# Beveiligde communicatie tussen finse en CTIserver configureren

## Inhoud

Inleiding **Voorwaarden** Vereisten Gebruikte componenten Achtergrondinformatie Configureren CCE CTI-server beveiligd Beveiligingsconfiguratie voltooien Generate Agent PG certificaatserver (CTI server) Ontvang het CSR-certificaat ondertekend door een CA De CCE PG's CA-ondertekende certificaten importeren Finesse-certificaat genereren Sign Finesecertificaat van CA FineReader-toepassing- en basiscertificaten importeren Verifiëren Problemen oplossen

## Inleiding

Dit document beschrijft hoe u certificaten van de certificaatautoriteit (CA) kunt implementeren tussen Cisco Finesse en Computer Telephony Integration (CTI) server in Cisco Contact Center Enterprise (CCE)-oplossing.

## Voorwaarden

## Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- CCE release 12.0(1)
- Finse release 12.0(1)
- CTI-server

## Gebruikte componenten

De informatie in dit document is gebaseerd op deze softwareversies:

• Packaged CCE (PCCE) 12.0(1)

• Finesse 12.0(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 levend is, zorg er dan voor dat u de mogelijke impact van om het even welke opdracht begrijpt.

## Achtergrondinformatie

In CCE versie 11.5 startte Cisco de ondersteuning van Transport Layer Security (TLS) versie 1.2, waarmee Session Initiation Protocol (SIP) en Real-time Transport Protocol (RTP)-berichten (Realtime Transport Protocol) veilig via TLS 1.2 kunnen worden getransporteerd. Vanaf CCE 12.0 en als onderdeel van bewegende Cisco de gegevensbeveiliging begon de ondersteuning van TLS op de meeste de oproepingsstromen van het contactcentrum : Ingebonden en Uitgaande stem, Multikanaal, en Extern gegevensbestand dip. De focus van dit document is inkomende stem, vooral de communicatie tussen Finse en CTI Server.

De CTI Server ondersteunt deze modi van verbindingen:

- Alleen beveiligde verbinding: Maakt beveiligde verbinding tussen de CTI Server en de CTI klanten (Finesse, dialer, CTIOS en censuur) mogelijk.
- Beveiligde verbinding zonder beveiliging (gemengde modus): Hiermee kan de beveiliging worden gegarandeerd, evenals de onveilige verbinding tussen de CTI-server en de CTI-klanten. Dit is de standaardverbindingsmodus. Deze modus wordt ingesteld wanneer u eerdere releases naar CCE 12.0(1) upgrade uitvoert.

Opmerking: De niet-beveiligde alleen-modus wordt niet ondersteund.

## Configureren

## CCE CTI-server beveiligd

Stap 1. Open op het PC Administration Workstation (AW) de **Unified CCE**-map en dubbelklik op **Perifere Gateway Setup**.



Stap 2. Selecteer CG3A en klik op Bewerken.

CC Ad	Instance Components	и
Ed	PG1A PG2A PG3A RoutesA Del	R
To set up Administration Data Interface Controller (NIC), We Web Setup tool.	Server (Distributor A/W), Router, Logger, Netw bV/iew or Network Gateway components, use t nt (Client A/W), use the Administration Client Inst	ork he aller
To set up Administration Clien and Setup tool.		

Stap 3. Klik op **Volgende** op de CTI-servereigenschappen. Selecteer **Ja** bij de vraag over het stoppen van de **CG3A** service.

Stap 4. Selecteer in de **eigenschappen van de CTI-servercomponenten** de optie **Alleen beveiligdeonly modus inschakelen.** Merk op dat u de **Secure Connection Port (46030)** hebt, aangezien u dezelfde poort in Finesse moet configureren tijdens de volgende oefening. Klik op **Volgende**.

CTI Server Component Properties
CTI Server configuration
Secured Connection Port 46030
Non-Secured Connection Port 42027
Agent Login Required for Client Events
Help < Back Next > Cancel

**Opmerking:** De standaard beveiligde communicatie is 42030, maar het lab gebruikt voor dit document is 40630. Het poortnummer maakt deel uit van een formule die de ICM systeem ID bevat. Wanneer de systeemid 1 (CG1a) is het standaardpoortnummer, in het algemeen,

42030. Aangezien de systeemid in het laboratorium 3 (CG3a) is, is het standaardhavenaantal 46030.

Stap 5. Klik op **Volgende** op de **eigenschappen van de CTI-netwerkinterface**. Controleer de **Setup-informatie** en klik op **Volgende**.

