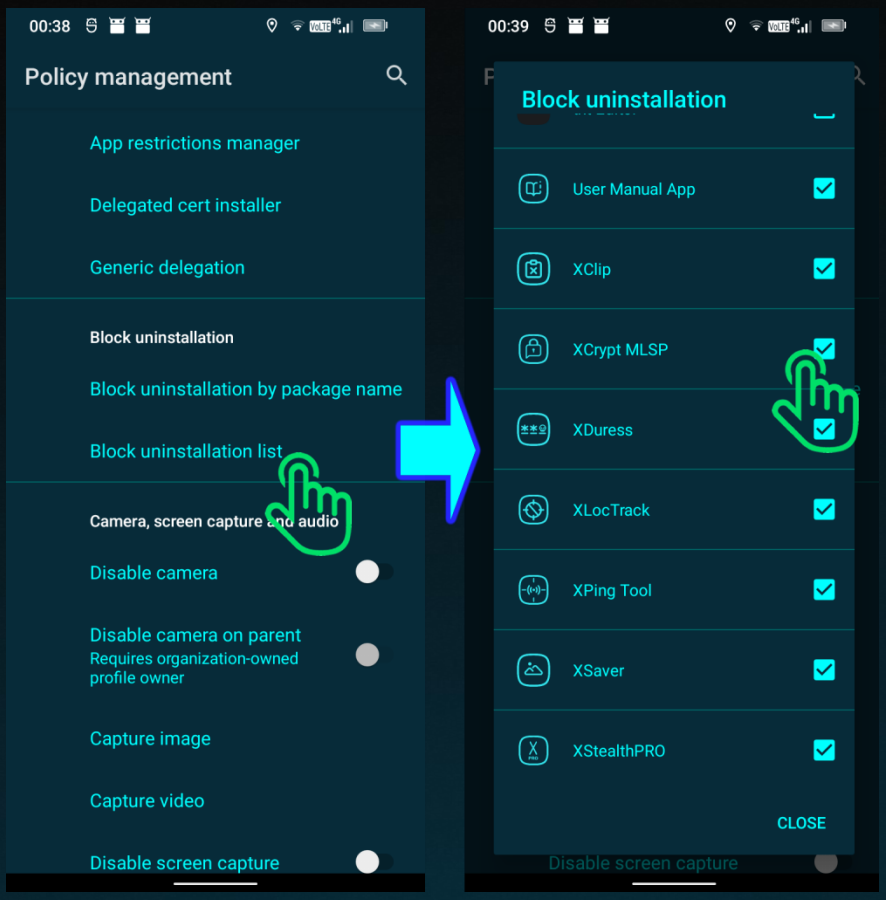
  ⚠ To be used only if you know what you are doing!
- **Delegated cert installer**. You can delegate which app handles the cert installation. Requires an organization-owned profile owner added by your organization's IT admin.
- **Generic delegation**. You can, for instance, choose which apps will have uninstallation blocked.



Generic delegation

Block uninstallation

- **Block uninstallation by package name**. You can prevent an app from being uninstalled by entering its package name. Requires knowing the package's full name.
- **Block uninstallation list**. You can choose which installed app will be blocked from being uninstalled.



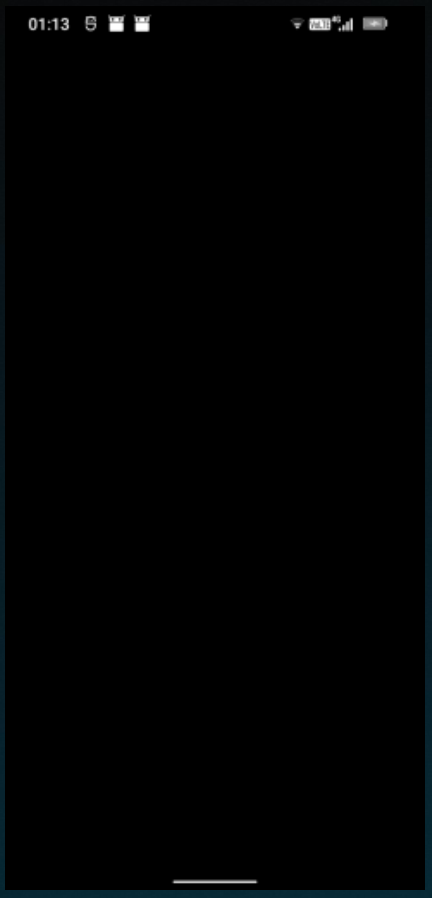
Block app uninstallation

All special app uninstallations are checked by default. Do not uncheck them to avoid unwanted issues.

If a factory reset is triggered by Self-Destruct, Secure Wipe, XDuress, or directly by you, all apps, including special apps, will be removed, even if you checked not to uninstall them. Factory reset/Secure wipe overwrites all settings.

Camera, screen capture, and audio

- **Disable camera**. Toggle camera on/off.
- **Disable camera on parent**. Requires an organization-owned profile owner.
- **Capture image**. You can take a photo.
- **Capture video**. You can record a video.
- **Disable screen capture**. It disables taking screenshots: all screenshots will be blacked out.



Blacked out screenshot

⚠ If you need to take a screenshot in case of technical issues, first disable the screen-capture setting, which prevents screenshots.

- **Disable screen capture on parent**. Requires an organization-owned profile owner added by your organization's IT admin.

Disable camera

Certificate management

- Request to manage credentials.
- Install a private/public key pair.
- Remove a private/public key pair.
- Override client certificates with alias.
- Generate a private/public key pair.
- Test signing/validation with a key.
- Install a CA certificate.
- Get a list of CA certificates.
- Remove all CA certificates.
- Grant key pair to app.

⚠️ All the above settings require an organization-owned profile owner and at least one CA certificate (a digital security file that verifies the identity of servers, apps, and websites).

WI-FI management

- **Create WI-FI configuration**. Enter the WI-FI SSID and choose the WEP or WPA/WPA2 security protocol, then save the network. The phone will use that WI-FI network.
- **Create EAP-TLS WI-FI configuration**. This is the standard for enterprise Wi-Fi security. You need at least a CA certificate.
- **DO created WI-FI configs are modifiable only by DO**. Enable this option to lock the WI-FI configuration to the Device Owner.
- **Modify WI-FI configuration**. Self-explanatory.
- **Modify Owned WI-FI configuration**. You can modify the owned WI-FI configuration.
- **Remove all networks not owned by DO**. When tapped, all WI-FI networks not owned by the Device Owner will be removed.

  ⚠️ All stored WI-FI network passwords will be deleted, and the network connection will be removed. To re-enable the Wi-Fi connection, restart the connection procedure and go to device Settings > Wi-Fi, then tap the desired Wi-Fi network and enter the Wi-Fi password.
- **Show WI-FI MAC address**. Self-explanatory.
- **Set WI-FI minimum security level**. Requires API level 33. Work only on Android 13 and above.

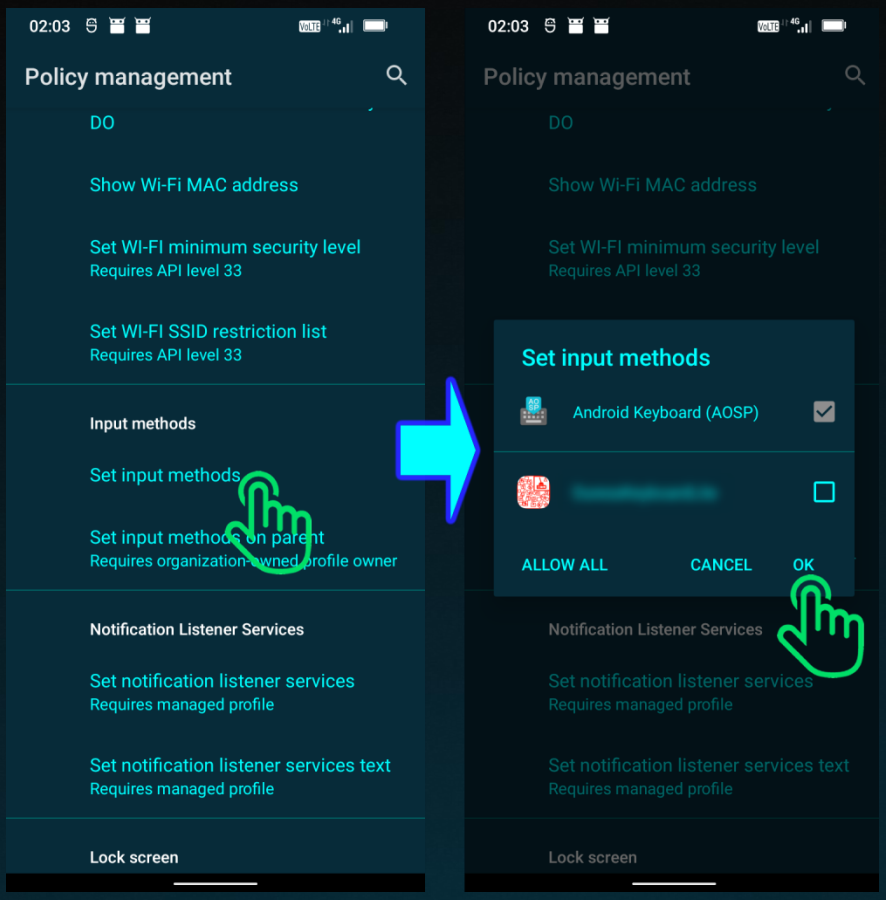
  ⚠️ Not working on XStealth PRO Tactical.
- **Set WI-FI SSID restriction list**. Requires API level 33. Work only on Android 13 and above.

  ⚠️ Not working on XStealth PRO Tactical.

Input methods

- **Set input methods**. You can choose between the Android native keyboard (AOSP) and other installed keyboard apps, and the phone will start using the keyboard app you picked.

  ✅ We recommend sticking with the Android native keyboard (AOSP), which has security patches applied by our x-dev team.
- **Set input methods on parent**. Requires an organization-owned profile owner.



Set keyboard

Notification listener services

- **Set notification listener services**. Requires a managed profile added by your organization's IT admin.
- **Set notification listener services text**. Requires a managed profile added by your organization's IT admin.

Lock screen

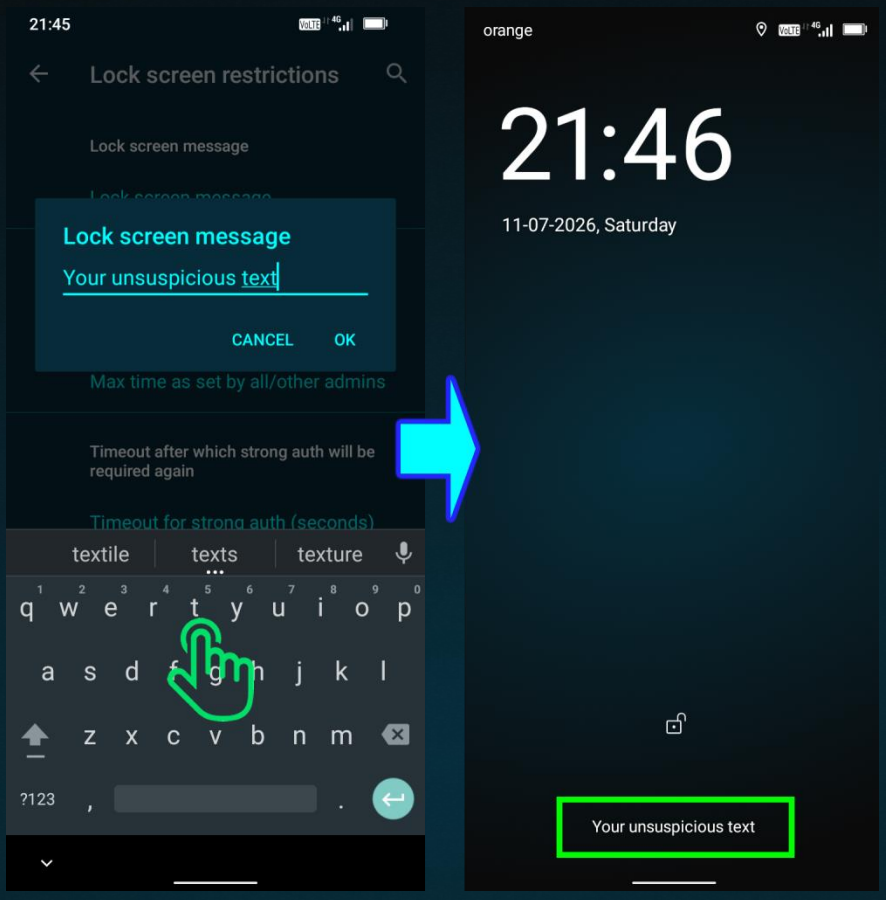
We suggest not enabling password functions in this section, as they will conflict with and overwrite the password and secure wipe settings you set in the Secure Wipe, Self-Destruct, and XDuress apps. As a result, some security settings for the Secure Wipe, Self-Destruct, and XDuress apps will not work.

- **Password complexity**. Requires Password constraints settings first. If no password is set up, password complexity shows "None".
- **Required password complexity**. It requires Password constraints settings first. If no password is set up, password complexity shows "None".
- **Active password compliant**. Shows the compliance status of the password you set with the security policy.
- **Separate challenge**. Requires profile owner.

  All the above options became available once you set up a screen lock by going to phone Settings > Security > Screen lock and setting up a PIN or password.
- **Lock screen restrictions**. You can set:

◉ Lock screen message. This is the text that will appear on the lock screen until you unlock it, if you consider this necessary.

⚠ As a tactical mission-ready phone, be aware not to enter text that could disclose the nature of the phone or mission. Instead of "XStealth PRO Tactical", you can use any unsuspicious text, such as "Personal phone".



Lock screen message

◉ Max time to screen lock

○ Max time to screen lock (seconds): define the number of seconds after the screen locks when not in use.

○ Max time as set by all/other admins. Set by your organization's IT admin.

◉ Timeout after which strong auth will be required again.

○ Timeout for strong auth (seconds). Define the time after the screen locks and requires strong authentication.

◉ Max password failures for local wipe.

○ Max password failures for local wipe.

○ Max failures as set by all/other admins. Set by your organization's IT admin.

◉ Keygurd features

○ Disable secure camera. It disables the ability to launch the camera directly from the lock screen (the keyguard). It prevents unauthorized individuals from taking photos without fully unlocking the device.

○ Disable secure notifications. It is a security policy that hides the contents of lock screen notifications. When enforced using Tactical DPC, sensitive information is either completely hidden or replaced with a generic "Contents hidden" message until the device is unlocked (depending on which notifications are

restricted - system or app notifications).

○ Disable unredacted notifications. Unredacted notifications refer to the system policy that controls whether full notification content appears on a locked screen. When this restriction is toggled off, sensitive push text is hidden on the lock screen (redacted) until the device is unlocked.

○ Disable face unlock. Not available on XStealth PRO Tactical, for security reasons.

○ Disable fingerprint. Not available on XStealth PRO Tactical, for security reasons.

○ Disable iris unlock. Not available on XStealth PRO tactical, for security reasons.

○ Disable text entry in secure keyguard screen. This is a strict security restriction applied via Android Enterprise to lock down the device's lock screen (or "keyguard"). When this policy is enabled, it prevents you from typing or using on-screen keyboards when a secure screen lock is active. It disables all text entry on the lock screen, meaning users cannot type a password or PIN, or even interact with notification pop-ups. It is typically used during covert actions to prevent unauthorized individuals from attempting brute-force attacks or accessing notification features that require text input on the lock screen.

○ Disable shortcuts. Require API level 33. Not available on XStealth PRO.

○ Disable widgets. Once enabled, you will not be able to add new app widgets to the phone screen.

⚠ Do not enable this option! All 3 security widgets from the main screen will stop working.

◉ Trust agent features

○ Set trust agent config. This is an Android Enterprise policy setting. It allows IT administrators to pass custom parameters to system-level Trust Agents (features like Google Smart Lock, Extended Unlock, or OEM-specific face unlock). Administrators can selectively disable all general trust agents on secure lock screens (PIN/Password/Pattern).

⚠ It needs a Managed account added by your organization's IT admin. If not present, the app crashes when you tap on "Set trust agent config", for security reasons.

- **Password constraints**

  ⚠ We suggest not enabling password functions in this section, as they will conflict with and overwrite the password and secure wipe settings you set in the Secure Wipe, Self-Destruct, and XDuress apps. As a result, some security settings for the Secure Wipe, Self-Destruct, and XDuress apps will not work.

◉ Password expiration

○ Password expiration (seconds). It is an Android Enterprise security policy that forces users to change their device or stealth profile PIN/password after a set number of days. This setting is used by administrators to test recurring passcode changes and ensure compliance. Administrators define a timeout (e.g., 30 or 90 days). Once the time expires, the OS prompts you to choose a new, valid PIN or password before you can access the device or stealth profile.

○ Expiration by all/other admins. This enforces the Device Administrator API. It refers to the management of this policy across multiple administration tiers.

○ Password history length. This setting dictates how many of the user's previously used screen lock PINs or passwords the system will remember, actively blocking you from reusing any of those passwords when they change their credentials.

◉ Password constraints.

○ Maximum password quality. Options: something, numeric, numeric (complex), alphabetic, alphanumeric, and complex. Is an admin-defined restriction set via Tactical DPC. It caps the strictest type or length of screen lock you can apply (e.g., preventing you from setting overly complex passwords).

○ Minimum password length. Applicable if a current quality password is enabled. Is governed by the OS's Password Complexity API. Rather than setting custom character lengths, administrators enforce one of three predefined complexity buckets (Low, Medium, or High). Through Tactical DPC, these bands dictate the following minimum length requirements: Low, Medium, and High.

○ Minimum number of letters. It dictates how many alphabetic characters (a-z) must be included in a user's lock screen password.

○ Minimum number of digits. It dictates the exact amount of numerical characters (0-9) a user must include in their device passcode or work profile PIN.

○ Minimum number of lower-case characters. It defines the required amount of lowercase letters (a-z) for a secure screen lock. This setting forces you to include at least this many lowercase characters in your password to comply.

○ Minimum number of upper-case characters. This requirement specifies how many uppercase letters a user's device lock password must contain. It utilizes four strict, predefined complexity categories: None, Low, Medium, and High.

○ Minimum number of symbols. It requires you to include a specific number of special characters (e.g., !, @, #, $) in the stealth profile or device passcode. This feature enforces the strictness of your password. Here is how it functions:

- Enabling the Policy: It is only enforced when the password quality is set to Complex.
- Customization: It requires you to enter at least the specified quantity of non-alphanumeric characters (for example, setting it to 2 means the password must contain at least two symbols like * and %).

○ Minimum number of non-letters. It forces you to include at least a certain number of non-alphabetical characters. A "non-letter" includes numerical digits (0-9) and symbols (\(!@\#\$\). This setting only activates when the Password Quality is set to PASSWORD_QUALITY_COMPLEX or High complexity.

- **Reset password**. It refers to a secure administrative tool used by IT departments and users to remotely change or clear the lock screen PIN, password, or pattern on a managed Android device (XStealth PRO Tactical). This allows the designated Device Owner or Profile Owner to change the user's password without knowing the previous PIN.

  Tactical Use Cases

  - Lock Recovery: If you forget your stealth profile or device password, the IT admin (or you) can instantly push a new passcode to unlock the device.
  - Compliance Enforcement: Administrators (or you) can reset and enforce strict password requirements (such as minimum length, complexity, or changing it after a set period of time).
- **Lock now**. When tapped, it instantly locks the device.
- **Request user to set a new password**. When tapped, it prompts you to choose a screen lock (Face Unlock + pattern, Face Unlock + PIN, Face Unlock + Password).
- **Set new password and specify minimum compl**exity (none, low, medium, high).
- **Set required password complexity** (none, low, medium, high).

- **Set required password complexity on parent**. Requires a profile owner added by your organization's IT admin.
- **Request user to set profile parent new password**. Requires the profile owner added by your organization's IT admin.
- **Request user to set profile parent new password** (device requirement only). Requires a managed profile added by your organization's IT admin.

Lock task

- **Manage lock task list**. Choose an app and lock its task. This will keep the app active in the foreground. This feature locks your device to a single app or a specific set of allowed apps, essentially turning it into a mission-specific device (Tactical mode). Tactical DPC acts as the administrator, allowing you to whitelist apps, hide the home screen, and block the status bar. When an app is pushed into Lock Task Mode, it pins the app to the foreground. Unlike standard Android screen pinning, you cannot escape the app by pressing the Home, Recent, or Back buttons, nor can you access system notifications.

   Tactical Use Case:

  - Dedicated Tactical Devices: Locking XStealth PRO Tactical to a single catalog app, or digital signage for a single-mission or covert action.
- **Check lock task permitted**. Enter a package name and check if the lock task is permitted.
- **Set lock task features**: system info, notifications, home, overview, global access (power button menu), and keyguard.

   Do not change those default settings unless you know what you are doing!
- **Self-start lock task mode** (pinned app mode). Allows your organization to automatically launch and "pin" a specific app to the screen on boot. You cannot exit the app, access the home screen, or view notifications, transforming the device into an impenetrable Tactical device.
  When enabled, the application takes over the screen and utilizes Android Enterprise management to enforce strict system restrictions:
  - System Button Blocking: The Home, Recent Apps, and Back buttons are disabled.
  - No Exiting: You cannot swipe away the app or access the Android settings.
  - Auto-Launch: If the app crashes or the device is rebooted, the X-OS will automatically restart and lock the device directly into the app.

   Tactical Use Cases:

  - Devices locked to a single app for digital signage or a single/specific tactical mission.
  - Tactical/enterprise Hardware: special agents that strictly require one workflow without the possibility of misuse.
- **Launch another activity in lock task mode**. It allows you to launch another application while retaining the system restrictions of lock task mode, creating a seamless, locked-down multi-app environment. For this to work, both the source app (Tactical DPC) and the target app must be explicitly added to the device's Lock Task Allowlist.
- **Stop lock task mode**. It stops the lock task mode once tapped.

Managed profile policies

- **Managed work profile specific policies**. Require a managed profile added by your organization's IT admin.

Bind to profile owner

- **Bind to profile owner service**. Requires Android Enterprise. It refers to an action that allows an administrator app or service to establish a secure cross-profile connection with the Profile Owner.
  ⚠ This function is locked on XStealth PRO Tactical due to the security risks associated with granting complete control over mission data.

