Configurazione di comunicazioni protette tra Finesse e il server CTI

Sommario

Introduzione **Prerequisiti** Requisiti Componenti usati Premesse **Configurazione CCE CTI Server Secure Finesse Secure Configuration** Genera certificato PG agente (server CTI) Ottenere il certificato CSR firmato da una CA Importa certificati firmati CA CCE PG Genera certificato Finesse Firma certificato Finesse da una CA Importa certificati firmati radice e applicazione Finesse Verifica Risoluzione dei problemi

Introduzione

In questo documento viene descritto come implementare i certificati firmati da CA (Certification Authority) tra Cisco Finesse e Computer Telephony Integration (CTI) Server nella soluzione Cisco Contact Center Enterprise (CCE).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

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

Componenti usati

Le informazioni di questo documento si basano sulle seguenti versioni software:

• Packaged CCE (PCCE) 12.0(1)

• Finesse 12.0(1)

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

Nella versione 11.5 di CCE, Cisco ha iniziato a supportare la versione 1.2 di Transport Layer Security (TLS), che consente il trasporto sicuro dei messaggi Session Initiation Protocol (SIP) e Real-time Transport Protocol (RTP) tramite TLS 1.2. Dalla versione 12.0 di CCE e nell'ambito della protezione dei dati in movimento, Cisco ha iniziato a supportare TLS 1.2 sulla maggior parte dei flussi di chiamate del contact center: Dip. voce in entrata e in uscita, multicanale ed esterna del database. Lo scopo di questo documento è la voce in entrata, in particolare la comunicazione tra Finesse e CTI Server.

Il server CTI supporta le seguenti modalità di connessione:

- Connessione protetta: Consente una connessione protetta tra il server CTI e i client CTI (Finesse, dialer, CTIOS e ctitest).
- Connessione protetta e non protetta (modalità mista): Consente connessioni protette e non protette tra il server CTI e i client CTI. Questa è la modalità di connessione predefinita. Questa modalità viene configurata quando si aggiornano le versioni precedenti a CCE 12.0(1).

Nota: Modalità non protetta non supportata.

Configurazione

CCE CTI Server Secure

Passaggio 1. Sulla stazione di lavoro amministrativa PCCE (AW), aprire la cartella **Unified CCE Tools** e fare doppio clic su **Peripheral Gateway Setup**.



Passaggio 2. Selezionare CG3A e fare clic su Modifica.

ICM Instances	Instance Components	44
Edit Delete	PG1A PG2A PG3A RoutetA	dit lete
To set up Administration Data Se	www.lDistributor.AWI.Router.Looper.Net	
Interface Controller (NIC), WebVi Web Setup tool. To set up Administration Client (C and Setup tool.	iew of Network Gateway components, use Xient AW), use the Administration Client Ins	the

Passaggio 3. Nelle proprietà del server CTI, fare clic su **Avanti**. Per informazioni sull'arresto del servizio **CG3A** durante l'installazione, selezionare **Sì**.

Passaggio 4. Nelle **proprietà dei componenti server CTI**, selezionare **Attiva modalità di sola protezione.** Prendere nota della **porta di connessione protetta (46030)**, in quanto nell'esercizio successivo sarà necessario configurare la stessa porta in Finesse. Fare clic su **Next** (Avanti).

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

Nota: La comunicazione protetta predefinita è 42030, tuttavia l'lab utilizzata per questo documento è 40630. Il numero di porta fa parte di una formula che include l'ID sistema ICM. Quando l'ID di sistema è 1 (CG1a), il numero di porta predefinito, in generale, è 42030.

Poiché l'ID di sistema nel lab è 3 (CG3a), il numero di porta predefinito è 46030.

Passaggio 5. In CTI Network Interface Properties, fare clic su Next. Controllare le informazioni di installazione e fare clic su Avanti.

