在思科語音作業系統(VOS)中通過CLI配置CA簽名的證書

目錄

簡介

本文說明如何使用指令行介面(CLI)將第三方憑證授權單位(CA)簽署的憑證上傳到任何以思科語音作業系統(VOS)為主的協同合作伺服器上的組態步驟。

必要條件

需求

思科建議您瞭解以下主題：

- 基本瞭解公鑰基礎架構(PKI)及其在Cisco VOS伺服器和Microsoft CA上的實施
- DNS基礎設施已預先配置

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- VOS伺服器：思科整合通訊管理員(CUCM)版本9.1.2
- CA:Windows 2012伺服器
- 客戶端瀏覽器：Mozilla Firefox版本47.0.1

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。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

背景資訊

在所有Cisco Unified Communications VOS產品中，至少有兩種憑證型別：應用程式(ccmadmin、ccmservice、cuadmin、cfadmin、cuic)和VOS平台(cmplatform、drf、cli)。

在某些特定情況下，通過網頁管理應用程式以及通過命令列執行與平台相關的活動非常方便。下面您可以找到有關如何僅通過CLI導$^{\text{入第}}$三方簽名證書的程式。在此範例中，Tomcat憑證已上傳。對於CallManager或任何其他應用程式，它看起來相同。

生成CA簽名證書

命令摘要

文章中所用命令的清單。

```
show cert list own
show cert own tomcat

set csr gen CallManager
show csr list own
show csr own CallManager

show cert list trust
set cert import trust CallManager
set cert import own CallManager CallManager-trust/allevich-DC12-CA.pem
```

檢查正確的證書資訊

列出所有上傳的受信任證書。

```
admin:show cert list own

tomcat/tomcat.pem: Self-signed certificate generated by system
ipsec/ipsec.pem: Self-signed certificate generated by system
CallManager/CallManager.pem: Certificate Signed by allevich-DC12-CA
CAPF/CAPF.pem: Self-signed certificate generated by system
TVS/TVS.pem: Self-signed certificate generated by system
```

檢查誰頒發了Tomcat服務的證書。

```
admin:show cert own tomcat

[
  Version: V3
  Serial Number: 85997832470554521102366324519859436690
  SignatureAlgorithm: SHA1withRSA (1.2.840.113549.1.1.5)
  Issuer Name: L=Krakow, ST=Malopolskie, CN=ucm1-1.allevich.local, OU=TAC, O=Cisco, C=PL
  Validity From: Sun Jul 31 11:37:17 CEST 2016
           To:   Fri Jul 30 11:37:16 CEST 2021
  Subject Name: L=Krakow, ST=Malopolskie, CN=ucm1-1.allevich.local, OU=TAC, O=Cisco, C=PL
  Key: RSA (1.2.840.113549.1.1.1)
    Key value: 3082010a0282010100a2
<output omited>
```

這是自簽名證書，因為頒發者匹配主題。

生成證書簽名請求(CSR)

