VPN 客户端

VPN 客户端概述

Cisco Unified IP 电话 的Cisco VPN 客户端用于为远程办公的员工创建安全的 VPN 连接。Cisco VPN 客户端的所有设置都是通过 Cisco Unified Communications Manager 管理 配置的。在企业内配置电话后，用户可以将其插入宽带路由器以实现即时连接。

注释 Unified Communications Manager 的美国出口无限制版本不提供 VPN 菜单及其选项。

VPN 客户端前提条件

预配置电话并在公司网络内建立初始连接以检索电话配置。您可以使用VPN进行后续连接，因为电话上已检索到该配置。

VPN 客户端配置任务流程

预配置电话并在公司网络内建立初始连接以检索电话配置。您可以使用VPN进行后续连接，因为电话上已检索到该配置。

过程

	命令或操作	目的
步骤 1	完成 Cisco IOS 前提条件， 第 2 页	完成 Cisco IOS 前提条件。如果要配置 Cisco IOS VPN，请执行此操作。

	命令或操作	目的
步骤 2	配置 Cisco IOS SSL VPN 以支持 IP 电话 ， 第 3 页	在 IP 电话上为 VPN 客户端配置 Cisco IOS。如果要配置 Cisco IOS VPN，请执行此操作。
步骤 3	满足 AnyConnect 的 ASA 前提条件 ， 第 4 页	满足 AnyConnect 的 ASA 前提条件。如果要配置 ASA VPN，请执行此操作。
步骤 4	在 IP 电话上为 VPN 客户端配置 ASA ， 第 5 页	在IP电话上为VPN客户端配置ASA。如果要配置ASA VPN，请执行此操作。
步骤 5	配置每个 VPN 网关的 VPN 集线器。	为避免用户在升级远程电话上的固件或配置信息时长时间延迟，将VPN集线器装在网络中靠近TFTP或Unified Communications Manager服务器的位置。如果这对您的网络而言不可行，您可以在 VPN 集线器旁边安装备用 TFTP 或负载服务器。
步骤 6	上传 VPN 集线器证书 ， 第 7 页	上传 VPN 集线器证书。
步骤 7	配置 VPN 网关 ， 第 7 页	配置 VPN 网关。
步骤 8	配置 VPN 组 ， 第 8 页	创建VPN组后，您可以添加刚配置的VPN网关中的一个网关。
步骤 9	执行下列操作之一： • 配置 VPN 配置文件 ， 第 9 页 • 配置 VPN 功能参数 ， 第 10 页	只有当您有多个 VPN 组时，才必须配置 VPN 配置文件。VPN 配置文件字段优先于 VPN 功能配置字段。
步骤 10	将 VPN 详细信息添加到通用电话配置文件 ， 第 12 页	将 VPN 组和 VPN 配置文件添加至通用电话配置文件。
步骤 11	将 Cisco Unified IP 电话 的固件升级至支持 VPN 的版本。	要运行 Cisco VPN 客户端，受支持的 Cisco Unified IP 电话必须在运行固件版本9.0(2)或更高版本。有关升级固件的更多信息，请参阅适用于您的 Cisco Unified IP 电话 型号的 Unified Communications Manager 的《*Cisco Unified IP* 电话管理指南》。
步骤 12	使用受支持的 Cisco Unified IP 电话建立 VPN 连接。	将您的 Cisco Unified IP 电话 连接到 VPN。

完成 Cisco IOS 前提条件

遵照此程序完成 Cisco IOS 前提条件。

步骤 1 安装 Cisco IOS 软件 15.1(2)T 或更高版本。

功能集/许可证：IOS ISR-G2 和 ISR-G3 通用（数据、安全与 UC）

功能集/许可证：IOS ISR 的高级安全

步骤 2 激活 SSL VPN 许可证。

配置 Cisco IOS SSL VPN 以支持 IP 电话

此程序用于完成 Cisco IOS SSL VPN 以支持 IP 电话。

步骤 1 在本地配置 Cisco IOS。

a) 配置网络接口。

示例：

```
router(config)# interface GigabitEthernet0/0
router(config-if)# description "outside interface"
router(config-if)# ip address 10.1.1.1 255.255.255.0
router(config-if)# duplex auto
router(config-if)# speed auto
router(config-if)# no shutdown
router#show ip interface brief (shows interfaces summary)
```

