# Genereren en toevoegen van certificaten die vereist zijn voor de installatie van Secure Endpoint Private Cloud 3.x.

## Inhoud

Inleiding Voorwaarden Vereisten Gebruikte componenten Achtergrondinformatie Certificaat maken Certificaten genereren op de Windows-server Een aanvraag voor certificaatondertekening genereren (CSR) Het indienen van de MVO bij de CA en het genereren van het certificaat De private sleutel exporteren en naar PEM-formaat converteren Certificaat op Linux-server genereren (strikte SSL-controle UITGESCHAKELD) Genereer zelf-ondertekende RootCA Een certificaat genereren voor elke service Eigen sleutel genereren MVO genereren Certificaat genereren Certificaat op Linux-server genereren (strikte SSL-controle ingeschakeld) Genereer zelf-ondertekende RootCA Een certificaat genereren voor elke service Maak een Extensies Configuration-bestand en sla het op (extensions.cnf) Eigen sleutel genereren **MVO** genereren Certificaat genereren De certificaten toevoegen aan Secure Console Private Cloud Verifiëren Problemen oplossen

## Inleiding

Dit document beschrijft het proces om certificaten te genereren die moeten worden geüpload bij elke nieuwe installatie van Secure Console Private Cloud of om de geïnstalleerde Certificate Services te vernieuwen.

## Voorwaarden

Vereisten

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

- Windows Server 2008
- CentOS 7/8
- Secure Console Virtual Private Cloud 3.0.2 (verder)
- OpenSSL 1.1.1

### Gebruikte componenten

Cisco raadt kennis van de volgende onderwerpen aan:

- Windows Server 2008 (vanaf)
- Private Cloud-installatie van Secure Console
- Public Key infrastructuur
- OpenSSL
- Linux CLI

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 zorgen dat u de potentiële impact van elke opdracht begrijpt.

## Achtergrondinformatie

Met de introductie van Secure Console Private Cloud 3.X zijn hostnamen en certificaat/sleutelparen vereist voor alle volgende services:

- Beheerportal
- Verificatie (nieuw in Private Cloud 3.x)
- Beveiligde console
- Dispositieserver
- Disposition Server uitgebreid protocol
- Disposition Update Service
- Firepower Management Center

Dit document wordt op een snelle manier besproken om de vereiste certificaten te genereren en te uploaden. U kunt elk van de parameters, inclusief het hashingalgoritme, sleutelgrootte en andere, aanpassen volgens het beleid van uw organisatie, en uw mechanisme voor het genereren van deze certificaten komt mogelijk niet overeen met wat hier gedetailleerd is.

**Waarschuwing**: de onderstaande procedure kan per CA-serverconfiguratie verschillen. Er wordt verwacht dat de CA-server van uw keuze al is voorzien en dat de configuratie van dezelfde server is voltooid. De volgende technologie beschrijft alleen een voorbeeld van het genereren van de certificaten en Cisco TAC is niet betrokken bij problemen met de productie van certificaten en/of CA-serverproblemen van enigerlei soort.

### Certificaat maken

Certificaten genereren op de Windows-server

Zorg ervoor dat de volgende rollen zijn geïnstalleerd en geconfigureerd op uw Windows-server.

- Active Directory-certificaatservices
- Certificeringsinstantie
- Webinschrijving voor certificeringsinstanties
- Online Responder
- Webservice voor certificaatinschrijving
- Web-service voor certificaatinschrijving
- Active Directory Domain Services
- DNS-servers
- Webserver (IIS)
- Active Directory Certificate Services
- Active Directory Domain Services
   DNS Server
   File Services
- Web Server (IIS)

#### Een aanvraag voor certificaatondertekening genereren (CSR)

Stap 1. Navigeer naar de MMC-console en voeg de Certificaten voor uw computeraccount toe zoals in de afbeelding hier.

