策略 - Apple

Apple 政策
应用与描述文件
自助服务终端与主屏幕
密码
限制
网络
软件更新
macOS
位置和地理围栏
账户
合规性规则

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。

应用与描述文件
本节介绍如何为 Apple 设备配置受管应用和账户负载。

应用管理
应用管理 面板包含与应用相关的常规限制以及受管应用列表。

常规应用限制

允许 App Clip
允许安装应用
允许移除应用
允许自动下载应用
允许隐藏应用
允许锁定应用
允许 App 内购买
允许修改默认浏览器
允许信任企业应用

受管应用

使用 添加应用
将应用添加到政策。每个受管应用都会显示为一张卡片。您可以展开卡片以编辑其设置，并使用删除操作移除
该应用。

App Store ID：受管应用的 App Store 标识符。
Bundle ID：应用包标识符。
安装行为 ：控制应用必须保持安装，还是可以由用户安装 /移除。
分配 ：许可证类型，由 Cerberus 为每台设备选择：公司设备使用设备许可证，个人 iPhone 和 iPad
（用户注册）使用 Managed Apple Account 的用户许可证。该字段无法更改。
VPP 许可证 ：通过 App Store 安装时使用的 VPP 许可证类型。

应用选择列表会显示每个应用的可用许可证和总许可证。免费应用会显示 无限制 ：Apple
为其提供无限许可证。一个应用只能添加到政策一次：如果应用的 App Store ID 或 Bundle ID
与政策中已有的应用相同，则会被拒绝；保存时列出同一应用两次的政策也会被拒绝。

应用选择列表会显示您的 Apple Business 资料库中的应用。要添加应用，请在 Apple Business 中打开 Apps
& Services → Apps & Books → App Store，搜索该应用并点击 View。对于免费应用，点击 Add，选择
All current and future（或 Organizational Units中与您的 Apps and Books
令牌对应的组织单位），点击 Add，然后 Review并确认。对于付费应用，点击其价格，选择 Managed
Licenses作为 License Type（Cerberus Enterprise 无法使用兑换代码），选择您的 Apps and Books
令牌的 Organizational Unit，输入 Licenses数量（每个订单最多 1,000 个），然后 Review
并购买。必须先通过 Settings → Payments & Billing → Apps & Services → Payment Methods 设置付款方式。随后应用会显示在应用选择列表中。

个人设备上的应用（用户注册）

使用用户注册注册的个人 iPhone 和 iPad 没有序列号，因此它们会获得政策中 App Store
应用，并使用设备上登录的 Managed Apple Account 的用户许可证 。Cerberus 会自行向 Apps and Books
注册该账户并分配许可证，包括免费应用。 Managed Apple Accounts 和 Apps and Books
令牌必须属于同一个 Apple Business
组织。付费应用每个账户使用一个许可证，由该账户的所有个人设备共享。

正在等待用户许可证 ：只有在 Apple
确认许可证后（通常在几分钟内），应用才会发送到设备。设备的 应用程序 面板会显示原因。
用户许可证失败 ：Apple 无法分配许可证，例如付费应用已无剩余许可证。请在 Apple Business
中添加许可证，然后使用 再次请求 ；Cerberus 也会每天自行重试。
安装提示 ： iOS 会在安装每个应用前询问用户。如果用户取消，应用会显示 正在等待用户批准安装
；再次请求 会再次显示提示。
释放
：从政策中移除应用，或取消注册该账户的最后一台个人设备，都会移除应用并释放其许可证，除非
同一账户的另一台已注册设备仍需要它。

有关详细信息，请参阅 Apple 账户驱动注册 。

受管配置

受管配置会按照应用供应商的文档说明为应用提供其设置（例如服务器地址或账户名称）。在政策中打开该应
用，然后点击 添加受管配置 。它会发送到运行 iOS 或 iPadOS 18.4 或更高版本 的 iPhone 和 iPad
，以及运行 macOS 27 或更高版本 的 Mac；目前不会发送到 Apple Vision Pro
。应用必须支持受管配置：不读取它的应用会忽略它。应用面板会在应用名称旁边显示键的数量。

键
：每一行都有一个键、一个类型和一个值。类型包括文本、整数、十进制数、布尔值、日期、文本列
表和整数列表。键区分大小写且必须唯一。 添加键 会添加一行； 移除配置 会移除所有键。
变量 ：文本和文本列表值可以包含 $EMAIL$、$USERNAME$、$FULLNAME$、$SERIAL$ 和
$UDID$，它们会被替换为每台设备及其用户的值。没有值的变量（例如没有用户的设备上的
$EMAIL$）会留空，系统日志会说明这一点。当用户的详细信息更改时，设备会获得新值；对于从
Google Directory 同步的用户，这些值会在下次更改政策或设备时更新。

导入配置 ：打开或粘贴应用供应商为 MDM 发布的文件，然后点击 读取 。AppConfig 规范文件 （
specfile.xml
）会列出应用支持的每个键及其描述、类型、默认值和允许值：选择要导入的键（具有默认值的键已
预先选中），并在导入后填写其他键。如果规范文件属于另一个应用，会出现警告。 属性列表
（整个属性列表或仅其 <dict>
）会按原样导入。然后选择是替换当前键还是添加到其中。不支持嵌套字典、数据值以及包含混合或
未知类型的列表，它们会被列为已跳过。 Apple
不会发布应用的配置键，因此如果供应商的文档中没有该文件，请向他们索取。 复制为 plist
会按设备接收时的原样复制配置，此时变量尚未替换。
限制 ：每个应用最多 200 个键；键最多 255 个字符；文本值最多 4,096 个字符；列表最多 200
个项目，每个项目最多 1,024 个字符；日期介于 1970 和 9999 之间；每个应用总共 64 KB。不适用于密码
：配置只会发送到为其构建的设备，日志仅显示键名称和类型，但仪表板管理员可以读取这些值，而
且设备下载配置的地址会随值变化，因此容易猜测的值（布尔值或小数字）可能会被推断出来。请勿
在受管配置中放置密码或其他机密信息。
状态 ：当设备报告应用未接受其配置时，设备的应用程序面板会在应用旁边显示 配置未接受
。这不会使设备不合规。设备无法下载配置则会使设备不合规。

