Manifest.permission | API reference | Android Developers

Archived: 2026-04-05 21:14:19 UTC

Manifest.permission Stay organized with collections Save and categorize content based on your preferences.

```
public static final class Manifest.permission
extends Object
```

Summary

Constants	
String	ACCEPT_HANDOVER Allows a calling app to continue a call which was started in another app.
String	ACCESS_BACKGROUND_LOCATION Allows an app to access location in the background.
String	ACCESS_BIOMETRIC_SENSOR_STRENGTHS Allows an application to retrieve the sensor security strengths of the biometric sensors.
String	ACCESS_BLOBS_ACROSS_USERS Allows an application to access data blobs across users.
String	ACCESS_CHECKIN_PROPERTIES Allows read/write access to the "properties" table in the checkin database, to change values that get uploaded.

String	ACCESS_COARSE_LOCATION Allows an app to access approximate location.
String	ACCESS_FINE_LOCATION Allows an app to access precise location.
String	ACCESS_HIDDEN_PROFILES Allows applications to access profiles with `android.content.pm.UserProperties#PROFILE_API_VISIBILITY_HIDDEN` user property, e.g.
String	ACCESS_LAUNCHER_DATA This permission protects a content provider within home/launcher applications, enabling management of home screen metadata such as shortcut placement, launch intents, and labels.
String	ACCESS_LOCAL_NETWORK Required to be able to advertise and connect to local network devices.
String	ACCESS_LOCATION_EXTRA_COMMANDS Allows an application to access extra location provider commands.
String	ACCESS_MEDIA_LOCATION Allows an application to access any geographic locations persisted in the user's shared collection.
String	ACCESS_NETWORK_STATE Allows applications to access information about networks.
String	ACCESS_NOTIFICATION_POLICY Marker permission for applications that wish to access notification policy.
String	ACCESS_WIFI_STATE Allows applications to access information about Wi-Fi networks.
String	ACCOUNT_MANAGER

	Allows applications to call into AccountAuthenticators.
String	`ACTIVITY_RECOGNITION` Allows an application to recognize physical activity.
String	`ADD_VOICEMAIL` Allows an application to add voicemails into the system.
String	`ANSWER_PHONE_CALLS` Allows the app to answer an incoming phone call.
String	`APPLY_PICTURE_PROFILE` Allows an app to apply a `ERROR(/MediaQualityManager.PictureProfile)` to a layer via `ERROR(/MediaCodec.PARAMETER_KEY_PICTURE_PROFILE)` and, additionally, system apps via `ERROR(/SurfaceControl.Transaction#setPictureProfileHandle)`.
String	`BATTERY_STATS` Allows an application to collect battery statistics Protection level: signature|privileged|development
String	`BIND_ACCESSIBILITY_SERVICE` Must be required by an `AccessibilityService`, to ensure that only the system can bind to it.
String	`BIND_ALTERNATIVE_MESSAGE_TRANSPORT_SERVICE` Permission needed to ensure that only the system process can bind with the `AlternativeMessageTransportService`.
String	`BIND_APPWIDGET` Allows an application to tell the AppWidget service which application can access AppWidget's data.
String	`BIND_APP_FUNCTION_SERVICE` Must be required by an `AppFunctionService`, to ensure that only the system can bind to it.

String	BIND_AUTOFILL_SERVICE Must be required by a AutofillService, to ensure that only the system can bind to it.
String	BIND_CALL_REDIRECTION_SERVICE Must be required by a CallRedirectionService, to ensure that only the system can bind to it.
String	BIND_CARRIER_MESSAGING_CLIENT_SERVICE A subclass of CarrierMessagingClientService must be protected with this permission.
String	BIND_CARRIER_MESSAGING_SERVICE *This constant was deprecated in API level 23. Use BIND_CARRIER_SERVICES instead*
String	BIND_CARRIER_SERVICES The system process that is allowed to bind to services in carrier apps will have this permission.
String	BIND_CHOOSER_TARGET_SERVICE *This constant was deprecated in API level 30. For publishing direct share targets, please follow the instructions in https://developer.android.com/training/sharing/receive.html#providing-direct-share-targets instead.*
String	BIND_COMPANION_DEVICE_SERVICE Must be required by any CompanionDeviceService s to ensure that only the system can bind to it.
String	BIND_CONDITION_PROVIDER_SERVICE Must be required by a ConditionProviderService, to ensure that only the system can bind to it.
String	BIND_CONTROLS Allows SystemUI to request third party controls.
String	BIND_CREDENTIAL_PROVIDER_SERVICE Must be required by a CredentialProviderService to ensure that only the system can bind to it.
String	BIND_DATA_MIGRATION_FOR_PRIVATECOMPUTE

	Allows the system to bind to an application's data migration service for Private Compute.
`String`	`BIND_DEVICE_ADMIN` Must be required by device administration receiver, to ensure that only the system can interact with it.
`String`	`BIND_DREAM_SERVICE` Must be required by an `DreamService`, to ensure that only the system can bind to it.
`String`	`BIND_INCALL_SERVICE` Must be required by a `InCallService`, to ensure that only the system can bind to it.
`String`	`BIND_INPUT_METHOD` Must be required by an `InputMethodService`, to ensure that only the system can bind to it.
`String`	`BIND_MIDI_DEVICE_SERVICE` Must be required by an `MidiDeviceService`, to ensure that only the system can bind to it.
`String`	`BIND_NFC_SERVICE` Must be required by a `HostApduService` or `OffHostApduService` to ensure that only the system can bind to it.
`String`	`BIND_NOTIFICATION_LISTENER_SERVICE` Must be required by an `NotificationListenerService`, to ensure that only the system can bind to it.
`String`	`BIND_PRINT_SERVICE` Must be required by a `PrintService`, to ensure that only the system can bind to it.
`String`	`BIND_QUICK_ACCESS_WALLET_SERVICE` Must be required by a `QuickAccessWalletService` to ensure that only the system can bind to it.

String	BIND_QUICK_SETTINGS_TILE Allows an application to bind to third party quick settings tiles.
String	BIND_REMOTEVIEWS Must be required by a RemoteViewsService, to ensure that only the system can bind to it.
String	BIND_SCREENING_SERVICE Must be required by a CallScreeningService, to ensure that only the system can bind to it.
String	BIND_TELECOM_CONNECTION_SERVICE Must be required by a ConnectionService, to ensure that only the system can bind to it.
String	BIND_TEXT_SERVICE Must be required by a TextService (e.g. SpellCheckerService) to ensure that only the system can bind to it.
String	BIND_TV_AD_SERVICE Must be required by a android.media.tv.ad.TvAdService to ensure that only the system can bind to it.
String	BIND_TV_INPUT Must be required by a TvInputService to ensure that only the system can bind to it.
String	BIND_TV_INTERACTIVE_APP Must be required by a TvInteractiveAppService to ensure that only the system can bind to it.
String	BIND_VISUAL_VOICEMAIL_SERVICE Must be required by a link VisualVoicemailService to ensure that only the system can bind to it.
String	BIND_VOICE_INTERACTION Must be required by a VoiceInteractionService, to ensure that only the system can bind to it.

String	BIND_VPN_SERVICE Must be required by a VpnService, to ensure that only the system can bind to it.
String	BIND_VR_LISTENER_SERVICE Must be required by an VrListenerService, to ensure that only the system can bind to it.
String	BIND_WALLPAPER Must be required by a WallpaperService, to ensure that only the system can bind to it.
String	BLUETOOTH Allows applications to connect to paired bluetooth devices.
String	BLUETOOTH_ADMIN Allows applications to discover and pair bluetooth devices.
String	BLUETOOTH_ADVERTISE Required to be able to advertise to nearby Bluetooth devices.
String	BLUETOOTH_CONNECT Required to be able to connect to paired Bluetooth devices.
String	BLUETOOTH_PRIVILEGED Allows applications to pair bluetooth devices without user interaction, and to allow or disallow phonebook access or message access.
String	BLUETOOTH_SCAN Required to be able to discover and pair nearby Bluetooth devices.
String	BODY_SENSORS Allows an application to access data from sensors that the user uses to measure what is happening inside their body, such as heart rate.
String	BODY_SENSORS_BACKGROUND

	Allows an application to access data from sensors that the user uses to measure what is happening inside their body, such as heart rate.
String	BROADCAST_PACKAGE_REMOVED Allows an application to broadcast a notification that an application package has been removed.
String	BROADCAST_SMS Allows an application to broadcast an SMS receipt notification.
String	BROADCAST_STICKY Allows an application to broadcast sticky intents.
String	BROADCAST_WAP_PUSH Allows an application to broadcast a WAP PUSH receipt notification.
String	CALL_COMPANION_APP Allows an app which implements the InCallService API to be eligible to be enabled as a calling companion app.
String	CALL_PHONE Allows an application to initiate a phone call without going through the Dialer user interface for the user to confirm the call.
String	CALL_PRIVILEGED Allows an application to call any phone number, including emergency numbers, without going through the Dialer user interface for the user to confirm the call being placed.
String	CAMERA Required to be able to access the camera device.
String	CAPTURE_AUDIO_OUTPUT Allows an application to capture audio output.
String	CAPTURE_KEYBOARD

	Allows the currently focused application to be able to consume keys before Android system get chance to process system keys and shortcuts.
String	CHANGE_COMPONENT_ENABLED_STATE Allows an application to change whether an application component (other than its own) is enabled or not.
String	CHANGE_CONFIGURATION Allows an application to modify the current configuration, such as locale.
String	CHANGE_NETWORK_STATE Allows applications to change network connectivity state.
String	CHANGE_WIFI_MULTICAST_STATE Allows applications to enter Wi-Fi Multicast mode.
String	CHANGE_WIFI_STATE Allows applications to change Wi-Fi connectivity state.
String	CLEAR_APP_CACHE Allows an application to clear the caches of all installed applications on the device.
String	CONFIGURE_WIFI_DISPLAY Allows an application to configure and connect to Wifi displays
String	CONTROL_LOCATION_UPDATES Allows enabling/disabling location update notifications from the radio.
String	CREDENTIAL_MANAGER_QUERY_CANDIDATE_CREDENTIALS Allows a browser to invoke the set of query apis to get metadata about credential candidates prepared during the CredentialManager.prepareGetCredential API.
String	CREDENTIAL_MANAGER_SET_ALLOWED_PROVIDERS

	Allows specifying candidate credential providers to be queried in Credential Manager get flows, or to be preferred as a default in the Credential Manager create flows.
String	`CREDENTIAL_MANAGER_SET_ORIGIN` Allows a browser to invoke credential manager APIs on behalf of another RP.
String	`DELETE_CACHE_FILES` Old permission for deleting an app's cache files, no longer used, but signals for us to quietly ignore calls instead of throwing an exception.
String	`DELETE_PACKAGES` Allows an application to delete packages.
String	`DELIVER_COMPANION_MESSAGES` Allows an application to deliver companion messages to system
String	`DETECT_SCREEN_CAPTURE` Allows an application to get notified when a screen capture of its windows is attempted.
String	`DETECT_SCREEN_RECORDING` Allows an application to get notified when it is being recorded.
String	`DIAGNOSTIC` Allows applications to RW to diagnostic resources.
String	`DISABLE_KEYGUARD` Allows applications to disable the keyguard if it is not secure.
String	`DUMP` Allows an application to retrieve state dump information from system services.
String	`ENFORCE_UPDATE_OWNERSHIP` Allows an application to indicate via `PackageInstaller.SessionParams.setRequestUpdateOwnership(boolean)` that it has the

	intention of becoming the update owner.
`String`	`EXECUTE_APP_ACTION` Allows an assistive application to perform actions on behalf of users inside of applications.
`String`	`EXECUTE_APP_FUNCTIONS` Allows an application to perform actions on behalf of users inside of applications.
`String`	`EXPAND_STATUS_BAR` Allows an application to expand or collapse the status bar.
`String`	`FACTORY_TEST` Run as a manufacturer test application, running as the root user.
`String`	`FOREGROUND_SERVICE` Allows a regular application to use `Service.startForeground`.
`String`	`FOREGROUND_SERVICE_CAMERA` Allows a regular application to use `Service.startForeground` with the type "camera".
`String`	`FOREGROUND_SERVICE_CONNECTED_DEVICE` Allows a regular application to use `Service.startForeground` with the type "connectedDevice".
`String`	`FOREGROUND_SERVICE_DATA_SYNC` Allows a regular application to use `Service.startForeground` with the type "dataSync".
`String`	`FOREGROUND_SERVICE_HEALTH` Allows a regular application to use `Service.startForeground` with the type "health".
`String`	`FOREGROUND_SERVICE_LOCATION` Allows a regular application to use `Service.startForeground` with the type "location".
`String`	`FOREGROUND_SERVICE_MEDIA_PLAYBACK`

	Allows a regular application to use `Service.startForeground` with the type "mediaPlayback".
`String`	`FOREGROUND_SERVICE_MEDIA_PROCESSING` Allows a regular application to use `Service.startForeground` with the type "mediaProcessing".
`String`	`FOREGROUND_SERVICE_MEDIA_PROJECTION` Allows a regular application to use `Service.startForeground` with the type "mediaProjection".
`String`	`FOREGROUND_SERVICE_MICROPHONE` Allows a regular application to use `Service.startForeground` with the type "microphone".
`String`	`FOREGROUND_SERVICE_PHONE_CALL` Allows a regular application to use `Service.startForeground` with the type "phoneCall".
`String`	`FOREGROUND_SERVICE_REMOTE_MESSAGING` Allows a regular application to use `Service.startForeground` with the type "remoteMessaging".
`String`	`FOREGROUND_SERVICE_SPECIAL_USE` Allows a regular application to use `Service.startForeground` with the type "specialUse".
`String`	`FOREGROUND_SERVICE_SYSTEM_EXEMPTED` Allows a regular application to use `Service.startForeground` with the type "systemExempted".
`String`	`GET_ACCOUNTS` Allows access to the list of accounts in the Accounts Service.
`String`	`GET_ACCOUNTS_PRIVILEGED` Allows access to the list of accounts in the Accounts Service.
`String`	`GET_PACKAGE_SIZE` Allows an application to find out the space used by any package.

String	GET_TASKS *This constant was deprecated in API level 21. No longer enforced.*
String	GLOBAL_SEARCH This permission can be used on content providers to allow the global search system to access their data.
String	HIDE_OVERLAY_WINDOWS Allows an app to prevent non-system-overlay windows from being drawn on top of it
String	HIGH_SAMPLING_RATE_SENSORS Allows an app to access sensor data with a sampling rate greater than 200 Hz.
String	INSTALL_LOCATION_PROVIDER Allows an application to install a location provider into the Location Manager.
String	INSTALL_PACKAGES Allows an application to install packages.
String	INSTALL_SHORTCUT Allows an application to install a shortcut in Launcher.
String	INSTANT_APP_FOREGROUND_SERVICE Allows an instant app to create foreground services.
String	INTERACT_ACROSS_PROFILES Allows interaction across profiles in the same profile group.
String	INTERNET Allows applications to open network sockets.

String	KILL_BACKGROUND_PROCESSES Allows an application to call ActivityManager.killBackgroundProcesses(String).
String	LAUNCH_CAPTURE_CONTENT_ACTIVITY_FOR_NOTE Allows an application to capture screen content to perform a screenshot using the intent action Intent.ACTION_LAUNCH_CAPTURE_CONTENT_ACTIVITY_FOR_NOTE.
String	LAUNCH_MULTI_PANE_SETTINGS_DEEP_LINK An application needs this permission for Settings.ACTION_SETTINGS_EMBED_DEEP_LINK_ACTIVITY to show its Activity embedded in Settings app.
String	LOADER_USAGE_STATS Allows a data loader to read a package's access logs.
String	LOCATION_HARDWARE Allows an application to use location features in hardware, such as the geofencing api.
String	MANAGE_DEVICE_LOCK_STATE Allows financed device kiosk apps to perform actions on the Device Lock service Protection level: internal|role Intended for use by the FINANCED_DEVICE_KIOSK role only.
String	MANAGE_DEVICE_POLICY_ACCESSIBILITY Allows an application to manage policy related to accessibility.
String	MANAGE_DEVICE_POLICY_ACCOUNT_MANAGEMENT Allows an application to set policy related to account management.
String	MANAGE_DEVICE_POLICY_ACROSS_USERS Allows an application to set device policies outside the current user that are required for securing device ownership without accessing user data.

String	MANAGE_DEVICE_POLICY_ACROSS_USERS_FULL Allows an application to set device policies outside the current user.
String	MANAGE_DEVICE_POLICY_ACROSS_USERS_SECURITY_CRITICAL Allows an application to set device policies outside the current user that are critical for securing data within the current user.
String	MANAGE_DEVICE_POLICY_AIRPLANE_MODE Allows an application to set policy related to airplane mode.
String	MANAGE_DEVICE_POLICY_APPS_CONTROL Allows an application to manage policy regarding modifying applications.
String	MANAGE_DEVICE_POLICY_APP_FUNCTIONS Allows an application to manage policy related to AppFunctions.
String	MANAGE_DEVICE_POLICY_APP_RESTRICTIONS Allows an application to manage application restrictions.
String	MANAGE_DEVICE_POLICY_APP_USER_DATA Allows an application to manage policy related to application user data.
String	MANAGE_DEVICE_POLICY_ASSIST_CONTENT Allows an application to set policy related to sending assist content to a privileged app such as the Assistant app.
String	MANAGE_DEVICE_POLICY_AUDIO_OUTPUT Allows an application to set policy related to audio output.
String	MANAGE_DEVICE_POLICY_AUTOFILL Allows an application to set policy related to autofill.
String	MANAGE_DEVICE_POLICY_BACKUP_SERVICE

	Allows an application to manage backup service policy.
`String`	`MANAGE_DEVICE_POLICY_BLOCK_UNINSTALL` Allows an application to manage policy related to block package uninstallation.
`String`	`MANAGE_DEVICE_POLICY_BLUETOOTH` Allows an application to set policy related to bluetooth.
`String`	`MANAGE_DEVICE_POLICY_BUGREPORT` Allows an application to request bugreports with user consent.
`String`	`MANAGE_DEVICE_POLICY_CALLS` Allows an application to manage calling policy.
`String`	`MANAGE_DEVICE_POLICY_CAMERA` Allows an application to set policy related to restricting a user's ability to use or enable and disable the camera.
`String`	`MANAGE_DEVICE_POLICY_CAMERA_TOGGLE` Allows an application to manage policy related to camera toggle.
`String`	`MANAGE_DEVICE_POLICY_CERTIFICATES` Allows an application to set policy related to certificates.
`String`	`MANAGE_DEVICE_POLICY_COMMON_CRITERIA_MODE` Allows an application to manage policy related to common criteria mode.
`String`	`MANAGE_DEVICE_POLICY_CONTENT_PROTECTION` Allows an application to manage policy related to content protection.
`String`	`MANAGE_DEVICE_POLICY_DEBUGGING_FEATURES` Allows an application to manage debugging features policy.

String	MANAGE_DEVICE_POLICY_DEFAULT_SMS Allows an application to set policy related to the default sms application.
String	MANAGE_DEVICE_POLICY_DEVICE_IDENTIFIERS Allows an application to manage policy related to device identifiers.
String	MANAGE_DEVICE_POLICY_DISPLAY Allows an application to set policy related to the display.
String	MANAGE_DEVICE_POLICY_FACTORY_RESET Allows an application to set policy related to factory reset.
String	MANAGE_DEVICE_POLICY_FUN Allows an application to set policy related to fun.
String	MANAGE_DEVICE_POLICY_INPUT_METHODS Allows an application to set policy related to input methods.
String	MANAGE_DEVICE_POLICY_INSTALL_UNKNOWN_SOURCES Allows an application to manage installing from unknown sources policy.
String	MANAGE_DEVICE_POLICY_KEEP_UNINSTALLED_PACKAGES Allows an application to set policy related to keeping uninstalled packages.
String	MANAGE_DEVICE_POLICY_KEYGUARD Allows an application to manage policy related to keyguard features.
String	MANAGE_DEVICE_POLICY_LOCALE Allows an application to set policy related to locale.
String	MANAGE_DEVICE_POLICY_LOCATION Allows an application to set policy related to location.

