Konfigurieren der sicheren Kommunikation zwischen Finesse und CTI-Server

Inhalt

Einführung Voraussetzungen Anforderungen Verwendete Komponenten Hintergrundinformationen Konfiguration **CCE CTI-Server - sicher Finesse Secure Configuration** Agenten-PG-Zertifikat generieren (CTI-Server) CSR-Zertifikat von einer Zertifizierungsstelle signieren lassen Importieren der signierten CCE PGs CA-Zertifikate Finesse-Zertifikat generieren Finesse-Zertifikat von einer Zertifizierungsstelle signieren Importieren von Finesse-Anwendungen und von Root signierten Zertifikaten Überprüfung Fehlerbehebung

Einführung

In diesem Dokument wird beschrieben, wie Zertifikate, die von der Zertifizierungsstelle (Certificate Authority, CA) signiert wurden, zwischen Cisco Finesse und dem Computer Telefony Integration (CTI) Server in der Cisco Contact Center Enterprise (CCE)-Lösung implementiert werden.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- CCE Version 12.0(1)
- Finesse Version 12.0(1)
- CTI-Server

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Softwareversionen:

• Packaged CCE (PCCE) 12.0(1)

• Finesse 12.0(1)

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Hintergrundinformationen

In der CCE-Version 11.5 hat Cisco die Unterstützung von Transport Layer Security (TLS) Version 1.2 eingeführt, mit der Session Initiation Protocol (SIP)- und Real-Time Transport Protocol (RTP)-Nachrichten sicher über TLS 1.2 übertragen werden können. Ab CCE 12.0 und als Teil der Sicherung der übertragenen Daten startete Cisco die Unterstützung von TLS 1.2 für die meisten Callflows im Contact Center: Eingangs- und Ausgangssprachübertragung, Multichannel und Dip für externe Datenbanken. Der Schwerpunkt dieses Dokuments liegt auf der eingehenden Sprachkommunikation, insbesondere der Kommunikation zwischen Finesse und CTI Server.

Der CTI-Server unterstützt die folgenden Verbindungsmodi:

- Sichere Verbindung: Ermöglicht sichere Verbindungen zwischen dem CTI-Server und den CTI-Clients (Finesse, Dialer, CTIOS und ctitest).
- Sichere und nicht gesicherte Verbindung (Mixed-Mode): Ermöglicht gesicherte sowie nicht sichere Verbindungen zwischen dem CTI-Server und den CTI-Clients. Dies ist der Standardverbindungsmodus. Dieser Modus wird konfiguriert, wenn Sie ältere Versionen auf CCE 12.0(1) aktualisieren.

Hinweis: Der ungesicherte Modus wird nicht unterstützt.

Konfiguration

CCE CTI-Server - sicher

Schritt 1: Öffnen Sie auf der PCCE Administrative Workstation (AW) den Ordner **Unified CCE Tools**, und doppelklicken Sie auf **Peripheral Gateway Setup**.



Schritt 2: Wählen Sie CG3A und klicken Sie auf Bearbeiten.

CC Add	Instance Compon	ents
Edit	PG1A PG2A PG3A RouterA	EdR Delete
To set up Administration Data 5 Interface Controller (NIC), Web	Server (Distributor AW), Router View or Network Gateway con	Logger, Network ponents, use the
web setup tool. To set up Administration Client and Setup tool.	(Client AW), use the Administra	tion Client Installer

Schritt 3: Klicken Sie in den CTI-Servereigenschaften auf Weiter. Bei der Frage, ob der CG3A-Dienst durch Setup beendet werden soll, wählen Sie Yes (Ja) aus.

Schritt 4: Wählen Sie in den **Eigenschaften der CTI-Serverkomponenten die Option Sicherer Modus aktivieren aus.** Beachten Sie den **geschützten Verbindungsport (46030)**, da Sie in der nächsten Übung denselben Port in Finesse konfigurieren müssen. Klicken Sie auf **Weiter**.

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

Hinweis: Der Standardwert für die sichere Kommunikation ist 42030. Die für dieses Dokument verwendete Übung ist 40630. Die Portnummer ist Teil einer Formel, die die ICM-System-ID enthält. Wenn die System-ID 1 (CG1a) lautet, lautet die Standardportnummer im Allgemeinen 42030. Da die System-ID im Labor 3 (CG3a) lautet, lautet die Standard-Portnummer 46030.

