

CIS Google Android Benchmark

v1.4.0 - 04-04-2022

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/>

Table of Contents

| | |
|---|-----------|
| Terms of Use | 1 |
| Table of Contents | 2 |
| Overview | 5 |
| Intended Audience | 5 |
| Consensus Guidance | 6 |
| Typographical Conventions | 7 |
| Recommendation Definitions | 8 |
| Title | 8 |
| Assessment Status | 8 |
| Automated | 8 |
| Manual | 8 |
| Profile | 8 |
| Description | 8 |
| Rationale Statement | 8 |
| Impact Statement | 9 |
| Audit Procedure | 9 |
| Remediation Procedure | 9 |
| Default Value | 9 |
| References | 9 |
| CIS Critical Security Controls® (CIS Controls®) | 9 |
| Additional Information | 9 |
| Profile Definitions | 10 |
| Acknowledgements | 11 |
| Recommendations | 12 |
| 1 Android OS Security Settings | 12 |
| 1.1 (L1) Ensure device firmware is up to date (Manual)..... | 13 |
| 1.2 (L1) Ensure 'Screen Lock' is set to 'Enabled' (Manual) | 15 |
| 1.3 (L1) Ensure 'Make pattern visible' is set to 'Disabled' (if using a pattern as device lock mechanism) (Manual)..... | 17 |
| 1.4 (L1) Ensure 'Automatically Lock' is set to 'Immediately' (Manual) | 19 |
| 1.5 (L1) Ensure 'Power button instantly locks' is set to 'Enabled' (Manual)..... | 21 |
| 1.6 (L1) Ensure 'Lock Screen Message' is configured (Manual) | 23 |
| 1.7 (L2) Do not connect to untrusted Wi-Fi networks (Manual) | 25 |
| 1.8 (L2) Ensure 'Show passwords' is set to 'Disabled' (Manual) | 26 |
| 1.9 (L1) Ensure 'Developer Options' is set to 'Disabled' (Manual)..... | 27 |
| 1.10 (L1) Ensure 'Install unknown apps' is set to 'Disabled' (Manual) | 29 |
| 1.11 (L1) Do not root a user device (Manual)..... | 31 |

| | |
|--|------------|
| 1.12 (L2) Ensure 'Smart Lock' is set to 'Disabled' (Manual) | 33 |
| 1.13 (L2) Ensure 'Lock SIM card' is set to 'Enabled' (Manual) | 35 |
| 1.14 (L2) Ensure 'Find My Device' is set to 'Enabled' (Manual) | 37 |
| 1.15 (L1) Ensure 'Use network-provided time' and 'Use network-provided time zone' are set to 'Enabled' (Manual)..... | 38 |
| 1.16 (L1) Ensure 'Remotely locate this device' is set to 'Enabled' (Manual)..... | 40 |
| 1.17 (L1) Ensure 'Allow remote lock and erase' is set to 'Enabled' (Manual) | 42 |
| 1.18 (L1) Ensure 'Scan device for security threats' is set to 'Enabled' (Manual) | 44 |
| 1.19 (L1) Ensure 'Improve harmful app detection' is set to 'Enabled' (Manual)..... | 46 |
| 1.20 (L1) Ensure 'Ask for unlock pattern/PIN/password before unpinning' is set to 'Enabled' (Manual)..... | 48 |
| 1.21 (L1) Ensure 'Screen timeout' is set to '1 minute or less' (Manual)..... | 50 |
| 1.22 (L1) Ensure 'Wi-Fi assistant' is set to 'Disabled' (Manual)..... | 52 |
| 1.23 (L1) Keep device Apps up to date (Manual)..... | 54 |
| 1.24 (L1) Ensure 'Add users from lock screen' is set to 'Disabled' (Manual) | 56 |
| 1.25 (L1) Ensure 'Guest profiles' do not exist (Manual) | 58 |
| 1.26 (L1) Review app permissions periodically (Manual) | 60 |
| 1.27 (L1) Ensure 'Instant apps' is set to 'Disabled' (Manual)..... | 62 |
| 1.28 (L1) Ensure 'Bluetooth' Pairing is Configured (Manual)..... | 64 |
| 1.29 (L1) Ensure that no 3rd party keyboards are installed (Manual) | 66 |
| 1.30 (L1) Review existing user profiles periodically (Manual) | 67 |
| 2 Android OS Privacy Settings | 68 |
| 2.1 (L1) Ensure 'Lock screen' is set to 'Don't show notifications at all' (Manual) | 69 |
| 2.2 (L2) Ensure 'Use location' is set to 'Disabled' (Manual)..... | 71 |
| 2.3 (L2) Ensure 'Back up to Google Drive' is 'Disabled' (Manual) | 73 |
| 2.4 (L1) Ensure 'Web and App Activity' is set to 'Disabled' (Manual) | 75 |
| 2.5 (L1) Ensure 'Device Information' is set to 'Disabled' (Manual) | 77 |
| 2.6 (L1) Ensure 'Voice & Audio Activity' is set to 'Disabled' (Manual) | 79 |
| 2.7 (L1) Ensure 'YouTube Search History' is set to 'Disabled' (Manual) | 81 |
| 2.8 (L1) Ensure 'YouTube Watch History' is set to 'Disabled' (Manual) | 83 |
| 2.9 (L1) Ensure 'Google Location History' is set to 'Disabled' (Manual) | 85 |
| 2.10 (L1) Ensure 'Opt out of Ads Personalization' is set to 'Enabled' (Manual)..... | 87 |
| 3 Android OS Chrome Browser Settings | 88 |
| 3.1 (L1) Ensure 'Microphone' is set to 'Enabled' (Manual) | 89 |
| 3.2 (L1) Ensure 'Location' is set to 'Enabled' (Manual)..... | 90 |
| 3.3 (L1) Ensure 'Allow third-party cookies' is set to 'Disabled' (Manual) | 91 |
| 3.4 (L1) Ensure 'Safe Browsing' is set to 'Enabled' (Manual)..... | 92 |
| 3.5 (L2) Ensure 'Search and URL suggestions' is set to 'Disabled' (Manual)..... | 94 |
| 3.6 (L2) Ensure 'Do Not Track' is set to 'Enabled' (Manual)..... | 95 |
| Appendix: Summary Table | 97 |
| Appendix: CIS Controls v7 IG 1 Mapped Recommendations | 99 |
| Appendix: CIS Controls v7 IG 2 Mapped Recommendations | 100 |
| Appendix: CIS Controls v7 IG 3 Mapped Recommendations | 101 |
| Appendix: CIS Controls v7 Unmapped Recommendations..... | 102 |
| Appendix: CIS Controls v8 IG 1 Mapped Recommendations..... | 103 |
| Appendix: CIS Controls v8 IG 2 Mapped Recommendations | 104 |
| Appendix: CIS Controls v8 IG 3 Mapped Recommendations | 105 |

Appendix: CIS Controls v8 Unmapped Recommendations..... 106
Appendix: Change History 107

Overview

All CIS Benchmarks focus on technical configuration settings used to maintain and/or increase the security of the addressed technology, and they should be used in **conjunction** with other essential cyber hygiene tasks like:

- Monitoring the base operating system for vulnerabilities and quickly updating with the latest security patches
- Monitoring applications and libraries for vulnerabilities and quickly updating with the latest security patches

In the end, the CIS Benchmarks are designed as a key **component** of a comprehensive cybersecurity program.

This document, Security Configuration Benchmark for Google Android, provides prescriptive guidance for establishing a secure configuration posture for the Google Android OS. This guide was tested against the Android 11.0.0 OS. This benchmark covers Android 11.0.x and all hardware devices on which this OS is supported.

In determining recommendations, the current guidance treats all Android mobile device platforms as having the same use cases and risk/threat scenarios. In all but a very few cases, configuration steps, default settings, and benchmark recommended settings are identical regardless of hardware platform. To obtain the latest version of this guide, please visit <http://cisecurity.org>. If you have questions, comments, or have identified ways to improve this guide, please write us at feedback@cisecurity.org.

Intended Audience

This document is intended for system and application administrators, security specialists, auditors, help desk, end users, and platform deployment personnel who plan to use, develop, deploy, assess, or secure solutions that use Android 11.0.x

Consensus Guidance

This CIS Benchmark was created using a consensus review process comprised of a global community of subject matter experts. The process combines real world experience with data-based information to create technology specific guidance to assist users to secure their environments. Consensus participants provide perspective from a diverse set of backgrounds including consulting, software development, audit and compliance, security research, operations, government, and legal.

Each CIS Benchmark undergoes two phases of consensus review. The first phase occurs during initial Benchmark development. During this phase, subject matter experts convene to discuss, create, and test working drafts of the Benchmark. This discussion occurs until consensus has been reached on Benchmark recommendations. The second phase begins after the Benchmark has been published. During this phase, all feedback provided by the Internet community is reviewed by the consensus team for incorporation in the Benchmark. If you are interested in participating in the consensus process, please visit <https://workbench.cisecurity.org/>.

Typographical Conventions

The following typographical conventions are used throughout this guide:

| Convention | Meaning |
|--------------------------------------|---|
| <code>Stylized Monospace font</code> | Used for blocks of code, command, and script examples. Text should be interpreted exactly as presented. |
| Monospace font | Used for inline code, commands, or examples. Text should be interpreted exactly as presented. |
| < <i>italic font in brackets</i> > | Italic texts set in angle brackets denote a variable requiring substitution for a real value. |
| <i>Italic font</i> | Used to denote the title of a book, article, or other publication. |
| Note | Additional information or caveats |

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

Detailed information pertaining to the setting with which the recommendation is concerned. In some cases, the description will include the recommended value.

Rationale Statement

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

Impact Statement

Any security, functionality, or operational consequences that can result from following 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.

Default Value

Default value for the given setting in this recommendation, if known. If not known, either not configured or not defined will be applied.

References

Additional documentation relative to the recommendation.

CIS Critical Security Controls® (CIS Controls®)

The mapping between a recommendation and the CIS Controls is organized by CIS Controls version, Safeguard, and Implementation Group (IG). The Benchmark in its entirety addresses the CIS Controls safeguards of (v7) "5.1 - Establish Secure Configurations" and (v8) "4.1 - Establish and Maintain a Secure Configuration Process" so individual recommendations will not be mapped to these safeguards.

Additional Information

Supplementary information that does not correspond to any other field but may be useful to the user.

Profile Definitions

The following configuration profiles are defined by this Benchmark:

- **Level 1**

Items in this profile intend to:

- be practical and prudent;
- provide a clear security benefit; and
- not negatively inhibit the utility of the technology beyond acceptable means.

- **Level 2**

This profile extends the "Level 1" profile. Items in this profile exhibit one or more of the following characteristics:

- are intended for environments or use cases where security is paramount.
- acts as defense in depth measure.
- may negatively inhibit the utility or performance of the technology.

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:

Contributor

Jordan Rakoske
Phil White

Editor

Chantel Duckworth
Justin Brown

Recommendations

1 Android OS Security Settings

This section provides the security recommendation for Android OS.

1.1 (L1) Ensure device firmware is up to date (Manual)

Profile Applicability:

- Level 1

Description:

Ensure that the device is kept up to date with security patch levels.

The recommended state for this setting is: Apply updates.

Rationale:

Firmware updates often include critical security fixes that reduce the probability of an attacker remotely exploiting the device. The device should be on the latest security patch level as applicable.

Impact:

None

Audit:

To verify that your device is updated to the most recent firmware version:

1. Tap `Settings` Gear Icon.
2. Tap `System`.
3. Tap `Advanced`.
4. Tap `System update`.
5. Verify that the `Android Security patch level` is current and that no new updates exist.

Remediation:

Follow the below steps to check and update the device security patch level:

1. Tap `Settings` Gear Icon.
2. Tap `System`.
3. Tap `Advanced`.
4. Tap `System Updates`.
5. Tap `Check for update`.
6. Apply the update if available.

Default Value:

By default, users are notified about security patch level updates but are not installed until the user initiates the process.

References:

1. <https://source.android.com/security/bulletin/index.html>

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|---|------|------|------|
| v8 | 7.3 <u>Perform Automated Operating System Patch Management</u> Perform operating system updates on enterprise assets through automated patch management on a monthly, or more frequent, basis. | ● | ● | ● |
| v8 | 7.4 <u>Perform Automated Application Patch Management</u> Perform application updates on enterprise assets through automated patch management on a monthly, or more frequent, basis. | ● | ● | ● |
| v7 | 3.4 <u>Deploy Automated Operating System Patch Management Tools</u> Deploy automated software update tools in order to ensure that the operating systems are running the most recent security updates provided by the software vendor. | ● | ● | ● |
| v7 | 3.5 <u>Deploy Automated Software Patch Management Tools</u> Deploy automated software update tools in order to ensure that third-party software on all systems is running the most recent security updates provided by the software vendor. | ● | ● | ● |

1.2 (L1) Ensure 'Screen Lock' is set to 'Enabled' (Manual)

Profile Applicability:

- Level 1

Description:

Enable Screen lock.

