



## Apple iOS 版 Cisco AnyConnect 安全移动客户端 4.0.x 版本说明

[Apple iOS 版 AnyConnect 版本说明](#) 2

[Apple iOS 移动设备版 AnyConnect](#) 2

[可用于 Apple iOS 的 AnyConnect 版本](#) 2

[支持的 Apple iOS 设备](#) 3

[在 Apple iOS 上升级 AnyConnect](#) 4

[Apple iOS 版 AnyConnect 4.0.07x 的新功能](#) 5

[Apple iOS 版旧版 AnyConnect 4.0.05x 的新功能](#) 6

[Apple iOS 版 AnyConnect 功能表](#) 11

[自适应安全设备要求](#) 14

[其他思科头端支持](#) 14

[已知问题和限制](#) 15

[AnyConnect Mobile 相关文档](#) 21

Revised: October 26, 2017,

# Apple iOS 版 AnyConnect 版本说明

## Apple iOS 移动设备版 AnyConnect

AnyConnect 安全移动客户端为远程用户提供与思科 ASA 5500 系列的安全 VPN 连接。通过该客户端，用户能够无缝、安全地远程访问企业网络，使安装的应用可如同直接连接到企业网络一般进行通信。AnyConnect 支持通过 IPv4 或 IPv6 隧道连接到 IPv4 和 IPv6 资源。

本文档适用于 AnyConnect 安全移动客户端和自适应安全设备 (ASA) 5500 的管理员，为 [思科 AnyConnect 安全移动客户端管理员指南，版本 4.0](#) 提供补充，并为 Apple iOS 设备上运行的 AnyConnect 提供版本特定的信息。

该 AnyConnect 应用仅在 Apple iTunes App Store 中提供。思科不分发 AnyConnect 移动版应用，您也不能从 ASA 部署该移动应用，但是，您可以从 ASA 为桌面设备部署其他版本的 AnyConnect，并同时支持此移动版本。

### AnyConnect 移动版支持策略

思科支持应用商店当前提供的 AnyConnect 版本；但是，修复和增强功能仅在最新发行的版本中提供。

### AnyConnect 许可

若要连接到 ASA 头端，需提供 AnyConnect 4.x Plus 或 Apex 许可证；试用许可证可用；请参阅 [思科 AnyConnect 订购指南](#)。

有关最新的最终用户许可协议，请参阅 [思科终端用户许可协议，AnyConnect 安全移动客户端版本 4.x](#)。

有关我们的开源许可确认，请参阅 [思科 AnyConnect 安全移动客户端版本 4.0 中使用的开源软件（适用于移动设备）](#)

## 可用于 Apple iOS 的 AnyConnect 版本

Apple iOS 版思科 AnyConnect 当前具有多个版本：

- **Cisco AnyConnect**

这是此新应用的初始版本。新思科 AnyConnect 是适用于 Apple iOS 的最新版本，建议使用此版本。（在试用版周期中，这版 AnyConnect 命名为 *AnyConnect 2017*。）

我们建议对于 Apple iOS 10.3 及更高版本使用此版本。此版本使用 iOS 提供的新扩展框架来实施 VPN 及其所有功能。为了确保您已收到最新的 Apple iOS 漏洞修复，请使用最新版本。

现在 AnyConnect 4.0.07x 中完全支持 Per App VPN 隧道功能。新扩展框架允许支持 TCP 和 UDP 应用。

自此以后，此新思科 AnyConnect 版本将是唯一包含所有增强功能及漏洞修复的版本。其编号为 4.0.07x。

请参阅 [Apple iOS 版 AnyConnect 4.0.07x 的新功能，第 5 页](#)。

- **思科旧版 AnyConnect**

旧版 AnyConnect 支持目前在应用商店已推出一段时间的 Apple iOS 6.0 及更高版本。此版本将随时间推移而退出，但目前仍然可用，以便轻松过渡到建议的最新版本。

旧版 AnyConnect 应用中的 Per App VPN 隧道功能不会获得 TAC 支持。客户若要使用 Per App VPN，应迁移到新版本。

仅应针对严重的安全问题更新旧版 AnyConnect。此版本继续编号为 4.0.05x。请参阅[Apple iOS 版旧版 AnyConnect 4.0.05x 的新功能，第 6 页](#)。

思科 AnyConnect 和旧版 AnyConnect 是不同的应用，其应用 ID 有所不同。因此：

- 不能将 AnyConnect 应用从旧版 4.0.05x 或更早版本升级到新的 4.0.07x 版本。思科 AnyConnect 4.0.07x 是单独的应用，使用不同的名称和图标进行安装。
- AnyConnect 的不同版本可以共存于移动设备之上，但思科不支持此操作。如果在安装了两个 AnyConnect 版本时尝试进行连接，行为可能与预期不同。请确保您的设备上只有一个 AnyConnect 应用，并且其版本适合您的设备和环境。
- 新 AnyConnect 应用版本 4.0.07072 或更高版本不能访问或使用以旧版 AnyConnect 版本 4.0.05069 及任何更早版本导入的证书。两个应用版本均可访问和使用 MDM 部署的证书。
- 如果要更新至新版本，应删除导入到旧版 AnyConnect 应用的应用数据，例如证书和配置文件。否则，它们将继续显示在系统 VPN 设置中。在卸载旧版 AnyConnect 应用之前删除应用数据。
- 当前的 MDM 配置文件不会触发新应用。EMM 供应商必须支持 VPNTType (VPN)、VPNSubType (com.cisco.anyconnect) 和 ProviderType (packet-tunnel)。为了与 ISE 集成，它们必须能够将唯一标识符传递给 AnyConnect，因为 AnyConnect 在新框架中不能再访问此信息。有关如何设置此功能，请咨询您的 EMM 供应商；有些可能需要自定义 VPN 类型，另一些在发布时可能无可用的支持。