Unified ICM/CCE PGSet	tup: cc-CG3A 🌅
Check Setup Information	
Setup has enough information to begin the configurat If you want to review or change and of the settings, - If satisfied, click Next to begin configuring the CTI Gal	ion operation. click Back. teway.
Current Settings:	
Setup Type: CTI Gateway, side A	<u>^</u>
Target Directory: C:\jicm	=
Configuration: PG node is pocealin1p CTI Gateway is simplexed DMP address is 3	
Unit address is 3	v
<	>
stalfshield	
<	Back Next > Cancel

Passaggio 6. Fare clic su Finish (Fine) come mostrato nell'immagine.

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

Passaggio 7. Fare clic su **Exit Setup** (Esci dall'installazione) e attendere la chiusura della finestra di installazione, come mostrato nell'immagine.

ICM Instances		Instance Compone	nts
cc	Add	AW CG24	Add
		LoggerA	
	Edit	PG1A PG2A	Edit
	Duble	PG3A	Datas
	Delete	PiouteiA	Delete
'o set up Administratio nterface Controller (NI Veb Setup tool.	n Data Server (I C), WebView or	Distributor AW/J. Router, Network Gateway comp	Logger, Network conents, use the
⁷ o set up Administratio nterface Controller (NI Veb Setup tool. rid Setup tool.	n Data Server ([C], WebView or n Client (Client A	Distributor AW), Router, Network Gateway comp W), use the Administrati	Logger, Network conents, use the on Client Installer
To set up Administratio nterface Controller (NI Web Setup tool. To set up Administratio and Setup tool. The Instance cc cann	m Data Server ([C], WebView or m Client (Client A ot be deleted be	Distributor AW), Router, Network Gateway comp (W), use the Administrati cause it has component	Logger, Network conents, use the on Client Installer s set up by the
To set up Administration Interface Controller (NI Web Setup tool. To set up Administration and Setup tool. The Instance cc cann Web Setup or Administ o remove those comp ietup.	n Data Server ([C], WebView or n Client (Client A ot be deleted be tration Client Set onents before de	Distributor AW), Router, Network Gateway comp (W), use the Administrati cause it has component up tool. You must use th sleting the instance in Po	Logger, Network conents, use the on Client Installer s set up by the e applicable tool sripheral Gateway

Passaggio 8. Sul desktop PCCEAllin1, fare doppio clic su Unified CCE Service Control.

Passaggio 9. Selezionare Cisco ICM cc CG3A e fare clic su Start.

Finesse Secure Configuration

Passaggio 1. Aprire un browser Web e passare a Amministrazione Finesse.

Passaggio 2. Scorrere verso il basso fino alla sezione **Contact Center Enterprise CTI Server Settings** (Impostazioni server CTI Contact Center Enterprise) come mostrato nell'immagine.

Contact Center Enter	erprise CTI Server Se	ettings	
Note: Any changes made to Contact Center Enterpris	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*	42027	B Side Port	
Peripheral ID*	5000		
Enable SSL encryption Save Reven	rt 🗌		

Passaggio 3. Nell'esercizio precedente, modificare la porta laterale A per la porta di comunicazione protetta configurata su CG3A: **46030**. Selezionare **Abilita crittografia SSL** e fare clic su **Salva**.

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		

Nota: Per eseguire il test della connessione, è necessario riavviare prima Finesse Tomcat Service o il server Finesse.

Passaggio 4. Uscire dalla pagina Amministrazione Finesse.

Passaggio 5. Aprire una sessione SSH con Finesse.

Passaggio 6. Nella sessione SSH FINESSEA, eseguire il comando:

riavvio del sistema utils

Quando viene richiesto se si desidera riavviare il sistema, immettere yes.

```
<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...
```

Genera certificato PG agente (server CTI)

Cisco CertUtils è un nuovo strumento rilasciato su CCE versione 12. È possibile utilizzare questo strumento per gestire tutti i certificati CCE per la voce in entrata. In questo documento vengono

usati questi CiscoCertUtils per generare le richieste di firma di certificati (CSR) dei gateway periferiche (PG).

Passaggio 1. Eseguire questo comando per generare un certificato CSR: **CiscoCertUtil** /generateCSR



Fornire le informazioni richieste, ad esempio:

Nome paese: STATI UNITI

Nome provincia: MA

Nome località: BXB

Nome organizzazione: Cisco

Unità organizzativa: CX

Nome comune: PCCEAllin1.cc.lab

Email: jdoe@cc.lab

Password di verifica: Treno1ng!

