

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

目次

[概要](#)

[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 サーバコンフィギュレーション](#)

[一般的な設定ステップ](#)

[AAA認証の設定](#)

[クライアント認証のための IP Phone ローカルで固有の認証 \(LSC \) との設定](#)

[Call Manager 設定](#)

[ルータから CUCM に自己署名か ID証明をエクスポートして下さい](#)

[VPNゲートウェイを設定し、グループ化し、CUCM でプロファイルして下さい](#)

[グループを適用し、よくある電話プロファイルの IP Phone にプロファイルして下さい](#)

[IP Phone によくある電話プロファイルを適用して下さい](#)

[新しい設定をダウンロードするために Call Manager に電話を再度登録して下さい](#)

[確認](#)

[ルータ 確認](#)

[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](#)

[関連するバグ](#)

概要

Cisco IP フォンが Cisco IOS ルータへの VPN 接続を確立できるようにこの資料に Cisco IOS[®] ルータおよび Call Manager デバイスを設定する方法を記述されています。これらの VPN 接続は必要これら二つのクライアント認証認証方法のどちらかの通信を保護するためです:

- 認証、許可、アカウンティング (AAA) サーバかローカルデータベース
- 電話認証

前提条件

要件

このドキュメントに関する固有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くものです。

- Cisco IOS 15.1(2)T またはそれ以降
 - 機能セット/ライセンス: Cisco IOS 統合サービス ルータ (ISR)-G2 のためのユニバーサル (データ及びセキュリティ及び UC)
 - 機能セット/ライセンス: Cisco IOS ISR のための拡張セキュリティ
 - Cisco Unified Communications Manager (CUCM) Release 8.0.1.100000-4 以降
 - IP Phone リリース 9.0(2)SR1S - Skinny Client Control Protocol (SCCP) またはそれ以降
- 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
- コール マネージャ リリース 8.5.1.10000-26
- IP Phone リリース 9.1(1)SR1S

このドキュメントの情報は、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、クリアな (デフォルト) 設定で作業を開始しています。ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

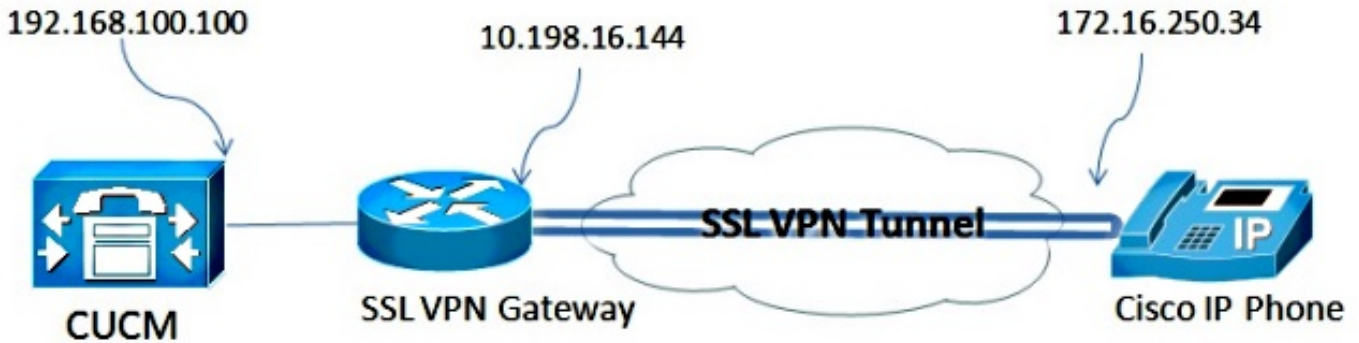
設定

このセクションはこの資料に説明がある機能を設定するのに必要とされる情報をカバーします。

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

この資料で使用されるトポロジは Secure Sockets Layer (SSL) VPNゲートウェイとして 1 Cisco IP Phone、Cisco IOS ルータ、および音声ゲートウェイとして CUCM が含まれています。



