

# Policies

- [Summary](#)
- [App management](#)
- [Kiosk mode](#)
- [Security](#)
- [Multimedia](#)
- [Cellular](#)
- [Networking](#)
- [System](#)
- [User management](#)
- [Personal usage](#)
- [Cross-profile policies](#)
- [Status reporting](#)
- [Misc](#)
- [Policy enforcement rules](#)

# Summary

Policies are the core entities of the system, since they define all the rules that must be applied and enforced on devices.

You can browse your policies and create new ones from the **Policies** section of the dashboard. To see the details or modify a policy, click on the selected item in the table.

A policy can be associated to an [enrollment token](#), so it will be automatically applied on devices during the provisioning process. You can also change the policy associated to a specific device after the provisioning.

Each device can be associated to only one policy at a time.

# App management

In this section you can set policies related to apps availability, installation, update and permission management.

Managed Google Play Accounts are automatically created when devices are provisioned.

## 1. Play Store mode

This mode controls which apps are available to the user in the Play Store and the behavior on the device when apps are removed from the policy.

**Whitelist (default):** Only apps that are in the policy are available and any app not in the policy will be automatically uninstalled from the device. Play Store will only shows available apps.

**Blacklist:** All apps are available and any app that should not be on the device should be explicitly marked as **blocked** in the applications policy. Play Store will shows all apps, except blocked ones.

## 2. Untrusted apps policy

The policy for untrusted apps (apps from unknown sources) enforced on the device. This option controls the Android system setting that allow if a user can install apps from outside the the Play Store (sideloading).

**Disallow (default):** Disallow untrusted app installs on entire device.

**Personal profile only:** For devices with work profiles, allow untrusted app installs in the device's personal profile only.

**Allow:** Allow untrusted app installs on entire device.

## 3. Google Play Protect

Whether Google Play Protect app verification is enforced.

**Enforced (default):** Force-enables app verification.

**User choice:** Allows the user to choose whether to enable app verification.

## 4. Default permission policy

The policy for granting runtime permission requests to apps.

**Prompt (default):** Prompt the user to grant a permission.

**Grant:** Automatically grant a permission.

**Deny:** Automatically deny a permission.

## 5. Install apps disabled

Whether user installation of apps is disabled.

## 6. Uninstall apps disabled

Whether user uninstallation of applications is disabled.

## 7. Permission policies

Explicit permission or group grants or denials for all apps. These values override the **Default permission policy** setting.

## 8. Applications

List of applications that must be included in the policy. The behavior of the list's content depends on the value set on **Play Store mode**.

If **Play Store mode** is **whitelist**, only apps that are in the policy are available and any app not in the policy will be automatically uninstalled from the device.

If **Play Store mode** is **blacklist**, all apps are available and any app that should not be on the device should be explicitly marked as **blocked** in the applications policy.

To add a new app, click on the + icon, then choose the app from Play Store and click on the **Select** button in the app card.

All apps that are published on the Play Store in your country are available for selection by default. To select your own private or web apps, you must upload them to the system first. For more information read the [Private apps](#) page.

Each app can be configured with its own settings, that are visually contained in a card:

## 8.1. Install type

The type of installation to perform for an app.

**Available:** The app is available to install.

**Preinstalled:** The app is automatically installed and can be removed by the user.

**Force installed:** The app is automatically installed and can't be removed by the user.

**Blocked:** The app is blocked and can't be installed. If the app was installed under a previous policy, it will be uninstalled.

**Required for setup:** The app is automatically installed and can't be removed by the user and will prevent setup from completion until installation is complete.

**Kiosk:** The app is automatically installed in kiosk mode: it's set as the preferred home intent and whitelisted for lock task mode. Device setup won't complete until the app is installed. After installation, users won't be able to remove the app. You can only set this **install type** for one app per policy. When this is present in the policy, status bar will be automatically disabled. For more information please read the dedicated [Kiosk mode](#) page.

## 8.2. Auto-update mode

Controls the auto-update mode for the app.

