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。

安全性
包含密码或私钥的描述文件只会发送到为其创建的设备：设备必须使用其管理证书对请求进行签名。密码和证书不会写入日志。

Revision #6
Created 2026-11-10 15:18:43 UTC by Admin
Updated 2026-11-12 09:58:21 UTC by Admin