macOS 的安全性

IT 概述

Apple 在设计 macOS 平台时采用的是硬件、软件和服务相集成的方法，因此，在设计上安全可靠，并可方便快捷地进行配置、部署和管理。macOS 具备 IT 专业人员所需的关键安全技术，方便 IT 专业人员在安全的企业网络中保护公司数据和进行集成。另外，Apple 还与标准机构合作，确保符合最新的安全认证。本概述将简要介绍其中的一些功能。

本文由以下主题领域组成：

- **系统安全：**构成 macOS 基础的集成式安全软件。
- **加密和数据保护：**在设备丢失或被盗时保护用户数据的架构和设计。
- **App 安全：**保护 Mac 免遭恶意软件侵害并驱动 app 安全运行而不损害平台完整性的系统。
- **身份验证和数字签名：**macOS 中用于进行凭证管理和支持行业标准技术的工具，如智能卡和 S/MIME。
- **网络安全：**针对传输中的数据提供安全验证和加密的行业标准联网协议。
- **设备控制：**用于管理 Apple 设备的方法，可防止未授权的使用并在设备丢失或被盗时启用远程擦除。

如需 macOS 部署和管理的更多信息，请参阅《macOS 部署参考》：help.apple.com/deployment/macos。

如需了解本文未涵盖的 Apple 服务的安全功能，请参阅《iOS 安全保护》：www.apple.com/business/docs/iOS_Security_Guide.pdf。

系统安全

macOS 系统安全旨在确保每台 Mac 的所有核心组件都能够为软件和硬件提供安全环境。此架构是 macOS 安全体系的核心，并且不会影响设备的正常使用。

UNIX

macOS 内核——操作系统的核心，基于伯克利软件套件 (BSD) 和 Mach 微内核。BSD 提供基本的文件系统和联网服务、用户和群组识别方案以及许多其他基础功能。另外，BSD 还可基于用户和群组 ID 对文件和系统资源执行限制。

Mach 提供内存管理、线程控制、硬件抽象化和进程间通信。Mach 端口用于代表任务和其他资源，Mach 可执行对端口的访问限制，控制哪些任务可向端口发送信息。BSD 安全策略和 Mach 访问权限构成了 macOS 安全体系的重要基础，是执行本地安全的关键。

内核的安全性对整个操作系统的安全性至关重要。代码签名可保护内核和第三方内核扩展，以及 Apple 开发的其他系统库和可执行文件。

用户权限模式

授予或拒绝访问权限 (有时也称作访问权) 是 Mac 安全的一个重要方面。权限是指执行某项特定操作的能力，例如获得数据访问权限或执行代码的权限。可在文件夹、子文件夹、文件、app 级别授予权限，也可针对文件中的特定数据、app 功能和管理功能授予权限。数字签名可识别 app 和系统组件的访问权限。

macOS 可在许多级别控制权限，包括 Mach 和内核的 BSD 组件。macOS 使用联网协议控制已联网 app 的权限。

强制访问控制

macOS 还使用强制访问控制——由开发者创建的设置安全限制的策略，此类策略无法被覆盖。此方法不同于自主访问控制，自主访问控制允许用户根据首选项中的设置来覆盖安全策略。强制访问控制属于底层技术，有助于实现多个重要功能 (包括沙箱技术、家长控制、托管的首选项、扩展和系统完整性保护)，但不向用户显示。

系统完整性保护

OS X 10.11 或更高版本采用一个名为“系统完整性保护”的系统级保护，可对特定关键文件系统位置中的组件进行只读限制，以防止恶意代码执行或修改此类组件。系统完整性保护是特定于电脑的一项设置，升级至 OS X 10.11 后，默认情况下处于开启状态；如果停用此项设置，将移除对物理存储设备上所有分区的保护。macOS 将此安全策略应用于系统上运行的每个进程，无论进程是在沙箱模式下运行还是使用管理权限运行。

如需有关上述文件系统只读区域的更多信息，请参阅 Apple 支持文章《关于系统完整性保护》：support.apple.com/zh-cn/HT204899。

内核扩展

macOS 提供内核扩展机制以允许将代码动态载入内核，无需重新编译或重新链接。由于这些内核扩展 (KEXT) 可提供模块化和动态载入，因此，对于需要访问内部内核接口 (例如硬件设备驱动程序或 VPN app) 的所有相对自包含服务而言，这些内核扩展是合理的选择。