**Default:** The app is automatically updated with low priority to minimize the impact on the user. The app is updated when all of the following constraints are met: (1) the device is not actively used, (2) the device is connected to an unmetered network, (3) the device is charging. The device is notified about a new update within 24 hours after it is published by the developer, after which the app is updated the next time the constraints above are met.

**Postponed:** The app is not automatically updated for a maximum of 90 days after the app becomes out of date. 90 days after the app becomes out of date, the latest available version is installed automatically with low priority (see **Default** Auto-update mode). After the app is updated it is not automatically updated again until 90 days after it becomes out of date

again. The user can still manually update the app from the Play Store at any time.

**High priority:** The app is updated as soon as possible. No constraints are applied. The device is notified immediately about a new update after it becomes available.

### 8.3. Minimum version code

The minimum version of the app that runs on the device. If set, the device attempts to update the app to at least this version code. If the app is not up-to-date, the device will contain a **non compliance detail** with **non compliance reason** set to **APP\_NOT\_UPDATED**. The app must already be published to Google Play with a version code greater than or equal to this value. At most 20 apps may specify a minimum version code per policy.

### 8.4. Delegated scopes

The scopes delegated to the app from Android Device Policy. You can grant other apps a selection of special Android permissions:

**Certificate installation:** Grants access to certificate installation and management.

**Managed configurations:** Grants access to managed configurations management.

**Block uninstall:** Grants access to blocking uninstallation.

**Permissions:** Grants access to permission policy and permission grant state.

**Package access:** Grants access to package access state.

**System app:** Grants access for enabling system apps.

### 8.5. Default permission policy

The default policy for all permissions requested by the app. If specified, this overrides the policy-level **Default permission policy** which applies to all apps. It does not override the **Permission policies** which applies to all apps.

**Prompt (default):** Prompt the user to grant a permission.

**Grant:** Automatically grant a permission.

**Deny:** Automatically deny a permission.

### 8.6. Connected work and personal app

Controls whether the app can communicate with itself across a device's work and personal profiles, subject to user consent (Android 11+).

**Disallowed (default):** Prevents the app from communicating cross-profile.

**Allowed:** Allows the app to communicate across profiles after receiving user consent.

## 8.7. Disabled

Whether the app is disabled. When disabled, the app data is still preserved.

## 8.8. Managed configuration

To configure the app's managed settings, click on the **Enable managed configuration** button. If a managed configuration is already set for the app, you can modify the configuration with the **Managed configuration** button, or delete it with the **Remove configuration** button.

**Managed configuration** option is available only for apps that supports this functionality.

## 8.9. Permission policies

Explicit permission grants or denials for the app. These values override the **Default permission policy** and **Permission policies** which apply to all apps.

## 8.10. Track IDs

List of the app's closed testing track IDs that a device can access. If multiple track IDs are selected, devices receive the latest version among all accessible tracks. If no track IDs is selected, devices only have access to the app's production track.

**Track IDs** option is available only for apps that have at least one track ID available for your organization. For more details on how to add your organization to a closed testing track for a specific app please read [here](#).

## 9. Private key selection

Allows showing UI on a device for a user to choose a private key alias if there are no matching rules in **Choose private key rules**.

For devices below Android P, setting this may leave enterprise keys vulnerable.

## 10. Choose private key rules

Controls apps' access to private keys. The rule determines which private key, if any, Android Device Policy grants to the specified app. Access is granted either when the app calls `KeyChain.choosePrivateKeyAlias` (or any overloads) to request a private key alias for a given URL, or for rules that are not URL-specific (that is, if `urlPattern` is not set, or set to the empty string or `.*`) on Android 11 and above, directly so that the app can call `KeyChain.getPrivateKey`, without first having to call `KeyChain.choosePrivateKeyAlias`. When an app calls `KeyChain.choosePrivateKeyAlias` if more than one `choosePrivateKeyRules` matches, the last matching rule defines which key alias to return.

## 10.1. Private key alias

The alias of the private key to be used.

