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。

Revision #6
Created 2026-11-10 15:18:42 UTC by Admin
Updated 2026-11-12 09:58:22 UTC by Admin