Nome società facoltativo: Cisco

Il certificato e la chiave host sono memorizzati nei percorsi C:\icm\ssl\certs e C:\icm\ssl\keys.

Passaggio 2. Passare alla cartella **C:\icm\ssl\certs** e verificare che il file **host.csr** sia stato generato.

Ottieni certificato CSR Firmato da una CA

Dopo la generazione, i certificati CSR devono essere firmati da un'autorità di certificazione di terze parti. In questo esercizio, l'autorità di certificazione Microsoft installata nel controller di dominio viene utilizzata come autorità di certificazione di terze parti.

Verificare che il modello di certificato utilizzato dalla CA includa l'autenticazione client e server, come illustrato nell'immagine quando si utilizza la CA Microsoft.

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.	tificate Templates More Actions b Server More Actions	(DC.cc.lab)
Application Policies	Edit Application F	"olicies Extension
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. Application policies:
Edt Description of Application Policies:		Any Purpose Attestation Identity Key Certificate Education Identity Key Certificate Education Identity Key Certificate
Server Authentication	Add	Code Signing CTL Usage Digital Rights Directory Service Email Replication Disallowed List Document Encryption Document Encryption Document Signing Domain Name System (DNS) Server Trust Dynamic Code Generator
OK Cancel Apply Help		OK Cancel

Passaggio 1. Aprire un browser Web e passare alla CA.

Passaggio 2. In Servizi certificati Microsoft Active Directory, selezionare Richiedi certificato.

	_ 0 X
🗲 💿 🖉 https://dc.ec.lab/certsrv/en-us/ 🖉 🖌 🔒 🖒 🏉 Microsoft Active Directory 🗴	↑ ★ 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. B certificate, you can verify your identity to people you communicate with over the Web, sign and e messages, and, depending upon the type of certificate you request, perform other security tasks.	y using a ncrypt
You can also use this Web site to download a certificate authority (CA) certificate, certificate chair certificate revocation list (CRL), or to view the status of a pending request.	n, or
For more information about Active Directory Certificate Services, see <u>Active Directory Certificate</u> Documentation.	Services
Select a task: Request a certificate View the status of a pending certificate request Download a CA certificate, certificate chain, or CRL	

Passaggio 3. Selezionare l'opzione Advanced certificate request.

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:					_

Passaggio 4. Nella **richiesta di certificato avanzata,** copiare e incollare il contenuto del certificato CSR di PG Agent nella casella **Richiesta salvata**.

Passaggio 5. Selezionare il modello **Server Web** con l'autenticazione client e server. In laboratorio, il modello CC Web Server è stato creato con l'autenticazione client e server.

To submit a sav Saved Reques	ved request to the CA, part t 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/SJojYzBGnHs J75nKDoyAh7C+F0u9tmg260 rArT900dxJem END CERTIFICATE RE <	rqH1509jMcZ3uZrciC SkUAZqin/56HjuGb4h c38yo1P/I7UsueE3OR SZaOZ3k9Wo5QzUTPmd CQUESTsna	* * *
Certificate Temp	ate:		
Ľ	CC Web Server	~	_
Additional Attribu	ites:		
Attributes:			_

Passaggio 6. Fare clic su Sottometti.

Passaggio 7. Selezionare **Base 64 encoded** (Codificato Base 64) e fare clic su **Download Certificate** (Scarica certificato), come mostrato nell'immagine.

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

Certificate Issued

The certificate you requested was issued to you.

○ DER encoded or ● Base 64 encoded

Download certificate Download certificate chain

Passaggio 8. Salvare il file e fare clic su OK. Il file viene salvato nella cartella Download.

Passaggio 9. Rinominare il file host.cer (facoltativo).

Passaggio 10. È inoltre necessario generare un certificato radice. Tornare alla pagina Certificato CA e selezionare Scarica certificato CA, catena di certificati o CRL. È sufficiente eseguire questa operazione una sola volta, poiché il certificato radice sarà lo stesso per tutti i server (PG Agent e 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 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> <u>View the status of a pending certificate request</u> <u>Download a CA certificate, certificate chain, or CRL</u>

Passaggio 11. Fare clic su Base 64 e selezionare Scarica certificato CA.

