Policies - Android

Summary

Android policies are the core entities of the system: they define the rules that are applied and enforced on managed devices.

You can browse your policies and create new ones from the **Policies** section of the dashboard. To open an Android policy, click the policy row in the table: the system opens the **Policy Editor** page.

A policy can be associated with an enrollment token, so it will be automatically applied to devices during the provisioning process. You can also change the policy assigned to a device after provisioning.

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

> Many policy options only apply to specific device types (fully managed, dedicated, work profile) and Android versions. Unsupported settings may be ignored by the device, or reported as non-compliant.

Policy Editor layout

The Policy Editor is organized as a set of expandable sections. At the top of the page you can always edit:

- **Name** (required)
- **Id** (read-only)
- **Description** (optional)

The sections below match the Policy Editor panels (for example: App management, Security, Networking, System, Personal usage, Cross-profile policies, and more). Use the chapter pages of this manual to understand each panel in detail.

Save, delete, and associated devices

Use **Save policy** to apply your changes. The button is disabled when there are no pending edits, or when the license is expired.

If you opened an existing policy (it has an Id), the page shows a **Delete policy** action and an **Associated devices** list at the bottom, so you can see how many devices are currently using the

policy.

App management

In this section, you can set policies related to app availability, installation, updates, 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. The Play Store will only show 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. The Play Store will show 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 determines whether a user can install apps from outside the Play Store (sideloading).

> **Disallow (default)**: Disallow untrusted app installs on the 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 the 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. App functions

Controls whether apps on fully managed devices or in work profiles are allowed to expose app functions. Requires Android 16 or above.

Allowed (default): Apps on fully managed devices or in work profiles can expose app functions.

Disallowed: Apps on fully managed devices or in work profiles cannot expose app functions.

6. Install apps disabled

Whether user installation of apps is disabled.

7. Uninstall apps disabled

Whether user uninstallation of applications is disabled.

8. Permission policies

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

Use **Add permission policy** to create entries and remove them with the delete action.

Each entry includes:

Android permission/group: The Android permission or group (required), for example **android.permission.READ_CALENDAR** or **android.permission_group.CALENDAR**.

Policy: Grant / Deny / Prompt (uses the same policy options as **Default permission policy**).

9. 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 set to **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 set to **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 **Add applications** button (or the **Add applications** 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:

9.1. 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.

9.2. Install constraints

Defines a set of restrictions for the app installation. When multiple constraints are selected, all of them must be satisfied for the app to be installed.

> This option is shown only when the **Install type** is **Preinstalled** or **Force installed**.

Unmetered network: Install the app only when the device is connected to an unmetered network (e.g. Wi-Fi).

Charging: Install the app only when the device is charging.

Idle: Install the app only when the device is idle.

9.3. 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.

9.4. 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.

9.5. 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.

9.6. Preferential Network

The preferential network service to use for this app. If set, the app will use the specified enterprise network slice for its connections when available. This must match a network slice configured in the **5G Network Slicing Configuration** section of the **Cellular** panel.

9.7. 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.

9.8. 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.

9.9. Always On VPN lockdown exemption

Specifies whether the app is allowed networking when the VPN is not connected and **lockdown enabled** is active. Only supported on devices running Android 10 and above.

Enforced (default): The app respects the always-on VPN lockdown setting.

Exempt: The app is exempt from the always-on VPN lockdown setting.

9.10. Work profile widgets

Specifies whether the app installed in the work profile is allowed to add widgets to the home screen.

Allowed: The application can add widgets to the home screen.

Disallowed: The application cannot add widgets to the home screen.

9.11. User control settings

Specifies whether user control is permitted for a given app. User control includes user actions like force-stopping and clearing app data (Android 11+). If **extensionConfig** is enabled for an app, user control is disallowed regardless of this setting. For kiosk apps, you can use **Allowed** to allow user control.

Unspecified: Uses the default behavior of the app to determine if user control is allowed or disallowed.

Allowed: User control is allowed for the app.

Disallowed: User control is disallowed for the app.

9.12. Disabled

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

9.13. Allow Credential Provider

Whether the app is allowed to act as a credential provider on Android 14 and above.

9.14. 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.