## 10.2. URL pattern

The URL pattern to match against the URL of the request. If not set or empty, it matches all URLs. This uses the regular expression syntax of `java.util.regex.Pattern`.

## 10.3. Package names

The package names to which this rule applies. The hash of the signing certificate for each app is verified against the hash provided by Play. If no package names are specified, then the alias is provided to all apps that call `KeyChain.choosePrivateKeyAlias` or any overloads (but not without calling `KeyChain.choosePrivateKeyAlias`, even on Android 11 and above). Any app with the same Android UID as a package specified here will have access when they call `KeyChain.choosePrivateKeyAlias`.

To delete an app, click on the **trashbin** icon, on the bottom of the app's card.



# Kiosk mode

With kiosk mode you can restrict device's functionality either to a single app or multiple apps. Choosing between single-app and multi-app kiosk mode depends on your business goals.

In **single-app kiosk mode**, a device is configured for a single application and does not allow end-users to access other apps on the device. They also cannot exit the app, making it a dedicated device for that specific app. To enable this mode, specify an app in the [App management](#) section with **Install type** set to **Kiosk**.

In **multi-app kiosk mode**, devices are allowed access to multiple applications. End-users can navigate between multiple apps through a custom launcher. To enable this mode, turn on the **Kiosk custom launcher** option.

When kiosk mode is enabled you can also configure if the end-users can access to some system functionalities, such as system settings, status bar and others.

## Kiosk custom launcher

Whether the kiosk custom launcher is enabled. This replaces the home screen with a launcher that locks down the device to the apps installed via the [App management](#) setting. Apps appear on a single page in alphabetical order.

## Power button actions

Sets the behavior of a device in kiosk mode when a user presses and holds (long-presses) the Power button.

**Default:** Unspecified, defaults to **Available**.

**Available:** The power menu (e.g. Power off, Restart) is shown when a user long-presses the Power button of a device in kiosk mode.

**Blocked:** The power menu (e.g. Power off, Restart) is not shown when a user long-presses the Power button of a device in kiosk mode. Note: this may prevent users from turning off the device.

## System error warnings

Specifies whether system error dialogs for crashed or unresponsive apps are blocked in kiosk mode. When blocked, the system will force-stop the app as if the user chooses the "close app" option on the UI.

**Default:** Unspecified, defaults to **Blocked**.

**Blocked:** All system error dialogs, such as crash and app not responding (ANR) are blocked. When blocked, the system force-stops the app as if the user closes the app from the UI.

**Enabled:** All system error dialogs such as crash and app not responding (ANR) are displayed.

## System navigation

Specifies which navigation features are enabled (e.g. Home, Overview buttons) in kiosk mode.

**Default:** Unspecified, defaults to **Disabled**.

**Enabled:** Home and overview buttons are enabled.

**Disabled:** The home and Overview buttons are not accessible.

**Home only:** Only the home button is enabled.

## Status bar

Specifies whether system info and notifications are disabled in kiosk mode.

**Default:** Unspecified, defaults to **Disabled**.

**Enabled:** System info and notifications are shown on the status bar in kiosk mode. Note: For this policy to take effect, the device's home button must be enabled using `kioskCustomization.systemNavigation`.

**Disabled:** System info and notifications are disabled in kiosk mode.

**System only:** Only system info is shown on the status bar.

## Device settings

Specifies whether the Settings app is allowed in kiosk mode.

**Default:** Unspecified, defaults to **Allowed**.

**Allowed:** Access to the Settings app is allowed in kiosk mode.

**Blocked:** Access to the Settings app is not allowed in kiosk mode.

# Security

In this section you can configure security-related policies.

## 1. Maximum time to lock

Maximum time (in seconds) for user activity until the device locks. A value of 0 means there is no restriction.

## 2. Stay on when charging

The battery plugged in modes for which the device stays on. When using this setting, it is recommended to clear **Maximum time to lock** so that the device doesn't lock itself while it stays on.