Schritt 5: Klicken Sie in den CTI-Netzwerkschnittstelleneigenschaften auf Weiter. Überprüfen Sie die Setup-Informationen, und klicken Sie auf Weiter.

Unified ICM/CCE PGSet	up: cc-CG3A
Check Setup Information	
Setup has enough information to begin the configurati If you want to review or change and of the settings, o If satisfied, click Next to begin configuring the CTI Gab	on operation. dick Back. seway.
Current Settings:	
Setup Type: CTI Gateway, side A	<u>^</u>
Target Directory: C:'jicm	=
Configuration: PG node is pccealin1p CTI Gateway is simplexed DMP address is 3	
<	>
	jack Njexit > Cancel

Schritt 6: Klicken Sie auf Fertig stellen wie im Bild gezeigt.

Unifie	ed 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. Yes, start the Unified ICM/CC Node Manager Click Finish to Complete Setup.
	< Back Finish Cancel

Schritt 7: Klicken Sie auf **Setup beenden** und warten Sie, bis das Setup-Fenster wie im Bild gezeigt geschlossen wird.

ICM Instances	Instance Compo	nents
ee 🖉	Add 0524	Add
	LoggerA	
	Edit PG1A	Edit
	PG3A	
	Delete RouteA	Delete
o set up Administration I nterface Controller (NIC). Veh Satur tool	Data Server (Distributor AW), Route WebView or Network Gateway co	r, Logger, Network mponents, use the
To set up Administration I Interface Controller (NIC), Veb Setup tool. To set up Administration (and Setup tool.	Data Server (Distributor AW), Route WebView or Network Gateway co Client (Client AW), use the Administ	r, Logger, Network mponents, use the ation Client Installer
To set up Administration I nterface Controller (NIC), Web Setup tool. To set up Administration (and Setup tool. The Instance cc cannot I Web Setup or Administrat o remove those compon ietup.	Data Server (Distributor AW), Route WebView or Network Gateway co Client (Client AW), use the Administ be deleted because it has compone tion Client Setup tool. You must use ents before deleting the instance in	r, Logger, Network mponents, use the ation Client Installer ents set up by the the applicable tool Peripheral Gateway

Schritt 8: Doppelklicken Sie auf dem Desktop PCCEAllin1 auf Unified CCE Service Control.

Schritt 9: Wählen Sie Cisco ICM cc CG3A aus, und klicken Sie auf Start.

Finesse Secure Configuration

Schritt 1: Öffnen Sie einen Webbrowser, und navigieren Sie zu Finesse Administration.

Schritt 2: Blättern Sie nach unten zum Abschnitt **Contact Center Enterprise CTI Server Settings** wie im Bild gezeigt.

Contact Center Enter	erprise CTI Server Se	ettings	
Note: Any changes made to Contact Center Enterpris	the settings on this gadget in ie 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*	42027	B Side Port	
Peripheral ID*	5000		
Enable SSL encryption Save Rever	٩		

Schritt 3: Ändern Sie den A-seitigen Port für den sicheren Kommunikationsport, der in der vorherigen Übung auf CG3A konfiguriert wurde: **46030.** Aktivieren Sie **SSL-Verschlüsselung aktivieren** und klicken Sie auf **Speichern**.

Contact Center Ent	erprise CTI Server S	ettings	
Note: Any changes made to Contact Center Enterpris	the settings on this gadget is se CTI Server Settings	require a restart of Cisco Finesse Torncat to	take effect.
A Side Host/IP Address*	10.10.10.10	8 Side Host/IP Address	
A Side Port*	46030	B Side Port	
Peripheral ID*	5000		
Enable SSL encryption	rt		

Hinweis: Um die Verbindung zu testen, müssen Sie den Finesse Tomcat Service zuerst neu starten oder den Finesse-Server neu starten.

Schritt 4: Melden Sie sich von der Finesse Administration-Seite ab.

Schritt 5: Öffnen Sie eine SSH-Sitzung mit Finesse.

Schritt 6: Führen Sie in der FINESSEA SSH-Sitzung den folgenden Befehl aus:

utils system restart

Geben Sie yes ein, wenn Sie gefragt werden, ob Sie das System neu starten möchten.

```
<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...
```

Agenten-PG-Zertifikat generieren (CTI-Server)

CiscoCertUtils ist ein neues Tool, das auf der CCE-Version 12 veröffentlicht wurde. Sie verwenden dieses Tool, um alle CCE-Zertifikate für eingehende Sprachanrufe zu verwalten. In

diesem Dokument verwenden Sie diese CiscoCertUtils, um CSRs (Peripheral Gateways) zu generieren.

