策略 - Android

- 摘要
- App 管理
- Kiosk 模式
- 安全
- 多媒体
- 蜂窝网络
- 网络
- 系统
- 位置和地理围栏
- 用户管理
- 个人使用
- 跨配置文件政策
- 状态报告
- 其他
- 合规性规则

摘要
Android 政策是系统的核心实体：它们定义了在受管设备上应用和执行的规则。

您可以从仪表板的 政策 部分浏览政策并创建新政策。要打开 Android
政策，请点击表格中的政策行：系统会打开 政策编辑器 页面。

政策可以与 注册令牌 关联，从而在配置过程中自动应用到设备。您还可以在配置后更改分配给设备的政策。

每台设备一次只能关联一个政策。

许多政策选项仅适用于特定设备类型（完全托管、专用、工作配置文件）和 Android
版本。不支持的设置可能会被设备忽略，或被报告为不合规。

政策编辑器布局
政策编辑器由一组可展开的部分组成。在页面顶部，您始终可以编辑：

名称 （必填）
ID（只读）
描述 （可选）

以下部分与政策编辑器面板相对应（例如：应用管理、安全、网络、系统、个人使用、跨配置文件政策等）。
打开已保存的政策时，设置已更改的部分已经展开，其他部分则保持关闭。请使用本手册的章节页面详细了解
每个面板。

保存、删除和关联设备
使用 保存政策 应用更改。没有待处理的编辑或许可证已过期时，该按钮会被停用。

如果您打开的是现有政策（带有 ID），页面底部会显示 删除政策 操作和 关联设备列表，以便您查看当前有多少台设备正在使用该政策。

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。

Kiosk 模式
使用 Kiosk 模式，你可以将设备的功能限制为单个应用或多个应用。选择单应用还是多应用 Kiosk
模式取决于你的业务目标。

在单应用 Kiosk 模式
下，设备配置为仅使用单个应用，并且不允许最终用户访问设备上的其他应用。他们也无法退出该应用，从而
使其成为该特定应用的专用设备。要启用此模式，请在 应用管理 部分中指定一个应用，并将 安装类型 设置为 Kiosk。

在多应用 Kiosk 模式
下，设备可以访问多个应用。最终用户可以通过自定义启动器在多个应用之间导航。要启用此模式，请开启
Kiosk 自定义启动器 选项。

启用 Kiosk 模式后，你还可以配置最终用户是否可以访问某些系统功能，例如系统设置和状态栏。

Kiosk 自定义启动器

是否启用 Kiosk 自定义启动器。这会将主屏幕替换为启动器，将设备锁定为通过 应用管理设置安装的应用。应用按字母顺序显示在单个页面上。

电源按钮操作

设置 Kiosk 模式下的设备在用户按住（长按）电源按钮时的行为。

可用（默认） ：当用户长按 Kiosk 模式下设备的电源按钮时，会显示电源菜单（例如关机、重启）。

已阻止 ：当用户长按 Kiosk
模式下设备的电源按钮时，不会显示电源菜单（例如关机、重启）。注意：这可能会阻止用户关闭设备。

系统错误警告

指定在 Kiosk
模式下是否阻止崩溃或无响应应用的系统错误对话框。阻止后，系统将强制停止该应用，就像用户在界面上选
择 “关闭应用 ”选项一样。

已阻止（默认） ：所有系统错误对话框，例如崩溃和应用无响应（ ANR
）都会被阻止。阻止后，系统会强制停止该应用，就像用户从界面关闭应用一样。
已启用 ：会显示所有系统错误对话框，例如崩溃和应用无响应（ ANR）。

系统导航
指定 Kiosk 模式下启用哪些导航功能（例如主屏幕、概览按钮）。
已禁用（默认） ：无法访问主屏幕和概览按钮。
仅主屏幕 ：仅启用主屏幕按钮。
已启用 ：启用主屏幕和概览按钮。

状态栏
指定在 Kiosk 模式下是否禁用系统信息和通知。
已禁用（默认） ：在 Kiosk 模式下禁用系统信息和通知。
仅系统 ：状态栏上仅显示系统信息。
已启用 ：在 Kiosk 模式下，状态栏上会显示系统信息和通知。注意：要使此政策生效，必须使用
kioskCustomization.systemNavigation 启用设备的主屏幕按钮。

设备设置
指定在 Kiosk 模式下是否允许使用设置应用。
允许（默认） ：在 Kiosk 模式下允许访问设置应用。
已阻止 ：在 Kiosk 模式下不允许访问设置应用。

安全
在本节中，您可以配置与安全相关的政策。

安全风险操作

选择当设备在状态报告中报告 SecurityRisk 时要执行的操作。

支持的 SecurityRisk 类型：

未知操作系统 ： Play Integrity API 检测到设备运行未知操作系统（ basicIntegrity 检查成功，但 ctsProfileMatch 失败）。

已入侵的操作系统 ： Play Integrity API 检测到设备运行已入侵的操作系统（ basicIntegrity
检查失败）。

硬件支持的评估失败 ：如果设备完整性字段中未显示 MEETS_STRONG_INTEGRITY 标签， Play Integrity API 会检测到设备不具备强大的系统完整性保证。

可用操作：

清除企业数据（默认）
：取消注册并清除工作数据（完全托管时清除整个设备，配置文件所属时仅清除工作配置文件）。

不执行操作 ：保持设备注册状态，不自动执行任何操作。

当您选择 清除企业数据 时，还可以配置清除选项：

保留恢复出厂设置保护 ：清除设备时保留恢复出厂设置保护 (FRP) 数据。

清除外部存储 ：执行清除时，同时清除设备的外部存储（如 SD 卡）。

清除 eSIM：对于企业所有设备，清除设备时会移除设备上的所有 eSIM
。在个人所有设备上，这会移除设备上受管理的 eSIM（通过 ADD_ESIM 命令添加的 eSIM
），不会移除任何个人所有的 eSIM。

