

# Configurar o telefone VPN do AnyConnect com autenticação de certificado em um ASA

## Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Conventions](#)

[Tipos de certificado do telefone](#)

[Configurar](#)

[Configurações](#)

[Verificar](#)

[Troubleshoot](#)

[Informações Relacionadas](#)

## Introduction

Este documento fornece uma configuração de exemplo que mostra como configurar os dispositivos Adaptive Security Appliance (ASA) e CallManager para fornecer autenticação de certificado para clientes AnyConnect executados em telefones IP da Cisco. Após a conclusão dessa configuração, os telefones IP da Cisco podem estabelecer conexões VPN com o ASA que utilizam certificados para proteger a comunicação.

## Prerequisites

### Requirements

Certifique-se de atender a estes requisitos antes de tentar esta configuração:

- Licença AnyConnect Premium SSL
- Licença do AnyConnect para Cisco VPN Phone

Dependendo da versão ASA, você verá "AnyConnect for Linksys phone" para ASA versão 8.0.x ou "AnyConnect for Cisco VPN Phone" para ASA versão 8.2.x ou posterior.

### Componentes Utilizados

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

- ASA - Versão 8.0(4) ou posterior
- Modelos de telefone IP - 7942 / 7962 / 7945 / 7965 / 7975
- Telefones - 8961 / 9951 / 9971 com firmware versão 9.1(1)
- Telefone - Versão 9.0(2)SR1S - Skinny Call Control Protocol (SCCP) ou posterior
- Cisco Unified Communications Manager (CUCM) - Versão 8.0.1.10000-4 ou posterior

As versões usadas neste exemplo de configuração incluem:

- ASA - Versão 9.1(1)
- CallManager - Versão 8.5.1.10000-26

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.**

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.

## Conventions

Consulte as [Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.](#)

## Tipos de certificado do telefone

A Cisco usa esses tipos de certificado em telefones:

- Certificado instalado pelo fabricante (MIC) - Os MICs estão incluídos em todos os telefones IP da Cisco 7941, 7961 e em modelos mais recentes. Os MICs são certificados de chave de 2048 bits assinados pela Autoridade de Certificação (CA) da Cisco. Quando um MIC está presente, não é necessário instalar um LSC (Locally Significant Certificate). Para que o CUCM confie no certificado MIC, ele utiliza os certificados CA pré-instalados CAP-RTP-001, CAP-RTP-002 e Cisco\_Manufacturing\_CA em seu repositório confiável de certificados.
- 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 preferido (ao contrário do uso de MICs) porque somente os telefones IP da Cisco que são provisionados manualmente por um administrador têm permissão para fazer download e verificar o arquivo CTL. **Note:** 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.

# Configurar

Nesta seção, você encontrará informações para configurar os recursos descritos neste documento.

**Note:** Use a [Command Lookup Tool \(somente clientes registrados\) para obter mais informações sobre os comandos usados nesta seção.](#)

## Configurações

Este documento descreve estas configurações:

- Configuração do ASA
- Configuração do CallManager
- Configuração de VPN no CallManager
- Instalação de certificado em telefones IP

### Configuração do ASA

A configuração do ASA é quase a mesma que quando você conecta um computador cliente AnyConnect ao ASA. No entanto, estas restrições aplicam-se:

- O tunnel-group deve ter um group-url. Este URL será configurado no CM na URL do gateway de VPN.
- A política de grupo não deve conter um túnel dividido.

Essa configuração usa um certificado ASA (autoassinado ou de terceiros) configurado e instalado anteriormente no ponto de confiança SSL (Secure Socket Layer) do dispositivo ASA. Para obter mais informações, consulte estes documentos:

- [Configurando certificados digitais](#)
- [ASA 8.x Instalar manualmente certificados de terceiros para uso com exemplo de configuração de WebVPN](#)
- [ASA 8.x: Acesso VPN com o AnyConnect VPN Client usando o exemplo de configuração de certificado autoassinado](#)

A configuração relevante do ASA é:

```
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
```

## Configuração do CallManager

Para exportar o certificado do ASA e importá-lo para o CallManager como um certificado Phone-VPN-Trust, faça o seguinte:

1. Registre o certificado gerado com CUCM.
2. Verifique o certificado usado para SSL.

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

3. Exportar o certificado.

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

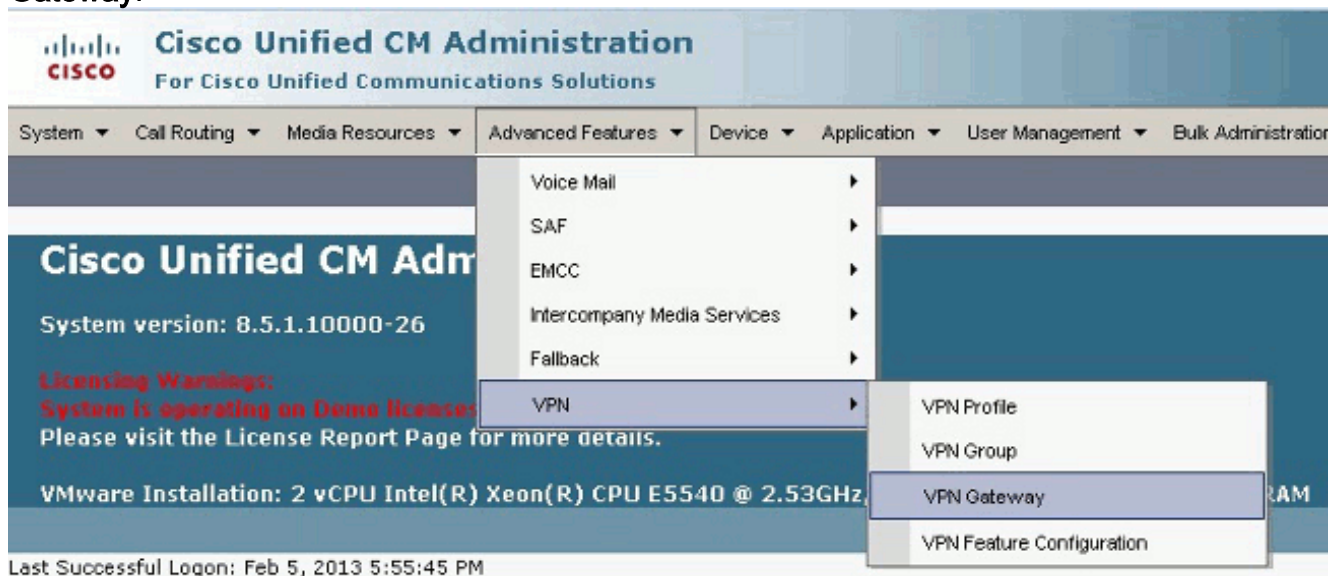
O certificado de identidade codificado PEM (Privacy Enhanced Mail) é o seguinte:

```
-----BEGIN CERTIFICATE-----ZHUXFjAUBgkqhkiG9w0BCQIWB0FTQTU1NDAwHhcNMTMwMTMwMTM1MzEwWhcNMjMw
MTI4MTM1MzEwWjAmMQwwCgYDVQQDEwNlZHUxZjAUBgkqhkiG9w0BCQIWB0FTQTU1
NDAwZz8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAMYcrysjZ+MawKBx8Zk69SW4AR
FSpV6FPcUL7xsovhw6hsJE/2VDgd3pkawc5jcl5vkcpTkhjbf2xC4C1q6ZQwpahde22sdf1
wsidpQWq1DDrJD1We83L/oqmhkWJO7QfNrGZh0Lv9xOpR7BFpZd1yFyzwAPkoB1l
-----END CERTIFICATE-----
```

