CIS Samsung Android OS 15 with Knox 3.x COPE STIG Benchmark

v1.0.0 - 09-12-2025

Terms of Use

Please see the below link for our current terms of use:

https://www.cisecurity.org/cis-securesuite/cis-securesuite-membership-terms-of-use/

For information on referencing and/or citing CIS Benchmarks in 3rd party documentation (including using portions of Benchmark Recommendations) please contact CIS Legal (legalnotices@cisecurity.org) and request guidance on copyright usage.

NOTE: It is ***NEVER*** acceptable to host a CIS Benchmark in ***ANY*** format (PDF, etc.) on a 3rd party (non-CIS owned) site.

Table of Contents

Target Technology Details

Samsung Android OS 15 with Knox 3.x COPE Secure Technical Implementation Guide (STIG)

Version: 1 Release: 1 Benchmark

Date: 30 Jan 2025

Intended Audience

This benchmark is intended for system and application administrators, security specialists, auditors, help desk, and platform deployment personnel who plan to develop, deploy, assess, or secure solutions that incorporate Samsung Android OS 15 with Knox 3.x COPE and are looking to comply with the STIG guidance

Recommendation Definitions

The following defines the various components included in a CIS recommendation as applicable. If any of the components are not applicable it will be noted, or the component will not be included in the recommendation.

Title

Concise description for the recommendation's intended configuration.

Assessment Status

An assessment status is included for every recommendation. The assessment status indicates whether the given recommendation can be automated or requires manual steps to implement. Both statuses are equally important and are determined and supported as defined below:

Automated

Represents recommendations for which assessment of a technical control can be fully automated and validated to a pass/fail state. Recommendations will include the necessary information to implement automation.

Manual

Represents recommendations for which assessment of a technical control cannot be fully automated and requires all or some manual steps to validate that the configured state is set as expected. The expected state can vary depending on the environment.

Profile

A collection of recommendations for securing a technology or a supporting platform. Most benchmarks include at least a Level 1 and Level 2 Profile. Level 2 extends Level 1 recommendations and is not a standalone profile. The Profile Definitions section in the benchmark provides the definitions as they pertain to the recommendations included for the technology.

Description

The Rule Title from the STIG.

Rationale Statement

Detailed reasoning for the recommendation to provide the user a clear and concise understanding on the importance of the recommendation.

Audit Procedure

Systematic instructions for determining if the target system complies with the recommendation.

Remediation Procedure

Systematic instructions for applying recommendations to the target system to bring it into compliance according to the recommendation.

Additional Information

References from the STIG Rule if applicable.

Profile Definitions

The following configuration profiles are defined by this Benchmark:

- **SEVERITY: CAT I**

  Items in this profile exhibit one or more of the following characteristics:

  - are considered to be high severity
  - are intended for environments or use cases where following STIG based security guidance is paramount.
  - acts as defense in depth measure.
  - may negatively inhibit the utility or performance of the technology.

  This profile is intended for servers and workstations.

- **SEVERITY: CAT II**

  Items in this profile exhibit one or more of the following characteristics:

  - are considered to be medium severity
  - are intended for environments or use cases where following STIG based security guidance is paramount.
  - acts as defense in depth measure.
  - may negatively inhibit the utility or performance of the technology.

  This profile is intended for servers and workstations.

- **SEVERITY: CAT III**

  Items in this profile exhibit one or more of the following characteristics:

  - are considered to be low severity
  - are intended for environments or use cases where following STIG based security guidance is paramount.
  - acts as defense in depth measure.
  - may negatively inhibit the utility or performance of the technology.

  This profile is intended for servers and workstations.

Acknowledgements

This Benchmark exemplifies the great things a community of users, vendors, and subject matter experts can accomplish through consensus collaboration. The CIS community thanks the entire consensus team with special recognition to the following individuals who contributed greatly to the creation of this guide:

The Recommendations in this Benchmark are a representation of the Rules in the unclassified DISA STIG for Samsung Android OS 15 with Knox 3.x COPE

Contributor

Tim Harrison CISSP, ICP, KMP, Center for Internet Security, New York

Recommendations

1 STIG RULES

Google Android 15

Samsung Android OS 15 with Knox 3.x COPE Secure Technical Implementation Guide (STIG)

Version: 1 Release: 1 Benchmark

Date: 30 Jan 2025

CLASSIFICATION unclassified

1.1 KNOX-15-000700 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

Samsung Android must not accept the certificate when it cannot establish a connection to determine the validity of a certificate.

```
GROUP ID: V-268981
RULE ID: SV-268981r1036039
```

Rationale:

Certificate-based security controls depend on the ability of the system to verify the validity of a certificate. If the MOS were to accept an invalid certificate, it could take unauthorized actions, resulting in unanticipated outcomes. At the same time, if the MOS were to disable functionality when it could not determine the validity of the certificate, this could result in a denial of service. Therefore, the ability to provide exceptions is appropriate to balance the tradeoff between security and functionality. Always accepting certificates when they cannot be determined to be valid is the most extreme exception policy and is not appropriate in the DOD context. Involving an Administrator or user in the exception decision mitigates this risk to some degree.

```
SFRID: FIA_X509_EXT.2.2
```

Audit:

Verify requirement KNOX-15-009300 (Common Criteria mode) has been implemented.

If "Common Criteria mode" has not been implemented, this is a finding.

Remediation:

Implement "Common Criteria mode". Refer to requirement KNOX-15-009300.

Additional Information:

CCI-000185

For public key-based authentication, validate certificates by constructing and verifying a certification path to an accepted trust anchor including checking certificate status information.

- NIST SP 800-53::IA-5 (2)
- NIST SP 800-53A::IA-5 (2).1
- NIST SP 800-53 Revision 4::IA-5 (2) (a)
- NIST SP 800-53 Revision 5::IA-5 (2) (b) (1)

1.2 KNOX-15-004900 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Samsung Android must be configured to enforce a minimum password length of six characters.

```
GROUP ID: V-269023
RULE ID: SV-269023r1036165
```

Rationale:

Password strength is a measure of the effectiveness of a password in resisting guessing and brute force attacks. The ability to crack a password is a function of how many attempts an adversary is permitted, how quickly an adversary can complete each attempt, and the size of the password space. The longer the minimum length of the password is, the larger the password space. Having a too-short minimum password length significantly reduces password strength, increasing the chance of password compromise and resulting device and data compromise.

```
SFRID: FMT_SMF.1.1 #1
```

Audit:

Review the configuration to determine if the Samsung Android devices are enforcing a minimum password length of six characters.

This validation procedure is performed on both the management tool and the Samsung Android device.

On the management tool, in the device password policies, verify "minimum password length" is set to `6`.

On the Samsung Android device:

1. Open Settings >> Lock screen >> Screen lock type.
2. Enter current password.
3. Tap "PIN".
4. Verify the text "PIN must contain at least", followed by a value of at least `6 digits`, appears above the PIN entry.

If on the management tool "minimum password length" is not set to `6`, or on the Samsung Android device the text "PIN must contain at least" is followed by a value of less than `6 digits`, this is a finding.

Remediation:

Configure the Samsung Android devices to enforce a minimum password length of six characters.

On the management tool, in the device password policies, set "minimum password length" to 6.

Additional Information:

CCI-004066

For password-based authentication, enforce organization-defined composition and complexity rules.

- NIST SP 800-53 Revision 5::IA-5 (1) (h)

1.3 KNOX-15-005000 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Samsung Android must be configured to not allow passwords that include more than four repeating or sequential characters.

```
GROUP ID: V-269024
RULE ID: SV-269024r1036168
```

Rationale:

Password strength is a measure of the effectiveness of a password in resisting guessing and brute force attacks. Passwords that contain repeating or sequential characters are significantly easier to guess than those that do not. Therefore, disallowing repeating or sequential characters increases password strength and decreases risk.

```
SFRID: FMT_SMF.1.1 #1
```

Audit:

Review the configuration to determine if the Samsung Android devices are disallowing passwords containing more than four repeating or sequential characters.

This validation procedure is performed on both the management tool and the Samsung Android device.

On the management tool, in the device password policies, verify "minimum password quality" is set to "Numeric(Complex)" or better.

On the Samsung Android device:

1. Open Settings >> Lock screen >> Screen lock type.
2. Enter current password.
3. Tap "PIN".
4. Verify PINs with more than four repeating or sequential numbers are not accepted.

If on the management tool "minimum password quality" is not set to "Numeric(Complex)" or better, or on the Samsung Android device a password with more than four repeating or sequential numbers is accepted, this is a finding.

Remediation:

Configure the Samsung Android devices to disallow passwords containing more than four repeating or sequential characters.

On the management tool, in the device password policies, set "minimum password quality" to "Numeric(Complex)" or better.

If the management tool does not support "Numeric(Complex)" but does support "Numeric", Knox Platform for Enterprise (KPE) can be used to achieve STIG compliance. In this case, configure this policy with value "Numeric" and use an additional KPE policy (innately by the management tool or via KSP) "Maximum Numeric Sequence Length" with value 4.

Additional Information:

CCI-004066

For password-based authentication, enforce organization-defined composition and complexity rules.

- NIST SP 800-53 Revision 5::IA-5 (1) (h)

1.4 KNOX-15-005100 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Samsung Android must be configured to lock the display after 15 minutes (or less) of inactivity.

```
GROUP ID: V-269025
RULE ID: SV-269025r1036171
```

Rationale:

The screen lock timeout must be set to a value that helps protect the device from unauthorized access. Having a too-long timeout would increase the window of opportunity for adversaries who gain physical access to the mobile device through loss, theft, etc. Such devices are much more likely to be in an unlocked state when acquired by an adversary, thus granting immediate access to the data on the mobile device. The maximum timeout period of 15 minutes has been selected to balance functionality and security; shorter timeout periods may be appropriate depending on the risks posed to the mobile device.

```
SFRID: FMT_SMF.1.1 #2
```

Audit:

Review the configuration to determine if the Samsung Android devices are locking the device display after 15 minutes (or less) of inactivity.

This validation procedure is performed on both the management tool and the Samsung Android device.

