解決して下さい AnyConnect VPN 電話- IP フォン、ASA および CUCM

目次

概要

この資料に IP 電話で問題を解決する方法を記述されていますように VPNゲートウェイ使用するおよび音声サーバとして使用する Cisco Unified Communications Manager （ CUCM ）に接続するため a に Cisco 適応型セキュリティ アプライアンス (ASA) ソフトウェア接続するために Secure Sockets Layer （ SSL ）プロトコル (Cisco AnyConnect セキュア モビリティ クライアント ）を使用する (ASA) 。

VPN 電話との AnyConnect の設定例に関しては、これらの文書を参照して下さい:

- IP Phone を使用する SSLVPN トンネルの設定例
- 証明書認証を使用した AnyConnect VPN Phone の設定例

背景説明

IP 電話を使用して SSL VPN を展開する前に、ASA 用と CUCM の米国輸出制限バージョン用の AnyConnect ライセンスに関する次の初期要件が満たされていることを確認します。

ASA 上の VPN 電話ライセンスの確認

VPN 電話ライセンスは ASA の機能を有効にします。 AnyConnect (IP 電話かどうかに関係なく) と接続可能なユーザ数を確認するには、AnyConnect Premium SSL ライセンスをチェックします。 詳細については、「IP Phone およびモバイル VPN 接続に ASA ライセンスが必要な理由」を参照してください。

ASA で、**show version command** コマンドを使用して、機能が有効になっているかどうかをチェックします。 ライセンス名は ASA リリースによって異なります。

- ASA リリース 8.0.x： ライセンス名は AnyConnect for Linksys Phone です。
- ASA リリース 8.2.x 以降： ライセンス名は AnyConnect for Cisco VPN Phone です。

ASA リリース 8.0.x のための例はここにあります:

```
ASA5505(config)# show ver

Cisco Adaptive Security Appliance Software Version 8.0(5)
Device Manager Version 7.0(2)
<snip>
Licensed features for this platform:
VPN Peers : 10
WebVPN Peers : 2
AnyConnect for Linksys phone : Disabled
<snip>
This platform has a Base license.
```

ASA リリース 8.2.x およびそれ以降のための例はここにあります:

```
ASA5520-C(config)# show ver

Cisco Adaptive Security Appliance Software Version 9.1(1)
Device Manager Version 7.1(1)
<snip>
Licensed features for this platform:
AnyConnect Premium Peers : 2 perpetual
AnyConnect Essentials : Disabled perpetual
AnyConnect for Cisco VPN Phone    : Disabled       perpetual
<snip>
This platform has an ASA 5520 VPN Plus license.
```

輸出制限 CUCM と輸出無制限 CUCM

VPN 電話機能を利用するには、CUCM の米国輸出制限バージョンを展開する必要があります。

CUCM の米国輸出制限バージョンを使用する場合は、次の点に注意してください。

- IP 電話のセキュリティ設定がシグナリングとメディアの暗号化を無効にするように変更されます。 これには VPN 電話機能による暗号化が含まれます。
- インポート/エクスポート経由で VPN の詳細をエクスポートできません。
- [VPN Profile]、[VPN Gateway]、[VPN Group]、および [VPN Feature Configuration] の各チェックボックスが表示されません。

注: CUCM の米国輸出無制限バージョンにアップグレードすると、このソフトウェアの米国

輸出制限バージョンにアップグレードしたり、その新規インストールを実行したりできなくなります。

ASA の一般的な問題

注: showコマンド出力の分析を表示するために Cisco CLI アナライザ（登録ユーザのみ）を使用できます。 **debug コマンドを**使用する前にまた Debug コマンド Ciscoドキュメントの重要な情報を参照する必要があります。

ASA で使用する証明書

ASA では、自己署名 SSL 証明書、サードパーティ SSL 証明書、およびワイルドカード証明書を使用できます。 このすべてが IP 電話と ASA 間の通信を保護します。

使用できるのは 1 つの ID 証明書だけです、これは、各インターフェイスに 1 つの証明書しか割り当てることができないためです。

サードパーティ SSL 証明書の場合は、ASA にチェーン全体をインストールして、中間証明書とルート証明書を含めます。

ASA エクスポートおよび CUCM インポート用のトラストポイント/証明書

SSL ネゴシエーション中に ASA から IP 電話に提示される証明書は、ASA からエクスポートして、CUCM にインポートする必要があります。 IP 電話が接続されているインターフェイスに割り当てられたトラストポイントをチェックして、ASA からエクスポートする証明書を確認します。

show run ssl コマンドを使用して、エクスポートするトラストポイント（証明書）を確認します。 詳細については、「証明書認証を使用した AnyConnect VPN Phone の設定例」を参照してください。

注: 1つ以上の ASA にサード・パーティ証明書を展開する場合、各 ID証明を各 ASA から エクスポートし、次に電話 VPN 信頼として CUCM にインポートする必要があります。

ASA は設定された RSA 証明書の代りに ECDSA 自己署名証明書を示します

この問題が発生するとき、新しいモデル電話はより古いモデル電話は問題を直面しないが接続されることができません。 この問題が発生するときここに口グオンします電話をであって下さい:

```
ASA5520-C(config)# show ver

Cisco Adaptive Security Appliance Software Version 9.1(1)
Device Manager Version 7.1(1)
<snip>
Licensed features for this platform:
AnyConnect Premium Peers : 2 perpetual
AnyConnect Essentials : Disabled perpetual
AnyConnect for Cisco VPN Phone    : Disabled       perpetual
<snip>
This platform has an ASA 5520 VPN Plus license.
```

バージョン 9.4.1 および それ 以降では、楕円カーブ暗号解読法は SSL/TLS のためにサポートされます。 新しい電話モデルのような楕円曲線可能な SSL VPN クライアントが ASA に接続するとき、楕円カーブ暗号スイートはネゴシエートされ、ASA は対応するインターフェイスが RSA ベースのトラストポイントで設定される時でさえ、楕円カーブ証明書との SSL VPN クライアントを示します。 ASA が自己署名 SSL 証明書を示すことを、管理者が **ssl 暗号**コマンドによって対応する暗号スイートを取除く必要がある防ぐために。 たとえば、RSA トラストポイントで設定されるインターフェイスのために RSA ベースの暗号だけネゴシエートされるように、管理者はこのコマンドを実行できます:

```
ssl cipher tlsv1.2 custom "AES256-SHA:AES128-SHA:DHE-RSA-AES256-SHA:DHE-RSA-AES128-SHA"
```

Cisco バグ ID CSCuu02848 の実装によって、優先順位は設定に与えられます。 明示的設定証明書は常に使用されます。 自己署名証明書は設定された証明書がない時だけ使用されます。

提案されたクライアント暗号	**RSA 証明書だけ**	**EC 証明書だけ**	**両方の証明書**	**な**
RSA はただ暗号化します	RSA 証明書を使用します RSA 暗号を使用します	RSA 自己署名証明書を使用します RSA 暗号を使用します	RSA 証明書を使用します RSA 暗号を使用します	RS しま RS

EC はただ暗号化します（まれ）	**接続は失敗します**	EC 証明書を使用します EC 暗号を使用します	EC 証明書を使用します EC 暗号を使用します	EC ます EC
両方の暗号だけ	RSA 証明書を使用します RSA 暗号を使用します	EC 証明書を使用します EC 暗号を使用します	EC 証明書を使用します EC 暗号を使用します	EC ます EC

IP 電話ユーザの認証用の外部データベース

IP Phone ユーザを認証するために外部 データベースを使用できます。 Lightweight Directory Access Protocol（LDAP）または Remote Authentication Dial In User Service （RADIUS）のようなプロトコルは VPN 電話ユーザの認証に使用することができます。

ASA 証明書と VPN 電話信頼リスト間での証明書ハッシュの照合

ASA SSL インターフェイスに割り当てられた証明書をダウンロードして CUCM 内の電話 VPN 信頼証明書としてアップロードする必要があることに注意してください。 環境によっては、ASA から提示されるこの証明書のハッシュと、CUCM サーバが生成してコンフィギュレーション ファイル経由で VPN 電話にプッシュするハッシュが一致しない場合があります。

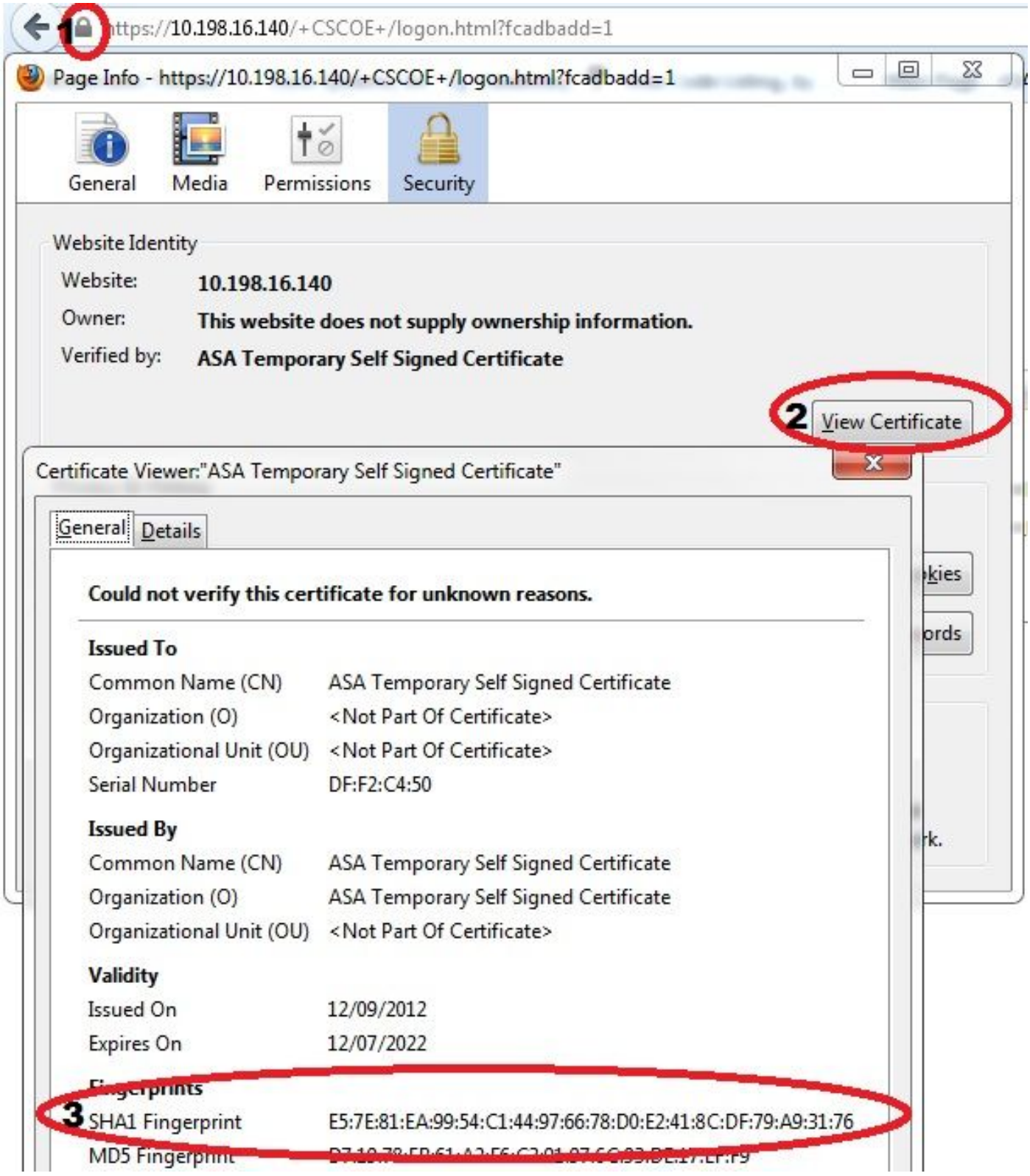
設定が完了したら、IP 電話と ASA 間の VPN 接続をテストしてください。 接続に成功しない場合は、ASA 証明書のハッシュと、IP 電話で想定されているハッシュが一致するかどうかを確認します。