在 AnyConnect 4.0.07x 及更高版本中使用新扩展框架会导致旧版 AnyConnect 4.0.05x 中的行为发生以下变化：

- 在新版本中，发送到头端的设备 ID 不再是 UDID，而且重置为出厂设置后，设备 ID 将发生变化，除非您的设备从其进行的备份中执行恢复。
- 您可以使用 MDM 部署的证书和使用 AnyConnect 中可用的某种方法导入的证书：SCEP、通过 UI 手动导入或通过 URI 处理程序导入。新版 AnyConnect 不能再使用通过邮件或识别的这些方法之外的任何其他机制导入的证书。
- 在使用 UI 创建连接条目时，用户必须接受显示的 iOS 安全消息。
- 用户创建的条目若与从 AnyConnect VPN 配置文件中下载的主机条目名称相同，当它们处于活动状态时，在断开连接前不会对其重命名。另外，断开连接后，下载的主机连接条目将出现在 UI 中，保持连接时则不会显示在 UI 中。

## 支持的 Apple iOS 设备

思科 *AnyConnect 4.0.07x* 作为最新的建议版本，可用于运行 Apple iOS 10.3 及更高版本的所有 iPhone、iPad 和 iPod Touch 设备。

如果设备不支持 Apple iOS 10.3 或更高版本，则仅可使用适用于运行 Apple iOS 6.0 及更高版本的所有 iPhone、iPad 和 iPod Touch 设备的旧版 *AnyConnect 4.0.05x*。旧版 AnyConnect 中的 Per App 隧道需要 Apple iOS 8.3 或更高版本。



---

注释 AnyConnect 在 iPod Touch 上的显示和操作与在 iPhone 上相同。

---

## 在 Apple iOS 上升级 AnyConnect

AnyConnect 的升级通过 Apple 应用商店进行。在 Apple 应用商店通知用户思科 AnyConnect 或旧版 AnyConnect 升级可用后，他们可按照此程序进行升级。



---

注释 不能将 AnyConnect 应用从旧版 4.0.05x 或更早版本升级到新的 4.0.07x 版本。思科 AnyConnect 4.0.07x 是单独的应用，使用不同的名称和图标进行安装。

在安装新版本 4.0.07xxx 之前，请参阅[可用于 Apple iOS 的 AnyConnect 版本，第 2 页](#)。思科建议您删除所有旧版 AnyConnect 应用数据，删除旧版 AnyConnect 应用，然后再安装新版本。

---

### 开始之前

在升级设备之前，必须断开 AnyConnect VPN 会话（若已建立）并关闭 AnyConnect 应用（若已打开）。如果不这样做，AnyConnect 将要求您重启设备，然后再使用新版本的 AnyConnect。



---

注释 使用 Apple 按需连接功能时，只有运行早于 4.0.05032 的旧版 AnyConnect 版本或早于 9.3 的 Apple iOS 版本，此功能才适用于您的环境。在更新 AnyConnect 后，为了确保正确建立按需连接 VPN 隧道，用户必须手动启动 AnyConnect 应用并建立连接。如果不这样做，在下次 iOS 系统尝试建立 VPN 隧道时，会显示错误消息“VPN 连接需要启动应用” (The VPN Connection requires an application to start up)。

---

### 过程

- 
- 步骤 1 轻触 iOS 主页上的应用商店图标。
  - 步骤 2 轻触 **AnyConnect** 升级通知。
  - 步骤 3 阅读新功能。
  - 步骤 4 点击**更新 (Update)**。
  - 步骤 5 输入您的 **Apple ID** 密码。
  - 步骤 6 点击 **OK**（确定）。  
系统将开始执行 AnyConnect 升级。
-

## Apple iOS 版 AnyConnect 4.0.07x 的新功能

### Apple iOS 移动设备版 AnyConnect 4.0.07075 的新功能

此次 AnyConnect 更新是运行早期版本的设备的维护版本。有关已解决问题的完整列表，请参阅[#unique\\_16](#)。

如果您的设备支持 iOS 10，思科建议您升级到此 AnyConnect 版本；并请参阅[已知问题和限制](#)，第 15 页，了解当前的运行注意事项。

### Apple iOS 移动设备版 AnyConnect 4.0.07074 的新功能

此次 AnyConnect 更新是运行早期版本的设备的维护版本。有关已解决问题的完整列表，请参阅[Apple iOS 版 AnyConnect 4.0.07074 中已解决的问题](#)，第 18 页。

如果您的设备支持 iOS 10，思科建议您升级到此 AnyConnect 版本；并请参阅[已知问题和限制](#)，第 15 页，了解当前的运行注意事项。

### Apple iOS 移动设备版 AnyConnect 4.0.07072 的新功能

此版思科 *AnyConnect* 是建议用于 Apple iOS 的最新版本。此版本支持 iOS 10.3 和更高版本。此版本使用 iOS 提供的新扩展框架来实施 VPN 及其所有功能。在试用版周期中，这版 AnyConnect 命名为 *AnyConnect 2017*。除新框架之外，此版本中现在完全支持下面介绍的 Per App 隧道。



---

**注释** 新 AnyConnect 应用版本 4.0.07072 或更高版本不能访问或使用以旧版 AnyConnect 版本 4.0.05069 及任何更早版本导入的证书。两个应用版本均可访问和使用 MDM 部署的证书。

---

自此以后，此思科 AnyConnect 版本将是唯一包含所有增强功能及漏洞修复的版本。其编号为 4.0.07xxx。

此次 AnyConnect 更新也是运行早期版本的设备的维护版本。有关已解决问题的完整列表，请参阅[Apple iOS 版 AnyConnect 4.0.07072 中已解决的问题](#)，第 18 页。

如果您的设备支持 iOS 10，思科建议您升级到此 AnyConnect 版本；并请参阅[已知问题和限制](#)，第 15 页，了解当前的运行注意事项。

#### Per App VPN

传统 VPN 系统隧道连接（可用作全隧道连接配置或拆分隧道连接配置）会根据目标地址通过隧道或以明文形式定向数据包。Per App VPN 隧道连接在第 7 层运行，根据来源应用通过隧道或以明文形式定向数据。Per App VPN 是拆分隧道连接，仅允许来自自己批准应用的数据到达企业网络。

在 Per App VPN 隧道连接模式下，会在移动设备上针对特定应用集建立连接。AnyConnect 为之隧道连接数据的应用集由 ASA 头端的管理员使用 AnyConnect 企业应用选择器工具和 ASA 自定义属性机制定义。此确定并批准的应用列表会发送给 AnyConnect 客户端，并用于在设备上强制实施 Per App VPN 隧道连接。对于不在该列表中的所有其他应用，数据在隧道之外发送或以明文形式发送。