1. 最长锁定时间

设备锁定前允许用户活动的最长时间（秒）。值为 0 表示无限制。

2. 充电时保持开启

设备保持开启的电池接入模式。使用此设置时，建议清除 最长锁定时间 ，以免设备在保持开启时自行锁定。
交流充电器 ：电源为交流充电器。
USB 端口 ：电源为 USB 端口。
无线充电器 ：电源为无线。

3. 锁屏已停用

如果为 true，则会为主显示器和 /或辅助显示器停用锁定屏幕。此政策仅在专用设备管理模式中受支持。

4. 密码要求

密码要求政策。
使用 配置密码要求 添加一个或多个密码要求块。使用 全部清除 移除所有已配置的密码要求。
密码要求可以使用 自动 范围（单一要求），或分别使用 设备 /工作配置文件
范围。基于复杂度的要求必须与同一范围的基于质量的要求配合使用。

4.1. 范围
密码要求适用的范围。
自动
：未指定范围。对于工作配置文件设备，密码要求应用于工作配置文件；对于完全托管或专用设备，应用
于整个设备。
设备 ：密码要求仅应用于设备。
工作配置文件 ：密码要求仅应用于工作配置文件。

4.2. 密码历史长度

密码历史的长度。设置此字段后，用户将无法输入与历史记录中任何密码相同的新密码。值为 0 表示无限制。

4.3. 清除前最多失败密码次数

设备被清除前可输入的错误设备解锁密码次数。值为 0 表示无限制。

4.4. 密码过期超时（天）

此设置强制用户在指定天数后定期更新密码。

4.5. 要求密码解锁

设备或工作配置文件使用强身份验证形式（密码、 PIN
、图案）解锁后，仍可使用任何其他身份验证方法（例如指纹、信任代理、人脸）解锁的时长。指定时间段过
后，只能使用强身份验证形式解锁设备或工作配置文件。

设备默认值 ：超时时间设置为设备默认值。

每天 ：超时时间设置为 24 小时。

4.6. 密码质量

所需的密码质量。

高复杂度 ：将高密码复杂度等级定义为：在 Android 12 及更高版本上： PIN 不含重复 (4444) 或有序
(1234、4321、2468) 序列，长度至少为 8；字母密码长度至少为 6；字母数字密码长度至少为 6。

中复杂度 ：将中密码复杂度等级定义为： PIN 不含重复 (4444) 或有序 (1234、4321、2468)
序列，长度至少为 4；字母密码长度至少为 4；字母数字密码长度至少为 4。

低复杂度 ：将低密码复杂度等级定义为：图案； PIN 包含重复 (4444) 或有序 (1234、4321、2468)
序列。

无 ：没有密码要求。

弱 ：设备至少必须使用低安全性生物识别技术进行保护。这包括能够识别个人身份且大致相当于 3 位 PIN 的技术（误检率低于 1/1,000）。

任意 ：需要密码，但对密码必须包含的内容没有限制。

数字 ：密码必须包含数字字符。

复杂数字 ：密码必须包含数字字符，且不含重复 (4444) 或有序 (1234、4321、2468) 序列。

字母 ：密码必须包含字母（或符号）字符。

字母数字 ：密码必须同时包含数字和字母（或符号）字符。
复杂 ：密码必须满足 passwordMinimumLength、passwordMinimumLetters、 passwordMinimumSymbols 等中指定的最低要求。例如，如果 passwordMinimumSymbols 为 2
，则密码必须至少包含两个符号。

4.7. 最小长度
允许的最小密码长度。值为 0 表示无限制。

4.8. 最少字母数

密码中所需的最少字母数。

4.9. 最少小写字母数

密码中所需的最少小写字母数。

4.10. 最少大写字母数

密码中所需的最少大写字母数。

4.11. 最少非字母字符数
密码中所需的最少非字母字符数（数字或符号）。

4.12. 最少数字位数

密码中所需的最少数字位数。

4.13. 最少符号数

密码中所需的最少符号数。

4.14. 统一锁
控制运行 Android 9
及更高版本且带工作配置文件的设备是否允许为设备和工作配置文件使用统一锁。对其他设备无效。允许统一锁 ：允许为设备和工作配置文件使用共同的锁。
要求单独的工作锁 ：工作配置文件需要单独的锁。

5. 恢复出厂设置已停用

是否停用从设置中恢复出厂设置。仅适用于完全托管设备。

6. 恢复出厂设置保护

用于恢复出厂设置保护的设备管理员电子邮件地址。当设备遭遇未经授权的恢复出厂设置时，需要其中一名管
理员使用 Google
账户电子邮件和密码登录才能解锁设备。如果未指定管理员，设备将不提供恢复出厂设置保护。仅适用于完全
托管设备。
管理员电子邮件 ：使用 启用恢复出厂设置保护 开始配置管理员。然后使用 添加管理员电子邮件添加地址，并使用删除操作将其移除。

7. 锁屏功能

可以停用的锁屏（锁定屏幕）功能。

7.1. 全部停用

停用所有当前和将来的锁屏自定义项。

7.2. 停用相机
在安全锁屏屏幕（例如 PIN）上停用相机。

7.3. 停用通知

在安全锁屏屏幕上停用显示所有通知。

7.4. 停用未隐藏内容的通知

在安全锁屏屏幕上停用未隐藏内容的通知。

7.5. 忽略信任代理状态
在安全锁屏屏幕上忽略信任代理状态。

7.6. 停用指纹

在安全锁屏屏幕上停用指纹传感器。

7.7. 停用向通知输入文本

在安全锁屏屏幕上停用向通知输入文本。

7.8. 停用人脸身份验证

在安全锁屏屏幕上停用人脸身份验证。

7.9. 停用虹膜身份验证

在安全锁屏屏幕上停用虹膜身份验证。

7.10. 停用所有生物识别身份验证

在安全锁屏屏幕上停用所有生物识别身份验证。

7.11. 停用所有快捷方式
在 Android 14 及更高版本上，在安全锁屏屏幕上停用所有快捷方式。

多媒体
在本部分中，你可以配置摄像头 /麦克风行为、 USB 数据访问、打印以及显示相关限制。

1. 摄像头访问

控制摄像头的使用以及用户是否可以访问摄像头访问开关（ Android 12+
）。通常，禁用摄像头在完全受管设备上适用于整个设备，而在工作配置文件设备上仅适用于工作配置文件内
部。