SSL VPN サーバコンフィギュレーション

このセクションは受信 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記述します。

一般的な 設定ステップ

1. 1024 バイトの長さの Rivest シャミールAddleman (RSA) キーを生成して下さい:

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

2. 自己署名証明書のためのトラストポイントを作成し、SSL RSA キーを接続して下さい:

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

3. トラストポイントが設定されたら、このコマンドで自己署名証明書を登録して下さい:

```
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. ヘッドエンドの AnyConnect 正しいパッケージを有効に して下さい。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、パッケージなしで、VPN トンネルは確立しません。Cisco.com で利用可能な最新のクライアントソフトウェア バージョンを使用するために推奨します。この例はバージョン 3.1.3103 を使用します。

より古い Cisco IOSバージョンでは、これはコマンド パッケージを有効にするためにです:

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

ただし、Cisco IOSバージョンで、これはコマンドです:

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

5. VPNゲートウェイを設定して下さい。WebVPN ゲートウェイはユーザからの SSL 接続を終えるために使用されます。

```
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
```

注: どちらか IP アドレスは電話が接続される、またはゲートウェイはルータでインターフェイスから直接ソースをたどられる必要がありますインターフェイスとして同じサブネットである必要をここでは使用しました。ゲートウェイもどの認証がによってクライアントに自体検証するためにルータ使用されるか定義するために使用されます。

6. 接続するときクライアントに 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て下さい:

```
ip local pool ap_phonenvpn 192.168.100.1 192.168.100.254
```

AAA認証の設定

このセクションは AAAサーバかローカルデータベースを設定する電話を認証するために必要なコマンドを説明します。電話のために認証のみの認証を使用するために計画する場合次のセクションに進んで下さい。

ユーザデータベースを設定して下さい

ルータのローカルデータベースか外部 AAAサーバは認証に使用することができます:

- ローカルデータベースを設定するために、入力して下さい:

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

- 認証のための遠隔 AAA RADIUS サーバを設定するために、入力して下さい:

```
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
```

仮想 な コンテキストおよびグループ ポリシーを設定して下さい

仮想 な コンテキストは VPN 接続を支配する属性を定義するために使用されます (以下を参照):

- 接続する時使用するべきかどの URL を
- クライアントアドレスをか割り当てるために使用するべきどのプールを
- 使用するべきかどの認証方式を

これらのコマンドはクライアントのために AAA認証を使用するコンテキストの例です:

```
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_phonenvpn" netmask 255.255.255.0
svc keep-client-installed
default-group-policy phones
```

クライアント認証のための IP Phone ローカルで固有の認証 (LSC) との設定

このセクションは電話のための認証ベース クライアント認証を設定する必要があるコマンドを説明します。ただし、これをするために、電話認証のさまざまな型のナレッジは必要となります:

- **製造業者インストール済み認証 (MIC)** - MIC は新しモデル Cisco すべての 7941、7961、および IP 電話に含まれています。MIC は Cisco 認証局 (CA) によって署名する 2,048 ビットキー認証です。MIC 認証を信頼する CUCM のためにそれは証明書信頼ストアでプレインストールされた CA 証明 CAP-RTP-001、CAP-RTP-002 および Cisco_Manufacturing_CA を使用します。この認証自体は、名前に示すように提供されるので、製造業者によってクライアント認証のためにこの認証を使用することを推奨しません。
- **LSC** : LSC は、認証または暗号化のデバイス セキュリティ モードを設定した後から CUCM と電話機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。これはより多くの安全な方法です (MIC の使用に対して)。
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) 認証のために、または他のどの目的で MIC を使用するために Cisco IP 電話を設定する顧客はそう自己の責任において。

この設定例では電話を認証するために、LSC は使用されます。

ヒント : 電話を接続するセキュア方法は認証および AAA 認証を結合する二重認証を使用することです。1 つの仮想 な コンテキスト以下それぞれのために使用されるコマンドを結合する場合これを設定できます。

クライアント 認証を検証するためにトラストポイントを設定して下さい

ルータは IP Phone からの LSC を検証するためにインストールされる CAPF 認証を備えなければなりません。その認証を得、ルータでインストールするために、これらのステップを完了して下さい:

1. CUCM Operating System (OS) 管理 Web ページに行ってください。
2. [Security] > [Certificate Management] を選択します。
注: この位置は CUCM バージョンに基づいて変更されるかもしれません。
3. 認証を CAPF と分類される見つけ、.pem ファイルをダウンロードして下さい。 .txt ファイルとしてそれを保存して下さい

4. certificate が得られたら、ルータの新しいトラストポイントを作成し、ここに示されているように CAPF のトラストポイントを、認証して下さい。base-64 のためにプロンプト表示されたとき CA 認証を符号化し、開始および最終行と共にダウンロードされた .pem ファイルのテキストを選択し、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
```

