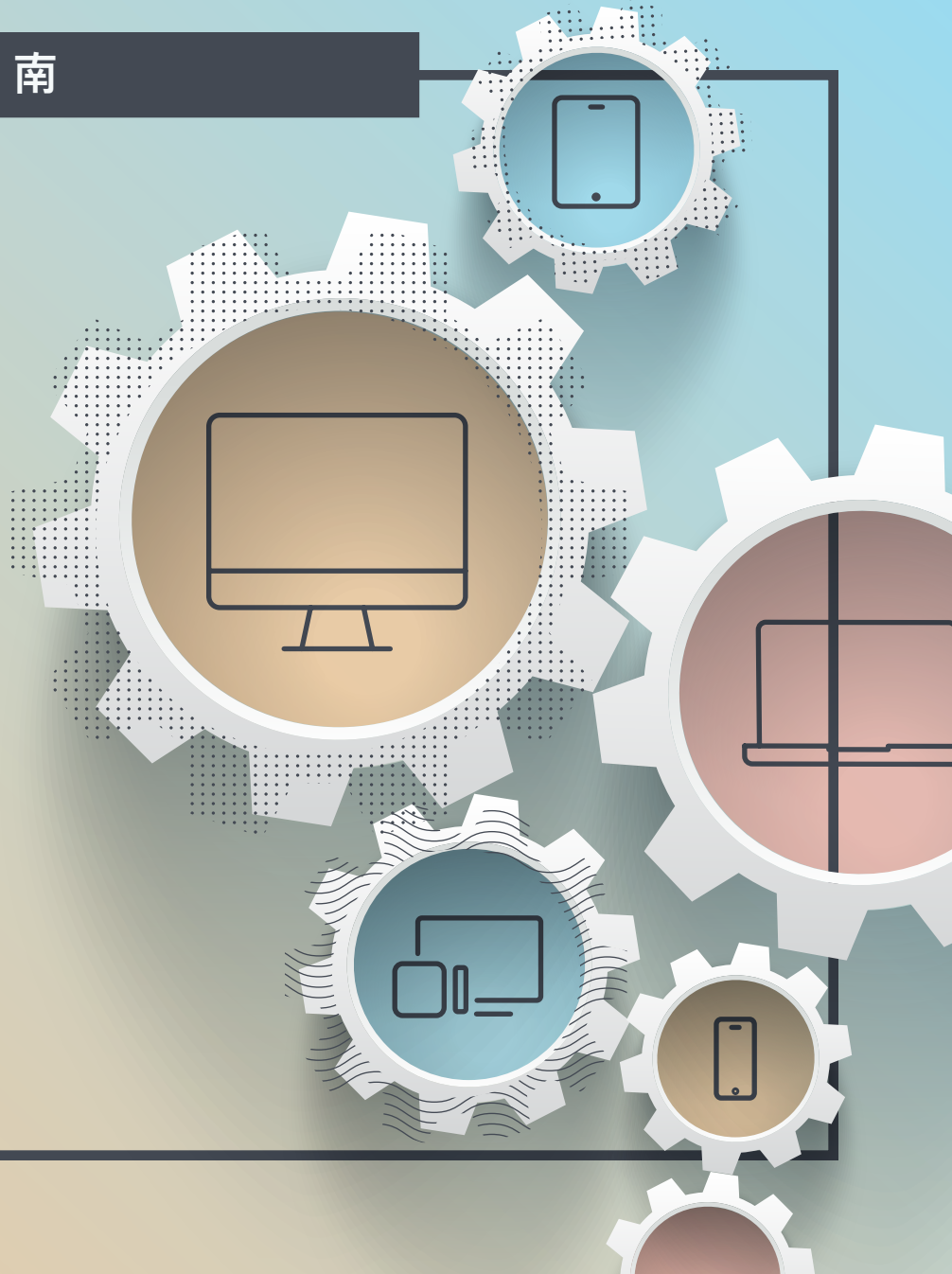
综合指南

适合初学者的 Apple

设备管理



根据福布斯近期发布的报告，Apple 设备在企业中的使用率增长了 20%，且截至 2020 年，该数字将有望翻一番 。

随着全球商业和教育环境中 Apple 设备数量的不断增加，实现技术性投资的最大化成为当务之急，因为这将有利于各组织机构发挥 Mac、iPad、iPhone 和 Apple TV 的全部潜力。新设备的涌入可能会给负责设备管理的 IT 人员（尤其是在已搭建好的 Windows 环境中管理设备的人员）带来沉重的负担。