您的移动设备管理器必须配置移动设备来通过隧道传输与 AnyConnect 配置相同的应用列表。ASA 头端和移动设备管理器之间的隧道连接应用集差异可能会导致意外应用行为。如果想要获得无缝的自动配置，请在 MDM 配置中配置 *App on Demand*，并使用数字证书连接到头端。

## Apple iOS 版旧版 AnyConnect 4.0.05x 的新功能

### Apple iOS 移动设备版旧版 AnyConnect 4.0.05069 的新功能

此版本 AnyConnect 现命名为 **旧版 AnyConnect**。

旧版 AnyConnect 支持目前在应用商店已推出一段时间的 Apple iOS 6.0 及更高版本。它将保持可用，以便于过渡到建议的最新版思科 *AnyConnect*。

旧版 AnyConnect 仅会更新升级到最新版本而无法解决的严重客户问题。此版本继续编号为 4.0.05x。请参阅 [Apple iOS 版旧版 AnyConnect 4.0.05x 的新功能](#)，第 6 页。

此次 AnyConnect 更新也是运行早期版本的设备的维护版本。有关已解决问题的完整列表，请参阅 [Apple iOS 版旧版 AnyConnect 4.0.05069 中已解决的问题](#)，第 18 页。

思科建议仅在设备不支持 iOS 10 时，再升级到此 AnyConnect 版本。请参阅 [已知问题和限制](#)，第 15 页，了解当前的运行注意事项。

### Apple iOS 移动设备版 AnyConnect 4.0.05066 的新功能

此次 AnyConnect 更新是运行早期版本的设备的维护版本。有关已解决问题的完整列表，请参阅 [Apple iOS 版 AnyConnect 4.0.05066 中已解决的问题](#)，第 18 页。

思科建议您升级到此最新 AnyConnect 版本，并查看 [已知问题和限制](#)，第 15 页了解当前的运行注意事项。



---

**注释** 请将与 Per App VPN 试用版功能相关的问题和反馈以邮件形式直接发送至 [ac-mobile-feedback@cisco.com](mailto:ac-mobile-feedback@cisco.com)，不要将问题提交到思科 TAC。

---

### Apple iOS 移动设备版 AnyConnect 4.0.05055 的新功能

此版 Apple iOS 版思科 AnyConnect 更新了对以前版本中引入的“暂停时断开连接” (Disconnect on Suspend) 和自动重新连接行为的支持。

现在，当选择“暂停时断开连接” (Disconnect on Suspend) 时，AnyConnect 将在设备休眠时断开连接并释放分配到 VPN 会话的资源，仅适用于按需连接。按此方式断开连接后，只有用户手动连接或配置了按需连接，AnyConnect 才会作出响应而重新连接。

此次 AnyConnect 更新也是运行早期版本的设备的维护版本。有关已解决问题的完整列表，请参阅 [Apple iOS 版 AnyConnect 4.0.05055 中已解决的问题](#)，第 19 页。

思科建议您升级到此最新 AnyConnect 版本，并查看 [已知问题和限制](#)，第 15 页了解当前的运行注意事项。



---

注释 请将与 Per App VPN 试用版功能相关的问题和反馈以邮件形式直接发送至 [ac-mobile-feedback@cisco.com](mailto:ac-mobile-feedback@cisco.com)，不要将问题提交到思科 TAC。

---

## Apple iOS 移动设备版 AnyConnect 4.0.05052 的新功能

此版 Apple iOS 版思科 AnyConnect 现在支持“暂停时断开连接” (Disconnect on Suspend) 和自动重新连接行为（如果管理员在 VPN 客户端配置文件中选择了它们）。当选择“暂停时断开连接” (Disconnect on Suspend) 时，AnyConnect 将在设备休眠时断开连接并释放分配到 VPN 会话的资源。只有用户手动连接或配置了按需连接，它才会作出响应而重新连接。

此次 AnyConnect 更新也是运行早期版本的设备的维护版本。有关已解决问题的完整列表，请参阅 [Apple iOS 版 AnyConnect 4.0.05052 中已解决的问题，第 19 页](#)。

思科建议您升级到此最新 AnyConnect 版本，并查看 [已知问题和限制，第 15 页](#) 了解当前的运行注意事项。



---

注释 请将与 Per App VPN 试用版功能相关的问题和反馈以邮件形式直接发送至 [ac-mobile-feedback@cisco.com](mailto:ac-mobile-feedback@cisco.com)，不要将问题提交到思科 TAC。

---

## Apple iOS 移动设备版 AnyConnect 4.0.05046 的新功能

此次 Apple iOS 设备版思科 AnyConnect 安全移动客户端更新可解决最近的 OpenSSL 漏洞。此外，它还是运行早期版本的设备的维护版本。有关已解决问题的完整列表，请参阅 [Apple iOS 版 AnyConnect 4.0.05046 中已解决的问题，第 19 页](#)。

思科建议您升级到此最新 AnyConnect 版本，并查看 [已知问题和限制，第 15 页](#) 了解当前的运行注意事项。



---

注释 请将与 Per App VPN 试用版功能相关的问题和反馈以邮件形式直接发送至 [ac-mobile-feedback@cisco.com](mailto:ac-mobile-feedback@cisco.com)，不要将问题提交到思科 TAC。

---

## Apple iOS 移动设备版 AnyConnect 4.0.05038 的新功能

此版本的 Apple iOS 版 AnyConnect 是一个维护版本，用于解决 4.0.05036 中的回归问题。有关详细信息，请参阅 [Apple iOS 版 AnyConnect 4.0.05038 中已解决的问题，第 20 页](#)。



---

注释 请将与 Per App VPN 试用版功能相关的问题和反馈以邮件形式直接发送至 [ac-mobile-feedback@cisco.com](mailto:ac-mobile-feedback@cisco.com)，不要将问题提交到思科 TAC。