应用选项

政策中的每个应用（ App Store 应用和自定义应用）都有这些选项。 设备默认值
将选择权留给设备。不支持某个选项的设备不会获得该选项；应用仍会安装。

自动更新 ：App Store 设置，始终或从不。 iOS、iPadOS、macOS 和 visionOS 26
或更高版本。对于自定义应用， App Store 设置的行为与 “从不 ”相同。
通过蜂窝网络下载 ：App Store 设置，始终或从不，用于自动安装和更新。仅适用于运行 iOS 或
iPadOS 26 或更高版本的受监管 iPhone 和 iPad。
备份应用数据 ：应用数据是否会包含在设备备份中。不适用于 Mac。
用户可以隐藏应用 和用户可以锁定应用 ： iOS 和 iPadOS 18.1
或更高版本，在受监管设备上强制执行。不允许锁定也会阻止隐藏。 允许隐藏应用 和允许锁定应用
限制适用于所有应用。
在需要客户 PIN 的 Tap to Pay 交易后锁定设备 ：仅限 iPhone。
关联域名 ：与应用关联的域名（例如用于通用链接或密码自动填充），最多 50
个。请输入纯主机名，例如 www.example.com，不要包含 applinks:、通配符或 ?mode=
。不适用于 Mac。
直接验证域名 ：设备直接检查域名的站点关联文件，而不是通过 Apple
的服务器。仅对无法从互联网访问的内部域名启用此功能。
移除 ：以 必需 方式安装的应用无法由用户移除。

Mac App Store 应用
应用选择列表会显示每个应用的平台（ iPhone/iPad、 Mac、Apple TV、Vision）；仅适用于 Mac
的应用会显示其 Mac 图标。仅适用于 Mac 的应用在添加时会应用到 Mac。没有 Mac 版本的 App Store

应用不会发送到 Mac：政策会在 适用于 下显示 “此应用没有 Mac 版本：不会发送到 Mac”。 Mac 会通过其 App
Store ID 获取 App Store 应用，因此在 Mac 上 Bundle ID 不同的应用也能正确安装。

Cerberus Enterprise 应用
Cerberus 会在每台 iPhone 和 iPad 上安装其 Cerberus Enterprise应用（要求 iOS 或 iPadOS 18.4
或更高版本 ），无论是否有政策。该应用会共享设备位置，并接收通知和实时跟踪请求。它以 必需
方式安装，并使用来自 Apps and Books 的设备许可证（个人设备上为用户许可证），因此用户无法删除它。

一次性设置 ：将免费应用添加到您的资料库一次。在 Apple Business 中，打开 Apps & Services
→ Apps & Books → App Store，搜索 "Cerberus Enterprise"，点击 View，然后 Add，选择
All current and future（位于 Organizational Units中），点击 Add，然后 Review
并确认。如果应用显示 Manage，则表示它已在您的资料库中：打开它并检查其组织单位是否为 All current and future units。在此之前，仪表板会显示横幅，设备会将应用显示为未安装。请参阅
账户设置 。
不在政策中
：该应用无法添加到政策。它会在应用选择列表中被禁用，并会作为自定义应用被拒绝（相同的
Bundle ID）。已列出它的政策在打开时该条目会被移除：保存政策以确认。
不安装于 ：运行低于 18.4 的 iOS 或 iPadOS 的设备。共享 iPad
支持安装，但应用功能尚未在那里验证。
个人设备 ：在使用用户注册的 iPhone 和 iPad 上，也会安装该应用，并显示安装提示，且使用
Managed Apple Account 的用户许可证。它会接收来自您组织的消息，并且除非政策开启
个人设备上的位置和地理围栏 且用户允许，否则不会访问位置。
保持安装 ：如果 Apps and Books
令牌过期或应用离开您的资料库，应用会保留在设备上，设备页面会显示 Apps and Books
需要处理。只有在 24 小时后应用中仍不在您的资料库中时，它才会被移除。

自定义应用

自定义应用是您自己的 iPhone 和 iPad 应用（.ipa 文件），不经 App Store 分发。在 Xcode
中，将应用导出为 Enterprise分发（ Apple Developer Enterprise Program：可安装到每台设备）或 Ad
Hoc分发（仅安装到其描述文件中注册的设备）。无法上传 App Store 构建版本。

点击 添加自定义应用 打开您组织的自定义应用。 上传应用 会添加一个 .ipa 文件（最大 2 GB
）。选择一个应用并点击 添加到政策 。列表会显示版本、签名类型、 ad hoc
应用描述文件中的设备数量以及描述文件的到期日期。

新版本 ：上传具有相同 Bundle ID
的应用。它会替换以前的版本，使用该应用的政策的设备会更新该应用。
要求 ：运行 iOS 17.2 或更高版本的 iPhone 和 iPad。无法安装该应用的设备不会获得它：例如
iPhone 上的仅 iPad 应用、低于应用要求的旧版 iOS、不在 ad hoc
应用描述文件中的设备，或已过期的描述文件。
到期 ：当描述文件过期时，应用将无法再打开。请在到期日期之前上传使用新描述文件签名的版本。

保留的 Bundle ID： Bundle ID 为 Cerberus Enterprise 应用（ com.lsdroid.Cerberus.Enterprise）的自定义应用无法添加到政策，因为 Cerberus
会自行安装该应用。
删除 ：先将该应用从其政策中移除；随后设备会将其删除。

Mac 软件包

自定义应用还接受 Mac 安装包（.pkg 文件）。该安装包必须是使用 productbuild构建的分发包（仅使用 pkgbuild 制作的组件包会被拒绝），并使用 Developer ID Installer
证书签名。建议对其进行公证并附加票据（ notarytool和 stapler
）。未签名的安装包、签名后更改过的安装包以及使用其他证书签名的安装包都会被拒绝。

使用 上传应用 上传 .pkg 文件，并将其添加到政策中：它会显示在 Mac 软件包 下。 iPhone 和 iPad
会忽略它。

运行 macOS 26 或更高版本 的 Mac（受监管，包括手动注册的 Mac，但不包括用户注册）会以 声明
形式获取该安装包： Mac 会自行下载、安装、重试和更新它，并报告其状态。较旧的 Mac
，以及作为受管理应用安装的安装包，会通过 MDM 命令 获取，适用于任何 macOS 版本。升级到 macOS 26 的 Mac 会自行改用声明；它可能会再次安装每个安装包。当 Mac
迁移到另一个包含相同安装包的政策时，也可能发生同样的情况。