用户选择（默认） ：默认设备行为。摄像头可用，并且（ Android 12+
）用户可以切换摄像头访问权限。

已禁用
：所有摄像头均已禁用（完全受管：整个设备；工作配置文件：仅限工作配置文件应用）。摄像头访问开
关在受管范围内不起作用。

强制执行 ：摄像头可用。在运行 Android 12+
的完全受管设备上，用户无法切换摄像头访问权限。在其他设备 /版本上，其行为与用户选择相同。

2. 麦克风访问

在完全受管设备上，控制麦克风的使用以及用户是否可以访问麦克风访问开关（ Android 12+
）。此设置对非完全受管设备不起作用。

用户选择（默认） ：默认行为。麦克风可用，并且（ Android 12+）用户可以切换麦克风访问权限。

已禁用 ：麦克风已禁用（整个设备）。麦克风访问开关不起作用。

强制执行 ：麦克风可用。在 Android 12+ 上，用户无法切换麦克风访问权限。在 Android 11
或更低版本上，其行为与用户选择相同。

3. USB 数据访问

控制可以通过 USB 传输哪些文件和 /或数据。仅在公司所有设备上受支持。

禁止文件传输（默认） ：禁止文件传输，但允许其他 USB 数据连接（例如鼠标 /键盘）。

禁止数据传输 ：禁止所有类型的 USB 数据传输（ Android 12+ 且 USB HAL 1.3+
）。如果不支持，设备将回退到 “禁止文件传输 ”。

允许数据传输 ：允许所有类型的 USB 数据传输。

4. 打印

控制是否允许打印（ Android 9+）。

允许（默认） ：允许打印。

不允许 ：不允许打印（ Android 9+）。

5. 屏幕亮度设置

控制屏幕亮度模式以及（可选）亮度值。

屏幕亮度模式：

用户选择（默认） ：允许用户配置屏幕亮度。

自动 ：亮度自动调节，用户无法更改。你仍然可以设置亮度值，该值会用于自动调节的一部分（完全受管
Android 9+；公司所有 Android 15+ 上的工作配置文件）。

固定 ：亮度设置为配置的值，用户无法更改。亮度值为必填项（完全受管 Android 9+；公司所有 Android 15+ 上的工作配置文件）。

屏幕亮度：

值范围为 1 到 255（ 1 = 最低， 255 = 最高）。值为 0 表示未设置亮度值。

6. 屏幕超时设置

控制用户是否可以配置屏幕超时，以及在强制执行时的超时值。

屏幕超时模式 字段用于在用户控制和强制执行行为之间进行选择。

用户选择（默认） ：允许用户配置屏幕超时。

强制执行 ：屏幕超时设置为配置的值，用户无法更改（完全受管 Android 9+；公司所有 Android 15+
上的工作配置文件）。

屏幕超时：
超时持续时间（秒）。值必须大于 0。如果大于 最长锁定时间 ，系统可能会将其限制，并报告不合规。

7. 屏幕截图已禁用

是否禁用屏幕捕获。

8. 调节音量已禁用

是否禁用调节主音量。

9. 装载物理介质已禁用

是否禁用装载物理外部介质。

蜂窝网络
在本部分中，您可以配置与蜂窝网络相关的政策。

1. 飞行模式

控制用户是否可以切换飞行模式。
用户选择（默认） ：允许用户打开或关闭飞行模式。
已禁用 ：飞行模式已禁用。不允许用户打开飞行模式。在 Android 9 及更高版本上受支持。

2. 蜂窝网络 2G

控制用户是否可以切换蜂窝网络 2G 设置。
用户选择（默认） ：允许用户打开或关闭蜂窝网络 2G。
已禁用 ：蜂窝网络 2G 已禁用。不允许用户通过设置打开蜂窝网络 2G。在 Android 14
及更高版本上受支持。

3. 覆盖 APN

控制覆盖 APN 是启用还是禁用。启用后，将仅使用配置的覆盖 APN，设备上的所有其他 APN 都将被忽略。已禁用（默认） ：所有已配置的 APN
设置都会保存在设备上，但处于禁用状态且不生效。设备上的其他所有 APN 仍会继续使用。
已启用 ：仅使用覆盖 APN，其他所有 APN 均被忽略。此设置只能在运行 Android 10
及以上版本的完全受管设备上配置。

4. APN 设置

配置一个或多个 APN 条目。使用 添加 APN创建条目，使用 移除 APN将其删除。

每个 APN 都有必填字段：
APN 类型 ：为此 APN 选择一种或多种流量类型（可用性取决于管理模式和 Android 版本）。 APN 名称 ：运营商提供的 APN 标识符。
显示名称 ：在界面中显示的友好名称。

可选 APN 字段：
认证类型 、用户名 、密码 ：配置运营商认证（如需要）。
协议 和漫游协议 ： IP 协议配置。
网络类型 ：限制此 APN 可使用的蜂窝技术（例如 LTE/5G NR）。
代理地址 和代理端口 ：用于数据流量的 HTTP 代理（如适用）。
MMS 代理地址 、 MMS 代理端口 、 MMSC（ MMS 中心 URI） ： MMS 相关设置。
数字运营商 ID（ MCC+MNC） 和运营商 ID：运营商标识字段。
始终开启设置 ：此 APN 激活的 PDU 会话是否应始终开启。支持 Android 15 及以上版本。 MVNO 类型 ：移动虚拟网络运营商标识符类型。
MTU IPv4和 MTU IPv6： IPv4/IPv6 路由的最大传输单元。支持 Android 13 及以上版本。

