

CA-ondertekend certificaat voor CVP-server voor HTTPS Web Access

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Configureren](#)

[Referentielijst opdracht](#)

[Back-up maken](#)

[CSR genereren](#)

[Lijst van de certificaten](#)

[Verwijder het bestaande OAMP-certificaat](#)

[Key Pair genereren](#)

[Nieuwe CSR genereren](#)

[Het certificaat afgeven op de CA](#)

[Importeren CA-gegenereerd certificaat](#)

[Verifiëren](#)

[Problemen oplossen](#)

[Gerelateerde informatie](#)

Inleiding

Dit document beschrijft hoe u certificaten (CA) kunt configureren en controleren die u hebt ondertekend op de Cisco Voice Portal (CVP) server en Management Portal (OAMP).

Voorwaarden

De op Microsoft Windows gebaseerde certificaatsserver van de Autoriteit is al vooraf ingesteld.

Vereisten

Cisco raadt u aan kennis te hebben van de PKI-infrastructuur.

Gebruikte componenten

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

CVP versie 11.0

Windows 2012 R2-server

Windows 2012 R2-certificeringsinstantie

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.

Configureren

Referentielijst opdracht

```
more c:\Cisco\CVP\conf\security.properties
cd c:\Cisco\CVP\conf\security
```

```
%kt% -list
%kt% -list | findstr Priv
%kt% -list -v -alias oamp_certificate
```

```
%kt% -genkeypair -alias oamp_certificate -v -keysize 2048 -keyalg RSA
%kt% -import -v -trustcacerts -alias oamp_certificate -file oamp.p7b
```

Back-up maken

Blader naar de map `c:\Cisco\CVP\conf\security` en archiveer alle bestanden. Als OAMP webtoegang niet werkt, vervangt u nieuwe bestanden door de back-up.

CSR genereren

Controleer uw veiligheidswachtwoord.

```
more c:\Cisco\CVP\conf\security.properties
Security.keystorePW = fc]@2zfe*Ufe2J,.0uM$ff
```

Blader naar `c:\Cisco\CVP\conf\security`.

```
cd c:\Cisco\CVP\conf\security
```

Opmerking: In dit artikel wordt de 'Windows-omgevingsvariabele' gebruikt om opdrachten voor Keytool veel korter en leesbaarder te maken. Zorg ervoor dat de variabele wordt geïnitieerd voordat een opdracht voor het sleutelgereedschap wordt toegevoegd.

1. Maak een tijdelijke variabele.

```
set kt=c:\Cisco\CVP\jre\bin\keytool.exe -storepass fc]@2zfe*Ufe2J,.0uM$ff -storetype JCEKS -
keystore .keystore
```

Typ de opdracht om er zeker van te zijn dat de variabele wordt geïnitieerd. Voer het juiste wachtwoord in.

```
echo %kt%
```

```
c:\Cisco\CVP\jre\bin\keytool.exe -storepass fc]@2zfe*Ufe2J,.0uM$ff -storetype JCEKS -keystore .keystore
```

Lijst van de certificaten

Lijst met geïnstalleerde certificaten in het toetsenbord.

```
%kt% -list
```

Tip: Als u de lijst wilt verfijnen, kunt u de opdracht wijzigen om alleen zelf ondertekende certificaten weer te geven.

```
%kt% -list | findstr Priv
```

```
vxml_certificate, May 27, 2016, PrivateKeyEntry, oamp_certificate, May 27, 2016, PrivateKeyEntry, wsm_certificate, May 27, 2016, PrivateKeyEntry, callserver_certificate, May 27, 2016, PrivateKeyEntry,
```

