Gestión de aplicaciones

En esta sección, puedes configurar políticas relacionadas con la disponibilidad de aplicaciones, la instalación, las actualizaciones y la gestión de permisos.

> Las cuentas de Google Play gestionadas se crean automáticamente al aprovisionar los dispositivos.

1. Modo de la tienda de aplicaciones

Este modo controla qué aplicaciones están disponibles para el usuario en la tienda de aplicaciones y cómo se comporta el dispositivo cuando las aplicaciones se eliminan de la configuración.

Lista blanca (predeterminado): Solo las aplicaciones incluidas en la configuración estarán disponibles, y cualquier aplicación que no esté en la configuración se desinstalará automáticamente del dispositivo. La tienda de aplicaciones solo mostrará las aplicaciones disponibles.

Lista negra: Todas las aplicaciones están disponibles, y cualquier aplicación que no deba estar en el dispositivo debe marcarse explícitamente como **bloqueada** en la configuración de las aplicaciones. La tienda de aplicaciones mostrará todas las aplicaciones, excepto las bloqueadas.

2. Política de aplicaciones no confiables

Política para aplicaciones no confiables (aplicaciones de fuentes desconocidas) aplicada al dispositivo. Esta opción controla la configuración del sistema Android que determina si un usuario puede instalar aplicaciones desde fuera de la Tienda Google Play (instalación manual).

No permitir (predeterminado): Deshabilitar la instalación de aplicaciones no confiables en todo el dispositivo.

Solo perfil personal: Para dispositivos con perfiles de trabajo, permitir la instalación de aplicaciones no confiables solo en el perfil personal del dispositivo.

Permitir: Permitir la instalación de aplicaciones no confiables en todo el dispositivo.

3. Google Play Protect

¿Se aplica la verificación de aplicaciones de Google Play Protect?

Obligatorio (predeterminado): Activa forzadamente la verificación de aplicaciones.

Elección del usuario: Permite al usuario elegir si habilitar o no la verificación de aplicaciones.

4. Política de permisos predeterminada

La política para conceder solicitudes de permisos en tiempo de ejecución a las aplicaciones.

Solicitar (predeterminado): Solicitar al usuario que conceda un permiso.

Otorgar: Otorgar automáticamente un permiso.

Denegar: Denegar automáticamente un permiso.

5. Funciones de la aplicación

Controla si las aplicaciones en dispositivos administrados o en perfiles de trabajo pueden mostrar sus funciones. Requiere Android 16 o superior.

Permitido (por defecto): Las aplicaciones en dispositivos totalmente administrados o en perfiles de trabajo pueden mostrar sus funciones.

No permitido: Las aplicaciones en dispositivos totalmente administrados o en perfiles de trabajo no pueden mostrar sus funciones.

6. Instalar aplicaciones desactivadas

¿Está desactivada la instalación de aplicaciones por parte del usuario?

7. Desinstalar aplicaciones: desactivado

¿Está desactivada la desinstalación de aplicaciones por parte del usuario?

8. Políticas de permisos

Permisos explícitos o concesiones/denegaciones de grupos para todas las aplicaciones. Estos valores anulan la configuración de la **política de permisos predeterminada**.

Utilice **"Agregar política de permisos"** para crear entradas y eliminarlas con la acción de eliminar.

Cada entrada incluye:

> **Permiso/grupo de Android**: El permiso o grupo de Android (obligatorio), por ejemplo **android.permission.READ_CALENDAR** o **android.permission_group.CALENDAR**.
>
> **Política**: Permitir / Denegar / Preguntar (utiliza las mismas opciones de política que la **política de permisos predeterminada**).

9. Aplicaciones

Lista de aplicaciones que deben incluirse en la política. El comportamiento del contenido de la lista depende del valor configurado en **el modo de Google Play**.

Si el **modo de Google Play** está configurado en **lista blanca**, solo estarán disponibles las aplicaciones que estén incluidas en la política, y cualquier aplicación que no esté en la política se desinstalará automáticamente del dispositivo.

Si el **modo Play Store** está configurado como **lista negra**, todas las aplicaciones están disponibles y cualquier aplicación que no deba estar en el dispositivo debe marcarse explícitamente como **bloqueada** en la política de aplicaciones.

Para agregar una nueva aplicación, haga clic en el botón **Añadir aplicaciones** (o en el icono **Añadir aplicaciones**), y luego seleccione la aplicación desde Play Store y haga clic en el botón **Seleccionar** en la tarjeta de la aplicación.