Unified ICM/CCE PGSetup	cc-CG3A ×
Check Setup Information	
Setup has enough information to begin the configuration If you want to review or change and of the settings, click If satisfied, click Next to begin configuring the CTI Gatew	operation. Back. ay.
Current Settings:	
Setup Type: CTI Gateway, side A	^
Target Directory: C:ljicm	Ξ
Configuration: PG node is pocealin1p CTI Gateway is simplexed DMP address is 3	
<	>
talShield	
< Bad	: Next > Cancel

Stap 6. Klik op Voltooien zoals in de afbeelding.

Unifie	Unified ICM/CCE PGSetup: cc-CG3A		
	Setup Complete PGSetup is complete. You may start the Unified ICM/CC Node Manager service now by checking the box below. Ves, start the Unified ICM/CC Node Manager Click Finish to Complete Setup.		
	< Back Finish Cancel		

Stap 7. Klik op **Exit Setup** en wacht tot het setup-venster is gesloten zoals in de afbeelding.

ICM Instances	Instance Compor	ents
cc	Add AW	Add
	LoggesA	
	Edit PG2A	Edit
	PG3A Perton	Dalata
	HouterA	Delete
To set up Administration D nterface Controller (NIC), Veb Setup tool.	Data Server (Distributor AW), Router WebView or Network Gateway con	, Logger, Network sponents, use the
To set up Administration D nterface Controller (NIC), Web Setup tool. To set up Administration D and Setup tool.	Data Server (Distributor AW), Router WebView or Network Gateway con Client (Client AW), use the Administra	, Logger, Network apponents, use the stion Client Installer
To set up Administration D nterface Controller (NIC), Web Setup tool. To set up Administration 0 and Setup tool. The Instance cc cannot t	Data Server (Distributor AW), Router WebView or Network Gateway con Client (Client AW), use the Administra be deleted because it has compone	, Logger, Network aponents, use the ation Client Installer
To set up Administration D nterface Controller (NIC), Web Setup tool. To set up Administration O and Setup tool. The Instance cc cannot b Web Setup or Administrat o remove those compone Setup.	Data Server (Distributor AW), Router WebView or Network Gateway con Client (Client AW), use the Administra be deleted because it has compone tion Client Setup tool. You must use ents before deleting the instance in I	, Logger, Network apponents, use the ation Client Installer Ints set up by the the applicable tool Peripheral Gateway

Stap 8. Op de PCline1 desktop dubbelklikt u op Unified CCE Service Control.

Stap 9. Selecteer Cisco ICM c CG3A en klik op Start.

### Beveiligingsconfiguratie voltooien

Stap 1. Open een webbrowser en navigeer naar Finse Administration.

Stap 2. Scrolt naar de **instellingen van de Enterprise CTI van het** vak **Contact Center** zoals in de afbeelding.

Contact Center Enter	erprise CTI Server Sett	ings	
Note: Any changes made to Contact Center Enterpris	the settings on this gadget required to the settings of the cTI Server Settings	ire a restart of Cisco Finesse Torncat to	take effect.
A Side Host/IP Address*	10.10.10.10	B Side Host/IP Address	
A Side Port*	42027	B Side Port	
Peripheral ID*	5000		
Enable SSL encryption Save Reven	q		

Stap 3. Verander de A zijpoort voor de beveiligde communicatiepoort die op CG3A is ingesteld in de vorige oefening: **46030**. Controleer **SSL-encryptie inschakelen** en klik op **Opslaan**.

Contact Center Ent	erprise CTI Server Se	ettings	
Note: Any changes made to Contact Center Enterpris	o the settings on this gadget r se CTI Server Settings	equire a restart of Cisco Finesse Torncat to	take effect.
A Side Host/IP Address*	10.10.10.10	B Side Host/IP Address	
A Side Port*	46030	B Side Port	
Peripheral ID*	5000		
Enable SSL encryption	rt		

**Opmerking:** Om de verbinding te testen, moet u eerst de Finse Tomcat Service opnieuw opstarten of de Finse server opnieuw opstarten.

Stap 4. Meld u uit op de pagina Eindtijd.

Stap 5. Open een SSH-sessie met Voltooien.

