Configure Secure Communication Between Finesse and CTI Server

Contents

Introduction **Prerequisites** Requirements **Components Used Background Information Configure CCE CTI Server Secure Finesse Secure Configuration** Generate Agent PG Certificate (CTI Server) Get the CSR Certificate Signed by a CA Import the CCE PGs CA Signed Certificates **Generate Finesse Certificate** Sign Finesse Certificate by a CA Import Finesse Application and Root Signed Certificates Verify **Troubleshoot**

Introduction

This document describes how to implement Certificate Authority (CA) signed certificates between Cisco Finesse and Computer Telephony Integration (CTI) Server in Cisco Contact Center Enterprise (CCE) solution.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

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

Components Used

The information in this document is based on these software versions:

• Packaged CCE (PCCE) 12.0(1)

• Finesse 12.0(1)

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

In CCE version 11.5 Cisco started the support of Transport Layer Security (TLS) version 1.2, which allows Session Initiation Protocol (SIP) and Real-time Transport Protocol (RTP) messages to be transported securely via TLS 1.2. From CCE 12.0 and as part of securing the data in motion, Cisco started the support of TLS 1.2 on most of the contact centre call flows: Inbound and Outbound voice, Multi-channel, and External database dip. The focus of this document is inbound voice, especially the communication between Finesse and CTI Server.

The CTI Server supports these modes of connections:

- Secured-Only Connection: Allows secured connection between the CTI Server and the CTI clients (Finesse, dialer, CTIOS and ctitest).
- Secured and Non-Secured Connection (Mixed-mode): Allows secured, as well as the nonsecure connection between the CTI Server and the CTI clients. This is the default connection mode. This mode will be configured when you upgrade previous releases to CCE 12.0(1).

Note: Non-secured only mode is not supported.

Configure

CCE CTI Server Secure

Step 1. On the PCCE Administrative Workstation (AW), open the **Unified CCE Tools** folder and double-click on **Peripheral Gateway Setup**.



Step 2. Select CG3A and click on Edit.

Cisco Unified ICM/Contact Ce	enter Enterprise Components Setup
ICM Instances Add Edit	Instance Components Add PG1A PG2A PG3A RoutesA Delete Delete Delete W]. use the Administration Client Installer cause it has components set up by the up tool. You must use the applicable tool leteing the instance in Peripheral Gateway
	Help Exit Setup

Step 3. On the CTI server properties, click **Next**. On the question about setup stopping the **CG3A** service, select **Yes**.

Step 4. On the **CTI Server Components Properties**, select **Enable Secured-only mode.** Note the **Secured Connection Port (46030)**, since you have to configure the same port in Finesse in the next exercise. Click **Next**.

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

Note: The default secure communication is 42030, however, the lab used for this document is 40630. The port number is part of a formula that includes the ICM system ID. When the system id is 1 (CG1a) the default port number, in general, is 42030. Since the system id in the lab is 3 (CG3a) the default port number is 46030.

Step 5. On the **CTI Network Interface Properties**, click **Next**. Check the **Setup Information** and click **Next**.



Step 6. Click on **Finish** as shown in the image.

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

Step 7. Click on **Exit Setup** and wait until the setup window closes as shown in the image.

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). Veb Satura 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

Step 8. On the PCCEAllin1 desktop, double-click on Unified CCE service Control.

Step 9. Select Cisco ICM cc CG3A and click on Start.

Finesse Secure Configuration

Step 1. Open a web browser and Navigate to Finesse Administration.

Step 2. Scroll down to the section **Contact Center Enterprise CTI Server Settings** as shown in the image.

Contact Center Enterprise CTI Server Settings				
Note: Any changes made to the settings on this gadget require a restart of Cisco Finesse Torncat to take effect. Contact Center Enterprise CTI Server Settings				
A Side Host/IP Address*	10.10.10.10	B Side Host/IP Address		
A Side Port*	42027	8 Side Port		
Peripheral ID*	5000			
Enable SSL encryption Save Reve	rt 🗌			

Step 3. Change the A side port for the secure communication port configured on CG3A in the previous exercise: **46030**. Check **Enable SSL encryption** and click **Save**.