**AC charger:** Power source is an AC charger.

**USB port:** Power source is a USB port.

**Wireless charger:** Power source is wireless.

## 3. Keyguard disabled

Whether the keyguard is disabled.

## 4. Password requirements

Password requirement policies. Different policies can be set for **work profile** or **fully managed** devices by setting the **Scope** field.

### 4.1. Scope

The scope that the password requirement applies to.

**Auto:** The scope is unspecified. The password requirements are applied to the work profile for work profile devices and the whole device for fully managed or dedicated devices.

**Device:** The password requirements are only applied to the device.

**Work profile:** The password requirements are only applied to the work profile.

## 4.2. Password history length

The length of the password history. After setting this field, the user won't be able to enter a new password that is the same as any password in the history. A value of 0 means there is no restriction.

## 4.3. Maximum failed passwords for wipe

Number of incorrect device-unlock passwords that can be entered before a device is wiped. A value of 0 means there is no restriction.

## 4.4. Password expiration timeout

This setting forces the user to periodically update their password, after the specified numbers of days.

## 4.5. Require password unlock

The length of time after a device or work profile is unlocked using a strong form of authentication (password, PIN, pattern) that it can be unlocked using any other authentication method (e.g. fingerprint, trust agents, face). After the specified time period elapses, only strong forms of authentication can be used to unlock the device or work profile.

**Device's default:** The timeout period is set to the device's default.

**Every day:** The timeout period is set to 24 hours.

## 4.6. Password quality

The required password quality.

**None:** There are no password requirements.

**Weak:** The device must be secured with a low-security biometric recognition technology, at minimum. This includes technologies that can recognize the identity of an individual that are roughly equivalent to a 3-digit PIN (false detection is less than 1 in 1,000).

**Any:** A password is required, but there are no restrictions on what the password must contain.

**Numeric:** The password must contain numeric characters.

**Numeric complex:** The password must contain numeric characters with no repeating (4444) or ordered (1234, 4321, 2468) sequences.

**Alphabetic:** The password must contain alphabetic (or symbol) characters.

**Alphanumeric:** The password must contain both numeric and alphabetic (or symbol) characters.

**Complex:** The password must meet the minimum requirements specified in `passwordMinimumLength`, `passwordMinimumLetters`, `passwordMinimumSymbols`, etc. For example, if `passwordMinimumSymbols` is 2, the password must contain at least two symbols.

## 4.7. Minimum length

The minimum allowed password length. A value of 0 means there is no restriction.

## 4.8. Minimum letters

Minimum number of letters required in the password.

## 4.9. Minimum lower case letters

Minimum number of lower case letters required in the password.

## 4.10. Minimum upper case letters

Minimum number of upper case letters required in the password.

## 4.11. Minimum non letter characters

Minimum number of non-letter characters (numerical digits or symbols) required in the password.

## 4.12. Minimum numerical digits

Minimum number of numerical digits required in the password.

## 4.13. Minimum symbols

Minimum number of symbols required in the password.

# 5. Factory reset disabled

Whether factory resetting from settings is disabled. Only apply to fully managed devices.

## 6. Factory reset protection

Email addresses of device administrators for factory reset protection. When the device experiences an unauthorized factory reset, it will require one of these admins to log in with the Google account email and password to unlock the device. If no admins are specified, the device won't provide factory reset protection. Only apply to fully managed devices.

## 7. Keyguard features

Keyguard (lock screen) features that can be disabled.

### 7.1. Disable all

Disable all current and future keyguard customizations.

### 7.2. Disable camera

Disable the camera on secure keyguard screens (e.g. PIN).

### 7.3. Disable notifications

Disable showing all notifications on secure keyguard screens.

### 7.4. Disable unredacted notifications

Disable unredacted notifications on secure keyguard screens.

### 7.5. Ignore trust agent state

Ignore trust agent state on secure keyguard screens.

### 7.6. Disable fingerprint

Disable fingerprint sensor on secure keyguard screens.

### 7.7. Disable text entry into notifications

Disable text entry into notifications on secure keyguard screens.