On the management tool, in the device password policies, verify "max time to screen lock" is set to "15 minutes" or less.

On the Samsung Android device:

1. Open Settings >> Lock screen.
2. Verify "Secure lock settings" is present and tap it.
3. Enter current password.
4. Tap "Auto lock when screen turns off".
5. Verify the listed timeout values are 15 minutes or less.

If on the management tool "max time to screen lock" is not set to "15 minutes" or less, or on the Samsung Android device "Secure lock settings" is not present and the listed Screen timeout values include durations of more than 15 minutes, this is a finding.

Remediation:

Configure the Samsung Android devices to lock the device display after 15 minutes (or less) of inactivity.

On the management tool, in the device password policies, set "max time to screen lock" to "15 minutes" or less.

A device password must be set for "max time to screen lock" to become active.

Additional Information:

CCI-000057

Prevent further access to the system by initiating a device lock after organization-defined time period of inactivity; and/or requiring the user to initiate a device lock before leaving the system unattended.

- NIST SP 800-53::AC-11 a
- NIST SP 800-53A::AC-11.1 (ii)
- NIST SP 800-53 Revision 4::AC-11 a
- NIST SP 800-53 Revision 5::AC-11 a

1.5 KNOX-15-005200 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Samsung Android must be configured to enable a screen-lock policy that will lock the display after a period of inactivity - Disable trust agents.

```
GROUP ID: V-269026
RULE ID: SV-269026r1036338
```

Rationale:

The screen lock timeout must be set to a value that helps protect the device from unauthorized access. Having a too-long timeout would increase the window of opportunity for adversaries who gain physical access to the mobile device through loss, theft, etc. Such devices are much more likely to be in an unlocked state when acquired by an adversary, thus granting immediate access to the data on the mobile device. The maximum timeout period of 15 minutes has been selected to balance functionality and security; shorter timeout periods may be appropriate depending on the risks posed to the mobile device.

```
SFRID: FMT_SMF.1.1 #2
```

Audit:

Review the configuration to determine if the Samsung Android devices are disabling Trust Agents.

This validation procedure is performed on both the management tool and the Samsung Android device.

On the management tool, in the device restrictions, verify "Trust Agents" are set to "Disable".

On the Samsung Android device:

1. Open Settings >> Security and privacy >> More security settings >> Trust agents.
2. Verify all listed Trust Agents are disabled and cannot be enabled. If a Trust Agent is not disabled in the list, verify for that Trust Agent, all of its listed Trustlets are disabled and cannot be enabled.

If on the management tool "Trust Agents" are not set to "Disable", or on the Samsung Android device a "Trust Agent" or "Trustlet" can be enabled, this is a finding.

Note: If the management tool has been correctly configured but a Trust Agent is still enabled, configure the "List of approved apps listed in managed Google Play" to disable it; refer to KNOX-15-005500.

Exception: Trust Agents may be used if the authorizing official (AO) allows a screen lock timeout after four hours (or more) of inactivity. This may be applicable to tactical use case.

Remediation:

Configure the Samsung Android devices to disable Trust Agents.

On the management tool, in the device restrictions, set "Trust Agents" to "Disable".

Additional Information:

CCI-000765

Implement multifactor authentication for access to privileged accounts.

- NIST SP 800-53::IA-2 (1)
- NIST SP 800-53A::IA-2 (1).1
- NIST SP 800-53 Revision 4::IA-2 (1)
- NIST SP 800-53 Revision 5::IA-2 (1)

1.6 KNOX-15-005300 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Samsung Android must be configured to not allow more than 10 consecutive failed authentication attempts.

```
GROUP ID: V-269027
RULE ID: SV-269027r1036177
```

Rationale:

The more attempts an adversary has to guess a password, the more likely the adversary will enter the correct password and gain access to resources on the device. Setting a limit on the number of attempts mitigates this risk. Setting the limit at 10 or fewer attempts gives authorized users the ability to make a few mistakes when entering the password but still provides adequate protection against dictionary or brute force attacks on the password.

```
SFRID: FMT_SMF.1.1 #2, FIA_AFL_EXT.1.5
```

Audit:

Review the configuration to determine if the Samsung Android devices are allowing only 10 or fewer consecutive failed authentication attempts.

This validation procedure is performed on both the management tool and the Samsung Android device.

On the management tool, in the device password policies, verify "max password failures for local wipe" is set to `10` attempts or less.

On the Samsung Android device:

1. Open Settings >> Lock screen.
2. Verify "Secure lock settings" is present and tap it.
3. Enter current password.
4. Verify "Auto factory reset" is grayed out, and cannot be configured. Note: When "Auto factory reset" is grayed out, this indicates the Administrator (MDM) is in control of the setting to wipe the device after 10 or fewer consecutive failed authentication attempts.

If on the management tool "max password failures for local wipe" is not set to `10` attempts or less, or on the Samsung Android device the "Auto factory reset" menu can be configured, this is a finding.

Remediation:

Configure the Samsung Android devices to allow only 10 or fewer consecutive failed authentication attempts.

On the management tool, in the device password policies, set "max password failures for local wipe" to `10` attempts or fewer.

A device password must be set for "max password failures for local wipe" to become active.

Additional Information:

CCI-000044

Enforce the organization-defined limit of consecutive invalid logon attempts by a user during the organization-defined time period.

- NIST SP 800-53::AC-7 a
- NIST SP 800-53A::AC-7.1 (ii)
- NIST SP 800-53 Revision 4::AC-7 a
- NIST SP 800-53 Revision 5::AC-7 a

1.7 KNOX-15-005400 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Samsung Android must be configured to enforce an application installation policy by specifying one or more authorized application repositories, including DOD-approved commercial app repository, management tool server, or mobile application store.

```
GROUP ID: V-269028
RULE ID: SV-269028r1036180
```

Rationale:

Forcing all applications to be installed from authorized application repositories can prevent unauthorized and malicious applications from being installed and executed on mobile devices. Allowing such installations and executions could cause a compromise of DOD data accessible by these unauthorized/malicious applications.

```
SFRID: FMT_SMF.1.1 #8
```

Audit:

Review the configuration to determine if the Samsung Android devices are disabling unauthorized application repositories.

This validation procedure is performed on both the management tool and the Samsung Android device.

On the management tool, in the Work profile restrictions, verify "installs from unknown sources globally" is set to "Disallow".

On the Samsung Android device:

1. Open Settings >> Security and privacy >> More privacy settings >> Install unknown apps.
2. In the "Personal" tab, verify that each app listed has the status "Disabled" under the app name or no apps are listed.
3. In the "Work" tab, verify that each app listed has the status "Disabled" under the app name or no apps are listed.

If on the management tool "installs from unknown sources globally" is not set to "Disallow", or on the Samsung Android device an app is listed with a status other than "Disabled", this is a finding.

Remediation:

Configure the Samsung Android devices to disable unauthorized application repositories.

COPE:

On the management tool, in the Work profile restrictions, set "installs from unknown sources globally" to "Disallow".

COBO:

On the management tool, in the device restrictions, set "installs from unknown sources globally" to "Disallow".

Note: Google Play must not be disabled. Disabling Google Play will cause system instability and critical updates will not be received.

Additional Information:

CCI-000366

Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

1.8 KNOX-15-005500 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Samsung Android's Work environment must be configured to enforce an application installation policy by specifying an application allowlist that restricts applications by the following characteristics: Names.

```
GROUP ID: V-269029
RULE ID: SV-269029r1036352
```

Rationale:

The application allowlist, in addition to controlling the installation of applications on the MD, must control user access/execution of all core and preinstalled applications, or the MD must provide an alternate method of restricting user access/execution to core and preinstalled applications.

Core application: Any application integrated into the OS by the OS or MD vendors.

Preinstalled application: Additional noncore applications included in the OS build by the OS vendor, MD vendor, or wireless carrier.

Requiring all authorized applications to be in an application allowlist prevents the execution of any applications (e.g., unauthorized, malicious) that are not part of the allowlist. Failure to configure an application allowlist properly could allow unauthorized and malicious applications to be downloaded, installed, and executed on the mobile device, causing a compromise of DOD data accessible by these applications.

The application allowlist, in addition to controlling the installation of applications on the MD, must control user access/execution of all core applications (included in the OS by the OS vendor) and preinstalled applications (provided by the MD vendor and wireless carrier), or the MD must provide an alternate method of restricting user access/execution to core and preinstalled applications.

```
SFRID: FMT_SMF.1.1 #8
```

Audit:

COPE:

Review the configuration to determine if the Work profile on the Samsung Android device is allowing users to install only applications that have been approved by the authorizing official (AO).

COBO:

Review the configuration to determine if the Samsung Android devices are allowing users to install only applications that have been approved by the AO.

This validation procedure is performed only on the management tool.

On the management tool, in the app catalog for managed Google Play, verify that only AO-approved apps are available.

If on the management tool the app catalog for managed Google Play includes non-AO-approved apps, this is a finding.

Remediation:

COPE:

Configure the Work profile on Samsung Android devices to allow users to install only applications that have been approved by the AO.

COBO:

Configure Samsung Android devices to allow users to install only applications that have been approved by the AO.

In addition to any local policy, the AO must not approve applications that have certain prohibited characteristic; these are covered in KNOX-15-005600.

On the management tool, in the app catalog for managed Google Play, add each AO-approved app to be available.

Note: Managed Google Play is an allowed App Store.

Additional Information:

CCI-001764

Prevent program execution in accordance with organization-defined policies, rules of behavior, and/or access agreements regarding software program usage and restrictions; rules authorizing the terms and conditions of software program usage.

