

在ASA上配置AnyConnect VPN电话的证书身份验证

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[规则](#)

[电话证书类型](#)

[配置](#)

[配置](#)

[验证](#)

[故障排除](#)

[相关信息](#)

简介

本文档提供的配置示例显示如何配置自适应安全设备(ASA)和CallManager设备，以为在思科IP电话上运行的AnyConnect客户端提供证书身份验证。完成此配置后，思科IP电话可以建立与ASA的VPN连接，这些连接使用证书来保护通信。

先决条件

要求

尝试进行此配置之前，请确保满足以下要求：

- AnyConnect Premium SSL许可证
- Cisco VPN电话许可证的AnyConnect

根据ASA版本，您将看到ASA版本8.0.x的“AnyConnect for Linksys电话”或8.2.x或更高版本的“AnyConnect for Cisco VPN Phone”。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- ASA - 8.0(4)版或更高版本

- IP电话型号 — 7942 / 7962 / 7945 / 7965 / 7975
- 电话 — 8961/9951/9971 ，带9.1(1)版固件
- 电话 — 版本9.0(2)SR1S — 瘦呼叫控制协议(SCCP)或更高版本
- 思科统一通信管理器(CUCM)- 8.0.1.10000-4版或更高版本

此配置示例中使用的版本包括：

- ASA — 版本9.1(1)
- CallManager — 版本8.5.1.10000-26

有关CUCM版本中支持的电话的完整列表，请完成以下步骤：

1. 打开此URL:<https://<CUCM服务器IP地址>:8443/cucreports/systemReports.do>
2. 选择**Unified CM Phone Feature List > Generate a new report > Feature:虚拟私有网络。**

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

规则

有关文档约定的更多信息，请参考 [Cisco 技术提示约定。](#)

电话证书类型

思科在电话中使用以下证书类型：

- 制造商安装证书(MIC) — 所有7941、7961和更新型号的思科IP电话都包含MIC。MIC是由思科证书颁发机构(CA)签名的2048位密钥证书。当存在MIC时，无需安装本地有效证书(LSC)。为使CUCM信任MIC证书，它在其证书信任库中使用预安装的CA证书CAP-RTP-001、CAP-RTP-002和Cisco_Manufacturing_CA。
- LSC — 在您配置设备安全模式进行身份验证或加密后，LSC可保护CUCM和电话之间的连接。LSC拥有Cisco IP电话的公钥，该公钥由CUCM证书颁发机构代理功能(CAPF)私钥签名。这是首选方法（与使用MIC相反），因为只有管理员手动调配的思科IP电话才允许下载和验证CTL文件。**注意：**由于安全风险增加，思科建议仅将MIC用于LSC安装，而不是继续使用。将思科IP电话配置为使用MIC进行传输层安全(TLS)身份验证或用于任何其他目的的客户会自行承担风险。

配置

本部分提供有关如何配置本文档所述功能的信息。

注意：使用[命令查找工具（仅限注册用户）](#)可获取有关本部分所使用命令的详细信息。

配置

本文档介绍以下配置：

- ASA 配置

- CallManager 配置
- CallManager上的VPN配置
- IP电话上的证书安装

ASA 配置

ASA的配置与将AnyConnect客户端计算机连接到ASA时的配置几乎相同。但是，这些限制适用：

- 隧道组必须具有group-url。此URL将在CM的VPN网关URL下配置。
- 组策略不得包含拆分隧道。

此配置使用ASA设备安全套接字层(SSL)信任点中以前配置和安装的ASA (自签名或第三方)证书。有关详细信息，请参阅以下文档：

- [配置数字证书](#)
- [在 ASA 8.x 上手动安装第三方供应商证书以便与 WebVPN 一起使用的配置示例](#)
- [ASA 8.x :VPN访问与使用自签名证书的AnyConnect VPN客户端配置示例](#)

ASA的相关配置是：

```
ip local pool SSL_Pool 10.10.10.1-10.10.10.254 mask 255.255.255.0
group-policy GroupPolicy_SSL internal
group-policy GroupPolicy_SSL attributes
split-tunnel-policy tunnelall
vpn-tunnel-protocol ssl-client
```

```
tunnel-group SSL type remote-access
tunnel-group SSL general-attributes
address-pool SSL_Pool
default-group-policy GroupPolicy_SSL
tunnel-group SSL webvpn-attributes
authentication certificate
group-url https://asa5520-c.cisco.com/SSL enable
```

```
webvpn
enable outside
anyconnect image disk0:/anyconnect-win-3.0.3054-k9.pkg
anyconnect enable
```

```
ssl trust-point SSL outside
```

CallManager 配置

要从ASA导出证书并将证书作为Phone-VPN-Trust证书导入CallManager，请完成以下步骤：

1. 向CUCM注册生成的证书。
2. 检查用于SSL的证书。

```
ASA(config)#show run ssl
ssl trust-point SSL outside
```

