SAMSUNG ANDROID OS 7 WITH KNOX 2.x SUPPLEMENTAL PROCEDURES

Version 1, Release 1

13 October 2017

Developed by Samsung and DISA for the DoD

Trademark Information

TABLE OF CONTENTS

Page

LIST OF TABLES

Page

1. SECURITY READINESS REVIEW

1.1 General

When conducting a Samsung Android 7.x Security Readiness Review (SRR), the Team Lead and the assigned Reviewer identify security deficiencies and provide data from which to predict the effectiveness of proposed or implemented security measures associated with the Samsung Android 7.x platform, its associated network infrastructure, and the individual devices that make up the system.

1.2 Mobile Policy Registration

Detailed policy guidance is available on the DISA Information Assurance Support Environment (IASE) website located at http://iase.disa.mil/stigs/mobility/Pages/policies.aspx. Use the Mobility Policy STIG to review the General Wireless Policy asset and the CMD Policy STIG to review the Smartphone Handheld asset.

2. SAMSUNG ANDROID WITH KNOX IMPLEMENTATION CONSIDERATIONS

2.1 Compliance via Third-Party Applications and Components

The Samsung Android with Knox platform provides various application program interfaces (APIs) for third-party solution vendors to configure Knox security components that can be used to implement several MDFPP STIG Template IA controls. This allows for the integration of any third-party applications and components to achieve compliance to the Samsung Android OS 7 with Knox 2.x STIG. The Samsung Android with Knox platform provides the following APIs:

- The Samsung MDM API includes more than 600 policies and 1,500 interfaces that are designed to be called by any MDM agent. Using these policies and interfaces, the MDM solution vendor can implement an MDM solution that can meet or exceed the STIG Template requirements. Examples of MDM vendors that implement the Samsung MDM API include Mobile Iron, AirWatch, BlackBerry, SOTI, MasS360, Centrify, and SAP.
- The Samsung MDM API includes advanced VPN policies and interfaces that allow an MDM admin to configure any third-party IPsec VPN solution that implements the MDM and Knox VPN Framework interfaces. The Samsung device built-in Android VPN client (StrongSwan based) can be configured using the advanced MDM APIs and benefit from the features of the Knox VPN Framework, as well as third-party clients such as Cisco AnyConnect and Pulse Secure.
- The Samsung Universal Credential Management Framework provides an interface that allows any third-party vendor to implement smart card reader functionality for the Samsung Android with Knox device. Solutions implementing this interface enable Samsung Android with Knox to support applications leveraging the DoD Common Access Card (CAC) for PKI-related transactions, including user authentication to DoD networks and websites, S/MIME digital signatures, and, if desired, device unlock. Examples of solutions that implement this interface include the Biometrics Associates Bluetooth Smart Card Reader.

2.2 Logic of STIG Requirements

The logic of some of the STIG configuration settings may differ from one MDM product to another. For example, the policy rule “Disable Manual Date Time Changes” may appear as “Allow Manual Date Time Changes” in some MDM consoles. In this case, the rule should be set to “Disable” instead of “Enable” as indicated in STIG requirement KNOX-07-013100 and the Configuration Table document.

2.3 Configuration of the Personal Space/Container

Section 1.1 of the Overview document states that the scope of this STIG includes the Corporate Owned Personally Enabled (COPE) use case where both a personal space/container and work container are set up on the Samsung Android 7 device. For the COPE use case, this version of the Samsung STIG implements fewer restrictions for data and apps in the personal container than previous versions of the STIG when specific conditions have been met (see next paragraph).

DoD mobile service providers may allow users full access to the Google Play app store for the personal space/container, including downloading and installing Google Play apps and syncing personal data on the device with personal cloud data storage accounts when ALL of the following conditions have been met:

- The site's Authorizing Official (AO) has approved full access to the Google Play app store for the personal space/container, including downloading and installing Google Play apps into the personal container and syncing personal data on the device with personal cloud data storage accounts[1]. Written approval must be available for any system compliance review.
- The site AO has provided guidance on acceptable use and restrictions, if any, on downloading and installing personal apps and data (music, photos, etc.) in the Samsung device personal space/container (guidance can be added to user training or the User Agreement).
- Site mobile devices are configured with a work-only container technology or application that is NIAP certified. Currently Samsung Knox is the only NIAP-certified container technology or application for Samsung mobile devices.
- The site MDM is configured to restrict the download of apps from all third-party app stores.
- Site mobile devices are configured by the MDM or user to restrict the use of DoD VPN profiles within the personal container.
- Site mobile device users receive training on known Google Play application risks and required STIG controls that must be enabled by the user (User Based Enforcement)[2]. See STIG requirement KNOX-07-019000 for more information.

2.4 DoD PKI Purebred

Purebred is a key management server and set of apps for mobile devices and provides a secure, scalable method of distributing software certificates for DoD PKI subscribers' use on commercial mobile devices.

Requirements for Samsung devices credentialed using DoD PKI Purebred are as follows:

- Users are responsible for maintaining positive control of their credentialed devices. The DoD PKI certificate policy requires subscribers to maintain positive control of the devices that contain private keys, and to report any loss of control so that the credentials can be revoked.
- Upon device retirement, turn in, or reassignment, ensure a factory data reset is performed prior to device hand off. Follow Mobility Service Provider decommissioning procedures as applicable.

