System

In this section, you can configure system-related policies.

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.

> **User choice (default)**: Auto date, time, and time zone are left to user's choice.
>
> **Enforced**: Enforce auto date, time, and time zone on the device.

4. Developer settings

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

> **Disabled (default)**: 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.

5. 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 (for example: AES-GCM encryption of Bluetooth Long Term Keys, additional validation for some network certificates, and cryptographic policy integrity checks). Common Criteria Mode is supported only on company-owned devices running Android 11 or above. Warning: Common Criteria Mode enforces a strict security model typically only required for highly sensitive organizations. Standard device use may be affected; enable it only if required.

Disabled (default): Disables Common Criteria Mode.

Enabled: Enables Common Criteria Mode.

6. Memory Tagging Extension (MTE)

Controls Memory Tagging Extension (MTE) on the device.

User choice (default): The user can choose to enable or disable MTE on the device (if supported by the device).

Enforced: MTE is enabled and the user is not allowed to change it (Android 14+; supported on fully managed devices and work profiles on company-owned devices).

Disabled: MTE is disabled and the user is not allowed to change it (Android 14+; supported on fully managed devices only).

7. Content protection

Controls whether content protection (which scans for deceptive apps) is enabled. This is supported on Android 15 and above.

Disabled (default): Content protection is disabled and the user cannot change this.

Enforced: Content protection is enabled and the user cannot change this (Android 15+).

User choice: Content protection is not controlled by the policy; the user can choose (Android 15+).

8. Assist content

Controls whether AssistContent is allowed to be sent to a privileged app such as an assistant app (for example, Circle to Search). AssistContent includes screenshots and information about an app, such as package name. This is supported on Android 15 and above.

Allowed (default): Assist content is allowed to be sent to a privileged app (Android 15+).

Disallowed: Assist content is blocked from being sent to a privileged app (Android 15+).

9. 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.

10. 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.

11. 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.

Use **Add default activity** to create entries. Within an entry, use **Add action** and **Add category** to build the intent filter.

11.1. 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.

11.2. 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.

11.3. 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.

12. 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.

12.1. Allowed input methods

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

Use **Add input method** to add entries and remove them with the delete action.

13. 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.

13.1. Allowed accessibility services

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

Use **Add accessibility service** to add entries and remove them with the delete action.

14. 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.

14.1. Maintenance window (Windowed only)

When **System update policy** is set to **Windowed**, you can define the daily maintenance window using the **from** and **to** fields.

14.2. 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. Each freeze period must not exceed 90 days.

Use **Add system update freeze period** to create entries.

15. Credential providers default

Controls which apps are allowed to act as credential providers on Android 14 and above.

Disallowed (default): Apps with credentialProviderPolicy unspecified are not allowed to act as a credential provider.

Disallowed except system: Apps with credentialProviderPolicy unspecified are not allowed to act as a credential provider, except for the OEM default credential providers.

Revision #72
Created 2022-03-28 15:20:34 UTC by Admin
Updated 2026-11-12 09:52:03 UTC by Admin