5. 小区广播配置已禁用

是否禁用小区广播配置。

6. 移动网络配置已禁用

是否禁用移动网络配置。

7. 漫游数据已禁用

是否禁用漫游数据服务。

8. 拨出电话已禁用

是否禁用拨出电话。

9. SMS 已禁用

是否禁用发送和接收 SMS 消息。

10. 5G 网络切片配置

配置优先网络服务设置以启用企业 5G 网络切片。最多可设置 5
个企业切片，并将应用分配到特定网络以优化流量路由。

10.1. 默认优先网络

用于不在应用列表中的应用，或应用的 优先网络 未设置时的默认优先网络 ID。必须为指定的网络 ID 提供配置（除非设置为 无优先网络 ）。

注意： com.google.android.apps.work.clouddpc和com.google.android.gms
等关键应用不包含在此默认设置中。

10.2. 网络服务配置

使用 添加网络配置 创建切片配置。最多可添加 5 个配置。每个配置包含：

优先网络 ID（自动分配） ：网络 ID 会自动分配，无法更改。

回退到默认连接 ：是否允许回退到设备范围的默认网络。如果不允许，当 5G
切片不可用时，应用将无法访问互联网。

非匹配网络 ：受此配置约束的应用是否可以使用优先服务以外的网络。如果设置为 不允许 ，
回退到默认连接 也必须设置为 不允许 。需要 Android 14 及以上版本。

网络
在本部分中，你可以配置与网络相关的政策。

Wi‑Fi 配置可以由系统通过 WiFi 配置 预置和管理。根据 配置 Wi‑Fi上设置的值，用户对添加 /
修改网络可能拥有有限的控制权或没有控制权。

设备无线状态

1. Wi‑Fi 状态

控制 Wi‑Fi 的当前状态以及用户是否可以更改其状态。
用户选择（默认） ：允许用户启用 /禁用 Wi‑Fi。
已启用 ：Wi‑Fi 处于开启状态，不允许用户将其关闭（ Android 13+）。
已禁用 ：Wi‑Fi 处于关闭状态，不允许用户将其开启（ Android 13+）。

2. 最低 Wi‑Fi 安全级别

设备可连接的 Wi‑Fi 网络的最低要求安全级别。在 Android 13
及以上版本上，支持完全受管设备以及公司所有设备上的工作配置文件。
开放网络（默认） ：设备可以连接所有类型的 Wi‑Fi 网络。
个人网络 ：不允许开放 Wi‑Fi 网络；要求至少达到个人安全级别（例如 WPA2‑PSK）。
企业网络 ：要求企业 EAP 网络；不允许低于此安全级别的 Wi‑Fi 网络。
192 位企业网络 ：要求 192 位企业网络；这是最严格的选项。

3. 超宽带 (UWB) 状态

控制超宽带设置的状态以及用户是否可以将其开启或关闭。

用户选择（默认） ：允许用户开启或关闭 UWB。

已禁用 ： UWB 已禁用，不允许用户通过设置将其开启（ Android 14+）。

设备连接管理

4. 蓝牙共享

控制是否允许蓝牙共享。

允许 ：允许蓝牙共享（完全受管设备上的默认值， Android 8+）。

不允许 ：不允许蓝牙共享（工作配置文件上的默认值， Android 8+）。

5. 配置 Wi‑Fi

控制 Wi‑Fi 配置权限。根据所选选项，用户在配置 Wi‑Fi 网络时拥有完全、有限或无控制权。

允许配置 Wi‑Fi（默认） ：允许用户配置 Wi‑Fi。

不允许添加 Wi‑Fi 配置 ：不允许添加新的 Wi‑Fi 配置。用户可以在已配置的网络之间切换（ Android
13+；完全受管和公司所有的工作配置文件）。

不允许配置 Wi‑Fi：不允许配置 Wi‑Fi
网络。对于完全受管设备，这会移除用户配置的网络，仅保留通过 WiFi 配置
配置的网络。对于公司所有的工作配置文件，现有网络不受影响，但用户无法添加 /移除 /修改 Wi‑Fi
网络。