9.15. 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.

Use **Add permission policy** to add one or more permission rules for the app card and remove them with the delete action.

9.16. 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.

10. Default application settings

Set default apps for supported types. When a default app is set for at least one type, users are prevented from changing default apps in that profile.

> Only one default application setting is allowed per **Default application type**. The list of default applications must not contain duplicates.

10.1. Default application type

Select the app category to configure (for example Browser, Dialer, SMS, Wallet, or Assistant). Availability depends on Android version and management mode.

10.2. Default application scopes

Select where the default app should apply (Fully managed, Work profile, or Personal profile). Only scopes supported by the selected type can be chosen.

> If none of the selected scopes are applicable to the device’s management mode, the device reports a non-compliance detail.

10.3. Default applications

List of apps that can be set as default for the selected type. The first installed and eligible app is set as the default.

> If scopes include **Fully managed** or **Work profile**, each app must also exist in the **Applications** list with **Install type** not set to **Blocked**.

11. 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.

12. 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.

Use **Add private key rule** to create entries and remove them with the delete action.

12.1. Private key alias

The alias of the private key to be used.

12.2. 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.

12.3. 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.

Use **Add package name** to add entries and remove them with the delete action.

> 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 a device's functionality 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 whether end users can access certain system features, such as system settings and the status bar.

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.

> **Available (default)**: 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.

Blocked (default): 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.

Disabled (default): The home and Overview buttons are not accessible.

Home only: Only the home button is enabled.

Enabled: Home and overview buttons are enabled.

Status bar

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

Disabled (default): System info and notifications are disabled in kiosk mode.

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

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.

Device settings

Specifies whether the Settings app is allowed in kiosk mode.

Allowed (default): 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.

Security risk actions

Choose what to do when a device reports a SecurityRisk in status reports.

Supported SecurityRisk types:

Unknown OS: Play Integrity API detects that the device is running an unknown OS (basicIntegrity check succeeds but ctsProfileMatch fails).

Compromised OS: Play Integrity API detects that the device is running a compromised OS (basicIntegrity check fails).

Hardware-backed evaluation failed: Play Integrity API detects that the device does not have a strong guarantee of system integrity, if the MEETS_STRONG_INTEGRITY label doesn't show in the device integrity field.

Available actions:

Wipe corporate data (default): Disenroll and wipe work data (entire device if fully managed, or only work profile for profile-owned).

No action: Leave the device enrolled and do nothing automatically.

When you select **Wipe corporate data**, you can also configure wipe options:

Preserve factory-reset protection: Preserve Factory Reset Protection (FRP) data when wiping the device.

Wipe external storage: Additionally wipe the device's external storage (such as SD cards) when performing the wipe.

Wipe eSIMs: For company-owned devices, this removes all eSIMs from the device when the device is wiped. In personally-owned devices, this will remove managed eSIMs (eSIMs which

are added via the ADD_ESIM command) on the devices and no personally owned eSIMs will be removed.

1. Max 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

If true, this disables the Lock Screen for primary and/or secondary displays. This policy is supported only in dedicated device management mode.

4. Password requirements

Password requirement policies.

Use **Configure Password Requirements** to add one or more password requirement blocks. Use **Clear All** to remove all configured password requirements.

Password requirements can use **Auto** scope (single requirement) or separate **Device**/**Work profile** scopes. Complexity-based requirements must be coupled with quality-based requirements for the same scope.

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. Max 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 (days)

This setting forces the user to periodically update their password, after the specified number 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.

Complexity high: Define the high password complexity band as: On Android 12 and above: PIN with no repeating (4444) or ordered (1234, 4321, 2468) sequences, length at least 8; alphabetic, length at least 6; alphanumeric, length at least 6.

Complexity medium: Define the medium password complexity band as: PIN with no repeating (4444) or ordered (1234, 4321, 2468) sequences, length at least 4; alphabetic, length at least 4; alphanumeric, length at least 4.

Complexity low: Define the low password complexity band as: pattern; PIN with repeating (4444) or ordered (1234, 4321, 2468) sequences.

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.

4.14. Unified lock

Controls whether a unified lock is allowed for the device and the work profile, on devices running Android 9 and above with a work profile. This has no effect on other devices.