More information is available at http://iase.disa.mil/pki-pke/Pages/purebred.aspx.

[1] It is recommended that the AO provide guidance on types of apps that should be avoided in the Google app store due to known risky functions or behaviors.
[2] UBE controls cannot be managed by the site MDM server and, therefore, must be managed by the mobile device user. See Section 5 of this document for more information.

3. SAMSUNG KNOX FOR ANDROID DUAL-PERSONA CAPABILITY

3.1 Overview

Samsung Knox for Android supports a dual-persona capability using "container" technology. The container provides a secure and isolated workspace for enterprise applications and data. Enterprise data and applications are placed inside the container. General productivity and morale applications and data reside outside the container. The user of the device has a separate home screen, launcher, and widgets for resources inside and outside of the container. The container supports several security-related features:

- Separate home screen, launcher, applications, and widgets.
- AES 256 encryption of all container data using a FIPS 140-2 validated cryptographic module.
- No interaction between applications and data inside and outside the container.
- Password-based access control mechanism that is independent of the device lock screen.
- Data in transit protection of all container network traffic using a VPN client integrated into the Knox VPN Framework. The Samsung device built-in Android VPN client (StrongSwan based) can be configured as such, which employs the platform's FIPS 140-2 validated cryptographic modules. Third-party clients are also supported.
- Container-only configuration and management policies, including application management, password complexity, CAC configurations for browser and email, and remote wipe of only the container.

MDM software can set security policies for the entire device or target them for the container only. In some deployment scenarios, organizations may implement relaxed security policies outside of the container where users are prohibited from performing DoD mission activities or storing DoD sensitive data outside of the container. While DoD organizations, at their discretion, may permit limited personal activity outside of the container, in all cases the entire device is subject to the terms of the DoD Information Systems User Agreement. Users do not have an expectation of privacy for activity outside the container.

3.2 Container Applications

Most wireless carriers add applications to mobile devices that are in addition to core applications included with the Android operating system. These additional applications are sometimes referred to as "bloatware". Bloatware applications have been found to track mobile device user activities, download usage statistics and other device data to third-party servers, and provide additional revenue opportunities for carriers. Unfortunately, it is very difficult or impossible to remove bloatware applications from Android devices. The Samsung Knox for Android container is used to create a work environment on the Samsung mobile device to separate DoD applications and data from the main device environment where the bloatware applications reside. When Samsung Android devices are used in the DoD, all applications used by the DoD must be installed in the Knox container, and all DoD data must be saved in the Knox container.

In Knox 2.x, applications no longer need to be containerized in order to be installed into the container. Any application from Google Play can be installed without modifications as long as application development follows guidelines specified here:

http://developer.android.com/about/versions/android-4.2.html#MultipleUsers

Several applications are installed by default during container creation and include basic applications needed for work (calendar, contacts, browser, email, file viewer). These default applications cannot be removed by the user.

In Knox 2.x, in addition to MDM application push, the administrator can configure the container to allow the user to install applications from Google Play or select from a list of applications installed outside the container and install them inside the container. By default, these two policies are disabled.

If the enterprise allows users to install applications inside the container, the enterprise can use MDM policies to whitelist container applications as well as to enable and disable container applications.

3.3 Container Isolation

The Knox container provides a completely separated Android environment with its own home screen, launcher, applications, and widgets. Various security mechanisms, such as SE for Android policies, provide isolation of container applications and data from applications and data outside the container, thereby blocking interaction between the two personas.

The Knox container also provides other features to prevent enterprise data leakage.

- Container application access to external storage is blocked by default by SE for Android policies.
- Device screenshot functions are disabled by default when inside the container.
- Full content of notifications (received emails) are not shown in the notification bar when outside the container. In Knox 2.x, MDM policy or user settings can be configured to show full content of notifications.
- Contact and calendar information from outside the container are accessible inside the container. MDM policy or user settings can be configured to show container contacts and calendar events outside the container.
- Container applications are blocked from sharing data with applications outside the container.
- In Knox 2.x, MDM policy can be configured to allow movement of files between the container and outside the container. Each direction can be configured independently. **Note:** The STIG requires movement of files in each direction to be disabled.

3.4 Container Data-at-Rest Encryption

All container data is stored encrypted in a separate file system. Access to the file system is limited to container applications and is enforced by SE for Android policies. Files are encrypted by default using the AES256-CBC cipher, a feature that cannot be turned off. Storage is shared between inside the container and outside the container, so storage for container applications is only limited by the amount of space available on the device.

The Container Data at Rest Encryption mechanism provides two levels of data protection:

- Protected Data – Data marked as "protected" is encrypted when the device is powered off
- Sensitive Data – Data marked as "sensitive" is encrypted when the device is in the Locked state in addition to the powered-off state protection

All container files are stored encrypted and are only decrypted when an application accesses the data. Container data is treated as "protected" data by default. During container creation, the user is required to enter a container password that will be used to control access into the container. This password is used to generate the container key encryption key (FEKEK), which is stored securely in TrustZone. The FEKEK encrypts the per-file data encryption keys (FEK). On a device reboot, the container encrypted file system is auto-mounted (following decryption and mounting of the underlying user data partition) without the need for the user to enter the container password. This allows applications within the container to be launched and operate in the background even if the user has not yet accessed the container. The container encryption mechanism is allowed to retrieve the FEKEK from TrustZone in order to auto-mount the file system. However, the user must still enter the password to access the container.

