

# Cisco IOS ルータへの AnyConnect VPN 電話接続の構成例

## 目次

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[設定](#)

[ネットワークトポロジ](#)

[SSL VPN サーバの設定](#)

[共通の設定手順](#)

[AAA 認証を使用する設定](#)

[クライアント認証に IP フォンのローカルで有効な証明書 \( LSC \) を使用する設定](#)

[Call Manager の設定](#)

[自己署名証明書またはアイデンティティ証明書をルータから CUCM にエクスポートする](#)

[CUCM で VPN ゲートウェイ、グループ、およびプロファイルを設定する](#)

[共通の電話プロファイルを使用してグループおよびプロファイルを IP フォンに適用する](#)

[共通の電話プロファイルを IP フォンに適用する](#)

[ローカルで固有の証明書 \( LSC \) IP 電話を on Cisco インストールして下さい](#)

[新しい設定をダウンロードするために電話を Call Manager に再度登録する](#)

[確認](#)

[ルータの検証](#)

[CUCM の検証](#)

[トラブルシューティング](#)

[SSL VPN サーバのデバッグ](#)

[電話からのデバッグ](#)

[関連バグ](#)

## 概要

このドキュメントでは、Cisco IP Phone が Cisco IOS ルータへの VPN 接続を確立できるように、Cisco IOS<sup>®</sup> ルータと Call Manager デバイスを設定する方法を説明します。これらの VPN 接続は、次の 2 つのクライアント認証方法のいずれかで通信を保護するために必要です。

- 認証、認可、およびアカウンティング ( AAA ) サーバまたはローカル データベース
- 電話証明書

## 前提条件

### 要件

このドキュメントに関しては個別の要件はありません。

## 使用するコンポーネント

このドキュメントの情報は、次のハードウェアとソフトウェアのバージョンに基づいています。

- Cisco IOS 15.1(2)T 以降
- フィーチャ セット/ライセンス : Cisco IOS のユニバーサル ( データおよびセキュリティおよび UC ) サービス統合型ルータ ( ISR ) -G2
- フィーチャ セット/ライセンス : Cisco IOS ISR の高度なセキュリティ
- Cisco Unified Communications Manager ( CUCM ) Release 8.0.1.100000-4 以降
- IP Phone リリース 9.0(2)SR1S - Skinny Call Control Protocol (SCCP) 以降

使用している CUCM のバージョンでサポートされる電話機の完全なリストについては、次の手順を実行してください。

1. この URL : [https:// <CUCM Server IP Address>:8443/cucreports/systemReports.do](https://<CUCM Server IP Address>:8443/cucreports/systemReports.do) を開きます。
2. [Unified CM Phone Feature List] > [Generate a new report] > [Feature: Virtual Private Network] の順に選択します。

この設定例で使用しているリリースには次のものが含まれています。

- Cisco IOS ルータ リリース 15.1(4)M4
- Call Manager リリース 8.5.1.10000-26
- IP Phone リリース 9.1(1)SR1S

本書の情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。このドキュメントで使用するすべてのデバイスは、初期 ( デフォルト ) 設定の状態から起動しています。稼働中のネットワークで作業を行う場合、コマンドの影響について十分に理解したうえで作業してください。

