

适用于 iOS 的 SonicWall™ Mobile Connect 5.0

用户指南

SONICWALL™

目录

Mobile Connect 简介	4
Mobile Connect 的工作原理	4
Mobile Connect 5.0 中的新功能	4
其他功能信息	5
支持的平台	6
Apple 产品支持	6
SonicWall 设备支持	7
需要的网络信息	7
安装和连接	9
安装 Mobile Connect	9
创建和保存连接	10
创建防火墙或 SMA 100 系列/ SRA 连接	10
创建 SMA 1000 系列/ E 级 SRA 连接	13
启动连接	15
配置按需连接	17
按需连接到 SMA 1000 系列/ E 级 SRA	17
按需连接到 SMA 100 系列/ SRA	18
配置受信任的网络检测	21
使用 Apple Configurator 2 和 Mobile Connect	22
配置 Per App VPN	25
设置、书签和文件	26
设置概述	26
设置部分	27
支持部分	28
URL 控制语法和参数	29
使用 addprofile 命令	29
使用 connect 命令	30
使用 disconnect 命令	31
使用 callbackurl 命令参数	31
使用书签	33
显示和过滤书签	33
支持的书签类型	34
使用文件	37
文件功能	39
监控和故障排除	45
监控 Mobile Connect	45
Mobile Connect 故障排除	46

SonicWall 支持	47
关于本文档	48

Mobile Connect 简介

适用于 iOS 的 SonicWall™ Mobile Connect 是一款适用于 Apple iPhone、iPod touch 和 iPad 的应用程序，可为受 SonicWall 安全设备保护的专用网络提供安全的移动连接。

主题：

- 第 4 页的 [Mobile Connect 的工作原理](#)
- 第 4 页的 [Mobile Connect 5.0 中的新功能](#)
- 第 5 页的 [其他功能信息](#)
- 第 6 页的 [支持的平台](#)

Mobile Connect 的工作原理

现代商业实践要求用户能够随时随地访问文件、内部网站等各种网络资源。同时，确保这些资源的安全需要持续不断的努力。尽管大多数用户意识到必须小心保护计算机免受网络安全风险，但人们对 iPhone、iPod touch 和 iPad 移动设备往往不具备这种安全意识。然而，移动设备遭遇的安全攻击越来越多。此外，移动设备通常使用不安全、不可信的公共 Wi-Fi 热点连接到互联网。因此，在需要防范使用移动设备的固有安全风险的同时，提供安全的移动访问是一个挑战。

适用于 iPhone、iPod touch 和 iPad 的 SonicWall Mobile Connect 应用程序为敏感网络资源提供安全的移动访问。Mobile Connect 在移动设备与受 SonicWall 安全设备保护的专用网络之间建立安全套接字层虚拟专用网络 (SSL VPN) 连接。所有进出专用网络的流量都通过 SSL VPN 隧道安全传输。

从 App Store 安装 SonicWall Mobile Connect 后，开始使用 Mobile Connect 的步骤如下：

- 1 请确保 Mobile Connect 将要使用的 SonicWall SMA、SRA 或防火墙设备连接到网络。
- 2 配置网络信息（服务器名称、用户名、密码等）。
- 3 Mobile Connect 建立与 SonicWall 安全设备的 SSL VPN 隧道。

现在即可访问专用网络上的资源。所有进出专用网络的流量都通过 SSL VPN 隧道安全传输。

Mobile Connect 5.0 中的新功能

本节介绍 Mobile Connect 5.0 版本中包含的增强功能。

- **iOS 11 兼容性** - Mobile Connect 采用了 iOS 11 中引入的醒目、动态的新风格元素，包括大标题栏、横向标签栏等等。
- **网络扩展支持** - Mobile Connect 现在利用 Apple 当前的 VPN 框架（名为“网络扩展”），以在 iOS 设备上实现更可靠的 VPN 连接。升级到 5.0 版本后，可能需要重新设置 Mobile Connect，包括更新 VPN 连接配置和证书（如果适用）。

- **安全 Web 书签** - Web 书签现在可以在 Mobile Connect 内启动，而不必启动第三方浏览器，实现无缝且更安全的用户体验。安全 Web 书签还支持单点登录，并需要使用支持安全 Web 书签策略的软件连接到 VPN 服务器。
- **其他 Touch ID 支持** - Mobile Connect 现在支持 Touch ID，用于到所支持的 SMA 1000 系列服务器的 VPN 连接。
- **全局 HA 支持** - Mobile Connect 包含针对运行 12.1 或更高版本的固件的 SMA 1000 系列服务器的 VPN 连接的全局高可用性和灾难恢复功能的更新。

其他功能信息

适用于 iOS 的 SonicWall Mobile Connect 继续支持以下功能：

- **Slide Over 和 Split View** - Mobile Connect 支持 iOS 9 和 10 功能，包括 iPad 上的 **Slide Over** 和 **Split View** 进行多任务处理。
- **Touch ID 支持** - Apple 的 Touch ID 是将指纹用作密码的无缝方式。在启用 Touch ID 的设备上，如果 VPN 服务器允许，Mobile Connect 允许用 Touch ID 替代用户名和密码进行身份验证。用户无需在登录屏幕上手动输入用户名和密码，只需用指尖进行身份验证即可。需要配置有 Touch ID 策略的兼容服务器软件。
- **文件书签** - 除 CIFS 服务器外，FTP 和 SFTP 服务器也支持文件书签。
- **带有 SSO 的 HTML5 书签** - Mobile Connect 支持使用包括 RDP、VNC 和 SSH 的 HTML5 书签的单点登录进行应用内访问。

支持以下第三方应用程序：

- Microsoft 远程桌面
- ServerAuditor
- vSSH

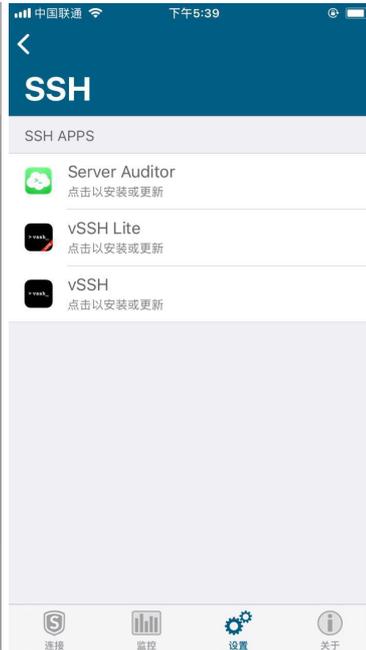
HTML5 书签本身显示在 Mobile Connect 内，并提供无缝和更安全的用户体验，包括对单点登录的支持。

HTML5 书签

本机 HTML5 书签



SSH 书签



RDP 书签



支持的平台

以下各节介绍 Mobile Connect 支持的平台和网络信息：

- 第 6 页的 [Apple 产品支持](#)
- 第 7 页的 [SonicWall 设备支持](#)
- 第 7 页的 [需要的网络信息](#)

Apple 产品支持

以下设备支持 SonicWall Mobile Connect：

- iPhone 8 和 8 Plus - 运行 iOS 11 或更高版本
- iPhone 7 和 7 Plus - 运行 iOS 10 或更高版本
- iPhone 6s 和 6s Plus - 运行 iOS 9 或更高版本
- iPhone 6 和 6 Plus - 运行 iOS 9 或更高版本
- iPhone 5、5c 和 5s - 运行 iOS 9 或更高版本
- iPhone 4 和 4S - 运行 iOS 9 或更高版本
- iPad Pro - 运行 iOS 9 或更高版本
- iPad Air 2 - 运行 iOS 9 或更高版本
- iPad Air（第五代）- 运行 iOS 9 或更高版本

- iPad（第四代）- 运行 iOS 9 或更高版本
- iPad（第三代）- 运行 iOS 9 或更高版本
- iPad 2 - 运行 iOS 9 或更高版本
- iPad mini 4 - 运行 iOS 9 或更高版本
- iPad mini 3 - 运行 iOS 9 或更高版本
- iPad mini（第二代）- 运行 iOS 9 或更高版本
- iPad mini - 运行 iOS 9 或更高版本
- iPod touch（第五代或更高）- 运行 iOS 9 或更高版本

注：使用早期版本的 SonicWall Mobile Connect 并运行 iOS 8 或更低版本的设备不能从 App Store 中更新到 iOS 版的 Mobile Connect 5.0.0，除非它们升级到 iOS 9 或更新版本。

SonicWall 设备支持

SonicWall Mobile Connect 是一个免费的应用程序，但需要以下 SonicWall 解决方案之一的并发用户许可证才能正常运行：

- 包括 TZ、NSA、E 级 NSA 和运行 SonicOS 5.8.1.0 或更高版本的 SuperMassive™ 9000 系列的 SonicWall 防火墙设备
 - 运行 7.5 或更高版本的 SonicWall Secure Mobile Access 100 系列/ SRA 设备
 - 运行 10.7 或更高版本的 SonicWall Secure Mobile Access 1000 系列/ E 级 SRA 设备
- 如要支持 Per App VPN，设备必须运行 SonicWall Secure Mobile Access (SMA) 11.0 或更高版本。

需要的网络信息

如需使用 Mobile Connect，网络管理员或 IT 支持需要以下信息：

- **服务器名称或地址** - 要连接的 SSL VPN 服务器的 IP 地址或 URL。SSL VPN 服务器可以是任何受支持的 SonicWall 设备。请参阅 [SonicWall 设备支持](#)。
- **用户名和密码** - 通常需要输入用户名和密码，但有些连接可能不需要。
- **域名** - SSL VPN 服务器的域名。Mobile Connect 可能会在第一次联系服务器时自动确定，也可能有多个可选择的域。

设备上的 DNS 域设置

在 Mobile Connect 用户能够访问专用网络之前，网络管理员必须在 SonicWall 设备上配置 DNS 域。当 Mobile Connect 用户访问专用网络上的 URL 时，配置的 DNS 域将用于解析主机名查找。对于与配置的 DNS 域不匹配的公共域，将使用 Wi-Fi 或蜂窝网络的 DNS 服务器。

