AnyConnect VPN与Cisco IOS路由器配置示例的电话连接

Contents

Introduction

本文描述如何配置Cisco IOS路由器和呼叫管理器设备，以便Cisco IP电话能建立与Cisco IOS路由器的VPN连接。这些VPN连接是需要的为了获取与这两个客户端验证方法之一的通信：

- 验证、授权和统计(AAA)服务器或本地数据库
- 电话证书

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

本文档中的信息基于下列硬件和软件版本：

- Cisco IOS 15.1(2)T或以上
- 功能集/许可证：普遍性(数据&安全& UC) Cisco IOS综合服务路由器的(ISR)-G2
- 功能集/许可证：Cisco IOS ISR的高级安全
- Cisco Unified通信管理器(CUCM)版本8.0.1.100000-4或以上
- IP电话版本9.0(2)SR1S -内部呼叫控制协议(SCCP)或以上

对于在您的CUCM版本的支持的电话一张完全列表，请完成这些步骤：

1. 打开此URL ：**https:// *<CUCM服务器IP Address>:8443/cucreports/systemReports.do***
2. 选择**统一的CM电话功能列表>生成新报告>功能：虚拟专用网络。**

用于此配置示例的版本包括：

- Cisco IOS Router Release 15.1(4)M4
- Call Manager版本8.5.1.10000-26
- IP电话版本9.1(1)SR1S

The information in this document was created from the devices in a specific lab environment.All of the devices used in this document started with a cleared (default) configuration.If your network is live, make sure that you understand the potential impact of any command.

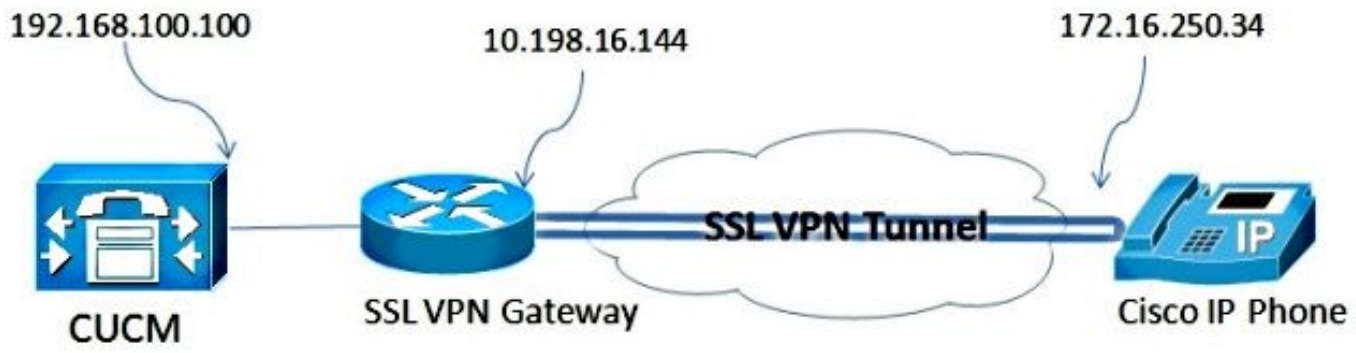
Configure

此部分包括需要的信息为了配置在本文描述的功能。

> **Note**: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。

网络拓扑

用于本文的拓扑包括一Cisco IP电话、Cisco IOS路由器作为安全套接字协议层(SSL) VPN网关和CUCM作为语音网关。



SSL VPN服务器配置

此部分描述如何配置Cisco IOS数据转发器为了允许入站SSL VPN连接。

常见配置步骤

1. 生成有1024个字节的长度的Rivest Shamir Adelman (RSA)键：

```
Router(config)#crypto key generate rsa general-keys label SSL modulus 1024
```

2. 创建自签证书的信任点，并且附有SSL RSA密钥：

```
Router(config)#crypto pki trustpoint server-certificate
enrollment selfsigned
usage ssl-server
serial-number
subject-name CN=10.198.16.144
revocation-check none
rsakeypair SSL
```

3. 一旦配置信任点，请登记自签证书用此命令：

```
Router(config)#crypto pki enroll server-certificate
% Include an IP address in the subject name? [no]: no
Generate Self Signed Router Certificate? [yes/no]: yes

Router Self Signed Certificate successfully created
```

4. Enable (event)在数据转发器的正确的AnyConnect程序包。电话不下载此程序包。但是，没有程序包， VPN隧道不设立。推荐使用最新的客户端软件版本可用在Cisco.com。此示例使用版本3.1.3103。

   在更旧的Cisco IOS版本中，这是命令为了enable (event)程序包：

```
Router(config)#webvpn install svc flash:anyconnect-win-3.1.03103-k9.pkg
```

   然而，在最新的Cisco IOS版本，这是命令：

```
Router(config)#crypto vpn anyconnect flash:/webvpn/anyconnect-win-
3.1.03103-k9.pkg sequence 1
```

5. 配置VPN网关。Webvpn gateway用于为了终止从用户的SSL连接。

```
Router(config)#crypto vpn anyconnect flash:/webvpn/anyconnect-win-
3.1.03103-k9.pkg sequence 1
```

   Note:任一使用的IP地址这里需要在相同子网作为电话接通的接口，或者网关需要直接地从接口来源在路由器。网关也用于为了定义路由器用于哪个认证为了验证本身对客户端。

6. 定义使用为了分配IP地址到客户端的本地地址池，当他们连接时：

```
Router(config)#crypto vpn anyconnect flash:/webvpn/anyconnect-win-
3.1.03103-k9.pkg sequence 1
```

与AAA认证的配置

此部分描述您需要为了配置AAA服务器或本地数据库为了验证您的电话的命令。如果计划使用仅使用证书的认证电话，请继续对下个部分。

配置用户数据库

路由器的本地数据库或一个外部AAA服务器可以用于认证：

- 为了配置本地数据库，请进入：

```
Router(config)#crypto vpn anyconnect flash:/webvpn/anyconnect-win-
3.1.03103-k9.pkg sequence 1
```