1. ASA から提示されるセキュア ハッシュ アルゴリズム 1（SHA1）ハッシュを確認します。
2. CUCM から IP 電話コンフィギュレーション ファイルをダウンロードするには、TFTP を使用します。
3. ハッシュは、16 進数から Base 64 に、または、Base 64 から 16 進数にデコードします。

SHA1 ハッシュの確認

ASA は、IP 電話が接続されているインターフェイス上で **ssl trustpoint** コマンドを使用して適用

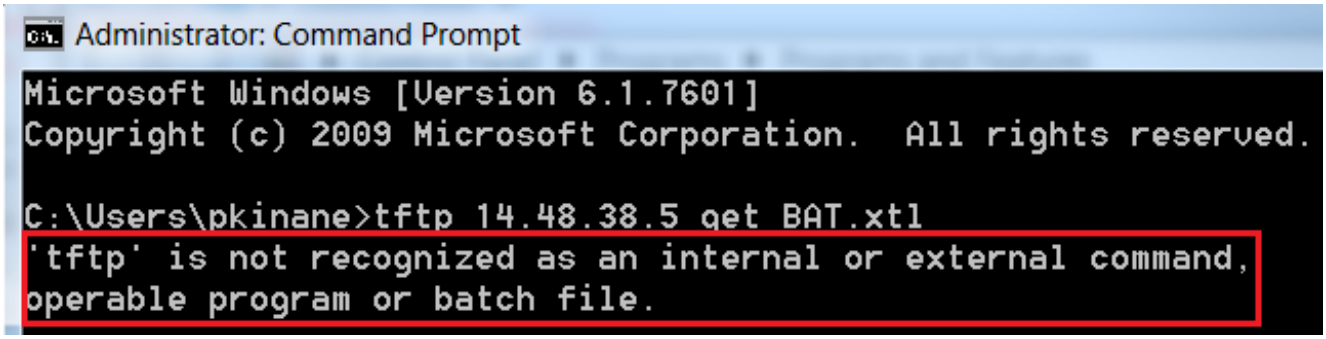
された証明書を提示します。 この証明書をチェックするには、ブラウザ（この例では Firefox）を開いて、電話を接続する URL（group-url）を入力します。

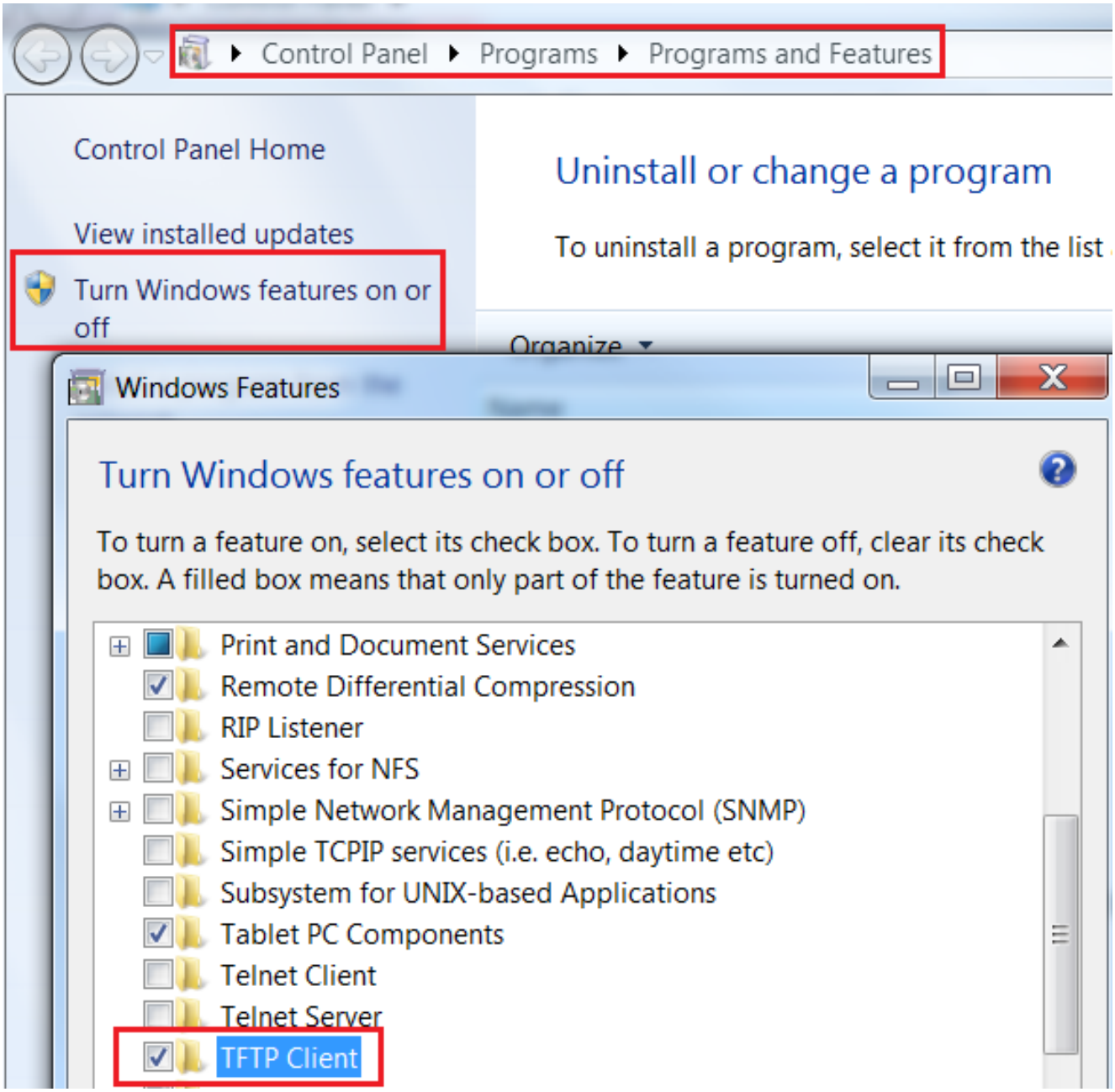


IP 電話コンフィギュレーション ファイルのダウンロード

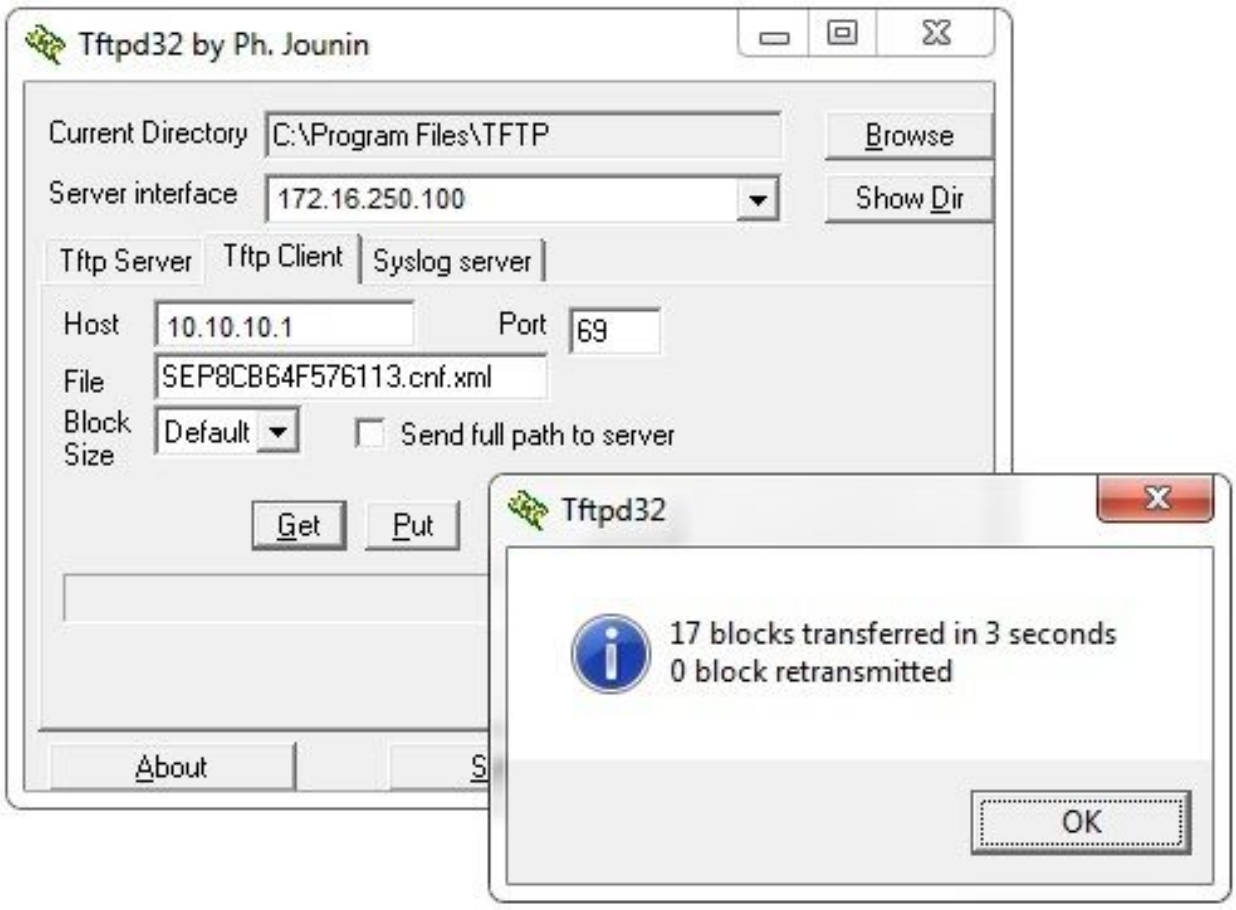
CUCM へのダイレクト アクセスを備えた PC から、接続の問題がある電話の TFTP コンフィギュレーション ファイルをダウンロードします。 次の 2 種類のダウンロード方法があります。