Networking

- **Network data usage stats**. It allows you or your organization to monitor how much mobile and Wi-Fi data individual applications consume. When configured, it simulates Android Enterprise policies, giving IT visibility into tactical data consumption and enabling enforcement of data-saving restrictions in managed profiles.
- **Set always-on VPN**. Select a VPN app from the list or manually enter a package name, check the Lockdown button, and set the VPN to always-on. It allows you to force a designated VPN app to establish and maintain a persistent connection, ensuring all network traffic is encrypted and routed through a specific server without your intervention.
  Core Capabilities
  - Persistent Connection: The VPN automatically connects when the device boots. You cannot disable it or switch to a different VPN app.
  - Lockdown Mode: You or IT admins can enforce "Block connections without VPN." If the VPN drops or fails to connect, the device completely cuts off internet access, preventing data leaks over unsecured networks.
  - Tactical Control: Typically used in tactical or fully-managed devices to ensure tactical unit traffic is routed securely through military secure servers.

  How it Works
  When you configure the "Always-on VPN" policy in Tactical DPC, it acts as the Device Owner or Profile Owner, programmatically granting the VPN app system permissions to govern network traffic.
  Implementation Details
  - App Packages: You must input the exact package name (e.g., com.company.vpnapp) of the target VPN client installed on the device.
  - XStealth PRO Tactical Enhancements: It provides refined APIs for this policy, allowing you or administrators to optionally exempt specific apps (like a captive portal or a critical internal tool) from the lockdown rule.
- **Preferential network service status**. Requires profile owner. This status configuration determines how managed apps handle connections:
  - Enabled (True): If the preferred tactical or 4G slice connection drops, the device falls back to the standard cell or Wi-Fi network.
  - Disabled (False): If the preferential network isn't available, the targeted stealth apps won't use the standard default network connection, keeping your mission data from leaking over unsecured public connections.
- **Enterprise slice**. Requires profile owner. It refers to a 4G network slicing capability that allows you or IT administrators to route all internet traffic generated from your phone's Stealth Profile through a dedicated, prioritized, and secure carrier network, while leaving other (personal) apps (if any) on the regular network.

How it Works
- 4G Network Slicing: Your mobile network operator virtually splits a single 4G connection into multiple independent virtual networks. A tactical slice guarantees bandwidth and priority specifically for tactical use.
- The XStealth PRO Tactical Feature: The X-OS lets your device's network tethering and connectivity modules separate data traffic at the operating system level.
- No Extra VPN Needed: While it operates like a secure expressway for tactical data, it is a network-level path and does not replace your secure VPN.

- **Set global HTTP proxy**. It allows you to force all HTTP and HTTPS network traffic on XStealth PRO Tactical to route through a specific proxy server. This forces the proxy system-wide rather than for a single Wi-Fi network.

  Tactical Use Cases & Key Details
  - System-Wide Routing: Unlike standard Wi-Fi proxy settings, it forces all apps and browsers (if any) across all networks (Wi-Fi and mobile data) to use the proxy.
  - Traffic Auditing: Commonly used by security admins to intercept, inspect, and log network traffic using tools like Charles Proxy, Burp Suite, or Fiddler.
  - Tactical Control: Used to enforce tactical network security and content filtering.
- **Clear global HTTP proxy**. It completely removes any system-wide proxy servers affecting the device's internet traffic. It essentially resets the X-OS network routing to a direct, unproxied connection.
- **Set private DNS mode**: off, automatic, specified host, or unknown. Enter the host name and set it. This prevents ISPs or data interceptors/network snoopers from seeing which websites you are visiting.

  You can force the device to use a specific, secure, and monitored DNS server to protect tactical data. Through the Tactical DPC app, you can set this mode on a fully managed device by executing the setGlobalPrivateDnsMode API to either:
  - Off: Disables the encrypted DNS.
  - Automatic: Uses the network's default DNS if it supports encryption.
  - Private DNS provider hostname: Forces the device to route all traffic through a specific, hardened DNS server (e.g., a tactical server or an ad-blocking/anti-tracking DNS like Cloudflare or AdGuard).

Permission management

Do not change those default settings unless you know what you are doing!

- **Get/Set default permission policy**: prompt, auto-accept, or auto- deny. It allows you to control how runtime permissions are handled for all applications across a managed device (XStealth PRO Tactical) or stealth profile. On XStealth PRO Tactical, we have introduced critical privacy restrictions that change how this policy behaves, specifically restricting the auto-granting of sensitive sensor data.

  How It Works (The 3 Policy States)
  When you use Set default permission policy inside Test DPC, you force the X-OS into one of three baseline global behaviors:

- PROMPT (0): Default Android behavior. The device user is prompted to manually allow or deny runtime permissions whenever an app requests them.
- GRANT (1): Auto-allow. The system automatically grants all runtime permissions requested by any app, completely bypassing user approval screens.
- DENY (2): Auto-reject. The system automatically denies all runtime permissions requested by any app without giving the user a choice.

- **Manage app permissions**. Choose an installed app and set permissions to "WRITE_EXTERNAL_STORAGE", "READ_EXTERNAL_STORAGE", and "ACCESS_MEDIA_LOCATION". This is a granular control tool that allows you to target a specific application and explicitly force an Allow, Deny, or Let user decide state for individual runtime permissions. While the "Default permission policy" sets a global baseline for all apps, the "Manage app permissions" overrides that baseline for a single chosen package.

  How It Works (The 3 Grant States)
  When you select an app inside Tactical DPC's "Manage app permissions" menu, you can alter individual permissions (e.g., Camera, Location, Contacts) to one of three states:
  - Allow (Granted): The system grants the specific permission to the app. You cannot revoke it via the system settings UI.
  - Don't Allow (Denied): The system strips the permission from the app. You cannot grant it via the system settings UI.
  - Let user decide (Default): Normal Android behavior. The Tactical DPC steps aside, allowing the application to prompt the user natively, and the user retains full control to toggle it on or off.

Single-use device

Traditionally known as a Dedicated Tactical Device or a "COSU—Corporate-Owned", it refers to a highly locked-down deployment mode where the phone is restricted to a specific task, function, or application. Instead of operating like a standard consumer smartphone, a single-use device behaves as a fixed-purpose tool—a Tactical smartphone ready for a specific mission/covet action.

- **Disable status bar**. It is a security restriction that completely blocks the user from expanding the notification shade, accessing notifications, or interacting with the Quick Settings panel (e.g., toggling Wi-Fi, Bluetooth, or Airplane mode).
- **Reenable status bar**. It enables the status bar so that you can use it again.
- **Disable keyguard**. It is a security restriction that completely removes the lock screen (keyguard) layer from the operating system. When activated, pressing the physical power button turns the screen directly on to the user interface, home launcher, or running app—completely bypassing the "swipe to unlock" screen, ensuring the device screen never becomes accidentally locked or blocked by a swipe screen if power fluctuates.

  How It Works and Strict Security Rules
  The feature mimics setting the device's system screen lock type to "None". However, X-OS enforces heavy security guardrails on how and when this policy can actually take effect:
  - Only Works on Unsecure Devices: This command will have no effect if a PIN, password, or pattern is currently set on the device. The X-OS prioritizes user data protection; it will refuse to bypass an active, secure lock screen.
  - Automatic Revocation: If an administrator disables the keyguard, but a user (or another policy)

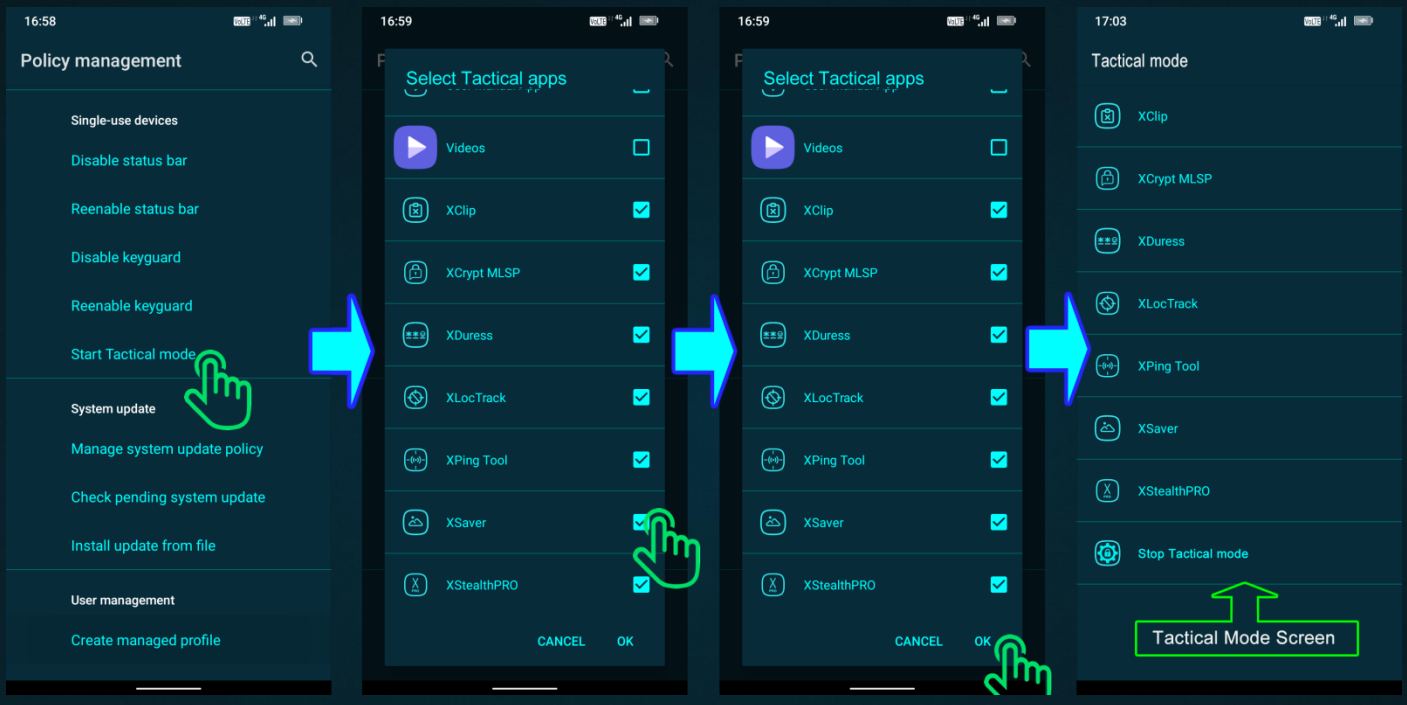
subsequently sets a password or PIN, the disablement is immediately overridden, and the keyguard turns back on.

- Instant Dismissal: If the keyguard is currently active but unsecure (e.g., standard swipe-to-unlock), triggering this policy will instantly dismiss the lock screen and take the user to the home screen.

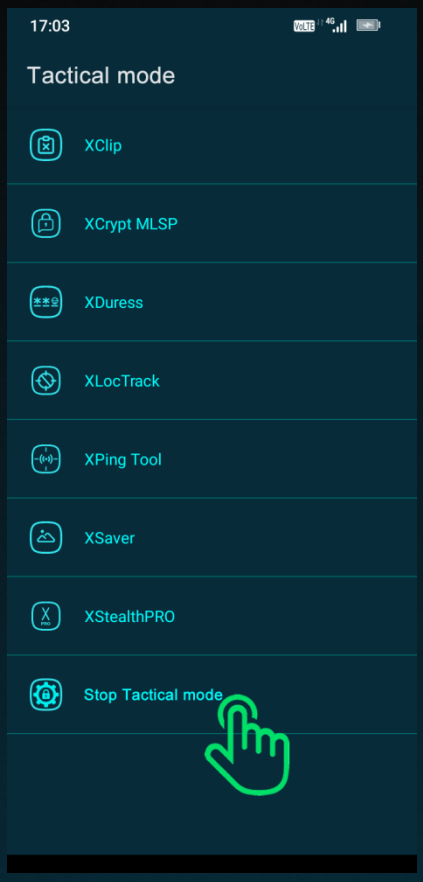
- **Reenable keyguard**. It reenables the keyguard and removes the above settings.
- **Start Tactical mode**. Select Tactical apps from the list, then tap OK. Tactical mode is a device lockdown feature that restricts your XStealth PRO Tactical to a single app or a specific set of applications, depending on the mission requirements. It prevents users from accessing system settings, notifications, or unauthorized apps, effectively turning your device into a dedicated, mission-purpose-built Stealth Phone.

  ⚠ Tactical mode is persistent after a phone restart.

  ⚠ Tap on Stop Tactical mode to exit Tactical mode.



Start Tactical mode



Stop Tactical mode

System update

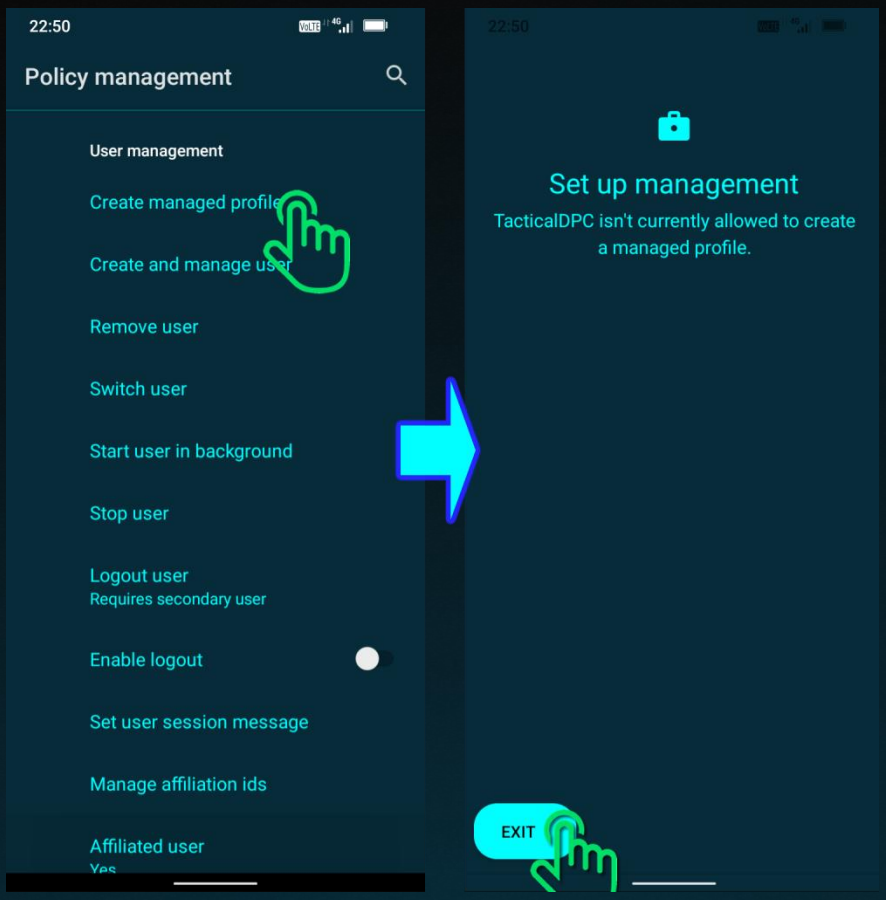
- **Manage system update policy**. You can choose between:
  - Automatic immediate install.
  - Install within a maintenance window.
  - Postpone.
  - None. This is the default setting, and you shouldn't change it.

  ⚠ All XStealth PRO versions do not use OTA (over-the-air) system updates! There is no point in setting up a new system update policy.
- **Check pending system update**. Tactical DPC will check whether a system update has been pushed for download.

  ⚠ If available, do not download it! Your phone is under attack.
- **Install update from file**. This option is designed for critical updates we send to users via email as a secure file attachment.

User management

This is a suite of APIs and menu features that allow a Tactical DPC to programmatically create, remove, cycle, and restrict multiple user profiles on a single physical hardware unit. Instead of relying on standard Android settings, this console allows an Enterprise Mobility Management (EMM) server to manage multi-user shifts, handle guest execution, or deploy dedicated Tactical workflows.



Create managed profile

- **Create managed profile**. This will lead you to the setup management screen. It requires a profile owner added by your organization's IT admin; otherwise, it will not work.
- **Create and manage user**. Requires an organization-owned profile owner. Provisions an independent secondary user profile entirely in the background without user intervention.
- **Remove user**. Requires a profile owner added by your organization's IT admin. Instantly deletes a secondary user profile and completely wipes its associated local application data.
- **Switch user**. Require at least a secondary user created by your organization's IT admin. Forcefully pushes a specific background user profile into the device foreground, instantly altering the active home screen layout and app array.
- **Start user in background**. Require at least a secondary user created by your organization's IT admin.
- **Stop user**. Require at least a secondary user created by your organization's IT admin. Allows Tactical DPC to execute operations within a secondary profile silently in the background before deciding to bring it into focus.
- **Logout user**. Require at least a secondary user created by your organization's IT admin.
- **Enable logout**. This is a security feature designed specifically for shared devices between multiple field operatives.
- **Set user session message**. Enter the start and end session messages, then tap SET MESSAGE.
- **Manage affiliation IDs**. Requires an organization-owned profile owner and affiliation ID. Contact your organization's IT admin.
- **Affiliated user**. It stays "Yes" so you can use certain features without being a profile owner.
- **Ephemeral user**. This is deactivated to keep the affiliated user option running.

User restrictions

- Set user restrictions

⦿ Allow web links to apps of the parent. To work, it requires a managed profile created by your organization's IT admin.

⦿ Disallow add managed profile. This is a user restriction that blocks the creation of a managed work container (Stealth Profile) on the device.

⚠ This setting is enabled by default and is persistent. Do not disable it! Otherwise, security weaknesses can be exploited by an attacker.

⦿ Disallow add user. This is a strict device security restriction that completely blocks the creation of new user profiles, secondary profiles, or guest accounts on the device. This restriction is primarily deployed when Tactical DPC operates in Device Owner (DO) mode on a military-owned asset. It ensures the physical device remains locked to a single primary user or a strictly controlled Tactical multi-shift setup. If an admin wants to use User Management features to programmatically spin up specific profiles, they typically leave this disabled or use it to block manual user intervention while handling creation via code.

⦿ Disallow adjust volume. This is a strict device management restriction that strips you or an attacker of the ability to change any audio volume level on the hardware. When enabled, you cannot use the physical Volume controls (+ and - buttons from the device's right side).

How It Works and What It Blocks
When this restriction is toggled to On, the X-OS system locks the master volume matrix:
- Dead Physical Keys: Pressing the physical volume up or volume down rocker buttons on the side of the device does absolutely nothing. No volume slider overlay appears on the screen.
- Frozen Settings Sliders: If a user navigates to system Settings > Sound, all volume sliders (Media, Call, Ring, Notification, and Alarm volume) are completely grayed out, frozen, or entirely non-interactive.
- Fixed Current Level: The audio volumes are permanently stuck at whatever decibel level they were set to the exact second the policy was activated.

⦿ Disallow apps control. This is a user restriction that prevents you from force-stopping installed special applications through the device's system settings.

How It Works and What It Blocks
When this restriction is toggled to On, the X-OS framework restricts access to the system Settings > Apps submenus:
- Blocks Force-Stopping: The Force Stop button is completely disabled for special apps. You cannot kill running background processes, sync clients, or location-tracking services.

⦿ Disallow Bluetooth.

⚠ XStealth PRO (both Dominator and Tactical versions) comes with disabled Bluetooth. There is no point in using the "Disallow Bluetooth" option.

⦿ Disallow change WI-FI state. Requires API level 33. Not available on XStealth PRO.

⦿ Disallow config Bluetooth.

⚠ XStealth PRO (both Dominator and Tactical versions) comes with disabled Bluetooth. There is no point in using "Disallow config Bluetooth" option.

⦿ Disallow config cell broadcasts. This is a device security restriction that blocks you from modifying baseband attack alert settings on the device.

How It Works and What It Blocks

When this restriction is toggled to On:

- The X-OS system locks baseband attack alerts.
- Grays Out Notification Settings: If a user navigates to system Settings > Notifications > Wireless emergency alerts, the menu options will be grayed out and non-interactive.

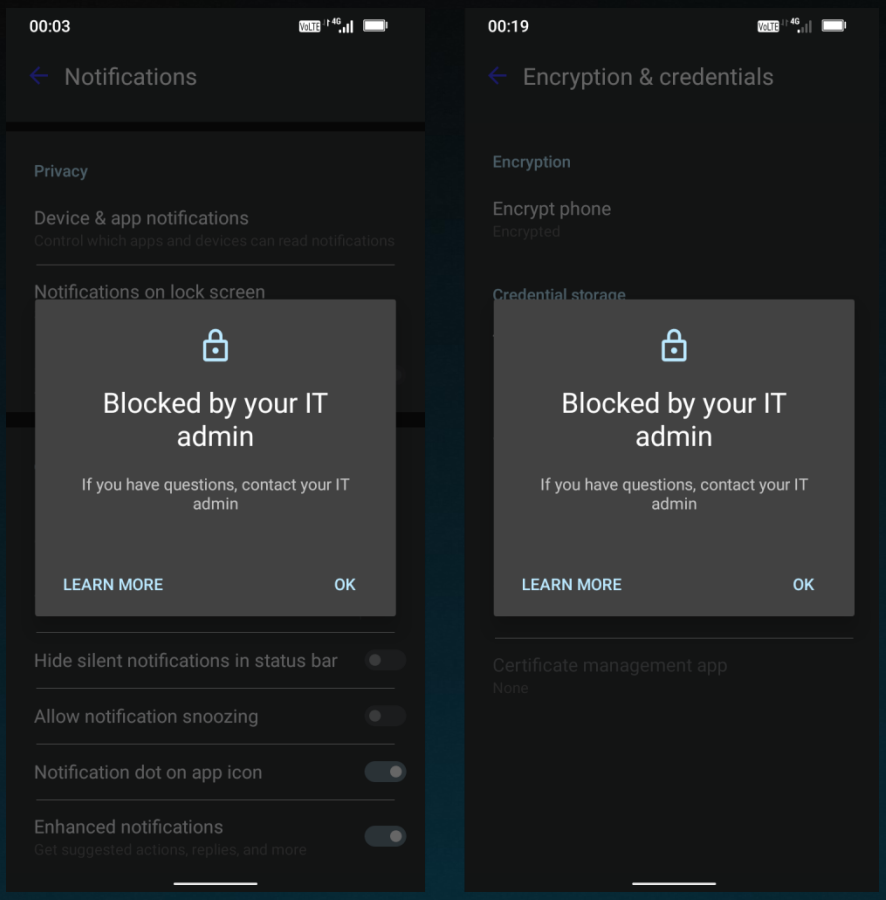
⚠ Do not enable this feature! Will affect the alert displayed when an IMSI Catcher/GSM Interceptor is active within the area.