Stap 6. Voer in de SSH-sessie van FINESSEA de opdracht uit:

#### herstart van het besturingssysteem

Voer **ja** in als u wilt dat het systeem opnieuw wordt gestart.

```
<sup>A</sup> Using username "administrator".
Command Line Interface is starting up, please wait ...
Welcome to the Platform Command Line Interface
VMware Installation:
2 vCPU: Intel(R) Xeon(R) CPU E5-2680 0 @ 2.70GHz
Disk 1: 146GB, Partitions aligned
8192 Mbytes RAM
admin:utils system restart
Do you really want to restart ?
Enter (yes/no)? yes
Appliance is being Restarted ...
Warning: Restart could take up to 5 minutes.
Stopping Service Manager...
```

#### Generate Agent PG certificaatserver (CTI server)

CiscoCertUtils is een nieuw gereedschap dat op CCE versie 12 wordt vrijgegeven. U gebruikt dit gereedschap om alle CCE-certificaten voor inkomende spraak te beheren. In dit document

gebruikt u deze CiscoCertUTS om de aanvragen voor certificaatsignalering (CSR's) van perifere gateways (PG's) te genereren.

Stap 1. Voer deze opdracht uit om een CSR-certificaat te genereren: Cisco certUtil /GenerateCSR



Verstrek de gevraagde informatie, bijvoorbeeld:

Naam land: VS

Naam land of provincie: MA

Naam lokaliteit: BXB

Naam organisatie: Cisco

Organisatorische eenheid: CX

Vaak voorkomende naam: PCCEAllin1.cc.lab

Email: jdoe@cc.lab

Een Challenge wachtwoord: Train1ng!

Een optionele bedrijfsnaam: Cisco

Het gastcertificaat en de sleutel worden opgeslagen in C:\icm\ssl\certs en C:\icm\ssl\keys.

Stap 2. Navigeer naar C:\icm\ssl\certs en controleer of het bestand host.csr gegenereerd is.

### CSR-certificaat verkrijgen Ondertekend door een CA

Nadat de CSR-certificaten zijn gegenereerd, moeten ze door een derde CA worden ondertekend. In deze oefening wordt Microsoft CA, geïnstalleerd in de Domain Controller, gebruikt als derde partij CA.

Zorg ervoor dat de certificaatsjabloon die door CA wordt gebruikt, client- en serververificatie bevat zoals in de afbeelding wordt weergegeven wanneer Microsoft CA wordt gebruikt.

Properties of New Template	ons	
Subject Name         Server         Issuance Requirements           Compatibility         General         Request Handling         Cryptography         Key Attestation           Superseded Templates         Extensions         Security           To modify an extension, select it, and then click Edit.           Extensions included in this template:	tificate Templates ( More Actions b Server More Actions Edit Application P	(DC.cc.lab)
Application Policies Basic Constraints	An application policy defi	Add Application Policy
Certificate Template Information Issuance Policies	Application pglicies:	An application policy (called enhanced key usage in Windows 2000) defines how a certificate can be used. Select the application policy required for valid signatures of certificates issued by this template.
Edit Description of Application Policies:		Any Purpose Attestation Identity Key Certificate Certificate Request Agent Clent Authentication Code Signing
	Add	CTL Usage Digital Rights Decorpt Service Email Replication Disallowed List Document Encryption Document Signing Domain Name System (DNS) Server Trust Dynamic Code Generator
OK Cancel Apply Help		OK Cancel

Stap 1. Open een webbrowser en navigeer naar de CA.

Stap 2. Selecteer in de Microsoft Active Directory certificaatservices en verzoek een certificaat.

	= 0 X
(← ) (② https://dc.ec.lab/certsrv/en-us/ P = @ C (③ Microsoft Active Directory ×	n 🖈 0
Microsoft Active Directory Certificate Services cc-DC-CA	Home
Welcome	
Use this Web site to request a certificate for your Web browser, e-mail client, or other program certificate, you can verify your identity to people you communicate with over the Web, sign and messages, and, depending upon the type of certificate you request, perform other security task	. By using a l encrypt cs.
You can also use this Web site to download a certificate authority (CA) certificate, certificate ch certificate revocation list (CRL), or to view the status of a pending request.	hain, or
For more information about Active Directory Certificate Services, see <u>Active Directory Certificate</u> Documentation.	te Services
Select a task: Request a certificate View the status of a pending certificate request Download a CA certificate, certificate chain, or CRL	

Stap 3. Selecteer de optie geavanceerde certificaataanvraag.

