Gestión de apps

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

> Las cuentas de Managed Google Play se crean automáticamente cuando se aprovisionan los dispositivos.

1. Modo de Play Store

Este modo controla qué apps están disponibles para el usuario en Play Store y el comportamiento del dispositivo cuando se eliminan apps de la política.

Lista blanca (predeterminado): solo están disponibles las apps que figuran en la política, y cualquier app que no esté en la política se desinstalará automáticamente del dispositivo. Play Store solo mostrará las apps disponibles.

Lista negra: todas las apps están disponibles y cualquier app que no deba estar en el dispositivo debe marcarse explícitamente como **bloqueada** en la política de aplicaciones. Play Store mostrará todas las apps, excepto las bloqueadas.

2. Política de apps no confiables

La política para apps no confiables (apps de orígenes desconocidos) aplicada en el dispositivo. Esta opción controla el ajuste del sistema Android que determina si un usuario puede instalar apps desde fuera de Play Store (instalación de apps de fuentes externas).

No permitir (predeterminado): no permite instalar apps no confiables en todo el dispositivo.

Solo perfil personal: en dispositivos con perfiles de trabajo, permite instalar apps no confiables solo en el perfil personal del dispositivo.

Permitir: permite instalar apps no confiables en todo el dispositivo.

3. Google Play Protect

Indica si se aplica la verificación de apps de Google Play Protect.

Aplicada (predeterminado): activa obligatoriamente la verificación de apps.

Elección del usuario: permite al usuario elegir si activa la verificación de apps.

4. Política de permisos predeterminada

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

Preguntar (predeterminado): pide al usuario que conceda un permiso.

Conceder: concede un permiso automáticamente.

Denegar: deniega un permiso automáticamente.

5. Funciones de las apps

Controla si las apps en dispositivos totalmente gestionados o en perfiles de trabajo pueden exponer funciones de apps. Requiere Android 16 o posterior.

Permitido (predeterminado): las apps en dispositivos totalmente gestionados o en perfiles de trabajo pueden exponer funciones de apps.

No permitido: las apps en dispositivos totalmente gestionados o en perfiles de trabajo no pueden exponer funciones de apps.

6. Instalación de apps desactivada

Indica si está desactivada la instalación de apps por parte del usuario.

7. Desinstalación de apps desactivada

Indica si está desactivada la desinstalación de apps por parte del usuario.

8. Políticas de permisos

Concesiones o denegaciones explícitas de permisos o grupos para todas las apps. Estos valores anulan el ajuste **Política de permisos predeterminada**.

Usa **Añadir política de permisos** para crear entradas y elimínalas 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**: Conceder / Denegar / Preguntar (usa las mismas opciones de política que **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 establecido en **Modo de Play Store**.

Si **Modo de Play Store** se establece en **lista blanca**, solo están disponibles las apps que figuran en la política y cualquier app que no esté en la política se desinstalará automáticamente del dispositivo.

Si **Modo de Play Store** se establece en **lista negra**, todas las apps están disponibles y cualquier app que no deba estar en el dispositivo debe marcarse explícitamente como **bloqueada** en la política de aplicaciones.

Para añadir una nueva app, haz clic en el botón **Añadir aplicaciones** (o en el icono **Añadir aplicaciones**), selecciona **Desde Managed Google Play** y, después, elige la app en Play Store y haz clic en el botón **Seleccionar** de la tarjeta de la app.

Para añadir una app que no está publicada en Google Play pero ya está presente en el dispositivo (por ejemplo, una app del sistema o del fabricante), haz clic en **Añadir aplicaciones**, selecciona **Por nombre de paquete (apps preinstaladas)**, escribe el nombre de paquete de la app (por ejemplo, **com.example.app**) y haz clic en **Añadir**.La app se añade con el tipo de instalación **Forzar instalación**. Para mostrar la app en el lanzador personalizado del modo quiosco, su **Tipo de instalación** debe ser **Preinstalada** o **Forzar instalación**: con **Disponible**, la app no se muestra.