Schritt 1: Führen Sie diesen Befehl aus, um ein CSR-Zertifikat zu generieren: **CiscoCertUtil** /generateCSR



Stellen Sie die angeforderten Informationen bereit, z. B.:

Ländername: USA

Bundesland/Region Name: MA

Ortsname: BXB

Name der Organisation: Cisco

Organisationseinheit: CX

Common Name: PCCEAllin1.cc.la

E-Mail: jdoe@cc.lab

Ein Challenge-Kennwort: Zug 1ng!

Optionaler Firmenname: Cisco

Das Hostzertifikat und der Hostschlüssel werden in C:\icm\ssl\certs und C:\icm\ssl\keys gespeichert.

Schritt 2: Navigieren Sie zum Ordner C:\icm\ssl\certs, und stellen Sie sicher, dass die Datei host.csr generiert wurde.

CSR-Zertifikat abrufen Unterzeichnet durch eine Zertifizierungsstelle

Nachdem die CSR-Zertifikate generiert wurden, müssen sie von einer Zertifizierungsstelle eines Drittanbieters signiert werden. In dieser Übung wird die im Domänencontroller installierte Microsoft CA als Drittanbieter-CA verwendet.

Stellen Sie sicher, dass die von der CA verwendete Zertifikatsvorlage die Client- und Serverauthentifizierung enthält, wie im Bild gezeigt, wenn die Microsoft CA verwendet wird.

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 X
Certificate Template Information Issuance Policies Key Usage Edt	Application policies:	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. Application policies:
Description of Application Policies:	Add	Certificate Request Agent Certificate Request Agent Citent Archentication Code Signing CTL Usage Digital Rights Directory Service Email Replication Disallowed List Document Encryption Document Signing Domain Name System (DNS) Server Trust Dynamic Code Generator New OK Cancel
	L	

Schritt 1: Öffnen Sie einen Webbrowser, und navigieren Sie zur CA.

Schritt 2: Wählen Sie in den Microsoft Active Directory-Zertifikatsdiensten die Option Zertifikat anfordern aus.

- D X
C C Attps://dc.ec.lab/certani/en-us/ D * 🗟 C Attree Directory × 0 🛣 C
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> Documentation.
Select a task: Request a certificate View the status of a pending certificate request Download a CA certificate, certificate chain, or CRL

Schritt 3: Wählen Sie die Option Erweiterte Zertifikatsanforderung aus.

Mici	rosoft Activ	e Directory Ce	ertifical × +				
\leftrightarrow	С°Ш		🛈 윮 https://dca	c.lab/certsrv/en	-us/certr	qus.asp	
CUCM	🛅 CUIC	🛅 Finesse	🛅 Remote Expert Mobile	🛅 MediaSense	CVP	CCE	
Microsoft	Active Dir	ectory Certifi	cate Services cc-DC-	CA			
Request	a Certif	icate					
							_
Select th	e certific Certificat	ate type:					_

Schritt 4: Kopieren Sie auf die **erweiterte Zertifikatsanforderung** den Inhalt des PG Agent CSR-Zertifikats und fügen Sie ihn in das Feld **Gespeicherte Anforderung ein**.

Schritt 5: Wählen Sie die **Webserver-**Vorlage mit Client- und Serverauthentifizierung aus. In der Übung wurde die CC-Webserver-Vorlage mit Client- und Serverauthentifizierung erstellt.

To submit a sav Saved Request	ved request to the CA, part box.	Copy and paste the of the expected CS	e contents R file
Saved Request:			_
Base-64-encoded certificate request CMC or PKCS #10 or PKCS #7):	3Lhn1D3GsLbIYivb7lbshWs gWL/H3DR1nRpJtLKfnLGgX5 +L3E0yNQ+W9/SJojYzBGnHx J75nKDoyAh7C+F0u9tmg261 rArT90OdxJem END CERTIFICATE RE <	rqH1509jMcZ3uZrciC SkUAZqin/56HjuGb4h c38yo1P/I7UsueE3OR SZaOZ3k9Wo5QzUTPmd CQUESTsna	•
Certificate Templ	ate:		
	CC Web Server	~	_
Additional Attribu	ites:		
Attributes:			_

Schritt 6: Klicken Sie auf Senden.