新版本 ：上传具有相同安装包标识符的安装包。它会替换之前的版本，使用它的政策中的 Mac
会安装新版本。
已跳过的 Mac： macOS 版本低于安装包要求的 Mac，以及对于仅为 Apple silicon
构建的安装包而言的 Intel Mac
。设备页面会将该安装包显示为已跳过，并说明原因；之前安装的版本会保留在 Mac 上。
安装 ：必需 （默认）会在 Mac 上安装该安装包； 可选 会使该安装包在 Mac 上可用但不安装。
macOS 26 不会在 “系统设置 ”或 App Store 中向用户显示可选安装包（已在 macOS 26.3
上测试），因此必须由 Mac 上的应用或脚本安装它们；仅当你已有此类应用或脚本时才选择 “可选 ”
。此设置适用于运行 macOS 26 或更高版本的 Mac；较旧的 Mac
始终会安装该安装包。作为受管理应用安装的安装包无法使用此选项。
安装包离开政策时移除其文件（ macOS 27 或更高版本） ：当安装包从政策中移除时，运行
macOS 27 或更高版本的 Mac 会删除它安装的文件。此选项默认关闭。在较旧的 Mac
上，文件会保留。作为受管理应用安装的安装包无法使用此功能。
作为受管理应用安装 ：为政策中的某个安装包开启此选项，以将其应用作为受管理应用安装（
macOS 11 或更高版本，不适用于用户注册）。随后 macOS 会在安装失败时报告， MDM
可以移除该应用。应用必须直接安装在 “应用程序 ”文件夹中，使用 Developer ID Application
证书签名并经过公证；在 macOS 11 到 13
上，安装包必须只包含该应用（不能有其他文件或脚本）。自定义应用会显示哪些安装包符合条件。
当无法在 Mac 上应用此选项时，安装包会照常安装在该 Mac 上，设备页面会说明原因。
受管理应用的 移除选项 ：安装包从政策中移除时移除应用 （默认开启）和 Mac
离开管理时移除应用
。移除应用还会删除其数据。如果用户已经安装了同一个应用，该副本会变为受管理应用并被一并移
除。

移除 ： MDM
命令无法卸载安装包。对于作为受管理应用安装的安装包，从政策中移除它会移除该应用（当该选项
开启时）；它的其他文件和安装包收据会保留。开启 移除安装包文件 的安装包会从运行 macOS 27
或更高版本的 Mac 上移除。其他安装包：从政策中移除它们只会停止新的安装，文件会保留在 Mac
上。被跳过的 Mac（例如在新版本需要更新的 macOS
之后）在安装包仍位于政策中时会保留该应用；此时从政策中移除安装包也会将其移除。请手动移除
Mac 上残留的文件（例如使用安装包自带卸载程序），并运行 sudo pkgutil --forget <identifier> 以清除安装包收据。
设备上的状态 ： Mac 的 “应用程序 ”面板会将政策中的每个安装包显示为排队中、已接受（ Mac
已接受该命令）、已下载、已安装（仅适用于包含应用的安装包，且在 Mac
上找到这些应用时）或失败（并显示错误）。 macOS
不会报告通过命令发送的安装包的安装情况，因此对于不含应用的安装包， “已下载 ”
是最后的状态。当 macOS 报告应用无法安装或已从 Mac
上移除时，作为受管理应用安装的安装包也会变为 “失败 ”。重新安装 会再次将安装包发送到 Mac。
使用声明时的状态 ：以声明形式交付的安装包会显示 声明 标签以及 Mac
报告的状态：排队中、可用（用户尚未安装的可选安装包）、等待用户操作、下载中、安装中、已安
装或失败（并说明原因，例如下载或安装失败，或 Mac 拒绝了声明）。 随政策移除文件
标签会标记那些在离开政策时由运行 macOS 27 的 Mac 移除其文件的安装包。 重新安装
仅在失败后出现，用于请求 Mac 重试；当 Mac 拒绝了声明时不会提供。

账户
账户 面板可让你配置应用于受管理设备的账户。它还包含一个用于账户修改的限制开关。

限制

允许修改账户 ：禁用后，用户无法修改 Apple 账户和互联网账户等账户。

添加账户

使用 添加 Google 账户 或添加邮件账户
将账户有效负载添加到政策中。每个账户会以卡片形式显示，并带有其配置字段。

来自用户的账户凭据

Google 和邮件账户卡片都提供一个 来自用户的账户凭据
开关。启用后，系统会按用户分别应用账户凭据。禁用后，你需要在政策中输入账户身份。

Google 账户字段

- [illegible]
- **Google** [illegible]
- [illegible]

[illegible]

[illegible] /[illegible]

- [illegible]
- [illegible]
- [illegible]

[illegible]

- [illegible] IMAP [illegible] POP[illegible]
- [illegible]
- **IMAP** [illegible] IMAP [illegible]
- [illegible]
- [illegible] 1–65535[illegible]

[illegible]

- [illegible]
- [illegible]
- [illegible] 1–65535[illegible]

S/MIME [illegible]

[illegible] S/MIME [illegible]

[illegible]

- **S/MIME** [illegible]
- [illegible]
- [illegible]
- [illegible]

[illegible]

- **S/MIME** [illegible]
- [illegible]
- [illegible]

>

自助服务终端与主屏幕
Apple 政策编辑器的 自助服务终端与主屏幕
部分可将设备锁定到单个应用、选择允许打开哪些应用、排列主屏幕并添加网站图标。每项设置都会作为配置
描述文件安装到设备上。

Apple 只会将其中大多数设置应用于受监督的 iPhone 和 iPad（通过 Automated Device Enrollment
注册或使用 Apple Configurator 准备的设备）。其他设备不会获得这些设置。 Web Clip
也可在未受监督的 iPhone 和 iPad 上使用。 Mac 不会获得这些设置中的任何一项。

选择应用
应用通过其 bundle ID 标识。输入应用名称即可从内置 Apple 应用和政策中的应用中选择，也可以输入任意
bundle ID，例如 com.example.app。

单应用模式
设备仅运行所选应用：用户无法返回主屏幕或打开其他应用。请先通过政策安装该应用。关闭此设置或移除该
应用后，设备会退出单应用模式。

选项 ：禁用触摸屏、旋转、音量按钮、响铃 /
静音开关、侧边按钮或自动锁定，并开启旁白或缩放等辅助功能。
用户可开启的辅助功能 ：用户可通过连按三次侧边按钮开启的功能。

允许和阻止的应用
阻止的应用 ：设备会隐藏这些应用并且不打开它们。 com.apple.webapp 会阻止所有 Web Clip
。设置以及 iPhone 上的电话无法被阻止。
仅允许部分应用 ：设备仅显示这些应用。将列表留空可允许所有应用。 政策应用
会添加由政策安装的应用； com.apple.webapp会允许所有 Web Clip。
可以启动单应用模式的应用 ：可以在需要时（例如考试期间）将设备锁定到自身的应用。

使用 仅允许部分应用 时，不在列表中的所有应用都会从设备上消失，包括政策中的应用。设置以及
iPhone上的电话始终保留。

主屏幕布局
安排程序坞和主屏幕页面。添加应用、应用文件夹和政策的 Web Clip，并使用 添加到
选择位置，然后拖动图标以在程序坞和页面之间移动它们。点击文件夹可更改其名称和应用。

用户无法移动图标或从主屏幕移除应用。不在布局中的应用会进入您定义页面之后的页面。 iPhone
在程序坞中显示四个图标。用户仍然可以在设置的存储空间中删除非必需的应用。要阻止此操作，请在应用管
理中关闭 允许移除应用 。