Controleer de zelf ondertekende OAMP-certificeringsinformatie.

```
%kt% -printcert -file oamp.crt
```

```
Owner: CN=CVP11, OU=TAC, O=Cisco, L=Krakow, ST=Malopolskie, C=PL Issuer: CN=CVP11, OU=TAC, O=Cisco, L=Krakow, ST=Malopolskie, C=PL Serial number: 3f44f086 Valid from: Fri May 27 08:13:38 CEST 2016 until: Mon May 25 08:13:38 CEST 2026 Certificate fingerprints: MD5: 58:F5:D3:18:46:FE:9A:8C:14:EA:73:0F:5F:12:E7:43 SHA1: 51:7F:E7:FF:25:B6:B8:02:CD:18:84:E7:50:9E:F2:ED:B1:9E:78:40 Signature algorithm name: SHA1withRSA Version: 3
```

Verwijder het bestaande OAMP-certificaat

Om een nieuw zeer belangrijk paar te genereren, verwijdert u het certificaat dat reeds bestaat.

```
%kt% -delete -alias oamp_certificate
```

Key Pair genereren

Start deze opdracht om een nieuw sleutelpaar te genereren voor het alias met de geselecteerde sleutel.

```
%kt% -genkeypair -alias oamp_certificate -v -keysize 2048 -keyalg RSA
```

What is your first and last name?

```
[Unknown]: cvp11.allevich.local
```

What is the name of your organizational unit?

```
[Unknown]: TAC
```

What is the name of your organization?

```
[Unknown]: Cisco
```

What is the name of your City or Locality?

```
[Unknown]: Krakow
```

What is the name of your State or Province?

```
[Unknown]: Malopolskie
```

What is the two-letter country code for this unit?

```
[Unknown]: PL
```

Is CN=cvp11, OU=TAC, O=Cisco, L=Krakow, ST=Malopolskie, C=PL correct?

```
[no]: yes
```

Generating 2,048 bit RSA key pair and self-signed certificate (SHA256withRSA) with a validity of 90 days for: CN=cvp11, OU=TAC, O=Cisco, L=Krakow, ST=Malopolskie, C=PL (RETURN if same as keystore password):
[Storing .keystore]

Controleer dat het sleutelpaar gegenereerd is.

```
c:\Cisco\CVP\conf\security>dir | findstr oamp.key
05/27/2016 08:13 AM 1,724 oamp.key
```

Zorg ervoor dat u de voor- en achternaam als uw OAMP-server invoert. De naam moet aan een IP-adres kunnen worden ontbinden. Deze naam wordt vermeld in het veld van de GN van het certificaat.

Nieuwe CSR genereren

Start deze opdracht om het certificaatverzoek voor het alias op te slaan en het in een bestand op te slaan (bijvoorbeeld oamp.csr).

```
%kt% -certreq -alias oamp_certificate -file oamp.csr
```

Controleer dat de CSR succesvol gegenereerd is.

```
dir oamp.csr
08/25/2016 08:13 AM 1,136 oamp.csr
```

Het certificaat afgeven op de CA

Om het certificaat te kunnen verkrijgen, hebt u een certificaatinstantie nodig die al is ingesteld.