- 为了配置认证的一个远程AAA RADIUS服务器，请进入：

```
Router(config)#crypto vpn anyconnect flash:/webvpn/anyconnect-win-
3.1.03103-k9.pkg sequence 1
```

配置虚拟上下文和组策略

虚拟上下文用于为了定义管理VPN连接的属性，例如：

- 使用的哪个URL，当您连接
- 使用的哪个池为了分配客户端地址
- 使用的哪个认证方法

这些命令是使用AAA认证客户端上下文的示例：

```
Router(config)#crypto vpn anyconnect flash:/webvpn/anyconnect-win-
3.1.03103-k9.pkg sequence 1
```

与IP电话局部重要的认证(LSC)的配置客户端验证的

此部分描述您需要为了配置电话的基于认证的客户端验证的命令。然而，为了执行此，要求电话证书的多种类型知识：

- **制造商预装证书(MIC) -** MICs在所有7941， 7961和新型号Cisco IP电话包括。MICs是由Cisco Certificate Authority (CA)签字的2,048位关键证书。为了CUCM能委托MIC认证，它在其认证信任存储使用被事先装配的CA证书CAP-RTP-001、CAP-RTP-002和Cisco_Manufacturing_CA。由于此认证制造商提供，如名字所示，没有推荐使用此认证客户端验证。
- **LSC -**，在您配置认证或加密的后，设备安全模式LSC巩固CUCM和电话之间的连接。LSC拥有Cisco IP电话的公共密钥，由CUCM认证机关代理功能(CAPF)专用密钥签字。这是更多安全的方法(与使用MICs相对)。
  警告：由于增加的安全风险， Cisco独自地推荐使用MICs为LSC安装和不为持续的使用。配置Cisco IP电话为了使用MICs传输层安全的用户(TLS)认证，或者其他目的，那么责任自负。

在此配置示例中， LSC用于为了验证电话。

> **提示**：最安全的方式连接您的电话将使用双重认证，结合认证和AAA认证。如果结合其中每一使用的命令在一虚拟上下文以下，您能配置此。

配置信任点为了验证客户端证书

路由器必须有安装的CAPF认证为了验证从IP电话的LSC。为了获得该认证和在路由器上安装它，请完成这些步骤：

1. 去CUCM操作系统(OS)管理网页。
2. 选择**安全> Certificate Management**。
   Note:此位置也许更改基于CUCM版本。
3. 查找认证被标记**CAPF**，并且下载**.pem**文件。保存它作为**.txt**文件
4. 一旦certifcate被提取，请创建在路由器的一新的信任点，并且验证与CAPF的信任点，如显示这里。当提示输入base-64编码CA证书，与开始和结束行一起选择并且粘贴在下载的.pem文件的文本。

```
Router(config)#crypto pki trustpoint CAPF
enrollment terminal
authorization username subjectname commonname
revocation-check none
Router(config)#crypto pki authenticate CAPF
Router(config)#

<base-64 encoded CA certificate>

quit
```

注释的事：

- 因为认证必须在路由器上，手工安装登记方法终端。
- 当客户端建立联系时，要求**username命令的授权**为了告诉路由器怎样使用作为用户名。在这种情况下，它使用共同名称(CN)。
- 因为电话证书没有被定义的一证书撤销列表(CRL)撤销检查需要被禁用。因此，除非是失效的，连接发生故障，并且公共密钥基础设施(PKI)调试显示此输出：

```
Jun 17 21:49:46.695: CRYPTO_PKI: (A0076) Starting CRL revocation check
Jun 17 21:49:46.695: CRYPTO_PKI: Matching CRL not found
Jun 17 21:49:46.695: CRYPTO_PKI: (A0076) CDP does not exist. Use SCEP to
query CRL.
Jun 17 21:49:46.695: CRYPTO_PKI: pki request queued properly
Jun 17 21:49:46.695: CRYPTO_PKI: Revocation check is complete, 0
Jun 17 21:49:46.695: CRYPTO_PKI: Revocation status = 3
Jun 17 21:49:46.695: CRYPTO_PKI: status = 0: poll CRL
Jun 17 21:49:46.695: CRYPTO_PKI: Remove session revocation service providers
CRYPTO_PKI: Bypassing SCEP capabilies request 0
Jun 17 21:49:46.695: CRYPTO_PKI: status = 0: failed to create GetCRL
Jun 17 21:49:46.695: CRYPTO_PKI: enrollment url not configured
Jun 17 21:49:46.695: CRYPTO_PKI: transaction GetCRL completed
Jun 17 21:49:46.695: CRYPTO_PKI: status = 106: Blocking chain verification
callback received status
Jun 17 21:49:46.695: CRYPTO_PKI: (A0076) Certificate validation failed
```

配置虚拟上下文和组策略

配置的这部分类似于配置以前使用，除了两点：

- 认证方法
- 信任点上下文用途为了验证电话

命令显示得这里：

```
Jun 17 21:49:46.695: CRYPTO_PKI: (A0076) Starting CRL revocation check
Jun 17 21:49:46.695: CRYPTO_PKI: Matching CRL not found
Jun 17 21:49:46.695: CRYPTO_PKI: (A0076) CDP does not exist. Use SCEP to
query CRL.
Jun 17 21:49:46.695: CRYPTO_PKI: pki request queued properly
Jun 17 21:49:46.695: CRYPTO_PKI: Revocation check is complete, 0
```

```
Jun 17 21:49:46.695: CRYPTO_PKI: Revocation status = 3
Jun 17 21:49:46.695: CRYPTO_PKI: status = 0: poll CRL
Jun 17 21:49:46.695: CRYPTO_PKI: Remove session revocation service providers
CRYPTO_PKI: Bypassing SCEP capabilies request 0
Jun 17 21:49:46.695: CRYPTO_PKI: status = 0: failed to create GetCRL
Jun 17 21:49:46.695: CRYPTO_PKI: enrollment url not configured
Jun 17 21:49:46.695: CRYPTO_PKI: transaction GetCRL completed
Jun 17 21:49:46.695: CRYPTO_PKI: status = 106: Blocking chain verification
callback received status
Jun 17 21:49:46.695: CRYPTO_PKI: (A0076) Certificate validation failed
```