### 7.8. Disable face authentication

Disable face authentication on secure keyguard screens.

## 7.9. Disable iris authentication

Disable iris authentication on secure keyguard screens.

## 7.10. Disable all biometric authentication

Disable all biometric authentication on secure keyguard screens.



# Multimedia

## Camera disabled

Whether all cameras on the device are disabled.

## Screen capture disabled

Whether screen capture is disabled.

## Adjust volume disabled

Whether adjusting the master volume is disabled.

## Mount physical media disabled

Whether the user mounting physical external media is disabled.

## Unmute microphone disabled

Whether the microphone is muted and adjusting microphone volume is disabled.

## USB file transfer disabled

Whether transferring files over USB is disabled.

# Cellular

## Cell broadcast config disabled

Whether configuring cell broadcast is disabled.

## Mobile networks config disabled

Whether configuring mobile networks is disabled.

## Roaming data disabled

Whether roaming data services are disabled.

## Outgoing calls disabled

Whether outgoing calls are disabled.

## SMS disabled

Whether sending and receiving SMS messages is disabled.

# Networking

IT admins can silently provision enterprise Wi-Fi configurations on managed devices. Wi-Fi configurations can also be lock down, to prevent users from creating configurations or modifying corporate configurations.

## 1. Bluetooth disabled

Whether bluetooth is disabled. Prefer this setting over `bluetoothConfigDisabled` because `bluetoothConfigDisabled` can be bypassed by the user.

## 2. Bluetooth contact sharing disabled

Whether bluetooth contact sharing is disabled.

## 3. Bluetooth config disabled

Whether configuring bluetooth is disabled.

## 4. Tethering config disabled

Whether configuring tethering and portable hotspots is disabled.

## 5. Wi-Fi config disabled

Whether configuring Wi-Fi access points is disabled.

## 6. Network reset disabled

Whether resetting network settings is disabled.

## 7. Outgoing beam disabled

Whether using NFC to beam data from apps is disabled.

## 8. Always On VPN app

Specify an Always On VPN to ensure that data from specified managed apps will always go through a configured VPN.

Note: this feature requires deploying a VPN client that supports both Always On and per-app VPN features.

## 9. VPN lockdown

Disallows networking when the VPN is not connected.

## 10. VPN config disabled

Whether configuring VPN is disabled.

## 11. Preferential network service

Controls whether preferential network service is enabled on the work profile. For example, an organization may have an agreement with a carrier that all of the work data from its employees' devices will be sent via a network service dedicated for enterprise use. An example of a supported preferential network service is the enterprise slice on 5G networks. This has no effect on fully managed devices.

**Disabled:** Preferential network service is disabled on the work profile.

**Enabled:** Preferential network service is enabled on the work profile.

## 12. Recommended global proxy

The network-independent global HTTP proxy. Typically proxies should be configured per-network in `openNetworkConfiguration`. However for unusual configurations like general internal filtering a

global HTTP proxy may be useful. If the proxy is not accessible, network access may break. The global proxy is only a recommendation and some apps may ignore it.

**Disabled**

**Direct proxy**

**Proxy auto-config (PAC)**

## 12.1 Host

The host of the direct proxy.

## 12.2 Port

The port of the direct proxy.

## 12.3. PAC URI

The URI of the PAC script used to configure the proxy.

## 12.4. Excluded hosts

For a direct proxy, the hosts for which the proxy is bypassed. The host names may contain wildcards such as \*.example.com.

# 13. WiFi configurations

Network configuration for the device.

## 13.1. Configuration name

## 13.2. SSID

## 13.3. Auto connect

Whether the network should be connected to automatically when in range.

## 13.4. Fast Transition

Indicating if the client should attempt to use Fast Transition (IEEE 802.11r-2008) with the network.

## 13.5. Hidden SSID

Indicating if the SSID will be broadcast.

## 13.6. Security

**WEP (Pre-Shared Key)**

**WPA/WPA2/WPA3-Personal (Pre-Shared Key)**

**WPA/WPA2/WPA3-Enterprise (Extensible Authentication Protocol)**

## 13.7. Passphrase

Password, for **Pre-Shared Key** security options.