当禁用配置 Wi‑Fi 且设备在启动时无法连接时，系统可以显示 网络逃生通道
，让用户临时连接并刷新政策。

6. Wi‑Fi 直连设置

控制 Wi‑Fi 直连设置的配置和使用。在运行 Android 13 及以上版本的公司所有设备上受支持。

允许（默认）：允许用户使用 Wi-Fi 直连。

不允许：不允许用户使用 Wi-Fi 直连。

7. 网络共享设置

控制网络共享设置。根据设置的值，用户会被部分或完全禁止使用不同形式的网络共享。

允许所有网络共享（默认）：允许配置和使用所有形式的网络共享。

不允许 **Wi-Fi** 网络共享：不允许用户使用 Wi-Fi 网络共享（公司所有 Android 13+）。

不允许所有网络共享：不允许所有形式的网络共享（完全受管 + 公司所有的工作配置文件）。

8. Wi-Fi SSID 政策

限制设备可以连接到哪些 Wi-Fi SSID（这不会影响可以在设备上配置哪些网络）。在运行 Android 13 及以上版本的公司所有设备上受支持。

SSID 拒绝列表（默认）：设备无法连接到任何 SSID 已列出的 Wi-Fi 网络，但可以连接到其他网络。

SSID 允许列表：设备只能连接到已列出的 SSID。SSID 列表不能为空。

使用 添加 **SSID**添加条目。根据所选政策类型，该列表会被解释为允许或拒绝的 SSID。

在政策编辑器界面中，对于允许列表，SSID 列表标记为 允许的 **Wi-Fi SSID**；对于拒绝列表，标记为 拒绝的 **Wi-Fi SSID**。

9. Wi-Fi 漫游设置

按 SSID 配置 Wi-Fi 漫游模式。使用 添加 **Wi-Fi** 漫游设置 创建条目。

每个条目包括：

SSID：漫游设置适用的 SSID（必填）。

Wi-Fi 漫游模式：默认 / 已禁用 / 积极。已禁用和积极需要 Android 15+，并且仅在完全受管设备和公司所有设备上的工作配置文件中受支持。

网络限制

10. 蓝牙已禁用

是否禁用蓝牙。优先使用此设置而不是 “蓝牙配置已禁用 ”，因为用户可以绕过 “蓝牙配置已禁用 ”。

11. 蓝牙联系人共享已禁用

是否禁用蓝牙联系人共享。

12. 蓝牙配置已禁用

是否禁用蓝牙配置。

13. 网络重置已禁用

是否禁用重置网络设置。

14. 传出 Beam 已禁用

是否禁用使用 NFC 从应用传输数据。

VPN

15. 始终开启的 VPN 应用

指定始终开启的 VPN 包名，以确保指定受管应用的数据始终通过已配置的 VPN。

注意：此功能需要部署同时支持始终开启和按应用 VPN 功能的 VPN 客户端。

16. VPN 锁定

当 VPN 未连接时不允许联网。

17. VPN 配置已禁用

是否禁用 VPN 配置。

代理和网络服务

18. 优先网络服务

控制是否在工作配置文件上启用优先网络服务。例如，组织可能与运营商达成协议，通过专供企业使用的运营
商网络服务发送工作数据（例如 5G 网络上的企业切片）。这对完全受管设备没有影响。
已禁用 ：工作配置文件上的优先网络服务已禁用。
已启用 ：工作配置文件上的优先网络服务已启用。

如果你使用企业网络切片，还请在 蜂窝网络 政策面板下配置 5G 网络切片配置 ，并使用应用的
优先网络 设置将其分配到切片。

19. 推荐的全局代理

与网络无关的全局 HTTP 代理。通常，应在 WiFi
配置中按网络配置代理。全局代理可能对常规内部过滤等特殊配置有用。全局代理仅是建议，某些应用可能会
忽略它。
已禁用
直接代理
代理自动配置 (PAC)

19.1. 主机

直接代理的主机。

19.2. 端口

直接代理的端口。

19.3. PAC URI

用于配置代理的 PAC 脚本 URI。

19.4. 排除的主机

对于直接代理，指绕过代理的主机。主机名可以包含通配符，例如 ***.example.com**。

使用 添加排除的主机 添加条目（仅适用于直接代理）。

Wi-Fi 配置

定义系统将在设备上应用的 Wi-Fi 网络配置。使用 添加 **Wi-Fi** 配置 创建条目，并使用删除操作将其移除。

20. Wi-Fi 配置字段

每个配置包括：

配置名称 ：必填。

SSID：必填。

自动连接 ：是否应在网络处于范围内时自动连接。

快速转换 ：客户端是否应尝试使用快速转换 (IEEE 802.11r-2008) 连接网络。

隐藏 **SSID**：SSID 是否会被广播。

MAC 随机化模式 ：硬件或自动 (Android 13+)。

20.1. 安全

Wi-Fi 安全选项：

WEP-PSK：WEP（预共享密钥）。

WPA-PSK：WPA/WPA2/WPA3-Personal（预共享密钥）。

WPA‑EAP：WPA/WPA2/WPA3-Enterprise（可扩展身份验证协议）。
WPA3 192 位模式 ：仅允许 WPA3 192 位模式的 WPA‑EAP 网络。

20.2. 密码短语（预共享密钥）
当安全类型为 WEP‑PSK或WPA‑PSK时显示。密码短语为必填项。

20.3. EAP 方法（企业）
当安全类型为 WPA‑EAP或WPA3 192 位模式 时显示。选择一种 EAP 外部方法： EAP‑TLS
EAP‑TTLS
PEAP
EAP‑SIM
EAP‑AKA

20.4. 第 2 阶段身份验证
仅对隧道外部方法（ EAP‑TTLS和 PEAP）显示。
MSCHAPv2
PAP

20.5. 来自用户的 EAP 凭据
启用后，系统会按用户自动在设备上应用 EAP 凭据。您可以在 用户 部分配置用户凭据。

20.6. 客户端证书
对于 EAP‑TLS，您可以分配用于 Wi‑Fi 身份验证的客户端证书。有关详细信息，请阅读 证书管理 页面。如果已分配证书，您可以使用 打开证书 查看，或使用 更改证书 选择其他证书。
或者，您可以指定 客户端证书密钥对别名 ，它引用存储在 Android 密钥库中并允许用于 Wi‑Fi
身份验证的客户端证书。

如果同时设置了 客户端证书 和客户端证书密钥对别名 ，则忽略密钥对别名。

20.7. 身份

用户身份。对于隧道外部协议 (PEAP、 EAP‑TTLS)，它用于在隧道内进行身份验证，而 匿名身份 用于隧道外的 EAP 身份。对于非隧道外部协议，它用于 EAP 身份。

20.8. 匿名身份

仅适用于隧道协议，表示向外部协议呈现的用户身份。

20.9. 密码

用户密码。如果未指定，则默认提示用户输入。

20.10. 服务器 CA 证书
用于验证主机证书链的 CA 证书列表。至少有一个 CA 证书必须匹配。有关详细信息，请阅读 证书管理 页面。使用 添加服务器 CA 证书 添加条目，并使用删除操作将其移除。

20.11. 域后缀匹配
服务器域名的约束列表。这些条目用作对身份验证服务器证书备用使用者名称的 DNS
名称进行后缀匹配的要求。

系统
在本节中，您可以配置与系统相关的政策。

1. 最低 API 级别

允许的最低 Android API 级别。

2. 加密政策

是否启用加密。
默认 ：此值会被忽略，即不需要加密。
启用但不使用密码 ：需要加密，但启动时不需要密码。
启用并使用密码 ：需要加密，且启动时需要密码。

3. 自动日期和时间

是否在企业所有设备上启用自动日期、时间和时区。
用户选择（默认） ：自动日期、时间和时区由用户选择。
强制 ：在设备上强制使用自动日期、时间和时区。

4. 开发者设置

控制对开发者设置的访问权限：开发者选项和安全启动。
已禁用（默认） ：禁用所有开发者设置并阻止用户访问这些设置。
已允许 ：允许所有开发者设置。用户可以访问并选择性地配置这些设置。

5. 通用准则模式

控制通用准则模式 ——信息技术安全评估通用准则 (CC)
所定义的安全标准。启用通用准则模式会增强设备上的特定安全组件（例如：蓝牙长期密钥的 AES-GCM
加密、对某些网络证书的额外验证以及加密策略完整性检查）。通用准则模式仅在运行 Android 11
或更高版本的公司自有设备上受支持。警告：通用准则模式会强制执行严格的安全模型，通常只有高度敏感的
机构才需要。可能会影响设备的正常使用；请仅在需要时启用。