> Todas las aplicaciones disponibles en la Play Store de su país están seleccionables de forma predeterminada. Para seleccionar sus propias aplicaciones privadas o web, debe subirlas al sistema primero. Para obtener más información, consulte la página **Aplicaciones privadas**.

Cada aplicación se puede configurar con sus propios ajustes, que se muestran visualmente en una tarjeta:

9.1. Tipo de instalación

El tipo de instalación a realizar para una aplicación.

> **Disponible**: La aplicación está disponible para su instalación.

Preinstalada: La aplicación se instala automáticamente y puede ser desinstalada por el usuario.

Instalación forzada: La aplicación se instala automáticamente y no puede ser desinstalada por el usuario.

Bloqueada: La aplicación está bloqueada y no se puede instalar. Si la aplicación se había instalado bajo una política anterior, se desinstalará.

Requerido para la configuración: La aplicación se instala automáticamente y el usuario no puede eliminarla; además, impedirá que la configuración se complete hasta que la instalación finalice.

Modo Quiosco: La aplicación se instala automáticamente en modo quiosco: se establece como la intención de inicio preferida y se incluye en la lista de aplicaciones permitidas para el modo de tarea bloqueada. La configuración del dispositivo no se completará hasta que se instale la aplicación. Después de la instalación, los usuarios no podrán eliminar la aplicación. Solo puede configurar este **tipo de instalación** para una sola aplicación por política. Cuando esta opción está presente en la política, la barra de estado se desactiva automáticamente.

Para obtener más información, consulte la página dedicada de **Modo Quiosco**.

9.2. Instalar restricciones

Define un conjunto de restricciones para la instalación de la aplicación. Cuando se seleccionan varias restricciones, todas deben cumplirse para que la aplicación se instale.

> Esta opción se muestra solo cuando el **tipo de instalación** es **preinstalada** o **instalada forzosamente**.

Red sin límite de datos: Instala la aplicación solo cuando el dispositivo esté conectado a una red sin límite de datos (por ejemplo, Wi-Fi).

Cargando: Instala la aplicación solo cuando el dispositivo se esté cargando.

En espera: Instala la aplicación solo cuando el dispositivo esté inactivo.

9.3. Modo de actualización automática

Controla el modo de actualización automática de la aplicación.

Predeterminado: La aplicación se actualiza automáticamente con baja prioridad para minimizar el impacto en el usuario. La aplicación se actualiza cuando se cumplen todas las siguientes condiciones: (1) el dispositivo no se está utilizando activamente, (2) el dispositivo está conectado a una red no limitada, (3) el dispositivo se está cargando. El dispositivo recibe una notificación sobre una nueva actualización dentro de las 24 horas posteriores a su publicación por el desarrollador, momento en el cual la aplicación se actualiza la próxima vez

que se cumplen las condiciones anteriores.

Aplazado: La aplicación no se actualiza automáticamente durante un máximo de 90 días después de que la aplicación quede obsoleta. 90 días después de que la aplicación quede obsoleta, la última versión disponible se instala automáticamente con baja prioridad (consulte el modo de actualización automática **predeterminado**). Después de que la aplicación se actualiza, no se actualiza automáticamente nuevamente hasta 90 días después de que vuelva a quedar obsoleta. El usuario aún puede actualizar manualmente la aplicación desde la Play Store en cualquier momento.

Prioridad alta: La aplicación se actualiza lo antes posible. No se aplican restricciones. El dispositivo se notifica inmediatamente sobre una nueva actualización una vez que está disponible.

9.4. Versión mínima requerida

La versión mínima de la aplicación que se ejecuta en el dispositivo. Si se establece, el dispositivo intenta actualizar la aplicación a al menos esta versión. Si la aplicación no está actualizada, el dispositivo mostrará un **detalle de incumplimiento** con la **razón de incumplimiento** establecida en **APP_NOT_UPDATED**. La aplicación debe estar publicada en Google Play con un código de versión mayor o igual a este valor. Un máximo de 20 aplicaciones pueden especificar un código de versión mínima por política.

9.5. Ámbitos delegados

Los ámbitos delegados a la aplicación desde la política del dispositivo Android. Puede otorgar a otras aplicaciones una selección de permisos especiales de Android:

Instalación de certificados: Otorga acceso a la instalación y administración de certificados.