3. 导出证书。

```
ASA(config)#crypto ca export SSL identity-certificate
```

隐私增强邮件(PEM)编码的身份证书如下：

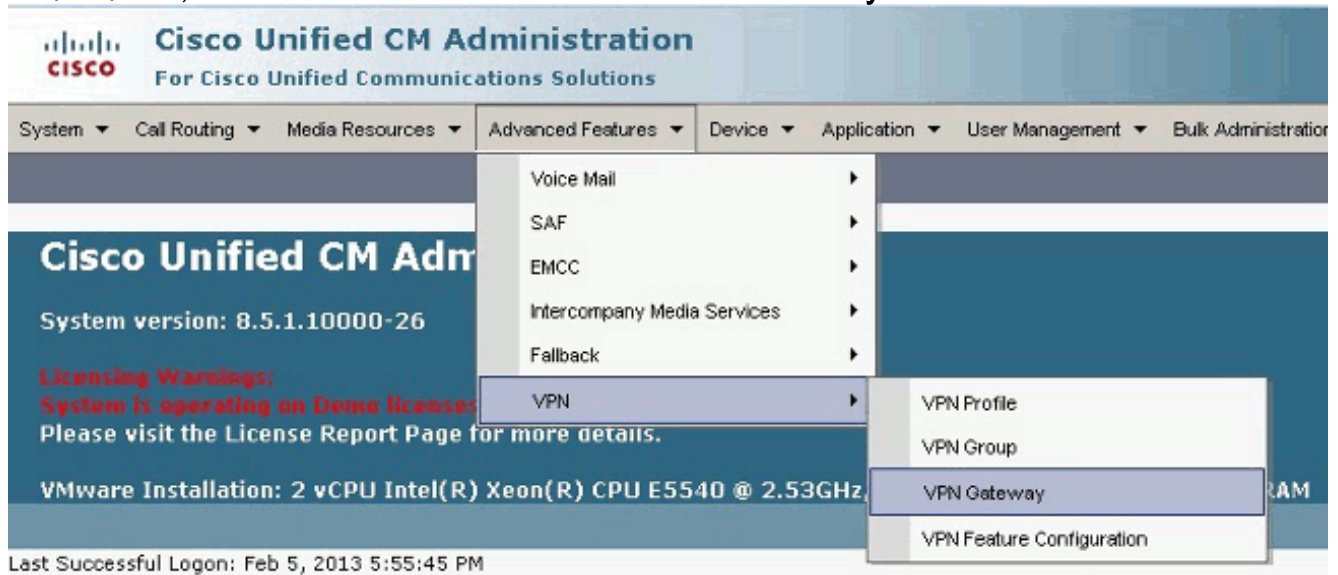
```
-----BEGIN CERTIFICATE-----ZHUXFjAUBgkqhkiG9w0BCQIWB0FTQTU1NDAwHhcNMTMwMTMwMTM1MzEwWhcNMjMw
MTI4MTM1MzEwWjAmMQwwCgYDVQQDEwNlZHUxZjAUBgkqhkiG9w0BCQIWB0FTQTU1
NDAwZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAMycrysjZ+MawKBx8Zk69SW4AR
FSpV6FPcUL7xsovhw6hsJE/2VDgd3pkawc5jcl5vkcpTkhjbf2xc4C1q6ZQwpahde22sdf1
wsidpQWq1DDrJD1We83L/oqmhkWJO7QfNrGZh0Lv9xOpR7BFpZd1yFyzwAPkoB11
-----END CERTIFICATE-----
```