呼叫管理器配置

此部分描述呼叫管理器配置步骤。

从路由器导出自已签署的或身份认证对CUCM

为了从路由器导出认证和导入认证到呼叫管理器作为电话VPN信任认证，请完成这些步骤：

1. 检查用于SSL的认证。

   ```
   Router#show webvpn gateway SSL
   SSL Trustpoint: server-certificate
   ```

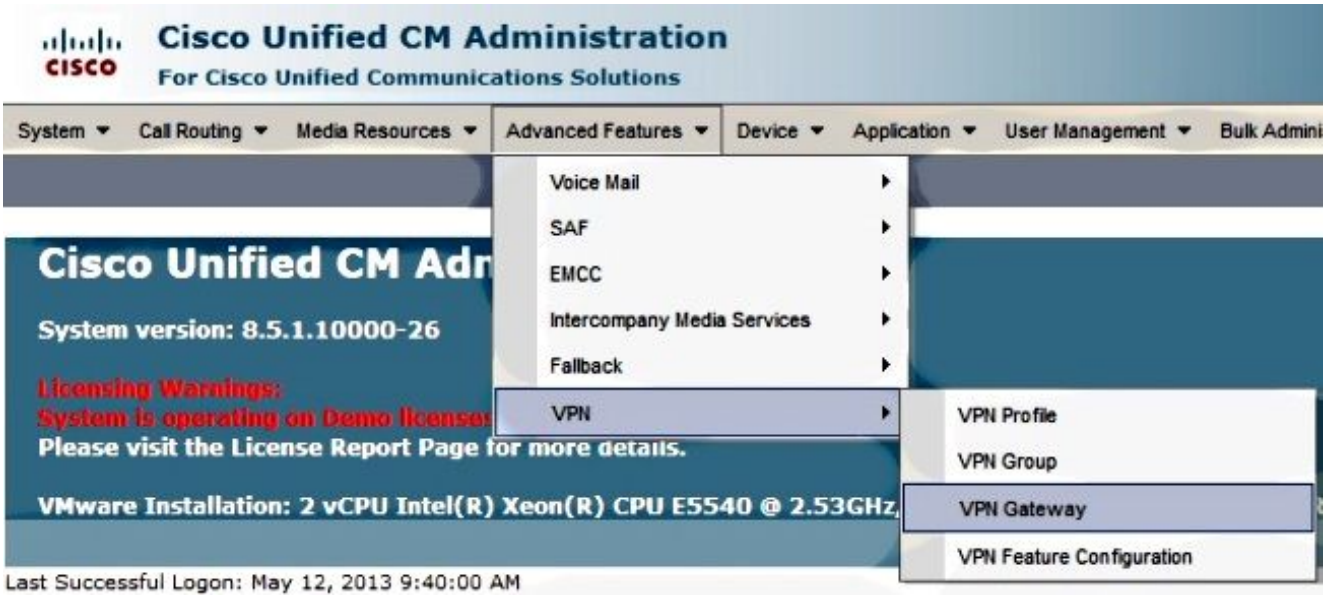
2. 导出认证。

   ```
   Router(config)#crypto pki export server-certificate pem terminal
   The Privacy Enhanced Mail (PEM) encoded identity certificate follows:
   -----BEGIN CERTIFICATE-----

   <output removed>

   -----END CERTIFICATE-----
   ```

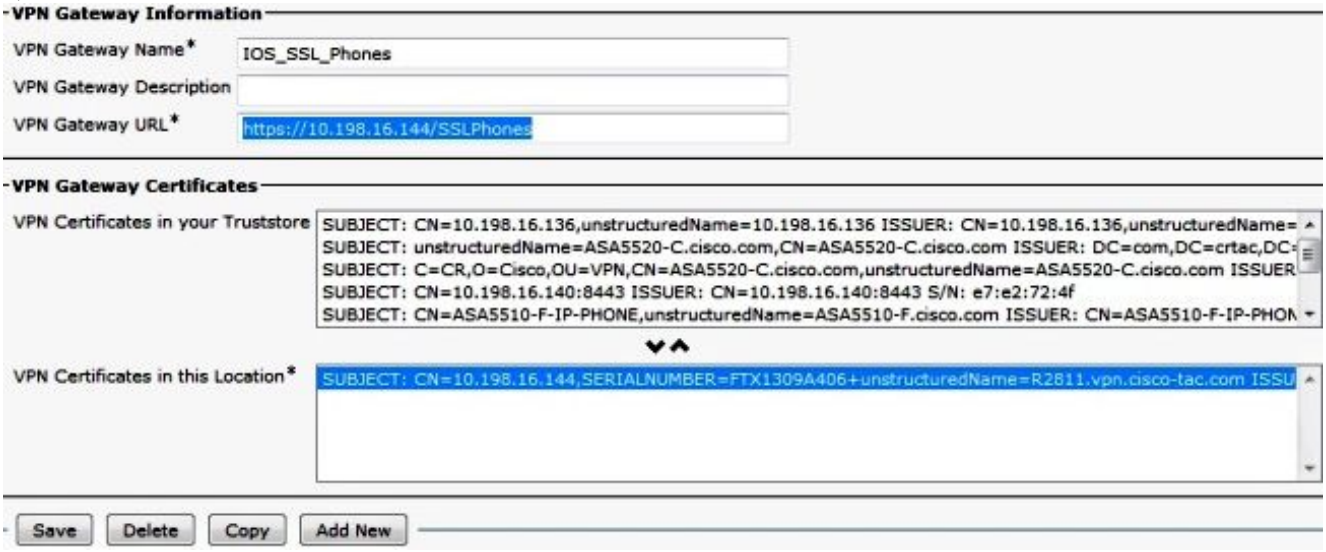
3. 从终端复制文本并且保存它作为.pem文件。
4. 登陆到呼叫管理器，并且选择**统一的OS管理> Security > Certificate Management >加载认证>挑选电话VPN信任**为了加载在上一步保存的证书文件。