String	MANAGE_DEVICE_POLICY_LOCK Allows an application to lock a profile or the device with the appropriate cross-user permission.
String	MANAGE_DEVICE_POLICY_LOCK_CREDENTIALS Allows an application to set policy related to lock credentials.
String	MANAGE_DEVICE_POLICY_LOCK_TASK Allows an application to manage lock task policy.
String	MANAGE_DEVICE_POLICY_MANAGED_SUBSCRIPTIONS Allows an application to set policy related to subscriptions downloaded by an admin.
String	MANAGE_DEVICE_POLICY_METERED_DATA Allows an application to manage policy related to metered data.
String	MANAGE_DEVICE_POLICY_MICROPHONE Allows an application to set policy related to restricting a user's ability to use or enable and disable the microphone.
String	MANAGE_DEVICE_POLICY_MICROPHONE_TOGGLE Allows an application to manage policy related to microphone toggle.
String	MANAGE_DEVICE_POLICY_MOBILE_NETWORK Allows an application to set policy related to mobile networks.
String	MANAGE_DEVICE_POLICY_MODIFY_USERS Allows an application to manage policy preventing users from modifying users.
String	MANAGE_DEVICE_POLICY_MTE Allows an application to manage policy related to the Memory Tagging Extension (MTE).
String	MANAGE_DEVICE_POLICY_NEARBY_COMMUNICATION

	Allows an application to set policy related to nearby communications (e.g. Beam and nearby streaming).
String	MANAGE_DEVICE_POLICY_NETWORK_LOGGING Allows an application to set policy related to network logging.
String	MANAGE_DEVICE_POLICY_ORGANIZATION_IDENTITY Allows an application to manage the identity of the managing organization.
String	MANAGE_DEVICE_POLICY_OVERRIDE_APN Allows an application to set policy related to override APNs.
String	MANAGE_DEVICE_POLICY_PACKAGE_STATE Allows an application to set policy related to hiding and suspending packages.
String	MANAGE_DEVICE_POLICY_PHYSICAL_MEDIA Allows an application to set policy related to physical media.
String	MANAGE_DEVICE_POLICY_PRINTING Allows an application to set policy related to printing.
String	MANAGE_DEVICE_POLICY_PRIVATE_DNS Allows an application to set policy related to private DNS.
String	MANAGE_DEVICE_POLICY_PROFILES Allows an application to set policy related to profiles.
String	MANAGE_DEVICE_POLICY_PROFILE_INTERACTION Allows an application to set policy related to interacting with profiles (e.g. Disallowing cross-profile copy and paste).
String	MANAGE_DEVICE_POLICY_PROXY Allows an application to set a network-independent global HTTP proxy.

String	MANAGE_DEVICE_POLICY_QUERY_SYSTEM_UPDATES Allows an application query system updates.
String	MANAGE_DEVICE_POLICY_RESET_PASSWORD Allows an application to force set a new device unlock password or a managed profile challenge on current user.
String	MANAGE_DEVICE_POLICY_RESTRICT_PRIVATE_DNS Allows an application to set policy related to restricting the user from configuring private DNS.
String	MANAGE_DEVICE_POLICY_RUNTIME_PERMISSIONS Allows an application to set the grant state of runtime permissions on packages.
String	MANAGE_DEVICE_POLICY_RUN_IN_BACKGROUND Allows an application to set policy related to users running in the background.
String	MANAGE_DEVICE_POLICY_SAFE_BOOT Allows an application to manage safe boot policy.
String	MANAGE_DEVICE_POLICY_SCREEN_CAPTURE Allows an application to set policy related to screen capture.
String	MANAGE_DEVICE_POLICY_SCREEN_CONTENT Allows an application to set policy related to the usage of the contents of the screen.
String	MANAGE_DEVICE_POLICY_SECURITY_LOGGING Allows an application to set policy related to security logging.
String	MANAGE_DEVICE_POLICY_SETTINGS Allows an application to set policy related to settings.

String	MANAGE_DEVICE_POLICY_SMS Allows an application to set policy related to sms.
String	MANAGE_DEVICE_POLICY_STATUS_BAR Allows an application to set policy related to the status bar.
String	MANAGE_DEVICE_POLICY_SUPPORT_MESSAGE Allows an application to set support messages for when a user action is affected by an active policy.
String	MANAGE_DEVICE_POLICY_SUSPEND_PERSONAL_APPS Allows an application to set policy related to suspending personal apps.
String	MANAGE_DEVICE_POLICY_SYSTEM_APPS Allows an application to manage policy related to system apps.
String	MANAGE_DEVICE_POLICY_SYSTEM_DIALOGS Allows an application to set policy related to system dialogs.
String	MANAGE_DEVICE_POLICY_SYSTEM_UPDATES Allows an application to set policy related to system updates.
String	MANAGE_DEVICE_POLICY_THREAD_NETWORK Allows an application to set policy related to Thread network.
String	MANAGE_DEVICE_POLICY_TIME Allows an application to manage device policy relating to time.
String	MANAGE_DEVICE_POLICY_USB_DATA_SIGNALLING Allows an application to set policy related to usb data signalling.

String	MANAGE_DEVICE_POLICY_USB_FILE_TRANSFER Allows an application to set policy related to usb file transfers.
String	MANAGE_DEVICE_POLICY_USERS Allows an application to set policy related to users.
String	MANAGE_DEVICE_POLICY_VPN Allows an application to set policy related to VPNs.
String	MANAGE_DEVICE_POLICY_WALLPAPER Allows an application to set policy related to the wallpaper.
String	MANAGE_DEVICE_POLICY_WIFI Allows an application to set policy related to Wifi.
String	MANAGE_DEVICE_POLICY_WINDOWS Allows an application to set policy related to windows.
String	MANAGE_DEVICE_POLICY_WIPE_DATA Allows an application to manage policy related to wiping data.
String	MANAGE_DOCUMENTS Allows an application to manage access to documents, usually as part of a document picker.
String	MANAGE_EXTERNAL_STORAGE Allows an application a broad access to external storage in scoped storage.
String	MANAGE_MEDIA Allows an application to modify and delete media files on this device or any connected storage device without user confirmation.
String	MANAGE_ONGOING_CALLS Allows to query ongoing call details and manage ongoing calls

	Protection level: signature|appop
String	MANAGE_OWN_CALLS Allows a calling application which manages its own calls through the self-managed ConnectionService APIs.
String	MANAGE_WIFI_INTERFACES Allows applications to get notified when a Wi-Fi interface request cannot be satisfied without tearing down one or more other interfaces, and provide a decision whether to approve the request or reject it.
String	MANAGE_WIFI_NETWORK_SELECTION This permission is used to let OEMs grant their trusted app access to a subset of privileged wifi APIs to improve wifi performance.
String	MASTER_CLEAR Not for use by third-party applications.
String	MEDIA_CONTENT_CONTROL Allows an application to know what content is playing and control its playback.
String	MEDIA_ROUTING_CONTROL Allows an application to control the routing of media apps.
String	MODIFY_AUDIO_SETTINGS Allows an application to modify global audio settings.
String	MODIFY_PHONE_STATE Allows modification of the telephony state - power on, mmi, etc.
String	MOUNT_FORMAT_FILESYSTEMS Allows formatting file systems for removable storage.
String	MOUNT_UNMOUNT_FILESYSTEMS

	Allows mounting and unmounting file systems for removable storage.
String	`NEARBY_WIFI_DEVICES` Required to be able to advertise and connect to nearby devices via Wi-Fi.
String	`NFC` Allows applications to perform I/O operations over NFC.
String	`NFC_PREFERRED_PAYMENT_INFO` Allows applications to receive NFC preferred payment service information.
String	`NFC_TRANSACTION_EVENT` Allows applications to receive NFC transaction events.
String	`OVERRIDE_MEDIA_SESSION_OWNER` Allows an application to override the owner of a MediaSession.
String	`OVERRIDE_WIFI_CONFIG` Allows an application to modify any wifi configuration, even if created by another application.
String	`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.
String	`PERSISTENT_ACTIVITY` *This constant was deprecated in API level 15. This functionality will be removed in the future; please do not use. Allow an application to make its activities persistent.*
String	`POST_NOTIFICATIONS` Allows an app to post notifications Protection level: dangerous

String	POST_PROMOTED_NOTIFICATIONS Required for apps to post promoted notifications.
String	PROCESS_OUTGOING_CALLS *This constant was deprecated in API level 29. Applications should use CallRedirectionService instead of the Intent.ACTION_NEW_OUTGOING_CALL broadcast.*
String	PROVIDE_OWN_AUTOFILL_SUGGESTIONS Allows an application to display its suggestions using the autofill framework.
String	PROVIDE_PRIVATE_COMPUTE_SERVICES Allows an application to act as Private Compute Services, which allows the application to communicate with Private Compute Core components.
String	PROVIDE_REMOTE_CREDENTIALS Allows an application to be able to store and retrieve credentials from a remote device.
String	QUERY_ADVANCED_PROTECTION_MODE Allows an application to query the device's advanced protection mode status.
String	QUERY_ALL_PACKAGES Allows query of any normal app on the device, regardless of manifest declarations.
String	RANGING Required to be able to range to devices using generic ranging module.
String	READ_ASSISTANT_APP_SEARCH_DATA Allows an application to query over global data in AppSearch that's visible to the ASSISTANT role.
String	READ_ASSIST_STRUCTURE_SCREEN_CONTENT Allows an assistant application to read screen content in the AssistStructure.

String	READ_BASIC_PHONE_STATE Allows read only access to phone state with a non dangerous permission, including the information like cellular network type, software version.
String	READ_CALENDAR Allows an application to read the user's calendar data.
String	READ_CALL_LOG Allows an application to read the user's call log.
String	READ_COLOR_ZONES Allows an application to read the aggregated color zones on the screen for use cases like TV ambient backlight usages.
String	READ_CONTACTS Allows an application to read the user's contacts data.
String	READ_DROPBOX_DATA Allows an application to access the data in Dropbox.
String	READ_EXTERNAL_STORAGE Allows an application to read from external storage.
String	READ_HOME_APP_SEARCH_DATA Allows an application to query over global data in AppSearch that's visible to the HOME role.
String	READ_INPUT_STATE *This constant was deprecated in API level 16. The API that used this permission has been removed.*
String	READ_LOGS Allows an application to read the low-level system log files.

String	READ_MEDIA_AUDIO Allows an application to read audio files from external storage.
String	READ_MEDIA_IMAGES Allows an application to read image files from external storage.
String	READ_MEDIA_VIDEO Allows an application to read video files from external storage.
String	READ_MEDIA_VISUAL_USER_SELECTED Allows an application to read image or video files from external storage that a user has selected via the permission prompt photo picker.
String	READ_NEARBY_STREAMING_POLICY Allows an application to read nearby streaming policy.
String	READ_PHONE_NUMBERS Allows read access to the device's phone number(s), which is exposed to instant applications.
String	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 PhoneAccount s registered on the device.
String	READ_PRECISE_PHONE_STATE Allows read only access to precise phone state.
String	READ_SMS Allows an application to read SMS messages.
String	READ_SYNC_SETTINGS Allows applications to read the sync settings.
String	READ_SYNC_STATS

	Allows applications to read the sync stats.
`String`	`READ_SYSTEM_PREFERENCES` Allows an application to access the Settings Preference services to read settings exposed by the system Settings app and system apps that contribute settings surfaced by the Settings app.
`String`	`READ_VOICEMAIL` Allows an application to read voicemails in the system.
`String`	`REBOOT` Required to be able to reboot the device.
`String`	`RECEIVE_BOOT_COMPLETED` Allows an application to receive the `Intent.ACTION_BOOT_COMPLETED` that is broadcast after the system finishes booting.
`String`	`RECEIVE_MMS` Allows an application to monitor incoming MMS messages.
`String`	`RECEIVE_SENSITIVE_NOTIFICATIONS` Allows apps with a NotificationListenerService to receive notifications with sensitive information Apps with a NotificationListenerService without this permission will not be able to view certain types of sensitive information contained in notifications This permission also allows apps with the SMS permissions to query and receive broadcasts about SMS messages that contain One Time Passwords Protection level: signature|preinstalled|knownSigner|role
`String`	`RECEIVE_SMS` Allows an application to receive SMS messages.
`String`	`RECEIVE_WAP_PUSH` Allows an application to receive WAP push messages.

String	RECORD_AUDIO Allows an application to record audio.
String	REORDER_TASKS Allows an application to change the Z-order of tasks.
String	REPOSITION_SELF_WINDOWS Allows an application to programmatically move and resize its tasks when the system is in a state that allows such operations, e.g. in a desktop-like environment.
String	REQUEST_COMPANION_PROFILE_APP_STREAMING Allows application to request to be associated with a virtual device capable of streaming Android applications (AssociationRequest.DEVICE_PROFILE_APP_STREAMING) by CompanionDeviceManager .
String	REQUEST_COMPANION_PROFILE_AUTOMOTIVE_PROJECTION Allows application to request to be associated with a vehicle head unit capable of automotive projection (AssociationRequest.DEVICE_PROFILE_AUTOMOTIVE_PROJECTION) by CompanionDeviceManager .
String	REQUEST_COMPANION_PROFILE_COMPUTER Allows application to request to be associated with a computer to share functionality and/or data with other devices, such as notifications, photos and media (AssociationRequest.DEVICE_PROFILE_COMPUTER) by CompanionDeviceManager .
String	REQUEST_COMPANION_PROFILE_GLASSES Allows app to request to be associated with a device via CompanionDeviceManager as "glasses" Protection level: normal
String	REQUEST_COMPANION_PROFILE_MEDICAL Allows application to request to associate with a AssociationRequest.DEVICE_PROFILE_MEDICAL device via CompanionDeviceManager .
String	REQUEST_COMPANION_PROFILE_NEARBY_DEVICE_STREAMING

	Allows application to request to stream content from an Android host to a nearby device (`AssociationRequest.DEVICE_PROFILE_NEARBY_DEVICE_STREAMING`) by `CompanionDeviceManager` .
`String`	`REQUEST_COMPANION_PROFILE_WATCH` Allows app to request to be associated with a device via `CompanionDeviceManager` as a "watch" Protection level: normal
`String`	`REQUEST_COMPANION_RUN_IN_BACKGROUND` Allows a companion app to run in the background.
`String`	`REQUEST_COMPANION_SELF_MANAGED` Allows an application to create a "self-managed" association.
`String`	`REQUEST_COMPANION_START_FOREGROUND_SERVICES_FROM_BACKGROUND` Allows a companion app to start a foreground service from the background.
`String`	`REQUEST_COMPANION_USE_DATA_IN_BACKGROUND` Allows a companion app to use data in the background.
`String`	`REQUEST_DELETE_PACKAGES` Allows an application to request deleting packages.
`String`	`REQUEST_IGNORE_BATTERY_OPTIMIZATIONS` Permission an application must hold in order to use `Settings.ACTION_REQUEST_IGNORE_BATTERY_OPTIMIZATIONS` .
`String`	`REQUEST_INSTALL_PACKAGES` Allows an application to request installing packages.
`String`	`REQUEST_OBSERVE_COMPANION_DEVICE_PRESENCE` Allows an application to subscribe to notifications about the presence status change of their associated companion device

String	REQUEST_OBSERVE_DEVICE_UUID_PRESENCE Allows an application to subscribe to notifications about the nearby devices' presence status change base on the UUIDs.
String	REQUEST_PASSWORD_COMPLEXITY Allows an application to request the screen lock complexity and prompt users to update the screen lock to a certain complexity level.
String	RESTART_PACKAGES *This constant was deprecated in API level 15. The ActivityManager.restartPackage(String) API is no longer supported.*
String	RUN_USER_INITIATED_JOBS Allows applications to use the user-initiated jobs API.
String	SCHEDULE_EXACT_ALARM Allows applications to use exact alarm APIs.
String	SEND_RESPOND_VIA_MESSAGE Allows an application (Phone) to send a request to other applications to handle the respond-via-message action during incoming calls.
String	SEND_SMS Allows an application to send SMS messages.
String	SET_ALARM Allows an application to broadcast an Intent to set an alarm for the user.
String	SET_ALWAYS_FINISH Allows an application to control whether activities are immediately finished when put in the background.

String	SET_ANIMATION_SCALE Modify the global animation scaling factor.
String	SET_BIOMETRIC_DIALOG_ADVANCED Allows an application to set the advanced features on BiometricDialog (SystemUI), including logo, logo description, and content view with more options button.
String	SET_DEBUG_APP Configure an application for debugging.
String	SET_PREFERRED_APPLICATIONS *This constant was deprecated in API level 15. No longer useful, see* *PackageManager.addPackageToPreferred(String)* *for details.*
String	SET_PROCESS_LIMIT Allows an application to set the maximum number of (not needed) application processes that can be running.
String	SET_TIME Allows applications to set the system time directly.
String	SET_TIME_ZONE Allows applications to set the system time zone directly.
String	SET_WALLPAPER Allows applications to set the wallpaper.
String	SET_WALLPAPER_HINTS Allows applications to set the wallpaper hints.
String	SHOW_POWER_MENU Permission needed to request to show the Power Menu.

String	SHOW_POWER_MENU_PRIVILEGED Permission needed to request to show the Power Menu.
String	SIGNAL_PERSISTENT_PROCESSES Allow an application to request that a signal be sent to all persistent processes.
String	SMS_FINANCIAL_TRANSACTIONS *This constant was deprecated in API level 31. The API that used this permission is no longer functional.*
String	START_FOREGROUND_SERVICES_FROM_BACKGROUND Allows an application to start foreground services from the background at any time.
String	START_VIEW_APP_FEATURES Allows the holder to start the screen with a list of app features.
String	START_VIEW_PERMISSION_USAGE Allows the holder to start the permission usage screen for an app.
String	STATUS_BAR Allows an application to open, close, or disable the status bar and its icons.
String	SUBSCRIBE_TO_KEYGUARD_LOCKED_STATE Allows an application to subscribe to device locked and keyguard locked (i.e., showing) state.
String	SYSTEM_ALERT_WINDOW Allows an app to create windows using the type WindowManager.LayoutParams.TYPE_APPLICATION_OVERLAY, shown on top of all other apps.
String	TRANSMIT_IR Allows using the device's IR transmitter, if available.
String	TURN_SCREEN_ON

	Allows an app to turn on the screen on, e.g. with `PowerManager.ACQUIRE_CAUSES_WAKEUP`.
`String`	`TV_IMPLICIT_ENTER_PIP` Allows an app to enter Picture-in-Picture mode when the user is not explicitly requesting it.
`String`	`UNINSTALL_SHORTCUT` **Don't use this permission in your app.**
`String`	`UPDATE_DEVICE_STATS` Allows an application to update device statistics.
`String`	`UPDATE_PACKAGES_WITHOUT_USER_ACTION` Allows an application to indicate via `PackageInstaller.SessionParams.setRequireUserAction(int)` that user action should not be required for an app update.
`String`	`USE_BIOMETRIC` Allows an app to use device supported biometric modalities.
`String`	`USE_EXACT_ALARM` Allows apps to use exact alarms just like with `SCHEDULE_EXACT_ALARM` but without needing to request this permission from the user.
`String`	`USE_FINGERPRINT` *This constant was deprecated in API level 28. Applications should request `USE_BIOMETRIC` instead*
`String`	`USE_FULL_SCREEN_INTENT` Required for apps targeting `Build.VERSION_CODES.Q` that want to use `notification full screen intents`.
`String`	`USE_ICC_AUTH_WITH_DEVICE_IDENTIFIER` Allows to read device identifiers and use ICC based authentication like EAP-AKA.

String	`USE_LOCATION_BUTTON` Allows an app use location button, which grants temporary location permission when a user clicks the button.
String	`USE_LOOPBACK_INTERFACE` Required to be able to interact with other applications via IP packets on the loopback interface.
String	`USE_PINNED_WINDOWING_LAYER` Allows an application to use `ActivityManager.AppTask.WINDOWING_LAYER_PINNED` for its Tasks, typically requested via `ActivityManager.AppTask.requestWindowingLayer(int, Executor, OutcomeReceiver)` .
String	`USE_SIP` Allows an application to use SIP service.
String	`UWB_RANGING` Required to be able to range to devices using ultra-wideband.
String	`VIBRATE` Allows access to the vibrator.
String	`WAKE_LOCK` Allows using PowerManager WakeLocks to keep processor from sleeping or screen from dimming.
String	`WRITE_APN_SETTINGS` Allows applications to write the apn settings and read sensitive fields of an existing apn settings like user and password.
String	`WRITE_CALENDAR` Allows an application to write the user's calendar data.

String	WRITE_CALL_LOG Allows an application to write and read the user's call log data.
String	WRITE_CONTACTS Allows an application to write the user's contacts data.
String	WRITE_EXTERNAL_STORAGE Allows an application to write to external storage.
String	WRITE_GSERVICES Allows an application to modify the Google service map.
String	WRITE_SECURE_SETTINGS Allows an application to read or write the secure system settings.
String	WRITE_SETTINGS Allows an application to read or write the system settings.
String	WRITE_SYNC_SETTINGS Allows applications to write the sync settings.
String	WRITE_SYSTEM_PREFERENCES Allows an application to access the Settings Preference services to write settings values exposed by the system Settings app and system apps that contribute settings surfaced in the Settings app.
String	WRITE_VOICEMAIL Allows an application to modify and remove existing voicemails in the system.