Files in the container file system can be optionally marked as "sensitive" and are then provided protection even when the container is in the locked state. This provides protection when the device is powered off, and, in addition, sensitive data can only be decrypted when the user has successfully authenticated into the container and the container transitions to the unlocked state. Also, when the container is in the locked state, new sensitive data can be written into new files that can only subsequently be decrypted when the container is unlocked. This allows applications such as email to continue receiving and storing new emails when the container is locked but preventing applications from accessing existing sensitive data until successful authentication by the user. The mechanism ensures that key material associated with decrypting sensitive data is not available in device memory when the container is in the locked state. A key management scheme is implemented that binds decryption of sensitive file FEKs to the container password. A public key cryptography-based mechanism is used to allow new files to be created and encrypted in the locked state but cannot be subsequently decrypted until the container is unlocked.

Sensitive Data Protection (SDP) APIs are provided to allow applications to optionally mark data as Sensitive. Applications then access and manipulate the data using normal Android interfaces (i.e., File I/O methods), with the SDP mechanism transparently handling the encryption. The Container Email application uses these APIs by default to handle email detail as "sensitive". Third-party applications can take advantage of the SDP mechanism via an SDK provided by Samsung. In addition, users can store files in the container's "Chamber" directory, in which all files are automatically marked as "sensitive" by the system.

3.5 Trusted Boot and Warranty Fuse-Based Container Protection

Samsung Knox for Android also implements security mechanisms that protect the container and On Device Encryption (ODE) when an invalid image is detected during the device boot process. This process works by blocking container creation or blocking access to the container if a container has already been created and not releasing the key required to decrypt user data with ODE.

The primary bootloader (in ROM) carries out signature verification of the secondary bootloader using the SHA-256 hash of a public key fused into the hardware at manufacture (hardware root-of-trust). The secondary bootloader image has the public key appended to it, which can be used to verify the signature of the bootloader image. The primary bootloader calculates the hash of the public key and compares it to the hash fused into hardware to verify its integrity before verifying the secondary bootloader's signature. The secondary bootloader also does signature verification of the kernel image. If the kernel image verification fails (indicating an invalid image has been loaded), the Knox Warranty Fuse (a one-time eFuse) is blown. A blown fuse will block container creation and access.

Trusted Boot works by taking cryptographic measurements of the bootloaders and kernel image during device boot and storing these measurements in TrustZone secure memory. A TrustZone secure world application compares these measurements with expected valid measurements. The valid measurements are generated during binary compile time and are signed and stored as a file on the device. A failed measurement check results in container creation and access being blocked. Following the successful boot, the stored measurements are also used for device attestation purposes to ensure that device is booted with known versions of boot chain software.

3.6 Data-in-Transit Protection

The Knox VPN Framework allows VPN client applications (those that are integrated with the framework) to be configured by MDM. VPN profiles for installed clients can be configured to be for full device, for the container, and also for specified applications (per app). The per-app configuration allows an MDM to select applications (inside or outside the container) to connect to the network via a specified VPN profile. When a VPN profile is configured to be for the container, all outbound traffic from applications inside the container is blocked from leaving the device. When connected, traffic from applications inside the container is routed via the VPN. Similarly, when a VPN profile is configured as a per-app, traffic for those specified applications is routed to the network.

The Samsung device built-in Android VPN client (StrongSwan based) is integrated with the Knox VPN Framework (via installation of the Samsung plugin application) and can be configured using the advanced MDM APIs and benefit from the features of the framework. This means that in addition to configuration as a full device application, it can be configured as a per-app or container VPN. The built-in VPN client employs the platform's FIPS 140-2 validated cryptographic modules.

3.7 Container Access Control

The Knox container has a separate authentication mechanism, which is implemented and configured independent of the device lock screen. PIN, password, pattern, or two-step verification using a biometric factor (fingerprint or iris dependent of device support) in addition to a PIN/password, can be used for container authentication. Compliant configurations will use a password for authentication, or optionally two-step verification using fingerprint and password to unlock the container.

When the Knox container is configured with a password and is locked, the user is required to enter the correct password to gain access into the container. The container is locked after a defined idle period of time, on device reboot, or manually by the user from the notification bar. Idle time can be configured by MDM. The lock mechanism cannot be disabled by the user or MDM.

If the user enters the wrong password more than a configured number of consecutive attempts, the container will go into an admin locked state. With Knox 2.x, the MDM can configure the container to wipe in this situation. Only the MDM can reset the container password and unlock the container. The maximum number of failed password attempts can be configured by MDM.

Container password complexity can be configured using MDM policies that are independent of the device lock screen password policies. The policy includes password length, complexity, and expiry.

The MDM can apply specific password policies for the Knox container password. This is independent of the device password policy. The policy includes password length and complexity, disabling or wiping the container following a configurable number of failed login attempts, password expiry time, etc.

