App 管理
在本部分中，您可以设置与 App 可用性、安装、更新和权限管理相关的政策。

配置设备时，系统会自动创建 Managed Google Play 账户。

1. Play Store 模式

此模式控制用户在 Play Store 中可以使用哪些 App，以及从政策中移除 App 时设备上的行为。

白名单（默认） ：只有政策中的 App 可用，任何不在政策中的 App 都将自动从设备中卸载。 Play
Store 只会显示可用的 App。

黑名单 ：所有 App 都可用，任何不应出现在设备上的 App 都应在应用程序政策中明确标记为 已阻止 。 Play Store 将显示除已阻止的 App 之外的所有 App。

2. 不受信任的 App 政策

在设备上强制执行的针对不受信任的 App（来自未知来源的 App）的政策。此选项控制 Android
系统设置，决定用户是否可以从 Play Store 之外安装 App（侧载）。

禁止（默认） ：禁止在整个设备上安装不受信任的 App。

仅个人资料 ：对于具有工作资料的设备，仅允许在该设备的个人资料中安装不受信任的 App。
允许 ：允许在整个设备上安装不受信任的 App。

3. Google Play Protect

是否强制执行 Google Play Protect App 验证。

强制执行（默认） ：强制启用 App 验证。
用户选择 ：允许用户选择是否启用 App 验证。

4. 默认权限政策

用于向 App 授予运行时权限请求的政策。
提示（默认） ：提示用户授予权限。
授予 ：自动授予权限。

拒绝 ：自动拒绝权限。

5. App 功能

控制完全受管理的设备上或工作资料中的 App 是否允许公开 App 功能。需要 Android 16 或更高版本。

允许（默认） ：完全受管理的设备上或工作资料中的 App 可以公开 App 功能。
不允许 ：完全受管理的设备上或工作资料中的 App 无法公开 App 功能。

6. 禁用 App 安装

是否禁用用户安装 App。

7. 禁用 App 卸载

是否禁用用户卸载应用程序。

8. 权限政策

为所有 App 明确授予或拒绝权限或权限组。这些值会覆盖 默认权限政策 设置。
使用 添加权限政策 创建条目，并使用删除操作将其移除。

每个条目包括：

Android 权限 /组 ：Android 权限或组（必填），例如 android.permission.READ_CALENDAR或 android.permission_group.CALENDAR。
政策 ：授予 /拒绝 /提示（使用与 默认权限政策 相同的政策选项）。

9. 应用程序

必须包含在政策中的应用程序列表。列表内容的行为取决于 Play Store 模式 设置的值。

如果 Play Store 模式 设为 白名单 ，则只有政策中的 App 可用，任何不在政策中的 App
都将自动从设备中卸载。

如果 Play Store 模式 设为 黑名单 ，则所有 App 都可用，任何不应出现在设备上的 App
都应在应用程序政策中明确标记为 已阻止 。

要添加新 App，请点击 添加应用程序 按钮（或 添加应用程序 图标），选择 从受管理的 Google Play 添加
，然后从 Play Store 中选择该 App，并点击 App 卡片中的 选择 按钮。

要添加未在 Google Play 上发布但已存在于设备上的 App（例如系统或制造商 App），请点击 添加应用程序
，选择 按包名（预装 App） ，输入 App 的包名（例如 com.example.app），然后点击 添加 。该 App
会以 强制安装 安装类型添加。要在 Kiosk 自定义启动器中显示该 App，其 安装类型 必须为 预安装 或强制安装
：如果为 可用 ，则不会显示该 App。

在受管理的 Google Play 上不可用的 App 会在应用程序列表中标记为 Android 图标。它们无法从
Google Play 安装，因此必须已存在于设备上：没有该 App 的设备无法安装它。

默认情况下，在您所在国家 /地区的 Play Store 上发布的所有 App 均可供选择。要选择您自己的私有

App 或 Web App，您必须先将其上传到系统。有关详细信息，请阅读 私有 App页面。

每个 App 都可以配置自己的设置，这些设置以卡片形式显示：

9.1. 安装类型

要为 App 执行的安装类型。

可用 ：该 App 可供安装。

预安装 ：该 App 会自动安装，用户可将其移除。

强制安装 ：该 App 会自动安装，用户无法将其移除。

已阻止 ：该 App 已被阻止，无法安装。如果该 App 是在之前的政策下安装的，它将被卸载。

安装所必需 ：该 App 会自动安装，用户无法将其移除，并且在安装完成之前，设备设置将无法完成。

Kiosk：该 App 会以 Kiosk 模式自动安装：它会被设为首选的主屏幕 Intent
，并加入锁定任务模式的白名单。在 App
安装完成之前，设备设置不会完成。安装后，用户将无法移除该 App。每个政策只能为一个 App 设置此

Kiosk

9.2.

App App

App

Wi-Fi App

App

App

9.3.

App

App (1) (2) (3)
24
App

App App 90 App 90
App
90 Play Store App

App

9.4.

APP_NOT_UPDATED
Google Play 20

9.5.