> **Allow unified lock**: A common lock for the device and the work profile is allowed.
>
> **Require separate work lock**: A separate lock for the work profile is required.

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.

Administrator emails: use **Enable Factory Reset Protection** to start configuring administrators. Then use **Add administrator email** to add addresses and remove them with the delete action.

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.

7.11. Disable all shortcuts

Disable all shortcuts on secure keyguard screen on Android 14 and above.

Multimedia

In this section, you can configure camera/microphone behavior, USB data access, printing, and display-related restrictions.

1. Camera access

Controls the use of the camera and whether the user can access the camera access toggle (Android 12+). In general, disabling the camera applies device-wide on fully managed devices, and only inside the work profile on work profile devices.

> **User choice (default)**: Default device behavior. Cameras are available and (Android 12+) the user can toggle camera access.
>
> **Disabled**: All cameras are disabled (fully managed: device-wide; work profile: only for work profile apps). The camera access toggle has no effect in the managed scope.
>
> **Enforced**: Cameras are available. On fully managed devices running Android 12+, the user cannot toggle camera access. On other devices/versions this behaves like User choice.

2. Microphone access

On fully managed devices, controls the use of the microphone and whether the user can access the microphone access toggle (Android 12+). This setting has no effect on devices that are not fully managed.

> **User choice (default)**: Default behavior. Microphone is available and (Android 12+) the user can toggle microphone access.
>
> **Disabled**: Microphone is disabled (device-wide). The microphone access toggle has no effect.
>
> **Enforced**: Microphone is available. On Android 12+, the user cannot toggle microphone access. On Android 11 or below, this behaves like User choice.

3. USB data access

Controls what files and/or data can be transferred via USB. Supported only on company-owned devices.

Disallow file transfer (default): File transfers are disallowed, but other USB data connections (e.g. mouse/keyboard) are allowed.

Disallow data transfer: All types of USB data transfers are prohibited (Android 12+ with USB HAL 1.3+). If unsupported, the device falls back to Disallow file transfer.

Allow data transfer: All types of USB data transfers are allowed.

4. Printing

Controls whether printing is allowed (Android 9+).

Allowed (default): Printing is allowed.

Disallowed: Printing is disallowed (Android 9+).

5. Screen brightness settings

Controls the screen brightness mode and (optionally) the brightness value.

Screen brightness mode:

User choice (default): The user is allowed to configure screen brightness.

Automatic: Brightness is automatic and the user cannot change it. You can still set a brightness value, which is used as part of automatic adjustment (fully managed Android 9+; work profiles on company-owned Android 15+).

Fixed: Brightness is set to the configured value and the user cannot change it. The brightness value is required (fully managed Android 9+; work profiles on company-owned Android 15+).

Screen brightness:

Value from 1 to 255 (1 = lowest, 255 = highest). A value of 0 means no brightness value is set.

6. Screen timeout settings

Controls whether the user can configure the screen timeout and, when enforced, the timeout value.

The **Screen timeout mode** field selects between user-controlled and enforced behavior.

User choice (default): The user is allowed to configure the screen timeout.

Enforced: Screen timeout is set to the configured value and the user cannot change it (fully managed Android 9+; work profiles on company-owned Android 15+).

Screen timeout:

Timeout duration in seconds. The value must be greater than 0. If it is greater than **Maximum time to lock**, the system may clamp it and report non-compliance.

7. Screen capture disabled

Whether screen capture is disabled.

8. Adjust volume disabled

Whether adjusting the master volume is disabled.

9. Mount physical media disabled

Whether mounting physical external media is disabled.

Cellular

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

1. Airplane mode

Controls whether airplane mode can be toggled by the user or not.

> **User choice (default)**: The user is allowed to toggle airplane mode on or off.
>
> **Disabled**: Airplane mode is disabled. The user is not allowed to toggle airplane mode on. Supported on Android 9 and above.

2. Cellular 2G

Controls whether cellular 2G setting can be toggled by the user or not.

> **User choice (default)**: The user is allowed to toggle cellular 2G on or off.
>
> **Disabled**: Cellular 2G is disabled. The user is not allowed to toggle cellular 2G on via settings. Supported on Android 14 and above.

