Exemplo de Configuração da Conexão Telefônica VPN do AnyConnect a um Cisco IOS Router

Contents

Introduction

Este documento descreve como configurar os dispositivos Cisco IOS® Router e Call Manager para que os Cisco IP Phones possam estabelecer conexões VPN com o Cisco IOS Router. Essas conexões VPN são necessárias para proteger a comunicação com um destes dois métodos de autenticação de cliente:

- Servidor de autenticação, autorização e contabilização (AAA) ou banco de dados local
- Certificado de telefone

Prerequisites

Requirements

Não existem requisitos específicos para este documento.

Componentes Utilizados

As informações neste documento são baseadas nas seguintes versões de hardware e software:

- Cisco IOS 15.1(2)T ou posterior
- Conjunto de recursos/Licença: Universal (dados e segurança e UC) para Cisco IOS Integrated Service Router (ISR)-G2
- Conjunto de recursos/Licença: Segurança avançada para Cisco IOS ISR
- Cisco Unified Communications Manager (CUCM) versão 8.0.1.10000-4 ou posterior
- Telefone IP versão 9.0(2)SR1S - Skinny Call Control Protocol (SCCP) ou posterior

Para obter uma lista completa dos telefones suportados em sua versão do CUCM, faça o seguinte:

1. Abra este URL: **https:// *<Endereço IP do servidor CUCM>*:8443/cucreports/systemReports.do**
2. Escolha **Lista de recursos do telefone Unified CM > Gerar um novo relatório > Recurso: Virtual Private Network**.

As versões usadas neste exemplo de configuração incluem:

- Roteador Cisco IOS versão 15.1(4)M4
- Call Manager versão 8.5.1.10000-26
- Telefone IP versão 9.1(1)SR1S

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. 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.

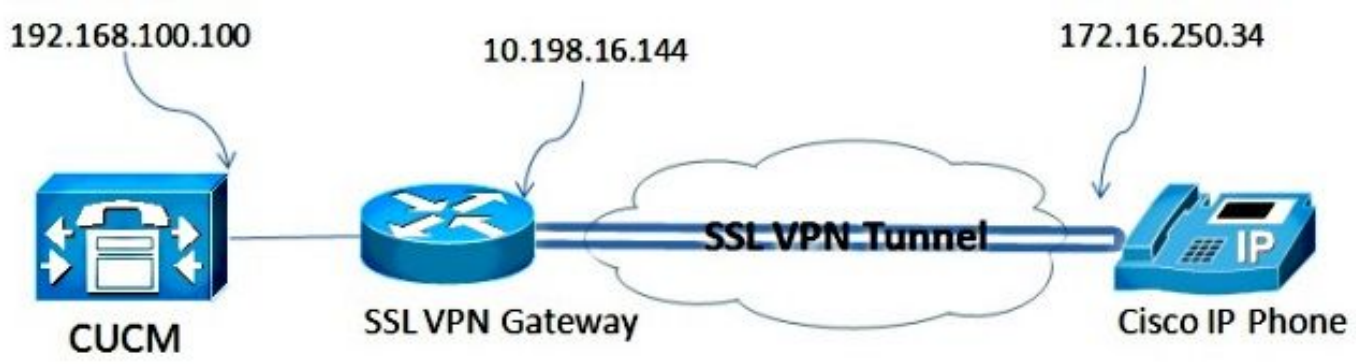
Configurar

Esta seção aborda as informações necessárias para configurar os recursos descritos neste documento.

> **Nota:** Use a Command Lookup Tool (somente clientes registrados) para obter mais informações sobre os comandos usados nesta seção.

Topologia de rede

A topologia usada neste documento inclui um Telefone IP da Cisco, o Cisco IOS Router como o Secure Sockets Layer (SSL) VPN Gateway e o CUCM como o gateway de voz.



Configuração do Servidor VPN SSL

Esta seção descreve como configurar o head-end do Cisco IOS para permitir conexões VPN SSL de entrada.

Etapas comuns da configuração

1. Gere a chave Rivest-Shamir-Adleman (RSA) com um comprimento de 1024 bytes:

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

2. Crie o ponto de confiança para o certificado autoassinado e anexe a chave RSA SSL:

```
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. Quando o ponto de confiança estiver configurado, inscreva o certificado autoassinado com este comando:

```
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. Ative o pacote AnyConnect correto no headend. O próprio telefone não faz download deste pacote. Mas, sem o pacote, o túnel VPN não é estabelecido. Recomenda-se usar a versão mais recente do software cliente disponível no Cisco.com. Este exemplo usa a versão 3.1.3103.

   Em versões mais antigas do Cisco IOS, este é o comando para ativar o pacote:

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

   No entanto, na versão mais recente do Cisco IOS, este é o comando:

```
Router(config)#crypto vpn anyconnect flash:/webvpn/anyconnect-win-
```

```
3.1.03103-k9.pkg sequence 1
```

5. Configure o gateway de VPN. O Gateway WebVPN é usado para encerrar a conexão SSL do usuário.

```
webvpn gateway SSL
ip address 10.198.16.144 port 443
ssl encryption 3des-sha1 aes-sha1
http-redirect port 80
ssl trustpoint server-certificate
inservice
```

   Nota: O endereço IP usado aqui precisa estar na mesma sub-rede da interface à qual os telefones se conectam, ou o gateway precisa ser originado diretamente de uma interface no Roteador. O gateway também é usado para definir qual certificado é usado pelo Roteador para se validar ao cliente.