Contact Center Ent	erprise CTI Server S	ettings	
Note: Any changes made to Contact Center Enterpris	o the settings on this gadget r 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		

Note: In order to test the connection, you need to restart Finesse Tomcat Service first or restart the Finesse server.

Step 4. Sign out from the Finesse Administration page.

Step 5. Open an SSH session with Finesse.

Step 6. On the FINESSEA SSH session, execute the command:

utils system restart

Enter **yes** when asked if you want to restart the system.

```
<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 Certificate (CTI Server)

The CiscoCertUtils is a new tool released on CCE Version 12. You use this tool to manage all CCE certificates for inbound voice. In this document, you use these CiscoCertUtils in order to

generate the Peripheral Gateways (PGs) Certificate Signing Requests (CSRs).

Step 1. Execute this command to generate a CSR certificate: CiscocertUtil /generateCSR



Provide the information requested, like for example:

Country Name: US

State or Province Name: MA

Locality Name: BXB

Organization Name: Cisco

Organizational Unit: CX

Common Name: PCCEAllin1.cc.lab

Email: jdoe@cc.lab

A Challenge password: Train1ng!

An optional company name: Cisco

The host certificate and key are stored in C:\icm\ssl\certs and C:\icm\ssl\keys.

Step 2. Navigate to C:\icm\ssl\certs folder and ensure that the file host.csr has been generated.

Get the CSR Certificate Signed by a CA

After the CSR certificates are generated, they need to be signed by a third-party CA. In this exercise, Microsoft CA installed in the Domain Controller is used as the third-party CA.

Ensure that the certificate template used by the CA includes client and server authentication as shown in the image when Microsoft CA is used.

Properties of New Template	pns	
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 F	(DC.cc.lab)
Application Policies Basic Constraints	An application policy defi	Add Application Policy
Key Usage	Application policies: Server Authentication	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.
Edt Description of Application Policies:	Add	Any Pupose Attestation Identity Key Certificate Certificate Request Agent Citent Authentication Code Signing CTL Usage Digital Rights Directory Service Email Replication Disallowed List Document Signing Domain Name System (DNS) Server Trust Dynamic Code Generator New
OK Cancel Apply Help	L	UK Cancel

Step 1. Open a web browser and navigate to the CA.

Step 2. On the Microsoft Active Directory Certificate Services, select Request a certificate.

	×
🗲 🕑 🖉 https://dc.ec.hab/certsiv/en-us/ 🖉 🖉 🖉 Microsoft Active Directory × 🕠 🔿	10
Microsoft Active Directory Certificate Services - cc-DC-CA H	lome
Welcome	
Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using 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.	a
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 Service</u> Documentation.	15
Select a task: Request a certificate View the status of a pending certificate request Download a CA certificate, certificate chain, or CRL	

Step 3. Select the **advanced certificate request** option.

Micr	osoft Activ	e Directory Ce	ertifical × +				
\leftrightarrow	C'û		🛈 🐔 https://do	cc.lab/certsrv/en	-us/certr	qus.asp	
🗎 СИСМ	🛅 CUIC	🛅 Finesse	🛅 Remote Expert Mobile	🗎 MediaSense	CVP	CCE CCE	
Microsoft	Active Dire	ectory Certifi	cate Services - cc-DC	CA			
Request	a Certif	icate					
Select the User C	e certific Certificat	ate type:					
Or, subm	it an <u>adv</u>	anced cer	rtificate request.				

Step 4. On the **advanced certificate request**, copy and paste the content of the PG Agent CSR certificate in the **Saved Request** box.

Step 5. Select the **Web Server** template with client and server authentication. In the lab, the CC Web Server template was created with client and server authentication.

To submit a sav Saved Reques	ved request to the CA, part t box.	Copy and paste the of the expected C	e contents SR file
Saved Request:			_
Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):	3LhnlD3GsLbIYivb7IbshW gWL/H3DR1nRpJtLKfnLGgX +L3E0yNQ+W9/SJojYzBGnH J75nKDoyAh7C+F0u9tmg26 rArT900dxJem END CERTIFICATE R <	fqH1509jMcZ3uZrci0 5kUAZqin/56HjuGb4 k38yo1P/I7UsueE30F DZaOZ3k9Wo5QzUTPmc EQUESTsna	