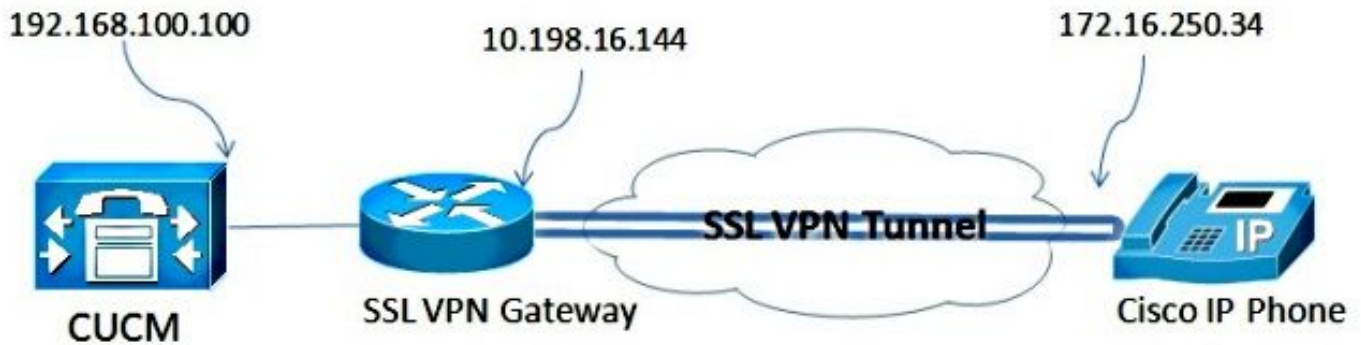
## 設定

この項では、このドキュメントで説明する機能の設定に必要な情報を説明します。

注: このセクションで使用されているコマンドの詳細を調べるには、[Command Lookup Tool](#) ( [登録ユーザ専用](#) ) を使用してください。

## ネットワーク トポロジ

このドキュメントで使用するトポロジには、1 台の Cisco IP Phone、セキュア ソケット レイヤ ( SSL ) VPN ゲートウェイとしての Cisco IOS ルータ、音声ゲートウェイとしての CUCM が含まれます。



## SSL VPN サーバの設定

この項では、着信 SSL VPN 接続を可能にするために Cisco IOS ヘッドエンドを設定する方法を説明します。

### 共通の設定手順

1. 1024 バイトの長さの Rivest-Shamir-Adleman ( RSA ) キーを生成して下さい:

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

2. 自己署名証明書のトラストポイントを作成し、SSL RSA キーをアタッチします。

```
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. トラストポイントを設定したら、次のコマンドで自己署名証明書を登録します。

```
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. ヘッドエンドで正しい AnyConnect パッケージを有効にします。電話自体はこのパッケージをダウンロードしません。しかし、パッケージがないと、VPN トンネルが確立されません。Cisco.com で入手できる最新のクライアント ソフトウェアのバージョンを使用することを推奨します。この例では、バージョン 3.1.3103 を使用します。

古い Cisco IOS バージョンでは、これはパッケージを有効にするためのコマンドです。

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

ただし、最新の Cisco IOS バージョンでは、これは次のコマンドです。

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

- VPN ゲートウェイを設定します。WebVPN ゲートウェイは、ユーザからの SSL 接続を終了するために使用されます。

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

注: ここで使用される IP アドレスが電話機を接続するインターフェイスと同じサブネット上にあるか、またはゲートウェイがルータのインターフェイスから直接送信される必要があります。ゲートウェイは、ルータがクライアントに対して自身を検証するために使用する証明書を定義するためにも使用されます。

- 接続時にクライアントに IP アドレスを割り当てるために使用するローカル プールを定義します。

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

## AAA 認証を使用する設定

この項では、電話を認証するために、AAA サーバまたはローカル データベースを設定する場合に必要なコマンドについて説明します。電話用に証明書のみ認証を使用する予定であれば、次の項に進んでください。

### ユーザ データベースの設定

ルータのローカル データベースまたは外部 AAA サーバを認証に使用できます。

- ローカル データベースを設定するには、次のコマンドを入力します。

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

- 認証のためにリモート AAA RADIUS サーバを設定するには、次のコマンドを入力します。

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

### 仮想コンテキストおよびグループ ポリシーの設定

仮想コンテキストは、次のような、VPN 接続を制御する属性を定義するために使用されます。

- 接続時に使用する URL
- クライアント アドレスを割り当てるために使用するプール
- 使用する認証方式

次のコマンドは、クライアントに AAA 認証を使用するコンテキストの例です。

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

### クライアント認証に IP フォンのローカルで有効な証明書 (LSC) を使用する設定

この項では、電話に対して証明書ベースのクライアント認証を設定するために必要なコマンドについて説明します。ただし、これを行うには、電話証明書の各種の知識が必要です。

