



Remote Access

- [服务发现要求工作流程，第 1 页](#)
- [服务发现要求，第 1 页](#)
- [Cisco Anyconnect 部署工作流程，第 3 页](#)
- [Cisco AnyConnect 部署，第 3 页](#)

服务发现要求工作流程

过程

	命令或操作	目的
步骤1	服务发现要求	
步骤2	DNS 要求	
步骤3	证书要求	
步骤4	测试_collab-edge SRV 记录，第 2 页	

服务发现要求

服务发现允许客户端自动在您的企业网络上检测和查找服务。移动设备和Remote Access的Expressway可使您访问企业网络上的服务。您应满足以下要求，以使客户端能够通过移动设备和Remote Access的Expressway 进行连接，然后发现服务：

- DNS 要求
- 证书要求
- 测试外部 SRV_collab-edge。

DNS 要求

通过 Remote Access 实现服务发现的 DNS 要求包括：

- 在外部 DNS 服务器上配置 `_collab-edge` DNS SRV 记录。
- 在内部名称服务器上配置 `_cisco-uds` DNS SRV 记录。
- 或者，对于 IM 和在线状态服务器和语音服务器的具有不同域的基于云的混合部署，可以配置语音服务域来找到具有 `_collab-edge` 记录的 DNS 服务器。

证书要求

在您配置远程访问之前，请下载 Cisco VCS Expressway 和 Cisco Expressway-E 服务器证书。服务器证书用于 HTTP 和 XMPP。

有关配置 Cisco VCS Expressway 证书的详细信息，请参阅《[Cisco vcs Expressway 上的配置证书](#)》。

测试 `_collab-edge` SRV 记录

测试 SRV 记录

在创建 SRV 记录后，测试以确认是否可以访问这些记录。



提示 如果您偏好基于 web 的选项，您也可以使用[协作解决方案分析器](#)站点上的 SRV 检查工具。

步骤 1 打开命令提示符。

步骤 2 输入 `nslookup`。

将显示默认的 DNS 服务器和地址。确认这是预期的 DNS 服务器。

步骤 3 输入 `set type=SRV`。

步骤 4 输入每个 SRV 记录的名称。

例如，`_cisco-uds._tcp.exempldomain`

- 显示服务器和地址 — 可以访问 SRV 记录。
- 显示 `_cisco-uds_tcp.exempldomain: 不存在的域` — 您的 SRV 记录存在问题。

Cisco Anyconnect 部署工作流程

过程

	命令或操作	目的
步骤 1	应用配置文件，第 3 页	
步骤 2	自动进行 VPN 连接，第 4 页	
步骤 3	AnyConnect 文档参考，第 7 页	
步骤 4	会话参数，第 7 页	

Cisco AnyConnect 部署

应用配置文件

将 Cisco AnyConnect 安全移动客户端下载到其设备后，ASA 必须为应用程序提供配置文件。

Cisco AnyConnect 安全移动客户端的配置文件包括 VPN 策略信息，例如公司 ASA VPN 网关、连接协议（IPSec 或 SSL）以及按需策略。

您可以通过以下方式之一为 Cisco Jabber iPhone 和 iPad 版本配置应用程序配置文件：

ASDM

我们建议您在 ASA 设备管理器 (ASDM) 上使用配置文件编辑器定义 Cisco AnyConnect 安全移动客户端的 VPN 配置文件。

使用此方法时，VPN 配置文件会在客户端首次建立 VPN 连接后自动下载到 Cisco AnyConnect 安全移动客户端。您可以对所有设备和 OS 类型使用此方法，也可以在 ASA 上集中管理 VPN 配置文件。

有关详细信息，请参阅您相应版本的《Cisco AnyConnect 安全移动客户端管理员指南》中的创建和编辑 AnyConnect 配置文件主题。

iPCU

您可以使用通过 iPhone 配置实用程序 (iPCU) 创建的 Apple 配置文件来配置 iOS 设备。Apple 配置文件是一种 XML 文件，包含设备安全策略、VPN 配置信息、Wi-Fi、邮件和日历设置等信息。

高级步骤如下所示：

1. 使用 iPCU 创建 Apple 配置文件。
有关详细信息，请参阅 iPCU 的文档。
2. 将 XML 配置文件导出为 .mobileconfig 文件。

3. 将 .mobileconfig 文件通过电子邮件发送给用户。

用户打开文件后，将 AnyConnect VPN 配置文件和其他配置文件设置安装到客户端应用程序。

MDM

您可以使用通过第三方移动设备管理 (MDM) 软件创建的 Apple 配置文件来配置 iOS 设备。Apple 配置文件是一种 XML 文件，包含设备安全策略、VPN 配置信息、Wi-Fi、邮件和日历设置等信息。