注意するべき事柄:

- 登録方式は認証がルータで手動でインストールされなければならないのでターミナルです。
- クライアントが接続をするときユーザ名として使用すればいいのか許可 `username` コマンドがルータに何を述べるために必要となります。この場合、それは Common Name (CN) を使用します。
- 失効チェックは電話認証に定義される証明書無効リスト (CRL) がないのでディセーブルにされる必要があります。このように無効でなければ、接続は失敗し、公開鍵インフラストラクチャ (PKI) デバッグはこの出力を示します:

```
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
```

仮想な コンテキストおよびグループ ポリシーを設定して下さい

設定のこの一部は 2 ポイントを除いて、以前に使用される設定に類似したです:

- 認証方式
- トラストポイント コンテキスト使用電話を認証するため

コマンドはここに示されています:

```
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_phonenvpn" netmask 255.255.255.0
  svc keep-client-installed
default-group-policy phones
```

Call Manager 設定

このセクションは Call Manager コンフィギュレーションのステップを記述します。

ルータから CUCM に自己署名か ID証明をエクスポートして下さい

認証をルータからエクスポートし、認証を電話 VPN 信頼認証として Call Manager にインポートするために、これらのステップを完了して下さい:

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-----
```

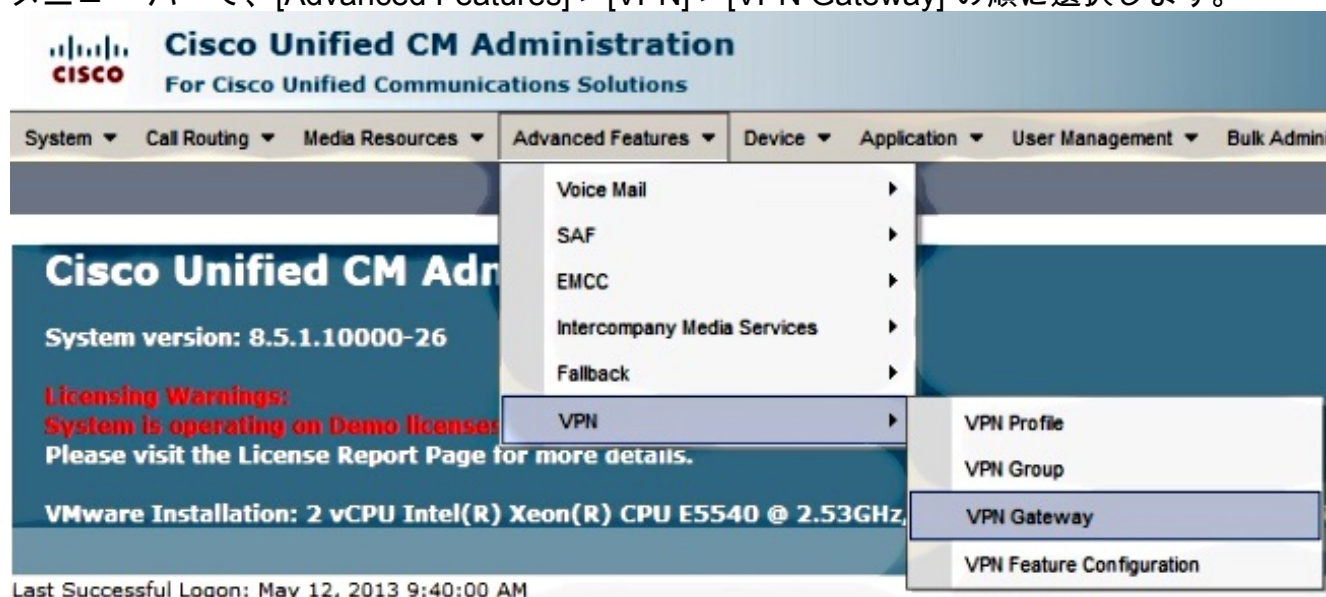
<output removed>