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

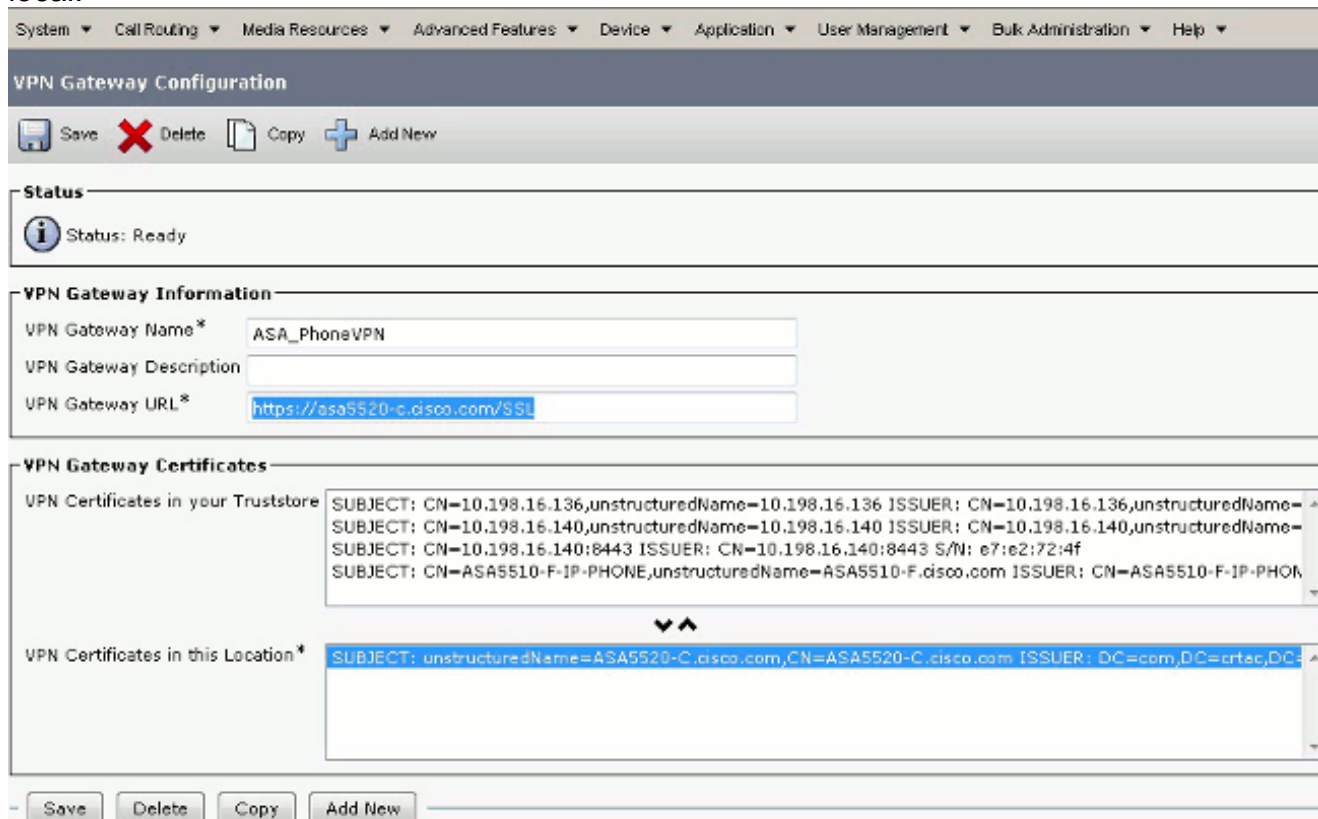
## Configuração de VPN no CallManager

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

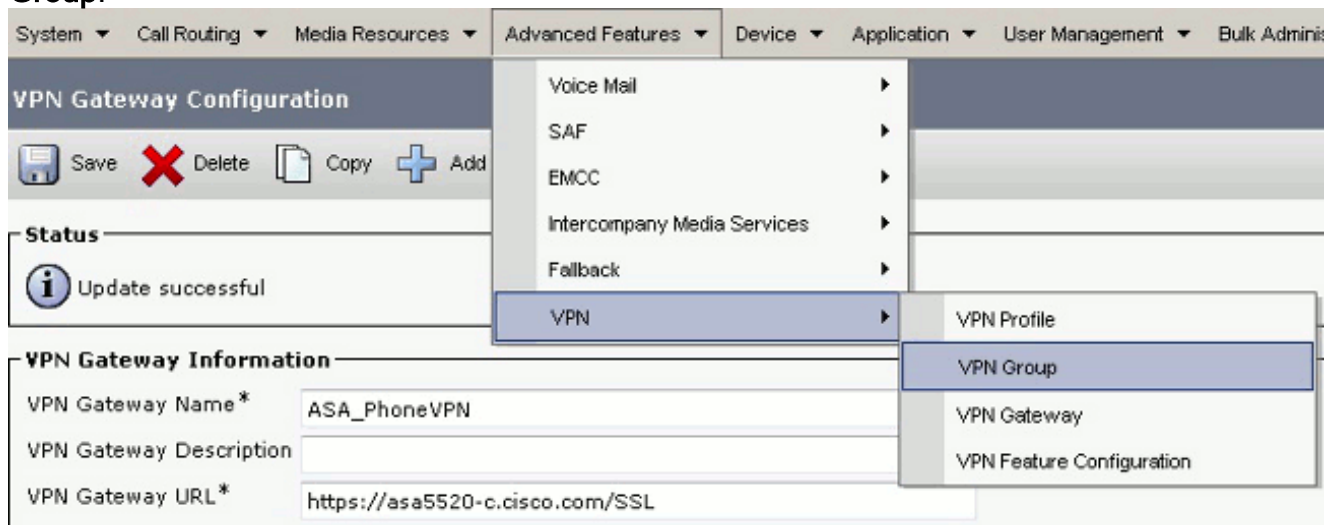


3. Na janela VPN Gateway Configuration, faça o seguinte: No campo Nome do gateway de VPN, insira um nome. Pode ser qualquer nome. No campo Descrição do gateway de VPN, insira uma descrição (opcional). No campo URL do gateway de VPN, insira o group-url definido no ASA. No campo Certificados VPN neste local, selecione o certificado que foi carregado anteriormente para o CallManager para movê-lo do armazenamento confiável para este

local.



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



5. No campo All Available VPN Gateways (Todos os gateways de VPN disponíveis), selecione o VPN Gateway definido anteriormente. Clique na seta para baixo para mover o gateway selecionado para os Gateways VPN Selecionados neste campo Grupo de VPN.

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

## VPN Group Configuration

Save Delete Copy Add New

**Status**

Status: Ready

**VPN Group Information**

VPN Group Name\* ASA\_PhoneVPN

VPN Group Description

**VPN Gateway Information**

All Available VPN Gateways

Selected VPN Gateways in this VPN Group\* ASA\_PhoneVPN

**Move the Gateway down**

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

System ▾ Call Routing ▾ Media Resources ▾ Advanced Features ▾ Device ▾ Application ▾ User Management ▾ Bulk Administ

## VPN Group Configuration

Save Delete Copy Add

**Status**

Status: Ready

**VPN Group Information**

VPN Group Name\* ASA\_PhoneVPN

VPN Group Description





- Voice Mail
- SAF
- EMCC
- Intercompany Media Services
- Fallback
- VPN**
  - VPN Profile**
  - VPN Group
  - VPN Gateway
  - VPN Feature Configuration