注：Mobile Connect 用户不需要执行与 DNS 相关的任何配置任务。以下的信息适用于 SonicWall 网络管理员。

DNS 域配置流程因所使用的 SonicWall 设备的类型而异：

- **SonicWall 防火墙设备** - 在“SSL VPN > 客户端设置”页面上，在 **DNS 域** 字段中输入 DNS 域名。

- **SonicWall SMA 100 系列/ SRA 设备** - 可以在全局、群组级别或单个用户级别配置 DNS 域：
 - **全局级别** - 在“网络 > DNS”页面上，在 **DNS 域** 字段中输入 DNS 域名。
 - **群组级别** - 在“用户 > 本地群组”页面上，单击该群组的编辑图标。单击 **NetExtender/Mobile Connect** 选项卡，并在 **DNS 域** 字段中输入 DNS 域。
 - **用户级别** - 在“用户 > 本地用户”页面上，单击该用户的编辑图标。单击 **NetExtender/Mobile Connect** 选项卡，并在 **DNS 域** 字段中输入 DNS 域。
- **SonicWall SMA 1000 系列/ E 级 SRA 设备** - 可以全局或为特定的 IP 地址池配置 DNS 域：
 - **全局级别** - 从设备管理控制台 (AMC) 的主导航菜单中，单击**网络设置**。在“名称解析”区域，单击**编辑**。显示“配置名称解析”页面。在**搜索域**字段中输入 DNS 域名。
 - **IP 地址池级别** - 从 AMC 的主导航菜单中，单击**服务**。在“访问服务”下的“网络隧道服务”区域，单击**配置**。显示“配置网络隧道服务”页面。单击要编辑的 IP 地址池的名称。显示“配置 IP 地址池”页面。在“高级”标题右侧，单击  箭头图标。选择自定义默认设置，然后在**搜索域**字段中输入 DNS 域名。

安装和连接

本部分介绍如何在设备上安装 Mobile Connect 以及如何使用 Mobile Connect 配置和启动 VPN 连接。

主题：

- 第 9 页的[安装 Mobile Connect](#)
- 第 10 页的[创建和保存连接](#)
- 第 15 页的[启动连接](#)
- 第 17 页的[配置按需连接](#)
- 第 21 页的[配置受信任的网络检测](#)
- 第 22 页的[使用 Apple Configurator 2 和 Mobile Connect](#)
- 第 25 页的[配置 Per App VPN](#)

安装 Mobile Connect

通过 Apple App Store 安装 SonicWall Mobile Connect。

下载并安装 Mobile Connect 应用程序的步骤如下：

- 1 在 iPhone、iPod touch 或 iPad 上点触 App Store 图标。



- 2 转到“搜索”选项卡，输入 Mobile Connect，然后点触搜索。
- 3 在搜索结果中，选择 Mobile Connect。

- 4 点触免费，然后点触安装。该应用程序安装在设备上。安装完成后，设备上会显示 SonicWall Mobile Connect 图标。



i 注：如果尝试下载 Mobile Connect 时遇到错误，请参阅 iTunes Store 客户支持，您可以在其中找到故障排除步骤和关于如何使用 iTunes 帐户报告问题的描述：
<http://www.apple.com/support/itunes/>。

创建和保存连接

创建 Mobile Connect 连接的流程根据要连接的 SonicWall 设备的类型略有不同。

- 第 10 页的 [创建防火墙或 SMA 100 系列/ SRA 连接](#)
- 第 13 页的 [创建 SMA 1000 系列/ E 级 SRA 连接](#)

创建防火墙或 SMA 100 系列/ SRA 连接

创建并保存到 SonicWall 网络安全设备或 SMA/SRA 的新连接的操作步骤如下：

- 1 第一次启动 Mobile Connect 时，点触添加连接。



- 2 在名称字段中，输入连接的描述性名称。
- 3 在服务器字段中，输入服务器（设备）的 URL 或 IP 地址。

4 点触下一步。Mobile Connect 尝试联系 SonicWall 设备。

- 如果 Mobile Connect 成功联系到设备，则服务器连接将添加到“连接”屏幕上的已保存连接的列表中。
- 如果尝试失败，则会显示警告消息，询问是否要保存连接。确认服务器地址或 URL 拼写正确，然后点触保存。

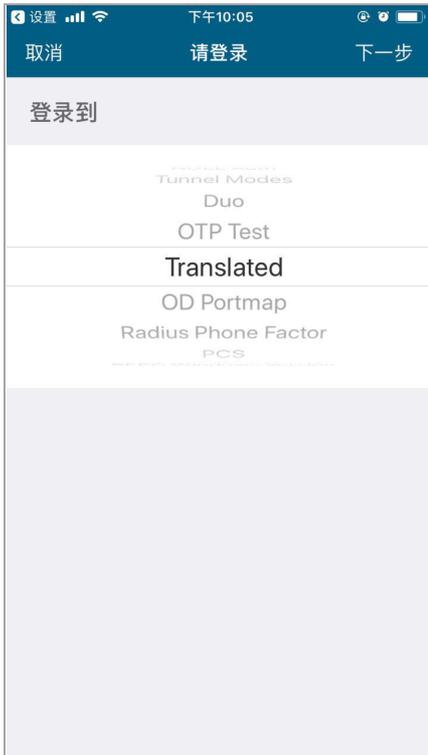


5 如果 Mobile Connect 成功联系到服务器，系统将提示输入用户名和密码，除非服务器不需要这些信息。将凭据输入到用户名和密码字段中。

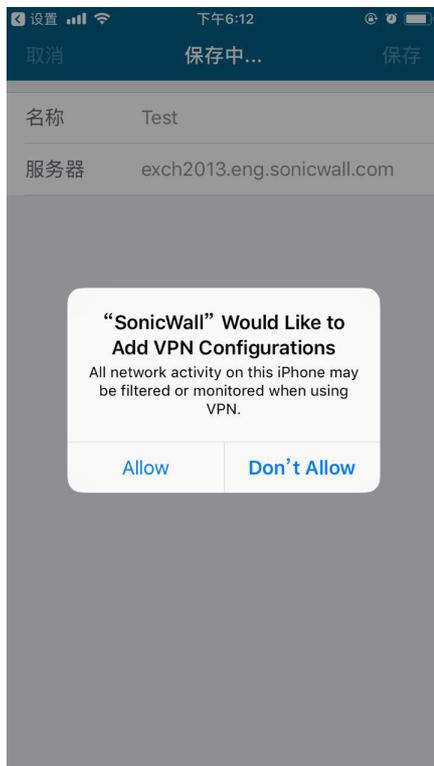


注：如果以前的屏幕截图与设备上显示的内容不匹配，则连接到 SonicWall SMA 1000 系列/ E 级 SRA 设备。请参阅第 13 页的 [创建 SMA 1000 系列/ E 级 SRA 连接](#)。

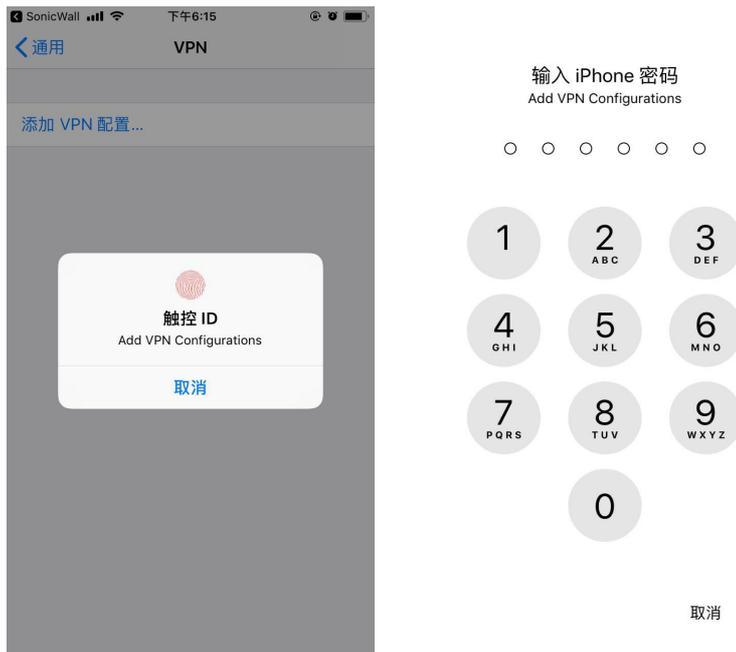
- 6 使用服务器的默认域自动填充域字段。如需选择不同的域，请点触域显示可用选项的下拉菜单，然后选择正确的域。



- 7 点触保存。iOS 可能会显示允许 SonicWall Mobile Connect 添加 VPN 连接的安全提示：



- 8 如果出现提示，请点触允许。iOS 设置应用程序打开，可能会提示输入 Touch ID 或密码来授予权限。



- 9 根据需要输入 Touch ID 或密码。然后显示选择服务器连接的 Mobile Connect “连接”屏幕。

创建 SMA 1000 系列/ E 级 SRA 连接

如需创建并保存到 SonicWall SMA 1000 系列/ E 级 SRA 设备的新连接，请执行以下步骤：

- 1 第一次启动 Mobile Connect 时，点触添加连接。



- 2 在名称字段中，输入连接的描述性名称。

- 3 在**服务器**字段中，输入服务器（设备）的 URL 或 IP 地址。
- 4 点触**下一步**。Mobile Connect 尝试联系 SonicWall 设备。
 - 如果 Mobile Connect 成功联系到设备，则服务器连接将添加到“连接”屏幕上的已保存连接的列表中。
 - 如果尝试失败，则会显示警告消息，询问是否要保存连接。确认服务器地址或 URL 拼写正确，然后点触**保存**。



单击**保存**可将服务器连接添加到“连接”屏幕上的已保存连接的列表中。

启动连接

保存新连接后，“连接”屏幕显示所有已配置连接列表。

“连接”屏幕



启动 **Mobile Connect** 会话的步骤如下：

- 1 点触列表中想要启动的连接。显示“连接”页面。



- 2 点触 **VPN** 开关启用 VPN。

- 3 如果出现提示（取决于连接的设备是否允许保存用户名和密码），请将凭据输入到用户名和密码字段中，然后点触**登录**。
- 4 当成功建立连接时，**状态**行变为**已连接**，VPN 开关处于开启状态。