The recommended state for this setting is: Enabled.

Rationale:

Enabling Screen Lock requires user authentication before interacting with the device. As a result, Screen Lock strengthens application and data protection and improves device security.

Impact:

A user will be prompted to unlock the device on every use.

Audit:

Verify that a Pattern, PIN or Password has been set for the device.

1. Tap Settings Gear Icon.
2. Tap Security.
3. Verify that Screen lock has Pattern, PIN or Password underneath the text.

Remediation:

To configure a Pattern, PIN or Password for the device:

1. Tap Settings Gear Icon.
2. Tap Security.
3. Tap Screen Lock.
4. Tap Pattern, PIN or Password.
5. Enter a complex Pattern, PIN or Password.
6. Tap Continue.
7. Enter in the same complex Pattern, PIN or Password again.
8. Tap OK.







Default Value:

By default, screen lock is not set.

References:

1. https://support.google.com/android/answer/9079129?hl=en&ref_topic=7029556&visit_id=636958548934918587-3326560713&rd=1

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|---|---|---|---|
| v8 | 4.3 <u>Configure Automatic Session Locking on Enterprise Assets</u> Configure automatic session locking on enterprise assets after a defined period of inactivity. For general purpose operating systems, the period must not exceed 15 minutes. For mobile end-user devices, the period must not exceed 2 minutes. |  |  |  |
| v7 | 16.11 <u>Lock Workstation Sessions After Inactivity</u> Automatically lock workstation sessions after a standard period of inactivity. |  |  |  |

1.3 (L1) Ensure 'Make pattern visible' is set to 'Disabled' (if using a pattern as device lock mechanism) (Manual)

Profile Applicability:

- Level 1

Description:

Disable pattern visibility if using a pattern as device lock mechanism.

The recommended state for this setting is: `Disabled`.

Rationale:

Keeping device unlock patterns visible during device unlock can reveal the pattern and is vulnerable to shoulder surfing attacks. Therefore, is it not a best practice to make the device pattern visible.

Impact:

The user would have to be careful while entering the device unlock pattern since visual feedback would not provide clues for tracing pattern input.

Audit:

Follow the below steps and verify that device unlock pattern is not visible:

1. Tap `Settings` `Gear Icon`.
2. Tap `Security`.
3. If `Screen lock` has `Pattern` underneath the text, follow further steps. If not, then this recommendation is not applicable.
4. Tap the `Gear Icon` next to `Screen lock`.
5. Verify that the `Make pattern visible` switch is `Disabled`.

Remediation:

To disable device unlock pattern visibility, follow the below steps:

1. Tap `Settings` `Gear Icon`.
2. Tap `Security`.
3. If `Screen lock` has `Pattern` underneath the text, follow further steps. If not, then this recommendation is not applicable.
4. Tap the `Gear Icon` next to `Screen lock`.
5. Toggle `Make pattern visible` to `OFF` position.

Default Value:

By default, device unlock pattern is visible.

References:

1. https://support.google.com/android/answer/9079129?hl=en&visit_id=636958548934918587-3326560713&rd=1

1.4 (L1) Ensure 'Automatically Lock' is set to 'Immediately' (Manual)

Profile Applicability:

- Level 1

Description:

Immediately lock the phone as soon as the device goes to sleep.

The recommended state for this setting is: `Immediately`.

Rationale:

Automatically and immediately lock the device as soon as it goes to sleep. This ensures no delay between the device entering the sleep state and the device being locked.

Impact:

None

Audit:

Follow the below steps and verify that `Automatically Lock` is set to `Immediately`:

1. Tap `Settings Gear Icon`.
2. Tap `Security`.
3. Tap the `Gear icon next to Screen lock`.
4. Verify that `Automatically lock` has a text `Immediately after sleep underneath it`.

Remediation:







Follow the below steps and set `Automatically Lock` to `Immediately`:

1. Tap `Settings Gear Icon`.
2. Tap `Security`.
3. Tap the `Gear icon next to Screen lock`.
4. Tap `Automatically lock`.
5. Tap `Immediately`.

Default Value:

By default, `Automatically lock` is set to 5 seconds after sleep.

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|---|---|---|---|
| v8 | 4.3 <u>Configure Automatic Session Locking on Enterprise Assets</u> Configure automatic session locking on enterprise assets after a defined period of inactivity. For general purpose operating systems, the period must not exceed 15 minutes. For mobile end-user devices, the period must not exceed 2 minutes. |  |  |  |
| v7 | 16.11 <u>Lock Workstation Sessions After Inactivity</u> Automatically lock workstation sessions after a standard period of inactivity. |  |  |  |

1.5 (L1) Ensure 'Power button instantly locks' is set to 'Enabled' (Manual)

Profile Applicability:

- Level 1

Description:

Pressing the power button should lock the device instantly.

The recommended state for this setting is: Enabled.

Rationale:

Enabling `Power button instantly locks` setting ensures that the device is instantly locked as well. This avoid a possible situation where a device is asleep but not locked and would be vulnerable to unauthorized use.

Impact:

None

Audit:

Follow the below steps and verify that `Power button instantly locks` is Enabled:

1. Tap `Settings Gear Icon`.
2. Tap `Security`.
3. Tap the `Gear icon` next to `Screen lock`.
4. Verify that `Power button instantly locks` is Enabled.

Remediation:

Follow the below steps to enable the `Power button instantly locks` setting:

1. Tap `Settings Gear Icon`.
2. Tap `Security`.
3. Tap the `Gear icon` next to `Screen lock`.
4. Toggle `Power button instantly locks` setting to ON position.







Default Value:

By default, `Power button instantly locks` setting is enabled.

References:

1. https://support.google.com/android/answer/9079129?hl=en&visit_id=636958548934918587-3326560713&rd=1

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|--|---|---|---|
| v8 | 4.3 Configure Automatic Session Locking on Enterprise Assets Configure automatic session locking on enterprise assets after a defined period of inactivity. For general purpose operating systems, the period must not exceed 15 minutes. For mobile end-user devices, the period must not exceed 2 minutes. |  |  |  |
| v7 | 16.11 Lock Workstation Sessions After Inactivity Automatically lock workstation sessions after a standard period of inactivity. |  |  |  |

1.6 (L1) Ensure 'Lock Screen Message' is configured (Manual)

Profile Applicability:

- Level 1

Description:

Set a message to be displayed on the locked screen.

The recommended state for this setting is: `Configure Lock Screen Message`.

Rationale:

When device screen is locked, a lock screen message helps to provide

- Deterrent warnings,
- Device recognition without needing to unlock the device
- Emergency contact information

Such information could be valuable to both your device security and personnel security. It is thus recommended to have a suitable lock screen message.

Impact:

Anyone who picks up the device can see the messages and emergency information without unlocking the phone.

Audit:

Follow the below steps and verify that `Lock screen message` is set:

1. Tap `Settings Gear Icon`.
2. Tap `Display`.
3. Tap `Advanced`.
4. Tap `Lock screen display`.
5. Tap `Lock screen message`.
6. Verify that a suitable `Lock screen message` is set.

Remediation:

Follow the below steps to set up a `Lock screen message`:

1. Tap `Settings Gear Icon`.
2. Tap `Display`.
3. Tap `Advanced`.
4. Tap `Lock screen display`.
5. Tap `Lock screen message`.
6. Write your message and tap `Save`.

Default Value:

By default, no message is set.

1.7 (L2) Do not connect to untrusted Wi-Fi networks (Manual)

Profile Applicability:

- Level 2

Description:

Do not connect to untrusted Wi-Fi networks.

The recommended state for this setting is: `Only connect to trusted networks.`

Rationale:

Connecting a device to an open untrusted network through unsecured channels can increase the remote attack surface of the device. The cellular data network is a more difficult medium to inspect compared to Wi-Fi. If a user is going to be using public Wi-Fi, using a secure VPN is recommended. In most cases, you should avoid using a public, untrusted or free Wi-Fi.

Impact:

A user might have to use cellular data and would not be able to take advantage of public Wi-Fi networks.

Audit:

Follow the below steps to verify that `Wi-Fi` is either disabled or not connected to an untrusted network:

1. Tap `Settings` Gear Icon.
2. Tap `Network & internet`.
3. Verify that the `Wi-Fi` switch is in the Off position or is connected to a trusted network only.

Remediation:

Follow the below steps to disable `Wi-Fi` or connect to a trusted network:

1. Tap `Settings` Gear Icon.
2. Tap `Network & internet`.
3. Toggle `Wi-Fi` setting to the Off position or connect to a trusted network.

References:

1. <https://support.google.com/android/answer/9075847?hl=en>

1.8 (L2) Ensure 'Show passwords' is set to 'Disabled' (Manual)

Profile Applicability:

- Level 2

Description:

Disable password visibility during input.

The recommended state for this setting is: *Disabled*.

Rationale:

This setting controls whether passwords typed into a user's Android device should be visible on screen or hidden. When this setting is disabled, the password is concealed, and only the most recent character is visible for a short time after it has been pressed. When this setting is enabled, the entire password can be viewed in plain text, if desired. Disabling this setting protects you against shoulder surfing attacks.

Impact:

Given the relative difficulty of typing letters accurately on a small on-screen keyboard, it can be helpful to get visual feedback on-screen that a user has typed all the characters of a password correctly. Disabling password visibility might impact user experience.

Audit:

Follow the below steps to verify *Show passwords* is set to *Disabled*:

1. Tap *Settings* Gear Icon.
2. Tap *Privacy*.
3. Verify that *Show passwords* slider is *OFF*.

Remediation:

Follow the below steps to disable *Show passwords*:

1. Tap *Settings* Gear Icon.
2. Tap *Privacy*.
3. Toggle *Show passwords* to *OFF* position.

Default Value:

By default, passwords are visible.

1.9 (L1) Ensure 'Developer Options' is set to 'Disabled' (Manual)

Profile Applicability:

- Level 1

Description:

Disable Developer Options.

The recommended state for this setting is: `Disabled`.

Rationale:

Enabling Developer Options allows a user to alter specific, very advanced settings on the device. This can severely affect how the device functions and expose additional developmental features to the user. This also exposes the device to respond to features such as USB debugging (when enabled) and other features that could be exploited to gain malicious access to the device sub-systems.

Impact:

None

Audit:

Follow the below steps to verify that `Developer Options` is `Disabled`:

1. Tap `Settings Gear Icon`.
2. Tap `System`.
3. Tap `Advanced`.
4. Tap `Developer options`.
5. Verify that it is `OFF`.

Remediation:

Follow the below steps to disable `Developer Options`:

1. Tap `Settings Gear Icon`.
2. Tap `System`.
3. Tap `Advanced`.
4. Tap `Developer options`.
5. Toggle it to `OFF` position.




Default Value:

By default, `Developer options` is disabled.

References:

1. <https://developer.android.com/studio/debug/dev-options>

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|--|---|---|---|
| v8 | <u>5.4 Restrict Administrator Privileges to Dedicated Administrator Accounts</u> Restrict administrator privileges to dedicated administrator accounts on enterprise assets. Conduct general computing activities, such as internet browsing, email, and productivity suite use, from the user's primary, non-privileged account. |  |  |  |
| v7 | <u>4 Controlled Use of Administrative Privileges</u> Controlled Use of Administrative Privileges | | | |

1.10 (L1) Ensure 'Install unknown apps' is set to 'Disabled' (Manual)

Profile Applicability:

- Level 1

Description:

Disable installation of apps from unknown sources.

The recommended state for this setting is: `Disabled`.

Rationale:

This setting determines whether applications can be installed from locations other than Google Play. Disabling installation from untrusted distribution channels protects against the inadvertent installation of untrusted or malicious applications. Google Play Apps are vetted by the Google Security Team and are generally considered safe. You should avoid installing apps from other sources.

Impact:

None

Audit:

Follow the below steps to verify that `Install unknown apps` is `Disabled`:

1. Tap `Settings` **Gear Icon**.
2. Tap `Apps & notifications`.
3. Tap `Advanced`.
4. Tap `Special app access`.
5. Tap `Install unknown apps`.
6. Verify that all of the apps in the list show `Not allowed`.

Remediation:

Follow the below steps to disable `Install unknown apps`:

1. Tap `Settings` **Gear Icon**.
2. Tap `Apps & notifications`.
3. Tap `Advanced`.
4. Tap `Special app access`.
5. Tap `Install unknown apps`.
6. Tap any app showing `Allowed`.
7. Toggle `Allow from this source` to `OFF` position.