- **Manufacturer Installed Certificate ( MIC )** - MIC は、7941、7961、および新しいモデルの Cisco IP Phone に含まれています。MIC はシスコの認証局 ( CA ) によって署名された 2,048 ビット キーの証明書です。CUCM は MIC 証明書を信頼するために、CUCM の証明書信頼ストアに事前にインストールされた CA 証明書 CAP-RTP-001、CAP-RTP-002、および Cisco\_Manufacturing\_CA を使用します。この証明書は名前が示すように製造者自身によって提供されるため、クライアント認証にこの証明書を使用することはお勧めしません。
- **LSC** - LSC は認証または暗号化におけるデバイスセキュリティ モードを設定した後 CUCM と電話間の接続を保護します。LSC は、CUCM Certificate Authority Proxy Function ( CAPF ) 秘密キーで署名された Cisco IP Phone の公開キーを処理します。これはより安全な方法です ( MIC の使用とは対照的に )。  
**注意：** セキュリティのリスクが高まっているため、LSC のインストールで MIC は単独で使用し、継続的に使用しないことをシスコは推奨します。Transport Layer Security ( TLS ) 認証やその他の目的で MIC を使用するように Cisco IP Phone を設定する場合は、お客様の責任で行ってください。

この設定例では、LSC は電話を認証するために使用されます。

**ヒント：** 電話を接続する最も安全な方法は、証明書と AAA 認証を組み合わせた二重認証を使用する方法です。それぞれに使用するコマンドを 1 つの仮想コンテキストで組み合わせると、これを設定できます。

## クライアント証明書を検証するためのトラストポイントの設定

IP フォンから LSC を検証するために、ルータに CAPF 証明書をインストールしておく必要があります。この証明書を取得し、ルータにインストールするには、次の手順を実行します。

1. CUCM Operating System (OS) Administration の Web ページにアクセスします。
2. [Security] > [Certificate Management] を選択します。  
**注:** この場所は CUCM のバージョンに基づいて変わる場合があります。
3. **CAPF** というラベルが付いた証明書を見つけ、.pem ファイルをダウンロードします。これを .txt ファイルとして保存します。
4. 証明書を抽出したら、ルータに新しいトラストポイントを作成し、次のように CAPF でトラストポイントを認証します。Base 64 でエンコードされた CA 証明書を求められた場合は、ダウンロードした .pem ファイルのテキストを BEGIN 行から END 行まで選択して貼り付けます。

```
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
```

### 注意事項：

- 証明書はルータに手動でインストールする必要があるため、登録方法は端末です。
- クライアントが接続を行うときにユーザ名として何を使用するかをルータに指示するには、**authorization username** コマンドが必要です。この例では、ルータは共通名 ( CN ) を使用します。

- 電話証明書には証明書失効リスト ( CRL ) が定義されていないため、失効チェックは無効にする必要があります。無効にしない場合、接続は失敗し、Public Key Infrastructure ( PKI ) のデバッグに次の出力が表示されます。

```
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 capabilities 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
```

## 仮想コンテキストおよびグループ ポリシーの設定

設定のこの部分は、次の 2 つの点を除いて、前に使用した設定に似ています。

- 認証方式
- 電話を認証するためにコンテキストで使用されるトラストポイント  
コマンドは次のとおりです。

```
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 capabilities 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
```