Micr	osoft Activ	e Directory Ce	artifical X	+				
$\leftrightarrow$ $\rightarrow$	Сю		i 🔒	https://dc.c	c.lab/certsrv/en	-us/certr	qus.asp	
🗎 СИСМ	🛅 CUIC	🛅 Finesse	🛅 Remote E	xpert Mobile	🛅 MediaSense	CVP	🛅 CCE	
Microsoft	Active Dire	ectory Certifi	cate Services	cc-DC-C	CA			
Request	a Certif	icate						_
Select the User C	e certific Certificat	ate type: e						
Or, subm	it an <u>adv</u>	anced cer	tificate req	<u>uest</u> .				

Stap 4. Op het **geavanceerde certificaatverzoek** kopieert en **voegt** u de inhoud van het PG Agent CSR-certificaat in het vak **Opslaan**.

Stap 5. Selecteer de sjabloon van **webserver** met client- en serververificatie. In het laboratorium, werd het sjabloon van de Server van het Web van CC gecreëerd met client en server authenticatie.

To submit a sav Saved Reques	box. Cop of the cap box.	y and paste the contents he expected CSR file	
Saved Request:			
Base-64-encoded certificate request CMC or PKCS #10 or PKCS #7):	SLhnlD3GsLbIYivb7IbshWfqH15 gWL/H3DR1nRpJtLKfnLGgX5xUAZ +L3E0yNQ+W9/SJ0JYzBGnHk38yo J75nKDoyAh7C+F0u9tmg26DZaOZ rArT9OOdxJem END CERTIFICATE REQUES <	09jMcZ3uZrciC ↑ qin/56HjuGb4h 1P/I7UsueE30R 3k9Wo5QzUTPmd Tsna ¥	
Certificate Templ	ate:		
Ċ	CC Web Server ~		
dditional Attribu	ites:		
Attributes:			

Stap 6. Klik op Inzenden.

Stap 7. Selecteer Base 64 gecodeerd en klik op Download certificaat zoals in de afbeelding.

Microsoft Active Directory Certificate Services -- cc-DC-CA

## Certificate Issued

The certificate you requested was issued to you.

O DER encoded or 
 Base 64 encoded
 Download certificate

				•	
27		22	70		L
	2.0	- 10	• *		-
к.,	-	2.1	. 1		
	-				

Download certificate chain

Stap 8. Sla het bestand op en klik op OK. Het bestand wordt opgeslagen in de map Downloads.

Stap 9. Geef het bestand een andere naam aan host.cer (optioneel).

Stap 10. U moet ook een basiscertificaat genereren. Ga terug naar de CA-pagina en selecteer vervolgens **een CA-certificaat, certificeringsketen of CRL downloaden**. U hoeft deze stap slechts één keer te doen, omdat het basiscertificaat voor alle servers hetzelfde is (PG Agent en Finse).

Microsoft Active Directory Certificate Services cc-DC-CA
Welcome
Use this Web site to request a certificate for your Web browser, $\varepsilon$ people you communicate with over the Web, sign and encrypt mescurity tasks.
You can also use this Web site to download a certificate authority status of a pending request.
For more information about Active Directory Certificate Services,
Select a task: <u>Request a certificate</u> View the status of a pending certificate request <u>Download a CA certificate, certificate chain, or CRL</u>

Stap 1. Klik op Base T64 en selecteer CA-certificaat downloaden.

Microsoft Active Directory Certificate Services cc-DC-CA
Download a CA Certificate, Certificate Chain, or CRL
To trust certificates issued from this certification authority,
To download a CA certificate, certificate chain, or CRL, se
CA certificate:
Current (co-DC-CA)
Encoding method:
ODER ⊛Base 64
Install CA certificate
Download CA certificate
Download CA certificate chain
Download latest base CRL
Download latest delta CRL

Stap 12. Klik op Opslaan bestand en selecteer **OK**. Het bestand wordt op de standaardlocatie **Downloads** opgeslagen.

### De CCE PG's CA-ondertekende certificaten importeren

Stap 1. Op de PG Agent navigeer naar C:\icm\ssl\certs en plak de wortel en de ondertekende PG Agent bestanden hier.

Stap 2. Hernoemen het host.pem-certificaat op c:\icm\ssl\certs als selfhost.pem.

Stap 3. Hernoemen host.cer naar host.pem in c:\icm\ssl\certs -map.

Stap 4. Installeer het basiscertificaat. Geef deze opdracht op in de opdrachtmelding: CiscoCertUtil /install C:\icm\ssl\certs\rootAll.cer



Stap 5. Installeer het door de toepassing ondertekende certificaat met dezelfde opdracht: **CiscoCertUtil /install C:\icm\ssl\certs\host.pem** 



Stap 6. Programmaoverzicht van de PDF. Open de Unified CCE Service Control en centrifugeer de Cisco ICM Agent PG.