Default Value:

By default, `Install unknown apps` is disabled.

References:

1. <https://support.google.com/pixelphone/answer/7391672?hl=en>

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|---|------|------|------|
| v8 | 2.3 <u>Address Unauthorized Software</u> Ensure that unauthorized software is either removed from use on enterprise assets or receives a documented exception. Review monthly, or more frequently. | ● | ● | ● |
| v8 | 2.5 <u>Allowlist Authorized Software</u> Use technical controls, such as application allowlisting, to ensure that only authorized software can execute or be accessed. Reassess bi-annually, or more frequently. | | ● | ● |
| v7 | 2.6 <u>Address unapproved software</u> Ensure that unauthorized software is either removed or the inventory is updated in a timely manner | ● | ● | ● |
| v7 | 2.7 <u>Utilize Application Whitelisting</u> Utilize application whitelisting technology on all assets to ensure that only authorized software executes and all unauthorized software is blocked from executing on assets. | | | ● |

1.11 (L1) Do not root a user device (Manual)

Profile Applicability:

- Level 1

Description:

Do not root a user device.

The recommended state for this setting is: `Do not Root`.

Rationale:

Rooting an Android device breaks the user-level restrictions set by Google. In addition, rooting enables any form of alteration to the device, which could allow privileged actions. As a result, rooting puts the device at greater risk because rooting can modify the device without restrictions. Rooting also voids the warranty and could make installing future security updates is problematic.

Impact:

While there is no direct impact to not rooting a device, returning to a non-rooted state often requires a full factory reset which likely results in complete data loss.

Audit:

Identifying a rooted device is not straightforward. You may need to install a terminal or root checker app to detect rooted devices. Alternatively, the device manufacturer may provide documentation describing how to detect rooting.

Remediation:

Follow your device manufacturer documentation to completely un-root a user device.




Default Value:

By default, devices are not rooted and run with user level restrictions.

References:

1. <http://www.wikihow.com/Check-if-Your-Android-Cellphone-Is-Rooted-or-Not>
2. <http://www.wikihow.com/Unroot-Android>

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|--|---|---|---|
| v8 | <u>5.4 Restrict Administrator Privileges to Dedicated Administrator Accounts</u> Restrict administrator privileges to dedicated administrator accounts on enterprise assets. Conduct general computing activities, such as internet browsing, email, and productivity suite use, from the user's primary, non-privileged account. |  |  |  |
| v7 | <u>4 Controlled Use of Administrative Privileges</u> Controlled Use of Administrative Privileges | | | |

1.12 (L2) Ensure 'Smart Lock' is set to 'Disabled' (Manual)

Profile Applicability:

- Level 2

Description:

Disable Smart Lock.

The recommended state for this setting is: Disabled.

Rationale:

Smart Lock detects the device's presence and automatically keeps it unlocked even if it has a screen password, pin or pattern enabled. Using Smart Lock allows the device to be unlocked if preconditions are met. As a best practice, do not set the device to unlock automatically. For example, if the device is stolen and taken to a location pre-defined in Smart Lock, it would automatically unlock. Similarly, if someone could replay the voice, the device would automatically unlock.

Impact:

The device would need to be manually unlocked every time.

Audit:

Follow the below steps to verify that Smart Lock is Disabled:

1. Tap the Settings Gear Icon.
2. Tap Security.
3. Tap Advanced.
4. Tap Trust agents.
5. Verify that Smart Lock (Google) is OFF.

Remediation:

Follow the below steps to disable Smart Lock:

1. Tap the Settings Gear Icon.
2. Tap Security.
3. Tap Advanced.
4. Tap Trust agents.
5. Toggle Smart Lock (Google) to OFF position.







Default Value:

By default, Smart Lock is enabled.

References:

1. https://support.google.com/android/answer/9075927?hl=en&visit_id=636959420073607202-2748220419&rd=1

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|--|---|---|---|
| v8 | 4.3 Configure Automatic Session Locking on Enterprise Assets Configure automatic session locking on enterprise assets after a defined period of inactivity. For general purpose operating systems, the period must not exceed 15 minutes. For mobile end-user devices, the period must not exceed 2 minutes. |  |  |  |
| v7 | 16.11 Lock Workstation Sessions After Inactivity Automatically lock workstation sessions after a standard period of inactivity. |  |  |  |

1.13 (L2) Ensure 'Lock SIM card' is set to 'Enabled' (Manual)

Profile Applicability:

- Level 2

Description:

Lock SIM card.

The recommended state for this setting is: `Enabled`.

Rationale:

If a device uses a SIM card(s), enable SIM card lock. A SIM card PIN locks the SIM and prevents anyone from removing the SIM card from your device and using it on another other device without knowing the PIN. Also, a user might choose to store your contacts and messages on the SIM card and thus it is highly recommended that you safeguard this valuable personal data by setting a custom PIN on the SIM card(s).

Note: Only phones that are not locked by the service provider can lock the SIM card.

Impact:

You would need to remember your SIM card PIN. If a user forgets the SIM card PIN, the user would need to contact the provider for support.

Audit:

Follow the below steps to verify that `Lock SIM card` is `Enabled`:

1. Tap the `Settings` Gear Icon.
2. Tap `Security`.
3. Tap `SIM card lock`.
4. Verify that `Lock SIM card` is `Enabled`.
5. If you have more than one SIM card, click on the 2nd SIM card tab and verify that `Lock SIM card` is `Enabled` there as well.

Remediation:

Follow the below steps to enable `Lock SIM card`:

1. Contact the SIM card provider and get the default SIM PIN.
2. Tap the `Settings Gear Icon`.
3. Tap `Security`.
4. Tap `SIM card lock`.
5. Toggle `Lock SIM card` to the on position.
6. Enter the default PIN provided by your SIM provider.
7. Press `OK`.
8. The `Lock SIM card` option will then be enabled.
9. Tap on `Change SIM PIN`.
10. Again, provide the default PIN provided (Old PIN) by your SIM card provider.
11. Type your new custom PIN.
12. Re-type your new custom PIN.
13. Press `OK`.
14. A custom SIM PIN is then set.
15. Repeat the process for the 2nd SIM, if applicable.

Default Value:

By default, `Lock SIM card` is disabled. Also, the SIM card has a default PIN set by the provider which is usually universally known.

References:

1. https://support.google.com/android/answer/6088895?hl=en-GB&visit_id=636959420073607202-2748220419&rd=1

1.14 (L2) Ensure 'Find My Device' is set to 'Enabled' (Manual)

Profile Applicability:

- Level 2

Description:

Setup `Find My Device` as a Device Administrator.

The recommended state for this setting is: `Enabled`.

Rationale:

If an Android device is lost, a user could use `Find My Device` to locate a device and also ring, lock, or erase the device data remotely

Impact:

Google may track your device location anytime.

Audit:

Follow the below steps to verify that `Find My Device` is `Enabled`:

1. Tap the `Settings` Gear Icon.
2. Tap `Security`.
3. Verify that the `Find My Device` is `ON`.

Remediation:

Follow the below steps to enable `Find My Device`:

1. Tap the `Settings` Gear Icon.
2. Tap `Security`.
3. Tap `Find My Device`.
4. Toggle slider to the `ON` position.

Default Value:

By default, `Find My Device` is not enabled.

References:

1. <https://support.google.com/android/answer/6160491?hl=en>

1.15 (L1) Ensure 'Use network-provided time' and 'Use network-provided time zone' are set to 'Enabled' (Manual)

Profile Applicability:

- Level 1

Description:

Enable `Use network-provided time`. For this setting to work correctly, enable the `network-provided time zone` setting.

The recommended state for this setting is: `Enabled`.

Rationale:

Using the `network-provided time` setting fetches the date and time information from the cellular provider and is generally more reliable. In addition, precise date and time could help forensics device recovery through Android Device Manager and maintain application and logs in a time-sync manner.

Impact:

None

Audit:

Follow the below steps to verify that `Use network-provided time` and `Use network-provided time zone` setting is `Enabled`:

1. Tap `Settings` **Gear Icon**.
2. Tap `System`.
3. Tap `Date & time`.
4. Verify that `Use network-provided time` setting is `Enabled`.
5. Verify that `Use network-provided time zone` setting is `Enabled` as well.

Remediation:

Follow the below steps to enable `Use network-provided time` and `Use network-provided time zone` settings:

1. Tap `Settings` **Gear Icon**.
2. Tap `System`.
3. Tap `Date & time`.
4. Toggle `Use network-provided time` setting to `ON` position.
5. Toggle `Use network-provided time zone` setting to `ON` position.

Default Value:

By default, Use network-provided time **and** Use network-provided time zone settings are Enabled.

References:

1. <https://support.google.com/nexus/answer/2841106?hl=en>

1.16 (L1) Ensure 'Remotely locate this device' is set to 'Enabled' (Manual)

Profile Applicability:

- Level 1

Description:

Enable remotely locating the device.

The recommended state for this setting is: Enabled.

Rationale:

Remotely locate this device setting helps to track a lost device using Find My Device. It must be enabled for improving the recovery possibility of a device.

Impact:

This setting requires a user to keep location services enabled all the time. This might be considered a privacy issue

Audit:

Follow the below steps to verify that Remotely locate this device setting is Enabled:

1. Tap Settings Gear Icon.
2. Tap Google.
3. Tap Security.
4. Tap Find My Device.
5. Verify that Remotely locate this device setting is Enabled.

Remediation:

Follow the below steps to enable Remotely locate this device:

1. Tap Settings Gear Icon.
2. Tap Google.
3. Tap Security.
4. Tap Find My Device.
5. Toggle Remotely locate this device setting to ON position.

Default Value:

By default, Remotely locate this device setting is enabled.

References:

1. <https://support.google.com/accounts/answer/3265955#location>

1.17 (L1) Ensure 'Allow remote lock and erase' is set to 'Enabled' (Manual)

Profile Applicability:

- Level 1

Description:

Enable remotely locking and erasing the device.

The recommended state for this setting is: Enabled.

Rationale:

Allow remote lock and erase setting helps a user to remotely lock a device or erase data through Find My Device. This helps to safeguard privacy and protect data from unsanctioned access.

Impact:

This setting requires a user to keep location services enabled all the time. This might be considered a privacy issue.

Audit:

Follow the below steps to verify that Allow remote lock and erase setting is Enabled:

1. Tap Settings Gear Icon.
2. Tap Security.
3. Tap Device admin apps.
4. Verify that Find My Device is Enabled and Allow remote lock and erase is listed underneath.

Remediation:

Follow the below steps to enable Allow remote lock and erase:

1. Tap Settings Gear Icon.
2. Tap Security.
3. Tap Device admin apps.
4. Tap Find My Device toggle.
5. Tap Activate this device.




Default Value:

By default, Allow remote lock and erase setting is enabled.

References:

1. <https://support.google.com/accounts/answer/3265955#location>

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|---|---|---|---|
| v8 | <u>3.5 Securely Dispose of Data</u> Securely dispose of data as outlined in the enterprise's data management process. Ensure the disposal process and method are commensurate with the data sensitivity. |  |  |  |
| v7 | <u>13 Data Protection</u> Data Protection | | | |

1.18 (L1) Ensure 'Scan device for security threats' is set to 'Enabled' (Manual)

Profile Applicability:

- Level 1

Description:

Scan device for security threats.

The recommended state for this setting is: Enabled.

Rationale:

Scan device for security threats setting lets Google regularly check your device and prevent or warn about potential harm. This should be always enabled.

Impact:

None

Audit:

Follow the below steps to verify that Scan device for security threats setting is Enabled:

1. Tap Settings Gear Icon.
2. Tap Google.
3. Tap Security.
4. Tap Google Play Protect.
5. Tap Settings Gear icon.
6. Verify that Scan device for security threats setting is Enabled.

Remediation:

Follow the below steps to enable Scan device for security threats:

1. Tap Settings Gear Icon.
2. Tap Google.
3. Tap Security.
4. Tap Google Play Protect.
5. Tap Settings Gear icon.
6. Toggle Scan device for security threats setting to ON position.

Default Value:

By default, `Scan device for security threats` setting is disabled.

References:

1. <https://support.google.com/googleplay/answer/2812853?hl=en>

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|---|------|------|------|
| v8 | 10.6 <u>Centrally Manage Anti-Malware Software</u> Centrally manage anti-malware software. | | ● | ● |
| v7 | 8.1 <u>Utilize Centrally Managed Anti-malware Software</u> Utilize centrally managed anti-malware software to continuously monitor and defend each of the organization's workstations and servers. | | ● | ● |

1.19 (L1) Ensure 'Improve harmful app detection' is set to 'Enabled' (Manual)

Profile Applicability:

- Level 1

Description:

Improve detection of harmful apps.