Public constructors

permission()

Inherited methods

From class `java.lang.Object`

`Object`	`clone()` Creates and returns a copy of this object.
`boolean`	`equals(Object obj)` Indicates whether some other object is "equal to" this one.
`void`	`finalize()` Called by the garbage collector on an object when garbage collection determines that there are no more references to the object.
`final Class<?>`	`getClass()` Returns the runtime class of this `Object`.
`int`	`hashCode()` Returns a hash code value for the object.
`final void`	`notify()` Wakes up a single thread that is waiting on this object's monitor.
`final void`	`notifyAll()` Wakes up all threads that are waiting on this object's monitor.
`String`	`toString()` Returns a string representation of the object.
`final void`	`wait(long timeoutMillis, int nanos)` Causes the current thread to wait until it is awakened, typically by being *notified* or *interrupted*, or until a certain amount of real time has elapsed.
`final void`	`wait(long timeoutMillis)`

	Causes the current thread to wait until it is awakened, typically by being *notified* or *interrupted*, or until a certain amount of real time has elapsed.
`final void`	`wait()` Causes the current thread to wait until it is awakened, typically by being *notified* or *interrupted*.

Constants

ACCEPT_HANDOVER

```
public static final String ACCEPT_HANDOVER
```

Allows a calling app to continue a call which was started in another app. An example is a video calling app that wants to continue a voice call on the user's mobile network.

When the handover of a call from one app to another takes place, there are two devices which are involved in the handover; the initiating and receiving devices. The initiating device is where the request to handover the call was started, and the receiving device is where the handover request is confirmed by the other party.

This permission protects access to the `TelecomManager.acceptHandover(Uri, int, PhoneAccountHandle)` which the receiving side of the handover uses to accept a handover.

Protection level: dangerous

Constant Value: "android.permission.ACCEPT_HANDOVER"

ACCESS_BACKGROUND_LOCATION

```
public static final String ACCESS_BACKGROUND_LOCATION
```

Allows an app to access location in the background. If you're requesting this permission, you must also request either `ACCESS_COARSE_LOCATION` or `ACCESS_FINE_LOCATION`. Requesting this permission by itself doesn't give you location access.

Protection level: dangerous

This is a hard restricted permission which cannot be held by an app until the installer on record allowlists the permission. For more details see `PackageInstaller.SessionParams.setWhitelistedRestrictedPermissions(Set)`.

Constant Value: "android.permission.ACCESS_BACKGROUND_LOCATION"

ACCESS_BIOMETRIC_SENSOR_STRENGTHS

```
public static final String ACCESS_BIOMETRIC_SENSOR_STRENGTHS
```

Allows an application to retrieve the sensor security strengths of the biometric sensors.

This permission is currently granted only to the WALLET role, the DEVICE_POLICY_MANAGEMENT role, and the SYSTEM_SHELL role (for easier control during testing).

Constant Value: "android.permission.ACCESS_BIOMETRIC_SENSOR_STRENGTHS"

ACCESS_BLOBS_ACROSS_USERS

```
public static final String ACCESS_BLOBS_ACROSS_USERS
```

Allows an application to access data blobs across users.

Constant Value: "android.permission.ACCESS_BLOBS_ACROSS_USERS"

ACCESS_CHECKIN_PROPERTIES

```
public static final String ACCESS_CHECKIN_PROPERTIES
```

Allows read/write access to the "properties" table in the checkin database, to change values that get uploaded.

Not for use by third-party applications.

Constant Value: "android.permission.ACCESS_CHECKIN_PROPERTIES"

ACCESS_COARSE_LOCATION

```
public static final String ACCESS_COARSE_LOCATION
```

Allows an app to access approximate location. Alternatively, you might want `ACCESS_FINE_LOCATION`.

Protection level: dangerous

Constant Value: "android.permission.ACCESS_COARSE_LOCATION"

ACCESS_FINE_LOCATION

```
public static final String ACCESS_FINE_LOCATION
```

Allows an app to access precise location. Alternatively, you might want `ACCESS_COARSE_LOCATION`.

Protection level: dangerous

Constant Value: "android.permission.ACCESS_FINE_LOCATION"

ACCESS_HIDDEN_PROFILES

```
public static final String ACCESS_HIDDEN_PROFILES
```

Allows applications to access profiles with `android.content.pm.UserProperties#PROFILE_API_VISIBILITY_HIDDEN` user property, e.g. `UserManager.USER_TYPE_PROFILE_PRIVATE`.

Protection level: normal

Constant Value: "android.permission.ACCESS_HIDDEN_PROFILES"

ACCESS_LAUNCHER_DATA

```
public static final String ACCESS_LAUNCHER_DATA
```

This permission protects a content provider within home/launcher applications, enabling management of home screen metadata such as shortcut placement, launch intents, and labels.

Constant Value: "android.permission.ACCESS_LAUNCHER_DATA"

ACCESS_LOCATION_EXTRA_COMMANDS

```
public static final String ACCESS_LOCATION_EXTRA_COMMANDS
```

Allows an application to access extra location provider commands.

Protection level: normal

Constant Value: "android.permission.ACCESS_LOCATION_EXTRA_COMMANDS"

ACCESS_MEDIA_LOCATION

```
public static final String ACCESS_MEDIA_LOCATION
```

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

Protection level: dangerous

Constant Value: "android.permission.ACCESS_MEDIA_LOCATION"

ACCESS_NETWORK_STATE

```
public static final String ACCESS_NETWORK_STATE
```

Allows applications to access information about networks.

Protection level: normal

Constant Value: "android.permission.ACCESS_NETWORK_STATE"

ACCESS_NOTIFICATION_POLICY

```
public static final String ACCESS_NOTIFICATION_POLICY
```

Marker permission for applications that wish to access notification policy. This permission is not supported on managed profiles.

Protection level: normal

Constant Value: "android.permission.ACCESS_NOTIFICATION_POLICY"

ACCESS_WIFI_STATE

```
public static final String ACCESS_WIFI_STATE
```

Allows applications to access information about Wi-Fi networks.

Protection level: normal

Constant Value: "android.permission.ACCESS_WIFI_STATE"

ACCOUNT_MANAGER

```
public static final String ACCOUNT_MANAGER
```

Allows applications to call into AccountAuthenticators.

Not for use by third-party applications.

Constant Value: "android.permission.ACCOUNT_MANAGER"

ACTIVITY_RECOGNITION

```
public static final String ACTIVITY_RECOGNITION
```

Allows an application to recognize physical activity.

Protection level: dangerous

Constant Value: "android.permission.ACTIVITY_RECOGNITION"

ADD_VOICEMAIL

```
public static final String ADD_VOICEMAIL
```

Allows an application to add voicemails into the system.

Protection level: dangerous

Constant Value: "com.android.voicemail.permission.ADD_VOICEMAIL"

ANSWER_PHONE_CALLS

```
public static final String ANSWER_PHONE_CALLS
```

Allows the app to answer an incoming phone call.

Protection level: dangerous

Constant Value: "android.permission.ANSWER_PHONE_CALLS"

BATTERY_STATS

```
public static final String BATTERY_STATS
```

Allows an application to collect battery statistics

Protection level: signature|privileged|development

Constant Value: "android.permission.BATTERY_STATS"

BIND_ACCESSIBILITY_SERVICE

```
public static final String BIND_ACCESSIBILITY_SERVICE
```

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

Protection level: signature

Constant Value: "android.permission.BIND_ACCESSIBILITY_SERVICE"

BIND_ALTERNATIVE_MESSAGE_TRANSPORT_SERVICE

```
public static final String BIND_ALTERNATIVE_MESSAGE_TRANSPORT_SERVICE
```

Permission needed to ensure that only the system process can bind with the `AlternativeMessageTransportService`.

Constant Value: "android.permission.BIND_ALTERNATIVE_MESSAGE_TRANSPORT_SERVICE"

BIND_APPWIDGET

```
public static final String BIND_APPWIDGET
```

Allows an application to tell the AppWidget service which application can access AppWidget's data. The normal user flow is that a user picks an AppWidget to go into a particular host, thereby giving that host application access to the private data from the AppWidget app. An application that has this permission should honor that contract.

Not for use by third-party applications.

Constant Value: "android.permission.BIND_APPWIDGET"

BIND_APP_FUNCTION_SERVICE

```
public static final String BIND_APP_FUNCTION_SERVICE
```

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

Protection level: signature

Constant Value: "android.permission.BIND_APP_FUNCTION_SERVICE"

BIND_AUTOFILL_SERVICE

```
public static final String BIND_AUTOFILL_SERVICE
```

Must be required by a `AutofillService`, to ensure that only the system can bind to it.

Protection level: signature

Constant Value: "android.permission.BIND_AUTOFILL_SERVICE"

BIND_CALL_REDIRECTION_SERVICE

```
public static final String BIND_CALL_REDIRECTION_SERVICE
```

Must be required by a `CallRedirectionService`, to ensure that only the system can bind to it.

Protection level: signature|privileged

Constant Value: "android.permission.BIND_CALL_REDIRECTION_SERVICE"

BIND_CARRIER_MESSAGING_CLIENT_SERVICE

```
public static final String BIND_CARRIER_MESSAGING_CLIENT_SERVICE
```

A subclass of `CarrierMessagingClientService` must be protected with this permission.

Protection level: signature

Constant Value: "android.permission.BIND_CARRIER_MESSAGING_CLIENT_SERVICE"

BIND_CARRIER_MESSAGING_SERVICE

```
public static final String BIND_CARRIER_MESSAGING_SERVICE
```

This constant was deprecated in API level 23.
Use `BIND_CARRIER_SERVICES` instead

Constant Value: "android.permission.BIND_CARRIER_MESSAGING_SERVICE"

BIND_CARRIER_SERVICES

```
public static final String BIND_CARRIER_SERVICES
```

The system process that is allowed to bind to services in carrier apps will have this permission. Carrier apps should use this permission to protect their services that only the system is allowed to bind to.

Protection level: signature|privileged

Constant Value: "android.permission.BIND_CARRIER_SERVICES"

BIND_CHOOSER_TARGET_SERVICE

```
public static final String BIND_CHOOSER_TARGET_SERVICE
```

This constant was deprecated in API level 30.
For publishing direct share targets, please follow the instructions in

https://developer.android.com/training/sharing/receive.html#providing-direct-share-targets instead.

Must be required by a `ChooserTargetService`, to ensure that only the system can bind to it.

Protection level: signature

Constant Value: "android.permission.BIND_CHOOSER_TARGET_SERVICE"

BIND_COMPANION_DEVICE_SERVICE

```
public static final String BIND_COMPANION_DEVICE_SERVICE
```

Must be required by any `CompanionDeviceService`s to ensure that only the system can bind to it.

Constant Value: "android.permission.BIND_COMPANION_DEVICE_SERVICE"

BIND_CONDITION_PROVIDER_SERVICE

```
public static final String BIND_CONDITION_PROVIDER_SERVICE
```

Must be required by a `ConditionProviderService`, to ensure that only the system can bind to it.

Protection level: signature

Constant Value: "android.permission.BIND_CONDITION_PROVIDER_SERVICE"

BIND_CONTROLS

```
public static final String BIND_CONTROLS
```

Allows SystemUI to request third party controls.

Should only be requested by the System and required by `ControlsProviderService` declarations.

Constant Value: "android.permission.BIND_CONTROLS"

BIND_CREDENTIAL_PROVIDER_SERVICE

```
public static final String BIND_CREDENTIAL_PROVIDER_SERVICE
```

Must be required by a CredentialProviderService to ensure that only the system can bind to it.

Protection level: signature

Constant Value: "android.permission.BIND_CREDENTIAL_PROVIDER_SERVICE"

BIND_DATA_MIGRATION_FOR_PRIVATECOMPUTE

```
public static final String BIND_DATA_MIGRATION_FOR_PRIVATECOMPUTE
```

Allows the system to bind to an application's data migration service for Private Compute.

Protection level: signature

Constant Value: "android.permission.BIND_DATA_MIGRATION_FOR_PRIVATECOMPUTE"

BIND_DEVICE_ADMIN

```
public static final String BIND_DEVICE_ADMIN
```

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

Protection level: signature

Constant Value: "android.permission.BIND_DEVICE_ADMIN"

BIND_DREAM_SERVICE

```
public static final String BIND_DREAM_SERVICE
```

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

Protection level: signature

Constant Value: "android.permission.BIND_DREAM_SERVICE"

BIND_INCALL_SERVICE

```
public static final String BIND_INCALL_SERVICE
```

Must be required by a `InCallService`, to ensure that only the system can bind to it.

Protection level: signature|privileged

Constant Value: "android.permission.BIND_INCALL_SERVICE"

BIND_INPUT_METHOD

```
public static final String BIND_INPUT_METHOD
```

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

Protection level: signature

Constant Value: "android.permission.BIND_INPUT_METHOD"

BIND_MIDI_DEVICE_SERVICE

```
public static final String BIND_MIDI_DEVICE_SERVICE
```

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

Protection level: signature

Constant Value: "android.permission.BIND_MIDI_DEVICE_SERVICE"

BIND_NFC_SERVICE

```
public static final String BIND_NFC_SERVICE
```

Must be required by a `HostApduService` or `OffHostApduService` to ensure that only the system can bind to it.

Protection level: signature

Constant Value: "android.permission.BIND_NFC_SERVICE"

BIND_NOTIFICATION_LISTENER_SERVICE

```
public static final String BIND_NOTIFICATION_LISTENER_SERVICE
```

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

Protection level: signature

Constant Value: "android.permission.BIND_NOTIFICATION_LISTENER_SERVICE"

BIND_PRINT_SERVICE

```
public static final String BIND_PRINT_SERVICE
```

Must be required by a `PrintService`, to ensure that only the system can bind to it.

Protection level: signature

Constant Value: "android.permission.BIND_PRINT_SERVICE"

BIND_QUICK_ACCESS_WALLET_SERVICE

```
public static final String BIND_QUICK_ACCESS_WALLET_SERVICE
```

Must be required by a `QuickAccessWalletService` to ensure that only the system can bind to it.

Protection level: signature

Constant Value: "android.permission.BIND_QUICK_ACCESS_WALLET_SERVICE"

BIND_QUICK_SETTINGS_TILE

```
public static final String BIND_QUICK_SETTINGS_TILE
```

Allows an application to bind to third party quick settings tiles.

Should only be requested by the System, should be required by TileService declarations.

Constant Value: "android.permission.BIND_QUICK_SETTINGS_TILE"

BIND_REMOTEVIEWS

```
public static final String BIND_REMOTEVIEWS
```

Must be required by a `RemoteViewsService`, to ensure that only the system can bind to it.

Protection level: signature|privileged

Constant Value: "android.permission.BIND_REMOTEVIEWS"

BIND_SCREENING_SERVICE

```
public static final String BIND_SCREENING_SERVICE
```

Must be required by a `CallScreeningService`, to ensure that only the system can bind to it.

Protection level: signature|privileged

Constant Value: "android.permission.BIND_SCREENING_SERVICE"

BIND_TELECOM_CONNECTION_SERVICE

```
public static final String BIND_TELECOM_CONNECTION_SERVICE
```

Must be required by a `ConnectionService`, to ensure that only the system can bind to it.

Protection level: signature|privileged

Constant Value: "android.permission.BIND_TELECOM_CONNECTION_SERVICE"

BIND_TEXT_SERVICE

```
public static final String BIND_TEXT_SERVICE
```

Must be required by a TextService (e.g. SpellCheckerService) to ensure that only the system can bind to it.

Protection level: signature

Constant Value: "android.permission.BIND_TEXT_SERVICE"

BIND_TV_AD_SERVICE

```
public static final String BIND_TV_AD_SERVICE
```

Must be required by a android.media.tv.ad.TvAdService to ensure that only the system can bind to it.

Protection level: signature|privileged

Constant Value: "android.permission.BIND_TV_AD_SERVICE"

BIND_TV_INPUT

```
public static final String BIND_TV_INPUT
```

Must be required by a `TvInputService` to ensure that only the system can bind to it.

Protection level: signature|privileged

Constant Value: "android.permission.BIND_TV_INPUT"

BIND_TV_INTERACTIVE_APP

```
public static final String BIND_TV_INTERACTIVE_APP
```

Must be required by a `TvInteractiveAppService` to ensure that only the system can bind to it.

Protection level: signature|privileged

Constant Value: "android.permission.BIND_TV_INTERACTIVE_APP"

BIND_VISUAL_VOICEMAIL_SERVICE

```
public static final String BIND_VISUAL_VOICEMAIL_SERVICE
```

Must be required by a link `VisualVoicemailService` to ensure that only the system can bind to it.

Protection level: signature|privileged

Constant Value: "android.permission.BIND_VISUAL_VOICEMAIL_SERVICE"

BIND_VOICE_INTERACTION

```
public static final String BIND_VOICE_INTERACTION
```

Must be required by a `VoiceInteractionService`, to ensure that only the system can bind to it.

Protection level: signature

Constant Value: "android.permission.BIND_VOICE_INTERACTION"

BIND_VPN_SERVICE

```
public static final String BIND_VPN_SERVICE
```

Must be required by a `VpnService`, to ensure that only the system can bind to it.

Protection level: signature

Constant Value: "android.permission.BIND_VPN_SERVICE"

BIND_VR_LISTENER_SERVICE

```
public static final String BIND_VR_LISTENER_SERVICE
```

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

Protection level: signature

Constant Value: "android.permission.BIND_VR_LISTENER_SERVICE"

BIND_WALLPAPER

```
public static final String BIND_WALLPAPER
```

Must be required by a `WallpaperService`, to ensure that only the system can bind to it.

Protection level: signature|privileged

Constant Value: "android.permission.BIND_WALLPAPER"

BLUETOOTH

```
public static final String BLUETOOTH
```

Allows applications to connect to paired bluetooth devices.

Protection level: normal

Constant Value: "android.permission.BLUETOOTH"

BLUETOOTH_ADMIN

```
public static final String BLUETOOTH_ADMIN
```

Allows applications to discover and pair bluetooth devices.

Protection level: normal

Constant Value: "android.permission.BLUETOOTH_ADMIN"

BLUETOOTH_ADVERTISE

```
public static final String BLUETOOTH_ADVERTISE
```

Required to be able to advertise to nearby Bluetooth devices.

Protection level: dangerous

Constant Value: "android.permission.BLUETOOTH_ADVERTISE"

BLUETOOTH_CONNECT

```
public static final String BLUETOOTH_CONNECT
```

Required to be able to connect to paired Bluetooth devices.

Protection level: dangerous

Constant Value: "android.permission.BLUETOOTH_CONNECT"

BLUETOOTH_PRIVILEGED

```
public static final String BLUETOOTH_PRIVILEGED
```

Allows applications to pair bluetooth devices without user interaction, and to allow or disallow phonebook access or message access.

Not for use by third-party applications.

Constant Value: "android.permission.BLUETOOTH_PRIVILEGED"

BLUETOOTH_SCAN

```
public static final String BLUETOOTH_SCAN
```

Required to be able to discover and pair nearby Bluetooth devices.

Protection level: dangerous

Constant Value: "android.permission.BLUETOOTH_SCAN"

BODY_SENSORS

```
public static final String BODY_SENSORS
```

Allows an application to access data from sensors that the user uses to measure what is happening inside their body, such as heart rate.

Protection level: dangerous

Constant Value: "android.permission.BODY_SENSORS"

BODY_SENSORS_BACKGROUND

```
public static final String BODY_SENSORS_BACKGROUND
```

Allows an application to access data from sensors that the user uses to measure what is happening inside their body, such as heart rate. If you're requesting this permission, you must also request `BODY_SENSORS`. Requesting this permission by itself doesn't give you Body sensors access.

Protection level: dangerous

This is a hard restricted permission which cannot be held by an app until the installer on record allowlists the permission. For more details see `PackageInstaller.SessionParams.setWhitelistedRestrictedPermissions(Set)`.

Constant Value: "android.permission.BODY_SENSORS_BACKGROUND"

BROADCAST_PACKAGE_REMOVED

```
public static final String BROADCAST_PACKAGE_REMOVED
```

Allows an application to broadcast a notification that an application package has been removed.

Not for use by third-party applications.

Constant Value: "android.permission.BROADCAST_PACKAGE_REMOVED"

BROADCAST_SMS

```
public static final String BROADCAST_SMS
```

Allows an application to broadcast an SMS receipt notification.

Not for use by third-party applications.

Constant Value: "android.permission.BROADCAST_SMS"

BROADCAST_STICKY

```
public static final String BROADCAST_STICKY
```

Allows an application to broadcast sticky intents. These are broadcasts whose data is held by the system after being finished, so that clients can quickly retrieve that data without having to wait for the next broadcast.

Protection level: normal

Constant Value: "android.permission.BROADCAST_STICKY"

BROADCAST_WAP_PUSH

```
public static final String BROADCAST_WAP_PUSH
```

Allows an application to broadcast a WAP PUSH receipt notification.

Not for use by third-party applications.

Constant Value: "android.permission.BROADCAST_WAP_PUSH"

CALL_COMPANION_APP

```
public static final String CALL_COMPANION_APP
```

Allows an app which implements the `InCallService` API to be eligible to be enabled as a calling companion app. This means that the Telecom framework will bind to the app's InCallService implementation when there are calls active. The app can use the InCallService API to view information about calls on the system and control these calls.

