CA-ondertekend certificaat via CLI configureren in Cisco Voice Operating System (VOS)

Inhoud

[Inleiding](#)
[Voorwaarden](#)
[Vereisten](#)
[Gebruikte componenten](#)
[Achtergrondinformatie](#)
[CA-ondertekend certificaat genereren](#)
[Samenvatting van opdrachten](#)
[certificaatinformatie controleren](#)
[certificaataanvraag genereren (CSR)](#)
[Generate Tomkservercertificaat](#)
[Tomatuurcertificaat importeren naar de Cisco VOS-server](#)
[CA-certificaat importeren](#)
[Tomkaaimatum-certificaat importeren](#)
[Start de service opnieuw](#)
[Verifiëren](#)
[Problemen oplossen](#)
[Terug plan](#)
[Verwante artikelen](#)

Inleiding

Dit document beschrijft de configuratiestappen in de manier waarop u het certificaat van derden (CA) wilt uploaden, dat is ondertekend op een Cisco Voice Operating System (VOS) gebaseerde collaboration-server door het gebruik van de opdrachtregel interface (CLI).

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Basisbegrip van PKI-infrastructuur (Public Key Infrastructure) en de implementatie ervan op Cisco VOS-servers en Microsoft CA
- DNS-infrastructuur is vooraf ingesteld

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- VOS-server: Cisco Unified Communications Manager (CUCM) versie 9.1.2
- VK: Windows 2012-server
- Clientbrowser: Mozilla Firefox versie 4.7.0.1

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Achtergrondinformatie

In alle Cisco Unified Communications VOS-producten zijn er ten minste twee aanmeldingstypen: toepassing zoals (cmadmin, compservice, cuadmin, cfadmin, cuic) en VOS-platform (compplatform, drf, cli).

In sommige specifieke scenario's is het zeer handig toepassingen te beheren via de webpagina en perrongerelateerde activiteiten uit te voeren via de opdrachtregel. Hieronder vindt u een procedure voor het importeren van door 3e partijen ondertekend certificaat alleen via CLI. In dit voorbeeld wordt het Tomcat-certificaat geüpload. Voor CallManager of een andere toepassing ziet het er hetzelfde uit.

CA-ondertekend certificaat genereren

Samenvatting van opdrachten

Een lijst met de opdrachten in het artikel.

```
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
```

certificaatinformatie controleren

Lijst van alle geüploade vertrouwde certificaten.

```
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
```

Controleer wie het certificaat voor de Tomcat-dienst heeft afgegeven.

```
admin:show cert own tomcat

[
  Version: V3
  Serial Number: 859978324705545211023663245198594366 90
  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>
```

Dit is een zelfgetekend certificaat, aangezien de uitgevende instelling met het onderwerp overeenkomt.

certificaataanvraag genereren (CSR)

CSR genereren.

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

Controleer dat het certificaataanvraag succesvol is gegenereerd.

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

Open de tekst en kopieer de inhoud naar het tekstbestand. Sla het op als **tac_tomcat.csr**-bestand.

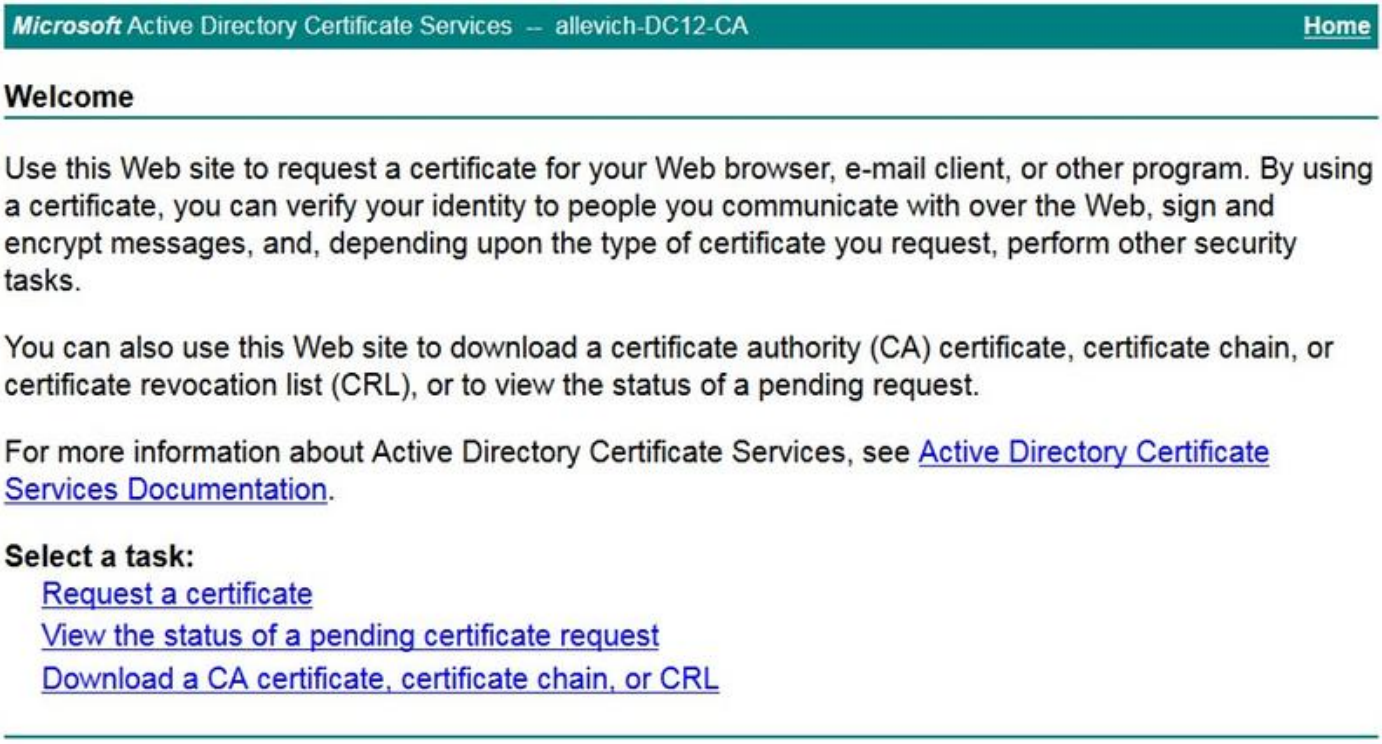
```
admin:show csr own tomcat

-----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-----
```