虽然其中的部分人员已十分熟悉 Apple，但仍有很多人是第一次涉足 Apple 设备管理。本指南面向后一类人员，提供了以下内容，可帮助读者了解和掌握 Apple 的管理技巧：

Apple 设备管理简介

在考虑如何管理 Apple 设备时，您可将整个生命周期分解成若干个您要完成的常见任务。无论是管理 Apple、PC、Android 设备还是上述所有设备，这些任务都将是相同的。

MDM 的工作原理

由于内置了移动设备管理 (MDM) 框架，大多数 Apple 设备都能够理解和应用远程擦除或密码限制等设置。配置参数文件和管理命令是 MDM 框架的两个核心组件。

上述组件通过 Apple 的推送通知服务器 (APNS) 与设备进行通信，该服务器将从 Apple 公司获取安全证书，从而保证其仅供您的组织机构使用。随后 Apple 的服务器将与设备持续连接，为您省去繁琐的连接操作。设备将向管理服务器发出反馈信息，并接收您所定义的命令、设置、配置或应用程序。

配置参数文件

...可为您的 Apple 设备定义各种设置，并告知设备如何运作。

您可将其用于自动配置密码设置、Wi-Fi 密码和 VPN 配置。配置参数文件也可用于限制 App Store、Web 浏览器或设备重命名等设备功能。这些配置文件均可利用 Jamf Pro 等 MDM 解决方案进行指定和部署。

管理命令

....是可发送到托管设备以进行特定操作的单一命令。如果您的设备不慎丢失，可将其设置为丢失模式或向其发送远程擦除命令。如果您需要升级操作系统，可通过发送命令来下载并安装更新。这些只是您能够在完全托管的 Apple 设备上执行的大量操作中的几个示例而已。

MDM 和客户端管理

虽然 Apple 的 MDM 框架可实现对 iOS 和 tvOS 设备的必要控制，但 macOS 是一个功能更为强大的平台，可能需要更高级的功能。借助客户端管理（仅适用于 macOS），您可在对设备进行管理注册后立即安装 Mac 代理或二进制文件。

该代理允许您添加隐藏的管理员帐户，允许远程访问 macOS 的根目录，并允许在计算机上运行更多的策略和脚本。由于基于代理的 Mac 管理超出了内置 MDM 的范畴，因此您需要通过第三方解决方案（如 Jamf Pro）充分利用 Mac 管理的高级功能。