> Las apps que no están disponibles en Managed Google Play se marcan con un icono de Android en la lista de aplicaciones. No se pueden instalar desde Google Play, así que ya deben estar presentes en el dispositivo: los dispositivos que no tienen la app no pueden instalarla.

>

> Todas las apps publicadas en Play Store en tu país están disponibles para seleccionarlas de forma predeterminada. Para seleccionar tus propias apps privadas o web, primero debes subirlas al sistema. Para obtener más información, lee la página **Apps privadas**.

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

9.1. Tipo de instalación

El tipo de instalación que se va a realizar para una app.

Disponible: la app está disponible para instalarla.

Preinstalada: la app se instala automáticamente y el usuario puede eliminarla.

Forzar instalación: la app se instala automáticamente y el usuario no puede eliminarla.

Bloqueada: la app está bloqueada y no se puede instalar. Si la app se instaló con una política anterior, se desinstalará.

Obligatoria para la configuración: la app se instala automáticamente, el usuario no puede eliminarla y evitará que finalice la configuración hasta que se complete la instalación.

Quiosco: la app se instala automáticamente en modo quiosco: se establece como intent de inicio preferido y se añade a la lista blanca para el modo de bloqueo de tareas. La configuración del dispositivo no finalizará hasta que se instale la app. Tras la instalación, los usuarios no podrán eliminar la app. Solo puedes establecer este **tipo de instalación** para una app por política. Cuando está presente en la política, la barra de estado se desactivará automáticamente. Para obtener más información, lee la página dedicada al **Modo quiosco**.

9.2. Restricciones de instalación

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

> Esta opción solo se muestra cuando el **Tipo de instalación** es **Preinstalada** o **Forzar instalación**.

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

Cargando: instala la app solo cuando el dispositivo se esté cargando.

Inactivo: instala la app solo cuando el dispositivo esté inactivo.

9.3. Modo de actualización automática

Controla el modo de actualización automática de la app.

Predeterminado: la app se actualiza automáticamente con baja prioridad para minimizar el impacto en el usuario. La app se actualiza cuando se cumplen todas estas condiciones: (1) el dispositivo no se está usando activamente, (2) el dispositivo está conectado a una red sin límite de datos y (3) el dispositivo se está cargando. El dispositivo recibe una notificación sobre una nueva actualización en las 24 horas siguientes a su publicación por el desarrollador, y la app se actualiza la próxima vez que se cumplan las condiciones anteriores.

Aplazado: la app no se actualiza automáticamente durante un máximo de 90 días desde que queda desactualizada. 90 días después de que la app quede desactualizada, se instala automáticamente la última versión disponible con baja prioridad (consulta el modo de actualización automática **Predeterminado**). Una vez actualizada, la app no vuelve a actualizarse automáticamente hasta 90 días después de quedar desactualizada de nuevo. El usuario siempre puede actualizar la app manualmente desde Play Store.

Alta prioridad: la app se actualiza lo antes posible. No se aplica ninguna restricción. El dispositivo recibe una notificación inmediata sobre una nueva actualización en cuanto está disponible.

9.4. Código de versión mínimo

La versión mínima de la app que se ejecuta en el dispositivo. Si se establece, el dispositivo intenta actualizar la app al menos a este código de versión. Si la app no está actualizada, el dispositivo contendrá un **detalle de incumplimiento** con el **motivo de incumplimiento** establecido en **APP_NOT_UPDATED**. La app ya debe estar publicada en Google Play con un código de versión mayor o igual que este valor. Como máximo, 20 apps pueden especificar un código de versión mínimo por política.

9.5. Ámbitos delegados

Los ámbitos delegados a la app desde Android Device Policy. Puedes conceder a otras apps una selección de permisos especiales de Android:

Instalación de certificados: concede acceso a la instalación y gestión de certificados.

Configuraciones gestionadas: concede acceso a la gestión de configuraciones gestionadas.

Bloquear desinstalación: concede acceso a bloquear la desinstalación.