---

思科建议您升级到此最新 AnyConnect 版本，并查看 [已知问题和限制，第 15 页](#) 了解当前操作注意事项。

## Apple iOS 移动设备版 AnyConnect 4.0.05036 的新功能

此版本的 Apple iOS 版 AnyConnect 是一个维护版本，用于解决 4.0.05032 中的回归问题。有关详细信息，请参阅 [Apple iOS 版 AnyConnect 4.0.05036 中已解决的问题](#)，第 20 页。



---

注释 请将与 Per App VPN 试用版功能相关的问题和反馈以邮件形式直接发送至 [ac-mobile-feedback@cisco.com](mailto:ac-mobile-feedback@cisco.com)，不要将问题提交到思科 TAC。

---

思科建议您升级到此最新 AnyConnect 版本，并查看 [已知问题和限制](#)，第 15 页了解当前操作注意事项。

## Apple iOS 移动设备版 AnyConnect 4.0.05032 的新功能

此 AnyConnect 4.0 版本现在支持：公共 IPv6 隧道连接和专用 IPv6 拆分隧道连接。

此外，针对同时运行 AnyConnect 4.0.05032 或更高版本及 Apple iOS 9.3 或更高版本的设备，已移除如下限制：升级后，如果在设备上使用 Apple iOS 按需连接功能来自动建立 VPN 连接，那么必须启动 AnyConnect 应用并建立 VPN 连接。如果不这样做，在下次 iOS 系统尝试建立 VPN 隧道时，将显示错误消息“VPN 连接需要启动应用” (The VPN Connection requires an application to start up)。



---

注释 与 Per App VPN Bata 功能相关的问题和反馈应以邮件形式直接发送至 [ac-mobile-feedback@cisco.com](mailto:ac-mobile-feedback@cisco.com)，而不应提交到思科 TAC

---

思科建议您升级到此最新 AnyConnect 版本，并查看 [已知问题和限制](#)，第 15 页了解当前操作注意事项。

## Apple iOS 移动设备版 AnyConnect 4.0.03021 的新功能

此 AnyConnect 4.0 版本是适用于运行早期版本的 AnyConnect 的 Apple iOS 设备的升级。它解决最新的 Open SSL 漏洞和其他问题。有关详细信息，请参阅 [Apple iOS 版 AnyConnect 4.0.03021 中已解决的问题](#)，第 20 页。



---

注释 与 Per App VPN Bata 功能相关的问题和反馈应以邮件形式直接发送至 [ac-mobile-feedback@cisco.com](mailto:ac-mobile-feedback@cisco.com)，而不应提交到思科 TAC

---

思科建议您升级到此最新 AnyConnect 版本，并查看 [已知问题和限制](#)，第 15 页了解当前操作注意事项。

## Apple iOS 移动设备版 AnyConnect 4.0.03016 的新功能

此 AnyConnect 4.0 版本是适用于运行早期版本的 AnyConnect 的 Apple iOS 设备的升级。它解决最新的 Open SSL 漏洞和 4.0 初始版本中发现的问题。有关详细信息，请参阅 [Apple iOS 版 AnyConnect 4.0.03016 中已解决的问题](#)。



---

注释 与 Per App VPN Bata 功能相关的问题和反馈应以邮件形式直接发送至 [ac-mobile-feedback@cisco.com](mailto:ac-mobile-feedback@cisco.com)，而不应提交到思科 TAC

---

思科建议您升级到此最新 AnyConnect 版本，并查看 [已知问题和限制](#)，第 15 页了解当前操作注意事项。

## Apple iOS 移动设备版 AnyConnect 4.0.03004 的新功能

此 AnyConnect 4.0 版本是适用于运行早期版本的 AnyConnect 的 Apple iOS 设备的升级。它解决最新的 Open SSL 漏洞和 4.0 初始版本中发现的问题。有关详细信息，请参阅 [Apple iOS 版 AnyConnect 4.0.03004 中已解决的问题](#)，第 21 页。



---

**注释** 与 Per App VPN Bata 功能相关的问题和反馈应以邮件形式直接发送至 [ac-mobile-feedback@cisco.com](mailto:ac-mobile-feedback@cisco.com)，而不应提交到思科 TAC。

---

思科建议您升级到此最新 AnyConnect 版本，并查看 [已知问题和限制](#)，第 15 页了解当前操作注意事项。

## Apple iOS 移动设备版 AnyConnect 4.0.01324 的新功能

此 AnyConnect 4.0 版本是适用于运行早期版本的 AnyConnect 的 Apple iOS 设备的升级，包含如下所述的新功能：

- TLS 1.2
- 其他本地化
- Per App VPN（仅提供试用版和支持）



---

**注释** 与此功能相关的问题和反馈应以邮件形式直接发送至 [ac-mobile-feedback@cisco.com](mailto:ac-mobile-feedback@cisco.com)，而不应提交到思科 TAC。

---

思科建议您升级到此最新 AnyConnect 版本。请查看 [已知问题和限制](#)，第 15 页了解当前操作注意事项。

### TLS 1.2

现在，AnyConnect 4.0 通过以下附加密码套件支持 TLS 版本 1.2：

- DHE-RSA-AES256-SHA256
- DHE-RSA-AES128-SHA256
- AES256-SHA256
- AES128-SHA256



---

**注释** AnyConnect TLS 1.2 要求使用同样支持 TLS 1.2 的安全网关。5500-X 型号上的 9.3(2) 版 ASA 便提供这样的网关。

---

### 其他本地化

移动设备版 AnyConnect 4.0 现在在 AnyConnect Apple iOS 应用中包括以下额外的语言翻译：

- 中文（台湾地区）(zh-tw)
- 荷兰语 (nl-nl)
- 法语 (fr-fr)
- 匈牙利语 (hu-hu)
- 意大利语 (it-it)
- 葡萄牙语（巴西）(pt-br)
- 俄语 (ru-ru)
- 西班牙语 (es-es)

有关移动本地化选项和详细信息，请参阅 [思科 AnyConnect 安全移动客户端管理员指南，版本 4.0](#) 中的移动设备上的本地化。

### Per App VPN 隧道连接

移动设备版 AnyConnect 4.0 已获得增强，除传统系统隧道连接外，还提供 Per App VPN 隧道连接。Per App VPN 隧道连接需要：

- Apple iOS 8.3 或更高版本
- 必须使用移动设备管理 (MDM) 解决方案将设备配置为使用 Per App。
- ASA 9.3.2 或更高版本，以便配置 Per App VPN 隧道。
- AnyConnect v4.0 Plus 或 Apex 许可证。