Configuraciones gestionadas: Otorga acceso a la administración de configuraciones gestionadas.

Bloquear desinstalación: Permite acceder a la función de bloqueo de desinstalación.

Permisos: Permite acceder a la configuración de las políticas de permisos y al estado de la concesión de permisos.

Acceso a paquetes: Permite acceder al estado de acceso a paquetes.

Aplicación del sistema: Permite el acceso para habilitar aplicaciones del sistema.

9.6. Red preferencial

El servicio de red preferencial a utilizar para esta aplicación. Si se especifica, la aplicación utilizará la segmentación de red empresarial definida para sus conexiones, cuando esté disponible. Debe coincidir con una segmentación de red configurada en la sección **Configuración de segmentación de red 5G** del panel **Celular**.

9.7. Política de permisos predeterminada

La política predeterminada para todos los permisos solicitados por la aplicación. Si se especifica, esto anula la política de **permisos predeterminada** que se aplica a todas las aplicaciones. No anula las **políticas de permisos** que se aplican a todas las aplicaciones.

Solicitar (predeterminado): Solicitar al usuario que conceda un permiso.

Otorgar: Otorgar automáticamente un permiso.

Denegar: Denegar automáticamente un permiso.

9.8. Trabajo conectado y aplicaciones personales

Controla si la aplicación puede comunicarse consigo misma entre los perfiles de trabajo y personales del dispositivo, sujeto al consentimiento del usuario (Android 11+).

No permitido (por defecto): Impide que la aplicación se comunique entre perfiles.

Permitido: Permite que la aplicación se comunique entre perfiles después de recibir el consentimiento del usuario.

9.9. Exención del bloqueo VPN Always On

Especifica si la aplicación puede acceder a la red cuando la VPN no está conectada y el **modo de bloqueo** está habilitado. Solo es compatible con dispositivos que ejecutan Android 10 o superior.

Obligatorio (por defecto): La aplicación respeta la configuración de bloqueo VPN permanente.

Exento: La aplicación está exenta de la configuración de bloqueo VPN permanente.

9.10. Widgets del perfil de trabajo

Especifica si la aplicación instalada en el perfil de trabajo puede agregar widgets a la pantalla de inicio.

Permitido: La aplicación puede agregar widgets a la pantalla de inicio.

No permitido: La aplicación no puede agregar widgets a la pantalla de inicio.

9.11. Configuración de controles para el usuario

Especifica si se permite el control del usuario para una aplicación determinada. El control del usuario incluye acciones como forzar la detención y borrar los datos de la aplicación (Android 11+). Si **extensionConfig** está habilitado para una aplicación, el control del usuario está deshabilitado independientemente de esta configuración. Para aplicaciones de quiosco, puedes usar **Permitido** para permitir el control del usuario.

No especificado: Utiliza el comportamiento predeterminado de la aplicación para determinar si el control del usuario está permitido o denegado.

Permitido: El control del usuario está permitido para la aplicación.

No permitido: El control del usuario no está permitido para la aplicación.

9.12. Desactivado

¿Está la aplicación desactivada? Cuando está desactivada, los datos de la aplicación se conservan.

9.13. Permitir proveedor de credenciales

Si la aplicación puede actuar como proveedor de credenciales en Android 14 y versiones posteriores.

9.14. Configuración gestionada

Para configurar la configuración gestionada de la aplicación, haga clic en el botón **Activar configuración gestionada**. Si ya existe una configuración gestionada para la aplicación, puede modificar la configuración con el botón **Configuración gestionada** o eliminarla con el botón **Eliminar configuración**.

> **La opción de configuración gestionada** solo está disponible para aplicaciones que admiten esta funcionalidad.

9.15. Políticas de permisos

Concesiones o denegaciones de permisos explícitas para la aplicación. Estos valores anulan la **política de permisos predeterminada** y las **políticas de permisos** que se aplican a todas las aplicaciones.

Utilice **Añadir política de permisos** para agregar una o más reglas de permisos a la tarjeta de la aplicación y elimínelas con la acción de eliminar.

9.16. Realice un seguimiento de los ID

Lista de los ID de la rama de pruebas cerradas de la aplicación a la que un dispositivo puede acceder. Si se seleccionan varios ID de rama, los dispositivos reciben la última versión disponible entre todas las ramas accesibles. Si no se selecciona ningún ID de rama, los dispositivos solo tienen acceso a la rama de producción de la aplicación.