Permisos: concede acceso a la política de permisos y al estado de concesión de permisos.

Acceso a paquetes: concede acceso al estado de acceso a paquetes.

App del sistema: concede acceso para activar apps del sistema.

9.6. Red preferente

El servicio de red preferente que se usará para esta app. Si se establece, la app usará el segmento de red empresarial especificado para sus conexiones cuando esté disponible. Debe coincidir con un segmento de red configurado en la sección **Configuración de segmentación de red 5G** del panel **Red móvil**.

9.7. Política de permisos predeterminada

La política predeterminada para todos los permisos solicitados por la app. Si se especifica, anula la **Política de permisos predeterminada** de la política, que se aplica a todas las apps. No anula las **Políticas de permisos**, que se aplican a todas las apps.

Preguntar (predeterminado): pide al usuario que conceda un permiso.

Conceder: concede un permiso automáticamente.

Denegar: deniega un permiso automáticamente.

9.8. App conectada de trabajo y personal

Controla si la app puede comunicarse consigo misma entre los perfiles de trabajo y personal de un dispositivo, con el consentimiento del usuario (Android 11 o posterior).

No permitido (predeterminado): impide que la app se comunique entre perfiles.

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

9.9. Excepción al bloqueo de VPN Always On

Especifica si se permite que la app use la red cuando la VPN no está conectada y el **bloqueo habilitado** está activo. Solo es compatible con dispositivos que ejecutan Android 10 o posterior.

Aplicado (predeterminado): la app respeta el ajuste de bloqueo de VPN Always On.

Exenta: la app está exenta del ajuste de bloqueo de VPN Always On.

9.10. Widgets del perfil de trabajo

Especifica si la app instalada en el perfil de trabajo puede añadir widgets a la pantalla de inicio.

Permitido: la aplicación puede añadir widgets a la pantalla de inicio.

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

9.11. Ajustes de control del usuario

Especifica si se permite el control del usuario para una app determinada. El control del usuario incluye acciones como forzar la detención y borrar los datos de la app (Android 11 o posterior). Si **extensionConfig** está habilitado para una app, el control del usuario no se permite independientemente de este ajuste. Para las apps de quiosco, puedes usar **Permitido** para permitir el control del usuario.

> **Sin especificar**: usa el comportamiento predeterminado de la app para determinar si se permite o no el control del usuario.
>
> **Permitido**: se permite el control del usuario para la app.
>
> **No permitido**: no se permite el control del usuario para la app.

9.12. Desactivada

Indica si la app está desactivada. Cuando está desactivada, los datos de la app se conservan.

9.13. Permitir proveedor de credenciales

Indica si se permite que la app actúe como proveedor de credenciales en Android 14 o posterior.

9.14. Configuración gestionada

Para configurar los ajustes gestionados de la app, haz clic en el botón **Habilitar configuración gestionada**. Si ya se ha establecido una configuración gestionada para la app, puedes modificarla con el botón **Configuración gestionada** o eliminarla con el botón **Eliminar configuración**.

> La opción **Configuración gestionada** solo está disponible para las apps que admiten esta funcionalidad.

9.15. Políticas de permisos

Concesiones o denegaciones explícitas de permisos para la app. Estos valores anulan la **Política de permisos predeterminada** y las **Políticas de permisos** que se aplican a todas las apps.

Usa **Añadir política de permisos** para añadir una o varias reglas de permisos a la tarjeta de la app y eliminarlas con la acción de eliminar.

9.16. IDs de pista

Lista de los ID de pista de prueba cerrada de la app a los que puede acceder un dispositivo. Si se seleccionan varios ID de pista, los dispositivos reciben la versión más reciente de todas las pistas accesibles. Si no se selecciona ningún ID de pista, los dispositivos solo tienen acceso a la pista de producción de la app.

>

> La opción**IDs de pista** solo está disponible para las apps que tienen al menos un ID de pista disponible para tu organización. Para obtener más detalles sobre cómo añadir tu organización a una pista de prueba cerrada para una app específica, lee aquí.