## Call Manager の設定

ここでは、Call Manager の設定手順について説明します。

### 自己署名証明書またはアイデンティティ証明書をルータから CUCM にエクスポートする

ルータから証明書をエクスポートし、電話と VPN 間の信頼性証明書として証明書を Call Manager にインポートするには、次の手順を実行します。

1. SSL に使用されている証明書を確認します。

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

## 2. 証明書をエクスポートします。

```
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. 端末からこのテキストをコピーし、.pem ファイルとして保存します。
4. 前の手順で保存した証明書ファイルをアップロードするには、Call Manager にログインし、[Unified OS Administration] > [Security] > [Certificate Management] > [Upload Certificate] > [Select Phone-VPN-trust] の順に選択します。

## CUCM で VPN ゲートウェイ、グループ、およびプロファイルを設定する

1. Cisco Unified CM Administration に移動します。
2. メニューバーから、[Advanced Features] > [VPN] > [VPN Gateway] を選択します。



3. [VPN Gateway Configuration] ウィンドウで、次の手順を実行してください。  
[VPN Map Name] フィールドで、名前を入力します。これは、どんな名前にもできます。  
[VPN Gateway Description] フィールドに説明を入力します (任意選択)。  
[VPN Gateway URL] フィールドに、ルータで定義されたグループ URL を入力します。  
[VPN Certificates in this Location] フィールドで、信頼ストアからこの場所に移動するために以前に Call Manager にアップロードした証明書を選択します。



**-VPN Gateway Information-**

VPN Gateway Name\*

VPN Gateway Description

VPN Gateway URL\*

---

**-VPN Gateway Certificates-**

VPN Certificates in your Truststore

SUBJECT: CN=10.198.16.136,unstructuredName=10.198.16.136 ISSUER: CN=10.198.16.136,unstructuredName=10.198.16.136  
SUBJECT: unstructuredName=ASA5520-C.cisco.com,CN=ASA5520-C.cisco.com ISSUER: DC=com,DC=crtac,DC=cisco.com  
SUBJECT: C=CR,O=Cisco,OU=VPN,CN=ASA5520-C.cisco.com,unstructuredName=ASA5520-C.cisco.com ISSUER: CN=10.198.16.140:8443  