Schritt 7: Wählen Sie **Base 64-verschlüsselt aus** und klicken Sie auf **Zertifikat herunterladen** wie im Bild gezeigt.

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

Certificate Issued

The certificate you requested was issued to you.

○ DER encoded or ● Base 64 encoded

ь.	-	-		5
N,	a	6	Ċ,	à
	~	c,	~	P
м.	-	-		

Download certificate Download certificate chain

Schritt 8: Speichern Sie die Datei, und klicken Sie auf **OK**. Die Datei wird im Ordner **Downloads** gespeichert.

Schritt 9: Benennen Sie die Datei in host.cer um (optional).

Schritt 10: Sie müssen auch ein Stammzertifikat generieren. Rufen Sie die Zertifizierungsstellenseite des Zertifizierungsstellers auf, und wählen Sie dann **Zertifizierungsstellenkette, Zertifikatskette oder CRL herunterladen aus**. Sie müssen diesen Schritt nur einmal durchführen, da das Root-Zertifikat für alle Server (PG Agent und Finesse) gleich sein wird.



Schritt 11: Klicken Sie auf **Base 64** und wählen Sie **Zertifizierungsstellenzertifikat herunterladen aus**.

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-Dict.CA)
Encoding method:
ODER ⊛Base 64
Install CA certificate
Download CA certificate
Download CA certificate chain
Download latest base CRL
Download latest delta CRL

Schritt 12: Klicken Sie auf "Datei speichern" und wählen Sie **OK aus**. Die Datei wird im Standardspeicherort **Downloads** gespeichert.

Importieren der signierten CCE PGs CA-Zertifikate

Schritt 1: Navigieren Sie auf dem PG-Agenten zu C:\icm\ssl\certs und fügen Sie den Stamm und die PG-Agent signierten Dateien hier ein.

Schritt 2: Benennen Sie das host.pem-Zertifikat auf c:\icm\ssl\certs als selfhost.pem um.

Schritt 3: Umbenennen Sie host.cer in host.pem im Ordner c:\icm\ssl\certs .

Schritt 4: Installieren Sie das Stammzertifikat. Geben Sie an der Eingabeaufforderung den folgenden Befehl ein: CiscoCertUtil /install C:\icm\ssl\certs\rootAll.cer



Schritt 5: Installieren Sie das von der Anwendung signierte Zertifikat, das denselben Befehl ausführt: **CiscoCertUtil /install C:\icm\ssl\certs\host.pem**



Schritt 6: Schalten Sie den PG aus. Öffnen Sie die Unified CCE Service Control, und starten Sie den Cisco ICM Agent PG aus.

Finesse-Zertifikat generieren

Schritt 1: Öffnen Sie den Webbrowser, und navigieren Sie zu Finesse OS Admin.

Schritt 2: Melden Sie sich mit den Anmeldeinformationen für OS Admin an, und navigieren Sie zu **Security > Certificate Management (**Verwaltung des **Zertifikats**), wie im Bild gezeigt.



Schritt 3: Klicken Sie auf CSR erstellen wie im Bild gezeigt.



Schritt 4: Verwenden Sie auf der Anforderung zur Signierung von Zertifikaten generieren die Standardwerte, und klicken Sie auf Generieren.

Status Status Warning: Generating a new CSR for a specific certificate type will overwrite th Generate Certificate Signing Request Certificate Purpose** Distribution* FINESSEA.cc.lab Subject Harmon (SAN)	e existing CSR for that type
Status Warning: Generating a new CSR for a specific certificate type will overwrite th Generate Certificate Signing Request Certificate Purpose** Itomcat Distribution* FINESSEA.cc.lab Common Name* FENESSEA.cc.lab	e existing CSR for that type
Status Warning: Generating a new CSR for a specific certificate type will overwrite th Generate Certificate Signing Request Certificate Purpose** Instribution* FENESSEA.cc.lab Common Name* FENESSEA.cc.lab	e existing CSR for that type
Warning: Generating a new CSR for a specific certificate type will overwrite th Generate Certificate Signing Request Certificate Purpose** Distribution* FINESSEA.cc.lab Common Name* FENESSEA.cc.lab Common Name* FENESSEA.cc.lab	e existing CSR for that type
Generate Certificate Signing Request Certificate Purpose** [tomcat.v] Distribution* [FINESSEA.cc.lab Common Name* [FINESSEA.cc.lab School Alternatio Names (School)	
Certificate Purpose** tomcat V Distribution* FINESSEA.cc.lab V Common Name* FINESSEA.cc.lab	
Common Name* FINESSEA.cc.lab v	
Common Name* FINESSEA.cc.lab	
Cubiart Alternate Names (CANo)	
Subject Alternate names (SANS)	
Parent Domain cc.lab	
Key Type** RSA	
Key Length* 2048 v	
Hash Algorithm* SHA256 🗸	

Schritt 5: Schließen Sie das Fenster Signaturanforderung für Zertifikat generieren, und wählen Sie

CSR herunterladen aus.