The recommended state for this setting is: Enabled.

Rationale:

Enabling `Improve harmful app detection` setting sends anonymous information to Google about apps not installed from Google Play. This is especially true if a user chooses to install apps from "Unknown sources" outside the Google Play Store. This information helps Google better protect everyone from harmful apps.

Impact:

User data needs to be sent to Google and could incur data charges based on the carrier. Also, this user data might contain but is not restricted to log information, URLs related to the app, device ID, the Android version, and IP address.

Audit:

Follow the below steps to verify that `Improve harmful app detection` setting is Enabled:

1. Tap `Settings` **Gear Icon**.
2. Tap `Google`.
3. Tap `Security`.
4. Tap `Google Play Protect`.
5. Verify that `Improve harmful app detection` setting is Enabled.

Remediation:

Follow the below steps to enable `Improve harmful app detection`:

1. Tap `Settings` **Gear Icon**.
2. Tap `Google`.
3. Tap `Security`.
4. Tap `Google Play Protect`.
5. Toggle `Improve harmful app detection` setting to **ON** position.

Default Value:

By default, `Improve harmful app detection` setting is disabled.

References:

1. <https://support.google.com/googleplay/answer/2812853?hl=en>

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|---|------|------|------|
| v8 | 10.6 <u>Centrally Manage Anti-Malware Software</u> Centrally manage anti-malware software. | | ● | ● |
| v7 | 8.1 <u>Utilize Centrally Managed Anti-malware Software</u> Utilize centrally managed anti-malware software to continuously monitor and defend each of the organization's workstations and servers. | | ● | ● |

1.20 (L1) Ensure 'Ask for unlock pattern/PIN/password before unpinning' is set to 'Enabled' (Manual)

Profile Applicability:

- Level 1

Description:

A user can pin an app and hand the device to a friend. With the screen pinned, the friend can use only that app. To use the other apps again, the user can unpin the screen.

The recommended state for this setting is: `Enabled`.

Rationale:

You might lend your device to a friend or anyone else for carrying out a single task such as playing a game. You should use screen pinning in such a situation. It locks the users to the particular screen. Users cannot use the device outside of that application until the screen is unpinned. Unpinning the screen should require re-authentication.

Impact:

None

Audit:

Follow the below steps to verify that `Ask for pattern/PIN/password before unpinning` setting is `Enabled`:

1. Tap the `Settings` Gear Icon.
2. Tap `Security`.
3. Tap `Advanced`.
4. Tap `Screen pinning`.
5. If `Screen Pinning` is `On`, then verify that `Ask for pattern/PIN/password before unpinning` setting is `Enabled`.

Remediation:

Follow the below steps to enable `Ask for pattern/PIN/password before unpinning`:

1. Tap the `Settings` Gear Icon.
2. Tap `Security`.
3. Tap `Advanced`.
4. Tap `Screen pinning`.
5. If you are using `Screen Pinning`, then toggle `Ask for pattern/PIN/password before unpinning` setting to `ON` position.

Default Value:

By default, if a user enables Screen pinning, then Ask for pattern/PIN/password before unpinning setting is also enabled if a user has previously chosen to lock a user device with a pattern, PIN or password. If a user has previously chosen to not lock a device, a user would be required to set it up by tapping Lock device when unpinning after enabling Screen pinning.

References:

1. <https://support.google.com/android/answer/6118421?hl=en>

1.21 (L1) Ensure 'Screen timeout' is set to '1 minute or less' (Manual)

Profile Applicability:

- Level 1

Description:

Set `Screen timeout` setting to 1 minute or less.

The recommended state for this setting is: `1 Minute or less`.

Rationale:

It is best practice to set an inactivity timeout to avoid unsanctioned device usage if the device is unattended. The inactivity timeout turns off the screen after a stipulated time but also kicks in other security features such as a screen lock that protect the device when it is left unattended.

Impact:

You would need to unlock your device after every time inactivity period is reached.

Audit:

Follow the below steps to verify that `Screen timeout` setting is set to 1 minute or less:

1. Tap on `Settings Gear Icon`.
2. Tap `Display`.
3. Tap `Advanced`.
4. Verify that `Screen timeout` is set to 1 minute or less.

Remediation:

Follow the below steps to set `Screen timeout` setting to 1 minute or less:

1. Tap on `Settings Gear Icon`.
2. Tap `Display`.
3. Tap `Advanced`.
4. Tap `Screen timeout`.
5. Tap on time duration of 1 minute or less.







Default Value:

By default, `Screen timeout` is set to 1 minute of inactivity.

References:

1. <https://support.google.com/android/answer/9084191?hl=en>

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|---|---|---|---|
| v8 | 4.3 <u>Configure Automatic Session Locking on Enterprise Assets</u> Configure automatic session locking on enterprise assets after a defined period of inactivity. For general purpose operating systems, the period must not exceed 15 minutes. For mobile end-user devices, the period must not exceed 2 minutes. |  |  |  |
| v7 | 16.11 <u>Lock Workstation Sessions After Inactivity</u> Automatically lock workstation sessions after a standard period of inactivity. |  |  |  |

1.22 (L1) Ensure 'Wi-Fi assistant' is set to 'Disabled' (Manual)

Profile Applicability:

- Level 1

Description:

Disable automatically connecting your device to open Wi-Fi.

The recommended state for this setting is: `Disabled`.

Rationale:

Wi-Fi assistant connects to any open Wi-Fi and tunnels the connection through Google VPN servers. It is considered best practice to only connect to trusted networks manually and leave this setting disabled.

Impact:

You would not benefit from open Wi-Fi connections and would require using cellular data.

Note: This setting is only available on Pixel and Nexus devices running Android 5.1 or later. Also, even on these devices this feature is dependent on the carrier and country so it may not be available or configurable in all cases.

Audit:

Follow the below steps to verify that `Wi-Fi assistant` is `Disabled`:

1. Tap `Settings` **Gear** Icon.
2. Tap `Google`.
3. Tap `Networking`.
4. Verify that `Wi-Fi assistant` is turned `OFF`.

Remediation:

Follow the below steps to disable `Wi-Fi assistant`:

1. Tap `Settings` **Gear** Icon.
2. Tap `Google`.
3. Tap `Networking`.
4. Toggle `Wi-Fi assistant` to `OFF` position.

Default Value:

By default, `Wi-Fi assistant` setting is enabled.

Note: On the Verizon variant this setting is disabled. Also, this feature is available only on Pixel phones and Nexus devices running Android 5.1 and up in the selected countries.

References:

1. <https://support.google.com/nexus/answer/6327199?hl=en>

1.23 (L1) Keep device Apps up to date (Manual)

Profile Applicability:

- Level 1

Description:

Regularly update your device apps.

The recommended state for this setting is: Update apps.

Rationale:

Keeping apps updated gives a user access to the latest features and improves app security and stability. Updating applications has similar advantages to patching. Therefore, it is best practice to keep device apps updated.

Impact:

A user might incur data charges.

Audit:

Follow the below steps to verify that Apps are up to date:

1. Tap/slide up Launcher.
2. Launch Play Store App in the App drawer.
3. Tap Menu.
4. Tap My apps & Games.
5. Verify that all apps are up to date.

Remediation:

Follow the below steps to update all Apps:

1. Tap/slide up Launcher.
2. Launch Play Store App in the App drawer.
3. Tap Menu.
4. Tap My apps & Games.
5. If there are any updates pending, then tap Update All.













Default Value:

By default, apps are automatically updated. If cellular data is not a concern or secure Wi-Fi is available then you can leave the default Playstore app setting to auto update the apps to ensure that apps are updated automatically.

References:

1. <https://support.google.com/googleplay/answer/113412?hl=en-IN>

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|---|---|---|---|
| v8 | 7.3 <u>Perform Automated Operating System Patch Management</u> Perform operating system updates on enterprise assets through automated patch management on a monthly, or more frequent, basis. |  |  |  |
| v8 | 7.4 <u>Perform Automated Application Patch Management</u> Perform application updates on enterprise assets through automated patch management on a monthly, or more frequent, basis. |  |  |  |
| v7 | 3.4 <u>Deploy Automated Operating System Patch Management Tools</u> Deploy automated software update tools in order to ensure that the operating systems are running the most recent security updates provided by the software vendor. |  |  |  |
| v7 | 3.5 <u>Deploy Automated Software Patch Management Tools</u> Deploy automated software update tools in order to ensure that third-party software on all systems is running the most recent security updates provided by the software vendor. |  |  |  |

1.24 (L1) Ensure 'Add users from lock screen' is set to 'Disabled' (Manual)

Profile Applicability:

- Level 1

Description:

Do not allow adding users on a locked device.

The recommended state for this setting is: `Disabled`.

Rationale:

Users and the guest profile can do most of the same things as the device's owner, but each profile has its own storage space. As a result, guests could install malicious apps or carry out other activities that compromise overall device security. Therefore, adding users from the lock screen setting should be disabled.

Impact:

Users will not be able to add additional users when the device is locked.

Audit:

Follow the below steps to verify that `Add users from lock screen` setting is 'Disabled':

1. Tap `Settings Gear Icon`.
2. Tap `System`.
3. Tap `Advanced`.
4. Tap `Multiple users`.
5. Verify that `Add users from lock screen` setting is `Disabled`.

Remediation:

Follow the below steps to disable `Add users from lock screen` setting:

1. Tap `Settings Gear Icon`.
2. Tap `System`.
3. Tap `Advanced`.
4. Tap `Multiple users`.
5. Toggle `Add users from lock screen` setting to `OFF` position.

Default Value:

By default, Add users from lock screen setting is enabled.

References:

1. <https://support.google.com/pixelphone/answer/2865944>

1.25 (L1) Ensure 'Guest profiles' do not exist (Manual)

Profile Applicability:

- Level 1

Description:

Do not add any guest profiles on the device.

The recommended state for this setting is: `Remove Guest profiles`.

Rationale:

Users and the guest profile can do most of the same things as the device's owner, but each profile has its own storage space. As a result, guests could install malicious apps or carry out other activities that compromise overall device security. Therefore, adding any guest profiles on the device is not recommended.

Impact:

None

Audit:

Follow the below steps to verify that the `Guest profile` do not exist:

1. Tap `Settings Gear Icon`.
2. Tap `System`.
3. Tap `Advanced`.
4. Tap `Multiple users`.
5. Verify that `Guests` is grayed out.

Remediation:

Follow the below steps remove the `Guest profile`:

1. Open `Quick Settings drawer`.
2. Tap the `Profile icon`.
3. Switch to `Guest profile`.
4. Open `Quick Settings drawer`.
5. Tap `Remove guest`.
6. Confirm removal by tapping `remove`.

Default Value:

By default, `Guest profiles` do not exist.

References:

1. <https://support.google.com/pixelphone/answer/2865944>
2. https://support.google.com/pixelphone/answer/6115141?hl=en&ref_topic=7083408

1.26 (L1) Review app permissions periodically (Manual)

Profile Applicability:

- Level 1

Description:

Review your device app's permissions periodically.

The recommended state for this setting is: Review app permissions regularly.

Rationale:

App permissions allow control over which capabilities or information apps could access on the device. Permissions can extend from using device hardware to accessing data. Periodically review all apps' permissions and ensure that those apps have legitimate permissions. Uninstall apps that may seek overbroad permissions.

Impact:

Some apps request more than their required permissions. Such apps might not work if the additional unnecessary permissions are disabled. In some cases, the app will not function as expected and permissions may have to be restored or the app may require reinstallation.

Audit:

Follow the below steps to review your app permissions:

1. Tap `Settings` `Gear Icon`.
2. Tap `Apps & notifications`.
3. Tap `See all apps`.
4. Tap on each permission and review the apps that have them.

Remediation:

Follow the below steps to set your app permissions appropriately:

1. Tap `Settings` `Gear Icon`.
2. Tap `Apps & notifications`.
3. Tap `App permissions`.
4. Tap on each permission and review the apps that have them.
5. Disable the app permissions that you feel are over-permissive.

Default Value:

By default, apps seek permissions on first use or during installation.

References:

1. <https://support.google.com/googleplay/answer/6270602?hl=en-IN>

1.27 (L1) Ensure 'Instant apps' is set to 'Disabled' (Manual)

Profile Applicability:

- Level 1

Description:

Disable instant apps.

The recommended state for this setting is: `Disabled`.

Rationale:

Instant apps allow using an app without installing it on the device. On clicking an app link, the browser downloads and runs the app module.

Exposure to an app like this is dangerous since a malicious link might be used to trick a user. Also, this feature will generally defy enterprise security policies and safeguards that rely on denying or allowing apps at installation time. Therefore, it is recommended to disable instant apps.