On devices running Android 5.x or earlier, when the device encryption is turned on, the user is required to configure a device unlock password. The device unlock password is also used as the device encryption password. However, on Android 6.x a password does not need to be configured when device encryption is turned on, and once turned on there is an option that allows the user to enable encryption password. DoD policy requires CC mode to be enabled, which in turn forces encryption password. Samsung devices launched with Android 6.x or later have encryption enabled by default, and this cannot be disabled. For devices with Android 5.x or later that do not have encryption enabled by default, encryption cannot be disabled once enabled.

When the device is rebooted, the user will be required to enter the following sequence of passwords.

- Encryption password: Only needs to be entered on device reboot. Same as the device unlock password.
- Device unlock password: Needs to be entered to unlock the device (personal environment). Device goes into locked state after defined period of user inactivity. Length and complexity can be controlled by MDM. However, when device encryption is enabled, the password must be at least four characters long (alphanumeric). **Note**: DoD

policy requires the device unlock password to be only four characters when not used to protect sensitive DoD data, but the Samsung Knox for Android platform will force a six-character password when device encryption is enabled.

- Container password: Unlocks the container, which enables access to the container home screen, applications, and data. Length and complexity can be controlled by MDM.

3.8 Container Configuration and Management

The Knox container can be fully managed by MDM using a variety of policies that are independent of the device policies. The MDM agent is installed outside the container; therefore, the administrator has the option to manage both the entire device and the container. All device-level policies in the Samsung Android OS 7 with Knox 2.x STIG are available, as well as the following container policies:

- Container management policies
- Container application management policies
- Container password policies
- Container email and browser policies
- Container VPN policies
- Container restriction policies

3.8.1 Container Management Policies

Samsung Knox for Android includes the following MDM controls for container management:

- Create container: Knox 2.x supports up to two container creations on the device.
- Remove container: Deletes the container and all data and applications inside the container.
- Lock/unlock container: MDM administrator has the ability to lock/unlock the container.

3.8.2 Container Application Management Policies

Users can be allowed to download and install applications into the container from Google Play (Knox 2.x only) or install from applications that are installed outside the container (Knox 2.x only). However, the MDM can further control container applications using the following policies:

- Package Whitelist: MDM can add and remove packages in the whitelist. If configured, only applications in the whitelist can be installed into the container.
- Install/uninstall packages in the container.
- Enable/disable packages: A user is blocked from using disabled applications. Applications that are disabled are no longer accessible by the user (do not appear in the launcher or in the installed list of applications).

- Start/stop applications: MDM can remotely start and stop applications inside the container.

3.8.3 Container Password Policies

Samsung Android includes the following MDM controls to manage container passwords:

- Set max number of failed password attempts after which the container will be disabled.
- Set expiration (specified in days) for container password.
- Set minimum password length.
- Set idle time after which container will be locked.
- Set the number of passwords to be stored as history. The user will not be able to reuse any of these when changing the password.
- Set the minimum number of changed characters when changing the password.
- Set password to be alphanumeric or complex (i.e., requiring characters other than alphanumeric characters).

3.8.4 Container Email and Browser Policies

Samsung Knox for Android includes the following MDM controls to configure the native email and browser applications inside the container:

- Set the browser HTTP proxy.
- Enable/disable browser JavaScript.
- Enable/disable browser cookies.
- Enable/disable Smartcard authentication in the browser: This configures the browser to use CAC. This is the same CAC specified in the Samsung Knox for Android STIG.
- Whitelist/blacklist accounts allowed in email: Accounts can be specified by domain name (e.g., ".@test.com").
- Enable/disable smart card credentials for a specified email account.

Samsung Knox for Android also includes MDM controls to provision Exchange accounts to be used with the native email client. The following parameters can be configured:

- Email address
- User name
- Domain name
- Sync interval
- Server address
- Use SSL/TLS

3.8.5 Container VPN Policies

The Knox VPN Framework provides MDM controls used to select compatible VPN client plug-ins installed on the device, configure VPN profiles, and create various types of configurations such as Per-App VPN, VPN for all container packages, all packages outside the Container (User 0), and device-wide.

3.8.6 Container Restriction Policies

Container restriction policies include various MDM controls such as disabling camera and microphone, moving files to SD card, etc.

3.9 Container Creation

MDM is required to activate a Knox Workspace license prior to creation of the container. Knox licenses are purchased by the enterprise from a Knox reseller and are managed using MDM. Prior to pushing a container-create policy, the MDM needs to push a Knox license to the device. On receiving the Knox license, the MDM agent will trigger the license activation process. An agent running on the device will validate the license with the Samsung Knox License Management (KLM) server. Container creation can only proceed if the Knox license validation succeeds.

3.10 Knox On-Premise Servers

All services necessary to enable Knox services on the device are hosted on the cloud. However, the Samsung Knox On-Premise server is also available for enterprises wanting to deploy and manage Knox services on premise. DoD implementations are expected to install, configure, and manage the Knox On-Premise servers on enterprise managed servers. Samsung provides the On-Premise server install packages, which are available for both Windows and Linux.