为提高 Mac 的安全性，需要用户同意才能载入与 macOS High Sierra 一起安装或在其后安装的内核扩展。这被称为用户批准的内核扩展载入。任何用户，即使没有管理员权限，也都可以批准内核扩展。

如果内核扩展存在以下情况，则无需授权：

- 升级至 macOS High Sierra 之前就已安装在 Mac 中。
- 正在替换以前批准的扩展。
- 从 macOS 恢复分区启动时，无需用户同意即可使用提供的 `spctl` 命令载入。
- 可通过移动设备管理 (MDM) 配置载入。从 macOS High Sierra 10.13.2 开始，你可以使用 MDM 来指定内核扩展列表，这些内核扩展无需用户同意就可以载入。为此，需要一台运行 macOS High Sierra 10.13.2 的 Mac，而且这台 Mac 要么已通过设备注册计划 (DEP) 注册了 MDM，要么已通过用户批准的 MDM 注册进行了注册。

如需有关内核扩展的更多信息，请参阅 Apple 支持文章《为 macOS High Sierra 中内核扩展的变化做好准备》：support.apple.com/zh-cn/HT208019。

固件密码

macOS 支持使用密码来防止意外修改特定系统上的固件设置。此固件密码可用于防止以下情况：

- 从未授权的系统宗卷启动
- 修改启动流程，例如，启动进入单用户模式
- 未经授权访问 macOS 恢复
- 通过雷雳等接口进行直接内存访问 (DMA)
- 需要 DMA 的目标磁盘模式

注意：iMac Pro 中的 T2 芯片可防止用户重置固件密码，即使他们获得 Mac 的物理访问权限也不行。在不带 T2 芯片的 Mac 上，必须采取额外预防措施，以防止用户以物理方式访问 Mac 的内部数据。

互联网恢复

Mac 电脑在无法从内置恢复系统启动时，将自动尝试通过互联网的 macOS 恢复方式进行启动。如果出现此种情况，Mac 在启动时将显示一个旋转的地球而不是 Apple 标志。用户可通过互联网恢复，重新安装最新版本的 macOS 或 Mac 自带的版本。

macOS 更新通过 App Store 进行分发并由 macOS 安装器执行，macOS 安装器在安装前将利用代码签名来确保安装器及其软件包的完整性和真实性。同样，互联网恢复服务是特定 Mac 自带的操作系统的权威来源。

如需有关 macOS 恢复功能的更多信息，请参阅 Apple 支持文章《关于 macOS 恢复功能》：support.apple.com/zh-cn/HT201314。

加密和数据保护

Apple 文件系统

Apple 文件系统 (APFS) 是一种全新的现代文件系统，适用于 macOS、iOS、tvOS 和 watchOS。这种文件系统已针对闪存/固态硬盘存储进行了优化，具有以下特点：强加密、写时复制元数据、空间共享、文件与目录克隆、快照、快速调整目录大小、原子级安全存储元、改进的文件系统基础，以及独有的写时复制设计，这种设计使用 I/O 合并来提供最大性能，同时确保数据可靠性。

APFS 根据需求分配磁盘空间。当单个 APFS 容器具有多个宗卷时，可共享容器的可用空间，并且可根据需要将可用空间分配到任意单个宗卷。每个宗卷仅使用整个容器的一部分，因此，可用空间是容器的总大小减去容器中所有系统宗卷使用的空间。

对于 macOS High Sierra，有效的 APFS 容器必须至少包含三个宗卷，对用户隐藏前两个宗卷：

- 预启动宗卷：包含在容器中启动每个系统宗卷所需的数据。
- 恢复宗卷：包含恢复磁盘。
- 系统宗卷：包含 macOS 和用户文件夹。

文件保险箱

每台 Mac 均提供内置加密功能，称为“文件保险箱”，以保护所有静态数据的安全。“文件保险箱”使用 XTS-AES-128 数据加密保护 Mac 上静态数据的安全。“文件保险箱”可用于为内部和可移动存储设备提供全卷保护。如果用户在“设置助理”过程中输入 Apple ID 和密码，则助理将建议启用“文件保险箱”和在 iCloud 中存储恢复密钥。

在 Mac 上启用“文件保险箱”的用户需要提供有效的凭证才能继续启动进程和获得专用启动模式 (例如“目标磁盘模式”) 的访问权限。如果没有有效的登录凭证或恢复密钥，则整个宗卷将保持加密状态，并且可防止未授权的访问，即使物理存储设备已移除并连接至另一台电脑。