以下为客户端管理功能示例：

安装 PKG/DMG

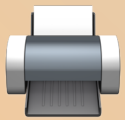
强制执行 FileVault

绑定到目录

运行脚本

自定义 Dock 栏

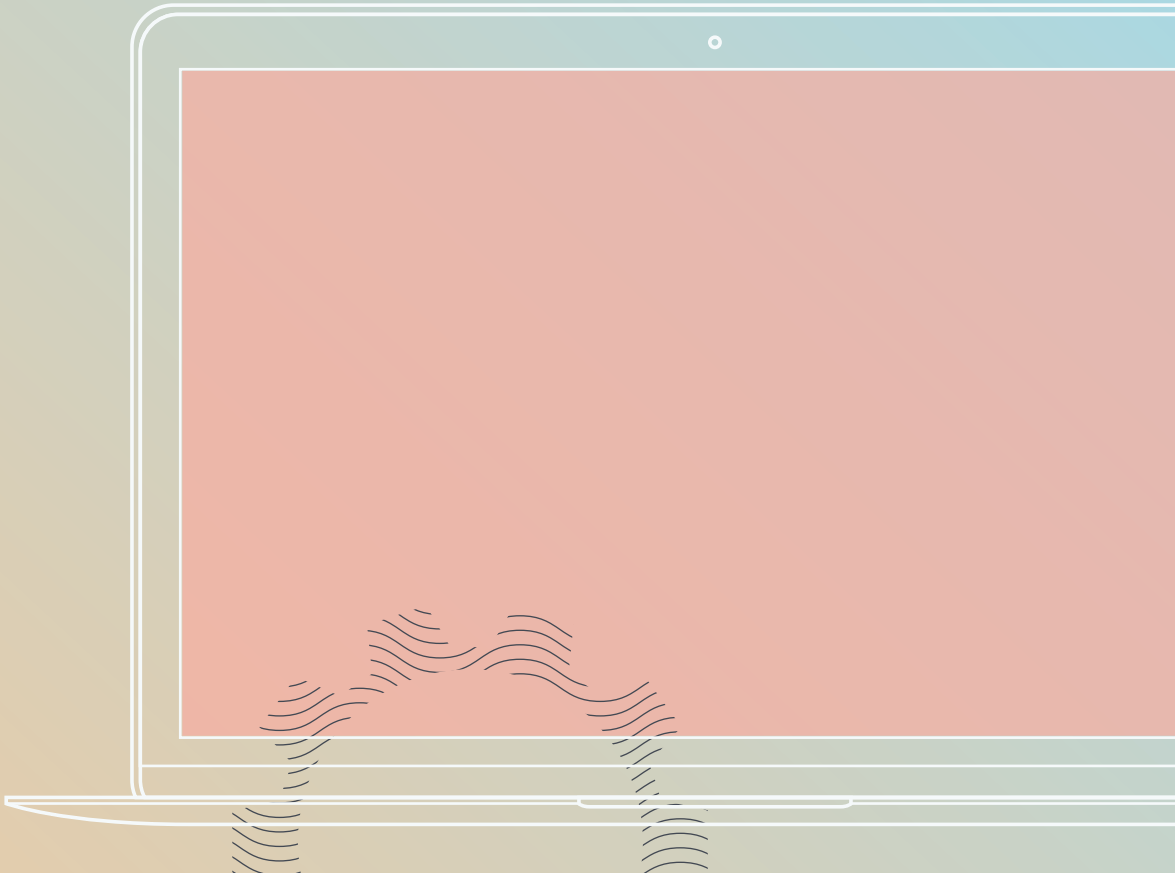
设置 EFI 密码



安装打印机

创建帐户

设置软件更新



Apple 服务和程序

随着 Apple 设备在企业和教育领域越来越受欢迎，如何实现最佳的大规模设备部署、处理 Apple ID 和购买应用程序已成为一项挑战。当然，Apple 正致力于解决这些问题并推出多种程序和服务，从而进一步推动设备管理，使批量管理设备变得更容易、更具成本效益。

并非所有 Apple 设备管理解决方案都支持 Apple 的程序和服务。请联系您的供应商，确保他们支持这些程序以及 Apple 常年进行的渐进式变更。

设备监管

监管是 iOS 和 tvOS 设备通过 DEP 或 Apple Configurator 注册后进入的一种特殊模式。监管有助于各机构更好地控制各自的 iOS 设备。包括托管丢失模式、阻止应用程序和静默安装应用程序在内的大量管理功能都需要监管。我们建议公司和学校将所有的设备均置于监管模式之下。

Apple ID

Apple ID 是用户用来访问 Apple 服务（如 App Store、iTunes Store、iCloud、iMessage 等等）的个人帐户凭证。您可允许最终用户在工作中使用他们的 Apple ID，或完全避免使用 Apple ID，这取决于组织机构的具体要求。如果您所在的组织为教育机构，则您的学生将接收到不同类型的 Apple ID（见下页）。

Apple School Manager

2017 年推出的 Apple School Manager 是一个基于 Web 的门户，可供 IT 管理员从固定位置集中监控人员、设备和内容。Apple School Manager 专为教育机构量身打造，可将多种课堂管理工具（如 Classroom 应用程序）合并到一个门户当中。Apple School Manager 支持托管 Apple ID 和共享 iPad，并可与学校的学生信息系统 (SIS) 集成使用。

Classroom 应用程序

Apple 的 Classroom 应用程序是一款 iPad 专用教学工具，可帮助教师简化课堂教学流程、鼓励学生间的互动和协作、将学生的iPad 设备固定用于某些应用程序或网页，以及查看学生设备以了解其理解情况。

托管 Apple ID

对于教育机构而言，托管 Apple ID 是适于学生的一类特殊 Apple ID。使用托管 Apple ID 无需专门许可，且 IT 管理员（也就是您）可借助托管 Apple ID 来创建和动态更新用户信息。托管 Apple ID 需在 Apple School Manager 门户中创建，可与 Classroom 数据以及学校的 SIS 同步。