---

**注释** AnyConnect 基础版或高级版许可证不支持 Per App VPN。拥有高级版或基础版许可证的客户有资格获取 AnyConnect 4.0 迁移许可证。有关详细信息，请参阅 [思科 AnyConnect 订购指南](#)。

---

传统 VPN 系统隧道连接（可用作全隧道连接配置或拆分隧道连接配置）会根据目标地址通过隧道或以明文形式定向数据包。Per App VPN 隧道连接在第 7 层运行，根据来源应用通过隧道或以明文形式定向数据。Per App VPN 是拆分隧道连接，仅允许来自自己批准应用的数据到达企业网络。

在 Per App VPN 隧道连接模式下，会在移动设备上针对特定应用集建立连接。AnyConnect 为之隧道连接数据的应用集由 ASA 头端的管理员使用 AnyConnect 企业应用选择器工具和 ASA 自定义属性机制定义。此确定并批准的应用列表会发送给 AnyConnect 客户端，并用于在设备上强制实施 Per App VPN 隧道连接。对于不在该列表中的所有其他应用，数据在隧道之外发送或以明文形式发送。

您的移动设备管理器必须配置移动设备来通过隧道传输与 AnyConnect 配置相同的应用列表。ASA 头端和移动设备管理器之间的隧道连接应用集差异可能会导致意外应用行为。如果想要获得无缝的自动配置，请在 MDM 配置中配置 *App on Demand*，并使用数字证书连接到头端。

AnyConnect 基于从 ASA 头端接收的配置信息确定它会在哪种模式下运行。具体而言，即在建立会话时，与连接相关的组策略或动态访问策略 (DAP) 中是存在还是缺少 Per App VPN 自定义属性。如果 Per App VPN 列表存在，AnyConnect 会在 Per App VPN 模式下运行；如果列表不存在，AnyConnect 会在系统隧道连接模式下运行。

## Apple iOS 版 AnyConnect 功能表

AnyConnect 在 Apple iOS 设备上支持以下功能：

类别：功能	Apple iOS
<b>部署和配置：</b>	
从应用存储区安装或升级。	是
思科 VPN 配置文件支持（手动导入）	是
思科 VPN 配置文件支持（连接时导入）	是
MDM 配置的连接条目	是
用户配置的连接条目	是
<b>隧道连接：</b>	
TLS	是
数据报 TLS (DTLS)	是
IPsec IKEv2 NAT-T	是
IKEv2 - 原始 ESP	否
Suite B（仅限 IPsec）	是
TLS 压缩	是，仅限 32 位设备
失效对等项检测	是
隧道保持连接	是
多个活动网络接口	否
Per App 隧道连接	是，需要思科 AnyConnect 4.0.09xxx 及 iOS 10.3 或更高版本。
完全隧道（OS 对于某些流量可能生成异常，例如传至应用商店的流量）。	是
拆分隧道（拆分包括）。	是
本地 LAN（拆分排除）。	是
拆分 DNS	是
自动重新连接/网络漫游	是
按需 VPN（由目标触发）	是，与 Apple iOS 按需连接兼容。
按需 VPN（由应用触发）	是，仅当在 Per App VPN 模式下运行时。

类别：功能	Apple iOS
重新生成密钥	是
IPv4 公共传输	是
IPv6 公共传输	是
IPv4 over IPv4 隧道	是
IPv6 over IPv4 隧道	是
IPv6 over IPv4 隧道	是
IPv6 over IPv6 隧道	是
默认域	是
DNS 服务器配置	是
专用端代理支持	是
代理例外	是，但不支持通配符规范
公共端代理支持	否
登录前横幅	是
登录后横幅	是
DSCP 保留	否
<b>连接和断开连接：</b>	
VPN 负载均衡	是
备用服务器列表	是
最佳网关选择	否
<b>身份验证：</b>	
SAML 2.0	否
客户端证书身份验证	是
在线证书状态协议 (OCSP)	否
手动用户证书管理	是
手动服务器证书管理	是
SCEP 传统注册（请针对您的平台进行确认）。	是
SCEP 代理注册（请针对您的平台进行确认）。	是
自动证书选择	是

类别：功能	Apple iOS
手动证书选择	是
智能卡支持	否
用户名和密码	是
令牌/质询	是
双重身份验证	是
组 URL（在服务器地址中指定）	是
组选择（下拉选择）	是
从用户证书预填充凭证	是
保存密码	否
<b>用户界面：</b>	
独立 GUI	是
本地 OS GUI	是，功能受限制
API/URI 处理程序（请参阅下文）	是
UI 自定义	否
UI 本地化	是，应用包含预先打包的语言。
用户首选项	是
支持一键式 VPN 访问的主屏幕构件	否
AnyConnect 特定状态图标	否
<b>移动安全评估：</b> （AnyConnect 标识扩展，ACIDex）	
序列号或唯一 ID 检查	是
与头端共用操作系统和 AnyConnect 版本	是
<b>AnyConnect NVM 支持</b>	否
<b>URI 处理：</b>	
添加连接条目	是
连接到 VPN	是
连接时预填充凭证	是
断开 VPN	是

类别：功能	Apple iOS
导入证书	是
导入本地化数据	是
导入 XML 客户端配置文件	是
URI 命令的外部（用户）控件	是
报告和故障排除：	
统计信息	是
日志记录/诊断信息 (DART)	是
认证：	
FIPS 140-2 第 1 层	是

## 自适应安全设备要求

以下功能对 ASA 有最低版本要求：



**注释** 请参阅您的平台的功能表，以确认这些功能在当前 AnyConnect 移动版本中的可用性。

- 必须升级到 ASA 9.3.2 或更高版本才能使用 TLS 1.2。
- 必须升级到 ASA 9.3.2 或更高版本才能使用 Per App VPN 隧道连接模式。
- 必须升级到 ASA 9.0 才能使用以下移动功能：
  - IPsec IKEv2 VPN
  - Suite B 加密
  - SCEP 代理
  - 移动状况
- ASA 版本 8.0(3) 和自适应安全设备管理器 (ASDM) 6.1(3) 是支持移动设备版 AnyConnect 的最低版本。