3. Override APNs

Controls whether override APNs are enabled or disabled. When enabled, only the configured override APNs are used and all other APNs on the device are ignored.

> **Disabled (default)**: All configured APN settings are saved on the device, but they are disabled and have no effect. All other APNs on the device remain in use.
>
> **Enabled**: Only the override APNs are used, all other APNs are ignored. This setting can only be configured on fully managed devices with Android 10 and above.

4. APN settings

Configure one or more APN entries. Use **Add APN** to create an entry and **Remove APN** to delete it.

Each APN has required fields:

APN Types: Select one or more traffic types for this APN (availability depends on management mode and Android version).

APN Name: The APN identifier provided by your carrier.

Display Name: Friendly name shown in UI.

Optional APN fields:

Auth Type, **Username**, **Password**: Configure carrier authentication (if required).

Protocol and **Roaming Protocol**: IP protocol configuration.

Network Types: Restrict the cellular technologies the APN may use (for example LTE/5G NR).

Proxy Address and **Proxy Port**: HTTP proxy for data traffic (if applicable).

MMS Proxy Address, **MMS Proxy Port**, **MMSC (MMS Center URI)**: MMS-related settings.

Numeric Operator ID (MCC+MNC) and **Carrier ID**: Carrier identification fields.

Always On Setting: Whether the PDU session activated by this APN should be always-on. Supported on Android 15 and above.

MVNO Type: Mobile virtual network operator identifier type.

MTU IPv4 and **MTU IPv6**: Maximum Transmission Unit for IPv4/IPv6 routes. Supported on Android 13 and above.

5. Cell broadcast config disabled

Whether configuring cell broadcast is disabled.

6. Mobile networks config disabled

Whether configuring mobile networks is disabled.

7. Roaming data disabled

Whether roaming data services are disabled.

8. Outgoing calls disabled

Whether outgoing calls are disabled.

9. SMS disabled

Whether sending and receiving SMS messages is disabled.

10. 5G Network Slicing Configuration

Configure preferential network service settings to enable enterprise 5G network slicing. You can set up to 5 enterprise slices and assign applications to specific networks for optimized traffic routing.

10.1. Default Preferential Network

Default preferential network ID for applications that are not in the applications list, or if an app's **Preferential Network** is not set. Must have a configuration for the specified network ID (unless set to **No Preferential Network**).

Note: Critical apps like **com.google.android.apps.work.clouddpc** and **com.google.android.gms** are excluded from this default setting.

10.2. Network Service Configurations

Use **Add Network Configuration** to create a slice configuration. You can add up to 5 configurations. Each configuration has:

> **Preferential Network ID (Auto-assigned)**: Network ID is automatically assigned and cannot be changed.
>
> **Fallback to Default Connection**: Whether fallback to the device-wide default network is allowed. If disallowed, apps cannot access the internet if the 5G slice is unavailable.
>
> **Non-Matching Networks**: Whether apps subject to this configuration can use networks other than the preferential service. If set to **Disallowed**, **Fallback to Default Connection** must also be **Disallowed**. Requires Android 14 and above.

Networking

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

> Wi-Fi configurations can be provisioned and managed by the system via **WiFi configurations**. Depending on the value set on **Configure Wi-Fi**, users may have limited or no control over adding/modifying networks.

Device radio state

1. Wi?Fi state

Controls current state of Wi-Fi and if the user can change its state.

User choice (default): User is allowed to enable/disable Wi-Fi.

Enabled: Wi-Fi is on and the user is not allowed to turn it off (Android 13+).

Disabled: Wi-Fi is off and the user is not allowed to turn it on (Android 13+).

2. Minimum Wi?Fi security level

The minimum required security level of Wi-Fi networks that the device can connect to. Supported on Android 13 and above, for fully managed devices and work profiles on company-owned devices.

Open network (default): The device can connect to all types of Wi-Fi networks.

Personal network: Disallows open Wi-Fi networks; requires at least personal security (for example WPA2-PSK).

Enterprise network: Requires enterprise EAP networks; disallows Wi-Fi networks below this security level.

192-bit enterprise network: Requires 192-bit enterprise networks; strictest option.