为保护企业设置中的数据，IT 应通过 MDM 来定义和执行“文件保险箱”配置策略。在管理加密宗卷方面，企业有多个方式可选，包括机构恢复密钥、个人恢复密钥 (可选择通过 MDM 进行存储) 或将这两种密钥组合使用。还可以将密钥旋转设置为 MDM 中的一个策略。

加密磁盘映像

在 macOS 中，加密磁盘映像可充当安全容器，用户可以在其中存储或传输敏感文稿和其他文件。加密磁盘映像是使用“/应用程序/实用工具”中的“磁盘工具”创建的。磁盘映像可使用 128 位或 256 位 AES 加密进行加密。由于装载的磁盘映像被视为连接至 Mac 的本地宗卷，因此，用户可以复制、移动和打开其中存储的文件及文件夹。与“文件保险箱”一样，系统可实时对磁盘映像的内容进行加密和解密。通过加密磁盘映像，用户可以安全地交换文稿、文件和文件夹，比如将加密磁盘映像保存到可移动介质上，以邮件附件的形式发送加密磁盘映像，或将加密磁盘映像存储在远程服务器上。

ISO 27001 和 27018 认证

根据 2017 年 7 月 11 日公布的适用性声明 v2.1，Apple 针对基础架构、开发及运营推出的信息安全管理系统 (ISMS) 已经获得 ISO 27001 和 ISO 27018 认证，这个系统支持以下产品和服务：Apple 校园教务管理、iCloud、iMessage 信息、FaceTime 通话和 iTunes U。经英国标准协会 (BSI) 认证，Apple 符合此项 ISO 标准。要查看 ISO 27001 和 ISO 27018 合规性证书，请参阅 BSI 网站：

www.bsigroup.com/en-GB/our-services/certification/certificate-and-client-directory/search-results/?searchkey=company=apple&licencenumber=IS+649475

www.bsigroup.com/en-GB/our-services/certification/certificate-and-client-directory/search-results/?searchkey=company=Apple&licencenumber=PII%20673269

密码验证 (FIPS 140-2)

对于 OS X 10.6 及之后的每个版本，macOS 中的密码模块经反复验证，符合美国联邦信息处理标准 (FIPS) 140-2 级别 1。与每个主要版本一样，Apple 在发布 Mac 操作系统后，会将这些模块提交至 CMVP 进行重新验证。此计划可验证 Apple app 和第三方 app 加密操作的完整性，确保这些 app 正确使用 macOS 加密服务和批准的算法。所有 Apple FIPS 140-2 一致性验证证书都可以在 CMVP 供应商页面上找到。CMVP 根据密码模块在 csrc.nist.gov/groups/STM/cmvp/inprocess.html 上的当前状态，在两个单独的列表列出了密码模块的验证状态。

共同准则认证 (ISO 15408)

Apple 之前已通过共同准则认证计划下的 macOS 认证，并且正在针对操作系统保护描述文件 (PP_OSv4.1) 重新评估 macOS High Sierra。Apple 将继续进行评估，努力获得目前可用的协作性保护描述文件 (cPP) 的新版本和更新版的认证。在开发侧重于评估关键移动安全技术的 cPP 方面，Apple 在国际技术社区 (ITC) 中发挥了主导作用。

安全认证、计划和指导

Apple 已与世界各地的政府展开合作，共同制定针对高风险环境的“设备强化”指南，目的是通过提供说明和建议来维护更为安全的环境。这些指南提供了定义明确且经过审慎核实的信息，介绍如何配置和使用 macOS 中的内置功能，从而增强保护。

有关 macOS 安全认证、验证和指导的最新信息，请参阅 Apple 支持文章《适用于 macOS 的产品安全认证、验证和指导》：support.apple.com/zh-cn/HT201159。

App 安全

macOS 采用内置技术，以确保仅安装信任的 app，并帮助抵御恶意软件攻击。为确保合法 app 不被篡改，macOS 还采用了一个分层方法进行 app 运行时保护和 app 签名。

门禁

为控制 app 的安装来源，macOS 提供了一个称作“门禁”的功能。“门禁”允许用户和组织设置安装 app 所必需的安全级别。

若设为最安全的“门禁”设置，则用户只可以安装 App Store 中已签署的 app。若设为默认设置，则用户可以安装 App Store 中的 app 和具有有效 Developer ID 签名的 app。这类签名表明 app 已通过 Apple 颁发的证书签名，且自此之后尚未修改。如果需要，也可以通过“终端”命令完全停用“门禁”。