	Vendor 🔺		Console Root	Edit Extensions
ctive Directory Do	Microsoft Cor		Certificates (Local Computer)	
ctive Directory Site	Microsoft Cor			Remove
ctive Directory Use	Microsoft Cor			
ctiveX Control	Microsoft Cor			Move Up
DSI Edit	Microsoft Cor			
uthorization Manager	Microsoft Cor			Move Down
ertificate Templates	Microsoft Cor	Add >		
ertificates	Microsoft Cor			
ertification Authority	Microsoft Cor			
omponent Services	Microsoft Cor			
omputer Managem	Microsoft Cor			
evice Manager	Microsoft Cor			
isk Management	Microsoft and			Manual
NS	Microsoft Cor			Advanced
Nino:				
where the				

Stap 2. Boor Certificaten (Lokale Computer) > Persoonlijk > Certificaten.

Stap 3. Klik met de rechtermuisknop op de lege ruimte en selecteer **Alle taken > Geavanceerde bewerkingen > Aangepaste aanvraag maken.** 



Stap 4. Selecteer Volgende in het inschrijvingsvenster.



Stap 5. Selecteer uw certificaatinschrijvingsbeleid en selecteer Volgende.

Select Certificate Enrollment Pol	icy
Certificate enrollment policy enables e enrollment policy may already be conf	nrolment for certificates based on predefined certificate templates. Certificat gured for you.
Configured by your administrat	or
Active Directory Enrolment Policy	0
Configured by you	Add Net
Custom Request	
Proceed without enrolment policy	

Stap 6. Kies de sjabloon als webserver en selecteer Volgende.

ertificate Enrollment	_ 0				
Certificate Enrollment					
Custom request					
Chose an option from t	he list below and configure the certificate options as required.				
Template:	Web Server				
	Suppress default extensions				
Request format:					
	Сомс				
Note: Key archival is n specified in the certific	ot available for certificates based on a custom certificate request, even when this option is ate template.				
Learn more about <u>cust</u>	m request				
	Next Cascal				

Stap 7. Als uw "Web Server" sjabloon correct is geconfigureerd en beschikbaar is voor inschrijving, wordt de status Available weergegeven. Selecteer **Details** om Eigenschappen uit te vouwen.

ertificate Information		
lick Next to use the options and then dick Next	iready selected for this template, or click Details to customize the	he certificate request,
no oten dick wext.		
Active Directory En	oliment Policy	
Web Server	(j) STATUS: Available	Details @
The following options de Key usage: Application policies:	scribe the uses and validity period that apply to this type of cer Digital signature Key encipherment Server Authentication	tificate:
Validity period (days	): 730	Properties

Stap 8. Voeg op zijn minst de CN- en DNS-kenmerken toe. De rest van de attributen kan worden toegevoegd volgens uw beveiligingsvereisten.

ertificate Properties		×
A Subject General Extensions	Private Key	
The subject of a certificate is the us enter information about the types of in a certificate.	ser or computer to which th of subject name and alterna	e certificate is issued. You can ative name values that can be used
Subject of certificate		
The user or computer that is received	ing the certificate	I
Subject name:		
Type:		CN=amp-vpc.cisco.com
Common name	Add >	
Value:		
	< Remove	
Alternative name:		DNS
Type:		amp-vpc.cisco.com
UNS I		
value:	Add >	
<b> </b>	man -	
	< Remove	
Learn more about subject name		
	~	Cancel Arathy
	04	Cancer Apply

Stap 9. Naar keuze een Vriendelijke Naam geven onder het tabblad Algemeen.

Stap 10. Selecteer op het tabblad **Private Key** en zorg ervoor dat u **private key exporteerbaar maken** onder het gedeelte **Key Options** inschakelt.