- NIST SP 800-53 Revision 4::CM-7 (2)
- NIST SP 800-53 Revision 5::CM-7 (2)

1.9 KNOX-15-005600 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Samsung Android's Work environment must be configured to not allow installation of applications with the following characteristics:

- Backs up MD data to non-DOD cloud servers (including user and application access to cloud backup services);
- Transmits MD diagnostic data to non-DOD servers;
- Voice assistant application if available when MD is locked;
- Voice dialing application if available when MD is locked;
- Allows synchronization of data or applications between devices associated with user;
- Payment processing;
- Allows unencrypted (or encrypted but not FIPS 140-2/140-3 validated) data sharing with other MDs or printers; and
- Backs up its own data to a remote system.

```
GROUP ID: V-269030
RULE ID: SV-269030r1036392
```

Rationale:

Requiring all authorized applications to be in an application allowlist prevents the execution of any applications (e.g., unauthorized, malicious) that are not part of the allowlist. Failure to configure an application allowlist properly could allow unauthorized and malicious applications to be downloaded, installed, and executed on the mobile device, causing a compromise of DOD data accessible by these applications. Applications with the listed characteristics have features that can cause the compromise of sensitive DOD data or have features with no known application in the DOD environment.

Application note: The application allowlist, in addition to controlling the installation of applications on the MD, must control user access/execution of all core and preinstalled applications, or the MD must provide an alternate method of restricting user access/execution to core and preinstalled applications.

Core application: Any application integrated into the OS by the OS or MD vendors.

Preinstalled application: Additional noncore applications included in the OS build by the OS vendor, MD vendor, or wireless carrier.

```
SFRID: FMT_SMF.1.1 #8
```

Audit:

Verify requirement KNOX-15-005500 (managed Google Play) has been implemented.

If managed Google Play has not been implemented, this is a finding.

Remediation:

The authorizing official (AO) must not approve applications with the following characteristics for installation by users in the Work profile:

- Backs up MD data to non-DOD cloud servers (including user and application access to cloud backup services);
- Transmits MD diagnostic data to non-DOD servers;
- Voice assistant application if available when MD is locked;
- Voice dialing application if available when MD is locked;
- Allows synchronization of data or applications between devices associated with user;
- Payment processing;
- Allows unencrypted (or encrypted but not FIPS 140-2/140-3 validated) data sharing with other MDs or printers; and
- Backs up its own data to a remote system.

Implement managed Google Play (refer to requirement KNOX-15-005500).

Additional Information:

CCI-000803

Implement mechanisms for authentication to a cryptographic module that meet the requirements of applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance for such authentication.

- NIST SP 800-53::IA-7
- NIST SP 800-53A::IA-7.1
- NIST SP 800-53 Revision 4::IA-7
- NIST SP 800-53 Revision 5::IA-7

1.10 KNOX-15-005700 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Samsung Android 15 allowlist must be configured to not include artificial intelligence (AI) applications that process device data in the cloud, including Google Gemini.

```
GROUP ID: V-269031
RULE ID: SV-269031r1036378
```

Rationale:

Sensitive DOD data could be exposed when an AI app processes device data in the cloud.

```
SFRID: FMT_SMF.1.1 #8
```

Audit:

Review managed Samsung Android 15 device configuration settings to determine if the mobile device has an AI application that processes device data in the cloud, including Google Gemini.

Verify requirement KNOX-15-009200 (disallow modify accounts) has been implemented.

The following validation procedure is performed on the management tool Administration Console.

Verify that the KPE API "isIntelligenceOnlineProcessingAllowed()" returns false or that the KSP configuration has the restriction "Allow process data only on device" set to true.

If "disallow modify accounts" is not set to "enable" (KNOX-15-009200) and the KPE API "isIntelligenceOnlineProcessingAllowed()" returns true and the KSP configuration does not have the restriction "Allow process data only on device" set to true, this is a finding.

Remediation:

On the EMM console:

1. Review the list of selected Managed Google Play apps.
2. Verify no AI applications that process device data in the cloud, including Google Gemini, are included.

Note: This restriction does not include Galaxy on device AI. Galaxy on device API is a "built-in" capability of Android 15 and processes device data on the device.

Disallow modify accounts (refer to requirement KNOX-15-009200).

Apply the "Disallow Intelligence Online Processing" using the KPE API or KSP. The KPE API is allowIntelligenceOnlineProcessing(false), and the KSP restriction is "Allow process data only on device", which should be set to "true".

Additional Information:

CCI-000803

Implement mechanisms for authentication to a cryptographic module that meet the requirements of applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance for such authentication.

- NIST SP 800-53::IA-7
- NIST SP 800-53A::IA-7.1
- NIST SP 800-53 Revision 4::IA-7
- NIST SP 800-53 Revision 5::IA-7

1.11 KNOX-15-005800 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Samsung Android must be configured to not display the following (Work Environment) notifications when the device is locked: All notifications.

```
GROUP ID: V-269032
RULE ID: SV-269032r1036192
```

Rationale:

Many mobile devices display notifications on the lock screen so that users can obtain relevant information in a timely manner without having to frequently unlock the phone to determine if there are new notifications. However, in many cases, these notifications can contain sensitive information. When they are available on the lock screen, an adversary can see them merely by being in close physical proximity to the device. Configuring the MOS to not send notifications to the lock screen mitigates this risk.

```
SFRID: FMT_SMF.1.1 #18
```

Audit:

Review the configuration to determine if the Samsung Android devices are not displaying (Work Environment) notifications when the device is locked.

Notifications of incoming phone calls are acceptable even when the device is locked.

This validation procedure is performed on both the management tool Administration Console and the Samsung Android device.

On the management tool, in the Work profile restrictions section, verify "Unredacted Notifications" is set to "Disallow".

COPE:

On the Samsung Android device:

1. Open Settings >> Notifications >> Lock screen (Edit).
2. Verify "Sensitive work profile notifications" is disabled.

If on the management tool "Unredacted Notifications" is not set to "Disallow", or on the Samsung Android device "Sensitive work profile notifications" is not disabled, this is a finding.

COBO:

On the Samsung Android device:

1. Open Settings >> Notifications >> Lock screen (Edit).
2. Verify "Lock screen notifications" menu is disabled.

If on the management tool "Unredacted Notifications" is not set to "Disallow", or on the Samsung Android device "Notifications" menu is not disabled, this is a finding.

Remediation:

Configure the Samsung Android devices to not display (Work Environment) notifications when the device is locked.

On the management tool, in the Work profile restrictions section, set "Unredacted Notifications" to "Disallow".

Additional Information:

CCI-000060

Conceal, via the device lock, information previously visible on the display with a publicly viewable image.

- NIST SP 800-53::AC-11 (1)
- NIST SP 800-53A::AC-11 (1).1
- NIST SP 800-53 Revision 4::AC-11 (1)
- NIST SP 800-53 Revision 5::AC-11 (1)

1.12 KNOX-15-006000 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

Samsung Android must be configured to enable encryption for data at rest on removable storage media or, alternately, the use of removable storage media must be disabled.

```
GROUP ID: V-269034
RULE ID: SV-269034r1036198
```

Rationale:

The MOS must ensure the data being written to the mobile device's removable media is protected from unauthorized access. If data at rest is unencrypted, it is vulnerable to disclosure. Even if the operating system enforces permissions on data access, an adversary can read removable media directly, thereby circumventing operating system controls. Encrypting the data ensures confidentiality is protected even when the operating system is not running.

```
SFRID: FMT_SMF.1.1 #20, #47d
```

Audit:

Review the configuration to determine if the Samsung Android devices are either enabling data-at-rest protection for removable media or disabling their use.

This requirement is not applicable for devices that do not support removable storage media.

This validation procedure is performed on both the management tool and the Samsung Android device.

On the management tool, in the device restrictions, verify "Mount physical media" is set to "Disallow".

On the Samsung Android device, verify that a microSD card cannot be mounted.

The device should ignore the inserted SD card and no notifications for the transfer of media files should appear, nor should any files be listed using a file browser, such as Samsung My Files.

If on the management tool "Mount physical media" is not set to "Disallow", or on the Samsung Android device a microSD card can be mounted, this is a finding.

Remediation:

Configure the Samsung Android devices to enable data-at-rest protection for removable media, or alternatively, disable their use.

This requirement is not applicable for devices that do not support removable storage media.

On the management tool, in the device restrictions, set "Mount physical media" to "Disallow".

This disables the use of all removable storage, e.g., microSD cards, USB thumb drives, etc.

If the deployment requires the use of microSD cards, Knox Platform for Enterprise (KPE) can be used to allow them in a STIG-approved configuration. In this case, do not configure this policy, and instead replace with KPE policy (innately by the management tool or via Knox Service Plugin [KSP]) "Enforce external storage encryption" with value "enable".

Additional Information:

CCI-001199

Protects the confidentiality and/or integrity of organization-defined information at rest.

- NIST SP 800-53::SC-28
- NIST SP 800-53A::SC-28.1
- NIST SP 800-53 Revision 4::SC-28
- NIST SP 800-53 Revision 5::SC-28

CCI-002235 Prevent non-privileged users from executing privileged functions.

- NIST SP 800-53 Revision 4::AC-6 (10)
- NIST SP 800-53 Revision 5::AC-6 (10)

1.13 KNOX-15-006100 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Samsung Android must be configured to disable authentication mechanisms providing user access to protected data other than a Password Authentication Factor: Face recognition.

```
GROUP ID: V-269035
RULE ID: SV-269035r1036201
```

Rationale:

Note: This requirement is Not Applicable for specific biometric authentication factors included in the product's Common Criteria evaluation.

The biometric factor can be used to authenticate the user to unlock the mobile device. Unapproved/evaluated biometric mechanisms could allow unauthorized users to have access to DOD sensitive data if compromised. By not permitting the use of unapproved/evaluated biometric authentication mechanisms, this risk is mitigated.

```
SFRID: FMT_SMF.1.1 #22, FIA_UAU.5.1
```

Audit:

Note: This requirement is not applicable for specific biometric authentication factors included in the product's Common Criteria evaluation.

Review the configuration to determine if the Samsung Android devices are disabling Face Recognition.

This validation procedure is performed on both the management tool and the Samsung Android device.

On the management tool in the device restrictions, verify "Face recognition" is set to "Disable".

On the Samsung Android device:

1. Open Settings >> Lock screen >> Screen lock type.
2. Enter current password.
3. Verify "Face" is disabled and cannot be enabled.

If on the management tool "Face Recognition" is not set to "Disable", or on the Samsung Android device "Face" can be enabled, this is a finding.