Protection level: normal

Constant Value: "android.permission.CALL_COMPANION_APP"

CALL_PHONE

```
public static final String CALL_PHONE
```

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

Note: An app holding this permission can also call carrier MMI codes to change settings such as call forwarding or call waiting preferences.

Protection level: dangerous

Constant Value: "android.permission.CALL_PHONE"

CALL_PRIVILEGED

```
public static final String CALL_PRIVILEGED
```

Allows an application to call any phone number, including emergency numbers, without going through the Dialer user interface for the user to confirm the call being placed.

Not for use by third-party applications.

Constant Value: "android.permission.CALL_PRIVILEGED"

CAMERA

```
public static final String CAMERA
```

Required to be able to access the camera device.

This will automatically enforce the uses-feature manifest element for *all* camera features. If you do not require all camera features or can properly operate if a camera is not available, then you must modify your manifest as appropriate in order to install on devices that don't support all camera features.

Protection level: dangerous

Constant Value: "android.permission.CAMERA"

CAPTURE_AUDIO_OUTPUT

```
public static final String 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.

Not for use by third-party applications.

Constant Value: "android.permission.CAPTURE_AUDIO_OUTPUT"

CAPTURE_KEYBOARD

```
public static final String CAPTURE_KEYBOARD
```

Allows the currently focused application to be able to consume keys before Android system get chance to process system keys and shortcuts.

The keys are always sent to the currently focussed application, this permission allows the focussed application to receive the keys that are normally consumed by the system for shortcuts, allowing it to have custom shortcut behavior primarily for use cases like virtual machine apps where the host OS wants to handle the shortcuts differently.

Certain shortcuts and system keys like Home, Overview, Power, etc are never sent to the currently focused application and are always consumed by the system.

User can escape out of the capture mode by long pressing the Escape key or simply navigating out of the application.

Protection level: normal

Constant Value: "android.permission.CAPTURE_KEYBOARD"

CHANGE_COMPONENT_ENABLED_STATE

```
public static final String CHANGE_COMPONENT_ENABLED_STATE
```

Allows an application to change whether an application component (other than its own) is enabled or not.

Not for use by third-party applications.

Constant Value: "android.permission.CHANGE_COMPONENT_ENABLED_STATE"

CHANGE_CONFIGURATION

```
public static final String CHANGE_CONFIGURATION
```

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

Protection level: signature|privileged|development

Constant Value: "android.permission.CHANGE_CONFIGURATION"

CHANGE_NETWORK_STATE

```
public static final String CHANGE_NETWORK_STATE
```

Allows applications to change network connectivity state.

Protection level: normal

Constant Value: "android.permission.CHANGE_NETWORK_STATE"

CHANGE_WIFI_MULTICAST_STATE

```
public static final String CHANGE_WIFI_MULTICAST_STATE
```

Allows applications to enter Wi-Fi Multicast mode.

Protection level: normal

Constant Value: "android.permission.CHANGE_WIFI_MULTICAST_STATE"

CHANGE_WIFI_STATE

```
public static final String CHANGE_WIFI_STATE
```

Allows applications to change Wi-Fi connectivity state.

Protection level: normal

Constant Value: "android.permission.CHANGE_WIFI_STATE"

CLEAR_APP_CACHE

```
public static final String CLEAR_APP_CACHE
```

Allows an application to clear the caches of all installed applications on the device.

Protection level: signature|privileged

Constant Value: "android.permission.CLEAR_APP_CACHE"

CONFIGURE_WIFI_DISPLAY

```
public static final String CONFIGURE_WIFI_DISPLAY
```

Allows an application to configure and connect to Wifi displays

Constant Value: "android.permission.CONFIGURE_WIFI_DISPLAY"

CONTROL_LOCATION_UPDATES

```
public static final String CONTROL_LOCATION_UPDATES
```

Allows enabling/disabling location update notifications from the radio.

Not for use by third-party applications.

Constant Value: "android.permission.CONTROL_LOCATION_UPDATES"

CREDENTIAL_MANAGER_QUERY_CANDIDATE_CREDENTIALS

```
public static final String CREDENTIAL_MANAGER_QUERY_CANDIDATE_CREDENTIALS
```

Allows a browser to invoke the set of query apis to get metadata about credential candidates prepared during the CredentialManager.prepareGetCredential API.

Protection level: normal

Constant Value: "android.permission.CREDENTIAL_MANAGER_QUERY_CANDIDATE_CREDENTIALS"

CREDENTIAL_MANAGER_SET_ALLOWED_PROVIDERS

```
public static final String CREDENTIAL_MANAGER_SET_ALLOWED_PROVIDERS
```

Allows specifying candidate credential providers to be queried in Credential Manager get flows, or to be preferred as a default in the Credential Manager create flows.

Protection level: normal

Constant Value: "android.permission.CREDENTIAL_MANAGER_SET_ALLOWED_PROVIDERS"

CREDENTIAL_MANAGER_SET_ORIGIN

```
public static final String CREDENTIAL_MANAGER_SET_ORIGIN
```

Allows a browser to invoke credential manager APIs on behalf of another RP.

Protection level: normal

Constant Value: "android.permission.CREDENTIAL_MANAGER_SET_ORIGIN"

DELETE_CACHE_FILES

```
public static final String DELETE_CACHE_FILES
```

Old permission for deleting an app's cache files, no longer used, but signals for us to quietly ignore calls instead of throwing an exception.

Protection level: signature|privileged

Constant Value: "android.permission.DELETE_CACHE_FILES"

DELETE_PACKAGES

```
public static final String DELETE_PACKAGES
```

Allows an application to delete packages.

Not for use by third-party applications.

Starting in `Build.VERSION_CODES.N`, user confirmation is requested when the application deleting the package is not the same application that installed the package.

Constant Value: "android.permission.DELETE_PACKAGES"

DELIVER_COMPANION_MESSAGES

```
public static final String DELIVER_COMPANION_MESSAGES
```

Allows an application to deliver companion messages to system

Constant Value: "android.permission.DELIVER_COMPANION_MESSAGES"

DETECT_SCREEN_CAPTURE

```
public static final String DETECT_SCREEN_CAPTURE
```

Allows an application to get notified when a screen capture of its windows is attempted.

Protection level: normal

Constant Value: "android.permission.DETECT_SCREEN_CAPTURE"

DETECT_SCREEN_RECORDING

```
public static final String DETECT_SCREEN_RECORDING
```

Allows an application to get notified when it is being recorded.

Protection level: normal

Constant Value: "android.permission.DETECT_SCREEN_RECORDING"

DIAGNOSTIC

```
public static final String DIAGNOSTIC
```

Allows applications to RW to diagnostic resources.

Not for use by third-party applications.

Constant Value: "android.permission.DIAGNOSTIC"

DISABLE_KEYGUARD

```
public static final String DISABLE_KEYGUARD
```

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

Protection level: normal

Constant Value: "android.permission.DISABLE_KEYGUARD"

DUMP

```
public static final String DUMP
```

Allows an application to retrieve state dump information from system services.

Not for use by third-party applications.

Constant Value: "android.permission.DUMP"

EXECUTE_APP_ACTION

```
public static final String EXECUTE_APP_ACTION
```

Allows an assistive application to perform actions on behalf of users inside of applications.

For now, this permission is only granted to the Assistant application selected by the user.

Protection level: internal|role

Constant Value: "android.permission.EXECUTE_APP_ACTION"

EXECUTE_APP_FUNCTIONS

```
public static final String EXECUTE_APP_FUNCTIONS
```

Allows an application to perform actions on behalf of users inside of applications.

This permission is currently only granted to privileged system apps.

Protection level: internal|privileged

Constant Value: "android.permission.EXECUTE_APP_FUNCTIONS"

EXPAND_STATUS_BAR

```
public static final String EXPAND_STATUS_BAR
```

Allows an application to expand or collapse the status bar.

Protection level: normal

Constant Value: "android.permission.EXPAND_STATUS_BAR"

FACTORY_TEST

```
public static final String FACTORY_TEST
```

Run as a manufacturer test application, running as the root user. Only available when the device is running in manufacturer test mode.

Not for use by third-party applications.

Constant Value: "android.permission.FACTORY_TEST"

FOREGROUND_SERVICE

```
public static final String FOREGROUND_SERVICE
```

Allows a regular application to use `Service.startForeground` .

Protection level: normal

Constant Value: "android.permission.FOREGROUND_SERVICE"

FOREGROUND_SERVICE_CAMERA

```
public static final String FOREGROUND_SERVICE_CAMERA
```

Allows a regular application to use `Service.startForeground` with the type "camera".

Protection level: normal|instant

Constant Value: "android.permission.FOREGROUND_SERVICE_CAMERA"

FOREGROUND_SERVICE_CONNECTED_DEVICE

```
public static final String FOREGROUND_SERVICE_CONNECTED_DEVICE
```

Allows a regular application to use `Service.startForeground` with the type "connectedDevice".

Protection level: normal|instant

Constant Value: "android.permission.FOREGROUND_SERVICE_CONNECTED_DEVICE"

FOREGROUND_SERVICE_DATA_SYNC

```
public static final String FOREGROUND_SERVICE_DATA_SYNC
```

Allows a regular application to use `Service.startForeground` with the type "dataSync".

Protection level: normal|instant

Constant Value: "android.permission.FOREGROUND_SERVICE_DATA_SYNC"

FOREGROUND_SERVICE_HEALTH

```
public static final String FOREGROUND_SERVICE_HEALTH
```

Allows a regular application to use `Service.startForeground` with the type "health".

Protection level: normal|instant

Constant Value: "android.permission.FOREGROUND_SERVICE_HEALTH"

FOREGROUND_SERVICE_LOCATION

```
public static final String FOREGROUND_SERVICE_LOCATION
```

Allows a regular application to use `Service.startForeground` with the type "location".

Protection level: normal|instant

Constant Value: "android.permission.FOREGROUND_SERVICE_LOCATION"

FOREGROUND_SERVICE_MEDIA_PLAYBACK

```
public static final String FOREGROUND_SERVICE_MEDIA_PLAYBACK
```

Allows a regular application to use `Service.startForeground` with the type "mediaPlayback".

Protection level: normal|instant

Constant Value: "android.permission.FOREGROUND_SERVICE_MEDIA_PLAYBACK"

FOREGROUND_SERVICE_MEDIA_PROCESSING

```
public static final String FOREGROUND_SERVICE_MEDIA_PROCESSING
```

Allows a regular application to use `Service.startForeground` with the type "mediaProcessing".

Protection level: normal|instant

Constant Value: "android.permission.FOREGROUND_SERVICE_MEDIA_PROCESSING"

FOREGROUND_SERVICE_MEDIA_PROJECTION

```
public static final String FOREGROUND_SERVICE_MEDIA_PROJECTION
```

Allows a regular application to use `Service.startForeground` with the type "mediaProjection".

Protection level: normal|instant

Constant Value: "android.permission.FOREGROUND_SERVICE_MEDIA_PROJECTION"

FOREGROUND_SERVICE_MICROPHONE

```
public static final String FOREGROUND_SERVICE_MICROPHONE
```

Allows a regular application to use `Service.startForeground` with the type "microphone".

Protection level: normal|instant

Constant Value: "android.permission.FOREGROUND_SERVICE_MICROPHONE"

FOREGROUND_SERVICE_PHONE_CALL

```
public static final String FOREGROUND_SERVICE_PHONE_CALL
```

Allows a regular application to use `Service.startForeground` with the type "phoneCall".

Protection level: normal|instant

Constant Value: "android.permission.FOREGROUND_SERVICE_PHONE_CALL"

FOREGROUND_SERVICE_REMOTE_MESSAGING

```
public static final String FOREGROUND_SERVICE_REMOTE_MESSAGING
```

Allows a regular application to use `Service.startForeground` with the type "remoteMessaging".

Protection level: normal|instant

Constant Value: "android.permission.FOREGROUND_SERVICE_REMOTE_MESSAGING"

FOREGROUND_SERVICE_SPECIAL_USE

```
public static final String FOREGROUND_SERVICE_SPECIAL_USE
```

Allows a regular application to use `Service.startForeground` with the type "specialUse".

Protection level: normal|appop|instant

Constant Value: "android.permission.FOREGROUND_SERVICE_SPECIAL_USE"

FOREGROUND_SERVICE_SYSTEM_EXEMPTED

```
public static final String FOREGROUND_SERVICE_SYSTEM_EXEMPTED
```

Allows a regular application to use `Service.startForeground` with the type "systemExempted". Apps are allowed to use this type only in the use cases listed in `ServiceInfo.FOREGROUND_SERVICE_TYPE_SYSTEM_EXEMPTED` .

Protection level: normal|instant

Constant Value: "android.permission.FOREGROUND_SERVICE_SYSTEM_EXEMPTED"

GET_ACCOUNTS

```
public static final String GET_ACCOUNTS
```

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

Note: Beginning with Android 6.0 (API level 23), if an app shares the signature of the authenticator that manages an account, it does not need `"GET_ACCOUNTS"` permission to read information about that account. On Android 5.1 and lower, all apps need `"GET_ACCOUNTS"` permission to read information about any account.

Protection level: dangerous

Constant Value: "android.permission.GET_ACCOUNTS"

GET_ACCOUNTS_PRIVILEGED

```
public static final String GET_ACCOUNTS_PRIVILEGED
```

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

Protection level: signature|privileged

Constant Value: "android.permission.GET_ACCOUNTS_PRIVILEGED"

GET_PACKAGE_SIZE

```
public static final String GET_PACKAGE_SIZE
```

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

Protection level: normal

Constant Value: "android.permission.GET_PACKAGE_SIZE"

GET_TASKS

```
public static final String GET_TASKS
```

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

Constant Value: "android.permission.GET_TASKS"

GLOBAL_SEARCH

```
public static final String GLOBAL_SEARCH
```

This permission can be used on content providers to allow the global search system to access their data. Typically it used when the provider has some permissions protecting it (which global search would not be expected to hold), and added as a read-only permission to the path in the provider where global search queries are performed. This permission can not be held by regular applications; it is used by applications to protect themselves from everyone else besides global search.

Protection level: signature|privileged

Constant Value: "android.permission.GLOBAL_SEARCH"

HIDE_OVERLAY_WINDOWS

```
public static final String HIDE_OVERLAY_WINDOWS
```

Allows an app to prevent non-system-overlay windows from being drawn on top of it

Constant Value: "android.permission.HIDE_OVERLAY_WINDOWS"

HIGH_SAMPLING_RATE_SENSORS

```
public static final String HIGH_SAMPLING_RATE_SENSORS
```

Allows an app to access sensor data with a sampling rate greater than 200 Hz.

Protection level: normal

Constant Value: "android.permission.HIGH_SAMPLING_RATE_SENSORS"

INSTALL_LOCATION_PROVIDER

```
public static final String INSTALL_LOCATION_PROVIDER
```

Allows an application to install a location provider into the Location Manager.

Not for use by third-party applications.

Constant Value: "android.permission.INSTALL_LOCATION_PROVIDER"

INSTALL_PACKAGES

```
public static final String INSTALL_PACKAGES
```

Allows an application to install packages.

Not for use by third-party applications.

Constant Value: "android.permission.INSTALL_PACKAGES"

INSTALL_SHORTCUT

```
public static final String 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. Instead, you should create an app shortcut by using the `requestPinShortcut()` method from the `ShortcutManager` class.

Protection level: normal

Constant Value: "com.android.launcher.permission.INSTALL_SHORTCUT"

INSTANT_APP_FOREGROUND_SERVICE

```
public static final String INSTANT_APP_FOREGROUND_SERVICE
```

Allows an instant app to create foreground services.

Protection level: signature|development|instant|appop

Constant Value: "android.permission.INSTANT_APP_FOREGROUND_SERVICE"

INTERACT_ACROSS_PROFILES

```
public static final String INTERACT_ACROSS_PROFILES
```

Allows interaction across profiles in the same profile group.

Constant Value: "android.permission.INTERACT_ACROSS_PROFILES"

INTERNET

```
public static final String INTERNET
```

Allows applications to open network sockets.

Protection level: normal

Constant Value: "android.permission.INTERNET"

LAUNCH_CAPTURE_CONTENT_ACTIVITY_FOR_NOTE

```
public static final String LAUNCH_CAPTURE_CONTENT_ACTIVITY_FOR_NOTE
```

Allows an application to capture screen content to perform a screenshot using the intent action `Intent.ACTION_LAUNCH_CAPTURE_CONTENT_ACTIVITY_FOR_NOTE`.

Protection level: internal|role

Intended for use by ROLE_NOTES only.

Constant Value: "android.permission.LAUNCH_CAPTURE_CONTENT_ACTIVITY_FOR_NOTE"

LOADER_USAGE_STATS

```
public static final String LOADER_USAGE_STATS
```

Allows a data loader to read a package's access logs. The access logs contain the set of pages referenced over time.

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

Protection level: signature|privileged|appop

A data loader has to be the one which provides data to install an app.

A data loader has to have both permission:LOADER_USAGE_STATS AND appop:LOADER_USAGE_STATS allowed to be able to access the read logs.

Constant Value: "android.permission.LOADER_USAGE_STATS"

LOCATION_HARDWARE

```
public static final String LOCATION_HARDWARE
```

Allows an application to use location features in hardware, such as the geofencing api.

Not for use by third-party applications.

Constant Value: "android.permission.LOCATION_HARDWARE"

MANAGE_DEVICE_LOCK_STATE

```
public static final String MANAGE_DEVICE_LOCK_STATE
```

Allows financed device kiosk apps to perform actions on the Device Lock service

Protection level: internal|role

Intended for use by the FINANCED_DEVICE_KIOSK role only.

Constant Value: "android.permission.MANAGE_DEVICE_LOCK_STATE"

MANAGE_DEVICE_POLICY_ACCESSIBILITY

```
public static final String MANAGE_DEVICE_POLICY_ACCESSIBILITY
```

Allows an application to manage policy related to accessibility.

`Manifest.permission.MANAGE_DEVICE_POLICY_ACROSS_USERS_FULL` is required to call APIs protected by this permission on users different to the calling user.

Protection level: internal|role

Intended for use by the DEVICE_POLICY_MANAGEMENT role only.

Constant Value: "android.permission.MANAGE_DEVICE_POLICY_ACCESSIBILITY"

MANAGE_DEVICE_POLICY_ACCOUNT_MANAGEMENT

```
public static final String MANAGE_DEVICE_POLICY_ACCOUNT_MANAGEMENT
```

Allows an application to set policy related to account management.

`Manifest.permission.MANAGE_DEVICE_POLICY_ACROSS_USERS` is required to call APIs protected by this permission on users different to the calling user.

Protection level: internal|role

Intended for use by the DEVICE_POLICY_MANAGEMENT role only.

Constant Value: "android.permission.MANAGE_DEVICE_POLICY_ACCOUNT_MANAGEMENT"

MANAGE_DEVICE_POLICY_ACROSS_USERS

```
public static final String MANAGE_DEVICE_POLICY_ACROSS_USERS
```

Allows an application to set device policies outside the current user that are required for securing device ownership without accessing user data.

Holding this permission allows the use of other held MANAGE_DEVICE_POLICY_* permissions across all users on the device provided they do not grant access to user data.

Protection level: internal|role

Intended for use by the DEVICE_POLICY_MANAGEMENT role only.

Constant Value: "android.permission.MANAGE_DEVICE_POLICY_ACROSS_USERS"

MANAGE_DEVICE_POLICY_ACROSS_USERS_FULL

```
public static final String MANAGE_DEVICE_POLICY_ACROSS_USERS_FULL
```

Allows an application to set device policies outside the current user.

Fuller form of `MANAGE_DEVICE_POLICY_ACROSS_USERS` that removes the restriction on accessing user data.

Holding this permission allows the use of any other held MANAGE_DEVICE_POLICY_* permissions across all users on the device.

Protection level: internal|role

Intended for use by the DEVICE_POLICY_MANAGEMENT role only.

Constant Value: "android.permission.MANAGE_DEVICE_POLICY_ACROSS_USERS_FULL"

MANAGE_DEVICE_POLICY_ACROSS_USERS_SECURITY_CRITICAL

```
public static final String MANAGE_DEVICE_POLICY_ACROSS_USERS_SECURITY_CRITICAL
```

Allows an application to set device policies outside the current user that are critical for securing data within the current user.

Holding this permission allows the use of other held MANAGE_DEVICE_POLICY_* permissions across all users on the device provided they are required for securing data within the current user.

Protection level: internal|role

Intended for use by the DEVICE_POLICY_MANAGEMENT role only.

Constant Value: "android.permission.MANAGE_DEVICE_POLICY_ACROSS_USERS_SECURITY_CRITICAL"

MANAGE_DEVICE_POLICY_AIRPLANE_MODE

```
public static final String MANAGE_DEVICE_POLICY_AIRPLANE_MODE
```

Allows an application to set policy related to airplane mode.