Certificate Properties	×
🔥 Subject   General   Extensions   Private Key	
Cryptographic Service Provider	۲
Key options Set the key length and export options for the private key. Key size: 2048	8
Allow private key to be archived     Strong private key protection	
Key type	۲
Key permissions	۲
Learn more about private key	
OK Cancel	Apply

Stap 11. Selecteer tot slot **OK**. Dit moet u naar het dialoogvenster Certificaatinschrijving leiden, waar u **Volgende** kunt selecteren.

Stap 12. Blader naar een locatie om het bestand .req op te slaan dat wordt verzonden naar de CA-server voor ondertekening.

#### Het indienen van de MVO bij de CA en het genereren van het certificaat

Stap 1. Navigeer naar de webpagina van MS AD Certificate Services zoals hieronder en selecteer **Certificaat aanvragen**.

Microsoft Active Directory Certificate Services -- bgl-amp-AD-CA

### Welcome

Use this Web site to request a certificate for your Web brov request, perform other security tasks.

You can also use this Web site to download a certificate au

For more information about Active Directory Certificate Ser

### Select a task:

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

Stap 2. Selecteer deze optie op de koppeling voor geavanceerde certificaataanvragen.

Microsoft Active Directory Certificate Services -- bgl-amp-AD-CA

### **Request a Certificate**

Select the certificate type: User Certificate

Or, submit an advanced certificate request.

Stap 3. Selecteer op Submit een certificaatverzoek door een basis-64-gecodeerd CMC- of PKCS-#10 te gebruiken, of dien een verlengingsverzoek in met behulp van een basis-64-gecodeerd PKCS-#7.

Stap 4. Open de inhoud van het eerder opgeslagen .req bestand (CSR) via Notepad. Kopieer de inhoud en plak deze hier. Zorg ervoor dat de certificaatsjabloon als **webserver** is geselecteerd



Stap 5. Selecteer tot slot Verzenden.

Stap 6. Op dit punt moet u in staat zijn om het certificaat te downloaden, zoals in de afbeelding.

Certificate Issued						
The certificate you requested was issued to you.						
DER encoded or      Description Base 64 encoded     Download certificate     Download certificate chain						

#### De private sleutel exporteren en naar PEM-formaat converteren

Stap 1. Installeer het certificaat in uw certificaatarchief door het .cer-bestand te openen en selecteer **Certificaat installeren**.

Stap 2. Navigeer naar de MMC snap-in die eerder is geselecteerd.

Stap 3. Navigeer naar de winkel waar het certificaat is geïnstalleerd.

Stap 4. Klik met de rechtermuisknop op het juiste certificaat en selecteer Alle taken > Exporteren.

🙀 console	Open	bgl-amp-AD-CA				
🔄 dispex	open	bgl-amp-AD-CA				
🛱 disp-pr	All Tasks 🕨 🕨	Open				
協助 について 協力 について について について について について について について について	Cut Copy	Request Certificate with New Key Renew Certificate with New Key				
	Delete	Manage Private Keys				
	Properties	Advanced Operations				
	Help	Export				

Stap 5. Bevestig bij de wizard Certificaat exporteren dat de privé-sleutel wordt geëxporteerd, zoals

in de afbeelding.

Certificate Export Wizard
Export Private Key
You can choose to export the private key with the certificate.
Private keys are password protected. If you want to export the private key with the certificate, you must type a password on a later page.
Do you want to export the private key with the certificate?
Yes, export the private key
C No, do not export the private key
Learn more about exporting private keys
< Back Next > Cancel
Contract Contract

Stap 6. Typ een wachtwoord en selecteer Volgende om de privé-sleutel op de schijf op te slaan.

Stap 7. Dit slaat de privé-sleutel op in .PFX-formaat, maar dit moet worden geconverteerd naar .PEM-formaat om dit te gebruiken met Secure Endpoint Private Cloud.

Stap 8. Installeer OpenSSL-bibliotheken.

Stap 9. Open een opdrachtprompt venster en verander naar de map waarin u OpenSSL hebt geïnstalleerd.