1. Windows の CLI セッションを開き、**tftp を-i** *<TFTP Server>* **GET SEP** *<Phone MAC アドレス >.cnf.xml* **コマンド**使用して下さい。
   注: ものと同じようなエラーを下記に受け取る場合、TFTP クライアント機能がイネーブルになっていることを確認する必要があります。





2. ファイルをダウンロードするのに Tftpd32 のようなアプリケーションを使用して下さい:

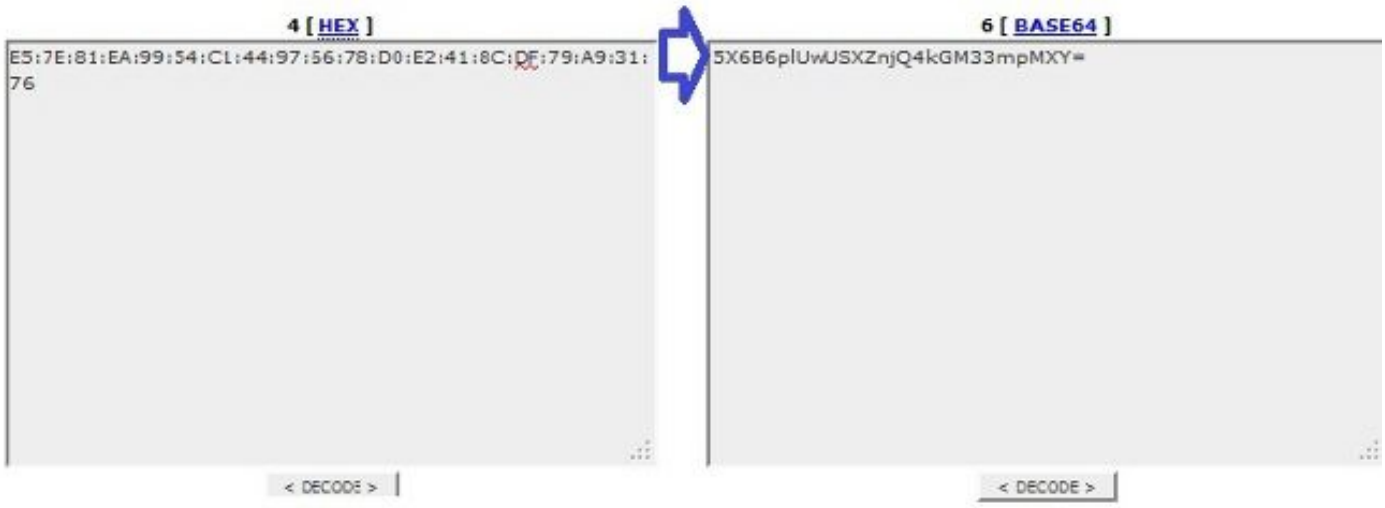


3. ファイルがダウンロードされたら、XML を開き、*vpnGroup* 設定を見つけて下さい。 次の例で、確認すべきセクションと certHash を示します。

```
<vpnGroup>
<mtu>1290</mtu>
<failConnectTime>30</failConnectTime>
<authMethod>2</authMethod>
<pswdPersistent>0</pswdPersistent>
<autoNetDetect>0</autoNetDetect>
<enableHostIDCheck>0</enableHostIDCheck>
<addresses>
<url1>https://10.198.16.140/VPNPhone</url1>
</addresses>
<credentials>
<hashAlg>0</hashAlg>
<certHash1>5X6B6plUwUSXZnjQ4kGM33mpMXY=</certHash1>
</credentials>
</vpnGroup>
```

ハッシュのデコード

両方のハッシュ値が一致することを確認します。 ブラウザはハッシュを 16 進数形式で表示しますが、XML ファイルでは Base 64 が使用されるため、一致を確認するには一方の形式から他方の形式に変換する必要があります。 さまざまな変換ツールを使用できます。 1 つの例が TRANSLATOR, BINARY です。



注: 上記ハッシュ値が一致しなかった場合は、VPN 電話が ASA とネゴシエートされた接続を信頼しないため、接続に失敗します。

VPN ロードバランシングと IP 電話

負荷分散された SSL VPN は VPN 電話でサポートされません。 VPN 電話は、実際の証明書を検証しませんが、代わりに、CUCM からプッシュダウンされたハッシュを使用してサーバを検証します。 VPN ロードバランシングの原理は HTTP リダイレクトであり、電話機が複数の証明書を検証する必要があるため、エラーが発生します。 VPN ロードバランシング エラーの症状には次のようなものがあります。

- 電話機がサーバ間を往復するため、接続に異常に時間がかかったり、最終的に失敗したりします。
- 電話機の口グには次のようなメッセージが書き込まれます。

```
<vpnGroup>
<mtu>1290</mtu>
<failConnectTime>30</failConnectTime>
<authMethod>2</authMethod>
<pswdPersistent>0</pswdPersistent>
```

```
    <autoNetDetect>0</autoNetDetect>
    <enableHostIDCheck>0</enableHostIDCheck>
    <addresses>
    <url1>https://10.198.16.140/VPNPhone</url1>
    </addresses>
    <credentials>
    <hashAlg>0</hashAlg>
    <certHash1>5X6B6plUwUSXZnjQ4kGM33mpMXY=</certHash1>
    </credentials>
    </vpnGroup>
```

CSD と IP 電話

現在、IP 電話は Cisco Secure Desktop（CSD）をサポートしていないため、CSD が tunnel-group に対してまたは ASA 内でグローバルに有効になっている場合は接続が行われません。

最初に ASA にイネーブルになっている CSD があるかどうか、確認して下さい。 ASA CLI で **show run webvpn** コマンドを入力して下さい:

```
ASA5510-F# show run webvpn
webvpn
enable outside
 csd image disk0:/csd_3.6.6210-k9.pkg
csd enable
anyconnect image disk0:/anyconnect-win-3.1.00495-k9.pkg 1
anyconnect enable
ASA5510-F#
```

CSD 問題を IP Phone 接続の間にチェックするために、ASA のログかデバッグをチェックして下さい。

ASA ログ

```
ASA5510-F# show run webvpn
webvpn
enable outside
 csd image disk0:/csd_3.6.6210-k9.pkg
csd enable
anyconnect image disk0:/anyconnect-win-3.1.00495-k9.pkg 1
anyconnect enable
ASA5510-F#
```

ASA デバッグ

```
debug webvpn anyconnect 255
<snip>
Tunnel Group: VPNPhone, Client Cert Auth Success.
WebVPN: CSD data not sent from client
http_remove_auth_handle(): handle 24 not found!
<snip>
```

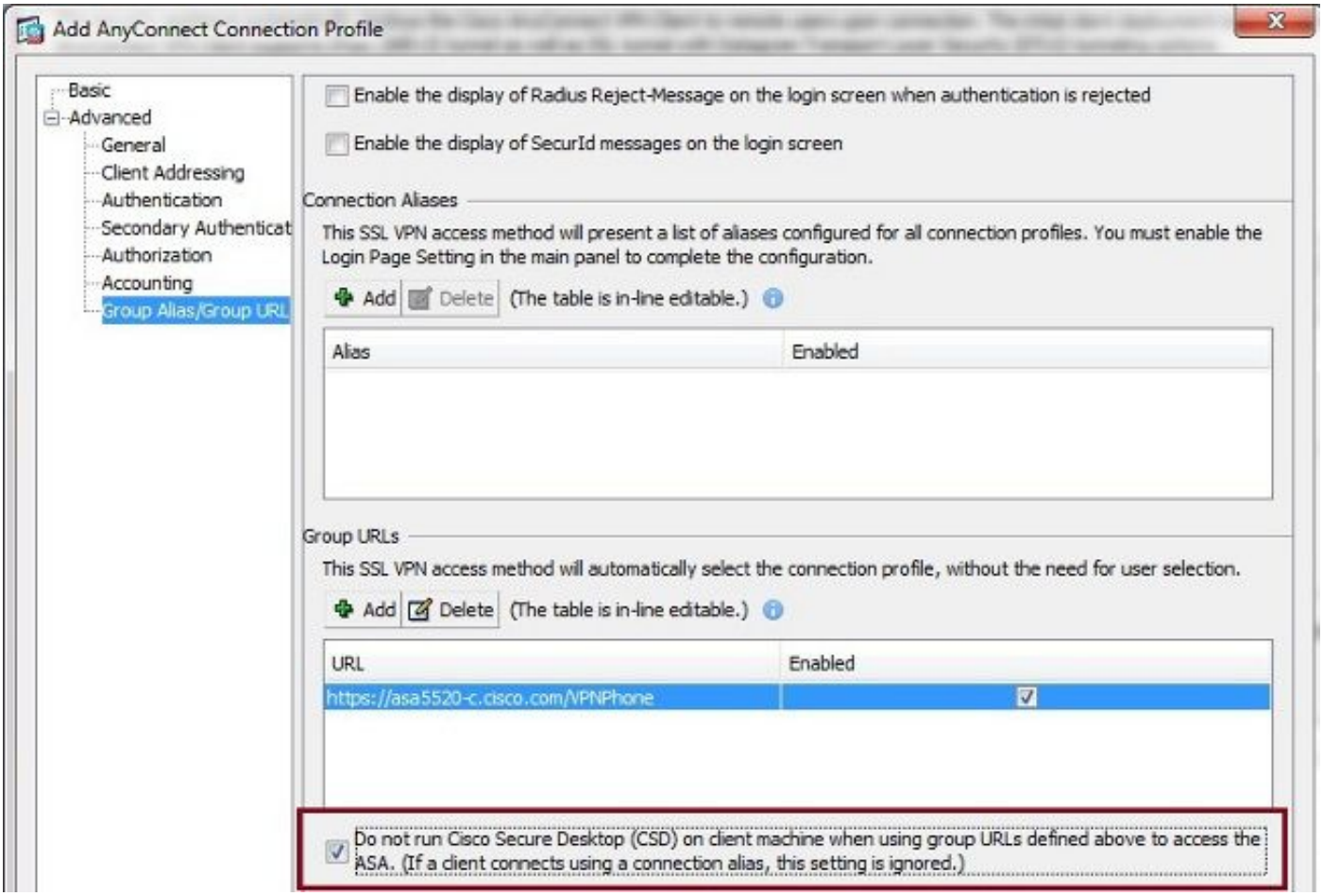
注: AnyConnect ユーザの高負荷との大きい配備では、Cisco は**デバッグ webvpn anyconnect を**有効に しないことを推奨します。 この出力は IP アドレスで絞り込むことができないため、大量の情報が生成される可能性があります。

ASA バージョン 8.2 および それ 以降では、トンネル グループの webvpn 属性の下で命じますなし **csd を**適用して下さい:

```
tunnel-group VPNPhone webvpn-attributes
authentication certificate
group-url https://asa5520-c.cisco.com/VPNPhone enable
 without-csd
```