## 其他思科头端支持

思科 IOS 15.3(3)M+/15.2(4)M+ 支持 AnyConnect SSL 连接。

Cisco ISR g2 15.2(4)M+ 支持 AnyConnect IKEv2 连接

思科 Firepower 威胁防御版本 6.2.1 及更高版本中支持 AnyConnect SSL 和 IKEv2。

## 已知问题和限制

### 已知兼容性问题

#### 在 AnyConnect 4.0.07xxx 中

- 当拆分排除配置中仅包含隧道 IPv6（未分配 IPv4 地址）时，连接到 ASA 的拆分隧道不起作用。  
除排除列表条目之外，所有流量均会通过隧道传输，然而拆分排除列表不被认可，所以所有 IPv6 流量都将被排除。请参阅 CSCvb80768：IPv6 拆分排除和 IPv4 全部丢弃将从隧道中排除所有 v6 流量。(RADAR 29623849)。
- 如果 AnyConnect UI 保持打开状态，并且 iOS 错误地断开了 UI 与内部 AnyConnect 扩展之间的进程间通信 (IPC)，则所有 UI 活动都会失败或响应错误。  
要解决此故障，必须关闭并重启 AnyConnect UI，由此重新建立 IPC。如果在 UI 关闭时 IPC 意外断开，则下次打开 UI 时，它会重新建立连接。请参阅 CSCvb95722：未能达到已暂停状态 (RADAR 29313229)。
- 对于按需连接，若已通过 ASA 将更新的 VPN 连接配置文件推送到客户端，则必须打开 AnyConnect UI。如果 UI 未打开，更新的配置文件将不会同步，因此不会使用所作的更改。  
遗憾的是，系统中没有标志指示用户打开 UI 来同步新配置文件（如同旧版 AnyConnect），所以更新的连接可能从未使用。目前没有解决此问题的方法。请参阅 CSCvc35923：使用按需 AC 不会通知用户必须打开 AC 来同步更新的连接配置文件 (RADAR 30173053)。
- 在受管 Per App 配置中，为 Per App 配置的应用流量在不当情况下通过用户创建（非受管）的 VPN 连接传输。  
请参阅 CSCvc36024：PerApp - 应用可通过非 PAV 完全隧道传输流量 (RADAR 29513803)。

#### 在旧版 AnyConnect 4.0.05xxx 中

- 网络漫游仅适用于低于 iOS 8 的版本。iOS 8 及更高版本始终如同已启用网络漫游一样运行，会尝试重新建立连接，直到成功。有关网络漫游的完整说明，请参阅 [Cisco AnyConnect 安全移动客户端用户指南，版本 4.0.x \(Apple iOS\)](#)。
- Apple ID 22784308 问题 - 按需选项“从不连接”失败。
- 设备休眠时收到 DTLS 数据包不会将其唤醒。但是，如果已启用通知或 Facetime，则 TLS 数据包将唤醒设备。当设备进入睡眠状态时，AnyConnect 将自动断开 DTLS 隧道，以便允许通过 TLS 连接接收的数据包将设备唤醒。设备恢复后，DTLS 隧道即可还原。
- 在 iPod Touch 上，在后台运行的语音应用无法通过 VPN 接收数据包。此功能在 iPhone 设备上可正常工作。
- 如果 VPN 配置中包含大量路由或 split-dns 规则，则 Apple 设备将无法建立 VPN 连接。例如，在以下情况下会发生此漏洞：连接状态下，ASA 配置推送了一个包含 VPN 拆分的列表，其中有 70 多个可以将流量引至单个子网的规则。若要防止此类漏洞，可应用全隧道配置或减少规则个数。
- 在移动设备上配置大量 VPN 连接，可能会导致 AnyConnect 变慢或故障。

- Apple iOS 将允许对设备的核心运营至关重要的流量，无论是否执行全隧道策略。不论执行何种隧道策略，Apple iOS 可不受阻碍发送的流量示例包括：

所有本地 LAN 流量

针对预先存在的连接（例如，在建立 VPN 连接前以流式传输的视频）的作用域路由

核心 Apple 服务（例如，可视语音邮件流量）

## Apple iOS 版 AnyConnect 准则和限制

Apple iOS 版 AnyConnect 仅支持与远程 VPN 接入相关的功能，例如：

- AnyConnect 可由用户手动配置、通过 iPhone 配置实用程序 (<http://www.apple.com/support/iphone/enterprise/>) 生成的 AnyConnect VPN 客户端配置文件配置或使用企业移动设备管理器配置。
- Apple iOS 设备仅支持一个 AnyConnect VPN 客户端配置文件。生成的配置内容始终与最近的配置文件匹配。例如，如果您连接到 vpn.example1.com，然后连接到 vpn.example2.com，则从 vpn.example2.com 导入的 AnyConnect VPN 客户端配置文件将替换从 vpn.example1.com 导入的配置文件。
- 此版本支持隧道保持激活功能；但是，它会降低设备电池的寿命。增加更新间隔值可以缓解此问题。

Apple iOS 按需连接注意事项：

- 当设备休眠时，由于 iOS 按需逻辑而自动连接的 VPN 会话及已配置“暂停时断开连接” (Disconnect on Suspend) 的 VPN 会话会断开连接。唤醒设备后，按需逻辑将根据需要重新连接 VPN 会话。
- 启动用户界面和 VPN 连接后，AnyConnect 将收集设备信息。因此，如果用户在一开始或在设备信息（例如操作系统版本）变更后，依赖于 iOS 的按需连接功能来启动连接，AnyConnect 有时候可能误报移动安全评估信息。
- 使用 Apple 按需连接功能时，只有运行早于 4.0.05032 的旧版 AnyConnect 版本或早于 9.3 的 Apple iOS 版本，此功能才适用于您的环境。在更新 AnyConnect 后，为了确保正确建立按需连接 VPN 隧道，用户必须手动启动 AnyConnect 应用并建立连接。如果不这样做，在下次 iOS 系统尝试建立 VPN 隧道时，会显示错误消息“VPN 连接需要启动应用” (The VPN Connection requires an application to start up)。