配置VPN网关、组和配置文件在CUCM

1. 连接对**Cisco Unified CM管理**。
2. 从菜单栏，请选择**高级特性> VPN > VPN网关。**

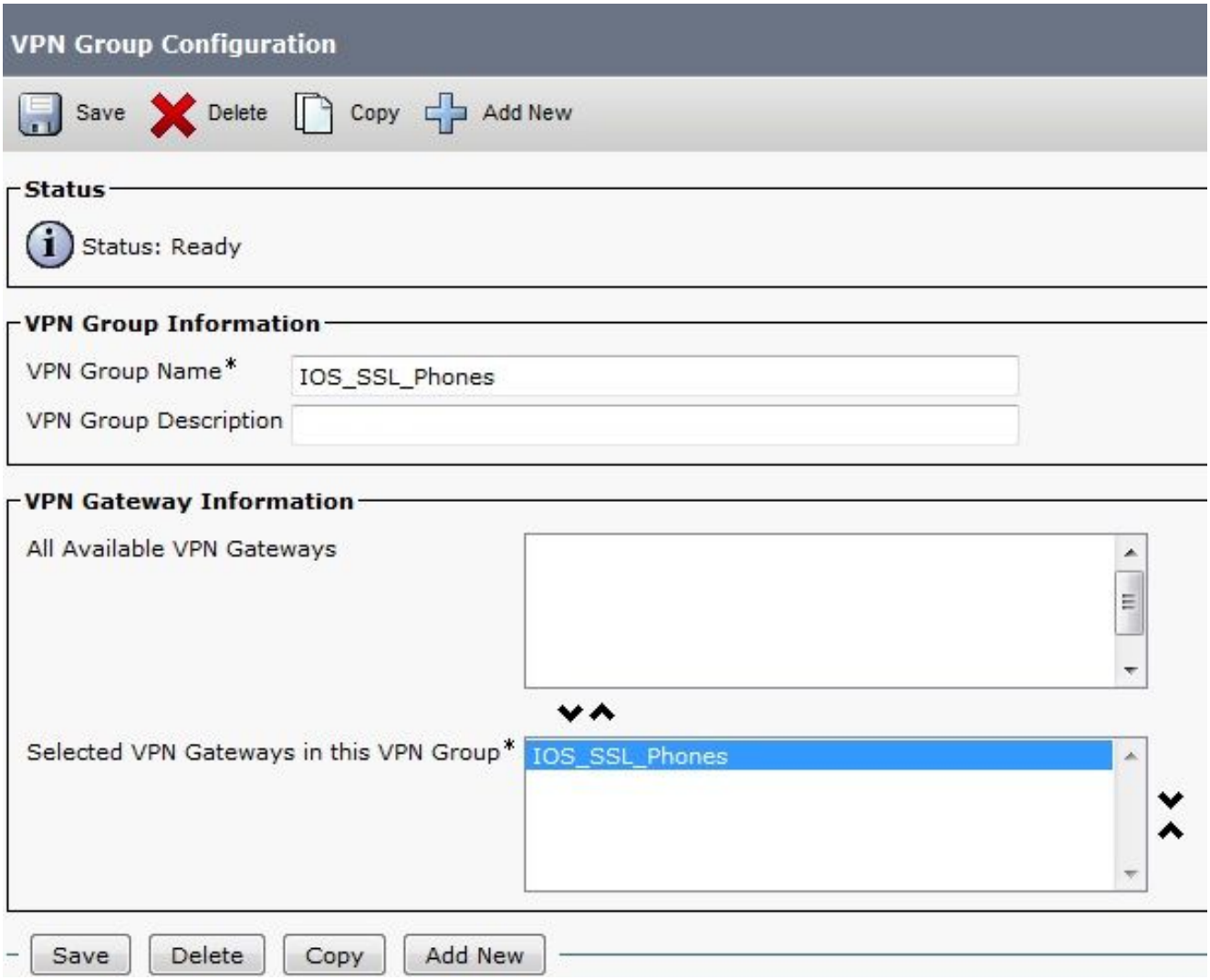


3. 在VPN网关配置窗口，请完成这些步骤：
在VPN网关名称字段，请输入名字。这可以是所有名字。在VPN网关说明字段，请输入说明(可选)。在VPN网关URL字段，请输入组URL定义在路由器。在此Location字段的VPN证书，请选择以前被加载到呼叫管理器为了从信任存储搬到它此位置的认证。

