

AnyConnect機能を使用した電話VPNのCUCMでのASA証明書の更新

内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[VPN Phoneサービスを中断せずにASA証明書を更新する方法](#)

[確認](#)

[関連情報](#)

概要

このドキュメントでは、電話サービスの中断を回避するために、AnyConnect機能を使用したVirtual Private Network(VPN)経由の電話用Cisco Unified Communications Manager(CUCM)の適応型セキュリティアプライアンス(ASA)証明書を更新する正しいプロセスについて説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- AnyConnect機能を備えた電話VPN。
- ASAおよびCUCM証明書。

使用するコンポーネント

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

- Cisco Unified Communications Manager 10.5.2.15900-8.
- Cisco適応型セキュリティアプライアンスソフトウェアバージョン9.8(2)20。
- Cisco IP Phone CP-8841

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ました。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。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

AnyConnectの電話VPN機能を使用すると、VPN接続を介して電話サービスをプロビジョニングで

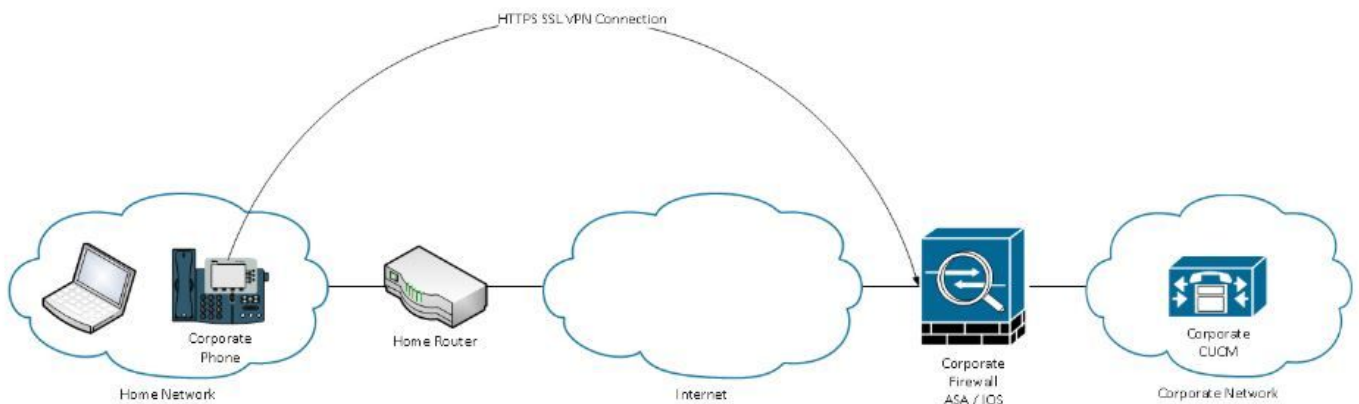
きます。

電話機がVPNに対応する前に、まず内部ネットワークでプロビジョニングする必要があります。これには、CUCM TFTP(Trivial file transfer Protocol)サーバへの直接アクセスが必要です。

ASAが完全に設定された後の最初のステップは、ASA Hypertext Transfer Protocol Secure(HTTPS)証明書を取得し、それをPhone-VPN-trustとしてCUCMサーバにアップロードし、それをCUCMの正しいVPNゲートウェイに割り当りますASA

電話機をネットワークの外部に移動してVPN機能を使用する前に、電話機をネットワーク内でプロビジョニングする必要があります。電話機を内部でプロビジョニングした後、VPNアクセス用に外部ネットワークに移動できます。