Certificate Temp	late:		
Ĺ	CC Web Server	~	
Additional Attribu	ites:		
Attributes:			_

Step 6. Click on Submit.

Step 7. Select **Base 64 encoded** and click on **Download Certificate** as shown in the image.

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

Step 8. Save the file and click **OK**. The file is saved in the **Downloads** folder.

Step 9. Rename the file to host.cer (optional).

Step 10. You also need to generate a root certificate. Go back to the CA certificate page and then select **Download a CA certificate, certificate chain, or CRL**. You just need to do this step once, since the root certificate will be the same for all the servers (PG Agent and Finesse).

Microsoft Active Directory Certificate Services cc-DC-CA
Welcome
Use this Web site to request a certificate for your Web browser, ε people you communicate with over the Web, sign and encrypt mesecurity 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>

Step 11. Click on Base 64 and select Download CA certificate.

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

Step 12. Click on Save File and select **OK**. The file will be saved in the default location, **Downloads**.

Import the CCE PGs CA Signed Certificates

Step 1. On the PG Agent navigate to C:\icm\ssl\certs and paste the root and the PG Agent signed files here.

Step 2. Rename the host.pem certificate on c:\icm\ssl\certs as selfhost.pem.

Step 3. Rename host.cer to host.pem on c:\icm\ssl\certs folder.

Step 4. Install the root certificate. On the command prompt, issue this command: CiscoCertUtil /install C:\icm\ssl\certs\rootAll.cer



Step 5. Install the application signed certificate running the same command: **CiscoCertUtil** /install C:\icm\ssl\certs\host.pem



Step 6. Cycle the PG. Open the Unified CCE Service Control, and cycle the Cisco ICM Agent PG.

Generate Finesse Certificate

Step 1. Open the web browser and navigate to Finesse OS Admin.

Step 2. Log in with OS Admin credentials and navigate to **Security > Certificate Management** as shown in the image.



Step 3. Click on Generate CSR as shown in the image.



Step 4. On the **Generate Certificate Signing Request**, use the default values, and click on **Generate.**

Generate 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**	tomcet v
Distribution*	FINESSEA.cc.lab v
Common Name*	FINESSEA.cc.lab
Subject Alternate Nat	mes (SANs)
Parent Domain	cc.lab
Key Type**	RSA
Key Length*	2048 v
Hash Algorithm*	SHA256 V
Generate Close	
@	
· indicates require	ed Rem.
is RSA.	icate Purpose ending with '-ECDSA' is selected, the certificate/key type is Elliptic Curve (EC). Otherwise, it

Step 5. Close the Generate Certificate Signing Request window and select Download CSR.

Show * Settings *	Security *	Software Upgrades *	Services *	Help *		
Certificate List						
Generate Self-signe	nd 🐴 Up	load Certificate/Certificate	chain 📳	Generate CSR	Download CSR	

Step 6. On the Certificate Purpose, select tomcat and click on Download CSR.

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

Step 7. Select **Save File** and click on **OK** as shown in the image.

Opening tomcat.csr		×
You have chosen to	open:	
tomcat.csr	5 1-	
from: https://	rile /finessea.cc.lab:8443	
What should Firefo	ox do with this file?	
O Open with	Browse	
Save File		
Do this autor	matically for files like this from now on.	
	OK Cancel	

Step 8. Close the **Download Certificate Signing Request** window. The certificate is saved in the default location (This PC > Downloads).

Step 9. Open Windows Explorer and navigate to that folder. Right-click on this certificate and rename it: **finessetomcat.csr**

Sign Finesse Certificate by a CA

In this section, the same Microsoft CA used in the previous step is used as the third-party CA.

Note: Ensure that the certificate template used by the CA includes client and server

authentication.

Step 1. Open a web browser and navigate to the CA.

Step 2. On the Microsoft Active Directory Certificate Services, select Request a certificate.



Step 3. Select the **advanced certificate request** option as shown in the image.