此外，在某些情况下，“门禁”可应用路径随机化，包括从未签名的磁盘映像或 app 下载位置和自动解压缩位置直接启动 app。在启动前，可通过路径随机化从文件系统中未自定的只读位置获取 app。这不但可防止 app 使用相对路径访问代码或内容，而且还可以防止 app 自行更新 (如果从只读位置启动)。使用“访达”移动 app (例如，将 app 移至“应用程序”文件夹) 意味着路径随机化不再适用。

默认保护模式的主要安全优势在于可提供广泛的生态系统保护。如果恶意软件作者设法窃取或通过其他方式获取 Developer ID 签名功能，并用它来分发恶意软件，则 Apple 可以通过撤销签名证书做出快速响应。这样便可阻止恶意软件进一步传播。此类保护将瓦解 Mac 上大多数恶意软件活动的经济模式，并为所有用户提供广泛的保护。

在安装任何 app 时，用户可以暂时覆盖上述设置。企业可以使用 MDM 解决方案来确立和执行“门禁”设置，并将证书添加到 macOS 信任策略以用于评估代码签名。

XProtect

macOS 采用内置技术进行基于签名的恶意软件检测。Apple 会监控新出现的恶意软件感染和病毒，并自动更新 XProtect 签名——独立于系统更新，以帮助 Mac 系统抵御恶意软件感染。XProtect 可自动检测和阻止已知恶意软件的安装。

恶意软件删除工具

如果恶意软件设法进入 Mac，macOS 还可通过技术手段来修复感染。除在生态系统中监控恶意软件活动以撤销 Developer ID (如果适用) 并签发 XProtect 更新外，Apple 还将签发 macOS 更新，为所有配置为接收自动安全更新的受感染系统删除恶意软件。恶意软件删除工具一旦收到更新的信息，就会在下一次重启之后删除恶意软件。恶意软件删除工具不会使 Mac 自动重启。

自动安全更新

Apple 会自动签发 XProtect 的更新和恶意软件删除工具。默认情况下，macOS 会每天检查这些更新。如需自动安全更新的更多信息，请参阅 Apple 支持文章《Mac App Store：自动安全更新》：support.apple.com/zh-cn/HT204536。

运行时保护

可对用户 app 空间中的系统文件、资源和内核进行保护。来自 App Store 的所有 app 都在沙箱模式下运行，以限制其访问其他 app 存储的数据。如果来自 App Store 的 app 需要从另一个 app 访问数据，则它只能通过使用 macOS 提供的 API 和服务来执行此操作。

强制 App 代码签名

来自 App Store 的所有 app 由 Apple 进行签名，以确保这些签名没有被篡改或更改。Apple 会对 Apple 设备提供的所有 app 进行签名。许多在 App Store 外部分发的 app 由开发者使用 Apple 颁发的 Developer ID 证书 (与私钥结合使用) 进行签名，以便在默认“门禁”设置下运行。

一般情况下，来自 App Store 外部的 app 也可使用 Apple 颁发的开发者证书签名。这样一来，你便可以验证 app 是否为原始 app，以及是否未被篡改。内部开发的 app 也应使用 Apple 颁发的 Developer ID 进行签名以便你可以验证其完整性。

强制访问控制 (MAC) 需要代码签名来启用受系统保护的授权。例如，需要通过防火墙进行访问的 app 必须使用适当的 MAC 授权进行签名。

身份验证和数字签名

为了方便安全地存储用户的凭证和数字身份，macOS 采用钥匙串和其他工具来支持身份验证和数字签名技术，如智能卡和 S/MIME 等。

钥匙串架构

macOS 提供一个名为“钥匙串”的资源库，可方便安全地存储用户名称和密码，包括数字身份、加密密钥和安全备注。该资源库可通过打开“应用程序”>“实用工具”中的“钥匙串访问”app 进行访问。借助钥匙串，你无需输入每个资源的凭证，甚至无需记住它们。系统会为每个 Mac 用户创建初始默认钥匙串，但用户也可以针对特定用途创建其他钥匙串。