以前のバージョンの ASA では、これができなかったため、唯一の回避策が CSD をグローバルに無効にすることでした。

Cisco Adaptive Security Device Manager（ASDM）で、この例で示すように、特定の接続プロファイルの CSD を無効にすることができます。

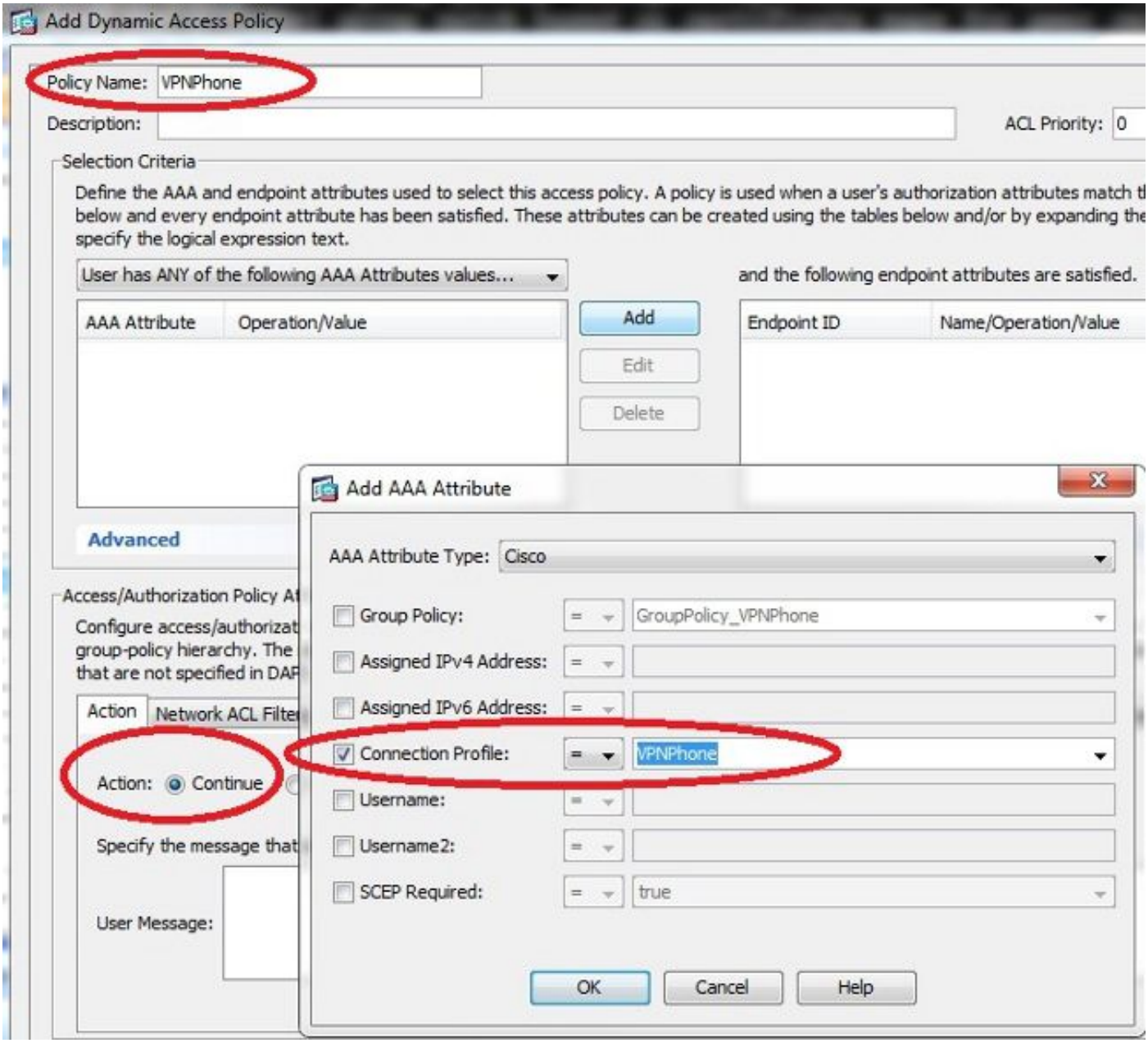


注: CSD を消すためにグループ URL を特色になります使用して下さい。

DAP ルール

ほとんどの展開では、IP 電話が ASA に接続されるだけでなく、さまざまなタイプのマシン（Microsoft、Linux、Mac OS）とモバイル デバイス（Android、iOS）も接続されます。 そのため、ダイナミック アクセス ポリシー（DAP）ルールの既存の設定が見つかることがよくあります。このルールでは、大抵、DfltAccessPolicy の下の Default Action が接続の停止になっています。

このような場合は、VPN 電話用の別の DAP ルールを作成します。 特定のパラメータを、接続プロファイルのような使用し、**続く**操作を設定して下さい:



IP 電話専用の DAP ポリシーを作成しなかった場合は、ASA に DfltAccessPolicy 違反と失敗した接続が表示されます。

```
%ASA-6-716038: Group <DfltGrpPolicy> User <CP-7962G-SEP8CB64F576113> IP
<172.16.250.9> Authentication: successful, Session Type: WebVPN.
%ASA-7-734003: DAP: User CP-7962G-SEP8CB64F576113, Addr 172.16.250.9: Session
Attribute aaa.cisco.grouppolicy = GroupPolicy_VPNPhone
<snip>
%ASA-6-734001: DAP: User CP-7962G-SEP8CB64F576113, Addr 172.16.250.9,
Connection AnyConnect: The following DAP records were selected for this
connection: DfltAccessPolicy
%ASA-5-734002: DAP: User CP-7962G-SEP8CB64F576113, Addr 172.16.250.9: Connection
   terminated by the following DAP records: DfltAccessPolicy
```

アクションが [Continue] に設定された IP 電話専用の DAP ポリシーを作成した場合は、接続でき

ます。

```
%ASA-7-746012: user-identity: Add IP-User mapping 10.10.10.10 -
LOCAL\CP-7962G-SEP8CB64F576113 Succeeded - VPN user
%ASA-4-722051: Group <GroupPolicy_VPNPhone> User <CP-7962G-SEP8CB64F576113> IP
<172.16.250.9> Address <10.10.10.10> assigned to session
%ASA-6-734001: DAP: User CP-7962G-SEP8CB64F576113, Addr 172.16.250.9, Connection
AnyConnect: The following DAP records were selected for this connection: VPNPhone
```

DfltGrpPolicy またはその他のグループからの継承値

多くの場合、DfltGrpPolicy は複数のオプションを使用してセットアップされます。 デフォルトで、これらの設定は、IP 電話で使用すべき group-policy 内で手動で指定されなかった場合に、IP 電話セッションに継承されます。

DfltGrpPolicy から継承された場合に接続に影響するパラメータは次のとおりです。

- group-lock
- vpn-tunnel-protocol
- vpn-simultaneous-logins
- vpn-filter

DfltGrpPolicy および GroupPolicy_VPNPhone でこの設定例があると仮定して下さい:

```
group-policy DfltGrpPolicy attributes
 vpn-simultaneous-logins 0
 vpn-tunnel-protocol ikev1 ikev2 l2tp-ipsec ssl-clientless
 group-lock value DefaultWEBVPNGroup
vpn-filter value NO-TRAFFIC

group-policy GroupPolicy_VPNPhone attributes
wins-server none
dns-server value 10.198.29.20
default-domain value cisco.com
```

接続は GroupPolicy_VPNPhone の下で明示的に規定 されなかった受継ぎ、IP Phone に接続の間に情報すべてを押します DfltGrpPolicy からのパラメータを。

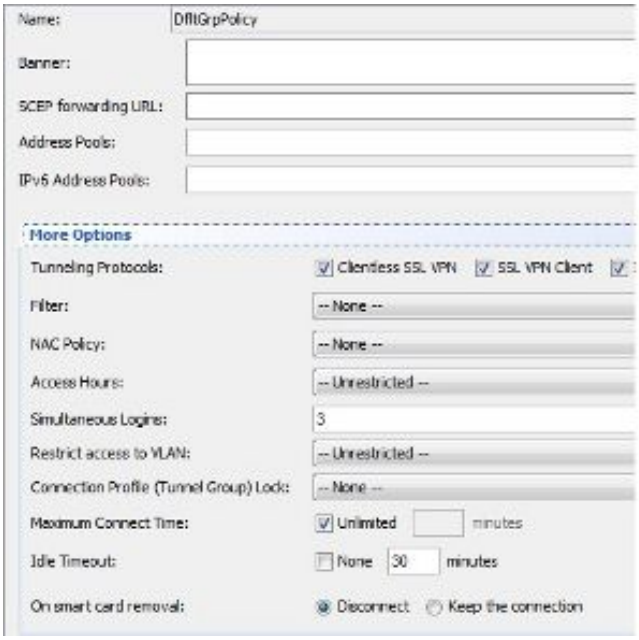
これを避けるために、手動でグループで直接必要とする値を規定 して下さい:

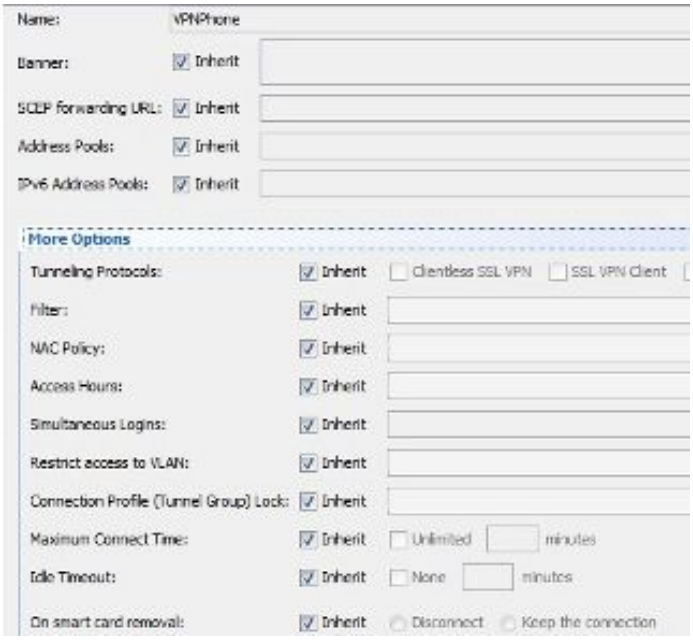
```
group-policy GroupPolicy_VPNPhone internal
group-policy GroupPolicy_VPNPhone attributes
wins-server none
dns-server value 10.198.29.20
 vpn-simultaneous-logins 3
vpn-tunnel-protocol ssl-client
group-lock value VPNPhone
 vpn-filter none
 default-domain value cisco.com
```

