

# 為具有AnyConnect功能的電話VPN更新CUCM上的ASA證書

## 目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[背景資訊](#)

[如何在不中斷VPN電話服務的情況下更新ASA證書？](#)

[驗證](#)

[相關資訊](#)

## 簡介

本文檔介紹使用AnyConnect功能更新思科統一通訊管理器(CUCM)上適用於虛擬專用網路(VPN)電話的自適應安全裝置(ASA)證書以避免電話服務中斷的正確過程。

## 必要條件

### 需求

思科建議您瞭解以下主題：

- 具有AnyConnect功能的電話VPN。
- ASA和CUCM證書。

### 採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 思科整合通訊管理員10.5.21590010-8。
- 思科調適型安全裝置軟體版本9.8(2)20。
- Cisco IP電話CP-8841。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

## 背景資訊

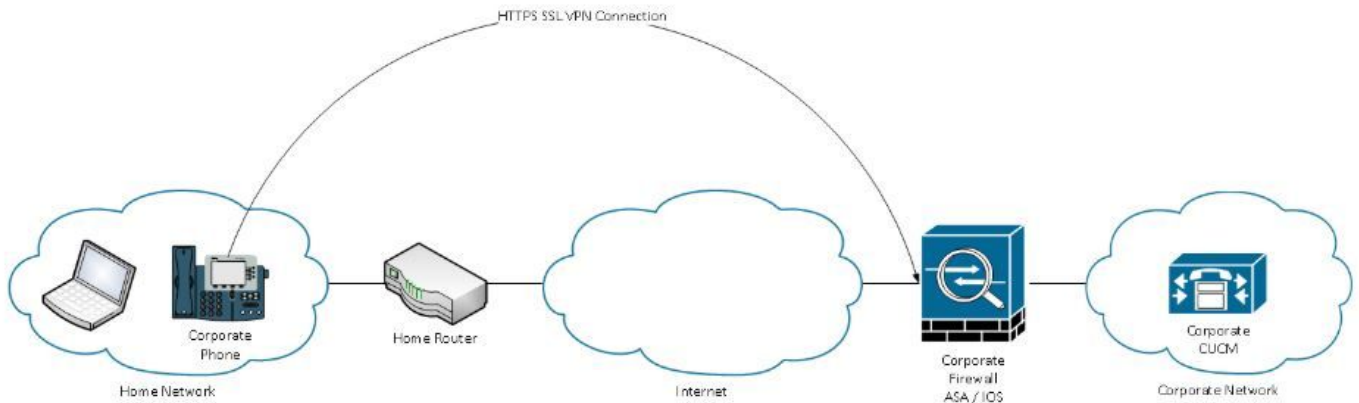
AnyConnect的電話VPN功能允許通過VPN連線提供電話服務。

在電話準備好用於VPN之前，必須先在內部網路中調配電話。這需要直接訪問CUCM TFTP（簡單檔案傳輸協定）伺服器。

ASA完全配置後的第一步是獲取ASA超文本傳輸協定安全(HTTPS)證書並將其以Phone-VPN-trust形式上傳到CUCM伺服器，然後將其分配到CUCM中的正確VPN網關。這允許CUCM伺服器構建一個IP電話配置檔案，告知電話如何到達ASA。

必須將電話調配到網路內部，然後才能將其移動到網路外部並使用VPN功能。在內部調配電話後，可將其移至外部網路以進行VPN訪問。

電話通過HTTPS在TCP埠443上連線到ASA。ASA使用配置的證書進行響應，並驗證提供的證書。



## 如何在不中斷VPN電話服務的情況下更新ASA證書？

有時，ASA證書需要更改，例如由於任何情況。

證書即將過期

證書由第三方簽署，證書頒發機構(CA)發生更改等

為了避免通過VPN與AnyConnect連線到CUCM的電話的服務中斷，需要遵循一些步驟。

**注意：**如果不遵循這些步驟，則需要再次在內部網路上調配電話，然後才能在外部網路上部署電話。

步驟1.生成新的ASA證書，但不要將其應用到介面。

證書可以是自簽名或CA簽名。

**附註：**有關ASA證書的詳細資訊，請參閱[配置數位證書](#)

步驟2.在CUCM發佈伺服器上將該證書作為電話VPN信任上傳到CUCM。

登入到Call Manager並導航到**Unified OS Administration > Security > Certificate Management > Upload Certificate > Select Phone-VPN-trust**。