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 (corbist 64)
Encoding method:
ODER ⊛Base 64
Install CA certificate
Download CA certificate
Download CA certificate chain
Download latest base CRL
Download latest delta CRL

Passaggio 12. Fare clic su Salva file e selezionare **OK**. Il file verrà salvato nel percorso predefinito **Download**.

Importa certificati firmati CA CCE PG

Passaggio 1. In PG Agent passare a C:\icm\ssl\certs e incollare qui i file radice e PG Agent firmati.

Passaggio 2. Rinominare il certificato host.pem in c:\icm\ssl\certs come selfhost.pem.

Passaggio 3. Rinominare host.cer in host.pem nella cartella c:\icm\ssl\certs.

Passaggio 4. Installare il certificato radice. Al prompt dei comandi, eseguire questo comando: CiscoCertUtil /install C:\icm\ssl\certs\rootAll.cer



Passaggio 5. Installare il certificato firmato dall'applicazione che esegue lo stesso comando: CiscoCertUtil /install C:\icm\ssl\certs\host.pem



Passaggio 6. Ciclare il PG. Aprire Unified CCE Service Control e riaccendere Cisco ICM Agent PG.

Genera certificato Finesse

Passaggio 1. Aprire il browser Web e passare a Finesse OS Admin.

Passaggio 2. Accedere con le credenziali di Amministratore del sistema operativo e selezionare **Security > Certificate Management**, come mostrato nell'immagine.



Passaggio 3. Fare clic su Generate CSR (Genera CSR) come mostrato nell'immagine.



Passaggio 4. In Genera richiesta di firma certificato, utilizzare i valori predefiniti e fare clic su Genera.

Generate Certificate Si	gning Request
Generate 🖳 Close	
-	
Status	
Warning: Generating	g a new CSR for a specific certificate type will overwrite the existing CSR for that type
-Generate Certificate S	iigning Request
Certificate Purpose**	tomcat v
Distribution*	FINESSEA.cc.lab
Common Name*	FINESSEA.cc.lab
Subject Alternate Nan	nes (SANs)
Parent Domain	cc.lab
Key Type**	RSA
Key Length*	2048 🗸
Hash Algorithm*	SHA256 V
	/
Generate Close	
	d have
· indicates require	
is RSA.	cate Purpose ending with "ECDSA" is selected, the certificate/key type is Elliptic Curve (EC). Otherwise, it

Passaggio 5. Chiudere la finestra Genera richiesta di firma certificato e selezionare Scarica CSR.

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

Passaggio 6. Nello scopo del certificato, selezionare tomcat e fare clic su Download CSR.

Download Certificate Signing Request
Download CSR The Close
Status Certificate names not listed below do not have a corresponding CSR Download Certificate Signing Request Certificate Purpose* tomcat v Download CSR Close indicates required item.
C States All definitions and Construction

Passaggio 7. Selezionare Save File (Salva file) e fare clic su OK, come mostrato nell'immagine.

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 gutor	nationally for thesince this north how on.	
	OK Cancel	

Passaggio 8. Chiudere la finestra **Scarica richiesta di firma certificato**. Il certificato viene salvato nel percorso predefinito (Questo PC > Download).

Passaggio 9. Aprire Esplora risorse e individuare la cartella. Fare clic con il pulsante destro del mouse sul certificato e rinominarlo: **finessetomcat.csr**

Firma certificato Finesse da una CA

In questa sezione viene utilizzata la stessa CA Microsoft utilizzata nel passaggio precedente come CA di terze parti.

Nota: Verificare che il modello di certificato utilizzato dalla CA includa l'autenticazione client e server.

Passaggio 1. Aprire un browser Web e passare alla CA.

Passaggio 2. In Servizi certificati Microsoft Active Directory, selezionare Richiedi certificato.

C C Microsoft Active Directory ×
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

Passaggio 3. Selezionare l'opzione Advanced certificate request come mostrato nell'immagine.



Passaggio 4. Nella **richiesta di certificato avanzata**, copiare e incollare il contenuto del certificato CSR Finesse nella casella **Richiesta salvata**.