Show * Settings	Security *	Software Upgrades *	Services *	Help *		
Certificate List						
Generate Set	r-signed D	oload Certificate/Certificate	chain 💽	Generate CSR	Download CSR	

Schritt 6: Wählen Sie im Feld Zertifikatzweck die Option **tomcat aus**, und klicken Sie auf **CSR herunterladen**.

Download Certificate Signing Request	
Download CSR 🔄 Close	
Certificate names not listed below do not have a corresponding CSR.	
Download Certificate Signing Request	
Certificate Purpose* tomcat	
Download CSR Close	_
 indicates required item. 	
c .	>

Schritt 7: Wählen Sie Datei speichern und klicken Sie auf OK, wie im Bild gezeigt.

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

Schritt 8: Schließen Sie das Fenster **Download Certificate Signing Request**. Das Zertifikat wird im Standardspeicherort gespeichert (**Dieser PC > Downloads**).

Schritt 9: Öffnen Sie Windows Explorer, und navigieren Sie zu diesem Ordner. Klicken Sie mit der rechten Maustaste auf dieses Zertifikat, und benennen Sie es um: **finessetomcat.csr**

Finesse-Zertifikat von einer Zertifizierungsstelle signieren

In diesem Abschnitt wird dieselbe Microsoft-CA verwendet, die im vorherigen Schritt verwendet wurde, wie die Drittanbieter-CA.

Hinweis: Stellen Sie sicher, dass die von der CA verwendete Zertifikatsvorlage die Clientund Serverauthentifizierung enthält.

Schritt 1: Öffnen Sie einen Webbrowser, und navigieren Sie zur CA.

Schritt 2: Wählen Sie in den Microsoft Active Directory-Zertifikatsdiensten die Option Zertifikat anfordern aus.

X
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> Documentation.
Select a task: Request a certificate View the status of a pending certificate request Download a CA certificate, certificate chain, or CRL

Schritt 3: Wählen Sie die Option Erweiterte Zertifikatsanforderung wie im Bild gezeigt aus.

Micr	osoft Activ	e Directory Ce	ertifical × +				
\leftrightarrow	C'û		🛈 윮 https://dc/	cc.lab/certsrv/en	-us/certr	qus.asp	
🗎 СИСМ	🛅 CUIC	🛅 Finesse	Remote Expert Mobile	🛅 MediaSense	CVP	CCE	
Microsoft	Active Dire	ectory Certifi	icate Services cc-DC-	CA			
Doguost							
Request	a Certif	icate					_
Select the	e certific	ate type:					_

Schritt 4: Kopieren Sie auf die **erweiterte Zertifikatsanforderung** den Inhalt des Finesse CSR-Zertifikats und fügen Sie ihn in das Feld **Gespeicherte Anforderung ein**.

Schritt 5: Wählen Sie die Webservervorlage mit Client- und Serverauthentifizierung aus. In dieser Übung wurde die CC-Webserver-Vorlage mit Client- und Serverauthentifizierung erstellt.

Microsoft Active Directory Certificate Services - cc-DC-CA					
Submit a Certificate Request or Renewal Request					
To submit a say Saved Reques	ved request to the CA, part t box.	Copy and paste the of the expected CS	e contents ^{PK(} SR file		
Saved Request:	/		_		
Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):	3LhnlD3GsLbIYivb7IbshW gWL/H3DR1nRpJtLKfnLGgX +L3E0yNQ+W9/SJojY2BGnH J75nRDoyAh7C+F0u9tmg26 rArT900dxJem END CERTIFICATE R <	fqH1509jMcZ3uZrciC 5kUAZqin/56HjuGb4h k38yo1P/I7UsueE3OR DZaOZ3k9Wo5QzUTPmd EQUESTsna	•		
Certificate Temp	late:		_		
C	CC Web Server	~			
Additional Attribution	utes:		_		
Attributes:		.a			
		Submit >	_		

Schritt 6: Klicken Sie auf Senden.