Impact:

Instant apps will not be available. Instead, the app links would open in the browser just as other regular links.

Audit:

Follow the below steps to verify that `Instant apps` is `Disabled`:

1. Tap on `Settings Gear Icon`.
2. Tap `Apps & notifications`.
3. Tap `Advanced`.
4. Tap `Default apps`.
5. Tap `Opening links`.
6. Verify that `Instant apps` setting is set to `OFF` position.

Remediation:

Follow the below steps to disable `Instant apps`:

1. Tap on `Settings Gear Icon`.
2. Tap `Apps & notifications`.
3. Tap `Advanced`.
4. Tap `Default apps`.
5. Tap `Opening links`.
6. Toggle `Instant apps` setting to `OFF` position.







Default Value:

By default, `Instant apps` is enabled.

References:

1. <https://support.google.com/googleplay/answer/7240211>
2. <https://www.appthority.com/mobile-threat-center/blog/will-googles-instant-apps-undermine-enterprise-security/>
3. <https://developer.android.com/topic/instant-apps/index.html>

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|---|------|---|---|
| v8 | 2.6 Allowlist Authorized Libraries Use technical controls to ensure that only authorized software libraries, such as specific .dll, .ocx, .so, etc., files, are allowed to load into a system process. Block unauthorized libraries from loading into a system process. Reassess bi-annually, or more frequently. | |  |  |
| v8 | 2.7 Allowlist Authorized Scripts Use technical controls, such as digital signatures and version control, to ensure that only authorized scripts, such as specific .ps1, .py, etc., files, are allowed to execute. Block unauthorized scripts from executing. Reassess bi-annually, or more frequently. | | |  |
| v7 | 2.3 Utilize Software Inventory Tools Utilize software inventory tools throughout the organization to automate the documentation of all software on business systems. | |  |  |
| v7 | 2.5 Integrate Software and Hardware Asset Inventories The software inventory system should be tied into the hardware asset inventory so all devices and associated software are tracked from a single location. | | |  |

1.28 (L1) Ensure 'Bluetooth' Pairing is Configured (Manual)

Profile Applicability:

- Level 1

Description:

Bluetooth provides wireless connections to a wide range of devices like handsfree headsets, internet sharing and data transfer.

The recommended state for Bluetooth is: `Disabled`

Rationale:

Some Bluetooth profiles provide for transfer of data without encryption or may be in violation of organization security policies and therefore should be disabled.

Impact:

Disabling Bluetooth could prevent the use of headsets or handsfree calling which are required in some locales.

Audit:

Verify that Bluetooth is configured according to site policies.

1. Tap `Settings` **Gear Icon**.
2. Tap `Connected Devices`.
3. Tap `Connection Preferences`.
4. Tap `Bluetooth`.
5. Verify that Bluetooth is turned off or that all paired devices are authorized.





Remediation:

1. Tap `Settings` **Gear Icon**.
2. Tap `Connected Devices`.
3. Tap `Connection Preferences`.
4. Tap `Bluetooth`.
5. Toggle `Bluetooth` setting to `OFF` position.

Default Value:

Bluetooth is enabled by default

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|---|------|---|---|
| v8 | <u>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u> Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function. | |  |  |
| v7 | <u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system. | |  |  |

1.29 (L1) Ensure that no 3rd party keyboards are installed (Manual)

Profile Applicability:

- Level 1

Description:

A number of 3rd party custom keyboards are available for Android devices.

Rationale:

Many 3rd party keyboards have been known to contain malware and provide an easy method to capture keystrokes.

Audit:







Verify that no 3rd Party keyboards are installed

1. Tap **Settings Gear Icon**.
2. Tap **Apps & Notifications**.
3. Tap **See All Apps**.
4. Review the list of installed apps and verify that no 3rd party keyboards are installed.

Remediation:

1. Tap **Settings Gear Icon**.
2. Tap **Apps & Notifications**.
3. Tap **See All Apps**.
4. Review the list of installed apps and remove any 3rd party keyboards that are installed.

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|---|---|---|---|
| v8 | 2.3 Address Unauthorized Software Ensure that unauthorized software is either removed from use on enterprise assets or receives a documented exception. Review monthly, or more frequently. |  |  |  |
| v7 | 2.6 Address unapproved software Ensure that unauthorized software is either removed or the inventory is updated in a timely manner |  |  |  |

1.30 (L1) Review existing user profiles periodically (Manual)

Profile Applicability:

- Level 1

Description:

Review any user profiles on the device. Remove those that are no longer required.

Rationale:

Users and the guest profile can do most of the same things as the device's owner, but each profile has its own storage space. As a result, additional users could install malicious apps or carry out other activities that compromise overall device security. Therefore, reviewing and removing unnecessary user profiles should be done periodically.

Audit:

Review the list of user profiles.

Follow the below steps to view the list of profile that exist:

1. Tap `Settings` Gear Icon.
2. Tap `System`.
3. Tap `Advanced`.
4. Tap `Multiple users`.
5. Review the list of user profiles.

Remediation:

1. Tap `Settings` Gear Icon.
2. Tap `System`.
3. Tap `Advanced`.
4. Tap `Multiple users`.
5. Tap any unnecessary profile.
6. Tap `Delete User`

2 Android OS Privacy Settings

This section provides the privacy-related recommendation for Android OS.

2.1 (L1) Ensure 'Lock screen' is set to 'Don't show notifications at all' (Manual)

Profile Applicability:

- Level 1

Description:

Disable notifications on the lock screen.

The recommended state for this setting is: Don't show notifications at all.

Rationale:

If the device is lost or unattended, disabling notifications prevents the information from appearing on the lock screen. This information might be confidential, and thus unwarranted disclosures could be avoided.

Impact:

The user will not see the contents of notifications on the lock screen, requiring the user to unlock the device each time.

Audit:

To verify notifications on the lock screen are not shown:

1. Tap Settings Gear Icon.
2. Tap Apps & notifications.
3. Tap Notifications.
4. Tap Advanced.
5. Tap Lock Screen.
6. Verify that Lock Screen is set to Don't show notifications at all.

Remediation:

Follow these steps to set the lock screen to show no notifications:

1. Tap Settings Gear Icon.
2. Tap Apps & notifications.
3. Tap Notifications.
4. Tap Advanced.
5. Tap Lock Screen.
6. Tap Lock Screen and set it to Don't show notifications at all.







Default Value:

By default, notification content is shown on the locked screen.

References:

1. https://support.google.com/pixelphone/answer/6111294?hl=en&ref_topic=7078221

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|---|---|---|---|
| v8 | 4.3 <u>Configure Automatic Session Locking on Enterprise Assets</u> Configure automatic session locking on enterprise assets after a defined period of inactivity. For general purpose operating systems, the period must not exceed 15 minutes. For mobile end-user devices, the period must not exceed 2 minutes. |  |  |  |
| v7 | 16.11 <u>Lock Workstation Sessions After Inactivity</u> Automatically lock workstation sessions after a standard period of inactivity. |  |  |  |

2.2 (L2) Ensure 'Use location' is set to 'Disabled' (Manual)

Profile Applicability:

- Level 2

Description:

Disable Location when not in use.

The recommended state for this setting is: `Disabled`.

Rationale:

Enabling a device's location allows applications to gather and use data showing the user's location. The user's location is determined by using available information from cellular network data, local Wi-Fi networks, Bluetooth, and GPS. If the user turns off Location Services, the user will be prompted to re-enable location the next time an application tries to use this feature.

Disabling location reduces the capability of an attacker to determine or track the user's location via websites, locally installed applications, or other means without the user's consent. Thus, it should be disabled when not in use.

Note: Location is significant for tracking the lost device if the device data is not disabled. Make an informed decision to determine what is best for the organization.

Impact:

Each time an application needs location data, the user activity would be interrupted to enable the location manually. Additionally, if the device is lost and the location is disabled, A user cannot use remote locate services such as Android Device Manager.

Audit:

Follow the below steps to verify that `Use location` is `Disabled`:

1. Tap `Settings` Gear Icon.
2. Tap `Location`.
3. Verify that `Use location` is `OFF`.

Remediation:

Follow the below steps to disable `Use location`:

1. Tap `Settings` Gear Icon.
2. Tap `Location`.
3. Toggle `Use Location` switch to the `OFF` position.

Default Value:

By default, Location is enabled.

References:

1. https://support.google.com/pixelphone/answer/3467281?hl=en&ref_topic=7083817

2.3 (L2) Ensure 'Back up to Google Drive' is 'Disabled' (Manual)

Profile Applicability:

- Level 2

Description:

Disable Backup to Google Drive.

The recommended state for this setting is: *Disabled*.

Rationale:

If a user can back up corporate device data to a personal Google account, the user can later restore the information to a new device. Because of privacy concerns, backing up personal data such as text messages, emails, photos, and contacts to any third party is not recommended.

Impact:

A backup of the device will not be taken, and restoration will not be possible.

Audit:

Follow the below steps to verify `Back up to Google Drive` is `Disabled`:

1. Tap `Settings` `Gear Icon`.
2. Tap `System`.
3. Tap `Advanced`.
4. Tap `Backup`.
5. Verify that `Back up to Google Drive` is `OFF`.

Remediation:

Follow the below steps to disable `Back up to Google Drive`:

1. Tap `Settings` `Gear Icon`.
2. Tap `System`.
3. Tap `Advanced`.
4. Tap `Backup`.
5. Tap `Back up to Google Drive`.
6. Toggle it to `OFF` position.
7. Tap `OK` on warning popup.






Default Value:

By default, Back up to Google Drive is disabled.

References:

1. <https://support.google.com/pixelphone/answer/7179901?hl=en>

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|---|---|---|---|
| v8 | <u>2.3 Address Unauthorized Software</u> Ensure that unauthorized software is either removed from use on enterprise assets or receives a documented exception. Review monthly, or more frequently. |  |  |  |
| v7 | <u>13.4 Only Allow Access to Authorized Cloud Storage or Email Providers</u> Only allow access to authorized cloud storage or email providers. | |  |  |

2.4 (L1) Ensure 'Web and App Activity' is set to 'Disabled' (Manual)

Profile Applicability:

- Level 1

Description:

Disable linking of web and app activity to your account when you are logged out. The recommended state for this setting is: `Disabled`.

Note: This setting is applicable only for Google Pixel line of devices.

Rationale:

When this setting is enabled, searches and activity from other Google services are linked and saved to the Google Account. This could be privacy-invasive, so it is recommended to disable this setting.

Impact:

Web and App activities would not be linked to the account. This would result in not receiving a personalized user experience.

Audit:

Follow the below steps to verify that `Web & App Activity` setting is `Disabled`:

1. Tap `Settings` `Gear` Icon.
2. Tap `Privacy`.
3. Tap `Advanced`.
4. Tap `Activity Controls`.
5. Verify that `Web & App Activity` setting is `Disabled`.

Remediation:

Follow the below steps to disable `Web & App Activity` setting:

1. Tap `Settings` `Gear` Icon.
2. Tap `Privacy`.
3. Tap `Advanced`.
4. Tap `Activity Controls`.
5. Toggle `Web & App Activity` setting to `OFF` position.

Default Value:

By default, Web & App Activity is enabled.

References:

1. <https://support.google.com/pixelphone/answer/6139018?co=GENIE.Platform%3DDesktop&hl=en>
2. <https://support.google.com/websearch/answer/54068>

2.5 (L1) Ensure 'Device Information' is set to 'Disabled' (Manual)

Profile Applicability:

- Level 1

Description:

Disable storing device information to your account.

The recommended state for this setting is: `Disabled`.

Note: This setting is applicable only for Google Pixel line of devices.

Rationale:

When the `Device Information` setting is enabled, contact lists, calendars, alarms, and applications are saved to provide a personalized experience. The `Device Information` setting saves this data and replicates the information on Google's servers. It is recommended to disable this setting as it could be considered a privacy issue for the organization.

Impact:

A user might not get a personalized experience.

Audit:

Follow the below steps to verify that `Device Information` setting is `Disabled`:

1. Tap `Settings Gear Icon`.
2. Tap `Privacy`.
3. Tap `Advanced`.
4. Tap `Activity Controls`.
5. Verify that `Device Information` setting is `Disabled`.

Remediation:

Follow the below steps to disable `Device Information` setting:

1. Tap `Settings Gear Icon`.
2. Tap `Privacy`.
3. Tap `Advanced`.
4. Tap `Activity Controls`.
5. Toggle `Device Information` setting to `OFF` position.

Default Value:

By default, Device Information is enabled.