4. 从终端复制文本并将其另存为.pem文件。

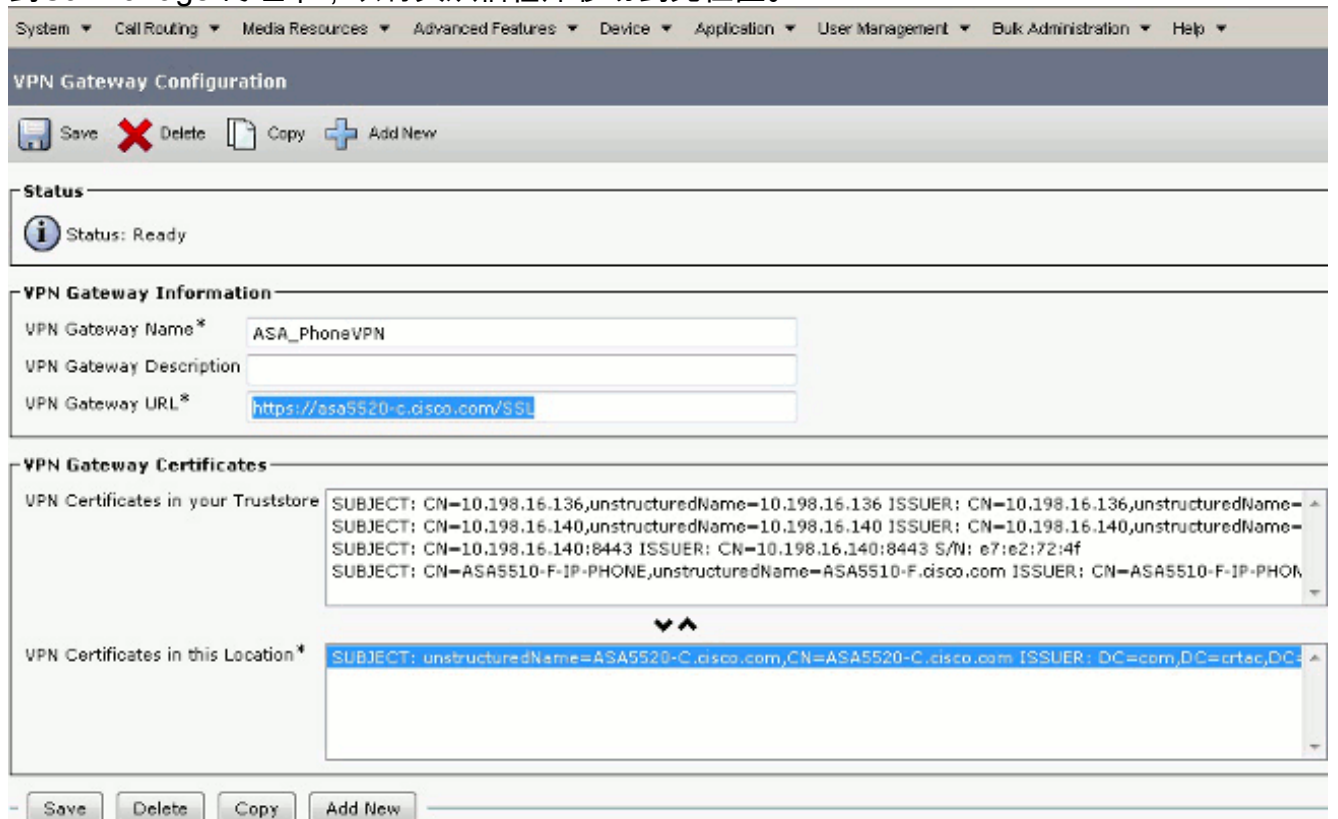
5. 登录CallManager并选择Unified OS Administration > Security > Certificate Management > Upload Certificate > Select Phone-VPN-trust以上传在上一步中保存的证书文件。

CallManager上的VPN配置

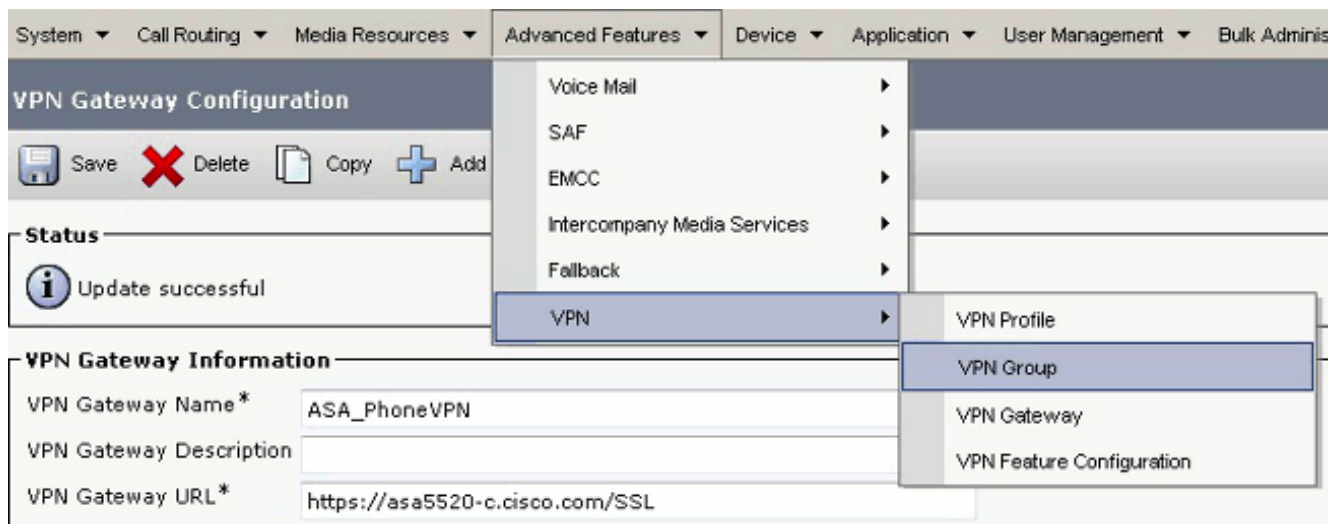
1. 导航至Cisco Unified CM管理。
2. 从菜单栏中，选择Advanced Features > VPN > VPN Gateway。