任何为入口定义的书签都显示在“状态”行的下方。可以通过点触它来启动书签。

- 5 按下 iPhone、iPod touch 或 iPad 上的“Home”按钮以显示其主屏幕。现在可以导航至其他应用程序来访问内联网络。iPhone、iPod touch 或 iPad 顶部的状态栏显示一个 VPN 图标，表示 Mobile Connect 会话仍处于连接状态。



如果 VPN 连接中断，则 VPN 图标会消失，无法再访问内联网络。如果设备连接从无线连接切换到蜂窝或其他网络类型，有可能会发生这种情况。

返回 Mobile Connect 重新建立连接。也可以在“设置”选项卡上配置**自动重新连接**，使 Mobile Connect 自动尝试重新建立中断的连接。

配置按需连接

按需连接功能使 Mobile Connect 在尝试访问专用网络上的域时自动建立 VPN 连接。这将提供无缝的 VPN 连接体验，无需手动启动 Mobile Connect。

注： 按需连接仅适用于到 SonicWall SMA 1000 系列/ E 级 SRA 和 SonicWall SMA 100 系列/ SRA 设备的连接。

请参阅以下章节：

- 第 17 页的[按需连接到 SMA 1000 系列/ E 级 SRA](#)
- 第 18 页的[按需连接到 SMA 100 系列/ SRA](#)

按需连接到 SMA 1000 系列/ E 级 SRA

确定按需连接是否适用于 SMA 1000 系列/ E 级 SRA 连接的最简单方法是在连接 VPN 时查看“连接”屏幕。如果信息指示符  出现在状态行的右侧，则可以在连接时配置按需连接。

信息指示符



SonicWall SMA 1000 系列/ E 级 SRA 设备上的 VPN 配置必须满足以下要求才能支持按需连接：

- 不能将 VPN 隧道配置为“全部重定向”模式。
- 必须将领域配置为使用客户端证书进行身份验证。连锁身份验证（使用第二个身份验证服务器）不支持按需连接。
- 必须存在一个有效的领域客户端证书。
- 用户必须至少有一次成功连接到设备。

如果 Mobile Connect 应用程序未运行，并且 VPN 连接尝试成功需要用户交互，则按需 VPN 可能无法连接。可能需要用户交互的一些场景包括以下内容：

- VPN 服务器的 SSL 证书是不受信任的。
- 个人设备授权在服务器上已启用，并且该设备尚未获得授权。
- 需要双因素用户身份验证，例如一次性密码。

按需连接到 SonicWall SMA 1000 系列/ E 级 SRA 的步骤如下：

- 1 在显示“按需连接”屏幕的“连接”选项卡上的“状态”行中，点触信息指示符 ⓘ 。



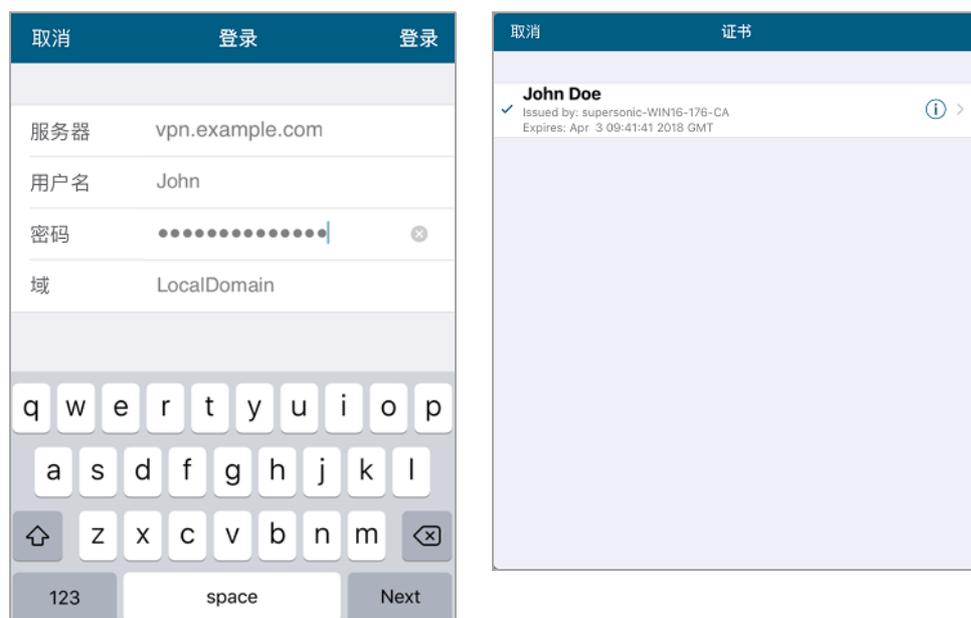
- 2 点触按需连接。
- 3 将域列表设置为以下之一：
 - a 当访问具有任何所列域后缀的资源时，将域列表设置为需要时连接使 Mobile Connect 建立 VPN 连接。
 - b 将域列表设置为从不连接以禁用所列域后缀的按需连接。
- 4 如果列出了多个域，则可以通过点触域名来启用单个域的按需连接。

ⓘ | 注：iOS 中不再支持始终连接域。它们的行为与需要时连接相同。

按需连接到 SMA 100 系列/ SRA

在 SonicWall SMA 100 系列/ SRA 设备上，除标准用户名和密码身份验证外，客户端证书身份验证还可用作第二个因素身份验证方法。如果在身份验证中需要客户端证书，则会自动提示用户从 iOS 设备中选择一个客户端证书。

选择证书



点触显示在客户端证书右侧的信息指示符 ⓘ，将显示该客户端证书的其他详细信息。

证书详细信息



默认情况下，VPN 配置使用**登录时选择**作为客户端证书设置。

为了支持按需连接，SonicWall SMA 100 系列/ SRA 设备上的 VPN 配置必须满足以下要求：

- 必须启用在域或用户级别配置的用户的有效客户端证书实施策略才能使用客户端证书进行身份验证。

- 用户的有效用户名和密码缓存策略（在全局、群组或用户级别配置）必须设置为允许保存用户名和密码。
- 用户的有效客户端证书必须存在于 iOS 设备上。
- iOS VPN 连接配置文件必须配置用户名和密码，并且必须选择合适的客户端证书。

配置到 SonicWall SMA 100 系列/ SRA 的按需连接的步骤如下：

- 1 在“编辑连接”屏幕上点触**证书**。
- 2 从列表选择一个客户端证书。

显示按需连接设置。



- 3 在“编辑连接”屏幕上点触**按需连接**以启用按需连接，并显示“按需连接”屏幕。
- 4 在“按需连接”屏幕上，访问具有任何所列域后缀的资源时，将**域列表**设置为**需要时连接**以使 Mobile Connect 建立 VPN 连接。

将**域列表**设置为**从不连接**会禁用所列域后缀的按需连接。



5 如果列出了多个域，请点触域名以启用单个域的按需连接。

① | 注：iOS 中不再支持始终连接域。它们的行为与需要时连接相同。



配置受信任的网络检测

iOS 按需连接功能的 Apple 受信任的网络检测 (TND) 增强功能具有以下属性：

- 只能与按需连接一起使用。
- 通过确定用户是否在可信网络上扩展按需连接功能。
- 使用 Apple Configurator 2 进行配置。
- 仅用于无线连接。在其他类型的网络连接上进行操作时，按需连接不使用 TND 来确定是否应该连接 VPN。

按需连接会在用户尝试访问具有在域列表中指定的主机名的目标时启动 VPN 连接。例如，如果 ***.example.com** 在 **始终连接** 列表中，当用户访问 **internal.example.com** 时，不管设备当前连接到哪个网络，客户端都会启动 VPN 连接。TND 比较 VPN 和本地 DNS 服务器以及 DNS 后缀，以确定是否使用 Mobile Connect 并连接 VPN，如下表所示：

DNS 比较和对登录的影响

DNS 后缀	DNS 服务器	登录
无	无	拒绝 - 无 VPN
无	相同	拒绝 - 无 VPN
相同	相同	拒绝 - 无 VPN
相同	相同和其他	已允许
相同	不同	已允许
不同	相同	已允许
部分匹配	部分匹配	已允许

部分匹配意味着如果为 TND 配置了两台 DNS 服务器，但只有一台 DNS 服务器与实际的网络环境相匹配，则仍然允许登录。

有关受信任的网络监测和按需连接的更多信息，请参阅 Apple Inc. 的文档。

如需确定 TND 是否可用于您的连接，请点触“连接”选项卡上“状态”行中的信息指示符。这将显示用于启用/禁用 TND 的受信任的网络按钮（如果可用）。

“受信任的网络”按钮



配置 TND 的步骤如下：

- 1 点触“连接”选项卡上“状态”行中的信息指示符 ⓘ >。
- 2 请确保已打开按需连接。
- 3 打开受信任的网络。

ⓘ | 注：受信任的网络检测仅适用于到 SonicWall SMA 1000 系列/E 级 SRA 设备的连接。

使用 Apple Configurator 2 和 Mobile Connect

Apple Configurator 2 使任何人都可以轻松地在商业和教育中批量配置和部署 iPhone、iPad 和 iPod touch。通过该软件，企业环境的管理员能够为 iOS 设备创建配置文件，为企业策略预配置设备设置，例如 VPN 配置、安全策略、无线设置等。