除用户钥匙串外，macOS 还依赖许多系统级钥匙串，这些钥匙串可维护身份验证资产并且不属于用户特有，如网络凭证和公钥基础架构 (PKI) 身份。System Roots 就属于上述钥匙串之一且不可改变，它存储 Internet PKI 根证书颁发机构 (CA) 证书，以便为在线银行服务和电子商务任务提供便利。同样，你可以在内部将预置 CA 证书部署到托管的 Mac 电脑，以协助验证内部网站和服务。

安全的鉴定框架

对钥匙串数据进行分区并使用“访问控制列表 (ACL)”进行保护，因此，使用不同身份的 app 无法访问第三方 app 存储的凭证，除非用户明确批准这样做。此保护为企业内 Apple 设备上的一系列 app 和服务的身份验证凭证提供了保护机制。

触控 ID

带“触控 ID”传感器的 Mac 系统可以使用指纹进行解锁。“触控 ID”不能代替对密码的需求，在启动、重启或退出 Mac 后再登录时仍需要使用密码。登录后，无论何时要求用户提供密码，他们都可以快速使用“触控 ID”进行身份验证。

用户还可以使用“触控 ID”解锁“备忘录”app中受密码保护的备忘录，Safari 浏览器首选项的“密码”面板，以及“系统首选项”中的多个首选项面板中。为提高安全性，要想解锁“系统首选项”中的“安全性和隐私”面板，用户必须输入一个密码，而不是使用“触控 ID”。如果开启了“文件保险箱”，则用户还必须输入一个密码才能管理“用户和群组”首选项。登录同一台 Mac 的多个用户可以使用“触控 ID”切换帐户。

如需“触控 ID”及其安全性的更多信息，请参阅 Apple 支持文章《关于“触控 ID”高级安全技术》：support.apple.com/zh-cn/HT204587。

通过 Apple Watch 自动解锁

使用 Apple Watch 的用户可以用它来自动解锁他们的 Mac。在确保 Apple Watch 和 Mac 相互靠近后，Apple Watch 可通过蓝牙低功耗 (BLE) 和点对点 Wi-Fi 安全解锁 Mac。这需要一个已配置双重认证 (TFA) 的 iCloud 帐户。

如需有关此协议以及连续互通和接力功能的更多信息，请参阅《iOS 安全保护》：www.apple.com/business/docs/iOS_Security_Guide.pdf。

智能卡

macOS Sierra 及更高版本提供对个人身份验证 (PIV) 卡的原生支持。这些卡在商业和政府机构中广泛用于 TFA、数字签名和加密。

智能卡包含一个或多个数字身份，拥有一对公私钥和一个关联证书。使用个人识别码 (PIN) 解锁智能卡后，可访问用于验证、加密和签名操作的私钥。此证书确定密钥可用于做什么，与其相关联的属性有哪些，以及它是否已由 CA 进行验证 (签名)。

智能卡可用于双重认证。解锁一张卡需要的双重认证包括“你拥有的物品” (卡) 和“你知道的信息”(PIN)。如果要通过智能卡登录窗口身份验证和客户端证书身份验证访问 Safari 浏览器上的网站，macOS Sierra 及更高版本可提供原生支持。另外，它还支持使用密钥 (PKINIT) 的 Kerberos 身份验证，以单点登录 Kerberos 支持的服务。

如需有关 macOS 上智能卡部署的更多信息，请参阅《macOS 部署参考》：help.apple.com/deployment/macos。

数字签名和加密

在“邮件”app 中，用户可以发送已进行数字签名和加密的信息。在兼容的智能卡中，邮件可自动发现附加的 PIV 令牌上数字签名和加密证书中，是否有适当的 RFC 822 格式的电子邮件地址主题或主题备用名称 (区分大小写)。如果配置的电子邮件帐户与附加的 PIV 令牌上的数字签名或加密证书上的电子邮件地址匹配，则“邮件”将自动在新信息窗口的工具栏中显示签名按钮。如果“邮件”具有收件人的电子邮件加密证书，或者可以在“Microsoft Exchange 全局地址列表 (GAL)”中发现它，则解锁的图标将显示在新的信息工具栏中。上锁的图标表示将使用收件人的公钥加密发送信息。

为 S/MIME 单独设置信息

macOS 支持为 S/MIME 单独设置信息。这表示在默认情况下，S/MIME 用户可以选择始终签名和加密信息，或有选择性地签名和加密单个信息。

借助配置描述文件、MDM 解决方案、简单证书注册协议 (SCEP) 或 Microsoft Active Directory 证书颁发机构，用于 S/MIME 的身份可交付到 Apple 设备。