電話機は、HTTPSを介してTCPポート443でASAに接続します。ASAは設定済みの証明書で応答し、提示された証明書を確認します。



VPN Phoneサービスを中断せずにASA証明書を更新する方法

たとえば、状況によってはASA証明書を変更する必要があります。

証明書の有効期限が近づいています

証明書はサードパーティによって署名され、認証局(CA)が変更されるなど

AnyConnectを使用してVPN経由でCUCMに接続されている電話機のサービスの中断を回避するには、いくつかの手順を実行します。

注意：手順に従わない場合は、電話機を外部ネットワークに導入する前に、内部ネットワークにプロビジョニングし直す必要があります。

ステップ1：新しいASA証明書を生成しますが、まだインターフェイスに適用しないでください。

証明書は、自己署名またはCA署名付きです。

注：ASA証明書の詳細については、『[デジタル証明書の設定](#)』を参照してください

ステップ2：その証明書をCUCMパブリッシャの電話VPN信頼としてCUCMにアップロードします。

Call Managerにログインし、[Unified OS Administration] > [Security] > [Certificate Management] > [Upload Certificate] > [Select Phone-VPN-trust]に移動します。

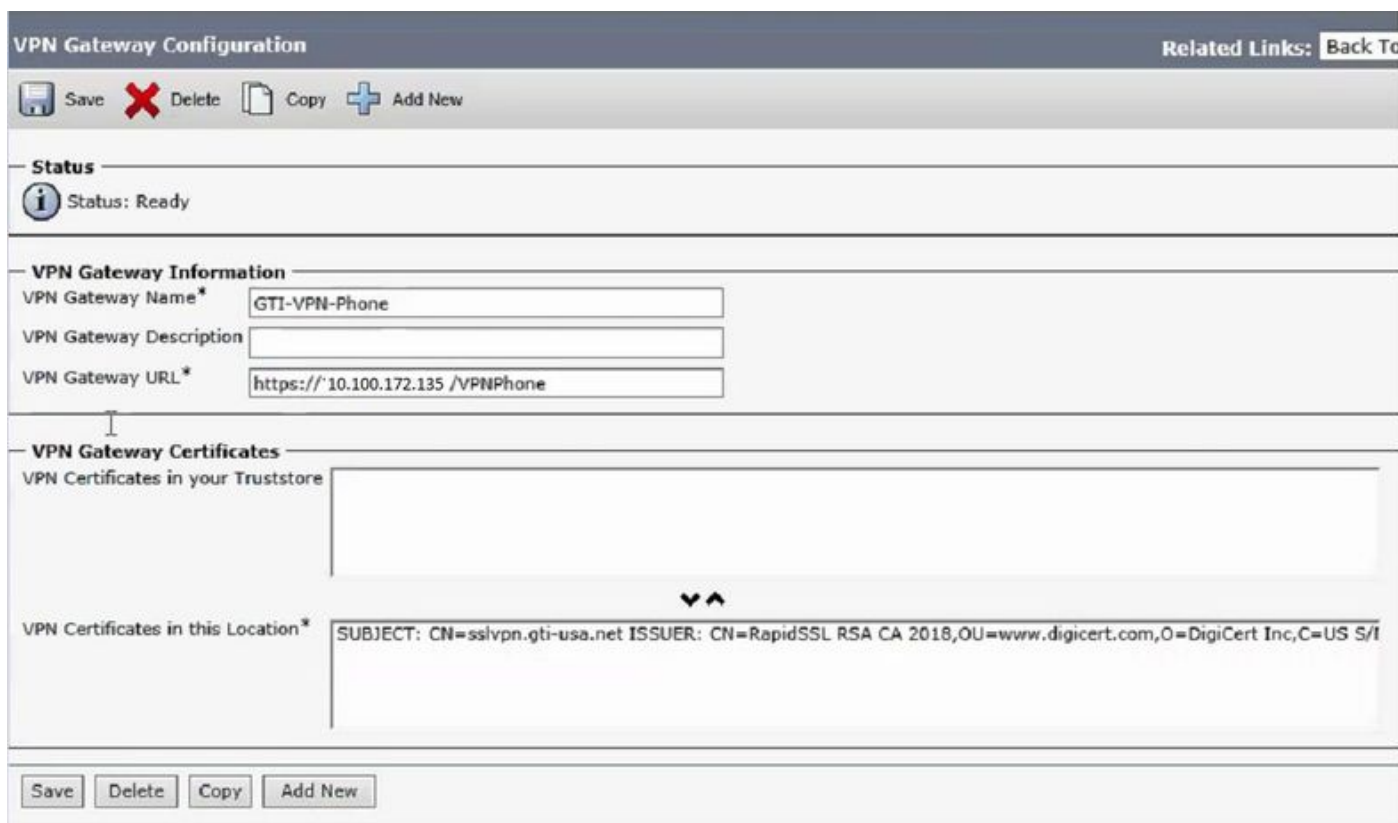
推奨事項として、完全な証明書チェーンをアップロードします。ルート証明書と中間証明書がすでにCUCMにアップロードされている場合は、次の手順に進みます。