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




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**

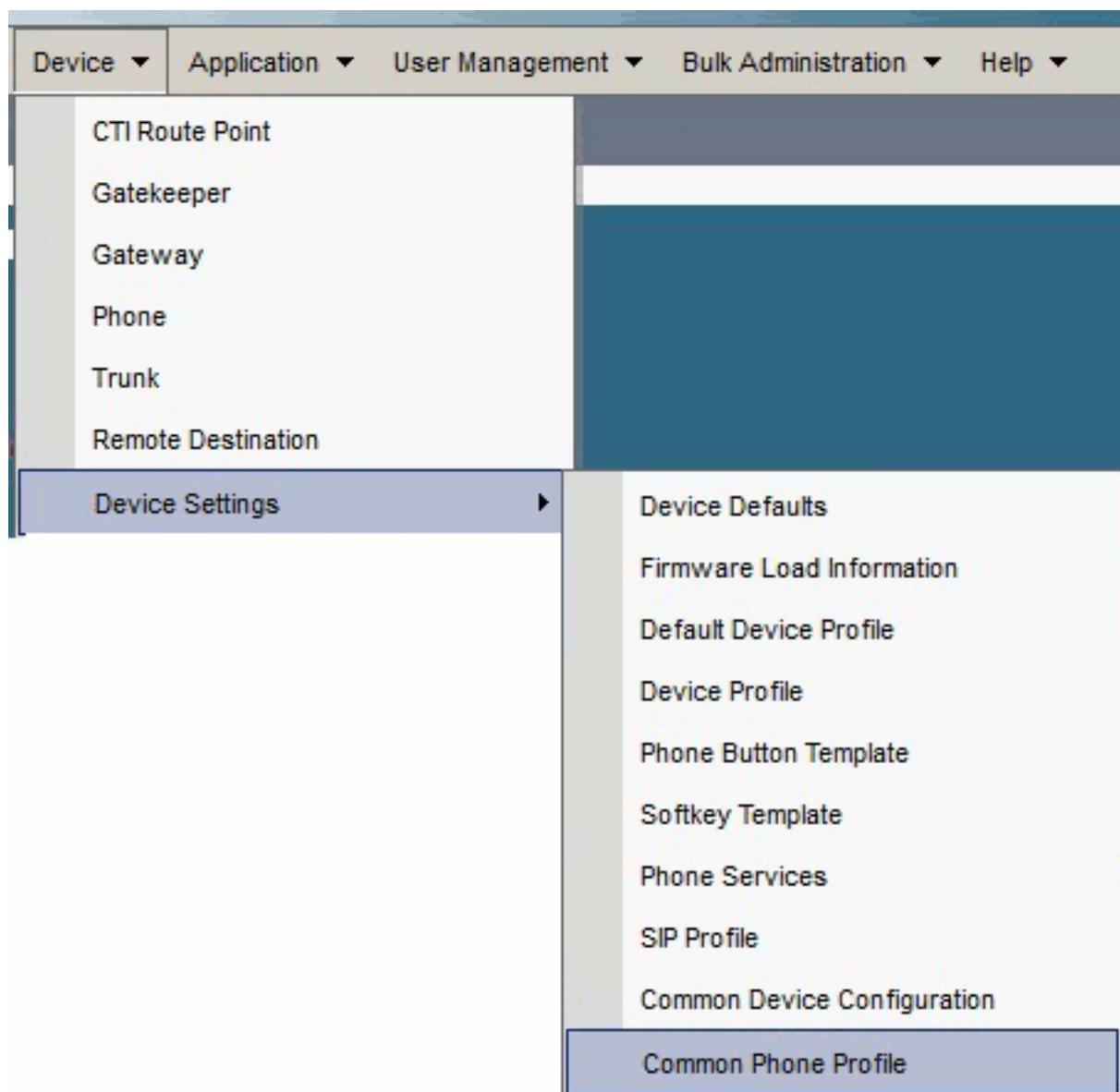
Client Authentication Method\*

Enable Password Persistence

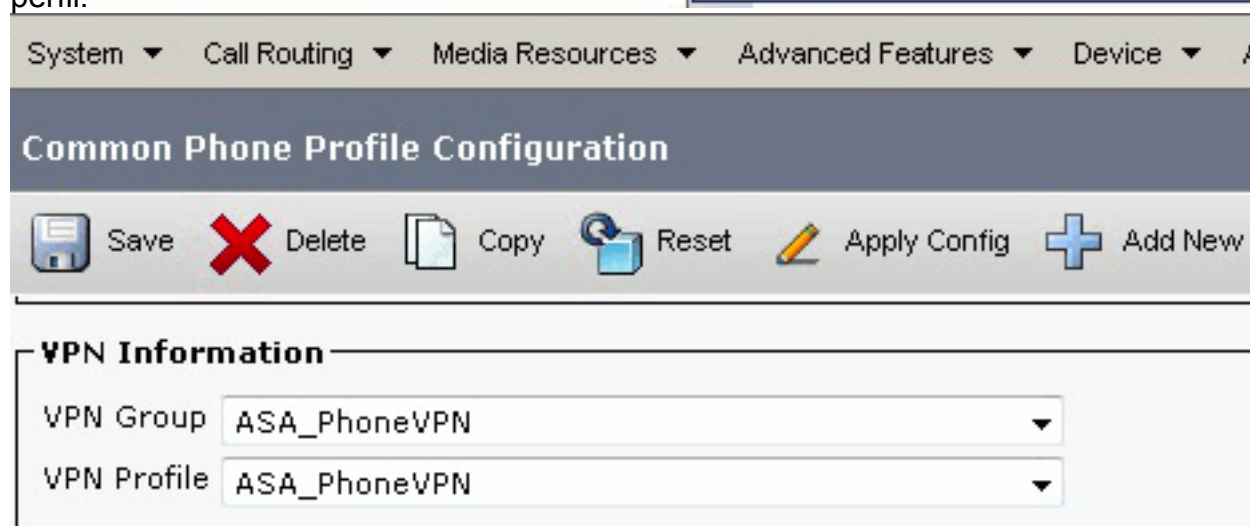
---

**Ativar detecção automática de rede:** Se habilitado, o telefone VPN executa ping no servidor TFTP e, 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 da URL do gateway de VPN com o CN/SAN do certificado. O cliente não consegue se conectar se não corresponder ou se um certificado curinga com um asterisco (\*) for 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.