高级步骤如下所示：

1. 使用 MDM 创建 Apple 配置文件。

有关使用 MDM 的信息，请参阅 Apple 文档。

2. 将 Apple 配置文件推送到注册的设备。

要为 Cisco Jabber Android 版本配置应用程序配置文件，请使用 ASA 设备管理器 (ASDM) 上的配置文件编辑器定义 Cisco AnyConnect 安全移动客户端的 VPN 配置文件。VPN 配置文件会在客户端首次建立 VPN 连接后自动下载到 Cisco AnyConnect 安全移动客户端。您可以对所有设备和 OS 类型使用此方法，也可以在 ASA 上集中管理 VPN 配置文件。有关详细信息，请参阅您相应版本的《Cisco AnyConnect 安全移动客户端管理员指南》中的创建和编辑 AnyConnect 配置文件主题。

自动进行 VPN 连接

当用户从公司 Wi-Fi 网络之外打开 Cisco Jabber 时，Cisco Jabber 需要 VPN 连接才能访问 Cisco UC 应用程序服务器。您可以将系统设置为允许 Cisco AnyConnect 安全移动客户端在后台自动建立 VPN 连接，从而确保为用户提供无缝连接体验。



注释 6023即使 VPN 设置为自动连接，VPN 也不会移动设备和Remote Access Expressway 之前启动，因为后者优先级较高。

设置受信任的网络连接

受信任网络检测功能可根据用户位置自动执行 VPN 连接，从而提升用户体验。当用户在公司 Wi-Fi 网络内部时，Cisco Jabber 可以直接接通 Cisco UC 基础设施。当用户离开公司 Wi-Fi 网络时，Cisco Jabber 会自动检测到位于受信任的网络之外。在这种情况下，Cisco AnyConnect Secure 移动客户端将发起 VPN，以确保连接到 UC 基础设施。



注释 受信任的网络检测功能与基于证书和基于密码的验证相配合。但是，基于证书的身份验证可提供最高程度的无缝式用户体验。

步骤 1 使用 ASDM 打开 Cisco AnyConnect 客户端配置文件。

步骤 2 列出客户端处于企业 Wi-Fi 网络内时接口可能收到的受信任 DNS 服务器和受信任 DNS 域名后缀。Cisco AnyConnect 客户端将对当前接口 DNS 服务器和域名后缀与配置文件中的设置进行比较。

注释 您必须指定所有 DNS 服务器，以确保受信任网络检测功能正常工作。如果您同时设置 TrustedDNSDomains 和 TrustedDNSServers，会话必须将要定义的两项设置同时匹配到受信任网络。

有关设置受信任网络检测的详细步骤，请参阅您对应版本的《Cisco AnyConnect 安全移动客户端管理员指南》中，配置 AnyConnect 功能（版本 2.5）或配置 VPN 访问（版本 3.0 或 3.1）一章中，受信任网络检测一节。

设置按需连接 VPN

Apple iOS 按需连接功能通过基于用户域自动进行 VPN 连接提升了用户体验。

当用户在公司 Wi-Fi 网络内部时，Cisco Jabber 可以直接接通 Cisco UC 基础设施。当用户离开公司 Wi-Fi 网络时，Cisco AnyConnect 会自动检测是否已连接到您在 AnyConnect 客户端配置文件中指定的域。如果是这样，应用程序将发起 VPN 连接，以确保连接到 UC 基础设施。设备上的所有应用程序（包括 Cisco Jabber）均可以利用此功能。



注释 按需连接仅支持通过证书进行身份验证的连接。

此功能提供以下选项：

- **始终连接** — Apple iOS 始终尝试与该列表中的域建立 VPN 连接。
- **视需要连接** — Apple iOS 只有在无法利用 DNS 解析地址时才尝试与该列表中的域建立 VPN 连接。
- **始终连接** — Apple iOS 始终尝试与该列表中的域建立 VPN 连接。



注意 Apple 计划在不久的将来删除“始终连接”选项。在删除“始终连接”选项后，用户可以选择“视需要连接”选项。在某些情况下，Cisco Jabber 用户在使用“视需要连接”选项时可能会出现一些问题。例如，如果 Cisco Unified Communications Manager 的主机名可在公司网络之外进行解析，则 iOS 将不会触发 VPN 连接。用户可以通过在发起呼叫之前手动启动 Cisco AnyConnect 安全移动客户端解决此问题。

步骤 1 使用 ASDM 配置文件编辑器、iPCU 或 MDM 软件打开 AnyConnect 客户端配置文件。

步骤 2 在 AnyConnect 客户端配置文件中，在“视需要连接”部分，输入可按需连接的域列表。

域列表可以包含通配符选项（例如，cucm.cisco.com、cisco.com 和 *.webex.com）。

在 Cisco Unified Communications Manager 上设置自动 VPN 访问

开始之前

- 必须将移动设备设置为通过基于证书的身份验证按需连接到 VPN。如需有关设置 VPN 连接的帮助，请联系您的 VPN 客户端和头端提供商。
- 有关 Cisco AnyConnect 安全移动客户端和 Cisco 自适应安全设备的要求，请参阅软件要求主题。
- 有关设置 Cisco AnyConnect 的信息，请参阅《Cisco AnyConnect VPN 客户端维护和操作指南》。

