Prefix is android.permission unless written otherwise.

Some information found [here](https://github.com/aosp-mirror/platform_frameworks_base/blob/master/core/res/AndroidManifest.xml).

Removed

USE\_CREDENTIALS

Deprecated in API level 23.

MANAGE\_ACCOUNTS

Deprecated in API level 23.

READ\_PROFILE

Deprecated in API level 23.

AUTHENTICATE\_ACCOUNTS

Deprecated in API level 23.

FLASHLIGHT

Deprecated in API level 24.

WRITE\_SMS

Deprecated in API level 23.

READ\_HISTORY\_BOOKMARKS

READ\_USER\_DICTIONARY

Deprecated in API level 23.

WRITE\_USER\_DICTIONARY

Deprecated in API level 23.

SUBSCRIBED\_FEEDS\_READ

SUBSCRIBED\_FEEDS\_WRITE

com.android.browser.permission.READ\_HISTORY\_BOOKMARKS

Deprecated in API level 23.

com.android.browser.permission.WRITE\_HISTORY\_BOOKMARKS

Deprecated in API level 23.

Dangerous

Dangerous permissions cover areas where the app wants data or resources that involve the user's private information, or could potentially affect the user's stored data or the operation of other apps. For example, the ability to read the user's contacts is a dangerous permission. If an app declares that it needs a dangerous permission, the user has to explicitly grant the permission to the app.

[android.app.action.DEVICE\_ADMIN\_ENABLED](https://developer.android.com/guide/topics/admin/device-admin)

I am categorizing this permission as dangerous based on Android’s description of how the Android Device Administration API can be used:

* “These APIs allow you to create security-aware apps that are useful in enterprise settings, in which IT professionals require rich control over employee devices.”
* “Here are examples of the types of apps that might use the Device Administration API:
  + Email clients.
  + Security apps that do remote wipe.
  + Device management services and apps.”

ACCESS\_BACKGROUND\_LOCATION

Allows an app to access location in the background.

ACCESS\_COARSE\_LOCATION

Allows an app to access approximate location.

ACCESS\_FINE\_LOCATION

Allows an app to access precise location.

ACCESS\_MEDIA\_LOCATION

Allows an application to access any geographic locations persisted in the user's shared collection.

ACTIVITY\_RECOGNITION

Allows an application to recognize physical activity.

[ACCESS\_SUPERUSER](https://www.sitepoint.com/developers-guide-risky-android-app-permissions/)

Allows root access.

* Deprecated in API level 22.

CALL\_PHONE

Allows an application to initiate a phone call without going through the Dialer user interface for the user to confirm the call.

CAMERA

Required to be able to access the camera device.

GET\_ACCOUNTS

Allows access to the list of accounts in the Accounts Service.

PROCESS\_OUTGOING\_CALLS

Allows an application to see the number being dialed during an outgoing call with the option to redirect the call to a different number or abort the call altogether.

* This constant was deprecated in API level 29. Applications should use CallRedirectionService instead of the Intent.ACTION\_NEW\_OUTGOING\_CALL broadcast.

READ\_CALENDAR

Allows an application to read the user's calendar data.

READ\_CALL\_LOG

Allows an application to read the user's call log.

READ\_CONTACTS

Allows an application to read the user's contacts data.

READ\_EXTERNAL\_STORAGE

Allows an application to read from external storage.

READ\_PHONE\_NUMBERS

Allows read access to the device's phone number(s).

READ\_PHONE\_STATE

Allows read only access to phone state, including the current cellular network information, the status of any ongoing calls, and a list of any PhoneAccounts registered on the device.

READ\_SMS

Allows an application to read SMS messages.

RECEIVE\_MMS

Allows an application to monitor incoming MMS messages.

RECEIVE\_SMS

Allows an application to receive SMS messages.

RECORD\_AUDIO

Allows an application to record audio.

SEND\_SMS

Allows an application to send SMS messages.

WRITE\_CALENDAR

Allows an application to write the user's calendar data.

WRITE\_CALL\_LOG

Allows an application to write (but not read) the user's call log data.

WRITE\_CONTACTS

Allows an application to write the user's contacts data.

WRITE\_EXTERNAL\_STORAGE

Allows an application to write to external storage.

Normal

ACCESS\_NETWORK\_STATE

Allows applications to access information about networks.

ACCESS\_NOTIFICATION\_POLICY

Marker permission for applications that wish to access notification policy.

ACCESS\_WIFI\_STATE

Allows applications to access information about Wi-Fi networks.

BLUETOOTH

Allows applications to connect to paired bluetooth devices.

BLUETOOTH\_ADMIN

Allows applications to discover and pair bluetooth devices.

BROADCAST\_STICKY

Allows an application to broadcast sticky intents.

CHANGE\_NETWORK\_STATE

Allows applications to change network connectivity state.