Stap 10. Voer de volgende opdracht uit om de privé-sleutel te extraheren en op te slaan in een nieuw bestand: (Als uw PFX-bestand niet in hetzelfde pad staat als waar de OpenSSL-bibliotheek is opgeslagen, moet u het exacte pad met de bestandsnaam specificeren)

openssl pkcs12 -in yourpfxfile.pfx -nocerts -out privatekey.pem -nodes Stap 11. Voer nu de volgende opdracht uit om ook de public cert te extraheren en op te slaan als een nieuw bestand:

openssl pkcs12 -in yourpfxfile.pfx -nokeys -out publiccert.pem -nodes

Certificaat op Linux-server genereren (strikte SSL-controle UITGESCHAKELD)

**Opmerking**: Strict TLS Check verifieert dat het certificaat voldoet aan de TLS-vereisten van Apple. Raadpleeg de <u>Admin Guide</u> voor meer informatie.

Zorg ervoor dat de Linux Server die u probeert te genereren van de vereiste certificaten de OpenSSL 1.1.1-bibliotheken heeft geïnstalleerd. Verifiëren of dit en de hieronder genoemde procedure kunnen variëren van de Linux-distributie die u gebruikt. Dit gedeelte is gedocumenteerd, zoals gedaan op een CentOS 8.4-server.

#### Genereer zelf-ondertekende RootCA

Stap 1. Genereer de Private Key voor Root CA-certificaat.

openssl genrsa -out Stap 2. Genereer het CA-certificaat.

```
openssl req \
-subj '/CN=
-addext "extendedKeyUsage = serverAuth, clientAuth" \
-outform pem -out
-key
-days "1000"
```

#### Een certificaat genereren voor elke service

Maak het certificaat aan voor verificatie, console, verwerking, uitgebreide disppositie, updateserver, Firepower Management Center (FMC) service volgens de DNS-naamvermelding. U dient het onderstaande proces voor het genereren van certificaten voor elke service te herhalen (verificatie, console, etc.).

Certificate (PEM .crt)			<pre> Qe Key (PEM .key) </pre>		
8	Certificate file has been uploaded.		Key file has been uploaded.		
0	Certificate is in a readable format.	0	Key contains a supported key type.		
D	Certificate start and end dates are valid.		Key contains public key material.		
0	Certificate contains a subject. Certificate contains a common name.		Image: Key contains private key material.           Image: Key contains a public key matching the uploaded certificate		
0					
9	Certificate contains a public key matching the uploaded	key.	+ Choose K		
0	Certificate matches hostname.				
Certificate is signed by a trusted root authority.					
	+ Chonea Cartil	cate			

#### Eigen sleutel genereren

openssl genrsa -out

Vervang <YourServiceName.key> door het nieuwe KEY-bestand dat moet worden gemaakt als Auth-Cert.key

#### MVO genereren

openssl req -new \ -subj '/CN= -key

Vervang de <YourServiceName.key> met het huidige (of nieuwe) KEY-bestand voor certificaten zoals Auth-Cert.key

Vervang <YourServiceName.csr> door CSR-bestandsnaam die moet worden gemaakt, zoals Auth-Cert.crt

#### Certificaat genereren

```
openssl x509 -req \
-in
-CAkey
-days 397 -sha256
```

Vervang <YourServiceName.csr> door feitelijke (of nieuwe) CSR-certificaten zoals Auth-Cert.csr

Vervang de <YourRootCAName.pem> door werkelijke (of nieuwe) PEM-bestandsnaam als RootCAName.pem

Vervang <YourServiceName.key> door het huidige (of nieuwe) KEY-bestand voor certificaten zoals Auth-Cert.key

Vervang <YourServiceName.crt> door bestandsnaam die moet worden gemaakt, zoals Auth-Cert.crt

#### Certificaat op Linux-server genereren (strikte SSL-controle ingeschakeld)

**Opmerking**: Strict TLS Check verifieert dat het certificaat voldoet aan de TLS-vereisten van Apple. Raadpleeg de <u>Admin Guide</u> voor meer informatie.