> **La opción de ID de rama** está disponible solo para aplicaciones que tengan al menos un ID de rama disponible para su organización. Para obtener más detalles sobre cómo agregar su organización a una rama de pruebas cerradas para una aplicación específica, consulte aquí.

10. Configuración predeterminada de la aplicación

Establecer las aplicaciones predeterminadas para los tipos admitidos. Cuando se establece una aplicación predeterminada para al menos un tipo, se impide que los usuarios cambien las aplicaciones predeterminadas en ese perfil.

> Solo se permite una configuración de aplicación predeterminada por cada **tipo de aplicación predeterminada**]. La lista de aplicaciones predeterminadas no debe contener duplicados.

10.1. Tipo de aplicación predeterminado

Seleccione la categoría de la aplicación que desea configurar (por ejemplo, Navegador, Marcador, SMS, Billetera o Asistente). La disponibilidad depende de la versión de Android y del modo de gestión.

10.2. Ámbitos de aplicación predeterminados

Seleccione dónde se aplicará la aplicación predeterminada (administración completa, perfil de trabajo o perfil personal). Solo se pueden seleccionar los ámbitos compatibles con el tipo seleccionado.

> Si ninguno de los ámbitos seleccionados es aplicable al modo de administración del dispositivo, el dispositivo informará de un detalle de incumplimiento.

10.3. Aplicaciones predeterminadas

Lista de aplicaciones que se pueden establecer como predeterminadas para el tipo seleccionado. La primera aplicación instalada y que cumpla los requisitos se establece como la predeterminada.

> Si los permisos incluyen **administración completa** o **perfil de trabajo**, cada aplicación también debe existir en la lista de **aplicaciones** con el **tipo de instalación** no establecido en **bloqueado**.

11. Selección de la clave privada

Permite mostrar una interfaz en un dispositivo para que el usuario seleccione un alias de clave privada si no existen reglas coincidentes en **Reglas de selección de clave privada**.

>

> Para dispositivos con versiones de Android anteriores a la P, establecer esto podría dejar las claves empresariales vulnerables.

12. Seleccione las reglas de la clave privada

Controla el acceso de las aplicaciones a las claves privadas. La regla determina qué clave privada, si existe, otorga la política de dispositivo Android a la aplicación especificada. El acceso se concede cuando la aplicación llama a KeyChain.choosePrivateKeyAlias (o cualquier función equivalente) para solicitar un alias de clave privada para una URL determinada, o para reglas que no son específicas de una URL (es decir, si urlPattern no está definido o está vacío o es igual a ".*") en Android 11 y versiones posteriores, directamente, para que la aplicación pueda llamar a KeyChain.getPrivateKey sin tener que llamar primero a KeyChain.choosePrivateKeyAlias. Cuando una aplicación llama a KeyChain.choosePrivateKeyAlias y más de una regla choosePrivateKeyRules coincide, la última regla que coincide define qué alias de clave se debe devolver.

Utilice **Agregar regla de clave privada** para crear entradas y eliminarlas con la acción de eliminar.

12.1. Alias de clave privada

El alias de la clave privada que se utilizará.

12.2. Patrón de URL

El patrón de URL que se utilizará para comparar con la URL de la solicitud. Si no se establece o está vacío, se aplicará a todas las URLs. Utiliza la sintaxis de expresiones regulares de java.util.regex.Pattern.

12.3. Nombres de paquetes

Los nombres de los paquetes a los que se aplica esta regla. El hash del certificado de firma de cada aplicación se verifica contra el hash proporcionado por Play. Si no se especifican nombres de paquetes, el alias se proporciona a todas las aplicaciones que llamen a KeyChain.choosePrivateKeyAlias o a cualquiera de sus métodos sobrecargados (pero no sin llamar a KeyChain.choosePrivateKeyAlias, incluso en Android 11 y versiones posteriores). Cualquier aplicación con el mismo UID de Android que un paquete especificado aquí tendrá acceso al llamar a KeyChain.choosePrivateKeyAlias.

Utilice **Añadir nombre del paquete** para agregar entradas y eliminarlas con la acción de eliminar.

> Para eliminar una aplicación, haga clic en el icono de **la papelera**, que se encuentra en la parte inferior de la tarjeta de la aplicación.

Revision #37
Created 2025-12-17 09:33:23 UTC by Admin
Updated 2026-04-22 15:49:42 UTC by Admin