步骤 1 确定将引导客户端按需启动 VPN 的 URL。

a) 使用以下方法之一确定引导客户端按需启动 VPN 的 URL。

- 视需要连接
 - 配置 Cisco Unified Communications Manager 通过域名（不是 IP 地址）访问，并确保此域名无法在防火墙外部解析。
 - 将此域名包含在 Cisco AnyConnect 客户端连接的按需连接域名列表中的“视需要连接”列表中。
 - 始终连接
 - 将步骤 4 中的参数设置为不存在的域名。当用户在防火墙内部或外部时，不存在的域名会导致 DNS 查询失败。
 - 将此域名包含在 Cisco AnyConnect 客户端连接的按需连接域名列表中的“始终连接”列表中。
- URL 必须仅包含域名。不要包含协议或路径（例如，使用“cm8ondemand.company.com”而不是“https://cm8ondemand.company.com/vpn”）。

b) 在 Cisco AnyConnect 中输入 URL，并验证此域上的 DNS 查询是否失败。

步骤 2 打开 **Cisco Unified CM** 管理界面。

步骤 3 导航到用户的设备页面。

步骤 4 在产品特定配置布局部分的**按需 VPN URL** 字段中，输入您在步骤 1 中为 Cisco AnyConnect 确定和使用的 URL。

URL 只能是域名，不能是协议或路径。

步骤 5 选择保存。

当 Cisco Jabber 打开时，它会向 URL 发起 DNS 查询。如果此 URL 与您在此过程中定义的按需域名列表条目（例如，cisco.com）匹配，Cisco Jabber 将间接发起 AnyConnect VPN 连接。

下一步做什么

- 测试此功能。

- 在 iOS 设备的互联网浏览器中输入 URL，然后验证是否自动启动 VPN。您应在状态栏中看到一个 VPN 图标。
 - 验证 iOS 设备是否可以使用 VPN 连接到公司网络。例如，在公司内联网上访问网页。如果 iOS 设备无法连接，请联系您的 VPN 技术提供商。
 - 与您的 IT 部门核实，您的 VPN 不会限制访问某些类型的流量（例如，管理员是否将系统设置为只允许电子邮件和日历流量）。
- 验证您将客户端设置为直接连接到公司网络。

AnyConnect 文档参考

有关 AnyConnect 要求和部署的详细信息，请参阅您对应版本的文档，网址如下：<https://www.cisco.com/c/en/us/support/security/anyconnect-secure-mobility-client/products-user-guide-list.html>

会话参数

您可以配置 ASA 会话参数来改善安全连接的性能。为了实现最佳的用户体验，您应配置以下 ASA 会话参数：

- 数据包传输层安全 (DTLS) — DTLS 是一个 SSL 协议，它提供了可防止延迟和数据丢失的数据路径。
- 自动重连 — 自动重连或会话保持，允许 Cisco AnyConnect 安全移动客户端从会话终端中恢复，并重新建立会话。
- 会话保持 — 该参数允许 VPN 会话从服务中断中恢复，并重新建立连接。
- 空闲超时 — 空闲超时定义了一个时间段，如果在这段时间内没有任何通信活动，ASA 将会终止安全连接。
- 失效对端检测 (DTD) — DTD 确保 ASA 和 Cisco AnyConnect 安全移动客户端能够快速检测失败的连接。

设置 ASA 会话参数

我们建议您按照以下方式设置 ASA 会话参数，以优化 Cisco AnyConnect 安全移动客户端的最终用户体验。

步骤 1 设置 Cisco AnyConnect 以使用 DTLS。

有关详细信息，请参阅《Cisco AnyConnect VPN 客户端管理员指南》（版本 2.0）的使用 ASDM 配置 AnyConnect 功能一章中的通过 AnyConnect (SSL) 连接启用数据报传输层安全 (DTLS) 主题。

步骤 2 设置会话保持（自动重连）。

- a) 使用 ASDM 打开 VPN 客户端配置文件。

- b) 将自动重新连接行为参数设置为恢复后重新连接。

有关详细信息，请参阅您对应版本的《Cisco AnyConnect 安全移动客户端管理员指南》中，配置 *AnyConnect* 功能（版本 2.5）或配置 *VPN* 访问（版本 3.0 或 3.1）一章中的配置自动重连主题。

步骤 3 设置空闲超时值。

- a) 创建针对具体 Cisco Jabber 客户端的组策略。
- b) 将“空闲超时”的值设置为 30 分钟。

有关详细信息，请参阅您对应版本的《Cisco ASA 5580 自适应安全设备命令参考》的 *vpn* 空闲超时部分。

步骤 4 设置失效对端检测 (DPD)。

- a) 禁用服务器端 DPD。
- b) 启用客户端 DPD。

有关详细信息，请参阅《Cisco ASA 5500 系列配置指南》，配置 *VPN* 一章中启用和调整失效对端检测主题（使用 CLI、8.4 和 8.6）。

当地语言翻译版本说明

思科可能会在某些地方提供本内容的当地语言翻译版本。请注意，翻译版本仅供参考，如有任何不一致之处，以本内容的英文版本为准。