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

3. 端末からのテキストをコピーし、.pem ファイルとして保存します。
4. Call Manager へのログインは、統一された OS 管理 > Security > Certificate Management > アップロード認証を > 選定された電話 VPN 信頼前の手順で保存される証明書ファイルをアップロードするために選択し。

VPNゲートウェイを設定し、グループ化し、CUCM でプロファイルして下さい

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



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)。ルータで定義される VPNゲートウェイ URL フィールドでは、グループ URL を入力して下さい。この Location フィールドの VPN 認証では、信頼ストアからこの位置にそれを移動するために Call Manager に以前にアップロードされた認証を選択して下さい。

-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,CN=ASA5520-C.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 S/N: e7:e2:72:4f
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. メニューバーで、[Advanced Features] > [VPN] > [VPN Group] の順に選択します。

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. すべての利用可能な VPNゲートウェイ フィールドで、以前に定義される VPNゲートウェイを選択して下さい。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*

VPN Group Description

VPN Gateway Information

All Available VPN Gateways

Selected VPN Gateways in this VPN Group*

Save Delete Copy Add New

6. メニューバーで、[Advanced Features] > [VPN] > [VPN Profile] の順に選択します。

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

VPN Group Configuration

Save Delete Copy Add

Status

Status: Ready

VPN Group Information

VPN Group Name*

VPN Group Description

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

7. VPN のプロファイルを設定するには、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*

IOS_SSL_Phones

Description

Enable Auto Network Detect

Tunnel Parameters

MTU*

1290

Fail to Connect*

30

Enable Host ID Check

Client Authentication

Client Authentication Method* Certificate

Enable Password Persistence

Save

Delete

Copy

Add New

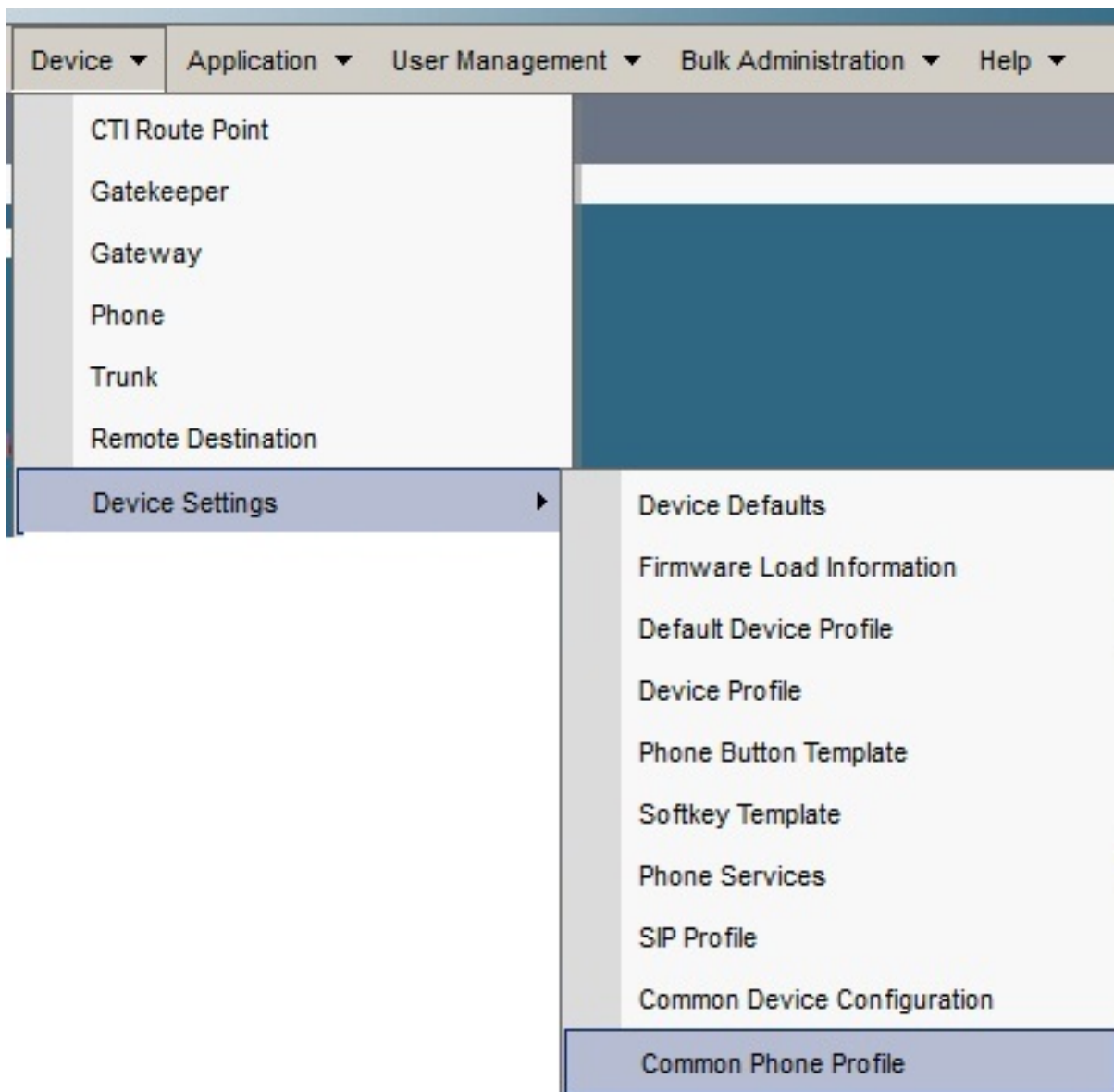
[Enable Auto Network Detect] : 有効にされた場合、VPN 電話は TFTPサーバを ping します。応答を受信しなかった場合は、VPN 接続を自動的に開始します。