注意：古いID証明書と新しいID証明書が同じCN（共通名）である場合は、バグ [CSCuh19734の回避策に従って、新しい証明書によって古いIDが上書きされないようにします。](#)このようにして、新しい証明書は電話VPNゲートウェイ設定用のデータベースに存在しますが、古い証明書は上書きされません。

ステップ3:VPNゲートウェイで、両方の証明書（古い証明書と新しい証明書）を選択します。

[Cisco Unified CM Administration] > [Advanced Features] > [VPN] > [VPN Gateway]に移動します。

[Location]フィールドの[VPN Certificates]に両方の証明書があることを確認します。



The screenshot displays the 'VPN Gateway Configuration' interface. At the top, there are navigation icons for Save, Delete, Copy, and Add New. The 'Status' section shows 'Status: Ready'. The 'VPN Gateway Information' section contains the following fields:

- VPN Gateway Name*: GTI-VPN-Phone
- VPN Gateway Description: (empty)
- VPN Gateway URL*: https://10.100.172.135 /VPNPhone

The 'VPN Gateway Certificates' section is divided into two parts:

- VPN Certificates in your Truststore: (empty)
- VPN Certificates in this Location*: SUBJECT: CN=sslvpn.gti-usa.net ISSUER: CN=RapidSSL RSA CA 2018,OU=www.digicert.com,O=DigiCert Inc,C=US S/I

At the bottom, there are buttons for Save, Delete, Copy, and Add New.