思科 AnyConnect 和旧版 AnyConnect 是不同的应用，其应用 ID 有所不同。因此：

- 不能将 AnyConnect 应用从旧版 4.0.05x 或更早版本升级到新的 4.0.07x 版本。思科 AnyConnect 4.0.07x 是单独的应用，使用不同的名称和图标进行安装。
- AnyConnect 的不同版本可以共存于移动设备之上，但思科不支持此操作。如果在安装了两个 AnyConnect 版本时尝试进行连接，行为可能与预期不同。请确保您的设备上只有一个 AnyConnect 应用，并且其版本适合您的设备和环境。
- 新 AnyConnect 应用版本 4.0.07072 或更高版本不能访问或使用以旧版 AnyConnect 版本 4.0.05069 及任何更早版本导入的证书。两个应用版本均可访问和使用 MDM 部署的证书。
- 如果要更新至新版本，应删除导入到旧版 AnyConnect 应用的应用数据，例如证书和配置文件。否则，它们将继续显示在系统 VPN 设置中。在卸载旧版 AnyConnect 应用之前删除应用数据。

- 当前的 MDM 配置文件不会触发新应用。EMM 供应商必须支持 VPNTType (VPN)、VPNSubType (com.cisco.anyconnect) 和 ProviderType (packet-tunnel)。为了与 ISE 集成，它们必须能够将唯一标识符传递给 AnyConnect，因为 AnyConnect 在新框架中不能再访问此信息。有关如何设置此功能，请咨询您的 EMM 供应商；有些可能需要自定义 VPN 类型，另一些在发布时可能无可用的支持。

在 AnyConnect 4.0.07x 及更高版本中使用新扩展框架会导致旧版 AnyConnect 4.0.05x 中的行为发生以下变化：

- 在新版本中，发送到头端的设备 ID 不再是 UDID，而且重置为出厂设置后，设备 ID 将发生变化，除非您的设备从其进行的备份中执行恢复。
- 您可以使用 MDM 部署的证书和使用 AnyConnect 中可用的某种方法导入的证书：SCEP、通过 UI 手动导入或通过 URI 处理程序导入。新版 AnyConnect 不能再使用通过邮件或识别的这些方法之外的任何其他机制导入的证书。
- 在使用 UI 创建连接条目时，用户必须接受显示的 iOS 安全消息。
- 用户创建的条目若与从 AnyConnect VPN 配置文件中下载的主机条目名称相同，当它们处于活动状态时，在断开连接前不会对其重命名。另外，断开连接后，下载的主机连接条目将出现在 UI 中，保持连接时则不会显示在 UI 中。

## Apple iOS 版 AnyConnect 4.0.7x 中未解决和已解决的问题

思科漏洞搜索工具 (<https://tools.cisco.com/bugsearch/>) 包含此版本中有关未解决和已解决的问题的详细信息。需要使用思科帐户才能访问该漏洞搜索工具。如果没有，请在 <https://tools.cisco.com/RPF/register/register.do> 中注册。

### Apple iOS 版 AnyConnect 4.0.5 中的未解决问题

标识符	标题
CSCuu76224	即使已播发 SOA 记录，也无法解析 .local
CSCuv44716	拆分隧道包含配置可能无法正常使用
CSCuy41307	AnyConnect 连接状态不同步
CSCuy99092	[ios] tungrp 上的 MTU 需要为 1380 或更低，才能传输 IPSec 流量
CSCuy99108	[ios] Anyconnect 无法丢弃 IPv6 流量
CSCuz38311	当 AAAA 响应缓慢时，建立的 iOS 4.0.05032/5036 连接速度缓慢
CSCuz39092	iOS - 4.0.05036 明确全部丢弃流量文本
CSCvb22398	OS 在休眠期间不触发 VPN - Radar # 27851312
CSCvb31542	iOS: PerApp SafariDom 内部站点的内部 CRL 失败 R#28176408
CSCvb78548	VPN 未能使用 T-Mobile IPv6 网络从 Wi-Fi 过渡到蜂窝网络
CSCve10517	iOS: 对于子域设置时，拆分 DNS 不起作用

### Apple iOS 版 AnyConnect 4.0.07075 中已解决的问题

标识符	标题
CSCvf07751	iOS: 4.0.7074 OS 未添加用于不含拆分 DNS 的拆分隧道的默认域

### Apple iOS 版 AnyConnect 4.0.07074 中已解决的问题

标识符	标题
CSCvc35923	AC-NF 未能通知用户必须打开 AC 来同步更新的配置文件

### Apple iOS 版 AnyConnect 4.0.07072 中已解决的问题

标识符	标题
CSCuq52458	Apple iOS: P 组默认域不能用于 Per App
CSCvb14706	iOS 10 上的 AC 启用调试日志而未激活配置, 显示两次错误
CSCvb57807	ipad AC 客户端证书在诊断中显示过期日期 1969 年 12 月 31 日或 1970 年 1 月 1 日
CSCve49663	iOS/Android: 在 ATT LTE 上未能尝试备份连接条目

### Apple iOS 版 AnyConnect 4.0.5x 中未解决和已解决的问题

思科漏洞搜索工具 (<https://tools.cisco.com/bugsearch/>) 包含此版本中有关未解决和已解决的问题的详细信息。需要使用思科帐户才能访问该漏洞搜索工具。如果没有, 请在 <https://tools.cisco.com/RPF/register/register.do> 中注册。

### Apple iOS 版旧版 AnyConnect 中未解决的问题

未解决的问题仅列在最新版本之下, 请参阅 [Apple iOS 版 AnyConnect 4.0.7x 中未解决和已解决的问题](#), 第 17 页。

### Apple iOS 版旧版 AnyConnect 4.0.05069 中已解决的问题

此版旧版 AnyConnect 中未修复任何问题。

### Apple iOS 版 AnyConnect 4.0.05066 中已解决的问题

标识符	标题
CSCuv35459	匹配的连接配置文件名称未重命名

标识符	标题
CSCuy12161	AnyConnect 应不再要求服务器证书具有密钥协议
CSCvb48664	针对 2016 年 9 月 OpenSSL 漏洞评估 AnyConnect
CSCvb57807	ipad AC 客户端证书在诊断中显示过期日期 1969 年 12 月 31 日或 1970 年 1 月 1 日
CSCvb59411	iOS: 在运行 iOS 10+ 的 32 位设备（例如 iPhone 5C、5、iPad 4 及更早产品）上执行 Deflate 压缩失败