作為建議，上傳完整的證書鏈，如果已在CUCM上上傳根證書和中間證書，請轉至下一步。

**注意：**請記住，如果舊身份憑證和新身份憑證具有相同的CN（一般名稱），則您需要依照錯

誤CSCuh19734的解決方法操作，以避免新憑證覆寫舊身份憑證。這樣，新證書就存在於電話VPN網關配置的資料庫中，但舊證書不會被覆蓋。

步驟3.在VPN網關上，選擇兩個證書（舊證書和新證書）。

導航至Cisco Unified CM管理>高級功能>VPN > VPN網關。

確保您在VPN Certificates in this Location欄位中有兩個證書。

The screenshot displays the 'VPN Gateway Configuration' page. At the top right, there is a 'Related Links: Back To' link. Below the title bar, there are icons for 'Save', 'Delete', 'Copy', and 'Add New'. The 'Status' section shows 'Status: Ready'. The 'VPN Gateway Information' section contains three input fields: 'VPN Gateway Name\*' with the value 'GTI-VPN-Phone', 'VPN Gateway Description' (empty), and 'VPN Gateway URL\*' with the value 'https://10.100.172.135 /VPNPhone'. The 'VPN Gateway Certificates' section has two sub-sections: 'VPN Certificates in your Truststore' (empty) and 'VPN Certificates in this Location\*' containing a certificate entry: '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'.