產生CSR。

```
admin:set csr gen tomcat
Successfully Generated CSR  for tomcat
```

驗證已成功生成證書簽名請求。

```
admin:show csr list own
tomcat/tomcat.csr
```

開啟它並將內容複製到文本檔案。將其另存為**tac_tomcat.csr**文件。

```
admin:show csr own tomcat
```

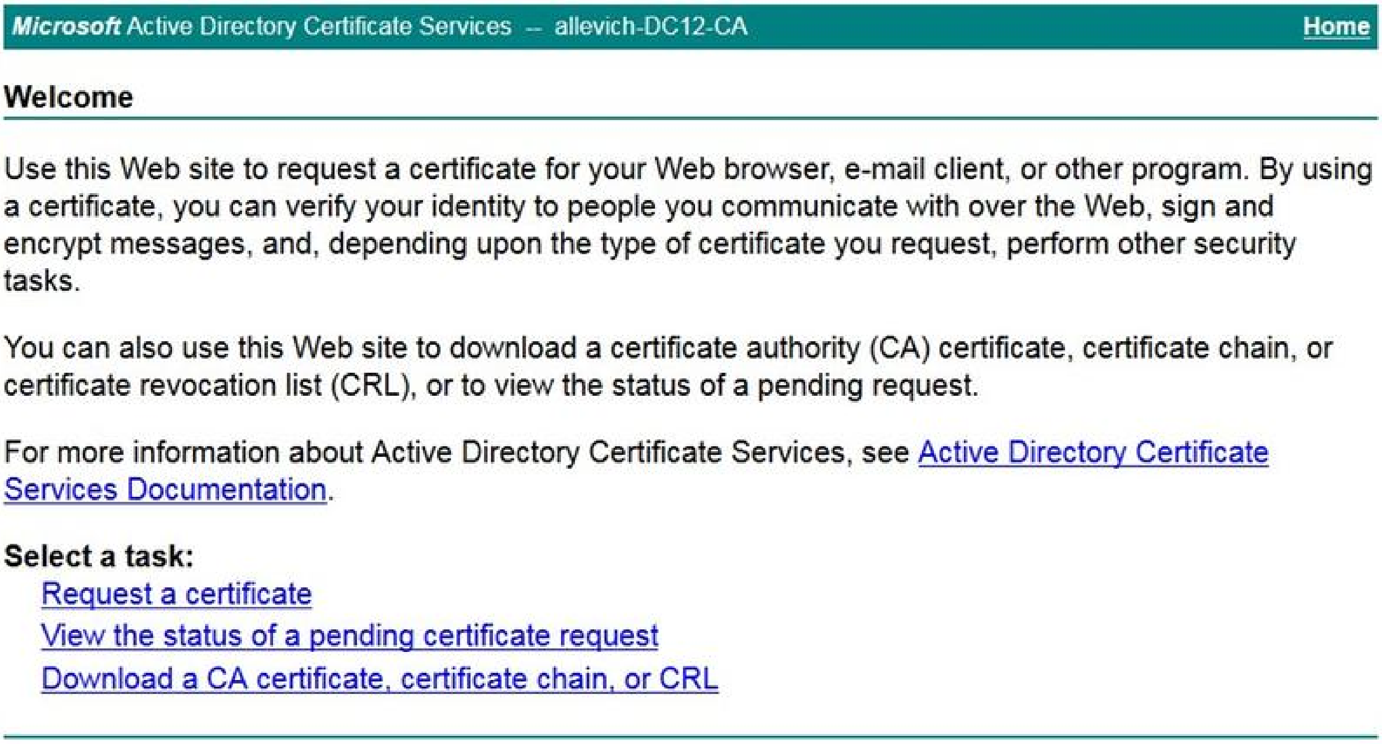
```
-----BEGIN CERTIFICATE REQUEST-----
MIIDSjCCAjICAQAwgb0xCzAJBgNVBAYTAlBMMRQwEgYDVQQIEwtNYWxvcG9sc2tp
ZTEPMA0GA1UEBxMGS3Jha293MQ4wDAYDVQQKEwVDaXNjbzEMMAoGA1UECxMDVEFD
MR4wHAYDVQQDExV1Y20xLTEuYWxsZXZpY2gubG9jYWwxSTBHBgNVBAUTQDlhMWJk
NDA5M2VjOGYxNjljODhmNGUyZTYwZTYzM2RjNjlhZmFkNDY1YTgzMDhkNjRhNGU1
MzExOGQ0YjZkZjcwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCVo5jh
lMqTUnYbHQUnYPt00PTflWbj7hi6PSYI7pVCbGUZBpIZ5PKwTD56OZ8SgpjYX5Pf
l9D09H2gtQJTMVv1Gm1eGdlJsbuABRKn6lWkO6b706MiGSgqel+41vnItjn3Y3kU
7h51nruJye3HpPQzvXXpOKJ/JeJc8InEvQcC/UQmFMKn0ulO0veFBHnG7TLDwDaQ
W1Al1rwrezN9Lwn2a/XZQR1P65sjmnkFFF2/FON4BmooeiiNJD0G+F4bKig1ymlR
84faF27plwHjcw8WAn2HwJT6O7TaE6EOJd0sgLU+HFAI3txKycS0NvLuMZYQH81s
/C74CIRWibEWT2qLAgMBAAGgRzBFBgkqhkiG9w0BCQ4xODA2MCcGA1UdJQQgMB4G
CCsGAQUFBwMBBggrBgEFBQcDAgYIKwYBBQUHAwUwCwYDVR0PBAQDAgO4MA0GCSqG
SIb3DQEBBQUAA4IBAQBUu1FhKuyQ1X58A6+7KPkYsWtioS0PoycltuQsVo0aav82
PiJkCvzWTeEo6v9qG0nnaI53e15+RPpWxpEgAIPPhtt6asDuW30SqSx4eClfgmKH
ak/tTuWmZbfyk2iqNFy0YgYTeBkG3AqPwWUCNoduPZ0/fo41QoJPwjE184U64WXB
gCzhIHfsV5DzYp3IR5C13hEa5fDgpD2ubQWja2LId85NGHEiqyiWqwmt07pTkBc+
7ZKa6fKnpACehrtVqEn02jOi+sanfQKGQqH8VYMFsW2uYFj9pf/Wn4aDGuJoqdOH
StV2Eh0afxPEq/1rQP3/rzq4NMYlJ7glyNFGPUVP
-----END CERTIFICATE REQUEST-----
```