CHANGE\_WIFI\_MULTICAST\_STATE

Allows applications to enter Wi-Fi Multicast mode.

CHANGE\_WIFI\_STATE

Allows applications to change Wi-Fi connectivity state.

DISABLE\_KEYGUARD

Allows applications to disable the keyguard if it is not secure.

DOWNLOAD\_WITHOUT\_NOTIFICATION

Allows to queue downloads without a notification shown while the download runs.

FOREGROUND\_SERVICE

Allows a regular application to use Service.startForeground.

GET\_PACKAGE\_SIZE

Allows an application to find out the space used by any package.

GET\_TASKS

* This constant was deprecated in API level 21. No longer enforced.

com.android.launcher.permission.INSTALL\_SHORTCUT

Allows an application to install a shortcut in Launcher.

* In Android O (API level 26) and higher, the INSTALL\_SHORTCUT broadcast no longer has any effect on your app because it's a private, implicit broadcast.

INTERNET

Allows applications to open network sockets.

KILL\_BACKGROUND\_PROCESSES

Allows an application to call ActivityManager.killBackgroundProcesses(String).

MANAGE\_OWN\_CALLS

Allows a calling application which manages its own calls through the self-managed ConnectionService APIs.

MODIFY\_AUDIO\_SETTINGS

Allows an application to modify global audio settings.

NFC

Allows applications to perform I/O operations over NFC.

PERSISTENT\_ACTIVITY

Allow an application to make its activities persistent.

* This constant was deprecated in API level 15. This functionality will be removed in the future; please do not use.

READ\_SYNC\_SETTINGS

Allows applications to read the sync settings.

READ\_SYNC\_STATS

Allows applications to read the sync stats.

RECEIVE\_BOOT\_COMPLETED

Allows an application to receive the Intent.ACTION\_BOOT\_COMPLETED that is broadcast after the system finishes booting.

REORDER\_TASKS

Allows an application to change the Z-order of tasks.

REQUEST\_DELETE\_PACKAGES

Allows an application to request deleting packages.

REQUEST\_IGNORE\_BATTERY\_OPTIMIZATIONS

Permission an application must hold in order to use Settings.ACTION\_REQUEST\_IGNORE\_BATTERY\_OPTIMIZATIONS.

RESTART\_PACKAGES

* This constant was deprecated in API level 15. The ActivityManager.restartPackage(String) API is no longer supported.

SET\_ALARM

Allows an application to broadcast an Intent to set an alarm for the user.

com.android.launcher.permission.UNINSTALL\_SHORTCUT

* Don't use this permission in your app.

USE\_BIOMETRIC

Allows an app to use device supported biometric modalities.

USE\_FINGERPRINT

Allows an app to use fingerprint hardware.

* This constant was deprecated in API level 28. Applications should request USE\_BIOMETRIC instead

USE\_FULL\_SCREEN\_INTENT

Required for apps targeting Build.VERSION\_CODES.Q that want to use notification full screen intents.

VIBRATE

Allows access to the vibrator.

WAKE\_LOCK

Allows using PowerManager WakeLocks to keep processor from sleeping or screen from dimming.

WRITE\_SYNC\_SETTINGS

Allows applications to write the sync settings.

Signature

The system grants these app permissions at install time, but only when the app that attempts to use a permission is signed by the same certificate as the app that defines the permission. Note: Some signature permissions aren't for use by third-party apps.

BATTERY\_STATS

Allows an application to collect battery statistics.

BIND\_ACCESSIBILITY\_SERVICE

Must be required by an AccessibilityService, to ensure that only the system can bind to it.

BIND\_DEVICE\_ADMIN

Must be required by device administration receiver, to ensure that only the system can interact with it.

BIND\_NOTIFICATION\_LISTENER\_SERVICE

Must be required by an NotificationListenerService, to ensure that only the system can bind to it.

CAPTURE\_AUDIO\_OUTPUT

Allows an application to capture audio output. Use the CAPTURE\_MEDIA\_OUTPUT permission if only the USAGE\_UNKNOWN), USAGE\_MEDIA) or USAGE\_GAME) usages are intended to be captured.

CHANGE\_CONFIGURATION

Allows an application to modify the current configuration, such as locale.

INTERACT\_ACROSS\_USERS

Allows an application to call APIs that allow it to do interactions across the users on the device, using singleton services and user-targeted broadcasts. This permission is not available to third party applications.

INTERACT\_ACROSS\_USERS\_FULL

Fuller form of INTERACT\_ACROSS\_USERS that removes restrictions on where broadcasts can be sent and allows other types of interactions

MANAGE\_DEVICE\_ADMINS

@SystemApi Required to add or remove another application as a device admin. Not for use by third-party applications.

MANAGE\_DOCUMENTS

Allows an application to manage access to documents, usually as part of a document picker.