[Enable Host ID Check] : 有効にされた場合、VPN 電話は認証の CN/Storage エリア ネットワーク (SAN) に対して VPNゲートウェイ URL の完全修飾ドメイン名 (FQDN) を比較します。クライアントはこれらの項目が一致するか、またはアスタリスク (*) のワイルドカード 認証が使用されれば接続し損います。






[Enable Password Persistence] : これは VPN 電話が次の VPN 試みのためのユーザ名 およびパスワードをキャッシュするようにします。

グループを適用し、よくある電話プロファイルの IP Phone にプロファイルして下さい

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。標準よくある電話プロファイルを使用するか、または新しいプロファイルを作成できます。



Common Phone Profile Configuration

Save  Delete  Copy  Reset  Apply Config  Add New

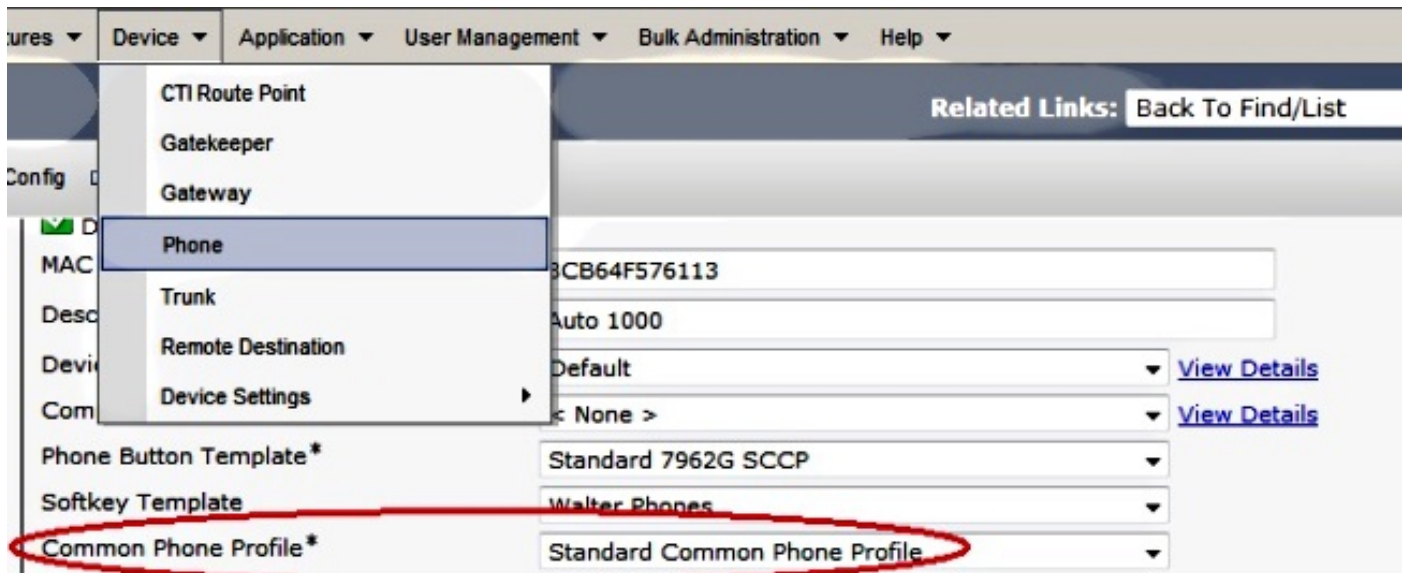
VPN Information

VPN Group

VPN Profile

IP Phone によくある電話プロファイルを適用して下さい

特定の電話/ユーザ向けの新しいプロファイルを作成した場合、Phone Configuration ウィンドウにナビゲートして下さい。よくある電話 Profile フィールドで、標準よくある電話プロファイルを選択して下さい。



新しい設定をダウンロードするために Call Manager に電話を再度登録して下さい

これはコンフィギュレーションプロセスの最後の段階です。

確認

ルータ 確認

ルータの VPN セッションの統計情報をチェックするために、これらのコマンドを使用できユーザ名および証明書認証があるように出力間の違いを (強調表示される) 確認します:

username/password 認証に関しては:

```
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
```

証明書認証に関しては:

```
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

IP Phone が割り当てられたアドレスの Call Manager に SSL 接続に提供されるルータ登録されていることを確認して下さい。

Device Name(Line) ^	Description	Device Pool	Device Protocol	Status	IP Address
SEP000874338546	Auto 1001	Default	SCCP	Unknown	Unknown
SEP8CB64F576113	Auto 1000	Default	SCCP	Unknown	Unknown
SEP8CB64F578B2C	Auto 1002	Default	SCCP	Registered with 192.168.100.100	10.10.10.5

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:
```

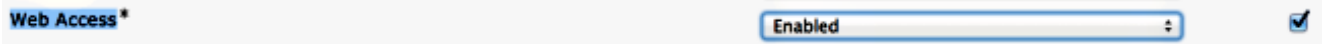
```
WebVPN (verbose) debugging is on
```

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

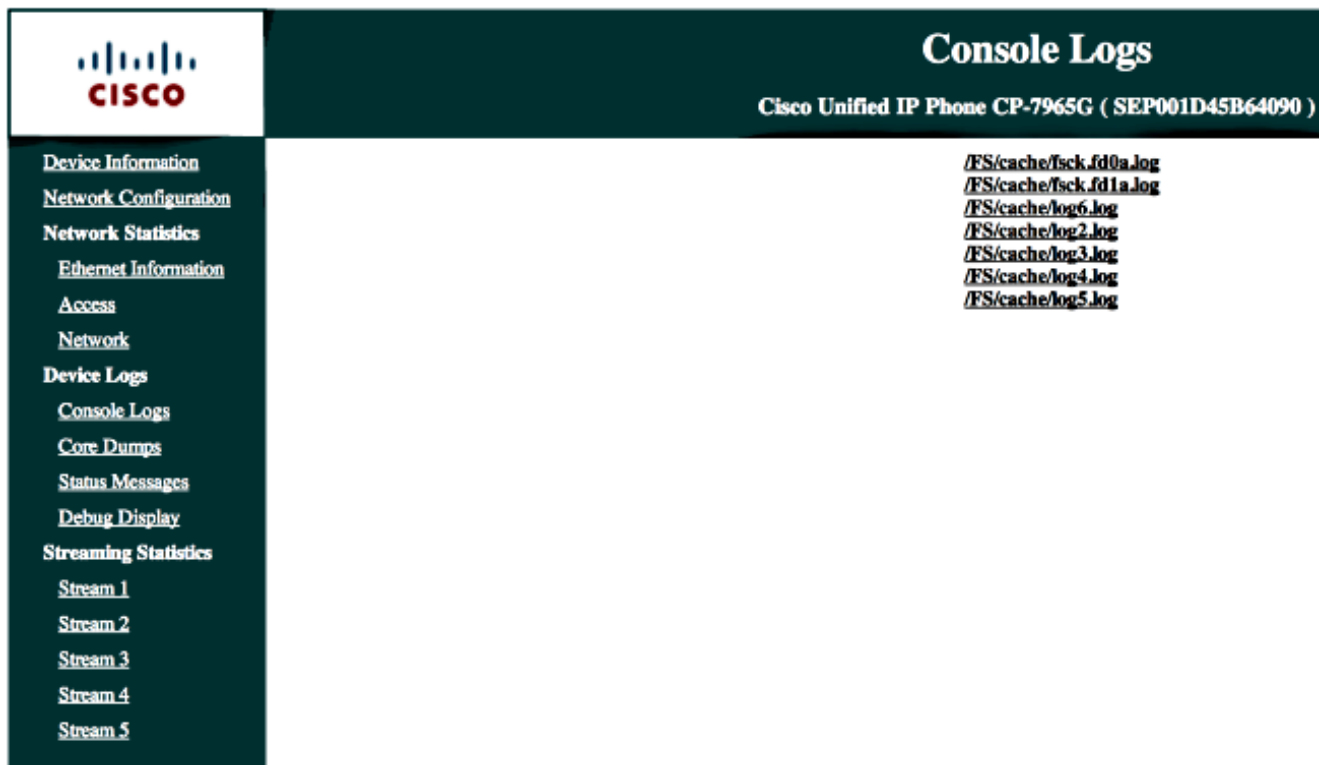
PKI:
Crypto PKI Msg debugging is on
Crypto PKI Trans debugging is on
Crypto PKI Validation Path debugging is on

電話からのデバッグ

1. CUCM からの **Device > Phone** へのナビゲート。
2. デバイスコンフィギュレーション ページで、**イネーブル**になったへの Web アクセスを設定して下さい。
3. 『SAVE』 をクリックし、次に**構成**を『Apply』 をクリックして下さい。



4. ブラウザから、電話の IP アドレスを入力し、左のメニューから**ログ**を『Console』 を選択して下さい。



5. /FS/cache/log *.log ファイルすべてをダウンロードして下さい。コンソール ログ ファイルは電話が VPN になぜについての接続されないか情報が含まれています。

関連するバグ

Cisco バグ ID [CSCty46387](#)、IOS SSLVPN: デフォルトでコンテキストをもらう拡張

Cisco バグ ID [CSCty46436](#)、IOS SSLVPN: クライアント 認証 検証 動作への拡張