Typ de gegeven URL in een browser

<http://<CA<ip-adres>/certsrv>

Selecteer vervolgens **certificaat aanvragen** en **geavanceerde certificaataanvraag**.

```
more oamp.csr
```

```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIIC/TCCAeUCAQAwgYcxIzAhBgkqhkiG9w0BCQEWFgFkbWluQGFSbGV2aWNoLmV2Y2F5MQswCQYD
VQQGEwJQTDEUMBIGA1UECBMLTWFSb3BvbHNraWUxZDZANBgNVBACTBktyYWtvdzEOMAwGA1UEChMF
Q2l1Z28xDDAKBgNVBAsTA1RBQzEOMAwGA1UEAxMFQ1ZQMTEwggEiMA0GCSqGSIb3DQEBAQUAA4IB
DwAwggEKAoIBAQCvQEGmJpmzimqQA6zclmbWnkzAj3PvGKe9Qg0REfOnHpLq+ddx66o6OGr6Ttb1
BrqI8UeN1JdfuQj/m4HZvKsqRv1AWA5CtGRzjboENXPMCGotk00b9643M8DY0Q9LQ/+PxdzYGhie
CxnHQURcAIsViphV4yxUVJ4QcLkzkbM9T8DSoJSJAI4gY+t03i0xxDTcXlaTQ1xkRYDba8JwzVHL
TkVwtSRK2jqIzJuBPZwpXMZc8RDkffBurrVXhFb8ylvR/Q7cAzHPgpPLuK6KmwpOKv8CRoWm13xA
EgRd39szkZfbawRzddTqw8hM/2cLSoUKx0NMFY5dXzIszQEYlK5XAgMBAAGgMDAuBgkqhkiG9w0B
CQ4xITAFMB0GA1UdDgQWBBRe8ul0CdlHckIm9VjD3ZL/uXhgGzANBgkqhkiG9w0BAQsFAAOCAQEA
c48VD1d/BJMaOXwz5rit1BCjxzLIMTNzv3W0K7ehtmYVTTaRCXLZ/sOX5ws807kwnOaZeIprZd
lGvumS+dUgun/2Q00rp+B44gRvpg9KUTvv5C6YoBslm4H2xp9yaQpgzLBJuKRgl8yIzYnIvoVuPx
racGSkyxKzxrvrxOX2qvxoVq71bf43Aps4+G85Cp3GWhIBQ+TtIKKxgZ/C64ThZgT9HtD9zbL3g0
U8bPlF6JNjztzjmuGEdqsNf0fAjPsfShQl0o4qIMBi7hBQusAwNBEB1xaAlYumD09+R/BK2KfMv
Iy4CdsEFwlmjBb541TJEYzwOh7tpRZkjOqyVMQ==
-----END NEW CERTIFICATE REQUEST-----
```

Kopieer en plak de gehele inhoud van de CSR naar het juiste menu. Selecteer **Web Server** als een certificaatsjabloon en **Base64 gecodeerd**. Klik vervolgens op de **Download certificaatketen**.

U kunt CA en webserver gegenereerd certificaat afzonderlijk exporteren of een volledige keten downloaden. In dit voorbeeld wordt de volledige kettingoptie gebruikt.

Importeren CA-gegenereerd certificaat

Installeer het certificaat uit het bestand.

```
%kt% -import -v -trustcacerts -alias oamp_certificate -file oamp.p7b
```

Nieuwe certificatieherstart **World Wide Web Publishing Service** toepassen en **Cisco CVP Services** voor **onbeperkt** gebruik.

Verifiëren

Gebruik dit gedeelte om te bevestigen dat de configuratie correct werkt.

Eenvoudig te controleren is inloggen op de CVP OAMP-webserver. U dient geen onbetrouwbaar waarschuwingsbericht te krijgen.

Een andere manier is om het OAMP certificaat te controleren dat met deze opdracht wordt gebruikt.

```
%kt% -list -v -alias oamp_certificate
```

```
Alias name: oamp_certificate  
Creation date: Oct 20, 2016  
Entry type: PrivateKeyEntry  
Certificate chain length: 2
```

Certificate [1]:

```
Owner: CN=cvp11.allevich.local, OU=TAC, O=Cisco, L=Krakow, ST=Malopolskie, C=PL  
Issuer: CN=pod1-POD1AD-CA, DC=pod1, DC=ccemea, DC=tac  
Serial number: 130c0db6000000000017  
Valid from: Thu Oct 20 12:48:08 CEST 2016 until: Sat Oct 20 12:48:08 CEST 2018  
Certificate fingerprints:  
MD5: BA:E8:FA:05:45:07:D0:3C:C8:81:1C:34:3D:21:AF:AC  
SHA1: 30:04:F2:EE:37:22:9D:8D:27:8F:54:D2:BA:D4:0F:33:74:34:87:D8  
Signature algorithm name: SHA1withRSA  
Version: 3
```