已禁用（默认） ：禁用通用准则模式。

已启用 ：启用通用准则模式。

6. Memory Tagging Extension (MTE)

控制设备上的 Memory Tagging Extension (MTE)。

用户选择（默认） ：用户可以选择在设备上启用或禁用 MTE（如果设备支持）。

强制启用 ： MTE 已启用，且不允许用户更改（ Android 14+
；在完全托管设备以及公司自有设备上的工作资料上受支持）。

已禁用 ： MTE 已禁用，且不允许用户更改（ Android 14+；仅在完全托管设备上受支持）。

7. 内容保护

控制是否启用内容保护（会扫描欺骗性应用）。此功能在 Android 15 及更高版本上受支持。

已禁用（默认） ：内容保护已禁用，用户无法更改此设置。

强制启用 ：内容保护已启用，用户无法更改此设置（ Android 15+）。

用户选择 ：内容保护不受政策控制；用户可以选择（ Android 15+）。

8. 辅助内容

控制是否允许将 AssistContent 发送到特权应用（例如助手应用，如圈选搜索）。 AssistContent
包含截图和有关应用的信息，例如包名。此功能在 Android 15 及更高版本上受支持。

已允许（默认） ：允许将辅助内容发送到特权应用（ Android 15+）。

已禁止 ：禁止将辅助内容发送到特权应用（ Android 15+）。

9. 创建窗口已禁用

是否禁用创建应用窗口之外的窗口。此选项会阻止显示以下系统界面： Toast 和 snackbar 、电话活动（如来电）和优先电话活动（如通话中）、系统提醒、系统错误和系统叠加层。

10. 网络应急通道

是否启用网络应急通道。如果启动时无法建立网络连接，应急通道会提示用户临时连接到网络，以便刷新设备
政策。应用政策后，临时网络将被遗忘，设备将继续启动。这样可以避免在上一项政策中没有合适的网络、且
设备以锁定任务模式启动到某个应用，或用户因其他原因无法访问设备设置时，出现无法连接网络的情况。

11. 默认活动

用于处理与特定 intent 过滤器匹配的 intent 的默认活动列表。例如，此功能允许 IT
管理员选择由哪个浏览器应用自动打开网页链接，或点按主屏幕按钮时使用哪个启动器应用。

使用 添加默认活动 创建条目。在条目中，使用 添加操作 和 添加类别 构建 intent 过滤器。

11.1. 接收方活动

应作为默认 intent 处理程序的活动。这应是 Android 组件名称，例如 com.android.enterprise.app/.MainActivity。或者，该值也可以是应用的包名，此时 Android Device Policy 会从该应用中选择合适的活动来处理 intent。

11.2. 操作

要在过滤器中匹配的 intent 操作。如果过滤器中包含任何操作，则 intent
的操作必须是这些值之一才能匹配。如果未包含任何操作，则忽略 intent 操作。

11.3. 类别

要在过滤器中匹配的 intent 类别。 intent
包含其所需的类别，所有这些类别都必须包含在过滤器中才能匹配。换言之，除非 intent 中指定了某个类别，否则向过滤器添加该类别不会影响匹配。

12. 允许的输入法

指定允许的输入法。

全部允许 ：未应用限制。允许所有输入法。
仅系统 ：仅允许系统内置输入法。
仅系统和提供的输入法 ：仅允许提供的输入法以及系统内置输入法。

12.1. 允许的输入法

允许的输入法包名。仅当 允许的输入法 设置为 仅系统和提供的输入法 时适用。使用 添加输入法 添加条目，并使用删除操作移除条目。

13. 允许的无障碍服务

指定允许的无障碍服务。
全部允许 ：可以使用任何无障碍服务。
仅系统 ：只能使用系统内置的无障碍服务。
仅系统和提供的服务 ：只能使用提供的服务以及系统内置的无障碍服务。

13.1. 允许的无障碍服务

允许的无障碍服务。仅当 允许的无障碍服务 设置为 仅系统和提供的服务 时适用。使用 添加无障碍服务 添加条目，并使用删除操作移除条目。

14. 系统更新政策

用于管理系统更新的配置。
默认 ：遵循设备的默认更新行为，通常需要用户接受系统更新。
自动 ：一旦有更新可用就自动安装。

窗口化 ：在每日维护窗口内自动安装。这还会将 Play
应用配置为在该窗口内更新。强烈建议自助服务终端设备使用此选项，因为这是 Play
更新持续固定在前台的应用的唯一方式。
推迟 ：最多可将自动安装推迟 30 天。

14.1. 维护窗口（仅窗口化）
当 系统更新政策 设置为 窗口化 时，可以使用 from和 to字段定义每日维护窗口。

14.2. 系统更新冻结期
每年重复的时间段，在此期间推迟无线 (OTA) 系统更新，以冻结设备上运行的 OS
版本。为防止设备无限期冻结，每个冻结期之间必须至少间隔 60 天。每个冻结期不得超过 90 天。使用 添加系统更新冻结期 创建条目。

15. 凭据提供程序默认值

控制哪些应用可以在 Android 14 及更高版本上充当凭据提供程序。

已禁止（默认） ：未指定 credentialProviderPolicy 的应用不允许充当凭据提供程序。
除系统外禁止 ：未指定 credentialProviderPolicy 的应用不允许充当凭据提供程序，但 OEM
默认凭据提供程序除外。

位置和地理围栏
此面板汇总了控制设备位置报告、位置强制执行和地理围栏定义的 Android 政策设置。当你希望 Cerberus Enterprise 收集设备位置，或检测设备进入或离开已配置区域时，请使用此面板。