Schritt 7: Wählen Sie **Base 64-verschlüsselt aus**, und klicken Sie auf **Zertifikat herunterladen**, wie im Bild gezeigt.

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

Certificate Issued

The certificate you requested was issued to you.

ODER encoded or
Base 64 encoded
Download certificate
Download certificate chain

Schritt 8: Speichern Sie die Datei, und klicken Sie auf **OK**. Die Datei wird im Ordner **Downloads** gespeichert.

Schritt 9: Benennen Sie die Datei in finesse.cer um.

Importieren von Finesse-Anwendungen und von Root signierten Zertifikaten

Schritt 1: Öffnen Sie auf einem Webproser die **Finesse OS Admin-**Seite, und navigieren Sie zu **Security > Certificate Management**.

Schritt 2: Klicken Sie auf die Schaltfläche Zertifikat/Zertifikat hochladen, wie im Bild gezeigt.

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

Schritt 3: Wählen Sie im Popup-Fenster tomcat-trust für Zertifikatzweck aus.

Schritt 4: Klicken Sie auf die Schaltfläche **Durchsuchen.** und wählen Sie die zu importierende Stammzertifikatdatei aus. Klicken Sie anschließend auf die Schaltfläche **Öffnen**.

Schritt 5: In der Beschreibung schreiben Sie etwas wie **tomcatrootcert** und klicken Sie auf **Upload** Schaltfläche wie im Bild gezeigt.

Upload Certificate/Certific	ate chain	
Dipload 🖳 Close		
Status Warning: Uploading a clo Upload Certificate/Certific	uster-wide certificate will distribute it to all servers in this cluster	
Certificate Purpose* Description(friendly name)	tomcatrostcert	
Upload File	Browse rootAll.cer	
Upload Close		=
(i) *- indicates required ite	im.	
¢		>

Schritt 6: Warten Sie, bis Sie den **Erfolg** sehen: Meldung **hochgeladenes Zertifikat** zum Schließen des Fensters

Sie werden gebeten, das System neu zu starten, aber fahren Sie zuerst mit dem Hochladen des Zertifikats der Finesse-Anwendung fort, und dann können Sie das System neu starten.

③ ▲ https://finessea.cc.lab:8443/cmplatform/certificateUpload.do		${igsidential}$	☆	≡
Upload Certificate/Certificate chain				
Depose 🖳 Close				
Status Success: Certificate Uploaded Restart the node(s) using the CLI command, "utils system restart".				
Upload Certificate/Certificate chain Certificate Purpose* tomcat-trust Description(friendly name)	~			
Upload Close •- indicates required item.				
(>

Schritt 7: Klicken Sie auf die Schaltfläche **Zertifikat/Zertifikatskette hochladen**, um das Finesse-Anwendungszertifikat zu importieren.

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

Schritt 8: Wählen Sie im Popup-Fenster **tomcat** for **Certificate Purpose (Tomcat** für **Zertifikatszwecke)** aus.

Schritt 9: Klicken Sie auf die Schaltfläche **Browse...** und wählen Sie die von Finesse CA signierte Datei **finesse.cer aus**. Klicken Sie anschließend auf die Schaltfläche **Öffnen**.

Schritt 10: Klicken Sie auf die Schaltfläche Hochladen.

Ittps://finessea.cc.lab	b:8443/cmplatform/certificateUpload.do	🗵 1	☆ ≡
pload Certificate/Certific	ate chain		
👌 Upload 🛛 🖳 Close			
Status Warning: Uploading a cl	uster-wide certificate will distribute it to all servers	in this cluster	
Upload Certificate/Certifi	cate chain		
Upload Certificate/Certifi Certificate Purpose	tomcat	~	
Upload Certificate/Certifi Certificate Purpose* Description(friendly name)	tomcat Self-signed certificate	v	

Schritt 11: Warten Sie, bis Sie den Erfolg sehen: Hochgeladenes Zertifikat.

Sie werden erneut aufgefordert, das System neu zu starten. Schließen Sie das Fenster, und fahren Sie mit dem Neustart des Systems fort.

Überprüfung

Für diese Konfiguration ist derzeit kein Überprüfungsverfahren verfügbar.

Fehlerbehebung

Für diese Konfiguration sind derzeit keine spezifischen Informationen zur Fehlerbehebung verfügbar.