## 13.8. EAP method

Extensible Authentication Protocol method

**EAP-TLS**

**EAP-TTLS**

**PEAP**

**EAP-SIM**

**EAP-AKA**

## 13.9. Phase 2 authentication

**MSCHAPv2**

**PAP**

## 13.10. EAP credentials from users

When enabled, the system will automatically apply EAP credentials on devices on a per-user basis. You can configure user's credentials in the **Users** section.

## 13.11. Client certificate

Certificate to use for authenticating devices with this WiFi network. For more information read the [Certificate management](#) section.

## 13.12. Identity

Identity of user. For tunneling outer protocols (PEAP, EAP-TTLS), this is used to authenticate inside the tunnel, and **Anonymous identity** is used for the EAP identity outside the tunnel. For non-tunneling outer protocols, this is used for the EAP identity. This value is subject to string

expansions.

### 13.13. Anonymous identity

For tunnelling protocols only, this indicates the identity of the user presented to the outer protocol. This value is subject to string expansions. If not specified, use empty string.

### 13.14. Password

Password of user. If not specified, defaults to prompting the user.

### 13.15. Server CA certificates

List of CA certificates to be used for verifying the host's certificate chain. At least one of the CA certificates must match. If not set, the client does not check that the server certificate is signed by a specific CA. A verification using the system's CA certificates may still apply. For more information read the [Certificate management](#) section.

# 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.

# User management

## Add user disabled

Whether adding new users and profiles is disabled.

## Modify accounts disabled

Whether adding or removing accounts is disabled.

## User credentials config disabled

Whether configuring user credentials is disabled.

## Remove user disabled

Whether removing other users is disabled.

## Set user icon disabled

Whether changing the user icon is disabled.

## Set wallpaper disabled

Whether changing the wallpaper is disabled.

## Blocked account types

Account types that can't be managed by the user. This option prevent device users from adding unapproved accounts.

# Personal usage

When [provisioning a company-owned device for work and personal use](#), you can specify some rules to limit how the user can operate the device for personal usage, outside the work profile.

This section only apply to company-owned devices with work profile. They will have no effect on fully managed or personally-owned devices.

## 1. Camera disabled

Whether camera is disabled.

## 2. Screen capture disabled

Whether screen capture is disabled.

## 3. Max days with work off

Controls how long the work profile can stay off.

## 4. Play Store mode

This mode controls which apps are allowed or blocked to the user in the personal profile's Play Store.

**Blocklist (default):** All apps are available and any app that should not be on the device should be explicitly marked as **Blocked** in the **Applications** section.

**Allowlist:** Only apps explicitly specified in the **Applications** section with **Install type** set to **Available** are allowed to be installed in the personal profile.

## 5. Applications

List of applications that must be allowed or blocked on the personal profile. The behavior of the list's content depends on the value set on **Play Store mode**.

To add a new app from Play Store, click on the **+** icon.

## 5.1. Install type

Types of installation behaviors a personal profile application can have.

**Blocked:** The app is blocked and can't be installed in the personal profile.

**Available:** The app is available to install in the personal profile.

## 6. Blocked account types

Account types that can't be managed by the user. This option prevent device users from adding unapproved accounts on their personal profile.

# Cross-profile policies

Only applies to devices with personal and work profiles.

## Show work contacts in personal profile

Whether contacts stored in the work profile can be shown in personal profile contact searches and incoming calls.

**Allowed (default):** Allows work profile contacts to appear in personal profile contact searches and incoming calls.

**Disallowed:** Prevents work profile contacts from appearing in personal profile contact searches and incoming calls.

## Cross-profile copy/paste

Whether text copied from one profile (personal or work) can be pasted in the other profile.

**Disallowed (default):** Prevents users from pasting into the personal profile text copied from the work profile. Text copied from the personal profile can be pasted into the work profile, and text copied from the work profile can be pasted into the work profile.