The Knox On-Premise server includes the following components:

- Knox License Management (KLM): The license management and compliance system for Samsung Knox. KLM is used to activate Knox services on supported devices.
- Global Server Load Balancing (GSLB): A dictionary server for the various services (e.g., KLM server). The URL for the GSLB server is coded into the enterprise-provided Knox license. During activation, the GSLB server will return the endpoints (URL) for the various services to the device agents.

An enterprise that decides to deploy the Knox On-Premise server will request the appropriate Knox license from the Knox reseller. The enterprise will provide its On-Premise GSLB server URL, which will be encoded into the Knox license.

The MDM agent will pass the Knox license to a KLM agent running off the device. This agent will connect to the GSLB server, which will return the KLM server URL. The agent then connects to the KLM server to get Knox license validation.

4. SAMSUNG KNOX FOR ANDROID IA FEATURES

The Samsung Knox for Android platform builds on top of the Android platform to provide strong guarantees for the protection of enterprise data by building a hardware-rooted trusted environment. This was accomplished by adding security features across the full software stack, from the bootloaders, kernel, TrustZone, and Android framework.

Key IA features found in Samsung Knox for Android that are not present in typical Android devices are:

- Mobile application quarantine
- Container support
- Smart card support
- Host-based firewall
- Ability to revoke mobile application permissions
- Over-the-air (OTA) audit log retrieval
- Support for PKI authentication and certificate verification in native browser
- Sensitive data protection
- Device attestation

4.1 Samsung Android Device Disposal

For Samsung Android devices never exposed to classified data, follow this procedure prior to disposing of (or transferring to another user) a mobile device via site property disposal procedures.

Note: Follow the device manufacturer's instructions for wiping all user data and installed applications from the device memory.

4.2 Samsung Device Encryption Guideline

The Samsung on Device Encryption mechanism (ODE) provides encryption of the device's user data partition, in which all user and application data is stored. External SD card storage can also optionally be encrypted.

The ODE Key Management mechanism incorporates a TrustZone-based component for protection of keys, in which recovery of the Data Encryption Key (DEK) is bound to both the user's password and the hardware-based device unique Root Encryption Key (REK). Both Key Management and Data Encryption implementations employ the platform's FIPS 140-2 validated cryptographic modules, including hardware cryptographic modules on devices that support them. Data is encrypted using AES-256-XTS for internal storage and AES-256-CBC for external SD card storage.

On devices with Android 6.x or later, a password does not need to be configured for ODE (a default password is used instead); however, there is an option to enable an encryption password

(same as the Lock Screen password). Use of an encryption password is enforced by the device's CC mode, which DoD policy requires to be enabled.

For devices that do not have encryption enabled by default, when device encryption is enabled for the first time, the user is given the option of doing a fast encryption. Users should be guided to enable fast encryption before starting the initial encryption process. The differences between a full encryption (fast encryption disabled) and fast encryption are:

- Full encryption encrypts the entire disk, including slack.
- Fast encryption encrypts only the files on the device but not slack, so the initial encryption time can be considerably less than full encryption.

Future files are encrypted regardless of the full or fast encryption.

5. SAMSUNG KNOX FOR ANDROID USER-BASED ENFORCEMENT

There are various features available on the device that, when enabled by the user, could result in unauthorized persons gaining access to sensitive information on the device. For features that cannot be disabled by MDM, the mitigation must include proper training of individual users.

5.1 Calendar Alarm

The default Samsung pre-installed Calendar application allows users to create events that include event title, location, date and time, and also notification alarms for the event. When the alarm is configured, at the specified time the event details will be shown on the device screen, even when the device is in a locked state. Users should be trained to not configure this option or to not include any sensitive information in the event title and location.

5.2 Content Transferring and Screen Mirroring

Samsung devices include various ways that allow the user to transfer files on their device to other devices and to display content from their device on select Samsung Smart TVs.

The “Quick Connect” and “Samsung Connect” features (device model dependent) are accessed from the notification bar and display a list of scanned devices that the user’s device can connect to. The user can select a device from this list to transfer selected files to (either via Wi-Fi Direct or Bluetooth) or to do screen mirroring. Depending on the selected device’s capabilities, either Miracast or DLNA technology will be used to provide screen mirroring. Both Miracast and DLNA will work over a Wi-Fi Direct connection or with devices connected to the same Wi-Fi access point. Whereas Miracast renders whatever is on the device screen to the target device, DLNA requires the playback on the target device.

Screen mirroring can also be initiated by selecting the file and then selecting “Share” and “Smart View” or by enabling “Smart View” in the Quick Settings panel.

The user can enable “MirrorLink” to allow integration of the device with car infotainment systems, connected over USB. This provides the user with the ability to access and control applications on the device via the car’s infotainment system. This is enabled by selecting “Connections”, “More Connections”, and “MirrorLink” in the Settings application.

The “Phone Visibility” option allows a user to make the device visible to other devices via wireless interfaces such as Bluetooth or Wi-Fi Direct, meaning other devices can attempt to initiate data transfers.

Users should be trained to not enable these options unless they are authorized to do so and they visually verify the recipient device. Users should be trained to not enable these options unless using an approved DoD screen mirroring technology with FIPS 140-2 validated Wi-Fi. Miracast must only be used with TVs, monitors, and Miracast dongles with FIPS 140-2 validated Wi-Fi clients.