Generate Tomkservercertificaat

genereren een certificaat voor Tomcat-dienst op de CA.

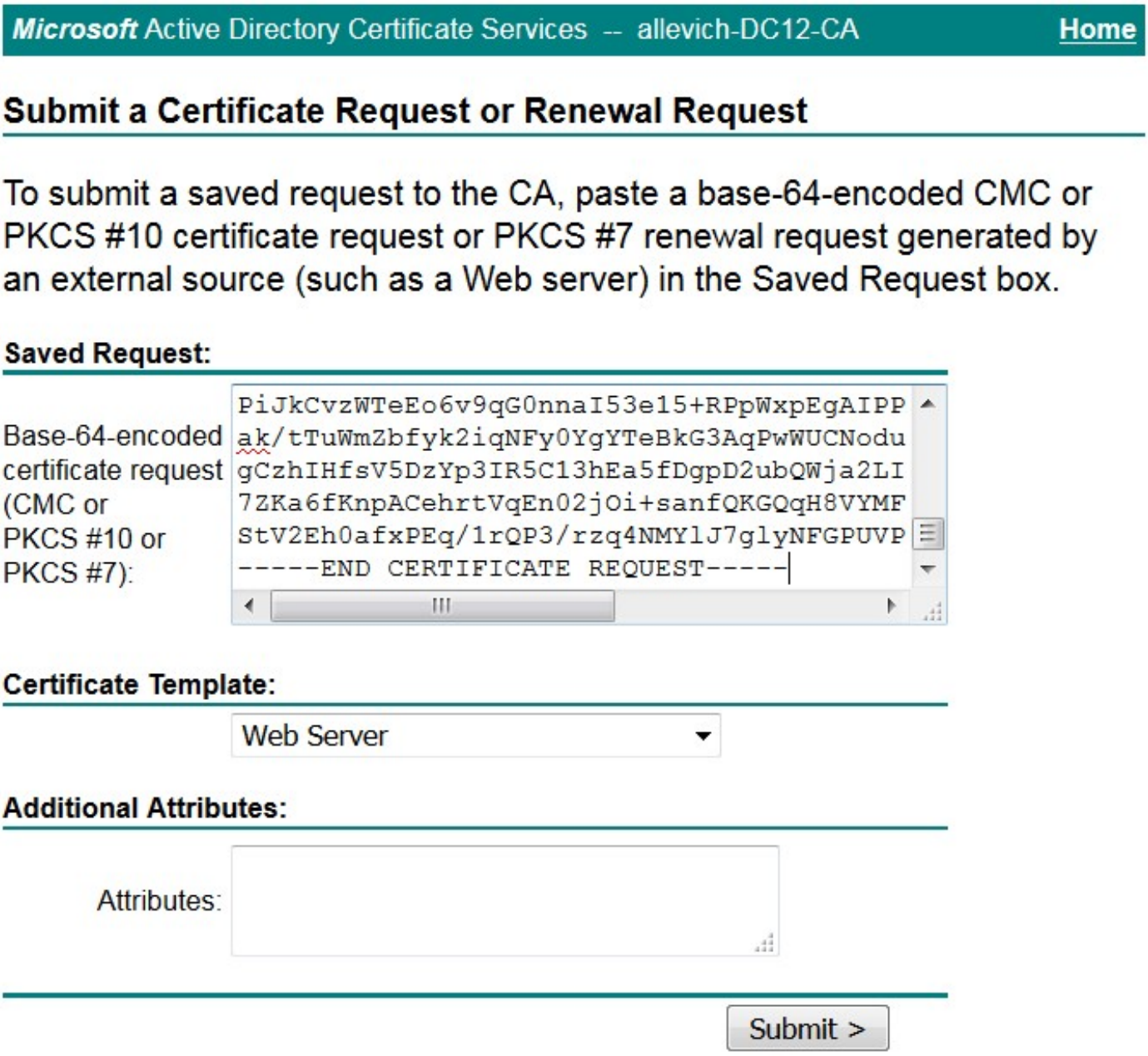
Open de webpagina voor de certificaatinstantie in een browser. Zet de juiste geloofsbrieven in de authenticatie.