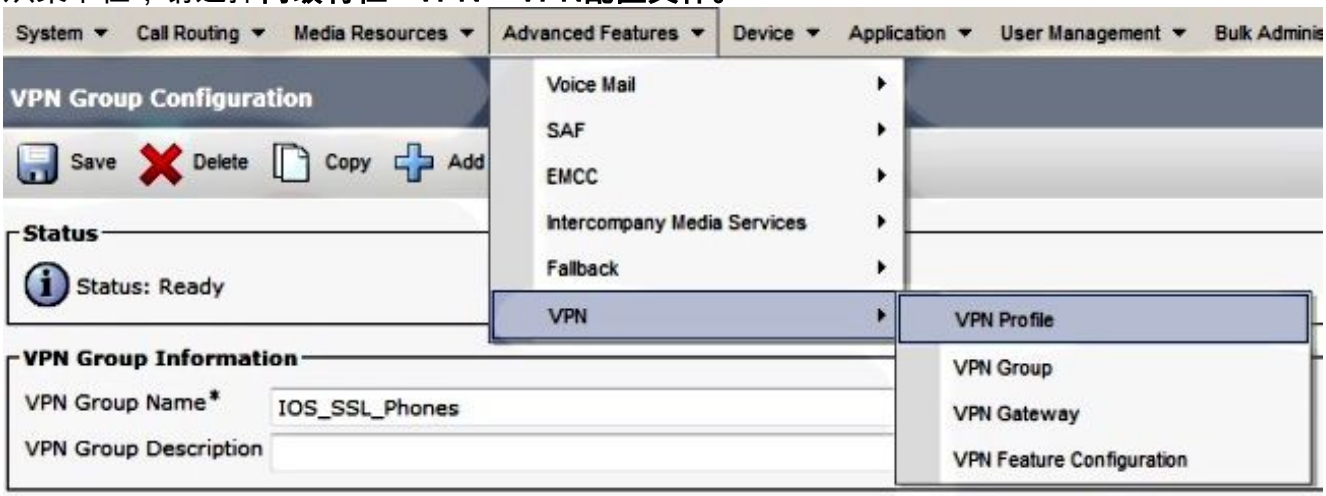


4. 从菜单栏，请选择**高级特性> VPN > VPN组。**

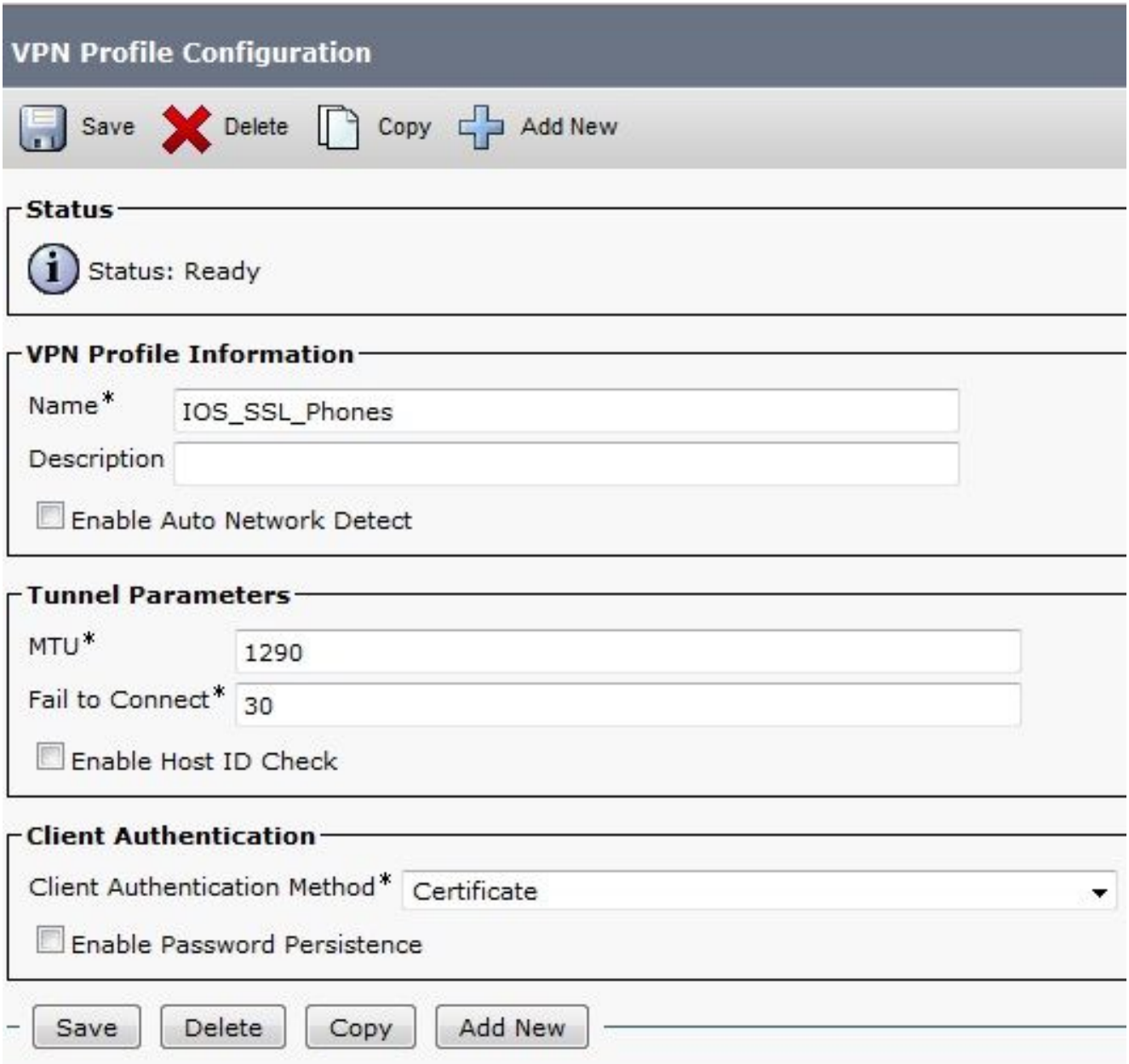
5. 在所有可用的VPN网关领域，请选择**VPN网关**先前定义。点击下箭头为了移动所选的网关向在此VPN组字段的所选的VPN网关。