3. Ultra wideband (UWB) state

Controls the state of the ultra wideband setting and whether the user can toggle it on or off.

User choice (default): The user is allowed to toggle UWB on or off.

Disabled: UWB is disabled and the user is not allowed to toggle it via settings (Android 14+).

Device connectivity management

4. Bluetooth sharing

Controls whether Bluetooth sharing is allowed.

Allowed: Bluetooth sharing is allowed (default on fully managed devices, Android 8+).

Disallowed: Bluetooth sharing is disallowed (default on work profiles, Android 8+).

5. Configure Wi?Fi

Controls Wi-Fi configuring privileges. Depending on the selected option, the user has full, limited, or no control in configuring Wi-Fi networks.

Allow configuring Wi-Fi (default): The user is allowed to configure Wi-Fi.

Disallow add Wi-Fi config: Adding new Wi-Fi configurations is disallowed. The user can switch between already configured networks (Android 13+; fully managed and company-owned work profiles).

Disallow configuring Wi-Fi: Disallows configuring Wi-Fi networks. For fully managed devices this removes user-configured networks and retains only networks configured via **WiFi configurations**. For company-owned work profiles, existing networks are not affected but users cannot add/remove/modify Wi-Fi networks.

> When configuring Wi-Fi is disabled and the device cannot connect at boot time, the system can show the **network escape hatch** to let the user temporarily connect and refresh policy.

6. Wi?Fi direct settings

Controls configuring and using Wi-Fi direct settings. Supported on company-owned devices running Android 13 and above.

Allow (default): The user is allowed to use Wi-Fi direct.

Disallow: The user is not allowed to use Wi-Fi direct.

7. Tethering settings

Controls tethering settings. Based on the value set, the user is partially or fully disallowed from using different forms of tethering.

Allow all tethering (default): Allows configuration and use of all forms of tethering.

Disallow Wi-Fi tethering: Disallows the user from using Wi-Fi tethering (company-owned Android 13+).

Disallow all tethering: Disallows all forms of tethering (fully managed + company-owned work profiles).

8. Wi?Fi SSID policy

Restrictions on which Wi-Fi SSIDs the device can connect to (this does not affect which networks can be configured on the device). Supported on company-owned devices running Android 13 and above.

SSID denylist (default): The device cannot connect to any Wi-Fi network whose SSID is listed, but can connect to other networks.

SSID allowlist: The device can connect only to the SSIDs listed. The SSID list must not be empty.

Use **Add SSID** to add entries. Depending on the selected policy type, the list is interpreted as allowed or denied SSIDs.

In the Policy Editor UI, the SSID list is labeled **Allowed Wi-Fi SSIDs** for allowlists and **Denied Wi-Fi SSIDs** for denylists.

9. Wi?Fi roaming settings

Configure Wi-Fi roaming mode per SSID. Use **Add Wi-Fi roaming setting** to create entries.

Each entry includes:

SSID: The SSID to which the roaming setting applies (required).

Wi-Fi roaming mode: Default / Disabled / Aggressive. Disabled and Aggressive require Android 15+ and are supported only on fully managed devices and work profiles on company-owned devices.

Network restrictions

10. Bluetooth disabled

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

11. Bluetooth contact sharing disabled

Whether bluetooth contact sharing is disabled.

12. Bluetooth config disabled

Whether configuring bluetooth is disabled.

13. Network reset disabled

Whether resetting network settings is disabled.

14. Outgoing beam disabled

Whether using NFC to beam data from apps is disabled.

VPN

15. Always On VPN app

Specify an Always On VPN package name 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.

16. VPN lockdown

Disallows networking when the VPN is not connected.

17. VPN config disabled

Whether configuring VPN is disabled.

Proxy and network services

18. 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 work data is sent via a carrier network service dedicated for enterprise use (for example, an 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.

> If you use enterprise network slicing, also configure **5G Network Slicing Configuration** under the **Cellular** policy panel and assign apps to a slice using their **Preferential Network** setting.

19. Recommended global proxy

The network-independent global HTTP proxy. Typically, proxies should be configured per-network in WiFi configurations. A global proxy may be useful for unusual configurations like general internal filtering. The global proxy is only a recommendation and some apps may ignore it.