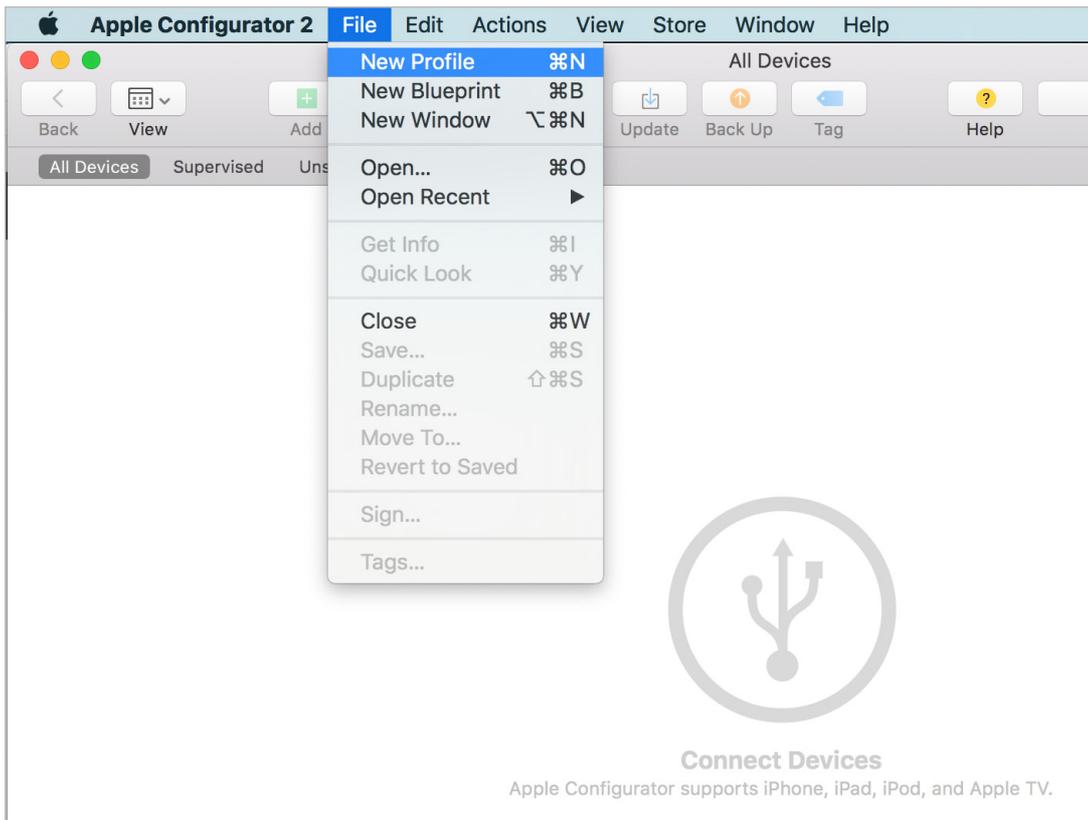
Apple Configurator 2 使管理员能够为其用户的 iOS 设备配置 Mobile Connect 配置文件。有关安装和使用 Apple Configurator 2 的信息，请访问：

<https://support.apple.com/en-us/HT205285>

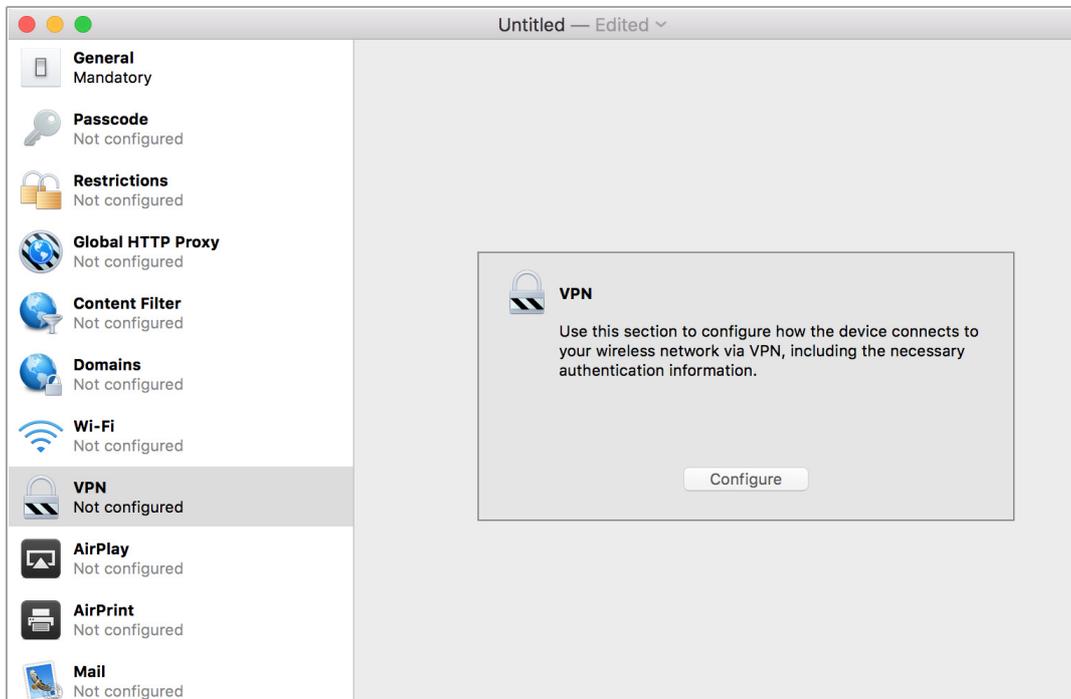
使用 Apple Configurator 2 配置 Mobile Connect 配置文件的步骤如下：

- 1 下载，安装并启动 Apple Configurator 2。

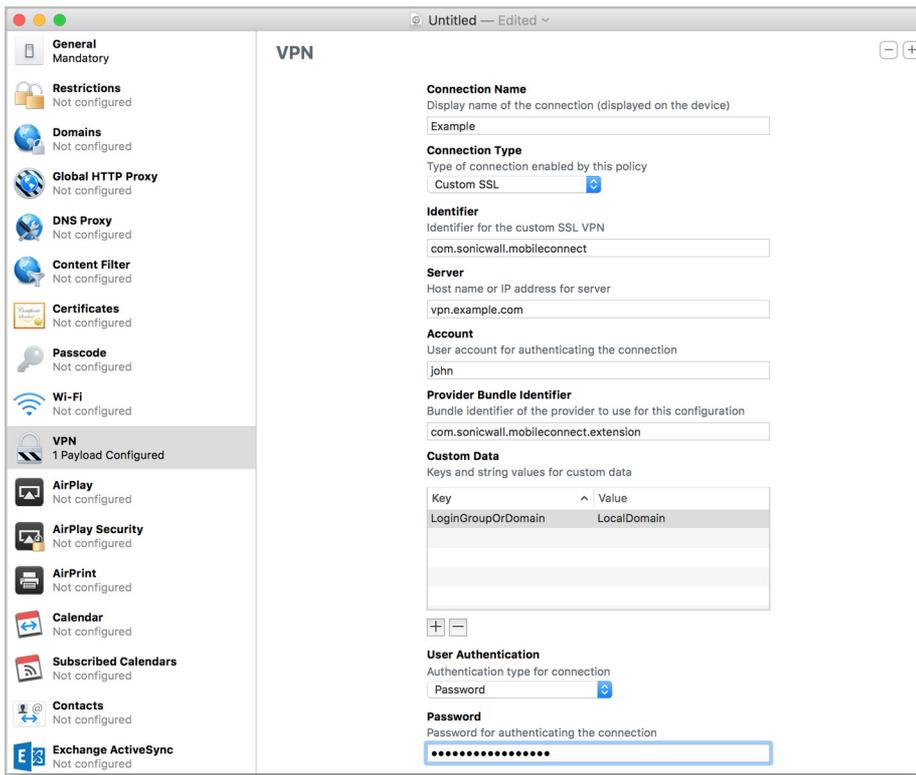
- 单击文件 > 新建描述文件。



- 选择 **VPN**，然后点触配置。



4 在连接名称字段中，输入连接的名称。



5 在连接类型下拉菜单中，选择自定义 SSL。

注： SonicWall Mobile Connect 选项适用于 Mobile Connect 4.0 及更早版本，不适用于 Mobile Connect 5.0 或更新版本。必须使用自定义 SSL 类型。

6 在标识符字段中，输入 com.sonicwall.mobileconnect。

7 在服务器字段中，输入 SonicWall 设备的主机名或 IP 地址。

8 （可选）在帐户字段中，输入帐户的用户名。

9 在供应商包标识符字段中，输入 com.sonicwall.mobileconnect.extension。

10 （可选）自定义数据部分可用于配置 **LoginGroupOrDomain** 密钥和值，该值取决于连接所使用的设备类型：

- 对于连接到 SonicWall 防火墙或 SMA 100 系列/SRA 设备的描述文件，请在值列中输入域名称。域的名称显示在 Mobile Connect 应用程序的编辑连接屏幕中。
- 对于连接到 SonicWall SMA 1000 系列/E 系列 SRA 设备的描述文件，请在值列中输入登录群组名称。在 Mobile Connect 中启动连接时，登录群组与在登录屏幕中选择的字段相同。

11 在用户验证下拉菜单中，选择密码。

12 （对到防火墙或 SMA 100 系列/SRA 设备的连接为可选）在密码字段中，如果要连接的 SonicWall 设备配置为允许保存密码，请输入用户帐户的密码。

注： 只有 SonicWall 防火墙或 SMA 100 系列/SRA 设备才能存储密码。SonicWall SMA 1000 系列/E 级 SRA 设备不能存储密码。

13 （可用于到 SonicWall SMA 1000 系列/ E 级 SRA 设备的连接）如果使用代理服务器进行连接，请在代理下拉菜单中选择手动或自动。如果不使用代理服务器，请将此设置保留为无。

i 注：只有 SonicWall SMA 1000 系列/E 级 SRA 设备支持通过代理的 Mobile Connect。目前，SonicWall 防火墙和 SMA 100 系列/ SRA 设备不支持通过代理的 Mobile Connect。

配置 Per App VPN

本节介绍 Mobile Connect 如何支持 iOS Per App VPN 功能。仅到已为应用程序访问控制配置的 SMA 1000 系列设备的 Mobile Connect VPN 连接支持 Per App VPN。

Per App VPN 需要使用移动设备管理 (MDM) 解决方案。另外，Per App VPN 通过 MDM 管理的 Web 列表仅由 MDM 管理的应用程序以及 Safari 支持。请参阅 MDM 解决方案提供商的文档，了解如何使用其解决方案配置 Per App VPN。

以下是使用 Per App VPN 和 Mobile Connect 的已知限制：

- 如果 MDM 解决方案未成功安装管理的应用程序并为管理的应用程序配置 Per App VPN 规则，则应用程序访问控制区域分类可能会失败。
- 连接到 SMA 1000 系列设备时，不会为 MDM 管理的 VPN 连接安装自定义 VPN 连接。
- 如果在 SMA 1000 系列设备上启用了设备授权，VPN 按需连接可能无法连接。这是因为应用程序中需要用户交互。