Web Clip
Web Clip 是主屏幕上的一个图标，用于打开网站。设置标签和 URL，并可选择一张图像（ PNG 或 JPEG ，裁剪为正方形）。

用户可以移除它 ：关闭后可将该图标保留在设备上。
全屏 ：网站会以 Web 应用形式打开，不显示 Safari 地址栏。 在其他网站上保持全屏 还会在 Web
应用中打开指向其他网站的链接。
使用此应用打开 ：使用某个应用代替 Safari 打开该 URL。

通知设置
选择设备如何显示某些应用的通知：是否允许、显示位置（锁定屏幕、通知中心、 CarPlay
）、标记、声音、重要警告、横幅样式、分组和预览。用户无法更改这些设置。

锁定屏幕消息
显示在锁定屏幕底部的消息，例如设备被找到时该联系谁，以及资产标签。两者都可以包含变量 $EMAIL$、 $USERNAME$、$FULLNAME$、$SERIAL$ 和 $UDID$：设备没有对应值的变量会留空。

密码
密码设置 部分用于控制设备密码要求及相关安全规则（例如最小长度和复杂性）。在 Mac 上（ macOS 13 或更高版本，不适用于用户注册），这些规则适用于用户的登录密码。

选项
在 Apple
政策编辑器中，密码选项通过开关和数字字段组合进行配置。许多字段都包含工具提示，用于说明支持的操作
系统版本和监管要求。

密码开关

下次认证时更改 ：在用户下次认证时强制重置密码。
要求字母数字密码 ：要求至少包含一个字母字符和一个数字。
要求复杂密码 ：要求使用 “复杂 ”
密码（不得包含重复或连续模式，并且至少包含一个非字母数字字符）。
要求密码
：要求设置密码，但不附加长度或质量要求。注意：设置其他密码相关键会隐式要求设置密码。

数字字段

失败尝试重置时间（分钟） ：失败尝试计数器重置前的分钟数（需要 “最大失败尝试次数 ”）。
最大失败尝试次数 ：在 iPhone 或 iPad 被擦除或 Mac 被锁定之前允许的失败尝试次数（范围：
2–11）。
最大宽限期（分钟） ：设备无需输入密码即可保持解锁的时间（ 0 = 无）。
最大不活动时间（分钟） ：设备锁定前的空闲时间（范围： 0–15）。
最大密码有效期（天） ：强制更改密码前的最大密码有效期（范围： 0–730）。
最少复杂字符数 ： “复杂 ”字符的最小数量（范围： 0–4）。
最小长度 ：密码的最小长度（范围： 0–16）。
密码重用限制 ：用于防止重复使用旧密码的密码历史长度（范围： 1–50）。

限制
“限制 ”部分用于控制受管理 Apple 设备上允许使用哪些操作系统功能。在 Apple 政策编辑器中，这些选项以包含多个开关的分组面板形式呈现。

应用管理 和 网络 面板的开关在 Apple 政策的 应用与描述文件 和 网络 页面中描述。

许多限制仅在特定的操作系统版本上受支持，并且可能需要受监管设备。请使用仪表板中的工具提示获
取权威要求。

在使用用户注册的设备（通过使用工作账户登录注册的个人设备）上， Apple
不允许的限制不会被发送。如果政策的限制均不适用，这些设备不会获得限制描述文件。政策编辑器会
显示有多少限制不适用于用户注册设备。

安全性
允许自动解锁
允许使用指纹解锁
允许修改指纹
允许抹掉内容和设置
允许启用限制
允许用户安装描述文件
允许主机配对
允许提交诊断
允许修改诊断提交
允许 Apple 个性化广告
允许修改远程管理

多媒体
允许相机
允许修改文件共享
允许 “文件 ”访问 USB 驱动器
允许通话录音
允许 AirPrint

允许存储 AirPrint 凭据
允许发现 AirPrint iBeacon

蜂窝网络
允许修改 App 蜂窝数据
允许修改蜂窝套餐
允许修改 eSIM
允许向外转移 eSIM
设备擦除时保留 eSIM
允许漫游时后台获取

蜂窝 APN

蜂窝 APN用于设置运营商提供的接入点名称 (APN)，例如用于专用或企业移动网络。设置 接入点名称
，并在运营商要求时设置认证（ PAP 或 CHAP）、用户名（允许使用 $EMAIL$ 等变量）、密码、 IP
版本（漫游时也适用）、代理服务器及其端口和 XLAT464。仅当运营商为你提供用于连接网络的单独 APN 时，才开启 附加 APN。

只有 iPhone 和蜂窝版 iPad
会获得此设置，且无需受监管。使用用户注册（个人设备）注册的设备不会获得此设置。
它仅适用于用于蜂窝数据的 SIM 卡。已通过其他方式安装 APN 描述文件的设备不会安装它。
密码与其他网络密码一样受到保护：描述文件只会发送到为其创建的设备，并且密码不会写入日志。

错误的 APN 会导致设备没有蜂窝数据：请先在装有该运营商 SIM 卡的测试设备上尝试这些设置。

系统与用户界面
允许 Handoff
允许自动更正
允许自动调暗
允许自动屏幕保护程序
允许 QuickPath 键盘
允许定义查询
允许修改设备名称
允许设备睡眠
允许 iPhone 镜像
允许 Mac 上的 iPhone 小组件

允许键盘快捷键

Apple 应用与服务
允许 iMessage
允许 Game Center
允许添加 Game Center 好友
允许查找设备
允许查找朋友
允许修改查找朋友
允许图书商店
允许图书商店成人内容
允许企业图书备份
允许企业图书元数据同步
允许 iTunes Store
允许成人内容

Siri 与 Apple Intelligence
允许 Siri
允许 Siri 用户生成内容
允许在锁定时使用 Siri
允许听写
允许外部智能集成
允许外部智能登录
允许 Genmoji
允许 Image Playground
允许 Image Wand

iCloud

允许 iCloud 通讯录
允许 iCloud 备份
允许 iCloud 书签
允许 iCloud 日历
允许 iCloud 桌面和文档
允许 iCloud 文档同步
允许 iCloud Freeform

允许 iCloud 钥匙串同步
允许 iCloud 邮件
允许 iCloud 备忘录
允许 iCloud 照片图库
允许 iCloud 私人中继
允许 iCloud 提醒事项

账户（限制）
账户面板同时包含一项限制和（可选的）账户配置。限制开关控制用户是否可以修改系统账户。

允许修改账户

网络

Apple 政策编辑器的 网络 部分在设备上配置 Wi-Fi 网络和 VPN，安装证书，并限制 AirDrop 和蓝牙等连接功能。每个 Wi-Fi 网络、VPN 和证书都会作为独立的配置描述文件安装，您可以在设备的 设置 > 通用 > **VPN** 与设备管理 中看到它（Mac：系统设置 > 通用 > 设备管理，或在 macOS 13 和 14 上为 隐私与安全 > 描述文件），也可以在设备页面的 描述文件、证书和安全 面板中看到它。