⦿ Disallow config credentials. This user restriction prevents you from modifying the device’s trusted security credentials. It is critical for preventing advanced security breaches, data leaks, or unapproved network bypasses on military-owned devices. It ensures that only the military/enterprise DPC can programmatically push down network certificates or VPN trust chains.

How It Works and What It Blocks

When this restriction is toggled to On, the X-OS framework completely locks down the device's cryptographic key storage and certificate authority (CA) settings:

- Blocks Custom Certificate Installation: An attacker cannot install user-level digital certificates (such as .crt, .p10, or .pfx files) from the device storage. This stops attackers from manually introducing custom root CA certificates, which could be used to intercept or modify network traffic.
- Prevents Deleting Trusted Credentials: Attackers are blocked from clearing, disabling, or tampering with the system's pre-installed trusted root CA certificates.
- Freezes Encryption Key Management: If an attacker navigates to system Settings > Security > More security settings > Encryption & credentials, the options to "Install from storage" or "Clear credentials" are grayed out, hidden, or completely non-interactive.



Notifications & Encryption credentials blocking

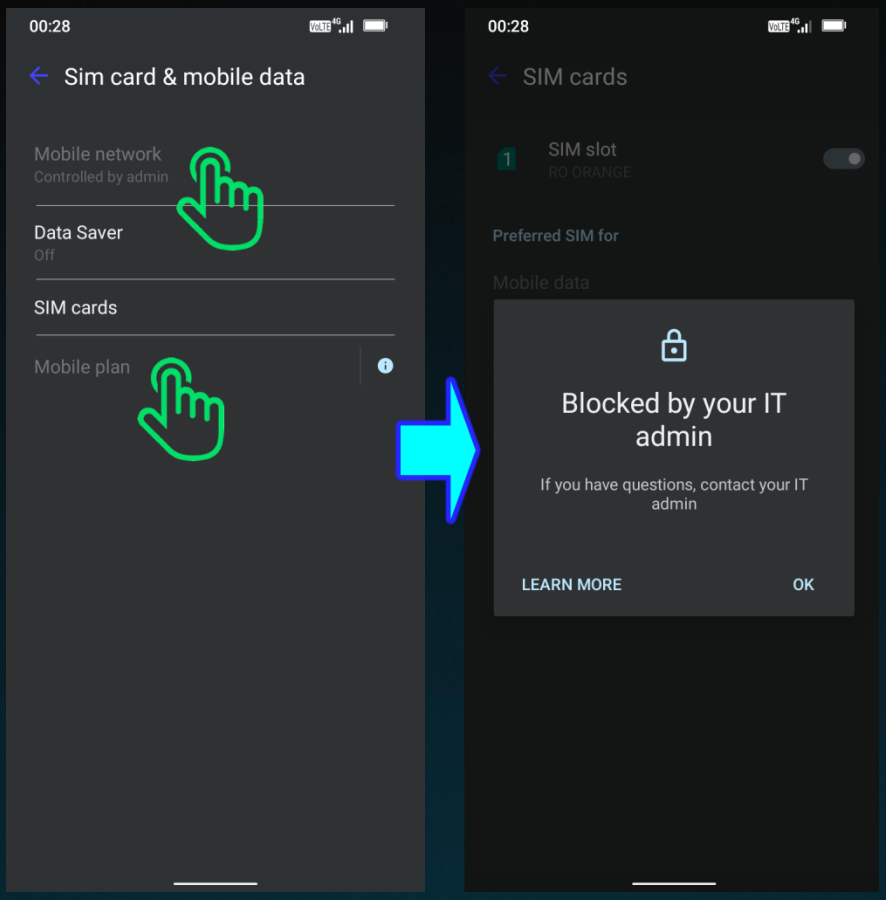
◉ Disallow config mobile networks. This is an administrative restriction that blocks you (or attackers) from changing any cellular data or mobile network configurations. It is widely used for tactical teams or field operatives. It ensures that devices remain connected to the internet during certain missions or covert operations for tracking, syncing, and remote management without risk of user/operative tampering.

How It Works and What It Blocks

When this restriction is toggled to On, the X-OS system locks the physical and virtual cellular radio controls:

- Blocks Cellular Data Toggles: Users cannot switch cellular data on or off, preventing them from manually severing a field device's cellular connection.
- Freezes Roaming Controls: The option to enable or disable data roaming is locked, preventing unexpected carrier roaming exploits.
- Locks APN Settings: Attackers are blocked from creating, editing, or selecting different Access Point Names (APNs). This ensures they cannot redirect cellular traffic away from secure military gateways or private APNs.
- Grays Out Settings UI: If a user navigates to system Settings > SIM card & mobile data / Mobile network, the entire configuration page is grayed out and unclickable.

⚠ Do not enable this function unless you or your organization has a clear scope for doing this! Will affect some detection capabilities.



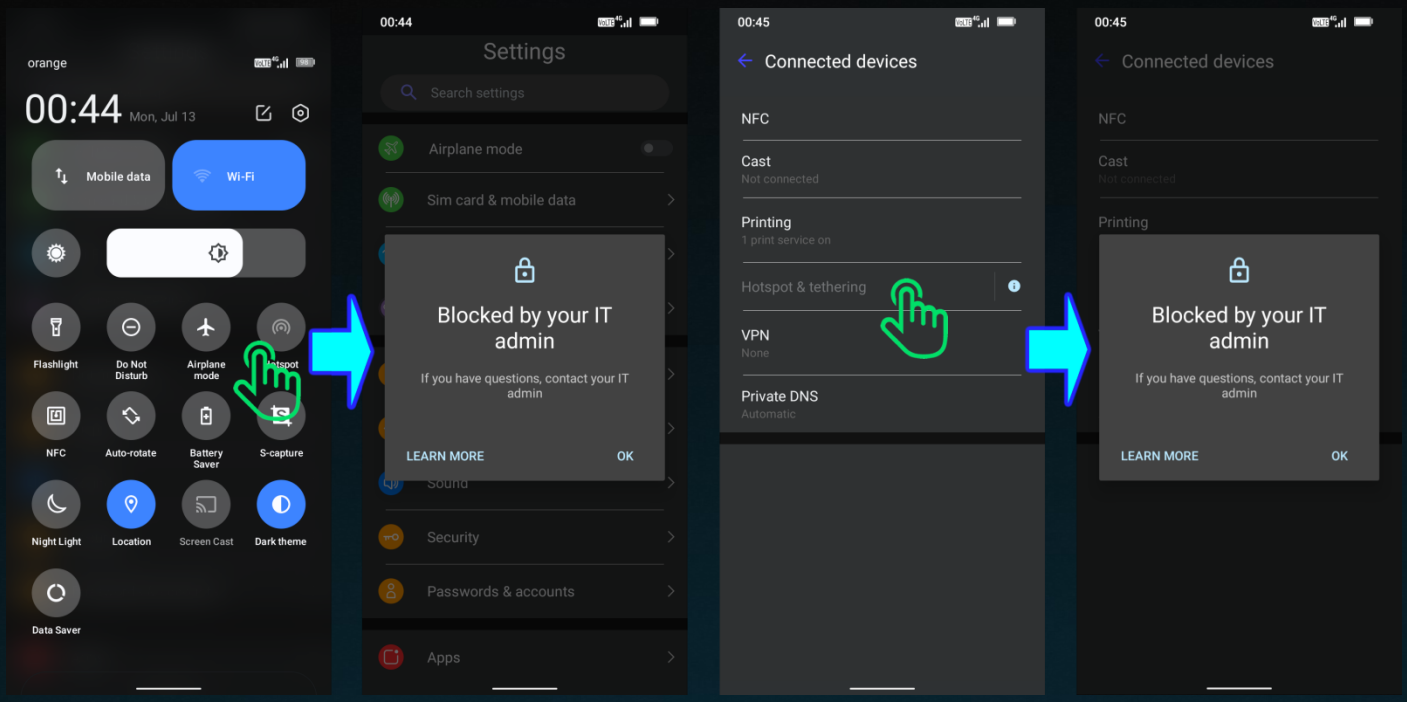
Disallow config mobile networks

◉ Disallow config tethering. This is a device management restriction that prevents users from sharing the device's internet connection with other hardware. This also protects against Wi-Fi interceptors.

How It Works and What It Blocks

When this restriction is toggled to On, the X-OS framework completely shuts down all native routing capabilities:

- Blocks All Sharing Methods: It simultaneously disables all forms of connection sharing, including
  - Wi-Fi Hotspot (Portable Hotspot)
  - Ethernet Tethering (Sharing data via a USB-to-Ethernet adapter)
- Turns Off Active Sessions: If the user has a hotspot running at the exact moment the policy is enforced, the X-OS will instantly terminate the session.



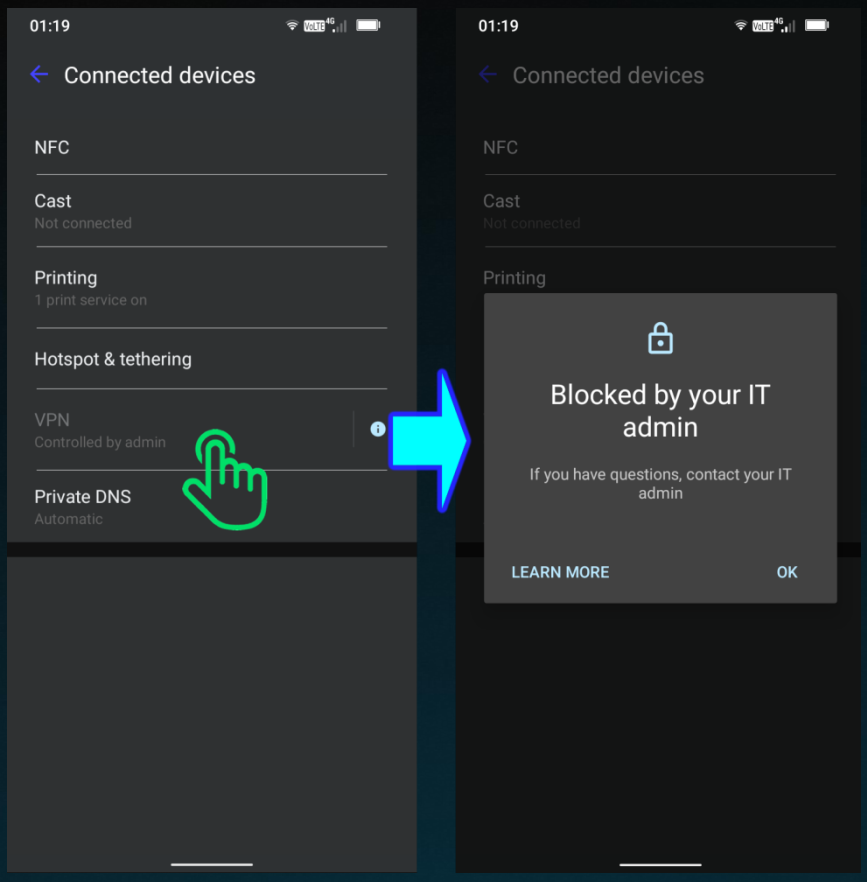
Disallow config Hotspot & tethering

◉ Disallow config VPN. This is a user restriction that prevents users or attackers from manually adding, editing, or deleting Virtual Private Network (VPN) configurations on the device. It is critical to ensure that tactical/corporate traffic cannot be maliciously or accidentally routed away from secure military inspection firewalls. It ensures users cannot bypass military web content filters or data loss prevention (DLP) systems.

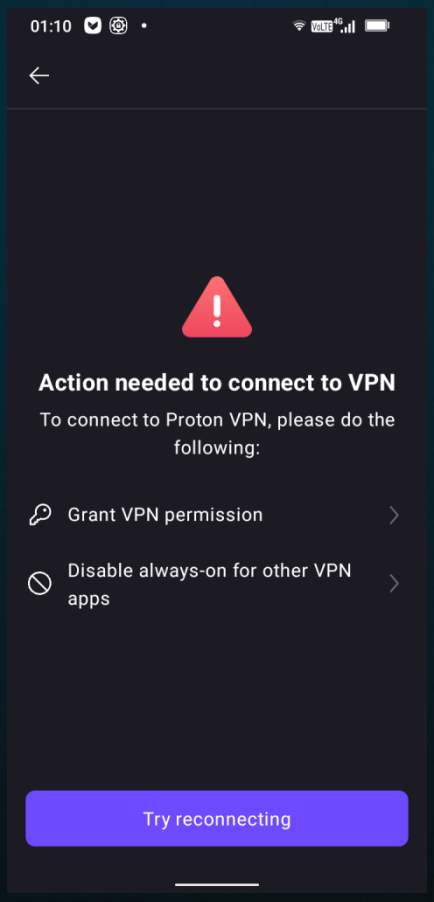
How It Works and What It Blocks

When this restriction is toggled to On, the X-OS framework locks the native network routing layers:

- Blocks Manual Setup: Users or attackers cannot manually enter server addresses, credentials, or custom protocol parameters (like IKEv2, L2TP, or IPSec) to route their traffic through external servers.
- Blocks Consumer VPN Apps: Third-party VPN sideloaded apps will fail to establish a new VPN connection because the X-OS will reject their requests to create a VpnService interface.
- Grays Out Settings UI: If an attacker navigates to system Settings > Connected devices > VPN, the option to tap the "+" icon to add a new network is grayed out.



Disallow config VPN



Disallow config VPN

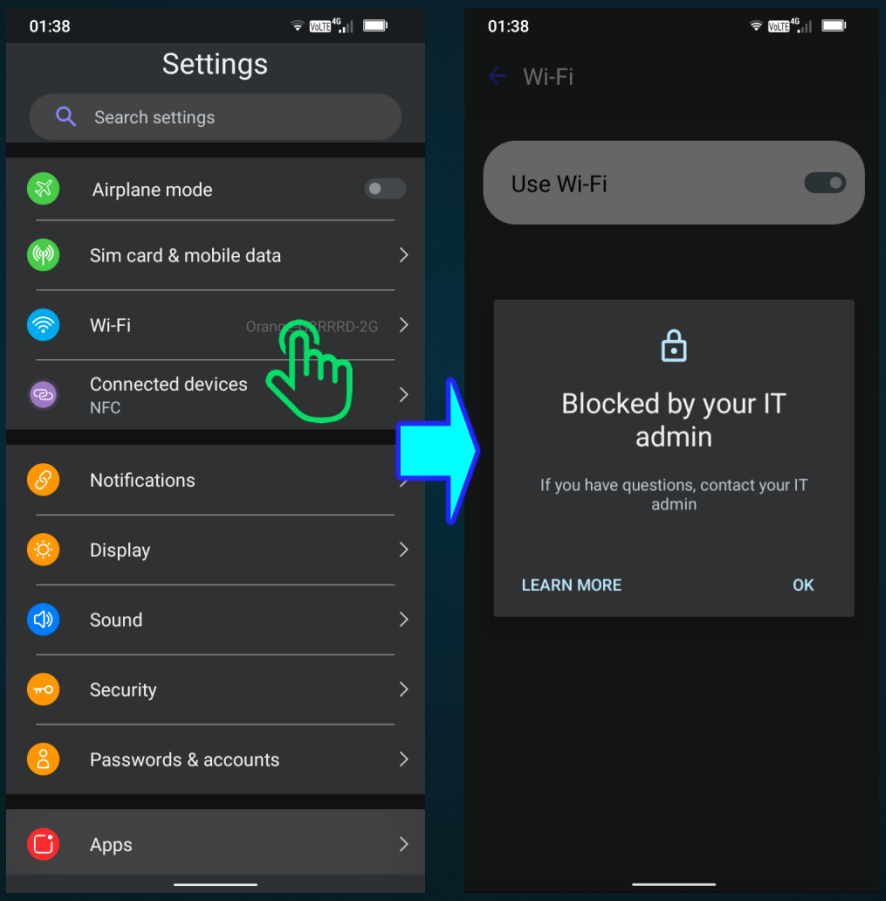
◉ Disallow config Wi-Fi. This is an administrative restriction that blocks users or attackers from adding, altering, or removing wireless network configurations. It is critical for Single-use dedicated devices (COSU)

or tactical teams. It ensures that devices stay on secure military Wi-Fi pipelines and prevents users from connecting to unmanaged, public hotspots that could expose data.

How It Works and What It Blocks

When this restriction is toggled to On, the X-OS system locks the local wireless network architecture:

- Blocks Adding Networks: Users or attackers cannot connect to new Wi-Fi networks. They are blocked from manually entering SSIDs or security keys or from scanning Wi-Fi QR codes.
- Blocks Modifying Networks: Users or attackers cannot edit existing Wi-Fi settings to add proxies, adjust IP settings (Static vs. DHCP), or change DNS configurations.
- Blocks Deleting Networks: The option to "Forget" currently saved networks is disabled.
- Allows Connecting to Existing Networks: Crucially, you can still tap and connect to networks that were already saved on the device before the policy was applied.
- Locks Settings UI: If you or an attacker navigates to system Settings > Wi-Fi, the whole page is unresponsive, and a lock message pops up on the screen.



Disallow config Wi-Fi

◉ Disallow content capture. This is a security policy that prevents the operating system or third-party apps from reading, scraping, or analyzing on-screen text and data.

◉ Disallow content suggestions. This security policy prevents the operating system from analyzing on-screen context to provide predictive recommendations, shortcuts, or smart actions.

◉ Disallow create windows. It is a user restriction that prevents apps and background processes from creating overlay windows over standard applications.

When this restriction is toggled to On, X-OS blocks the window manager from initializing non-application layouts. It specifically disables the creation of the following window types:

- System and Application Overlays.
- Alerts and Errors.
- Toasts and Phone Layouts.

⚠ Do not enable this option unless you want to stop the security alerts displayed by the special apps. We do not recommend turning this on.

◉ Disallow system error dialogs. This is an X-OS user restriction designed to suppress standard system pop-ups that appear when an application crashes, freezes, or becomes unresponsive. It forces the device to handle application failures silently in the background, ensuring uninterrupted user interaction.

How It Works

When an app fails, X-OS normally halts execution and displays a native system prompt. When this restriction is active:

- Suppressed Prompts: The system intercepts and skips rendering the user-facing alert box.
- Immediate Force-Stop: The X-OS system treats the crash or freeze as if the user explicitly clicked the "Close app" or "Force stop" button.
- Silent Lifecycle Restart: If the app is configured under Lock Task Mode (Tactical Mode), the system instantly restarts the dead application package cleanly, bypassing the stuck state.
- No Telemetry Pop-ups: Because there is no UI component visible to receive explicit user interaction, the operating system does not collect or prompt for standard crash feedback telemetry.

What It Blocks

This policy blocks three specific types of X-OS warning dialogs:

- ANR (Application Not Responding) Dialogs: The pop-ups that appear when an application’s main thread freezes for more than 5 seconds (preventing the classic "App isn't responding. Close app / Wait" prompt).
- Crash (App Has Stopped) Prompts: The critical alerts are generated when an unhandled runtime exception or software bug crashes an active app layer.
- OEM System Error Alerts: System-level warnings generated by vendor-specific UI packages when background components drop unexpectedly.

◉ Disallow cross profile copy/paste. Requires a managed profile added by your organization's IT admin. This is an X-OS security policy that prevents users from copying text, images, or data to the clipboard inside a managed container (Stealth Profile) and pasting it into the personal sandbox (or vice versa). It serves as a data loss prevention (DLP) firewall, ensuring that sensitive data remains inside tactical-approved applications.

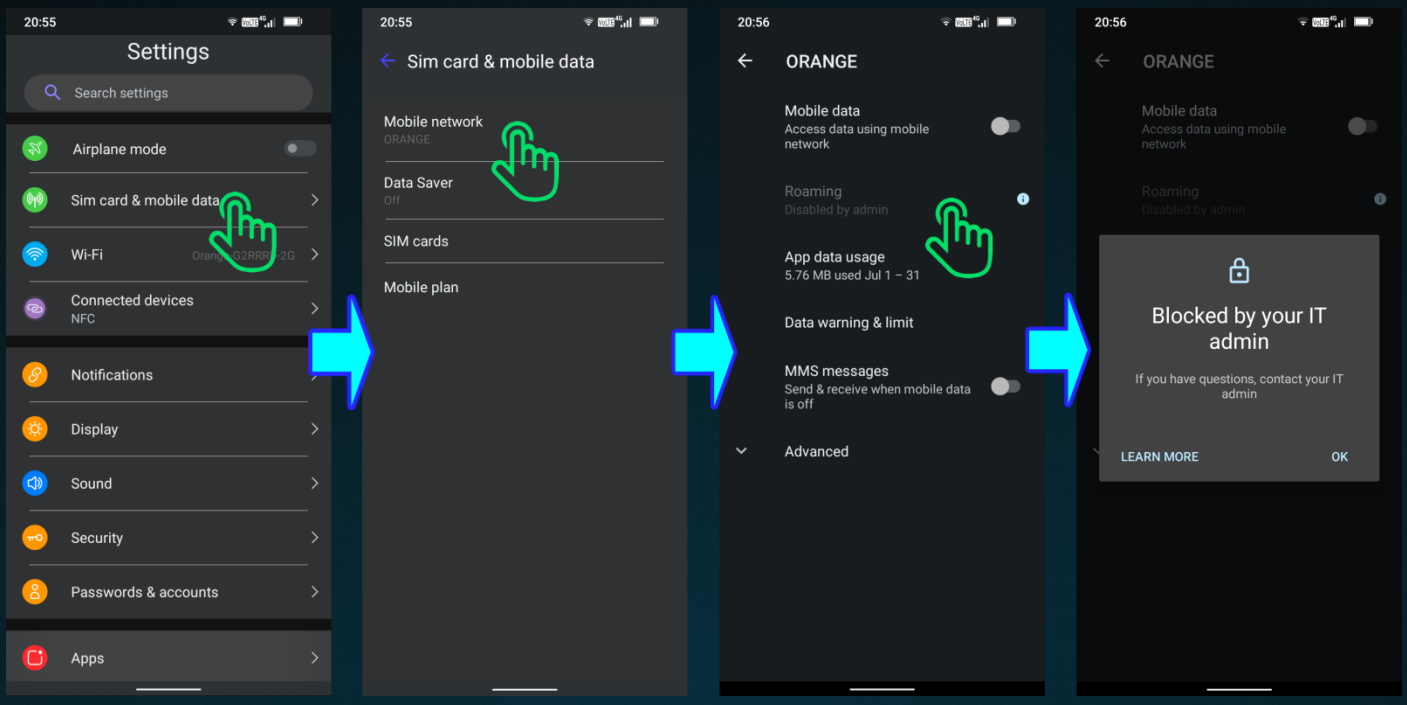
◉ Disallow data roaming. This is an X-OS user restriction that prevents your device from connecting to cellular data networks outside its real carrier's coverage area (or military-operated mobile network), preventing the device from "migrating" to an active GSM Interceptor with data interception capabilities. No secondary user or work profile can bypass the roaming block. It is a critical security control policy used by tactical command centers/organizations to eliminate unexpected, unwanted, or out-of-network data roaming incidents on tactical-managed devices.