Disabled

Direct proxy

Proxy auto-config (PAC)

19.1. Host

The host of the direct proxy.

19.2. Port

The port of the direct proxy.

19.3. PAC URI

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

19.4. Excluded hosts

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

Use **Add excluded host** to add entries (available for direct proxy only).

WiFi configurations

Define Wi-Fi network configurations that the system will apply on devices. Use **Add Wi-Fi configuration** to create an entry and remove it with the delete action.

20. Wi?Fi configuration fields

Each configuration includes:

Configuration name: Required.

SSID: Required.

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

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

Hidden SSID: Whether the SSID will be broadcast.

MAC randomization mode: Hardware or Automatic (Android 13+).

20.1. Security

Wi-Fi security options:

WEP-PSK: WEP (Pre-Shared Key).

WPA-PSK: WPA/WPA2/WPA3-Personal (Pre-Shared Key).

WPA-EAP: WPA/WPA2/WPA3-Enterprise (Extensible Authentication Protocol).

WPA3 192-bit mode: WPA-EAP network allowing only WPA3 192-bit mode.

20.2. Passphrase (Pre?Shared Key)

Shown when Security is **WEP-PSK** or **WPA-PSK**. The passphrase is required.

20.3. EAP method (Enterprise)

Shown when Security is **WPA-EAP** or **WPA3 192-bit mode**. Select one EAP outer method:

EAP-TLS

EAP-TTLS

PEAP

EAP-SIM

EAP-AKA

20.4. Phase 2 authentication

Shown for tunneling outer methods (**EAP-TTLS** and **PEAP**).

MSCHAPv2

PAP

20.5. EAP credentials from users

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

20.6. Client certificate

For **EAP-TLS**, you can assign a client certificate used for Wi-Fi authentication. For more information read the **Certificate management** page.

If a certificate is already assigned, you can use **Open certificate** to view it or **Change certificate** to select a different one.

Alternatively, you can specify **Client certificate key pair alias**, which references a client certificate stored in the Android keychain and allowed for Wi-Fi authentication.

> If both **Client certificate** and **Client certificate key pair alias** are set, the key pair alias is ignored.

20.7. 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.

20.8. Anonymous identity

For tunneling protocols only, this indicates the identity of the user presented to the outer protocol.

20.9. Password

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

20.10. Server CA certificates

List of CA certificates to be used for verifying the host’s certificate chain. At least one CA certificate must match. For more information read the **Certificate management** page.

Use **Add Server CA certificate** to add entries and remove them with the delete action.

20.11. Domain suffix matches

A list of constraints for the server domain name. The entries are used as suffix match requirements against the DNS name(s) of the alternative subject name of an authentication server certificate.

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.

Location and geofence

This panel groups the Android policy settings that control device location reporting, location enforcement, and geofence definitions. Use it when you want Cerberus Enterprise to collect device locations or detect when devices enter or leave configured areas.

Location reporting

Report location

Enables device geolocation reporting. Location data collected through this setting is used by the **dashboard location map**, the device overview location history, and geofence processing.

> On devices that are not fully managed, location data may still depend on the Cerberus Enterprise app having the required location permissions and on location services being enabled on the device.

Location mode

Controls the device location setting on company-owned devices.

- **User choice**: location services are not restricted by the policy.
- **Enforced**: location services are enabled on the device.
- **Disabled**: location services are disabled on the device.

Share location disabled

Disables location sharing for work apps. On profile-owner devices, this affects the work profile. On fully managed devices, it disables location for the whole device and overrides the device location mode.

Automatic behavior with active geofences

Active geofences require location reporting to work. When at least one geofence is active, Cerberus Enterprise automatically keeps the related location settings consistent.

- **Report location** is forced on while active geofences exist.
- **Location mode** is forced to **Enforced**.
- **Share location disabled** is forced off.

If you try to disable **Report location** while one or more geofences are active, Cerberus Enterprise shows a confirmation dialog. If you continue, all active geofences in the policy are deactivated.

Geofence list

A policy can contain up to **10 geofences**. Geofence names must be unique within the policy.