网络安全

除了 Apple 用于保护 Mac 电脑数据的内置安全保护机制外，企业还可以采用许多网络安全措施来确保信息在来往于 Mac 时安全无虞。

移动办公用户必须能在全球任何地方访问公司网络，因此很重要的一点是确保他们得到授权并且数据在传输期间受到保护。macOS 使用标准联网协议并使开发者能够访问这些协议，以确保通信经过验证、授权和加密。为了实现这些安全目标，macOS 集成了经证实的技术和最新标准来进行 Wi-Fi 数据网络连接。

TLS

macOS 支持传输层安全性 (TLS 1.0、TLS 1.1 和 TLS 1.2) 和 DTLS。它可同时支持 AES-128 和 AES-256，并且倾向于使用采用完全正向保密的密码套件。Safari 浏览器、日历、邮件和其他互联网 app 会自动使用此协议在设备与网络服务之间建立一条加密的通信通道。

高级 API (如 CFNetwork) 使开发者可以轻松在 app 中采用 TLS，而低级 API (如 SecureTransport) 则提供精细控制。CFNetwork 不允许使用 SSLv3，并禁止那些使用 WebKit 的 app (如 Safari 浏览器) 进行 SSLv3 连接。

从 macOS High Sierra 和 iOS 11 开始，除非得到用户信任，否则不再允许使用 SHA-1 证书进行 TLS 连接。另外，不允许使用 RSA 密钥少于 2048 位的证书。macOS Sierra 和 iOS 10 中已弃用 RC4 对称密码套件。默认情况下，通过 SecureTransport API 实施的 TLS 客户端或服务器不会启用 RC4 密码套件，并且在 RC4 是唯一可用密码套件时无法进行连接。为提升安全性，需要使用 RC4 的服务或 app 应当进行升级，以使用安全的现代化密码套件。

App 传输安全

“App 传输安全”提供默认连接要求，以便 app 遵循使用 NSURLConnection、CFURL 或 NSURLSession API 进行安全连接的最佳做法。默认情况下，“App 传输安全”会对密码选择进行限制，以便仅包含提供正向保密的套件，特别是 GCM 或 CBC 模式中的 ECDHE_ECDSA_AES 和 ECDHE_RSA_AES。App 能够针对每个域停用正向保密要求，在这种情况下，RSA_AES 将添加至可用的密码集。

服务器必须支持 TLS 1.2 和正向保密，证书必须有效且已使用 SHA-256 进行签名，或最好具有一个至少 2048 位的 RSA 密钥或 256 位的椭圆曲线密钥。

除非 app 覆盖了“App 传输安全”，否则，不符合这些要求的网络连接将无法连接。无效的证书会导致硬故障和无法连接。“App 传输安全”将自动应用于针对 macOS 10.11 或更高版本编译的 app。

VPN

安全网络服务 (例如虚拟专用网络 (VPN)) 通常只需要很少的设置和配置，就能与 macOS 配合使用。Mac 电脑可与支持以下协议和验证方式的 VPN 服务器配合使用：

- IKEv2/IPSec，通过共享密码、RSA 证书、ECDSA 证书、EAP-MSCHAPv2 或 EAP-TLS 进行验证
- SSL-VPN，使用适当的、来自 App Store 的客户端 app
- Cisco IPSec，可以通过密码、RSA SecurID 或 CRYPTOCard 进行用户验证，也可通过共享密钥和证书进行机器验证

- L2TP/IPSec，可以通过 MS-CHAPV2 密码、RSA SecurID 或 CRYPTOCard 进行用户验证，也可通过共享密钥进行机器验证

除来自第三方的 VPN 解决方案外，macOS 还支持以下解决方案：

- **VPN On Demand**，适用于使用基于证书验证的网络。IT 策略通过使用 VPN 配置描述文件来指定哪些域需要 VPN。
- **为 App 单独设置 VPN**，有助于更精确地建立 VPN 连接。MDM 可以为每个托管的 app 以及 Safari 浏览器中的特定网域指定一个连接。这有助于确保进出公司网络的数据始终是安全的，并可以确保用户的个人数据不进出公司网络。