How It Works

When this restriction is pushed to a device, the X-OS system overrides user preferences and actively modifies the cellular radio state:

- Forced Deactivation: The X-OS instantly forces the native "Data Roaming" switch in the device's Network

Settings to the Off position.
- UI Lockout: The toggle for data roaming in the system settings becomes unavailable, preventing the device user from turning it back on.
- Network Interception: If the device detects it has disconnected from its home Public Land Mobile Network (PLMN) or military-operated mobile network, the X-OS telephony framework automatically severs the cellular data pipe while allowing standard cellular voice and SMS to function (unless voice roaming is separately restricted).

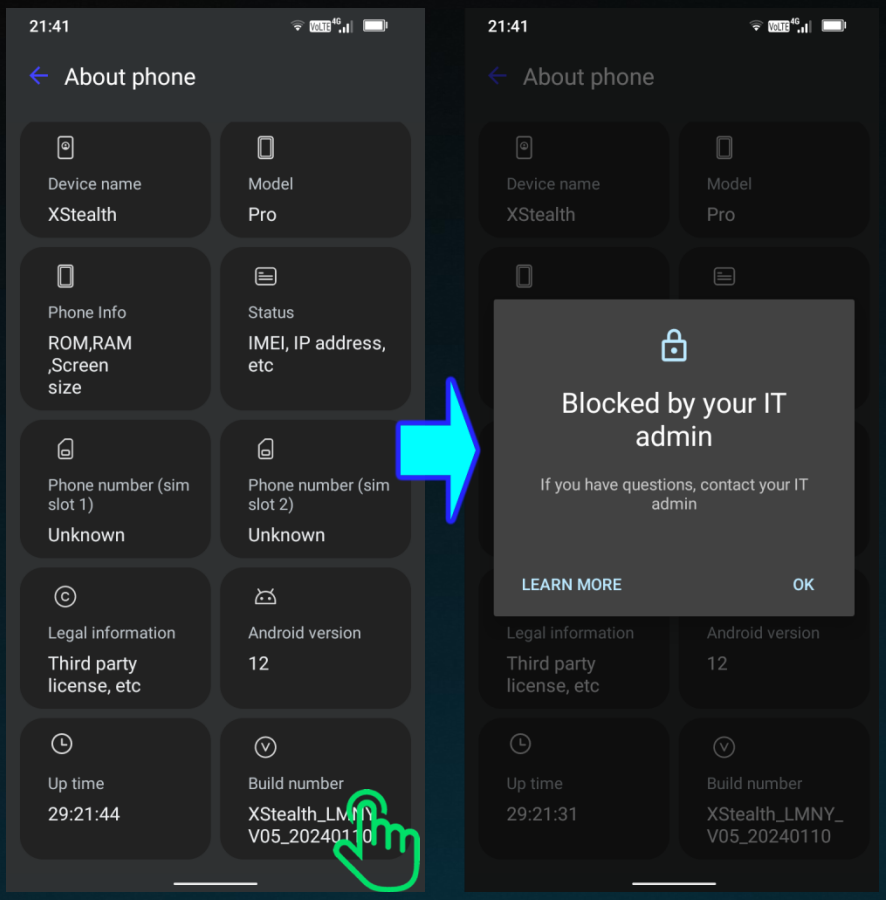


Disallow data roaming

◉ Disallow debugging features. This is a security user restriction that completely blocks developer options on the device. It is a critical infrastructure security policy that shields devices from unauthorized external data extraction, application sideloading, and physical tampering. Because debugging access cuts into the deepest structural levels of the operating system, the restriction is absolute. It completely blocks ADB and developer options across the entire physical hardware stack, securing both the Personal and Tactical profiles.

Tactical Use Case

Very useful when Tactical DPC access is restricted with a PIN/Password: Developer options cannot be accessed. As a consequence, ADB (via USB-C) will not work (wireless ADB is removed by default), forensic analysis will fail due to an unavailable ADB connection, and so on.



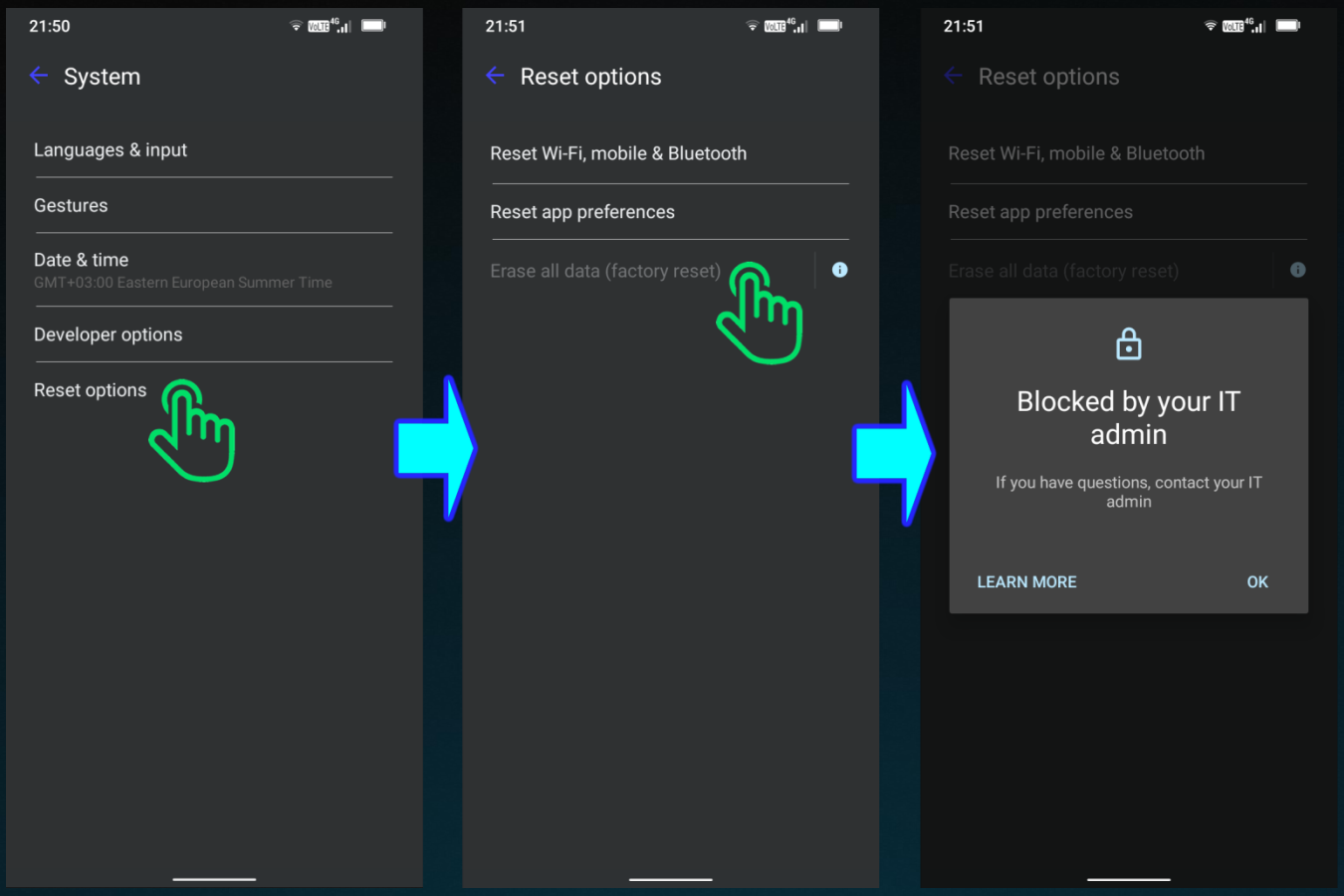
Disallow debugging features

◉ Disallow factory reset. This is a user restriction that prevents a device from being wiped and restored to its original factory settings by the local user or attacker. It is a vital theft-deterrent and asset-protection policy used by Command and Control Centers/organizations to ensure secure management frameworks cannot be easily erased or bypassed.

How It Works

When this restriction is toggled to On, the X-OS system enforces a strict lockdown on system restoration pathways:

- Removes Settings Menu Toggle: The "Factory Data Reset" or "Erase All Data" option inside the system settings menu is completely locked behind an administrative message.
- Blocks Recovery Mode Wiping: It instructs the bootloader/recovery environment to block or restrict the manual "Wipe Data / Factory Reset" command triggered by hardware buttons.
- Prevents Tactical DPC Removal: By ensuring the device cannot be wiped, it prevents an attacker/unauthorized user from wiping the device to strip away the Tactical DPC profile and investigate or reuse the hardware.



Disallow factory reset

Do not enable this feature if you want Secure Wipe, Self Destruct, and XDuress apps to work. We strongly suggest not enabling this feature.

◉ Disallow fun. When this restriction is toggled to On, the device becomes an incredibly rigid, heavily sanitized "Military-Owned, Tactical Single-Use" (COSU) device.

What it Actually Blocks

Turning on this toggle actually alters specific behaviors inside XStealth PRO Tactical:

- Blocks the System Easter Egg: By far its most prominent effect. If you activate "Disallow fun," repeatedly tapping the "Android version" option inside the system settings will no longer launch the native Android 12 Easter Egg game (the dynamic Material You color clock and hidden space-emoji minigame).
- Locks Down DocumentsUI Debugging: Within the internal X-OS codebase, having this restriction enabled blocks access to experimental or hidden debug menus inside the system's native file manager (DocumentsUI).

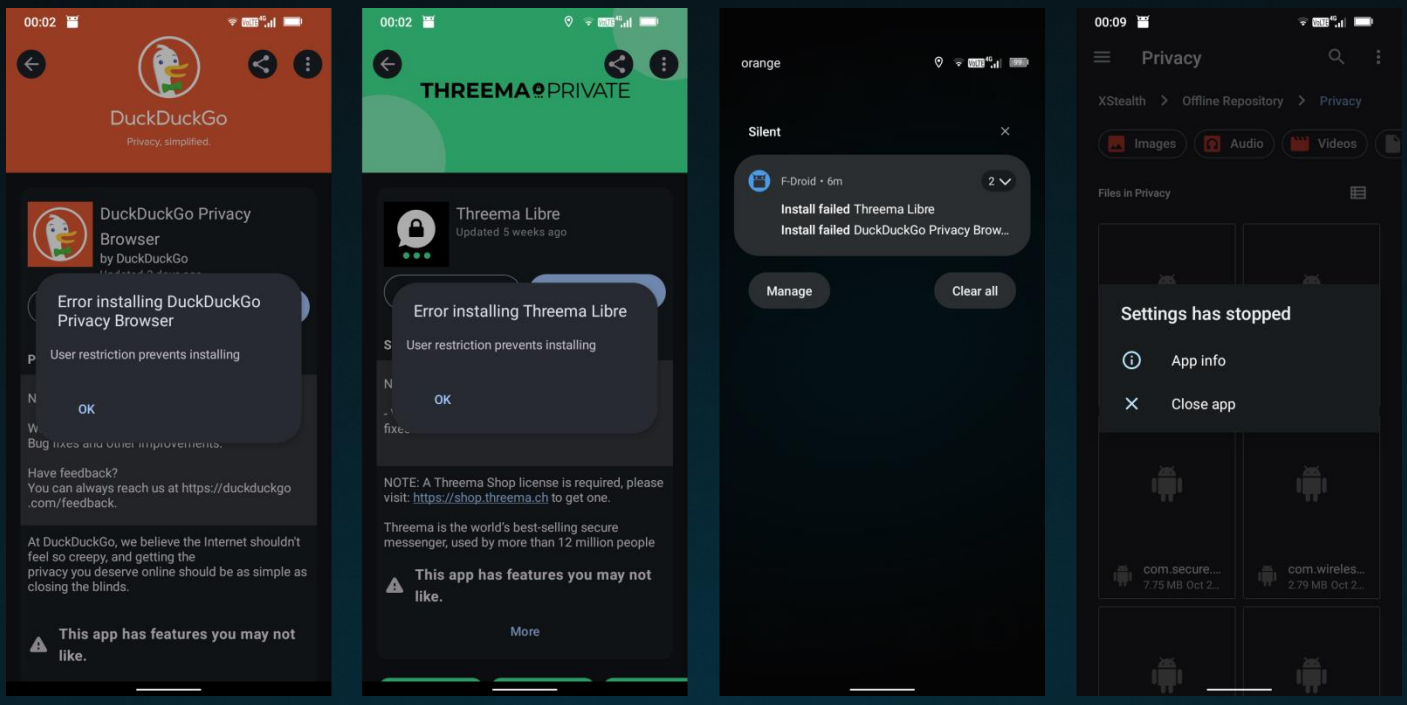
◉ Disallow install apps. This is a user restriction that completely blocks the device from installing new software applications or updating existing applications. It serves as a foundational security and Data Loss Prevention (DLP) policy used to freeze the application layout of tactical devices, preventing the insertion of unapproved, forensic-grade, or malicious software.

How It Works

When this restriction is toggled to On, the X-OS operating system intercepts the package installer pipeline at a deep system level:

- Blocks all App Stores (if any installed): It disables app installations via the FOSS App Stores (if any), OEM

app stores, and managed military/enterprise catalogs. The "Install" button inside these marketplaces will typically prompt an administrative lockout error.
- Blocks Sideloading (APKs): Even if the user transfers an APK file locally (via USB or cloud storage) or tries to trigger an install from a browser, the native PackageInstaller instantly crashes or denies the installation intent.
- Blocks ADB Installations: It intercepts and stops installations sent via the command line tool (adb install app.apk), rendering the device immune to computer-based application pushing.

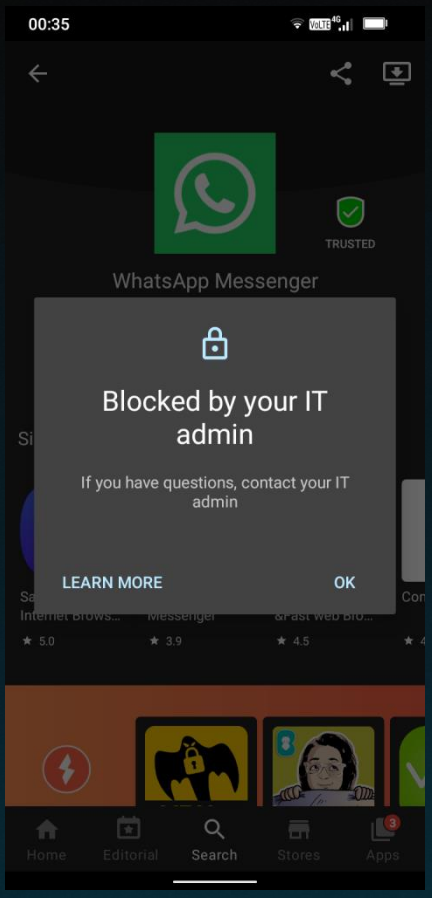


Disallow install apps

◉ Disallow install unknown sources. This is a security restriction that prevents you or attackers from enabling the "Install Unknown Apps" permission for any application. It is a foundational security control designed to block the sideloading of unapproved .apk files from browsers, file managers, or chat apps (if any), while ensuring the device can still download apps from trusted FOSS app stores like the F-Droid. The restriction applies to the entire operating system across all physical profiles, completely disabling sideloading.

How It Works
When this restriction is toggled to On, the X-OS system actively blocks the pipeline:
- Locks System Settings: If a user navigates to Settings > Apps > Special app access > Install unknown apps, the entire menu or individual application toggles (such as for Aptoide, Aurora Store, DuckDuckGo, or F-Droid) display an administrative lockout warning.
- Intercepts Runtime Requests: If an unapproved application attempts to trigger a package installation intent programmatically, the native system Package Installer intercepts the request and instantly denies it.
- What it Excludes: This policy strictly targets untrusted sources. It explicitly does not block applications installed via the Android Debug Bridge (ADB) or designated, trusted system military/enterprise app stores.

⚠ XStealth PRO Tactical has no App Stores installed. It can be installed upon request, but it is not recommended.



Disallow install unknown sources

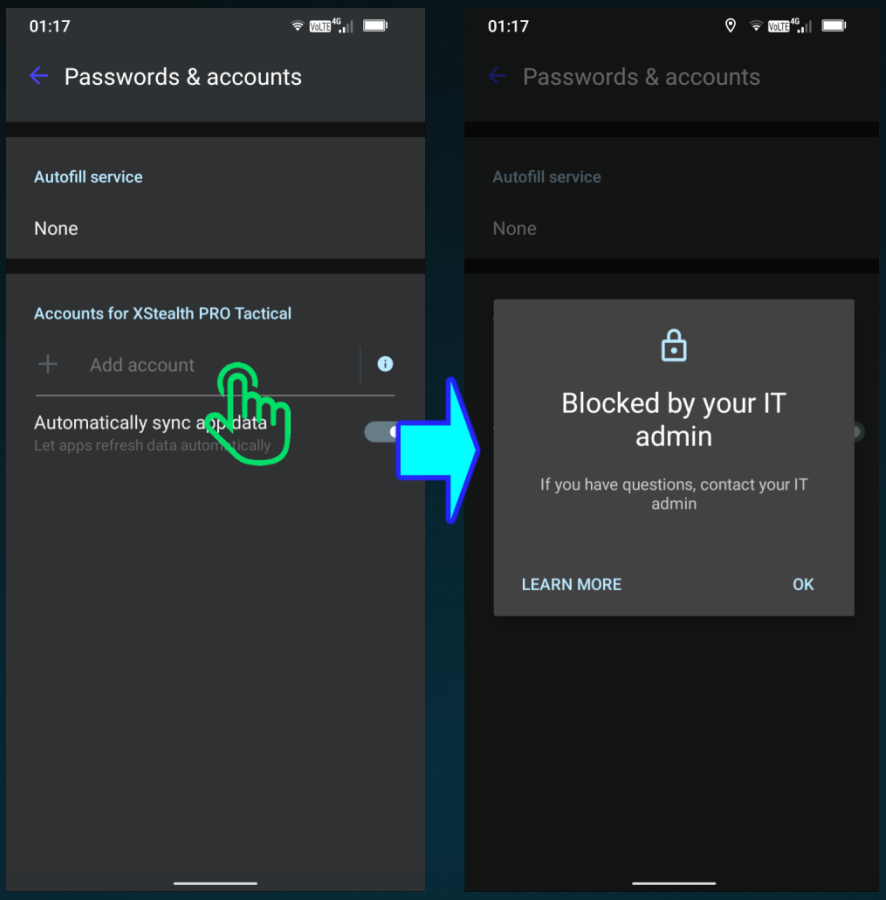
◉ Disallow installs from unknown sources globally. Blocks sideloading device-wide. When this restriction is toggled to On, the entire physical device is affected. It blocks the "Install Unknown Apps" toggles across all user spaces, accounts, and profiles on the device, including the user's personal sandbox.

When enabled:
- System Lockdown: The native settings menus for installing unknown apps become globally locked and completely inaccessible across both personal and Stealth profiles.
- Third-Party Blocks: No app on the device (whether Threema or a local file explorer) can be granted permission to trigger a package installation manually.
- Trusted Exceptions: It does not block apps distributed through officially authorized systems or applications explicitly pushed via the computer using the Android Debug Bridge (ADB).

◉ Disallow modify accounts. This is a user restriction that completely blocks device users from manually adding, changing, or removing user accounts. It serves as a critical security and Data Loss Prevention (DLP) safeguard, preventing users from connecting personal storage accounts (such as personal Google or cloud drives) to exfiltrate sensitive data. No user, secondary profile, or guest account can modify accounts anywhere on the physical system hardware.

How It Works & What It Blocks
When this restriction is toggled to On, the X-OS system enforces strict controls across the device configuration layer:
- Blocks Manual Additions: You cannot add new accounts under Settings > Passwords & accounts. This applies to all third-party sync accounts, including Google, Microsoft Exchange, and IMAP.
- Prevents Manual Removals: You are explicitly barred from removing existing Tactical accounts pre-

configured on the hardware by the Command and Control Center/enterprise.
- Locks System Preferences: The "Add account" button inside System Settings is entirely grayed out.
- Allows Programmatic Updates: This policy only blocks manual user interaction. Legitimate system authenticators and enterprise apps can still programmatically push, sync, or update account configurations in the background.



Disallow modify accounts

◉ Disallow mount physical media. This is a user restriction that prevents you/attackers from mounting or accessing external physical storage volumes attached to the device. It serves as a physical Data Loss Prevention (DLP) safeguard, ensuring that attackers cannot plug in peripherals to exfiltrate sensitive files or inject untrusted, malicious local data. When enabled, external storage is completely disabled across the entire physical motherboard layout. Blocks data from being copied to SD cards and memory sticks, and prevents a computer from accessing internal files over a data cable. It is used to prevent attackers from injecting malicious scripts or siphoning system data via physical USB ports.

How It Works & What It Blocks
When this restriction is toggled to On, the X-OS system monitors the hardware layer and actively cuts off the external storage pipeline:
- Blocks Hardware Mounting: If a user connects a physical storage medium to the device, the X-OS blocks the software mounting process entirely. The volume is rejected before the system file system assigns it a readable mount point path.
- Blocks SD Cards: Prevents the system from reading or formatting physical MicroSD cards inserted into the device's card tray.
- Blocks USB OTG (On-The-Go): Disallows flash drives, external solid-state drives (SSDs), or hard drives plugged directly into the device's USB-C port via an OTG adapter.

- Hides Storage in File Managers: Native or third-party file explorers will show absolutely zero external partitions, rendering the attached hardware invisible to the user.

- Maintains Charging/Midi Paths: This restriction specifically targets storage storage media volumes. It does not prevent the USB port from charging the phone or connecting non-storage USB peripherals such as physical keyboards, mice, or barcode scanners unless separate USB hardware policies are applied.

⚠ When this restriction is toggled to On, some security features of Self-Destruct and Secure Wipe will not work, for example, Secure Wipe when an external device is connected to the USB-C port.