共享 iPad

共享 iPad 可为学生提供个性化学习体验，从而扩展了 iPad 设备的价值。
如果每名学生都拥有专属的唯一 ID，则他们可以进行登录和注销操作，同时确保各自的应用程序、相关内容和工作进度均完好无损。共享 iPad 仅适用于教育机构，且需要搭配 Apple School Manager 使用。

生命周期管理阶段

Apple 的设备管理框架（通常被称为 MDM 框架）涵盖了 Apple 设备整个生命周期中的六大关键要素。

MDM 是 Apple 公司推出的内置式管理框架，适用于 macOS、iOS 和 tvOS，并具有以下功能：

1 部署和配置

将设备交付给最终用户控制

2 配置管理

为设备应用正确设置

3 应用程序管理

可确保每台设备上都有正确的软件和应用程序

4 库存

报告每台设备的状态

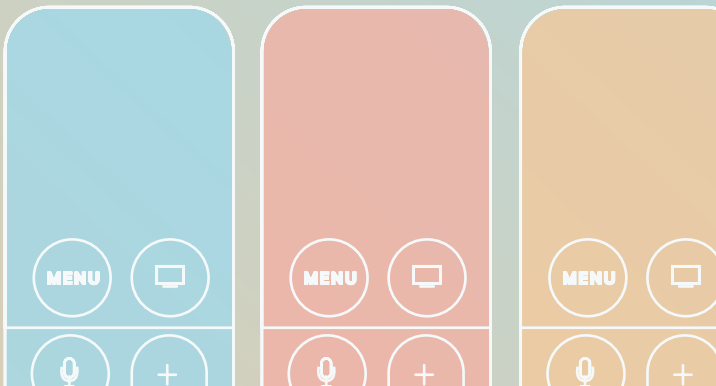
5 安全

确保设备符合组织机构的标准

6 用户授权

允许用户自行获取资源和服务

从初始部署到最终用户体验的整个过程当中，了解、管理您环境中的设备，并在整个生命周期为其提供支持是至关重要的。这可以确保 Apple 设备的安全性，并最大限度地发挥设备的潜力 。



1 部署和配置

在为最终用户配置设备之前，必须将设备注册到 MDM 解决方案的管理体系当中。尽管有多种注册方法可供使用，但推荐企业和教育机构使用以下两种方法，以获得积极、高效的最终用户体验：

	描述	用户体验	监管（仅适用于 iOS）	最适合
通过 Apple School Manager 进行自动部署（仅限教育领域）	OTA 自动注册	产品采用收缩薄膜包装，且设备会在开机时自动进行配置	支持无线连接	iPad 程序可供幼儿园及中小学的孩子使用。可为学生提供开箱即用的体验
Apple Configurator（仅适用于 iOS 和 tvOS）	注册需通过经由 USB 线连接到设备的 Mac 应用程序完成（不适用于 Apple TV 4k）	IT 人员将对安装过程进行管理，随后将设备移交给用户	支持有线连接	支持实验室共享和移动设备型号
通过 URL 启动的用户	OTA 手动注册	用户通过访问特定 URL 来配置设备	无	当前位于现场的非托管设备或需要重新注册到新 MDM 服务器的设备

2 配置管理

在谈到配置 Apple 设备时，简直整个世界都任您掌控！您可以根据最终用户的需求，对单台设备或设备组进行个性化定制。

如果您不知道从何处下手，可以先在此处查看 MDM 配置参数文件列表，或加入 Jamf Nation 对话 。

配置参数文件

可通过创建配置参数文件来定义 iOS、macOS 和 tvOS 中的设置。可将这些小型 XML 文件分发到使用托管解决方案的设备。可应用 Wi–Fi、VPN、电子邮件设置及其他设置，使用户可以无缝连接到所需的资源。

策略

macOS 客户端管理可应用独特的策略，这些策略已超出了 MDM 配置参数文件基本设备管理功能的范畴，可协助您安装自定义软件和打印机、管理本地用户帐户以及执行高级管理工作流。