设置、书签和文件

本节介绍可从 Mobile Connect 中的“设置”屏幕访问的可配置元素，包括连接设置、URL 控制、书签和文件书签。

主题：

- 第 26 页的 [设置概述](#)
- 第 29 页的 [URL 控制语法和参数](#)
- 第 33 页的 [使用书签](#)
- 第 37 页的 [使用文件](#)

设置概述

SonicWall Mobile Connect 为连接和日志记录选项提供了一些设置。“设置”屏幕还提供支持信息，其中包括用户指南和设备信息。

“设置”页面



可用的设置和选择如下所述：

- 第 27 页的 [设置部分](#)
- 第 28 页的 [支持部分](#)

设置部分

以下选项由“设置”屏幕的 **设置部分** 进行控制：

- **启动时连接** - 对 Mobile Connect 进行设置，使其在启动应用程序时自动启动与上次使用的配置文件的连接。
- **自动重新连接** - 对 Mobile Connect 进行设置，使其在连接丢失时自动尝试重新连接。如果设备连接切换到不同的网络类型（例如，从无线网络切换到蜂窝网络），SSL VPN 连接可能会中断。此设置可让应用程序依靠持续的 VPN 连接。对重新连接所用的时间没有限制。
- **URL 控制** - 允许其他移动应用程序使用特殊 URL 将操作请求传递给 Mobile Connect。这些操作请求可以创建 VPN 连接条目并连接或断开 VPN 连接。例如，另一个应用程序可以启动 Mobile Connect，根据需要访问内部资源，然后使用 `mobileconnect://` 或 `sonicwallmobileconnect://` URL 方案断开连接。

有关 URL 控制的附加信息，请参阅第 29 页的 [URL 控制语法和参数](#)。

- **Touch ID** - 对 Mobile Connect 进行设置，使其在进行用户名/密码身份验证期间提示需要 Touch ID。需要连接到配置了 Touch ID 策略的服务器。
- **书签** - 显示集中配置的 VPN 资源（如 URL、Outlook Web Access 和 iOS 应用程序）快捷方式，称为书签。当连接 VPN 时，这些书签显示在主“连接”选项卡上，提供对常用应用程序的一键式访问。

如果使用 SMA 100 系列/SRA 设备，请向下拉动并释放“连接”屏幕以刷新书签。只要服务器书签和第三方 iOS 应用程序都支持，则 Mobile Connect 支持“远程桌面”选项（如屏幕尺寸）以及启用/禁用音频。

注：只有运行版本 7.5 或更高版本的 SonicWall SMA 100 系列/SRA 设备以及运行 SonicOS 5.9.0.2 和更高版本的下一代防火墙设备才支持书签。

有关书签的附加信息，请参阅第 33 页的 [使用书签](#)。

- **文件** - 删除已下载并存储在设备上的所有缓存文件。请注意，缓存的文件在设备上进行了加密以增强安全性。

注：只有运行 7.5 或更高版本的 SonicWall SMA 100 系列/SRA 设备支持文件功能，运行 SonicOS 的设备上不支持文件功能。

有关文件的附加信息，请参阅第 37 页的 [使用文件](#)。

- **日志** - 用于两个目的：
 - 启用 Mobile Connect 活动的完整调试日志消息。除非 SonicWall 支持人员指导启用此设置，否则请将此部分禁用。
 - 删除已保存在此设备上的所有日志文件。

SMA 1000 系列/ E 级 SRA 的附加设置

针对与 SonicWall SMA 1000 系列/ E 级 SRA 设备的连接，可以修改两个附加选项。

查看这些选项的步骤如下：

- 1 转到连接选项卡，点触连接线以显示连接列表。
- 2 点触要修改连接左侧的信息指示符。

显示“编辑连接”屏幕。



可以配置以下选项：

- 记住凭证 - 启用保存 VPN 连接的用户身份验证凭证。默认情况下处于启用状态，可以通过 SonicWall SMA 1000 系列/E 级 SRA 服务器配置进行控制。
 - 忘记此登录群组 - Mobile Connect 会记住在配置连接时指定的登录群组。如需更改为其他登录群组，请点触忘记此登录群组。下次连接到服务器时，系统会提示您选择一个新的登录群组。
- 注：** 如果未显示这些选项，则连接到 SonicWall 防火墙或 SMA 100 系列/SRA 设备。

支持部分

“设置”屏幕的支持部分中提供以下选择：

- 用户指南 - 显示 SonicWall Mobile Connect 用户指南。
- 设备信息 - 显示有关 iOS 设备、无线连接、蜂窝连接、蓝牙连接和 DNS 服务器的信息。
- 电子邮件日志 - 创建一封将 Mobile Connect 日志文件发送给 SonicWall 支持人员的电子邮件。点触发送以发送电子邮件。

URL 控制语法和参数

本部分提供了 URL 控制功能的全部 URL 参数。URL 控制当前支持 `addprofile`、`connect` 和 `disconnect` 命令。也支持回调 URL。

主题：

- 第 29 页的[使用 `addprofile` 命令](#)
- 第 30 页的[使用 `connect` 命令](#)
- 第 31 页的[使用 `disconnect` 命令](#)
- 第 31 页的[使用 `callbackurl` 命令参数](#)

使用 `addprofile` 命令

`addprofile` 命令需要名称或服务器参数，并且适用两者。所有其他参数是可选的。在 Mobile Connect 中打开 URL 时，URL 中包含的所有参数都将保存在与该名称和服务器关联的连接条目中。

语法：

```
mobileconnect://addprofile[/]?name=ConnectionName&server=ServerAddress  
[&Parameter1=Value&Parameter2=Value...]
```

`addprofile` 命令参数

命令参数	说明
名称	创建并显示在 Mobile Connect 连接列表中的 VPN 连接条目的唯一名称。只有在唯一的情况下，Mobile Connect 才接受该名称。区分大小写。
服务器	希望连接的 SonicWall 设备的域名或 IP 地址。例如： <code>vpn.example.com</code>
用户名	可选：VPN 连接中使用的用户名。
密码	可选：VPN 连接中使用的密码。
领域	可选：VPN 连接配置文件中使用的领域。仅适用于 SMA 1000 系列/E 级 SRA 连接。
域	可选：VPN 连接配置文件中使用的域。仅适用于 SMA 100 系列/SRA 和防火墙连接。
sessionid	可选：用于身份验证的会话 ID 或小组 ID。
连接	可选：如果显示并且值为非空，则在成功添加配置文件时启动连接。
callbackurl	可选：在处理完 <code>addprofile</code> 命令之后，要由 Mobile Connect 打开的回调 URL。有关回调 URL 语法和选项的完整详细信息，请参阅第 31 页的 使用 <code>callbackurl</code> 命令参数 。

示例：

以下是 `addprofile` 命令的示例：

```
mobileconnect://addprofile/?name=Example&server=vpn.example.com
```

```
sonicwallmobileconnect://addprofile/?name=Example&server=vpn.example.com
```

```
mobileconnect://addprofile?name=Example%20&server=vpn.example.com
mobileconnect://addprofile?name=vpn.example.com
mobileconnect://addprofile?server=vpn2.example.com
mobileconnect://addprofile?name=SRA%20Connection&server=sslvpn.example.com
&username=test&password=password&domain=LocalDomain&connect=1
mobileconnect://addprofile?name=EX%20Connection&server=workplace.example.com
&username=test&password=password&realm=Corp&connect=1
```

① | 注：URL 中使用的参数值中的所有适当字符都需要进行 URL 编码。例如，如需匹配空格，请输入 %20。

使用 connect 命令

connect 命令用于轻松建立 VPN 连接。连接信息可以嵌入到 URL 中，可以提供给用户进行简单的设置和配置。此外，还可以提供一个回调 URL，在连接尝试完成后由 Mobile Connect 打开，使其他应用程序能够无缝启动 VPN 连接。

语法：

```
mobileconnect://connect[/]?[name=ConnectionName|server=ServerAddress]
[&Parameter1=Value&Parameter2=Value...]
```

connect 命令参数

命令参数	说明
名称	创建并显示在 Mobile Connect 连接列表中的 VPN 连接条目的唯一名称。只有在唯一的情况下，Mobile Connect 才接受该名称。区分大小写。
服务器	希望进行连接的 SonicWall 设备的域名或 IP 地址。例如：vpn.example.com
用户名	可选：VPN 连接中使用的用户名。
密码	可选：VPN 连接中使用的密码。
领域	可选：VPN 连接配置文件中使用的领域。仅适用于 SMA 1000 系列/E 级 SRA 连接。
域	可选：VPN 连接配置文件中使用的域。仅适用于 SMA 100 系列/SRA 和防火墙连接。
sessionid	可选：用于身份验证的会话 ID 或小组 ID。
连接	可选：如果显示并且值为非空，则在成功添加配置文件时启动连接。
callbackurl	可选：回调 URL 在处理完 connect 命令后由 Mobile Connect 打开。有关 callbackurl 语法和选项的完整详细信息，请参阅第 31 页的 使用 callbackurl 命令参数 。

示例：

以下是 connect 命令的示例：

```
mobileconnect://connect/?name=Example
sonicwallmobileconnect://connect/?name=Example
mobileconnect://connect?name=Example
```

```
mobileconnect://connect?server=vpn.example.com
mobileconnect://connect?name=Example%20&server=vpn.example.com
mobileconnect://connect?name=SRA%20Connection&server=sslvpn.example.com
&username=test&password=password&domain=LocalDomain
mobileconnect://connect?name=EX%20Connection&server=workplace.example.com
&username=test&password=password&realm=Corp
```

使用 disconnect 命令

disconnect 命令用于断开活动的连接。此外，还可以提供一个回调 URL，在连接断开后由 Mobile Connect 打开，就可以返回主叫应用程序。如果没有有效的 VPN 连接，则忽略 disconnect 命令。

语法：

```
mobileconnect://disconnect[/]
mobileconnect://disconnect[/]?[callbackurl=CallBackURL]
```

disconnect 命令参数

命令参数	说明
callbackurl	可选：在处理 disconnect 命令后，为 callbackurl 定义的 URL 由 Mobile Connect 打开。有关 callbackurl 语法和选项的完整详细信息，请参阅第 31 页的 使用 callbackurl 命令参数 。