b) 配置静态路由和默认路由：

router(config)# **ip route** <目标_*ip*> < 掩码> < 网关_*ip*>

示例：

```
router(config)# ip route 10.10.10.0 255.255.255.0 192.168.1.1
```

步骤 2 生成并注册 CAPF 证书，以使用 LSC 对 IP 电话进行身份验证。

步骤 3 从 Unified Communications Manager 导入 CAPF 证书。

a) 从 Cisco Unified 操作系统管理中，选择**安全** > **证书管理**。

注释 此位置可能因 Unified Communications Manager 版本而有所变化。

b) 查找 Cisco_Manufacturing_CA 和 CAPF 证书。下载 .pem 文件并另存为 .txt 文件。

c) 在 Cisco IOS 软件上创建信任点。

```
hostname(config)# crypto pki trustpoint trustpoint_name
hostname(config-ca-trustpoint)# enrollment terminal
hostname(config)# crypto pki authenticate trustpoint
```

提示输入 base 64 编码的 CA 证书时，复制并粘贴所下载的 .pem 文件中的文本以及 BEGIN 和 END 行。对其他证书重复执行此程序。

d) 生成以下 Cisco IOS 自签证书并向 Unified Communications Manager 注册，或替换为从 CA 导入的证书。

- 生成自签名证书。

```
Router> enable
Router# configure terminal
Router(config)# crypto key generate rsa general-keys label <name>
<exportable -optional>Router(config)# crypto pki trustpoint <name>
Router(ca-trustpoint)# enrollment selfsigned
Router(ca-trustpoint)# rsakeypair <name> 2048 2048
Router(ca-trustpoint)#authorization username subjectname commonname
Router(ca-trustpoint)# crypto pki enroll <name>
Router(ca-trustpoint)# end
```

- 在 Unified Communications Manager 中的 VPN 配置文件上生成启用主机 ID 检查的自签证书。

示例：

```
Router> enable
Router# configure terminal
Router(config)# crypto key generate rsa general-keys label <name>
<exportable -optional>Router(config)# crypto pki trustpoint <name>
Router(ca-trustpoint)# enrollment selfsigned
Router(config-ca-trustpoint)# fqdn <full domain
name>Router(config-ca-trustpoint)# subject-name CN=<full domain
name>, CN=<IP>Router(ca-trustpoint)#authorization username
subjectname commonname
Router(ca-trustpoint)# crypto pki enroll <name>
Router(ca-trustpoint)# end
```

- 向 Unified Communications Manager 注册生成的证书。

  示例：

  ```
  Router(config)# crypto pki export <name> pem terminal
  ```

  复制终端中的文本并另存为 .pem 文件，然后使用 Cisco Unified 操作系统管理将其上传到 Unified Communications Manager。

步骤 4 在 Cisco IOS 上安装 AnyConnect。

从 cisco.com 下载 Anyconnect 程序包并安装到闪存。

示例：

```
router(config)#webvpn install svc
flash:/webvpn/anyconnect-win-2.3.2016-k9.pkg
```

步骤 5 配置 VPN 功能。

注释 要同时使用电话的证书和密码验证，使用电话 MAC 地址创建一个用户。用户名区分大小写。例如：

```
username CP-7975G-SEP001AE2BC16CB password k1kLGQIoxyCO4ti9 encrypted
```

满足 AnyConnect 的 ASA 前提条件

遵照以下程序来满足 AnyConnect 的 ASA 前提条件。

步骤 1 安装 ASA 软件（版本 8.0.4 或更高版本）和兼容的 ASDM。

步骤 2 安装兼容的 AnyConnect 程序包。

步骤 3 激活许可证。

a) 使用以下命令检查当前许可证的功能：

显示激活密钥详细信息

b) 如有需要，使用其他 SSL VPN 会话获取新的许可证并启用 Linksys 电话。

步骤 4 确保使用非默认 URL 配置隧道组，如下所示：

```
tunnel-group phonevpn type remote-access
tunnel-group phonevpn general-attribute
  address-pool vpnpool
tunnel-group phonevpn webvpn-attributes
  group-url https://172.18.254.172/phonevpn enable
```

配置非默认 URL 时，考虑以下事项：

- 如果 ASA 的 IP 地址具有公共 DNS 条目，可以将其替换为完全限定域名 (FQDN)。
- 在 Unified Communications Manager 中，只能在 VPN 网关上使用单个 URL（FQDN 或 IP 地址）。
- 最好使证书 CN 或使用者备用名称与 group-url 中的 FQDN 或 IP 地址匹配。
- 如果 ASA 证书 CN 或 SAN 与 FQDN 或 IP 地址不匹配，则取消选中 Unified Communications Manager 中的主机 ID 复选框。