#### Genereer zelf-ondertekende RootCA

Stap 1. Genereer de Private Key voor Root CA-certificaat.

openssl genrsa -out Stap 2. Genereer het CA-certificaat.

openssl req \ -subj '/CN= -outform pem -out -key -days "1000"

#### Een certificaat genereren voor elke service

Maak het certificaat aan voor verificatie, console, verwerking, uitgebreide disppositie, updateserver, Firepower Management Center (FMC) service volgens de DNS-naamvermelding. U dient het onderstaande proces voor het genereren van certificaten voor elke service te herhalen (verificatie, console, etc.).

AP fo	r Endpoints Console Certificate		Disable Strict TLS Check	Undo	Replace Certificate
	<pre>@ Certificate (PEM .crt)</pre>	L	Q. Koy (DEM	key)	
0	Certificate file has been uploaded.	0	Key file has been uploaded.		
0	Certificate is in a readable format.	0	Key contains a supported key typ	oe.	
0	Certificate start and end dates are valid.	٥	Key contains public key material.		
0	Certificate contains a subject.	0	Key contains private key material	L	
0	Certificate contains a common name.	0	Key contains a public key matchi	ing the u	ploaded certificate.
0	Certificate contains a public key matching the uploaded key.				+ Choose Key
0	Certificate matches hostname.	-			
0	Certificate is signed by a trusted root authority.				
0	Certificate issued after 07/01/2019 must have a validity period of 825 days or less.				
0	Certificate issued after 09/01/2020 must have a validity period of 398 days or less.				
0	Certificate does not use sha-1 signature algorithm.				
0	Certificate using RSA keys must use a key size of 2048 or more.				
0	Certificate must specify server certificate in Extended Key Usage extension.				
	+ Choose Certificate				

### Maak een Extensies Configuration-bestand en sla het op (extensions.cnf)

```
[v3_ca]
basicConstraints = CA:FALSE
keyUsage = critical, digitalSignature, keyEncipherment
extendedKeyUsage = critical, serverAuth, clientAuth
```

#### Eigen sleutel genereren

openssl genrsa -out Vervang <YourServiceName.key> door een nieuwe KEY-bestandsnaam die moet worden gemaakt als Auth-Cert.key

#### MVO genereren

```
openssl req -new \
-key
-subj '/CN=
-out
```

Vervang de <YourServiceName.key> met de huidige (of nieuwe) certificaatTOETS zoals Auth-Cert.key

Vervang <YourServiceName.csr> door het huidige (of nieuwe) certificaat CSR zoals Auth-Cert.csr

#### Certificaat genereren

```
openssl x509 -req -in
-CA
-CAcreateserial -out
-extensions v3_ca -extfile extensions.cnf \
-days 397 -sha256
```

Vervang <YourServiceName.csr> door huidige (of nieuwe) CSR-certificaten zoals Auth-Cert.csr

Vervang <YourRootCAName.pem> door huidige (of nieuwe) PEM-bestandsnaam als RootCAName.pem

Vervang <YourServiceName.key> door huidig (of nieuw) KEY-bestand voor certificaten, zoals Auth-Cert.key

Vervang <YourServiceName.crt> door bestandsnaam die moet worden gemaakt, zoals Auth-Cert.crt

### De certificaten toevoegen aan Secure Console Private Cloud

Stap 1. Nadat de certificaten zijn gegenereerd op basis van een van de bovengenoemde methoden, kunt u het corresponderende certificaat uploaden voor elk van de services. Als ze correct zijn gegenereerd, worden alle selectietekens ingeschakeld zoals in de afbeelding hier.



## Verifiëren

Er is momenteel geen verificatieprocedure beschikbaar voor deze configuratie.

## Problemen oplossen

Er is momenteel geen specifieke troubleshooting-informatie beschikbaar voor deze configuratie.

#### Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.