生成Tomcat伺服器證書

為CA上的Tomcat服務生成證書。

在瀏覽器中開啟證書頒發機構的網頁。在身份驗證提示中輸入正確的憑據。

http://dc12.allevich.local/certsrv/



Microsoft Active Directory Certificate Services -- allevich-DC12-CA　　Home

Welcome

Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks.

You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request.

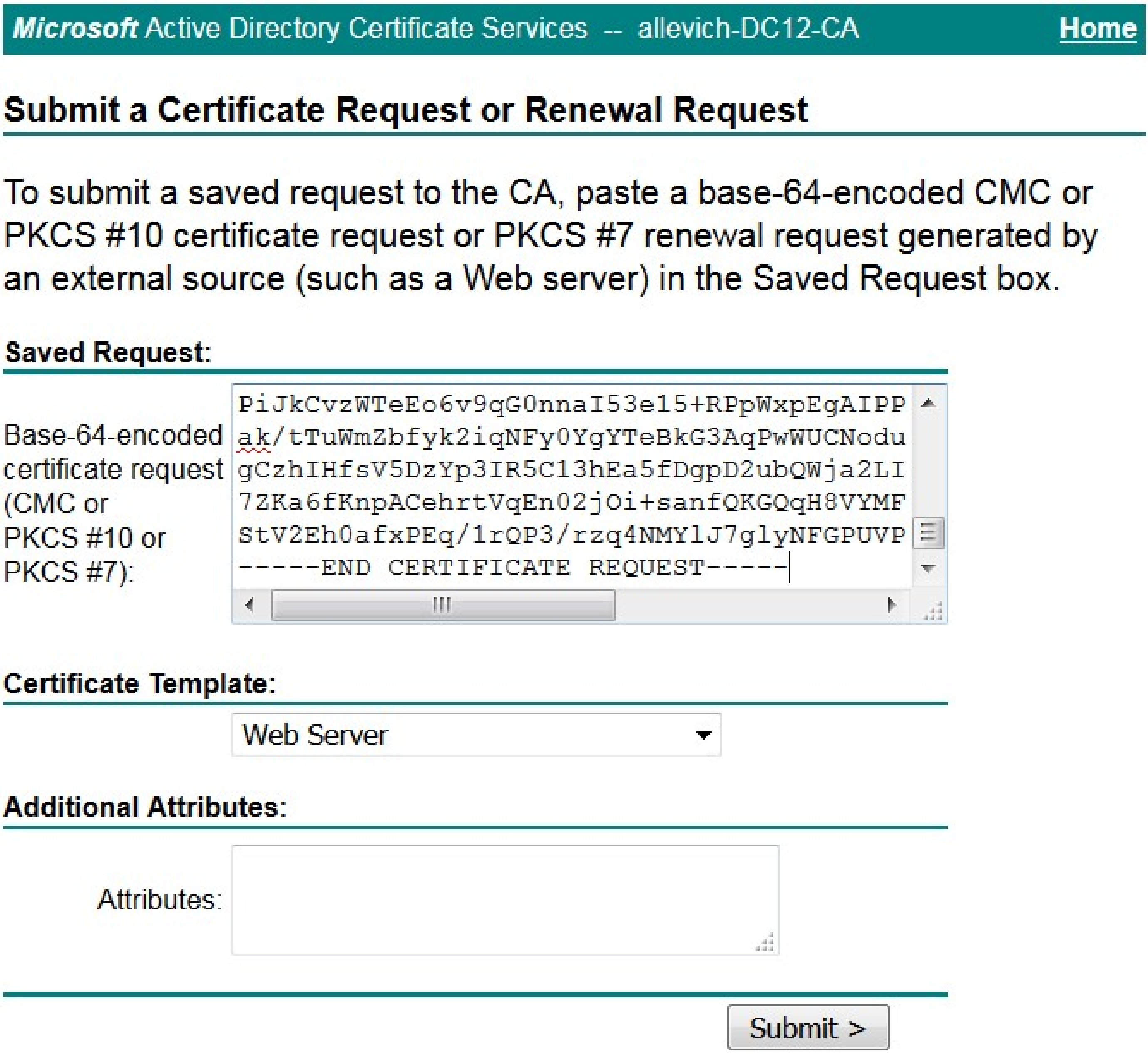
For more information about Active Directory Certificate Services, see Active Directory Certificate Services Documentation.