智能定位

可收集所有托管设备的详细库存信息（包括您自行定义的库存属性），以确定哪些设备需要执行软件更新、安全强化或其他管理措施。如果您的设备管理解决方案允许，则您可以根据库存条件构建组，然后由系统自动将设备管理任务触发到特定的个人或组，或通过企业应用程序目录向用户提供所需的项目。

脚本

在您的客户端管理解决方案中，部分策略会利用 Apple 设备管理功能在 macOS 上运行 shell 脚本。任何可以通过命令行在终端中执行的内容均可用作脚本。脚本运行功能使得系统的灵活性大大超过标准配置参数文件，并为丰富设备管理功能提供了无限的可能。

3 应用程序管理

应用程序基本原理

如今，我们对 iPhone、iPad 和 Apple TV 设备上的 App Store 已经堪称了如指掌。App Store 是消费者通过各自设备获取应用程序的唯一途径。Apple 将对开发人员的代码进行审核，以确保应用程序的安全性和性能。这也是 Apple 在安全性方面备受赞誉的重要原因之一。但是在使用 Mac 时，您也可以从 App Store 之外的渠道获得软件。

未收入 Mac App Store 的热门软件包括 Microsoft Office 和 Adobe Creative Suite，因此拥有可部署自定义软件的 Mac 客户端管理工具是非常重要的。一些管理工具（如 Jamf Pro）可通过创建安装前后快照来构建自定义的 .pkg 或 .dmg（Mac 软件安装文件类型）文件。可将该软件包部署到托管 Mac 上，这一过程中无需用户具有管理员身份。

Apple 设备之所以广受消费者欢迎，是因为这些设备采用了开箱即用的原生通信、学习和产能工具，而 App Store 中丰富的应用程序库则是 Apple 生态系统的另一大特色。您可以通过设备管理解决方案管理您的应用程序部署，从而确保用户得到所需的应用程序 – 该方案可根据实际使用情况进行配置并确保环境中的安全性。

无论您的组织机构是选择利用 Apple 内置的应用程序、从 App Store 数百万个应用程序中选择一个（或多个）使用，还是自行创建内部自定义应用程序，您都需要确保用户获得所需的全部应用程序，并在您的环境中为其提供适当保护。

以下是三个应用程序管理选项，可供您用于您的设备。

- 部署应用程序
- 使用 Apple School Manager 部署教育类应用程序
- 部署 Apple TV 的应用程序

软件的安装与修补

生成软件安装快照

创建自定义的 .pkg 或 .dmg 文件

通过 Jamf Agent 推送安装

对于 App Store 中的软件，我们可以使用 Apple 程序为其授权并将应用程序分发到设备，全程无需使用 Apple ID。

最佳实践

部署 Apple TV 的应用程序

Apple TV 可为企业应用程序（通常称为内部应用程序）提供支持。正如您的 iOS 设备一样，系统可自动将这些应用程序上传到您的管理服务器，并将其推送到您的 Apple TV 设备，全程无需提供 AppleID。热门的 Apple TV 企业应用程序包括数字标牌、紧急警报等。

配置参数文件

凭借 MDM 解决方案，IT 人员可以使用 tvOS 配置参数文件定义设置，并将其分发到 Apple TV 设备。因此，Wi-Fi、限制和 AirPlay 设置更适于 OTA 应用。此外，可将 Apple TV 设备置于“单一应用模式”(Single App Mode)，即可按照类别自定义 Apple TV 观赏体验；或将其置于“会议显示模式”(Conference Display Mode)，即可获得直观的演示工作流。

智能定位

凭借自动收集详细库存信息（包括来自所有托管设备的 Apple TV 设备名称）的功能，IT 人员能够快速、准确地判断需要对哪些设备采取措施。根据此库存信息，IT 人员可以构建目标群，用以触发自动设备管理任务。例如，现在 IT 人员可在未配置 AirPlay 设置的情况下找到全部的 Apple TV 设备，然后部署该项配置。

自定义应用程序和显示支持

如果企业通过独特的应用程序功能来实现自定义全屏观赏体验，则 IT 人员可以利用 MDM 通过 OTA 完成上述应用程序的自定义部署。此外，现在 IT 人员可以通过最新的 tvOS 设置主屏幕布局，以显示/隐藏应用程序，并根据年龄分级来限制媒体内容。

想要了解 Apple TV 部署的详细情况吗?