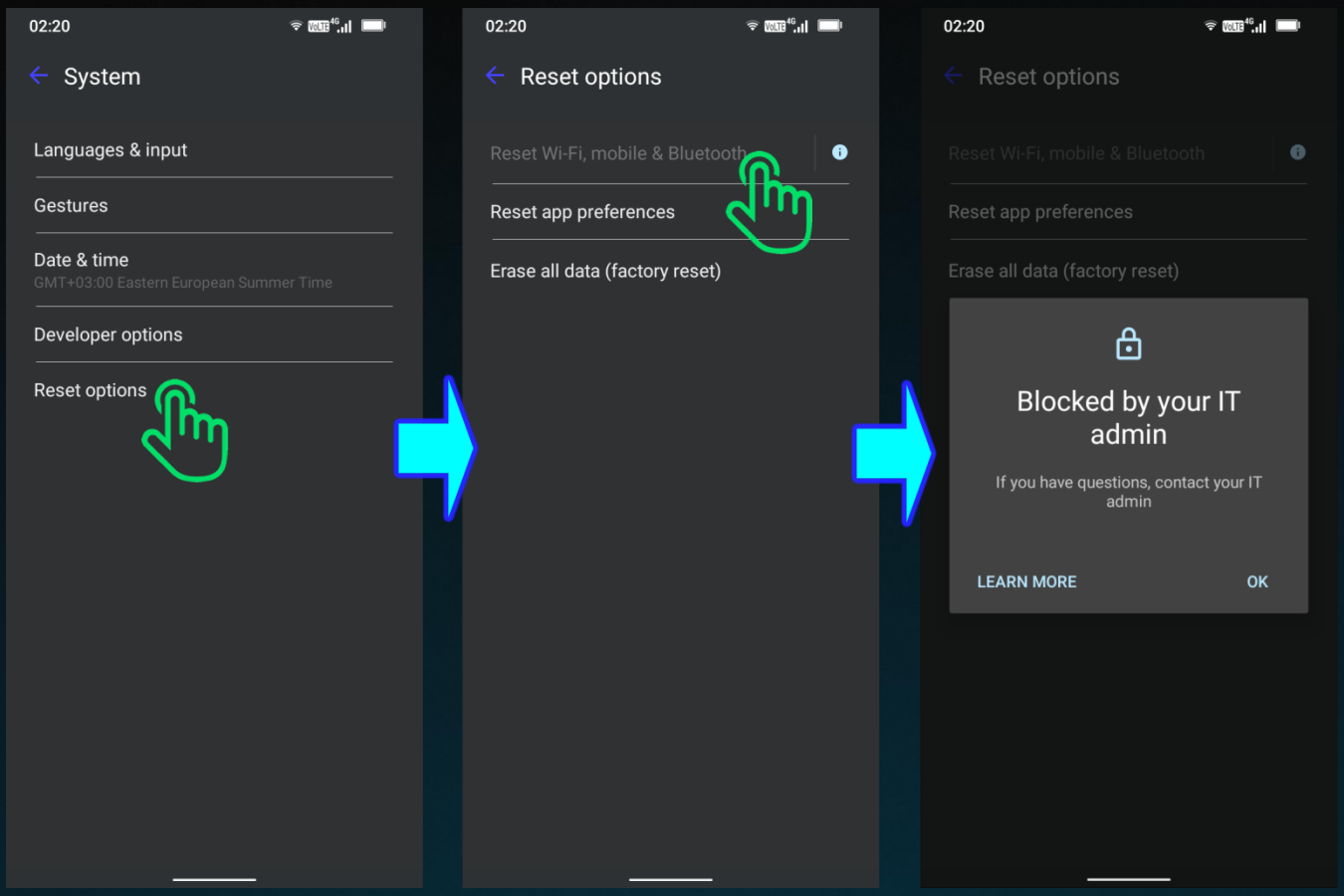
◉ Disallow network reset. This is a user restriction that prevents you or attackers from wiping the device's connectivity configurations. It is a key asset-integrity policy that prevents attackers from clearing configured network connections, removing secure Wi-Fi certificates, or disrupting active Mobile Device Management (MDM) communications. Neither you nor attackers can initiate a network reset under any circumstances. Prevents the erasure of saved Wi-Fi networks and stops attackers from modifying or connecting to unauthorized Wi-Fi hotspots.

How It Works & What It Blocks
When this restriction is toggled to On, the X-OS system actively locks down the system connectivity preferences:
- Disables System Toggles: The "Reset Wi-Fi, mobile & Bluetooth" or "Reset network settings" options inside Settings > System > Reset options are completely grayed out, and lock users out with an administrative message.
- Blocks Wi-Fi Wipeouts: It blocks the mass deletion of all saved secure Wi-Fi SSIDs, tactical/enterprise network security configurations, and pre-shared authentication keys.
- Configurations: It ensures custom Access Point Names (APNs) and local network routes cannot be wiped by the attacker to bypass traffic inspection.

◉ Disallow outgoing beam. This security policy prevents you and attackers from transmitting application data or files via Near Field Communication (NFC). This policy acts as a legacy Data Loss Prevention (DLP) safeguard to close data exfiltration vulnerabilities through short-range radio signals. It stops close-proximity tap-and-share file exfiltration and disallows high-speed local ad-hoc file beaming to nearby devices.

How It Works & What It Blocks
When this restriction is toggled to On, the X-OS framework restricts the NFC subsystem:
- Blocks Android Beam Outbound: It completely disables the outbound transmission of photos, contacts, files, or deep-linked URLs over NFC.
- Disables P2P Data Sharing: The physical action of tapping two phones together back-to-back will fail to initialize a data push channel from the restricted device.
- Preserves Inbound & Payment Traffic: This restriction specifically targets outgoing data beams. It does not block inbound data from other devices, and it generally does not interfere with standard NFC actions like mobile payments, reading NFC tags, or badge-in scanning unless a broader, total restriction is applied.

⚠ Toggle this restriction to ON when XStealth PRO Tactical devices are deployed in high-security, classified environments (like government data centers or secure record facilities), to satisfy STIG validation by entirely neutralizing unmonitored short-range air-gapped data transfers.



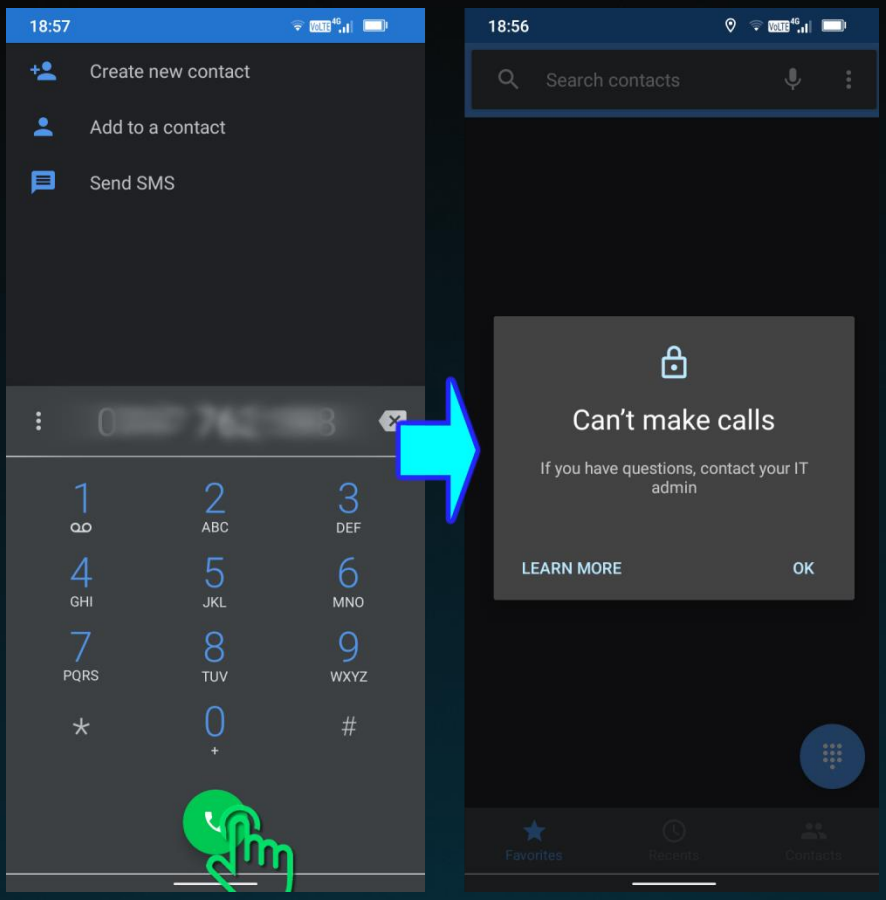
Disallow NFC

◉ Disallow outgoing calls. This is a user restriction that completely blocks the device from initiating standard cellular phone calls. It serves as a security measure to freeze a device's outbound communication when the covert mission requires it. The restriction applies to the entire operating system across all physical profiles, completely disabling cellular dialing. It is intended to harden Tactical mobile comms: For dedicated Tactical devices operating in high-security, classified environments, users or admins can toggle this restriction to ensure tactical teams cannot open the cellular line to make voice calls that could trigger unwanted attention from IMSI catchers in the area.

How It Works & What It Blocks

When this restriction is toggled to On, the X-OS telephony and telecom framework intercepts outbound dialing requests at the OS level:

- Blocks Voice Calls: The native Phone application is blocked from dialing out. If a user types a number and presses call, the operation instantly terminates, displaying a toast notification stating that the action is not allowed by the administrator.
- Intercepts App Intents: Third-party applications (if any) trying to invoke dialing intents (such as Intent.ACTION_CALL) will fail or throw a security exception, completely shutting down automated dialing pipelines.
- Crucial Exception (Emergency Calls): This policy strictly targets standard cellular outbound lines. It explicitly does NOT block emergency calls (such as emergency services). Emergency dialer channels remain unhindered for public safety compliance.
- Allows Inbound Calls: By default, this specific restriction only blocks outgoing traffic. The device can still receive incoming phone calls unless a separate, distinct call-blocking policy is specified.



Disallow outgoing calls

⚠ To establish a complete communication barrier on a tactical handset involved in spec ops, Command and Control Centers typically pair this restriction with other telephony toggles inside Tactical DPC: Disallow SMS and Disallow Config mobile networks.

◉ Disallow remove managed profile. This is a built-in user restriction that blocks device users or attackers from deleting the Stealth profile. When this policy is activated, the "Remove stealth profile" button in the phone settings is either grayed out or hidden. It acts as a tamper-protection mechanism for IT administrators. It prevents attackers from easily uninstalling the Tactical DPC app or ditching Tactical/corporate policies.

◉ Disallow remove user. This is a strict device restriction that prevents secondary users or guests from being deleted from an Android device. When enabled, the setting to delete any existing user or guest profile is completely blocked. It only restricts the removal of other users. It does not prevent a secondary user from deleting themselves if they are currently logged in to their own profile.

What It Blocks
The "Remove User" Button:
- The primary delete button inside Settings > System > Multiple users becomes completely unclickable for the primary administrator.
- Quick Settings Removal: The shortcut to delete a Guest profile directly from the notification shade/Quick Settings dropdown is blocked.
- App-Driven Deletion: Other standard apps or third-party management tools are programmatically blocked from calling user-removal APIs.

- Accidental Erasing: It blocks the master user from accidentally deleting critical, pre-configured secondary profiles used for other tactical team members or dedicated Tactical tasks.

⦿ Disallow safe boot. This security restriction prevents attackers from rebooting the device into Safe Mode, thereby preventing further hardware or software attacks.

How It Works
- The Security Gap: In normal Android environments, booting into Safe Mode disables all third-party applications. This allows attackers to bypass MDM management, circumvent control restrictions, or remove security tools.
- The Enforcement: When this restriction is toggled to On, the X-OS framework alters its boot sequence listener. If an attacker long-presses the "Power Off" option to trigger the "Reboot to safe mode" prompt, the system denies the command or completely suppresses the option.
- Hardware Interception: It can also block hardware button combinations (like holding Power + Volume Down during boot) used to force Safe Mode manually.

What It Blocks
- The Safe Mode Prompt: Disables the software trigger within the power menu.
- Tactical DPC Evasion: Prevents attackers from turning off Tactical DPC to run unmonitored apps.
- Policy Circumvention: Stops attackers from bypassing security-mandated restrictions (e.g., blocked websites, camera bans, app install limits).

⦿ Disallow set user icon. This is a security restriction that prevents attackers from changing the profile picture or avatar. This restriction applies directly to the specific user profile it is set on, meaning an admin can lock the icon for a secondary user while leaving the primary user unrestricted.

How It Works
- System Lock: When this restriction is toggled to On, the X-OS framework blocks any changes to the current user's photo.
- UI Gray-Out: The option to tap, edit, or upload a photo inside Settings > System > Multiple users or the notification shade profile menu becomes unclickable.
- API Block: It programmatically rejects any background software calls to the UserManager.setUserIcon() method.

What It Blocks
- Camera / Gallery Uploads: Users cannot take a new photo or select an existing picture from the gallery to use as their avatar.
- Default Avatar Changes: Attackers are blocked from switching between the built-in, color-coded Android default icons.
- Corporate Identity Tampering: It prevents attackers from changing mandated corporate or institutional avatar images on shared or dedicated devices.

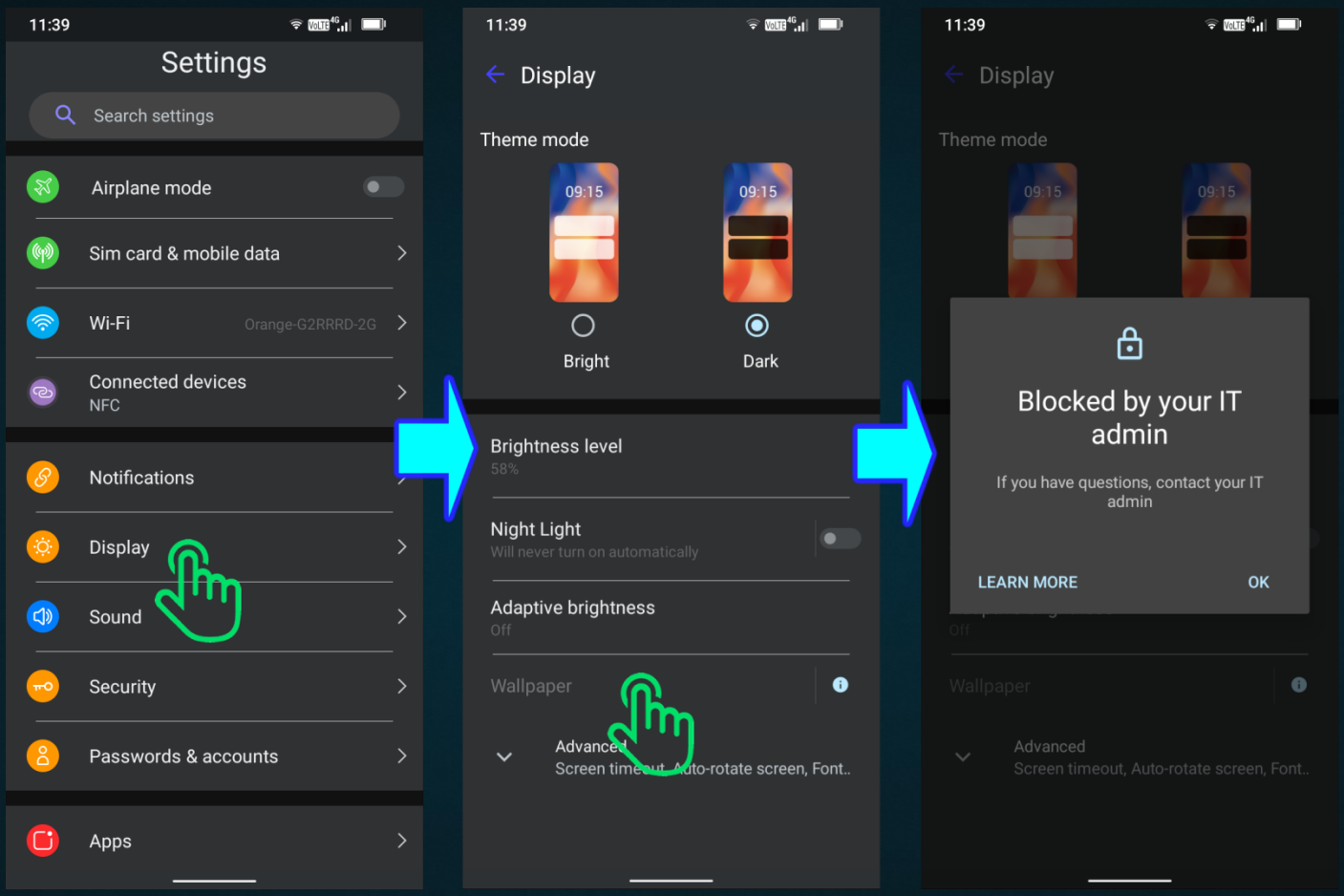
⦿ Disallow set wallpaper. This is a security restriction that prevents attackers from changing their home screen or lock screen background image. It completely locks down the background image of the entire phone. This is commonly used in Tactical devices to avoid images that can hide viruses or spyware.

How It Works

The X-OS dynamically disables wallpaper customization menus throughout the device interface, rendering the options unclickable.

What It Blocks

- Settings Modification: The Settings > Display > Wallpaper becomes unclickable, and displays a message stating the action is blocked by an administrator.
- Third-Party App Changes: Photos apps (like Gallery) and file managers are blocked from using the "Set as wallpaper" action.
- Launcher Customization: Third-party launchers (if any) are programmatically blocked from altering the desktop background image.



Disallow set wallpaper

◉ Disallow share location. This is a security restriction that prevents you or attackers from turning on location services. It completely prevents the primary device user from enabling global tracking data across the entire operating system.

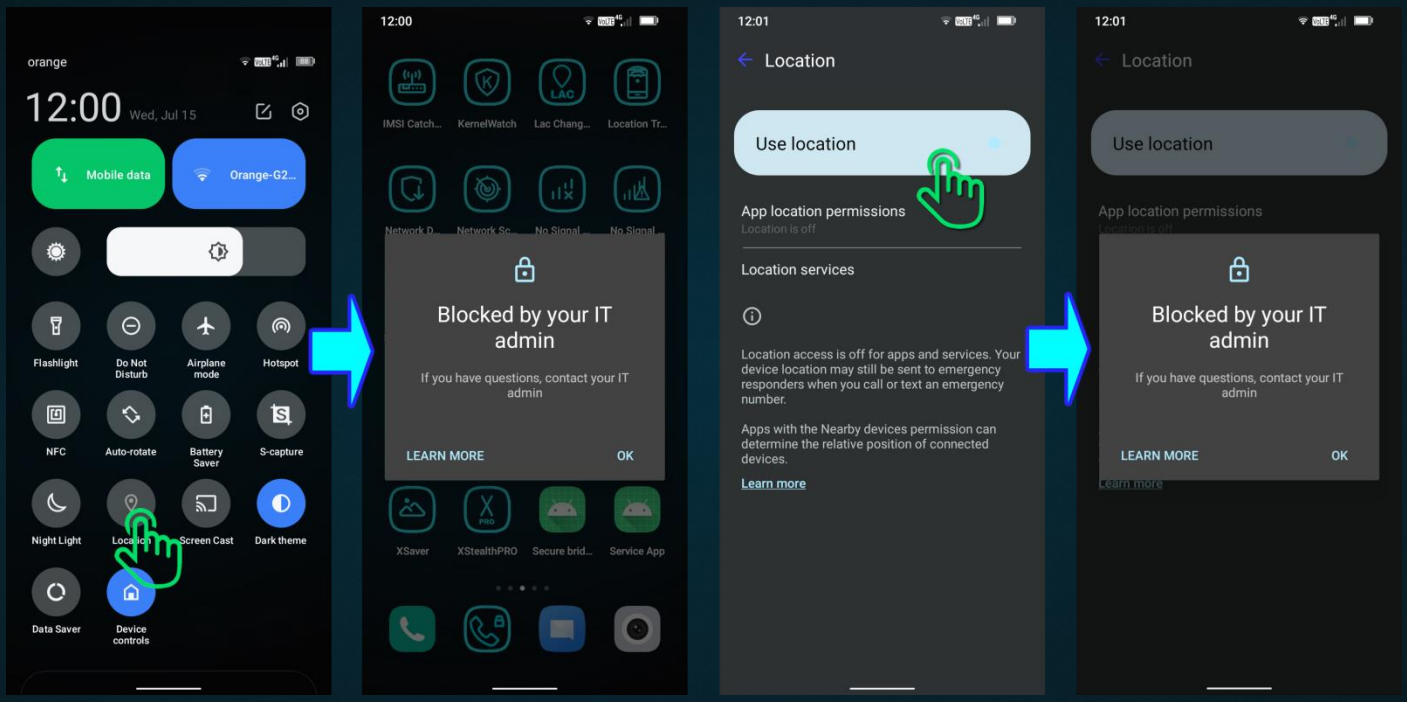
How It Works

- Enforcement: When this restriction is toggled to On, the Tactical DPC commands the operating system to set the location sharing restriction to true.
- State Interception: If location services are already turned off, the system completely locks the toggle, preventing the attacker from ever turning it on.
- Profile Mirroring: In a standard Stealth Profile setup, location tracking usually mirrors whatever the primary personal profile uses. Enabling this policy overrides that behavior, completely severing location

access and forcing it off inside the managed environment.

What It Blocks
- The Global Location Toggle: The master "Use Location" switch found inside Settings > Location is grayed out.
- Quick Settings Tile: Tapping the "Location" shortcut icon in the notification quick-settings dropdown will trigger an administrative warning.
- App Permission Grants: Applications inside the container cannot prompt the user with a pop-up requesting new ACCESS_FINE_LOCATION or ACCESS_COARSE_LOCATION permissions, as the underlying platform subsystem denies the request by default.
- Location Spoofing/Sharing: System-level emergency or regular location-sharing features (like Google Maps location sharing) are programmatically blocked from starting.

⚠ Unless you or your tactical team has a very specific mission that forces you not to enable GPS, DO NOT ENABLE “Disallow share location” feature! It will affect the functions of special apps.



Disallow share location

◉ Disallow SMS. This is a user restriction that completely disables the sending and receiving of Short Message Service (SMS) text messages. It locks down carrier-based messaging globally for the hardware.