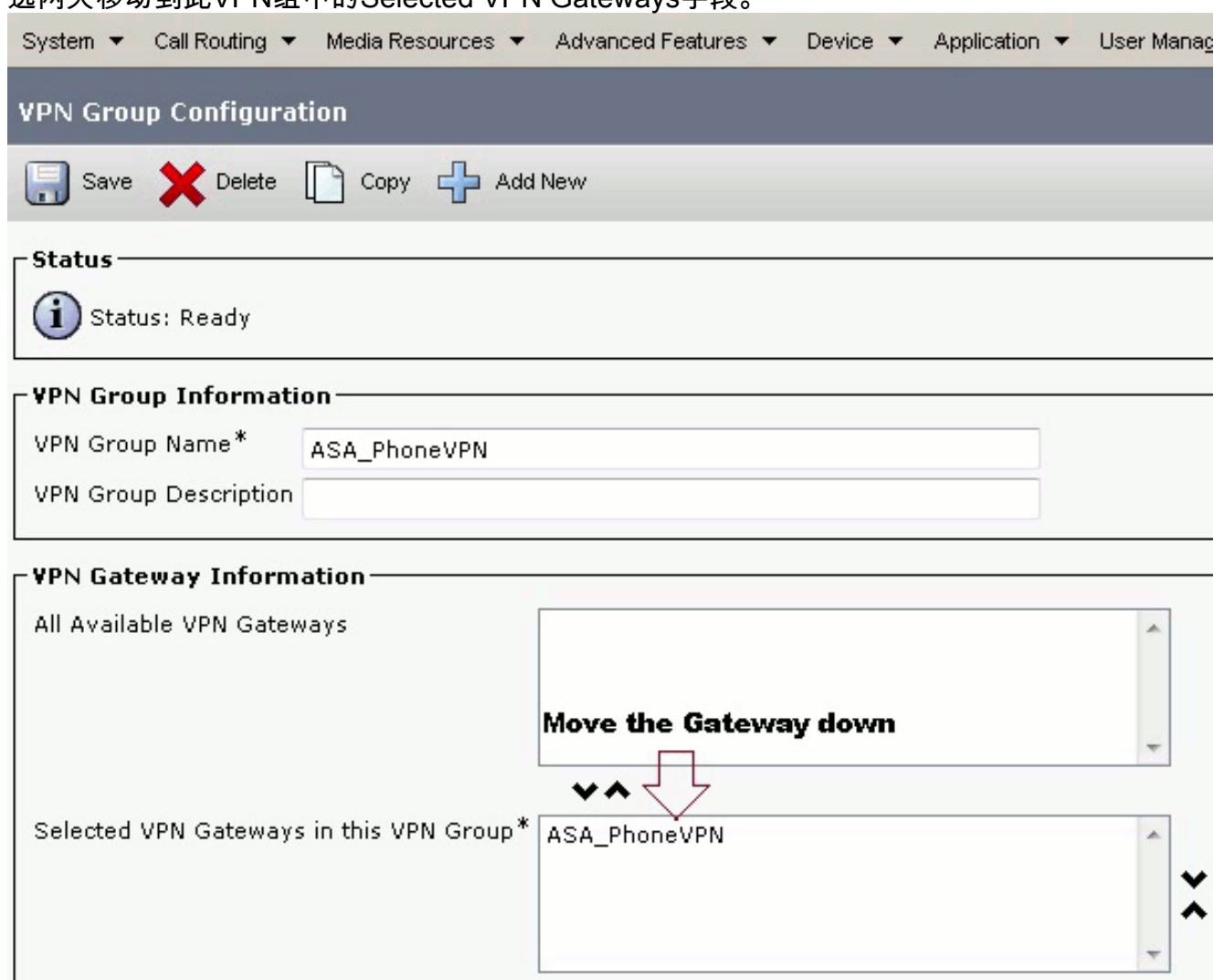
3. 在VPN网关配置窗口中，完成以下步骤：在VPN Gateway Name字段中，输入名称。这可以是任何名称。在VPN Gateway Description字段中，输入说明（可选）。在VPN Gateway URL字段中，输入在ASA上定义的group-url。在“此位置”字段的“VPN证书”中，选择之前上传到CallManager的证书，以将其从信任库移动到此位置。