欢迎您参阅我们的“Apple TV 管理”白皮书

4 库存

MDM 解决方案支持通过查询 Apple 设备收集大量库存数据，确保您始终拥有最新的设备信息并能够做出明智的管理决策。库存信息包括序列号、操作系统版本、所安装的应用程序等等，可按照多个时间间隔从设备进行收集。

以下是使用 MDM 收集数据的示例：

硬件详细信息

- 设备类型
- 设备型号
- 设备名称
- 序列号
- 唯一设备标识符 (UDID)
- 电池电量

软件详细信息

- 操作系统版本
- 已安装应用程序列表
- 存储容量
- 可用空间
- iTunes Store 状态

管理详细信息

- 托管状态
- 监管状态
- IP 地址
- 注册方法
- 安全状态

其他详细信息

- 已安装配置文件
- 已安装证书
- 激活锁定状态
- 购买信息
- 上次库存更新时间

4 库存

库存为什么至关重要?

如果一种事物无法衡量，也就谈不上对它的管理。您通过 MDM 解决方案收集的库存数据适用于广泛的业务需求，并可帮助您回答以下常见问题：

- 我的设备是否都处于安全状态?
- 我们已经部署了多少个应用程序?
- 某设备正在运行哪个版本的 iOS、macOS 和 tvOS?

某些管理解决方案甚至允许您收集有关特定硬件和软件加载项的额外（自定义）库存信息。例如，您可以查明上次运行第三方备份实用程序的时间，或安装了哪些打印机驱动程序。

智能定位

利用库存数据，您可通过智能定位对设备进行动态分组，并将配置参数文件和限制部署到这些设备。在 Jamf 中，该功能被称为“智能分组”。

静态分组对比智能分组

静态分组是指一组定义明确（如教室或实验室）的设备。您可以将管理策略应用于整个组。

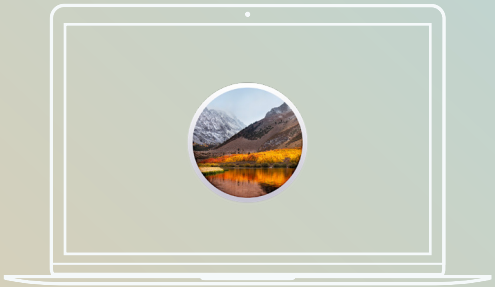
而智能分组具有动态属性，且始终随库存数据不断变化。您可利用该特性对设备进行动态分组，并将配置参数文件和限制部署到这些设备。

5 安全

确保设备的安全性、机密性以及对企业资源的访问权限无疑是一切组织机构的首要任务。为了实现这一目的，Apple 公司在 macOS、iOS 和 tvOS 中创建了大量的安全特性。

您可以结合 MDM 解决方案，确保您的设备、应用程序和网络均处于安全状态。

iOS 安全特性



macOS 安全特性

- Software Updates
- Secure System
- App Store
- Touch ID
- Hardware Encryption
- App Sandboxing
- Privacy
- Supervision

- Software Updates
- System Integrity Protection (SIP)
- Gatekeeper
- App Store
- FileVault Encryption
- XProtect
- App Sandboxing
- Privacy

tvOS 充分利用了 iOS 中的诸多安全特性，例如来自 Apple 的直接软件更新、经过审查和安全防护处理的 App Store 应用程序、通过“应用程序沙盒”(App Sandboxing) 实现的应用程序数据保护以及通过监管进行的更深层次的管理。

您可凭借管理功能部署 Apple TV 设置，以实现 AirPlay 安全防护自动化。该功能允许您将 Apple 设备与 Apple TV 进行配对，只有相应的设备才能够通过无线方式共享其屏幕内容。

5 安全

Unix 是 Apple 操作系统的基础，为 Apple 设备提供了强大的内核。Apple 的操作系统将安全性视为第一要务，并在此基础上增加了独有的安全设置。这些设置可通过 MDM 解决方案进行管理。