6. Defina o pool local usado para atribuir endereços IP aos clientes quando eles se conectarem:

```
ip local pool ap_phonevpn 192.168.100.1 192.168.100.254
```

Configuração com autenticação AAA

Esta seção descreve os comandos necessários para configurar o servidor AAA ou o banco de dados local para autenticar seus telefones. Se você planeja usar a autenticação somente certificado para os telefones, vá para a próxima seção.

Configurar o banco de dados do usuário

O Banco de Dados Local do Roteador ou um Servidor AAA externo pode ser usado para autenticação:

- Para configurar o banco de dados local, insira:

```
aaa new-model
aaa authentication login SSL local
username phones password 0 phones
```

- Para configurar um servidor AAA RADIUS remoto para autenticação, digite:

```
aaa new-model
aaa authentication login SSL group radius
radius-server host 192.168.100.200 auth-port 1812 acct-port 1813
radius-server key cisco
```

Configurar o contexto virtual e a política de grupo

O contexto virtual é usado para definir os atributos que governam a conexão VPN, como:

- Qual URL usar ao conectar
- Que pool usar para atribuir endereços de cliente
- Que método de autenticação usar

Estes comandos são um exemplo de um contexto que usa autenticação AAA para o cliente:

```
webvpn context SSL
```

```
aaa authenticate list SSL
gateway SSL domain SSLPhones
!
ssl authenticate verify all
inservice
!
policy group phones
functions svc-enabled
svc address-pool "ap_phonevpn" netmask 255.255.255.0
svc keep-client-installed
default-group-policy phones
```

Configuração com o LSC (Locally Significant Certificate) do telefone IP para autenticação do cliente

Esta seção descreve os comandos necessários para configurar a autenticação de cliente baseada em certificado para os telefones. Entretanto, para fazer isso, é necessário conhecer os vários tipos de certificados de telefone:

- **Certificado instalado pelo fabricante (MIC) -** Os MICs estão incluídos em todos os telefones IP da Cisco 7941, 7961 e de modelo mais recente. Os MICs são certificados de chave de 2.048 bits assinados pela Autoridade de Certificação (CA) da Cisco. Para que o CUCM confie no certificado MIC, ele usa os certificados CA pré-instalados CAP-RTP-001, CAP-RTP-002 e Cisco_Manufacturing_CA em seu repositório confiável de certificados. Como esse certificado é fornecido pelo próprio fabricante, conforme indicado no nome, não é recomendável usar esse certificado para autenticação de cliente.
- **LSC -** O LSC protege a conexão entre o CUCM e o telefone depois que você configura o modo de segurança do dispositivo para autenticação ou criptografia. O LSC possui a chave pública para o telefone IP da Cisco, que é assinado pela chave privada da Função de Proxy da Autoridade de Certificação (CAPF - Certificate Authority Proxy Function) do CUCM. Esse é o método mais seguro (ao contrário do uso de MICs).
  Cuidado: Devido ao aumento do risco à segurança, a Cisco recomenda o uso de MICs somente para instalação de LSC e não para uso contínuo. Os clientes que configuram os telefones IP da Cisco para usar MICs para autenticação TLS (Transport Layer Security), ou para qualquer outra finalidade, fazem isso por sua própria conta e risco.

Neste exemplo de configuração, o LSC é usado para autenticar os telefones.

> **Dica:** A maneira mais segura de conectar seu telefone é usar a autenticação dupla, que combina certificado e autenticação AAA. Você pode configurar isso se combinar os comandos usados para cada um em um contexto virtual.

Configure o ponto confiável para validar o certificado do cliente

O roteador deve ter o certificado CAPF instalado para validar o LSC do telefone IP. Para obter esse certificado e instalá-lo no Roteador, faça o seguinte:

1. Vá para a página da Web Administração do sistema operacional (SO) do CUCM.
2. Escolha **Segurança > Gerenciamento de certificado**.
   Nota: Esse local pode ser alterado com base na versão do CUCM.
3. Localize o certificado **CAPF** e baixe o arquivo **.pem**. Salve-o como um arquivo **.txt**
4. Quando o certificado for extraído, crie um novo ponto de confiança no Roteador e autentique

o ponto de confiança com CAPF, como mostrado aqui. Quando for solicitado o certificado CA codificado em base 64, selecione e cole o texto no arquivo .pem baixado junto com as linhas BEGIN e END.

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



quit
```

Observação:

- O método de inscrição é terminal porque o certificado precisa ser instalado manualmente no Roteador.
- O comando **authorization username** é necessário para informar ao Roteador o que usar como nome de usuário quando o cliente fizer a conexão. Nesse caso, usa o nome comum (CN).
- Uma verificação de revogação precisa ser desativada porque os certificados de telefone não têm uma lista de revogação de certificado (CRL) definida. Portanto, a menos que esteja desabilitada, a conexão falha e as depurações de Public Key Infrastructure (PKI) mostrem esta saída:

```
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
```

Configurar o contexto virtual e a política de grupo

Essa parte da configuração é semelhante à configuração usada anteriormente, exceto dois pontos:

- O método de autenticação
- O ponto de confiança que o contexto usa para autenticar os telefones

Os comandos são mostrados aqui:

```
webvpn context SSL
gateway SSL domain SSLPhones
authentication certificate
ca trustpoint CAPF
!
ssl authenticate verify all
inservice
```

```
!
policy group phones
 functions svc-enabled
 svc address-pool "ap_phonevpn" netmask 255.255.255.0
 svc keep-client-installed
default-group-policy phones
```

Configuração do Call Manager

Esta seção descreve as etapas de configuração do Call Manager.

Exportar o certificado de identidade ou autoassinado do roteador para o CUCM

Para exportar o certificado do Roteador e importá-lo para o Call Manager como um certificado Phone-VPN-Trust, faça o seguinte:

1. Verifique o certificado usado para SSL.

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

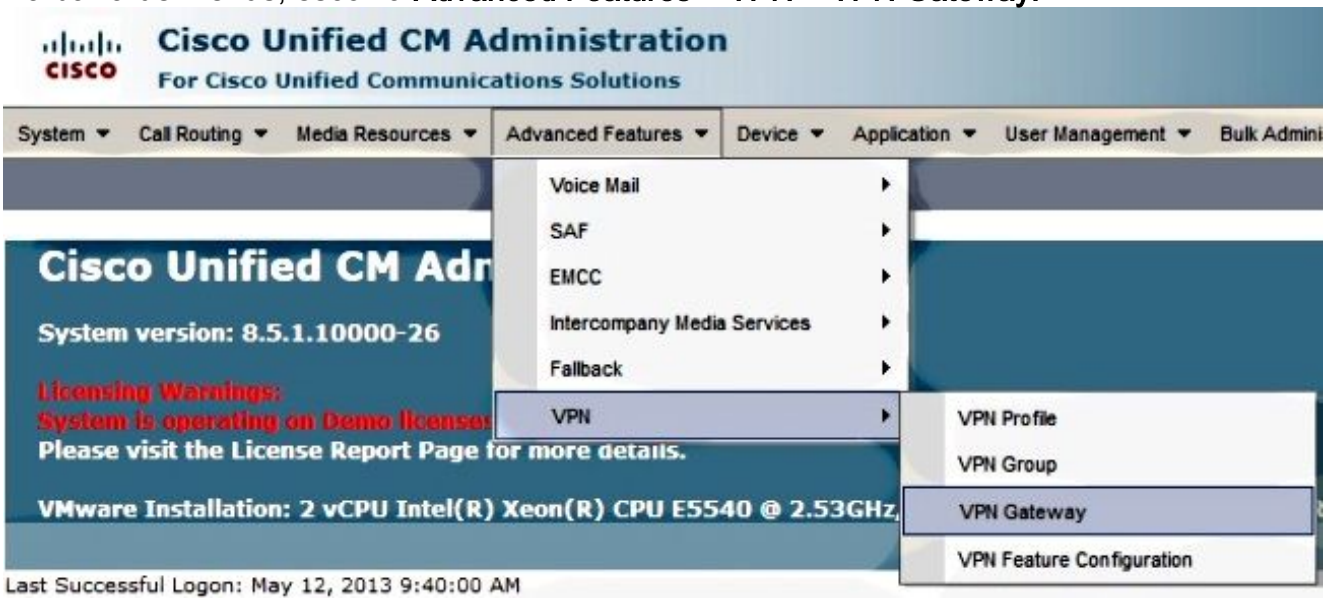
2. Exportar o certificado.

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

   <output removed>

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

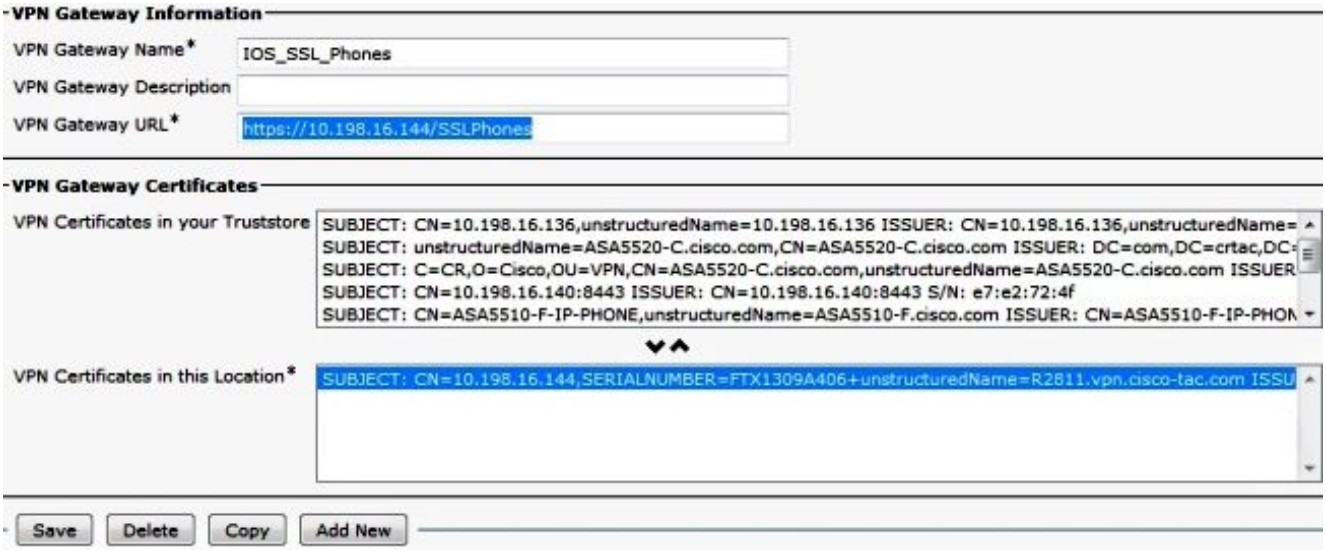