References:

1. <https://support.google.com/pixelphone/answer/6139018?co=GENIE.Platform%3DDesktop&hl=en>
2. <https://support.google.com/accounts/answer/6135999>

2.6 (L1) Ensure 'Voice & Audio Activity' is set to 'Disabled' (Manual)

Profile Applicability:

- Level 1

Description:

Disable saving your voice and other audio to your Google Account. The recommended state for this setting is: `Disabled`.

Note: This setting is applicable only for Google Pixel line of devices.

Rationale:

Google records your voice and other audio when you use audio activations. Audio can be saved even when your device is offline. When `Voice & Audio Activity` is off, voice inputs won't be saved to your Google Account, even if you're signed in. Instead, they may only be saved using anonymous identifiers. It is recommended to disable this setting as it could be considered a privacy issue for the organization.

Impact:

This would result in not receiving a personalized user experience.

Audit:

Follow the below steps to verify that `Voice & Audio Activity` setting is `Disabled`:

1. Tap `Settings` `Gear Icon`.
2. Tap `Privacy`.
3. Tap `Advanced`.
4. Tap `Activity Controls`.
5. Verify that `Voice & Audio Activity` setting is `Disabled`.

Remediation:

Follow the below steps to disable `Voice & Audio Activity` setting:

1. Tap `Settings` `Gear Icon`.
2. Tap `Privacy`.
3. Tap `Advanced`.
4. Tap `Activity Controls`.
5. Toggle `Voice & Audio Activity` setting to `OFF` position.

Default Value:

By default, Voice & Audio Activity setting is enabled.

References:

1. <https://support.google.com/pixelphone/answer/6139018?co=GENIE.Platform%3DDesktop&hl=en>
2. <https://support.google.com/websearch/answer/6030020>

2.7 (L1) Ensure 'YouTube Search History' is set to 'Disabled' (Manual)

Profile Applicability:

- Level 1

Description:

Disable storing YouTube Search History to a user's account.

The recommended state for this setting is: `Disabled`.

Note: This setting is applicable only for Google Pixel line of devices.

Rationale:

Turning on the `YouTube Search History` setting stores all YouTube searches to the user's Google account. YouTube and Google search history influences the recommendations seen on the YouTube homepage. It is recommended to disable this setting as it could be considered a privacy issue for the organization.

Impact:

This would result in not receiving a personalized user experience.

Audit:

Follow the below steps to verify that `YouTube Search History` setting is `Disabled`:

1. Tap `Settings` **Gear Icon**.
2. Tap `Privacy`.
3. Tap `Advanced`.
4. Tap `Activity Controls`.
5. Verify that `YouTube Search History` setting is `Disabled`.

Remediation:

Follow the below steps to disable `YouTube Search History` setting:

1. Tap `Settings` **Gear Icon**.
2. Tap `Privacy`.
3. Tap `Advanced`.
4. Tap `Activity Controls`.
5. Toggle `YouTube Search History` setting to `OFF` position.

Default Value:

By default, YouTube Search History setting is enabled.

References:

1. <https://support.google.com/pixelphone/answer/6139018?co=GENIE.Platform%3DDesktop&hl=en>
2. <https://support.google.com/youtube/answer/57711>

2.8 (L1) Ensure 'YouTube Watch History' is set to 'Disabled' (Manual)

Profile Applicability:

- Level 1

Description:

Disable storing YouTube Watch History to a user account.

The recommended state for this setting is: `Disabled`.

Note: This setting is applicable only for Google Pixel line of devices.

Rationale:

Turning on the `YouTube Watch History` setting stores all YouTube watch history to the user's Google account. YouTube and Google watch history influences the recommendations seen on the YouTube homepage. It is recommended to disable this setting as it could be considered a privacy issue for the organization.

Impact:

This would result in not receiving a personalized user experience.

Audit:

Follow the below steps to verify that `YouTube Watch History` setting is `Disabled`:

1. Tap `Settings` **Gear Icon**.
2. Tap `Privacy`.
3. Tap `Advanced`.
4. Tap `Activity Controls`.
5. Verify that `YouTube Watch History` is `Disabled`.

Remediation:

Follow the below steps to disable `YouTube Watch History` setting:

1. Tap `Settings` **Gear Icon**.
2. Tap `Privacy`.
3. Tap `Advanced`.
4. Tap `Activity Controls`.
5. Toggle `YouTube Watch History` setting to `OFF` position.

Default Value:

By default, YouTube Watch History setting is enabled.

References:

1. <https://support.google.com/pixelphone/answer/6139018?co=GENIE.Platform%3DDesktop&hl=en>
2. <https://support.google.com/youtube/answer/95725>

2.9 (L1) Ensure 'Google Location History' is set to 'Disabled' (Manual)

Profile Applicability:

- Level 1

Description:

Disable storing your location history.

The recommended state for this setting is: Disabled.

Note: This setting is applicable only for Google Pixel line of devices.

Rationale:

When the `Google Location History` setting is enabled, the device periodically sends diagnostic information to Google. This setting stores location history to provide results and recommendations across Google products. It is recommended to disable this setting as it could be considered a privacy issue for the organization.

Impact:

This would result in not receiving a personalized user experience.

Audit:

Follow the below steps to verify that `Google Location History` setting is Disabled:

1. Tap `Settings` **Gear Icon**.
2. Tap `Privacy`.
3. Tap `Advanced`.
4. Tap `Activity Controls`.
5. Verify that `Google Location History` setting is turned OFF.

Remediation:

Follow the below steps to disable `Google Location History` setting:

1. Tap `Settings` **Gear Icon**.
2. Tap `Privacy`.
3. Tap `Advanced`.
4. Tap `Activity Controls`.
5. Toggle `Google Location History` setting to OFF position.

Default Value:

By default, Google Location History setting is enabled.

References:

1. <https://support.google.com/pixelphone/answer/6139018?co=GENIE.Platform%3DDesktop&hl=en>
2. <https://support.google.com/accounts/answer/3118687>

2.10 (L1) Ensure 'Opt out of Ads Personalization' is set to 'Enabled' (Manual)

Profile Applicability:

- Level 1

Description:

Restrict apps from building your app profile.

The recommended state for this setting is: Enabled.

Rationale:

Apps leverage the app/browsing data to build a profile for displaying personalized ads. Disabling this setting prevents building profiles from various app/browsing activities to protect privacy.

Impact:

This would result in not receiving a personalized user experience.

Audit:

Follow the below steps to verify that Opt out of Ads Personalization setting is Enabled:

1. Tap Settings Gear Icon.
2. Tap Google.
3. Tap Ads.
4. Verify that Opt out of Ads Personalization setting is turned ON.

Remediation:

Follow the below steps to enable Opt out of Ads Personalization setting:

1. Tap Settings Gear Icon.
2. Tap Google.
3. Tap Ads.
4. Toggle Opt out of Ads Personalization setting to ON position.

Default Value:

By default, Opt out of Ads Personalization setting is disabled.

References:

1. <https://support.google.com/ads/answer/2662922?hl=en>

3 Android OS Chrome Browser Settings

3.1 (L1) Ensure 'Microphone' is set to 'Enabled' (Manual)

Profile Applicability:

- Level 1

Description:

This setting controls if a site asks before accessing the microphone.

The recommended state for this setting is: `Enabled`.

Rationale:

Websites will have to ask permission before being allowed to access the microphone, which will help prevent unwanted access to the microphone and help protect against potential privacy concerns.

Impact:

Users will be prompted each time a website requests access to the microphone.

Audit:

Follow the below steps to verify that `Microphone` is `Enabled`:

1. Tap `Chrome Icon`.
2. Tap `Menu Icon`.
3. Tap `Settings`.
4. Tap `Site settings`.
5. Verify that `Microphone` displays `Ask first`.

Remediation:

Follow the below steps to `Enable` the `Microphone` permission request:

1. Tap `Chrome Icon`.
2. Tap `Menu Icon`.
3. Tap `Settings`.
4. Tap `Site settings`.
5. Tap `Microphone`.
6. Toggle to the `ON` position.

Default Value:

`Enabled`.

3.2 (L1) Ensure 'Location' is set to 'Enabled' (Manual)

Profile Applicability:

- Level 1

Description:

This setting controls if a site asks before accessing the location.

The recommended state for this setting is: `Enabled`.

Rationale:

Websites will have to ask permission before being allowed to access the location, which will help prevent unwanted access to the user's location and help protect against potential privacy concerns.

Impact:

Users will be prompted each time a website requests access to the location.

Audit:

Follow the below steps to verify that `Location` is `Enabled`:

1. Tap `Chrome Icon`.
2. Tap `Menu Icon`.
3. Tap `Settings`.
4. Tap `Site settings`.
5. Verify that `Location` displays `Ask first`.

Remediation:

Follow the below steps to `Enable` the `Location` permission request:

1. Tap `Chrome Icon`.
2. Tap `Menu Icon`.
3. Tap `Settings`.
4. Tap `Site settings`.
5. Tap `Location`.
6. Toggle to the `ON` position.

Default Value:

`Enabled`.

3.3 (L1) Ensure 'Allow third-party cookies' is set to 'Disabled' (Manual)

Profile Applicability:

- Level 1

Description:

A third-party cookie is sent by a domain that differs from the domain in the browser's address bar.

The recommended state for this setting is: Disabled.

Rationale:

Blocking third-party cookies can help protect users' privacy by eliminating several website tracking cookies.

Impact:

Blocking third-party cookies may adversely affect the functionality of some sites.

Audit:

Follow the below steps to verify that Allow third-party cookies is Disabled:

1. Tap Chrome Icon.
2. Tap Menu Icon.
3. Tap Settings.
4. Tap Site settings.
5. Verify that Allow third-party cookies displays Allowed, except third-party.

Remediation:

Follow the below steps to Disabled the Allow third-party cookies option:

1. Tap Chrome Icon.
2. Tap Menu Icon.
3. Tap Settings.
4. Tap Site settings.
5. Tap Allow third-party cookies.
6. Uncheck the Allow third-party cookies checkbox.

Default Value:

Enabled.

3.4 (L1) Ensure 'Safe Browsing' is set to 'Enabled' (Manual)

Profile Applicability:

- Level 1

Description:

This setting controls the `Safe Browsing` feature.

The recommended state for this setting is: `Enabled`.

Rationale:

Google Safe Browsing helps protect devices by warning users when they attempt to navigate dangerous sites or download harmful files.

Impact:

Users will be shown a warning message before visiting a dangerous site or downloading a harmful app.

Audit:

Follow the below steps to verify that `Safe Browsing` is `Enabled`:

1. Tap `Chrome Icon`.
2. Tap `Menu Icon`.
3. Tap `Settings`.
4. Tap `Privacy`.
5. Verify that `Safe Browsing` checkbox is checked.

Remediation:

Follow the below steps to `Enable` the `Safe Browsing` feature:

1. Tap `Chrome Icon`.
2. Tap `Menu Icon`.
3. Tap `Settings`.
4. Tap `Privacy`.
5. Check **the** `Safe Browsing` checkbox.

Default Value:

Enabled.

References:

1. <https://safebrowsing.google.com/>

3.5 (L2) Ensure 'Search and URL suggestions' is set to 'Disabled' (Manual)

Profile Applicability:

- Level 2

Description:

Google Chrome uses a prediction service to show related searches, matches from browsing history, and popular websites while a user types in the address bar.

The recommended state for this setting is: Disabled.

Rationale:

Having search suggestions processed is considered a privacy concern.

Audit:

Follow the below steps to verify that Search and URL suggestions is Disabled:

1. Tap Chrome Icon.
2. Tap Menu Icon.
3. Tap Settings.
4. Tap Privacy.
5. Verify that Search and URL suggestions checkbox is unchecked.

Remediation:

Follow the below steps to Disable the Search and URL suggestions feature:

1. Tap Chrome Icon.
2. Tap Menu Icon.
3. Tap Settings.
4. Tap Privacy.
5. Uncheck the Search and URL suggestions checkbox.

Default Value:

Enabled.

References:

1. <https://support.google.com/chrome/answer/114836?hl=en&co=GENIE.Platform%3DAndroid>

3.6 (L2) Ensure 'Do Not Track' is set to 'Enabled' (Manual)

Profile Applicability:

- Level 2

Description:

When browsing the web on computers or Android devices, users can request websites not to collect or track browsing data.

The recommended state for this setting is: `Enabled`.

Note: Chrome doesn't provide details of which websites and web services respect Do Not Track requests and how websites interpret them.

Rationale:

Many websites will still collect and use browsing data to improve security, provide content, services, ads, and recommendations on their websites, and generate reporting statistics.

Audit:

Follow the below steps to verify that `Do Not Track` is `Enabled`:

1. Tap `Chrome Icon`.
2. Tap `Menu Icon`.
3. Tap `Settings`.
4. Tap `Privacy`.
5. Tap `Do Not Track`.
6. Verify that `Do Not Track` toggle is `on`.