在 IP 电话上为 VPN 客户端配置 ASA

此程序用于为 IP 电话上的 VPN 客户端配置 ASA。

注释 替换 ASA 证书将导致 Unified Communications Manager 不可用。

步骤 1 本地配置

a) 配置网络接口。

示例：

```
ciscoasa(config)# interface Ethernet0/0
ciscoasa(config-if)# nameif outside
ciscoasa(config-if)# ip address 10.89.79.135 255.255.255.0
ciscoasa(config-if)# duplex auto
ciscoasa(config-if)# speed auto
ciscoasa(config-if)# no shutdown
ciscoasa#show interface ip brief (shows interfaces summary)
```

b) 配置静态路由和默认路由。

ciscoasa(config)# **route** <interface_name> <ip_address> <netmask> <gateway_ip>

示例：

```
ciscoasa(config)# route outside 0.0.0.0 0.0.0.0 10.89.79.129
```

c) 配置 DNS。

示例：

```
ciscoasa(config)# dns domain-lookup inside
ciscoasa(config)# dns server-group DefaultDNS
ciscoasa(config-dns-server-group)# name-server 10.1.1.5 192.168.1.67 209.165.201.6
```

步骤 2 生成和注册 Unified Communications Manager 及 ASA 的必要证书。

从 Unified Communications Manager 导入以下证书。

- CallManager - TLS 握手期间验证 Cisco UCM（只有混合模式群集需要）
- Cisco_Manufacturing_CA - 使用厂商预装证书 (MIC) 验证 IP 电话。
- CAPF - 使用 LSC 验证 IP 电话。

要导入这些 Unified Communications Manager 证书，请执行以下操作：

a) 从 Cisco Unified 操作系统管理中，选择**安全** > **证书管理**。
b) 找到证书 Cisco_Manufacturing_CA 和 CAPF。下载 `.pem` 文件并保存 asa `.txt` 文件。
c) 在 ASA 上创建信任点。

示例：

```
ciscoasa(config)# crypto ca trustpoint trustpoint_name
ciscoasa(ca-trustpoint)# enrollment terminal
ciscoasa(config)# crypto ca authenticate trustpoint_name
```

提示输入 base 64 编码 CA 证书时，复制并粘贴所下载的 `.pem` 文件中的文本以及 BEGIN 和 END 行。对其他证书重复执行此程序。

d) 生成以下 ASA 自签证书并向 Unified Communications Manager 注册，或替换为从 CA 导入的证书。

- 生成自签名证书。

  示例：

  ```
  ciscoasa> enable
  ciscoasa# configure terminal
  ciscoasa(config)# crypto key generate rsa general-keys label <name>
  ciscoasa(config)# crypto ca trustpoint <name>
  ciscoasa(ca-trustpoint)# enrollment self
  ciscoasa(ca-trustpoint)# keypair <name>
  ciscoasa(config)# crypto ca enroll <name>
  ciscoasa(config)# end
  ```

- 在 Unified Communications Manager 中的 VPN 配置文件上生成启用主机 ID 检查的自签证书。

  示例：

  ```
  ciscoasa> enable
  ciscoasa# configure terminal
  ciscoasa(config)# crypto key generate rsa general-keys label <name>
  ciscoasa(config)# crypto ca trustpoint <name>
  ciscoasa(ca-trustpoint)# enrollment self
  ciscoasa(ca-trustpoint)# fqdn <full domain name>
  ciscoasa(config-ca-trustpoint)# subject-name CN=<full domain name>,CN=<IP>
  ciscoasa(config)# crypto ca enroll <name>
  ciscoasa(config)# end
  ```

- 向 Unified Communications Manager 注册生成的证书。

  示例：

  ```
  ciscoasa(config)# crypto ca export <name> identity-certificate
  ```

  复制终端中的文本并另存为 .pem 文件，然后将其上传至 Unified Communications Manager。

步骤 3 配置 VPN 功能。您可以使用以下示例 ASA 配置摘要，指导您进行配置。

注释 要同时使用电话的证书和密码验证，使用电话 MAC 地址创建一个用户。用户名区分大小写。例如：

```
ciscoasa(config)# username CP-7975G-SEP001AE2BC16CB password k1kLGQIoxyCO4ti9 encrypted
ciscoasa(config)# username CP-7975G-SEP001AE2BC16CB attributes
ciscoasa(config-username)# vpn-group-policy GroupPhoneWebvpn
ciscoasa(config-username)#service-type remote-access
```