示例：

以下是 disconnect 命令的示例：

```
mobileconnect://disconnect
mobileconnect://disconnect/
sonicwallmobileconnect://disconnect
mobileconnect://disconnect?callbackurl=customapp%3A%2F%2Fhost%3Fstatus%3D%24STATUS%24%26login_group%3D%24LOGIN_GROUP%26error_code%3D%24ERROR_CODE%24
sonicwallmobileconnect://disconnect?callbackurl=customapp%3A%2F%2Fhost%3Fstatus%3D%24STATUS%24%26login_group%3D%24LOGIN_GROUP%26error_code%3D%24ERROR_CODE%24
```

使用 callbackurl 命令参数

callbackurl 是每个 connect/disconnect/addprofile 命令的可选查询字符串参数。如果一个回调 URL 包含在一个命令中，当该命令完成时，该 URL 将由 Mobile Connect 启动。在使用 URL 调用 Mobile Connect 时，第三方应用程序可以使用 callbackurl 参数来包含要由 Mobile Connect 启动的 URL。

callbackurl 值可以包含特殊令牌，Mobile Connect 将评估并动态替换这些特殊令牌，以将额外的状态和连接信息提供给由回调 URL 打开的应用程序。令牌按照指定令牌的顺序进行就地评估。

为确保其正常运行，基础 callbackurl URL 值格式应符合 RFC 1808 的要求，并应能独立于 Mobile Connect 启动。例如，它应该通过网页或 iOS web clip 启动。

URL 语法：

<scheme>://<net_loc>/<path>;<params>?<query>#<fragment>

注：必须对 callbackurl 的 URL 值进行正确的 URL 编码，以确保 Mobile Connect 能够正确处理回调 URL。URL 中使用的参数值中的所有适当字符都需要进行 URL 编码。例如，如需匹配空格，请输入 %20。

可以在 URL 的 <query> 元素中指定表 **callbackurl 支持的动态令牌** 的任意数量的动态令牌。管理员可以在网站上配置回调 URL 或向其用户发送电子邮件时使用这些功能，例如自动配置 VPN 配置文件。动态令牌很有用，因为其允许 Mobile Connect 向打开回调 URL 时正在启动的网站或应用程序提供信息。

callbackurl 支持的动态令牌

动态令牌	说明
\$ERROR_CODE\$	失败连接尝试的错误的数值。
\$ERROR_MESSAGE\$	失败连接尝试的错误消息的字符串值。
\$LOGIN_GROUP\$	身份验证登录群组或领域的字符串值。仅适用于 SMA 1000 系列/E 级 SRA 连接。
\$COMMUNITY\$	身份验证团体的字符串值。仅适用于 SMA 1000 系列/E 级 SRA 连接。
\$ZONE\$	EPC（终端控制）区域的字符串值。仅适用于 SMA 1000 系列/E 级 SRA 连接。
\$TUNNEL_IP\$	Mobile Connect IPv4 客户端地址的字符串值。
\$TUNNEL_MODE\$	根据隧道模式，取 split、split-nonlocal、redirectall 或 redirectall-nonlocal 之一。仅适用于 SonicWall SMA 1000 系列/E 级 SRA 连接。
\$ESP_ENABLED\$	根据 ESP（封装安全有效负载）是否启用，取是或否之一。仅适用于 SonicWall SMA 1000 系列/E 级 SRA 连接。 ESP 是一份用于提供机密性、数据源验证、无连接完整性、反重放服务（一种局部序列完整性）和有限的流量保密性的协议。

示例：

以下是使用 callbackurl 的示例：

回调 URL (1):

```
customapp://host?status=$STATUS&login_group=$LOGIN_GROUP&error_code=$ERROR_CODE$
```

对应的带有使用 URL 编码的 callbackurl 值的完整 URL:

```
mobileconnect://connect?sessionid=<teamid>&callbackurl=customapp%3A%2Fhost%2Fstatus%3D%24STATUS%24%26login_group%3D%24LOGIN_GROUP%26error_code%3D%24ERROR_CODE%24
```

回调 URL (2):

```
myapp://callback?status=$STATUS&login_group=$LOGIN_GROUP&error_code=$ERROR_CODE$
```

对应的带有使用 URL 编码的 callbackurl 值的完整 URL:

```
mobileconnect://connect?sessionId=<teamid>&callbackurl=myapp%3A%2F%2Fcallback
%3Fstatus%3D%24STATUS%24%26login_group%3D%24LOGIN_GROUP%26error_code%3D%24
ERROR_CODE%24
```

回调 URL (3):

```
http://server/example%20file.html
```

对应的带有使用 URL 编码的 callbackurl 值的完整 URL:

```
mobileconnect://connect?callbackurl=http%3A%2F%2Fserver%2Fexample%20file.html
```

使用书签

主题:

- 第 33 页的[显示和过滤书签](#)
- 第 34 页的[支持的书签类型](#)

显示和过滤书签

Mobile Connect 连接屏幕显示已配置的书签。当书签数量多于五个时，可以通过点触显示的显示：<书签类型>行过滤书签列表。借此您可以按类型过滤书签的长列表。选择要显示的书签类型，或选择全部显示所有书签。

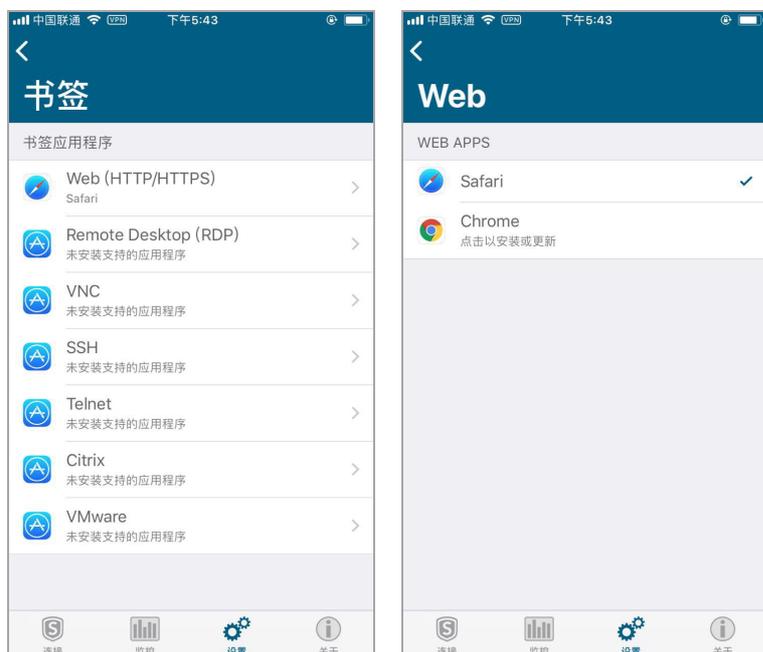
显示书签



选择未安装的应用程序书签会提示安装该应用程序。也可以随时使用设置 > 书签屏幕进行安装书签引用的应用程序。

除了安装书签应用程序外，**设置 > 书签**屏幕也可用于选择和安装支持多个第三方应用程序的书签应用程序。例如，可以将 Safari 和 Google Chrome 选作 Web 书签。

带有多个应用程序的 Web 书签



支持的书签类型

本节介绍 Mobile Connect 支持的书签类型和相关应用程序。

注：在 Mobile Connect iOS 5.0 中，SonicWall SMA 1000 系列/E 级 SRA 设备仅支持 Web 和桌面书签。

主题：

- 第 34 页的 **桌面书签**
- 第 36 页的 **Web 书签**
- 第 36 页的 **Mobile Connect 书签**
- 第 37 页的 **终端书签**

桌面书签

桌面书签有一个显示在用户入口的名称和一个内部类型。

支持以下几种类型的桌面书签：

- 第 35 页的 **RDP 书签**
- 第 35 页的 **VNC 书签**
- 第 36 页的 **Citrix 书签**

RDP 书签

RDP 书签入口名称和内部类型

入口名称	内部类型
终端服务 (RDP - ActiveX)	RDP5ActiveX
终端服务 (RDP - Java)	RDP5Java
终端服务 (RDP - HTML5)	RDP5HTML5

i | 注：RDP (HTML5) 书签在 Mobile Connect 内启动，不会启动第三方应用程序。

RDP 书签类型尝试使用关联的 RDP 应用程序启动，如设置屏幕中的配置。请参阅表 [RDP 应用程序和版本](#)。

RDP 应用程序和版本

应用程序	iOS 版本
Microsoft 远程桌面	8.1.35
Parallels Client (旧 2X)	15.0.3883

应将屏幕分辨率等其他细节提供给客户。但是，支持传递这样的参数根据应用程序而有所不同。例如：

- Parallels 2X Client 不接受 iOS 上的屏幕分辨率设置

VNC 书签

VNC 书签入口名称和内部类型

入口名称	内部类型
虚拟网络计算 (VNC)	VNC
虚拟网络计算 (VNC - HTML5)	VNCHTML5

i | 注：VNC (HTML5) 书签在 Mobile Connect 内启动，不会启动第三方应用程序。

VNC 书签类型尝试使用关联的 VNC 应用程序启动，如设置屏幕中的配置。

VNC 应用程序和版本

应用程序	iOS 版本
远程 VNC	4.8.10

应将屏幕分辨率等其他细节提供给客户。但是，支持传递这样的参数根据应用程序而有所不同。

Citrix 书签

Citrix 书签入口名称和内部类型

入口名称	内部类型
Citrix 入口 (Citrix)	Citrix
Citrix 入口 (Citrix)	Citrix_https

Citrix 书签类型尝试使用关联的 Citrix 应用程序启动。

Citrix 应用程序和版本

应用程序	iOS 版本
Citrix Receiver	7.3

应将屏幕分辨率等其他细节提供给客户。但是，支持传递这样的参数根据应用程序而有所不同。

Web 书签

Web 书签有一个显示在用户入口的名称和一个内部类型。

Web 书签入口名称和内部类型

入口名称	内部类型
Web (HTTP)	HTTP
安全 Web (HTTPS)	HTTPS
外部 Web 站点	URL
外部 Web 站点	URL_https

这些书签会在关联的 Web 浏览器中启动，并且提供的“名称或 IP 地址” (HostID) 作为参数显示在浏览器中。

浏览器类型和版本

浏览器类型	iOS 版本
任何浏览器	-
Safari	是
Google Chrome	61.0.3163.73

Mobile Connect 书签

Mobile Connect 书签有一个显示在用户入口的名称和一个内部类型。

Mobile Connect 书签入口名称和内部类型

入口名称	内部类型
Mobile Connect	MC

Mobile Connect 书签类型完全依靠操作系统来确定并启动正确的应用程序。书签要正确配置以启动。Mobile Connect 应用程序尝试按原样启动它。（例如，telnet://server）。