此外，您可以将苹果的部署程序与 MDM 解决方案搭配使用，从而在您的环境中更好地管理上述设置。

5 安全

适于 macOS、iOS 和 tvOS 的 MDM 安全命令

macOS

- 强制执行 FileVault
- 强制执行 Gatekeeper 设置
- 设置软件更新
- 锁定、擦除和重新启动计算机
- 删除受限的应用程序
- 删除 MDM

iOS

- 启用丢失模式
- 锁定和擦除设备
- 远程擦除
- 更新 iOS
- 清除限制和密码
- 删除 MDM

tvOS

- 远程擦除
- 重新启动设备
- 单一应用模式
- 删除受限的应用程序

适于 iOS 的 MDM 丢失模式

您可利用 Apple 的丢失模式和 MDM 解决方案，锁定、找到并恢复丢失或被盗的 iOS 设备，而不会因使用持续追踪而降低机密性。丢失模式激活后，iOS 设备就会收到自定义的锁屏消息，随后停用一切功能并将所在位置发送给 IT 人员。

条件访问

对于应用了 Windows Azure AD 和 Office 365 的组织机构，必须要为 Mac 设备提供条件访问路径。MDM 解决方案堪称同类最佳产品，其中集成了内置式条件访问插件。

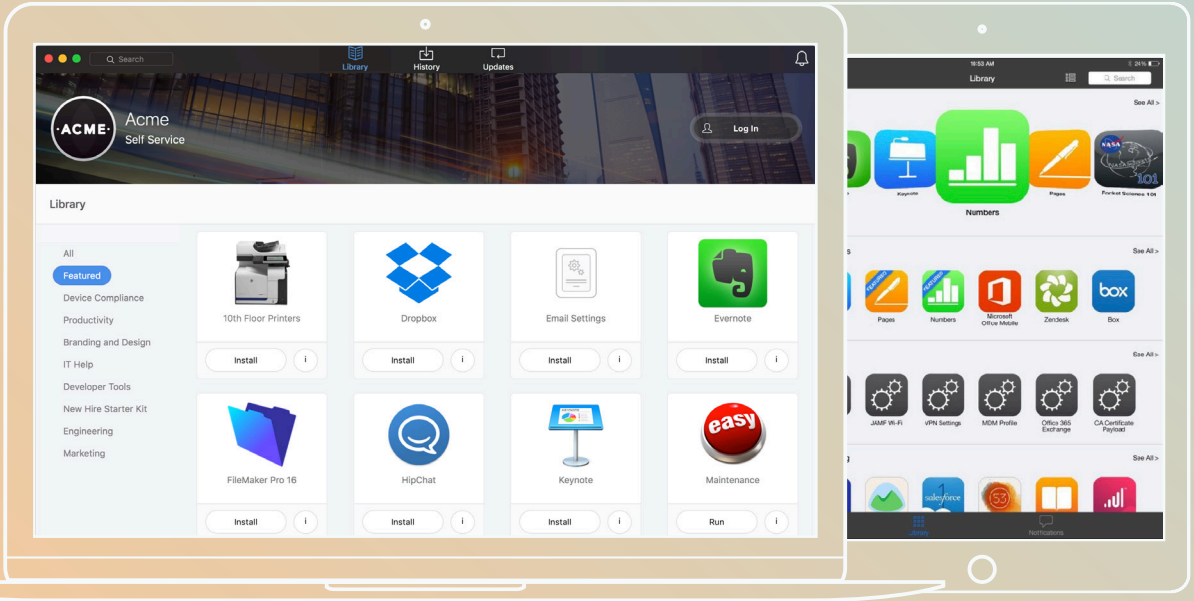
软件升级

在历年开发 macOS、iOS 和 tvOS 主版本的过程中，Apple 一直走在创新道路的前沿。Apple 每年都会面向消费者重磅推出全新功能，同时增加安全屏障并修复存在的漏洞。这些更新对于保护员工或学生的设备数据而言至关重要。您的管理解决方案不仅要能够部署来自 Apple 的更新内容，还需要迅速支持（理想情况为当日）所有随之而来的全新管理功能。

6 用户授权与采用

随着 Lyft、Amazon Prime 和 WebMD 等自助式工具的兴起，如今的员工们都希望能够随时获得所需的工具。通过企业应用程序目录，用户只需在设备上轻轻一点，即可访问资源、内容、一级帮助以及受信任的应用程序，进而满足自身需求，而无需向 IT 部门提交帮助台票证。