ASA 证书配置

有关 *ASA* 证书配置的详细信息，请参阅在 ASA 上配置采用证书验证的 AnyConnect VPN 电话

上传 VPN 集线器证书

在设置 ASA 以支持 VPN 时，在 ASA 上生成证书。将生成的证书下载到您的 PC 或工作站，然后使用本部分所述步骤将其上传到 Unified Communications Manager。Unified Communications Manager 会将证书保存在 Phone-VPN-trust 列表中。

ASA 将在 SSL 握手期间发送此证书，Cisco Unified IP 电话 会将其与存储在 Phone-VPN-trust 列表中的值进行比较。

如果 Cisco Unified IP 电话 上安装了当地有效证书 (LSC)，它默认会发送其 LSC。

要使用设备级证书验证，请在 ASA 中安装根 MIC 或 CAPF 证书，以便 Cisco Unified IP 电话 受信任。

要将证书上传到 Unified Communications Manager，请使用 Cisco Unified 操作系统管理。

步骤 1 从 Cisco Unified 操作系统管理中，选择 **安全** > **证书管理**。

步骤 2 单击**上传证书**。

步骤 3 从**证书用途**下拉列表，选择 **Phone-VPN-trust**。

步骤 4 单击**浏览**选择您要上传的文件。

步骤 5 单击**上传文件**。

步骤 6 选择另一要上传的文件或单击**关闭**。

有关详细信息，请参阅证书管理一章。

配置 VPN 网关

确保您已为每个 VPN 网关配置 VPN 集线器。配置 VPN 集线器后，上传 VPN 集线器证书。有关详细信息，请参阅上传 VPN 集线器证书，第 7 页。

此程序用于配置 VPN 网关。

步骤 1 从 Cisco Unified CM 管理中，选择 **高级功能** > **VPN** > **VPN 网关**。

步骤 2 请执行以下任务之一：

a) 单击**新增**以配置新的配置文件。

b) 单击要复制的 VPN 网关旁边的**复制**。

c) 找到适当的 VPN 网关，然后修改设置以更新现有配置文件。

步骤 3 在 **VPN 网关配置**窗口中配置这些字段。有关详细信息，请参阅VPN 客户端的 VPN 网关字段，第 8 页。

步骤 4 单击**保存**。

VPN 客户端的 VPN 网关字段

下表介绍了 VPN 客户端的 VPN 网关字段。

表 *1: VPN* 客户端的 *VPN* 网关字段

字段	说明
VPN 网关名称	输入 VPN 网关的名称。
VPN 网关说明	输入 VPN 网关的说明。
VPN 网关 URL	输入网关中主 VPN 集线器的 URL。 **注释** 您必须通过组 URL 配置 VPN 集线器，并且将此 URL 用作网关 URL。 有关配置信息，请参阅 VPN 集线器文档，如： • *ASA* 上使用 *ASDM* 配置的 *SSL VPN* 客户端示例
此网关中的 VPN 证书	使用向上和向下箭头键分配证书给网关。如果您没有为网关分配证书，VPN 客户端将无法连接至该集线器。 **注释** 您可以分配最多 10 个证书给一个 VPN 网关，必须分配至少一个证书给每个网关。只有与电话-VPN-信任角色关联的证书才会显示在可用的 VPN 证书列表中。

配置 VPN 组

此程序用于配置 VPN 组。

步骤 1 从 Cisco Unified CM 管理中，选择 **高级功能** > **VPN** > **VPN 组**。

步骤 2 请执行以下任务之一：

a) 单击**新增**以配置新的配置文件。

b) 单击要复制现有 VPN 组的 VPN 组旁边的**复制**。

c) 找到适当的 VPN 组，然后修改设置以更新现有配置文件。

步骤 3 配置 **VPN 组配置**窗口中的字段。有关详细信息，请参阅VPN 客户端的 VPN 网关字段，第 8 页，查看字段说明详细信息。

步骤 4 单击**保存**。

VPN 客户端的 VPN 组字段

下表介绍了 VPN 客户端的 VPN 组字段。

表 *2: VPN* 客户端的 *VPN* 组字段

字段	定义
VPN 组名称	输入 VPN 组的名称。
VPN 组说明	输入 VPN 组的说明。
所有可用的 VPN 网关	滚动可查看所有可用的 VPN 网关。
此 VPN 组中的所选 VPN 网关	使用上下箭头按键可将可用的 VPN 网关移入或移出此 VPN 组。 如果 VPN 客户端遇到严重错误，不能连接至特定 VPN 网关，它将尝试移至列表中的下一个 VPN 网关。 **注释** 您可以添加最多三个 VPN 网关至 VPN 组。此外，VPN 组中的证书总数不能超过 10 个。