SUBJECT: CN=10.198.16.140:8443 ISSUER: CN=10.198.16.140:8443 S/N: e7:e2:72:4f  
SUBJECT: CN=ASA5510-F-IP-PHONE,unstructuredName=ASA5510-F.cisco.com ISSUER: CN=ASA5510-F-IP-PHONE

VPN Certificates in this Location\*

SUBJECT: CN=10.198.16.144,SERIALNUMBER=FTX1309A406+unstructuredName=R2811.vpn.cisco-tac.com ISSUER: CN=10.198.16.144,SERIALNUMBER=FTX1309A406+unstructuredName=R2811.vpn.cisco-tac.com

Save Delete Copy Add New

4. メニューバーから、[Advanced Features] > [VPN] > [VPN Group] を選択します。

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

**VPN Gateway Configuration**

Save ~~Delete~~ Copy Add

**Status**

*i* Status: Ready

**VPN Gateway Information**

VPN Gateway Name\*

VPN Gateway Description

VPN Gateway URL\*

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

5. [All Available VPN Gateways] フィールドで、以前に定義した [VPN Gateway] を選択します。下矢印をクリックして選択したゲートウェイを移動し、この [VPN Group] フィールドの [Selected VPN Gateways] に移動します。



## VPN Group Configuration

Save Delete Copy Add New

### Status

Status: Ready

### VPN Group Information

VPN Group Name\* IOS\_SSL\_Phones

VPN Group Description

### VPN Gateway Information

All Available VPN Gateways



Selected VPN Gateways in this VPN Group\* IOS\_SSL\_Phones

Save Delete Copy Add New

6. メニューバーから、[Advanced Features] > [VPN] > [VPN Profile] を選択します。

The screenshot shows the 'VPN Group Configuration' page with the 'Advanced Features' menu open. The menu items are: Voice Mail, SAF, EMCC, Intercompany Media Services, Fallback, VPN, VPN Profile, VPN Group, VPN Gateway, and VPN Feature Configuration. The 'VPN Profile' item is highlighted. The page content shows the 'Status' as 'Ready' and the 'VPN Group Name' as 'IOS\_SSL\_Phones'.