DfltGrpPolicy のデフォルト値を確認するには、show run all group-policy コマンドを使用します。次の例で、出力の違いを明示します。

```
ASA5510-F# show run group-policy DfltGrpPolicy
group-policy DfltGrpPolicy attributes
 dns-server value 10.198.29.20 10.198.29.21
 vpn-tunnel-protocol ikev1 ikev2 l2tp-ipsec ssl-client ssl-clientless
 default-domain value cisco.com
ASA5510-F#

ASA5510-F# sh run all group-policy DfltGrpPolicy
group-policy DfltGrpPolicy internal
group-policy DfltGrpPolicy attributes
banner none
wins-server none
dns-server value 10.198.29.20 10.198.29.21
dhcp-network-scope none
vpn-access-hours none
vpn-simultaneous-logins 3
vpn-idle-timeout 30
vpn-idle-timeout alert-interval 1
vpn-session-timeout none
vpn-session-timeout alert-interval 1
vpn-filter none
ipv6-vpn-filter none
vpn-tunnel-protocol ikev1 ikev2 l2tp-ipsec ssl-client ssl-clientless
```

ASDM 経由で属性を継承した group-policy の出力を以下に示します。





サポートされる暗号方式

7962G IP 電話とファームウェア バージョン 9.1.1 でテストされた AnyConnect VPN 電話は、どちらも Advanced Encryption Standard (AES) である AES256-SHA と AES128-SHA の 2 つの暗号方式のみをサポートします。 正しい暗号が ASA で規定 されない場合、接続は ASA ログに示すように、拒否されます:

```
%ASA-7-725010: Device supports the following 2 cipher(s).
%ASA-7-725011: Cipher[1] : RC4-SHA
%ASA-7-725011: Cipher[2] : DES-CBC3-SHA
%ASA-7-725008: SSL client outside:172.16.250.9/52684 proposes the following
2 cipher(s).
%ASA-7-725011: Cipher[1] : AES256-SHA
%ASA-7-725011: Cipher[2] : AES128-SHA
%ASA-7-725014: SSL lib error. Function: SSL3_GET_CLIENT_HELLO Reason: no
   shared cipher
```

ASA にイネーブルになっている正しい暗号があるかどうか確認するために **show run をすべての ssl** 入力し、**ssl** コマンドを**示して下さい**:

```
ASA5510-F# show run all ssl
ssl server-version any
ssl client-version any
ssl encryption rc4-sha1 aes128-sha1 aes256-sha1 3des-sha1
ssl trust-point SSL outside
```

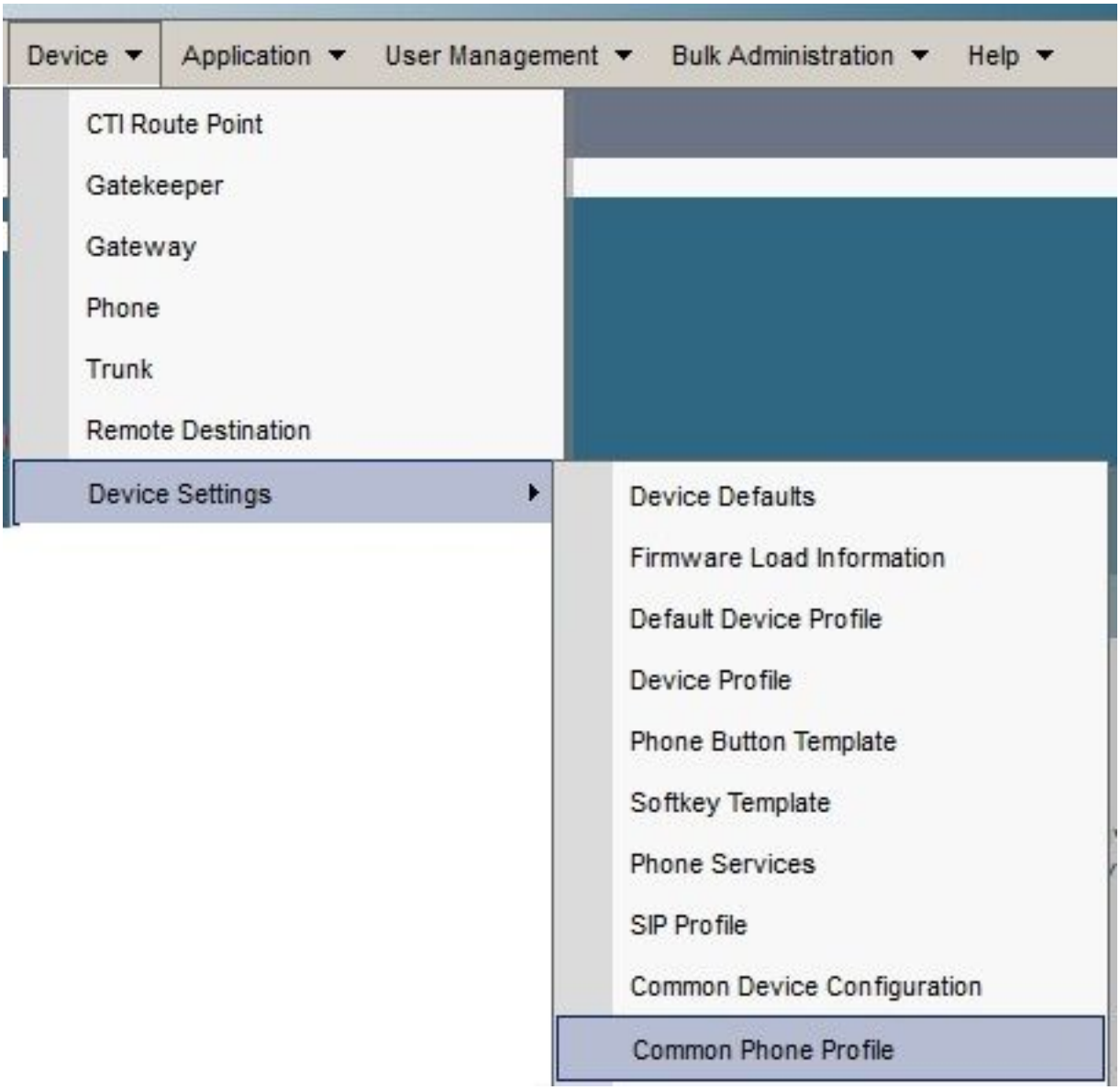
```
ASA5510-F#

ASA5510-F# show ssl
Accept connections using SSLv2, SSLv3 or TLSv1 and negotiate to SSLv3 or TLSv1
Start connections using SSLv3 and negotiate to SSLv3 or TLSv1
Enabled cipher order: rc4-sha1 aes128-sha1 aes256-sha1 3des-sha1
Disabled ciphers: des-sha1 rc4-md5 dhe-aes128-sha1 dhe-aes256-sha1 null-sha1
SSL trust-points:
outside interface: SSL
Certificate authentication is not enabled
ASA5510-F#
```

CUCM の一般的な問題

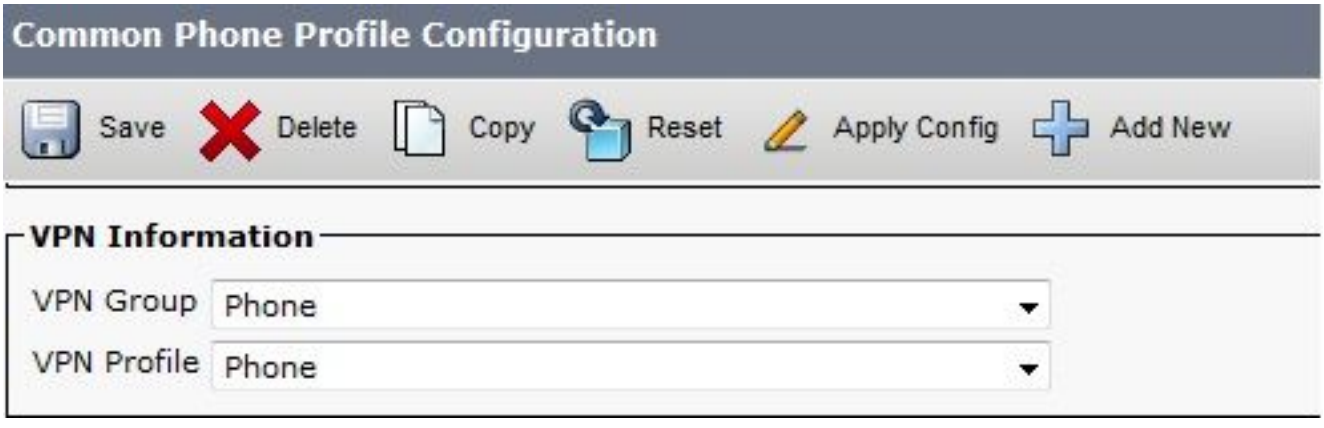
IP 電話に適用されない VPN 設定

CUCM 上でコンフィギュレーション（ゲートウェイ、グループ、およびプロファイル）を作成したら、共通電話プロファイル内の VPN 設定を適用します。

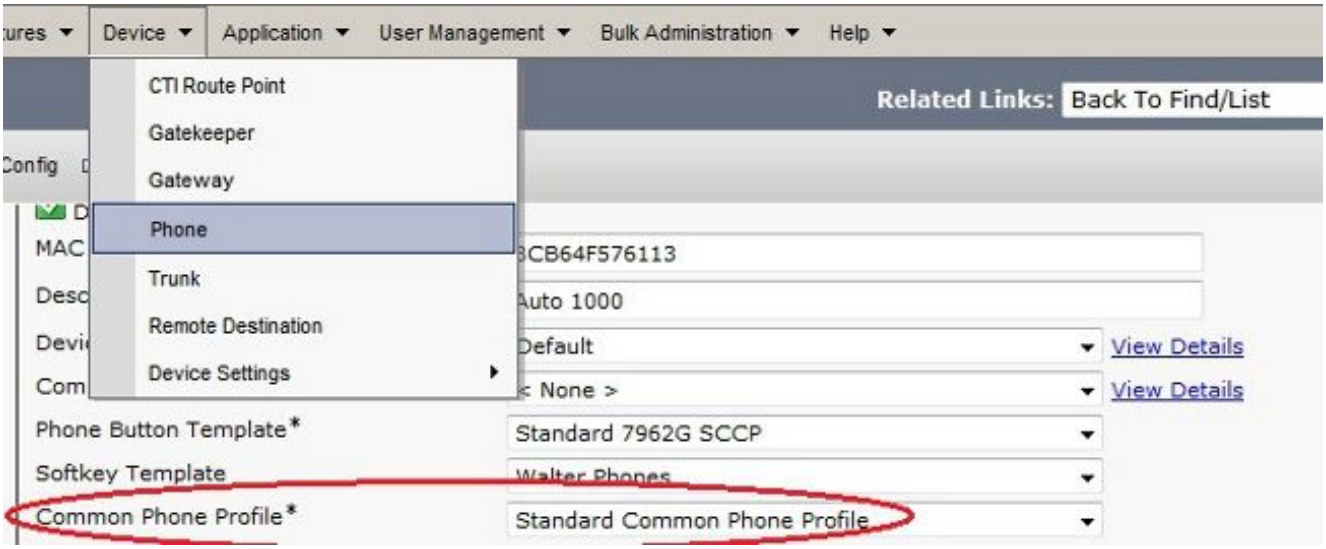
1. [Device] > [Device Settings] > [Common Phone Profile] に移動します。