6. 从菜单栏，请选择**高级特性> VPN > VPN配置文件。**



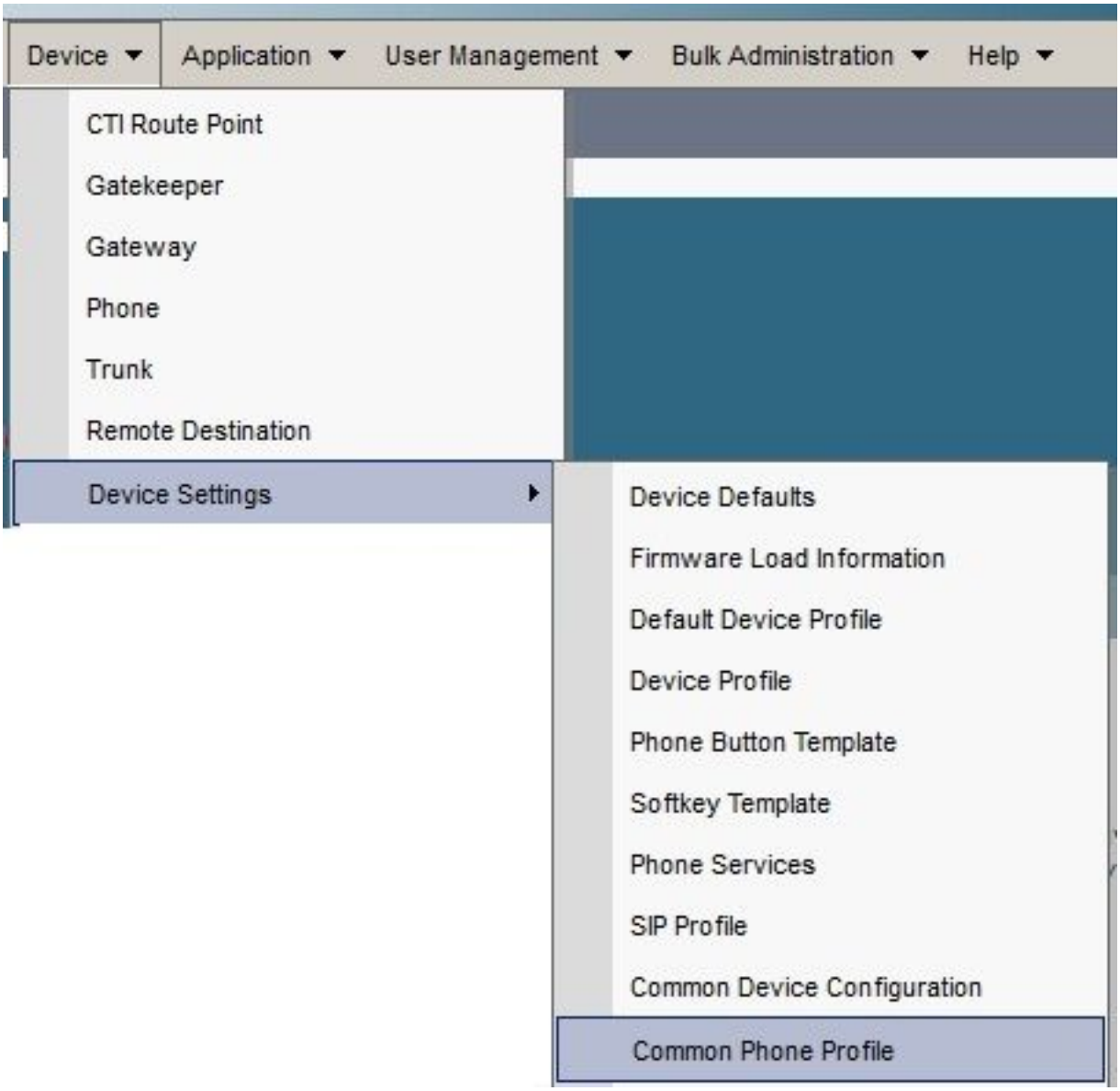
7. 为了配置VPN配置文件，请填入用星号(*)标记的所有字段。

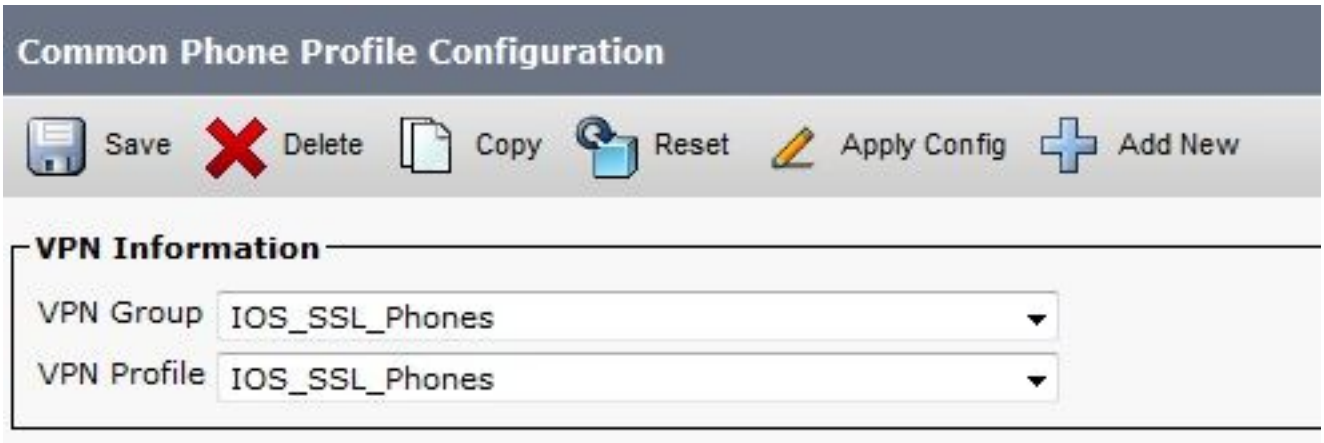


Enable (event)自动网络发现：如果能够的话， VPN电话连接TFTP server。如果无响应被接受，自动起动VPN连接。**Enable (event)主机标识符检查：**如果能够的话， VPN电话对CN/Storage区域网络(SAN)比较VPN网关URL的完全合格的域名(FQDN)认证。客户端不能连接，如果这些项目不配比或，如果使用与星号(*)的一个通配符认证。**特权密码持续时间：**这允许VPN电话缓存下个VPN尝试的用户名和密码。