> 证书取自 证书 页面：请先在那里导入它们。政策只会引用它们，因此证书绝不会被复制到政策中。

限制

- 允许 **AirDrop**
- 允许 **AirPlay** 传入请求
- 允许修改蓝牙
- 允许修改蓝牙共享
- 允许 “文件 ”访问网络驱动器
- 允许修改互联网共享
- 允许内容缓存
- 允许 **iTunes** 文件共享

Wi-Fi 网络

点击 添加 **Wi-Fi** 网络 并填写：

- 网络名称 **(SSID)**：网络的名称，最多 32 个字符。
- 安全性 ：无（开放网络）、WEP、WPA 或 WPA2、WPA2 或 WPA3、仅 WPA3，或任意。
- 密码：个人网络的密码。
- 自动加入 和 隐藏网络 （适用于不广播名称的网络）。
- 代理：无、手动（服务器和端口）或自动（PAC 文件 URL，留空则通过 WPAD 在网络中查找设置）。
- 描述文件名称 （可选）和 应用于 ，用于将网络限制为某些设备类型。

企业网络 (802.1X)

当用户使用自己的凭据或证书而非共享密码进行认证时，请开启 企业网络 **(802.1X)**。

认证 ： PEAP、TTLS（及其内部认证，例如 MSCHAPv2）或 TLS（仅证书）。
设备用户的凭据 ：每台设备使用其用户的 EAP 身份、匿名身份和密码，这些在 “用户 ”
页面中设置。没有用户的设备不会获得该网络。
身份 、匿名身份 和密码 ：对所有设备都相同。身份可以包含变量 $EMAIL$、$USERNAME$、 $FULLNAME$、$SERIAL$ 和 $UDID$。将密码留空可让用户在设备上输入。
身份证书 ：设备出示的客户端证书（ TLS 必需）。请参阅下方的证书选项。
受信任的证书 ：签发 RADIUS 服务器证书的 CA 证书。它们会随网络一起安装。
受信任的服务器名称 ：设备接受的 RADIUS 服务器证书名称，例如 radius.example.com 或 *.example.com。

VPN

点击 添加 VPN以配置 IKEv2 或 Cisco IPSec VPN，这些协议内置于 iOS、 iPadOS 和 macOS（无需 VPN 应用）。

类型 和服务器 。对于 IKEv2，还需设置 远程标识符 （服务器身份，留空表示服务器地址）和
本地标识符 ，它们可以包含变量 $EMAIL$、$USERNAME$、$FULLNAME$、$SERIAL$ 和
$UDID$。
设备的 认证 ：证书（来自 “证书 ”页面、设备用户的证书，或从 SCEP 服务器请求）、共享密钥（
IPSec 可附带组名称），或对于仅检查用户名和密码的 IKEv2 服务器则不使用认证。
受信任的证书 ：VPN 服务器的 CA 证书，会随 VPN 一起安装。对于 IKEv2
，你还可以设置预期的服务器证书签发者和名称。
用户名和密码 ：用户还需使用用户名（允许变量）和密码进行认证（ IKEv2 使用 EAP， IPSec 使用 XAuth）。将密码留空可让用户在设备上输入。
VPN 名称 （显示在 “设置 ”中）和 应用于 。

连接

用户在 “设置 ”中连接 ：VPN 已安装，用户在需要时开启它。
按需连接 ：设备会自动连接 VPN。启用 受信任的 Wi-Fi 时除外 后， VPN 不会在你列出的 Wi-Fi
网络上使用，例如办公室网络。
始终开启 （仅限 IKEv2、受监管的 iPhone 和 iPad）：所有流量在蜂窝网络和 Wi-Fi 上都会经过
VPN，用户无法将其关闭。其他设备不会获得此 VPN。如果 VPN
使用用户名，则必须在政策中设置密码。
按应用 VPN：只有部分应用使用 VPN。请在 应用管理 部分中为每个应用选择 VPN（应用的 VPN 字段，在 Mac 上不可用），并可选择列出使用它的 Safari 域。

请先在测试设备上测试 “始终开启 ”或按需 VPN：如果无法访问服务器，设备可能会没有连接。

全局代理、加密 DNS 和 Web

内容过滤器
这些设置应用于设备的所有流量。请使用各自的开关开启它们。

全局 HTTP 代理 （受监管的 iPhone 和 iPad、 Mac）：所有 HTTP
流量都会在每个网络上经过代理。设置服务器和端口（可附带用户名和密码），或设置自动配置（
PAC 文件 URL，留空则在网络上查找）。 允许 Wi-Fi 登录页面
可让用户在不使用代理的情况下登录公共 Wi-Fi 网络。
加密 DNS：设备通过 DNS over HTTPS（服务器 URL）或 DNS over TLS（服务器名称）使用你的
DNS 服务器解析名称，可选择仅对某些域生效。在受监管设备上，你可以阻止用户将其关闭。
Web 内容过滤器 （受监管的 iPhone 和 iPad）： iOS
内置的过滤器会限制成人网站，可使用始终允许或始终阻止的网站列表，或仅允许网站列表，并在
Safari 中显示为书签。

错误的代理或 DNS 服务器可能导致设备没有连接：请先在测试设备上尝试这些设置。

证书
点击 添加证书 以单独安装证书： Safari 和应用必须信任的证书颁发机构，或应用使用的身份。 Wi-Fi 网络或 VPN 的证书无需在此添加。

证书选项

“证书 ”页面中的证书 ：在所有设备上使用相同的证书。点击 选择证书 来选择它。
设备用户的证书
：每台设备会获得与其用户关联的客户端证书。用户没有证书的设备不会获得它。当你将另一份证书
关联到用户时，设备会更新。
从 SCEP 服务器请求 ：每台设备从你的 SCEP 服务器（例如 Microsoft NDES
）请求自己的证书，因此私钥永远不会离开设备。设置服务器 URL
、服务器要求时的质询、主题（例如 CN=$EMAIL$）、备用名称、密钥大小和密钥用途。

使用旧版 RC2 加密保护的客户端证书（ .p12）无法安装在 Apple 设备上。请在导入前使用 3DES 或
AES 加密重新导出它们。

软件更新
Apple 政策编辑器中的 软件更新 部分可让设备保持最新：它可以要求设备在截止日期前使用特定 OS 版本，并控制设备下载和安装更新的方式。

必需的 OS 更新
点击 添加必需更新 以要求某个 OS
版本。设备会下载更新，告知用户截止日期，并在用户之前未安装的情况下于截止日期安装。已运行该版本或
更高版本的设备会忽略它。需要 iOS 和 iPadOS 17 或 macOS 14。