Extensions:

```
#1: ObjectId: 1.3.6.1.4.1.311.20.2 Criticality=false  
0000: 1E 12 00 57 00 65 00 62 00 53 00 65 00 72 00 76 ...W.e.b.S.e.r.v  
0010: 00 65 00 72 .e.r
```

```
#2: ObjectId: 1.3.6.1.5.5.7.1.1 Criticality=false  
AuthorityInfoAccess [  
[  
accessMethod: caIssuers  
accessLocation: URName: ldap:///CN=pod1-POD1AD-CA,CN=AIA,  
]  
]
```

```
#3: ObjectId: 2.5.29.35 Criticality=false  
AuthorityKeyIdentifier [  
]
```

```
KeyIdentifier [  
0000: 9B 33 47 9E 76 DB F3 92 B2 F8 F9 86 3A 59 BA DE .3G.v.....:Y..  
0010: C5 0B E5 E4 ....  
]  
]
```

```
#4: ObjectID: 2.5.29.31 Criticality=false  
CRLDistributionPoints [  
[DistributionPoint:  
[URName: ldap:///CN=pod1-POD1AD-CA,CN=POD1AD,CN=CDP]  
]]
```

```
#5: ObjectID: 2.5.29.37 Criticality=false  
ExtendedKeyUsages [  
serverAuth  
]
```

```
#6: ObjectID: 2.5.29.15 Criticality=true  
KeyUsage [  
DigitalSignature  
Key_Encipherment  
]
```

```
#7: ObjectID: 2.5.29.14 Criticality=false  
SubjectKeyIdentifier [  
KeyIdentifier [  
0000: CD FC 95 D1 60 44 9A 34 A9 EE 0E 3F C7 F5 5D 3C ....`D.4...?..]<  
0010: 46 DF 47 D9 F.G.  
]  
]
```

Certificate[2]:

```
Owner: CN=pod1-POD1AD-CA, DC=pod1, DC=ccemea, DC=tac  
Issuer: CN=pod1-POD1AD-CA, DC=pod1, DC=ccemea, DC=tac  
Serial number: 305dba13e0def8b474fefeb92f54acd  
Valid from: Thu Sep 08 18:06:37 CEST 2016 until: Wed Sep 08 18:16:36 CEST 2021  
Certificate fingerprints:  
MD5: 50:04:5F:89:CA:7C:D6:71:82:10:C3:04:57:78:AB:AE  
SHA1: A6:3B:07:29:AF:3A:07:73:9D:9B:4F:88:B5:A8:17:AC:0A:6D:C3:0D  
Signature algorithm name: SHA1withRSA  
Version: 3
```

Extensions:

```
#1: ObjectID: 1.3.6.1.4.1.311.21.1 Criticality=false  
0000: 02 01 00 ...
```

```
#2: ObjectID: 2.5.29.19 Criticality=true  
BasicConstraints:[  
CA:true  
PathLen:2147483647  
]
```

```
#3: ObjectID: 2.5.29.15 Criticality=false  
KeyUsage [  
DigitalSignature  
Key_CertSign  
Crl_Sign  
]
```

```
#4: ObjectID: 2.5.29.14 Criticality=false  
SubjectKeyIdentifier [  
KeyIdentifier [  
]
```

```
0000: 9B 33 47 9E 76 DB F3 92 B2 F8 F9 86 3A 59 BA DE .3G.v.....:Y..
0010: C5 0B E5 E4 ....
]
]
```

Problemen oplossen

Deze sectie verschaft informatie die u kunt gebruiken om problemen met uw configuratie op te lossen.

Als u de opdrachtsyntaxis moet controleren, raadpleegt u de Configuration and Administration Guide voor CVP.

http://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/cust_contact/contact_center/customer_voice_portal/cvp8_5/configuration/guide/ConfigAdminGuide_8-5.pdf

Gerelateerde informatie

[CA-ondertekend certificaat via CLI configureren in Cisco Voice Operating System \(VOS\)](#)

[Procedure om Windows Server zelfgetekend of certificeringsinstantie \(CA\) te verkrijgen en te uploaden.](#)

Technische ondersteuning en documentatie – Cisco Systems