3. Copie o texto do terminal e salve-o como um arquivo **.pem**.
4. Faça login no Call Manager e escolha **Unified OS Administration > Security > Certificate Management > Upload Certificate > Select Phone-VPN-trust** para fazer o upload do arquivo de certificado salvo na etapa anterior.

Configure o gateway de VPN, o grupo e o perfil no CUCM

1. Navegue até **Cisco Unified CM Administration**.
2. Na barra de menus, escolha **Advanced Features > VPN > VPN Gateway.**

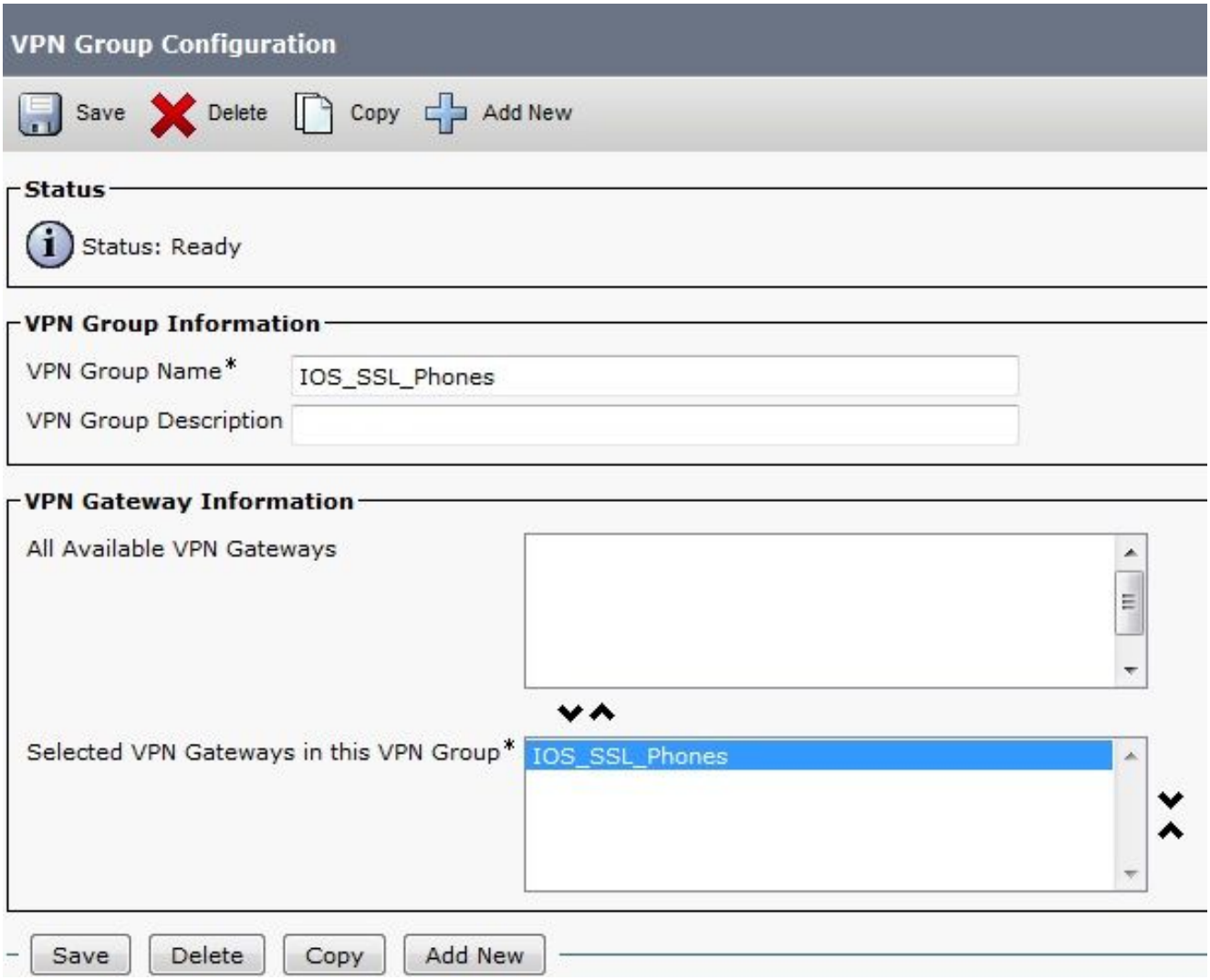


3. Na janela VPN Gateway Configuration, faça o seguinte:
   No campo Nome do gateway de VPN, insira um nome. Pode ser qualquer nome.No campo Descrição do gateway de VPN, insira uma descrição (opcional).No campo URL do gateway de VPN, digite a URL do grupo definida no Roteador.No campo Certificados VPN neste local, escolha o certificado que foi carregado anteriormente para o Call Manager para movê-lo do armazenamento confiável para esse