Note that the administrator can also restrict the underlying connection method (Bluetooth, Wi-Fi Direct, etc.) via MDM controls, or the administrator can explicitly disable the application package that implements the service.

5.3 Content Sharing

Select Samsung devices include the “Nearby devices” feature, which allows the user to share files on their device with other devices over a Wi-Fi connection. This allows other devices to connect to the user’s device and download selected files (videos, photos, music) to that device. This is disabled by default but can be enabled by the user from the following setting:

Device settings >> More connection settings >> Nearby device scanning

The user can also transfer files by selecting the file and then selecting “Share” and “Transfer files to device”, which initiates a scan for nearby devices, or by explicitly selecting the transfer method in the same dialog (e.g., Bluetooth, Wi-Fi Direct, etc.).

Users should be trained to not enable these options unless they are authorized to do so and they visually verify the recipient device.

Note that the administrator can also restrict the underlying connection method (Bluetooth, Wi-Fi Direct, etc.) via MDM controls, or the administrator can explicitly disable the application package that implements the service. See STIG requirement KNOX-07-019100.

5.4 Report diagnostic information

Samsung devices include the “Report diagnostic info” feature, which allows the device to collect diagnostic and usage data and automatically transmit this data to Samsung servers. The purpose is to allow Samsung to analyze the data to improve product and service quality and address unexpected shutdowns or system errors.

Settings >> General Management >> Report Diagnostic Info

Users should be trained to not enable this option. See STIG requirement KNOX-07-005900.

5.5 Certificate Removal

DoD PKI certificates may be installed on the device by the administrator both directly and via MDM.

Installed certificates can be deleted manually by the user, via the Settings application (Lock Screen and Security >> Other Security Settings >> User Certificates).

Users should be trained to not remove DoD root and intermediate PKI certificates. See STIG requirement KNOX-07-012300.

5.6 Samsung DeX Station

The Samsung DeX Station provides a desktop experience for select Samsung devices that have the capability to include the DeX mode. The dock provides the capability to connect the Samsung device to an external monitor, keyboard, mouse, and Ethernet cable.

Users should be trained to not connect the DeX Station to a DoD network via an Ethernet cable. See STIG requirement KNOX-07-017000.

5.7 Phone Visibility

The Phone Visibility feature allows other devices to find the user's phone and transfer files. The user's phone will appear in the list of available devices when files are transferred via Transfer files to devices.

Users should be trained to disable Phone Visibility. See STIG requirement KNOX-07-017200.

5.8 Smart Call

The Smart Call feature provides Caller ID and spam protection but requires the DoD user's name and phone number to be uploaded into an online service.

Users should be trained to disable Smart Call. See STIG requirement KNOX-07-018000.

5.9 Samsung WiFi Sharing

WiFi Sharing is a new option included in the Samsung tethering feature. It allows a Samsung device user to share their Wi-Fi connection with other Wi-Fi-enabled devices but could allow unauthorized devices to access a DoD network.

Users should be trained to disable Samsung WiFi Sharing. See STIG requirement KNOX-07-019200.

5.10 VPN Profiles

The cybersecurity risk of a DoD network could be elevated when a Samsung mobile device with an unmanaged personal space/container connects to a DoD network via a VPN client in the device personal space/container.

Users should be trained to not configure a DoD network (work) VPN profile in any third-party VPN client installed in the personal space/container on a Samsung device. See STIG requirement KNOX-07-017130.

6. SAMSUNG KNOX FOR ANDROID APPLICATION DISABLE POLICIES

The Samsung Knox for Android supports application disable policies that allow administrators to disable core and preinstalled applications[3] by specifying package names. As each device and operator variant will be pre-installed with different sets of applications, the administrator must identify any application that could pose a threat to sensitive information on the device and disable such applications by configuring application disable policies.

6.1 Public Cloud Backup Applications

Android allows users to back up and sync application data, user files, and settings to Google servers or other third-party cloud services, such as Samsung accounts and Dropbox. Samsung Knox for Android supports policy to disable Google backup, but other third-party services are disabled using application disable policies. The administrator must identify any such service pre-installed on the Knox container and disable these applications unless use is approved by the AO. This list includes:

- Samsung account (including Samsung Cloud)
- Dropbox
- Drive (Google)
- OneDrive (Microsoft)

6.2 Content Sharing Applications

Samsung devices include various methods that allow a device to share content with or send content to other devices nearby. The administrator must identify any such service pre-installed on the device in the Knox container and disable these applications unless use is approved by the AO. This list includes:

- Group Play
- Samsung Connect (Quick Connect)

6.3 Mobile Printing

Mobile printing applications provide the capability for wireless printing from a Samsung Android device. Setting up wireless printing from a mobile device to a DoD network connected printer is problematic due to the print server requirements listed in the MultiFunction Device STIG and the DoD Wi-Fi network requirements listed in the Network Infrastructure STIG. If a mobile device is directly connected to a DoD network via a VPN or Wi-Fi connection, it may be able to print to network printers if the printer drivers or a printer app is installed.