Remediation:

Note: This requirement is not applicable for specific biometric authentication factors included in the product's Common Criteria evaluation.

Configure the Samsung Android devices to disable Face Recognition.

On the management tool, in the device restrictions, set "Face Recognition" to "Disable".

Additional Information:

CCI-000765

Implement multifactor authentication for access to privileged accounts.

- NIST SP 800-53::IA-2 (1)
- NIST SP 800-53A::IA-2 (1).1
- NIST SP 800-53 Revision 4::IA-2 (1)
- NIST SP 800-53 Revision 5::IA-2 (1)

1.14 KNOX-15-006400 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Samsung Android must be configured to disable developer modes.

```
GROUP ID: V-269038
RULE ID: SV-269038r1036210
```

Rationale:

Developer modes expose features of the MOS that are not available during standard operation. An adversary may leverage a vulnerability inherent in a developer mode to compromise the confidentiality, integrity, and availability of DOD sensitive information. Disabling developer modes mitigates this risk.

```
SFRID: FMT_SMF.1.1 #26
```

Audit:

Review the configuration to determine if the Samsung Android devices are disabling developer modes.

This validation procedure is performed on both the management tool and the Samsung Android device.

On the management tool, in the device restrictions, verify "Debugging Features" is set to "Disallow".

On the Samsung Android device:

1. Open Settings >> About phone >> Software information.
2. Tap on the Build Number to try to enable "Developer Options" and validate that action is blocked.

If on the management tool "Debugging Features" is not set to "Disallow" or on the Samsung Android device "Developer options" action is not blocked, this is a finding.

Remediation:

Configure the Samsung Android devices to disable developer modes.

On the management tool, in the device restrictions, set "Debugging Features" to "Disallow".

Additional Information:

CCI-000381

Configure the system to provide only organization-defined mission essential capabilities.

- NIST SP 800-53::CM-7
- NIST SP 800-53A::CM-7.1 (ii)
- NIST SP 800-53 Revision 4::CM-7 a
- NIST SP 800-53 Revision 5::CM-7 a

1.15 KNOX-15-006700 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

Samsung Android must be configured to display the DOD advisory warning message at startup or each time the user unlocks the device.

```
GROUP ID: V-269041
RULE ID: SV-269041r1036219
```

Rationale:

Before granting access to the system, the mobile operating system is required to display the DOD-approved system use notification message or banner that provides privacy and security notices consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Required banners help ensure that DOD can audit and monitor the activities of mobile device users without legal restriction.

System use notification messages can be displayed when individuals first access or unlock the mobile device. The banner must be implemented as a "click-through" banner at device unlock (to the extent permitted by the operating system). A "click-through" banner prevents further activity on the information system unless and until the user executes a positive action to manifest agreement by clicking on a box indicating "OK."

The approved DOD text must be used exactly as required in the Knowledge Service referenced in DODI 8500.01. For devices accommodating banners of 1300 characters, the banner text is:

You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only. By using this IS (which includes any device attached to this IS), you consent to the following conditions: -The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations. -At any time, the USG may inspect and seize data stored on this IS. -Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG-authorized purpose. -This IS includes security measures (e.g., authentication and access controls) to protect USG interests--not for your personal benefit or privacy. -Notwithstanding the above, using this IS does not constitute consent to PM, LE, or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. Refer to User Agreement for details.

For devices with severe character limitations, the banner text is:

I've read & consent to terms in IS user agreem't.

The Administrator must configure the banner text exactly as written without any changes.

```
SFRID: FMT_SMF.1.1 #36
```

Audit:

Confirm if Method #1 or #2 is used at the Samsung device site and follow the appropriate procedure.

This validation procedure is performed on both the management tool and the Samsung Android device.

Validation procedure for Method #1: Place the DOD warning banner in the user agreement signed by each Samsung Android device user.

Review the signed user agreements for several Samsung Android device users and verify the agreement includes the required DOD warning banner text.

Validation procedure for Method #2 (preferred method): Configure the warning banner text in the Lock screen message on each managed mobile device.

On the management tool, in the device restrictions section, verify "Lock Screen Message" is set to the DOD-mandated warning banner text.

On the Samsung Android device, verify the required DOD warning banner text is displayed on the Lock screen.

If the warning text has not been placed in the signed user agreement, or if on the management tool "Lock Screen Message" is not set to the DOD-mandated warning banner text, or on the Samsung Android device the required DOD warning banner text is not displayed on the Lock screen, this is a finding.

Remediation:

Configure the DOD warning banner by either of the following methods (required text is found in the Vulnerability Description):

Method #1: Place the DOD warning banner in the user agreement signed by each Samsung Android device user.

Method #2 (preferred method): Configure the warning banner text in the Lock screen message on each managed mobile device.

On the management tool, in the device restrictions section, set "Lock Screen Message" to the DOD-mandated warning banner text.

Additional Information:

CCI-000048

Display an organization-defined system use notification message or banner to users before granting access to the system that provides privacy and security notices consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidelines.

- NIST SP 800-53::AC-8 a
- NIST SP 800-53A::AC-8.1 (ii)
- NIST SP 800-53 Revision 4::AC-8 a
- NIST SP 800-53 Revision 5::AC-8 a

1.16 KNOX-15-007200 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Samsung Android must be configured to disable USB mass storage mode.

```
GROUP ID: V-269046
RULE ID: SV-269046r1036337
```

Rationale:

USB mass storage mode enables the transfer of data and software from one device to another. This software can include malware. When USB mass storage is enabled on a mobile device, it becomes a potential vector for malware and unauthorized data exfiltration. Prohibiting USB mass storage mode mitigates this risk.

```
SFRID: FMT_SMF.1.1 #39
```

Audit:

Review the configuration to determine if the Samsung Android devices are disabling USB mass storage mode.

This validation procedure is performed on both the management tool and the Samsung Android device.

On the management tool, in the device restrictions, verify "USB file transfer" has been set to "Disallow".

On the Samsung Android device, first, connect the device to a computer with a USB cable. From the home screen, swipe down and view all device notifications. Verify that a "File Transfer" is not an option. Note: Connecting to the device and viewing notifications (without the policy being applied) will show a series of options including "Transferring files".

If on the management tool "USB file transfer" is not set to "Disallow", or on the Samsung Android device a "File Transfer" is an option, this is a finding.

Remediation:

Configure the Samsung Android devices to disable USB mass storage mode.

On the management tool, in the device restrictions, set "USB file transfer" to "Disallow".

DeX drag and drop file transfer capabilities will be prohibited, but all other DeX capabilities remain usable.

Additional Information:

CCI-002546

Physically or logically disable or remove organization-defined connection ports or input/output devices on organization-defined systems or system components.

- NIST SP 800-53 Revision 4::SC-41
- NIST SP 800-53 Revision 5::SC-41

1.17 KNOX-15-007300 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Samsung Android must be configured to not allow backup of all applications and configuration data to locally connected systems.

```
GROUP ID: V-269047
RULE ID: SV-269047r1036237
```

Rationale:

Data on mobile devices is protected by numerous mechanisms, including user authentication, access control, and cryptography. When the data is backed up to an external system (either locally connected or cloud based), many if not all of these mechanisms are no longer present. This leaves the backed-up data vulnerable to attack. Disabling backup to external systems mitigates this risk.

```
SFRID: FMT_SMF.1.1 #40
```

Audit:

Verify requirement KNOX-15-007200 (disallow USB file transfer) has been implemented.

If "Disallow USB file transfer" has not been implemented, this is a finding.

Remediation:

Ensure "USB file transfer" has been disallowed (refer to requirement KNOX-15-007200).

Additional Information:

CCI-001090

Prevent unauthorized and unintended information transfer via shared system resources.

- NIST SP 800-53::SC-4
- NIST SP 800-53A::SC-4.1
- NIST SP 800-53 Revision 4::SC-4
- NIST SP 800-53 Revision 5::SC-4

1.18 KNOX-15-007400 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Samsung Android must be configured to not allow backup of all applications, configuration data to remote systems. (This requirement applies to the Work Profile for COPE.)

- Disable Data Sync Framework.

```
GROUP ID: V-269048
RULE ID: SV-269048r1036240
```

Rationale:

Backups to remote systems (including cloud backup) can leave data vulnerable to breach on the external systems, which often offer less protection than the MOS. Where the remote backup involves a cloud-based solution, the backup capability is often used to synchronize data across multiple devices. In this case, DOD devices may synchronize DOD sensitive information to a user's personal device or other unauthorized computers that are vulnerable to breach. The Data Sync Framework allows apps to synchronize data between the mobile device and other web-based services. This uses accounts for services the user has added to the mobile device. Preventing the user from adding accounts to the device mitigates this risk.

For COBO/COPE (work profile) data cannot be backed up remotely via Backup Services. Work (profile) data could be backed up through adding an account to an app that supports the data sync framework; however, this is mitigated by preventing adding any accounts to the Work profile.

```
SFR ID: FMT_SMF_EXT.1.1 #40

SFRID: FMT_SMF.1.1 #40
```

Audit:

Verify requirement KNOX-15-009200 (disallow modify accounts) has been implemented.

If "disallow modify accounts" has not been implemented, this is a finding.

Remediation:

Disallow modify accounts (refer to requirement KNOX-15-009200).

Additional Information:

CCI-001090

Prevent unauthorized and unintended information transfer via shared system resources.

- NIST SP 800-53::SC-4
- NIST SP 800-53A::SC-4.1
- NIST SP 800-53 Revision 4::SC-4
- NIST SP 800-53 Revision 5::SC-4

1.19 KNOX-15-007700 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Samsung Android must be configured to enable authentication of personal hotspot connections to the device using a preshared key.

```
GROUP ID: V-269050
RULE ID: SV-269050r1036381
```

Rationale:

If no authentication is required to establish personal hotspot connections (Wi-Fi and Bluetooth), an adversary may be able to use that device to perform attacks on other devices or networks without detection. A sophisticated adversary may also be able to exploit unknown system vulnerabilities to access information and computing resources on the device. Requiring authentication to establish personal hotspot connections mitigates this risk.