无线局域网

macOS 支持行业标准的 Wi-Fi 协议，包括 WPA2 企业级，可针对公司无线网络提供访问验证服务。WPA2 企业级使用 128 位 AES 加密，可为用户提供最高级别的安全保障：在通过 Wi-Fi 网络连接发送和接收通信时，可确保用户的数据始终受到保护。由于 Mac 电脑支持 802.1X，因此可以集成到广泛的 RADIUS 验证环境中。802.1X 无线验证的方法包括 EAP-TLS、EAP-TTLS、EAP-FAST、EAP-AKA、PEAPv0、PEAPv1 和 LEAP。

还可以在 macOS 的登录窗口使用 WPA/WPA2 企业级验证，以便用户在登录时进行网络验证。

macOS 设置助理支持使用 TTLS 或 PEAP 对用户名称和密码凭证进行 802.1X 验证。

防火墙

macOS 采用内置防火墙以防止 Mac 受到来自网络访问和拒绝服务的攻击。它支持以下配置：

- 阻止所有传入连接，无论使用何种 app
- 自动允许内置软件接收传入连接
- 自动允许已下载和签名的软件接收传入连接
- 基于用户指定的 app 添加或拒绝访问权限
- 防止 Mac 响应 ICMP 探查和端口扫描请求

单点登录

macOS 支持使用 Kerberos 对企业网络进行身份验证。App 可使用 Kerberos 对有权访问服务的用户进行身份验证。Kerberos 还可用于一系列的网络活动，从安全的 Safari 浏览器会话和网络文件系统验证，到第三方 app。可支持基于证书的验证 (PKINIT)，但需要采用开发者 API 的 app。

GSS-API SPNEGO 令牌和 HTTP Negotiate 协议可与基于 Kerberos 的认证网关和支持 Kerberos 工单的 Windows Integrated Authentication 系统配合使用。Kerberos 支持基于开源 Heimdal 项目。

支持以下加密类型：

- AES128-CTS-HMAC-SHA1-96
- AES256-CTS-HMAC-SHA1-96
- DES3-CBC-SHA1
- ARCFOUR-HMAC-MD5

要配置 Kerberos，可通过“工单查看器”获取工单，然后登录一个 Windows Active Directory 域或使用命令行 `kinit` 工具。

“隔空投送”的安全性

支持“隔空投送”的 Mac 电脑使用 BLE 和 Apple 创建的点对点 Wi-Fi 技术，向附近设备发送文件和信息，包括支持“隔空投送”、运行 iOS 7 或更高版本的 iOS 设备。Wi-Fi 无线电用于在设备之间直接通信，无需使用任何互联网连接或 Wi-Fi 接入点。此连接使用 TLS 进行加密。

如需关于“隔空投送”、“隔空投送”的安全性和其他 Apple 服务的更多信息，请参阅《iOS 安全保护》的“网络安全”部分：www.apple.com/business/docs/iOS_Security_Guide.pdf。

设备控制

macOS 支持一系列易于执行和管理的灵活安全策略和配置。这使得企业可以保护公司信息并确保员工遵守企业要求，即便员工使用的是自带电脑 (例如，在参与“自带设备办公”(BYOD) 计划的过程中) 也无妨。

企业可以使用密码保护、配置描述文件和第三方 MDM 解决方案来管理设备群，并确保公司数据的安全，即使员工在其个人 Mac 电脑上访问这些数据也无妨。

密码保护

在使用“触控 ID”的 Mac 电脑上，最小密码长度为八位字符。始终建议使用又长又复杂的密码，因为这些密码很难猜，也很难受到攻击。

管理员可利用 MDM 或要求用户手动安装配置描述文件来执行复杂密码要求和其他策略。对于 macOS 密码策略有效负载安装，需要用到管理员密码。

如需 MDM 设置中每个可用策略的详细信息，请参阅 help.apple.com/deployment/mdm/#/mdm4D6A472A。

如需有关每个策略的开发者详细信息，请参阅《配置描述文件参考》：developer.apple.com/library/ios/featuredarticles/iPhoneConfigurationProfileRef。

配置执行

配置描述文件是一个 XML 文件，管理员可通过它向 Mac 电脑分发配置信息。如果用户删除配置描述文件，由该描述文件定义的所有设置也将随之删除。管理员可以将策略与 Wi-Fi 和数据访问进行关联，以便执行设置。例如，提供电子邮件配置的配置描述文件还可以用来指定设备密码策略。除非密码符合管理员的要求，否则用户无法访问邮件。

macOS 配置描述文件包含多项可以指定的设置，其中包括：

- 密码策略
- 对设备功能进行限制 (例如，停用摄像头)
- Wi-Fi 或 VPN 设置
- 邮件或 Exchange Server 设置
- LDAP 目录服务设置
- 防火墙设置
- 凭证和密钥
- 软件更新