**Allowed:** Text copied in either profile can be pasted in the other profile.

## Cross-profile data sharing

Whether data from one profile (personal or work) can be shared with apps in the other profile. Specifically controls simple data sharing via intents. Management of other cross-profile communication channels, such as contact search, copy/paste, or connected work & personal apps, are configured separately.

**Disallowed:** Prevents data from being shared from both the personal profile to the work profile and the work profile to the personal profile.

**Work to Personal disallowed (default):** Prevents users from sharing data from the work profile to apps in the personal profile. Personal data can be shared with work apps.

**Allowed:** Data from either profile can be shared with the other profile.





# Status reporting

In this section you can configure which data should be retrieved from device. The status data can be consulted from the [Device status](#) dashboard page.

## Geolocation

Whether geolocation reporting is enabled.

## Application reports

Whether app reports are enabled. (Information reported about an installed app.)

This option is required by the system and can't be disabled.

## Include removed apps

Whether removed apps are included in application reports.

## Device settings

Whether device settings reporting is enabled. (Information about security related device settings on device.)

## Software info

Whether software info reporting is enabled. (Information about device software.)

## Memory info

Whether memory reporting is enabled. (An event related to memory and storage measurements.)

## Network info

Whether network info reporting is enabled. (Device network info.)

## Display info

Whether displays reporting is enabled. Report data is not available for personally-owned devices with work profiles. (Device display information.)

## Power management events

Whether power management event reporting is enabled. Report data is not available for personally-owned devices with work profiles.

## Hardware status

Whether hardware status reporting is enabled. Report data is not available for personally-owned devices with work profiles.

## System properties

Whether system properties reporting is enabled.

## Common Criteria Mode

Whether Common Criteria Mode reporting is enabled.

# Misc

## 1. Easter egg game disabled

Whether the Easter egg game in Settings is disabled.

## 2. Skip first use hints

Flag to skip hints on the first use. Enterprise admin can enable the system recommendation for apps to skip their user tutorial and other introductory hints on first start-up.

## 3. Short support message

A message displayed to the user in the settings screen wherever functionality has been disabled by the admin. If the message is longer than 200 characters it may be truncated.

## 4. Long support message

A message displayed to the user in the device administrators settings screen.

## 5. Owner lock screen info

The device owner information to be shown on the lock screen.

## 6. Setup actions

Actions to take during the setup process. During the enrollment, you can require the user to open one or more apps that are needed for device setup.

### 6.1. Launch app

Package name of app to be launched

## 6.2. Title

Provides a user-facing message, to explain to the user why the app is required to be launched.

## 6.3. Description

Provides a user-facing message, to explain to the user why the app is required to be launched.

# Policy enforcement rules

If a device or work profile fails to comply with any of the policy settings listed below, Android Device Policy immediately blocks usage of the device or work profile by default:

- **Password requirements**
- **Encryption policy**
- **Keyguard disabled**
- **Permitted input methods**
- **Permitted accessibility services**

If the device or work profile remains not compliant after 10 days, Android Device Policy will factory-reset the device or delete the work profile.

In this section you can override the default compliance enforcement rules or add new ones.

## Rules

List of rules that define the behavior when a particular policy can not be applied on device.

### Setting name

The top-level policy to enforce. For example, **Applications** or **Password requirements**.

### Block after days

Number of days the policy is non-compliant before the device or work profile is blocked. To block access immediately, set to 0. **Block after days** must be less than **Wipe after days**.

### Block scope

Specifies the scope of block action. Only applicable to devices that are company-owned.

**Work profile:** Block action is only applied to apps in the work profile. Apps in the personal profile are unaffected.

**Entire device:** Block action is applied to the entire device, including apps in the personal profile.

### Wipe after days

Number of days the policy is non-compliant before the device or work profile is wiped.

**Wipe after days** must be greater than **Block after days**.

## Preserve factory-reset protection

Whether the factory-reset protection data is preserved on the device. This setting doesn't apply to work profiles.