`Manifest.permission.MANAGE_DEVICE_POLICY_ACROSS_USERS` is required to call APIs protected by this permission on users different to the calling user.

Protection level: internal|role

Intended for use by the DEVICE_POLICY_MANAGEMENT role only.

Constant Value: "android.permission.MANAGE_DEVICE_POLICY_AIRPLANE_MODE"

MANAGE_DEVICE_POLICY_APPS_CONTROL

```
public static final String MANAGE_DEVICE_POLICY_APPS_CONTROL
```

Allows an application to manage policy regarding modifying applications.

`Manifest.permission.MANAGE_DEVICE_POLICY_ACROSS_USERS_FULL` is required to call APIs protected by this permission on users different to the calling user.

Protection level: internal|role

Intended for use by the DEVICE_POLICY_MANAGEMENT role only.

Constant Value: "android.permission.MANAGE_DEVICE_POLICY_APPS_CONTROL"

MANAGE_DEVICE_POLICY_APP_FUNCTIONS

```
public static final String MANAGE_DEVICE_POLICY_APP_FUNCTIONS
```

Allows an application to manage policy related to AppFunctions.

Protection level: internal|role

Constant Value: "android.permission.MANAGE_DEVICE_POLICY_APP_FUNCTIONS"

MANAGE_DEVICE_POLICY_APP_RESTRICTIONS

```
public static final String MANAGE_DEVICE_POLICY_APP_RESTRICTIONS
```

Allows an application to manage application restrictions.

`Manifest.permission.MANAGE_DEVICE_POLICY_ACROSS_USERS_FULL` is required to call APIs protected by this permission on users different to the calling user.

Protection level: internal|role

Intended for use by the DEVICE_POLICY_MANAGEMENT role only.

Constant Value: "android.permission.MANAGE_DEVICE_POLICY_APP_RESTRICTIONS"

MANAGE_DEVICE_POLICY_APP_USER_DATA

```
public static final String MANAGE_DEVICE_POLICY_APP_USER_DATA
```

Allows an application to manage policy related to application user data.

`Manifest.permission.MANAGE_DEVICE_POLICY_ACROSS_USERS_FULL` is required to call APIs protected by this permission on users different to the calling user.

Protection level: internal|role

Intended for use by the DEVICE_POLICY_MANAGEMENT role only.

Constant Value: "android.permission.MANAGE_DEVICE_POLICY_APP_USER_DATA"

MANAGE_DEVICE_POLICY_ASSIST_CONTENT

```
public static final String MANAGE_DEVICE_POLICY_ASSIST_CONTENT
```

Allows an application to set policy related to sending assist content to a privileged app such as the Assistant app.

Protection level: internal|role

Intended for use by the DEVICE_POLICY_MANAGEMENT role only.

Constant Value: "android.permission.MANAGE_DEVICE_POLICY_ASSIST_CONTENT"

MANAGE_DEVICE_POLICY_AUDIO_OUTPUT

```
public static final String MANAGE_DEVICE_POLICY_AUDIO_OUTPUT
```

Allows an application to set policy related to audio output.

`Manifest.permission.MANAGE_DEVICE_POLICY_ACROSS_USERS_FULL` is required to call APIs protected by this permission on users different to the calling user.

Protection level: internal|role

Intended for use by the DEVICE_POLICY_MANAGEMENT role only.

Constant Value: "android.permission.MANAGE_DEVICE_POLICY_AUDIO_OUTPUT"

MANAGE_DEVICE_POLICY_AUTOFILL

```
public static final String MANAGE_DEVICE_POLICY_AUTOFILL
```

Allows an application to set policy related to autofill.

`Manifest.permission.MANAGE_DEVICE_POLICY_ACROSS_USERS_FULL` is required to call APIs protected by this permission on users different to the calling user.

Protection level: internal|role

Intended for use by the DEVICE_POLICY_MANAGEMENT role only.

Constant Value: "android.permission.MANAGE_DEVICE_POLICY_AUTOFILL"

MANAGE_DEVICE_POLICY_BACKUP_SERVICE

```
public static final String MANAGE_DEVICE_POLICY_BACKUP_SERVICE
```

Allows an application to manage backup service policy.

`Manifest.permission.MANAGE_DEVICE_POLICY_ACROSS_USERS_FULL` is required to call APIs protected by this permission on users different to the calling user.

Protection level: internal|role

Intended for use by the DEVICE_POLICY_MANAGEMENT role only.

Constant Value: "android.permission.MANAGE_DEVICE_POLICY_BACKUP_SERVICE"

MANAGE_DEVICE_POLICY_BLOCK_UNINSTALL

```
public static final String MANAGE_DEVICE_POLICY_BLOCK_UNINSTALL
```

Allows an application to manage policy related to block package uninstallation.

Protection level: internal|role

Intended for use by the DEVICE_POLICY_MANAGEMENT role only.

Constant Value: "android.permission.MANAGE_DEVICE_POLICY_BLOCK_UNINSTALL"

MANAGE_DEVICE_POLICY_BLUETOOTH

```
public static final String MANAGE_DEVICE_POLICY_BLUETOOTH
```

Allows an application to set policy related to bluetooth.

`Manifest.permission.MANAGE_DEVICE_POLICY_ACROSS_USERS_FULL` is required to call APIs protected by this permission on users different to the calling user.

Protection level: internal|role

Intended for use by the DEVICE_POLICY_MANAGEMENT role only.

Constant Value: "android.permission.MANAGE_DEVICE_POLICY_BLUETOOTH"

MANAGE_DEVICE_POLICY_BUGREPORT

```
public static final String MANAGE_DEVICE_POLICY_BUGREPORT
```

Allows an application to request bugreports with user consent.

`Manifest.permission.MANAGE_DEVICE_POLICY_ACROSS_USERS_FULL` is required to call APIs protected by this permission on users different to the calling user.

Protection level: internal|role

Intended for use by the DEVICE_POLICY_MANAGEMENT role only.

Constant Value: "android.permission.MANAGE_DEVICE_POLICY_BUGREPORT"

MANAGE_DEVICE_POLICY_CALLS

```
public static final String MANAGE_DEVICE_POLICY_CALLS
```

Allows an application to manage calling policy.

`Manifest.permission.MANAGE_DEVICE_POLICY_ACROSS_USERS_FULL` is required to call APIs protected by this permission on users different to the calling user.

Protection level: internal|role

Intended for use by the DEVICE_POLICY_MANAGEMENT role only.

Constant Value: "android.permission.MANAGE_DEVICE_POLICY_CALLS"

MANAGE_DEVICE_POLICY_CAMERA

```
public static final String MANAGE_DEVICE_POLICY_CAMERA
```

Allows an application to set policy related to restricting a user's ability to use or enable and disable the camera.

`Manifest.permission.MANAGE_DEVICE_POLICY_ACROSS_USERS` is required to call APIs protected by this permission on users different to the calling user.

Protection level: internal|role

Intended for use by the DEVICE_POLICY_MANAGEMENT role only.

Constant Value: "android.permission.MANAGE_DEVICE_POLICY_CAMERA"

MANAGE_DEVICE_POLICY_CAMERA_TOGGLE

```
public static final String MANAGE_DEVICE_POLICY_CAMERA_TOGGLE
```

Allows an application to manage policy related to camera toggle.

Protection level: internal|role

Intended for use by the DEVICE_POLICY_MANAGEMENT role only.

Constant Value: "android.permission.MANAGE_DEVICE_POLICY_CAMERA_TOGGLE"

MANAGE_DEVICE_POLICY_CERTIFICATES

```
public static final String MANAGE_DEVICE_POLICY_CERTIFICATES
```

Allows an application to set policy related to certificates.

`Manifest.permission.MANAGE_DEVICE_POLICY_ACROSS_USERS_FULL` is required to call APIs protected by this permission on users different to the calling user.

Protection level: internal|role

Intended for use by the DEVICE_POLICY_MANAGEMENT role only.

Constant Value: "android.permission.MANAGE_DEVICE_POLICY_CERTIFICATES"

MANAGE_DEVICE_POLICY_COMMON_CRITERIA_MODE

```
public static final String MANAGE_DEVICE_POLICY_COMMON_CRITERIA_MODE
```

Allows an application to manage policy related to common criteria mode.

`Manifest.permission.MANAGE_DEVICE_POLICY_ACROSS_USERS_FULL` is required to call APIs protected by this permission on users different to the calling user.

Protection level: internal|role

Intended for use by the DEVICE_POLICY_MANAGEMENT role only.

Constant Value: "android.permission.MANAGE_DEVICE_POLICY_COMMON_CRITERIA_MODE"

MANAGE_DEVICE_POLICY_CONTENT_PROTECTION

```
public static final String MANAGE_DEVICE_POLICY_CONTENT_PROTECTION
```

Allows an application to manage policy related to content protection.

Protection level: internal|role

Constant Value: "android.permission.MANAGE_DEVICE_POLICY_CONTENT_PROTECTION"

MANAGE_DEVICE_POLICY_DEBUGGING_FEATURES

```
public static final String MANAGE_DEVICE_POLICY_DEBUGGING_FEATURES
```

Allows an application to manage debugging features policy.

`Manifest.permission.MANAGE_DEVICE_POLICY_ACROSS_USERS_FULL` is required to call APIs protected by this permission on users different to the calling user.

Protection level: internal|role

Intended for use by the DEVICE_POLICY_MANAGEMENT role only.

Constant Value: "android.permission.MANAGE_DEVICE_POLICY_DEBUGGING_FEATURES"

MANAGE_DEVICE_POLICY_DEFAULT_SMS

```
public static final String MANAGE_DEVICE_POLICY_DEFAULT_SMS
```

Allows an application to set policy related to the default sms application.

`Manifest.permission.MANAGE_DEVICE_POLICY_ACROSS_USERS` is required to call APIs protected by this permission on users different to the calling user.

Protection level: internal|role

Intended for use by the DEVICE_POLICY_MANAGEMENT role only.

Constant Value: "android.permission.MANAGE_DEVICE_POLICY_DEFAULT_SMS"

MANAGE_DEVICE_POLICY_DEVICE_IDENTIFIERS

```
public static final String MANAGE_DEVICE_POLICY_DEVICE_IDENTIFIERS
```

Allows an application to manage policy related to device identifiers.

Protection level: internal|role

Intended for use by the DEVICE_POLICY_MANAGEMENT role only.

Constant Value: "android.permission.MANAGE_DEVICE_POLICY_DEVICE_IDENTIFIERS"

MANAGE_DEVICE_POLICY_DISPLAY

```
public static final String MANAGE_DEVICE_POLICY_DISPLAY
```

Allows an application to set policy related to the display.

`Manifest.permission.MANAGE_DEVICE_POLICY_ACROSS_USERS_FULL` is required to call APIs protected by this permission on users different to the calling user.

Protection level: internal|role

Intended for use by the DEVICE_POLICY_MANAGEMENT role only.

Constant Value: "android.permission.MANAGE_DEVICE_POLICY_DISPLAY"

MANAGE_DEVICE_POLICY_FACTORY_RESET

```
public static final String MANAGE_DEVICE_POLICY_FACTORY_RESET
```

Allows an application to set policy related to factory reset.

`Manifest.permission.MANAGE_DEVICE_POLICY_ACROSS_USERS_FULL` is required to call APIs protected by this permission on users different to the calling user.

Protection level: internal|role

Intended for use by the DEVICE_POLICY_MANAGEMENT role only.

Constant Value: "android.permission.MANAGE_DEVICE_POLICY_FACTORY_RESET"

MANAGE_DEVICE_POLICY_FUN

```
public static final String MANAGE_DEVICE_POLICY_FUN
```

Allows an application to set policy related to fun.

`Manifest.permission.MANAGE_DEVICE_POLICY_ACROSS_USERS_FULL` is required to call APIs protected by this permission on users different to the calling user.

Protection level: internal|role

Intended for use by the DEVICE_POLICY_MANAGEMENT role only.

Constant Value: "android.permission.MANAGE_DEVICE_POLICY_FUN"

MANAGE_DEVICE_POLICY_INPUT_METHODS

```
public static final String MANAGE_DEVICE_POLICY_INPUT_METHODS
```

Allows an application to set policy related to input methods.

`Manifest.permission.MANAGE_DEVICE_POLICY_ACROSS_USERS` is required to call APIs protected by this permission on users different to the calling user.

Protection level: internal|role

Intended for use by the DEVICE_POLICY_MANAGEMENT role only.

Constant Value: "android.permission.MANAGE_DEVICE_POLICY_INPUT_METHODS"

MANAGE_DEVICE_POLICY_INSTALL_UNKNOWN_SOURCES

```
public static final String MANAGE_DEVICE_POLICY_INSTALL_UNKNOWN_SOURCES
```

Allows an application to manage installing from unknown sources policy.

MANAGE_SECURITY_CRITICAL_DEVICE_POLICY_ACROSS_USERS is required to call APIs protected by this permission on users different to the calling user.

Protection level: internal|role

Intended for use by the DEVICE_POLICY_MANAGEMENT role only.

Constant Value: "android.permission.MANAGE_DEVICE_POLICY_INSTALL_UNKNOWN_SOURCES"

MANAGE_DEVICE_POLICY_KEEP_UNINSTALLED_PACKAGES

```
public static final String MANAGE_DEVICE_POLICY_KEEP_UNINSTALLED_PACKAGES
```

Allows an application to set policy related to keeping uninstalled packages.

`Manifest.permission.MANAGE_DEVICE_POLICY_ACROSS_USERS_FULL` is required to call APIs protected by this permission on users different to the calling user.

Protection level: internal|role

Intended for use by the DEVICE_POLICY_MANAGEMENT role only.

Constant Value: "android.permission.MANAGE_DEVICE_POLICY_KEEP_UNINSTALLED_PACKAGES"

MANAGE_DEVICE_POLICY_KEYGUARD

```
public static final String MANAGE_DEVICE_POLICY_KEYGUARD
```

Allows an application to manage policy related to keyguard features. Like whether the camera, notifications are allowed on the secure keyguard screens.

`Manifest.permission.MANAGE_DEVICE_POLICY_ACROSS_USERS_SECURITY_CRITICAL` is required to call APIs protected by this permission on users different to the calling user.

Protection level: internal|role

Intended for use by the DEVICE_POLICY_MANAGEMENT role only.

Constant Value: "android.permission.MANAGE_DEVICE_POLICY_KEYGUARD"

MANAGE_DEVICE_POLICY_LOCALE

```
public static final String MANAGE_DEVICE_POLICY_LOCALE
```

Allows an application to set policy related to locale.

`Manifest.permission.MANAGE_DEVICE_POLICY_ACROSS_USERS_FULL` is required to call APIs protected by this permission on users different to the calling user.

Protection level: internal|role

Intended for use by the DEVICE_POLICY_MANAGEMENT role only.

Constant Value: "android.permission.MANAGE_DEVICE_POLICY_LOCALE"

MANAGE_DEVICE_POLICY_LOCATION

```
public static final String MANAGE_DEVICE_POLICY_LOCATION
```

Allows an application to set policy related to location.

`Manifest.permission.MANAGE_DEVICE_POLICY_ACROSS_USERS_FULL` is required to call APIs protected by this permission on users different to the calling user.

Protection level: internal|role

Intended for use by the DEVICE_POLICY_MANAGEMENT role only.

Constant Value: "android.permission.MANAGE_DEVICE_POLICY_LOCATION"

MANAGE_DEVICE_POLICY_LOCK

```
public static final String MANAGE_DEVICE_POLICY_LOCK
```

Allows an application to lock a profile or the device with the appropriate cross-user permission.

`Manifest.permission.MANAGE_DEVICE_POLICY_ACROSS_USERS_FULL` is required to call APIs protected by this permission on users different to the calling user.

Protection level: internal|role

Intended for use by the DEVICE_POLICY_MANAGEMENT role only.

Constant Value: "android.permission.MANAGE_DEVICE_POLICY_LOCK"

MANAGE_DEVICE_POLICY_LOCK_CREDENTIALS

```
public static final String MANAGE_DEVICE_POLICY_LOCK_CREDENTIALS
```

Allows an application to set policy related to lock credentials.

`Manifest.permission.MANAGE_DEVICE_POLICY_ACROSS_USERS_SECURITY_CRITICAL` is required to call APIs protected by this permission on users different to the calling user.

Protection level: internal|role

Intended for use by the DEVICE_POLICY_MANAGEMENT role only.

Constant Value: "android.permission.MANAGE_DEVICE_POLICY_LOCK_CREDENTIALS"

MANAGE_DEVICE_POLICY_LOCK_TASK

```
public static final String MANAGE_DEVICE_POLICY_LOCK_TASK
```

Allows an application to manage lock task policy.

`Manifest.permission.MANAGE_DEVICE_POLICY_ACROSS_USERS_FULL` is required to call APIs protected by this permission on users different to the calling user.

Protection level: internal|role

Intended for use by the DEVICE_POLICY_MANAGEMENT role only.

Constant Value: "android.permission.MANAGE_DEVICE_POLICY_LOCK_TASK"

MANAGE_DEVICE_POLICY_MANAGED_SUBSCRIPTIONS

```
public static final String MANAGE_DEVICE_POLICY_MANAGED_SUBSCRIPTIONS
```

Allows an application to set policy related to subscriptions downloaded by an admin.

`Manifest.permission.MANAGE_DEVICE_POLICY_ACROSS_USERS_FULL` is required to call APIs protected by this permission on users different to the calling user.

Protection level: internal|role

Intended for use by the DEVICE_POLICY_MANAGEMENT role only.

Constant Value: "android.permission.MANAGE_DEVICE_POLICY_MANAGED_SUBSCRIPTIONS"

MANAGE_DEVICE_POLICY_METERED_DATA

```
public static final String MANAGE_DEVICE_POLICY_METERED_DATA
```

Allows an application to manage policy related to metered data.

`Manifest.permission.MANAGE_DEVICE_POLICY_ACROSS_USERS_FULL` is required to call APIs protected by this permission on users different to the calling user.

Protection level: internal|role

Intended for use by the DEVICE_POLICY_MANAGEMENT role only.

Constant Value: "android.permission.MANAGE_DEVICE_POLICY_METERED_DATA"

MANAGE_DEVICE_POLICY_MICROPHONE

```
public static final String MANAGE_DEVICE_POLICY_MICROPHONE
```

Allows an application to set policy related to restricting a user's ability to use or enable and disable the microphone.

`Manifest.permission.MANAGE_DEVICE_POLICY_ACROSS_USERS` is required to call APIs protected by this permission on users different to the calling user.

Protection level: internal|role

Intended for use by the DEVICE_POLICY_MANAGEMENT role only.

Constant Value: "android.permission.MANAGE_DEVICE_POLICY_MICROPHONE"

MANAGE_DEVICE_POLICY_MICROPHONE_TOGGLE

```
public static final String MANAGE_DEVICE_POLICY_MICROPHONE_TOGGLE
```

Allows an application to manage policy related to microphone toggle.

Protection level: internal|role

Intended for use by the DEVICE_POLICY_MANAGEMENT role only.

Constant Value: "android.permission.MANAGE_DEVICE_POLICY_MICROPHONE_TOGGLE"

MANAGE_DEVICE_POLICY_MOBILE_NETWORK

```
public static final String MANAGE_DEVICE_POLICY_MOBILE_NETWORK
```

Allows an application to set policy related to mobile networks.

`Manifest.permission.MANAGE_DEVICE_POLICY_ACROSS_USERS_FULL` is required to call APIs protected by this permission on users different to the calling user.

Protection level: internal|role

Intended for use by the DEVICE_POLICY_MANAGEMENT role only.

Constant Value: "android.permission.MANAGE_DEVICE_POLICY_MOBILE_NETWORK"

MANAGE_DEVICE_POLICY_MODIFY_USERS

```
public static final String MANAGE_DEVICE_POLICY_MODIFY_USERS
```

Allows an application to manage policy preventing users from modifying users.

`Manifest.permission.MANAGE_DEVICE_POLICY_ACROSS_USERS_FULL` is required to call APIs protected by this permission on users different to the calling user

Protection level: internal|role

Intended for use by the DEVICE_POLICY_MANAGEMENT role only.

Constant Value: "android.permission.MANAGE_DEVICE_POLICY_MODIFY_USERS"

MANAGE_DEVICE_POLICY_MTE

```
public static final String MANAGE_DEVICE_POLICY_MTE
```

Allows an application to manage policy related to the Memory Tagging Extension (MTE).

Protection level: internal|role

Intended for use by the DEVICE_POLICY_MANAGEMENT role only.

Constant Value: "android.permission.MANAGE_DEVICE_POLICY_MTE"

MANAGE_DEVICE_POLICY_NEARBY_COMMUNICATION

```
public static final String MANAGE_DEVICE_POLICY_NEARBY_COMMUNICATION
```

Allows an application to set policy related to nearby communications (e.g. Beam and nearby streaming).

`Manifest.permission.MANAGE_DEVICE_POLICY_ACROSS_USERS_FULL` is required to call APIs protected by this permission on users different to the calling user.