Application note: If hotspot functionality is permitted, it must be authenticated via a preshared key. There is no requirement to enable hotspot functionality, and it is recommended this functionality be disabled by default.

```
SFRID: FMT_SMF.1.1 #41
```

Audit:

This is a "User-Based Enforcement (UBE)" control.

Check a sample of Samsung phones at the site and verify the Wi-Fi hotspot preshared key (password) is set to "WPA2/WPA3-Personal" or "WPA3-Personal".

1. Click Settings >> Connections >> Mobile Hotspot and Tethering >> Mobile Hotspot.
2. Select Network name >> Password >> Band.
3. Click on the "Security" link and verify either "WPA2/WPA3-Personal" or "WPA3-Personal" have been selected.

If the Wi-Fi hotspot security is not set to "WPA2/WPA3-Personal" or "WPA3-Personal", this is a finding.

Remediation:

This is a "User-Based Enforcement (UBE)" control.

Train users to not change the default Wi-Fi hotspot security setting: 15-character complex Wi-Fi hotspot preshared key (password) ("WPA2/WPA3-Personal" or WPA3-Personal"). (KNOX-15-009400).

If the required preshared key is not set up, train users to use the following procedure to set up the required setting:

1. Click Settings >> Network & Internet >> Hotspot & tethering.
2. Enable "WiFi hotspot".
3. Tap on the words to the left of the slide called "Wi-Fi Hotspot", to bring up the configuration options.
4. Click the "Security" link and select "WPA2/WPA3-Personal" or "WPA3-Personal".

Additional Information:

CCI-001443

Protect wireless access to the system using authentication of users and/or devices.

- NIST SP 800-53::AC-18 (1)
- NIST SP 800-53A::AC-18 (1).1
- NIST SP 800-53 Revision 4::AC-18 (1)
- NIST SP 800-53 Revision 5::AC-18 (1)

CCI-002314 Employ automated mechanisms to control remote access methods.

- NIST SP 800-53 Revision 4::AC-17 (1)
- NIST SP 800-53 Revision 5::AC-17 (1)

1.20 KNOX-15-007900 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Samsung Android's Work profile must be configured to disable exceptions to the access control policy that prevent application processes and groups of application processes from accessing all data stored by other application processes and groups of application processes.

```
GROUP ID: V-269052
RULE ID: SV-269052r1036252
```

Rationale:

App data sharing gives apps the ability to access the data of other apps for enhanced user functionality. However, sharing also poses a significant risk that unauthorized users or apps will obtain access to DOD sensitive information. To mitigate this risk, there are data sharing restrictions, primarily from sharing data from personal (unmanaged) apps and work (managed) apps. If a user is allowed to make exceptions to the data sharing restriction policy, the user could enable unauthorized sharing of data, leaving it vulnerable to breach. Limiting the granting of exceptions to either the Administrator or common application developer mitigates this risk.

Copy/paste of data between applications in different application processes or groups of application processes is considered an exception to the access control policy; therefore, the Administrator must be able to enable/disable the feature. Other exceptions include allowing any data or application sharing between process groups.

```
SFRID: FMT_SMF.1.1 #42, FDP_ACF_EXT.1.2
```

Audit:

Review the Samsung documentation and inspect the configuration to verify the Samsung Android devices are enabling an access control policy that prevents application processes and groups of application processes from accessing all data stored by other application processes and groups of application processes.

This validation procedure is performed on both the management tool and the Samsung Android device.

On the management tool, in the Work profile restrictions, set "Cross profile copy/paste" to "Disallow".

On the Samsung Android device:

1. Using any Work app, copy text to the clipboard.
2. Using any Personal app, verify the clipboard text cannot be pasted.

If on the management tool "Cross profile copy/paste" is not set to "Disallow", or on the Samsung Android device the clipboard text can be pasted into a Personal app, this is a finding.

Remediation:

Configure the Samsung Android devices to enable an access control policy that prevents application processes and groups of application processes from accessing all data stored by other application processes and groups of application processes.

On the management tool, in the Work profile restrictions section, set "Cross profile copy/paste" to "Disallow".

Additional Information:

CCI-002530

Maintain a separate execution domain for each executing system process.

- NIST SP 800-53 Revision 4::SC-39
- NIST SP 800-53 Revision 5::SC-39

CCI-002233

Prevent the organization-defined software from executing at higher privilege levels than users executing the software.

- NIST SP 800-53 Revision 4::AC-6 (8)
- NIST SP 800-53 Revision 5::AC-6 (8)

1.21 KNOX-15-008300 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

Samsung Android must be configured to disable all Bluetooth profiles except for HSP (Headset Profile), HFP (Hands-Free Profile), SPP (Serial Port Profile), A2DP (Advanced Audio Distribution Profile), AVRCP (Audio/Video Remote Control Profile), and PBAP (Phone Book Access Profile).

```
GROUP ID: V-269056
RULE ID: SV-269056r1036264
```

Rationale:

Some Bluetooth profiles provide the capability for remote transfer of sensitive DOD data without encryption or otherwise do not meet DOD IT security policies; therefore, must be disabled.

```
SFRID: FMT_SMF_EXT.1.1/BLUETOOTH BT-8
```

Audit:

Review the Samsung documentation and inspect the configuration to verify the Samsung Android devices are paired only with devices that support HSP, HFP, SPP, A2DP, AVRCP, and PBAP Bluetooth profiles.

This validation procedure is performed on both the management tool and the Samsung Android device.

On the management tool, in the device restrictions section, verify "Bluetooth" is set to the AO-approved selection: "Allow" if the AO has approved the use of Bluetooth or "Disallow" if the AO has not approved its use.

On the Samsung Android device:

1. Open Settings >> Connections >> Bluetooth.
2. Verify all listed paired Bluetooth devices use only authorized Bluetooth profiles.

If on the management tool "Bluetooth" is not set to the AO-approved value, or the Samsung Android device is paired with a device that uses unauthorized Bluetooth profiles, this is a finding.

Remediation:

Configure the Samsung Android devices to disable Bluetooth, or if the AO has approved the use of Bluetooth (for example, for hands-free use), train users to only pair devices that support HSP, HFP, SPP, A2DP, AVRCP, and PBAP profiles.

On the management tool, in the device restrictions section, set "Bluetooth" to the AO-approved selection: "Allow" if the AO has approved the use of Bluetooth or "Disallow" if the AO has not approved its use.

The user training requirement is satisfied in requirement KNOX-15-009400.

Additional Information:

CCI-000381

Configure the system to provide only organization-defined mission essential capabilities.

- NIST SP 800-53::CM-7
- NIST SP 800-53A::CM-7.1 (ii)
- NIST SP 800-53 Revision 4::CM-7 a
- NIST SP 800-53 Revision 5::CM-7 a

CCI-001761 Defines the functions, ports, protocols, software, and services within the information system that are to be disabled or removed when deemed unnecessary and/or nonsecure.

- NIST SP 800-53 Revision 4::CM-7 (1) (b)
- NIST SP 800-53 Revision 5::CM-7 (1) (b)

1.22 KNOX-15-008400 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Samsung Android must be configured to disable ad hoc wireless client-to-client connection capability.

```
GROUP ID: V-269057
RULE ID: SV-269057r1036267
```

Rationale:

Ad hoc wireless client-to-client connections allow mobile devices to communicate with each other directly, circumventing network security policies and making the traffic invisible. This could allow the exposure of sensitive DOD data and increase the risk of downloading and installing malware of the DOD mobile device.

```
SFRID: FMT_SMF_EXT.1.1/WLAN
```

Audit:

Review the configuration to determine if the Samsung Android devices are disallowing Wi-Fi Direct.

This validation procedure is performed on both the management tool and the Samsung Android device.

On the management tool, in the user restrictions, verify "Wi-Fi Direct" has been set to "Disallow".

On the Samsung Android device:

1. Open Settings >> Connections >> Wi-Fi.
2. From the hamburger menu, select Wi-Fi Direct.
3. Verify that Wi-Fi Direct cannot be selected.

If on the management tool "Wi-Fi Direct" is not set to "Disallow", or on the Samsung Android device a Wi-Fi direct device is listed that can be connected to, this is a finding.

Remediation:

Configure the Samsung Android devices to disallow Wi-Fi Direct.

On the management tool, in the user restrictions, set "Wi-Fi Direct" to "Disallow".

Wi-Fi direct connections and pairing between devices will become unavailable.

Additional Information:

CCI-002536

Protect organization-defined external and internal wireless links from organization-defined types of signal parameter attacks or references to sources for such attacks.

- NIST SP 800-53 Revision 4::SC-40
- NIST SP 800-53 Revision 5::SC-40

1.23 KNOX-15-008600 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Samsung Android's Work environment must allow only the Administrator (management tool) to perform the following management function: Install/remove DOD root and intermediate PKI certificates.

```
GROUP ID: V-269059
RULE ID: SV-269059r1036273
```

Rationale:

DOD root and intermediate PKI certificates are used to verify the authenticity of PKI certificates of users and web services. If the user is allowed to remove root and intermediate certificates, the user could allow an adversary to falsely sign a certificate in such a way that it could not be detected. Restricting the ability to remove DOD root and intermediate PKI certificates to the Administrator mitigates this risk.

```
SFRID: FMT_MOF_EXT.1.2 #47
```

Audit:

COPE:

Review the configuration to determine if the Samsung Android devices' Work profile is preventing users from removing DOD root and intermediate PKI certificates.

This validation procedure is performed on both the management tool and the Samsung Android device.

On the management tool, in the Work profile restrictions, verify "Configure credentials" is set to "Disallow".

On the Samsung Android device:

1. Open Settings >> Security and privacy >> More security settings >> View security certificates.
2. In the System tab, verify no listed certificate in the Work profile can be untrusted.
3. In the User tab, verify no listed certificate in the Work profile can be removed.

If on the management tool the device "Configure credentials" is not set to "Disallow", or on the Samsung Android device a certificate can be untrusted or removed, this is a finding.

COBO:

Review the configuration to determine if the Samsung Android devices are preventing users from removing DOD root and intermediate PKI certificates.

This validation procedure is performed on both the management tool and the Samsung Android device.