适于 Mac 的应用程序目录



适于 Mac 的应用程序目录

例如：适于 Mac 和 iOS 的 Jamf 自助服务提供了可以无缝集成到任何组织机构内部资源或企业内联网中的品牌应用程序目录。

通过企业应用程序目录，用户可以访问以下内容：

- App Store、B2B、内部应用程序和第三方软件
- 电子邮件、VPN 和其他配置
- 电子书、指南与视频
- 书签与快捷方式
- 打印机映射和驱动程序
- 帮助台票证与硬件要求
- 密码重置与合规性信息
- 基本维护与系统诊断
- 软件与操作系统升级
- 单点登录 (SSO) 集成
- 本地化语言支持英语、法语、德语、日语以及简体中文

6 用户授权与采用

按需式应用程序和资源目录的优势。

适用于 IT 的内容。

- 减少维护环境控制时使用的帮助台票证和支持成本
- 可在任何一个托管 Mac、iPad 或 iPhone 上自动安装应用程序目录，如 Jamf Self Service
- 集成目录服务，以根据部门、用户角色、位置以及其他内容对内容进行自定义
- 自动执行零层支持的常用 IT 任务，如密码重置、系统诊断

适用于用户的内容。

- 使终端用户可以即时访问多元化资源的全方位自助服务目标
- 提供直观用户界面，可针对本地语言和您的环境对其进行自定义
- 提供常用的书签 web 服务，如 HR 工具、通信平台或用于轻松访问公司有价值信息的内部资源
- 无需 IT 帮助，即可安装组织机构许可的应用程序
- 提供诸如打印机安装和软件更新等常见 IT 问题的快速解决方案
- 接收可用服务和安全增强功能的实时通知

MDM 解决方案堪称同类最佳产品，应该能够将您的应用程序目录品牌化，以匹配您现有的企业资源。这样，您的应用程序目录即可无缝集成到现有的内部属性中，同时使熟悉度和易用性得到提升。

意外利好：第三方集成内容

Apple 设备管理只是您技术组合的一个组成部分，但正是这个部分起到了重要甚至关键的作用。无论您使用的是帮助台票证系统（如 ServiceNow）还是 Okta 等一些 SSO 身份验证工具，您的 Apple 设备管理解决方案都必须与您现有的 IT 工具无缝集成。

我们正致力于利用第三方集成内容（如 Jamf Marketplace 中的那些集成内容）来强化您所拥有的功能，使您的生态系统更具力量。从跨行业的集成内容到具体的解决方案，此类集成内容实现了 IT 团队与服务的连接，并打造出一体化、安全和无缝的最终用户体验。

基础架构规划

用于托管管理环境的位置与您所选择的管理解决方案同等重要。云托管不仅使升级变得轻而易举，同时还减少了 IT 部门所面临的来自服务器管理、灾难恢复等方面的压力。

越来越多的组织机构正逐渐转为使用云托管

以下是 Eventbrite 等企业组织转为使用云技术的几个原因：

云托管的优势

服务器配置（持续的安全与更新管理）

备份管理和测试

存储基础架构的全球可用性

灾难恢复；异地位置

数据库管理（持续的安全与更新）

服务器监控和响应团队

业界领先的 Apple 管理

Apple 正逐步建立起一个互联的生态系统，其中的应用程序和服务能够跨设备相互兼容。不断发展的企业合作伙伴关系（IBM、Cisco、SAP 等）以及技术选择计划的蓬勃发展，必将使 Mac、iPad、iPhone 和 Apple TV 设备的使用量空前提升。

为了能够充分利用 Apple 与您的技术性投资，您需要一个符合 Apple 发展方向的管理解决方案；且这个解决方案需要从问世的第一天就向世人证明，帮助人们充分利用 Apple 设备是它的第一要务。

作为 Apple 设备管理的黄金标准，Jamf 自 2002 年以来一直致力于维护 Apple 生态系统，是最受广大企业和学校信赖的产品，并始终如一地为整个生态系统提供管理经验。

jamf

Jamf 能够与各类 Apple 服务集成，并即时支持Apple 设备的诸多操作系统与功能，可为您提供必要的工具以满足所有支持需求，让您可以更加专注于战略性任务，从而帮助您的组织机构节省时间和金钱。

您只要免费试用一下我们的产品，就会明白为什么 93% 的 Jamf 客户年复一年地坚持与我们合作。

开始试用