Passaggio 5. Selezionare il modello di server Web con l'autenticazione client e server. In questa esercitazione il modello CC Web Server è stato creato con l'autenticazione client e server.

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 box.	Copy and paste the of the expected CSI	contents ^{PK(} R file
Saved Request:			_
Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):	3LhnlD3GsLbIYivb7lbshW gWL/H3DR1nRpJtLKfnLGgX +L3E0yNQ+W9/SJojY2BGnH J75nRDoyAh7C+F0u9tmg26 rArT900dxJem END CERTIFICATE RJ <	fqH1509jMcZ3uZrciC / SkUAZqin/56HjuGb4h k38yo1P/17UsueE30R DZaOZ3k9Wo5QzUTPmd EQUESTsna	
Certificate Temp	ate: CC Web Server		-
Additional Attrib	utes:		_
Attributes:		-1	
		Submit >	-

Passaggio 6. Fare clic su Sottometti.

Passaggio 7. Selezionare **Base 64 encoded** (Codificato Base 64) e fare clic su **Download certificate** (Scarica certificato), come mostrato nell'immagine.

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

Passaggio 8. Salvare il file e fare clic su OK. Il file viene salvato nella cartella Download.

Passaggio 9. Rinominare il file finesse.cer.

Importa certificati firmati radice e applicazione Finesse

Passaggio 1. In un browser Web aprire la pagina **Finesse OS Admin** e passare a **Sicurezza** > **Gestione certificati**.

Passaggio 2. Fare clic sul pulsante **Carica certificato/catena di certificati** come mostrato nell'immagine.

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

Passaggio 3. Nella finestra popup selezionare tomcat-trust for Certificate Purpose.

Passaggio 4. Fare clic sul pulsante **Sfoglia...** e selezionare il file del certificato radice da importare. Quindi, fare clic sul pulsante **Apri**.

Passaggio 5. Nella descrizione, scrivere qualcosa come **tomcatrootcert** e fare clic sul pulsante **Upload**, come mostrato nell'immagine.

Upload 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	٦
Certificate Purpose*	tomcat-trust v	
Description(friendly name)	tomcatrootcert	
upidad File	Browse rootAll.cer	
Upload Close		
(i) *- indicates required its	ım.	
t		>

Passaggio 6. Attendere fino a quando non viene visualizzata la schermata **Operazione riuscita**: Messaggio di **caricamento certificato** per chiudere la finestra.

Verrà richiesto di riavviare il sistema, ma prima continuare con il caricamento del certificato firmato dell'applicazione Finesse, quindi riavviare il sistema.

🛈 🚯 https://finessea.cc.lab:	8443/cmplatform/certificateUpload.do		⊠ ☆	≡
Upload Certificate/Certificat	te chain			
Dipload 🖳 Close				
Status Success: Certificate Uplow Restart the node(s) using	ded the CLI command, "utils system restart".			
Upload Certificate/Certifica	ate chain			_
Certificate Purpose*	tomcat-trust	~		
Description(friendly name) Upload File	Browse No file selected.			
Upload Close				
i *- indicates required item	r.			
<				>

Passaggio 7. Fare clic sul pulsante **Carica catena di certificati/certificati** per dedicare più tempo all'importazione del certificato dell'applicazione Finesse.

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

Passaggio 8. Nella finestra popup selezionare tomcat for Certificate Purpose.

Passaggio 9. Fare clic sul pulsante **Sfoglia...** e selezionare il file firmato Finesse CA, **finesse.cer**. Quindi, fare clic sul pulsante **Apri**.

Passaggio 10. Fare clic sul pulsante Upload.

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

Passaggio 11. Attendere finché non viene visualizzata la schermata **Operazione riuscita**: Messaggio **di certificato caricato**.

Viene nuovamente richiesto di riavviare il sistema. Chiudere la finestra e continuare a riavviare il sistema.

Verifica

Attualmente non è disponibile una procedura di verifica per questa configurazione.

Risoluzione dei problemi

Al momento non sono disponibili informazioni specifiche per la risoluzione dei problemi di questa configurazione.