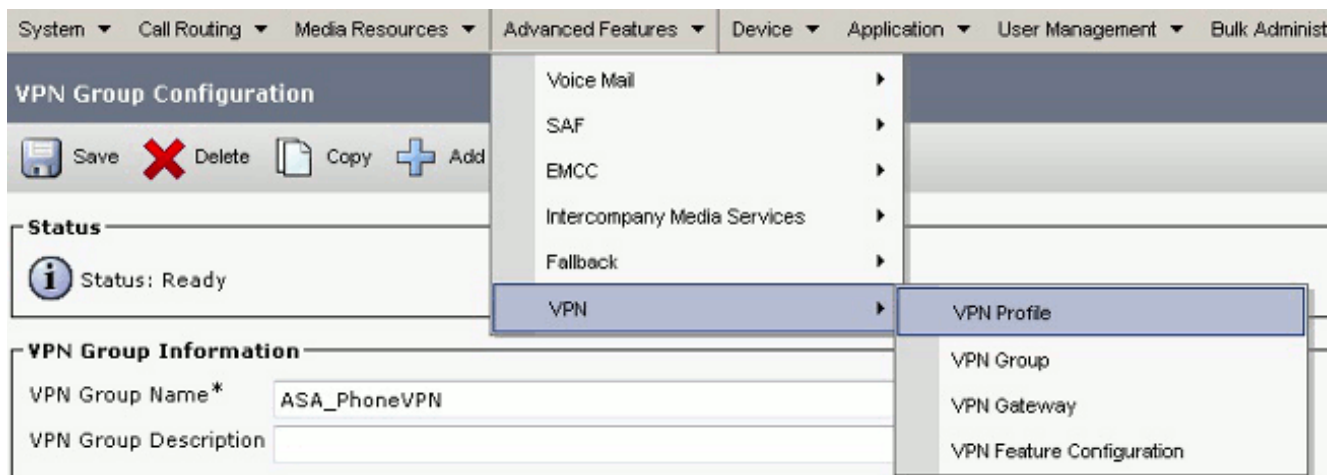
4. 从菜单栏中，选择Advanced Features > VPN > VPN Group。



5. 在All Available VPN Gateways字段中，选择之前定义的VPN Gateway。单击向下箭头，将所选网关移动到此VPN组中的Selected VPN Gateways字段。



