Apple 政策
Apple 政策定义了 Cerberus Enterprise 通过 MDM 应用于 Apple 设备的管理设置。这些设置可在仪表板的
Apple 政策编辑器中进行配置。

开始之前

Apple 设备管理要求配置 Apple Management (APNs)。如有需要，请阅读 Apple Management 设置 (APNs) 页面。

打开 Apple 政策编辑器
在仪表板中，打开 政策 ，然后点击 创建新的 Apple 政策 。要编辑现有 Apple
政策，请在政策表格中点击其所在行。

编辑器布局
Apple 政策编辑器由一组可展开的部分组成。在页面顶部，您可以随时编辑：

名称 （必填）
ID（只读）
描述 （可选）

政策部分
以下部分与 Apple
政策编辑器中当前可用的面板相对应。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：

App 管理 ：配置与 App 相关的限制、受管理的 App 以及 Cerberus Enterprise App 设置。 Kiosk 模式与主屏幕 ：单一 App 模式、允许和阻止的 App、主屏幕布局、 Web Clip
、通知设置和锁定屏幕信息。
安全 ：控制自动解锁和生物识别解锁等功能。

密码设置 ：配置密码要求及相关规则。
多媒体 ：允许 /禁止相机及相关功能。
蜂窝网络 ：控制与蜂窝网络相关的设置（应用的蜂窝数据设置、 eSIM、套餐变更）以及蜂窝 APN。网络 ：Wi-Fi 网络（也包括企业 802.1X）、 VPN、证书、全局代理、加密 DNS 和 Web
内容过滤器，以及 AirDrop 和蓝牙等连接限制。
系统与用户界面 ：限制 Handoff、设备名称和屏幕保护程序等系统功能。
软件更新 ：要求在截止日期前使用某个 OS 版本，并控制更新的下载和安装方式。
macOS： Mac 的防火墙、 Gatekeeper
、屏幕保护程序与锁定、外部和网络存储、屏幕共享、隐私权限和登录项。
Apple 应用与服务 ：限制 iMessage、Game Center 和“查找 ”等 Apple 应用与服务。 Siri 与 Apple Intelligence：限制 Siri、听写和 Apple Intelligence 功能。 iCloud：允许或禁止特定的 iCloud 服务（备份、钥匙串同步、私人中继等）。
位置和地理围栏 ：安装了 Cerberus Enterprise 应用的 iPhone 和 iPad
会在进入或离开这些区域时报告，供事件规则使用。
账户 ：限制账户修改，并配置邮件、 Exchange、Google、日历、通讯录和目录账户。
合规性规则 ：使设备不合规的要求（密码、最低 OS 版本、监督、 FileVault
），并可选择阻止设备。

Apple 政策编辑器中的许多选项都包含工具提示，其中说明了要求和受支持的 OS 版本。

保存、删除和关联设备
使用 保存政策 应用您的更改。当没有待处理的编辑或许可证已过期时，该按钮会被禁用。

编辑现有政策时，页面还会显示 删除政策 操作。编辑器可在底部显示 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。

后续页面
App 与描述文件：配置已安装的 App 和配置描述文件。
Kiosk 模式与主屏幕：单一 App 模式、允许的 App、主屏幕布局和 Web Clip。
密码：配置密码要求及相关安全选项。
限制：定义允许的功能和 OS 级别的限制。
网络： Wi-Fi 网络、 VPN、证书和连接限制。
软件更新：必需的 OS 更新和软件更新设置。
macOS： Mac 的防火墙、 Gatekeeper、屏幕锁定、存储、隐私权限和登录项。
位置和地理围栏： iPhone 和 iPad 报告进入和离开的区域，以及它们正常工作所需的条件。账户：邮件、 Exchange、Google、日历、通讯录和目录账户。
合规性规则：设备要求以及阻止不合规设备。

Revision #6
Created 2026-11-10 15:18:40 UTC by Admin

Updated 2026-11-12 09:58:19 UTC by Admin