适用于组和配置文件有普通的电话配置文件的IP电话

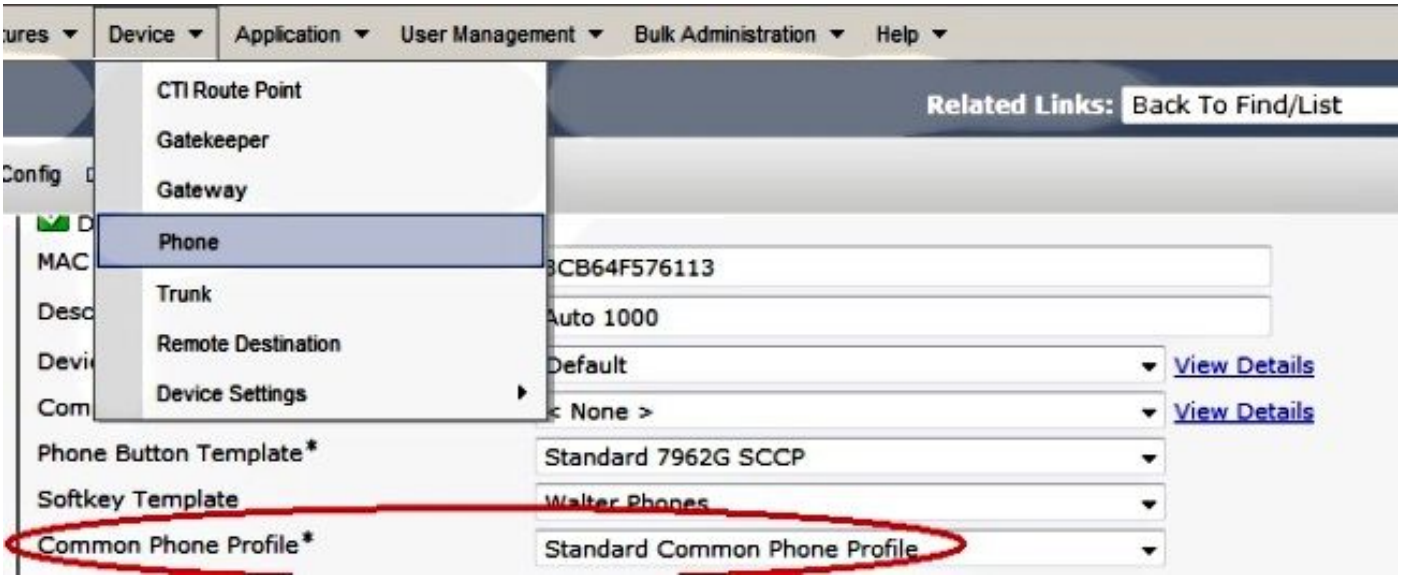
在普通的电话配置文件配置窗口，请点击**运用设置**为了运用新的VPN配置。您能使用标准的**普通的电话配置文件**或创建新配置文件。





适用于普通的电话配置文件IP电话

如果创建了特定电话/用户的一新配置文件，请连接对**Phone Configuration窗口**。在普通的电话配置文件字段，请选择**标准的普通的电话**配置文件。



在Cisco IP电话上安装局部重要的证书(LSC)

以下指南可以用于在Cisco IP电话上安装局部重要的证书。 如果使用LSC使用，此步骤只是需要的认证。 不要求LSC安装认证使用Manufacterer预装证书(MIC)或用户名和密码。

[在一个电话上安装LSC CUCM簇安全模式设置对不安全](#)。

再注册电话到呼叫管理器为了下载新的配置

这是最终步骤在配置流程中。

Verify

路由器验证

为了检查VPN会话的统计数据在路由器的，您能使用这些命令，并且检查输出之间的区别(突出显示)用户名和证书验证：

用户名/密码认证：

```
Router#show webvpn session user phones context SSL
Session Type : Full Tunnel
Client User-Agent : Cisco SVC IPPhone Client v1.0 (1.0)

Username : phones                Num Connection : 1
Public IP : 172.16.250.34 VRF Name : None
Context : SSL Policy Group : SSLPhones
Last-Used : 00:00:29 Created : 15:40:21.503 GMT
Fri Mar 1 2013
Session Timeout : Disabled Idle Timeout : 2100
DPD GW Timeout : 300 DPD CL Timeout : 300
Address Pool : SSL MTU Size : 1290
Rekey Time : 3600 Rekey Method :
Lease Duration : 43200
Tunnel IP : 10.10.10.1 Netmask : 255.255.255.0
Rx IP Packets : 106 Tx IP Packets : 145
CSTP Started : 00:11:15 Last-Received : 00:00:29
```

```
CSTP DPD-Req sent : 0 Virtual Access : 1
Msie-ProxyServer : None Msie-PxyPolicy : Disabled
Msie-Exception :
Client Ports : 51534
DTLS Port : 52768
Router#

Router#show webvpn session context all
WebVPN context name: SSL
Client_Login_Name  Client_IP_Address  No_of_Connections  Created  Last_Used
phones             172.16.250.34             1         00:30:38  00:00:20
```