[3] A core app is defined as an app bundled by the operating system vendor (e.g., Google). A preinstalled app is included on the device by a third-party integrator, including the device manufacturer or cellular service provider (e.g., Samsung, Verizon Wireless, or AT&T).

6.4 Core and Preinstalled Applications

6.4.1 Introduction

The core and preinstalled application lists below may not reflect the exact list on any specific device that is being reviewed. Small modifications to app names or app package names can be expected between various carriers' OS builds. Also, additional apps not on the lists may be included in an OS build, or the OS build may not include all apps on a list. The app lists below should be compared to the list of apps installed on a device being reviewed.

6.4.2 Disabled Core and Preinstalled Applications

Tables 6-1, 6-2, and 6-3 list core and preinstalled applications that should be disabled unless there is a mission need for their use. DoD Commands and Agencies should fully vet these apps, using the Application Software Protection Profile (APPSWPP) prior to approving their use.

Table 6-1: Disabled Applications – Personal Area

Application Package Name	Application Name
com.amazon.mShop.android	Amazon
com.amazon.fv	Amazon App Suite
com.amazon.mShop.android.install	Amazon Installation Status
com.amazon.mShop.android.shopping	Amazon Shopping
com.android.egg	Android Easter Egg
com.google.android.apps.walletnfcrel	Android Pay
com.dti.att	AT&T App Select
com.att.callprotect	AT&T Call Protect
com.wavemarket.waplauncher	AT&T FamilyMap
com.att.android.digitallocker	AT&T Locker
com.yahoo.mobile.client.android.mail.att	AT&T Mail
com.asurion.android.mobilerecovery.att	AT&T Protect Plus
net.aetherpal.device	AT&T Remote Support[4]
com.samsung.android.widgetapp.briefing	Briefing Feed
com.cequint.ecid	Caller Name ID
com.vcast.mediamanager	Cloud
com.samsung.android.slinkcloud	CloudGateway
com.cnn.mobile.android.phone.edgepanel	CNN for Edge Panel
com.tmobile.pr.adapt	com.tmobile.pr.adapt
com.smithmicro.netwise.director.cricket	Cricket Wi-Fi Manager
com.aetherpal.attdh.se	Device Help
com.metro.simlock	Device Unlock
com.tmobile.simlock	Device Unlock
com.directv.dvrscheduler	DIRECTV

[4] Transmits diagnostic information (see Knox-07-001700)

Application Package Name	Application Name
com.att.dtv.shaderemote	DIRECTV Remote
com.google.android.apps.docs	Drive
com.LogiaGroup.LogiaDeck	DT Ignite
com.facebook.katana	Facebook
com.facebook.system	Facebook App Installer
com.facebook.appmanager	Facebook App Manager
com.facebook.services	Facebook Services
com.samsung.android.widgetapp.yahooedge.finance	Finance
com.sec.android.app.samsungapps	Galaxy Apps
com.sec.android.widgetapp.samsungapps	Galaxy Essentials Widget
com.samsung.android.game.gamehome	Game Launcher
com.samsung.android.game.gametools	Game Tools
com.ampsvc.android	Games Assistant
com.samsung.android.hmt.vrsvc	Gear VR Service
com.samsung.android.app.vrsetupwizardstub	Gear VR SetupWizardStub
com.samsung.android.hmt.vrshell	Gear VR Shell
com.google.android.gm	Gmail
com.google.android.apps.books	Google Play Books
com.google.android.play.games	Google Play Games
com.google.android.videos	Google Play Movies
com.google.android.music	Google Play Music
com.google.android.apps.magazines	Google Play Newsstand
com.android.vending	Google Play Store
com.google.android.apps.plus	Google+
com.hancom.office.editor.hidden	Hancom Office Editor
com.google.android.talk	Hangouts
com.samsung.helphub	Help
com.imdb.mobile	IMDb
com.instagram.android	Instagram
com.verizon.llkagent	LLKAgent
com.lookout	Lookout
com.google.android.feedback	Market Feedback Agent
com.verizon.messaging.vzmsgs	Message+
com.facebook.orca	Messenger
com.handmark.metro.launcher	Metro App Store
com.metropcs.metrozone	metroZONE
com.samsung.android.app.mhswrapperusc	Mobile Hotspot
com.dti.cricket	Mobile Services
com.vzw.hss.widgets.infozone	My InfoZone
com.vzw.hss.myverizon	My Verizon
com.verizon.mips.services	My Verizon Services
com.att.myWireless	myAT&T