ステップ4:VPNグループ、プロファイル、および共通の電話プロファイルが正しく設定されていることを確認します。

ステップ5：電話機をリセットします。

この手順により、電話機は新しい設定値をダウンロードでき、電話機に両方の証明書ハッシュが確実に設定されるため、古い証明書と新しい証明書を信頼できます。

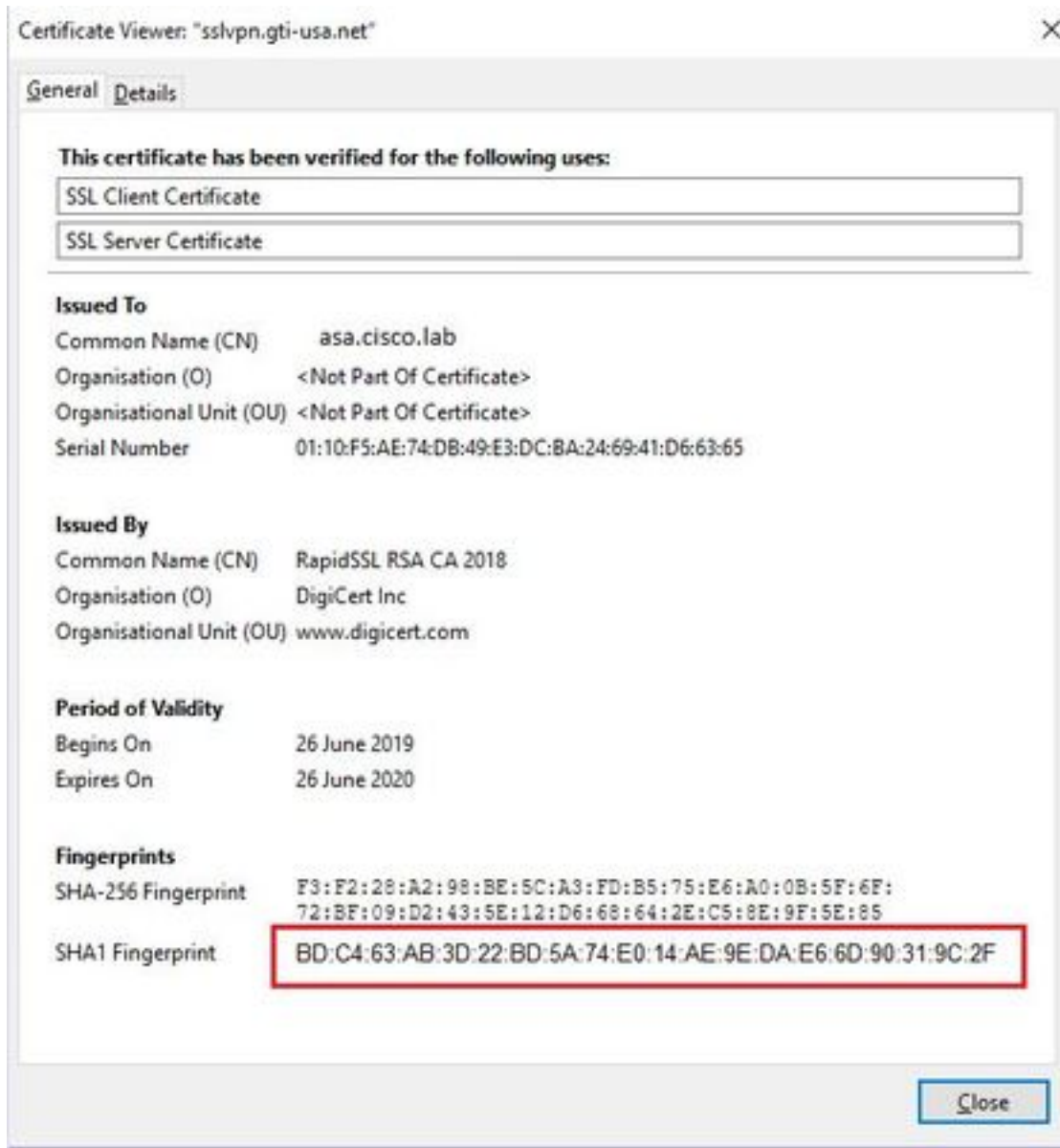
ステップ6:ASAインターフェイスに新しい証明書を適用します。

証明書がASAインターフェイスに適用されると、電話機はその新しい証明書を信頼する必要があります。これは、前の手順で両方の証明書ハッシュが存在するためです。

確認

このセクションでは、手順が正しく実行されていることを確認します。

ステップ1：古いASA証明書と新しいASA証明書を開き、SHA-1フィンガープリントをメモします。



ステップ2:VPN経由で接続する電話機を選択し、その設定ファイルを収集します。

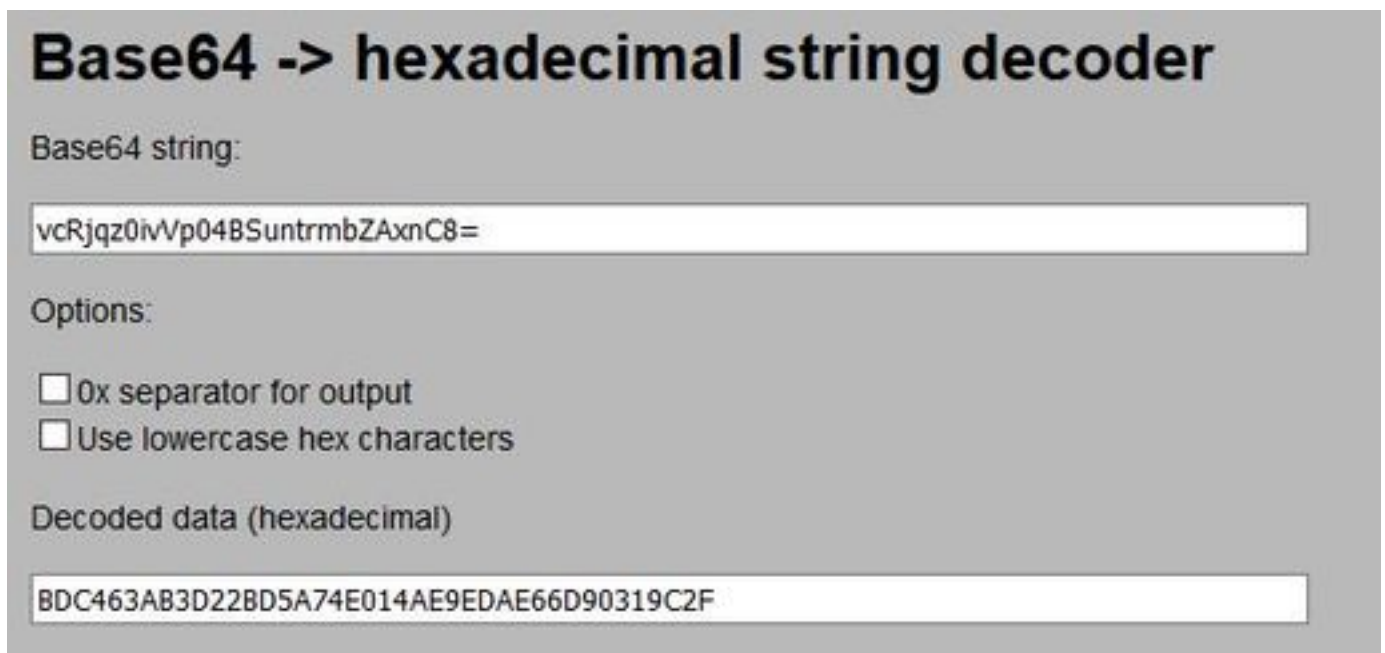
注：電話機設定ファイルの収集方法の詳細については、『[CUCMから電話機の設定ファイルを取得する2つの方法](#)』を参照してください

ステップ3：設定ファイルが作成されたら、次のセクションを探します。

```
<vpnGroup>
<mtu>1290</mtu>
<failConnectTime>30</failConnectTime>
<authMethod>2</authMethod>
<pswdPersistent>0</pswdPersistent>
<autoNetDetect>1</autoNetDetect>
<enableHostIDCheck>0</enableHostIDCheck>
<addresses>
<url1> https://radc.cgsinc.com/Cisco_VOIP_VPN</url1>;
</addresses>
<credentials>
<hashAlg>0</hashAlg>

</credentials>
</vpnGroup>
```

ステップ4：設定ファイルのハッシュはBase 64形式で印刷され、ASA証明書のハッシュは16進形式で印刷されるため、Base 64からHexadecimalへのデコーダを使用して、両方のハッシュ（電話とASA）が一致することを確認できます。



Base64 -> hexadecimal string decoder

Base64 string:

vcRjqz0ivVp04BSuntrmbZAxnC8=

Options:

0x separator for output

Use lowercase hex characters

Decoded data (hexadecimal)

BDC463AB3D22BD5A74E014AE9EDAE66D90319C2F

関連情報

AnyConnect VPN Phone機能の詳細については、次を参照してください。

- ASA 上の証明書認証を使用した AnyConnect VPN 電話の設定.

<https://www.cisco.com/c/en/us/support/docs/unified-communications/unified-communications-manager-callmanager/115785-anyconnect-vpn-00.html>