6. 从菜单栏中，选择Advanced Features > VPN > VPN Profile。

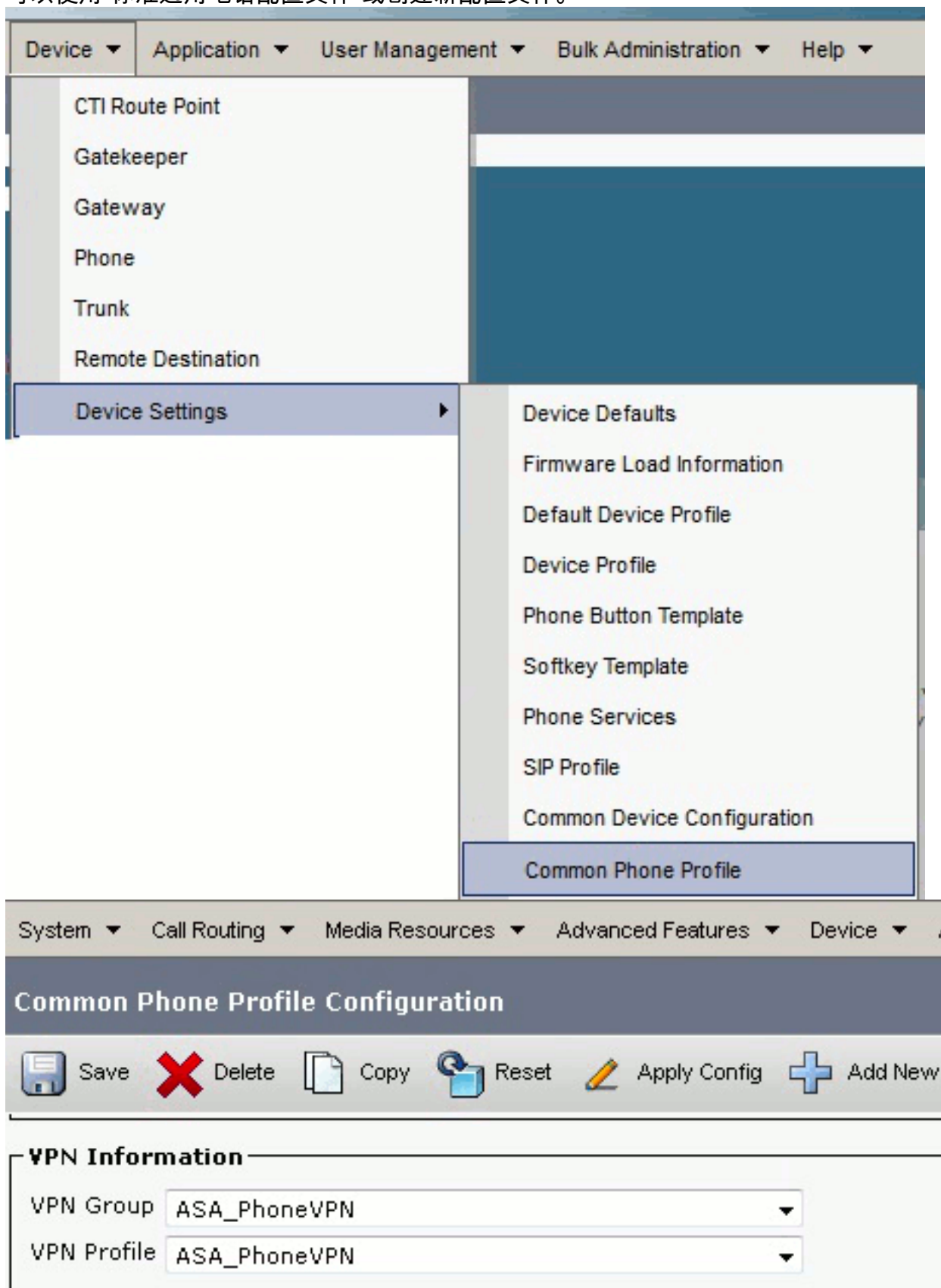


7. 要配置VPN配置文件，请填写标有星号(*)的所有字段。

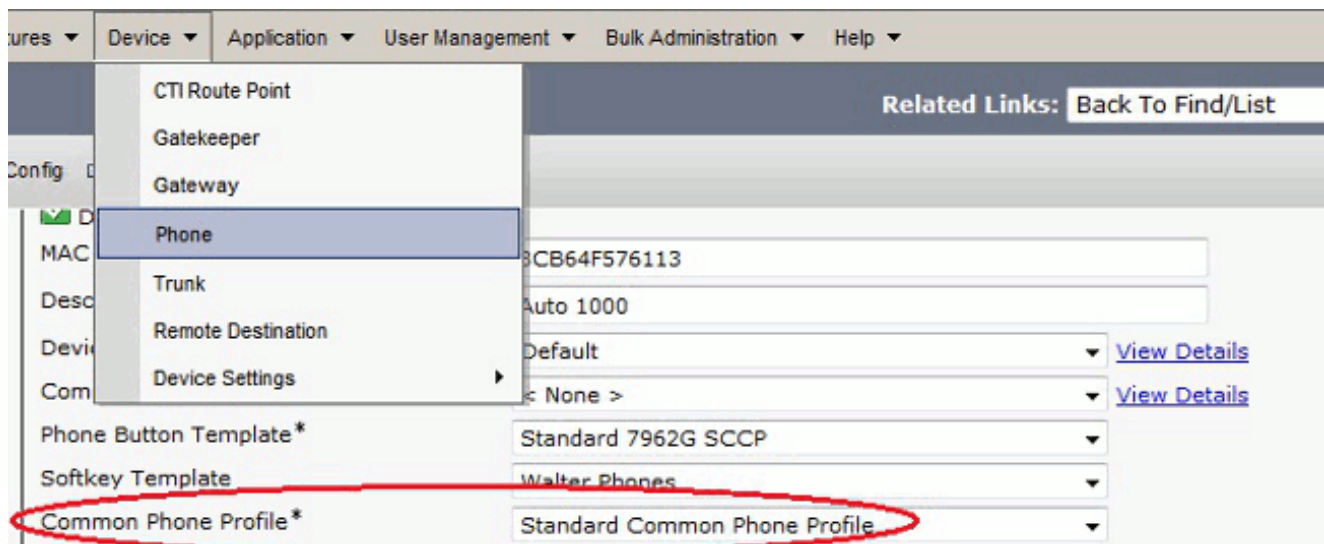
启用自动网络检测：如果启用，VPN电话会ping TFTP服务器，如果未收到响应，它会自动启动VPN连接。**启用主机ID检查：**如果启用，VPN电话将VPN网关URL的FQDN与证书的CN/SAN进行比较。如果客户端不匹配或使用带星号(*)的通配符证书，则客户端无法连接。**启用密码持久性：**这允许VPN电话缓存用户名和密码，以便下次尝试VPN。

8. 在Common Phone Profile Configuration窗口中，单击**Apply Config**以应用新的VPN配置。您

可以使用“标准通用电话配置文件”或创建新配置文件。



9. 如果为特定电话/用户创建了新配置文件，请转至“电话配置”窗口。在Common Phone Profile字段中，选择Standard Common Phone Profile。