步驟4.檢查VPN組、配置檔案和公共電話配置檔案是否設定正確。

步驟5.重置電話。

此步驟允許電話下載新的配置設定，並確保電話具有證書雜湊，以便他們能夠信任舊證書和新證書。

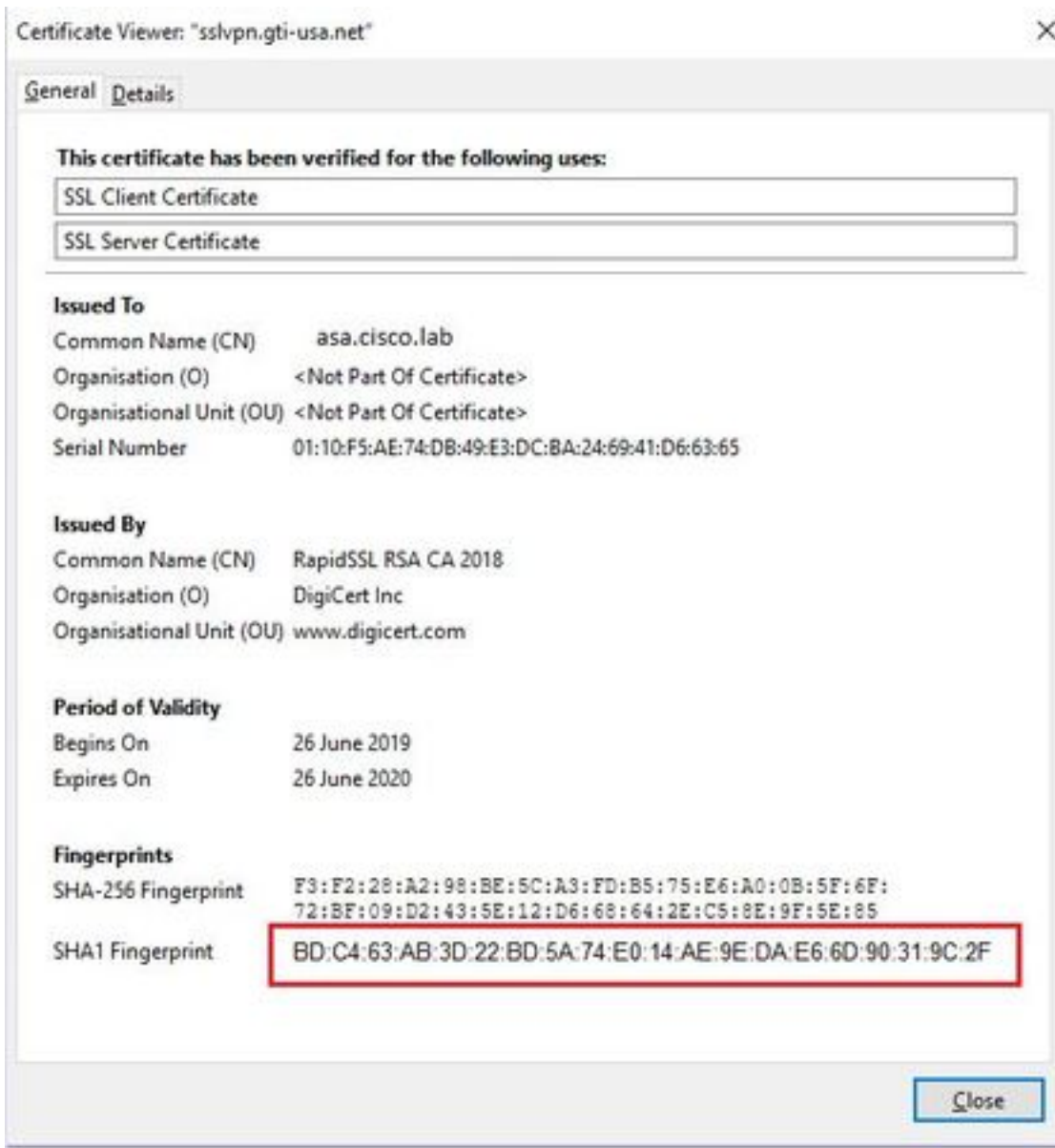
步驟6.在ASA介面上應用新證書。

在ASA介面上應用證書後，電話應該信任該新證書，因為它們具有上一步中兩個證書雜湊。

## 驗證

使用本節內容，確認您已正確執行步驟。

步驟1.開啟舊的和新的ASA證書並記下SHA-1指紋。



步驟2.選擇應通過VPN連線的電話並收集其配置檔案。

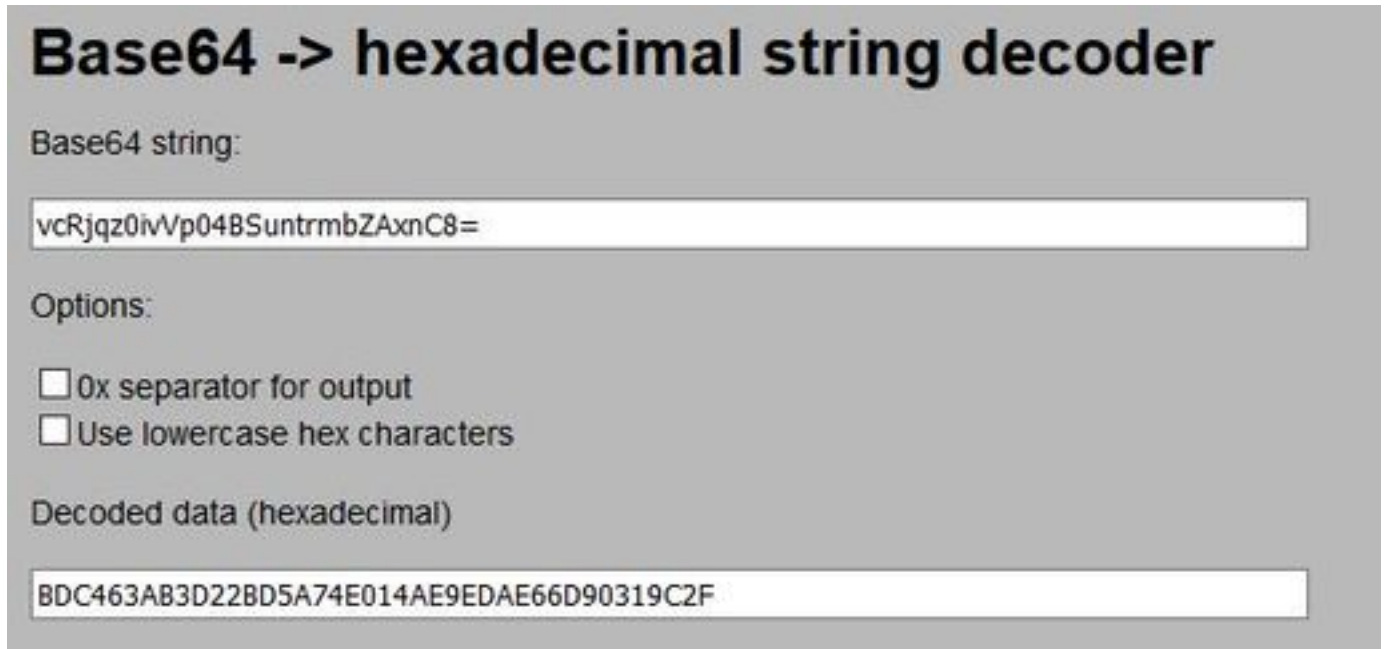
附註：有關如何收集電話配置檔案的詳細資訊，請參閱[從CUCM獲取電話配置檔案的兩種方法](#)

步驟3.獲得配置檔案後，請查詢以下部分：

```
<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>
```

步驟4. 配置檔案中的雜湊以Base 64格式列印，ASA證書以十六進位制格式列印，因此您可以使用從Base 64到十六進位制的解碼器來驗證雜湊（電話和ASA）是否匹配。



**Base64 -> hexadecimal string decoder**

Base64 string:

vcRjqz0ivVp04BSuntrmbZAxnC8=

Options:

0x separator for output

Use lowercase hex characters

Decoded data (hexadecimal)

BDC463A83D22BD5A74E014AE9EDAE66D90319C2F

## 相關資訊

有關AnyConnect VPN電話功能的詳細資訊：

- 在ASA上配置帶有證書身份驗證的AnyConnect VPN電話。

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