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

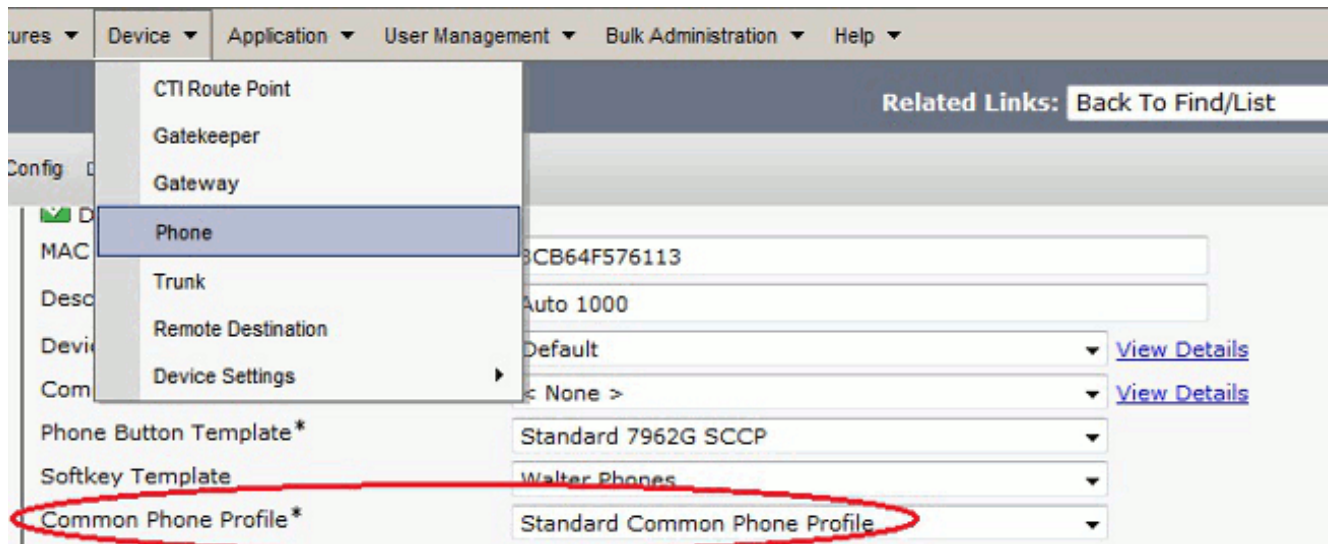


perfil.



9. Se você criou um novo perfil para telefones/usuários específicos, vá para a janela Configuração do telefone. No campo Common Phone Profile, escolha **Standard Common Phone Profile**.





10. Registre o telefone no CallManager novamente para baixar a nova configuração.





### Configuração de autenticação de certificado

Para configurar a autenticação de certificado, faça o seguinte no CallManager e no ASA:

1. Na barra de menus, escolha **Advanced Features > VPN > VPN Profile**.
2. Confirme se o campo Client Authentication Method está definido como **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. Faça login no CallManager. Na barra de menus, escolha **Unified OS Administration > Security > Certificate Management > Find**.

4. Exportar os certificados corretos para o método de autenticação de certificado selecionado: MICs: Cisco\_Manufacturing\_CA - Autentica telefones IP com um MIC

Find Certificate List where  ▾ begins with  ▾    

Certificate Name	Certificate Type	.PEM File
tomcat	certs	<a href="#">tomcat.pem</a>
ipsec	certs	<a href="#">ipsec.pem</a>
tomcat-trust	trust-certs	<a href="#">CUCM85.pem</a>
ipsec-trust	trust-certs	<a href="#">CUCM85.pem</a>
CallManager	certs	<a href="#">CallManager.pem</a>
CAPF	certs	<a href="#">CAPF.pem</a>
TVS	certs	<a href="#">TVS.pem</a>
CallManager-trust	trust-certs	<a href="#">Cisco_Manufacturing_CA.pem</a>
CallManager-trust	trust-certs	<a href="#">CAP-RTP-001.pem</a>
CallManager-trust	trust-certs	<a href="#">Cisco Root CA 2048.pem</a>
CallManager-trust	trust-certs	<a href="#">CAPF-18cf046e.pem</a>
CallManager-trust	trust-certs	<a href="#">CAP-RTP-002.pem</a>

LSCs: Cisco Certificate Authority Proxy Function (CAPF) - Autentica telefones IP com um LSC