Protection level: internal|role

Intended for use by the DEVICE_POLICY_MANAGEMENT role only.

Constant Value: "android.permission.MANAGE_DEVICE_POLICY_NEARBY_COMMUNICATION"

MANAGE_DEVICE_POLICY_NETWORK_LOGGING

```
public static final String MANAGE_DEVICE_POLICY_NETWORK_LOGGING
```

Allows an application to set policy related to network logging.

`Manifest.permission.MANAGE_DEVICE_POLICY_ACROSS_USERS_FULL` is required to call APIs protected by this permission on users different to the calling user.

Protection level: internal|role

Intended for use by the DEVICE_POLICY_MANAGEMENT role only.

Constant Value: "android.permission.MANAGE_DEVICE_POLICY_NETWORK_LOGGING"

MANAGE_DEVICE_POLICY_ORGANIZATION_IDENTITY

```
public static final String MANAGE_DEVICE_POLICY_ORGANIZATION_IDENTITY
```

Allows an application to manage the identity of the managing organization.

`Manifest.permission.MANAGE_DEVICE_POLICY_ACROSS_USERS_FULL` is required to call APIs protected by this permission on users different to the calling user.

Protection level: internal|role

Intended for use by the DEVICE_POLICY_MANAGEMENT role only.

Constant Value: "android.permission.MANAGE_DEVICE_POLICY_ORGANIZATION_IDENTITY"

MANAGE_DEVICE_POLICY_OVERRIDE_APN

```
public static final String MANAGE_DEVICE_POLICY_OVERRIDE_APN
```

Allows an application to set policy related to override APNs.

`Manifest.permission.MANAGE_DEVICE_POLICY_ACROSS_USERS_FULL` is required to call APIs protected by this permission on users different to the calling user.

Protection level: internal|role

Intended for use by the DEVICE_POLICY_MANAGEMENT role only.

Constant Value: "android.permission.MANAGE_DEVICE_POLICY_OVERRIDE_APN"

MANAGE_DEVICE_POLICY_PACKAGE_STATE

```
public static final String MANAGE_DEVICE_POLICY_PACKAGE_STATE
```

Allows an application to set policy related to hiding and suspending packages.

`Manifest.permission.MANAGE_DEVICE_POLICY_ACROSS_USERS` is required to call APIs protected by this permission on users different to the calling user.

Protection level: internal|role

Intended for use by the DEVICE_POLICY_MANAGEMENT role only.

Constant Value: "android.permission.MANAGE_DEVICE_POLICY_PACKAGE_STATE"

MANAGE_DEVICE_POLICY_PHYSICAL_MEDIA

```
public static final String MANAGE_DEVICE_POLICY_PHYSICAL_MEDIA
```

Allows an application to set policy related to physical media.

`Manifest.permission.MANAGE_DEVICE_POLICY_ACROSS_USERS_FULL` is required to call APIs protected by this permission on users different to the calling user.

Protection level: internal|role

Intended for use by the DEVICE_POLICY_MANAGEMENT role only.

Constant Value: "android.permission.MANAGE_DEVICE_POLICY_PHYSICAL_MEDIA"

MANAGE_DEVICE_POLICY_PRINTING

```
public static final String MANAGE_DEVICE_POLICY_PRINTING
```

Allows an application to set policy related to printing.

`Manifest.permission.MANAGE_DEVICE_POLICY_ACROSS_USERS_FULL` is required to call APIs protected by this permission on users different to the calling user.

Protection level: internal|role

Intended for use by the DEVICE_POLICY_MANAGEMENT role only.

Constant Value: "android.permission.MANAGE_DEVICE_POLICY_PRINTING"

MANAGE_DEVICE_POLICY_PRIVATE_DNS

```
public static final String MANAGE_DEVICE_POLICY_PRIVATE_DNS
```

Allows an application to set policy related to private DNS.

`Manifest.permission.MANAGE_DEVICE_POLICY_ACROSS_USERS_FULL` is required to call APIs protected by this permission on users different to the calling user.

Protection level: internal|role

Intended for use by the DEVICE_POLICY_MANAGEMENT role only.

Constant Value: "android.permission.MANAGE_DEVICE_POLICY_PRIVATE_DNS"

MANAGE_DEVICE_POLICY_PROFILES

```
public static final String MANAGE_DEVICE_POLICY_PROFILES
```

Allows an application to set policy related to profiles.

`Manifest.permission.MANAGE_DEVICE_POLICY_ACROSS_USERS_FULL` is required to call APIs protected by this permission on users different to the calling user.

Protection level: internal|role

Intended for use by the DEVICE_POLICY_MANAGEMENT role only.

Constant Value: "android.permission.MANAGE_DEVICE_POLICY_PROFILES"

MANAGE_DEVICE_POLICY_PROFILE_INTERACTION

```
public static final String MANAGE_DEVICE_POLICY_PROFILE_INTERACTION
```

Allows an application to set policy related to interacting with profiles (e.g. Disallowing cross-profile copy and paste).

`Manifest.permission.MANAGE_DEVICE_POLICY_ACROSS_USERS_FULL` is required to call APIs protected by this permission on users different to the calling user.

Protection level: internal|role

Intended for use by the DEVICE_POLICY_MANAGEMENT role only.

Constant Value: "android.permission.MANAGE_DEVICE_POLICY_PROFILE_INTERACTION"

MANAGE_DEVICE_POLICY_PROXY

```
public static final String MANAGE_DEVICE_POLICY_PROXY
```

Allows an application to set a network-independent global HTTP proxy.

`Manifest.permission.MANAGE_DEVICE_POLICY_ACROSS_USERS_FULL` is required to call APIs protected by this permission on users different to the calling user.

Protection level: internal|role

Intended for use by the DEVICE_POLICY_MANAGEMENT role only.

Constant Value: "android.permission.MANAGE_DEVICE_POLICY_PROXY"

MANAGE_DEVICE_POLICY_QUERY_SYSTEM_UPDATES

```
public static final String MANAGE_DEVICE_POLICY_QUERY_SYSTEM_UPDATES
```

Allows an application query system updates.

`Manifest.permission.MANAGE_DEVICE_POLICY_ACROSS_USERS_FULL` is required to call APIs protected by this permission on users different to the calling user.

Protection level: internal|role

Intended for use by the DEVICE_POLICY_MANAGEMENT role only.

Constant Value: "android.permission.MANAGE_DEVICE_POLICY_QUERY_SYSTEM_UPDATES"

MANAGE_DEVICE_POLICY_RESET_PASSWORD

```
public static final String MANAGE_DEVICE_POLICY_RESET_PASSWORD
```

Allows an application to force set a new device unlock password or a managed profile challenge on current user.

`Manifest.permission.MANAGE_DEVICE_POLICY_ACROSS_USERS_FULL` is required to call APIs protected by this permission on users different to the calling user.

Protection level: internal|role

Intended for use by the DEVICE_POLICY_MANAGEMENT role only.

Constant Value: "android.permission.MANAGE_DEVICE_POLICY_RESET_PASSWORD"

MANAGE_DEVICE_POLICY_RESTRICT_PRIVATE_DNS

```
public static final String MANAGE_DEVICE_POLICY_RESTRICT_PRIVATE_DNS
```

Allows an application to set policy related to restricting the user from configuring private DNS.

`Manifest.permission.MANAGE_DEVICE_POLICY_ACROSS_USERS` is required to call APIs protected by this permission on users different to the calling user.

Protection level: internal|role

Intended for use by the DEVICE_POLICY_MANAGEMENT role only.

Constant Value: "android.permission.MANAGE_DEVICE_POLICY_RESTRICT_PRIVATE_DNS"

MANAGE_DEVICE_POLICY_RUNTIME_PERMISSIONS

```
public static final String MANAGE_DEVICE_POLICY_RUNTIME_PERMISSIONS
```

Allows an application to set the grant state of runtime permissions on packages.

`Manifest.permission.MANAGE_DEVICE_POLICY_ACROSS_USERS_FULL` is required to call APIs protected by this permission on users different to the calling user.

Protection level: internal|role

Intended for use by the DEVICE_POLICY_MANAGEMENT role only.

Constant Value: "android.permission.MANAGE_DEVICE_POLICY_RUNTIME_PERMISSIONS"

MANAGE_DEVICE_POLICY_RUN_IN_BACKGROUND

```
public static final String MANAGE_DEVICE_POLICY_RUN_IN_BACKGROUND
```

Allows an application to set policy related to users running in the background.

`Manifest.permission.MANAGE_DEVICE_POLICY_ACROSS_USERS_FULL` is required to call APIs protected by this permission on users different to the calling user.

Protection level: internal|role

Intended for use by the DEVICE_POLICY_MANAGEMENT role only.

Constant Value: "android.permission.MANAGE_DEVICE_POLICY_RUN_IN_BACKGROUND"

MANAGE_DEVICE_POLICY_SAFE_BOOT

```
public static final String MANAGE_DEVICE_POLICY_SAFE_BOOT
```

Allows an application to manage safe boot policy.

`Manifest.permission.MANAGE_DEVICE_POLICY_ACROSS_USERS_FULL` is required to call APIs protected by this permission on users different to the calling user.

Protection level: internal|role

Intended for use by the DEVICE_POLICY_MANAGEMENT role only.

Constant Value: "android.permission.MANAGE_DEVICE_POLICY_SAFE_BOOT"

MANAGE_DEVICE_POLICY_SCREEN_CAPTURE

```
public static final String MANAGE_DEVICE_POLICY_SCREEN_CAPTURE
```

Allows an application to set policy related to screen capture.

`Manifest.permission.MANAGE_DEVICE_POLICY_ACROSS_USERS` is required to call APIs protected by this permission on users different to the calling user.

Protection level: internal|role

Intended for use by the DEVICE_POLICY_MANAGEMENT role only.

Constant Value: "android.permission.MANAGE_DEVICE_POLICY_SCREEN_CAPTURE"

MANAGE_DEVICE_POLICY_SCREEN_CONTENT

```
public static final String MANAGE_DEVICE_POLICY_SCREEN_CONTENT
```

Allows an application to set policy related to the usage of the contents of the screen.

`Manifest.permission.MANAGE_DEVICE_POLICY_ACROSS_USERS_FULL` is required to call APIs protected by this permission on users different to the calling user.

Protection level: internal|role

Intended for use by the DEVICE_POLICY_MANAGEMENT role only.

Constant Value: "android.permission.MANAGE_DEVICE_POLICY_SCREEN_CONTENT"

MANAGE_DEVICE_POLICY_SECURITY_LOGGING

```
public static final String MANAGE_DEVICE_POLICY_SECURITY_LOGGING
```

Allows an application to set policy related to security logging.

`Manifest.permission.MANAGE_DEVICE_POLICY_ACROSS_USERS_FULL` is required to call APIs protected by this permission on users different to the calling user.

Protection level: internal|role

Intended for use by the DEVICE_POLICY_MANAGEMENT role only.

Constant Value: "android.permission.MANAGE_DEVICE_POLICY_SECURITY_LOGGING"

MANAGE_DEVICE_POLICY_SETTINGS

```
public static final String MANAGE_DEVICE_POLICY_SETTINGS
```

Allows an application to set policy related to settings.

`Manifest.permission.MANAGE_DEVICE_POLICY_ACROSS_USERS_FULL` is required to call APIs protected by this permission on users different to the calling user.

Protection level: internal|role

Intended for use by the DEVICE_POLICY_MANAGEMENT role only.

Constant Value: "android.permission.MANAGE_DEVICE_POLICY_SETTINGS"

MANAGE_DEVICE_POLICY_SMS

```
public static final String MANAGE_DEVICE_POLICY_SMS
```

Allows an application to set policy related to sms.

`Manifest.permission.MANAGE_DEVICE_POLICY_ACROSS_USERS_FULL` is required to call APIs protected by this permission on users different to the calling user.

Protection level: internal|role

Intended for use by the DEVICE_POLICY_MANAGEMENT role only.

Constant Value: "android.permission.MANAGE_DEVICE_POLICY_SMS"

MANAGE_DEVICE_POLICY_STATUS_BAR

```
public static final String MANAGE_DEVICE_POLICY_STATUS_BAR
```

Allows an application to set policy related to the status bar.

Protection level: internal|role

Intended for use by the DEVICE_POLICY_MANAGEMENT role only.

Constant Value: "android.permission.MANAGE_DEVICE_POLICY_STATUS_BAR"

MANAGE_DEVICE_POLICY_SUPPORT_MESSAGE

```
public static final String MANAGE_DEVICE_POLICY_SUPPORT_MESSAGE
```

Allows an application to set support messages for when a user action is affected by an active policy.

`Manifest.permission.MANAGE_DEVICE_POLICY_ACROSS_USERS_FULL` is required to call APIs protected by this permission on users different to the calling user.

Protection level: internal|role

Intended for use by the DEVICE_POLICY_MANAGEMENT role only.

Constant Value: "android.permission.MANAGE_DEVICE_POLICY_SUPPORT_MESSAGE"

MANAGE_DEVICE_POLICY_SUSPEND_PERSONAL_APPS

```
public static final String MANAGE_DEVICE_POLICY_SUSPEND_PERSONAL_APPS
```

Allows an application to set policy related to suspending personal apps.

`Manifest.permission.MANAGE_DEVICE_POLICY_ACROSS_USERS_FULL` is required to call APIs protected by this permission on users different to the calling user.

Protection level: internal|role

Intended for use by the DEVICE_POLICY_MANAGEMENT role only.

Constant Value: "android.permission.MANAGE_DEVICE_POLICY_SUSPEND_PERSONAL_APPS"

MANAGE_DEVICE_POLICY_SYSTEM_APPS

```
public static final String MANAGE_DEVICE_POLICY_SYSTEM_APPS
```

Allows an application to manage policy related to system apps.

`Manifest.permission.MANAGE_DEVICE_POLICY_ACROSS_USERS_FULL` is required to call APIs protected by this permission on users different to the calling user.

Protection level: internal|role

Intended for use by the DEVICE_POLICY_MANAGEMENT role only.

Constant Value: "android.permission.MANAGE_DEVICE_POLICY_SYSTEM_APPS"

MANAGE_DEVICE_POLICY_SYSTEM_DIALOGS

```
public static final String MANAGE_DEVICE_POLICY_SYSTEM_DIALOGS
```

Allows an application to set policy related to system dialogs.

`Manifest.permission.MANAGE_DEVICE_POLICY_ACROSS_USERS_FULL` is required to call APIs protected by this permission on users different to the calling user.

Protection level: internal|role

Intended for use by the DEVICE_POLICY_MANAGEMENT role only.

Constant Value: "android.permission.MANAGE_DEVICE_POLICY_SYSTEM_DIALOGS"

MANAGE_DEVICE_POLICY_SYSTEM_UPDATES

```
public static final String MANAGE_DEVICE_POLICY_SYSTEM_UPDATES
```

Allows an application to set policy related to system updates.

`Manifest.permission.MANAGE_DEVICE_POLICY_ACROSS_USERS_FULL` is required to call APIs protected by this permission on users different to the calling user.

Protection level: internal|role

Intended for use by the DEVICE_POLICY_MANAGEMENT role only.

Constant Value: "android.permission.MANAGE_DEVICE_POLICY_SYSTEM_UPDATES"

MANAGE_DEVICE_POLICY_THREAD_NETWORK

```
public static final String MANAGE_DEVICE_POLICY_THREAD_NETWORK
```

Allows an application to set policy related to Thread network.

Protection level: internal|role

Intended for use by the DEVICE_POLICY_MANAGEMENT role only.

Constant Value: "android.permission.MANAGE_DEVICE_POLICY_THREAD_NETWORK"

MANAGE_DEVICE_POLICY_TIME

```
public static final String MANAGE_DEVICE_POLICY_TIME
```

Allows an application to manage device policy relating to time.

`Manifest.permission.MANAGE_DEVICE_POLICY_ACROSS_USERS_FULL` is required to call APIs protected by this permission on users different to the calling user.

Protection level: internal|role

Intended for use by the DEVICE_POLICY_MANAGEMENT role only.

Constant Value: "android.permission.MANAGE_DEVICE_POLICY_TIME"

MANAGE_DEVICE_POLICY_USB_DATA_SIGNALLING

```
public static final String MANAGE_DEVICE_POLICY_USB_DATA_SIGNALLING
```

Allows an application to set policy related to usb data signalling.

Protection level: internal|role

Intended for use by the DEVICE_POLICY_MANAGEMENT role only.

Constant Value: "android.permission.MANAGE_DEVICE_POLICY_USB_DATA_SIGNALLING"

MANAGE_DEVICE_POLICY_USB_FILE_TRANSFER

```
public static final String MANAGE_DEVICE_POLICY_USB_FILE_TRANSFER
```

Allows an application to set policy related to usb file transfers.

`Manifest.permission.MANAGE_DEVICE_POLICY_ACROSS_USERS_FULL` is required to call APIs protected by this permission on users different to the calling user.

Protection level: internal|role

Intended for use by the DEVICE_POLICY_MANAGEMENT role only.

Constant Value: "android.permission.MANAGE_DEVICE_POLICY_USB_FILE_TRANSFER"

MANAGE_DEVICE_POLICY_USERS

```
public static final String MANAGE_DEVICE_POLICY_USERS
```

Allows an application to set policy related to users.

`Manifest.permission.MANAGE_DEVICE_POLICY_ACROSS_USERS_FULL` is required to call APIs protected by this permission on users different to the calling user.

Protection level: internal|role

Intended for use by the DEVICE_POLICY_MANAGEMENT role only.

Constant Value: "android.permission.MANAGE_DEVICE_POLICY_USERS"

MANAGE_DEVICE_POLICY_VPN

```
public static final String MANAGE_DEVICE_POLICY_VPN
```

Allows an application to set policy related to VPNs.

`Manifest.permission.MANAGE_DEVICE_POLICY_ACROSS_USERS_FULL` is required to call APIs protected by this permission on users different to the calling user.

Protection level: internal|role

Intended for use by the DEVICE_POLICY_MANAGEMENT role only.

Constant Value: "android.permission.MANAGE_DEVICE_POLICY_VPN"

MANAGE_DEVICE_POLICY_WALLPAPER

```
public static final String MANAGE_DEVICE_POLICY_WALLPAPER
```

Allows an application to set policy related to the wallpaper.

`Manifest.permission.MANAGE_DEVICE_POLICY_ACROSS_USERS_FULL` is required to call APIs protected by this permission on users different to the calling user.

Protection level: internal|role

Intended for use by the DEVICE_POLICY_MANAGEMENT role only.

Constant Value: "android.permission.MANAGE_DEVICE_POLICY_WALLPAPER"

MANAGE_DEVICE_POLICY_WIFI

```
public static final String MANAGE_DEVICE_POLICY_WIFI
```

Allows an application to set policy related to Wifi.

`Manifest.permission.MANAGE_DEVICE_POLICY_ACROSS_USERS` is required to call APIs protected by this permission on users different to the calling user.

Protection level: internal|role

Intended for use by the DEVICE_POLICY_MANAGEMENT role only.

Constant Value: "android.permission.MANAGE_DEVICE_POLICY_WIFI"

MANAGE_DEVICE_POLICY_WINDOWS

```
public static final String MANAGE_DEVICE_POLICY_WINDOWS
```

Allows an application to set policy related to windows.

`Manifest.permission.MANAGE_DEVICE_POLICY_ACROSS_USERS_FULL` is required to call APIs protected by this permission on users different to the calling user.

Protection level: internal|role

Intended for use by the DEVICE_POLICY_MANAGEMENT role only.

Constant Value: "android.permission.MANAGE_DEVICE_POLICY_WINDOWS"

MANAGE_DEVICE_POLICY_WIPE_DATA

```
public static final String MANAGE_DEVICE_POLICY_WIPE_DATA
```

Allows an application to manage policy related to wiping data.

`Manifest.permission.MANAGE_DEVICE_POLICY_ACROSS_USERS` is required to call APIs protected by this permission on users different to the calling user.

Protection level: internal|role

Intended for use by the DEVICE_POLICY_MANAGEMENT role only.

Constant Value: "android.permission.MANAGE_DEVICE_POLICY_WIPE_DATA"

MANAGE_DOCUMENTS

```
public static final String MANAGE_DOCUMENTS
```

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

This permission should *only* be held by the platform document management app and the shell (for CTS). This permission cannot be granted to third-party apps.

Constant Value: "android.permission.MANAGE_DOCUMENTS"

MANAGE_EXTERNAL_STORAGE

```
public static final String MANAGE_EXTERNAL_STORAGE
```

Allows an application a broad access to external storage in scoped storage. Intended to be used by few apps that need to manage files on behalf of the users.

Protection level: signature|appop|preinstalled

Constant Value: "android.permission.MANAGE_EXTERNAL_STORAGE"

MANAGE_ONGOING_CALLS

```
public static final String MANAGE_ONGOING_CALLS
```

Allows to query ongoing call details and manage ongoing calls

Protection level: signature|appop

Constant Value: "android.permission.MANAGE_ONGOING_CALLS"

MANAGE_OWN_CALLS

```
public static final String MANAGE_OWN_CALLS
```

Allows a calling application which manages its own calls through the self-managed `ConnectionService` APIs. See `PhoneAccount.CAPABILITY_SELF_MANAGED` for more information on the self-managed ConnectionService APIs.