MANAGE\_USERS

@SystemApi Allows an application to call APIs that allow it to query and manage users on the device. This permission is not available to third party applications.

MODIFY\_PHONE\_STATE

Allows modification of the telephony state - power on, mmi, etc.

OVERRIDE\_WIFI\_CONFIG

@SystemApi Allows an application to modify any wifi configuration, even if created by another application. Once reconfigured the original creator cannot make any further modifications. Not for use by third-party applications.

PACKAGE\_USAGE\_STATS

Allows an application to collect component usage statistics

* Declaring the permission implies intention to use the API and the user of the device can grant permission through the Settings application.

READ\_LOGS

Allows an application to read the low-level system log files.

READ\_PRIVILEGED\_PHONE\_STATE

Allows read access to privileged phone state.

REBOOT

Required to be able to reboot the device.

REQUEST\_INSTALL\_PACKAGES

Allows an application to request installing packages.

STATUS\_BAR

Allows an application to open, close, or disable the status bar and its icons.

SYSTEM\_ALERT\_WINDOW

Allows an app to create windows using the type WindowManager.LayoutParams.TYPE\_APPLICATION\_OVERLAY, shown on top of all other apps.

TETHER\_PRIVILEGED

@SystemApi Allows applications to change tether state and run tether carrier provisioning. Not for use by third-party applications.

UPDATE\_APP\_OPS\_STATS

@SystemApi Allows an application to update application operation statistics. Not for use by third party apps.

WRITE\_SECURE\_SETTINGS

Allows an application to read or write the secure system settings.

WRITE\_SETTINGS

Allows an application to read or write the system settings.

[com.android.launcher.permission.WRITE\_SETTINGS](https://android.googlesource.com/platform/packages/apps/Launcher2/+/master/AndroidManifest.xml)

Allows the app to change settings and shortcuts in Home, according to [this](http://androidpermissions.com/permission/com.android.launcher.permission.WRITE_SETTINGS).

Other

[com.amazon.device.messaging.permission.RECEIVE](https://developer.amazon.com/docs/adm/integrate-your-app.html)

This permission allows your app access to receive push notifications from ADM.

[com.android.launcher.permission.READ\_SETTINGS](http://androidpermissions.com/permission/com.android.launcher.permission.READ_SETTINGS)

Allows the app to read the settings and shortcuts in Home.

[com.anddoes.launcher.permission.UPDATE\_COUNT](https://stackoverflow.com/questions/20136483/how-to-interface-with-the-badgeprovider-on-samsung-phones-to-add-a-count-to-the)

For badge counts on Apex phones.

[com.android.vending.BILLING](https://stackoverflow.com/questions/16581277/what-is-com-android-vending-billing-how-to-use-it)

Allows in-app billing on Google Play.

com.facebook.katana.provider.ACCESS

com.facebook.mlite.provider.ACCESS

com.facebook.orca.provider.ACCESS

com.facebook.permission.prod.FB\_APP\_COMMUNICATION

com.facebook.receiver.permission.ACCESS

[com.google.android.c2dm.permission.RECEIVE](http://androidpermissions.com/permission/com.google.android.c2dm.permission.RECEIVE)

Allows apps to accept cloud to device messages sent by the app's service. Using this service will incur data usage. Malicious apps could cause excess data usage.

[com.google.android.finsky.permission.BIND\_GET\_INSTALL\_REFERRER\_SERVICE](https://ottonova.tech/our-android-apps-permissions-explained/)

Recognize where the app was installed from.

[com.google.android.gms.permission.ACTIVITY\_RECOGNITION](https://developer.android.com/guide/topics/location/transitions)

Detect when users start or end an activity.

[com.google.android.providers.gsf.permission.READ\_GSERVICES](http://androidpermissions.com/permission/com.google.android.providers.gsf.permission.READ_GSERVICES)

Allows this app to read Google service configuration data.

com.htc.launcher.permission.READ\_SETTINGS

com.htc.launcher.permission.UPDATE\_SHORTCUT

com.huawei.android.launcher.permission.CHANGE\_BADGE

com.huawei.android.launcher.permission.READ\_SETTINGS

com.huawei.android.launcher.permission.WRITE\_SETTINGS

com.majeur.launcher.permission.UPDATE\_BADGE

com.nokia.pushnotifications.permission.RECEIVE

com.oppo.launcher.permission.READ\_SETTINGS

com.oppo.launcher.permission.WRITE\_SETTINGS

com.sec.android.provider.badge.permission.READ

com.sec.android.provider.badge.permission.WRITE

com.sonyericsson.home.permission.BROADCAST\_BADGE

com.sonymobile.home.permission.PROVIDER\_INSERT\_BADGE

me.everything.badger.permission.BADGE\_COUNT\_READ

me.everything.badger.permission.BADGE\_COUNT\_WRITE

Unknown

android.permission.READ\_APP\_BADGE