Android Device Policy App App Android

权限 ：授予权限政策和权限授予状态的访问权限。
包访问权限 ：授予包访问状态的访问权限。
系统 App：授予启用系统 App 的访问权限。

9.6. 优先网络
要用于此 App 的优先网络服务。如果设置，该 App 将在可用时使用指定的企业网络切片进行连接。这必须与
5G 网络切片配置 部分（位于 蜂窝网络 面板中）中配置的网络切片相匹配。

9.7. 默认权限政策
该 App 请求的所有权限的默认政策。如果指定，这会覆盖适用于所有 App 的政策级 默认权限政策
。它不会覆盖适用于所有 App 的权限政策 。
提示（默认） ：提示用户授予权限。
授予 ：自动授予权限。
拒绝 ：自动拒绝权限。

9.8. 连接的工作和个人 App
控制该 App 是否可以在设备的工作资料和个人资料之间与自身通信，但需征得用户同意（ Android 11 及更高版本）。
不允许（默认） ：阻止该 App 跨资料通信。
允许 ：在获得用户同意后，允许该 App 跨资料通信。

9.9. 始终开启的 VPN 锁定豁免
指定当 VPN 未连接且 锁定已启用 处于活动状态时，是否允许该 App 联网。仅在运行 Android 10
及更高版本的设备上受支持。
强制执行（默认） ：该 App 遵循始终开启的 VPN 锁定设置。
豁免 ：该 App 不受始终开启的 VPN 锁定设置约束。

9.10. 工作资料小组件
指定是否允许安装在工作资料中的 App 向主屏幕添加小组件。
允许 ：该应用程序可以向主屏幕添加小组件。
不允许 ：该应用程序无法向主屏幕添加小组件。

9.11. 用户控制设置
指定是否允许对指定 App 进行用户控制。用户控制包括强制停止和清除 App 数据等用户操作（ Android 11 及更高版本）。如果为某个 App 启用了 extensionConfig，则无论此设置如何，都不允许用户控制。对于
Kiosk App，您可以使用 允许 来允许用户控制。
未指定 ：使用该 App 的默认行为来决定是允许还是禁止用户控制。
允许 ：允许对该 App 进行用户控制。
不允许 ：禁止对该 App 进行用户控制。

9.12. 已禁用
该 App 是否已禁用。禁用后， App 数据仍会保留。

9.13. 允许凭据提供程序
是否允许该 App 在 Android 14 及更高版本上充当凭据提供程序。

9.14. 受管理的配置
要配置该 App 的受管理设置，请点击 启用受管理的配置 按钮。如果已为该 App
设置受管理的配置，您可以使用 受管理的配置 按钮修改配置，或使用 移除配置 按钮将其删除。

受管理的配置 选项仅适用于支持此功能的 App。

9.15. 权限政策
该 App 的明确权限授予或拒绝。这些值会覆盖适用于所有 App 的默认权限政策 和权限政策 。
使用 添加权限政策 为 App 卡片添加一条或多条权限规则，并使用删除操作将其移除。

9.16. 轨道 ID
设备可以访问的 App 封闭测试轨道 ID 列表。如果选择了多个轨道 ID
，设备将收到所有可访问轨道中的最新版本。如果未选择任何轨道 ID，设备只能访问该 App 的生产轨道。

轨道 ID选项仅适用于至少有一个轨道 ID 可供您的组织使用的 App。有关如何为特定 App
将您的组织添加到封闭测试轨道的更多详细信息，请阅读 此处 。

10. 默认应用程序设置

为受支持的类型设置默认 App。当至少为一种类型设置了默认 App 后，用户将无法在该资料中更改默认 App。

每个 默认应用程序类型 只允许一个默认应用程序设置。默认应用程序列表不得包含重复项。

10.1. 默认应用程序类型

选择要配置的 App 类别（例如浏览器、拨号器、短信、钱包或数字助理）。可用性取决于 Android
版本和管理模式。

10.2. 默认应用程序范围

选择默认 App 的适用范围（完全受管理、工作资料或个人资料）。只能选择所选类型支持的范围。

如果所选范围均不适用于设备的管理模式，设备会报告一条不合规详细信息。

10.3. 默认应用程序

可设置为所选类型默认值的 App 列表。第一个已安装且符合条件的 App 将设为默认值。

如果范围包括 完全受管理 或工作资料 ，则每个 App 还必须存在于 应用程序 列表中，且其 安装类型
未设置为 已阻止 。

11. 私钥选择

允许在设备上显示界面，以便在没有匹配 选择私钥规则 的规则时让用户选择私钥别名。

对于低于 Android P 的设备，设置此选项可能会使企业密钥面临风险。

12. 选择私钥规则

控制 App 对私钥的访问权限。该规则决定 Android Device Policy 向指定 App 授予哪个私钥（如果有）。当
App 调用 KeyChain.choosePrivateKeyAlias（或任何重载）为给定 URL
请求私钥别名时，会授予访问权限；对于不特定于 URL 的规则（即未设置 urlPattern
，或将其设置为空字符串或 .*），在 Android 11 及更高版本上，会直接授予访问权限，以便 App 可以调用
KeyChain.getPrivateKey，而无需先调用 KeyChain.choosePrivateKeyAlias。当 App 调用
KeyChain.choosePrivateKeyAlias 且有多条 choosePrivateKeyRules
匹配时，最后匹配的规则决定要返回的密钥别名。

使用 添加私钥规则 创建条目，并使用删除操作将其移除。

12.1. 私钥别名

要使用的私钥别名。

12.2. URL 模式

用于与请求 URL 匹配的 URL 模式。如果未设置或为空，则匹配所有 URL。这使用 java.util.regex.Pattern 的正则表达式语法。

12.3. 包名

此规则适用的包名。每个 App 的签名证书哈希都会与 Play
提供的哈希进行验证。如果未指定包名，则会向所有调用 KeyChain.choosePrivateKeyAlias 或任何重载的 App 提供该别名（但即使是在 Android 11 及更高版本上，也必须调用 KeyChain.choosePrivateKeyAlias ）。任何与此处指定的包具有相同 Android UID 的 App，在调用 KeyChain.choosePrivateKeyAlias
时将获得访问权限。

使用 添加包名 添加条目，并使用删除操作将其移除。

要删除 App，请点击 App 卡片底部的 回收站 图标。

Revision #6
Created 2026-11-10 15:18:53 UTC by Admin
Updated 2026-11-12 09:58:33 UTC by Admin