Select a task:

Request a certificate
View the status of a pending certificate request
Download a CA certificate, certificate chain, or CRL

下載CA根證書。選擇**Download a CA certificate， certificate chain， or CRL**選單。在下一個選單中，從清單中選擇適當的CA。編碼方法應為**Base 64**。請下載CA證書並將其儲存到名為**ca.cer**的作業系統。

按**Request a Certificate**，然後按**Advanced Certificate Request**。將**Certificate Template**設定為Web伺服器，並從文字檔案**tac_tomcat.csr**中貼上CSR內容，如下所示。



Microsoft Active Directory Certificate Services -- allevich-DC12-CA

Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CMC or PKCS #10 certificate request or PKCS #7 renewal request generated by an external source (such as a Web server) in the Saved Request box.

Saved Request:

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):

PiJkCvzWTeEo6v9qG0nnaI53e15+RPpWxpEgAIPP
ak/tTuWmZbfyk2iqNFy0YgYTeBkG3AqPwWUCNodu
gCzhIHfsV5DzYp3IR5C13hEa5fDgpD2ubQWja2LI
7ZKa6fKnpACehrtVqEn02jOi+sanfQKGQqH8VYMF
StV2Eh0afxPEq/1rQP3/rzq4NMYlJ7glyNFGPUVP
-----END CERTIFICATE REQUEST-----

Certificate Template:

Web Server

Additional Attributes:

Attributes:

提示：如果操作在實驗室中完成（或Cisco VOS伺服器且CA位於同一管理域中），則節省從記憶體緩衝區複製並貼上CSR的時間。

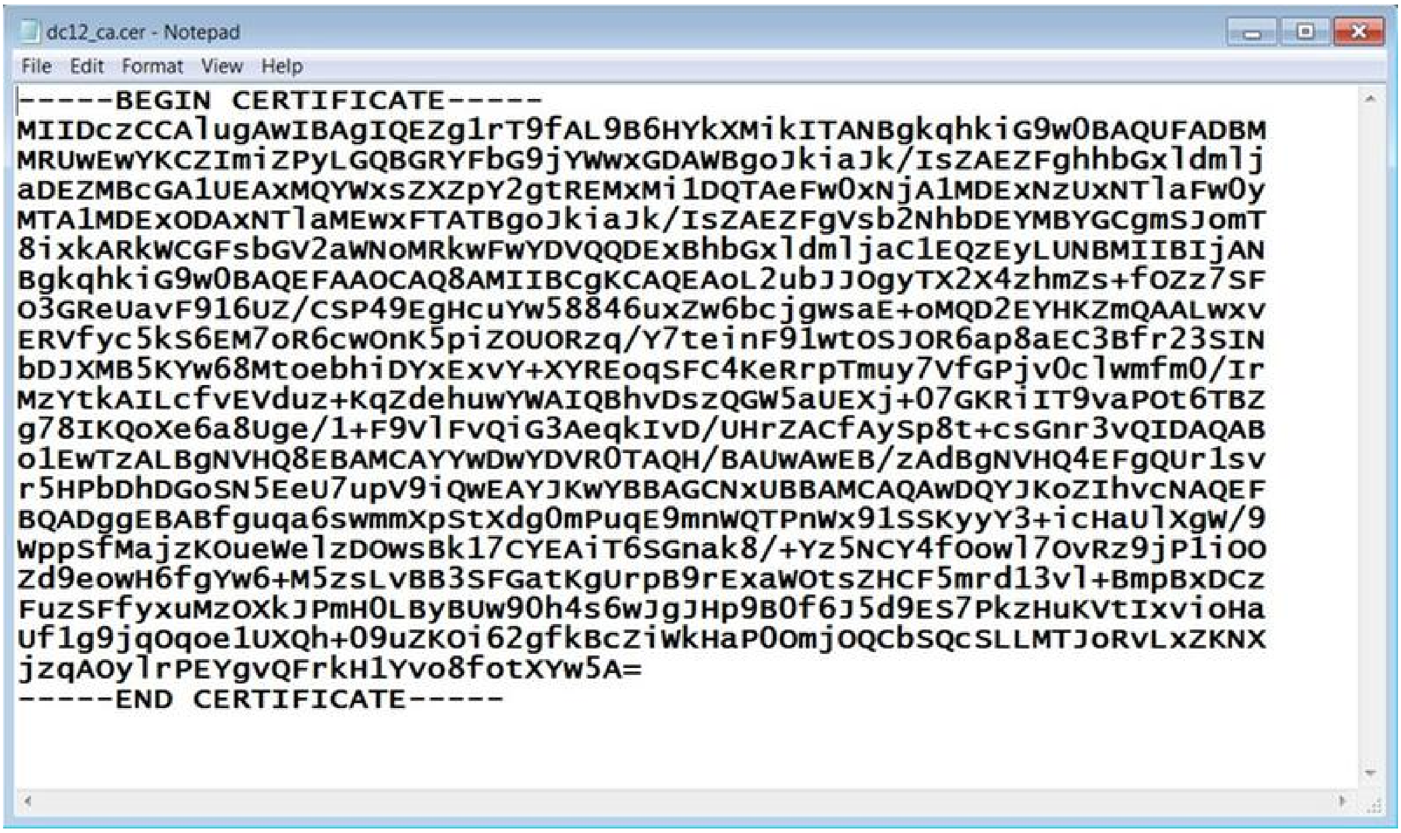
按**提交**。選擇**Base 64 encoded**選項並下載Tomcat服務的證書。