#### Apple iOS 版 AnyConnect 4.0.05055 中已解决的问题

标识符	标题
CSCvb14706	iOS 10 上的 AC 启用调试日志而未激活配置，显示两次错误
CSCvb26000	AC iOS: ENH - 使“暂停时断开连接” (DisconnectOnSuspend) 功能依赖于 OS 自动 VPN

#### Apple iOS 版 AnyConnect 4.0.05052 中已解决的问题

标识符	标题
CSCuv97696	Apple #22457371 iOS 9 - 使用 RequiredDNSServers 的按需规则在首次 DNS 连接时失败
CSCva32660	AC iOS: 启用客户端旁路协议导致连接失败
CSCva56275	AC iOS: ENH - 支持“暂停时断开连接” (DisconnectOnSuspend) 配置文件选项
CSCva86673	iOS 10 - IPv6 APNS 与仅支持具有 v4 的地址通过隧道的网络兼容

#### Apple iOS 版 AnyConnect 4.0.05046 中已解决的问题

标识符	标题
CSCut14163	连接到具有多个 IN A 的 FQDN 时，3.0.12240 配置文件损坏
CSCuy15657	更改选择的 VPN 配置文件失败
CSCuy77264	Advanced 一词在 UI 中未正确对齐
CSCuz33124	让所有具有 v4 地址的流量通过隧道并丢弃所有具有 v6 地址的流量会阻止流量传递到专用网络

标识符	标题
CSCuz38302	连接到具有多个 IN A 的 FQDN 时，4.0.05036 配置文件损坏
CSCuz38319	iOS 4.0.05032/5036 - MTU 进程的奇怪行为 - 断开连接/重新连接
CSCuz38432	iOS: 4.0.05036 无网络连接 - 错误消息 - 无法连接
CSCuz39090	iOS - 4.0.05036 客户端版本字符串被错误地报告为 Windows
CSCuz52506	针对 2016 年 5 月 OpenSSL 漏洞评估 AnyConnect
CSCuz94483	iOS AnyConnect 4.0.5036+ PAC URL 不运行
CSCva03743	AnyConnect iOS 多次重新连接
CSCva26758	iOS - 支持通过 DNS64/NAT64 网络上的 IP 连接到 IPv4 头端
CSCva30253	在某些情况下，AnyConnect 对话框显示的字体颜色错误

#### Apple iOS 版 AnyConnect 4.0.05038 中已解决的问题

标识符	标题
CSCuz38302	连接到具有多个 IN A 的 FQDN 时，4.0.05036 配置文件损坏
CSCuz38319	iOS 4.0.05032/5036 - MTU 进程的奇怪行为 - 断开连接/重新连接
CSCuz38432	iOS: 4.0.05036 无网络连接 - 错误消息 - 无法连接
CSCuz39090	iOS - 4.0.05036 客户端版本字符串被错误地报告为 Windows

#### Apple iOS 版 AnyConnect 4.0.05036 中已解决的问题

标识符	标题
CSCuo47016	XMLSoft libxml2 基于解码堆的缓冲区下溢漏洞
CSCuy15657	更改选择的 VPN 配置文件失败
CSCuz33124	让所有具有 v4 地址的流量通过隧道并丢弃所有具有 v6 地址的流量会阻止流量传递到专用网络

#### Apple iOS 版 AnyConnect 4.0.03021 中已解决的问题

标识符	标题
CSCut56282	AnyConnect iPhone: 按需域无法通过配置文件更新

标识符	标题
CSCux38698	Anyconnect IKEv2 缓冲区溢出
CSCux41420	针对 2015 年 12 月 OpenSSL 漏洞评估 AnyConnect
CSCux81967	AC 版权信息需要更改为 2016 年
CSCuy25393	在 iPad Pro 上通过 AnyConnect 发送邮件日志失败
CSCuy54600	针对 2016 年 3 月 OpenSSL 漏洞评估 AnyConnect

### Apple iOS 版 AnyConnect 4.0.03016 中已解决的问题

标识符	标题
CSCuv97696	Apple #22457371 iOS 9 - 使用 RequiredDNSServers 的按需规则在首次 DNS 连接时失败
CSCuw11134	iOS 9 - 拆分隧道与所有 DNS 通过隧道 - AAAA DNS 屏蔽导致 DNS 故障
CSCuw54786	iOS - 报告错误的 UDID - 更改设备并从备份还原

### Apple iOS 版 AnyConnect 4.0.03004 中已解决的问题

标识符	标题
CSCut46503	2015 年 3 月 OpenSSL 漏洞
CSCuu96241	在 4.0 升级后，通过外部应用启用 AC 时会遇到启动问题
CSCuu99043	登录屏幕在离开屏幕然后返回时不可用

## AnyConnect Mobile 相关文档

有关详细信息，请参阅以下文档：

- [AnyConnect 版本说明](#)
- [AnyConnect 管理员指南](#)
- [思科 ASA 系列文档一览](#)

Apple 提供有关在 Apple iOS 设备上使用 VPN 连接的其他信息：

- <https://developer.apple.com/library/ios/search/?q=vpn+server+configuration>

- <http://support.apple.com/kb/ht1424>

思科和思科徽标是思科和/或其附属公司在美国和其他国家/地区的商标或注册商标。要查看思科商标列表，请访问此网址：<http://www.cisco.com/go/trademarks>。  
文中提及的第三方商标为其相应所有者的财产。“合作伙伴”一词的使用并不意味着思科和任何其他公司之间存在合作关系。(1110R)

© 2015-2017 Cisco Systems, Inc. All rights reserved.



美洲总部  
Cisco Systems, Inc.  
San Jose, CA 95134-1706  
USA

亚太区总部  
Cisco Systems (USA) Pte. Ltd.  
Singapore

欧洲总部  
Cisco Systems International BV  
Amsterdam, The Netherlands

Cisco 在全球拥有 200 多个办事处。相关地址、电话和传真号码可见于  
Cisco 位于 [www.cisco.com/go/offices](http://www.cisco.com/go/offices) 上的网站。