2. VPN 情報を入力します。



3. **Device > Phone** へのナビゲートは電話 設定にこのプロファイルを割り当てられます確認し、：



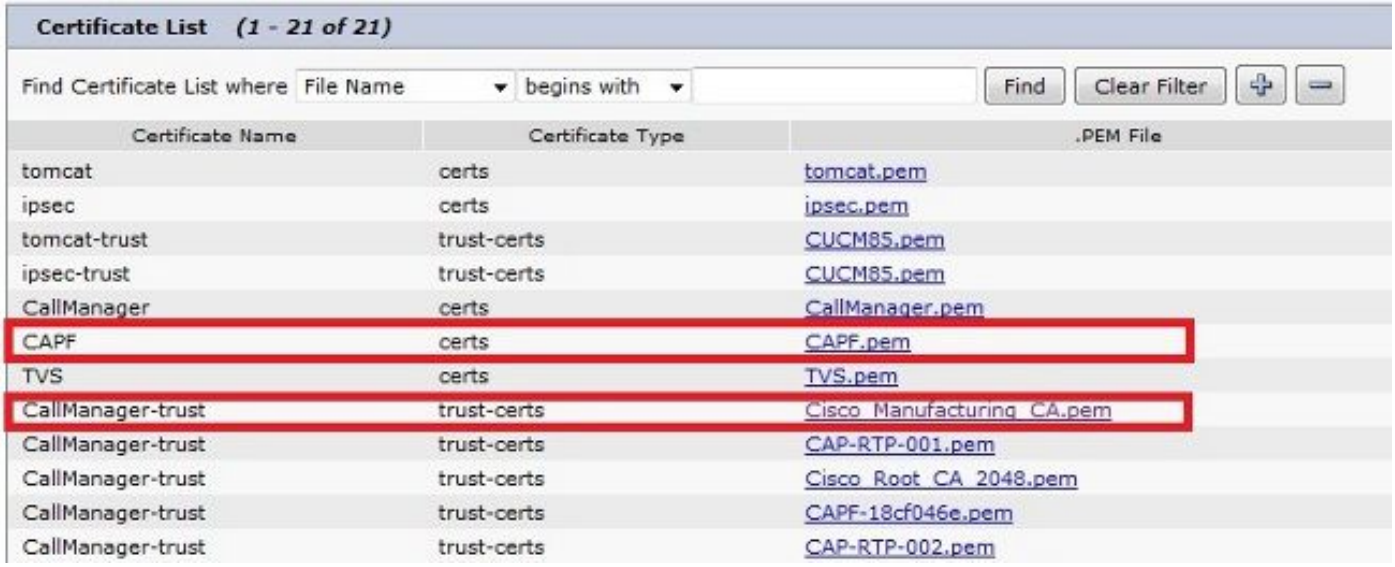
証明書認証方法

IP 電話の証明書認証を設定する方法には、 Manufacturer Installed Certificate（MIC）とローカルで有効な証明書（LSC）の 2 種類があります。 状況に最適なオプションを選択するには、「証明書認証を使用した AnyConnect VPN Phone の設定例」を参照してください。

証明書認証を設定するときに、CUCM サーバから証明書（ルート CA）をエクスポートして、ASA にインポートします。

1. CUCM にログインします。
2. [Unified OS Administration] > [Security] > [Certificate Management] に移動します。
3. Certificate Authority Proxy Function（CAPF）または Cisco_Manufacturing_CA を探します。証明書のタイプは MIC または LSC 証明書認証を使用したかどうかによって異なります。
4. ファイルをローカル コンピュータにダウンロードします。

ファイルがダウンロードされれば、CLI による ASA へのログインか ASDM は CA 認証としておよび証明書をインポートします。



Certificate List (1 - 21 of 21)

Find Certificate List where File Name begins with Find Clear Filter

Certificate Name	Certificate Type	.PEM File
tomcat	certs	tomcat.pem
ipsec	certs	ipsec.pem
tomcat-trust	trust-certs	CUCM85.pem
ipsec-trust	trust-certs	CUCM85.pem
CallManager	certs	CallManager.pem
CAPF	certs	CAPF.pem
TVS	certs	TVS.pem
CallManager-trust	trust-certs	Cisco_Manufacturing_CA.pem
CallManager-trust	trust-certs	CAP-RTP-001.pem
CallManager-trust	trust-certs	Cisco_Root_CA_2048.pem
CallManager-trust	trust-certs	CAPF-18cf046e.pem
CallManager-trust	trust-certs	CAP-RTP-002.pem

デフォルトでは、VPN をサポートするすべての電話機に MIC があらかじめロードされています。 7960 および 7940 モデルの電話機には MIC が付属しないため、LSC を安全に登録するための特別なインストール手順が必要です。

最新の Cisco IP Phone (8811、8841、8851、8861) には、新しい製造元 SHA2 CA によって署名された MIC 証明書が含まれています。

- CUCM バージョン 10.5(1) は、新しい SHA2 証明書を含んでおり、これを信頼します。
- 以前の CUCM バージョンを実行する場合は、新しい製造元 CA 証明書をダウンロードし、次のいずれかを実行する必要があります。

  電話機が LSC を取得するために CAPF を使って認証できるようにするため、証明書を CAPF 信頼にアップロードします。

  電話機が SIP 5061 のために MIC を使って認証できるようにする場合は、証明書を CallManager 信頼にアップロードします。

ヒント： 現在 CUCM で旧バージョンが実行されている場合は、SHA2 CA を取得するためにこのリンクをクリックします。

注意： シスコでは、LSC のインストールのみに MIC を使用することを推奨します。 シスコは、CUCM による TLS 接続の認証で LSC をサポートします。 MIC ルート証明書は侵害される可能性があるため、TLS 認証やその他の目的で MIC を使用するように電話機を設定する場合は、お客様の責任で行ってください。 MIC が侵害された場合、シスコは一切の責任を負いません。

デフォルトで、電話機に LSC が組み込まれている場合は、電話機に MIC が組み込まれているかどうかに関係なく、認証で LSC が使用されます。 電話機に MIC と LSC が組み込まれている場合は、認証で LSC が使用されます。 電話機に LSC が組み込まれていないが、MIC が組み込まれている場合は、認証で MIC が使用されます。

> **注:** 証明書認証の場合は、ASA から SSL 証明書をエクスポートして、CUCM にインポートする必要があることに注意してください。

ホスト ID チェック

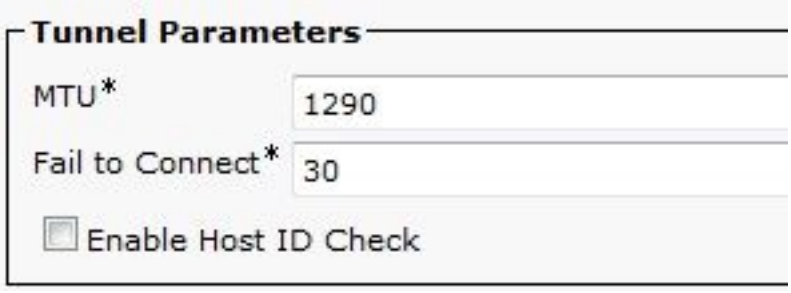
証明書のタイトル内の一般名（CN）が電話機から VPN 経由で ASA に接続するときに使用される URL（group-url）と一致しない場合は、CUCM 上のホスト ID チェックを無効にするか、ASA 上のその URL と一致する ASA 内の証明書を使用します。

この操作は、ASA の SSL 証明書がワイルドカード証明書の場合、SSL 証明書に別の SAN（Subject Alternative Name）が含まれている場合、または URL が完全修飾ドメイン名（FQDN）の代わりに IP アドレスを使用して作成された場合に必要です。

これは、証明書の CN が電話機から到達しようとしている URL と一致しない場合の IP 電話ログの例です。

```
1231: NOT 07:07:32.445560 VPNC: DNS has wildcard, starting checks...
1232: ERR 07:07:32.446239 VPNC: Generic third level wildcards are not allowed,
stopping checks on host=(test.vpn.com) and dns=(*.vpn.com)
1233: NOT 07:07:32.446993 VPNC: hostID not found in subjectAltNames
1234: NOT 07:07:32.447703 VPNC: hostID not found in subject name
1235: ERR 07:07:32.448306 VPNC: hostIDCheck failed!!
```

ホストID を無効に するために**進んだ機能** > **VPN** > **VPN プロファイル**に CUCM を、ナビゲートチェックインして下さい:



その他のトラブルシューティング

ASA で使用するログとデバッグ

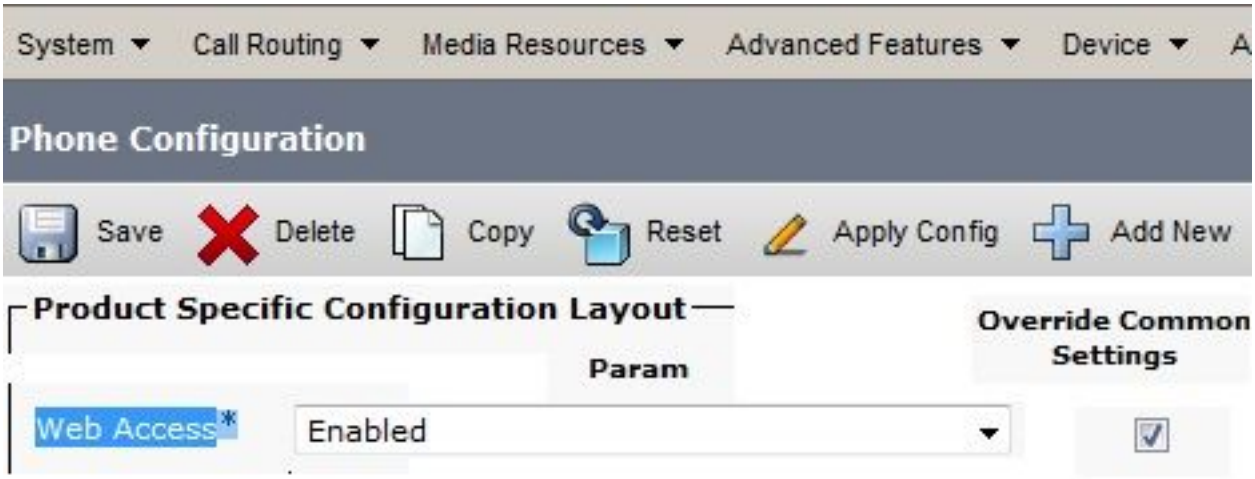
ASA では、これらのデバッグと口グを有効にしてトラブルシューティングに利用できます。

```
1231: NOT 07:07:32.445560 VPNC: DNS has wildcard, starting checks...
1232: ERR 07:07:32.446239 VPNC: Generic third level wildcards are not allowed,
stopping checks on host=(test.vpn.com) and dns=(*.vpn.com)
1233: NOT 07:07:32.446993 VPNC: hostID not found in subjectAltNames
1234: NOT 07:07:32.447703 VPNC: hostID not found in subject name
1235: ERR 07:07:32.448306 VPNC: hostIDCheck failed!!
```