附註：如果大量執行憑證產生，請確保將憑證名稱變更為有意義的名稱。

將Tomcat證書匯入Cisco VOS伺服器

匯入CA證書

開啟使用名稱**ca.cer**儲存的CA證書。必須先匯入。



```
-----BEGIN CERTIFICATE-----
MIIDczCCAlugAwIBAgIQEZg1rT9fAL9B6HYkXMikITANBgkqhkiG9w0BAQUFADBM
MRUwEwYKCZImiZPyLGQBGRYFbG9jYWwxGDAWBgoJkiaJk/IsZAEZFghhbGxldmlj
aDEZMBcGA1UEAxMQYWxsZXZpY2gtREMxMi1DQTAeFw0xNjA1MDExNzUxNTlaFw0y
MTA1MDExODAxNTlaMEwxFTATBgoJkiaJk/IsZAEZFgVsb2NhbDEYMBYGCgmSJomT
8ixkARkWCGFsbGV2aWNoMRkwFwYDVQQDExBhbGxldmljaC1EQzEyLUNBMIIBIjAN
BgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAoL2ubJJOgyTX2X4zhmZs+fOZz7SF
O3GReUavF916UZ/CSP49EgHcuYw58846uxZw6bcjgwsaE+oMQD2EYHKZmQAALwxv
ERVfyc5kS6EM7oR6cwOnK5piZOUORzq/Y7teinF91wtOSJOR6ap8aEC3Bfr23SIN
bDJXMB5KYw68MtoebhiDYxExvY+XYREoqSFC4KeRrpTmuy7VfGPjv0clwmfm0/Ir
MzYtkAILcfvEVduz+KqZdehuwYWAIQBhvDszQGW5aUEXj+07GKRiIT9vaPOt6TBZ
g78IKQoXe6a8Uge/1+F9VlFvQiG3AeqkIvD/UHrZACfAySp8t+csGnr3vQIDAQAB
o1EwTzALBgNVHQ8EBAMCAYYwDwYDVR0TAQH/BAUwAwEB/zAdBgNVHQ4EFgQUr1sv
r5HPbDhDGoSN5EeU7upV9iQwEAYJKwYBBAGCNxUBBAMCAQAwDQYJKoZIhvcNAQEF
BQADggEBABfguqa6swmmXpStXdg0mPuqE9mnWQTPnWx91SSKyyY3+icHaUlXgW/9
WppSfMajzKOueWelzDOwsBk17CYEAiT6SGnak8/+Yz5NCY4fOowl7OvRz9jP1iOO
Zd9eowH6fgYw6+M5zsLvBB3SFGatKgUrpB9rExaWOtsZHCF5mrd13vl+BmpBxDCz
FuzSFfyxuMzOXkJPmH0LByBUw90h4s6wJgJHp9B0f6J5d9ES7PkzHuKVtIxvioHa
Uf1g9jqOqoe1UXQh+09uZKOi62gfkBcZiWkHaP0OmjOQCbSQcSLLMTJoRvLxZKNX
jzqAOylrPEYgvQFrkH1Yvo8fotXYw5A=
-----END CERTIFICATE-----
```

將其內容複製到緩衝區，然後在CUCM CLI中鍵入以下命令：

```
admin:set cert import trust tomcat
```

```
Paste the Certificate and Hit Enter
```

將會顯示貼上CA證書的提示。如下圖所示。

```
-----BEGIN CERTIFICATE-----
MIIDczCCAlugAwIBAgIQEZg1rT9fAL9B6HYkXMikITANBgkqhkiG9w0BAQUFADBM
MRUwEwYKCZImiZPyLGQBGRYFbG9jYWwxGDAWBgoJkiaJk/IsZAEZFghhbGxldmlj
aDEZMBcGA1UEAxMQYWxsZXZpY2gtREMxMi1DQTAeFw0xNjA1MDExNzUxNTlaFw0y
MTA1MDExODAxNTlaMEwxFTATBgoJkiaJk/IsZAEZFgVsb2NhbDEYMBYGCgmSJomT
8ixkARkWCGFsbGV2aWNoMRkwFwYDVQQDExBhbGxldmljaC1EQzEyLUNBMIIBIjAN
BgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAoL2ubJJOgyTX2X4zhmZs+fOZz7SF
O3GReUavF916UZ/CSP49EgHcuYw58846uxZw6bcjgwsaE+oMQD2EYHKZmQAALwxv
ERVfyc5kS6EM7oR6cwOnK5piZOUORzq/Y7teinF91wtOSJOR6ap8aEC3Bfr23SIN
bDJXMB5KYw68MtoebhiDYxExvY+XYREoqSFC4KeRrpTmuy7VfGPjv0clwmfm0/Ir
MzYtkAILcfvEVduz+KqZdehuwYWAIQBhvDszQGW5aUEXj+07GKRiIT9vaPOt6TBZ
g78IKQoXe6a8Uge/1+F9VlFvQiG3AeqkIvD/UHrZACfAySp8t+csGnr3vQIDAQAB
o1EwTzALBgNVHQ8EBAMCAYYwDwYDVR0TAQH/BAUwAwEB/zAdBgNVHQ4EFgQUr1sv
r5HPbDhDGoSN5EeU7upV9iQwEAYJKwYBBAGCNxUBBAMCAQAwDQYJKoZIhvcNAQEF
BQADggEBABfguqa6swmmXpStXdg0mPuqE9mnWQTPnWx91SSKyyY3+icHaUlXgW/9
WppSfMajzKOueWelzDOwsBk17CYEAiT6SGnak8/+Yz5NCY4fOowl7OvRz9jP1iOO
Zd9eowH6fgYw6+M5zsLvBB3SFGatKgUrpB9rExaWOtsZHCF5mrd13vl+BmpBxDCz
FuzSFfyxuMzOXkJPmH0LByBUw90h4s6wJgJHp9B0f6J5d9ES7PkzHuKVtIxvioHa
Uf1g9jqOqoe1UXQh+09uZKOi62gfkBcZiWkHaP0OmjOQCbSQcSLLMTJoRvLxZKNX
jzqAOylrPEYgvQFrkH1Yvo8fotXYw5A=
-----END CERTIFICATE-----
```