适用于 （必填）： iPhone 和 iPad，或 Mac。每个 OS 都有自己的版本号，因此请分别为每个 OS
添加一条必需更新。
OS 版本 ：要安装的版本，例如 18.5 或 15.4.1。
构建版本 （可选）：特定构建版本，例如测试版或后台安全改进。
安装期限 ：截止日期，采用每台设备的本地时间。过去的日期会使设备尽快安装更新。
详细信息 URL（可选）：向用户显示的关于该更新的网页。

设备会在设备页面的 设备状态 面板中报告更新进度（下载、安装、失败）。

软件更新设置
打开 iPhone 和 iPad 的软件更新设置 或Mac 的软件更新设置
，以控制这些设备上的更新。开关关闭时，设备会保留自己的设置。需要 iOS 和 iPadOS 18 或 macOS 15 ：较旧的设备会忽略这些设置。

延迟更新 ：仅在经过指定天数（ 1 到 90 天）后向用户显示新更新。在 Mac
上，您可以为重大更新、次要更新和其他系统更新设置不同的时间段。
向用户显示的更新 （ iPhone 和 iPad
）：当有多个更新可用时，显示全部更新、仅显示最旧的次要更新或仅显示最新的更新。
标准用户可以安装更新 （ Mac）：没有管理员权限的用户可以安装 macOS 更新。
通知用户有关必需更新的信息 ：显示有关必需更新及其截止日期的通知。
自动下载 、自动安装 和自动安全更新 ：让用户决定（ Apple
的默认设置），或将它们始终开启或始终关闭。
后台安全改进 ：向用户提供 Apple 的快速安全修复，并选择用户是否可以移除它们。

测试版计划 ：允许用户加入 Apple 测试版计划，或将设备从计划中移除并加以阻止（在 iPhone 和
iPad 上，仅限受监督的设备）。

从设备页面安装更新
设备的 设备状态 面板会列出可用于该设备的更新。使用 检查更新 让设备提供列表，使用 安装
立即安装某个更新，或下载该更新并让用户安装。这适用于受监督的 iPhone 和 iPad 以及 Mac。Apple 会在 iOS、 iPadOS 和 macOS 27 中移除这些命令：在这些版本上，请使用政策中的必需更新。

macOS

Apple 政策编辑器的 macOS部分可管理 Mac 的安全性、隐私和登录设置： FileVault、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、登录项，以及允许载入的系统和内核扩展。
它还会安装系统服务和后台任务的配置文件。政策中的其他设备不会获得这些设置。开启某项设置即可管理它
；关闭时，用户保留自己的选择。

大多数设置会作为配置描述文件安装到 Mac 上，可在 “系统设置 ”>“通用 ”>“设备管理 ”中查看。
FileVault、隐私权限、登录项和扩展设置需要用户批准的 MDM：对于通过注册 URL 或二维码注册的
Mac，用户需在 “系统设置 ”中批准注册描述文件。设备页面会在 用户批准的 MDM
字段中显示该状态。当用户稍后批准后， Mac 会自动获得这些设置。

FileVault

FileVault 会加密 Mac 的磁盘。开启此设置后，用户会被要求使用其密码开启 FileVault， Mac
会将其个人恢复密钥发送到 Cerberus Enterprise
，并使用仅属于贵组织的密钥加密。该密钥会显示在设备页面的 FileVault
字段中，也可在该字段中更改（请参阅设备命令）。此设置需要 macOS 13 或更高版本以及用户批准的 MDM
；没有用户批准的 MDM 时， Mac 不会被要求开启 FileVault，但如果用户自行开启，其密钥会被存储。

登录时要求
：在下次登录时、跳过若干次之后（用户每次登录和注销时都会被再次询问），或仅在用户注销时。
注销时不询问 ：仅在登录时询问用户。不能与 “仅在注销时询问 ”同时使用。
向用户显示恢复密钥 ：默认关闭，因此只有管理员可以从设备页面获知密钥。
阻止关闭 FileVault：默认开启。
待机时从内存中移除密钥 ： Mac 从待机状态唤醒时，用户需要再次输入密码。
密钥的存放位置 ：在登录窗口中向用户显示的文本，例如恢复 Mac 时应联系谁（默认为 “Cerberus
Enterprise”）。

获得此设置时已经加密的 Mac 会保留其当前密钥， Cerberus Enterprise
不会收到该密钥：只有在用户关闭并重新开启 FileVault 后（且 “阻止关闭 FileVault”
已关闭），密钥才会被存储。关闭此设置或将 Mac 从管理中移除不会关闭 FileVault
，已存储的密钥仍然有效。当服务器未配置为存储恢复密钥时，无法保存此设置。

防火墙

开启防火墙 ：关闭时，防火墙会保持关闭，用户无法将其开启。
阻止所有传入连接 ：只有基本的网络服务（ DHCP、 Bonjour、IPSec）可以接收连接。
隐身模式 ： Mac 不会响应 ping 请求以及发往已关闭端口的连接。
允许内置软件 和允许已下载的签名应用 在不询问用户的情况下接收连接（ macOS 12.3
或更高版本）。
特定应用的规则 ：按 bundle ID 允许或阻止某个应用的传入连接。

Gatekeeper
Gatekeeper 会在应用打开前对其进行检查。选择 Mac 仅打开 App Store
应用，还是也打开已识别开发者的应用。关闭 Gatekeeper
后，任何应用都可以打开，包括未签名或已损坏的应用。在 macOS 15
或更高版本上，你还可以选择是否询问用户将阻止的恶意软件发送给 Apple。

屏幕保护程序与锁定
在一段无操作时间后启动屏幕保护程序，并在屏幕保护程序启动或显示器睡眠时要求输入密码，可立即要求或
延迟要求。保留为 不受管理 的设置将维持用户的选择。

外部和网络存储
允许、设为只读或阻止 Mac 的外部存储（ USB 驱动器、 SD 卡、外置磁盘）和网络存储（文件共享）。需要
macOS 15 或更高版本。

屏幕共享
限制使用屏幕共享连接到这些 Mac 的人员：从 Mac 复制文件或向 Mac
复制文件、高性能连接以及虚拟显示器的数量。开启屏幕共享仍由用户自行选择。需要 macOS 14 或更高版本。

隐私权限
授予或拒绝应用在 “系统设置 ”>“隐私与安全性 ”
中本应由用户允许的访问权限，例如为备份应用授予完全磁盘访问权限，或拒绝某个应用访问相机。对于每项
权限，请选择：

权限
：完全磁盘访问权限、辅助功能、自动化、文件夹、联系人、日历、照片、相机、麦克风、屏幕录制
以及 “隐私与安全性 ”中的其他权限。
访问权限
：允许或拒绝。相机、麦克风、屏幕录制和输入监控无法通过描述文件允许，只能拒绝；对于屏幕录
制和输入监控，你还可以让用户在没有管理员权限的情况下允许它们。
应用 ：应用的 bundle ID，或程序的路径（例如命令行工具）。
代码要求 ：通过签名标识应用。可在 “终端 ”中使用 codesign -dr - /Applications/Example.app
获取，并复制 designated => 之后的文本。
自动化 还需要受控制的应用（例如访达）及其代码要求。