Protection level: normal

Constant Value: "android.permission.MANAGE_OWN_CALLS"

MANAGE_WIFI_INTERFACES

```
public static final String MANAGE_WIFI_INTERFACES
```

Allows applications to get notified when a Wi-Fi interface request cannot be satisfied without tearing down one or more other interfaces, and provide a decision whether to approve the request or reject it.

Not for use by third-party applications.

Constant Value: "android.permission.MANAGE_WIFI_INTERFACES"

MANAGE_WIFI_NETWORK_SELECTION

```
public static final String MANAGE_WIFI_NETWORK_SELECTION
```

This permission is used to let OEMs grant their trusted app access to a subset of privileged wifi APIs to improve wifi performance. Allows applications to manage Wi-Fi network selection related features such as enable or disable global auto-join, modify connectivity scan intervals, and approve Wi-Fi Direct connections.

Not for use by third-party applications.

Constant Value: "android.permission.MANAGE_WIFI_NETWORK_SELECTION"

MASTER_CLEAR

```
public static final String MASTER_CLEAR
```

Not for use by third-party applications.

Constant Value: "android.permission.MASTER_CLEAR"

MEDIA_CONTENT_CONTROL

```
public static final String MEDIA_CONTENT_CONTROL
```

Allows an application to know what content is playing and control its playback.

Not for use by third-party applications due to privacy of media consumption

Constant Value: "android.permission.MEDIA_CONTENT_CONTROL"

MEDIA_ROUTING_CONTROL

```
public static final String MEDIA_ROUTING_CONTROL
```

Allows an application to control the routing of media apps.

Only for use by role COMPANION_DEVICE_WATCH

Constant Value: "android.permission.MEDIA_ROUTING_CONTROL"

MODIFY_AUDIO_SETTINGS

```
public static final String MODIFY_AUDIO_SETTINGS
```

Allows an application to modify global audio settings.

Protection level: normal

Constant Value: "android.permission.MODIFY_AUDIO_SETTINGS"

MODIFY_PHONE_STATE

```
public static final String MODIFY_PHONE_STATE
```

Allows modification of the telephony state - power on, mmi, etc. Does not include placing calls.

Not for use by third-party applications.

Constant Value: "android.permission.MODIFY_PHONE_STATE"

MOUNT_FORMAT_FILESYSTEMS

```
public static final String MOUNT_FORMAT_FILESYSTEMS
```

Allows formatting file systems for removable storage.

Not for use by third-party applications.

Constant Value: "android.permission.MOUNT_FORMAT_FILESYSTEMS"

MOUNT_UNMOUNT_FILESYSTEMS

```
public static final String MOUNT_UNMOUNT_FILESYSTEMS
```

Allows mounting and unmounting file systems for removable storage.

Not for use by third-party applications.

Constant Value: "android.permission.MOUNT_UNMOUNT_FILESYSTEMS"

NEARBY_WIFI_DEVICES

```
public static final String NEARBY_WIFI_DEVICES
```

Required to be able to advertise and connect to nearby devices via Wi-Fi.

Protection level: dangerous

Constant Value: "android.permission.NEARBY_WIFI_DEVICES"

NFC

```
public static final String NFC
```

Allows applications to perform I/O operations over NFC.

Protection level: normal

Constant Value: "android.permission.NFC"

NFC_PREFERRED_PAYMENT_INFO

```
public static final String NFC_PREFERRED_PAYMENT_INFO
```

Allows applications to receive NFC preferred payment service information.

Protection level: normal

Constant Value: "android.permission.NFC_PREFERRED_PAYMENT_INFO"

NFC_TRANSACTION_EVENT

```
public static final String NFC_TRANSACTION_EVENT
```

Allows applications to receive NFC transaction events.

Protection level: normal

Constant Value: "android.permission.NFC_TRANSACTION_EVENT"

OVERRIDE_MEDIA_SESSION_OWNER

```
public static final String OVERRIDE_MEDIA_SESSION_OWNER
```

Allows an application to override the owner of a MediaSession.

Not for use by third-party applications due to privacy of media applications.

Constant Value: "android.permission.OVERRIDE_MEDIA_SESSION_OWNER"

OVERRIDE_WIFI_CONFIG

```
public static final String OVERRIDE_WIFI_CONFIG
```

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.

Constant Value: "android.permission.OVERRIDE_WIFI_CONFIG"

PACKAGE_USAGE_STATS

```
public static final String 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.

Protection level: signature|privileged|development|appop|retailDemo

Constant Value: "android.permission.PACKAGE_USAGE_STATS"

PERSISTENT_ACTIVITY

```
public static final String PERSISTENT_ACTIVITY
```

This constant was deprecated in API level 15.
This functionality will be removed in the future; please do not use. Allow an application to make its activities persistent.

Constant Value: "android.permission.PERSISTENT_ACTIVITY"

POST_NOTIFICATIONS

```
public static final String POST_NOTIFICATIONS
```

Allows an app to post notifications

Protection level: dangerous

Constant Value: "android.permission.POST_NOTIFICATIONS"

POST_PROMOTED_NOTIFICATIONS

```
public static final String POST_PROMOTED_NOTIFICATIONS
```

Required for apps to post promoted notifications.

This is required in addition to (not instead of) `POST_NOTIFICATIONS`.

Protection level: normal|appops

Constant Value: "android.permission.POST_PROMOTED_NOTIFICATIONS"

PROCESS_OUTGOING_CALLS

```
public static final String PROCESS_OUTGOING_CALLS
```

This constant was deprecated in API level 29.
Applications should use `CallRedirectionService` instead of the `Intent.ACTION_NEW_OUTGOING_CALL` broadcast.

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.

Protection level: dangerous

This is a hard restricted permission which cannot be held by an app until the installer on record allowlists the permission. For more details see
`PackageInstaller.SessionParams.setWhitelistedRestrictedPermissions(Set)`.

Constant Value: "android.permission.PROCESS_OUTGOING_CALLS"

PROVIDE_OWN_AUTOFILL_SUGGESTIONS

```
public static final String PROVIDE_OWN_AUTOFILL_SUGGESTIONS
```

Allows an application to display its suggestions using the autofill framework.

For now, this permission is only granted to the Browser application.

Protection level: internal|role

Constant Value: "android.permission.PROVIDE_OWN_AUTOFILL_SUGGESTIONS"

PROVIDE_PRIVATE_COMPUTE_SERVICES

```
public static final String PROVIDE_PRIVATE_COMPUTE_SERVICES
```

Allows an application to act as Private Compute Services, which allows the application to communicate with Private Compute Core components.

Protection level: signature|privileged

Constant Value: "android.permission.PROVIDE_PRIVATE_COMPUTE_SERVICES"

PROVIDE_REMOTE_CREDENTIALS

```
public static final String PROVIDE_REMOTE_CREDENTIALS
```

Allows an application to be able to store and retrieve credentials from a remote device.

Protection level: signature|privileged|role

Constant Value: "android.permission.PROVIDE_REMOTE_CREDENTIALS"

QUERY_ADVANCED_PROTECTION_MODE

```
public static final String QUERY_ADVANCED_PROTECTION_MODE
```

Allows an application to query the device's advanced protection mode status.

Constant Value: "android.permission.QUERY_ADVANCED_PROTECTION_MODE"

QUERY_ALL_PACKAGES

```
public static final String QUERY_ALL_PACKAGES
```

Allows query of any normal app on the device, regardless of manifest declarations.

Protection level: normal

Constant Value: "android.permission.QUERY_ALL_PACKAGES"

RANGING

```
public static final String RANGING
```

Required to be able to range to devices using generic ranging module.

Protection level: dangerous

Constant Value: "android.permission.RANGING"

READ_ASSISTANT_APP_SEARCH_DATA

```
public static final String READ_ASSISTANT_APP_SEARCH_DATA
```

Allows an application to query over global data in AppSearch that's visible to the ASSISTANT role.

Constant Value: "android.permission.READ_ASSISTANT_APP_SEARCH_DATA"

READ_ASSIST_STRUCTURE_SCREEN_CONTENT

```
public static final String READ_ASSIST_STRUCTURE_SCREEN_CONTENT
```

Allows an assistant application to read screen content in the AssistStructure.

Note: Beginning with `ERROR(C android.os.Build.VERSION_CODES.CINNAMON_BUN /Android C android.os.Build.VERSION_CODES.CINNAMON_BUN)` This permission is required by any VoiceInteractionService that wishes to receive screen content in the AssistStructure when the assistant's VoiceInteractionService is invoked either via hotword detection or from the system. If this permission is not held, the AssistStructure will only obtain window data and will omit any screen content from the provided AssistStructure.

Protection level: normal

Constant Value: "android.permission.READ_ASSIST_STRUCTURE_SCREEN_CONTENT"

READ_BASIC_PHONE_STATE

```
public static final String READ_BASIC_PHONE_STATE
```

Allows read only access to phone state with a non dangerous permission, including the information like cellular network type, software version.

Constant Value: "android.permission.READ_BASIC_PHONE_STATE"

READ_CALENDAR

```
public static final String READ_CALENDAR
```

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

Protection level: dangerous

Constant Value: "android.permission.READ_CALENDAR"

READ_COLOR_ZONES

```
public static final String READ_COLOR_ZONES
```

Allows an application to read the aggregated color zones on the screen for use cases like TV ambient backlight usages.

Protection level: normal

Constant Value: "android.permission.READ_COLOR_ZONES"

READ_CONTACTS

```
public static final String READ_CONTACTS
```

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

Protection level: dangerous

Constant Value: "android.permission.READ_CONTACTS"

READ_DROPBOX_DATA

```
public static final String READ_DROPBOX_DATA
```

Allows an application to access the data in Dropbox.

Not for use by third-party applications.

Constant Value: "android.permission.READ_DROPBOX_DATA"

READ_EXTERNAL_STORAGE

```
public static final String READ_EXTERNAL_STORAGE
```

Allows an application to read from external storage.

Note: Starting in API level 33, this permission has no effect. If your app accesses other apps' media files, request one or more of these permissions instead: `READ_MEDIA_IMAGES`, `READ_MEDIA_VIDEO`, `READ_MEDIA_AUDIO`. Learn more about the storage permissions that are associated with media files.

This permission is enforced starting in API level 19. Before API level 19, this permission is not enforced and all apps still have access to read from external storage. You can test your app with the permission enforced by enabling *Protect USB storage* under **Developer options** in the Settings app on a device running Android 4.1 or higher.

Also starting in API level 19, this permission is *not* required to read or write files in your application-specific directories returned by `Context.getExternalFilesDir(String)` and `Context.getExternalCacheDir()`.

Starting in API level 29, apps don't need to request this permission to access files in their app-specific directory on external storage, or their own files in the `MediaStore`. Apps shouldn't request this permission unless they need to access other apps' files in the `MediaStore`. Read more about these changes in the scoped storage section of the developer documentation.

If *both* your `minSdkVersion` and `targetSdkVersion` values are set to 3 or lower, the system implicitly grants your app this permission. If you don't need this permission, be sure your `targetSdkVersion` is 4 or higher.

This is a soft restricted permission which cannot be held by an app it its full form until the installer on record allowlists the permission. Specifically, if the permission is allowlisted the holder app can access external storage and the visual and aural media collections while if the permission is not allowlisted the holder app can only access to the visual and aural medial collections. Also the permission is immutably restricted meaning that the allowlist state can be specified only at install time and cannot change until the app is installed. For more details see `PackageInstaller.SessionParams.setWhitelistedRestrictedPermissions(Set)`.

Protection level: dangerous

Constant Value: "android.permission.READ_EXTERNAL_STORAGE"

READ_HOME_APP_SEARCH_DATA

```
public static final String READ_HOME_APP_SEARCH_DATA
```

Allows an application to query over global data in AppSearch that's visible to the HOME role.

Constant Value: "android.permission.READ_HOME_APP_SEARCH_DATA"

READ_INPUT_STATE

```
public static final String READ_INPUT_STATE
```

This constant was deprecated in API level 16.
The API that used this permission has been removed.

Allows an application to retrieve the current state of keys and switches.

Not for use by third-party applications.

Constant Value: "android.permission.READ_INPUT_STATE"

READ_LOGS

```
public static final String READ_LOGS
```

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

Not for use by third-party applications, because Log entries can contain the user's private information.

Constant Value: "android.permission.READ_LOGS"

READ_MEDIA_VISUAL_USER_SELECTED

```
public static final String READ_MEDIA_VISUAL_USER_SELECTED
```

Allows an application to read image or video files from external storage that a user has selected via the permission prompt photo picker. Apps can check this permission to verify that a user has decided to use the photo picker, instead of granting access to `READ_MEDIA_IMAGES` or `READ_MEDIA_VIDEO`. It does not prevent apps from accessing the standard photo picker manually. This permission should be requested alongside `READ_MEDIA_IMAGES` and/or `READ_MEDIA_VIDEO`, depending on which type of media is desired.

This permission will be automatically added to an app's manifest if the app requests `READ_MEDIA_IMAGES`, `READ_MEDIA_VIDEO`, or `ACCESS_MEDIA_LOCATION` regardless of target SDK. If an app does not request this permission, then the grant dialog will return `PERMISSION_GRANTED` for `READ_MEDIA_IMAGES` and/or `READ_MEDIA_VIDEO`, but the app will only have access to the media selected by the user. This false grant state will persist until the app goes into the background.

Protection level: dangerous

Constant Value: "android.permission.READ_MEDIA_VISUAL_USER_SELECTED"

READ_PHONE_NUMBERS

```
public static final String READ_PHONE_NUMBERS
```

Allows read access to the device's phone number(s), which is exposed to instant applications.

Protection level: dangerous

Constant Value: "android.permission.READ_PHONE_NUMBERS"

READ_PHONE_STATE

```
public static final String 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 `PhoneAccount`s registered on the device.

Note: If *both* your `minSdkVersion` and `targetSdkVersion` values are set to 3 or lower, the system implicitly grants your app this permission. If you don't need this permission, be sure your `targetSdkVersion` is 4 or higher.

Protection level: dangerous

Constant Value: "android.permission.READ_PHONE_STATE"

READ_PRECISE_PHONE_STATE

```
public static final String READ_PRECISE_PHONE_STATE
```

Allows read only access to precise phone state. Allows reading of detailed information about phone state for special-use applications such as dialers, carrier applications, or ims applications.

Constant Value: "android.permission.READ_PRECISE_PHONE_STATE"

READ_SYNC_SETTINGS

```
public static final String READ_SYNC_SETTINGS
```

Allows applications to read the sync settings.

Protection level: normal

Constant Value: "android.permission.READ_SYNC_SETTINGS"

READ_SYNC_STATS

```
public static final String READ_SYNC_STATS
```

Allows applications to read the sync stats.

Protection level: normal

Constant Value: "android.permission.READ_SYNC_STATS"

READ_SYSTEM_PREFERENCES

```
public static final String READ_SYSTEM_PREFERENCES
```

Allows an application to access the Settings Preference services to read settings exposed by the system Settings app and system apps that contribute settings surfaced by the Settings app.

This allows the calling application to read settings values through the host application, agnostic of underlying storage.

Constant Value: "android.permission.READ_SYSTEM_PREFERENCES"

READ_VOICEMAIL

```
public static final String READ_VOICEMAIL
```

Allows an application to read voicemails in the system.

Protection level: signature|privileged|role

Constant Value: "com.android.voicemail.permission.READ_VOICEMAIL"

REBOOT

```
public static final String REBOOT
```

Required to be able to reboot the device.

Not for use by third-party applications.

Constant Value: "android.permission.REBOOT"

RECEIVE_BOOT_COMPLETED

```
public static final String RECEIVE_BOOT_COMPLETED
```

Allows an application to receive the `Intent.ACTION_BOOT_COMPLETED` that is broadcast after the system finishes booting. If you don't request this permission, you will not receive the broadcast at that time. Though holding this permission does not have any security implications, it can have a negative impact on the user experience by increasing the amount of time it takes the system to start and allowing applications to have themselves running without the user being aware of them. As such, you must explicitly declare your use of this facility to make that visible to the user.

Protection level: normal

Constant Value: "android.permission.RECEIVE_BOOT_COMPLETED"

RECEIVE_MMS

```
public static final String RECEIVE_MMS
```

Allows an application to monitor incoming MMS messages.

Protection level: dangerous

This is a hard restricted permission which cannot be held by an app until the installer on record allowlists the permission. For more details see `PackageInstaller.SessionParams.setWhitelistedRestrictedPermissions(Set)` .

Constant Value: "android.permission.RECEIVE_MMS"

RECEIVE_SENSITIVE_NOTIFICATIONS

```
public static final String RECEIVE_SENSITIVE_NOTIFICATIONS
```

Allows apps with a NotificationListenerService to receive notifications with sensitive information

Apps with a NotificationListenerService without this permission will not be able to view certain types of sensitive information contained in notifications

This permission also allows apps with the SMS permissions to query and receive broadcasts about SMS messages that contain One Time Passwords

Protection level: signature|preinstalled|knownSigner|role

Constant Value: "android.permission.RECEIVE_SENSITIVE_NOTIFICATIONS"

RECEIVE_SMS

```
public static final String RECEIVE_SMS
```

Allows an application to receive SMS messages.

Protection level: dangerous

This is a hard restricted permission which cannot be held by an app until the installer on record allowlists the permission. For more details see `PackageInstaller.SessionParams.setWhitelistedRestrictedPermissions(Set)` .

Constant Value: "android.permission.RECEIVE_SMS"

RECEIVE_WAP_PUSH

```
public static final String RECEIVE_WAP_PUSH
```

Allows an application to receive WAP push messages.

Protection level: dangerous

This is a hard restricted permission which cannot be held by an app until the installer on record allowlists the permission. For more details see `PackageInstaller.SessionParams.setWhitelistedRestrictedPermissions(Set)` .

Constant Value: "android.permission.RECEIVE_WAP_PUSH"

RECORD_AUDIO

```
public static final String RECORD_AUDIO
```

Allows an application to record audio.

Protection level: dangerous

Constant Value: "android.permission.RECORD_AUDIO"

REORDER_TASKS

```
public static final String REORDER_TASKS
```

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

Protection level: normal

Constant Value: "android.permission.REORDER_TASKS"

REPOSITION_SELF_WINDOWS

```
public static final String REPOSITION_SELF_WINDOWS
```

Allows an application to programmatically move and resize its tasks when the system is in a state that allows such operations, e.g. in a desktop-like environment. It is only extended to the `default browser` and OEM specific signature apps.

Protection level: signature|role

Constant Value: "android.permission.REPOSITION_SELF_WINDOWS"

REQUEST_COMPANION_PROFILE_APP_STREAMING

```
public static final String REQUEST_COMPANION_PROFILE_APP_STREAMING
```

Allows application to request to be associated with a virtual device capable of streaming Android applications (`AssociationRequest.DEVICE_PROFILE_APP_STREAMING`) by `CompanionDeviceManager` .

Not for use by third-party applications.

Constant Value: "android.permission.REQUEST_COMPANION_PROFILE_APP_STREAMING"

REQUEST_COMPANION_PROFILE_AUTOMOTIVE_PROJECTION

```
public static final String REQUEST_COMPANION_PROFILE_AUTOMOTIVE_PROJECTION
```

Allows application to request to be associated with a vehicle head unit capable of automotive projection (`AssociationRequest.DEVICE_PROFILE_AUTOMOTIVE_PROJECTION`) by `CompanionDeviceManager` .

Not for use by third-party applications.

Constant Value: "android.permission.REQUEST_COMPANION_PROFILE_AUTOMOTIVE_PROJECTION"

REQUEST_COMPANION_PROFILE_COMPUTER

```
public static final String REQUEST_COMPANION_PROFILE_COMPUTER
```

Allows application to request to be associated with a computer to share functionality and/or data with other devices, such as notifications, photos and media (`AssociationRequest.DEVICE_PROFILE_COMPUTER`) by `CompanionDeviceManager` .

Not for use by third-party applications.

Constant Value: "android.permission.REQUEST_COMPANION_PROFILE_COMPUTER"

REQUEST_COMPANION_PROFILE_GLASSES

```
public static final String REQUEST_COMPANION_PROFILE_GLASSES
```

Allows app to request to be associated with a device via `CompanionDeviceManager` as "glasses"

Protection level: normal

Constant Value: "android.permission.REQUEST_COMPANION_PROFILE_GLASSES"

REQUEST_COMPANION_PROFILE_NEARBY_DEVICE_STREAMING

```
public static final String REQUEST_COMPANION_PROFILE_NEARBY_DEVICE_STREAMING
```

Allows application to request to stream content from an Android host to a nearby device (`AssociationRequest.DEVICE_PROFILE_NEARBY_DEVICE_STREAMING`) by `CompanionDeviceManager` .