证书验证：

```
Router#show webvpn session user SEP8CB64F578B2C context all
Session Type : Full Tunnel
Client User-Agent : Cisco SVC IPPhone Client v1.0 (1.0)

Username : SEP8CB64F578B2C      Num Connection : 1
Public IP : 172.16.250.34 VRF Name : None
CA Trustpoint  : CAPF
Context : SSL Policy Group :
Last-Used : 00:00:08 Created : 13:09:49.302 GMT
Sat Mar 2 2013
Session Timeout : Disabled Idle Timeout : 2100
DPD GW Timeout : 300 DPD CL Timeout : 300
Address Pool : SSL MTU Size : 1290
Rekey Time : 3600 Rekey Method :
Lease Duration : 43200
Tunnel IP : 10.10.10.2 Netmask : 255.255.255.0
Rx IP Packets : 152 Tx IP Packets : 156
CSTP Started : 00:06:44 Last-Received : 00:00:08
CSTP DPD-Req sent : 0 Virtual Access : 1
Msie-ProxyServer : None Msie-PxyPolicy : Disabled
Msie-Exception :
Client Ports : 50122
DTLS Port : 52932


Router#show webvpn session context all
WebVPN context name: SSL
Client_Login_Name  Client_IP_Address  No_of_Connections  Created  Last_Used
SEP8CB64F578B2C    172.16.250.34             1         3d04h     00:00:16
```

CUCM验证

确认IP电话向有分配的地址的呼叫管理器登记路由器提供给SSL连接。

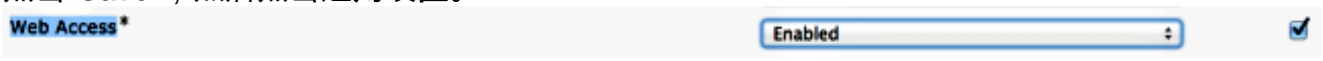
Troubleshoot

在SSL VPN服务器的调试

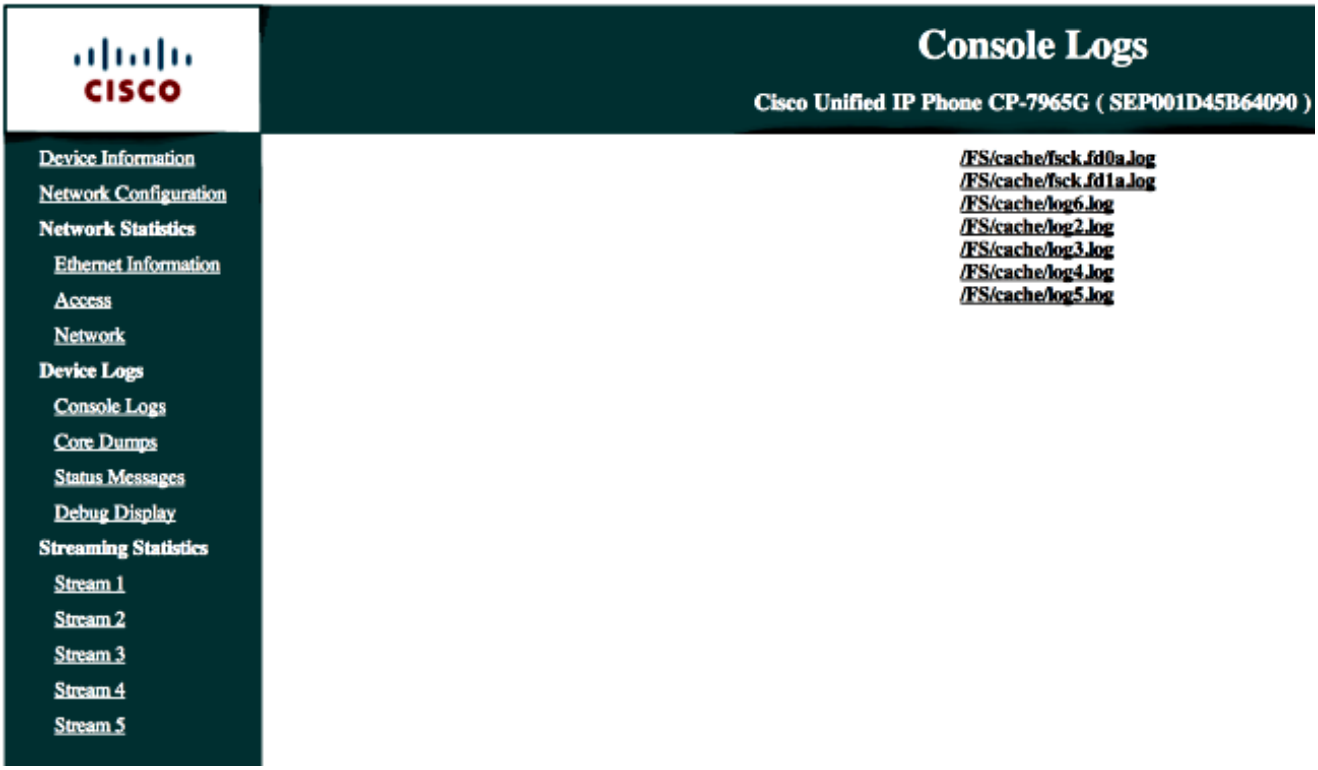
```
Router#show debug

WebVPN Subsystem:
WebVPN (verbose) debugging is on
WebVPN HTTP debugging is on
WebVPN AAA debugging is on
WebVPN tunnel debugging is on
WebVPN Tunnel Events debugging is on
WebVPN Tunnel Errors debugging is on
Webvpn Tunnel Packets debugging is on


PKI:
Crypto PKI Msg debugging is on
Crypto PKI Trans debugging is on
Crypto PKI Validation Path debugging is on
```

从电话的调试

1. 连接对从CUCM的**Device > Phone**。
2. 在设备配置页，请设置对**启用的**Web访问。
3. 点击**"Save"**，然后点击**运用设置**。



4. 从浏览器，请输入电话的IP地址，并且从在左边的菜单选择**控制台日志**。



5. 下载所有**/FS/cache/log *.log**文件。console log文件包含关于电话为什么的信息不能接通到VPN。

相关Bug

Cisco Bug ID CSCty46387， IOS SSLVPN ：安排的增进上下文是默认值
Cisco Bug ID CSCty46436， IOS SSLVPN ：对客户端证书验证工作情况的增进