Remediation:

Follow the below steps to `Enabled` the `Do Not Track` feature:

1. Tap `Chrome Icon`.
2. Tap `Menu Icon`.
3. Tap `Settings`.
4. Tap `Privacy`.
5. Tap `Do Not Track`.
6. Toggle the `Do Not Track` to the `ON` position.

Default Value:

Disabled.

References:

1. <https://support.google.com/chrome/answer/2790761?hl=en&co=GENIE.Platform%3DAndroid>

Appendix: Summary Table

| CIS Benchmark Recommendation | | Set Correctly | |
|------------------------------|--|--------------------------|--------------------------|
| | | Yes | No |
| 1 | Android OS Security Settings | | |
| 1.1 | (L1) Ensure device firmware is up to date (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.2 | (L1) Ensure 'Screen Lock' is set to 'Enabled' (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.3 | (L1) Ensure 'Make pattern visible' is set to 'Disabled' (if using a pattern as device lock mechanism) (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.4 | (L1) Ensure 'Automatically Lock' is set to 'Immediately' (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.5 | (L1) Ensure 'Power button instantly locks' is set to 'Enabled' (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.6 | (L1) Ensure 'Lock Screen Message' is configured (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.7 | (L2) Do not connect to untrusted Wi-Fi networks (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.8 | (L2) Ensure 'Show passwords' is set to 'Disabled' (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.9 | (L1) Ensure 'Developer Options' is set to 'Disabled' (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.10 | (L1) Ensure 'Install unknown apps' is set to 'Disabled' (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.11 | (L1) Do not root a user device (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.12 | (L2) Ensure 'Smart Lock' is set to 'Disabled' (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.13 | (L2) Ensure 'Lock SIM card' is set to 'Enabled' (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.14 | (L2) Ensure 'Find My Device' is set to 'Enabled' (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.15 | (L1) Ensure 'Use network-provided time' and 'Use network-provided time zone' are set to 'Enabled' (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.16 | (L1) Ensure 'Remotely locate this device' is set to 'Enabled' (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.17 | (L1) Ensure 'Allow remote lock and erase' is set to 'Enabled' (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.18 | (L1) Ensure 'Scan device for security threats' is set to 'Enabled' (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.19 | (L1) Ensure 'Improve harmful app detection' is set to 'Enabled' (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.20 | (L1) Ensure 'Ask for unlock pattern/PIN/password before unpinning' is set to 'Enabled' (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.21 | (L1) Ensure 'Screen timeout' is set to '1 minute or less' (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.22 | (L1) Ensure 'Wi-Fi assistant' is set to 'Disabled' (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |

| CIS Benchmark Recommendation | | Set Correctly | |
|------------------------------|--|--------------------------|--------------------------|
| | | Yes | No |
| 1.23 | (L1) Keep device Apps up to date (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.24 | (L1) Ensure 'Add users from lock screen' is set to 'Disabled' (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.25 | (L1) Ensure 'Guest profiles' do not exist (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.26 | (L1) Review app permissions periodically (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.27 | (L1) Ensure 'Instant apps' is set to 'Disabled' (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.28 | (L1) Ensure 'Bluetooth' Pairing is Configured (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.29 | (L1) Ensure that no 3rd party keyboards are installed (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.30 | (L1) Review existing user profiles periodically (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 2 | Android OS Privacy Settings | | |
| 2.1 | (L1) Ensure 'Lock screen' is set to 'Don't show notifications at all' (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.2 | (L2) Ensure 'Use location' is set to 'Disabled' (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.3 | (L2) Ensure 'Back up to Google Drive' is 'Disabled' (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.4 | (L1) Ensure 'Web and App Activity' is set to 'Disabled' (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.5 | (L1) Ensure 'Device Information' is set to 'Disabled' (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.6 | (L1) Ensure 'Voice & Audio Activity' is set to 'Disabled' (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.7 | (L1) Ensure 'YouTube Search History' is set to 'Disabled' (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.8 | (L1) Ensure 'YouTube Watch History' is set to 'Disabled' (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.9 | (L1) Ensure 'Google Location History' is set to 'Disabled' (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.10 | (L1) Ensure 'Opt out of Ads Personalization' is set to 'Enabled' (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 3 | Android OS Chrome Browser Settings | | |
| 3.1 | (L1) Ensure 'Microphone' is set to 'Enabled' (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.2 | (L1) Ensure 'Location' is set to 'Enabled' (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.3 | (L1) Ensure 'Allow third-party cookies' is set to 'Disabled' (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4 | (L1) Ensure 'Safe Browsing' is set to 'Enabled' (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.5 | (L2) Ensure 'Search and URL suggestions' is set to 'Disabled' (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.6 | (L2) Ensure 'Do Not Track' is set to 'Enabled' (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |

Appendix: CIS Controls v7 IG 1 Mapped Recommendations

| Recommendation | | Set Correctly | |
|----------------|---|--------------------------|--------------------------|
| | | Yes | No |
| 1.1 | (L1) Ensure device firmware is up to date | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.2 | (L1) Ensure 'Screen Lock' is set to 'Enabled' | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.4 | (L1) Ensure 'Automatically Lock' is set to 'Immediately' | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.5 | (L1) Ensure 'Power button instantly locks' is set to 'Enabled' | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.10 | (L1) Ensure 'Install unknown apps' is set to 'Disabled' | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.12 | (L2) Ensure 'Smart Lock' is set to 'Disabled' | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.21 | (L1) Ensure 'Screen timeout' is set to '1 minute or less' | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.23 | (L1) Keep device Apps up to date | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.29 | (L1) Ensure that no 3rd party keyboards are installed | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1 | (L1) Ensure 'Lock screen' is set to 'Don't show notifications at all' | <input type="checkbox"/> | <input type="checkbox"/> |

Appendix: CIS Controls v7 IG 2 Mapped Recommendations

| Recommendation | | Set Correctly | |
|----------------|---|--------------------------|--------------------------|
| | | Yes | No |
| 1.1 | (L1) Ensure device firmware is up to date | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.2 | (L1) Ensure 'Screen Lock' is set to 'Enabled' | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.4 | (L1) Ensure 'Automatically Lock' is set to 'Immediately' | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.5 | (L1) Ensure 'Power button instantly locks' is set to 'Enabled' | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.10 | (L1) Ensure 'Install unknown apps' is set to 'Disabled' | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.12 | (L2) Ensure 'Smart Lock' is set to 'Disabled' | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.18 | (L1) Ensure 'Scan device for security threats' is set to 'Enabled' | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.19 | (L1) Ensure 'Improve harmful app detection' is set to 'Enabled' | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.21 | (L1) Ensure 'Screen timeout' is set to '1 minute or less' | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.23 | (L1) Keep device Apps up to date | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.27 | (L1) Ensure 'Instant apps' is set to 'Disabled' | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.28 | (L1) Ensure 'Bluetooth' Pairing is Configured | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.29 | (L1) Ensure that no 3rd party keyboards are installed | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1 | (L1) Ensure 'Lock screen' is set to 'Don't show notifications at all' | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.3 | (L2) Ensure 'Back up to Google Drive' is 'Disabled' | <input type="checkbox"/> | <input type="checkbox"/> |

Appendix: CIS Controls v7 IG 3 Mapped Recommendations

| Recommendation | | Set Correctly | |
|----------------|---|--------------------------|--------------------------|
| | | Yes | No |
| 1.1 | (L1) Ensure device firmware is up to date | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.2 | (L1) Ensure 'Screen Lock' is set to 'Enabled' | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.4 | (L1) Ensure 'Automatically Lock' is set to 'Immediately' | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.5 | (L1) Ensure 'Power button instantly locks' is set to 'Enabled' | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.10 | (L1) Ensure 'Install unknown apps' is set to 'Disabled' | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.12 | (L2) Ensure 'Smart Lock' is set to 'Disabled' | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.18 | (L1) Ensure 'Scan device for security threats' is set to 'Enabled' | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.19 | (L1) Ensure 'Improve harmful app detection' is set to 'Enabled' | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.21 | (L1) Ensure 'Screen timeout' is set to '1 minute or less' | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.23 | (L1) Keep device Apps up to date | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.27 | (L1) Ensure 'Instant apps' is set to 'Disabled' | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.28 | (L1) Ensure 'Bluetooth' Pairing is Configured | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.29 | (L1) Ensure that no 3rd party keyboards are installed | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1 | (L1) Ensure 'Lock screen' is set to 'Don't show notifications at all' | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.3 | (L2) Ensure 'Back up to Google Drive' is 'Disabled' | <input type="checkbox"/> | <input type="checkbox"/> |

Appendix: CIS Controls v7 Unmapped Recommendations

| Recommendation | | Set Correctly | |
|----------------|---|--------------------------|--------------------------|
| | | Yes | No |
| 1.3 | (L1) Ensure 'Make pattern visible' is set to 'Disabled' (if using a pattern as device lock mechanism) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.6 | (L1) Ensure 'Lock Screen Message' is configured | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.7 | (L2) Do not connect to untrusted Wi-Fi networks | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.8 | (L2) Ensure 'Show passwords' is set to 'Disabled' | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.13 | (L2) Ensure 'Lock SIM card' is set to 'Enabled' | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.14 | (L2) Ensure 'Find My Device' is set to 'Enabled' | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.15 | (L1) Ensure 'Use network-provided time' and 'Use network-provided time zone' are set to 'Enabled' | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.16 | (L1) Ensure 'Remotely locate this device' is set to 'Enabled' | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.20 | (L1) Ensure 'Ask for unlock pattern/PIN/password before unpinning' is set to 'Enabled' | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.22 | (L1) Ensure 'Wi-Fi assistant' is set to 'Disabled' | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.24 | (L1) Ensure 'Add users from lock screen' is set to 'Disabled' | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.25 | (L1) Ensure 'Guest profiles' do not exist | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.26 | (L1) Review app permissions periodically | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.30 | (L1) Review existing user profiles periodically | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.2 | (L2) Ensure 'Use location' is set to 'Disabled' | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.4 | (L1) Ensure 'Web and App Activity' is set to 'Disabled' | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.5 | (L1) Ensure 'Device Information' is set to 'Disabled' | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.6 | (L1) Ensure 'Voice & Audio Activity' is set to 'Disabled' | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.7 | (L1) Ensure 'YouTube Search History' is set to 'Disabled' | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.8 | (L1) Ensure 'YouTube Watch History' is set to 'Disabled' | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.9 | (L1) Ensure 'Google Location History' is set to 'Disabled' | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.10 | (L1) Ensure 'Opt out of Ads Personalization' is set to 'Enabled' | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.1 | (L1) Ensure 'Microphone' is set to 'Enabled' | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.2 | (L1) Ensure 'Location' is set to 'Enabled' | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.3 | (L1) Ensure 'Allow third-party cookies' is set to 'Disabled' | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4 | (L1) Ensure 'Safe Browsing' is set to 'Enabled' | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.5 | (L2) Ensure 'Search and URL suggestions' is set to 'Disabled' | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.6 | (L2) Ensure 'Do Not Track' is set to 'Enabled' | <input type="checkbox"/> | <input type="checkbox"/> |

Appendix: CIS Controls v8 IG 1 Mapped Recommendations

| Recommendation | | Set Correctly | |
|----------------|---|--------------------------|--------------------------|
| | | Yes | No |
| 1.1 | (L1) Ensure device firmware is up to date | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.2 | (L1) Ensure 'Screen Lock' is set to 'Enabled' | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.4 | (L1) Ensure 'Automatically Lock' is set to 'Immediately' | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.5 | (L1) Ensure 'Power button instantly locks' is set to 'Enabled' | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.9 | (L1) Ensure 'Developer Options' is set to 'Disabled' | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.10 | (L1) Ensure 'Install unknown apps' is set to 'Disabled' | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.11 | (L1) Do not root a user device | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.12 | (L2) Ensure 'Smart Lock' is set to 'Disabled' | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.17 | (L1) Ensure 'Allow remote lock and erase' is set to 'Enabled' | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.21 | (L1) Ensure 'Screen timeout' is set to '1 minute or less' | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.23 | (L1) Keep device Apps up to date | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.29 | (L1) Ensure that no 3rd party keyboards are installed | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1 | (L1) Ensure 'Lock screen' is set to 'Don't show notifications at all' | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.3 | (L2) Ensure 'Back up to Google Drive' is 'Disabled' | <input type="checkbox"/> | <input type="checkbox"/> |