Not for use by third-party applications.

Constant Value: "android.permission.REQUEST_COMPANION_PROFILE_NEARBY_DEVICE_STREAMING"

REQUEST_COMPANION_PROFILE_WATCH

```
public static final String REQUEST_COMPANION_PROFILE_WATCH
```

Allows app to request to be associated with a device via `CompanionDeviceManager` as a "watch"

Protection level: normal

Constant Value: "android.permission.REQUEST_COMPANION_PROFILE_WATCH"

REQUEST_COMPANION_SELF_MANAGED

```
public static final String REQUEST_COMPANION_SELF_MANAGED
```

Allows an application to create a "self-managed" association.

Constant Value: "android.permission.REQUEST_COMPANION_SELF_MANAGED"

REQUEST_COMPANION_START_FOREGROUND_SERVICES_FROM_BACKGROUND

```
public static final String REQUEST_COMPANION_START_FOREGROUND_SERVICES_FROM_BACKGROUND
```

Allows a companion app to start a foreground service from the background.

Protection level: normal

Constant Value: "android.permission.REQUEST_COMPANION_START_FOREGROUND_SERVICES_FROM_BACKGROUND"

REQUEST_COMPANION_USE_DATA_IN_BACKGROUND

```
public static final String REQUEST_COMPANION_USE_DATA_IN_BACKGROUND
```

Allows a companion app to use data in the background.

Protection level: normal

Constant Value: "android.permission.REQUEST_COMPANION_USE_DATA_IN_BACKGROUND"

REQUEST_IGNORE_BATTERY_OPTIMIZATIONS

```
public static final String REQUEST_IGNORE_BATTERY_OPTIMIZATIONS
```

Permission an application must hold in order to use `Settings.ACTION_REQUEST_IGNORE_BATTERY_OPTIMIZATIONS`.

Protection level: normal

Constant Value: "android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS"

REQUEST_INSTALL_PACKAGES

```
public static final String REQUEST_INSTALL_PACKAGES
```

Allows an application to request installing packages. Apps targeting APIs greater than 25 must hold this permission in order to use `Intent.ACTION_INSTALL_PACKAGE`.

Protection level: signature

Constant Value: "android.permission.REQUEST_INSTALL_PACKAGES"

REQUEST_OBSERVE_COMPANION_DEVICE_PRESENCE

```
public static final String REQUEST_OBSERVE_COMPANION_DEVICE_PRESENCE
```

Allows an application to subscribe to notifications about the presence status change of their associated companion device

Constant Value: "android.permission.REQUEST_OBSERVE_COMPANION_DEVICE_PRESENCE"

REQUEST_OBSERVE_DEVICE_UUID_PRESENCE

```
public static final String REQUEST_OBSERVE_DEVICE_UUID_PRESENCE
```

Allows an application to subscribe to notifications about the nearby devices' presence status change base on the UUIDs.

Not for use by third-party applications.

Constant Value: "android.permission.REQUEST_OBSERVE_DEVICE_UUID_PRESENCE"

REQUEST_PASSWORD_COMPLEXITY

```
public static final String REQUEST_PASSWORD_COMPLEXITY
```

Allows an application to request the screen lock complexity and prompt users to update the screen lock to a certain complexity level.

Protection level: normal

Constant Value: "android.permission.REQUEST_PASSWORD_COMPLEXITY"

RESTART_PACKAGES

```
public static final String RESTART_PACKAGES
```

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

Constant Value: "android.permission.RESTART_PACKAGES"

RUN_USER_INITIATED_JOBS

```
public static final String RUN_USER_INITIATED_JOBS
```

Allows applications to use the user-initiated jobs API. For more details see `JobInfo.Builder.setUserInitiated(boolean)`.

Protection level: normal

Constant Value: "android.permission.RUN_USER_INITIATED_JOBS"

SCHEDULE_EXACT_ALARM

```
public static final String SCHEDULE_EXACT_ALARM
```

Allows applications to use exact alarm APIs.

This is a special access permission that can be revoked by the system or the user. It should only be used to enable **user-facing features** that require exact alarms. For more details, please go through the associated developer docs.

Apps need to target API `Build.VERSION_CODES.S` or above to be able to request this permission. Note that apps targeting lower API levels do not need this permission to use exact alarm APIs.

Apps that hold this permission and target API `Build.VERSION_CODES.TIRAMISU` and below always stay in the `WORKING_SET` or lower standby bucket.

If your app relies on exact alarms for core functionality, it can instead request `USE_EXACT_ALARM` once it targets API `Build.VERSION_CODES.TIRAMISU`. All apps using exact alarms for secondary features (which should still be user facing) should continue using this permission.

Protection level: signature|privileged|appop

Constant Value: "android.permission.SCHEDULE_EXACT_ALARM"

SEND_RESPOND_VIA_MESSAGE

```
public static final String SEND_RESPOND_VIA_MESSAGE
```

Allows an application (Phone) to send a request to other applications to handle the respond-via-message action during incoming calls.

Not for use by third-party applications.

Constant Value: "android.permission.SEND_RESPOND_VIA_MESSAGE"

SET_ALARM

```
public static final String SET_ALARM
```

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

Protection level: normal

Constant Value: "com.android.alarm.permission.SET_ALARM"

SET_ALWAYS_FINISH

```
public static final String SET_ALWAYS_FINISH
```

Allows an application to control whether activities are immediately finished when put in the background.

Not for use by third-party applications.

Constant Value: "android.permission.SET_ALWAYS_FINISH"

SET_ANIMATION_SCALE

```
public static final String SET_ANIMATION_SCALE
```

Modify the global animation scaling factor.

Not for use by third-party applications.

Constant Value: "android.permission.SET_ANIMATION_SCALE"

SET_BIOMETRIC_DIALOG_ADVANCED

```
public static final String SET_BIOMETRIC_DIALOG_ADVANCED
```

Allows an application to set the advanced features on BiometricDialog (SystemUI), including logo, logo description, and content view with more options button.

Not for use by third-party applications.

Constant Value: "android.permission.SET_BIOMETRIC_DIALOG_ADVANCED"

SET_DEBUG_APP

```
public static final String SET_DEBUG_APP
```

Configure an application for debugging.

Not for use by third-party applications.

Constant Value: "android.permission.SET_DEBUG_APP"

SET_PREFERRED_APPLICATIONS

```
public static final String SET_PREFERRED_APPLICATIONS
```

This constant was deprecated in API level 15.
No longer useful, see `PackageManager.addPackageToPreferred(String)` for details.

Constant Value: "android.permission.SET_PREFERRED_APPLICATIONS"

SET_PROCESS_LIMIT

```
public static final String SET_PROCESS_LIMIT
```

Allows an application to set the maximum number of (not needed) application processes that can be running.

Not for use by third-party applications.

Constant Value: "android.permission.SET_PROCESS_LIMIT"

SET_TIME

```
public static final String SET_TIME
```

Allows applications to set the system time directly.

Not for use by third-party applications.

Constant Value: "android.permission.SET_TIME"

SET_TIME_ZONE

```
public static final String SET_TIME_ZONE
```

Allows applications to set the system time zone directly.

Not for use by third-party applications.

Constant Value: "android.permission.SET_TIME_ZONE"

SET_WALLPAPER

```
public static final String SET_WALLPAPER
```

Allows applications to set the wallpaper.

Protection level: normal

Constant Value: "android.permission.SET_WALLPAPER"

SET_WALLPAPER_HINTS

```
public static final String SET_WALLPAPER_HINTS
```

Allows applications to set the wallpaper hints.

Protection level: normal

Constant Value: "android.permission.SET_WALLPAPER_HINTS"

```
public static final String SHOW_POWER_MENU
```

Permission needed to request to show the Power Menu.

Granted to the current holder of the ASSISTANT role.

Constant Value: "android.permission.SHOW_POWER_MENU"

```
public static final String SHOW_POWER_MENU_PRIVILEGED
```

Permission needed to request to show the Power Menu.

Granted to certain privileged apps.

Constant Value: "android.permission.SHOW_POWER_MENU_PRIVILEGED"

SIGNAL_PERSISTENT_PROCESSES

```
public static final String SIGNAL_PERSISTENT_PROCESSES
```

Allow an application to request that a signal be sent to all persistent processes.

Not for use by third-party applications.

Constant Value: "android.permission.SIGNAL_PERSISTENT_PROCESSES"

SMS_FINANCIAL_TRANSACTIONS

```
public static final String SMS_FINANCIAL_TRANSACTIONS
```

This constant was deprecated in API level 31.
The API that used this permission is no longer functional.

Allows financial apps to read filtered sms messages. Protection level: signature|appop

Constant Value: "android.permission.SMS_FINANCIAL_TRANSACTIONS"

START_FOREGROUND_SERVICES_FROM_BACKGROUND

```
public static final String START_FOREGROUND_SERVICES_FROM_BACKGROUND
```

Allows an application to start foreground services from the background at any time. *This permission is not for use by third-party applications*, with the only exception being if the app is the default SMS app. Otherwise, it's only usable by privileged apps, app verifier app, and apps with any of the EMERGENCY or SYSTEM GALLERY roles.

Constant Value: "android.permission.START_FOREGROUND_SERVICES_FROM_BACKGROUND"

START_VIEW_APP_FEATURES

```
public static final String START_VIEW_APP_FEATURES
```

Allows the holder to start the screen with a list of app features.

Protection level: signature|installer

Constant Value: "android.permission.START_VIEW_APP_FEATURES"

START_VIEW_PERMISSION_USAGE

```
public static final String START_VIEW_PERMISSION_USAGE
```

Allows the holder to start the permission usage screen for an app.

Protection level: signature|installer

Constant Value: "android.permission.START_VIEW_PERMISSION_USAGE"

STATUS_BAR

```
public static final String STATUS_BAR
```

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

Not for use by third-party applications.

Constant Value: "android.permission.STATUS_BAR"

SUBSCRIBE_TO_KEYGUARD_LOCKED_STATE

```
public static final String SUBSCRIBE_TO_KEYGUARD_LOCKED_STATE
```

Allows an application to subscribe to device locked and keyguard locked (i.e., showing) state.

Protection level: signature|privileged|module|role

Intended for use by ROLE_ASSISTANT, VDM, and signature / privileged apps only.

Constant Value: "android.permission.SUBSCRIBE_TO_KEYGUARD_LOCKED_STATE"

SYSTEM_ALERT_WINDOW

```
public static final String SYSTEM_ALERT_WINDOW
```

Allows an app to create windows using the type `WindowManager.LayoutParams.TYPE_APPLICATION_OVERLAY`, shown on top of all other apps. Very few apps should use this permission; these windows are intended for system-level interaction with the user.

Note: If the app targets API level 23 or higher, the app user must explicitly grant this permission to the app through a permission management screen. The app requests the user's approval by sending an intent with action `Settings.ACTION_MANAGE_OVERLAY_PERMISSION`. The app can check whether it has this authorization by calling `Settings.canDrawOverlays()`.

Protection level: signature|setup|appop|installer|pre23|development

Constant Value: "android.permission.SYSTEM_ALERT_WINDOW"

TRANSMIT_IR

```
public static final String TRANSMIT_IR
```

Allows using the device's IR transmitter, if available.

Protection level: normal

Constant Value: "android.permission.TRANSMIT_IR"

TURN_SCREEN_ON

```
public static final String TURN_SCREEN_ON
```

Allows an app to turn on the screen on, e.g. with `PowerManager.ACQUIRE_CAUSES_WAKEUP`.

Intended to only be used by home automation apps.

Constant Value: "android.permission.TURN_SCREEN_ON"

UNINSTALL_SHORTCUT

```
public static final String UNINSTALL_SHORTCUT
```

Don't use this permission in your app.
This permission is no longer supported.

Constant Value: "com.android.launcher.permission.UNINSTALL_SHORTCUT"

UPDATE_DEVICE_STATS

```
public static final String UPDATE_DEVICE_STATS
```

Allows an application to update device statistics.

Not for use by third-party applications.

Constant Value: "android.permission.UPDATE_DEVICE_STATS"

UPDATE_PACKAGES_WITHOUT_USER_ACTION

```
public static final String UPDATE_PACKAGES_WITHOUT_USER_ACTION
```

Allows an application to indicate via `PackageInstaller.SessionParams.setRequireUserAction(int)` that user action should not be required for an app update.

Protection level: normal

Constant Value: "android.permission.UPDATE_PACKAGES_WITHOUT_USER_ACTION"

USE_BIOMETRIC

```
public static final String USE_BIOMETRIC
```

Allows an app to use device supported biometric modalities.

Protection level: normal

Constant Value: "android.permission.USE_BIOMETRIC"

USE_EXACT_ALARM

```
public static final String USE_EXACT_ALARM
```

Allows apps to use exact alarms just like with `SCHEDULE_EXACT_ALARM` but without needing to request this permission from the user.

This is only intended for use by apps that rely on exact alarms for their core functionality. You should continue using `SCHEDULE_EXACT_ALARM` if your app needs exact alarms for a secondary feature that users may or may not use within your app.

Keep in mind that this is a powerful permission and app stores may enforce policies to audit and review the use of this permission. Such audits may involve removal from the app store if the app is found to be misusing this permission.

Apps need to target API `Build.VERSION_CODES.TIRAMISU` or above to be able to request this permission. Note that only one of `USE_EXACT_ALARM` or `SCHEDULE_EXACT_ALARM` should be requested on a device. If your app is already using `SCHEDULE_EXACT_ALARM` on older SDKs but needs `USE_EXACT_ALARM` on SDK 33 and above, then `SCHEDULE_EXACT_ALARM` should be declared with a max-sdk attribute, like:

```
<uses-permission android:name="android.permission.SCHEDULE_EXACT_ALARM"
        android:maxSdkVersion="32" />
```

Apps that hold this permission, always stay in the `WORKING_SET` or lower standby bucket.

Constant Value: "android.permission.USE_EXACT_ALARM"

USE_FINGERPRINT

```
public static final String USE_FINGERPRINT
```

This constant was deprecated in API level 28.
Applications should request `USE_BIOMETRIC` instead

Allows an app to use fingerprint hardware.

Protection level: normal

Constant Value: "android.permission.USE_FINGERPRINT"

USE_ICC_AUTH_WITH_DEVICE_IDENTIFIER

```
public static final String USE_ICC_AUTH_WITH_DEVICE_IDENTIFIER
```

Allows to read device identifiers and use ICC based authentication like EAP-AKA. Often required in authentication to access the carrier's server and manage services of the subscriber.

Protection level: signature|appop

Constant Value: "android.permission.USE_ICC_AUTH_WITH_DEVICE_IDENTIFIER"

USE_LOCATION_BUTTON

```
public static final String USE_LOCATION_BUTTON
```

Allows an app use location button, which grants temporary location permission when a user clicks the button.

Protection level: normal

Constant Value: "android.permission.USE_LOCATION_BUTTON"

USE_LOOPBACK_INTERFACE

```
public static final String USE_LOOPBACK_INTERFACE
```

Required to be able to interact with other applications via IP packets on the loopback interface.

Protection level: normal

Constant Value: "android.permission.USE_LOOPBACK_INTERFACE"

USE_PINNED_WINDOWING_LAYER

```
public static final String USE_PINNED_WINDOWING_LAYER
```

Allows an application to use `ActivityManager.AppTask.WINDOWING_LAYER_PINNED` for its Tasks, typically requested via `ActivityManager.AppTask.requestWindowingLayer(int, Executor, OutcomeReceiver)`.

Granting this permission allows an app to request its task be placed above normal application windows.

To ensure system integrity and a consistent user experience, the system imposes several restrictions on tasks using this layer. These may include, but are not limited to:

- Forcing the task to be completely opaque and display system decorations.
- Strictly limiting the number of tasks in this layer (e.g., only one at a time).
- Limiting the application's control over the task's initial size and position.
- Making the task non-movable programmatically (including restrictions on workarounds like resizing).
- Providing users with immediate settings access to disable the feature.

See the API documentation for `ActivityManager.AppTask.requestWindowingLayer(int, Executor, OutcomeReceiver)` for the full documentation.

Protection level: normal

Constant Value: "android.permission.USE_PINNED_WINDOWING_LAYER"

USE_SIP

```
public static final String USE_SIP
```

Allows an application to use SIP service.

Protection level: dangerous

Constant Value: "android.permission.USE_SIP"

UWB_RANGING

```
public static final String UWB_RANGING
```

Required to be able to range to devices using ultra-wideband.

Protection level: dangerous

Constant Value: "android.permission.UWB_RANGING"

VIBRATE

```
public static final String VIBRATE
```

Allows access to the vibrator.

Protection level: normal

Constant Value: "android.permission.VIBRATE"

WAKE_LOCK

```
public static final String WAKE_LOCK
```

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

Protection level: normal

Constant Value: "android.permission.WAKE_LOCK"

WRITE_APN_SETTINGS

```
public static final String WRITE_APN_SETTINGS
```

Allows applications to write the apn settings and read sensitive fields of an existing apn settings like user and password.

Not for use by third-party applications.

Constant Value: "android.permission.WRITE_APN_SETTINGS"

WRITE_CALENDAR

```
public static final String WRITE_CALENDAR
```

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

Protection level: dangerous

Constant Value: "android.permission.WRITE_CALENDAR"

WRITE_CALL_LOG

```
public static final String WRITE_CALL_LOG
```

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

Note: If your app uses the `WRITE_CONTACTS` permission and *both* your `minSdkVersion` and `targetSdkVersion` values are set to 15 or lower, the system implicitly grants your app this permission. If you don't need this permission, be sure your `targetSdkVersion` is 16 or higher.

Protection level: dangerous

This is a hard restricted permission which cannot be held by an app until the installer on record allowlists the permission. For more details see `PackageInstaller.SessionParams.setWhitelistedRestrictedPermissions(Set)`.

Constant Value: "android.permission.WRITE_CALL_LOG"

WRITE_CONTACTS

```
public static final String WRITE_CONTACTS
```

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

Protection level: dangerous

Constant Value: "android.permission.WRITE_CONTACTS"

WRITE_EXTERNAL_STORAGE

```
public static final String WRITE_EXTERNAL_STORAGE
```

Allows an application to write to external storage.

Note: If your app targets `Build.VERSION_CODES.R` or higher, this permission has no effect.

If your app is on a device that runs API level 19 or higher, you don't need to declare this permission to read and write files in your application-specific directories returned by `Context.getExternalFilesDir(String)` and `Context.getExternalCacheDir()`.

Learn more about how to modify media files that your app doesn't own, and how to modify non-media files that your app doesn't own.

If your app is a file manager and needs broad access to external storage files, then the system must place your app on an allowlist so that you can successfully request the MANAGE_EXTERNAL_STORAGE permission. Learn more about the appropriate use cases for `minSdkVersion` and `targetSdkVersion` values are set to 3 or lower, the system implicitly grants your app this permission. If you don't need this permission, be sure your `targetSdkVersion` is 4 or higher.

Protection level: dangerous

Constant Value: "android.permission.WRITE_EXTERNAL_STORAGE"

WRITE_GSERVICES

```
public static final String WRITE_GSERVICES
```

Allows an application to modify the Google service map.

Not for use by third-party applications.

Constant Value: "android.permission.WRITE_GSERVICES"

WRITE_SECURE_SETTINGS

```
public static final String WRITE_SECURE_SETTINGS
```

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

Not for use by third-party applications.

Constant Value: "android.permission.WRITE_SECURE_SETTINGS"

WRITE_SETTINGS

```
public static final String WRITE_SETTINGS
```

Allows an application to read or write the system settings.

Note: If the app targets API level 23 or higher, the app user must explicitly grant this permission to the app through a permission management screen. The app requests the user's approval by sending an intent with action `Settings.ACTION_MANAGE_WRITE_SETTINGS`. The app can check whether it has this authorization by calling `Settings.System.canWrite()`.

Protection level: signature|preinstalled|appop|pre23

Constant Value: "android.permission.WRITE_SETTINGS"

WRITE_SYNC_SETTINGS

```
public static final String WRITE_SYNC_SETTINGS
```

Allows applications to write the sync settings.

Protection level: normal

Constant Value: "android.permission.WRITE_SYNC_SETTINGS"

WRITE_SYSTEM_PREFERENCES

```
public static final String WRITE_SYSTEM_PREFERENCES
```

Allows an application to access the Settings Preference services to write settings values exposed by the system Settings app and system apps that contribute settings surfaced in the Settings app.

This allows the calling application to write settings values through the host application, agnostic of underlying storage.

Protection Level: signature|privileged|appop

Constant Value: "android.permission.WRITE_SYSTEM_PREFERENCES"

WRITE_VOICEMAIL

```
public static final String WRITE_VOICEMAIL
```

Allows an application to modify and remove existing voicemails in the system.

Protection level: signature|privileged|role

Constant Value: "com.android.voicemail.permission.WRITE_VOICEMAIL"

Public constructors

permission

```
public permission ()
```