如需描述文件的当前列表，请参阅《配置描述文件参考》：help.apple.com/deployment/mdm/#/mdm5370d089。

为了验证配置描述文件的来源、完整性并保护其中的内容，可以对配置描述文件进行签名和加密。配置描述文件还可以锁定到 Mac，以便彻底禁止用户删除这些文件，或必须使用密码才能删除。在 MDM 解决方案中注册了 Mac 的配置描述文件可以移除，但是，这样做也会移除托管的配置信息、数据和 app。

用户可以安装从 Safari 浏览器下载的、在邮件信息中发送的或使用 MDM 解决方案实时发送的配置描述文件。当用户在 DEP 或 Apple 校园教务管理中设置 Mac 时，电脑会下载并自动安装用于 MDM 注册的描述文件。

MDM

macOS 支持 MDM，可让企业在组织内部安全地配置和管理规模化的 Mac、iPhone、iPad 和 Apple TV 部署。MDM 功能建立在现有的 macOS 技术 (比如配置描述文件、无线注册和 Apple 推送通知服务 (APNs)) 的基础之上。例如，APNs 用于唤醒设备，因此，它可以通过安全连接与 MDM 解决方案直接通信。机密或专有信息不会通过 APNs 进行传输。

利用 MDM，IT 部门可在企业环境中注册 Mac 电脑、以无线方式配置和更新设置、监控公司策略的遵守情况，甚至可以远程擦除或锁定托管的 Mac 电脑。

设备注册

作为 Apple 校园教务管理和 Apple 部署计划的一部分，可通过设备注册，快捷地部署机构直接从 Apple 或相关 Apple 授权经销商购买的 Mac 电脑。

机构可以在 MDM 中自动注册电脑，无需在用户拿到这些电脑之前进行物理操作或预先准备。注册电脑后，管理员登录计划网站，将计划与 MDM 解决方案进行关联。然后，系统将为购买的电脑自动分配一个 MDM 解决方案。注册 Mac 后，便会自动安装 MDM 指定的任何配置、限制或控制。电脑和 Apple 服务器之间的所有通信在传输时，都会使用 HTTPS (SSL) 进行加密。

可通过移除“设置助理”中的特定步骤，进一步精简用户的设置流程，以便用户可以快速启动和运行。管理员还可以控制用户是否可以从电脑移除 MDM 描述文件，并确保从最开始就设置了设备限制。将电脑从包装中取出并激活后，可在企业的 MDM 解决方案中注册这台电脑，并安装所有管理设置、app 和书籍。注意，并非所有国家或地区都可以使用设备注册计划。

如需有关商务应用的更多信息，请参阅《Apple 部署计划帮助》：help.apple.com/deployment/business。如需有关教育应用的更多信息，请参阅《Apple 校园教务管理帮助》：help.apple.com/schoolmanager。

限制措施

可以由管理员启用限制措施，或在某些情况下停用限制措施，以防止用户访问特定的 app、服务或设备功能。限制措施将在配置描述文件中以“限制”有效负载的形式发送到设备。可将限制措施应用于 macOS、iOS 和 tvOS。

可在以下网址查看 IT 经理可用限制措施的当前列表：help.apple.com/deployment/mdm/#/mdm2pHf95672

远程擦除和远程锁定

Mac 管理员或用户可以远程擦除 Mac 电脑。仅当 Mac 已启用“文件保险箱”时才能进行即时远程擦除。当 MDM 或 iCloud 触发远程擦除命令时，电脑将发送确认消息并执行擦除。使用远程锁定时，MDM 需要对 Mac 电脑应用一个六位数密码，用户必须输入此密码才能解除锁定。

隐私

Apple 认为隐私是一项基本人权，因此，Apple 每款产品的设计理念都是尽可能直接在设备上进行处理、限制数据的收集和使用、让信息的使用和控制透明化，并构建强大的安全基础。

Apple 拥有大量内置控件和选项，让 macOS 用户可以决定 app 如何使用、何时使用以及使用哪些信息。如需更多信息，请参阅 www.apple.com/cn/privacy。