Appendix: CIS Controls v8 IG 2 Mapped Recommendations

| Recommendation | | Set Correctly | |
|----------------|---|--------------------------|--------------------------|
| | | Yes | No |
| 1.1 | (L1) Ensure device firmware is up to date | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.2 | (L1) Ensure 'Screen Lock' is set to 'Enabled' | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.4 | (L1) Ensure 'Automatically Lock' is set to 'Immediately' | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.5 | (L1) Ensure 'Power button instantly locks' is set to 'Enabled' | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.9 | (L1) Ensure 'Developer Options' is set to 'Disabled' | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.10 | (L1) Ensure 'Install unknown apps' is set to 'Disabled' | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.11 | (L1) Do not root a user device | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.12 | (L2) Ensure 'Smart Lock' is set to 'Disabled' | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.17 | (L1) Ensure 'Allow remote lock and erase' is set to 'Enabled' | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.18 | (L1) Ensure 'Scan device for security threats' is set to 'Enabled' | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.19 | (L1) Ensure 'Improve harmful app detection' is set to 'Enabled' | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.21 | (L1) Ensure 'Screen timeout' is set to '1 minute or less' | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.23 | (L1) Keep device Apps up to date | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.27 | (L1) Ensure 'Instant apps' is set to 'Disabled' | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.28 | (L1) Ensure 'Bluetooth' Pairing is Configured | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.29 | (L1) Ensure that no 3rd party keyboards are installed | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1 | (L1) Ensure 'Lock screen' is set to 'Don't show notifications at all' | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.3 | (L2) Ensure 'Back up to Google Drive' is 'Disabled' | <input type="checkbox"/> | <input type="checkbox"/> |

Appendix: CIS Controls v8 IG 3 Mapped Recommendations

| Recommendation | | Set Correctly | |
|----------------|---|--------------------------|--------------------------|
| | | Yes | No |
| 1.1 | (L1) Ensure device firmware is up to date | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.2 | (L1) Ensure 'Screen Lock' is set to 'Enabled' | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.4 | (L1) Ensure 'Automatically Lock' is set to 'Immediately' | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.5 | (L1) Ensure 'Power button instantly locks' is set to 'Enabled' | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.9 | (L1) Ensure 'Developer Options' is set to 'Disabled' | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.10 | (L1) Ensure 'Install unknown apps' is set to 'Disabled' | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.11 | (L1) Do not root a user device | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.12 | (L2) Ensure 'Smart Lock' is set to 'Disabled' | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.17 | (L1) Ensure 'Allow remote lock and erase' is set to 'Enabled' | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.18 | (L1) Ensure 'Scan device for security threats' is set to 'Enabled' | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.19 | (L1) Ensure 'Improve harmful app detection' is set to 'Enabled' | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.21 | (L1) Ensure 'Screen timeout' is set to '1 minute or less' | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.23 | (L1) Keep device Apps up to date | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.27 | (L1) Ensure 'Instant apps' is set to 'Disabled' | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.28 | (L1) Ensure 'Bluetooth' Pairing is Configured | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.29 | (L1) Ensure that no 3rd party keyboards are installed | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1 | (L1) Ensure 'Lock screen' is set to 'Don't show notifications at all' | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.3 | (L2) Ensure 'Back up to Google Drive' is 'Disabled' | <input type="checkbox"/> | <input type="checkbox"/> |

Appendix: CIS Controls v8 Unmapped Recommendations

| Recommendation | | Set Correctly | |
|----------------|---|--------------------------|--------------------------|
| | | Yes | No |
| 1.3 | (L1) Ensure 'Make pattern visible' is set to 'Disabled' (if using a pattern as device lock mechanism) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.6 | (L1) Ensure 'Lock Screen Message' is configured | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.7 | (L2) Do not connect to untrusted Wi-Fi networks | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.8 | (L2) Ensure 'Show passwords' is set to 'Disabled' | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.13 | (L2) Ensure 'Lock SIM card' is set to 'Enabled' | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.14 | (L2) Ensure 'Find My Device' is set to 'Enabled' | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.15 | (L1) Ensure 'Use network-provided time' and 'Use network-provided time zone' are set to 'Enabled' | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.16 | (L1) Ensure 'Remotely locate this device' is set to 'Enabled' | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.20 | (L1) Ensure 'Ask for unlock pattern/PIN/password before unpinning' is set to 'Enabled' | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.22 | (L1) Ensure 'Wi-Fi assistant' is set to 'Disabled' | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.24 | (L1) Ensure 'Add users from lock screen' is set to 'Disabled' | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.25 | (L1) Ensure 'Guest profiles' do not exist | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.26 | (L1) Review app permissions periodically | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.30 | (L1) Review existing user profiles periodically | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.2 | (L2) Ensure 'Use location' is set to 'Disabled' | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.4 | (L1) Ensure 'Web and App Activity' is set to 'Disabled' | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.5 | (L1) Ensure 'Device Information' is set to 'Disabled' | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.6 | (L1) Ensure 'Voice & Audio Activity' is set to 'Disabled' | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.7 | (L1) Ensure 'YouTube Search History' is set to 'Disabled' | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.8 | (L1) Ensure 'YouTube Watch History' is set to 'Disabled' | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.9 | (L1) Ensure 'Google Location History' is set to 'Disabled' | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.10 | (L1) Ensure 'Opt out of Ads Personalization' is set to 'Enabled' | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.1 | (L1) Ensure 'Microphone' is set to 'Enabled' | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.2 | (L1) Ensure 'Location' is set to 'Enabled' | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.3 | (L1) Ensure 'Allow third-party cookies' is set to 'Disabled' | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4 | (L1) Ensure 'Safe Browsing' is set to 'Enabled' | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.5 | (L2) Ensure 'Search and URL suggestions' is set to 'Disabled' | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.6 | (L2) Ensure 'Do Not Track' is set to 'Enabled' | <input type="checkbox"/> | <input type="checkbox"/> |

Appendix: Change History

| Date | Version | Changes for this version |
|----------|---------|---|
| 4-Apr-22 | v1.4.0 | 1.2 - UPDATE - Rationale, Impact, Audit, Remediation - Ensure 'Screen Lock' is set to 'Enabled' |
| 4-Apr-22 | v1.4.0 | 1.3 - UPDATE - Rationale, Impact, Audit, Remediation - Ensure 'Make pattern visible' is set to 'Disabled' |
| 4-Apr-22 | v1.4.0 | 1.4 - UPDATE - Rationale, Audit, Remediation - Ensure 'Automatically Lock' is set to 'Immediately' |
| 4-Apr-22 | v1.4.0 | 1.5 - UPDATE - Audit, Remediation - Ensure 'Power button instantly locks' is set to 'Enabled' |
| 4-Apr-22 | v1.4.0 | 1.6 - UPDATE - Impact, Audit, Remediation - Ensure 'Lock Screen Message' is configured |
| 4-Apr-22 | v1.4.0 | 1.7 - Update - Audit, Remediation - Do not connect to untrusted Wi-Fi networks |
| 4-Apr-22 | v1.4.0 | 1.8 - UPDATE - Rationale - Ensure 'Show passwords' is set to 'Disabled' |
| 4-Apr-22 | v1.4.0 | 1.9 - UPDATE - Rationale - Ensure 'Developer Options' is set to 'Disabled' |
| 4-Apr-22 | v1.4.0 | 1.10 - Update - Rationale - Ensure 'Install unknown apps' is set to 'Disabled' |
| 4-Apr-22 | v1.4.0 | 1.11 - UPDATE - Rationale, Impact, Audit -Do not root a user device |
| 4-Apr-22 | v1.4.0 | 1.12 - UPDATE - Rationale - Ensure 'Smart Lock' is set to 'Disabled' |
| 4-Apr-22 | v1.4.0 | 1.14 - UPDATE - Audit, Remediation - Ensure 'Find My Device' is set to 'Enabled' |
| 4-Apr-22 | v1.4.0 | 1.15 - UPDATE - Rationale - Ensure 'Use network-provided time' and 'Use network-provided time zone' are set to 'Enabled' |
| 4-Apr-22 | v1.4.0 | 1.16 - UPDATE - Audit, Remediation - Ensure 'Remotely locate this device' is set to 'Enabled' |
| 4-Apr-22 | v1.4.0 | 1.17 - UPDATE - Audit, Remediation - Ensure 'Allow remote lock and erase' is set to 'Enabled' |
| 4-Apr-22 | v1.4.0 | 1.18 - UPDATE - Audit, Remediation - Ensure 'Scan device for security threats' is set to 'Enabled' |
| 4-Apr-22 | v1.4.0 | 1.19 - UPDATE - Rationale, Impact - Ensure 'Improve harmful app detection' is set to 'Enabled' |
| 4-Apr-22 | v1.4.0 | 1.20 - UPDATE - Description, Audit, Remediation - Ensure 'Ask for unlock pattern/PIN/password before unpinning' is set to 'Enabled' |
| 4-Apr-22 | v1.4.0 | 1.21 - UPDATE - Rationale - Ensure 'Screen timeout' is set to '1 minute or less' |
| 4-Apr-22 | v1.4.0 | 1.22 - UPDATE - Rationale, Impact - Ensure 'Wi-Fi assistant' is set to 'Disabled' |
| 4-Apr-22 | v1.4.0 | 1.23 - UPDATE - Rationale - Keep device Apps up to date |

| Date | Version | Changes for this version |
|----------|---------|--|
| 4-Apr-22 | v1.4.0 | 1.24 - UPDATE - Rationale - Ensure 'Add users from lock screen' is set to 'Disabled' |
| 4-Apr-22 | v1.4.0 | 1.25 - UPDATE - Rationale - Ensure 'Guest profiles' do not exist |
| 4-Apr-22 | v1.4.0 | 1.26 - UPDATE - Rationale, Impact - Review app permissions periodically |
| 4-Apr-22 | v1.4.0 | 1.27 - UPDATE - Rationale, Impact - Ensure 'Instant apps' is set to 'Disabled' |
| 4-Apr-22 | v1.4.0 | 1.28 - ADD - Ensure 'Bluetooth' Pairing is Configured |
| 4-Apr-22 | v1.4.0 | 1.29 - ADD - Ensure that no 3rd party keyboards are installed |
| 4-Apr-22 | v1.4.0 | 1.30 - ADD - Review existing user profiles periodically |
| 4-Apr-22 | v1.4.0 | 2.1 - UPDATE - Description, Rationale, Impact - Ensure 'Lock screen' is set to 'Don't show notifications at all' |
| 4-Apr-22 | v1.4.0 | 2.2 - UPDATE - Rationale, Impact - Ensure 'Use location' is set to 'Disabled' |
| 4-Apr-22 | v1.4.0 | 2.3 - UPDATE - Rationale, Impact - Ensure 'Back up to Google Drive' is 'Disabled' |
| 4-Apr-22 | v1.4.0 | 2.4 - UPDATE - Description, Rationale, Impact - Ensure 'Web and App Activity' is set to 'Disabled' |
| 4-Apr-22 | v1.4.0 | 2.5 - UPDATE - Description, Rationale - Ensure 'Device Information' is set to 'Disabled' |
| 4-Apr-22 | v1.4.0 | 2.6 - UPDATE - Description, Rationale, Impact - Ensure 'Voice & Audio Activity' is set to 'Disabled' |
| 4-Apr-22 | v1.4.0 | 2.7 - UPDATE - Description, Rationale, Impact - Ensure 'YouTube Search History' is set to 'Disabled' |
| 4-Apr-22 | v1.4.0 | 2.9 - UPDATE - Description, Rationale, Impact - Ensure 'Google Location History' is set to 'Disabled' |
| 4-Apr-22 | v1.4.0 | 2.10 - UPDATE - Rationale, Impact, Audit, Remediation - Ensure 'Opt out of Ads Personalization' is set to 'Enabled' |
| 4-Apr-22 | v1.4.0 | 3.1 - UPDATE - Rationale, Impact, Audit, Remediation - Ensure 'Microphone' is set to 'Enabled' |
| 4-Apr-22 | v1.4.0 | 3.2 - UPDATE - Rationale, Impact, Audit Remediation - Ensure 'Location' is set to 'Enabled' |
| 4-Apr-22 | v1.4.0 | 3.3 - UPDATE - Rationale, Impact, Audit, Remediation - Ensure 'Allow third-party cookies' is set to 'Disabled' |
| 4-Apr-22 | v1.4.0 | 3.4 - UPDATE - Rationale, Impact, Audit, Remediation - Ensure 'Safe Browsing' is set to 'Enabled' |
| 4-Apr-22 | v1.4.0 | 3.5 - UPDATE - Description, Rationale, Audit, Remediation - Ensure 'Search and URL suggestions' is set to 'Disabled' |
| 4-Apr-22 | v1.4.0 | 3.6 - UPDATE - Description, Rationale, Audit, Remediation - Ensure 'Do Not Track' is set to 'Enabled' |