登录项和后台项
与规则匹配的登录项和后台项会受到管理：它们无需询问即可运行，并且用户无法在 “系统设置 ”>“通用 ”>“
登录项 ”中将其关闭。规则可匹配应用的开发者团队 ID、其 bundle ID
，或启动守护进程或代理的标签（也可匹配其第一部分）。需要 macOS 13 或更高版本。

系统扩展
系统扩展是应用扩展 macOS 功能的现代方式：网络过滤器与 VPN
、终端安全代理和驱动程序。开启此设置后，所列开发者团队的系统扩展无需询问用户即可载入。需要 macOS 10.15 或更高版本以及用户批准的 MDM。

团队 ID：开发者的 10 个字符的团队 ID（例如可在应用的 “签名者 ”详细信息中查看，或使用
codesign -dv 获取）。每个团队只能出现一次。
允许 ：该团队的所有扩展，或仅具有所列 bundle ID 的扩展。
类型 ：将团队限制为驱动程序、网络或终端安全扩展。未选择任何类型时，允许所有类型。
移除 （仅适用于所列扩展）：应用可以在没有管理员的情况下移除其扩展（ macOS 12
及更高版本），在系统完整性保护开启时无法关闭或移除该扩展，或者无法在 “系统设置 ”和 “访达 ” 中移除它（ macOS 15 及更高版本）。运行较旧 macOS 的 Mac 仍允许该扩展，但没有移除选项。
用户可以批准其他系统扩展 ：默认开启。关闭后，只有描述文件允许的扩展可以载入；如果 Mac 上的任何描述文件将其关闭，则它处于关闭状态。

在 macOS 11.3
及更高版本上，移除此设置会关闭它曾允许的系统扩展，例如安全代理或网络过滤器。当关闭此设置、
删除政策以及 Mac
迁移到不包含此设置的政策时，就会发生这种情况。编辑器在关闭此设置前会请求确认。

内核扩展（旧版）
内核扩展是扩展 macOS
的较旧且已弃用的方式：当供应商提供系统扩展时，请优先使用系统扩展。所列团队的内核扩展（团队的所有
扩展，或仅所列 bundle ID 的扩展）会在重新启动后无需询问用户即可载入。需要 macOS 10.13.2
或更高版本以及用户批准的 MDM。

用户可以批准其他内核扩展 ：默认关闭，因此只有所列团队可以载入内核扩展。
标准用户也可以批准它们 ：在用户批准开启时，没有管理员权限的用户也可以批准它们（ macOS
11 及更高版本）。

在搭载 Apple silicon 的 Mac 上，仅靠描述文件还不够：必须有人以恢复模式启动 Mac，在 “
启动安全性实用工具 ”中选择 “降低安全性 ”，并允许用户管理来自已识别开发者的内核扩展。 Mac
还可能需要一个托管在 Cerberus Enterprise 中的 Bootstrap Token 来批准它们（请参阅设备页面的
Bootstrap Token 字段）。

Mac 文件
服务配置文件和后台任务使用的文件需要上传到贵组织的 Mac 文件 中： zip 归档和属性列表（ .plist），最大
20 MB。可使用 macOS 部分的 Mac 文件 按钮，或在某项设置中使用 选择文件
来上传文件、检查其使用位置或删除它们。政策正在使用的文件无法删除。要更改文件，请上传新版本并在政
策中选择它： Mac 会重新下载它。

服务配置文件
从 zip 归档安装系统服务的配置文件。内置服务包括 SSH 服务器 (sshd)、sudo、PAM、打印 (CUPS)、 Apache Web 服务器、 bash、zsh、智能卡登录和授权。你也可以使用自己的服务，并使用类似
com.example.service 的反向 DNS 标识符：它会通过 macOS
的受管理配置文件库查找文件。每个服务只能有一项设置。需要 macOS 14 或更高版本。

内置服务仅使用归档中的文件，并忽略其自身文件（例如 sshd 的 /etc/ssh
）：请将完整配置放入归档中，并使用从磁盘根目录开始的文件夹（例如 etc/ssh/sshd_config
）。这些文件在 Mac 上是只读的，并会随此设置一起移除。请先在一台 Mac 上测试归档：错误的
sudo 或 PAM 配置可能导致用户无法登录或无法使用管理员权限。

后台任务
由 launchd 启动的后台运行程序和脚本。用户无法关闭它们，它们会随此设置一起移除。需要 macOS 15 或更高版本。对于每个任务，请选择：

任务标识符 ：一个反向 DNS 标识符，例如 com.example.task，每个任务必须不同。
程序和脚本 （可选）：一个 zip 归档， Mac 会将其解压到 /var/db/ManagedConfigurationFiles/BackgroundTaskServices/Services/
后接任务标识符。请保留文件的可执行权限，并且不要在其中放入属性列表。
launchd 属性列表 ：启动这些程序的作业，作为守护进程（针对整个系统，以 root
身份）或代理（在每个用户会话中）载入。请使用上述文件夹中的路径引用这些程序。

任务需要程序或至少一个属性列表。当文件发生变化时， Mac 会重新启动该任务。

位置和地理围栏
Apple 政策编辑器的 位置和地理围栏 部分定义了区域，例如站点或仓库。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，事件规则可以对此做出反应：发送电子邮件、锁定或停用设备，或再次启用
设备。 Mac 不使用地理围栏。

地理围栏字段
使用 添加地理围栏 创建新条目。一个政策最多可包含 10 个地理围栏
，并且它们的名称在政策内必须唯一。每个地理围栏包含以下字段：

名称 ：必填且唯一。
纬度 和经度 ：区域的中心。你也可以点击地图来设置。
半径（米） ：必填，范围为 200到 10000米。
描述 ：供管理员使用的可选备注。
报告进入 和报告离开 ：选择要生成哪些事件。至少需保持开启一个。
活动 ：启用或停用地理围栏而不删除它。

每个地理围栏都有一个地图预览。已保存的地理围栏的中心和半径处于锁定状态：使用地图上的锁定按钮进行
更改。其他按钮会将地图居中到该区域或你的当前位置。

保存政策时， Cerberus Enterprise 会要求政策中的 iPhone 和 iPad
获取新的地理围栏。这通常需要几分钟，但 iOS
可能会延迟，例如在低电量模式下或没有网络连接时。设备页面会显示应用何时尚未应用最新的地理围栏。

要求
地理围栏在安装了 Cerberus Enterprise 应用的 iPhone 和 iPad 上有效。 Mac 会忽略它们。在设备上：

已安装 Cerberus Enterprise 应用（ Cerberus 会安装它），并且用户至少打开过它一次；
该应用的位置访问权限设置为 始终 ；
精确位置 已为该应用开启；
后台 App 刷新 已开启。

