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。

Revision #6
Created 2026-11-10 15:18:48 UTC by Admin Updated 2026-11-12 09:58:28 UTC by Admin