Application Package Name	Application Name
com.mizmowireless.acctmgt	myCricket
com.nuance.nmc.sihome.metropcs	myMetro
com.privacystar.android.metro	name iD
com.samsung.android.widgetapp.yahooedge.news	News
com.gotv.nflgamecenter.us.lite	NFL Mobile
com.verizon.v4b	One Talk
com.microsoft.office.onenote	OneNote
com.samsung.android.service.peoplestripe	PeopleStripe
com.americanexpress.plenti	Plenti
com.directv.promo.shade	Remote
com.samsung.android.controltv	Remote Control
com.osp.app.signin	Samsung Account
com.sec.android.app.sns3	Samsung Galaxy
com.samsung.android.mateagent	Samsung Galaxy Friends
com.samsung.android.spay	Samsung Pay
com.sec.app.samsungprintservice	Samsung Print Service Plugin
com.samsung.android.themestore	Samsung Themes
com.synchronoss.dcs.att.r2g	Setup & Transfer
com.slacker.radio	Slacker Radio
com.locationlabs.cni.att	Smart Limits
com.samsung.android.widgetapp.yahooedge.sport	Sports
com.samsung.sprint.chameleon	Sprint Chameleon
com.asurion.android.verizon.vms	Support & Protection
com.tmobile.pr.mytmobile	T-Mobile
com.tmobile.services.nameid	T-Mobile Name ID
com.ubercab	Uber
com.telecomsys.directedsms.android.SCG	Verizon Location Agent
com.motricity.verizon.ssodownloadable	Verizon Login
com.customermobile.preload.vzw	Verizon Store Demo Mode
com.samsung.android.visioncloudagent	VisionCloudAgent
com.samsung.tmovvm	Visual Voicemail
com.samsung.vzwapiservice	VzwApiService
com.whatsapp	WhatsApp
com.samsung.android.app.withtv	withTV
com.samsung.android.widgetapp.yahooedge	Yahoo! Edge
com.google.android.youtube	YouTube
com.yellowpages.android.ypmobile	YP
***Note**: The following applications are not included in Android 7 firmware. However, devices with 5.x firmware will retain these installed applications on upgrading to 7.0 firmware, and therefore, these must be kept on the disabled application list.*	
com.amazon.venezia	Appstore
com.beatsmusic.android.client	Beats Music

Application Package Name	Application Name
com.intsig.camdict	CamDictionary
com.sec.chaton	ChatON
com.att.digitallife.android.phone22	Digital Life
com.dropbox.android	Dropbox
com.microsoft.office.excel	Excel
com.verizon.familybase.companion	FamilyBase Companion
com.hp.android.printservice	HP Print Service Plugin
com.isis.mclient.verizon.activity	Isis Wallet
com.callpod.android_apps.keeper	Keeper
com.facebook.orca	Messenger
com.samsung.milk.milkvideo	Milk Video
com.microsoft.skydrive	OneDrive
com.microsoft.office.powerpoint	PowerPoint
com.skype.raider	Skype
com.isis.mclient.atnt.activity	Wallet
com.microsoft.office.word	Word

Table 6-2: Disabled Applications – Container

Application Package Name	Application Name
com.sec.android.app.samsungapps	Galaxy Apps
com.hancom.office.editor.hidden	Hancom Office Editor
com.osp.app.signin	Samsung Account
com.samsung.android.themestore	Samsung Themes

Table 6-3: Disabled Applications – Samsung System Services

Application Package Name	Application Name
com.samsung.android.bio.face.service	Face
com.samsung.android.app.simplesharing	Link Sharing
com.samsung.android.nearby.mediaserver	Nearby Devices
com.samsung.android.allshare.service.mediashare	Nearby Service
com.samsung.android.oneconnect	Quick Connect
com.samsung.android.scloud	Samsung Cloud
com.samsung.android.easysetup	Samsung Connect
com.samsung.android.app.mirrorlink	Samsung MirrorLink 1.1
com.sec.android.easyMover	Smart Switch
com.sec.android.easyMover.Agent	Smart Switch
com.samsung.android.smartmirroring	Smart View
com.samsung.android.app.talkback	Voice Assistant

6.5 Auditing/Reviewing Device Applications

Applications are controlled by three APIs: application whitelist, application blacklist, and application disable. The application whitelist and blacklist are used to control installing applications. All applications are added to the blacklist using the ".*" wildcard so that only applications listed on the whitelist can be installed. Approved core and preinstalled applications are added to the whitelist so that updates can be installed. Application disable is used to disable undesirable/unapproved core and preinstalled applications. Core and preinstalled applications listed on the "disable" list are not removed from the device but cannot be seen and/or launched by the user. There are two sets of these controls, one for applications in the personal area of the device and one for applications in the container.

7. ADDITIONAL SAMSUNG FEATURES

7.1 Samsung Wearables

The use of Samsung Wearables is based on the approval of the AO. As the Samsung Wearables do not have access to the Knox container, no further configuration is required.

7.2 Biometric Authentication

Selected Samsung Android 7 devices incorporate fingerprint, facial, and iris biometric authentication mechanisms that can be configured to allow users to authenticate to unlock the device and also the Knox Workspace Container (as part of two-step authentication). Fingerprint authentication is the only DoD-approved biometric authentication mechanism because both facial and iris biometric authentication have not been certificated by NIAP as compliant with the Protection Profile for Mobile Device Fundamentals (MDF).

The user must first register a fingerprint with the system. In order to use fingerprint for device authentication, the user must also create a password, which is used as the authentication factor at first boot prior to first use of fingerprint authentication.

The fingerprint authentication mechanism is implemented in TrustZone. Only the TrustZone component can access data from the fingerprint sensor, with biometric templates being securely stored in TrustZone and not accessible by software in the normal world. Verification of captured fingerprint images against stored templates is carried out within TrustZone, with no fingerprint data being exposed to the normal world.

Use of biometrics for device and Knox Workspace authentication can be disabled by the administrator via MDM controls.