位于该部分顶部的 个人设备上的位置和地理围栏 默认关闭。关闭期间， Cerberus
不会收集个人设备（用户注册）的位置，不会生成它们的地理围栏事件，其设备页面也不会提供定位或

实时追踪。开启后，政策中的个人设备会像公司设备一样共享其位置和地理围栏事件，但前提是用户允
许 Cerberus Enterprise 应用访问位置； iOS
询问之前，该应用会向用户说明这一点。贵组织有责任告知用户并遵守有关员工位置的当地规定。丢失
模式和 MDM 位置请求在个人设备上始终不可用（ Apple 不允许）。

在低电量模式 下，地理围栏仍会继续工作，但 iOS
会延迟报告离开某个区域，并且位置不够精确；政策更改后，它还可能将获取新地理围栏的时间延迟数小时，
直到应用再次运行（例如在下一次跨越边界时，或用户打开应用时）。

事件如何到达
iOS
会代表应用监视这些区域，并在设备跨越边界时唤醒应用，即使应用未打开也是如此。事件可能会在跨越边界
几分钟后到达，而较小的区域或短暂的停留可能会被遗漏： iOS
需要设备越过边界移动一段距离，并在那里停留一段时间。

如果应用无法运行，例如在设备解锁前重新启动之后，服务器稍后也会根据应用发送的位置检测跨越。无论由
应用还是服务器检测到，每次跨越只会触发一次事件规则。

当应用数小时未联系服务器时，服务器会请求 iOS 唤醒它，以便它能再次检查其地理围栏。 iOS
不保证这些请求。

设备页面
在设备页面上， 地理围栏 标签页（位于 位置地图
面板中）会显示设备的进出记录。当政策包含活动地理围栏时，状态行会说明地理围栏功能在该设备上是否有
效，或为何无法使用：应用尚未联系服务器或需要更新，位置访问权限未设为 始终 ，精确位置 或后台 App 刷新 已关闭，应用上次报告其设置时 低电量模式 处于开启状态，或者应用尚未应用最新的地理围栏。

地理围栏转换记录和位置保留 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。

限制
复制政策不会复制其地理围栏：请在副本中重新添加。
iPhone 和 iPad 上的地理围栏事件属于尽力而为：由 iOS 决定应用何时可以运行。

账户
Apple 政策编辑器的 账户 部分可为 iPhone、iPad 和 Mac 添加邮件、 Exchange、Google
、日历、通讯录和目录账户。点击 添加账户 并选择类型。该部分还包含 允许修改账户 限制（受监管设备）。

在 Mac（ macOS 13 或更高版本）上，账户会在已注册管理的用户（通常是注册该 Mac
的用户）登录时安装到其会话中。设备页面会在 Mac 用户
下列出这些用户及其账户状态。使用设备用户电子邮件地址的账户会采用 Cerberus Enterprise
中分配给该 Mac 的用户。

常用设置
设备用户的名称和电子邮件 （邮件、 Exchange、Google
）：每台设备使用其用户的名称和电子邮件地址，这些信息在用户页面中设置（对于 Google
，为用户自己的 Google
账户）。没有用户或用户没有电子邮件地址的设备不会获得该账户。否则，请设置固定的电子邮件地
址和全名。
账户名称 （可选）：账户在 “设置 ”和应用中的名称。
用户名 和密码 （可选）：用户名可以包含变量 $EMAIL$、$USERNAME$、$FULLNAME$、 $SERIAL$ 和 $UDID$。将密码留空可让用户在设备上输入，或将两者都留空以让用户输入。
适用于 ：将账户限制为某些设备类型。

账户类型
邮件账户 ： IMAP 或 POP
接收服务器和发送服务器，及其端口和身份验证。发送服务器可以使用与接收服务器相同的用户名和
密码。
Exchange 账户 （Exchange ActiveSync
）：服务器，留空则从电子邮件地址中查找。选择服务（邮件、通讯录、日历、提醒事项、备忘录）
以及用户是否可以更改它们。使用 新式身份验证 (OAuth)时，用户通过您的身份提供商（例如 Microsoft 365）的页面登录。 身份验证证书 （ iOS 17
或更高版本）使用证书对设备进行身份验证。
Google 账户 ：用户使用指定的电子邮件地址登录 Google 账户。
日历账户 (CalDAV)和通讯录账户 (CardDAV)：服务器、端口和路径。
目录 (LDAP)：服务器和端口，以及用于查找联系人的搜索（搜索基点、范围和描述）。
订阅日历 ：日历的 URL（ https、http 或 webcal）。

S/MIME

邮件和 Exchange 账户可以使用 S/MIME 对邮件进行签名和加密（ iOS 17
或更高版本）。对于每个账户，请选择证书：证书页面中的某个证书、设备用户的证书，或从 SCEP
服务器请求的证书。您可以允许用户将其关闭、选择其他证书，并且对于加密，为每封邮件显示一个开关。

安全
密码和证书不属于发送到设备的设置：每台设备都会使用其管理证书签署请求，从 Cerberus Enterprise 下载自己的凭据。它们不会写入日志。

合规性规则
Apple 政策编辑器的 合规性规则
部分会为政策中的设备设定要求。违反规则的设备会立即变为不合规：设备页面会在 设备不合规的原因
中说明原因，设备列表也会将其显示为不合规。当政策中的某项设置无法应用到设备上时，该设备也会被视为
不合规。

规则
密码 ：设备设有密码，并且符合政策的密码设置。
最低操作系统版本 ：适用于 iPhone 和 iPad，或适用于 Mac。要更新设备，请在 “软件更新 ”
中添加必需的更新。
受监管设备 ：使用注册描述文件或通过用户注册方式注册的设备不受监管。
FileVault 已开启（ Mac） ： Mac 的磁盘已使用 FileVault 加密。其他设备不受影响。

当设备发送状态时、保存政策时以及每小时都会检查规则。状态未知的设备（例如尚未报告 FileVault 的 Mac ）不会违反规则。

阻止设备
开启 如果设备仍不合规则阻止设备 ，并设置多少天后（ 0 表示立即阻止）。受监管的 iPhone 和 iPad
会进入丢失模式，并显示你设置的消息。其他设备会被锁定一次； Mac 会重新启动并要求输入 PIN，该 PIN 会显示在命令历史记录中该命令的详细信息里。

解除阻止 ：当设备再次合规时，丢失模式会自动关闭。
自行关闭丢失模式
：在设备再次合规并再次违反规则之前，它不会被再次阻止。可使用此操作让用户修复设备。

要收到通知或以其他方式做出响应，请为 设备变为不合规 创建事件规则：该事件还会包含原因。