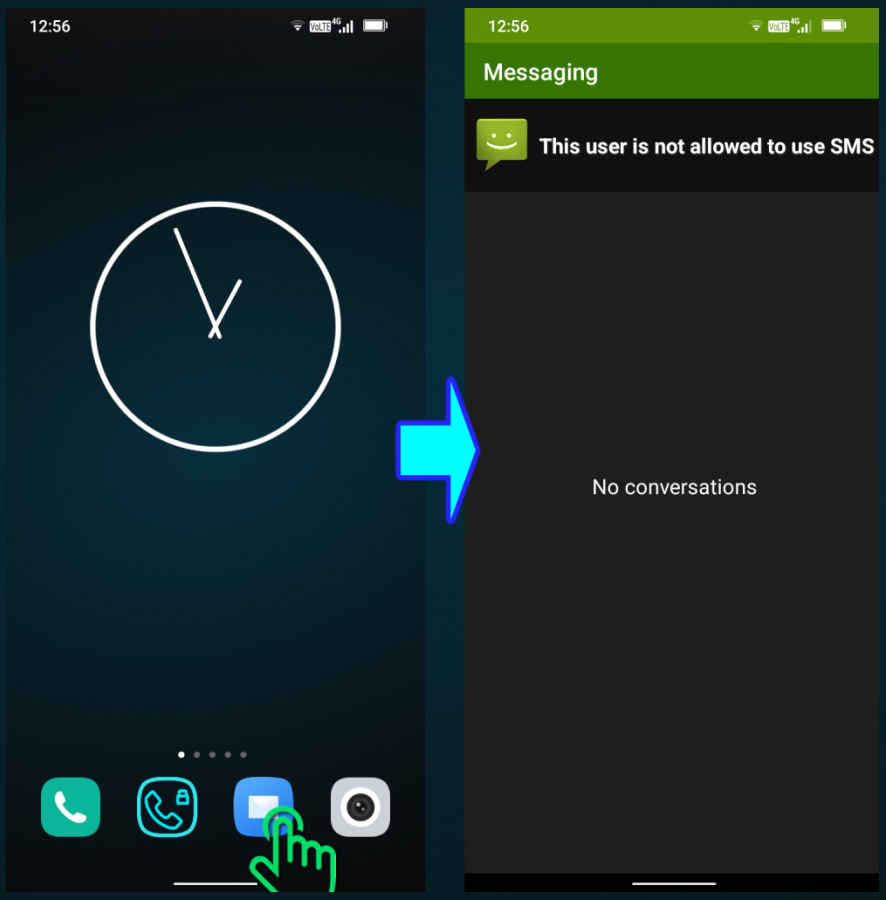
How It Works
- Framework Suppression: When this restriction is toggled to On, the X-OS operating system actively blocks the telephony subsystem from routing text messages.
- System-Level Precedence: This restriction bypasses user permissions entirely. Even if a messaging app explicitly holds the SEND_SMS or RECEIVE_SMS runtime permissions, the underlying X-OS will immediately fail the action with an internal safety block.

What It Blocks
- Outgoing Texts: Users cannot compose or transmit standard outbound SMS messages.
- Inbound Texts: The device completely drops incoming network signals for SMS, meaning texts sent to the

phone's number will never arrive, show notifications, or populate the database.
- Default Messaging App Access: System default clients (like Google Messages) are effectively neutralized, often displaying an error or stating that an administrator has disabled the feature.
- Two-Factor Authentication (2FA) & OTPs: Users are physically blocked from receiving automated carrier-based verification codes or One-Time Passwords used to log into third-party corporate accounts.
- Premium Rate SMS: Prevents end-users or attackers from accidentally or intentionally text-subscribing to expensive premium numbers or malicious services.

⚠ Note on Data Messaging: DISALLOW_SMS strictly intercepts carrier cellular text protocols. It does not block internet-based messaging protocols such as Threema, Signal, or Microsoft Teams unless separate application-blocking policies are in place.

⚠ Unless you or your tactical team has a very specific mission that forces you not to use SMS, DO NOT ENABLE this feature! It will affect the functions of special apps such as XPing and XCrypt MLSP. Also, detection functions such as LTP (Location Tracking Pings) will be hardly affected.



Disallow SMS

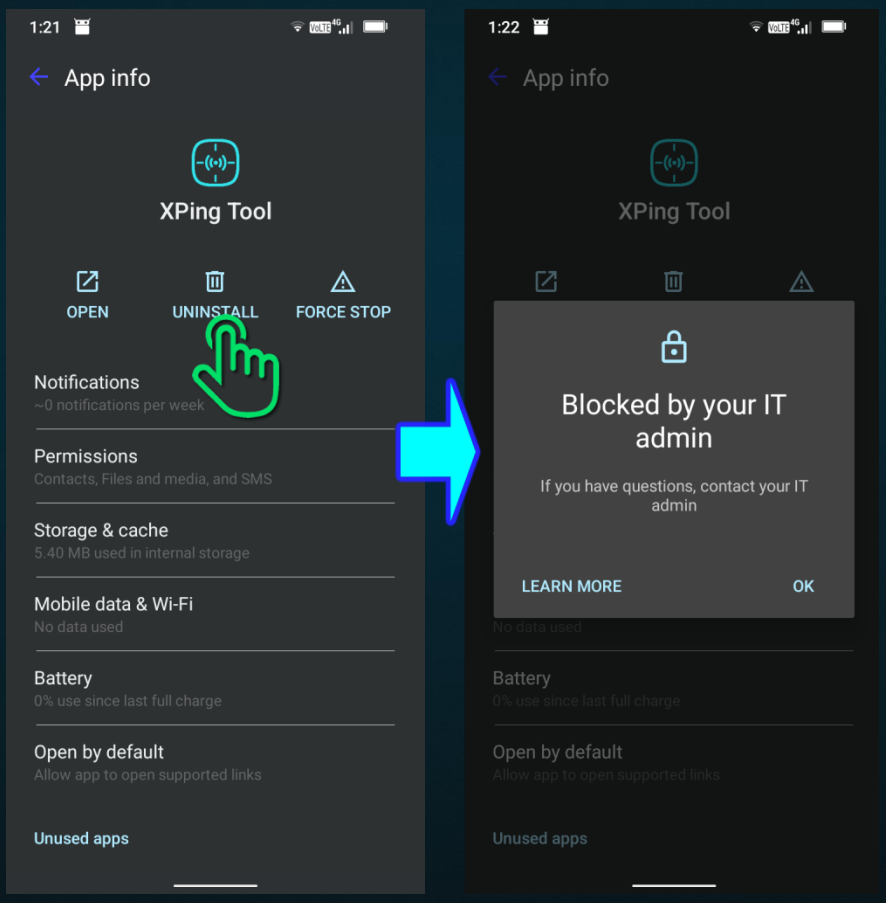
◉ Disallow uninstall apps. This is a user restriction that prevents attackers or users from deleting applications from the device, locking down all profiles so no applications can be uninstalled anywhere on the device.

How It Works
- System-Level Block: When this restriction is toggled to On, the X-OS framework sets the DISALLOW_UNINSTALL_APPS flag to true.
- UI Manipulation: The X-OS operating system immediately updates the interface. The "Uninstall" button inside the system Settings menu and the drag-and-drop "Uninstall" trash bin on the home screen launcher

are hidden, grayed out, or completely removed.
- Package Manager Interception: If an attacker, user, or a malicious process attempts to bypass the UI and forcefully trigger an uninstallation via code, the system's PackageManager intercepts the request and rejects it, throwing an internal administrative error.

What It Blocks
- Manual Deletions: Attackers or users cannot manually delete any user-installed applications, utility tools, or side-loaded APK files.
- MDM Removal: It prevents attackers or users from deleting critical tactical tools, tracking software, or mandated stealth applications.
- Storage-Clearing Deletions: Users cannot uninstall large apps to free up device storage space.
- Malicious App Tampering: Malware, attackers, or unauthorized users cannot delete military/corporate security agents or anti-virus applications running on the device.

⚠ Note on Exceptions: This policy strictly stops the removal of applications. It does not block users from updating apps to newer versions, nor does it prevent them from choosing "Disable" for pre-installed system apps when the system allows it.



Disallow uninstall apps

⦿ Disallow unmute microphone. This user restriction permanently mutes the device's microphone. It enforces a hard mute globally across all user profiles and containers on the physical hardware.

How It Works
- The Forced State: When this restriction is toggled to On, the X-OS operating system actively triggers a global mute on the master microphone audio stream.

- The Blocking Logic: Once muted by the policy, any physical or software-based attempt by the user to turn the microphone back on is completely blocked. The system intercepts the volume/mute controls and denies the "unmute" instruction.
- X-OS Privacy Intersect: X-OS introduced dedicated Quick Settings tiles to completely block/unblock Microphone access. If DISALLOW_UNMUTE_MICROPHONE is active, the microphone is hard-muted at the framework layer, overriding any user adjustments to these new privacy toggles or volume sliders.

What It Blocks
- Voice Recording & Input: All apps attempting to record audio or stream voice inputs receive absolute silence or a zeroed-out audio stream.
- Phone Calls & VoIP: During standard cellular calls or VoIP conversations (e.g., Zoom, Microsoft Teams, Slack), the user cannot unmute themselves; the microphone stays dead on the other end.
- Voice Assistants: System assistants (like Google Assistant) are completely blocked from hearing wake-words like "Hey Google" or registering any voice commands.
- Volume Settings Modification: Any microphone input adjustment sliders inside Settings > Sound & vibration are either locked, grayed out, or entirely missing.

Note on Eavesdropping Protection: This restriction is widely favored in top-secret government/corporate environments, secure government facilities, or high-security tactical environments to ensure a device cannot be used as a covert listening or recording device.

◉ Disallow USB file transfer. This is a security restriction that prevents users or attackers from transferring files between a mobile device and a computer over a USB connection. Tactical DPC enforces this restriction globally across the entire physical hardware to protect corporate endpoints from data leaks.

How It Works
- Protocol Block: When this restriction is toggled to On, the X-OS operating system instructs the USB hardware abstraction layer (HAL) to strictly neutralize file transfer protocols.
- Selective Filtering: It acts as a specialized data filter. It selectively targets data storage protocols while leaving basic hardware interface signaling intact

What It Blocks
- MTP (Media Transfer Protocol): The standard protocol used to browse and move folders between Android and Windows/Mac computers is completely disabled.
- PTP (Picture Transfer Protocol): Camera-emulation mode used to import photos into desktop software is hidden and blocked.
- USB Mass Storage Mounting: The system cannot mount internal storage or the SD card as a physical disk drive on a computer.
- The USB Configuration UI: When a USB cable is plugged in, the system notification dropdown menu grays out or hides the "File Transfer / Android Auto" and "MIDI" checkboxes, forcing the connection type exclusively to "No data transfer / Charge only".

What it does NOT block: Standard non-storage USB peripherals—such as external USB mice, physical keyboards, wired game controllers, and basic USB charging—continue to function normally.

When enabled, the Self-Destruct feature will not work when a USB data cable is connected to the phone's USB-C port.

◉ Ensure verify apps. This is an X-OS security restriction that forces the device's malware-scanning service (Google Play Protect) to remain permanently enabled. While this feature applies to XStealth ULTRA devices (based on the Samsung Galaxy series and a few other brands), it does not apply to the XStealth PRO series, which are 100% degoogled phones with no Google dependencies, such as Google Play Protect. Instead, X-OS uses its own framework to verify new app installations. However, XStealth PRO Tactical has no App Stores so that no apps can be installed.

◉ Disallow autofill. This is a security restriction that prevents credential managers and password vaults (if any) from automatically inputting data into text fields. It serves as a critical data loss prevention (DLP) mechanism to prevent sensitive tactical credentials, addresses, and payment data from leaking across different apps or profiles, and shuts off global password tools.

How It Works
System Flag Toggling: When this restriction is toggled to On, the app forces the device's internal DISALLOW_AUTOFILL flag to true.
- Subsystem Shutdown: The X-OS immediately communicates this block to the platform's core AutofillManager service.
- Input Interception: When the attacker or user taps into a text input field (such as a username, password, or credit card box), the system forces AutofillManager.isEnabled() to return false. This prevents any installed credential tool from reading the input fields or offering data injections.

What It Blocks
- Password Manager Prompts (if any): Floating overlay prompts from password managers (such as Google Autofill, 1Password, Bitwarden, or Dashlane) are completely suppressed.
- Settings Page Access: The configuration submenus under Settings > Passwords & accounts become hidden entirely. Users cannot switch or add new autofill providers.
- Browser Data Form-Filling: Web browsers (like Google Chrome) are blocked from auto-populating saved mailing addresses, telephone numbers, and credit card info into online forms.
- Inline Keyboard Suggestions: It stops predictive keyboards (like Gboard) from displaying sensitive credentials or addresses directly inside the keyboard suggestion strip.

◉ Disallow Bluetooth sharing. It works only on the XStealth ULTRA series.

⚠ XStealth PRO (both Dominator and Tactical versions) comes with permanently disabled Bluetooth at the hardware level. There is no point in using the "Disallow Bluetooth sharing" option.

◉ Disallow separate challenge. This security restriction requires the stealth profile to use the exact same screen lock (PIN, pattern, or password) as the personal profile. Requires a managed profile added by your organization's IT admin.

◉ Disallow user switch. This is a user restriction that prevents a device from switching between different local user profiles. It allows the primary admin to block secondary users from stealing the active screen session.

How It Works
- Session Lock: When this restriction is toggled to On, the app forces the device's internal DISALLOW_USER_SWITCH database flag to true.

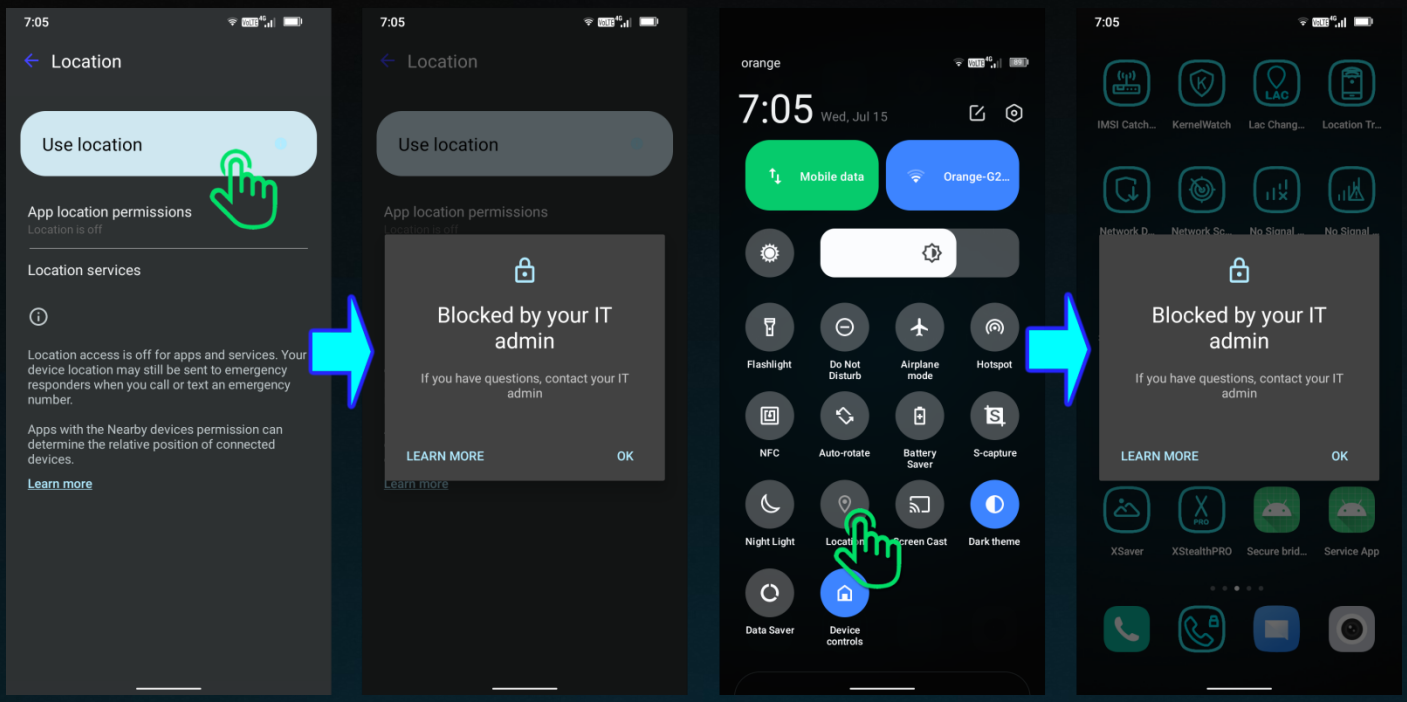
- Multi-User Freeze: The X-OS operating system immediately disables the underlying multi-user switching mechanism. The system will reject any background API requests to swap active profiles via UserManager.switchUser().
- State Preservation: The device becomes locked into whichever profile was active at the exact moment the restriction was applied.

What It Blocks
- Quick Settings User Icons: The user profile shortcut icon in the top-right corner of the notification shade/Quick Settings dropdown is hidden or unclickable.
- Lock Screen Profile Switching: The multi-user account list typically visible on the lock screen disappears, preventing anyone from swapping profiles without unlocking the device first.
- Settings Menu Redirection: The profile selection options inside Settings > System > Multiple users are completely grayed out, displaying a message that an admin has blocked the action.
- Guest Session Escapes: If an administrator forces a device into a "Guest" profile and then triggers this restriction, the guest user is physically trapped and cannot return to the primary owner profile.

⦿ Disallow config location. This is an attacker/user restriction that prevents users from changing any location-related settings or permissions. It locks down location configurations globally across the entire physical hardware. This is heavily used by Command and Control Centers to ensure field operatives or agents cannot disable GPS tracking to hide their location from C2.

How It Works
- State Freezing: When this restriction is toggled to On, the X-OS framework locks whatever location configuration is currently active. If location is on, it stays on permanently; if it is off, it stays off permanently.
- UI Gray-Out: The X-OS operating system immediately modifies the Settings app. All toggles, sliders, and menus related to location services become unclickable.
- Permission Lock: It also locks the location permissions for individual apps, preventing the attacker/user from manually revoking or granting GPS access to installed applications.
What It Blocks
- Master Location Toggle: The main "Use location" switch inside Settings > Location is entirely frozen.
- App-Level Location Permissions: Users cannot go to Settings > Apps to change an application's location permission (e.g., changing an app from "Allow all the time" to "Don't allow").
- Location Provider Toggles: It blocks tweaking individual location sub-settings, such as Google Location Accuracy, Wi-Fi scanning, and Bluetooth scanning for location.
- Quick Settings Changes: Tapping the "Location" quick-settings tile in the notification shade will not change its state; it will show an administrative warning.

 Unless you or your tactical team has a very specific mission that forces you not to enable GPS, DO NOT ENABLE this feature! It will affect the functions of special apps.



Disallow config location

◉ Disallow airplane mode. This is a security restriction that prevents attackers/users from turning on Airplane Mode. IT administrators deploy it to guarantee that Tactical devices remain permanently connected to cellular and data networks. This is critical for preventing field operatives or attackers from disconnecting a Tactical asset from the Command and Control Center's radar.

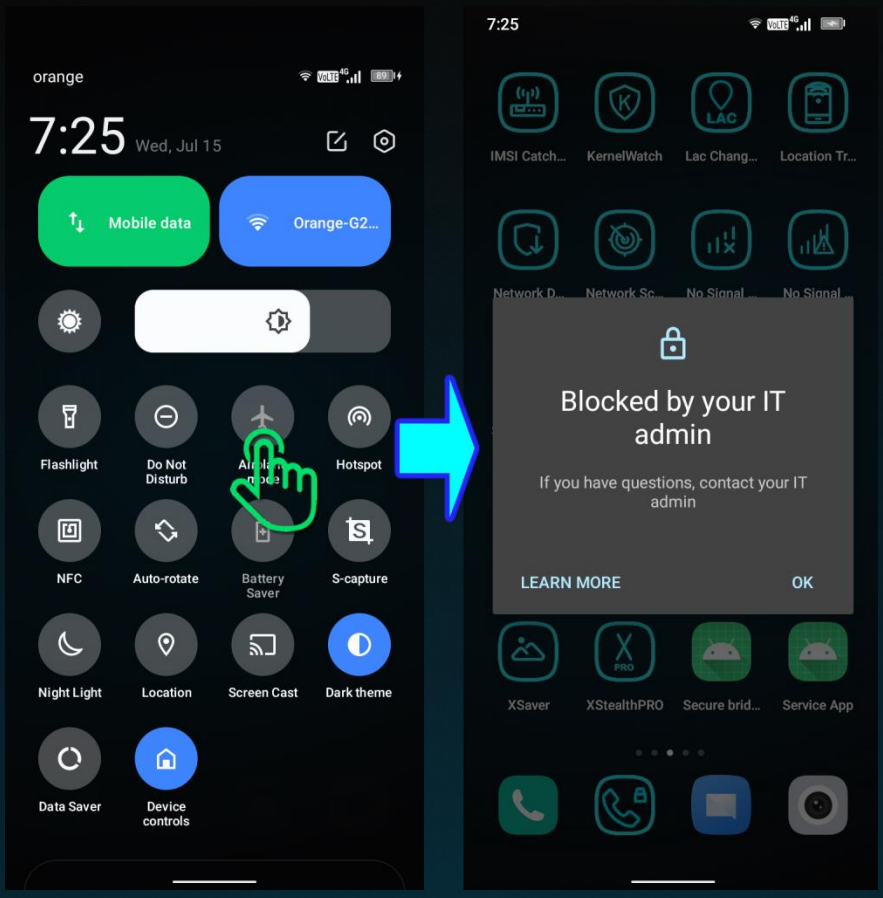
How It Works

- State Freezing: When this restriction is toggled to On, the app forces the device's internal DISALLOW_AIRPLANE_MODE flag to true.
- UI Disabling: The X-OS system immediately modifies the interface. The standard toggle switch for Airplane Mode is either hidden or grayed out.
- Network Continuity: If Airplane Mode is off when the policy is applied, it is locked off. If an attacker/user tries to toggle it, the action is blocked, ensuring the device's cellular and Wi-Fi radios remain active.

What It Blocks

- The Quick Settings Tile: Toggling Airplane Mode from the notification pull-down panel is completely blocked.
- Settings Modification: The Airplane Mode switch bar inside Settings > Network & Internet is completely frozen.
- Offline Evasion: It stops attackers/users from going offline to deliberately block real-time tracking, bypass mobile device management (MDM) geofencing limits, or stop Tactical data syncing.
- Power Menu Triggers: On devices where the physical power button menu provides an option to go offline, that option is removed. Not available for XStealth PRO versions.

⚠ It is used on critical missions and spec ops that require full radio silence.