终端书签

终端书签有一个显示在用户入口的名称和一个内部类型。

终端书签入口名称和内部类型

入口名称	内部类型
Telnet	Telnet
Telnet (HTML5)	TelnetHTML5
Secure Shell 版本 1 (SSHv1)	SSH
Secure Shell 版本 2 (SSHv2)	SSHv2
Secure Shell 版本 2 (HTML5)	SSHv2HTML5

注： Telnet (HTML5) 和 SSH (HTML5) 书签在 Mobile Connect 内启动，不启动第三方应用程序。

应用程序和版本是：

终端应用程序和版本

应用程序	iOS 版本
ServerAuditor	2.2.2
vSSH	1.11
vSSH Lite	1.11

使用文件

Mobile Connect 5.0 支持通过文件书签对文件进行安全移动访问。文件书签通过首先检查并执行服务器配置的文件策略，然后在 Mobile Connect 应用程序中安全地下载和显示文件，从而实现对文件的安全访问。

服务器配置的策略包括控制文件是否可以打印、复制到剪贴板、在第三方应用程序中打开或安全地缓存在 iOS 设备上。文件书签也可以创建到文件夹或文件共享根目录，以允许目录导航。

注： 在 iOS 版的 Mobile Connect 5.0 中，只有具有 SRA 7.5 或更高版本固件的 SonicWall SMA 100 系列/SRA 设备才支持文件书签。在未来的版本中，SMA 1000 系列/E 级 SRA 和下一代防火墙设备将支持文件书签。

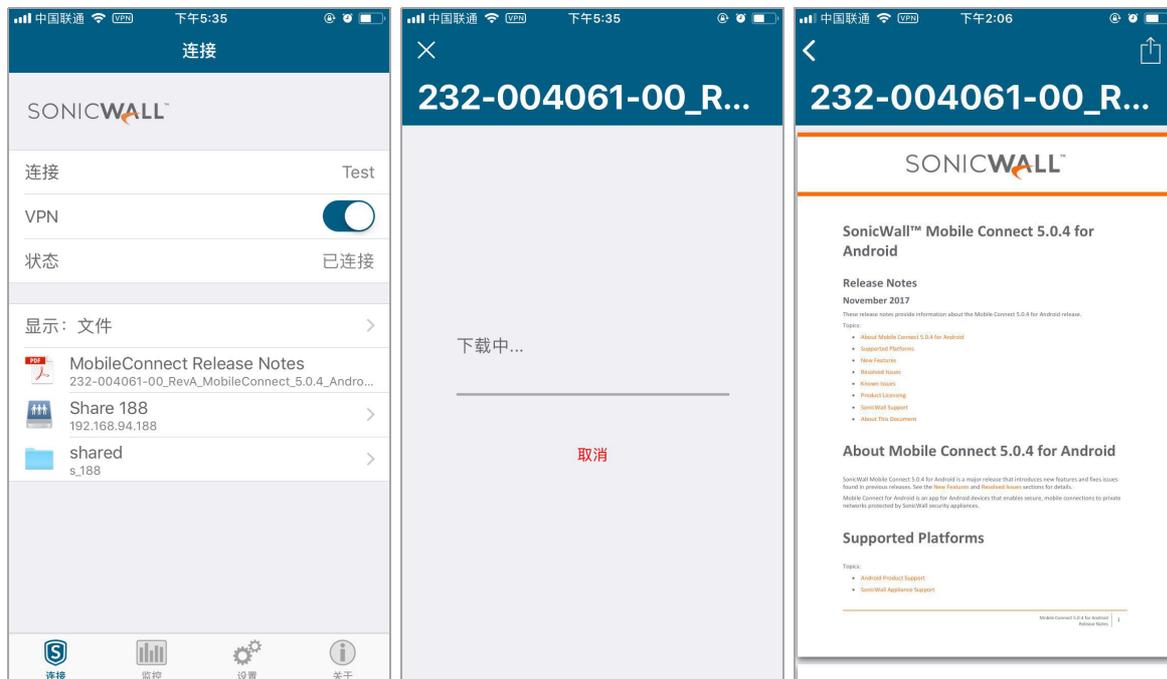
在服务器设备上为用户配置文件书签时，它们会在建立 VPN 后出现在书签列表中，并且可以在书签数量多于五个时通过显示的**显示：文件行**进行过滤。请参阅[显示文件书签](#)。

显示文件书签



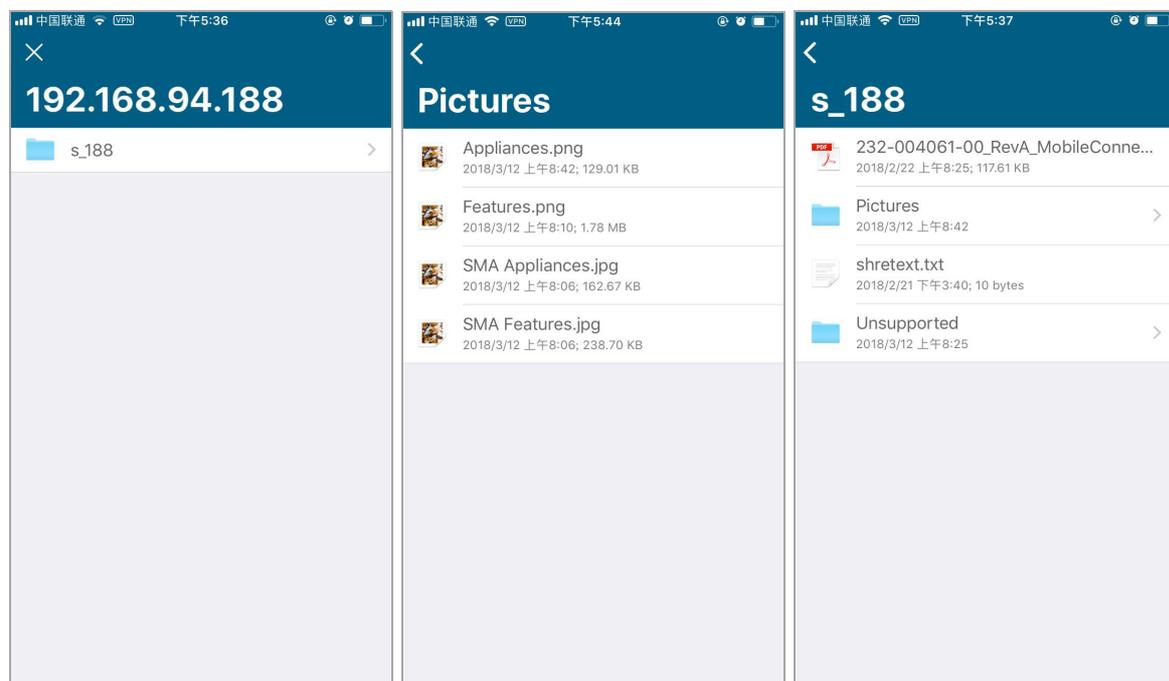
选择文件书签可以查询服务器，并执行服务器上为该文件书签配置的所有文件策略。如果文件尚未在设备上缓存，则可以从 SMA 100 系列/ SRA 设备中安全地下载该文件。文件下载后，将显示在 Mobile Connect 应用程序中。请参阅[使用文件书签下载文件](#)。

使用文件书签下载文件



选择到文件夹或目录的文件书签允许目录浏览，包括下载和查看文件夹中的任何文件。每次尝试浏览文件夹或查看文件都会查询服务器实施访问策略。请参阅[浏览文件夹和查看文件](#)。

浏览文件夹和查看文件



有关支持的文件类型和可以对文件执行的其他操作的信息，请参阅第 39 页的[文件功能](#)。

文件功能

这些功能支持多种文件类型，允许对通过文件书签访问的文件执行许多重要功能。

请参阅以下章节：

- 第 39 页的[支持的文件类型](#)
- 第 40 页的[不支持的文件类型](#)
- 第 40 页的[文件策略和操作](#)

支持的文件类型

Mobile Connect 支持 Apple iOS 原生支持的文件类型，如表[支持的文件类型](#)所示。

支持的文件类型

文件类型	文件扩展名
图像	.jpg、.jpeg、.tif、.tiff、.png
音乐	.mp3、.m4a、.wav
电影	.mov、.mp4
Microsoft Word 文档	.doc、.docx
Microsoft Excel 电子表格	.xls、.xlsx
Microsoft PowerPoint 演示文稿	.ppt、.pptx