10. 再次将电话注册到CallManager以下载新配置。





证书身份验证配置

要配置证书身份验证，请在CallManager和ASA中完成以下步骤：


1. 从菜单栏中，选择**Advanced Features > VPN > VPN Profile**。
2. 确认Client Authentication Method字段设置为Certificate。

System ▾ Call Routing ▾ Media Resources ▾ Advanced Features ▾ Device ▾ Application ▾

VPN Profile Configuration

 Save
  Delete
  Copy
  Add New

Status

 Status: Ready

VPN Profile Information

Name*

Description

Enable Auto Network Detect

Tunnel Parameters

MTU*

Fail to Connect*



Enable Host ID Check

Client Authentication

Client Authentication Method*

Enable Password Persistence

3. 登录CallManager。从菜单栏中，选择**Unified OS Administration > Security > Certificate Management > Find**。
4. 导出所选证书身份验证方法的正确证书：MIC:Cisco_Manufacturing_CA — 使用MIC对IP电话进行身份验证

Find Certificate List where File Name ▾ begins with ▾  

Certificate Name	Certificate Type	.PEM File
tomcat	certs	tomcat.pem
ipsec	certs	ipsec.pem
tomcat-trust	trust-certs	CUCM85.pem
ipsec-trust	trust-certs	CUCM85.pem
CallManager	certs	CallManager.pem
CAPF	certs	CAPF.pem
TVS	certs	TVS.pem
CallManager-trust	trust-certs	Cisco_Manufacturing_CA.pem
CallManager-trust	trust-certs	CAP-RTP-001.pem
CallManager-trust	trust-certs	Cisco_Root_CA_2048.pem
CallManager-trust	trust-certs	CAPF-18cf046e.pem
CallManager-trust	trust-certs	CAP-RTP-002.pem

LSC:思科证书颁发机构代理功能(CAPF) — 使用LSC对IP电话进行身份验证

Certificate Name	Certificate Type	.PEM File	.DER File
tomcat	certs	tomcat.pem	tomcat.der
ipsecc	certs	ipsecc.pem	ipsecc.der
tomcat-trust	trust-certs	CUCM85.pem	CUCM85.der
ipsecc-trust	trust-certs	CUCM85.pem	CUCM85.der
CallManager	certs	CallManager.pem	CallManager.der
CAPF	certs	CAPF.pem	CAPF.der
TVS	certs	TVS.pem	TVS.der
CallManager-trust	trust-certs	Cisco_Manufacturing_CA.pem	

5. 查找证书，即Cisco_Manufacturing_CA或CAPF。下载.pem文件并另存为.txt文件
6. 在ASA上创建新信任点，并使用之前保存的证书对信任点进行身份验证。当系统提示您输入base-64编码的CA证书时，选择文本并粘贴到下载的.pem文件中以及BEGIN和END行。示例显示：

```
ASA (config)#crypto ca trustpoint CM-Manufacturing
ASA(config-ca-trustpoint)#enrollment terminal
ASA(config-ca-trustpoint)#exit
ASA(config)#crypto ca authenticate CM-Manufacturing
ASA(config)#
```

```
<base-64 encoded CA certificate>
```

```
quit
```

7. 确认隧道组上的身份验证已设置为证书身份验证。

```
tunnel-group SSL webvpn-attributes
authentication certificate
group-url https://asa5520-c.cisco.com/SSL enable
```

IP电话上的证书安装

IP电话可以与MIC或LSC配合使用，但每个证书的配置过程不同。

MIC安装

默认情况下，支持VPN的所有电话都预装了MIC。7960和7940电话不附带MIC，需要特殊安装程序才能使LSC安全注册。

注意：思科建议仅将MIC用于LSC安装。思科支持LSC对与CUCM的TLS连接进行身份验证。由于MIC根证书可能受到危害，将电话配置为使用MIC进行TLS身份验证或用于任何其他目的的客户会自行承担风险。如果MIC受到危害，思科不承担任何责任。

LSC安装

1. 在CUCM上启用CAPF服务。
2. 激活CAPF服务后，分配电话指令以在CUCM中生成LSC。登录到Cisco Unified CM管理，然后选择**设备>电话**。选择您配置的电话。
3. 在“证书颁发机构代理功能(CAPF)信息”部分，确保所有设置都正确，并将操作设置为将来日期。

Certification Authority Proxy Function (CAPF) Information

Certificate Operation*

Authentication Mode*

Authentication String

Key Size (Bits)*

Operation Completes By (YYYY:MM:DD:HH)

Certificate Operation Status: None

Note: Security Profile Contains Addition CAPF Settings.