On the management tool, in the device restrictions, verify "Configure credentials" is set to "Disallow".

On the Samsung Android device:

1. Open Settings >> Security and privacy >> More security settings >> View security certificates.
2. In the System tab, verify no listed certificate in the device can be untrusted.
3. In the User tab, verify no listed certificate in the device can be removed.

If on the management tool in the device restrictions "Configure credentials" is not set to "Disallow", or on the Samsung Android device a certificate can be untrusted or removed, this is a finding.

Remediation:

COPE:

Configure the Samsung Android devices' Work profile to prevent users from removing DOD root and intermediate PKI certificates.

On the management tool, in the Work profile restrictions, set "Configure credentials" to "Disallow".

COBO:

Configure the Samsung Android devices to prevent users from removing DOD root and intermediate PKI certificates.

On the management tool, in the device restrictions, set "Configure credentials" to "Disallow".

Additional Information:

CCI-000370

Manage configuration settings for organization-defined system components using organization-defined automated mechanisms.

- NIST SP 800-53::CM-6 (1)
- NIST SP 800-53A::CM-6 (1).1
- NIST SP 800-53 Revision 4::CM-6 (1)
- NIST SP 800-53 Revision 5::CM-6 (1)

1.24 KNOX-15-008800 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Samsung Android must be enrolled as a COPE device.

```
GROUP ID: V-269060
RULE ID: SV-269060r1036276
```

Rationale:

The Work profile is the designated application group for the COPE use case.

```
SFRID: FMT_MOF_EXT.1.2 #47
```

Audit:

Review the configuration to determine if the Samsung Android devices are enrolled in a DOD-approved use case.

This validation procedure is performed on both the management tool Administration Console and the Samsung Android device.

On the management tool, verify the default enrollment is set to "Work profile for company-owned devices".

On the Samsung Android device:

1. Open Settings >> Security and privacy >> More security settings >> Device admin apps.
2. Verify the management tool Agent is listed.
3. Go to the app drawer.
4. Verify a "Personal" and "Work" tab are present.

If on the management tool the default enrollment is not set as "Work profile for company-owned devices", or on the Samsung Android device the "Personal" and "Work" tabs are not present or the management tool Agent is not listed, this is a finding.

Remediation:

Enroll the Samsung Android devices in a DOD-approved use case.

On the management tool, configure the default enrollment as "Work profile for company-owned devices".

Refer to the management tool documentation to determine how to configure the device enrollment.

Additional Information:

CCI-000366

Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

1.25 KNOX-15-008900 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Samsung Android must be configured to disallow configuration of the device's date and time.

```
GROUP ID: V-269061
RULE ID: SV-269061r1036279
```

Rationale:

Determining the correct time a particular application event occurred on a system is critical when conducting forensic analysis and investigating system events.

Periodically synchronizing internal clocks with an authoritative time source is necessary to correctly correlate the timing of events that occur across the enterprise. The three authoritative time sources for Samsung Android are an authoritative time server that is synchronized with redundant United States Naval Observatory (USNO) time servers as designated for the appropriate DOD network (NIPRNet or SIPRNet), the Global Positioning System (GPS), or the wireless carrier.

Time stamps generated by the audit system in Samsung Android must include both date and time. The time may be expressed in Coordinated Universal Time (UTC), a modern continuation of Greenwich Mean Time (GMT), or local time with an offset from UTC.

```
SFRID: FMT_MOF_EXT.1.2 #47
```

Audit:

Review the configuration to determine if the Samsung Android devices are disallowing the users from changing the date and time.

This validation procedure is performed on both the management tool and the Samsung Android device.

On the management tool, in the device restrictions, verify "Configure Date/Time" is set to "Disallow".

On the Samsung Android device:

1. Open Settings >> General management >> Date and time.
2. Verify "Automatic date and time" is on and the user cannot disable it.

If on the management tool "Configure Date/Time" is not set to "Disallow", or on the Samsung Android device "Automatic date and time" is not set or the user can disable it, this is a finding.

Remediation:

Configure the Samsung Android devices to disallow users from changing the date and time.

On the management tool, in the device restrictions, set "Configure Date/Time" to "Disallow".

Additional Information:

CCI-000366

Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

1.26 KNOX-15-009000 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Samsung Android's Work profile must have the DOD root and intermediate PKI certificates installed.

```
GROUP ID: V-269062
RULE ID: SV-269062r1036282
```

Rationale:

DOD root and intermediate PKI certificates are used to verify the authenticity of PKI certificates of users and web services. If the root and intermediate certificates are not available, an adversary could falsely sign a certificate in such a way that it could not be detected. Providing access to the DOD root and intermediate PKI certificates greatly diminishes the risk of this attack.

```
SFRID: FMT_MOF_EXT.1.2 #47
```

Audit:

COPE:

Review the configuration to determine if the Samsung Android's Work profile has the DOD root and intermediate PKI certificates installed.

This validation procedure is performed on both the management tool and the Samsung Android device.

The current DOD root and intermediate PKI certificates may be obtained in self-extracting zip files at https://cyber.mil/pki-pke (for NIPRNet).

On the management tool, in the Work profile policy management, verify the DOD root and intermediate PKI certificates are installed.

On the Samsung Android device:

1. Open Settings >> Security and privacy >> More security settings >> View security certificates.
2. In the User tab, verify the DOD root and intermediate PKI certificates are listed in the Work profile.

If on the management tool the DOD root and intermediate PKI certificates are not listed in the Work profile, or on the Samsung Android device the DOD root and intermediate PKI certificates are not listed in the Work profile, this is a finding.

COBO:

Review the configuration to determine if the Samsung Android devices have the DOD root and intermediate PKI certificates installed.

This validation procedure is performed on both the management tool and the Samsung Android device.

The current DOD root and intermediate PKI certificates may be obtained in self-extracting zip files at https://cyber.mil/pki-pke (for NIPRNet).

On the management tool, in the device policy management, verify the DOD root and intermediate PKI certificates are installed.

On the Samsung Android device:

1. Open Settings >> Security and privacy >> More security settings >> View security certificates.
2. In the User tab, verify the DOD root and intermediate PKI certificates are listed in the device.

If on the management tool the DOD root and intermediate PKI certificates are not listed in the device, or on the Samsung Android device the DOD root and intermediate PKI certificates are not listed in the device, this is a finding.

Remediation:

Install the DOD root and intermediate PKI certificates into the Samsung Android devices (install in Work profile for COPE).

The current DOD root and intermediate PKI certificates may be obtained in self-extracting zip files at https://cyber.mil/pki-pke (for NIPRNet).

On the management tool, in the device policy management (Work profile for COPE), install the DOD root and intermediate PKI certificates.

Additional Information:

CCI-000366

Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

1.27 KNOX-15-009100 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Samsung Android's Work environment must be configured to enable audit logging.

```
GROUP ID: V-269063
RULE ID: SV-269063r1036383
```

Rationale:

Audit logs enable monitoring of security-relevant events and subsequent forensics when breaches occur. They help identify attacks so that breaches can either be prevented or limited in their scope. They facilitate analysis to improve performance and security.

```
SFRID: FMT_MOF_EXT.1.2 #47
```

Audit:

COPE:

Review the configuration to determine if the Samsung Android devices' Work profile is enabling audit logging.

This validation procedure is performed on the management tool only.

On the management tool, in the Work profile restrictions, verify "Security logging" is set to "Enable".

If on the management tool "Security logging" is not set to "Enable", this is a finding.

COBO:

Review the configuration to determine if the Samsung Android devices are enabling audit logging.

This validation procedure is performed on the management tool only.

On the management tool, in the device restrictions, verify "Security logging" is set to "Enable".

If on the management tool "Security logging" is not set to "Enable", this is a finding.

Remediation:

Configure the Samsung Android devices' Work profile to enable audit logging. (COPE)

Configure the Samsung Android devices to enable audit logging. (COBO)

On the management tool, in the Work profile restrictions section, set "Security logging" to "Enable".

Additional Information:

CCI-000366

Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

1.28 KNOX-15-009200 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Samsung Android's Work environment must be configured to prevent users from adding personal email accounts to the work email app.

```
GROUP ID: V-269064
RULE ID: SV-269064r1036288
```

Rationale:

If the user is able to add a personal email account (POP3, IMAP, EAS) to the work email app, it could be used to forward sensitive DOD data to unauthorized recipients. Restricting email account addition to the Administrator or to allowlisted accounts mitigates this vulnerability.

```
SFRID: FMT_MOF_EXT.1.2 #47
```

Audit:

Review the configuration to determine if Samsung Android devices are preventing users from adding personal email accounts to the work email app.

On the management tool, in the device restrictions section, verify "Modify accounts" is set to "Disallow".

COPE:

On the Samsung Android device:

1. Open Settings >> Accounts and backup >> Manage accounts.
2. Navigate to the "Work" tab.
3. Verify no account can be added.

COBO:

On the Samsung Android device:

1. Open Settings >> Accounts and backup >> Manage accounts.
2. Verify no account can be added.

If on the management tool "Modify accounts" is not set to "Disallow", or on the Samsung Android device an account can be added, this is a finding.

Remediation:

Configure the Samsung Android devices to prevent users from adding personal email accounts to the work email app.

On the management tool, in the Work profile restrictions, set "Modify accounts" to "Disallow". (COPE)

On the management tool, in the device restrictions, set "Modify accounts" to "Disallow". (COBO)

Additional Information:

CCI-000366

Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

1.29 KNOX-15-009300 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

Samsung Android's Work profile must be configured to enable Common Criteria (CC) mode.

```
GROUP ID: V-269065
RULE ID: SV-269065r1036291
```

Rationale:

The CC mode feature is a superset of other features and behavioral changes that are mandatory MDFPP requirements. If CC mode is not implemented, the device will not be operating in the NIAP-certified compliant CC mode of operation.

When enforcing Android Enterprise (AE) CC mode on a Samsung Android device, additional Samsung-specific security features are also enabled.

CC mode implements the following behavioral/functional changes to meet MDFPP requirements:

- How the Bluetooth and Wi-Fi keys are stored using different types of encryption.
- Download mode is disabled and all updates will occur via Firmware Over the Air (FOTA) only.