Disallow airplane mode

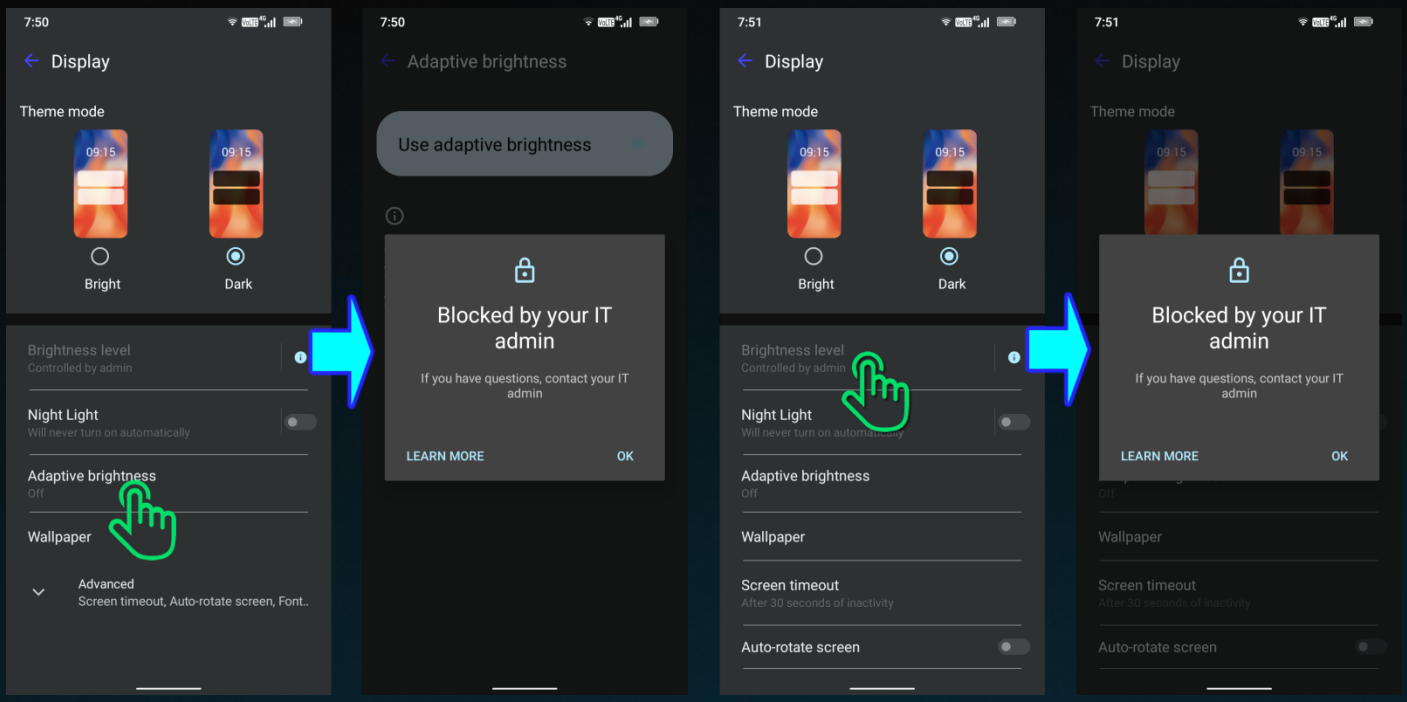
◉ Disallow config brightness. This is a security restriction that prevents users from changing the device screen brightness and display illumination settings. It is commonly deployed on Tactical devices to ensure optimal display visibility when using night-vision tactical goggles and to prevent unauthorized screen dimming.

How It Works

- UI Lockout: When this restriction is toggled to On, the app forces the device's internal DISALLOW_CONFIG_BRIGHTNESS flag to true.
- Slider Disabling: The X-OS system immediately modifies the System UI layout. The brightness adjustment slider in the Quick Settings notification pull-down menu is grayed out.
- Baseline Anchoring: IT administrators generally use this setting to explicitly set a permanent screen brightness level (e.g., 20%) first, and then toggle this restriction to lock that setting into place, for tactical mission use.

What It Blocks

- The Quick Settings Slider: Users cannot drag the quick-access brightness bar to dim or brighten the screen.
- Adaptive / Auto-Brightness Toggles: The switch to turn on or off "Adaptive brightness" inside Settings > Display becomes unclickable.
- System Display Menus: The main brightness configuration options inside the X-OS Settings application are completely grayed out.
- App-Level Disruption: Third-party utility apps or custom launchers (if any) are programmatically blocked from overriding the master display luminosity layers.



Disallow config brightness

◉ Disallow config date time. This is a security restriction that prevents attackers or users from manually changing the device's date, time, or time zone settings. It functions as a critical anti-tampering measure on Tactical networks, preventing attackers or field operatives from altering timestamps to cheat logging systems or manipulate time-sensitive app functionality. It locks the date and time fields globally for the hardware. This is essential for missions, spec ops, etc.

How It Works
- UI Lockout: When this restriction is toggled to On, the app switches the system's DISALLOW_CONFIG_DATE_TIME database flag to true.
- Settings Freezing: The X-OS system instantly responds by modifying the interface layout. The user-facing menus for time customization are disabled.
- Network Clock Enforcement: Administrators typically combine this restriction with a policy that forces network-provided time (setAutoTimeEnabled). Once both are active, the phone is locked onto accurate cellular network time, and the attacker/user cannot manipulate the clock.

What It Blocks
- Manual Time Changes: The "Set time automatically" switch inside Settings > System > Date & time is frozen, and the manual "Date" and "Time" picking wheels are grayed out.
- Time Zone Manipulation: The "Set time zone automatically" toggle is locked, blocking users from choosing a different geographical region to shift the system clock.
- Timestamp Evasion: It stops attackers/users from rolling back the clock to bypass app license expirations, manipulate shifts on field operatives' time-tracking tools, or delay tactical security certificate checks.
- Log Desynchronization: It ensures that audit trails, device location pings, and security logs remain sequentially accurate, preventing malicious activities from being hidden behind incorrect timestamps.

◉ Disallow config screen timeout. This is a security restriction that prevents users from changing how long the display remains on before turning off or going to sleep mode.

How It Works
- UI Lockout: When this restriction is toggled to On, the app flips the device's internal DISALLOW_CONFIG_SCREEN_TIMEOUT flag to true.
- Menu Freezing: The X-OS system immediately updates the System UI. The dropdown menu or list of time options for screen standby becomes grayed out.
- Tactical mode Stabilization: Administrators typically use Tactical DPC to programmatically set a specific timeout length (or use a separate command to keep the screen permanently awake while plugged in) and then toggle this restriction to lock that preference down.

What It Blocks
- Timeout Adjustments: The "Screen timeout" or "Sleep" menu inside Settings > Display becomes unclickable, preventing attackers/users from altering the timing interval (e.g., changing it from 30 seconds to 30 minutes).
- Power-Saving Alterations: It stops attackers/users from forcing the screen to turn off quickly to disrupt dedicated Tactical tasks, or conversely, extending it indefinitely to drain the device's battery.
- Third-Party Display Overrides: Standard third-party personalization apps (if any) or alternative launcher tools (if any) are programmatically blocked from overriding the master framework's sleep timer settings.

◉ Disallow ambient display. This is a security restriction that prevents the device screen from lighting up for low-power glances or notifications when the display is turned off. This is critical on Tactical devices to prevent onlookers from reading sensitive data or verification codes that flash onto a resting phone. It also serves as a powerful battery-preservation measure.

How It Works
- UI Suppression: When this restriction is toggled to On, the app flips the device's internal DISALLOW_AMBIENT_DISPLAY flag to true.
- Lock Screen Freezing: The X-OS framework immediately suppresses low-power wake triggers. The screen is forced to remain entirely dark and powered off unless the physical power button is pressed or biometrics are used.

What It Blocks
- Always-On Display (AOD): Completely disables the clock, battery percentage, and notification icons that normally persist on an OLED screen while the device is sleeping.
- Lift-to-Wake / Ambient Wake: Blocks the device accelerator from waking up the low-power display layout when a user picks up the phone from a flat surface.
- Tap-to-Wake: Stops the screen from partially waking up when a user double-taps the dark display pane.
- Pulse Notifications: Prevents incoming app alerts or text messages from briefly illuminating a grayscale preview on an otherwise sleeping lock screen.

◉ Disallow sharing data into the profile. Requires a managed profile. This user restriction prevents personal data and files from entering the secure work profile container. It serves as a strict inbound data barrier. It prevents data leaks and malware contamination by ensuring that personal, unmanaged files cannot be introduced into Tactical systems.

How It Works
- Intent Neutralization: When this restriction is toggled to On, the X-OS framework modifies the system's

cross-profile communication rules. It breaks down the default built-in intent communication filters that X-OS automatically creates to connect the personal and Tactical sides.
- Isolation Enforcement: By default, X-OS allows users to pass items from the personal side to the Tactical side to make things easier. Activating this policy tells the DevicePolicyManagerService to block those entry paths, turning the Tactical profile into a one-way isolated sandbox.

What It Blocks
- Personal-to-Work Shares: If you open a photo, PDF, or text snippet in a personal app (like a web browser, if any) and open the Android Share Sheet, Tactical apps will be completely missing from the target list.
- In-App Work File Picking: If you are inside a Tactical app and tap "Attach File," the app is programmatically blocked from opening the personal file manager or gallery to choose a personal photo.
- Cross-Profile Clipboard Transfers: Copy-pasting text fields from a personal browser or app into a Tactical document or text field is intercepted and blocked.

⦿ Disallow printing. This is a security restriction that prevents attackers/users from sending documents or data to physical or digital printers from their managed environment.

How It Works
When this restriction is toggled to On, it utilizes the system-level DISALLOW_PRINTING user restriction. This tells the X-OS system to hide or disable all printing-related hooks across the device, entirely preventing the "Print" option from appearing in the Android Sharesheet or in-app menus.
This restriction is designed for data security. In Tactical environments, it ensures sensitive Tactical data cannot be physically printed or removed from the secure ecosystem via hardcopy documents.

What It Blocks
When enabled, this policy restricts the following:
- System Print Services: It turns off the OS-level printing subsystem, preventing the device from discovering or connecting to Wi-Fi or cloud printers.
- Third-Party Printing Plugins: It blocks installed printing services (if any) from operating.
- "Print to PDF": Even the option to save a screen or document as a digital PDF via the system print dialog is disabled.

⦿ Disallow config private DNS. This security policy prevents users from manually changing or viewing the "Private DNS" settings on a device.
Security teams couple this restriction with a globally enforced Tactical DNS server. By blocking access to the Private DNS settings, they ensure that all device traffic is routed strictly through their secure, monitored resolvers, preventing data exfiltration, malware infections, and circumvention of firewalls.

How It Works
When enabled in Tactical DPC, the app triggers the system-level DISALLOW_CONFIG_PRIVATE_DNS user restriction flag. The X-OS system immediately locks down the Private DNS menu located in the device's network settings (Settings > Network & internet > Private DNS). The attacker/user can no longer toggle between Off, Automatic, or type in a Private DNS provider hostname. The menu options will either be completely grayed out.

What It Blocks

- Manual DNS Swapping: Attackers/users cannot input custom, encrypted DNS-over-TLS (DoT) providers (such as AdGuard or Cloudflare) to bypass network rules.
- Bypassing Content Filters: It blocks users from turning Private DNS "Off" or switching it to an unencrypted state to escape web filters imposed by the organization's network.
- Disabling Enterprise Ad-Blockers: If an administrator forces a specific enterprise DNS configuration globally, this policy prevents the user from overriding it.

⦿ Disallow microphone toggle. This security policy prevents users from disabling system-wide microphone access, ensuring that the device's hardware microphone remains active and available for Tactical apps.

How It Works
When enabled via Tactical DPC, the app deploys the underlying system flag DISALLOW_MICROPHONE_TOGGLE. The X-OS immediately overrides manual user controls:
- Quick Settings Lockout: The global "Mic Access" Quick Settings tile becomes unclickable.
- Privacy Menu Override: The hardware microphone toggle under Settings > Privacy is locked down.
- Automatic Re-enabling: If a user had already disabled microphone access right before this policy was turned on, Android will force-enable the microphone automatically the moment the restriction is applied.

What It Blocks
- Manual Mic Disabling: Attackers/users cannot block microphone access across the entire device.
- Accidental Muting: It blocks users from accidentally toggling off hardware access, which could otherwise break critical Tactical apps.
- Circumvention of Tactical Apps: It prevents field operatives from shutting off the microphone to bypass Tactical voice-recording, communication, or Tactical compliance tools.

⦿ Disallow camera toggle. This security policy prevents attackers/users from disabling system-wide camera hardware access, ensuring the device's hardware camera remains active and available for Tactical use.

How It Works
When enabled via Tactical DPC, the app deploys the underlying system flag DISALLOW_CAMERA_TOGGLE. The X-OS immediately overrides manual user controls:
- Quick Settings Lockout: The global "Camera Access" Quick Settings tile becomes unclickable.
- Privacy Menu Override: The hardware camera toggle under Settings > Privacy is locked down.
- Automatic Re-enabling: If an attacker/user had already disabled camera access right before this policy was turned on, X-OS will force-enable the camera automatically the moment the restriction is applied.

What It Blocks
- Manual Camera Disabling: Attackers/users cannot block camera access across the entire device.
- Accidental Disabling: It blocks users from accidentally shutting off the hardware, which would break tactical-critical workflows like identity verification.
- Circumvention of Tactical Apps: It prevents attackers/users from shutting off the camera to bypass Tactical video-recording, field-service, or remote-support tools.

⦿ Disallow Wi-Fi tethering. Requires API level 33. Not available on XStealth PRO versions.

⦿ Disallow shared admin-configured Wi-Fi. Requires API level 33. Not available on XStealth PRO versions.

◉ Disallow Wi-Fi direct. Requires API level 33. Not available on XStealth PRO versions.

◉ Disallow add Wi-Fi config. Requires API level 34. Not available on XStealth PRO versions.

◉ Disallow Cellular 2G. Requires API level 33. Not available on XStealth PRO versions.

◉ Disallow config locale. This security policy prevents attackers/users from changing the device language. It locks down regional and systemic language preferences to maintain uniformity across deployed Tactical hardware. No attacker/user or secondary profile on the device can modify the core language.
In tactical missions, maintaining a fixed language is critical. Enabling this policy ensures that a user cannot accidentally or maliciously render a device unusable or unreadable to other Tactical team members by switching it to an unfamiliar language or character set.

How It Works
When enabled via Tactical DPC, the app pushes the system-level user restriction flag DISALLOW_CONFIG_LOCALE to the X-OS. The operating system immediately locks out manual configuration:
- Settings Lockout: The language settings menu (Settings > System > Languages & input > Languages) becomes completely unclickable.
- Prompt Blocks: If an app or website tries to redirect the user to the native system settings to download a new regional language pack, X-OS intercepts and blocks the action.

What It Blocks
- Language Changes: Users cannot swap the primary system interface text between languages (e.g., changing from English to Spanish).
- System-Wide Regional Modifications: It blocks users from adding secondary languages or shifting the order of preferred languages.
- Locale-Dependent Keyboards: Users cannot manually add a localized system keyboard layout that requires installing a totally new system language profile.

◉ Disallow ultra wideband radio. Requires API level 34. Not available on XStealth PRO versions.

◉ Disallow config default apps. Requires API level 33. Not available on XStealth PRO versions.

◉ Disallow assist content. This security policy prevents AI assistants and privileged overlay apps from reading, scraping, or analyzing contextual data from the active screen.
With the integration of advanced generative AI models into default device assistants, sensitive Tactical data can easily leak into external AI datasets. If a field operative uses an AI assistant to "summarize an email" or "explain this spreadsheet," that classified Tactical information gets sent to third-party servers. When toggled to On, it stops data sprawl at the OS level while still allowing the user to use the assistant for basic, non-contextual commands (like checking the weather or setting an alarm).
⚠ For maximum security, XStealth PRO versions have no AI assistants. There is no point in disallowing assist content.

◉ Disallow SIM globally. Requires API level 33. Not available on XStealth PRO versions.

◉ Disallow add private profile. This is a security policy introduced in Android 15 that prevents users from creating or using a Private Space on their device. Private Space is a feature that creates an isolated,

password-protected area on the device to hide sensitive personal apps from the main app drawer and notifications.

⚠ XStealth PRO versions run on X-OS, a proprietary Android 12 fork. It does not have the Private Space option.

- **Set user restrictions on parent**. Requires an organization-owned profile manager added by your organization's IT admin.

Settings management

- **Keep the device on while plugged in**. This security policy keeps the device's screen fully lit and prevents it from entering sleep mode as long as it is connected to a power source. This feature is highly functional for Tactical/dedicated deployment scenarios:
  - Tactical and Digital Signage Modes: Essential for critical missions where the screen must remain visible to field operatives 24/7.
  - Continuous Integration (CI) and Automation Testing: When running automated security tests via ADB over a USB cable, it ensures the screen doesn't turn off, which would otherwise freeze or crash the tests.

  How It Works
  When you toggle this setting in Tactical DPC, the app modifies the global system environment via the STAY_ON_WHILE_PLUGGED_IN settings flag. The X-OS immediately overrides standard user sleep configurations (like a 30-second screen timeout). As long as the device detects incoming current from a wall outlet, a computer, or a wireless charging pad, the display will remain on indefinitely.

  What It Blocks
  - Automatic Screen Dimming: Prevents the device from reducing brightness or turning off the screen after periods of user inactivity.
  - Lock Screen Interruption: It blocks the phone from locking itself while active on a power source.
  - Standard Screen Timeout Policies: It overrides any local user settings configured under Settings > Display > Screen timeout.
- **Allow installs from unknown sources**. Deprecated. Not available on XStealth PRO versions.
- **Set location enabled**. This is a security policy that allows you or IT administrators to programmatically force a device's global location services (GPS) to be turned completely on or off. It is primarily designed to control the global, hardware-level location setting of the physical device. By using "Set location enabled" to force GPS on, and then applying DISALLOW_CONFIG_LOCATION, you or an IT administrator creates an absolute lockdown scenario: the device's location services are permanently turned on, and the user is completely blocked from going into Settings > Location to turn it off. This is crucial for XStealth PRO Tactical, where GPS must never be disabled.

  How It Works
  When you toggle this setting in Tactical DPC, it directly executes the system API DevicePolicyManager.setLocationEnabled(ComponentName, boolean). Unlike normal users, who must manually toggle GPS via the notification shade or settings app, Tactical DPC forces the X-OS to instantly change the device's location state in the background.

What It Blocks and Enforces
- Remote Activation: Command and Control Centers/admins can remotely force location services to turn ON globally, ensuring tracking and geofencing applications can function immediately.
- Remote Deactivation: Command and Control Centers/admins can force location services OFF completely if a device enters a highly secure area where tracking or location mapping is prohibited or affects the mission.
- Overriding User Intent: If you or an administrator forces location services to be enabled, it acts as a baseline state.

- **Set location mode** (deprecated version of set location enabled). This feature is disabled.
   If tapped, the Tactical DPC app will shut down.

Support messages

- **Set short support message**. This security policy allows you or IT administrators to customize the text a user or attacker sees when Tactical restrictions block a device feature or setting.

   Tactical Use Case
  Instead of disclosing to attackers or forensic examiners the real nature of the phone and special features, you can insert a text that will confuse the unauthorized reader. For example, you or an admin might set the short support message to: "Faulty device! System failure, please factory reset the device."

  Key Constraints
  - Character Limit: As the name implies, it is meant to be short (typically a single, concise sentence) so it cleanly fits inside native Android UI dialog boxes without truncation.

  How It Works
  When you type a message into this field in Tactical DPC, it invokes the DevicePolicyManager.setShortSupportMessage() system API. Whenever an attacker attempts to alter a locked setting or perform an action blocked by an administrator, the X-OS blocks the action and displays this customized text string directly within the native system interface.

  What It Blocks (Operational Context)
  This setting does not block device features on its own. Instead, it replaces the generic, default Android error message, which usually says "Action not allowed. Contact your IT administrator"—with a specific, custom string defined by you or your organization.
- **Set long support messages**
  Set long support messages. This security policy allows you or IT administrators to display a detailed, multi-sentence help message or a Tactical policy document directly within the device's native system settings. Admins deploy the long support message to fulfill compliance mandates. It is typically used to display:
  - Detailed Acceptable Use Policies (AUP) for company hardware.
  - Data privacy disclaimers outlining exactly what network traffic the organization can and cannot monitor.

- Comprehensive support instructions, including full helpdesk email addresses, phone numbers, and operational hours.
- Instructions on how to return the device if found.

How It Works
When you enter text into this field in Tactical DPC, it invokes the DevicePolicyManager.setLongSupportMessage() system API. Unlike the Short Support Message (which pops up quickly when a user taps a blocked setting), the Long Support Message acts as a permanent, easily accessible resource page hosted within the main device settings layout.

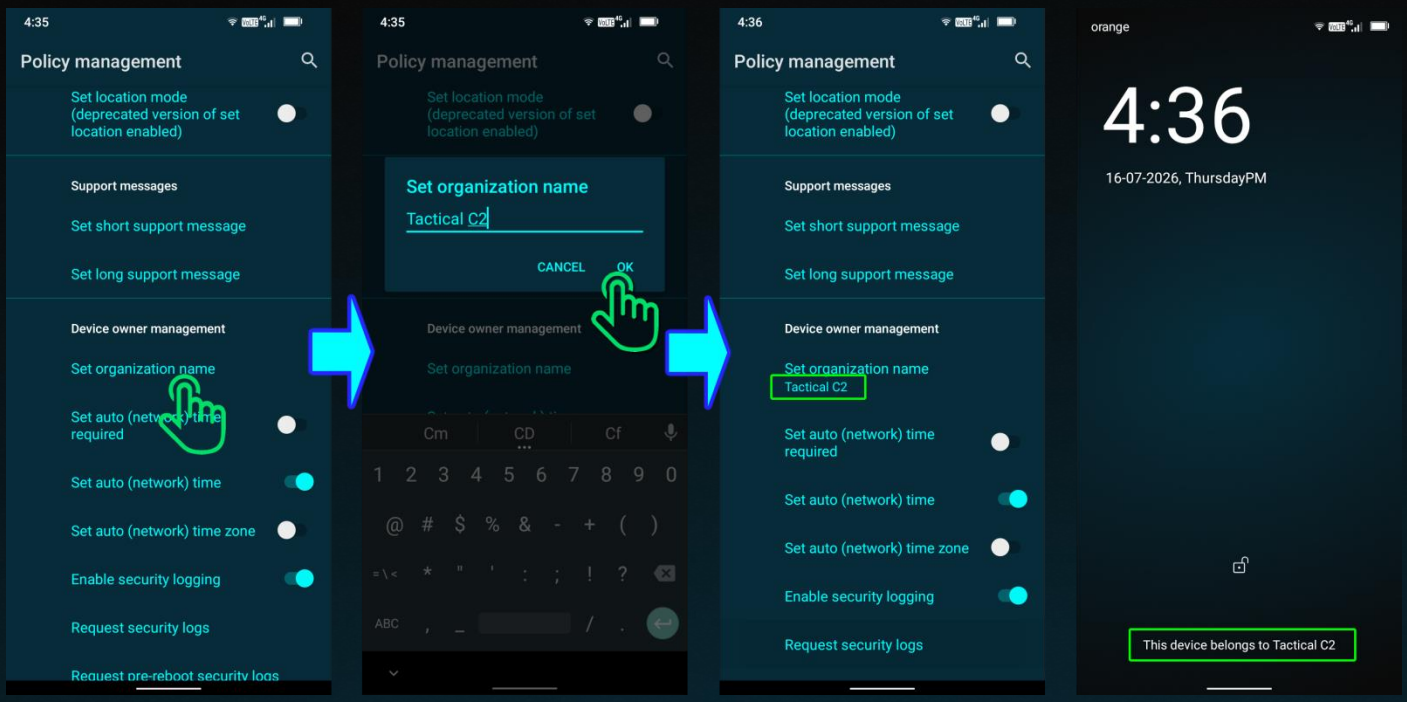
Where It Appears
The X-OS renders this detailed text inside the device's management interface. A user can read it by navigating to:
- Settings > Safety & emergency > Enterprise info.
- Tapping on the active device administrator/DPC icon in the settings menu.