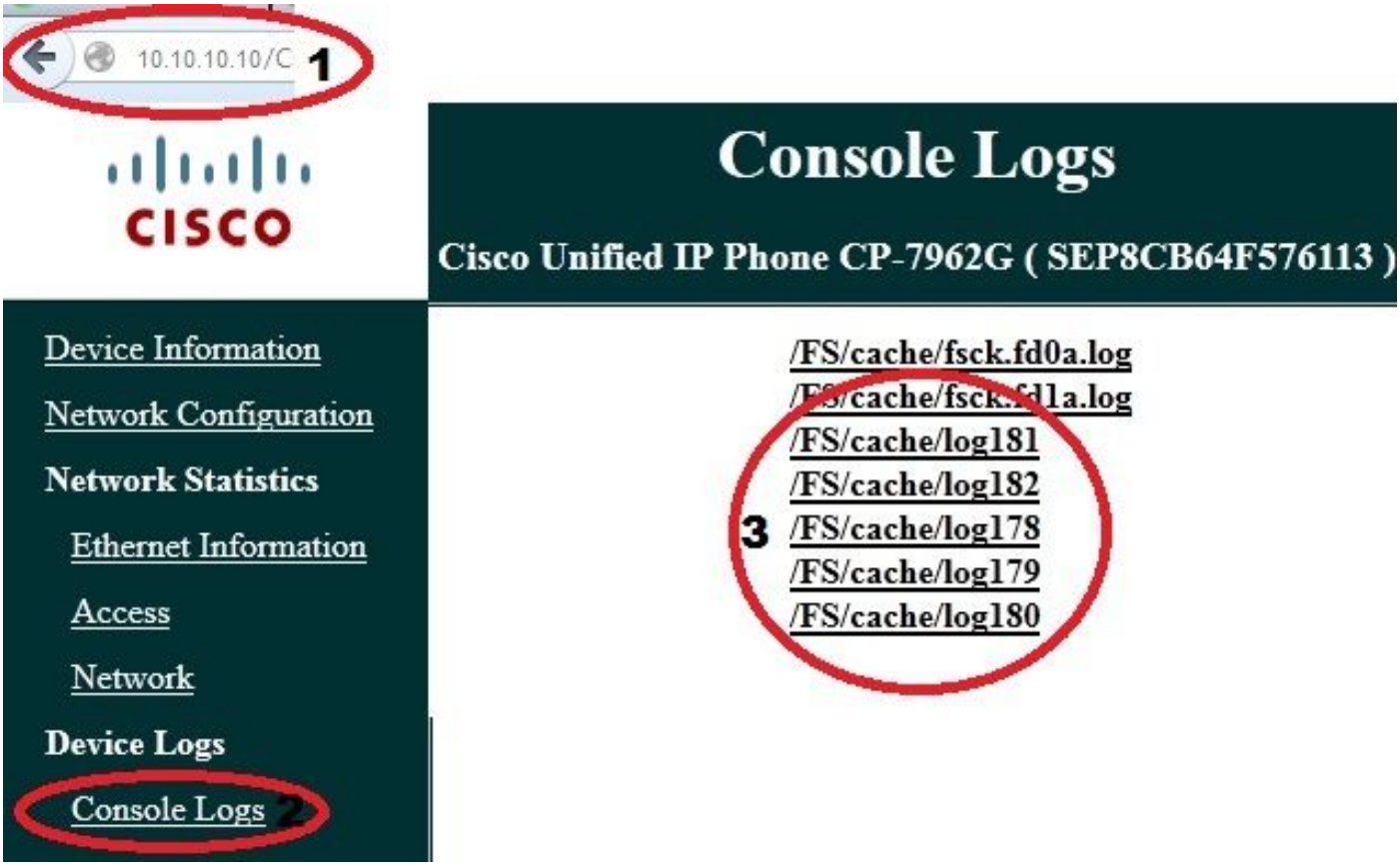
> **注:** AnyConnect ユーザの高負荷との大きい配備では、Cisco は**デバッグ webvpnh anyconnect を**有効に しないことを推奨します。 この出力は IP アドレスで絞り込むことができないため、大量の情報が生成される可能性があります。

IP 電話ログ

電話口グにアクセスするには、Web アクセス機能を有効にします。 CUCM に口グインして、[Device] > [Phone] > [Phone Configuration] に移動します。 この機能を有効にする IP 電話を探して、Web アクセス用のセクションを探します。 IP 電話に設定変更を適用します。



この新しい機能を導入するためにサービスを有効にして電話機をリセットしたら、ブラウザで IP 電話ログにアクセスできます。 そのサブネットへのアクセス権が付与されたコンピュータから電話機の IP アドレスを使用します。 コンソール ログに行き、5 つのログファイルをチェックして下さい。 この 5 つのファイルが電話機によって上書きされるため、すべてのファイルをチェックして必要な情報を探す必要があります。



ASA ログと IP 電話ログの関連付けの問題

次の例は、ASA と IP 電話からのログを関連付ける方法を示しています。 この例では、ASA 上の証明書のハッシュが電話機のコンフィギュレーション ファイル内の証明書のハッシュと一致していません。これは、ASA 上の証明書が別の証明書に置き換えられたためです。

ASA ログ

```
%ASA-7-725012: Device chooses cipher : AES128-SHA for the SSL session with
client outside:172.16.250.9/50091
%ASA-7-725014: SSL lib error. Function: SSL3_READ_BYTES Reason: tlsv1 alert
unknown ca
%ASA-6-725006: Device failed SSL handshake with client outside:172.16.250.9/50091
```

電話ログ

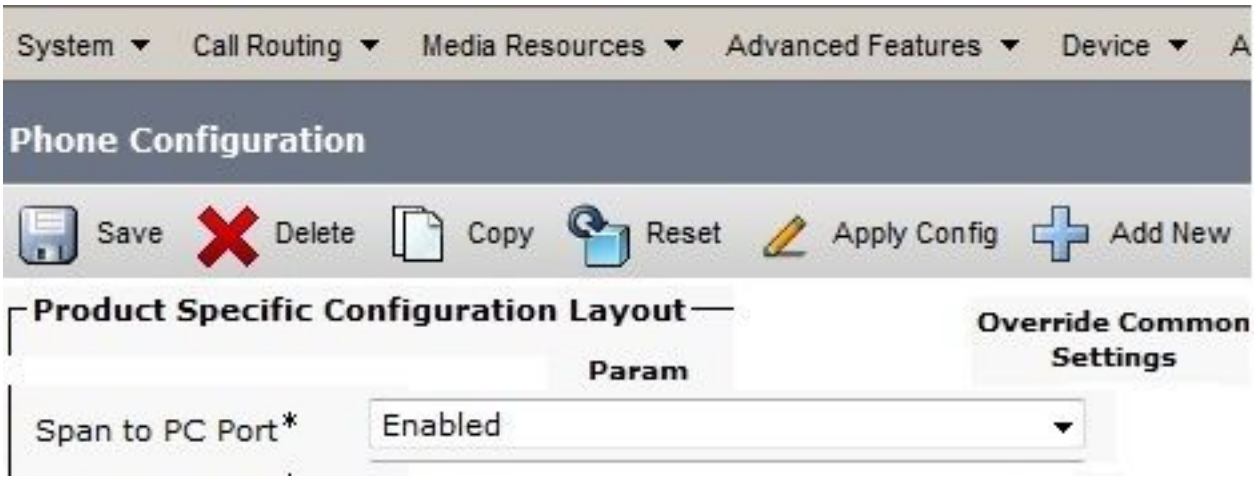
```
 902: NOT 10:19:27.155936 VPNC: ssl_state_cb: TLSv1: SSL_connect: before/connect
initialization
903: NOT 10:19:27.162212 VPNC: ssl_state_cb: TLSv1: SSL_connect: unknown state
904: NOT 10:19:27.361610 VPNC: ssl_state_cb: TLSv1: SSL_connect: SSLv3 read server hello A
905: NOT 10:19:27.364687 VPNC: cert_vfy_cb: depth:1 of 1, subject:
</CN=10.198.16.140/unstructuredName=10.198.16.140>
906: NOT 10:19:27.365344 VPNC: cert_vfy_cb: depth:1 of 1, pre_err: 18 (self signed certificate)
907: NOT 10:19:27.368304 VPNC: cert_vfy_cb: peer cert saved: /tmp/leaf.crt
908: NOT 10:19:27.375718 SECD: Leaf cert hash = 1289B8A7AA9FFD84865E38939F3466A61B5608FC
909: ERR 10:19:27.376752 SECD: EROR:secLoadFile: file not found </tmp/issuer.crt>
910: ERR 10:19:27.377361 SECD: Unable to open file /tmp/issuer.crt
911: ERR 10:19:27.420205 VPNC: VPN cert chain verification failed, issuer certificate not found
and leaf not trusted
912: ERR 10:19:27.421467 VPNC: ssl_state_cb: TLSv1: write: alert: fatal:
unknown CA
913: ERR 10:19:27.422295 VPNC: alert_err: SSL write alert: code 48, unknown CA
914: ERR 10:19:27.423201 VPNC: create_ssl_connection: SSL_connect ret -1 error 1
915: ERR 10:19:27.423820 VPNC: SSL: SSL_connect: SSL_ERROR_SSL (error 1)
916: ERR 10:19:27.424541 VPNC: SSL: SSL_connect: error:14090086:SSL
routines:SSL3_GET_SERVER_CERTIFICATE:certificate verify failed
 917: ERR 10:19:27.425156 VPNC: create_ssl_connection: SSL setup failure
918: ERR 10:19:27.426473 VPNC: do_login: create_ssl_connection failed
919: NOT 10:19:27.427334 VPNC: vpn_stop: de-activating vpn
920: NOT 10:19:27.428156 VPNC: vpn_set_auto: auto -> auto
921: NOT 10:19:27.428653 VPNC: vpn_set_active: activated -> de-activated
922: NOT 10:19:27.429187 VPNC: set_login_state: LOGIN: 1 (TRYING) --> 3 (FAILED)
923: NOT 10:19:27.429716 VPNC: set_login_state: VPNC : 1 (LoggingIn) --> 3
(LoginFailed)
924: NOT 10:19:27.430297 VPNC: vpnc_send_notify: notify type: 1 [LoginFailed]
925: NOT 10:19:27.430812 VPNC: vpnc_send_notify: notify code: 37
[SslAlertSrvrCert]
926: NOT 10:19:27.431331 VPNC: vpnc_send_notify: notify desc: [alert: Unknown
CA (server cert)]
```

```
927: NOT 10:19:27.431841 VPNC: vpnc_send_notify: sending signal 28 w/ value 13 to
pid 14
928: ERR 10:19:27.432467 VPNC: protocol_handler: login failed
```