In addition, CC mode adds new restrictions not to meet MDFPP requirements but to offer better security above what is required:

- Force password info following FOTA update for consistency.
- Disable Remote unlock by FindMyMobile.
- Restrict biometric attempts to 10.

```
SFRID: FMT_MOF_EXT.1.2 #47
```

Audit:

Review the configuration to determine if the Samsung Android devices are enabling CC mode.

This validation procedure is performed on both the management tool and the Samsung Android device.

On the management tool, in the Work profile restrictions, verify "Common Criteria mode" is set to "Enable".

On the Samsung Android device, put the device into "Download mode" (press and hold down the Home + Power + Volume Down buttons at the same time) and verify the text "Blocked by CC Mode" is displayed on the screen.

If on the management tool "Common Criteria mode" is not set to "Enable", or on the Samsung Android device the text "Blocked by CC Mode" is not displayed in "Download mode", this is a finding.

Remediation:

Configure the Samsung Android devices to enable CC mode.

On the management tool, in the Work profile restrictions, set "Common Criteria mode" to "Enable".

Additional Information:

CCI-000366

Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

1.30 KNOX-15-009400 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Samsung Android device users must complete required training.

```
GROUP ID: V-269066
RULE ID: SV-269066r1036385
```

Rationale:

The security posture of Samsung devices requires the device user to configure several required policy rules on their device. User-Based Enforcement (UBE) is required for these controls. In addition, if the authorizing official (AO) has approved the use of an unmanaged personal space, the user must receive training on risks. If a user is not aware of their responsibilities and does not comply with UBE requirements, the security posture of the Samsung mobile device may become compromised, and DOD sensitive data may become compromised.

```
SFRID: FMT_MOF_EXT.1.2 #47
```

Audit:

Review a sample of site User Agreements for Samsung device users or similar training records and training course content.

Verify Samsung device users have completed required training. The intent is that required training is renewed on a periodic basis in a time period determined by the AO.

If any Samsung device user has not completed required training, this is a finding.

Remediation:

Have all Samsung device users complete training on the following topics. Users should acknowledge they have reviewed training via a signed User Agreement or similar written record.

Training topics:

- Operational security concerns introduced by unmanaged applications/unmanaged personal space including applications using Global Positioning System (GPS) tracking.
- Need to ensure no DOD data is saved to the personal space or transmitted from a personal app (for example, from personal email).
- If the Purebred key management app is used, users are responsible for maintaining positive control of their credentialed device at all times. The DOD PKI certificate policy requires subscribers to maintain positive control of the

devices that contain private keys and report any loss of control so the credentials can be revoked. Upon device retirement, turn-in, or reassignment, ensure a factory data reset is performed prior to device handoff. Follow Mobility service provider decommissioning procedures as applicable.

- How to configure the following UBE controls (users must configure the control) on the Samsung device:
    1. Secure use of Calendar Alarm.
    2. Local screen mirroring and MirrorLink procedures (authorized/not authorized for use).
    3. Do not connect Samsung devices (via either DeX Station or dongle) to any DOD network via Ethernet connection.
    4. Do not upload DOD contacts via smart call and caller ID services.
    5. Do not configure a DOD network (work) VPN profile on any third-party VPN client installed in the personal space.
    6. If Bluetooth connections are approved for mobile device, types of allowed connections (for example car hands-free, but not Bluetooth wireless keyboard).
    7. How to perform a full device wipe.
    8. Use default Wi-Fi hotspot password: 15-character complex Wi-Fi hotspot preshared password enabled ("WPA2/WPA3-personal").
- AO 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.

Additional Information:

CCI-000366

Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

1.31 KNOX-15-009500 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

The Samsung Android device must have the latest available Samsung Android operating system (OS) installed.

```
GROUP ID: V-269067
RULE ID: SV-269067r1036297
```

Rationale:

Required security features are not available in earlier OS versions. In addition, earlier versions may have known vulnerabilities.

```
SFRID: FMT_MOF_EXT.1.2 #47
```

Audit:

Review the configuration to confirm if the Samsung Android devices have the most recently released version of Samsung Android installed.

This procedure is performed on both the management tool and the Samsung Android device.

In the management tool management console, review the version of Samsung Android installed on a sample of managed devices. This procedure will vary depending on the management tool product. Refer to the notes below to determine the latest available OS version.

On the Samsung Android device, to determine the installed OS version:

1. Open Settings.
2. Tap "About phone".
3. Tap "Software information".

If the installed version of Android OS on any reviewed Samsung devices is not the latest released by the wireless carrier, this is a finding.

Note: Some wireless carriers list the version of the latest Android OS release by mobile device model online:

ATT: https://www.att.com/devicehowto/dsm.html#!/popular/make/Samsung

Verizon Wireless: https://www.verizonwireless.com/support/software-updates/

Google Android OS patch website: https://source.android.com/security/bulletin/

Samsung Android OS patch website:
https://security.samsungmobile.com/securityUpdate.smsb

Remediation:

Install the latest released version of Samsung Android OS on all managed Samsung devices.

Note: In most cases, OS updates are released by the wireless carrier (for example, T-Mobile, Verizon Wireless, and ATT).

Additional Information:

CCI-000366

Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

1.32 KNOX-15-009700 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Samsung Android device must be configured to enforce that Wi-Fi Sharing is disabled.

```
GROUP ID: V-269069
RULE ID: SV-269069r1036388
```

Rationale:

Wi-Fi Sharing is an optional configuration of Wi-Fi Tethering/Mobile Hotspot, which allows the device to share its Wi-Fi connection with other wirelessly connected devices instead of its mobile (cellular) connection.

Wi-Fi Sharing grants the "other" device access to a corporate Wi-Fi network and may possibly bypass the network access control mechanisms. This risk can be partially mitigated by requiring the use of a preshared key for personal hotspots.

SFRID: FMT_SMF.1.1 #47

Audit:

Review device configuration settings to confirm Wi-Fi Sharing is disabled.

Mobile Hotspot must be enabled to enable Wi-Fi Sharing. If the authorizing official (AO) has not approved Mobile Hotspot, and it has been verified as disabled on the EMM console, no further action is needed.

If Mobile Hotspot is being used, use the following procedure to verify Wi-Fi Sharing is disabled:

On the EMM console:

COBO:

1. Open "Set user restrictions".
2. Verify "Disallow sharing admin configured Wi-Fi" is toggled to "ON".

COPE:

1. Open "Set user restrictions on parent".
2. Toggle "Disallow sharing admin configured Wi-Fi" to "ON".

If on the EMM console, "Disallow sharing admin configured Wi-Fi" is not enabled, this is a finding.

Remediation:

Configure the Samsung Android 15 device to disable Wi-Fi Sharing.

Mobile Hotspot must be enabled to enable Wi-Fi Sharing. If the AO has not approved Mobile Hotspot, and it has been disabled on the EMM console, no further action is needed.

If Mobile Hotspot is being used, use the following procedure to disable Wi-Fi Sharing:

On the EMM console:

COBO:

1. Open "Set user restrictions".
2. Toggle "Disallow sharing admin configured Wi-Fi" to "ON".

COPE:

1. Open "Set user restrictions on parent".
2. Toggle "Disallow sharing admin configured Wi-Fi" to "ON".

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

1.33 KNOX-15-009800 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Samsung Android device work profile must be configured to enforce the system application disable list.

```
GROUP ID: V-269070
RULE ID: SV-269070r1036306
```

Rationale:

The system application disable list controls user access to/execution of all core and preinstalled applications.

Core application: Any application integrated into Samsung Android 15 by Samsung.

Preinstalled application: Additional noncore applications included in the Samsung Android 15 build by Samsung or the wireless carrier.

Some system applications can compromise DOD data or upload users' information to non-DOD-approved servers. A user must be blocked from using such applications that exhibit behavior that can result in compromise of DOD data or DOD user information.

The site administrator must analyze all preinstalled applications on the device and disable all applications not approved for DOD use by configuring the system application disable list.

```
SFRID: FMT_SMF.1.1 #47
```

Audit:

Review the configuration to confirm the system application disable list is enforced. This setting is enforced by default. Verify only approved system apps have been placed on the core allowlist.

This procedure is performed on the management tool.

Review the system app allowlist and verify only approved apps are on the list.

On the management tool, in the Apps management section, select "Unhide apps" and verify the names of the apps listed.

If on the management tool the system app allowlist contains unapproved core apps, this is a finding.

Remediation:

Configure the Samsung Android 15 device to enforce the system application allow list.

The required configuration is the default configuration when the device is enrolled. If the device configuration is changed, use the following procedure to bring the device back into compliance:

On the management tool:

1. Open "Apps management" section.
2. Select "unhide apps".
3. Enter names of apps to unhide (allow).

Configure a list of approved Samsung core and preinstalled apps in the core app allowlist.

Additional Information:

CCI-000366

Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

1.34 KNOX-15-009600 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Samsung Android device must be configured to enable Certificate Revocation List (CRL) status checking.

```
GROUP ID: V-269068
RULE ID: SV-269068r1036300
```

Rationale:

A CRL allows a certificate issuer to revoke a certificate for any reason, including improperly issued certificates and compromise of the private keys. Checking the revocation status of the certificate mitigates the risk associated with using a compromised certificate. For this reason, users must not be able to disable this configuration.

Samsung Android can control CRL checking but only using Knox APIs. Alternatively, CRL checking is based on app development best practice.

```
SFRID: FMT_MOF_EXT.1.2 #47
```

Audit:

Review the configuration to confirm that revocation checking is enabled. Verify the revocation checklist is set to "All Applications".

This procedure is performed on the management tool.

On the management tool:

1. Open Certificates Policy >> Revocation section.
2. Select "Get CRL".
3. Verify Toast message "Get revocation check: true".

If on the management tool the revocation check is disabled, this is a finding.

Remediation:

Configure the Samsung Android devices to enable CRL revocation checks for all applications. These revocation checks must be enabled using the Knox KPE APIs.

On the management tool, in the Certificate Policy restrictions, enable "Revocation Checks" for "All Applications".