How It Differs from the Short Support Message
The short and long support messages are designed to work together as a two-tier info system:
- Short Support Message: A punchy, single-sentence fragment (e.g., "Contact IT at ext. 4455"). It pops up right next to a grayed-out button to explain an immediate block.
- Long Support Message: A full-length paragraph. It provides comprehensive structural context, links, and operational details about why the device is monitored.

 Tactical Use Case
Instead of disclosing the phone's true nature and special features to attackers or forensic examiners, you can insert a full text (including phone numbers, emails, and links to web pages) that will confuse unauthorized readers and conceal the real mission behind the verifiable information displayed by the phone. For example, you or an admin might set the long support message to a set of information that can be easily verified and confirmed by the covert company or entity invoked in the message.

Device owner management

- **Set organization name**. It allows you to set a custom text that appears on the device's lock screen. You can leave it unchanged if no other tactical requirements impose text changes.



Set organization name

- **Set auto (network) time required**. This security policy requires a Tactical device to use only network-provided data and time.

  What it Does
  - Blocks Manual Overrides: Completely disables the attacker/user's ability to manually change the device's clock, date, or time zone.
  - Removed Date & Time Settings: The toggle for automatic time in the device's system settings (Settings > System > Date & time) becomes unavailable, being completely removed from the device Settings.
  - Prevents Exploits: It stops attackers/users from bypassing time-based restrictions (like app usage limits or security certificates) by rolling back the system clock.
- **Set auto (network time)**. This is an administrative command that instantly forces the device to synchronize its system clock with network-provided time. Unlike "Set auto (network) time required" (which is a permanent, locked restriction policy), this command is a one-time manual trigger that instantly updates the clock.

  What it Does
  - Triggers Immediate Sync: It signals the X-OS to immediately fetch the correct, current time from the cellular network or NTP (Network Time Protocol) servers.
  - Overwrites Manual Clocks: If the device time was previously set manually to a future or past date, this action instantly snaps it back to the true global time.

  How it Works
  - API Call: When you tap this option, Tactical DPC executes the Android Enterprise Device Policy Manager API (DevicePolicyManager.setAutoTimeEnabled).
  - Network Query: The X-OS reaches out to the carrier network or standard internet time servers to pull a highly precise timestamp.
  - Clock Adjustment: The local system clock updates instantly without requiring a device reboot.

- **Set auto (network) time zone**. This is an administrative command that toggles the system's ability to automatically detect and set its time zone based on network data.

  What it Does
  - Toggles Auto Detection: It turns the "Set time zone automatically" switch inside the X-OS system settings (Settings > System > Date & time) strictly ON or OFF.
  - Overwrites Manual Selection: Turning it ON forces the phone to update its geographic zone using cellular tower data or location services, correcting any manually selected incorrect zones.
  - Granular Control: Unlike the strict "required" policies, this feature tests the basic state toggle of the automatic time zone function.
  - Zone Update: When this setting is toggled to On, the device scans neighboring cell towers to look up the exact local timezone offset and updates the UI clock display instantly.
- **Enable security logging**. This is an administrative function used to monitor military/corporate-owned devices for suspicious or malicious activity. It turns on a system-wide audit trail that tracks device events without requiring user consent.

  How It Works
  - API Trigger: Activating this feature in Tctical DPC executes the Android Enterprise framework API DevicePolicyManager.setSecurityLoggingEnabled(..., true).
  - Event Collection: The X-OS begins logging specific critical security events into a secure system buffer. Recorded actions include:
  a. App Behavior: Fresh app launches and installations.
  b. Authentication: Successful or failed device lockscreen attempts.
  c. Developer Exploits: Potentially harmful adb (Android Debug Bridge) commands executed via USB.
  d. System Changes: Media mounts, reboots, and security cryptographic key modifications.
  - Retrieval Callbacks: When a substantial batch of logs accumulates, the system sends an onSecurityLogsAvailable() callback to the Tactical DPC app. The admin can then pull the logs using retrieveSecurityLogs() or look at historical data from before the last reboot via retrievePreRebootSecurityLogs().
  What It Locks (Device Restrictions)
  Enabling security logging forces strict device-wide privacy and security restrictions. It strictly limits or completely locks out the following:
  - Blocks Multi-User Profiles: Security logging is incompatible with standard multi-user setups. If multiple unaffiliated user profiles exist on the device, enabling security logging is blocked. Once enabled, the user cannot add new secondary profiles or guest accounts.
  - Tamper-Resistant Pre-Reboot Logs: Users cannot wipe or clear these specific logs by simply restarting the phone; the X-OS deliberately retains logs across a reboot cycle so malicious actions cannot be covered up by a power cycle.

  Retrieving Security Logs
  X-OS builds security logs in a protected buffer. When the log buffer accumulates enough events (usually a batch of a few thousand entries), the operating system triggers a broadcast (a system notification on the phone screen indicating logs are ready). Tap it to execute retrieveSecurityLogs() and print the text entries to the screen or export them.

- **Request security logs**. This is an explicit UI command that forces the Tactical DPC app to manually query the operating system for any compiled, unread audit logs. While "Enable security logging" turns the log collector on, "Request security logs" is the on-demand action button used to fetch and review the captured events.

  What it Does
  - Triggers Log Retrieval: It invokes the Android Enterprise API DevicePolicyManager.retrieveSecurityLogs() under the hood.
  - Dumps the Buffer: If the X-OS has a filled batch of system logs waiting, this action pulls them from the protected system memory and displays them inside Tactical DPC's UI or outputs them to Logcat.
  - Resets the Batch State: Successfully requesting and viewing these logs clears them out of the immediate unread buffer backlog, so the next batch can pile up.

  The System Limitation Restriction
  Clicking "Request security logs" will not always show new data immediately. X-OS deliberately limits how often a Device Owner can fetch logs to prevent spam and tracking overhead:
  - Returns null if empty: If you tap it before the system has generated its minimum threshold batch of logging events (usually ~2,000 events), the request will return an empty or null payload.

  How to Use It
  Ensure Enable security logging is turned ON first.
  1. Generate events (e.g., plug in a USB debugging cable, try a wrong lock screen PIN a few times).
  2. Open Tactical DPC and locate Request security logs.
  3. Tap it. If the buffer is full, it will display the timestamped system actions. If it is empty, a toast message or blank screen will indicate no logs are ready.
- **Request pre-reboot security logs**. This is an administrative command that retrieves the security audit logs captured during the device's previous power cycle (before its last restart). While normal security logs live in a volatile buffer that usually requires a large batch of events to trigger a download, pre-reboot logs are saved across a single system restart, so admins or security analysts can analyze critical events leading up to a device shutdown.

   XStealth PRO versions have removed this option for security reasons.
- **Request bug report**. This is an administrative command that captures a comprehensive system diagnostic file (a .zip containing logcat dumps, dumpstate information, kernel data, and system metrics) directly from the device. Unlike pulling logs via USB debugging, this command lets IT administrators remotely request technical diagnostics from a field operative's device.

  What it Does
  - Triggers a Global Diagnostic: It signals the X-OS to immediately start bundling system-wide error logs, memory stats, thread dumps, and device info.
  - Displays a Progress Notification: Once clicked, the X-OS takes over and displays a persistent progress bar notification saying "Taking bug report..." while it collects data.
  - Shares Securely: When the file is ready, the system provides a prompt allowing Tactical DPC to view, handle, or export the resulting file via email, cloud storage, or developer utilities.

Important Operational Rules

Throttled Execution: X-OS imposes a strict cooldown period on this API. If you request multiple bug reports in rapid succession, the X-OS will reject the command to prevent device performance degradation and battery drain.

How to Use It

1. Open Tactical DPC.
2. Locate and tap Request bug report.
3. Watch your device's notification tray; you will see a progress bar indicating that the system is capturing diagnostic files.
4. Once completed, tap the notification to review the prompt and choose where to send or save the diagnostic archive.

- **Enable backup service**. This is an administrative control that turns the X-OS data backup and restore framework completely ON or OFF for the entire device.
  By default, when a device is provisioned with a Device Owner (DO), Android automatically disables the backup service to prevent corporate data from leaking into personal cloud storage.
   For security reasons, the Backup feature has been completely removed from XStealth PRO versions.
- **Enable Common Criteria mode**. This is an administrative toggle that configures the device to meet the strict security compliance standards defined by the international Common Criteria for Information Technology Security Evaluation (CC). It is used primarily by governments, defense agencies, and high-security enterprises to ensure a device operates under a vetted, maximum-security posture.

  What it Does

  When you turn on CC mode, the X-OS activates a preset package of hardened security behaviors. The exact modifications:

  - Hardened Cryptography: Forces the device to strictly use cryptographic modules that are certified under FIPS 140 or equivalent CC standards for encryption (e.g., storage encryption, VPNs, and TLS connections).
  - Stricter Password Enforcement: Enhances underlying lock screen security, preventing the bypass of cryptographic keys until full authentication occurs.
  - Enhanced Integrity Checks: Elevates the system's baseline verification of boot sectors, system apps, and memory spaces.
  - Auditing Alignment: Adjusts how system security events are tracked to ensure they capture the exact parameters required by government compliance audits.

  Once active, any cloud-based mobile device management (MDM) server or app can run isCommonCriteriaModeEnabled() to verify the device's government-grade security posture.

  When activated, CC Mode introduces strict restrictions to lock down the operating system:

  - Advanced Encryption: Forces AES-GCM encryption for Bluetooth Long Term Keys and Wi-Fi configurations.
  - Firmware Protections: Blocks manual bootloader download modes and requires high-level RSA signatures for Over-The-Air (FOTA) updates.
  - Data Sanitization: Mandates "zeroization" (immediate, secure wiping) of cryptographic keys when deleted.

⚠ CC Mode cannot be toggled in the standard device settings menu; it must be remotely deployed and managed by your organization's IT administrator via an Enterprise Mobility Management (EMM) or Mobile Device Management (MDM) platform.

- **Enable USB data signaling**. This is a physical-layer hardware security restriction that controls whether a device's USB port can pass data or is strictly limited to charging only, intended to protect Tactical devices from data theft, malware injection via USB ("juice jacking"), or unauthorized access.

  What it Does
  - Blocks/Allows Physical Data Transfer: When disabled, the phone's physical USB data pins are electronically disconnected or ignored by the hardware controller.
  - Turns the Port Charging-Only: If disabled, plugging the phone into a computer or charging station allows it to draw power and charge, but the computer will not even detect that an Android device is attached.
  - Implicitly Disables ADB & Tethering: Turning data signaling OFF instantly breaks USB Debugging (ADB), MTP (File Transfer), USB Tethering, and external peripheral data links. This eliminates advanced hardware attack surfaces. It also implicitly blocks raw Human Interface Device (HID) data streams (like rogue external hardware trackers).

  How to Use It
  Toggle the state:
  - True (Enabled): Standard USB functionality behaves normally (ADB, file transfer, and peripherals function).
  - False (Disabled): The phone switches to charging-only mode immediately. If you are currently connected via ADB to run Test DPC, your connection will drop instantly.

  ⚠ Keep this option enabled if you need the Self Destruct mechanism to work when a USB data cable is plugged into the phone.
- **Remove this device owner**. This is an administrative command that strips the app of its elevated Device Owner (DO) privileges and reverts Tactical DPC back to a normal, unprivileged app. Because a Device Owner has total control over the X-OS system, this command represents a formal resignation of those Tactical/corporate management rights.

  What it Does
  - Relinquishes Admin Control: It immediately terminates the app's ability to enforce Tactical/corporate policies, block settings, or monitor the device.
  - Wipes Active Restrictions: Any policies previously set by Tactical DPC—such as blocked USB data signaling, locked Wi-Fi networks, disabled camera access, or forced automatic time—are instantly deleted and restored to factory defaults.
  - Allows App Deletion: Under normal conditions, X-OS blocks you from uninstalling Tactical DPC app. Running this command restores Tactical DPC to its standard application status, allowing you to uninstall it normally from the home screen or app drawer.

  ⚠ This action is not reversible! Once you remove the DO, there is no chance to restore the app full functionality provided by the DO privileges.
- **Reboot device**. This is an administrative command that forces the Android hardware to execute a clean system restart immediately.

What it Does

- Forces a Soft Restart: It bypasses the standard user-facing power menu (which usually asks you to tap "Restart" or "Power Off") and immediately shuts down all active processes to reboot the operating system.
- Refreshes Device Memory: It cleans out volatile RAM caches and forces system services to reload.
- Applies Pending Updates: It is frequently used to complete the installation of Tactical system updates, security patches, or deep configuration policies that require a clean boot to activate.

- **Set factory reset protection policy**. This is an administrative command that configures Factory Reset Protection (FRP) for Tactical-managed devices. This function is disabled to preserve the phone's overall security.

  ⚠ If tapped, Tactical DPC will shut down for security reasons.
- **Suspend personal apps**. This is an administrative control used on Tactical or COPE (Corporate-Owned, Personally Enabled) devices to temporarily disable all personal applications, leaving only Tactical applications accessible. It allows organizations to instantly lock down the personal side of a device—for example, when a field operative starts a highly secure mission, when a device is reported lost in a mission, or to enforce compliance policies.

  ⚠ Requires an organization-owned profile owner, added by your organization's IT admin.
- **Stealth profile max time off (seconds)**. This is a Tactical compliance policy that sets a countdown timer for how long a field operative may keep their Stealth Profile completely off. If the field operative leaves their Stealth Profile paused or deactivated longer than this limit, the X-OS will automatically punish the device by suspending all personal apps until the Stealth Profile is turned back on.

  ⚠ Requires an organization-owned profile owner added by your organization's IT admin.

Data wipe

- **Remove Stealth profile**. This is an administrative command that completely deletes the managed Tactical container (Stealth Profile) from the device. This command allows an IT administrator to wipe tactical data from a field operative's phone remotely.

  ⚠ Requires a managed profile added by your organization's IT admin.
- **Factory reset device**. This is an administrative action that triggers a complete hardware wipe of the device, erasing all data and restoring it to its original out-of-the-box state. This command also allows remote corporate security wipe, which is what an IT department does when a Tactical/enterprise-managed phone is permanently lost, stolen, seized, or assigned to a new field operative. Contact your organization's IT department for more information regarding remote wipe. You cannot trigger a remote wipe by yourself.

  What it Does

  - Erases the Whole Device: It formats the internal partition, deleting all Stealth/special applications, photos, local files, system settings, and synced accounts.
  - Strips All Management: Because the device is completely wiped, Tactical DPC is entirely removed from the device, ending its Device Owner (DO) status.
  - Triggers External Storage Wipes (Optional): When using this command, Tactical DPC provides advanced parameters to securely wipe physical SD cards or secondary external storage units along

with the internal drive.

Crucial Security Restrictions
- Irreversible: Unlike the "Remove Stealth profile" command (which safely leaves personal data intact), this function provides no recovery paths. Once tapped and confirmed, the hardware wipe cannot be undone.

⚠ This action will erase all user data, folders, apps, and special apps. DO NOT factory reset the device unless you have to!

Transfer ownership

- **Transfer ownership to component**. This is an administrative tool that lets you pass full management rights (Device Owner) from Tactical DPC directly to another application on the device.

  What it Does
  - Hands Over the Reins: It relinquishes Tactical DPC's elevated administrative control over the operating system or Stealth profile, shifting those exact permissions to a target application you specify.
  - Preserves Active System Policies: The X-OS implicitly maintains all existing configurations, rules, and background restrictions across the transfer. The target app inherits them instantly.
  - Passes Custom Migration Bundles: It allows Tactical DPC to package custom data payloads (key-value strings) into a secure transfer bundle. The receiving application can extract this data to instantly verify its setup parameters.
  Strict Security Verification: To prevent malware from hijacking device ownership, the X-OS enforces two rigid cryptographic guardrails:
  - Manifest Tag Requirement: The receiving app must have the <support-transfer-ownership /> flag declared inside its XML device admin metadata.
  - Signature Matching: The app signing certificate of the target component must match expectations to ensure a verified handoff.

  How to Use It
  1. Ensure your target application is installed on the same device and configured to accept ownership transfers.
  2. Open Tactical DPC and locate Transfer ownership to component.
  3. In the input dialog, type the exact Package Name (e.g., com.example.mymdm) and the Receiver Class Name of the target application.
  4. (Optional) Add any test key-value strings to the migration bundle field.
  5. Tap OK. If the target app is compiled correctly, Tactical DPC will instantly lose its Device Owner/Profile Owner badge, and the target app will inherit full management rights.

  ⚠ You cannot transfer ownership to any app installed on your phone! You need a special app that is built to handle elevated privileges. Use this setting only if you know what you are doing!

Cross profile

- **Demonstrate CrossProfileApps API**. This is a testing option used by your organization's IT admin to verify how applications interact at the boundary between a personal profile and a managed Stealth Profile.

Requirements

The secure environment must meet specific parameters:

- Dual-Installation: The Tactical DPC app must be installed on both sides of the device (both in the primary personal user space and inside the managed Stealth Profile).
- Profile Coexistence: A managed Stealth Profile configuration must actively exist on the device.

 You cannot run this test on your own. Contact your organization's IT admin for more info.

- **Allow listed cross profile apps**. Requires a managed profile added by your organization's IT admin.

Nearby streaming policies

- **Nearby notification streaming policy.** This is an administrative command that controls whether notifications from pre-installed apps can be streamed wirelessly from the XStealth PRO tactical to trusted nearby devices. It allows IT administrators to block tactical/corporate data, text messages, or authentication tokens from leaking into nearby linked ecosystems (such as a Chromebook, a smart tablet, or a connected PC cross-device ecosystem).

  What it Does

  - Controls Cross-Device Leakage: It dictates whether notification text and rich data can be broadcast via cross-device system services (if any, like Google's "Cross-Device Services" or "Link to Windows") to external hardware displays.
  - Mitigates Shoulder Surfing: Restricting this ensures that sensitive push alerts (such as corporate 2FA codes, emails, or internal database flags) only appear on the physical screen of the field operative's managed phone.
  - Granular Rule Enforcement: Rather than shutting off local radios entirely, this command isolates and targets the native Notification Streaming pipelines specifically.

  How to Use It

  1. Open the Tactical DPC app.
  2. Locate the Nearby notification streaming policy in the management list.
  3. Tap it to trigger the dialog drop-down menu.
  4. Select your preferred constraint tier (Disabled, Enabled, or Not Set) and apply it.
- **Nearby app streaming policy**. This is a security command that controls whether the device is allowed to project its applications onto external virtual displays. This security feature dictates whether the physical device can stream a live video/interactive feed of its apps to nearby connected systems—such as a Chromebook (via Phone Hub), a smart tablet, or a linked PC.

  What it Does

  - Blocks/Allows Remote App Execution: App streaming allows a user to interact with their phone's apps directly from a secondary laptop or monitor. This policy allows Tactical/enterprise admins to disable that casting capability to completely protect organizational data.
  - Prevents Exfiltration of Managed Apps: If a field operative has proprietary or highly confidential apps running inside their managed space, blocking app streaming ensures that those interfaces cannot be mirrored or interacted with on unmanaged secondary screens.
  - Secures the Virtual Display Layer: It targets X-OS's hardware virtual display system, killing the pipeline before third-party "cross-device" applications can hook into it.

Policy Configuration Tiers

The dialog provides three system settings:

1. 0 (Not Controlled by Policy): The platform default takes over; app streaming remains available if the user configures it.
2. 1 (Disabled): Streaming application interfaces to external nearby hardware are strictly blocked.
3. 2 (Enabled): App streaming is explicitly whitelisted for trusted connections.

How to Use It

1. Open the Tactical DPC.
2. Scroll to find the Nearby app streaming policy in the list of configuration options.
3. Tap it to pull up the parameter dialog.
4. Select your preferred tier (e.g., set to 1 to test an enterprise ban) and tap OK.
5. To verify: Attempt to use a native projection ecosystem (if any, like ChromeOS Phone Hub app streaming) to observe the system block the virtual window from opening.

MTE settings

- **Set MTE policy**. This is a security tool that configures the device's hardware-level Memory Tagging Extension (MTE) policy. MTE is an advanced ARM architecture hardware feature designed to prevent memory corruption vulnerabilities (such as buffer overflows and use-after-free exploits), which account for a large percentage of severe Android security flaws.
  Hardware & Reboot Requirements: This feature requires specific hardware support (such as modern Armv9 processors). Furthermore, the device must be manually rebooted for any changes to the MTE policy actually to compile and take effect.
   Requires API level 34. Not available for XStealth PRO versions.

Credential manager

- **Set credential Provider Allowlist**. Requires API level 34. Not available for XStealth PRO versions.
- **Set credential Provider Allowlist and System**. Requires API level 34. Not available for XStealth PRO versions.
- **Set credential Provider Blocklist**. Requires API level 34. Not available for XStealth PRO versions.
- **Clear policy**. Requires API level 34. Not available for XStealth PRO versions.

SILENT. SECURE. MISSION READY.

X PRO

Tactical

X	XStealth PRO	Tactical
	STATUS: Operational	