Certificate Name	Certificate Type	.PEM File	.DER File
tomcat	certs	<a href="#">tomcat.pem</a>	<a href="#">tomcat.der</a>
psec	certs	<a href="#">ipsec.pem</a>	<a href="#">ipsec.der</a>
tomcat-trust	trust-certs	<a href="#">CUCM85.pem</a>	<a href="#">CUCM85.der</a>
psec-trust	trust-certs	<a href="#">CUCM85.pem</a>	<a href="#">CUCM85.der</a>
CallManager	certs	<a href="#">CallManager.pem</a>	<a href="#">CallManager.der</a>
CAPF	certs	<a href="#">CAPF.pem</a>	<a href="#">CAPF.der</a>
TVS	certs	<a href="#">TVS.pem</a>	<a href="#">TVS.der</a>
CallManager-trust	trust-certs	<a href="#">Cisco_Manufacturing_CA.pem</a>	

- Localize o certificado, Cisco\_Manufacturing\_CA ou CAPF. Baixe o arquivo .pem e salve como um arquivo .txt
- Crie um novo ponto de confiança no ASA e autentique o ponto de confiança com o certificado salvo anteriormente. Quando for solicitado um certificado CA codificado em base 64, selecione e cole o texto no arquivo .pem baixado junto com as linhas BEGIN e END. Um exemplo é mostrado:

```
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
```

- Confirme se a autenticação no grupo de túneis está definida como autenticação de certificado.

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

## Instalação de certificado em telefones IP

Os telefones IP podem funcionar com MICs ou LSCs, mas o processo de configuração é diferente para cada certificado.

### Instalação do MIC

Por padrão, todos os telefones que suportam VPN são pré-carregados com MICs. Os telefones 7960 e 7940 não vêm com um MIC e exigem um procedimento de instalação especial para que o LSC se registre com segurança.

**Note:** A Cisco recomenda que você use MICs somente para instalação LSC. A Cisco suporta LSCs para autenticar a conexão TLS com CUCM. Como os certificados raiz MIC podem ser comprometidos, os clientes que configuram telefones para usar MICs para autenticação TLS ou para qualquer outro propósito o fazem por sua própria conta e risco. A Cisco não assume nenhuma responsabilidade se os MICs forem comprometidos.

### Instalação LSC

- Ative o serviço CAPF no CUCM.
- Depois que o serviço CAPF for ativado, atribua as instruções do telefone para gerar um LSC no CUCM. Faça login no Cisco Unified CM Administration e escolha **Device > Phone**. Selecione o telefone configurado.
- Na seção Informações da função proxy da autoridade de certificação (CAPF), verifique se todas as configurações estão corretas e se a operação está definida para uma data futura.

**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. Se Authentication Mode estiver definido como Null String ou Existing Certificate, nenhuma ação adicional será necessária.
5. Se Authentication Mode estiver definido como uma string, selecione manualmente **Settings > Security Configuration > \*\*# > LSC > Update** no console do telefone.

## Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

### Verificação do ASA

```
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

## Verificação de CUCM

The screenshot shows the 'Find and List Phones' interface in CUCM. It displays a table with the following data:

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

A red circle highlights the status 'Registered with: 192.168.100.1' and the IP address '10.10.10.2' in the second row. A red arrow points to the IP address column header, and a text box above it says 'IP Phone registered with the CUCM using VPN address'.

## Troubleshoot

Atualmente, não existem informações disponíveis específicas sobre Troubleshooting para esta configuração.

### Erros relacionados

- ID de bug da Cisco [CSCtf09529](#), Adicionar suporte para o recurso VPN no CUCM para telefones 8961, 9951, 9971

- ID de bug da Cisco [CSCuc71462](#), failover de VPN de telefone IP leva 8 minutos
- ID de bug da Cisco [CSCtz42052](#), Suporte de VPN SSL do Telefone IP para Números de Porta Não Padrão
- ID de bug da Cisco [CSCth96551](#), nem todos os caracteres ASCII são suportados durante o login de usuário VPN do telefone + senha.
- ID de bug da Cisco [CSCuj71475](#), entrada de TFTP manual necessária para VPN de telefone IP
- ID de bug da Cisco [CSCum10683](#), telefones IP que não registram chamadas perdidas, efetuadas ou recebidas

## Informações Relacionadas

- [Suporte Técnico e Documentação - Cisco Systems](#)