   local.

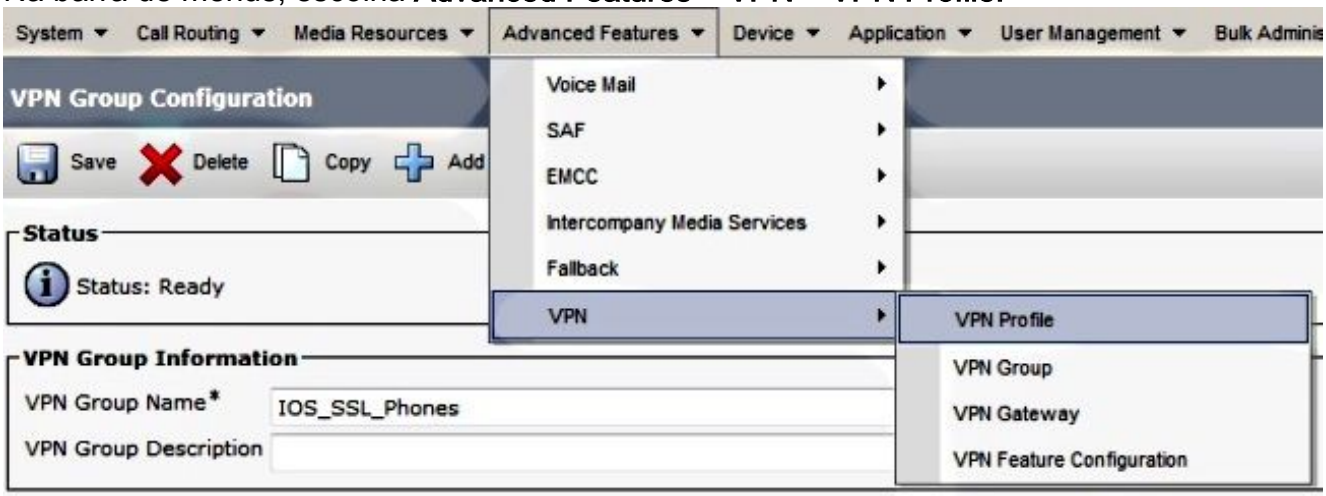


4. Na barra de menus, escolha **Advanced Features > VPN > VPN Group.**

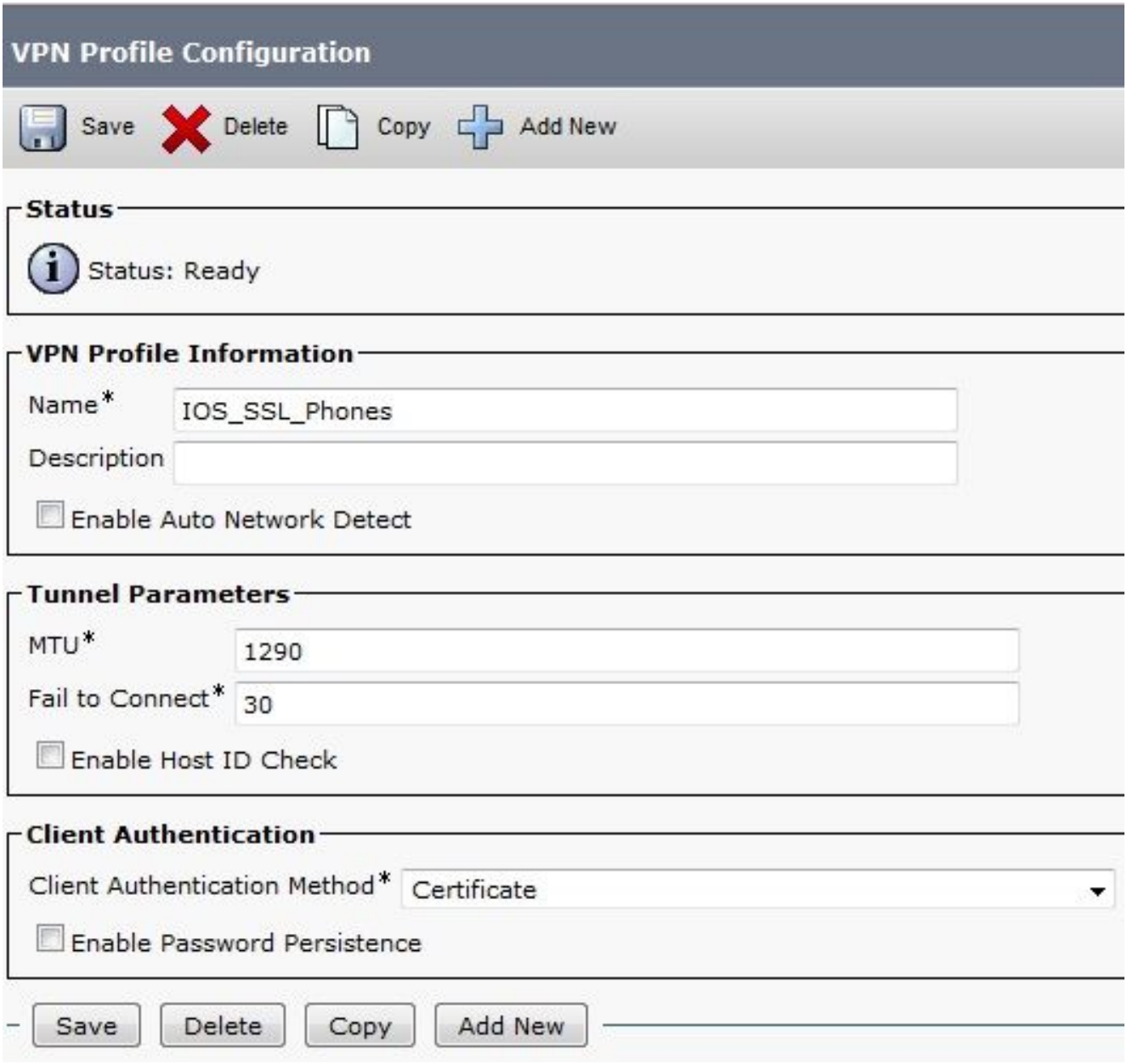
5. No campo Todos os gateways VPN disponíveis, escolha o **VPN Gateway** previamente definido. Clique na seta para baixo para mover o gateway selecionado para os Gateways VPN Selecionados neste campo Grupo de VPN.



6. Na barra de menus, escolha **Advanced Features > VPN > VPN Profile.**



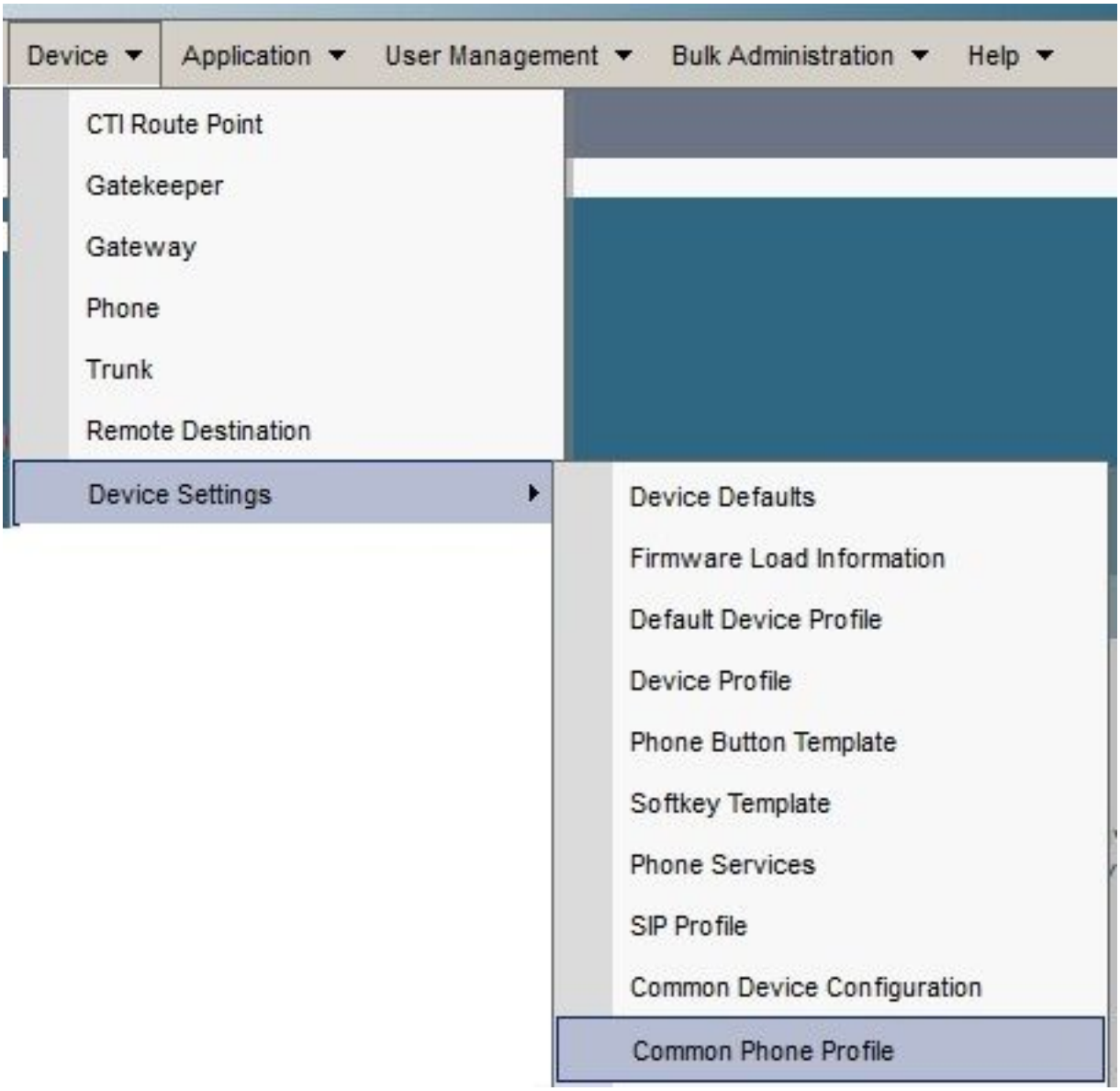
7. Para configurar o perfil de VPN, preencha todos os campos marcados com um asterisco (*).

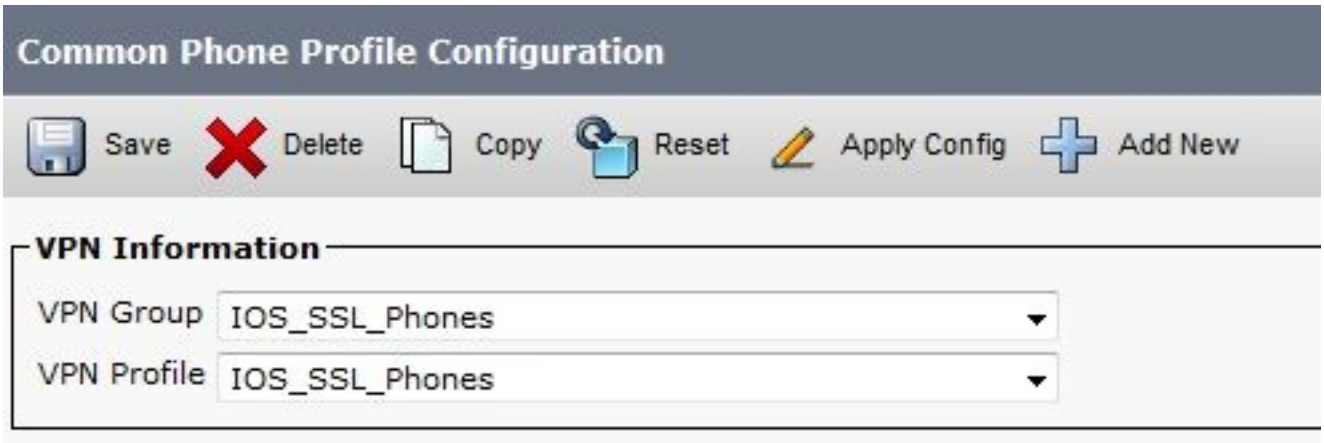


Ativar detecção automática de rede: Se habilitado, o telefone VPN executa ping no servidor TFTP. Se nenhuma resposta for recebida, ele inicia automaticamente uma conexão VPN.