配置 VPN 配置文件

此程序用于配置 VPN 配置文件。

步骤 1 从 Cisco Unified CM 管理中，选择 **高级功能** > **VPN** > **VPN 配置文件**。

步骤 2 请执行以下任务之一：

a) 单击**新增**以配置新的配置文件。

b) 单击要复制的 VPN 配置文件旁边的**复制**以复制现有配置文件。

c) 要更新现有配置文件，请在 **VPN 配置文件查找条件**中指定适当的过滤器，单击**查找**，然后修改设置。

步骤 3 配置 **VPN 配置文件配置**窗口中的字段。有关详细信息，请参阅VPN 客户端的 VPN 配置文件字段，第 10 页，查看字段说明详细信息。

步骤 4 单击**保存**。

VPN 客户端的 VPN 配置文件字段

下表介绍了 VPN 配置文件字段详细信息。

表 *3: VPN* 配置文件字段详细信息

字段	定义
名称	输入 VPN 配置文件的名称。
说明	输入 VPN 配置文件的说明。
启用自动网络检测	选中此复选框时，VPN 客户端只能在它检测到位于公司网络外时运行。 默认设置：禁用。
MTU	输入最大传输单位 (MTU) 的大小，单位为字节。 默认值：1290 字节。
连接失败	此字段指定系统创建 VPN 通道时等待登录或连接操作完成的时长。 默认值：30 秒
启用主机 ID 检查	选中此复选框时，网关证书 subjectAltName 或 CN 必须与 VPN 客户端所连接的 URL 相符。 默认设置：启用
客户端验证方法	从下拉列表中，选择客户端验证方法： • 用户和密码 • 仅密码 • 证书（LSC 或 MIC）
启用密码持久性	选中此复选框时，用户密码会保存在电话中，直至出现失败的登录尝试，用户手动清除密码，或者电话重置或断电。

配置 VPN 功能参数

步骤 1 从 Cisco Unified CM 管理中，选择 **高级功能** > **VPN** > **VPN 功能配置**。

步骤 2 配置 **VPN 功能配置**窗口中的字段。有关详细信息，请参阅VPN 功能参数 ， 第 11 页。

步骤 3 单击**保存**。

执行以下任务：

- 将 Cisco Unified IP 电话的固件升级至支持 VPN 的版本。有关升级固件的更多信息，请参阅适用于您的 Cisco Unified IP 电话 型号的《*Cisco Unified IP* 电话管理指南》。
- 使用受支持的 Cisco Unified IP 电话建立 VPN 连接。

VPN 功能参数

下表介绍了 VPN 功能参数。

表 *4: VPN* 功能参数

字段	默认值
启用自动网络检测	设为 True 时，VPN 客户端仅在其检测到自己位于公司网络外时才会运行。 默认值：False
MTU	此字段指定最大传输单位： 默认值：1290 字节 最小值：256 字节 最大值：1406 字节
保持连接	此字段指定系统发送保持连接消息的速率。 **注释** 如果是小于 Unified Communications Manager 中指定的值的非零值，“VPN 集线器”中的保持连接设置将覆盖此设置。 默认值：60 秒 最小值：0 最大值：120 秒
连接失败	此字段指定系统创建 VPN 通道时等待登录或连接操作完成的时长。 默认值：30 秒 最小值：0 最大值：600 秒

字段	默认值
客户端验证方法	从下拉列表中，选择客户端验证方法： • 用户和密码 • 仅密码 • 证书（LSC 或 MIC） 默认值：用户和密码
启用密码持久性	该项为 True 时，如果“重置”按键或 “**#**” 用于重置，用户密码将保存在电话中。如果电话断电或您发起出厂重置，密码将不会保存，并且电话将提示输入凭证。 默认值：False
启用主机 ID 检查	设为 True 时，网关证书 subjectAltName 或 CN 必须与 VPN 客户端所连接的 URL 相符。 默认值：True

将 VPN 详细信息添加到通用电话配置文件

此程序用于将 VPN 详细信息添加到通用电话配置文件。

步骤 1 从 Cisco Unified CM 管理中，选择 **设备** > **设备设置** > **通用电话配置文件**。

步骤 2 单击**查找**，然后选择要将 VPN 详细信息添加到的通用电话配置文件。

步骤 3 在 **VPN 信息**部分，选择适当的 **VPN 组**和 **VPN 配置文件**。

步骤 4 依次单击**保存**、**应用配置**。

步骤 5 在应用配置窗口中单击**确定**。