7. VPN のプロフィールを設定するには、アスタリスク (\*) でマーキングされているすべてのフィールドを入力します。

## 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

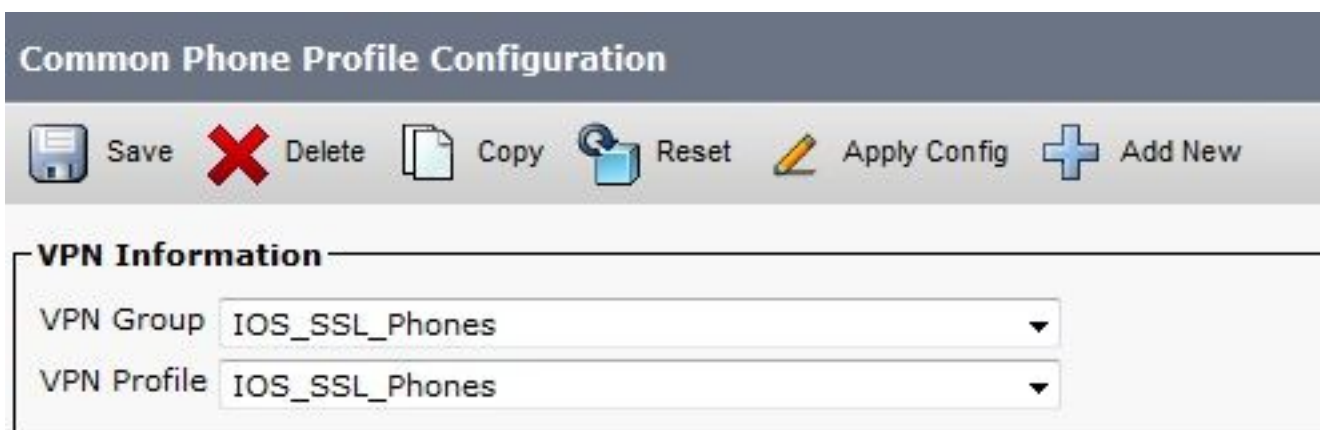
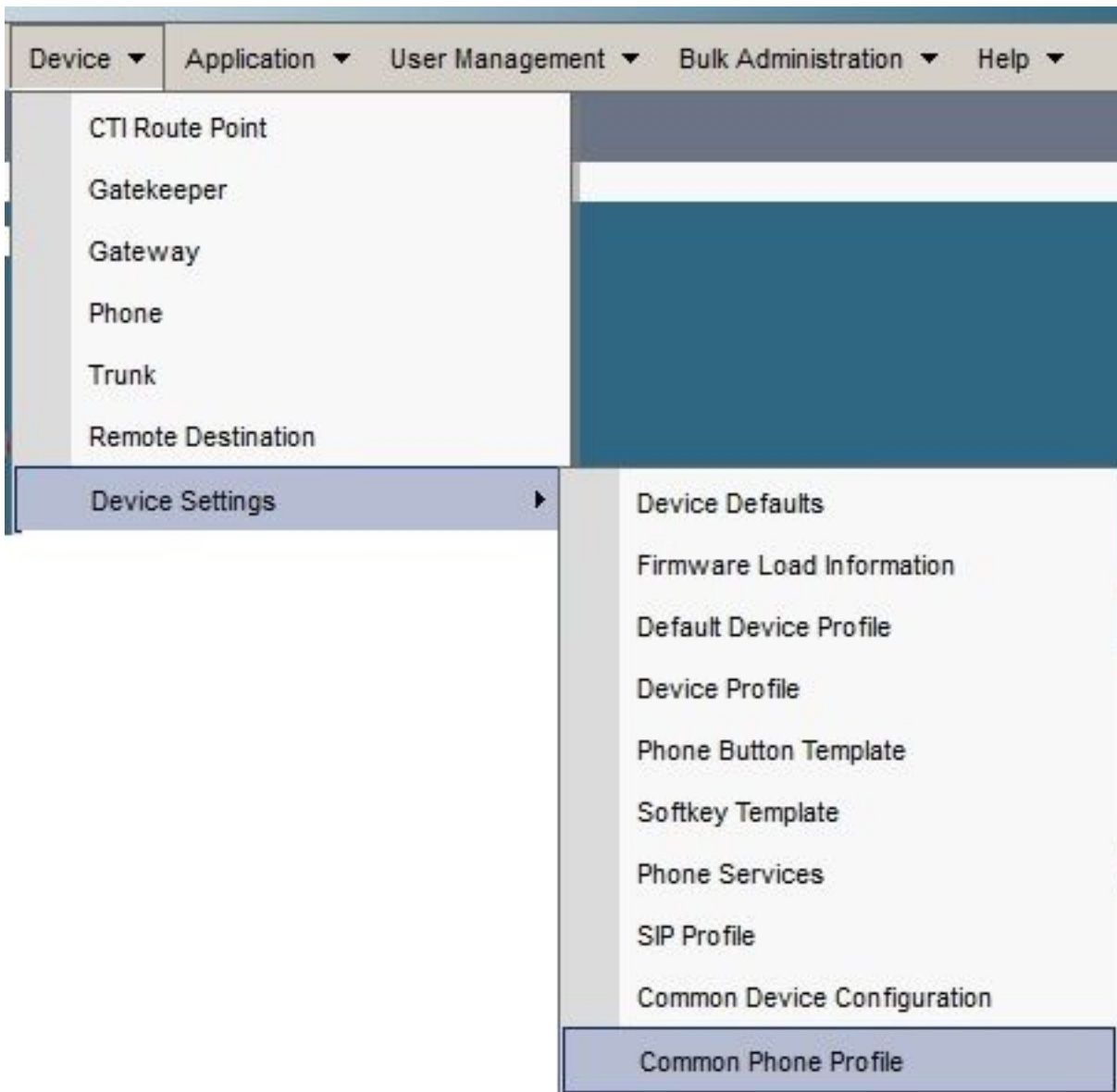
Client Authentication Method\*

Enable Password Persistence

[Enable Auto Network Detect] : 有効にした場合、VPN Phone は TFTP サーバを ping します。応答を受信しなかった場合は、VPN 接続を自動的に開始します。[Enable Host ID Check] : 有効にした場合、VPN Phone は VPN ゲートウェイ URL の完全修飾ドメイン名 ( FQDN ) と証明書の CN/ストレージ エリア ネットワーク ( SAN ) を比較します。これらの項目が一致しないか、またはアスタリスク ( \* ) の付いたワイルドカード証明書 ( \* ) が使用されている場合、クライアントは接続できません。[Enable Password Persistence] : これを使用すると、VPN Phone は次の VPN 接続試行に備えてユーザ名とパスワードをキャッシュします。

## 共通の電話プロファイルを使用してグループおよびプロファイルを IP フォンに適用する

新しい VPN 設定を適用するには、[Common Phone Profile Configuration ] ウィンドウで [Apply Config] をクリックします。標準の [Common Phone Profile] を使用するか、または新しいプロファイルを作成できます。



## 共通の電話プロファイルを IP フォンに適用する

特定の電話機/ユーザ用の新しいプロファイルを作成した場合は、[Phone Configuration] ウィンドウに移動します。[Common Phone Profile] フィールドで、[Standard Common Phone Profile] を選択します。



## ローカルで固有の証明書 ( LSC ) IP 電話を on Cisco インストールして下さい

次のガイドがローカルで固有の証明書 IP 電話を on Cisco インストールするのに使用することができます。このステップは LSC を使用して認証が使用される場合その時だけ必要です。Manufacturer を使用して認証は証明書 ( MIC ) をインストールしましたまたはユーザ名 およびパスワードは LSC がインストールされるように要求しません。

[非セキュアに CUCM クラスタ セキュリティモードが設定されていると電話で LSC をインストールして下さい。](#)

## 新しい設定をダウンロードするために電話を Call Manager に再度登録する

これは、設定プロセスの最後の手順です。

## 確認

### ルータの検証

ルータの VPN セッションの統計情報を確認するには、次のコマンドを使用して、ユーザ名と証明書認証の出力の違い ( 強調表示 ) を確認します。

### ユーザ名/パスワード認証の場合：