PC ポート機能へのスパン

コンピュータを電話機に直接接続することができます。 電話機のバックプレーン内にスイッチ ポートがあります。

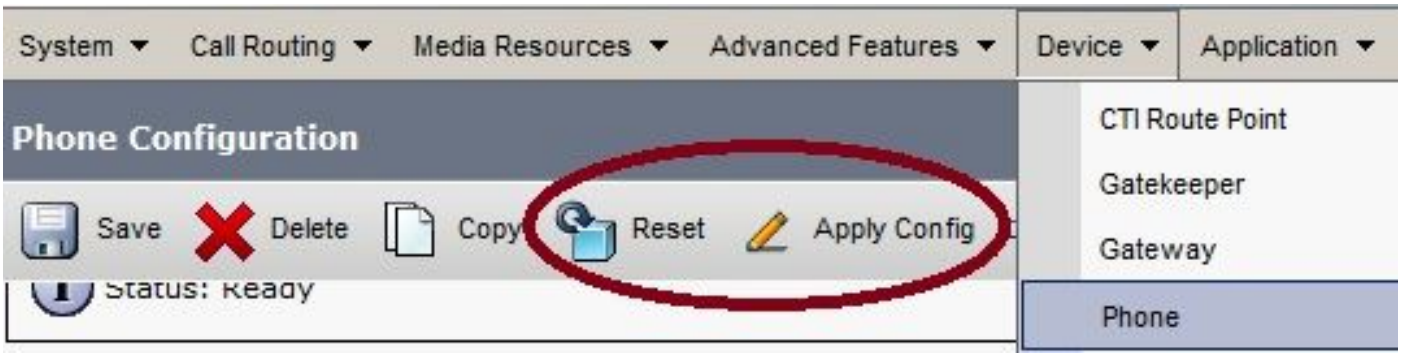
以前行ったように電話機を設定して、CUCM 上の PC ポートへのスパンを有効にし、設定を適用します。 電話機が各フレームのコピーを PC に送信し始めます。 分析のためのトラフィックをキャプチャ するために混合モードで Wireshark を使用して下さい。



VPN 経由で接続された状態での IP 電話設定の変更

IP 電話が AnyConnect 経由でネットワーク外部から接続された状態で、VPN 設定を変更できるかという質問をよく受けます。 答えは「はい」ですが、いくつかの構成設定を確認する必要があります。

CUCM 内で必要な変更を加えてから、その変更を電話機に適用します。 新しい設定を電話機にプッシュするための 3 つのオプション（Apply Config、Reset、Restart）があります。 3 つすべてのオプションが VPN と電話機および ASA 間の接続を解除しますが、証明書認証が使用されている場合は自動的に再接続されます。 認証、許可、およびアカウンティング（AAA）を使用している場合は、クレデンシャルの再入力が要求されます。



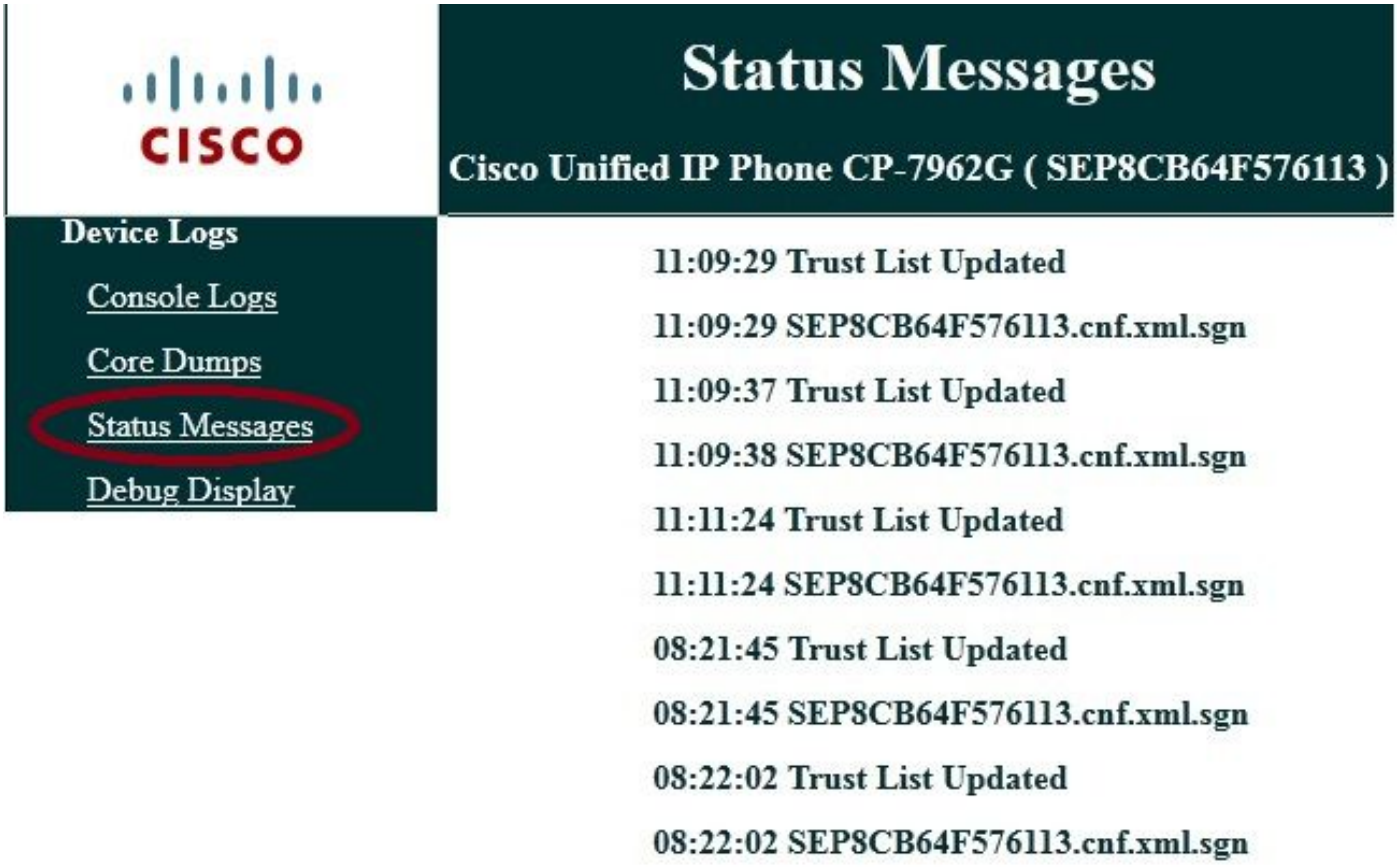
注: IP 電話がリモート側に存在する場合は、外部 DHCP サーバから IP アドレスを受け取るのが一般的です。 IP 電話で CUCM から新しい設定を受信するには、本社の TFTP サーバに接続する必要があります。 通常は、CUCM が TFTP サーバを兼ねています。

更新されたコンフィギュレーション ファイルを受信するには、TFTP サーバの IP アドレスが電話機のネットワーク設定内で正しくセットアップされていることを確認します。 確認のために、DHCP サーバからオプション 150 を使用するか、手動で電話機の TFTP を設定します。 この TFTP サーバには AnyConnect セッション経由でアクセスできます。

IP 電話がローカル DHCP サーバから TFTP サーバを受信しているが、そのアドレスが正しくない場合は、代替 TFTP サーバ オプションを使用して、DHCP サーバから提供される TFTP サーバの IP アドレスを上書きすることができます。 この手順では、代替 TFTP サーバの適用方法を説明します。

1. [Settings] > [Network Configuration] > [IPv4 Configuration] に移動します。
2. [代替 TFTP (Alternate TFTP)] オプションにスクロールします。
3. 電話機で代替 TFTP サーバを使用する場合は、[Yes] ソフトキーを押します。 それ以外の場合は、[No] ソフトキーを押します。 オプションがロックされている場合は、* * # を押してロックを解除します。
4. Save ソフトキーを押します。
5. [TFTP Server 1] オプションで代替 TFTP サーバを適用します。

Web ブラウザまたは電話機メニューで直接ステータス メッセージを確認して、電話機が正しい情報を受信していることを確認します。 通信が正しくセットアップされている場合は、次のようなメッセージが表示されます。



電話機が TFTP サーバから情報を受信できない場合は、TFTP エラー メッセージが表示されます。

ASA SSL 証明書の更新

AnyConnect VPN 電話のセットアップは正しく機能しているが、ASA SSL 証明書の期限が近づいてきた場合に、すべての IP 電話をメイン サイトに移動して、新しい SSL 証明書を電話機に導入する必要はありません。 VPN が接続された状態で、新しい証明書を追加することができます。

ID 証明書の代わりに ASA のルート CA 証明書をエクスポートまたはインポートしてから、更新で同じベンダー (CA) を引き続き使用する場合は、CUCM 内の証明書を変更する必要がありません。これは、証明書を流用できるためです。 ただし、ID 証明書を使用していた場合は、次の手順が必要になります。 そうしないと、ASA と IP 電話間のハッシュ値が一致しないため、接続が電話機で信頼されません。

1. ASA 上の証明書を更新します。
   注: 詳細については、「ASA 8.x： ASDM を使用した SSL 証明書の更新とインストール」を参照してください。 別のトラストポイントを作成して、すべての VPN IP 電話に証明書を適

用するまで、**ssl trustpoint <name> outside** コマンドを使用してこの新しい証明書を適用しないでください。
2. 新しい証明書をエクスポートします。

3. 電話 VPN 信頼証明書として新しい証明書を CUCM にインポートします。
注: 同じ CN の証明書をアップロードする CSCuh19734 **を上書きします電話 VPN 信頼の古い証明書を**理解しておいて下さい
4. CUCM の [VPN Gateway Configuration] に移動して、新しい証明書を適用します。 これで、次の両方の証明書が存在することになります。 期限が迫っている証明書とまだ ASA に適用されていない新しい証明書。

5. この新しい設定を IP 電話に適用します。 [Apply Config] > [Reset] > [Restart] に移動して、VPN トンネル経由で新しい設定変更を IP 電話に導入します。 すべての IP 電話が VPN 経由で接続されており、それらからトンネル経由で TFTP サーバに到達可能なことを確認します。

6. TFTP を使用してステータス メッセージとコンフィギュレーション ファイルをチェックし、IP 電話が更新されたコンフィギュレーション ファイルを受信したことを確認します。

7. ASA で新しい SSL トラストポイントを適用して、古い証明書を置き換えます。

注: ASA SSL 証明書がすでに期限切れで、IP 電話が AnyConnect 経由で接続できない場合は、 変更（新しい ASA 証明書ハッシュなど）を IP 電話にプッシュできます。 手動で IP 電話内の TFTP をパブリック IP アドレスに設定して IP 電話がそこから情報を取得できるようにします。 パブリック TFTP サーバを使用して、コンフィギュレーション ファイルをホストします。 たとえば、ASA 上でポート フォワーディングを作成して、そのトラフィックを内部 TFTP サーバにリダイレクトします。