### Finesse-certificaat genereren

Stap 1. Open de webbrowser en navigeer naar Finesse OS Admin.

Stap 2. Meld u aan bij de inloggegevens van het besturingssysteem en navigeer naar **Security >** certificaatbeheer zoals in de afbeelding.



Stap 3. Klik op Generate CSR zoals in de afbeelding.



Stap 4. Gebruik in de aanvraag voor het genereren van certificaten de standaardwaarden en klik op Generate.

enerate Certificate Si	igning Request
Generate 🖳 Close	
•	
Status	
Warning: Generatin	g a new CSR for a specific certificate type will overwrite the existing CSR for that type
Generate Certificate	Signing Request
Certificate Purpose**	tomcat
Distribution*	FINESSEA.cc.lab
Common Name*	FINESSEA.cc.lab
Subject Alternate Nar	mes (SANs)
Parent Domain	cc.lab
Key Type**	RSA
Key Length	2048 v
Hash Algorithm*	SH4256 V
Generate Close	SHA256 V
(i) *- indicates require	ed item.
When the Certif	cate Purpose ending with '-ECDSA' is selected, the certificate/key type is Elliptic Curve (EC). Otherwise, it
is RSA.	

Stap 5. Sluit het venster Generate certificaatsignalering en selecteer CSR downloaden.

Show *	Settings *	Security *	Software Upgrades *	Services *	Help *		
Certifica	ite List						
Gen	erate Self-sign	ed 🐴 Up	load Certificate/Certificate	chain 💽	Generate CSR	Download CSR	

Stap 6. Selecteer in het gedeelte Certificaat de optie Tomé en klik op Download CSR.



Stap 7. Selecteer **Opslaan bestand** en klik op **OK** zoals in de afbeelding.

Opening tomcat.csr		×
You have chosen to	open:	
tomcat.csr		
which is: csr	file	
from: https://	finessea.cc.lab:8443	
What should Firefo	ox do with this file?	
O Open with	Browse	
Save File		
Do this autor	natically for files like this from now on	
_ Do this gotor	nationary for mes nice this north now on.	
	OK Cancel	

Stap 8. Sluit het venster **Download** de **certificaatsignalering**. Het certificaat wordt opgeslagen op de standaardlocatie (**Deze pc > Downloads**).

Stap 9. Open Windows Verkenner en navigeer naar deze map. Klik met de rechtermuisknop op dit certificaat en hernoem het: **finessetomcat.csr** 

### Sign Finesecertificaat van CA

In deze sectie, wordt de zelfde Microsoft CA die in de vorige stap wordt gebruikt gebruikt als de derde CA.

**Opmerking:** Zorg ervoor dat de certificaatsjabloon die door CA wordt gebruikt, client- en serververificatie omvat.

Stap 1. Open een webbrowser en navigeer naar de CA.

Stap 2. Selecteer in de Microsoft Active Directory certificaatservices en verzoek een certificaat.

×
Microsoft Active Directory Certificate Services cc-DC-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 <u>Active Directory Certificate Services</u> <u>Documentation</u> .
Select a task: Request a certificate View the status of a pending certificate request Download a CA certificate, certificate chain, or CRL

Stap 3. Selecteer de optie geavanceerde certificaataanvraag zoals in de afbeelding.



Stap 4. Op het **verzoek** van het **geavanceerde certificaat** kopieert en **voegt** u de inhoud van het Fins CSR-certificaat in het vak **Opslaan** aanvraag toe.

Stap 5. Selecteer de Webserversjabloon met client- en serververificatie. In dit lab werd de CC Web Server sjabloon gemaakt met client en server authenticatie.

Microsoft Active	Directory Certificate Services	cc-DC-CA	
Submit a Cert	ificate Request or Renew	val Request	
To submit a say Saved Reques	ved request to the CA, part to the CA, part to the CA, part to the the total to the	Copy and paste the of the expected CS	contents <sup>P</sup> K( R file
Saved Request:			_
Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):	3LhnlD3GsLbIYivb7lbshW gWL/H3DR1nRpJtLKfnLGgX +L3E0yNQ+W9/SJojY2BGnH J75nKDoyAh7C+F0u9tmg26 rArT900dxJem END CERTIFICATE RJ <	fqH1509jMcZ3uZrciC 5kUAZqin/56HjuGb4h k38yoIP/I7UsueE3OR DZaOZ3k9Wo5QzUTPmd EQUESTsna	< >
Certificate Temp	late:		_
L	CC Web Server	$\sim$	
Additional Attribu	utes:		_
Attributes:		A	
		Submit >	-

Stap 6. Klik op Inzenden.