如果信任證書上傳成功，將顯示此輸出。

```
Import of trust certificate is successful
```

驗證CA憑證是否成功匯入為Tomcat-trust憑證。

```
admin:show cert list trust

tomcat-trust/ucm1-1.pem: Trust Certificate
tomcat-trust/allevich-win-CA.pem: w2008r2 139
<output omited for brevity>
```

匯入Tomcat證書

下一步是匯入Tomcat CA簽名的證書。該操作與tomcat-trust cert的操作看起來相同，只是命令不同。

```
set cert import own tomcat tomcat-trust/allevich-DC12-CA.pem
```

重新啟動服務

最後重新啟動Tomcat服務。

```
utils service restart Cisco Tomcat
```

> **注意**：請記住，它會干擾Web伺服器相關服務（如分機移動、未接呼叫、公司目錄等）的操作。

驗證

驗證生成的證書。

```
admin:show cert own tomcat

[
  Version: V3
  Serial Number: 2765292404730765620225406600715421425487314965
  SignatureAlgorithm: SHA1withRSA (1.2.840.113549.1.1.5)
  Issuer Name: CN=allevich-DC12-CA, DC=allevich, DC=local
  Validity From: Sun Jul 31 12:17:46 CEST 2016
           To:   Tue Jul 31 12:17:46 CEST 2018
  Subject Name: CN=ucm1-1.allevich.local, OU=TAC, O=Cisco, L=Krakow, ST=Malopolskie, C=PL
  Key: RSA (1.2.840.113549.1.1.1)
    Key value: 3082010a028201010095a
```

確保頒發者名稱屬於構造該證書的CA。

通過在瀏覽器中鍵入伺服器的FQDN來登入網頁，不會顯示證書警告。

疑難排解

本文的目的是給出一個包含命令語法的過程，說明如何通過CLI上傳證書，而不是突出公鑰基礎設施(PKI)的邏輯。 它不包括SAN證書、從屬CA、4096證書金鑰長度以及許多其他方案。

在某些極少數情況下，通過CLI上傳Web伺服器證書時，操作失敗，顯示錯誤消息「無法讀取CA證書」。解決方法是使用網頁安裝證書。

非標準證書頒發機構配置可能導致證書安裝問題。嘗試使用基本預設組態從另一個CA產生和安裝憑

證。

退出計畫

如果需要生成自簽名證書，也可以在CLI中完成。

鍵入下面的命令，Tomcat證書將重新生成為自簽名證書。

```
admin:set cert regen tomcat

WARNING: This operation will overwrite any CA signed certificate previously imported for  tomcat

Proceed with regeneration (yes|no)? yes
Successfully Regenerated Certificate for tomcat.

You must restart services related to tomcat for the regenerated certificates to become active.
```

要應用新證書，必須重新啟動Tomcat服務。

```
admin:utils service restart Cisco Tomcat

 Don't press Ctrl-c while the service is getting RESTARTED.If Service has not Restarted
Properly, execute the same Command Again

Service Manager is running
Cisco Tomcat[STOPPING]
Cisco Tomcat[STOPPING]
Commanded Out of Service
Cisco Tomcat[NOTRUNNING]
Service Manager is running
Cisco Tomcat[STARTING]
Cisco Tomcat[STARTING]
Cisco Tomcat[STARTED]
```

相關文章

通過網頁上傳證書

獲取和上傳Windows Server自簽名或證書頒發機構(CA)的過程......