4. 如果“身份验证模式”(Authentication Mode)设置为空字符串或现有证书(Null String or Existing Certificate), 则无需进一步操作。
5. 如果Authentication Mode设置为字符串, 请在电话控制台中手动选择Settings > Security Configuration > **# > LSC > Update。

验证

使用本部分可确认配置能否正常运行。

ASA验证

```
ASA5520-C(config)#show vpn-sessiondb detail anyconnect
```

```
Session Type: AnyConnect Detailed
```

```
Username : CP-7962G-SEPXXXXXXXXXXXXX
Index : 57
Assigned IP : 10.10.10.2 Public IP : 172.16.250.15
Protocol : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License : AnyConnect Premium, AnyConnect for Cisco VPN Phone
Encryption : AnyConnect-Parent: (1)AES128 SSL-Tunnel: (1)AES128
DTLS-Tunnel: (1)AES128
Hashing : AnyConnect-Parent: (1)SHA1 SSL-Tunnel: (1)SHA1
DTLS-Tunnel: (1)SHA1Bytes Tx : 305849
Bytes Rx : 270069Pkts Tx : 5645
Pkts Rx : 5650Pkts Tx Drop : 0
Pkts Rx Drop : 0Group Policy :
GroupPolicy_SSL Tunnel Group : SSL
Login Time : 01:40:44 UTC Tue Feb 5 2013
Duration : 23h:00m:28s
Inactivity : 0h:00m:00s
NAC Result : Unknown
VLAN Mapping : N/A VLAN : none
```

```
AnyConnect-Parent Tunnels: 1
SSL-Tunnel Tunnels: 1
DTLS-Tunnel Tunnels: 1
```

```
AnyConnect-Parent:
Tunnel ID : 57.1
Assigned IP : 10.10.10.2 Public IP : 172.16.250.15
Encryption : AES128 Hashing : SHA1
```

Encapsulation: TLSv1.0 TCP Dst Port : 443
Auth Mode : Certificate
Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes
Client Type : AnyConnect Client Ver : Cisco SVC IPPhone Client v1.0 (1.0)
Bytes Tx : 1759 Bytes Rx : 799
Pkts Tx : 2 Pkts Rx : 1
Pkts Tx Drop : 0 Pkts Rx Drop : 0

SSL-Tunnel:
Tunnel ID : 57.2
Public IP : 172.16.250.15
Encryption : AES128 Hashing : SHA1
Encapsulation: TLSv1.0 TCP Src Port : 50529
TCP Dst Port : 443 Auth Mode : Certificate
Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes
Client Type : SSL VPN Client
Client Ver : Cisco SVC IPPhone Client v1.0 (1.0)
Bytes Tx : 835 Bytes Rx : 0
Pkts Tx : 1 Pkts Rx : 0
Pkts Tx Drop : 0 Pkts Rx Drop : 0

DTLS-Tunnel:
Tunnel ID : 57.3
Assigned IP : 10.10.10.2 Public IP : 172.16.250.15
Encryption : AES128 Hashing : SHA1
Encapsulation: DTLSv1.0 UDP Src Port : 51096
UDP Dst Port : 443 Auth Mode : Certificate
Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes
Client Type : DTLS VPN Client
Client Ver : Cisco SVC IPPhone Client v1.0 (1.0)
Bytes Tx : 303255 Bytes Rx : 269270
Pkts Tx : 5642 Pkts Rx : 5649
Pkts Tx Drop : 0 Pkts Rx Drop : 0

CUCM验证

The screenshot shows the 'Find and List Phones' interface in CUCM. The table below shows the results of a search for phones where the device name begins with 'SEP'. The status of the phone is 'Registered with 192.168.100.1' and the IP address is '10.10.10.2', both of which are circled in red. A red arrow points to the IP address column header.

Device Name	Description	Device Pool	Device Protocol	Status	IP Address
SEPXXXXXXXXXXXX	Auto 1001	Default	SCCP	Unknown	Unknown
SEPXXXXXXXXXXXX	Auto 1000	Default	SCCP	Registered with 192.168.100.1	10.10.10.2

故障排除

目前没有针对此配置的故障排除信息。

相关 Bug

- Cisco Bug ID [CSCtf09529](#) , 在CUCM中为8961、9951和9971电话添加对VPN功能的支持
- Cisco Bug ID [CSCuc71462](#),IP电话VPN故障切换需要8分钟
- Cisco Bug ID [CSCtz42052](#),IP电话SSL VPN支持非默认端口号

- Cisco Bug ID [CSCth96551](#) , 电话VPN用户+密码登录时不支持所有ASCII字符。
- Cisco Bug ID [CSCuj71475](#),IP电话VPN需要手动输入TFTP
- Cisco Bug ID [CSCum10683](#) ,IP电话不记录未接、已拨或已接呼叫

相关信息

- [技术支持和文档 - Cisco Systems](#)