Additional Information:

CCI-000366

Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

1.35 KNOX-15-009900 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Samsung Android device must be provisioned as a fully managed device and configured to create a work profile.

```
GROUP ID: V-269071
RULE ID: SV-269071r1036343
```

Rationale:

The Android Enterprise work profile is the designated application group for the COPE use case.

```
SFRID: FMT_SMF.1.1 #47
```

Audit:

Verify requirement KNOX-15-008800 (COPE enrollment) has been implemented.

If "COPE enrollment" has not been implemented, this is a finding.

Remediation:

Implement "COPE enrollment" (refer to requirement KNOX-15-008800).

Additional Information:

CCI-000366

Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

1.36 KNOX-15-010000 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Samsung Android device work profile must be configured to disable automatic completion of workspace internet browser text input.

```
GROUP ID: V-269072
RULE ID: SV-269072r1036312
```

Rationale:

The autofill functionality in the web browser allows the user to complete a form that contains sensitive information, such as personally identifiable information (PII), without previous knowledge of the information. By allowing the use of autofill functionality, an adversary who learns a user's Android device password, or who otherwise is able to unlock the device, may be able to further breach other systems by relying on the autofill feature to provide information unknown to the adversary. By disabling the autofill functionality, the risk of an adversary gaining further information about the device's user or compromising other systems is significantly mitigated.

```
SFRID: FMT_SMF.1.1 #47
```

Audit:

Review the work profile Chrome Browser app on the Samsung device autofill setting.

This validation procedure is performed on the management tool.

On the management tool:

1. Open "Managed Configurations" section.
2. Select the Chrome Browser version from the work profile.
3. Verify "PasswordManagerEnabled" is turned "OFF".
4. Verify "AutofillAddressEnabled" is turned "OFF".
5. Verify "AutofillCreditCardEnabled" is turned "OFF".

If on the management tool any of the browser autofill settings are set to "On" in the Chrome Browser Settings, this is a finding.

Remediation:

Configure the Samsung device to disable the autofill functionality.

The required configuration is the default configuration when the device is enrolled. If the device configuration is changed, use the following procedure to bring the device back into compliance:

On the management tool:

1. Open the "Managed configurations" section.
2. Select the Chrome Browser version from the work profile.
3. Ensure "PasswordManagerEnabled" is turned "OFF".
4. Ensure "AutofillAddressEnabled" is turned "OFF".
5. Ensure "AutofillCreditCardEnabled" is turned "OFF".

Additional Information:

CCI-000366

Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

1.37 KNOX-15-010100 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Samsung Android device work profile must be configured to disable the autofill services.

```
GROUP ID: V-269073
RULE ID: SV-269073r1036315
```

Rationale:

The autofill services allow the user to complete text inputs that could contain sensitive information, such as personally identifiable information (PII), without previous knowledge of the information. By allowing the use of autofill services, an adversary who learns a user's Android device password, or who otherwise is able to unlock the device, may be able to further breach other systems by relying on the autofill services to provide information unknown to the adversary. By disabling the autofill services, the risk of an adversary gaining further information about the device's user or compromising other systems is significantly mitigated.

Examples of apps that offer autofill services include Samsung Pass, Google, Dashlane, LastPass, and 1Password.

```
SFRID: FMT_SMF.1.1 #47
```

Audit:

Review the Samsung work profile configuration settings to confirm that autofill services are disabled.

This validation procedure is performed on the management tool.

On the management tool:

1. Open "Set user restrictions".
2. Verify "Disable autofill" is toggled to "ON".

If on the management tool the "disallow autofill" is not selected, this is a finding.

Remediation:

Configure the Samsung device to disable the autofill services.

On the management tool, in the Work profile User restrictions section, set "Disable autofill" to "Enable".

Additional Information:

CCI-000366

Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

1.38 KNOX-15-010200 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

The Samsung Android device must be configured to disable the use of third-party keyboards.

```
GROUP ID: V-269074
RULE ID: SV-269074r1036318
```

Rationale:

Many third-party keyboard applications are known to contain malware.

```
SFRID: FMT_SMF.1.1 #47
```

Audit:

Review the managed Samsung device configuration settings to confirm that no third-party keyboards are enabled.

This procedure is performed on the management tool.

On the management tool:

1. Open "Input methods".
2. Tap "Set input methods".
3. Verify only the approved keyboards are selected.

If third-party keyboards are allowed, this is a finding.

Remediation:

Configure the Samsung device to disallow the use of third-party keyboards.

On the management tool:

1. Open "Input methods".
2. Tap "Set input methods".
3. Select only the approved keyboard.

Additionally, Administrators can configure application allowlists for Google Play that do not have any third-party keyboards for user installation.

Additional Information:

CCI-000366

Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

1.39 KNOX-15-010300 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Samsung Android device must be configured to disable all data signaling over [assignment: list of externally accessible hardware ports (for example, USB)].

```
GROUP ID: V-269075
RULE ID: SV-269075r1036321
```

Rationale:

If a user is able to configure the security setting, the user could inadvertently or maliciously set it to a value that poses unacceptable risk to DOD information systems. An adversary could exploit vulnerabilities created by the weaker configuration to compromise DOD sensitive information.

```
SFRID: FMT_MOF_EXT.1.2 #24
```

Audit:

Review the device configuration to confirm the USB port is disabled except for charging the device.

On the management tool: Verify "Disallow usb file transfer" is toggled to "OFF".

If on the management tool the USB port is not disabled, this is a finding.

Remediation:

Configure the Samsung device to disable the USB port (except for charging the device).

On the management tool: Toggle "Disallow usb file transfer" to "OFF".

Additional Information:

CCI-002235

Prevent non-privileged users from executing privileged functions.

- NIST SP 800-53 Revision 4::AC-6 (10)
- NIST SP 800-53 Revision 5::AC-6 (10)

1.40 KNOX-15-010400 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

The Samsung Android device must be configured to perform the following management function: Disable Phone Hub.

```
GROUP ID: V-269076
RULE ID: SV-269076r1036324
```

Rationale:

It may be possible to transfer work profile data on a DOD Android device to an unauthorized Chromebook if the user has the same Google Account set up on the Chromebook. This may result in the exposure of sensitive DOD data.

```
SFRID: FMT_MOF_EXT.1.2 #47
```

Audit:

Review the management tool to confirm Phone Hub has been disabled.

On the management tool:

1. Open "Nearby notification streaming policy".
2. Verify "Nearby notification streaming policy" is set to "Disabled".
3. Open "Nearby app streaming policy".
4. Verify "Nearby app streaming policy" is set to "Disabled".

If on the management tool the "Nearby Streaming Policy" is not set to "Disabled", this is a finding.

Note: From a Chromebook, if a device is connected to the Phone Hub, try to set up the Notifications. It will fail to connect to the device to complete the setup if Phone Hub has been disabled on the DOD Android device.

Remediation:

Configure the Samsung device to disable the nearby notification and app streaming policy to disable Phone Hub.

On the management tool:

1. Open "Nearby notification streaming policy".
2. Set "Nearby notification streaming policy" to "Disabled".
3. Open "Nearby app streaming policy".
4. Set "Nearby app streaming policy" to "Disabled".

Additional Information:

CCI-001090

Prevent unauthorized and unintended information transfer via shared system resources.

- NIST SP 800-53::SC-4
- NIST SP 800-53A::SC-4.1
- NIST SP 800-53 Revision 4::SC-4
- NIST SP 800-53 Revision 5::SC-4

Appendix: Summary Table

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1	**STIG RULES**		
1.1	KNOX-15-000700 (Manual)	☐	☐
1.2	KNOX-15-004900 (Manual)	☐	☐
1.3	KNOX-15-005000 (Manual)	☐	☐
1.4	KNOX-15-005100 (Manual)	☐	☐
1.5	KNOX-15-005200 (Manual)	☐	☐
1.6	KNOX-15-005300 (Manual)	☐	☐
1.7	KNOX-15-005400 (Manual)	☐	☐
1.8	KNOX-15-005500 (Manual)	☐	☐
1.9	KNOX-15-005600 (Manual)	☐	☐
1.10	KNOX-15-005700 (Manual)	☐	☐
1.11	KNOX-15-005800 (Manual)	☐	☐
1.12	KNOX-15-006000 (Manual)	☐	☐
1.13	KNOX-15-006100 (Manual)	☐	☐
1.14	KNOX-15-006400 (Manual)	☐	☐
1.15	KNOX-15-006700 (Manual)	☐	☐
1.16	KNOX-15-007200 (Manual)	☐	☐
1.17	KNOX-15-007300 (Manual)	☐	☐
1.18	KNOX-15-007400 (Manual)	☐	☐
1.19	KNOX-15-007700 (Manual)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.20	KNOX-15-007900 (Manual)	☐	☐
1.21	KNOX-15-008300 (Manual)	☐	☐
1.22	KNOX-15-008400 (Manual)	☐	☐
1.23	KNOX-15-008600 (Manual)	☐	☐
1.24	KNOX-15-008800 (Manual)	☐	☐
1.25	KNOX-15-008900 (Manual)	☐	☐
1.26	KNOX-15-009000 (Manual)	☐	☐
1.27	KNOX-15-009100 (Manual)	☐	☐
1.28	KNOX-15-009200 (Manual)	☐	☐
1.29	KNOX-15-009300 (Manual)	☐	☐
1.30	KNOX-15-009400 (Manual)	☐	☐
1.31	KNOX-15-009500 (Manual)	☐	☐
1.32	KNOX-15-009700 (Manual)	☐	☐
1.33	KNOX-15-009800 (Manual)	☐	☐
1.34	KNOX-15-009600 (Manual)	☐	☐
1.35	KNOX-15-009900 (Manual)	☐	☐
1.36	KNOX-15-010000 (Manual)	☐	☐
1.37	KNOX-15-010100 (Manual)	☐	☐
1.38	KNOX-15-010200 (Manual)	☐	☐
1.39	KNOX-15-010300 (Manual)	☐	☐
1.40	KNOX-15-010400 (Manual)	☐	☐

Appendix: Change History

Date	Version	Changes for this version
Sep 12, 2025	1.0.0	Initial CIS Release