```
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

## 証明書認証の場合：

Router#**show webvpn session user SEP8CB64F578B2C context all**

Session Type : Full Tunnel  
Client User-Agent : Cisco SVC IPPhone Client v1.0 (1.0)

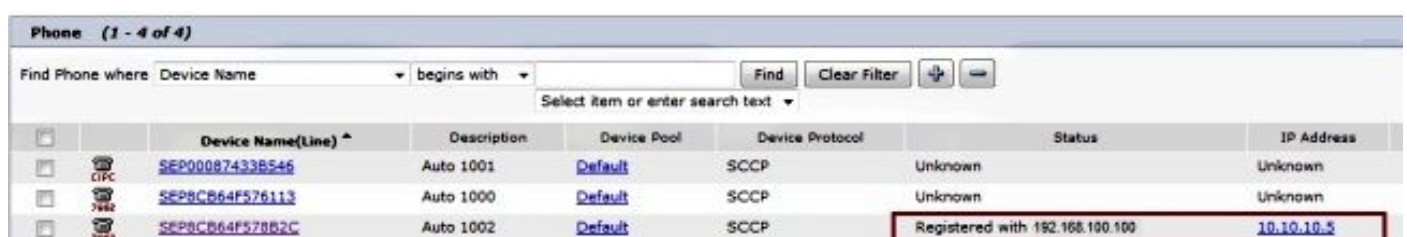
Username : **SEP8CB64F578B2C** Num Connection : 1  
Public IP : 172.16.250.34 VRF Name : None  
**CA Trustpoint : CAPF**  
Context : SSL Policy Group :  
Last-Used : 00:00:08 Created : 13:09:49.302 GMT  
Sat Mar 2 2013  
Session Timeout : Disabled Idle Timeout : 2100  
DPD GW Timeout : 300 DPD CL Timeout : 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 の検証

ルータが SSL 接続に提供した割り当てられたアドレスで IP フォンが Call Manager に登録されていることを確認します。



Device Name(Line) ^	Description	Device Pool	Device Protocol	Status	IP Address
SEP000874338546	Auto 1001	Default	SCCP	Unknown	Unknown
SEP8CB64F578B113	Auto 1000	Default	SCCP	Unknown	Unknown
SEP8CB64F578B2C	Auto 1002	Default	SCCP	Registered with 192.168.100.100	10.10.10.2

# トラブルシューティング

## SSL VPN サーバのデバッグ

Router#**show debug**

WebVPN Subsystem:

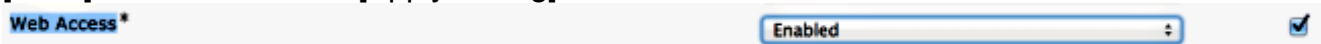
WebVPN (verbose) debugging is on  
WebVPN HTTP debugging is on  
WebVPN AAA debugging is on  
WebVPN tunnel debugging is on  
WebVPN Tunnel Events debugging is on  
WebVPN Tunnel Errors debugging is on  
Webvpn Tunnel Packets debugging is on

PKI:

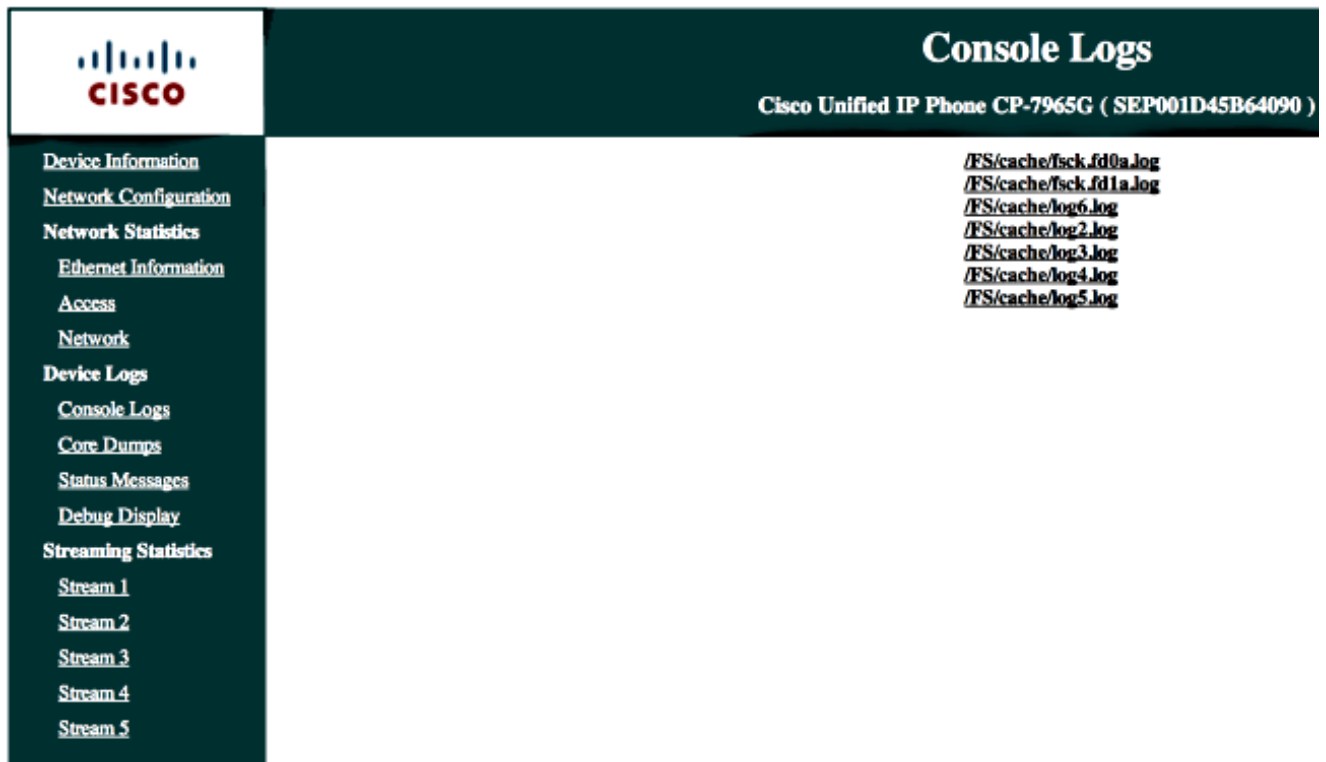
Crypto PKI Msg debugging is on  
Crypto PKI Trans debugging is on  
Crypto PKI Validation Path debugging is on

## 電話からのデバッグ

1. CUCM から [Device] > [Phone] に移動します。
2. デバイス設定ページで、[Web Access] を [Enabled] に設定します。
3. [Save] をクリックして、[Apply Config] をクリックします。



4. ブラウザから電話の IP アドレスを入力し、左側のメニューで [Console Logs] を選択します。

A screenshot of the Cisco Unified IP Phone management interface. The top header shows the Cisco logo and the title 'Console Logs' for device 'Cisco Unified IP Phone CP-7965G ( SEP001D45B64090 )'. On the left is a dark sidebar menu with various options like 'Device Information', 'Network Configuration', 'Device Logs', and 'Console Logs'. The 'Console Logs' option is highlighted. On the right side of the page, a list of log files is displayed: /FS/cache/fsck\_fd0a.log, /FS/cache/fsck\_fd1a.log, /FS/cache/log6.log, /FS/cache/log2.log, /FS/cache/log3.log, /FS/cache/log4.log, and /FS/cache/log5.log.

5. すべての /FS/cache/log\*.log ファイルをダウンロードします。コンソール ログ ファイルには、電話が VPN に接続できない理由についての情報が含まれています。



## 関連するバグ

Cisco bug ID [CSCty46387](#)、IOS SSLVPN : コンテキストをデフォルトにするための拡張  
Cisco bug ID [CSCty46436](#)、IOS SSLVPN : クライアント証明書検証の動作に対する拡張