Stap 7. Selecteer Base 64 gecodeerd en klik op Download certificaat zoals in de afbeelding.

Microsoft Active Directory Certificate Services -- cc-DC-CA

Certificate Issued

The certificate you requested was issued to you.

Stap 8. Sla het bestand op en klik op OK. Het bestand wordt opgeslagen in de map Downloads.

Stap 9. Geef het bestand een andere naam aan finesse.cer.

#### FineReader-toepassing- en basiscertificaten importeren

Stap 1. Open pagina van **Finesse OS-**beheerder op een webserver en navigeer naar **Security** >**certificaatbeheer**.

Stap 2. Klik op de knop Upload certificaatketting/certificaat zoals in de afbeelding.

Certificate List	
Generate Self-signed	Upload Certificate/Certificate chain
Certificate List	
Find Certificate List when	re Certificate
Generate Self-signed	Upload Certificate/Certificate chain Generate CSR

Stap 3. Selecteer in het pop-upvenster de optie vertrouwen voor het certificaatdoel.

Stap 4. Klik op de knop **Bladeren...** en selecteer de optie root-certificeringsbestand dat moet worden geïmporteerd. Klik vervolgens op de knop **Openen**.

Stap 5. Schrijf in de beschrijving iets **dat** lijkt op **een** boomstam en klik op de knop **Upload** zoals in de afbeelding.

Upload Certificate/Certific	ate chain	
Upload 🖳 Close		
Status		_
Warning: Uploading a clu	ster-wide certificate will distribute it to all servers in this cluster	
Upload Certificate/Certific	cate chain	_
Certificate Purpose*	tomcat-trust	
Description(friendly name)	tomcatrootcert	
Upload File	Browse rootAll.cer	
Upload Close		_
i *- indicates required ite	ım.	
		>

Stap 6. Wacht tot u het **succes** ziet: **Het geüpload** bericht van het **certificaat** om het venster te sluiten.

U wordt gevraagd het systeem opnieuw te starten, maar eerst moet u het ondertekende certificaat voor de Finse-toepassing uploaden, waarna u het systeem opnieuw kunt opstarten.

🛈 🚯 https://finessea.cc.lat	x8443/cmplatform/certificateUpload.do		. ⊡	☆	≣
Upload Certificate/Certific	ate chain				
Dipload 🖳 Close					
Status Success: Certificate Upl	paded g the CLI command, "utils system restart".				
Upload Certificate/Certific Certificate Purpose* Description(friendly name)	tomcat-trust	v			
Upload File	Browse No file selected.				
Upload Close					
(i) *- indicates required its	ım.				
<					>

Stap 7. Klik op meer tijd op de knop **Upload Certificate/certificaatketen** om het Finse toepassingscertificaat te importeren.

Certificate List	
Generate Self-signed	Upload Certificate/Certificate chain
Certificate List	
Find Certificate List whe	re Certificate 💌 begins with 💌
Generate Self-signed	Upload Certificate/Certificate chain Generate CSR

Stap 8. Selecteer in het pop-upvenster de optie om voor certificaatdoel te kiezen.

Stap 9. Klik op de knop **Bladeren...** en selecteer de optie Finse CA-ondertekend bestand, **finesse.cer**. Klik vervolgens op de knop **Openen**.

Stap 10. Klik op de knop Upload.

			~	
pload Certificate/Certific	ate chain			
Upload 🖳 Close				
Status				_
Warning: Unloading a cl	urter-wide certificate will distribute it to all sequence	in this cluster		
Warning: oploading a ci	uster-wide certificate will distribute it to all servers	in this cluster		
Upload Certificate/Certifi	cate chain			
Certificate Purpose*	tomcat			
Description(friendly_name)	Self-signed certificate			
Description(friendly name) Joload File	Self-signed certificate			

Stap 1. Wacht tot u het succes ziet: certificaatgeüpload.

U wordt opnieuw gevraagd het systeem opnieuw te starten. Sluit het venster en blijf het systeem opnieuw opstarten.

## Verifiëren

Er is momenteel geen verificatieprocedure beschikbaar voor deze configuratie.

## Problemen oplossen

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