位置报告

报告位置

启用设备地理位置报告。通过此设置收集的位置数据用于 仪表板位置地图
、设备概览位置历史和地理围栏处理。

位置历史记录和地理围栏事件保留 90 天
，更早的数据每晚自动删除。每台已注册设备的最新位置始终保留，因此它会保留在地图上。

在未完全受管理的设备上，位置数据可能仍取决于 Cerberus Enterprise
应用是否拥有所需的位置权限，以及设备是否启用了位置服务。

在个人 Apple 设备（用户注册）上，位置和地理围栏默认关闭：仅当 Apple 政策开启
个人设备上的位置和地理围栏 ，且用户允许 Cerberus Enterprise 应用使用位置时，它们才可用。

位置模式

控制公司所有设备上的设备位置设置。

用户选择 ：位置服务不受政策限制。
强制执行 ：设备上已启用位置服务。
已禁用 ：设备上的位置服务已禁用。

共享位置已禁用

为工作应用禁用位置共享。在配置文件所有者设备上，这会影响工作配置文件。在完全受管设备上，这会禁用
整个设备的位置并覆盖设备位置模式。

启用地理围栏时的自动行为
活动地理围栏需要位置报告才能正常工作。当至少有一个地理围栏处于活动状态时， Cerberus Enterprise 会自动保持相关位置设置一致。

存在活动地理围栏时， 报告位置 会被强制开启。
位置模式 被强制设置为 强制执行 。
共享位置已禁用 会被强制关闭。

如果你在一个或多个地理围栏处于活动状态时尝试禁用 报告位置 ， Cerberus Enterprise
会显示确认对话框。如果继续，政策中的所有活动地理围栏都将被停用。

地理围栏列表
一个政策最多可包含 10 个地理围栏 。地理围栏名称在政策内必须唯一。

使用 添加地理围栏 创建新条目。每个地理围栏包含以下主要字段：

名称 ：必填且唯一。
纬度 和经度 ：区域的中心。
半径（米） ：必填，范围为 200至 10000米。
描述 ：供管理员使用的可选备注。
报告进入 和报告退出 ：选择应生成哪些转换事件。
活动 ：启用或禁用地理围栏而不删除它。

每个地理围栏必须至少保持启用 报告进入 或报告退出 中的一项。

此前最小半径为 100 米。小于 200
米的现有地理围栏会继续正常工作，并且在保存政策时会保持原样，即使你移动或重命名它们也是如此
。如果你更改其半径，则半径必须至少为 200 米。

地图编辑工具
每个地理围栏卡片都包含该区域的地图预览。你可以在地图上或通过数值字段编辑几何形状。

当区域编辑已解锁时，点击地图可移动地理围栏中心。
使用 当前位置 按钮将地图居中到浏览器的当前位置。
使用 重新居中地图 按钮恢复该地理围栏的首选视口。
使用锁定按钮防止意外更改地理围栏几何形状。

地理围栏数据的显示位置

可以在 Android 的设备概览 页面中，通过位置面板的 地理围栏标签页查看地理围栏转换。该标签页会在专用地图上显示转换，并提供筛选工具和转换列表。

用户管理

添加用户已禁用
是否禁用添加新用户和配置文件。对于 managementMode 为 DEVICE_OWNER 的设备，此字段会被忽略，且绝不允许用户添加或移除用户。

修改账户已禁用
是否禁用添加或移除账户。

用户凭据配置已禁用
是否禁用配置用户凭据。

移除用户已禁用
是否禁用移除其他用户。

设置用户图标已禁用
是否禁用更改用户图标。

设置壁纸已禁用
是否禁用更改壁纸。

工作账户设置身份验证
控制用户在工作账户设置期间进行身份验证的方式。此选项仅适用于由受管理的 Google 域 (Google Workspace) 提供支持的 Android 企业。

在设备设置 /注册期间，此政策会影响是否需要登录工作账户，但 Google Admin Console 设置 使用 Google 进行身份验证 和注册令牌类型仍可能要求身份验证。

对于已注册的设备，此政策仅在设备由受管理的 Google Play 账户管理时适用（即注册时未使用 使用
Google 注册进行身份验证 ）。

有关更多详细信息和故障排除，请参阅 使用 Google 注册进行身份验证 。

阻止的账户类型

用户无法管理的账户类型。此选项可防止设备用户添加未经批准的账户。

使用 添加阻止的账户类型 添加一个或多个账户类型。

每个条目都有一个 账户类型 字段（必填）。输入诸如 com.google的字符串。使用删除操作移除条目。

个人使用

当为工作和个人用途配置企业所有设备
时，您可以指定一些规则，以限制用户在工作配置文件之外将设备用于个人用途的方式。

本节仅适用于带工作配置文件的企业所有设备。对完全托管或个人所有设备无效。

1. 相机已停用

相机是否已停用。

2. 屏幕截图已停用

屏幕截图是否已停用。

3. 工作关闭的最长天数

控制工作配置文件可保持关闭的时长。

4. 蓝牙共享

控制是否允许在带工作配置文件的企业所有设备的个人配置文件中进行蓝牙共享。

5. 私人空间

控制是否允许在设备上使用私人空间。

6. Play 商店模式

此模式控制个人配置文件的 Play 商店中允许或阻止用户使用哪些应用。

阻止名单（默认） ：所有应用均可用，任何不应出现在设备上的应用都应在 应用 部分明确标记为 已阻止
。
允许名单 ：只有在 应用 部分明确指定且 安装类型 设为 可用 的应用才允许安装到个人配置文件。

7. 应用

必须在个人配置文件中允许或阻止的应用列表。列表内容的行为取决于 Play 商店模式 的设置值。
要从 Play 商店添加新应用，请点击 +图标。

7.1. 安装类型

个人配置文件应用可以采用的安装行为类型。
已阻止 ：该应用被阻止，无法安装到个人配置文件。
可用 ：该应用可安装到个人配置文件。

8. 阻止的账户类型

用户无法管理的账户类型。此选项可防止设备用户在其个人配置文件中添加未经批准的账户。

跨配置文件政策
仅适用于同时具有个人配置和工作配置的设备。

跨配置文件复制 /粘贴

从一个配置文件（个人或工作）复制的文本是否可以粘贴到另一个配置文件。

不允许（默认）
：阻止用户将从工作配置文件复制的文本粘贴到个人配置文件。从个人配置文件复制的文本可以粘贴到工
作配置文件。

允许 ：在任一配置文件中复制的文本都可以粘贴到另一个配置文件。

跨配置文件数据共享
来自一个配置文件（个人或工作）的数据是否可以与其他配置文件中的应用共享。具体控制通过 intent 进行的简单数据共享。其他跨配置文件通信渠道（例如联系人搜索、复制 /粘贴、
或已连接的工作 & 个人应用）的管理需单独配置。

