System

1. Minimum API level

The minimum allowed Android API level.

2. Encryption policy

Whether encryption is enabled.

Default: This value is ignored, i.e. no encryption required.

Enabled without password: Encryption required but no password required to boot.

Enabled with password: Encryption required with password required to boot.

3. Auto date and time

Whether auto date, time, and time zone is enabled on a company-owned device.

Default: Unspecified. Defaults to **User choice**.

User choice: Auto date, time, and time zone are left to user's choice.

Enforced: Enforce auto date, time, and time zone on the device.

4. Location mode

The degree of location detection enabled. The user may change the value unless the user is otherwise blocked from accessing device settings. Only apply to company-owned devices.

Default: Defaults to **User choice**.

User choice: Location setting is not restricted on the device. No specific behavior is set or enforced.

Enforced: Enable location setting on the device.

Disabled: Disable location setting on the device.

5. Developer settings

Controls access to developer settings: developer options and safe boot.

Default: Unspecified. Defaults to **Disabled**.

Disabled: Disables all developer settings and prevents the user from accessing them.

Allowed: Allows all developer settings. The user can access and optionally configure the settings.

6. Common Criteria Mode

Controls Common Criteria Mode—security standards defined in the Common Criteria for Information Technology Security Evaluation (CC). Enabling Common Criteria Mode increases certain security components on a device, including AES-GCM encryption of Bluetooth Long Term Keys, and Wi-Fi configuration stores. Warning: Common Criteria Mode enforces a strict security model typically only required for IT products used in national security systems and other highly sensitive organizations. Standard device use may be affected. Only enabled if required.

Default: Unspecified. Defaults to **Disabled**.

Disabled: Default. Disables Common Criteria Mode.

Enabled: Enables Common Criteria Mode.

7. Share location disabled

Whether location sharing is disabled for work apps. On profile-owner devices, disable location for work profile. On fully managed devices, disable location on entire device (also overriding "Location mode").

8. Create windows disabled

Whether creating windows besides app windows is disabled. This option prevents the following system UIs from being displayed: toasts and snackbars, phone activities (such as incoming calls) and priority phone activities (such as ongoing calls), system alerts, system errors and system overlays.

9. Network escape hatch

Whether the network escape hatch is enabled. If a network connection can't be made at boot time, the escape hatch prompts the user to temporarily connect to a network in order to refresh the device policy. After applying policy, the temporary network will be forgotten and the device will continue booting. This prevents being unable to connect to a network if there is no suitable network in the last policy and the device boots into an app in lock task mode, or the user is otherwise unable to reach device settings.

10. Default activities

A list of default activities for handling intents that match a particular intent filter. For example, this feature would allow IT admins to choose which browser app automatically opens web links, or which launcher app is used when tapping the home button.

10.1. Receiver activity

The activity that should be the default intent handler. This should be an Android component name, e.g. com.android.enterprise.app/.MainActivity. Alternatively, the value may be the package name of an app, which causes Android Device Policy to choose an appropriate activity from the app to handle the intent.

10.2. Action

The intent actions to match in the filter. If any actions are included in the filter, then an intent's action must be one of those values for it to match. If no actions are included, the intent action is ignored.

10.3. Category

The intent categories to match in the filter. An intent includes the categories that it requires, all of which must be included in the filter in order to match. In other words, adding a category to the filter has no impact on matching unless that category is specified in the intent.

11. Permitted input methods

Specifies permitted input methods.

> **All allowed**: No restriction applied. All input methods are allowed.
>
> **Only system's**: Only system's built-in input methods are allowed.

Only system's and provided: Only the provided and the system's built-in input methods are allowed.

11.1. Allowed input methods

Input method package names that are allowed. Only applies when **Permitted input methods** is set to **Only system's and provided**.

12. Permitted accessibility services

Specifies permitted accessibility services.

All allowed: Any accessibility service can be used.

Only system's: Only the system's built-in accessibility services can be used.

Only system's and provided: Only the provided and the system's built-in accessibility services can be used.

12.1. Allowed accessibility services

Allowed accessibility services. Only applies when **Permitted accessibility services** is set to **Only system's and provided**.

13. System update policy

Configuration for managing system updates.

Default: Follow the default update behavior for the device, which typically requires the user to accept system updates.

Automatic: Install automatically as soon as an update is available.

Windowed: Install automatically within a daily maintenance window. This also configures Play apps to be updated within the window. This is strongly recommended for kiosk devices because this is the only way apps persistently pinned to the foreground can be updated by Play.

Postpone: Postpone automatic install up to a maximum of 30 days.

14. System update freeze periods

An annually repeating time period in which over-the-air (OTA) system updates are postponed to freeze the OS version running on a device. To prevent freezing the device indefinitely, each freeze period must be separated by at least 60 days.

Revision #2
Created 28 March 2022 15:20:34 by Admin
Updated 21 March 2023 13:01:17 by Admin