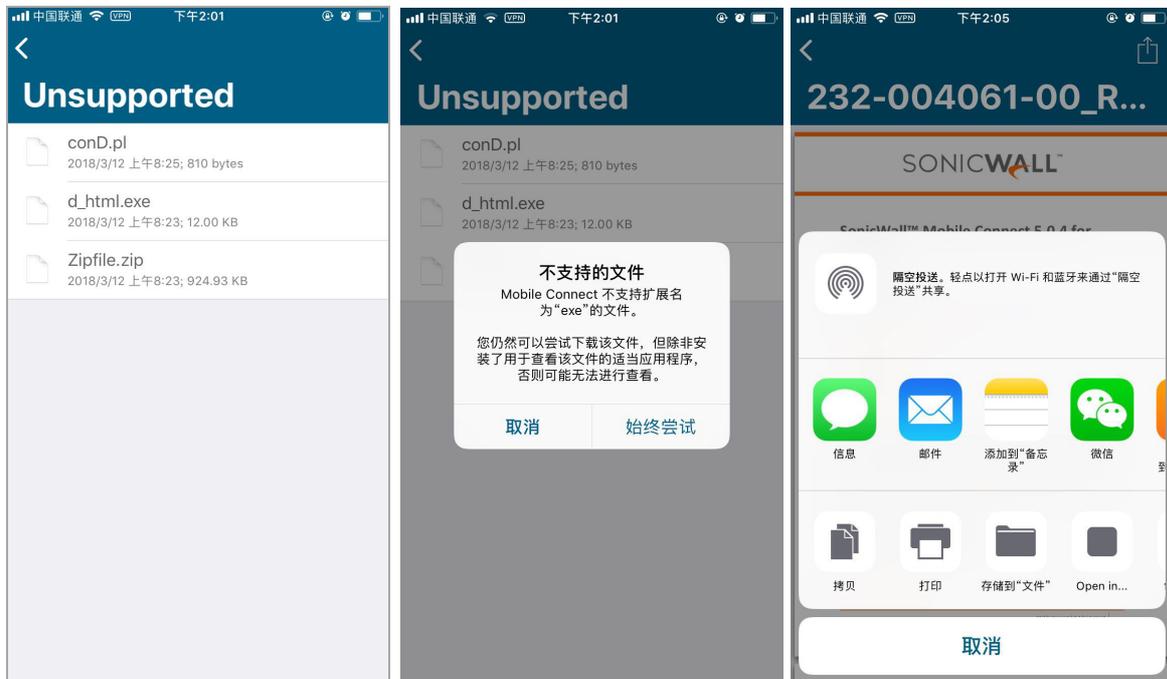
支持的文件类型

文件类型	文件扩展名
Adobe PDF	.pdf
Keynote 演示文稿	.key
Pages 文件	.pages
Numbers 电子表格	.numbers
Web 页面	.htm、.html
文本和富文本文件	.txt、.rtf

不支持的文件类型

如果不支持某个文件类型，则会显示不支持的文件消息，标识除非安装了可以查看该文件的其他应用程序，否则该文件可能无法查看。点触[仍然尝试](#)尝试使用另一个可能注册于处理此文件类型的应用程序打开该文件。请参阅[尝试打开不受支持的文件](#)。

尝试打开不受支持的文件



文件策略和操作

在 iOS 上，可以在服务器上配置策略来控制可以对文件执行的操作，其中包括：

- 打印
- 复制到剪贴板
- 在第三方应用程序中打开
- 安全地缓存在设备上

如果文件已启用一条“允许”策略（“允许打印”、“允许复制”或“允许在以下程序中打开”），则在查看文件时，导航栏右上角将显示[共享](#)按钮。

“共享”按钮



请参阅以下章节：

- 第 41 页的[允许所有操作](#)
- 第 42 页的[允许打印](#)
- 第 43 页的[允许复制](#)
- 第 44 页的[允许在应用程序中打开](#)

允许所有操作

当服务器允许所有文件策略时，点触共享按钮将显示可以对文件执行的所有操作的图标。

所有操作按钮



允许打印

如果文件启用了“允许打印”策略，则点触共享会显示打印按钮。

“打印”按钮



允许复制

如果文件启用了“允许复制”策略，则点触共享按钮将显示复制按钮。

“复制”按钮

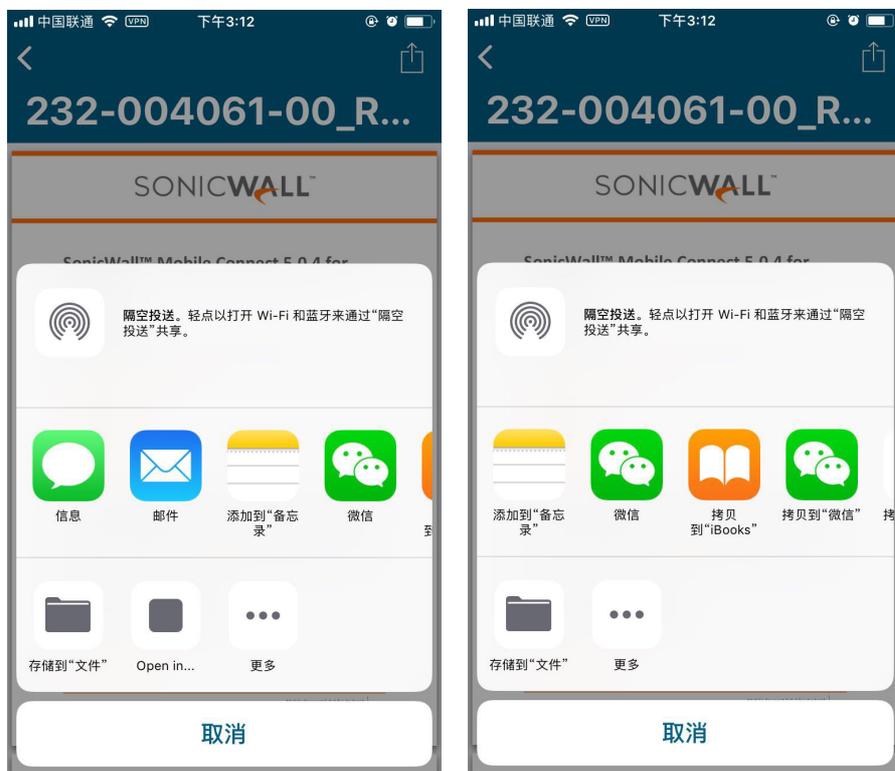


允许在应用程序中打开

如果文件启用了“允许在以下程序中打开”策略，则点触共享按钮将显示在以下程序中打开按钮以及可以打开该文件的其他应用程序的图标。

点触在以下程序中打开按钮显示可以打开该文件的应用程序的列表。

“在以下程序中打开”按钮和应用程序



监控和故障排除

本节介绍了“监控”屏幕并提供故障排除提示，包括如何联系支持。

主题：

- 第 45 页的 [监控 Mobile Connect](#)
- 第 46 页的 [Mobile Connect 故障排除](#)

监控 Mobile Connect

监控屏幕显示有关连接、传输流量的统计信息、DNS 信息和已安装路由的其他详细信息。

“监控”屏幕



Mobile Connect 的关于屏幕显示版本号和法律文本。

“关于”屏幕



Mobile Connect 故障排除

如果无法连接到 SonicWall 服务器，请完成以下步骤以排除连接故障：

- 1 请仔细检查是否在连接配置中正确输入了服务器名称。
- 2 转到 iPhone、iPod touch 或 iPad 上的 Safari 浏览器，尝试导航到 SMA /SRA 设备 Web 门户。
- 3 如果无法加载 Web 门户，则问题出在 SonicWall 设备上。如果问题仍然存在，请联系网络管理员。
- 4 如果 Web 门户在 Safari 浏览器上成功加载却仍然无法建立 Mobile Connect 连接，请通知 SonicWall 支持，如下所示：
 - a 在“设置”选项卡上，启用调试日志。
 - b 再次尝试连接到服务器，以确保记录了此次尝试的完整调试消息。
 - c 然后返回到“设置”选项卡并点触电子邮件日志。在邮件客户端中发起一封附带 Mobile Connect 日志的电子邮件。将电子邮件发送到 Support@sonicwall.com。将任意其他评论添加到电子邮件，然后点触发送。SonicWall 支持人员会在审核案例后与您联系。

SonicWall 支持

购买了拥有有效维护合同的 SonicWall 产品的客户和试用版本的客户都可以获得技术支持。

支持门户提供了各种自助工具，使您可以快速并独立地解决问题，一年 365 天，一天 24 小时不间断。如需访问支持门户，请转至 <https://www.sonicwall.com/zh-cn/support>。

通过访问支持门户，您可以：

- 查看知识库文章和技术文档
- 查看视频教程
- 访问 MySonicWall
- 了解 SonicWall 的专业服务
- 查看 SonicWall 支持服务和保修信息
- 注册培训和认证
- 请求技术支持或客户服务

如需联系 SonicWall 支持，请访问 <https://www.sonicwall.com/zh-cn/support/contact-support>。

关于本文档

图例



警告：“警告”图标用来提示可能造成财产损失或人员伤亡的情况。



小心：“小心”图标用来提示如不按照相应说明进行操作，可能引起硬件损坏或数据丢失。



重要提示、注意、提示、手机或视频：信息图标表示支持的信息。

Mobile Connect 用户指南
更新日期 - 2018 年 2 月
软件版本 - 5.0
232-004165-00 修订版 A

版权所有 © 2017 SonicWall Inc. 保留所有权利。

SonicWall 是 SonicWall Inc. 和/或其附属公司在美国和/或其他国家/地区的商标或注册商标。所有其他商标和注册商标均为其各自所有者的财产。

本文档中的信息与 SonicWall Inc. 和/或其附属公司的产品一起提供。本文档或者通过销售 SonicWall 产品不以禁止反言或以其他方式授予任何知识产权的许可，无论是明示的还是暗示的。除了本产品的许可协议中规定的条款与条件，SonicWall 和/或其附属公司不承担有关其产品的任何责任和任何明确、暗示或法定的担保，包括但不限于暗示的适销性、适用于某一特定用途或不侵权的担保。在任何情况下，即使已告知和/或其附属公司发生此类损害的可能性，SonicWall 和/或其附属公司都不对由于停止使用或无法使用本文档而产生的任何直接的、间接的、继发的、惩罚性的、特殊的或偶然的损害（包括但不限于利润损失，业务中断或信息丢失的损失）承担任何责任。SonicWall 和/或其附属公司对本文档内容的准确性或完整性不作任何陈述或保证，并保留随时更改规格和产品说明的权利，恕不另行通知。SonicWall Inc. 和/或其附属公司不作任何承诺更新本文档中包含的信息。

如需获取更多信息，请访问 <https://www.sonicwall.com/zh-cn/legal>。

最终用户产品协议

如需查看 SonicWall 最终用户产品协议，请访问：<https://www.sonicwall.com/zh-cn/legal/license-agreements>。可根据地理位置选择语言，以查看适用于所在地区的 EUPA。

开源代码

SonicWall 能在适用于每项许可证要求的情况下提供一张具有限制性许可证（例如，GPL、LGPL、AGPL）的开源代码的机读光盘。如需获得完整版机读光盘，请将您的书面申请，附带保付支票或汇票（金额 25 美元，收款人为 "SonicWall Inc."）邮寄至以下地址：

通用公共许可证源代码请求
SonicWall Inc. Attn: Jennifer Anderson
5455 Great America Parkway
Santa Clara, CA 95054