Step 4. On the **advanced certificate request**, copy and paste the content of the Finesse CSR certificate in the **Saved Request** box.

Step 5. Select the Web server template with client and server authentication. In this lab, the CC Web Server template was created with client and server authentication.

Microsoft Active	Directory Certificate Services	cc-DC-CA	
Submit a Cert	ificate Request or Renew	val Request	
To submit a sa Saved Reques	ved request to the CA, part to the CA, part to the CA, part to the the total to the the the total tota	Copy and paste the of the expected CS	e contents ^P 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:		_
C	CC Web Server	~	
Additional Attrib	utes:		_
Attributes:		a	
		Submit >	-

Step 6. Click on Submit.

Step 7. Select **Base 64 encoded** and click on **Download certificate** as shown in the image.

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

Certificate Issued

The certificate you requested was issued to you.

Step 8. Save the file and click **OK**. The file is saved in the **Downloads** folder.

Step 9. Rename the file to **finesse.cer**.

Import Finesse Application and Root Signed Certificates

Step 1. On a web proser open **Finesse OS Admin** page and navigate to **Security** > **Certificate Management**.

Step 2. Click on the **Upload Certificate/Certificate chain** button as shown in the image.

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

Step 3. In the pop-up window select tomcat-trust for Certificate Purpose.

Step 4. Click on the **Browse...** button and select the root certificate file to import. Then, click the **Open** button.

Step 5. In the description write something like **tomcatrootcert** and click on **Upload** button as shown in the image.

Upload Certificate/Certific	ate chain	
🕒 Upload 🖳 Close		
Status Warning: Uploading a clu	uster-wide certificate will distribute it to all servers in this cluster	
Upload Certificate/Certifi	cate chain	٦
Certificate Purpose*	tomcat-trust	
Upload File	Browse rootAll.cer	
Upload Close		_
(i) *- indicates required ite	im.	
c		>

Step 6. Wait until you see the **Success: Certificate Uploaded** message to close the window.

You will be requested to restart the system, but first, continue with uploading the Finesse application signed certificate, and then you can restart the system.

🛈 🔏 https://finessea.cc.lab	:8443/cmplatform/certificateUpload.do		☆	≡
Upload Certificate/Certifica	ite chain			
Dipload 🖳 Close				
Status Success: Certificate Uplo Restart the node(s) using	aded ; the CLI command, "utils system restart".		 	
Upload Certificate/Certific	ate chain			_
Certificate Purpose*	tomcat-trust	~		
Description(friendly name) Upload File	Browse No file selected.			
Upload Close				
(i) *- indicates required ite	m.			
¢				>

Step 7. Click on more time on **Upload Certificate/Certificate chain** button in order to import the Finesse application certificate.

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

Step 8. In the pop-up window select **tomcat** for **Certificate Purpose**.

Step 9. Click on the **Browse...** button and select the Finesse CA signed file, **finesse.cer**. Then, click the **Open** button.

Step 10. Click on the **Upload** button.

pload Certificate/Certific	ate chain		
Upload 🖳 Close			
Status			
Status Warning: Uploading a clu Upload Certificate/Certifi	uster-wide certificate will distribute it to all servers	in this cluster	
Status Warning: Uploading a cli Upload Certificate/Certific Certificate Purpose*	uster-wide certificate will distribute it to all servers i	in this cluster	
Status Warning: Uploading a clu Upload Certificate/Certific Certificate Purpose [®] Description(friendly name)	uster-wide certificate will distribute it to all servers i cate chain tomcat Self-signed certificate	in this cluster	

Step 11. Wait until you see the Success: Certificate Uploaded message.

Again, you are requested to restart the system. Close the window and continue to restart the system.

Verify

There is currently no verification procedure available for this configuration.

Troubleshoot

There is currently no specific troubleshooting information available for this configuration.