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



Download het CA root certificaat. Selecteer **Een CA-certificaat, certificeringsketen of CRL-**menu **downloaden**. Kies in het volgende menu de juiste CA in de lijst. De coderingsmethode zou **Base64** moeten zijn. Download het CA-certificaat en bewaar het op het besturingssysteem met naam **ca.cer**.

Druk op **Aanvragen van een certificaat** en vervolgens op **geavanceerde certificaataanvraag**. Stel **certificaatsjabloon** in op webserver en plak de CSR-inhoud uit het tekstbestand **tac_tomcat.csr** zoals aangegeven.



Tip: Als de bewerking in het lab (of Cisco VOS server en de CA is onder hetzelfde beheerdomein) wordt uitgevoerd om tijdkopie op te slaan en de CSR vanaf de geheugenbuffer te plakken.

Druk op **Inzenden**. Selecteer **Base64 gecodeerde** optie en download het certificaat voor de Tomcat-service.

Opmerking: Indien de certificatenproductie in bulk wordt uitgevoerd, zorg er dan voor dat een naam van het certificaat wordt gewijzigd in een betekenisvolle naam.

Tomatuurcertificaat importeren naar de Cisco VOS-server

CA-certificaat importeren

Open het CA-certificaat dat was opgeslagen met een naam **ca.cer**. Het moet eerst worden

geïmporteerd.

Kopieert de inhoud naar de buffer en type de volgende opdracht in de CUCM CLI:

```
admin:set cert import trust tomcat

Paste the Certificate and Hit Enter
```

Het CA-certificaat wordt automatisch geplakt. Plakt het filter zoals hieronder aangegeven.

```
-----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-----
```

Als het uploaden van een trust certificaat succesvol is, wordt deze uitvoer weergegeven.

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

Controleer dat het CA-certificaat is ingevoerd als Tomcat-trust.

```
admin:show cert list trust

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

Tomkaaimatum-certificaat importeren

De volgende stap is het importeren van een door Tomcat ondertekend certificaat. De operatie ziet er hetzelfde uit als bij een trustkaart van een tomcat-trust, alleen de opdracht is anders.

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

Start de service opnieuw

En tenslotte start Tomcat opnieuw.

```
utils service restart Cisco Tomcat
```

> **Voorzichtig:** Houd in gedachten dat het de werking van web server-afhankelijke services verstoort, zoals Extension Mobility, gemiste oproepen, Corporate Directory en de andere.

Verifiëren

Controleer het certificaat dat is gegenereerd.

```
admin:show cert own tomcat

[
  Version: V3
  Serial Number: 276529240473076562022540660071542142548731496 5
  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
```

Zorg ervoor dat de naam van de emittent behoort tot de CA die het certificaat heeft opgesteld.

Aanmelden bij de webpagina door FQDN van de server in een browser te typen en er wordt geen certificaatwaarschuwing weergegeven.

Problemen oplossen

Het doel van dit artikel is om een procedure met syntax van commando's te geven over de manier waarop het certificaat via CLI moet worden geüpload, niet om de logica van de PKI-infrastructuur

(Public Key Infrastructuur) te benadrukken. Het heeft geen betrekking op SAN-certificaten, subordinair CA, de lengte van de 94096-certificaatsleutel en vele andere scenario's.

In een paar zeldzame gevallen wanneer een webservercertificaat via de CLI wordt geüpload, heeft de bewerking een foutbericht "Kan CA-certificaat niet lezen". Hiervoor is het mogelijk het certificaat te installeren via de webpagina.

Een niet-standaard configuratie van de certificaatinstantie kan leiden tot het probleem met de installatie van het certificaat. Probeer het certificaat van een andere CA met een standaardconfiguratie te produceren en te installeren.

Terug plan

Mocht er een vereiste zijn om een zelf ondertekend certificaat te genereren, dan kan dit ook in de CLI gebeuren.

Typ de onderstaande opdracht en het Tomcat-certificaat wordt aan de zelfgetekende teruggegeven.

```
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.
```

Om een nieuw certificaat toe te passen, moet de Tomcat-dienst opnieuw worden gestart.

```
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]
```

Verwante artikelen

Uploadcertificaat via webpagina

Procedure om Windows Server zelfgetekend of certificeringsinstantie (CA) te verkrijgen en te uploaden.