Use **Add geofence** to create a new entry. Each geofence contains these main fields:

- **Name**: required and unique.
- **Latitude** and **Longitude**: the center of the area.
- **Radius (m)**: required, from **100** to **10000** meters.
- **Description**: optional notes for administrators.
- **Report enter** and **Report exit**: choose which transition events should be generated.
- **Active**: enables or disables the geofence without deleting it.

> At least one of **Report enter** or **Report exit** must stay enabled for each geofence.

Map editing tools

Each geofence card includes a map preview of the area. You can edit the geometry from the map or from the numeric fields.

- Click the map to move the geofence center when area editing is unlocked.
- Use the **Current location** button to center the map on your current browser position.
- Use the **Recenter map** button to restore the preferred viewport for that geofence.
- Use the lock button to prevent accidental changes to the geofence geometry.

Where geofence data appears

Geofence transitions can be reviewed in the Android **Device overview** page, inside the **Geofence** tab of the location panel. That tab shows transitions on a dedicated map together with filtering tools and the transition list.

User management

Add user disabled

Whether adding new users and profiles is disabled. For devices where managementMode is **DEVICE_OWNER** this field is ignored and the user is never allowed to add or remove users.

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.

Work account setup authentication

Controls how users authenticate during work account setup. This option is available only for Android enterprises backed by a managed Google domain (Google Workspace).

During device setup/enrollment, this policy influences whether a work account sign-in is required, but the Google Admin Console setting **Authenticate Using Google** and the enrollment token type

can still require authentication.

For already enrolled devices, this policy only applies if the device is managed by a managed Google Play account (i.e., enrolled without **Authenticate Using Google Enrollment**).

For more details and troubleshooting, refer to **Authenticate Using Google enrollment**.

Blocked account types

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

Use **Add blocked account type** to add one or more account types.

Each entry has an **Account type** field (required). Enter a string such as **com.google**. Remove an entry using the delete action.

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 personale usage, outside the work profile.

> This section only apply to company-owned devices with work profile. They will have no effect on fully manged 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. Bluetooth sharing

Controls whether bluetooth sharing is allowed in the personal profile of a company-owned device with a work profile.

5. Private space

Controls whether a private space is allowed on the device.

6. 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.

7. 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.

7.1. 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.

8. 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.

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.
>
> **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.

Work profile widgets default

Default behavior for work profile widgets. If a specific app does not define a widgets policy, it follows the default set here.

Cross-profile app functions

Controls whether personal profile apps can invoke app functions from work profile apps. This requires Android 16 or above.

>

> This setting depends on the policy-level**App functions** option (in the App management section). If App functions is set to **Disallowed**, the API will reject Cross-profile app functions set to **Allowed**.

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 the personal profile.

Disallowed: Prevents personal apps from accessing work profile contacts and looking up work contacts.

Disallowed except system: Prevents most personal apps from accessing work profile contacts, except for the OEM default Dialer, Messages, and Contacts apps (Android 14+).

When Work contacts in personal profile is configured, you can optionally define a list of **Exempted package name** entries. Depending on the selected mode, these exemptions behave as allowlist or blocklist for personal apps.

Status reporting

In this section, you can configure which data should be retrieved from the device. The status data can be viewed in the **Device status** dashboard page.

Application reports

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

> This option is required by the system (for companion-app integration) and is always enabled; it 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.

Use **Add setup action** to create entries and remove them with the delete action.

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.

7. Enterprise display name visibility

Controls whether the enterprise display name is visible on the device (for example, as a lock screen message on company-owned devices).

Visible (default): The enterprise display name is visible on the device (supported on work profiles on Android 7+ and fully managed devices on Android 8+).

Hidden: The enterprise display name is hidden on the device.

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 cannot be applied to a device.

Use **Add rule** to create a new rule. Each rule card can be removed using the delete action.

Setting name

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

Required. The value must match a supported top-level policy name; otherwise the field is marked as invalid.

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**. Only applicable to devices that are company-owned.

Allowed range: 0–300.

Block scope

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

Default (new rule): **Work profile**.

> **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**. Only applicable to devices that are company-owned.

Required. Default (new rule): **1**.

Allowed range: 1–300.

Preserve factory-reset protection

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

Default (new rule): enabled.