10. Ajustes de aplicaciones predeterminadas

Establece apps predeterminadas para los tipos compatibles. Cuando se establece una app predeterminada para al menos un tipo, los usuarios no pueden cambiar las apps predeterminadas en ese perfil.

> Solo se permite un ajuste de aplicación predeterminada por **Tipo de aplicación predeterminada**. La lista de aplicaciones predeterminadas no debe contener duplicados.

10.1. Tipo de aplicación predeterminada

Selecciona la categoría de app que quieres configurar (por ejemplo, Navegador, Teléfono, SMS, Cartera o Asistente). La disponibilidad depende de la versión de Android y del modo de gestión.

10.2. Ámbitos de aplicación predeterminada

Selecciona dónde debe aplicarse la app predeterminada (Totalmente gestionado, Perfil de trabajo o Perfil personal). Solo se pueden elegir los ámbitos compatibles con el tipo seleccionado.

> Si ninguno de los ámbitos seleccionados se aplica al modo de gestión del dispositivo, el dispositivo informa de un detalle de incumplimiento.

10.3. Aplicaciones predeterminadas

Lista de apps que se pueden establecer como predeterminadas para el tipo seleccionado. La primera app instalada y apta se establece como predeterminada.

> Si los ámbitos incluyen **Totalmente gestionado** o **Perfil de trabajo**, cada app también debe existir en la lista **Aplicaciones** con el **Tipo de instalación** distinto de **Bloqueada**.

11. Selección de clave privada

Permite mostrar en un dispositivo una interfaz para que el usuario elija un alias de clave privada si no hay reglas coincidentes en **Elegir reglas de clave privada**.

En dispositivos anteriores a Android P, esta opción puede dejar las claves empresariales vulnerables.

12. Elegir reglas de clave privada

Controla el acceso de las apps a las claves privadas. La regla determina qué clave privada, si alguna, concede Android Device Policy a la app especificada. El acceso se concede cuando la app llama a KeyChain.choosePrivateKeyAlias (o a cualquiera de sus sobrecargas) para solicitar un alias de clave privada para una URL determinada, o bien, para las reglas que no son específicas de una URL (es decir, si urlPattern no está establecido o se establece en la cadena vacía o .*) en Android 11 y versiones posteriores, directamente para que la app pueda llamar a KeyChain.getPrivateKey sin tener que llamar antes a KeyChain.choosePrivateKeyAlias. Cuando una app llama a KeyChain.choosePrivateKeyAlias y coincide más de una choosePrivateKeyRules, la última regla coincidente define qué alias de clave se devuelve.

Usa **Añadir regla de clave privada** para crear entradas y elimínalas con la acción de eliminar.

12.1. Alias de clave privada

El alias de la clave privada que se va a usar.

12.2. Patrón de URL

El patrón de URL que se compara con la URL de la solicitud. Si no se establece o está vacío, coincide con todas las URL. Usa la sintaxis de expresiones regulares de java.util.regex.Pattern.

12.3. Nombres de paquete

Los nombres de paquete a los que se aplica esta regla. El hash del certificado de firma de cada app se verifica con el hash proporcionado por Play. Si no se especifica ningún nombre de paquete, el alias se proporciona a todas las apps que llamen a KeyChain.choosePrivateKeyAlias o a cualquiera de sus sobrecargas (pero no sin llamar a KeyChain.choosePrivateKeyAlias, incluso en Android 11 y versiones posteriores). Cualquier app con el mismo UID de Android que un paquete especificado aquí tendrá acceso cuando llame a KeyChain.choosePrivateKeyAlias.

Usa **Añadir nombre de paquete** para añadir entradas y elimínalas con la acción de eliminar.

Para eliminar una app, haz clic en el icono **papelera**, en la parte inferior de la tarjeta de la app.

Revision #7
Created 2026-11-10 15:14:58 UTC by Admin
Updated 2026-11-12 09:54:36 UTC by Admin