不允许 ：阻止从个人配置文件向工作配置文件以及从工作配置文件向个人配置文件共享数据。

不允许从工作配置文件共享到个人配置文件（默认）
：阻止用户将工作配置文件中的数据共享到个人配置文件中的应用。个人数据可以与工作应用共享。

允许 ：来自任一配置文件的数据都可以与另一个配置文件共享。

工作配置文件小组件默认值
工作配置文件小组件的默认行为。如果特定应用未定义小组件政策，则遵循此处设置的默认值。

跨配置文件应用功能
控制个人配置文件中的应用是否可以调用工作配置文件应用的应用功能。这需要 Android 16 及以上版本。

此设置取决于政策级别的 应用功能 选项（位于应用管理部分）。如果应用功能设置为 不允许 ，API
将拒绝将跨配置文件应用功能设置为 允许 。

个人配置文件中的工作联系人

存储在工作配置文件中的联系人是否可以显示在个人配置文件的联系人搜索和来电中。

允许（默认） ：允许工作配置文件联系人显示在个人配置文件中。

不允许 ：阻止个人应用访问工作配置文件联系人以及查找工作联系人。

除系统应用外不允许 ：阻止大多数个人应用访问工作配置文件联系人，但 OEM
默认电话、信息与联系人应用除外（ Android 14+）。

配置 “个人配置文件中的工作联系人 ”后，你可以选择定义 豁免包名
条目列表。根据所选模式，这些豁免对个人应用表现为允许列表或阻止列表。

状态报告

在本节中，您可以配置应从设备检索哪些数据。可以在 设备状态 仪表板页面中查看状态数据。

应用报告
是否启用应用报告。（报告的关于已安装应用的信息。）

此选项是系统所需的（用于配套应用集成），始终启用；无法停用。

包括已移除的应用
应用报告中是否包括已移除的应用。

设备设置
是否启用设备设置报告。（有关设备上安全相关设备设置的信息。）

软件信息
是否启用软件信息报告。（有关设备软件的信息。）

内存信息
是否启用内存报告。（与内存和存储测量相关的事件。）

网络信息
是否启用网络信息报告。（设备网络信息。）

显示信息
是否启用显示器报告。个人所有且带工作配置文件的设备无法使用报告数据。（设备显示信息。）

电源管理事件
是否启用电源管理事件报告。个人所有且带工作配置文件的设备无法使用报告数据。

硬件状态
是否启用硬件状态报告。个人所有且带工作配置文件的设备无法使用报告数据。

系统属性
是否启用系统属性报告。

通用准则模式
是否启用通用准则模式报告。

其他

1. 彩蛋游戏已禁用

是否禁用设置中的彩蛋游戏。

2. 跳过首次使用提示

用于在首次使用时跳过提示的标志。企业管理员可以启用系统建议，让应用在首次启动时跳过用户教程和其他
介绍性提示。

3. 简短支持消息

当管理员禁用了某些功能时，在设置界面中向用户显示的消息。如果消息超过 200 个字符，可能会被截断。

4. 长支持消息

在设备管理员设置界面中向用户显示的消息。

5. 所有者锁屏信息

要在锁屏上显示的设备所有者信息。

6. 设置操作

在设置过程中要执行的操作。在注册期间，你可以要求用户打开设备设置所需的一个或多个应用。使用 添加设置操作 创建条目，并使用删除操作将其移除。

6.1. 启动应用

要启动的应用的包名

6.2. 标题

提供面向用户的消息，向用户解释为什么需要启动该应用。

6.3. 描述

提供面向用户的消息，向用户解释为什么需要启动该应用。

7. 企业显示名称可见性

控制企业显示名称是否在设备上可见（例如，在公司所有设备上作为锁屏消息）。
可见（默认） ：企业显示名称在设备上可见（支持 Android 7+ 上的工作配置文件和 Android 8+ 上的完全受管设备）。
隐藏 ：企业显示名称在设备上隐藏。

合规性规则
如果设备或工作配置文件未遵守下面列出的任何政策设置， Android Device Policy 默认会立即阻止使用该设备或工作配置文件：

密码要求
加密政策
锁屏已停用
允许的输入法
允许的无障碍服务

如果设备或工作配置文件在 10 天后仍不合规， Android Device Policy 会将设备恢复出厂设置或删除工作配置文件。

在本节中，您可以覆盖默认的合规性执行规则或添加新规则。

规则

定义特定政策无法应用于设备时的行为的规则列表。

使用 添加规则 创建新规则。可以使用删除操作移除每个规则卡片。

设置名称

要执行的顶级政策。例如 应用 或密码要求 。

必填。 该值必须与受支持的顶级政策名称匹配；否则该字段会被标记为无效。

多少天后阻止

政策不合规多少天后阻止设备或工作配置文件。要立即阻止访问，请设为 0。多少天后阻止 必须小于多少天后清除 。仅适用于企业所有设备。

允许范围： 0–300。

阻止范围

指定阻止操作的范围。仅适用于企业所有设备。

默认（新规则）： 工作配置文件 。

工作配置文件 ：阻止操作仅应用于工作配置文件中的应用。个人配置文件中的应用不受影响。

整个设备 ：阻止操作应用于整个设备，包括个人配置文件中的应用。

多少天后清除
政策不合规多少天后清除设备或工作配置文件。
多少天后清除 必须大于 多少天后阻止 。仅适用于企业所有设备。必填。 默认（新规则）： 1。
允许范围： 1–300。

保留恢复出厂设置保护
是否在设备上保留恢复出厂设置保护数据。此设置不适用于工作配置文件。
默认（新规则）：已启用。