**Ativar verificação de ID de host:** Se habilitado, o telefone VPN compara o FQDN (Fully Qualified Domain Name, nome de domínio totalmente qualificado) da URL do gateway de VPN com o CN/Storage Area Network (SAN) do certificado. O cliente não consegue se conectar se esses itens não correspondem ou se um certificado curinga com um asterisco (*) é usado.**Habilitar persistência da senha:** Isso permite que o telefone VPN armazene em cache o nome de usuário e a senha para a próxima tentativa de VPN.

Aplique o grupo e o perfil ao telefone IP com o perfil de telefone comum

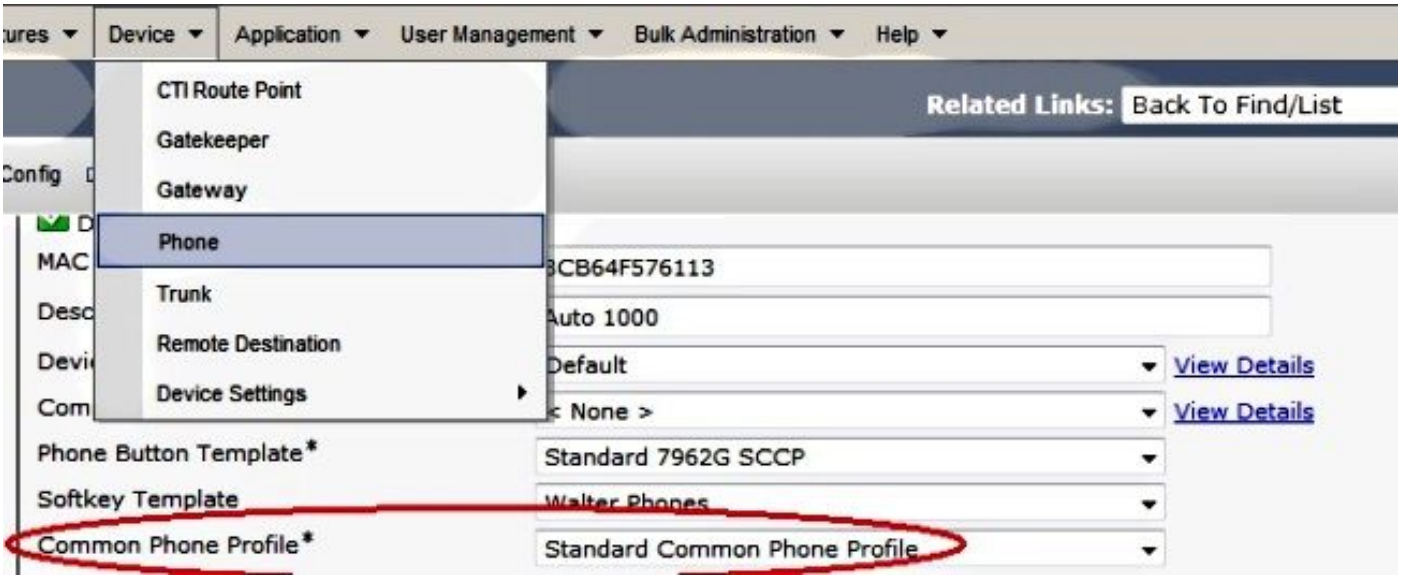
Na janela Common Phone Profile Configuration, clique em **Apply Config** para aplicar a nova configuração de VPN. Você pode usar o **Common Phone Profile** padrão ou criar um novo perfil.





Aplique o perfil de telefone comum ao telefone IP

Se você criou um novo perfil para telefones/usuários específicos, navegue até a janela **Configuração do telefone**. No campo Common Phone Profile, escolha o perfil **do telefone comum padrão**.



Instalar certificados localmente significativos (LSC) em telefones IP da Cisco

O guia a seguir pode ser usado para instalar certificados localmente significativos em telefones IP da Cisco. Essa etapa só é necessária se for usada a autenticação usando o LSC. A autenticação usando o Certificado Instalado pelo Fabricante (MIC) ou o nome de usuário e a senha não exigem a instalação de um LSC.

Instale um LSC em um telefone com o modo de segurança de cluster CUCM definido como Não seguro.

Registre o telefone no Call Manager novamente para baixar a nova configuração

Esta é a etapa final no processo de configuração.

Verificar

Verificação do roteador

Para verificar as estatísticas da sessão VPN no Roteador, você pode usar estes comandos e verificar as diferenças entre as saídas (destacadas) de nome de usuário e autenticação de certificado:

Para autenticação de nome de usuário/senha:

```
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
```

Para autenticação de certificado:

```
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
```

Verificação de CUCM

Confirme se o telefone IP está registrado no Call Manager com o endereço atribuído pelo roteador à conexão SSL.

Troubleshoot

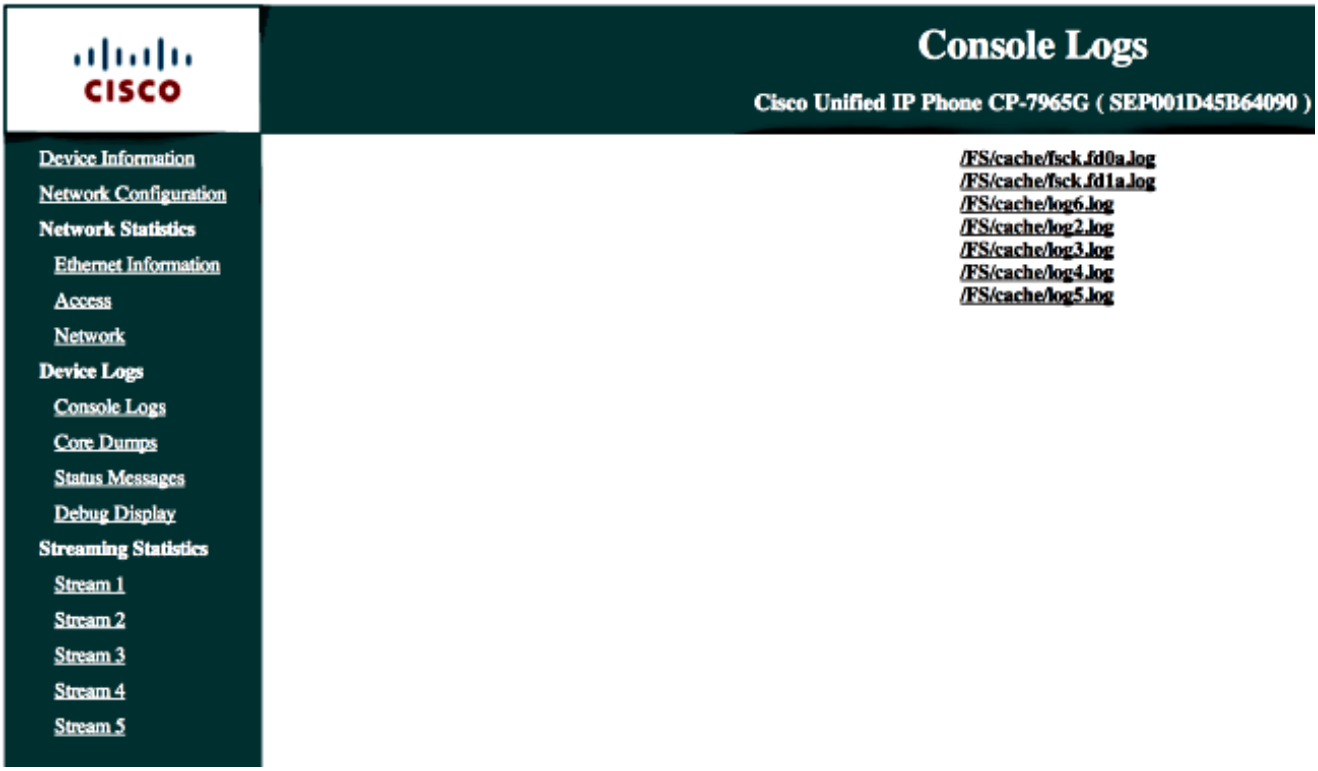
Depurações no Servidor VPN SSL

```
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
```

Depurações do telefone

1. Navegue até **Dispositivo > Telefone** do CUCM.
2. Na página de configuração do dispositivo, defina Web Access (Acesso à Web) como **Enabled (Habilitado)**.
3. Clique em **Salvar** e, em seguida, clique em **Aplicar configuração**.

4. Em um navegador, digite o endereço IP do telefone e escolha **Logs de console** no menu à esquerda.



5. Descarregue todos os arquivos **/FS/cache/log*.log**. Os arquivos de log do console contêm informações sobre por que o telefone não consegue se conectar à VPN.

Erros relacionados

ID de bug da Cisco CSCty46387 , IOS SSLVPN: A melhoria para ter um contexto é um padrão
ID de bug da Cisco CSCty46436 , IOS SSLVPN: Aprimoramento do comportamento de validação de certificado do cliente